Sardar Vallabhbhai Patel
National Police Academy,
Hyderabad

Cyber Crime Investigation Manual

Volume - III

CYBER X

Foreword

Cybercrime is one of the biggest challenges we face today. In the past decade, as technology has grown at an incredible pace, so has our dependence on the internet. While this has improved our lives in countless ways, it has also created new opportunities for criminals. From disrupting critical infrastructure to stealing financial assets and sensitive data, cybercrimes can cause serious harm. What makes it even more alarming is how easy and rewarding these crimes can be, often happening across borders without much cost.

Technology has brought great opportunities but also increased our vulnerability to cyber threats. As cybercrimes grow more frequent and complex, the lack of trained professionals to handle such cases effectively is a major challenge. The shortage of skilled officers leads to delays and unresolved cases, highlighting the need for stronger efforts to build a capable workforce to combat these threats efficiently and on time.

At the Sardar Vallabhbhai Patel National Police Academy (SVPNPA), we've been working hard to bridge this gap. Through our CyberX unit (previously NDCRTC), we've trained over 15,000 officers and staff since 2015. These officers are now better equipped to handle the complexities of cybercrime investigations.

To further support our investigators, the CyberX unit has developed five comprehensive manuals. These manuals are designed to be practical, user-friendly guides to help officers navigate the often-complicated process of cybercrime investigations. They focus on bridging the knowledge and skill gaps, offering clear and actionable insights.

I strongly encourage all investigators to use these manuals to their full advantage. They cover the latest tools and techniques, providing the confidence and clarity needed to take on even the most challenging cases. Together, we can make significant progress in the fight against cybercrime and ensure justice in this ever-changing digital world.

Amit Garg, IPS
Director
Sardar Vallabhbhai Patel
National Police Academy

Contributors:

Mohammed Arif Ali Khan:

Mohammed Arif Ali Khan is working as Chief Forensic Analyst at SVPNPA. He has a decade long experience in capacity building in cyber-crime investigation and digital forensics. He has also worked with the Cyber Crimes Cell, CID Hyderabad and specializes in solving cases related to online harassment, job frauds, fake websites, etc. His interest in Cyber Security was rewarded by companies like Indeed.com, AT&T, Mail.ru for finding security vulnerabilities in their services.

Parmesh Naik:

Parmesh Naik is Senior Forensic Analyst at SVPNPA with over eight years of experience in training law enforcement personnel, specializing in OSINT, Linux forensics, and Malware analysis. His profound understanding of digital forensics is demonstrated through the innovative software tools he has developed, which have become essential in law enforcement investigations.

Shaik Ghousal Mubarak:

Shaik Ghousal Mubarak is working as a Senior Forensic Analyst at SVPNPA. He holds a vast experience of 10 years in the domain of cybercrime investigation.
He previously worked as a cyber-crime consultant at CID Cyber Crimes Hyderabad. He is holding a PG-Diploma in Advance Computing and a B-Tech in Computer Science. His area of interest is Financial Fraud Investigations. Additionally, he is a regular guest speaker at various Police academies, Central Agencies, and other institutions.

Nitin Sharma:

Nitin Sharma is working as the Lead Forensic Analyst at SVPNPA, he imparts training to law enforcement officers and specializes in areas such as Internet Crime Investigation, Cryptocurrency Investigation & Digital Forensics. He holds a PG diploma in Cyber Law & Cyber Forensics from NLSIU Bangalore and an M-Tech in Cyber Security from Gujarat Forensic Sciences University. His extensive experience includes assisting field officers in cases ranging from Internet crimes to Dark Web & Cryptocurrency investigations for agencies like NIA, NCRB, Punjab Police, and others.

Aishwarya Tiwari:

Aishwarya Tiwari is a Forensic Analyst in NDCRTC with four years of specialized experience in training law enforcement agencies and conducting research in cryptocurrency investigation. Aishwarya's expertise is further solidified by a CHFI Certification, a CEH Certification from EC Council, and a Blockchain and Cryptocurrency Diploma from Oxford, London. Aishwarya, continues to make

significant contributions to cyber forensics and security, driven by a steadfast commitment to innovation and excellence in protecting digital assets and mitigating cyber threats.

Priya Ghurde:

Priya Ghurde currently holds the position of 'Cyber Investigation and Forensic Specialist' at the Indian Cyber Crime Coordination Centre (I4C), cryptocurrency-related offenses. Prior to her tenure at I4C, she served as Lead Forensic Analyst at SVPNPA. She has total experience of six years in the field of Cyber Crime Investigation and Cyber Security. She imparts training to law enforcement officers and specializes in areas such as Internet Crime Investigation, Dark web Monitoring & Digital Forensics. She holds B-Tech Degree in Information Technology along with certifications including Cyber Shiksha from Microsoft and CHFI from EC-Council. Her extensive experience includes assisting field officers in cases ranging from Dark Web related investigations to Digital Forensic Investigations for agencies like NIA, NCRB, Punjab Police, and others.

Ashmit Sharma:

Ashmit Sharma, presently serving as Scientist 'B' (Forensic Electronics) at CFSL, DFSS, MHA, GoI (Bhopal) previously as Lead Forensic Analyst at SVPNPA. He is a seasoned professional with expertise in digital forensics. Armed with B-Tech in ECE and an MSc in Forensic Science, Ashmit has honed his skills across various prestigious organizations including RFSL (NR, Dharamshala, HP), CFL (State Crime Branch, Haryana), and CFDML(SFIO). His dedication to continuous learning is evident through his publication of two international papers, focusing on smartphone and WhatsApp vulnerabilities, further establishing his reputation as an avid learner in the field

Mohammed Nazim:

Mohammed Nazim is working as a Forensic Analyst at SVPNPA, equipped with a Computer Science Engineering background and accreditation as an Information Security Management Systems Auditor (ISO 27001). Specializing in CDR/IPDR analysis and fueled by a fervour for Internet Governance, Nazim extends his expertise generously to esteemed institutions such as police academies, NIA, Central Detective Training Institute, and ESCI

Contents

1. Digital Forensics

2. Digital Payment Frauds

3. OSINT and Social Media Analysis

1. Digital Forensics

1. Basics of Disk Forensics

1.1 Concept of Disk Forensics

Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc. The process of Disk Forensics includes Identification of digital evidence, Seizure & Acquisition of the evidence and authentication of the evidence.

Main process of Disk Forensics involves the following actions:

- **Identification** (recognize incident, requirement for action, intelligence for investigation)
- Authentication
- **Preparation** (intelligence for search, adequate toolkits, operational briefing, task allocation)
- **Securing and Evaluating the Scene** (ensure safety, confirm computer equipment present and recognize further possibilities, secure equipment, identify and protect evidence, conduct interviews)
- **Documenting the Scene** (create a permanent record of the scene by means of photography and note taking, document condition and location of computers and related components whether these are to be removed or not, mark and label artefacts, use seals and sealable containers, evidence bags)
- **Evidence Collection** (cater for computer devices found to be switched on or off, attending to order of volatility (see Glossary), collect computer hardware and media while preserving evidential value, obtain analogue evidence such as passwords, handwritten notes, computer manuals, printouts)
- **Packaging, Transportation and Storage** (protect equipment and media during transfer avoiding extreme temperatures, physical impact and vibration, static electricity and magnetic sources, establish procedures for reception and storage of machines and media, maintain chain of custody, inventory for storage in secure area free of contaminants)
- **Initial Inspection** (identification of devices, external and internal physical examination of computers, tool selection and expectations)
- **Forensic Imaging and Copying** (e.g. for hard drive – removal of physical disk from computer, digital preview and capture using physical or logical disk acquisition, with write blockers, followed by return of original media to evidence custodian)
- **Forensic Examination and Analysis** (use forensic techniques and tools for analysis and processing including: creation of cryptographic hash values and filtering with hash libraries, file viewing, file exporting and expansion of compound files (e.g. email), extraction of metadata, searching and indexing)
- **Presentation and Report** (document procedures, analysis and findings, use log files, bookmarks and notes made during the examination, make conclusions, prepare exhibits suitable for court)

1.2 Digital Evidence

Computer forensics involves acquiring digital evidence from a computer hard drive, a mobile phone, a tablet or PDA, or other storage media (like CD/DVD, USB thumb drive) among other places, in a systematic way.

'Digital evidence' is any kind of file or data/metadata that is presented in digital format and could be used for trial in court of law.

a) Digital Evidence Types

There are two main types of digital evidences with respect to who has created them. i.e., User-created data and Machine/ Network Created Data.

User-created data includes anything created by a user using a digital device. It includes the following and more:

- Text files (e.g., MS Office documents, IM chat, bookmarks), spreadsheets, database, and any text stored in digital format, Audio and video files, Digital images, Webcam recordings (digital photos and videos), Address book and calendar, Hidden and encrypted files (including zipped folders) created by the computer user, Previous backups (including both cloud storage backups and offline backups like CD/DVDs and tapes), Account details (username, picture, password), E-mail messages and attachments (both online and client e-mails as Outlook), Web pages, social media accounts, cloud storage, and any online accounts created by the user.

Machine/network-created data includes any data which is auto generated by a digital device. It includes the following and more:

- Computer logs. These include the following logs under Windows OS: Application, Security, Setup, System, Forward Events, Applications, and Services Logs.
- Router logs, including third-party service provider (e.g., Internet service providers (ISPs) commonly store users' account web browsing history logs)
- Configuration files and audit trails
- Browser data (browser history, cookies, download history)
- Instant messenger history and buddy list (Skype, WhatsApp)
- GPS tracking info history (from devices with GPS capability)
- Device Internet protocol (IP) and MAC addresses in addition to the IP addresses associated with a LAN network and the broadcast settings,
- Applications history (e.g., recently opened file on MS Office) and Windows history,
- Restore points under Windows machines
- Temporary files
- E-mail header information
- Registry files in Windows OS
- System files (both hidden and ordinary)
- Printer spooler files
- Hidden partition and slack space (can also contain hidden user information)

- Bad cluster
- Paging and hibernation files
- Memory dump files
- Virtual machines
- Surveillance video recordings

1.3 File system and data storage

File systems provide a mechanism for the operating system to keep track of files in a partition. Before user can use a storage device to store data and install applications and OS, user need to initialize it first through writing the data structures of the file system to the drive. Windows OS uses either the FAT or the NTFS file system to install itself on hard drives.

File system analysis examines data in a volume (i.e., a partition or disk) and interprets them as a file system. There are many end results from this process, but examples include listing the files in a directory, recovering deleted content, and viewing the contents of a sector.

a) FAT

The File Allocation Table (FAT) file system is one of the most simple file systems found in common operating systems. FAT is the primary file system of the Microsoft DOS and Windows 9x operating systems, but the NT, 2000, and XP line has defaulted to the New Technologies File System (NTFS), which is discussed later in the book. FAT is supported by all Windows and most Unix operating systems and will be encountered by investigators for years to come, even if it is not the default file system of desktop Windows systems. FAT is frequently found in compact flash cards for digital cameras and USB "thumb drives. "Many people are familiar with the basic concepts of the FAT file system but may not be aware of data hiding locations, addressing issues, and its more subtle behaviors.

The layout of the data is slightly different in FAT12/ 16 and FAT32. In FAT12/ 16 the beginning of the data is reserved for the root directory, but in FAT32 the root directory can be anywhere in the data area (although it is rare for it to not be in the beginning of the data area). The dynamic size and location of the root directory allows FAT32 to adapt to bad sectors in the beginning of the data are and allows the directory to grow as large as it needs to. The FAT12/ 16 root directory has a fixed size that is given in the boot sector. The starting address for the FAT32 root directory is given in the boot sector, and the FAT structure is used to determine its size. Figure 1.1 shows how the various boot sector values are used to determine the layout of FAT12/16andFAT32 file systems.

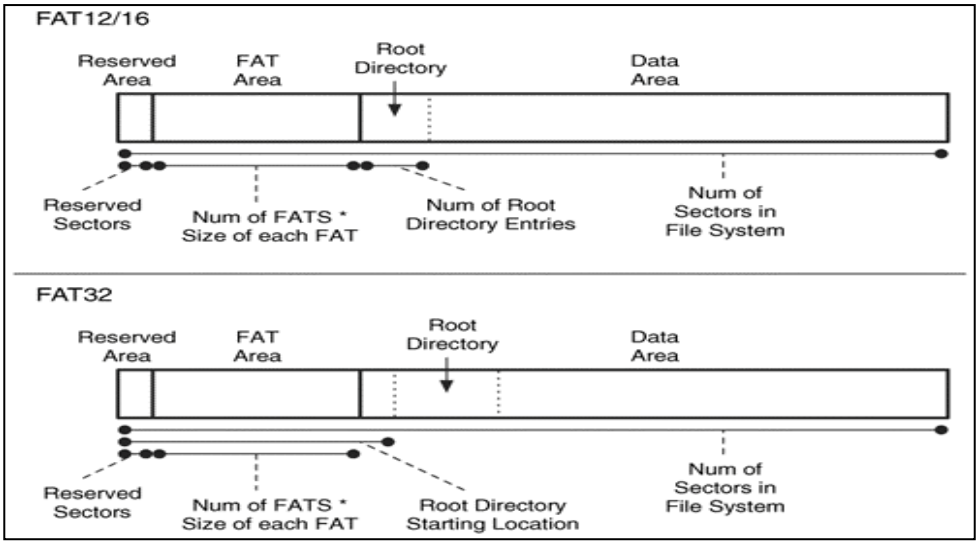


Figure: FAT file system layout and data from the boot sector that is used to calculate the locations and sizes

b) NTFS

NTFS is a proprietary file system developed by Microsoft for its modern Windows operating system; formatting a volume with NTFS results in the creation of several metadata files such as the master file table ($MFT), $Bitmap, $LogFile and others, which contain information about all the files and folders on the NTFS volume.

Figure: Sample formatted new technology file system volume

In the NTFS file system, each file stored within it is composed of a set of data streams: the primary stream is the one that holds the actual data a user sees when opening a file. The other stream is called the alternative data stream (ADS). Digital forensics examiners should search within data streams of all files stored on an NTFS partition, as they can contain hidden data.

2. Live Forensics

2.1 Introduction - Live Forensics

Live forensics considers the value of the data that may be lost by powering down a system and collects it while the system is still running. The other objective of live forensics is to minimize impacts to the integrity of data while collecting evidence from the suspect system. Live Forensics is a methodology for extracting forensically sound evidence from "live" system. According to traditional forensics procedure, power plug is pulled to switch off the system when the system is in the running mode. But in live forensics, before pulling the cord we collect information such as details in memory, running process, network connection etc. In Live Forensic volatile data that may be lost by a power down is collected from a running system.

❖ Why Live Forensics

Live forensics considers the value of the data that may be lost by powering down a system and collects it while the system is still running. It is a methodology, which advocates extracting "live" system data before pulling the cord to preserve memory, process, and network information that would be lost with traditional forensic approach

- Extract volatile forensic data that would be lost on power off
- Will have minor impacts to the underlying machine's operating state
- Often used in incident handling to determine if an event has occurred
- May or may not proceed a full traditional forensic analysis

Data on a system has an order of volatility. Live Forensics focuses on extracting and examination of the volatile forensic data that would be lost on power off. Data from the memory, swap space, network processes, and running systems processes is the most volatile and will be lost on system reboot. The goal live forensics is to extract and preserve the volatile data on a system while, to the extent possible, otherwise preserving the state of the system. When powering down a computer system, a lot of volatile information is lost. So, Live Forensics has become an important part of digital forensic investigations. This information will not be available for further analysis, although it may contain valuable clues regarding the incident, and there is sometimes no other way to obtain it other than collecting it on the running system.

❖ Live / Volatile Data

The information that can be collected during Live Response includes the system date and time, a list of current network connections and open TCP/UDP ports, a list of running processes, system users, the names of the loaded kernel modules, a list of recently used/open files, the information regarding network connections and ports, installed software's, event logs, open files and dlls, registry, Memory, images of entire disks, deleted files.

- System time
- Logged-on user(s)
- Open files
- Network information
- Network connections
- Process information
- Process to port mapping
- Process memory
- Network Status
- Clipboard contents
- Service/ driver information
- Command history

- Mapped drives
- Shares

❖ **Nonvolatile Information**

- Event logs,
- security log of the system,
- system information
- Windows Registry
- Installed software's,
- network details
- Internet history

❖ **Live Forensics before Pulling the Power Plug**

Before pulling the Power Plug if the machine is in running mode at the scene of crime, then first live forensics must be performed. Otherwise, all crucial information available in the suspect's system will be lost forever. And the information collection by live forensic is very crucial as it can provide useful hints in the offline forensics.

2.2 Acquisition of RAM Dump (Acquiring Volatile Memory)

Data is volatile when it will be lost when a device is switched off or rebooted. Volatile data may be overwritten due to normal use (e.g., when closing a particular application on a PC, the reserved data space will vanish from RAM memory, permitting other applications to utilize its space for activity). The process of capturing data from volatile memory is known as dumping.

Capturing and analyzing volatile memory is more difficult than the traditional acquisition of hard drives because capturing a live memory requires specialized software tools. As well as analyzing volatile data forensic image files needs specialized software, as RAM does not store data in the similar way as hard drives do.

Volatile memory can be found in other devices along with computers; for example, networking devices like routers and switches also have volatile data stored in their logs.

Following is the list of information which can be found in RAM:

- Cryptographic keys
- Processes running
- Executed console commands
- Clipboard contents
- Network information
- Decrypted contents
- Registry hives
- Text files and images
- Deleted files
- Web browsing logs
- Open/active registry keys
- Internet account passwords (e.g., e-mail, social media, and cloud storage)
- Instant messages
- Exploit-related information

- Malware (rootkits and Trojan horses)
- Evidence of activity not typically stored on the local hard disk

❖ **RAM Dump Using FTK Imager**

FTK Imager is a Windows acquisition tool and it can be downloaded directly from Access Data web site free of cost. FTK Imager available in two types "FTK Imager" and "FTK Imager Lite". Both the software has same features and functions. Only difference is lite version can be run from a pendrive or External Source, so Setup is not required for this version.

❖ **Challenges faced during RAM Dump Acquisition**

Acquiring volatile memory might face a couple of challenges by the forensic examiners. The following are some scenarios.

i) Windows Is Locked

We might come across a running computer with a login screen (locked computer). It is advisable to perform a hard shutdown. However, we can bypass the Windows login page with no reboot by using some tools/techniques to avoid losing RAM contents:

- Put computer in Hibernation mode, it will allow hibernate file to store in Disk.

ii) Administrative Privileges

Most of the RAM Dump capturing software tools needs administrative privileges in order to work. If target PC is running with limited user permission (e.g., user account) it would be challenging to capture RAM Dump.

iii) Capturing Tool Footprint

The RAM Dump capturing tool will also leave some traces on the target machine. This means some data may be overwritten as a result of acquiring live memory. Traces of capture tool can be justified, if documented properly.

2.3 Importance of Pulling the Plug

A live system will have numerous background processes running which are continually reading and writing data to and from hard drive. When forensic examiner decides to shut down the system, pulling the plug might be best suitable option. Because normal shutdown will start a chain of actions, that involve writing a lot of data to the hard drive, possibly overwriting important evidence.

Removing power plug will "freeze" the system in its current state, making sure that the data on the system is no longer modified. But before pulling the plug one must ensure to capture the RAM since all the data stored in RAM will be lost once, we pull out the plug.

2.4 Analysis of RAM Dump

The most important principle to remember for a forensic examiner is **"Whatever works is always in the memory and whatever happens is always in the memory".** Hence it is very necessary to capture and analyze memory dumps. It gives an examiner clearer picture about the current state of the system. There are many tools available in market to perform RAM Dump analysis which extracts certain type of information from the dump. Here we are going to explain use of '**Bulk Extractor'** for RAM Dump analysis.

❖ Analysis RAM dump using Bulk Extractor

Bulk extractor is a computer forensics tool that scans a disk image, a file or a directory of files and extracts useful information without parsing the file system or file system structures. The results can be easily inspected, parsed or processed with automated tools.

Bulk Extractor also creates a histogram of features that it finds, as features that are more common tend to be more important. The program can be used for law enforcement, defense, intelligence and cyber-investigation applications.

Bulk Extractor now creates an output directory that includes:

- **ccn.txt** -- Credit card numbers
- **ccn_track2.txt** -- Credit card "track 2″ information
- **domain.txt** – Internet domains found on the drive, including dotted-quad addresses found in text.
- **email.txt**–Email addresses
- **ether.txt** – Ethernet MAC address found through IP packet carving of swap files and compressed system hibernation files and file fragments.
- **exitf.txt** – EXIFs from JPEGs and video segments. This feature file contains all of the EXIF fields, expanded as XML records.
- **find.txt** – The results of specific regular expression search requests.
- **ip.txt** – IP addresses found through IP packet carving.
- **telephone.txt** – US and international telephone numbers.
- **url.txt** – URLs, typically found in browser cache, email messages and pre-compiled into executables.
- **url_searches.txt** – A histogram of terms used in Internet searches from services such as Google, Bing, Yahoo and others.
- **wordlist.txt** – A list of all "words" extracted from the disk, useful for password cracking.
- **wordlist_*.txt** – The wordlist with duplicates removed, formatted in a form that can be easily imported into a popular password-cracking program.
- **zip.txt** – A file containing information regarding every ZIP file component found on the media. This is exceptionally useful as ZIP files contain internal structure and ZIP is increasingly the compound file format of choice for a variety of products such as Microsoft Office.

For each of the above, two additional files may be created:

- ***_stopped.txt** – Bulk Extractor supports a stop list, or a list of items that do not need to be brought to the user's attention. However rather than simply suppressing this information, which might cause something critical to be hidden, stopped entries are stored in the stopped files.
- ***_histogram.txt** – Bulk Extractor can also create histogram of feature. This is important, as experience has shown that email addresses, domain names and other information that appear more frequently on a hard drive or in a cell phone's memory can be used to rapidly create a pattern of life report.

2.5 Hiberfile, Swapfile and Pagefile

Swapfile.sys, Hiberfil.sys, and Pagefile.sys are three important system files required for the proper functioning of the Windows OS. The default location of these files is in system drive (usually the C:\ drive). All three files will be always hidden in the system.

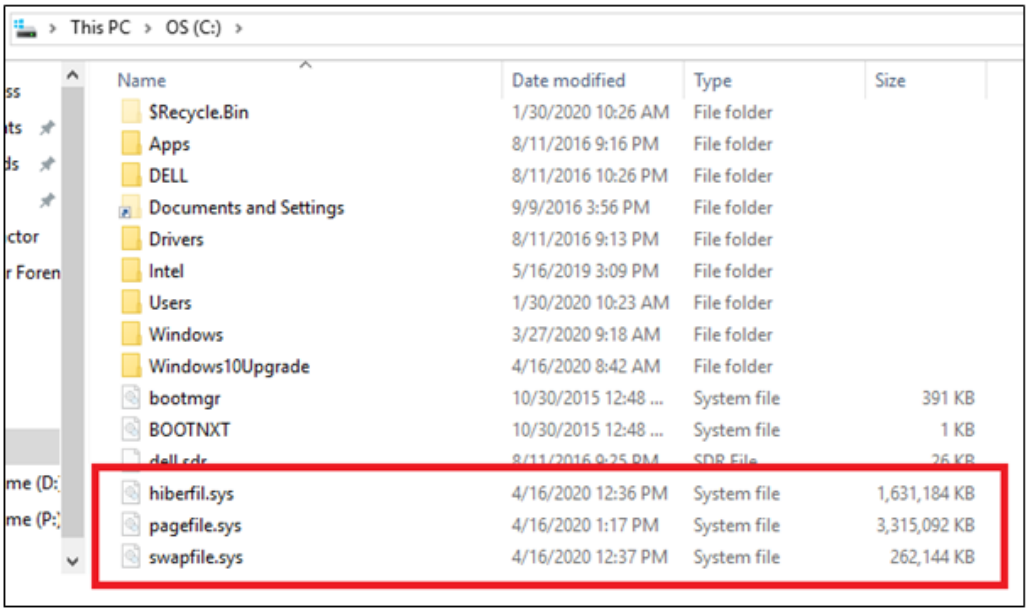


Figure: Hiberfile, Pagefile, Swapfile

❖ Hiberfil.sys

This is a file used by Windows to enable the hibernation feature; the approximate size of this file is about 3/4th of system RAM. The hibernation file in earlier versions of Windows (e.g., 7 and Vista) stored kernel session, device drivers, and application data while in modern versions of Windows (like 8 and 10) it stores only the kernel session and device drivers, making it notably less in size.

hiberfil.sys can store a pile of important information about the running machine. Following tool can investigate the hiberfil.sys file:

- **Volatility**, free and open source tool: *www.volatilityfoundation.org*

❖ Pagefile.sys

Forensic examiners should not ignore the importance of virtual memory, as this file can hold important information shifted from RAM. For example, fragments of decrypted files can still reside there, and encryption keys or passwords (or a fragment of it) can also be found here. The pagefile.sys is a hidden system file, it resides by default at %SystemDrive%\pagefile.sys; however, a user can change its default location.

Nowadays capacity of the physical memory is increasing with the continual advance of computing power (for example, it is common these days to buy a laptop with 16 GB of RAM memory). This effectively limits the need to swap any files to the virtual memory, which results in low expectations of computer forensic investigators when investigating pagefile.sys.

❖ **Swapfil.sys**

Swapfile is used to store the idle and other non-active objects transferred from the RAM, whenever a user tries to access an idle process again, its information will be shifted to the RAM. In modern Windows versions (like 8 and 10) we can see that both Pagefile and Swapfile exist together on a system drive; we can consider that these two files form together what is known now as virtual memory in Windows OS. Swapfile has a fixed size in modern Windows versions (8, 10), which is 256 MB.

3. Analysis of Forensics Image

3.1 Keyword Search

A keyword search allows one to search for keywords and phrases across the major fields of the catalog: authors, titles, series, subjects, notes, contents notes, and publishers.

Unlike the other search options, the Keyword Search can find words and phrases within a title, series, or subject. The Keyword search finds all items in the Catalog that include all of your search terms.

3.2 File signature

A file signature is data used to identify or verify the content of a file.

- File magic number: bytes within a file used to identify the format of the file; generally a short sequence of bytes (most are 2-4 bytes long) placed at the beginning of the file; See list of file signatures
- File checksum or more generally the result of an hash function over the file content: data used to verify that the file content integrity, generally against transmission errors or malicious attacks. The signature can be included at the end of the file or in a separate file.

List of Some File Signatures:

File Extension	HEX Signature	Description
3gp, 3g2	66 74 79 70 33 67	3rd Generation Partnership Project 3GPP and 3GPP2 multimedia files
z, tar.z	1F 9D	compressed file (often tar zip) using Lempel-Ziv-Welch algorithm
gif	47 49 46 38 37 61	Image file encoded in the Graphics Interchange Format (GIF)
tif, tiff	49 49 2A 00	Tagged Image Format

jpg, jpeg	FF D8 FF E0 nn nn 4A 46 49 46 00 01 FF D8 FF E1 nn nn 45 78 69 66 00 00	JPEG raw or in the JFIF or Exif file format

Table: File Signatures

3.3 File Carving

File carving is a well-known computer forensics term used to describe the identification and extraction of file types from unallocated clusters using file signatures. A file signature, also commonly referred to as a magic number, is a constant numerical or text value used to identify a file format. The object of carving is to identify and extract (carve) the file based on this signature information alone.

File Carving, Data Carving, or just Carving is a general term for extracting data (files) out of raw data, much like "carving" a sculpture from a stone. File carving should be done on a disk image, rather than on the original disk.

a) Cluster based file carving

In a cluster based file-system like FAT or NTFS a new file must start in a new cluster. It follows then that the file signature appears near a cluster boundary. Carving speed is therefore achieved by searching for file signatures only near cluster boundaries.

b) Sector based file carving

In certain situations, it may be advantageous to perform a lower level search for sector-aligned file signatures. This search may recover additional files, for example files from a previous volume which had a different cluster layout and is no longer aligned to current cluster boundaries.

Carving in sector mode will increase the time needed to complete search.

c) Byte based file carving

In certain situations, it may be advantageous to data carve on a byte by byte level. This has the additional benefit of locating files where the file signature is neither aligned with a cluster or sector boundary. A byte-based data carve is commonly used when searching for a file within a file (such as within backup file, or when searching an image of a cell phone.

Carving in byte mode will increase the time needed to complete the search.

3.4 Mismatch File Search

The Mismatch File Search module analyzes the content of files and identifies any files whose raw bytes are not consistent with their file extension.

3.5 Image Analysis using Autopsy

Autopsy is a digital forensics platform and graphical interface to “The Sleuth Kit” and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card. Autopsy advantages

1. Free

2. Open Source
3. Better results

Autopsy is built into the SANS Investigative Forensic Toolkit Workstation (SIFT Workstation) that you can download fromforensics.sans.org.

Autopsy is available from http://www.sleuthkit.org/autopsy**.**

a) Start using Autopsy

Step1: Installation

Download the Autopsy setup, just double click and install software. It will automatically install the software.

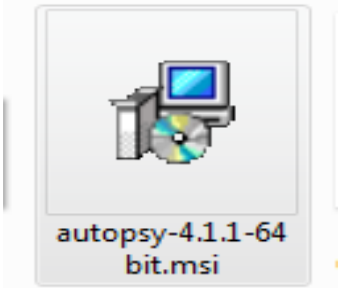


Figure: Autopsy setup

Step2: Run First Time

After installation just run Autopsy as Administrator, after sometime you will receive the window as given below

Figure: Starting Autopsy

There will be three options

1. Create New Case: To create new case.
2. Open Recent Case: To open recent case which we analyzed.
3. Open Existing Case: To open Existing/ Old. Here we select "Create New Case".

Step3: Enter the Case Details

After clicking "Create New Case", you will see a window which ask about the case name and base directory where you want to save case related files and information. After filling information click "Next".

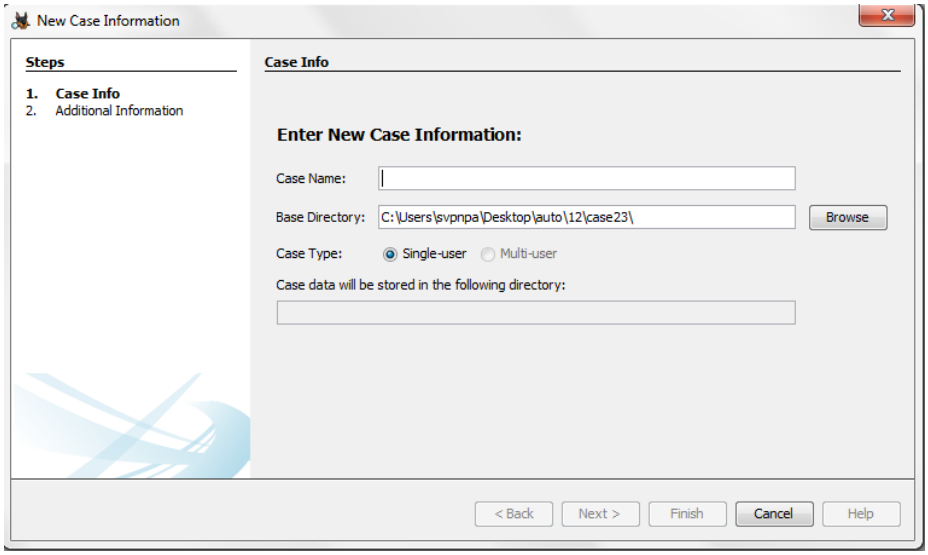


Figure: New Case Details

Step 4: Enter the Case Number and Examiner Name

Next window is for case number and examiner name, put unique case number and examiner name and click "Finish".

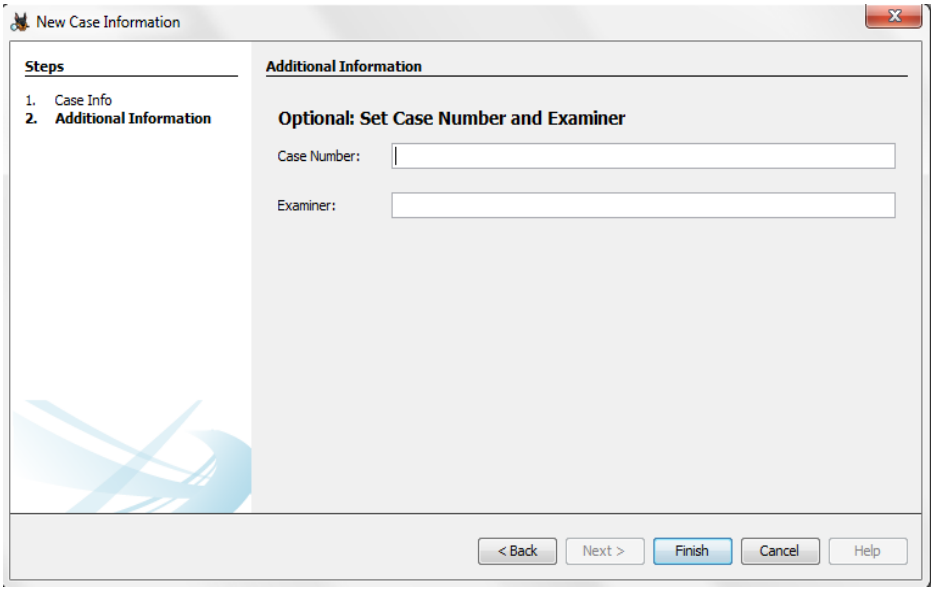


Figure: Case Number

Step 5: Add evidence item.

You can add a data source in several ways:

- After you create a case, it automatically prompts you to add a data source.
- There is a toolbar item to add a Data Source when a case is open.
- The "Case", "Add Data Source" menu item when a case is open.

The data source must remain accessible for the duration of the analysis because the case contains a reference to the data source. It does not copy the data source into the case folder.

Regardless of the type of data source, there are some common steps in the process:

1. You will be prompted to specify the data source to add.
2. Autopsy will perform a basic examination of the data source and populate an embedded database with an entry for each file in the data source. No content is analyzed in the process, only the files are enumerated.
3. While it is examining the data source, you will be prompted with a list of ingest modules to enable.

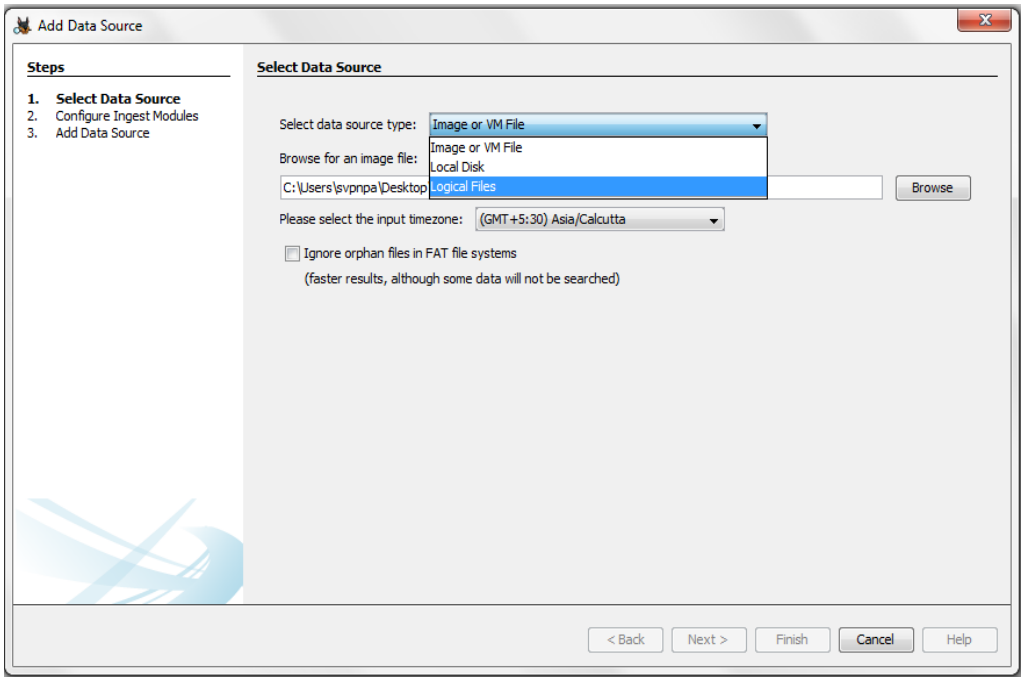


Figure: Add Data Source

To add a new data source at beginning, follow this:

Select file location by clicking browse.

Now select the Time Zone, it will be the same as evidence item. If evidence seized from a machine which follow GMT+5:30 time zone, then we also select the same.

Last option is to check a box, which will ignore orphan files. Orphan file are default DLL file in windows system. After all set click "Next"

Step 6: Configuring Ingest Modules

You will be presented with an interface to configure ether ingest modules. From here, you can choose to enable or disable each module and some modules will have further configuration settings.

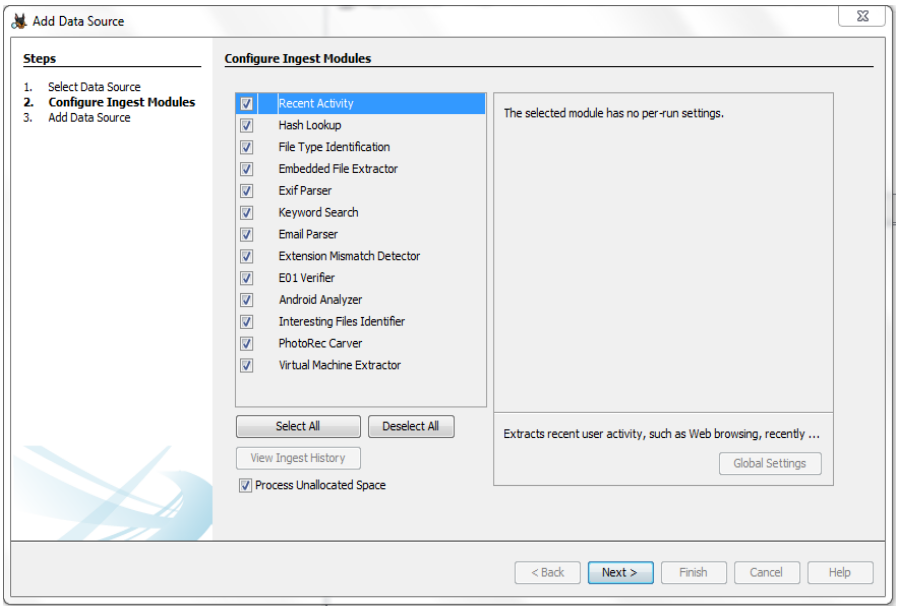


Figure: Ingest Module Configuration

There are two places to configure ingest modules. When you select the module name, you may have some "runtime" options to configure in the panel to the right. These are generally settings that you may want to change from image to image.

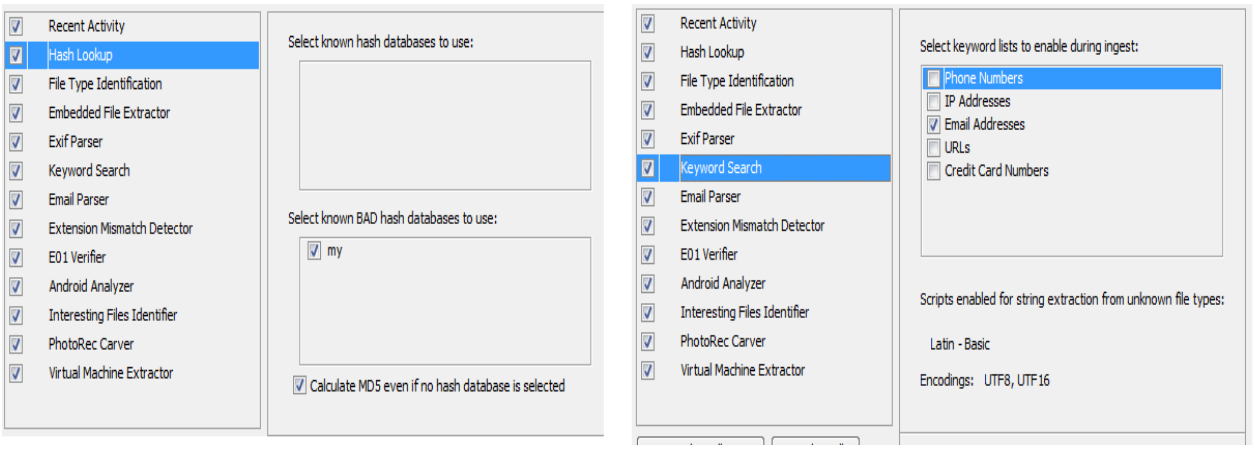


Figure: Runtime options for Keyword Search

There may also be an "Advanced" button that is enabled in the lower corner. Pressing this button allows you to change global settings that are not specific to a single image. This advanced configuration panel can often be found in the "Tools", "Options" menu too.

As an example, the hash lookup module will allow you to enable or disable hash databases in the “run time” options panel, but require you to go to the "Advanced" dialog to add or remove hash databases from the Autopsy configuration.

Autopsy now ask you about to "Finish" the configuration and start the analysis

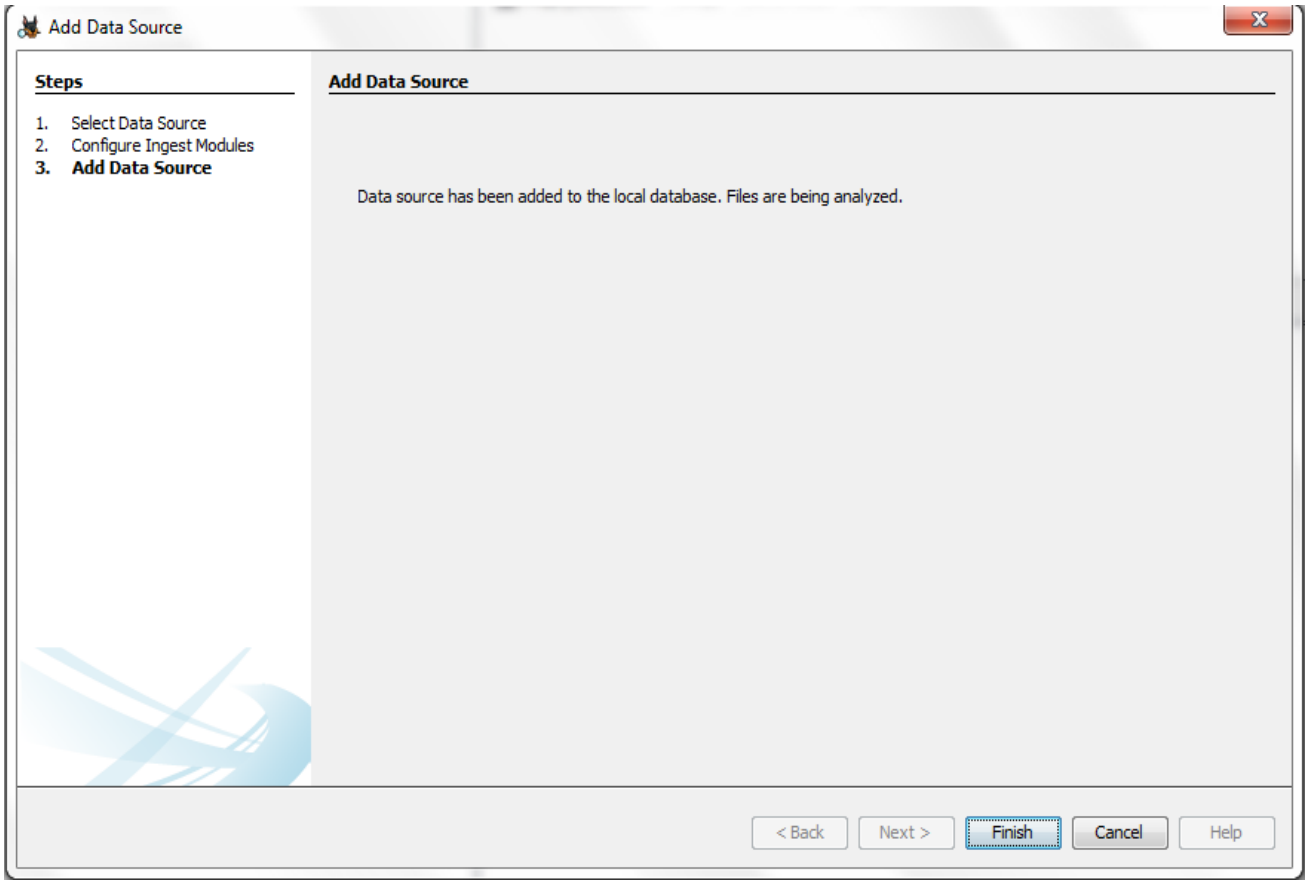


Figure: Finish Configuration

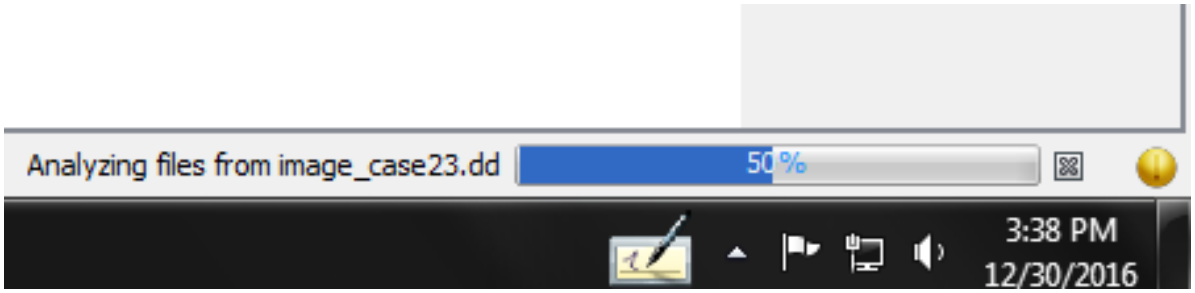


Figure: Analysis Started

After clicking "Finish", it will analyze the data source, and the progress bar will be shown at bottom right as shown above.

b) Analyze Evidence Source

Recent Activity Module:

The Recent Activity module extracts user activity as saved by web browsers (including web searches), installed programs, and the operating system. It also runs Regripper on the Registry hive.

This allows you to see what activity has occurred in the last seven days of usage, what web sites were visited, what the machine did, and what it connected to.

Results show up in the tree under "Extracted Content".

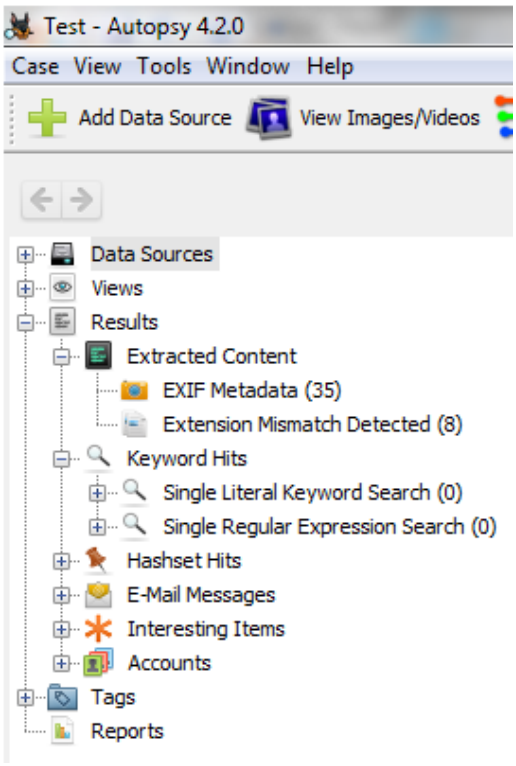


Figure: Extracted Content

Hexadecimal Analysis:

You can also analyze data using hexadecimal values; just click "Data Sources", hexadecimal value will available at right panel, like given below.

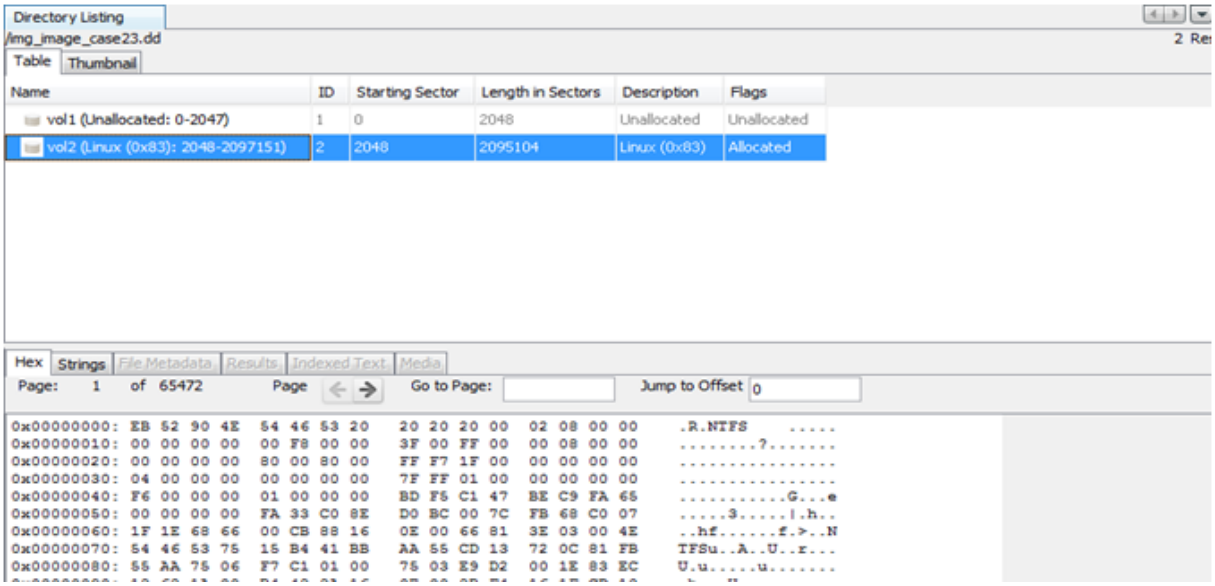


Figure: Hexadecimal Values

Keyword Search:

Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions. Searches can be performed on either the full file system image or just the unallocated

space. An index file can be created for faster searches. Strings that are frequently searched for can be easily configured into Autopsy for automated searching.

To search keyword, go to tools-->Options and select "Keyword Search" tab. Now add some keyword to search in evidence source. From here you can create new list or you can use existing list to analyze.

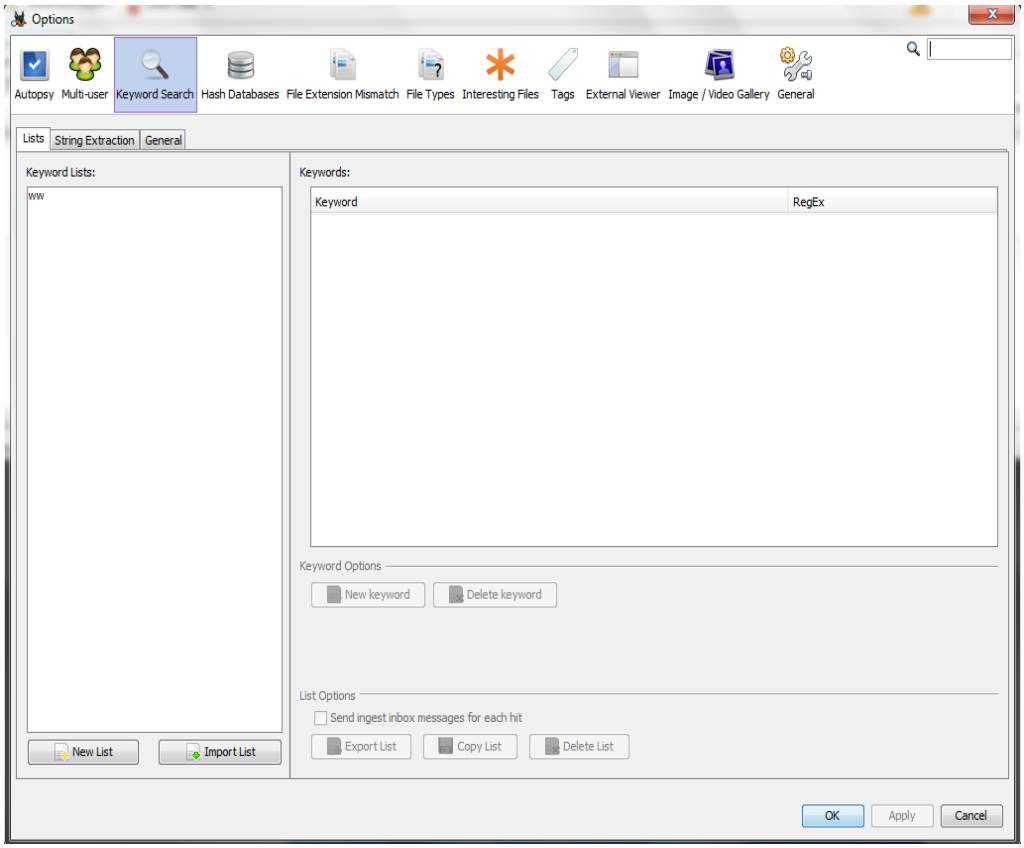


Figure: Keyword Search

Content Viewer:

The Content Viewer lives in the lower right-hand side of the Autopsy main screen and show pictures, video, hex, text, extracted strings, metadata, etc. They are enabled when you select a file in the file list above it.

The Content Viewer is context-aware, meaning it will present different views of the content based on the type of file selected. For example, a .JPG would show up as a picture, a text file would show up as text, and a .bin file would show up as hex output.

The screen shots below show some examples of content viewers in action. First screen shot shows the image, second shows hexadecimal values of that image and third screen shot shows the metadata information of this image.

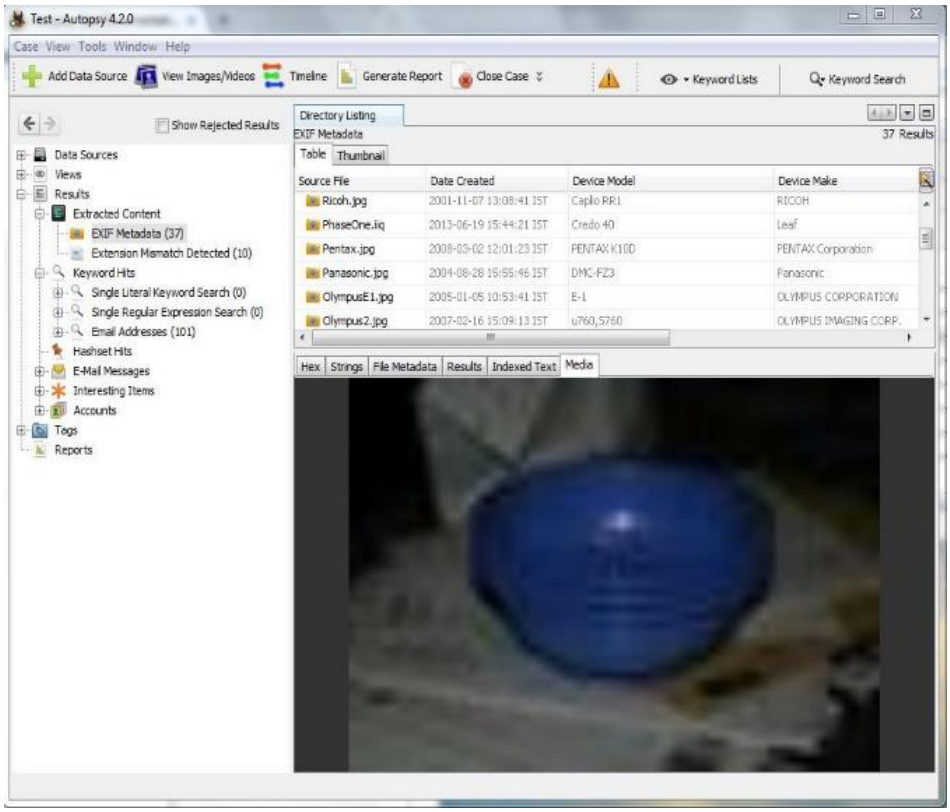


Figure: Images Present in Source

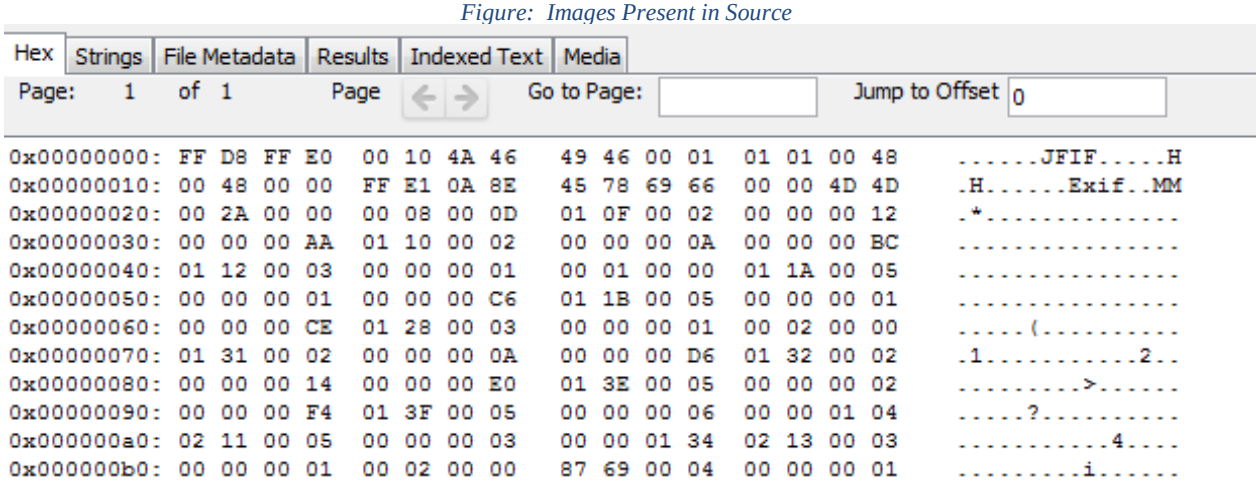


Figure: Hexadecimal Values

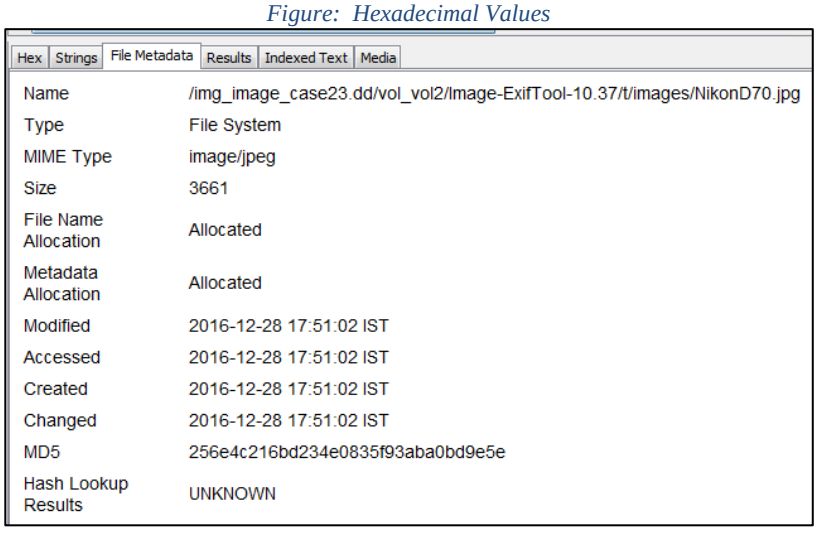


Figure: Metdata Information

Email Parser Module:

The Email Parser module identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them, adding the results to the Blackboard. This module skips known files and creates a Black board artifact for each message. It adds email attachments as derived files. This allows the user to identify email-based communications from the system being analyzed. The results of this show up in the "Results", "E-Mail Messages" portion of the tree.

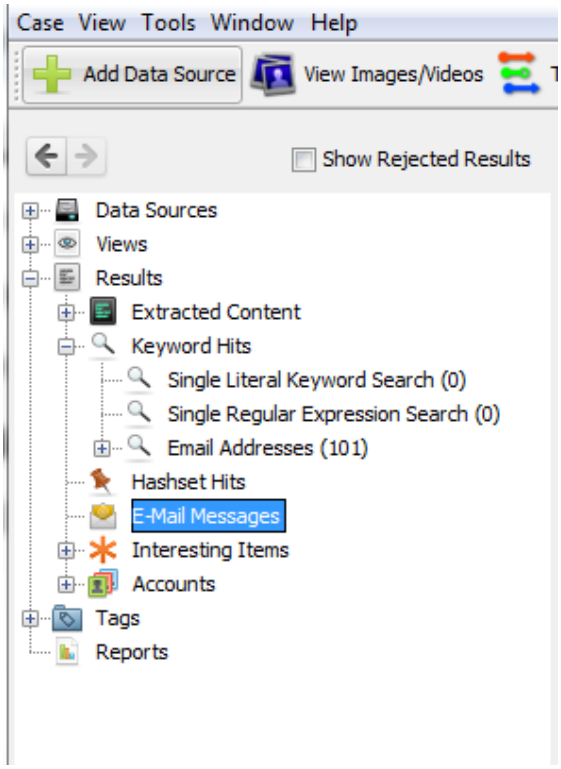


Figure: e-mail Messages

Photo RecCarver Module:

The Photo RecCarver module carves files from unallocated space in the data source and sends the files found through ingest processing chain. This can help viewer discover more information about files that used to be on the device and were subsequently deleted. These are simply extra files that were found in "empty" portions of the device storage. The results of carving show up on the tree under the appropriate data source with the heading

"$CarvedFiles".

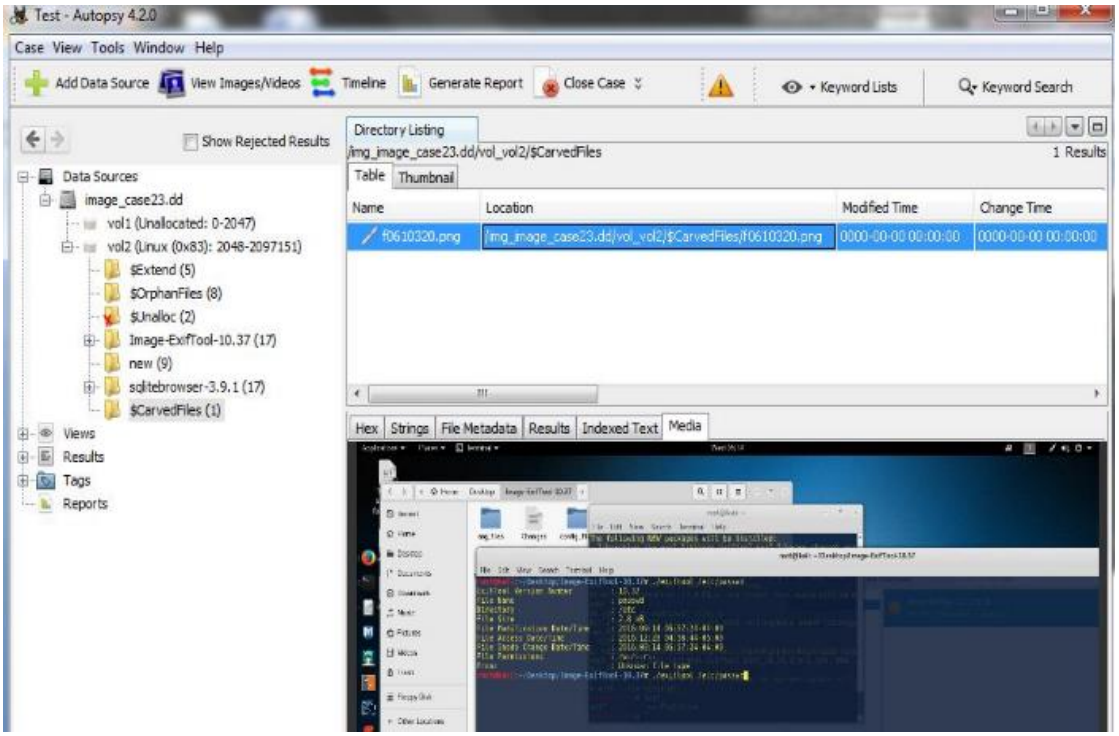


Figure: Carved Files

Timeline analysis:

To analyze timeline of data source click on "Timeline" button, it will create a timeline using file MAC

Time stamp.

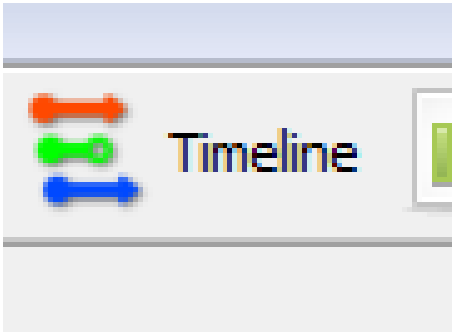


Figure: Timeline Icon

This timeline will show "File system" and "Web activity" in graphical view. You can click any of this column and print details.

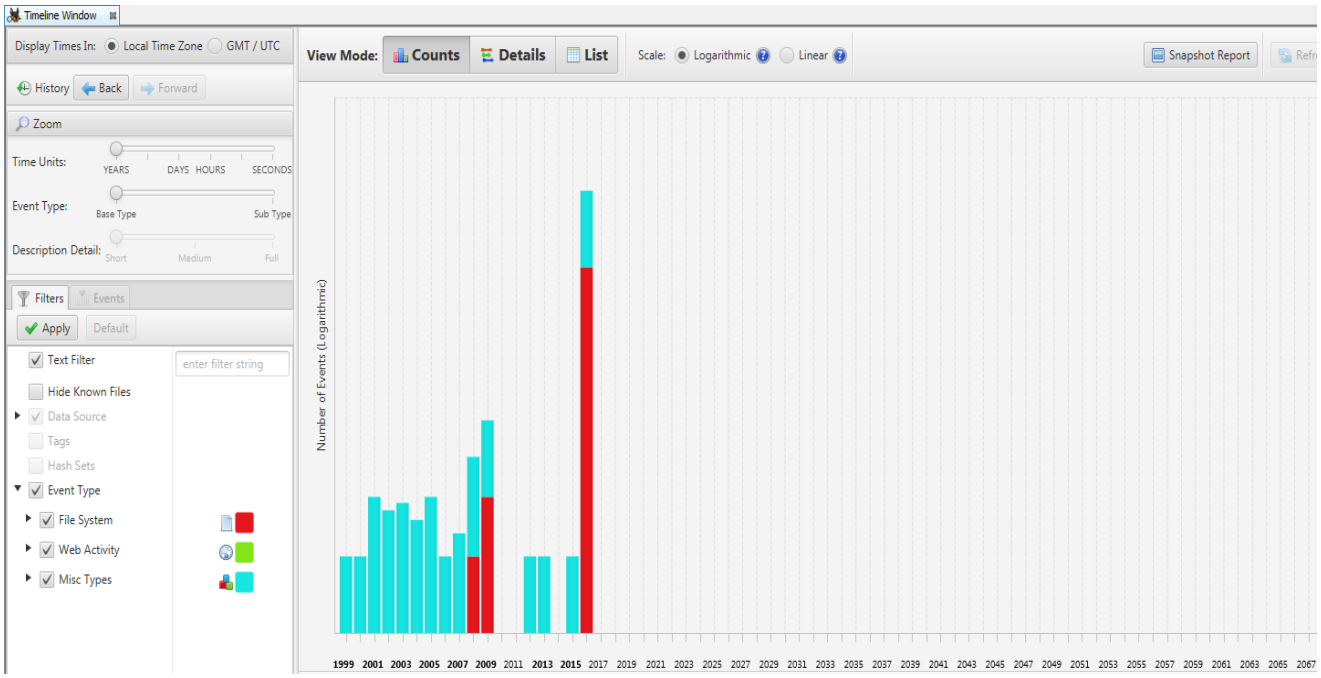


Figure: Timeline Graph

Reporting:

To generate the report, we have to create some tag or bookmarks.

1. Tagging

Tagging (or Bookmarking) allows you to create a reference to a file or object and easily find it later. When an interesting item is discovered, the user can tag it by right-clicking the item and selecting one of the tag options.

When you tag a Black board artifact result, you have the choice to either:

- Tag File– use this when the file itself is of interest
- Tag Result–use this when the result is of interest

Which to choose depends upon the context and what you desire in the final report. For example, we are choosing Tag File here.

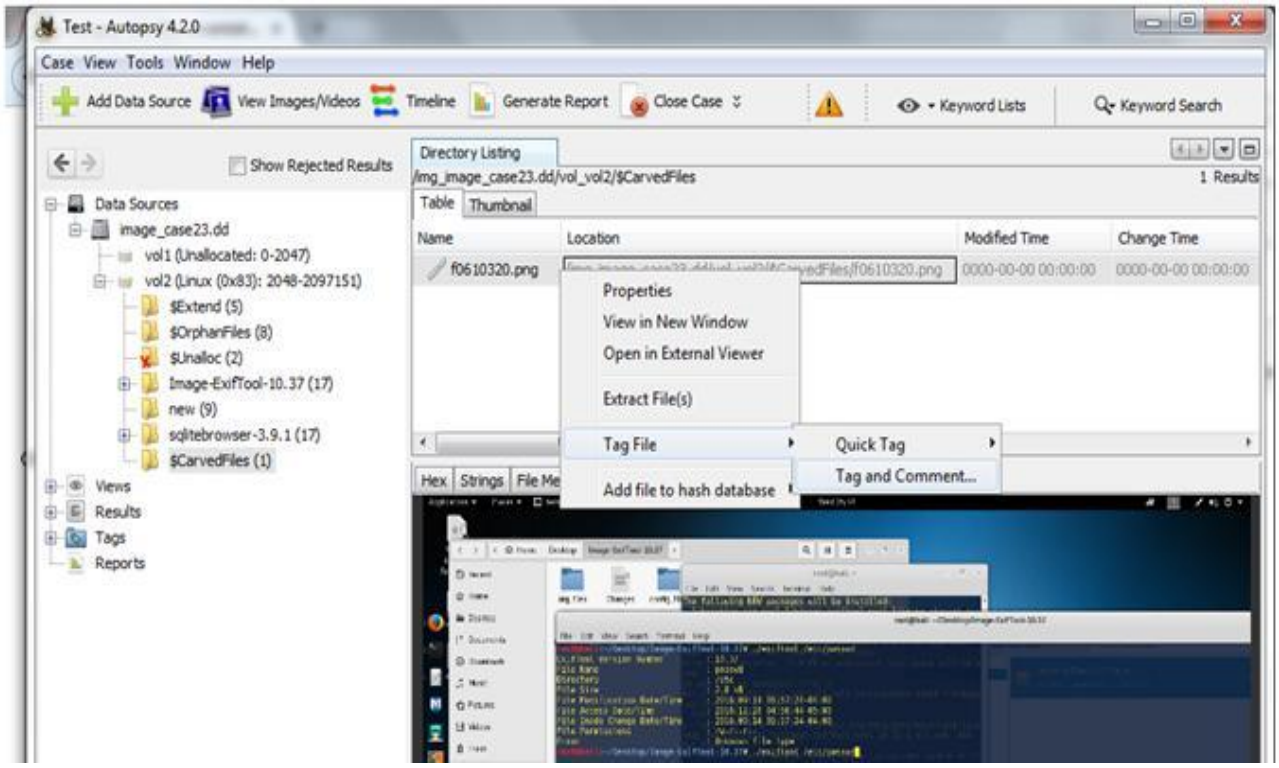


Figure: Adding Tag to Object or File

Once you have chosen to tag the file or the result, there are two more options:

- Quick Tag–use this if you just want the tag
- Tag and Comment–use this if you need to add a comment about this tag.

After clicking Tag and Comment, window will pop-up. Enter Comment and continue.

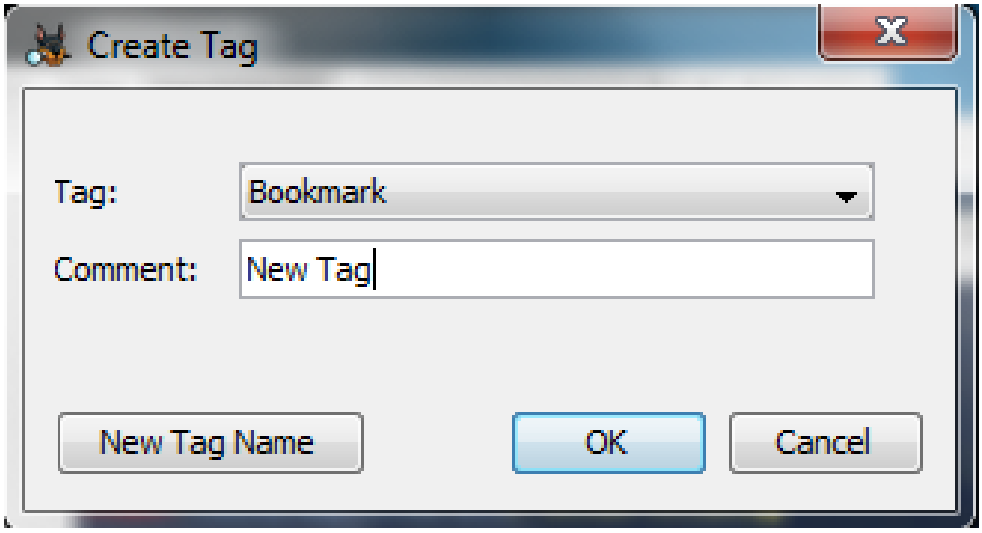


Figure: Adding Comment to Tag

2. Generate Report:

To create reports, go to "Tools", "Generate Report". You can choose several different types of reports. We will go through the HTML report here.

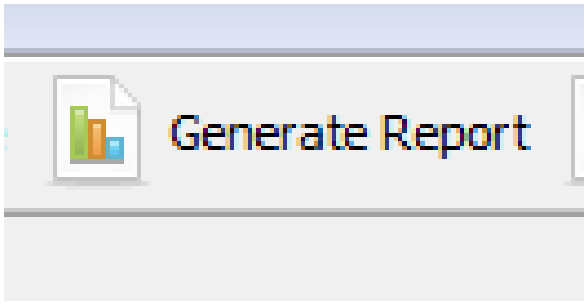


Figure: Generate Report Icon

Select HTML here and click next.

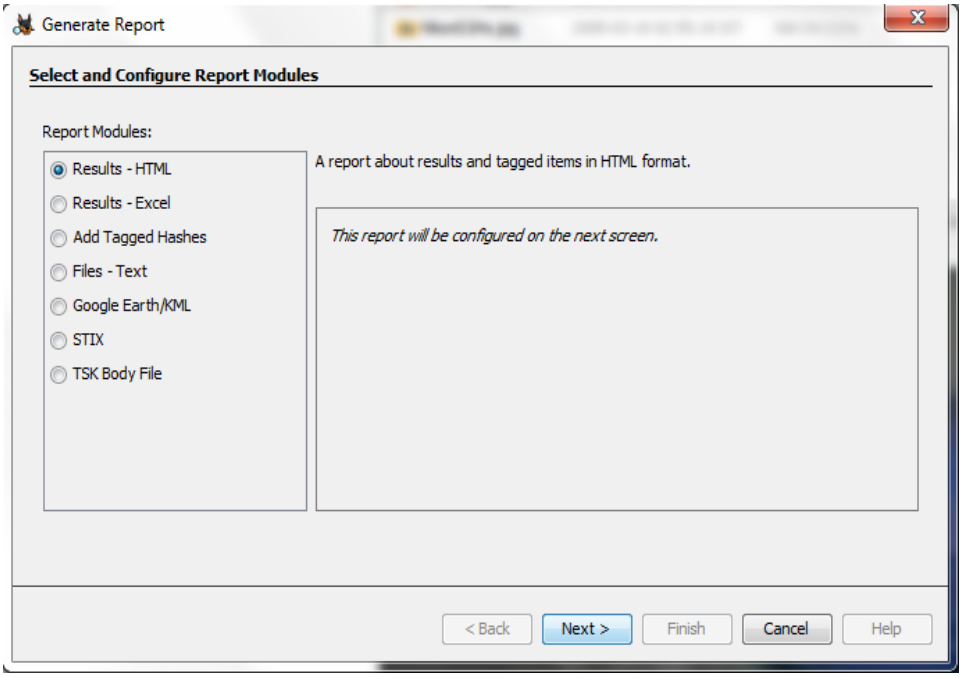


Figure: Select Report Format

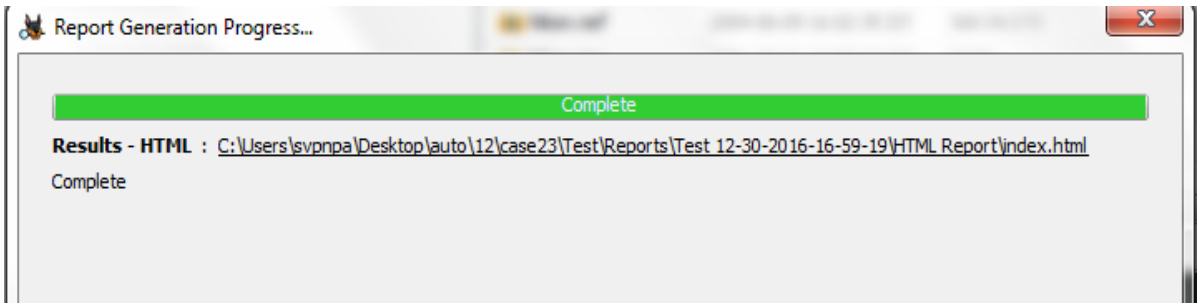


Figure: Report Generated

The report will be generated at the given location, you can click on a hyperlink and open it in a browser, and view it. It will show all details related to the case.

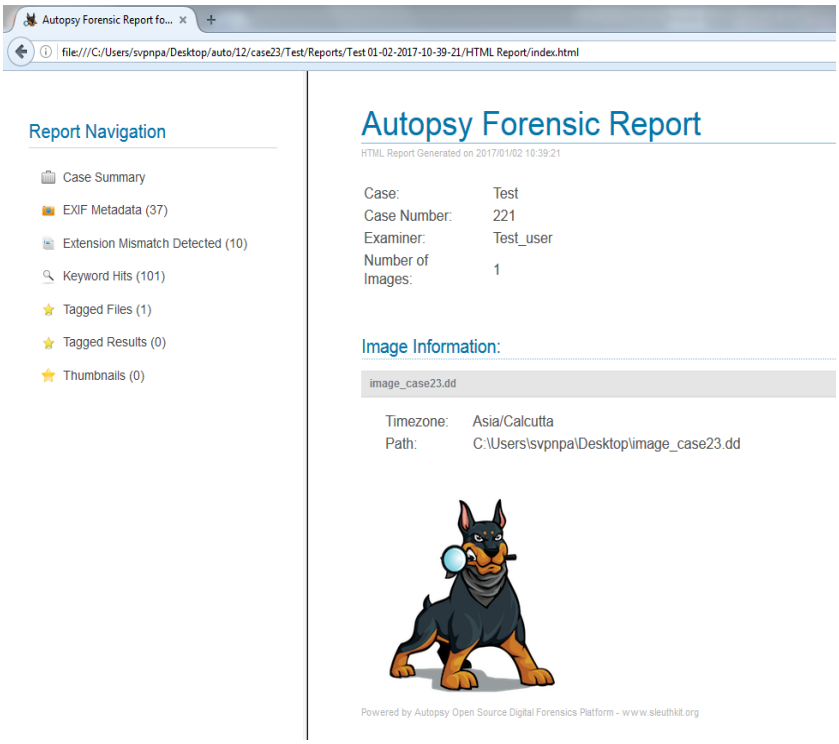


Figure: Autopsy Forensic Report

4. Windows Forensics

4.1 Windows Forensics and Its Importance

Microsoft Windows is a graphical user interface (GUI) operating system that has been distributed in various forms since 1985. Overtime, windows became the most common operating system that was installed on a computer system. Each version has brought changes to the user interface, though not all have been popular. Each version has had different ways of storing data that is of forensics value to the examiner.

An artifact refers to anything man-made – a Windows artifact, for the purpose of computer forensics, is evidential data that is automatically saved by the windows operating system as a result of a person interacting with or using the computer. It does not refer to the default files that saved to the computer on install – most of which may have no bearing on an investigation.

4.2 Artifacts in Windows PC

❖ **Shell Link Files**

A "shell link file" is more commonly referred to as a Link file or shortcut. It is a special file that contains "links" or "pointers" to other resources, for example, programs, data files, folders, and printers, They provide a powerful and convenient way for users to gain quick access to frequently used programs and files, They are most often implemented via icons on the desktop or items presented from a menu such as Windows Start Menu.

During an examination of a Windows system many Link files (Ink) will be found. These files contain some very useful information about the target file including:

- File MAC Times.
- File Size.
- Volume Details - Serial Number, Label.
- Original File Path.

The information within a link file can vary depending on:

- Version of Windows was in use.
- If the link file was created by an application / user / 0S.
- File system of target file.

The best thing about a Link file is that it will often demonstrate a user's knowledge of a file, and their interaction with that file. The file structure is quite complex, but well documented online. Two useful and free tools for parsing Link files are; Simple File Parser by Chris Mayhew — https://code.google.com/p/simple-file-parser/ ,

In the example in Figure 5.1 below, we can see that we are looking at a Link File that was found on our suspect user profile's desktop, and has the file name "Image Magick Display.ink', but it is actually pointing to the folder at "C:\Program Files\ImageMagick-7.0.10-Q16\imdisplay.exe"

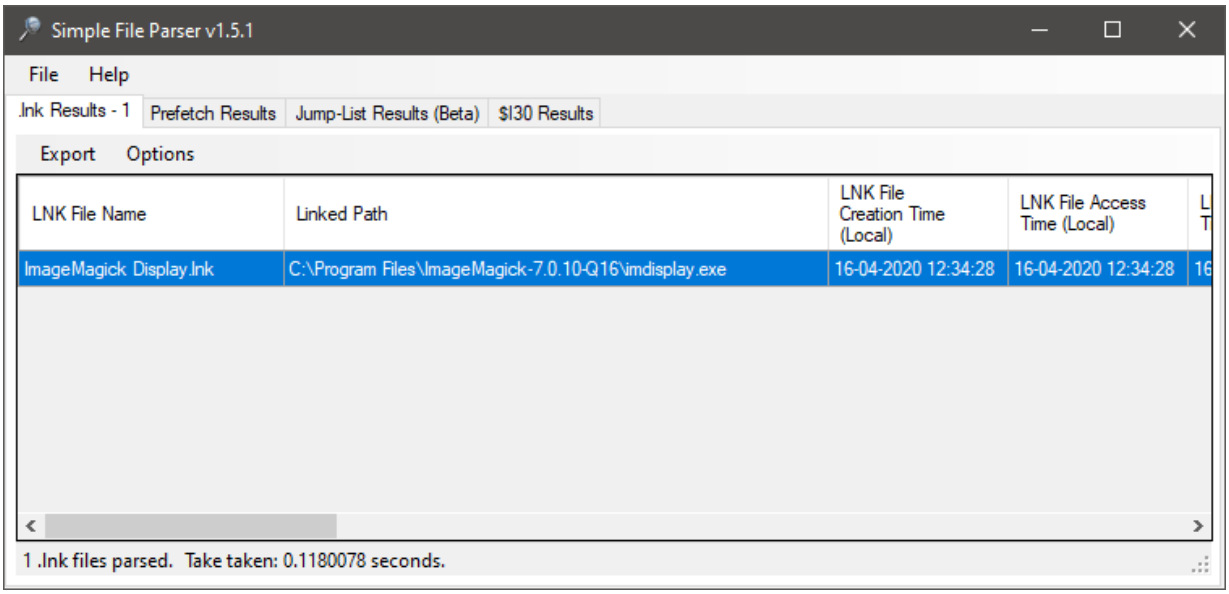


Figure: Link File Example

It is important to understand that the times stored within a Link file relate to the actual target file - and they are stored in FILETIME format and are UTC.

In Figures 5.2 and 5.3, the tool Simple File Parser is displaying MAC times for the link file itself (taken from the file system) and the MAC times for the target (parsed from the link file itself). There is a minor bug with this tool that it says (Local) under the embedded time, which is incorrect - it is UTC.

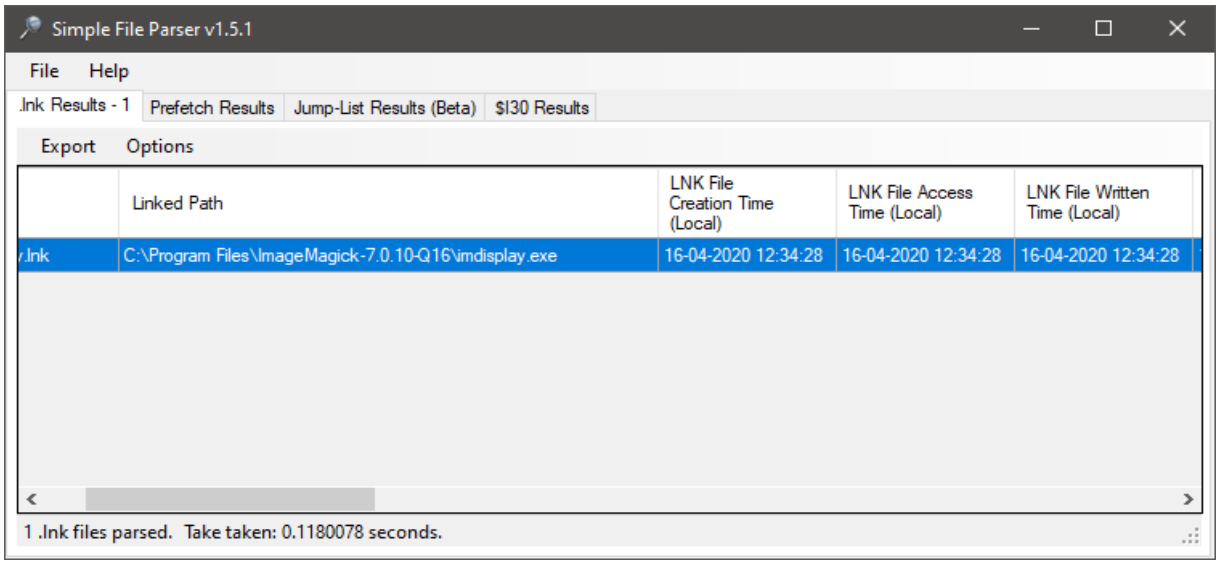


Figure: Link File MAC

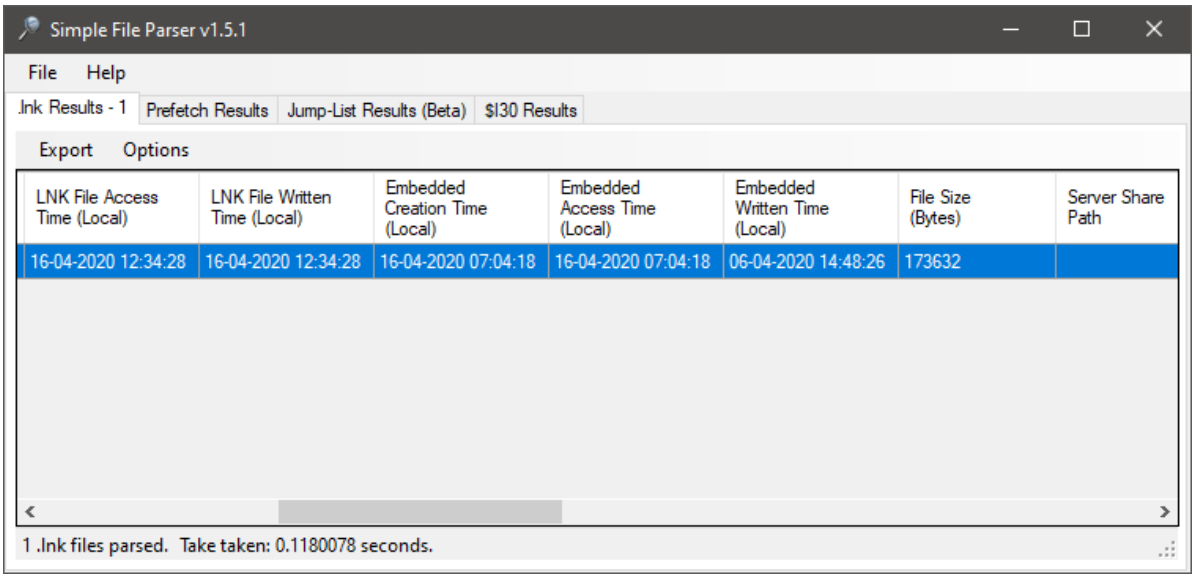


Figure: MAC for target from link file content

In the example above, the folder C:\Program Files\ImageMagick-7.0.10-Q16\imdisplay.exe was created at 16 April 2020 at 12:34:28 UTC.

A link file's embedded time becomes very powerful when the examiner can cross check the MAC times of the target within the file system to those within the link file ~ any file system date and time entries that are after those embedded within the link file show that a user has interacted with the file.

There are many forensic implications relating to the content of these files. The Volume Serial Number can be used to tie a specific thumb drive, USB drive, memory card or other removable media to a specific computer system. The MAC address can be used to identify a single computer. Even if MAC spoofing is used, the original MAC will still be inside the Link File.

By default, when a file or document is opened in either by double clicking, or using a programs File > Open dialog, a link (ink) file is created in the Recent folder. Table 5.1 provides the location in Windows XP, Vista,7,8 and 10 operating systems.

In a Windows XP system, the files are displayed in the Documents item on the Start Menu,

Location found	Windows version
C:\Documents and Settings\ %Username%\Recent	XP
C:\Users\%Username%\Appdata\Roaming\Microsoft\Windows\ Recent	Vista, 7, 8, 10

Table: Link File Location

Figure 5.4 shows the recently accessed files. Typically, the start menu will only show the ten most recent items (though this can be changed in the Start Menu properties), but the actual recent folder will contain a link file for every user file that has been recently opened.

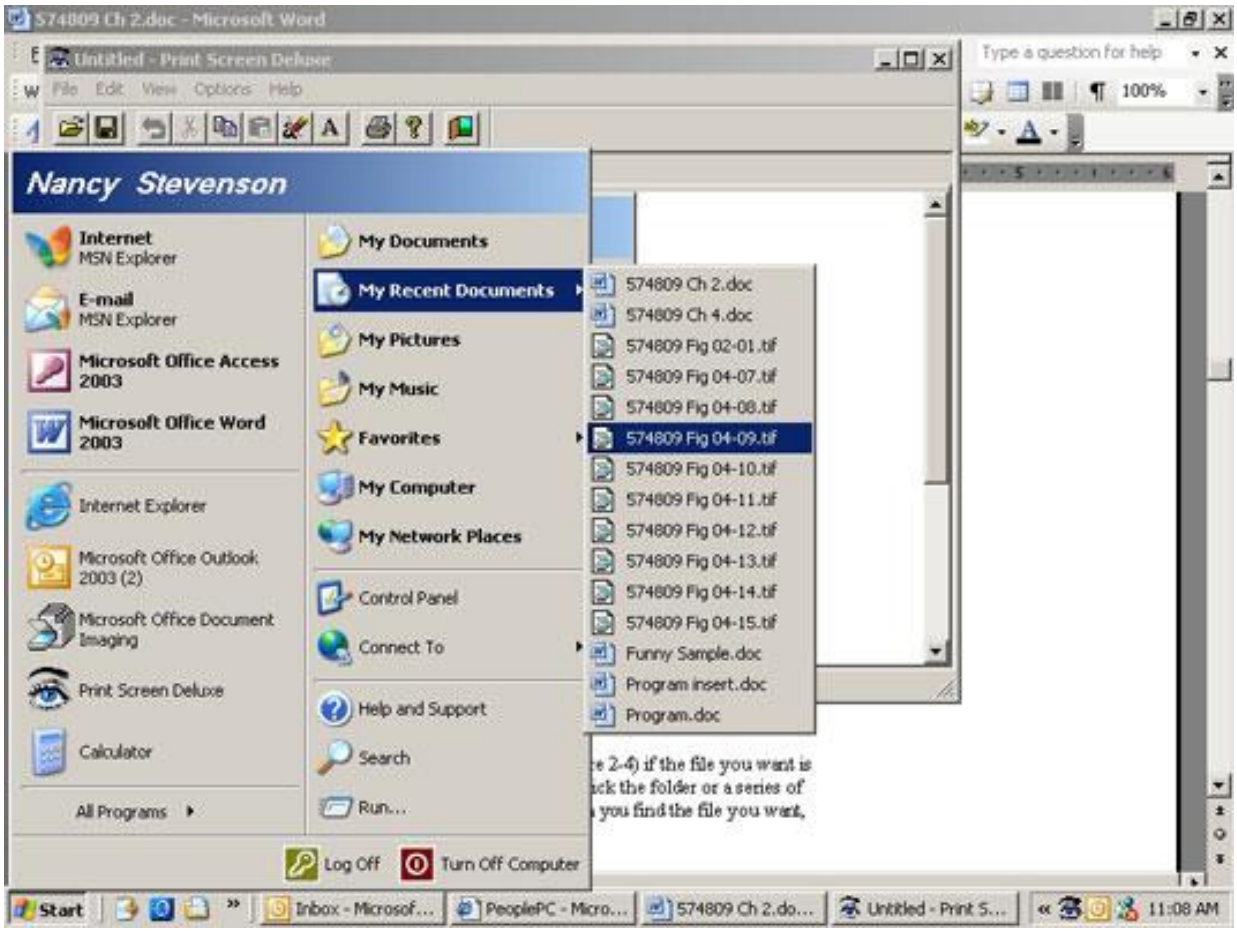


Figure: Recent items as seen in Windows XP

It is possible for a user to clear the list, which clears the start menu and all the link files are deleted by using the Clear button located on the Start Menu Programs tab of the Taskbar Properties dialog, as shown in Figure 5.5.

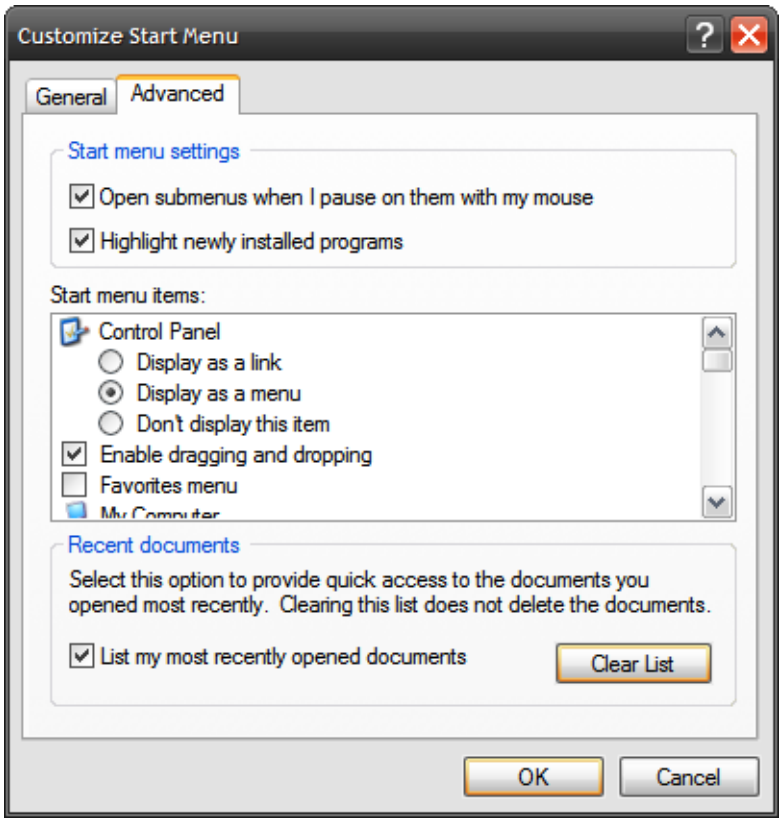


Figure: Clear XP recent Folder

In Windows Vista, 7, and 8 the files are displayed in "Recent Items", which is a virtual folder when viewed with Windows Explorer. Shortcuts appear to be the actual file as they show the file extension of the target, as seen in Figure 5.6. In reality, this is not the case, the folder is called Recent, and the file extension is still * Ink.

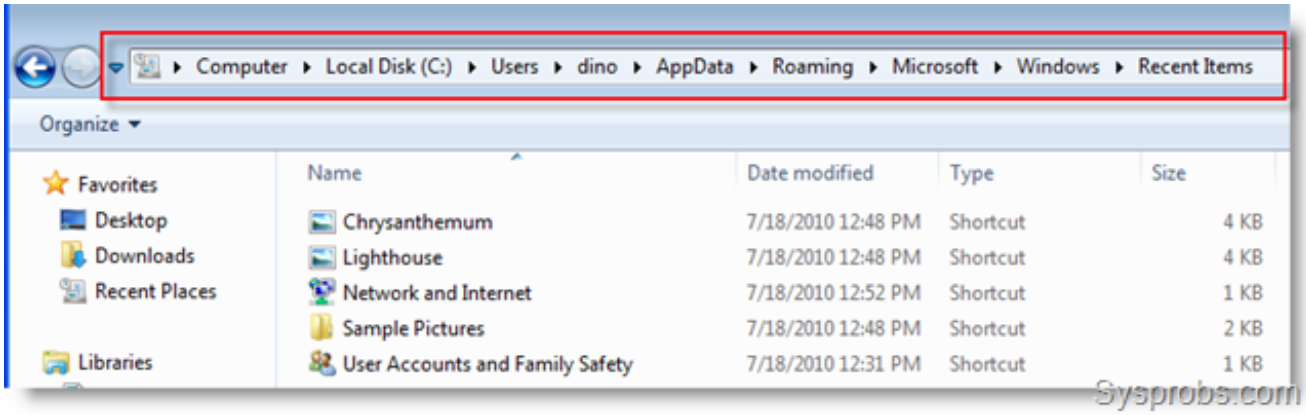


Figure: Virtual Folder "Recent items" as seen in Windows Explorer

In a Windows 7 system, the parent folders from recently accessed files are displayed in Recent Places, as shown in Figure 5.7.

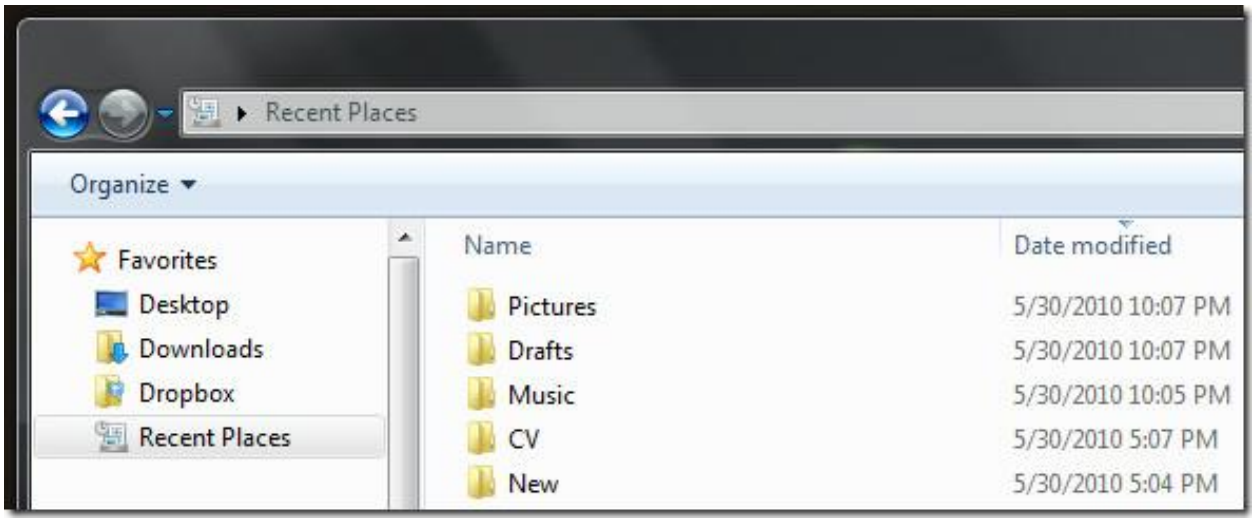


Figure: Recent Places in Windows 7

The start menu in Windows 7 operates differently to XP. Displaying Recent Items in the start menu from the shell link files is actually disabled by default - even though the link files are still created in the recent folder. A separate entry called Recent Items can be enabled by the user in Windows 7, as shown in Figure.

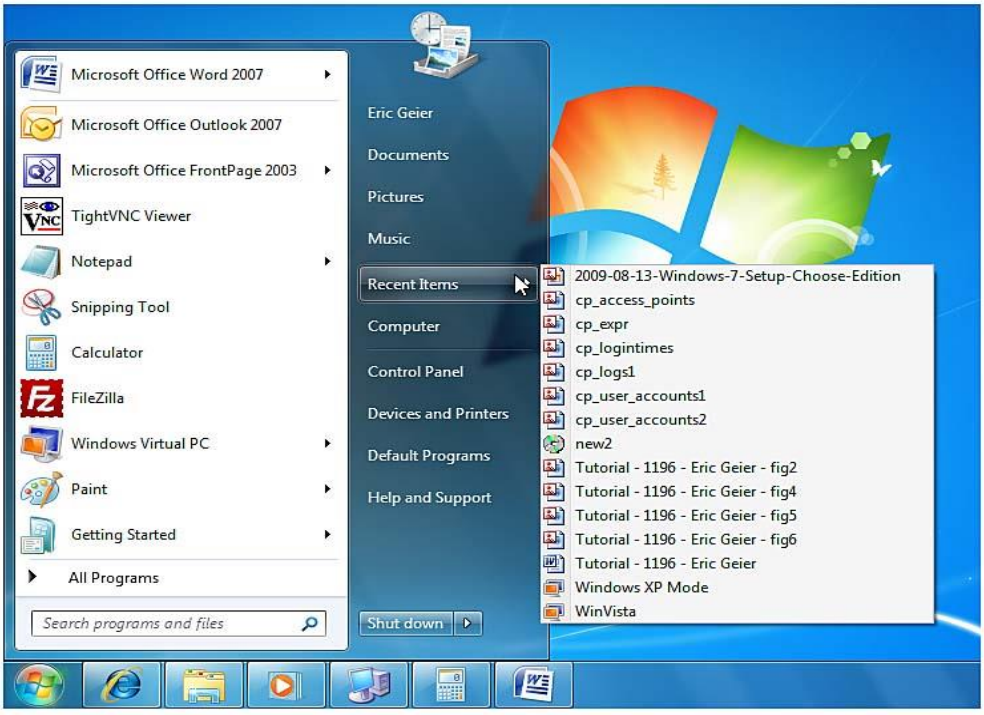


Figure: Recent Items in Windows 7

The user can enable it in the Start menu options in Windows 7 and determine how many items to display, as shown in Figure, However the same option does not exist in Windows 8. In Windows 8 the Start menu, as it previously existed has disappeared, but the link files are still created in the recent folder.

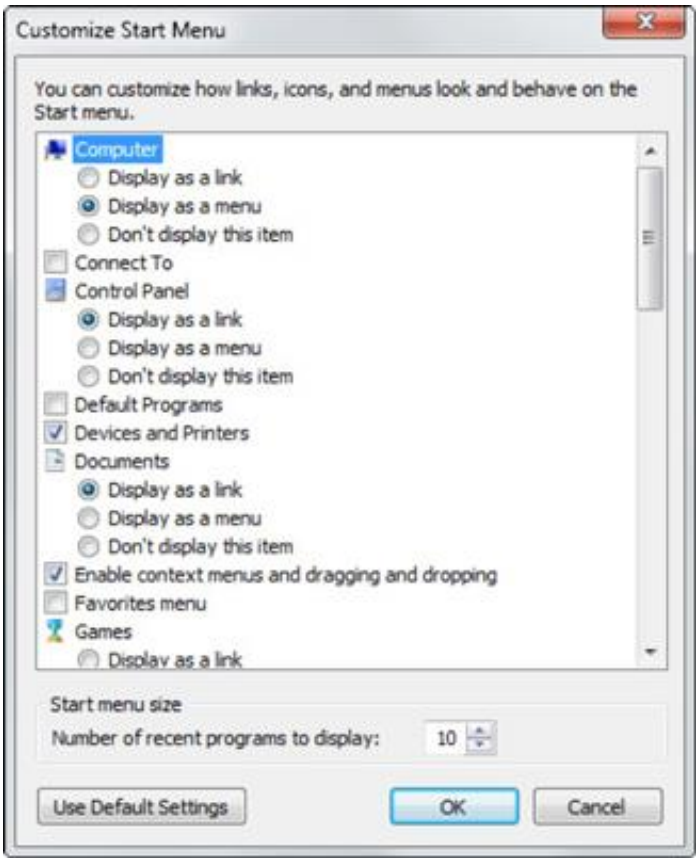


Figure: Recent Items start menu settings in Windows 7

Recent item *.Ink file creation can be disabled by the user. It can be done for an individual user in their NTUser.dat file at:

Software\Microsoft\ Windows Current Version\Policies\Explorer**No Recent Docs History**

with a **dword** value of 0000 0001.

Recent Items link file creation can also be disabled in the computer security policy:

Computer Policy\User Configuration\Administrative Templates\Start Menu and Taskbar\Do not keep history of recently opened documents.

Windows 10 ushered in a rebirth of the Start Menu however the recent items option is still not available in the Start Menu. Rather the recent items are more integrally tied to Windows Explorer and their “Quick Access” view as seen in Figure 5.10 below. This view has a default of 20 Recent Files although the operating system will contain additional Link files in the above described recent folder.

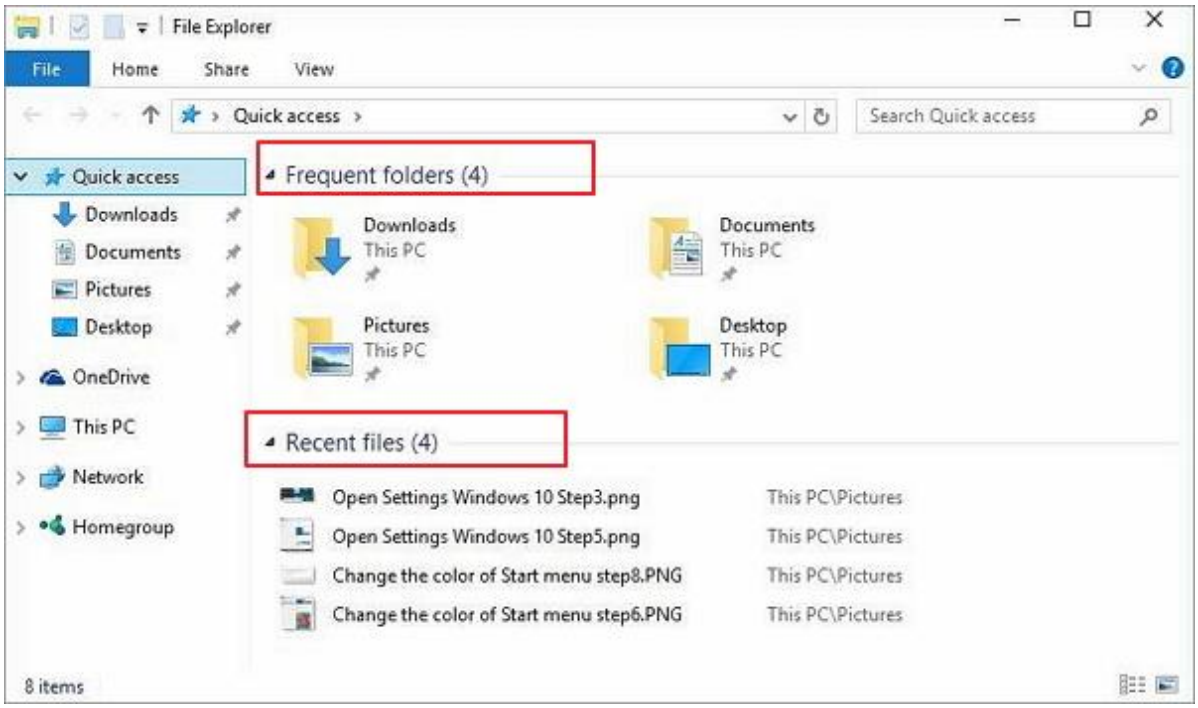


Figure: Windows 10 default Quick access view with recent files and frequent folders

In Windows 10, the Explorer also gives users the option to exclude recent files from view in "quick Access". This option turns off the view within Windows Explorer Quick access, but the Operating System still collects the Link files in the recent folder.

The standard folder options window in the General tab allows users to exclude files and frequent folders independently. It also gives users a very quick way to clear all link files from the Recent Items folder as seen in Figure below.

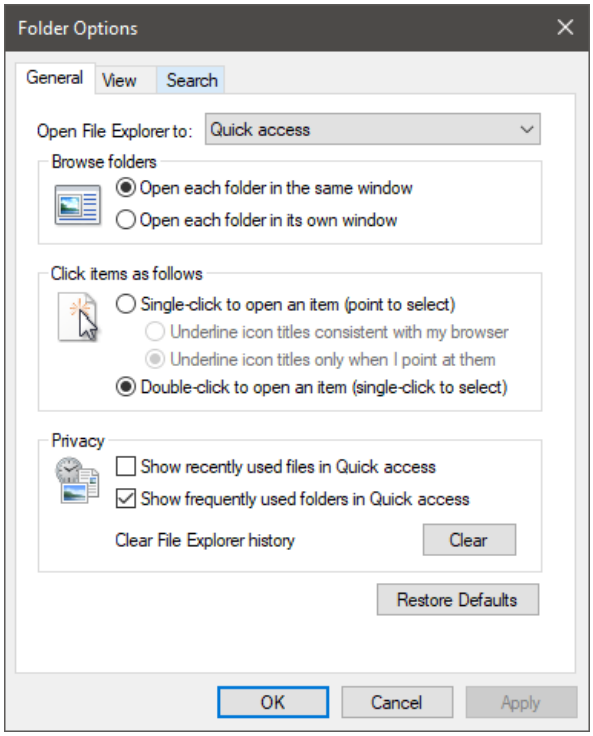


Figure: Windows Explorer Folder Option

❖ **Jump Lists**

Windows 7 introduced a new feature called “Jump Lists”, which are essentially a list of recent files that have been opened (or attempted to open) by a particular application. It is like the “Recent” folder, except that each list only applies to one program.

This artifact often provides significant insight to user activity and be especially beneficial if Link files in the Recent folder have been deleted, or even if the application has been deleted. It is possible the most under-utilized and yet most valuable artifact to the forensic investigator, as it proves user knowledge of a file through their interaction with it.

Observe in Figure 5.12, the start menu on the left shows that there are two documents that are in the Recent history for Microsoft Word 2013. However, the same start menu shown on the right shows that Recent Items is empty, and indeed, the Recent folder displayed at the bottom of Figure 12 is indeed empty. This is because the shortcuts for an individual program are stored in Jump List files, rather than shortcuts in the Recent folder.

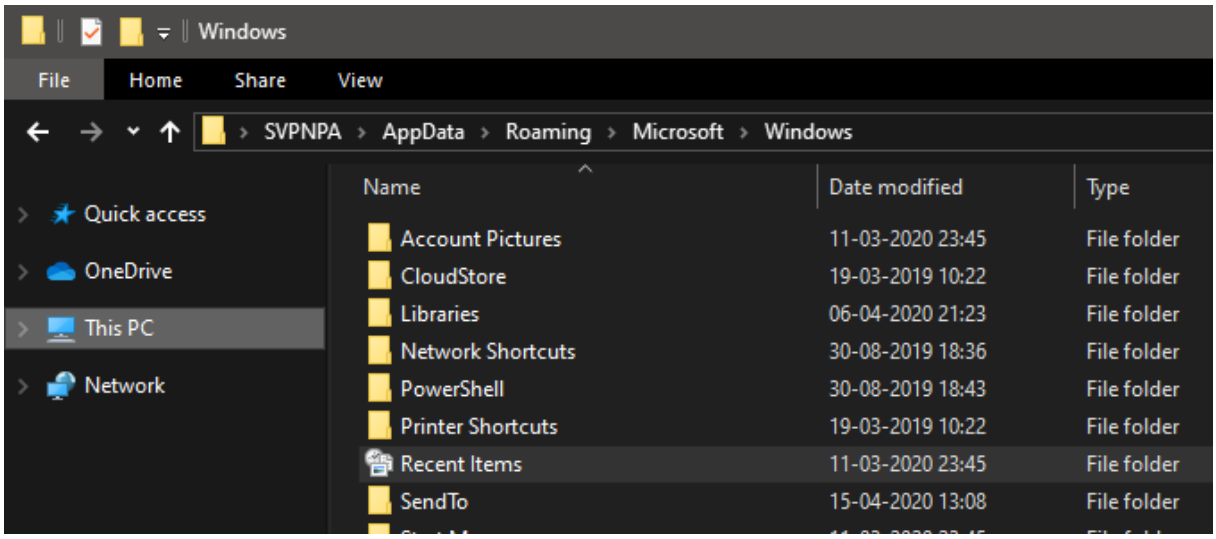


Figure: Windows Jump list and Recent Items

Clearing the items in the Recent folder does not eliminate the Jump List data unless the user first reveals the hidden folders containing the Jump List data and manually deletes them, which is not easy as they are "Super Hidden”.

‘There are two main types of Jump Lists:

1. Automatic - this Jump List is automatically populated by the system. It records information about file usage and stores that information in destination file associated to the program used to open the file.

2. Custom - this Jump List is maintained by the individual application and can provide a list of tasks specific to the program menu along with custom defined categories.

Jump List data for all applications is stored in the users’ profile in the path:

%User Profile%\ AppData\ Roaming Microsoft\Windows\Recent

When this folder is viewed in Windows Explorer, nothing unusual is noted, as shown in Figure 5.12. However, when this folder is viewed with a forensic tool, additional folders appear:

%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations.

%UserProfile%\ AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations.

Figure below shows the recent folder with the folders Automatic Destinations and Custom Destinations visible.

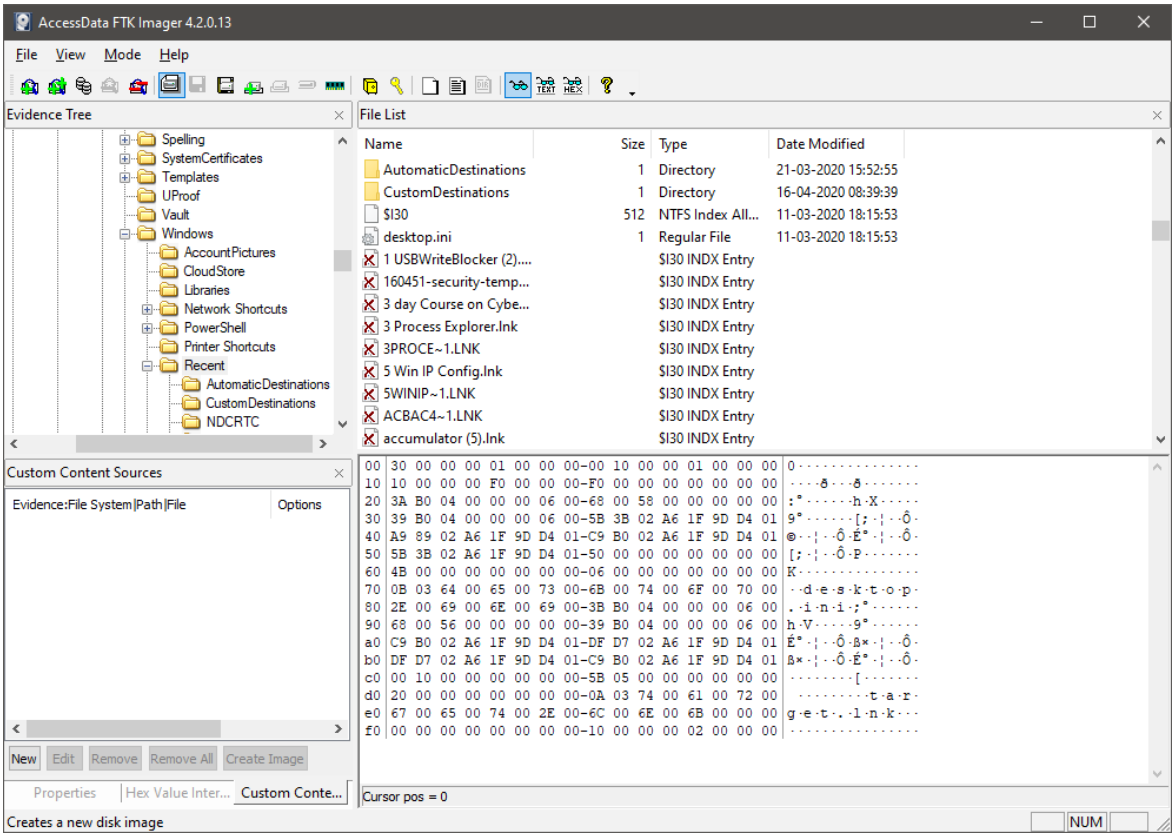


Figure: Jump list folder

The recent item data from the Jump Lists populate these two folders. Each program will have its own file name, referred to by its "Jump List ID" and may have both an Automatic Destinations-ms and Custom Destinations-ms file. By examining each file with a text editor, it can be determined which file links to which program's Jump List entry.

More jump list IDs can be found at http://www.forensicswikiorg/wiki/List of Jump List IDs. This is not an exhaustive list, and a program's Jump List Id will often change each (program) version update.

A Jump List is an Object Linking and Embedding (OLE) compound file. It is a container that defines blocks that are assigned to a stream using multiple allocation tables, and is not unlike the FAT file system. There are two main parts to a Jump List - the Destination List (Dest List) and the Link Files themselves. 'The Dest List is a brief listing of all items in the Jump List, their path, date and time and the entry number for each item. This view is useful to try and find a specific item.

There will also be a more detailed entry for each file in the Jump List, which contains the same information as a Link File.

Most major forensic tools will parse Jump List content; however, a useful free tool is available for examining automatic custom lists, called Jump Lister:

http://www.woanware.co.uk/forensics/jumplister,

Figure shows Jump Lister displaying the Destination List.

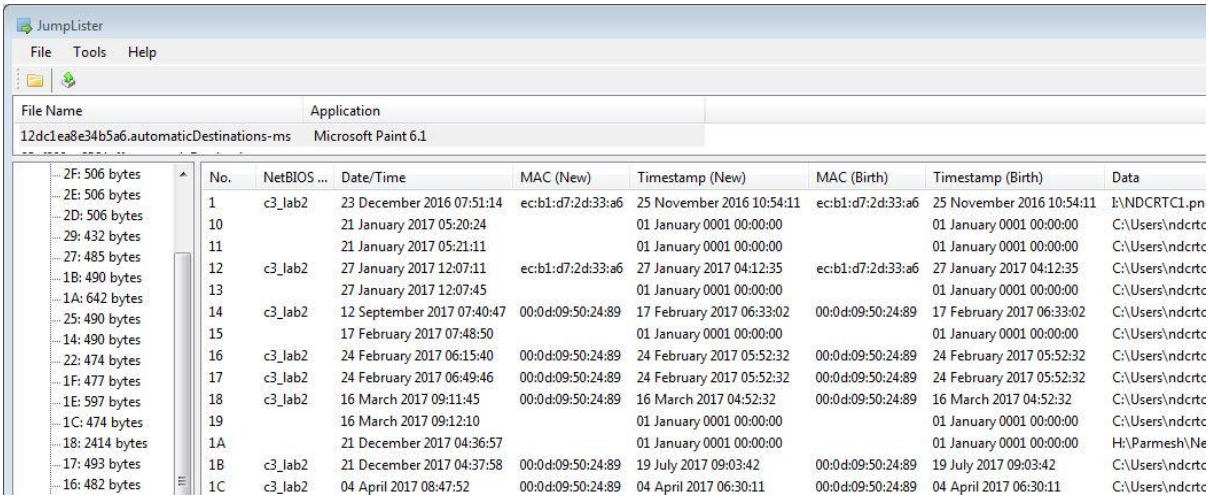


Figure: Jump list content

Within each of the data streams is a Link file, and as such, the same information can be found including: The Created and Modified Timestamps, the Serial Number of the volume the item was located on, the type of volume and the full path. This information is extremely useful to tie a piece of removable media that contains evidence not only to the exhibit computer, but also to a specific user account. Figure 5.15 shows the details stored in Jump List entry 13 when viewed by Jump Lister.

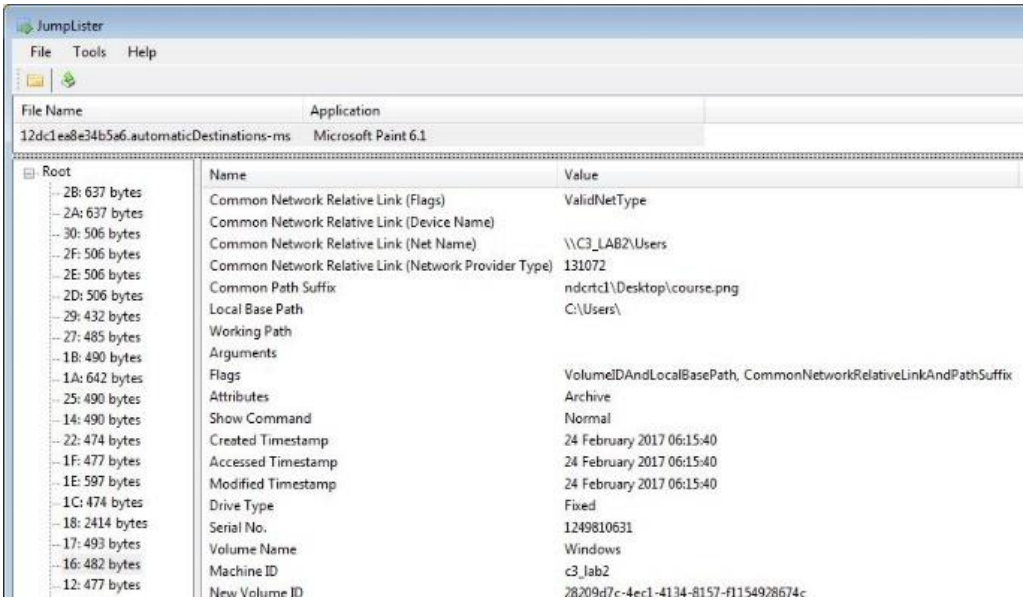
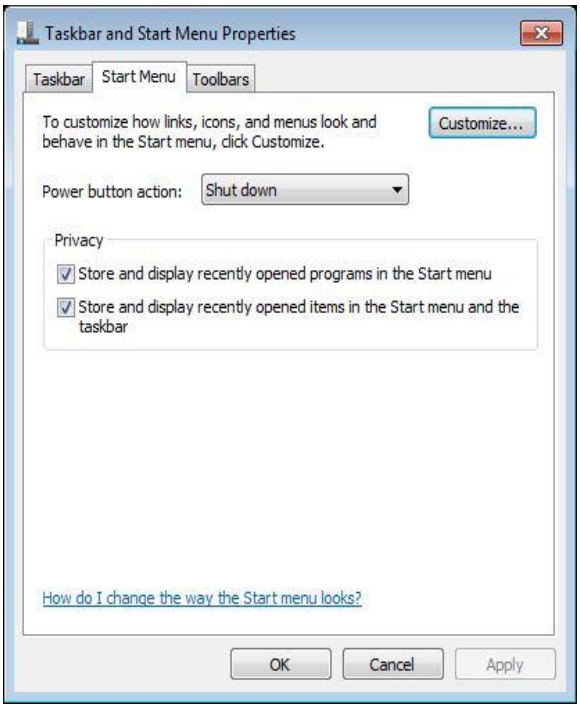


Figure: Jump list entry content

Windows 7

By default, Jump Lists are enabled in Windows 7, and will display up to the last ten files opened by an application. It can be disabled by the user in the Task Bar and Start Menu Properties, as shown in Figure 5.16. Although it only shows the last ten items, many more are recorded in both the Recent Folder and the Jump Lists,



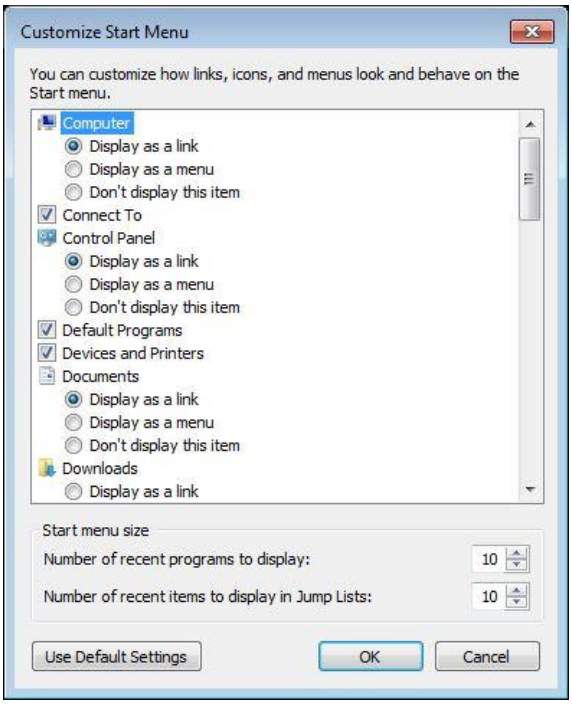


Figure: Jump list entry content

Windows 8

Jump Lists remain enabled by default in Windows 8, and have been evolved for the Start Experience. A feature called Secondary Tiles also utilizes Jump Lists, where a user can pin a new tile to the Start Experience for a part of a metro app. An example may be a pinned tile for a specific web site, The Taskbar properties has a new Jump Lists tab for all settings in Windows 8, as seen in Figure 5.17.

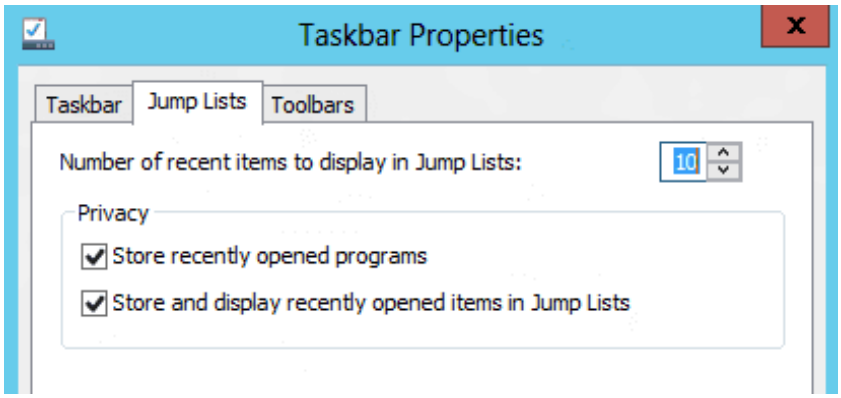


Figure: Windows 8 Jump list setting

Windows 10

Jump lists are enabled by default in Windows 10 and users still have the ability to disable their use in the Start Menu and on the Taskbar. In Windows 10, the binary structure of the destination list has changed slightly which has created issues for some of the tools described above. The destination list and Link files are still viewable with a compound file viewer and with most major forensic tools.

Also, in Windows 10, Microsoft has added functionality with Windows Explorer tying into the Jump Lists, specifically the "Frequent Folders" view in "Quick Access". The file with the Jump List ID "01b4d95cf55d32a", is the location utilized by Windows Explorer to populate the Frequent Folders viewed. Within the Frequent Folders Jump List a user can pin folders to Quick Access, manually adding data to this Jump List, and/or the Operating system will track 4 folders automatically which the user frequently interacts with.

When a folder is manually pinned to the Frequent Folders view, it is given a pinned status and location. The order is logically first at the top left then reading to the right. Shown in Figure 5.18 is the pin order, 1 will begin at the top left of the Windows Explorer Frequent Folders.

#	App ID	Linked Path	Volume Name	Volume Serial Number	Target NetBIOS Na...	Accessed Count	Pin Status
6	f01b4d95cf55d32a	C:\Users\Student\Desktop\One more folder	TI10657300E	AC12CDF7	laptop012	10	Not Pinned
2	f01b4d95cf55d32a	C:\Users\Student\Desktop\Registry Practical	TI10657300E	AC12CDF7	laptop012	57	Not Pinned
21	f01b4d95cf55d32a	C:\Users\Student\Videos	TI10657300E	AC12CDF7	laptop012	1	Pin order 1
17	f01b4d95cf55d32a	C:\Users\Student\Downloads	TI10657300E	AC12CDF7	laptop012	15	Pin order 2
22	f01b4d95cf55d32a					0	Pin order 4
18	f01b4d95cf55d32a	C:\Users\Student\Desktop	TI10657300E	AC12CDF7	laptop012	17	Pin order 4
20	f01b4d95cf55d32a	C:\Users\Student\Documents	TI10657300E	AC12CDF7	laptop012	1	Pin order 5
19	f01b4d95cf55d32a	C:\Users\Student\Pictures	TI10657300E	AC12CDF7	laptop012	1	Pin order 6
16	f01b4d95cf55d32a	C:\Users\Student\Desktop\bjcavsfan	TI10657300E	AC12CDF7	laptop012	3	Pin order 7
15	f01b4d95cf55d32a	C:\Users\Student\Desktop\New folder	TI10657300E	AC12CDF7	laptop012	0	Pin order 8
14	f01b4d95cf55d32a	C:\Users\Student\Desktop\FAT Practical	TI10657300E	AC12CDF7	laptop012	0	Pin order 9

Figure: Windows 10 frequent folders pinned status

The automatically pinned folders displayed are populated using the access count in the Jump List. The access count has not proven to be completely reliable for an actual count of access by a user, however it does show interaction with folders and the access count typically increases with more frequent use, but this is not always 100% accurate.

During testing it was also determined that the highest Access Count was not always automatically pinned, however the folders automatically pinned always came from the highest part of the list. The Jump List also tracks additional folders accessed, which are not pinned nor automatically displayed by Windows Explorer. The "Frequent Folders" view may also continue to show folders to the user that he/she has already deleted.

- **Recycle Bin**

The Recycle Bin was designed by Microsoft to protect user's data from accidental deletion, and to protect users from themselves, by "recycling" unwanted files instead of deleting them, as shown in the Delete File confirmation dialogue - "..move this file to the Recycle Bin?", in Figure 5.19.

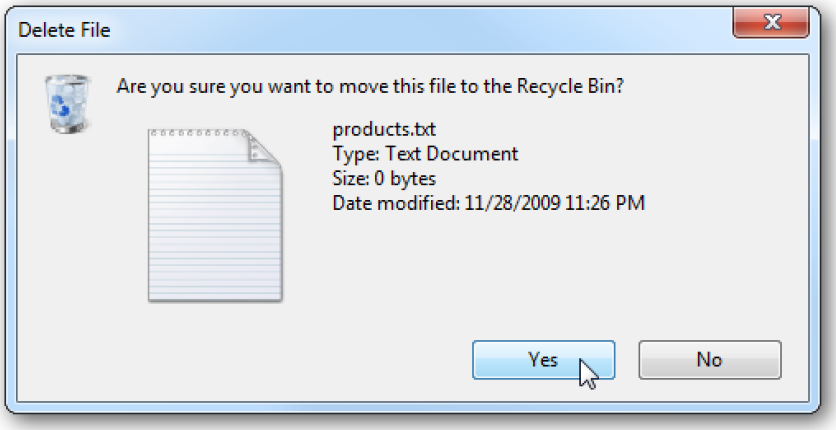


Figure: "Delete" File warning

The Recycle Bin is a series of hidden system folders that contain the unwanted files. When a user "deletes" a file in Microsoft Windows, the file content is not deleted or moved. The directory entry is moved (FAT) or the $MFT entry is changed (NTFS) to show that the file is now located in the Recycle Bin.

A Recycle Bin is only created on volume marked as a Fixed Disk (non-removable). The on-disk format and operation of the Recycle Bin is affected by two things - the version of Microsoft Windows and the file system in use. The effect of the files system is the same on all versions of the Microsoft Windows Operating System:

- On a FAT volume, all Recycle Bin files are stored under the root folder.
- On an NTFS volume, the first time a user deletes a file, a folder is created under the Recycle Bin, and is given a file name which is the user's Security Identifier (SID). Everything that is deleted by this user account is then placed under this folder.

The SID is the same as used in Registry, and can be matched to the user's name in the Registry Key:

HKLM\SOFTWARE \ Microsoft\WindowsNT\CurrentVersion\ProfileList.

A Recycle Bin that Contains multiple SID's with different domain or computer identifiers indicates the volume may have been connected to multiple Computers, or accessed by users from different domains.

In all versions of Windows, pressing Shift+Delete will bypass the Recycle Bin, and the files will be marked as deleted in the file system, as shown in the Delete File confirmation dialogue "...permanently delete this file?" in Figure 5.20 - note that there is no Recycle Bin icon in this window.

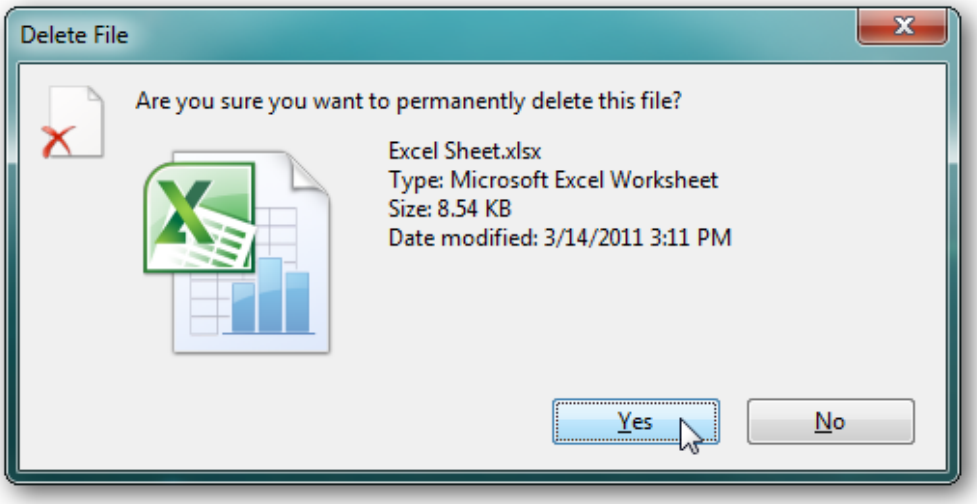


Figure: "Delete" File warning

In Windows XP, the Recycle Bin is actually a hidden system folder in the root of the volume. The folder name is dependent on the file system:

- "Recycler" on NTFS volumes - %drive letter%\Recycler\%SID%\
- "Recycled" on FAT volumes - %drive letter%\Recycled\

By default, the Recycle Bin can grow in size up to ten percent of the volume size. Any files/folders that are too large for the Recycle Bin will be deleted. Figure shows the Recycle Bin on an NTFS volume, with two SID's.

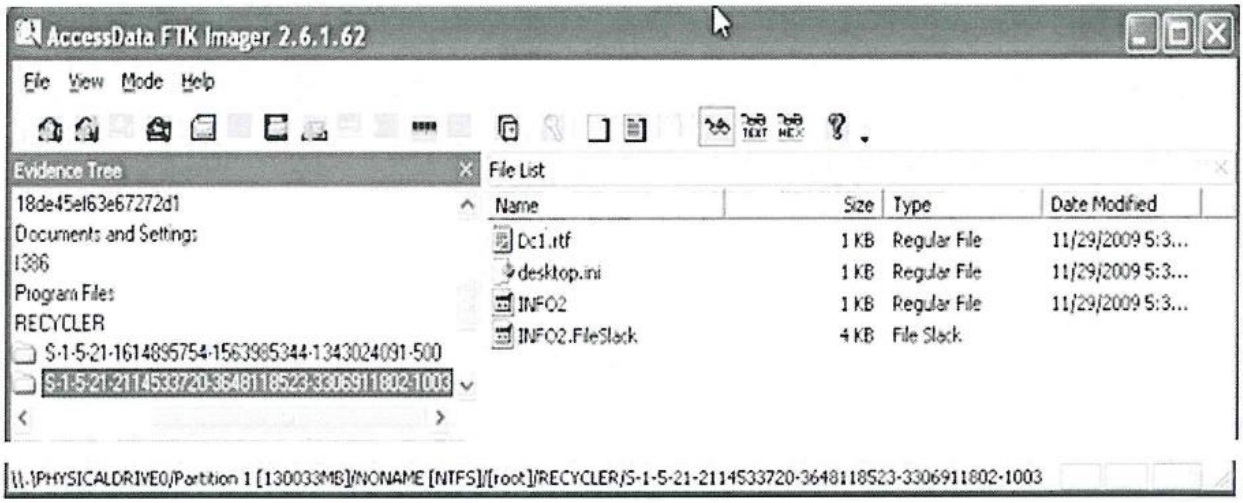


Figure: user-1003 Recycle Bin Files

The SID's in the Recycler shown in Figure 5.21 have different domain/computer identities. This can mean that the volume has been connected to more than one computer or that the volume has been connected to one computer, where a user with a domain account has recycled files and a local computer account have recycled files.

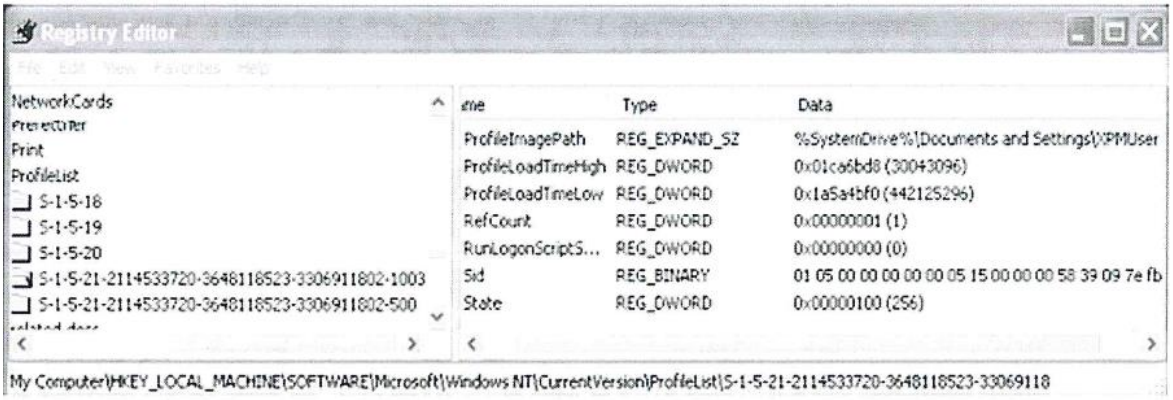


Figure: user – 1003 User Profile Path

By default, Windows creates a Recycle Bin folder on each non-removable drive it connected to the system. The recycle bin located on the Desktop shows files deleted from all non-removable volumes on the system. Microsoft maintains an INFO2 file within each \Recycler folder, which contains the original path of the deleted files.

When a user or Windows compliant application deletes a file, three things occur - with slight differences for each file system:

1. **NTFS** - The File Record is changed to show a new parent $MFT record number for the folder with the account SID - \\Recycler\%SID%.

FAT - The first character of the file name is replaced with 0xE5 to show the deletion.

When a directory is deleted on a FAT volume, the parent directory entry is marked as deleted by replacing the first character in the directory name with OxE5. The file names within the deleted directory are NOT changed.

2. NTFS - the file name is changed.

FAT - A new directory entry is created for the file in the \Recycler folder. With the exception of the file name, the new entry in the \Recycler folder contains the same file attributes, file dates/times, and starting cluster number as the original entry.

3. A new entry is added to the INFO2 file located in the \Recycled (or \Recycler\%SID%) folder. 800 bytes are allocated for each entry in the INFO2, which contains:

- Date and time of deletion.
- File Size.
- It's index number in the recycle bin (its order in the recycle bin)
  - 1is assigned to the first file,
  - 2 to the next,
  - etc.
- The Path and original file name of the file deleted to the recycle bin.

XP Recycle Bin File Name Rules:

The file name for the new entry in the \Recycler folder follows a very specific file naming convention. This naming convention is:

- Drive letter,
- File number,
- Original file extension.

Take for example, the file C:\My Pictures\bomb diagram.jpg. If this was deleted to an empty Recycle Bin, the new file name would be:

DC1JPG - Drive C, first file deleted, JPG extension retained.

If the file D:\Secret\Payments.xls was Recycled and the user's SID folder already contained four files, then new file name would be:

DDOS.XLS - Drive D fifth deleted file.

When the Recycle Bin is emptied, if the last file in the recycle bin was entry number 10 and the bin was emptied, the next deleted file sent to the recycle bin would be 11. If the user empties the bin and logs off, the count is reset to 1.

EMPTYING THE RECYCLE BIN

If an individual file is removed from the Recycle Bin, (it is restored, or deleted) the first character of the ASCII path in the INFO2 file is changed to 0x00.

If the entire Recycle Bin is emptied, Windows, resizes the INFO2 file to 20 bytes and modifies the Desktop.ini file. It should be noted that even though the INFO2 file has been resized, the previous entries, or portions thereof, may be recoverable.

The modified date of the file desktop.ini is a good indication of then the Recycle Bin was emptied.

$RECYCLE.BIN — VisTA,7,8 AND 10

There has been a significant change to the way Windows Vista\7\8\10 stores deleted files. The Recycle Bin is still a hidden system folder but the name has been changed to $Recycle.Bin.

As with Windows XP, it is configured for each logical drive and is not created on drives marked "removable". The folder name for the Recycle Bin has been renamed, and is the same for both FAT and NTFS file systems:

- FAT - %drive letter%\$Recycle.Bin\.
- NTFS - %drive letter%\Recycle.Bin\%SID%\.

The first notable change is that the individual SID (user folder) is created when a user logs on for the first time. The most significant change is that the $Recycle.Bin uses a set of paired files to track one deleted item.

FILE DELETION

When a file is deleted, the original directory entry is still marked as deleted in the same way in FAT, or if it is NTFS, the $MFT is changed in the same way as described during an XP Recycle function.

This original file becomes the first of the paired Recycle Bin files, and is renamed "$Rxxxxxx" - $R followed by a random six alphanumeric character file name. The extension from the deleted file remains the same. This file contains the content of the original file.

Example >>> MyPicture.jpg – will become - - - - **$R123456.jpg**

The second paired file is an administrative file and the file name is starts with $I, then has the same random six characters as the $R and the extension - - - **$I123456.jpg**.

This file is 544 bytes long, in Windows Vista,7 and 8, but in Windows 10 the file uses additional values to determine the length of the file path and name, only using what is necessary. The $I file tracks the deleted file's time of deletion (offset 0x10) and the full path to the original location. There are few differences with regard to Windows Vista, 7,8 and Windows 10, however there are two main differences to keep in mind. The first change is that the header of the $I file changed from 0x01 00 00 00 00 00 00 00 to 0x02 00 00 00 00 00 00 00. The second change is that the $I file now tracks the length of the file path and name so that it doesn't have to assign 544 bytes to each $1 file. Figure 5.24 shows the $R and $1 files.

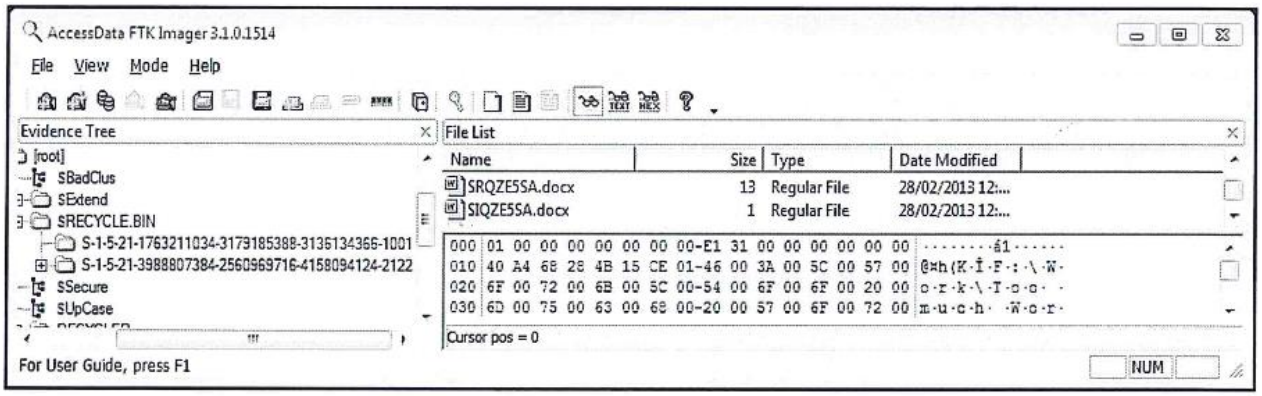


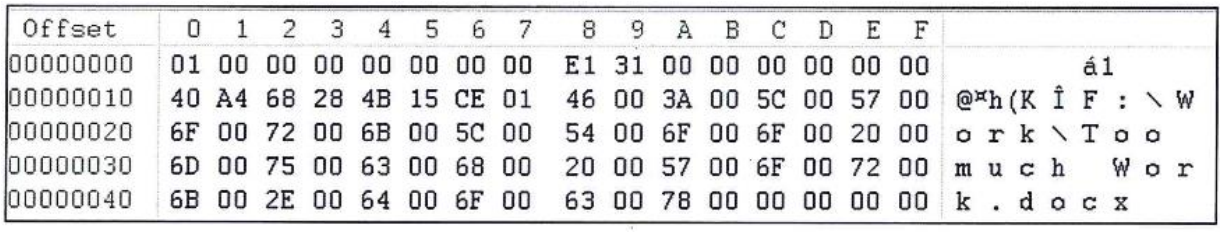
Figure: $Recycle.Bin $I file content

The data structure for the $I file in Windows Vista,7 and 8 is given in the table 5.3

Offset	Length	Description
0x00	8 bytes	File Header
0x08	8 bytes	Original File Size in bytes
0x10	8 bytes	File Recycled Time (FILETIME – UTC)
0x20 / 18	~	Original File Name and Full Path - Unicode

Table: $I file structure

A $I file is shown figure 25



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	01	00	00	00	00	00	00	00	E1	31	00	00	00	00	00	00	á1
00000010	40	A4	68	28	4B	15	CE	01	46	00	3A	00	5C	00	57	00	@¤h(K Î F : \ W
00000020	6F	00	72	00	6B	00	5C	00	54	00	6F	00	6F	00	20	00	o r k \ T o o
00000030	6D	00	75	00	63	00	68	00	20	00	57	00	6F	00	72	00	m u c h W o r
00000040	6B	00	2E	00	64	00	6F	00	63	00	78	00	00	00	00	00	k . d o c x

Figure: $I file content

The original file was F:\Work\Too much Work.docx. It was 0x31E1 (12,679) bytes long and was recycled on 28 February 2013 00:32:58 UTC.

The data structure for the $1 files in Windows 10 is given in the Table 5.4.

Offset	Length	Description
0x00	8 bytes	File Header
0x08	8 bytes	Original File Size in bytes
0x10	8 bytes	File Recycled Time (FILETIME – UTC)
0x18	4 bytes	File path length (in ASCII characters)
0x1C	~	Original File Name and Full Path - Unicode

Table: $I file structure

DIRECTORY DELETION

If a directory is deleted, then there will be a $R and $I entry in the Recycle Bin for that directory. The $R will still contain all the sub-directories and files with their original (unaltered) names. The directory (FAT) or INDX (NTFS) content remain unchanged.

EMPTY RECYCLE BIN

On removal from $Recycle Bin, the files are deleted but may still be recovered.

There has been a lot of speculation that Windows 7and 8 may deliberately over-write (wipe) files that have been deleted after the Recycle Bin is emptied, or deleted files that have bypassed the Recycle Bin. Before passing judgment on this theory, two points need to be taken into consideration.

- While a Windows operating system is in a powered-on state, there is a lot of disk activity on the system drive (C:\), even though there is no user interaction and it appears there may be no applications open. But Windows Defender will be running, Windows Update may be downloading patches, Windows Search is Indexing, in addition to all the system files that Windows interacts with in the background.
- Due to the nature of NTFS, a $I record will be resident in the $MFT. Combined with the constant disk activity, the $MFT entry is often reassigned quite quickly, making the $1 content unrecoverable. The same applies with the $MFT entry for the $R record.

Microsoft Windows 7,8 and 10 do not deliberately wipe deleted files - regardless if they have been through the Recycle Bin or bypassed it. Normal Windows activity on a running system will over-write deleted files and make it appear that wiping is occurring. This is proven by running the test on a non-system volume, or by using a large number of test files.

Once the file records have been re-used, remnants of the file content can be carved from unallocated space.

❖ RAM Files

Random Access Memory (RAM) is volatile (data not retained when power is removed), high speed memory that is used by a computer system to store data for quicker access by the processor than if the data had been retrieved from the hard drive. RAM is allocated in blocks, called pages, which are typically 4096 bytes. The operating system manages the RAM, and allocates the RAM pages to it, to running programs, and to files that are currently in use.

Windows uses special files on the hard disk for to help manage RAM, called virtual memory. This virtual memory is used to enhance performance, by creating making the RAM appear larger or by speeding up the shut-down / start-up process.

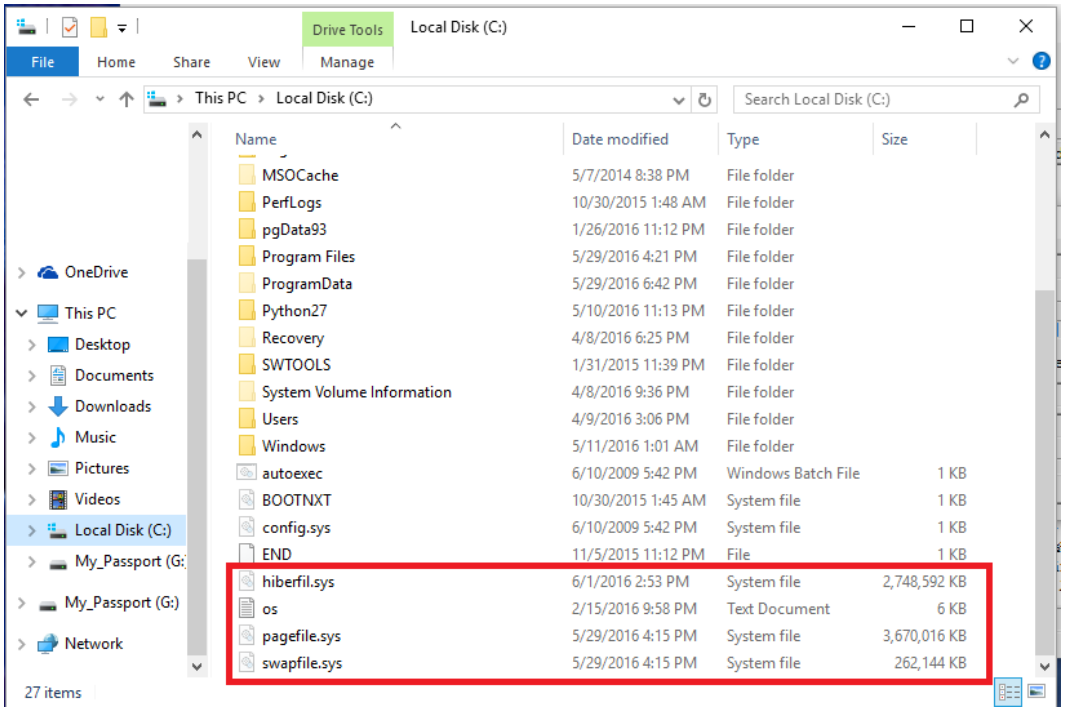


Figure: Picture of Pagefile.sys

Pagefile

Windows uses a pagefile file(s) to hold parts of programs and data that do not fit in memory. The operating system moves data from the pagefile to memory as needed and moves data out of memory to the pagefile to make room for new data. On XP, Vista and 7 systems it is named pagefile.sys. Windows 8 and 10 added a second virtual memory file named Swapfile.sys.

The pagefile is potentially a dynamite location to find data that the user does not know is still on the disk. In fact, while running, the contents of pagefile are not accessible to the user. Although the content is not formatted for easy reading, passwords, graphics, text files, file names, URLs and other valuable information is often found within this file.

Figure 37 shows a .jpg image that was a screen shot of a Windows 7 start menu found in a pagefile. A file does not have to be saved to the internal hard drive to be found in the page file - if it was created on the computer and not saved, it may appear in the pagefile.sys.

By default, pagefile.sys is created in the root folder of the drive that holds the Windows system files. The user can change the size of the pagefile, move it to a separate physical drive, spread it across multiple disk drives or even disable it. The default file size of pagefile.sys will range between 1.5 to 3 times the sizes of the physical RAM; however, the pagefile.sys file size will not decrease.

When the system is shutdown, the paging file remains intact. However, the Registry key below can be set to 1, in which case Windows will fill inactive pages in the paging file with zeros whenever you shut down the system. HKLM\System\CurrentControlSet\Control\Session_Manager\MemoryManagement\ClearPageFileAtShutdown.

Windows 8 and 10

In Windows 8 and 10, Microsoft utilizes two swap files, Pagefile.sys and Swapfile.sys to handle the operating system demand on the RAM, as shown in Figure 44. According to Microsoft, the Pagefile is utilized for RAM, and the Swapfile is utilized for swapping out applications - more specifically for metro mode applications. Therefore, it increases the chance to finding important artifacts from the swap file.

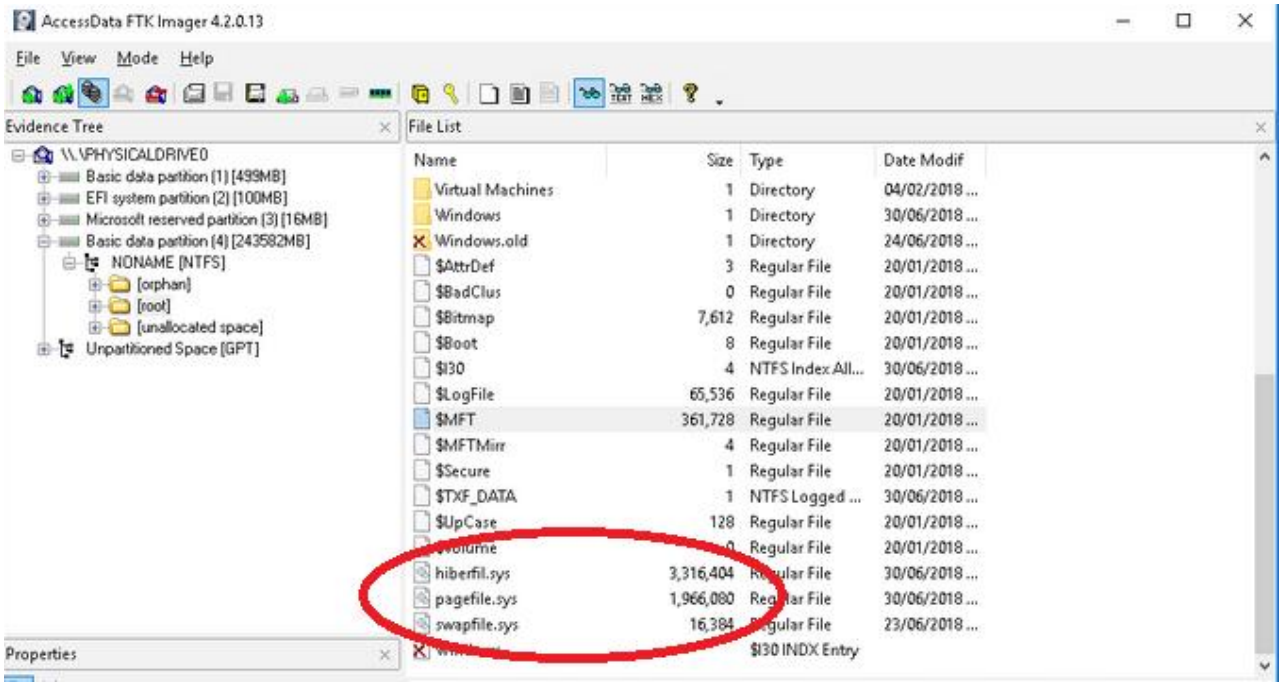


Figure: Windows 8 Ram swap files

Hibernation

Hibernation is a power mode that allows the computer to power completely off, but retain its current state. All open programs are retained by saving the content of the Random-Access Memory

to the hard disk drive, in a C:\Hiberfil.sys. When the computer is powered back on, the contents of Hiberfil.sys is copied into RAM, and the computer returns to the same state as when the computer was shut down.
Just like the RAM and swapfiles, Hiberfil.sys will often contain files or parts of files that the user has been working on, even if the user didn't save those files to the internal hard drive. The hiberfil.sys files is compressed and can be read using MoonSols Windows Memory Toolkit, http://www.moonsols.com/windows-memory-toolkit/.

Analyzing RAM Files

A RAM file and a RAM dump both contain live data which can include unencrypted passwords, and running program data. The latter is very important when investigating a computer that may be infected by a virus or other exploit. In depth RAM analysis is beyond the scope of this course, and requires specialized tools to be done effectively. Some RAM analysis tools are discussed below.

Strings

Strings.exe (http://technet.microsoft.com/en-us/sysinternals/bb897439) is a command line utility for extracting Unicode and/or ASCII strings, which may include plaintext passwords. It will work on any type of file and makes a dictionary file that may assist cracking encrypted files. To use:

1. Copy stings.exe in the same folder as the RAM dump or the RAM file - use 8.3 file names.
2. Open a command window and navigate to the folder containing the RAM image and "strings.exe"
3. Run the command specifying:

a. Input file - which file(s) should strings.exe scan for text; and,

b. Output file - where the output should go.

strings.exe [input file name] > [output file name] Excluding Square brackets.

Bulk Extractor

Bulk Extractor (http://www.forensicswiki.org/wiki/Bulk_extractor#Download) is a simple Graphical User Interface (GUI) program, which requires Java to be installed.

Like strings, it will get ASCII and Unicode strings, but also refine the results into credit card numbers (ccn), e-mail, MAC addresses, Uniform Resource Locators (URL) and telephone numbers, and much more, as shown below.

To run the tool > select tools > Run Bulk Extractor. There is a list of scanners that can selected to find selected information.

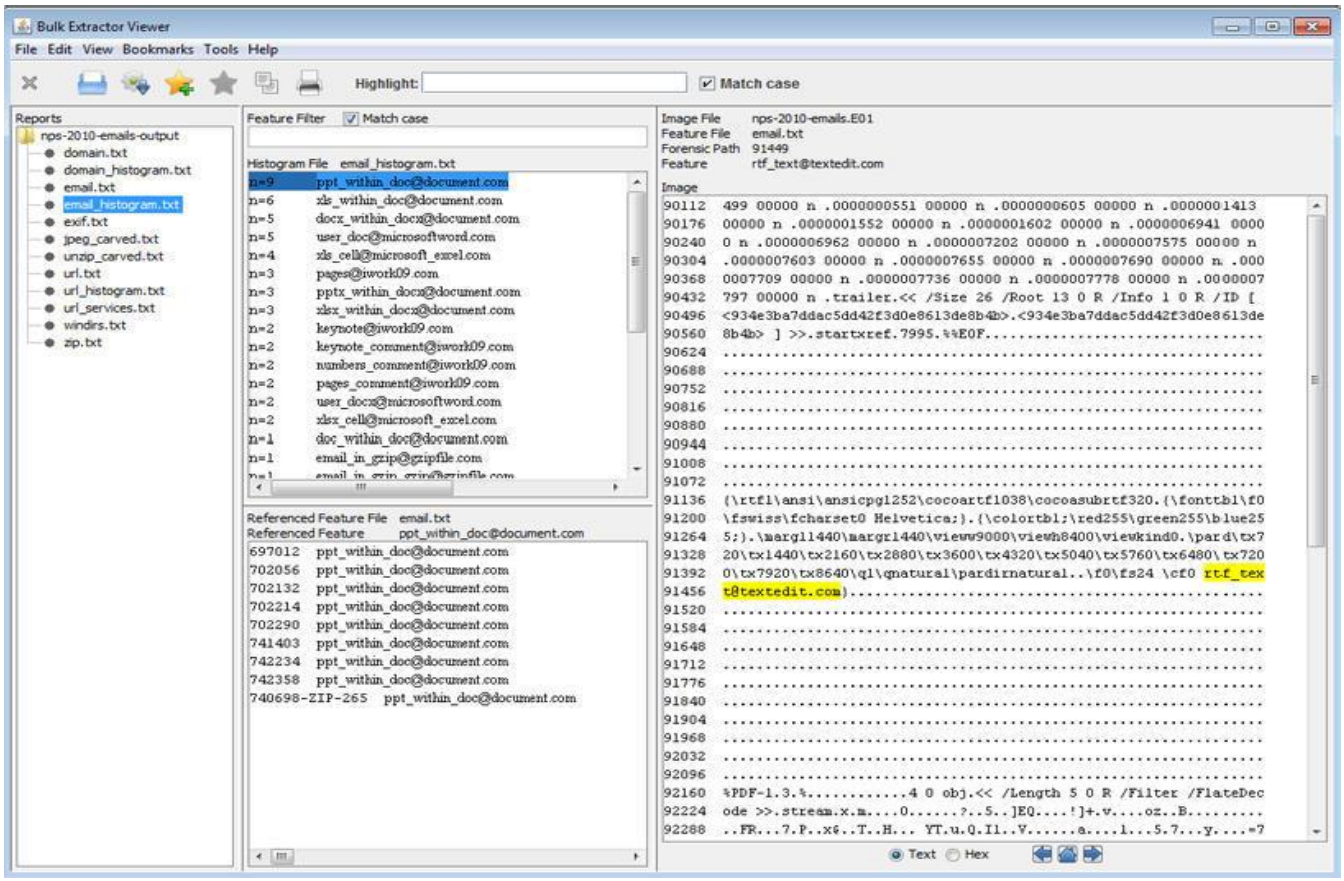


Figure: Bulk Extractor

Mandiant Redline

Redline (https://www.mandiant.com/resources/download/redline) is probably the most powerful GUI RAM application, when you get past the default scripts or configure a series of capture and analysis scripts that work! The drawbacks are that it is still experimental for Windows 8 and it will only analyze RAM image files in Data Dump (DD) format, and the analysis computer must have sufficient RAM to load the entire RAM image.

SIFT Workstation

The SIFT workstation (http://digital-forensics.sans.org/community/downloads) is an advanced and completely virtual machine based forensic investigation tool, with powerful utilities tool for RAM analysis. It must be run in VMWare, and is predominantly command line based (for RAM tools).

Volatility

The Volatility Foundation (http://www.volatilityfoundation.org/) released Volatility in 2007 as an Open Source Project to support memory forensic analysis. Volatility is multiplatform tool which integrates structured analysis of memory samples. This tool is a command line-based tool which incorporates plugins for various Operating Systems, applications, and platforms (i.e. Windows, Linux, and Mac).

❖ **Backup and Restore**

System Restore and backup tools in Windows operating system are very useful in forensic investigations, as they contain a history of what was on the computer and what user interaction there has been over a period of time. They can contain valuable evidence that has been deleted, but Windows has kindly preserved without the suspect knowing. The Backup and Restore feature have changed significantly with different releases of Windows Operating System.

Restore Points (WINDOWS XP)

Windows XP System Restore is a feature designed to allow the user to restore the PC, in the event of a problem, to a previous known state without losing personal data such as documents, favorites, e-mail and history lists. It is not unusual to find more than a hundred Restore Points on a system.

By default, System Restore creates Restore Points daily and whenever a significant event occurs, for example an application or device driver installations.

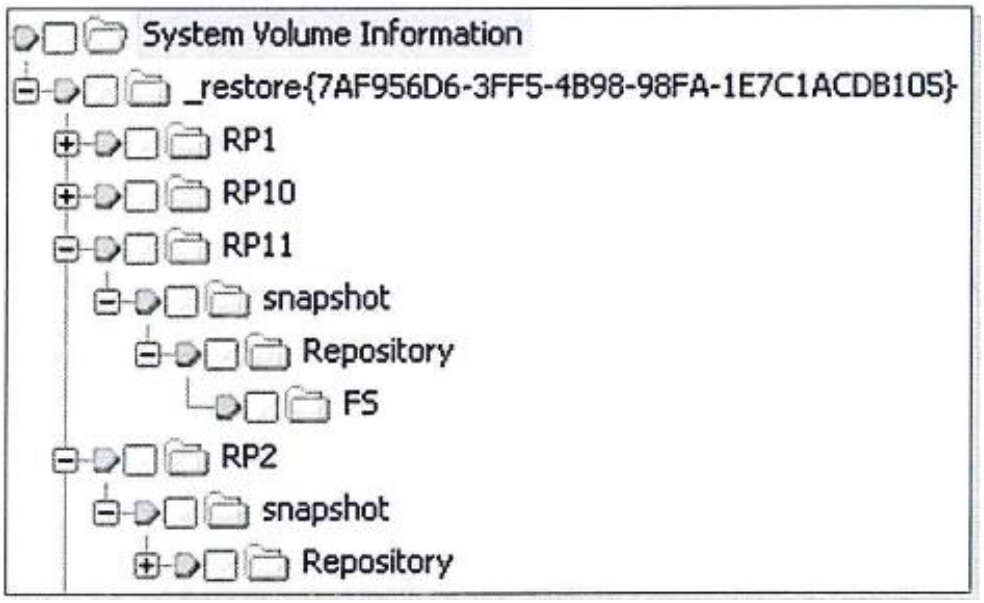


Figure: Restore point

The actual restore points are stored a _restore subfolder within the folder the folder "System Volume Information" which is on the root of every volume that has System Restore enabled, as shown in Figure.

The Alfa-numeric designator in the folder name _restore{7AF956D6-3FF5-4B98-98FA-1E7C1ACDB105} is the computers GUID.

Under that folder is a folder for each Restore Point that has been created. These folders are named RP#, where # is an incremental number beginning with 0. It is not uncommon for there to be more than 100 RP# folders on a system, each representing a separate System Restore Point.

The Restore Point numbering is relative to the computer that creates the Restore Point — not the volume. For example, on a new volume, the first Restore Point created may actually be RP197, where restore points RPO - RP196 were made on the C:\ drive only.

The RP# folder contains backup copies of changed and deleted files as well as files created by System Restore that are used to properly restore the system to this Restore Point. One file of particular note in this folder is the RP.LOG file, that contains the name and settings of the restore point.

The Restore Point name is found at offset 0x10 of the file RP.LOG, and the last eight bytes is the date and time (FILETIME) that the Restore Point was created. The file RP.LOG will only be found on the system volume - Restore Point folders on non-system volumes do not have a copy.

Most Restore Points are created by the system in a manner unknown to the user and are stored in a hidden system folder which the user cannot see. This makes them an ideal location to look for evidence in those cases where the subject may have tried to eliminate or hide evidence of his activities

There are two very valuable pieces of information within a Restore Point:

1. The subfolder named \snapshot contains slightly renamed copies of all registry hive files on the volume that contain settings as they were at a specific point in time. Figure 47 shows the Registry files.
2. All shortcuts - shortcuts created by the user and automatically created by Windows XP in the %user_profile%\ Recent folder.

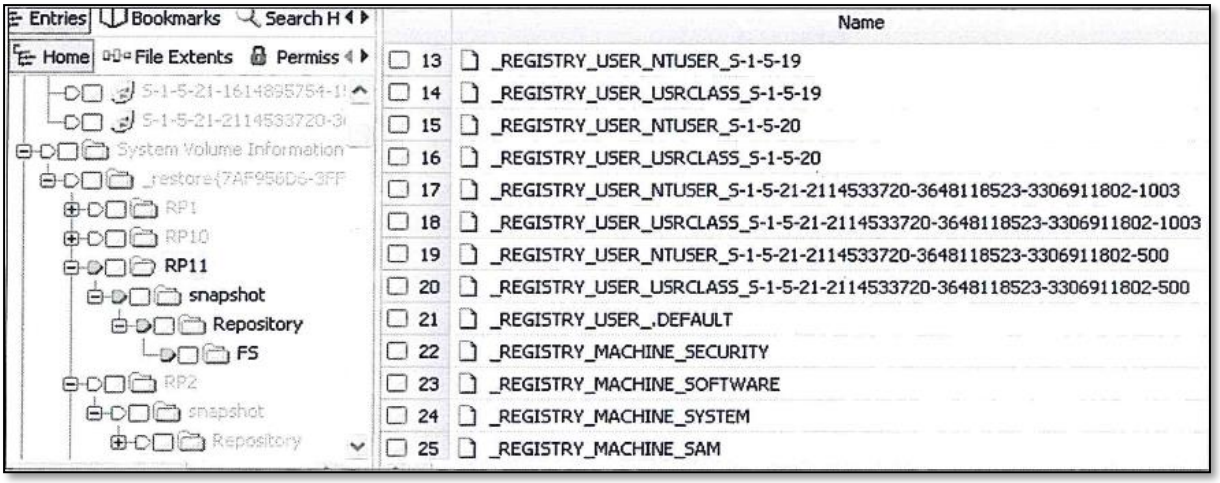


Figure: Registry Keys in Restore Point

Together, these two components of a Restore Point can be used to see what user interaction has occurred with the computer at a specific time.

Restore Points are a very simple back-up — each Restore Point is a Full Back-up, so the files can be examined in isolation to any other Restore Point on the system.

With the release of newer versions of Windows operating systems, Restore Points have been changed to a combination of backup and restore utilities. Variations to each of these utilities have continued with each release, which will be explained below.

File Backup

File Backup is used to back up all files on the system except for system files, program files, the Recycle Bin, temporary files and EFS encrypted files. The backup files can be written to the hard disk, external drive, CD/DVD or a Network. It is primarily designed to backup user files.

Windows vista and 7

The Backup & Restore tool is accessed from the "Back up your computer" tool in the Control Panel, as shown in Figure 5.39.

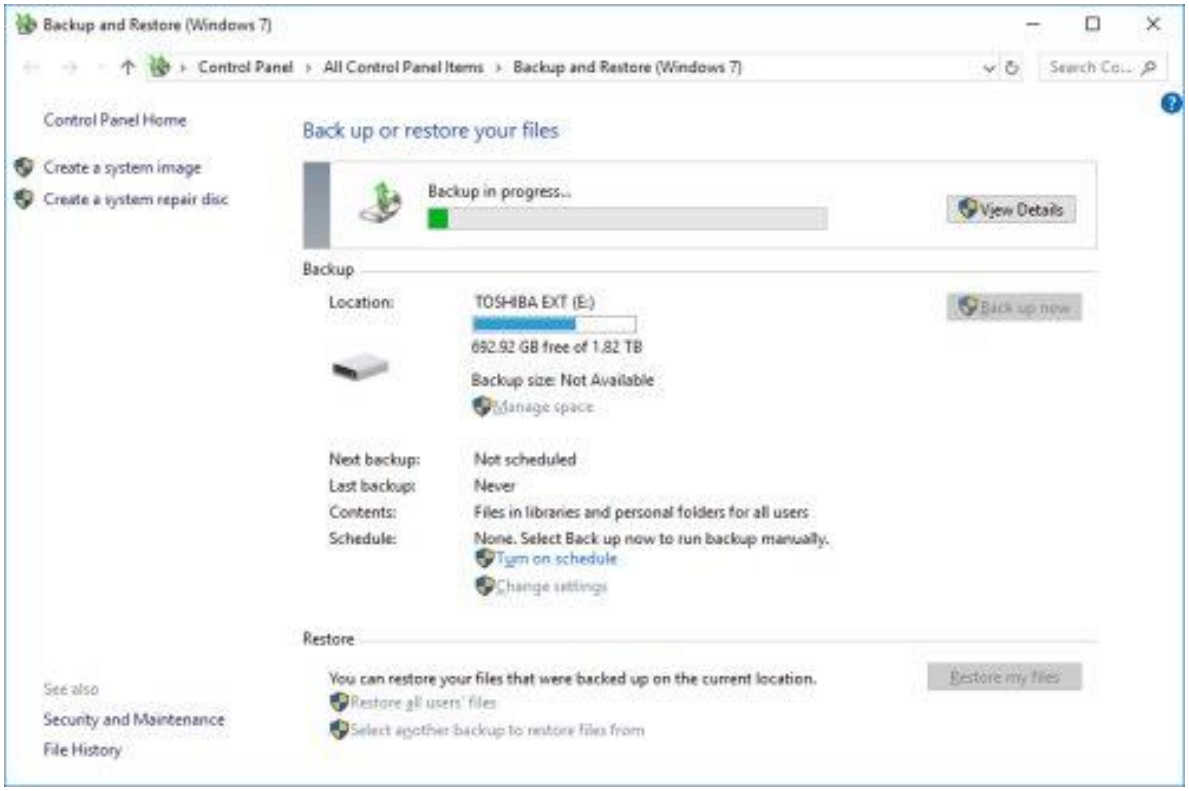


Figure: Windows Backup and Restore

When a user sets up the Backup tool, they must first choose a backup destination, which will generally be an external disk. They user can either manually select what files are included in the backup, or allow Windows to choose, and they can set the frequency that each backup is created.

The backup is saved to the backup destination's (e.g. USB drive) root folder which is given the computer name. A sub-folder is created with the date the backup was set-up in the following format. Each back-up in that set is then placed in a sub-folder which has a file name that includes the date and time the back-up was created.

The backed-up files are stored within zip archives, as shown in Figure 5.40. A large backup may have many hundred zip archives, each of which are normally around 200 Mb in size, but vary depending on how the source files are divided between each archive.

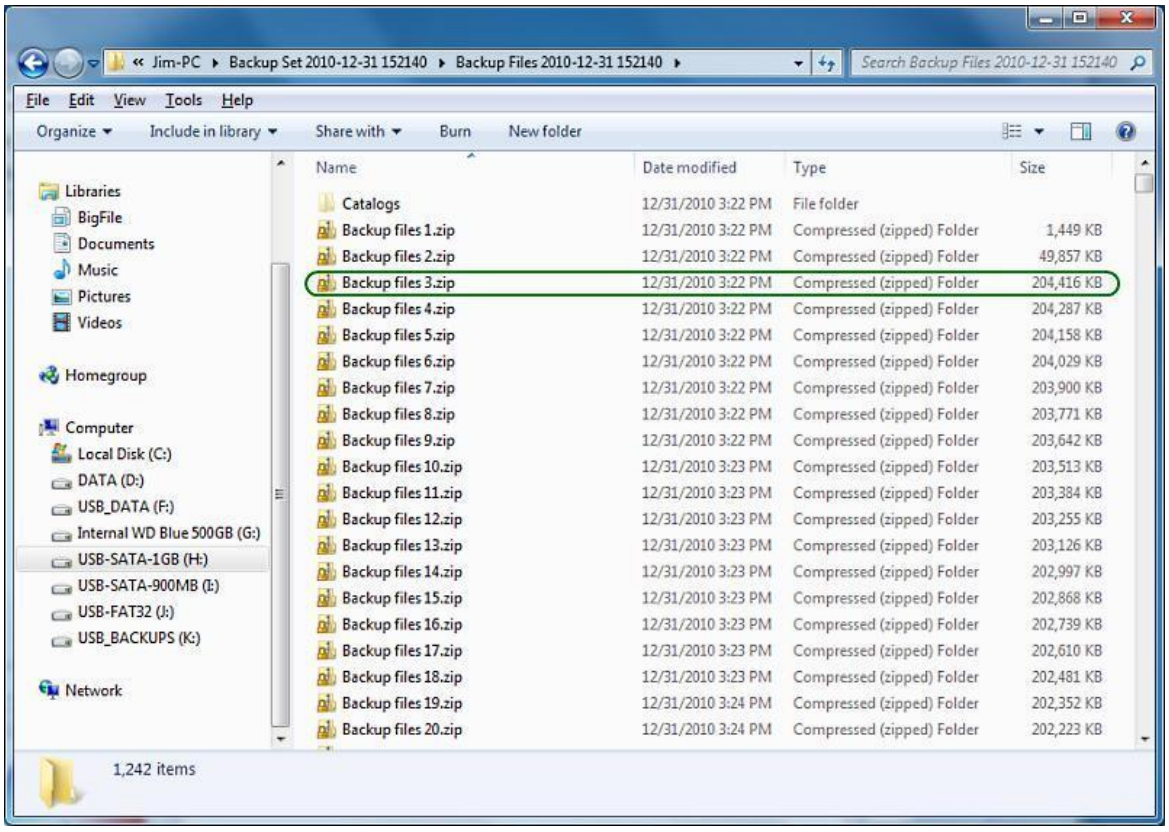


Figure: Windows 7/Vista backup

It is possible to go through each Zip archive to locate a file of particular interest, but it is a very cumbersome method. More importantly, a backup may contain evidential files that have since been deleted, so it is more effective to use the Restore tool to process these files - even when examining a backup of that has been located on an exhibit.

Analysis

Should a Windows Vista or 7 backups be located on a suspect hard drive, it can be connected through a write blocker (or if a forensic back-up be mounted using FTK Imager or EnCase with the Physical Disk Emulator suite) on a Windows Vista, 7 or 8 laboratory computers, as shown under the recovery section.

Windows 8 and 10 - File History

In Windows 8 and 10, File History is the new File Backup Utility. File History is disabled by default, but can be quickly activated in the control panel to back up the users Libraries, Contacts, Favorites and Desktop, or when an external drive is connected. Once enabled, files will be backed up on schedule after changes have been made to their content. File History requires a non-system volume to store the backup, as shown in Figure 5.41

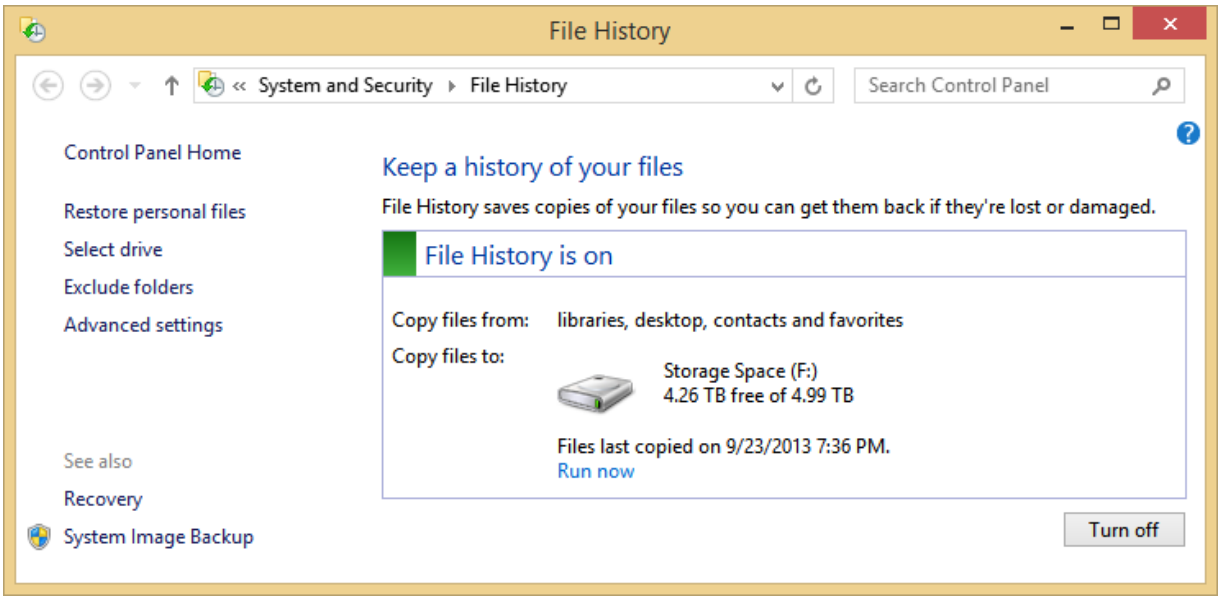


Figure: Windows File history

Windows 8 does not allow a user to select which files to backup, but it does allow users to exclude certain folders or libraries from the back up process by selecting the "Exclude folders" link on the left side of the window shown in Figure. The user can also set the backup schedule.

In Windows 10, specifically through the immersive settings application users now have the ability to add additional folders and not just to exclude. It should be noted that Users still have the ability to interact with File History through the control panel in Windows 10, however if this is used it is not possible to add folders. Adding folders is only available through the immersive settings application.

The backups are stored in a folder called "FileHistory" on the drive the user selected. Unlike Windows 7, the backed-up files are not in zip archives, but are stored within the same folder structure and can be accessed with Windows Explorer. The file name is appended with the date and time that backup version was created in UTC, as shown in the Figure 5.42.

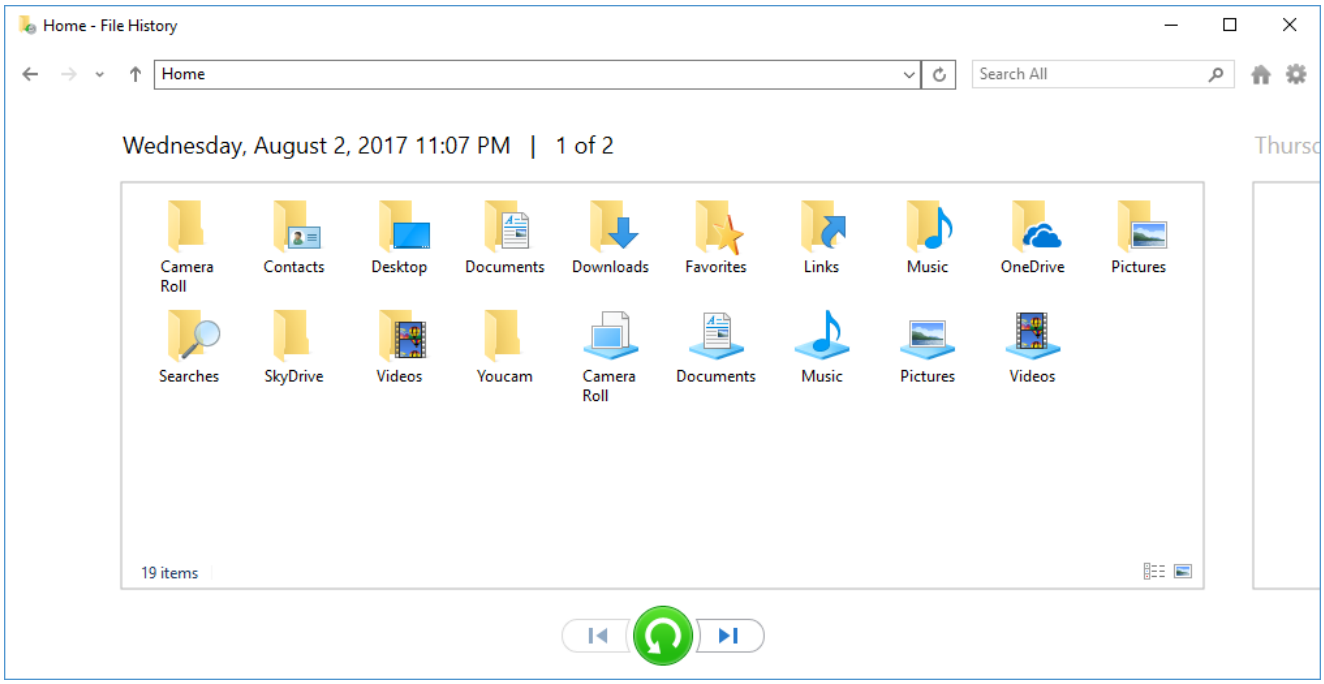


Figure: File History Content

Restoring Backup Files

Windows vista and 7

Because a Windows 7 file backup splits all the files into zip archives, it is much easier to use Windows to restore them to the original file structure on a sterile volume. The following steps show how to do this:

1. Mount the suspect hard drive to a laboratory computer through a write blocker (or if a forensic back-up be mounted using FTK Imager or EnCase with the Physical Disk Emulator suite).
    a. Under Backup and Restore, click “Select another backup to restore files from” as shown in the lower part of the Back and Restore pane shown in Figure 5.39.
    b. The tool will locate all backup sets on every volume mounted to the laboratory computer, and display the volume the backup set is on and the date range.
2. Select the appropriate volume.
3. In the next window, check the box “Select all files from this backup”, and then choose a different date, as shown in the middle pane in Figure 5.43.
4. Note the date and time of the backup, as shown in the right pane in Figure 5.43, and create a folder with the same name on a forensically sterile volume.

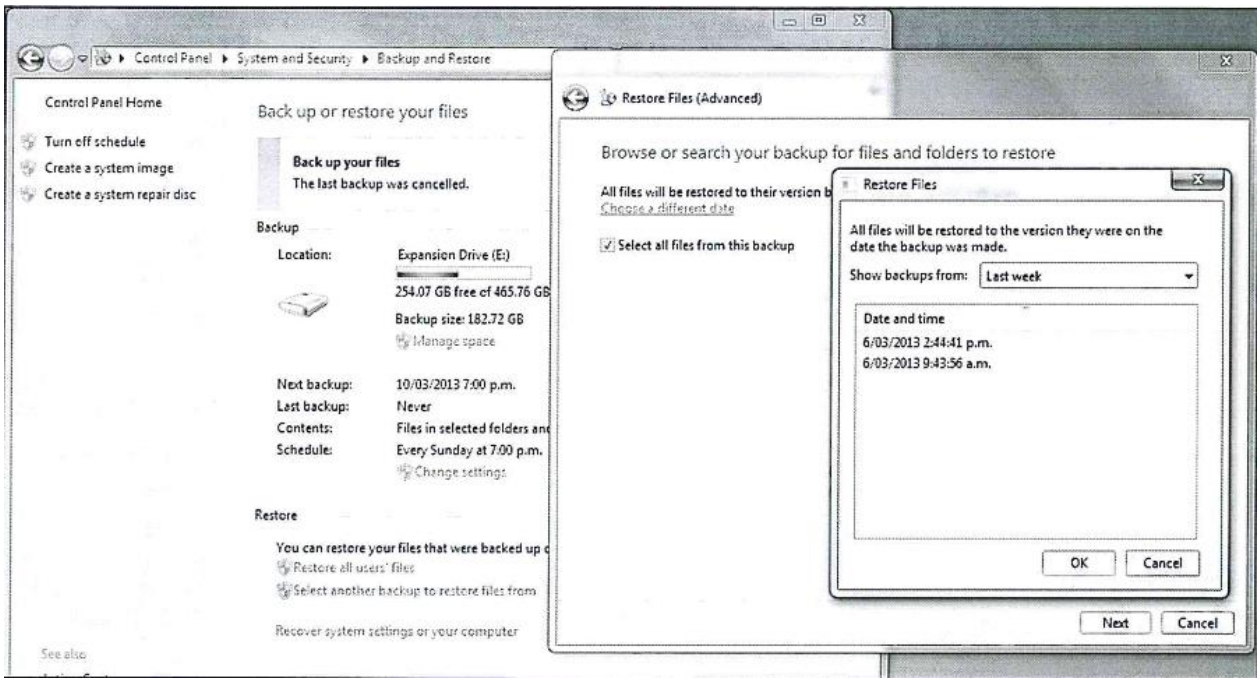


Figure: Restore File Backup

The Back-up and Restore tool can then be used to restore all files to a new location, which should be a forensically sterile laboratory volume. If there are multiple backups, create a folder for each backup named with the date and time of each backup.

5. Restore the files to the folder created in step 5, and ensure the "Restore the files to their original subfolders" option is checked, as shown in Figure 5.44. This will recreate the directory tree structure from the original source.

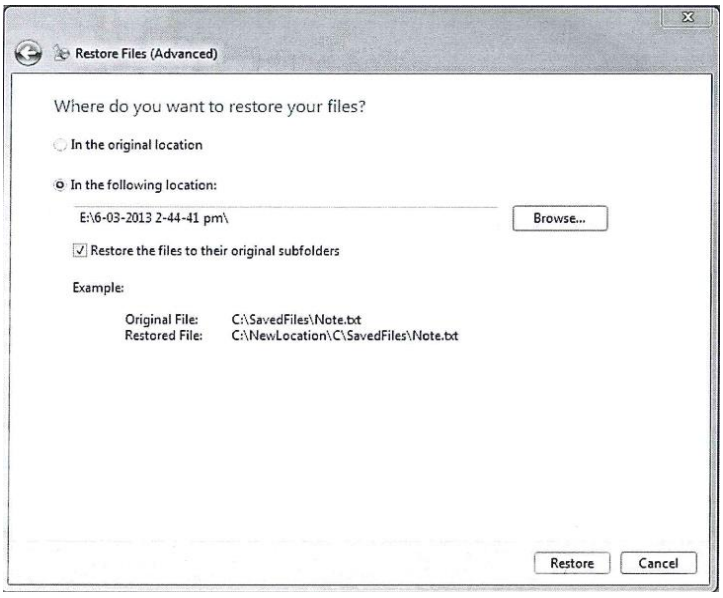


Figure: Restore Path

6. After all back-ups have been restored, create a forensic back-up of the volume for analysis of the previous versions of files, and for files that have been deleted since the backup was created.

   Even though the Windows 7 backup format is different in Windows 8, should a volume that contains a Windows 7 File backup be connected to a Windows 8 Computer, Windows 8 is able to recognize and recover the files.

Windows 8 and 10

In Windows 8 and 10, the user can restore backed up files using the “Restore personal files” tool in File History. The volume that contains the Windows File History should be connected to the examiner's computer with a write blocker first.

It is then possible to restore a complete folder, or browse down to an individual file, as shown in Figure.

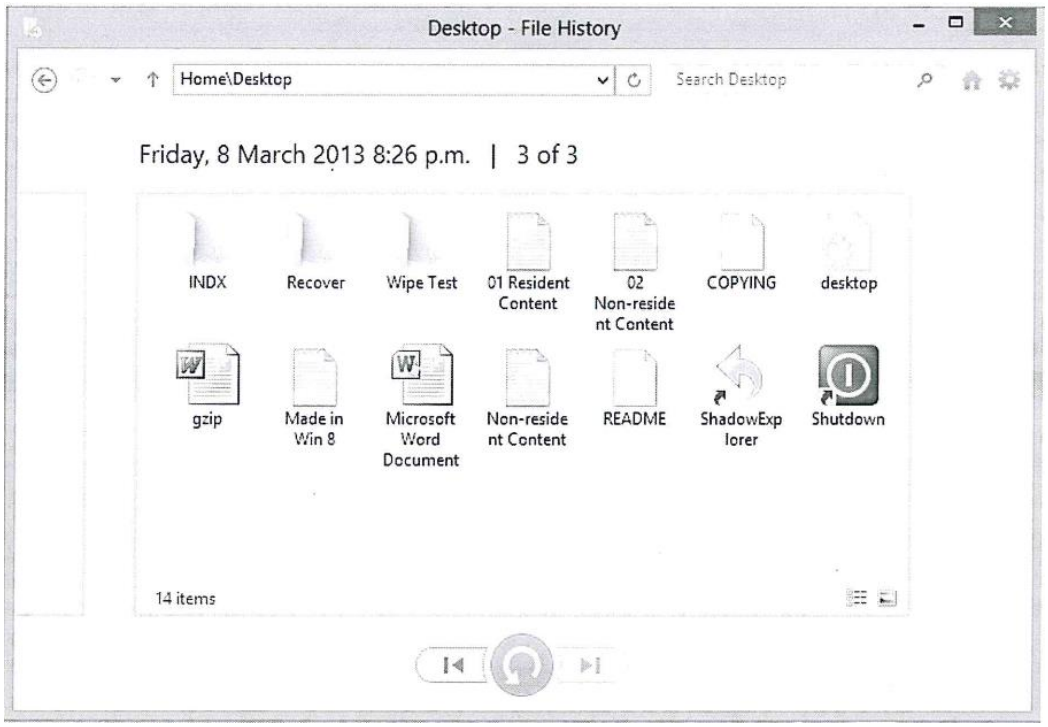


Figure: Desktop File history (8 March 2013)

The nice thing about this tool for the user is that when a folder or file is selected, the user can browse through a preview of each version. For example, compare the content of the Desktop folder on 5 March 2013 in Figure 5.46 below, to the content in the same folder on 8 March 2013, Figure above.

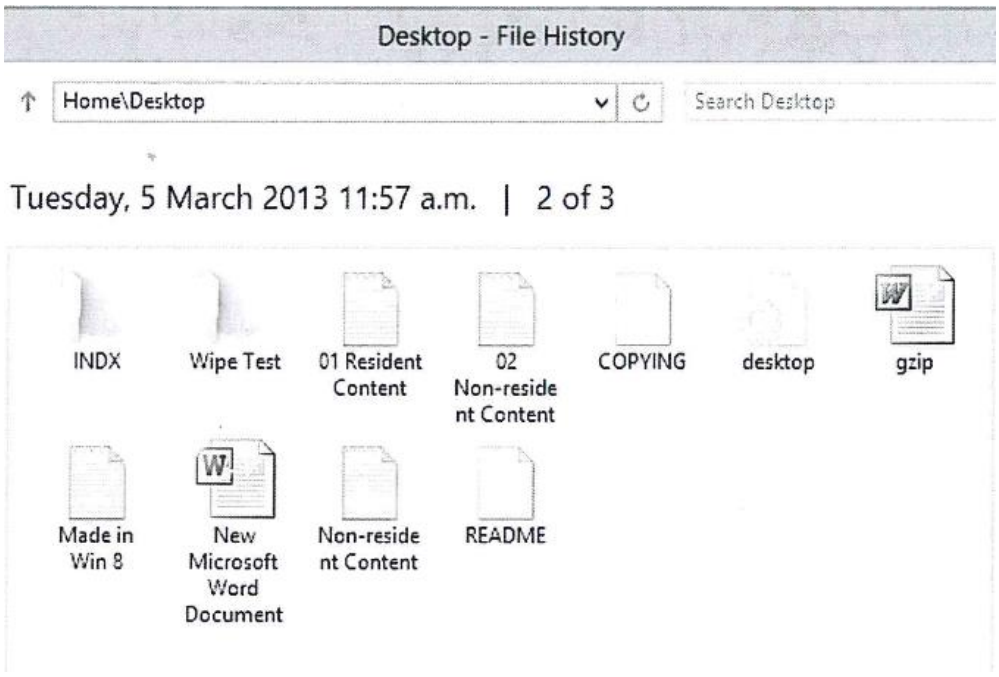


Figure: Desktop File history (5 March 2013)

From a forensic investigator's point of view, the files within a Windows 8 and 10 back-up are very easy to deal with, because each version of a file has the date appended to its filename, as shown in Figure.

However, that will not show when an evidentiary file was added to or deleted from a folder. Research is continuing on a definitive method to determine this - the information will be located in the Catalog#.edb files in the Configuration folder. The structure of the catalogue is still under review.

Volume Snapshot Service (VSS)

With Windows Vista, a new service, called Volume Snapshot Service (VSS) was introduced to replace the Restore Point methodology of Windows XP. VSS is a differential backup system that creates restore points called a volume snapshot or shadow copy.

The system is more efficient on disk space, in that only the changes that are made to a file content since the last snapshot was taken is saved in the next snapshot. A differential backup saves the changed (differences) to a file only. A single snapshot may only contain a fragment of a file, unless that file is brand new.

From a forensic perspective, this makes recovery more complicated, as a file cannot necessarily be manually recovered from a single snapshot. Variations to the file may be contained in other snapshots, therefore the backup utility used to create the differential files needs to be used to put them back together again.

The data is located in the System Volume Information folder, which is secured to not even allow administrators access to all of the resources. The content of each snapshot is kept in a file that has two GUIDs as the file name. Figure 5.47 shows the contents of the System Volume Information Folder as seen with a forensic tool.

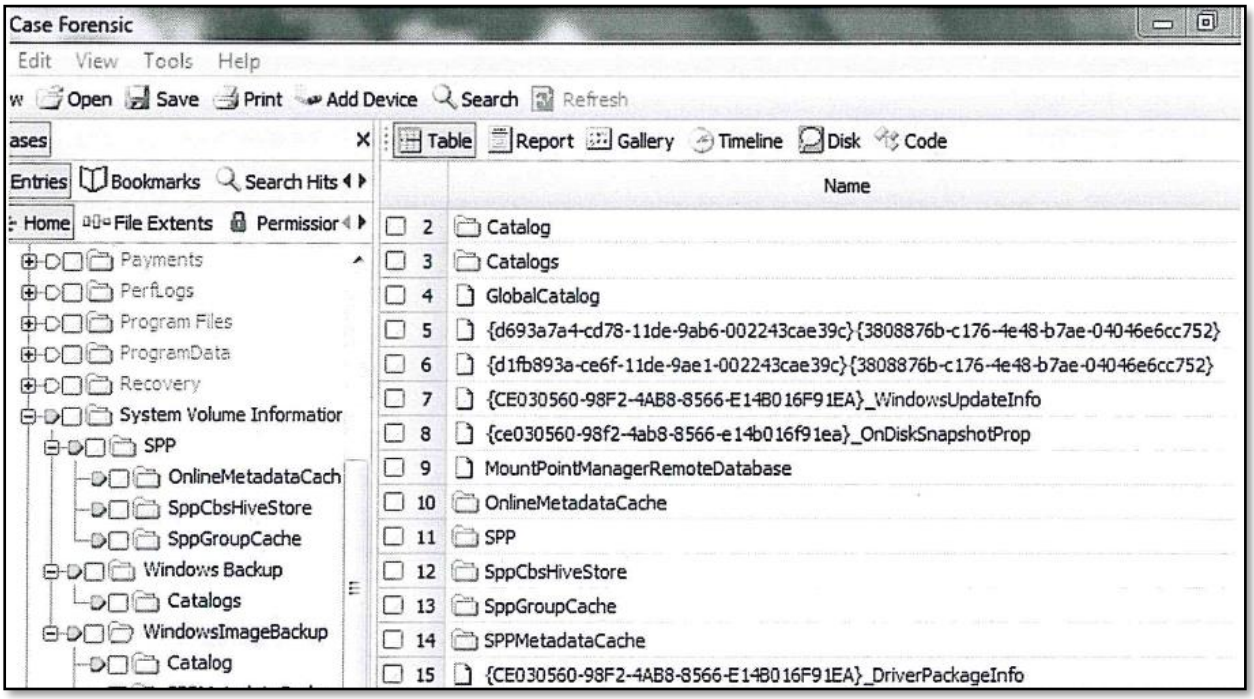


Figure : VSS files

System Restore

The system restore feature is used to recover data from the Shadow Copies. System Restore, which is available in all versions of Vista, 7, 8 and 10, is primarily concerned with certain system specific settings. System Restore creates restore points at certain interval or events much like what is seen with XP.

Windows Vista and 7

In Windows Vista and 7, System Restore is enabled by default.

Windows 8 and 19

System Restore is "Disabled by default. It can be enabled in the Control Panel under System Protection.

Previous Version

A component of System Restore is previous versions. This service's purpose is to recover previous versions of the user's files and folders. Previous Versions only stores the changes to a particular file and only one version of the files is saved within a snapshot. For example, if a file is modified several times in one day, only the current version is saved when the volume snapshot is created. Previous versions of files are still available after the Recycle Bin has been emptied and possibly after several defragment operations.

Windows Vista and 7

This service runs on all versions of Vista and 7, however, only users of Business, Enterprise, and Ultimate have a GUI interface to access the service. Figure 5.48 below shows the previous versions

available for a file from a compatible 7 system. The previous versions of a file are accessed through its properties - where the user has the option to Open, Copy or Restore.

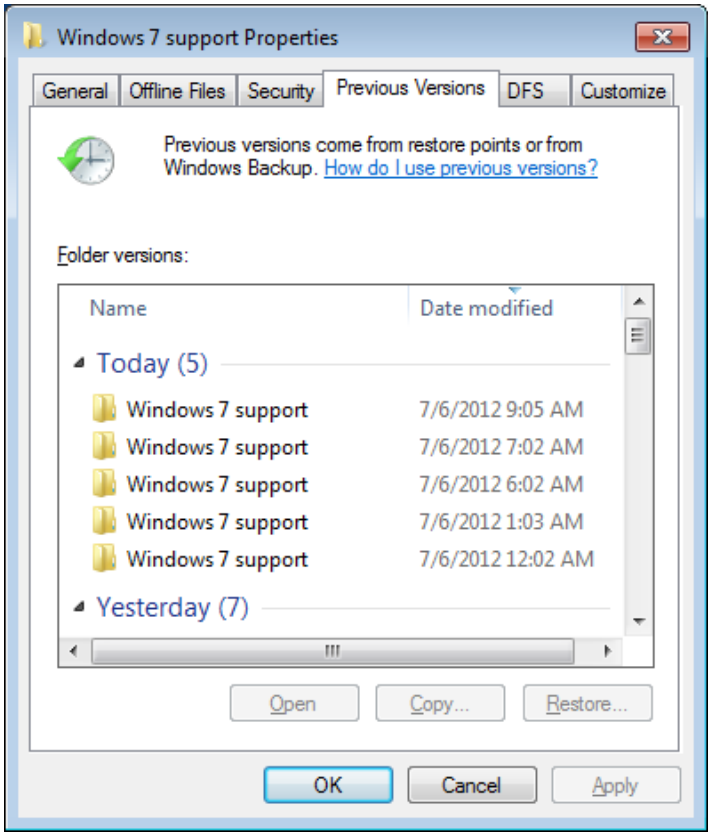


Figure: Previous versions of folder

Users running Home Basic and Home Premium can utilize third party tools such as Shadow Explorer which will permit access to previous versions of files. Shadow Explorer is a useful tool to quickly browse the content of a snapshot. Figure 5.49 shows the contents of the Desktop folder on April8, 2009 at 11:06a.m.

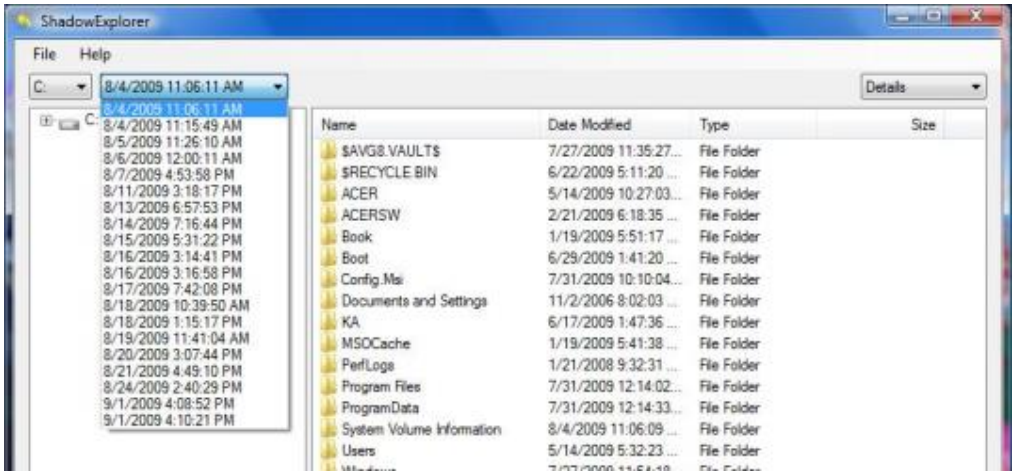


Figure: Shadow Explorer

In Vista, triggers for Volume Snapshots creation are:

- Every 24 hours
- Manually by user

- Before a Windows Update
- Unsigned driver installation
- An application calling the Snapshot API

In Windows 7, the only difference is that the snapshots are created every 7 days rather than every 24 hours.

Windows 8
As System Restore is disabled by default, it must be enabled in Windows 8 to access the Previous Versions tab. However, the tab is still only available on network shares. To access it locally, use the path \\localhost\c$ in Windows Explorer (where "c" represents the volume letter you are wanting to access).

The user can then select the desired folder and find the Previous Version tab in the properties and from here the selected files can be either copied or restored, as shown in Figure 5.50.

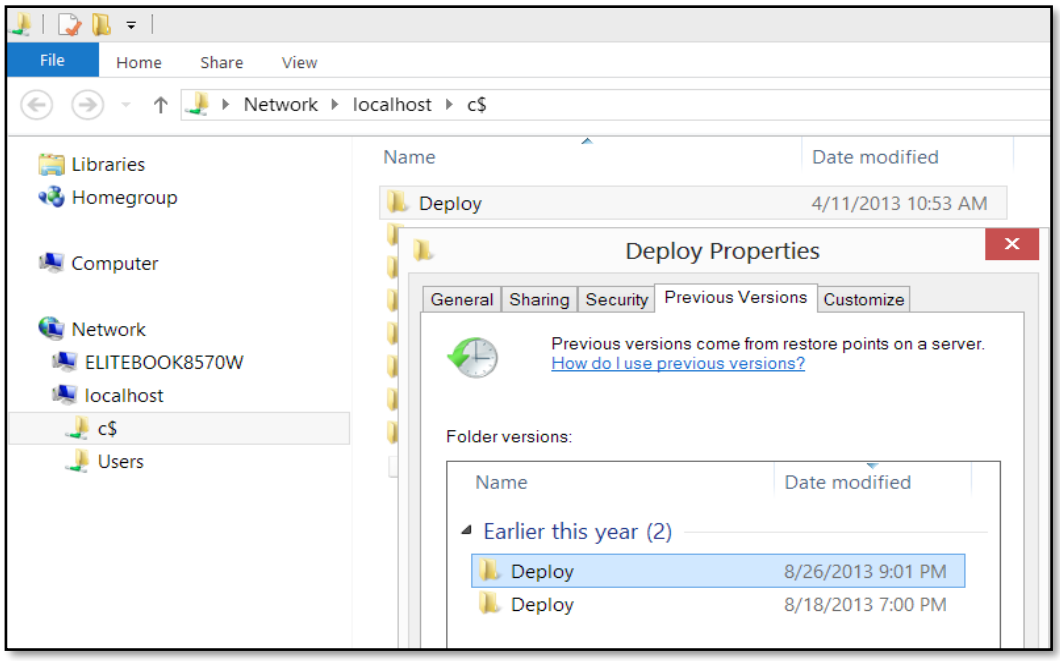


Figure: Windows 8 Path to access previous version

Windows 10

The Previous Versions tab in Windows 10 is available with all versions of the Operating System and the tab is now viewable in properties even if System Restore is not enabled. Other than the availability of the tab the functionality of Previous Versions has not changed.

❖ Access Control List

An Access Control List (ACL) contains a list of permissions that are attached to an object and are used to manage access to computer resources. By analyzing ACLs, an examiner can determine which user account was able to view and/or modify a file. This can come into play in child sexual

“exploitation cases, fraud cases, and such where proving who saved, altered, or created a file may be in contention.

There are two types of ACLs:

System Access Control List (SACL): the ACL is managed by the system and used to control auditing of attempts to access the object.

Discretionary Access Control List (DACL): the permissions are stored here that control what users and groups of users are allowed what type of access to the object.

The ACL contains many entries that are referred to as an access control entry (ACE). Each contains an ID code that identifies the user and group and the particular permissions that are to be applied.

A “deny” permission will take precedence over “allow”. The types of permission can be:

- **Full Control (FC)** - list contents of a folder, read and open files, create new files, delete files and subfolders. Change permissions on files and subfolders, and take ownership of files.
- **Modify (M)** - allows the user to read, change, create, and delete files, but not to change permissions or take ownership of files.
- **Read & Execute (R&E)** - allows the user to view files or execute programs.
- **Read (R)** - allows the user to list the contents of a folder, read file attributes, read permissions, and synchronize files.
- **Write (W)** - allows the user to create files, write data, read attributes and permissions, and synchronize files.
- **Special Permissions (SP)** - the assigned permissions don't match any of the preceding
- **List Folder Contents (LFC)** (folder only) - Read & Executer permission for folders.

File permissions can be accessed by the user in the security tab of the properties window, as shown pc in Figure below.

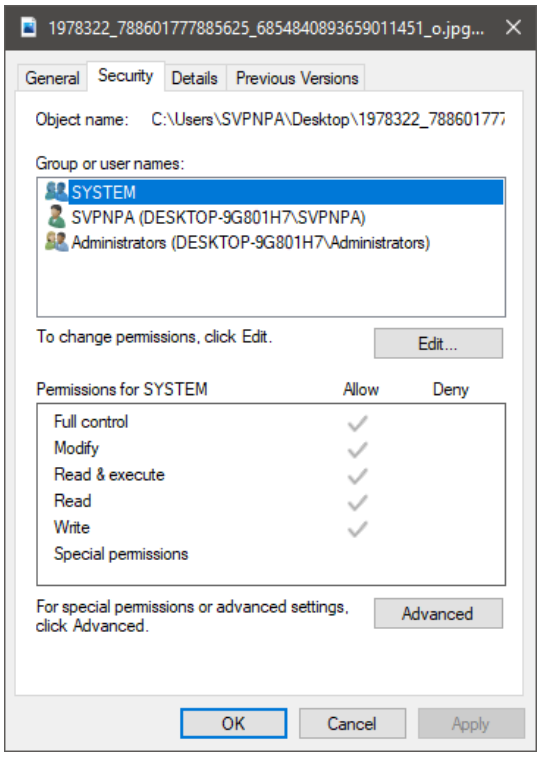


Figure: Permission Settings

Although permissions are most commonly associated with files and folders, they may also be used to regulate which users may make registry modifications, perform backups and restores, create pagefiles and shared objects, load/unload device drivers, shutdown the system, run batch processes, and generate security audits.

Ownership

The ACL will also show who the "owner" of a file is. Typically, the user account that was used to create a file will be assigned ownership of the file - this is a quite useful artifact to help link a single user account to a file. It is possible to change the owner in the advanced security.

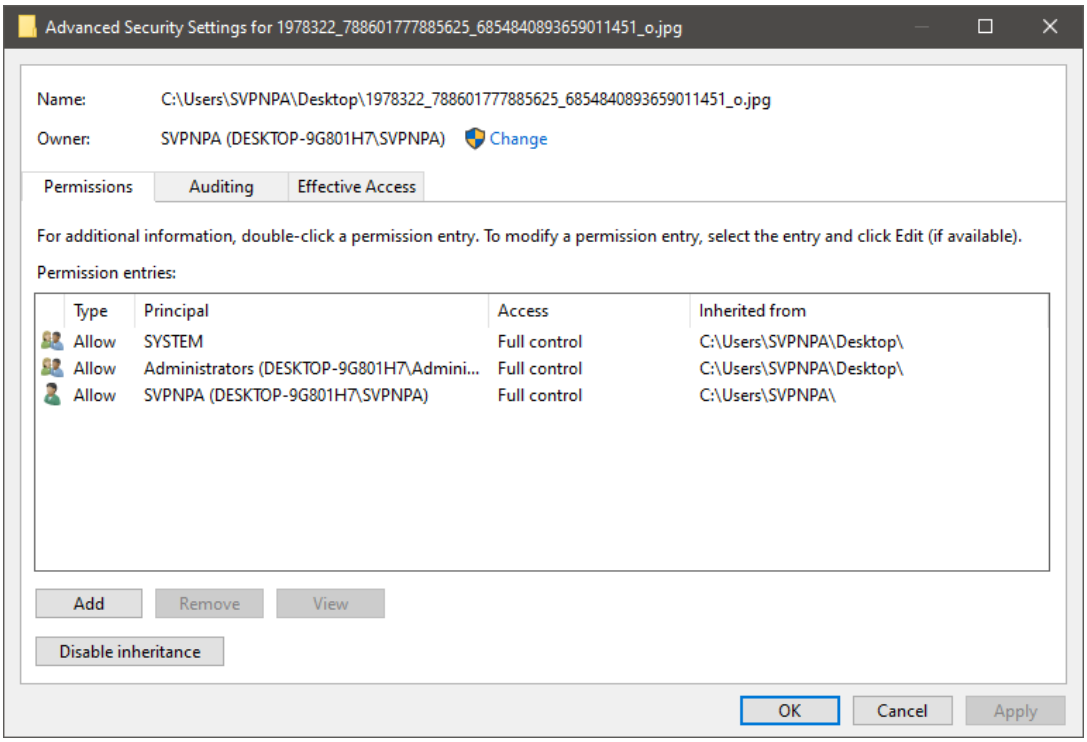


Figure: Advanced Security Settings

User Account Group

To make it easier to manage what a user account is allowed to do, Microsoft created user account groups. Each user group has default permissions already applied to that group, which are normally used to control access to a particular function or administrative tool within Windows. Those permissions are applied to each individual user account that is placed within the group. Figure below shows the list of default user groups in Windows 8.

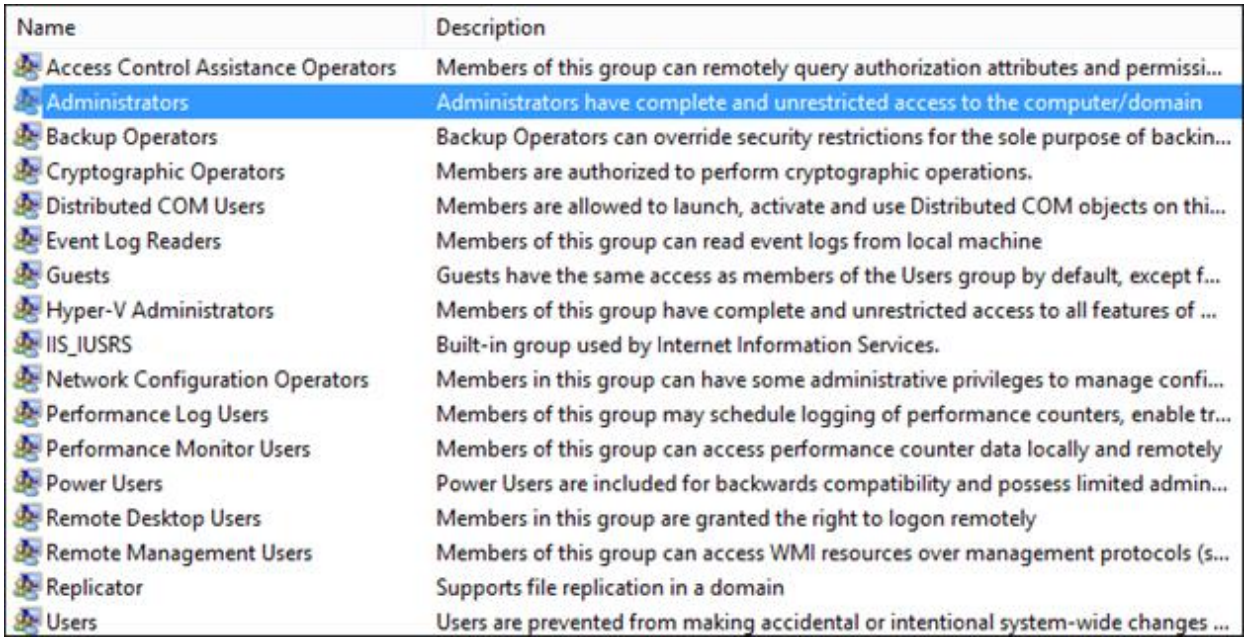


Figure: User Account Groups

It is also possible to create additional user account groups and assign permissions to control access to certain files in a corporate environment, for example, Payroll, Human Resources, Accounting,

etc. In this situation, a folder would be created for each work group to save their files in, and permissions for that folder would restrict all other workgroup user accounts.

Forensic Relevance
When doing a forensic examination of evidentiary files, understanding which user accounts can access the file due to its ACL and which user account "owns" the file can be very useful in proving culpability. Due to the way that the NTFS file system stores the user permissions for a file, it is a very difficult task to manually extrapolate an ACL. Forensic tools will do this automatically.

- **Prefetch**

With all of the improvement to computers over the last fifteen years, the biggest consumer complaint to Microsoft from users is the speed at which systems boot, recover from hibernation, and launch applications.

To combat these complaints, Microsoft introduced prefetching. Prefetching speeds up computer performance by bringing the data and code pages of programs used during the boot process and in subsequent program launches into memory from the disk before that data and code is actually demanded.

The prefetch files that are created as a result of the tracing what files are called for during system boot and application launch are located in the folder %WINDOWS%\PREFETCH. The file's name is the name of the application to which the trace applies followed by a dash and the hexadecimal representation of a hash of the file's path, ending with the .PF file extension. The file signature(header) for .PF files varies between versions:

- Windows XP 11 00 00 00.53 43 43 41 OF 00 00 00
- Windows Vista/7 170000 0053 43 41 11 00 00 00 00
- Windows 8 1A 00 00 00 53 43 41 11 00 00 00 00
- Windows 10 4D 41 4D 04

Bytes 5-8, in XP through 8, (53 43 43 41 hex) are "SCCA" in ASCII which is easier to remember as search string for examiners who need to recover deleted .PF files.

Looking at the content of a .PF file, the name of the executable file being traced is located at offset 10h and is visible in plain text. Figure 5.54 shows the file name. The file will also contain the run count, last run date and list of files used by the application when it loads.

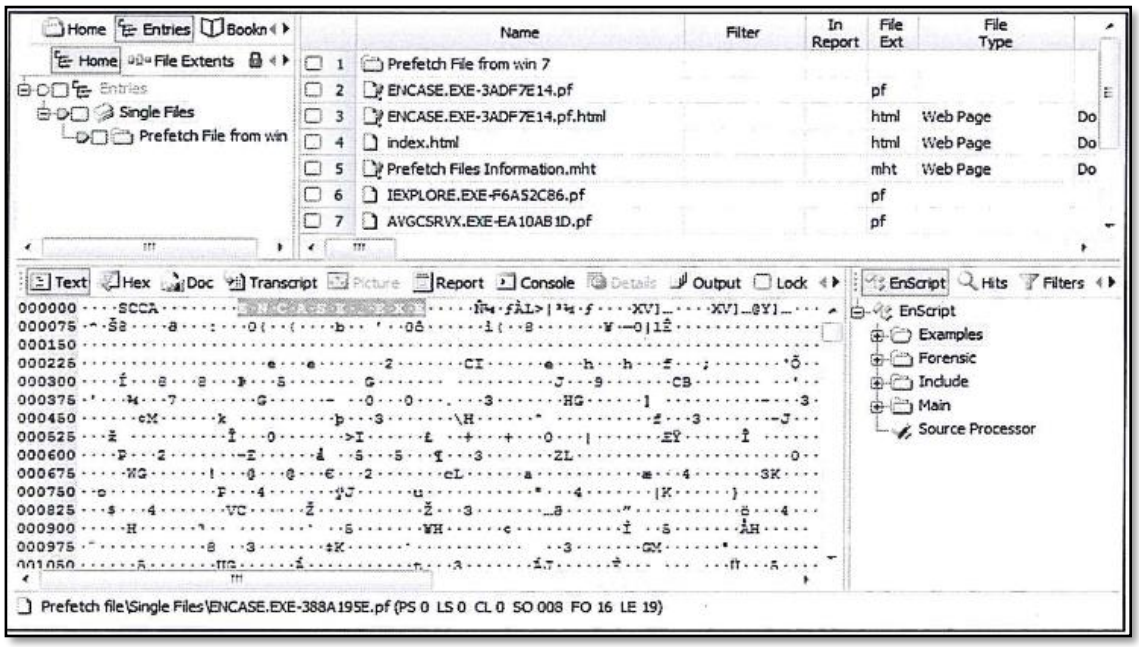


Figure : Prefetch Executable filename

In a forensic examination, prefetch files can be used to help determine when an application was last run. This is useful for creating a timeline of events or if attempting to determine if a virus or other exploit is active on a computer. Table 5.5 below gives the offsets for XP prefetch files.

Bytes		Data	Format
Offset	Length		
0x04	4	Header	SCCA
0x10	60	Application Name	Unicode
0x78	8	Last Run Date	FILETIME
0x90	4	Execution Run Count	Hex

Table: XP Prefetch format

The execution count is the number of times the application has been run. It is of note that if the application runs as part of the boot process the run count is NOT updated - this only applies to application launches that are not part of the startup or auto run processes.

The content of the .PF file also includes a record of the files and directories accessed during the first 10 seconds of application launch.

Even launching the most benign program can cause the operating system to access a number of files. Not all these are necessarily used by the application proper but as applications are launched and traces are done that data are used in subsequent launches.

Examining the files and directories accessed during the launch of an application can be very beneficial because it can reveal hidden directories, point to user accounts or show an application was accessed from an external storage drive. Simple File Parser by Chris Mayhew is available free from https://code.google.com/p/simple-file-parser/, and can parse XP and Vista/7 prefetch files.

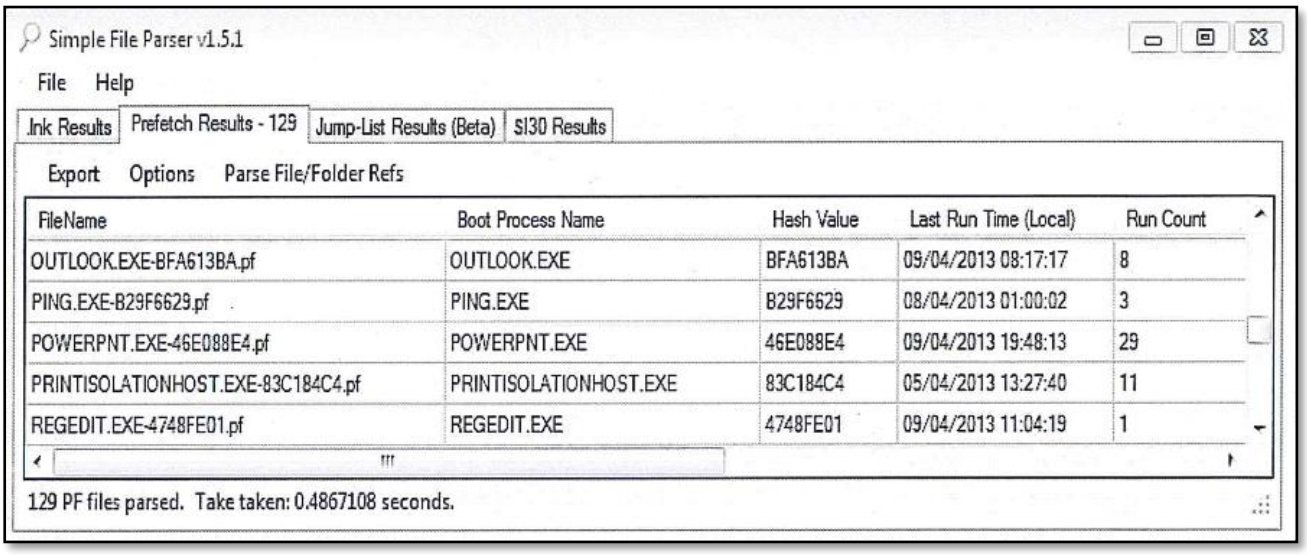


Figure: XP Prefetch Report using Simple File Parser

Windows Vista and 7

In Windows Vista and 7, there is a minor change to the data structure of a prefetch file, as given in Table 5.6 below.

Bytes		Data	Format
Offset	Length		
0x04	4	Header	SCCA
0x10	60	Application Name	Unicode
0x80	8	Last Run Date	FILETIME
0x90	4	Execution Run Count	Hex

Table: Vista/7 Prefetch file structure

Windows 8

Windows 8 + has up to 1024 individual prefetch files. An individual application can have multiple prefetch files, for example, if the application is moved to a new directory a new prefetch file would be created as the. There have also been some changes to the file format, which allow a prefetch file to store the last eight runtimes of an application.

There are some anomalies with this edition to take note of. The run count only increments when a new date and time entry is added to the prefetch file. Once the run count reaches 10, Windows 8 only periodically updates the date and time and therefore also the run count. Testing has shown that once this occurs, the prefetch file is periodically updated when the program is open for a length of time and an "open" or "save" occurs within the program. Table 5.7 gives the data structure for a Windows 8 prefetch file.

Bytes		Data	Format
Offset	Length		
0x04	4	Header	SCCA
0x10	60	Application Name	Unicode
0x80	8	Last Run Date	FILETIME
0x88	8	2nd Last Run Date	FILETIME
0x90	8	3rd Last Run Date	FILETIME
0x98	8	4th Last Run Date	FILETIME

0xA0	8	5thLast Run Date	FILETIME
0xA8	8	6thLast Run Date	FILETIME
0xB0	8	7thLast Run Date	FILETIME
0xB8	8	8thLast Run Date	FILETIME
0x90	4	Execution Run Count	Hex

Table 4.1 Vista/7 Prefetch

A free tool is available to parse.all versions of Prefetch Files, called WinPrefetchView. It is available from, https://www.nirsoft.net/utils/win_prefetch_view.html.An example of a Windows 8 Prefetch file is given in Figure 5.56 below. Note that there are multiple programs.

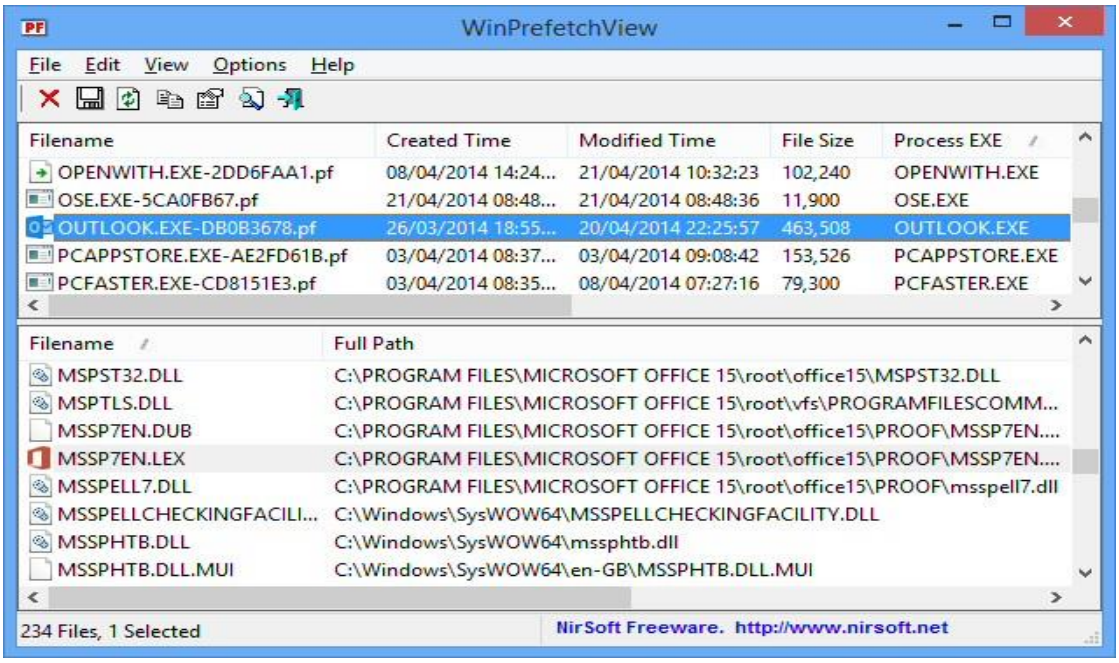


Figure : Windows 8 Prefetch in WinPrefetchView

Windows 10

Windows 10 has changed Prefetch only in the format in which the file is stored on disk. Windows 10 is now using the same compression as Windows 8.1 utilized in the compression of Superfetch files. Forensically speaking this doesn't change the role or functionality of Prefetch as described above, but it does change the tools used to view the contents of a prefetch file. Because the file needs to be uncompressed the data structure given above is not feasible for analysing the binary file. Also, Simple File Parser and Prefetcher, at the time this manual is written do not support the decompression of the Windows 10 prefetch files. The prefetch files are still located in the same directory, with the same extension, however the file header is now 0x4D 41 4D 04.

4.3 Event logs

Microsoft defines an "event" as any occurrence that is potentially noteworthy - either to the user, the operating system, or to an application

Events are categorized into 3 classes: System, Application and Security. By default, in XP, all three logs are stored in the C:\Windows\system32\config folder and are called SecEvent.Evt,AppEvent.Evt and SecEvent.Evt, respectively. These logs record errors, failures, successes, information and warnings.

- **SecEvent.Evt** - Contains log records of system processes and device drive activity. Event logs include things such as device drivers that fail to start or stop properly, hardware failures, duplicate IP addresses, and the starting/stopping/pausing of system processes.
- **AppEvent.Evt** - Contains log records of events related to the application software installed on the system. The events logged include errors, warnings, and any other information an application is designed to report. The developers of the application determine what gets logged.
- **SecEvent.Evt** - Contains the events of the security processes used by NT, 2K and XP. Some of the security events that can be logged include changes in user privileges, logins and logouts, file and directory access, and printer activity.

Windows XP

With XP, event log files are viewed using Microsoft's Event Viewer. It is accessed through Start > Settings > Control Panel >Administrative Tools >Event Viewer. Figure 5.62 below shows the System Event log.

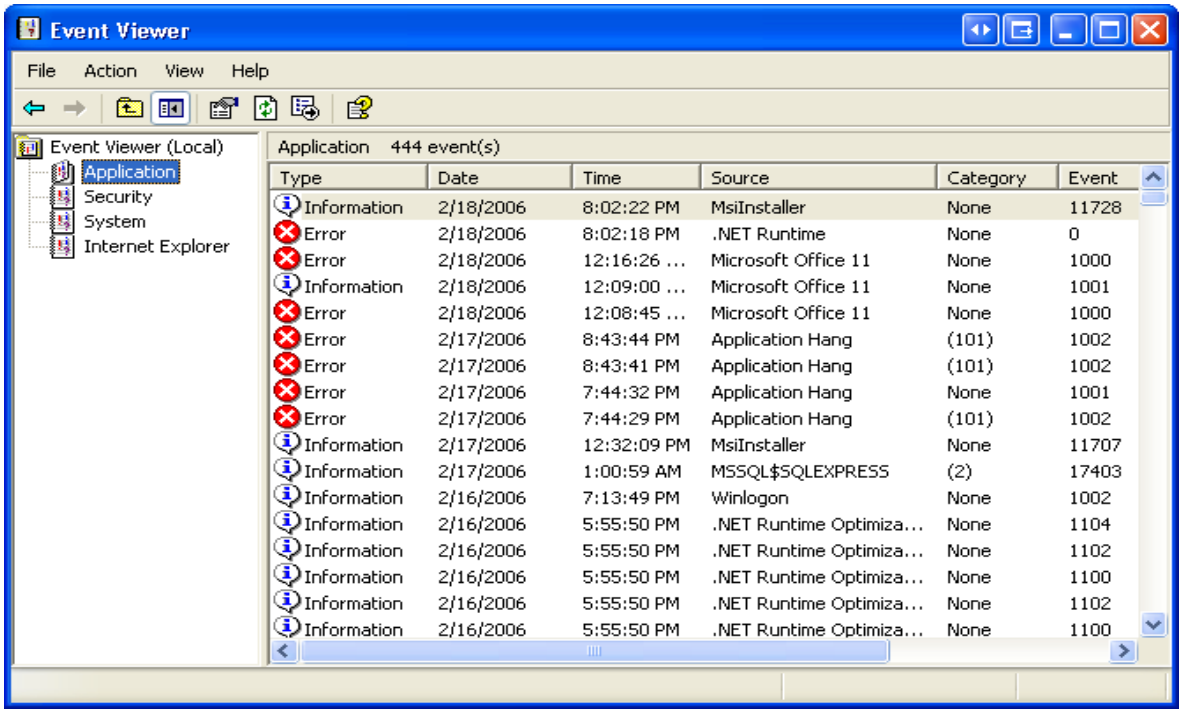


Figure: XP Event Viewer

However, reviewing XP event logs from a suspect's system on your examination system can be difficult. Caution must be used when examining Event Log files copied from the suspects system to the examination system.

Because the descriptive messages for each event log entry are stored in the Registry and other system files, simply copying the *.evt files from the suspects system to yours for examination can result in missing, or possibly, misinterpreted information.

Furthermore, Event Logs reference users by their associated SID (Security Identifier), not usernames. When viewed in the event viewer, the translation is made. However, when the logs are

viewed on a different system, the SID is displayed. More importantly, the forensic computer must have the same time zone setting as the suspect computer as event log entries are in UTC.

EventLogExplorer (www.eventlogxp.com) is a useful tool for event log analysis and recognizes both *evt and *.evtx. Another option is to export to a spread sheet format for timeline analysis and making notes.

Windows Vista, 7,8 AND 10

There are significant changes to Event Logs with Vista and 7 including their format and the restructuring into two main categories of Event Logs.

Event Logs now have the extension .EVTX and utilize the XML format. They are now stored in C:\Windows\System32\winevt\logs. The two main categories of Event Logs are now Windows Logs and Applications and Services Logs. Windows Logs still contain the logs that were available in XP but now include the logs Setup.EVTX and ForwardedEvents.EVTX.

- Windows Logs are much the same as those in Windows XP
- The Applications and Services Logs store events from a single application or component rather than events that might have system wide impact. The category subtypes found in this log include: Admin, Operational, Analytic and Debug logs. These logs are designed to aid IT Professionals using the Event Viewer to troubleshoot problems and are beyond the scope of this paper.
- Setup.EVTX - logs events that are related to application setup.
- ForwardedEvents.EVTX - stores events collected from remote computers with a created event subscription.

The Vista, 7, 8 and 10 event viewer is much more robust and has built in support that provides the definition of each log function as well as advanced options including filtering, sorting and custom view options.

Event Logs can be useful in a forensic examination to show that a user may or may not have performed a particular action at a particular time. They can be useful for a number of things from tracing logins in the case of logging into a restricted network, proving the computer was running during a particular time, showing time change/time change synchronization events, USB driver installation and wireless connections just to name a few monitored actions.

Figure 5.63 below shows a manually time changed event. The time was changed by the user. Notice the values are recorded in UTC time.

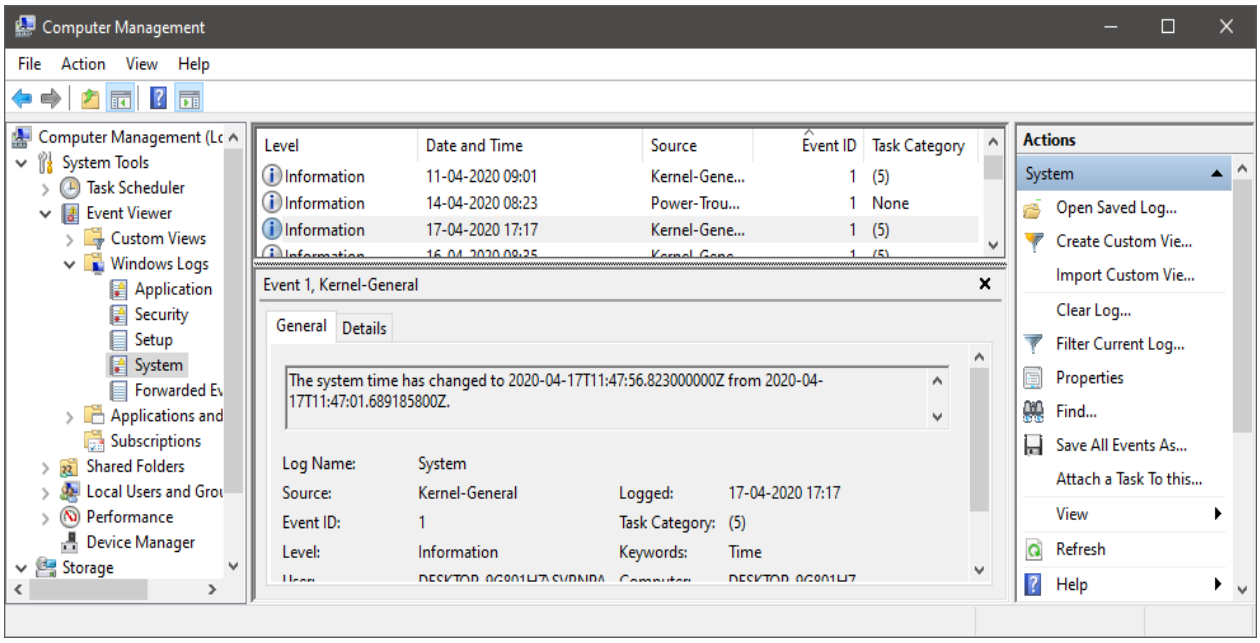


Figure: System Time change in System log

Some events may be shown in more than one log. Figure 5.64 below shows the same time change event also captured in the Security log.

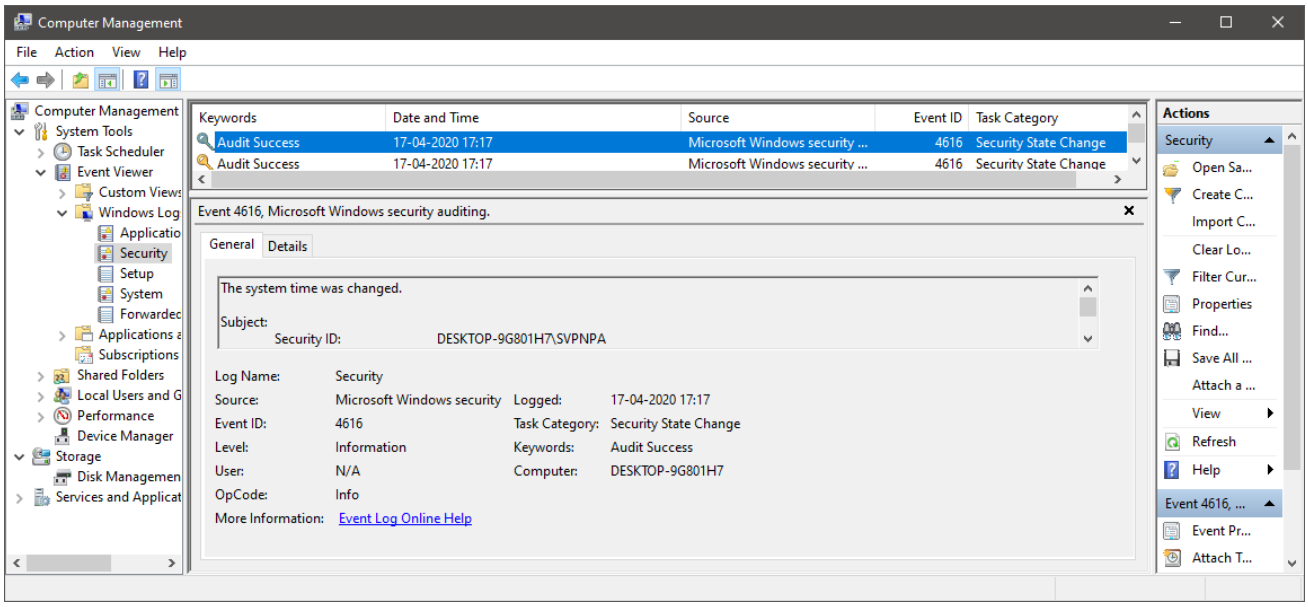


Figure: System Time change in Security log

To examine a Windows Vista + event log, copy the content of the folder C:\Windows\System32\winevt\logs to the forensic machine. The event logs can be accessed through Windows built in Event Viewer by selecting Action > Open Saved Log. The same precaution exists as Windows XP, the examiner's computer must be set to the same time zone as the suspect computer as the Event Log is written in UTC. **Event Log explorer** is useful for *.evtx files and can export to spreadsheet for additional manipulation.

4.4 Windows Registry

The Windows Registry can be an excellent source of potential evidence. Unfortunately, the Registry is still widely underutilized in day-to-day computer examinations. The registry can store system settings, hardware information, passwords, application cache and much more.

The Microsoft Computer Dictionary, Fifth Edition, defines the registry as:
A central hierarchical database used in Microsoft Windows 9x, Windows CE, Windows NT, and Windows 2000 used to store information necessary to configure the system for one or more users, applications and hardware devices.
The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create property sheet settings for folders and application icons, what hardware exists on the system, and which ports are being used.
The Registry replaces most of the text-based .ini files used in Windows 3.x and MS-DOS configuration files, Such as the Autoexec.bat and Config.sys. Although the Registry is common for several Windows 'platforms, there are some differences among them.
See the Recommended Resources for relevant Knowledge Base articles from Microsoft.
The Registry contains three (3) major categories of data may be of evidentiary value.

1) **User Specific Information** — such as Desktop Preferences, Typed URLs, Messenger Contacts, MRU Lists and Passwords.
2) **System Specific Information** — such as Network Settings, Time Zone Information, Registered Owner details, Last Shutdown Date/Time and Hardware information.
3) **Application Specific Information** — such as File Associations, Application Registration Information etc.

The information stored within the registry is often difficult to find.

There are two distinct types of registries in use throughout all recent distributions of Windows, referred to in this document as 95 and NT respectively:

1) 95/98/98SE/ME
2) NT/2000/XP/VISTA/WINDOWS 7/WINDOWS 8/WINDOWS 10

In order to examine a suspect's registry, the first step is to identify which type of registry is in use. If you already know which operating system is being used, you can identify the registry type instantly. If not, the quickest way to identify the registry type is by understanding the files used by each registry type and their locations within the folder hierarchy.

The core registry files for both types of registries can be found in the Windows directory. The Windows directory is normally very easy to find but it is important to remember that this directory is customizable.

With that said, in 99.9% of cases, the Windows directory will be called either "WINDOWS" or "WINNT" andreside in the root directory of C drive. We shall refer to this directory as <windir> throughout this document.

Windows 95, 98, ME, XP, VISTA and WINDOWS 7, WINDOWS 8, and WINDOWS 10 use "WINDOWS" as the default Windows directory. Windows NT and 2000 use "WINNT" as the default directory. Another important directory is the profiles directory referred to as <profiles> from this point forward. This directory is also customizable; however, by default this directory will be called "<windir>/profiles" under Windows 95, 98 and NT. Under Windows ME, 2000, and XP, it will be called "Documents and Settings". Windows Vista and higher has the profiles in the root directory in the "Users" subdirectory.

I. Logical Layout

We have established that Windows 95 and NT registries store their data in different files and these files have a different internal structure. This is the registry's physical layout. The logical layout however, appears the same under both 95 and NT registries.

The layout of a Windows registry can be compared to a file system. The registry contains "keys" which can be compared to directories and "values" that can be compared with files. A key can contain any number of subkeys and any number of values. There are typically five (5) root level keys in a Windows registry:

- KEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CLASSES ROOT
- HKEY_CURRENT_USER
- HKEY_CURRENT_CONFIG

HKEY_LOCAL_MACHINE, referred to hereafter as HKLM, is by far the most significant key in the registry. HKLM has subkeys named Software, System, Security, Sam and Hardware. In Windows registries, these subkeys are each stored in a separate registry file with the exception of the Hardware subkey. This key is dynamically created when the system boots and is not written to disk at shutdown.

Each user of the system has their own user file containing all user-based settings and data. These files are stored in the user's profile directory and are named NTUSER.DAT and USER.DAT under NT and 95 registries respectively. The HKEY_USERS key is the point where each of these user files is grafted to the logical registry layout.

HKEY_CLASSES_ROOT can be ignored because it is merely alias for the HKEY_LOCAL_MACHINE/Software/Classes subkey. The Classes subkey stores file extension associations.

HKEY_CURRENT_USER, referred to hereafter as HKCU is merely an alias for a subkey of HKEY USERS for the user currently logged on. When examining a registry of a system that has been shutdown there is no current user and therefore this key does not exist. For a running system, an application does not need to know how many users are on the system or which one is logged on. It can reference HKCU and the correct settings and data will be provided to it.

HKEY_CURRENT_CONFIG is an alias to the current hardware profile, which is stored at HKLM\System\CurrentControlSet\Hardware Profiles\Current. Please note, CurrentControlSet is also an alias and it points to the control set currently in use eg. HKLM\System\ControlSet001. By visiting HKLM\System\Select you can determine which is the current control set, default control set, faulty control set, and the last known good control set. These values are named Current, Default, Failed and LastKnown-Good, respectively.

Code	Type	Description
0	REG_NONE	Data with no particular type. This data is written to the registry by the system or applications and is displayed in hexadecimal format as a Binary Value.
1	REG_SZ	A fixed-length text string.
2	REG_EXPAND_SZ	A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.
3	REG_BINARY	Raw binary data. Most hardware component information is stored as binary data and is
4	REG_DWORD or REG_DWORD LITTLE_ENDIAN	Data represented by a number that Is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in binary, hexadecimal, or decimal format.
5	REG_DWORD_BIG ENDIAN	The SameasREG_ DWORD_LITTLE_ENDIANexcept that DWORD_LITTLE_ENDIAN has the least significant byte at the lowest address and DWORD_BIG_ENDIAN has the least significant byte at the highest address.
6	REG_LINK	A Unicode string naming a symbolic link.
7	REG_MULTI_SZ	A multiple string. Values that contain lists or multiple values in a form that people can read are usually this type. Entries are separated by spaces, commas, or other marks.
8	REG_RESOURCE_LIST	A series of nested arrays designed to store are source list used by a hardware device driver or one of the physical devices it controls. This data is detected and written into the \ResourceMap tree by the system and is displayed in hexadecimal format.
9	REG_FULL_RESOURCE_ DESCRIPTOR	A series of nested arrays designed to store are source list used by a physical hardware device. This data is detected and written into the\HardwareDescription tree by the system and is displayed in hexadecimal format.
10	REG_RESOURCE_ REQUIREMENTS	A series of nested arrays designed to store a device driver's list of possible hardware resources it or one of the physical devices it controls can use, from which the system writes a subset into the\ResourceMap tree. This data is detected by the system and is displayed in hexadecimal format.

11	REG_QWORD	Data represented by a number that is a 64-bitinteger. This data is displayed as a Binary Value. It was first introduced in Windows 2000.

Table: Windows Registry

Physical Layout

The file hierarchy for 95/98/98SE/ME style registries is as follows:

File Location	File Description
<windir>/SYSTEM.DAT	The System file
<windir>/USER.DAT	The User file
<profiles>/<username>/USER.DAT	Zero or more User files

Table: File hierarchy for 95/98/98SE/ME style registries

A typical single user system will not have a profiles directory and all user settings will be stored in the mainUSER.DAT file. In this case, the only files necessary for a registry examination are SYSTEM.DAT andUSER.DAT from <windir>.

The file hierarchy for NT/2000/XP/VISTA/WINDOWS7/8/10 style registries is as follows:

File Location	File Description
<windir>/system32/config/SYSTEM	The System file
<windir>/system32/config/SOFTWARE	The Software file
<windir>/system32/config/SECURITY	The Security file
<windir>/system32/config/SAM	The Sam file
<windir>/system32/config/systemprofile/NTUSER.DAT	The User file
<profiles>/<username>/NTUSER. DAT	One or more User files

Table: File hierarchy for NT/2000/XP/VISTA/WINDOWS7/8/10 style registries

Window NT/2000/XP/VISTA/WINDOWS7-10 requires at least one user, the Administrator account. Even a single user system will typically have six user accounts, each with an NTUSER.DAT file, e.g., Darren Freestone, Administrator, Default User, All Users, LocalService, NetworkService, Software Tools

Before selecting an appropriate tool for exploring the Registry it's important to understand the distinction between Live and Non-Live Registries. A live registry is available only when Windows is up and running and contains volatile information that will be lost upon shutdown.

Regedit can be used to explore a live registry but access to the **SAM** and **SECURITY** keys will not be allowed. When the machine is shut down and a copy of the hard disk is made, it is possible to locate and examine the contents of the individual registry files. This process is referred to as examining a non-Live registry.

Regedit

All versions of Windows are distributed with a version of Regedit (regedit.exe or regedt32.exe), which allows the user to interface directly with the system registry. Regedit is provided for advanced users, and Microsoft warns that making changes can cause serious damage to your

system. Regedit displays the keys in the left-hand pane in a hierarchical tree-view. The right-hand pane displays each value present in the currently selected key. For each value the user sees the value name, value type and value data.

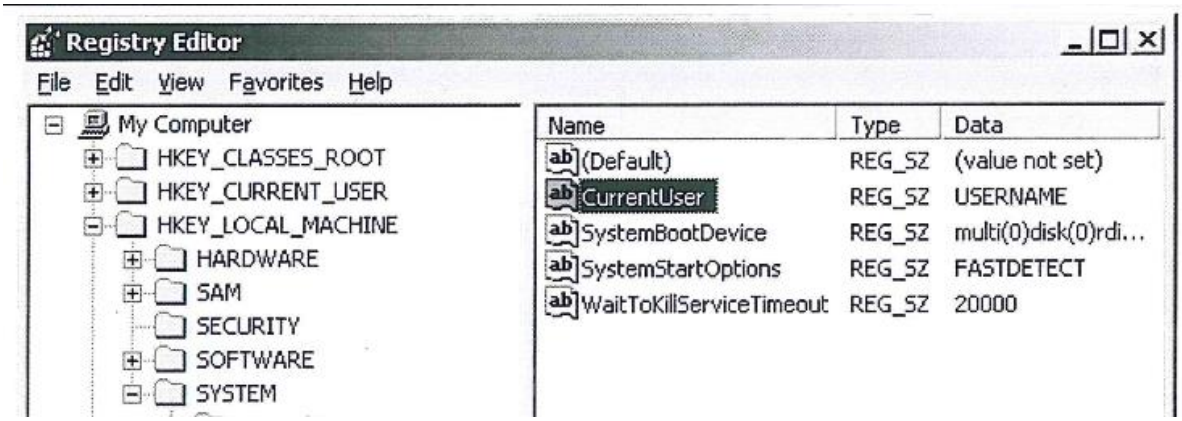


Figure: Regedit Home Screen

If you wish to conduct an examination of the registry of a live Windows system, you could use Regedit. This technique presents a few problems. The first problem is that you will not have access to the HKLM/Sam and HKLM/Security keys. This is for security reasons. Another problem with using Regedit is you will have difficulty extracting important information into report form.

Another major reason for not using Regedit to examine the system registry is that in most cases the registry you are examining will NOT be live, i.e., you will have a disk image of the Windows file system, including the registry files, but you will not actually boot the system. If you perform a restore operation and boot the disk image, then using Regedit would be a possibility.

Registry Browser

Registry Browser is a WIN32 application, designed to work a NON-LIVE windows registry. It should be installed onto your lab machine. It supports both 95 and NT registries. RB requires to the Windows directory <windir> of the target system in order to function.

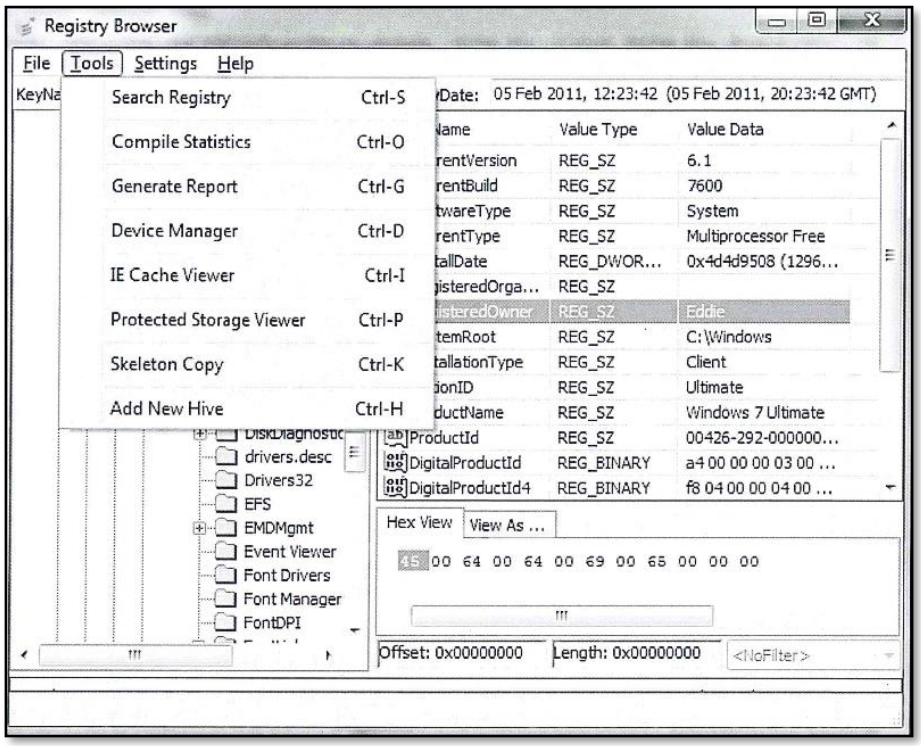


Figure: Registry Browser Home Screen

If your forensic software does not allow third party applications like RB to directly access the files and folders of the imaged file system, then you should familiarize yourself with the process of exporting registry files so that they can be made available to RB or other third-party applications.

During the exporting process, you must ensure the original directory structure is maintained so that the result is a skeleton of the <windir> and <profiles> directories. See pictured Windows 10 example (Figure 5.67)

Registry Browser has a similar screen layout to Regedit and is therefore simple to use. It has superior searching options and a predefined yet customizable reporting function. The report uses a template file, which can be customized by the user to include new keys and values without needed an updated version of the application.

RegRipper

RegRipper is created and maintained by Harlan Carvey. RegRipper is a Windows Registry data extraction and correlation tool. RegRipper uses plugins (similar to Nessus) to access specific Registry hive files in order to access and extract specific keys, values, and data, and does so by bypassing the Win32API. RegRipper isn't a registry Viewer, but a collection of scripts used to extract certain items of interest from thehive files. RegRipper, being written in Pearl, makes it easy to add new items to extract from the hives by writing a short script. Examiners can write custom scripts to locate specific item during examinations.

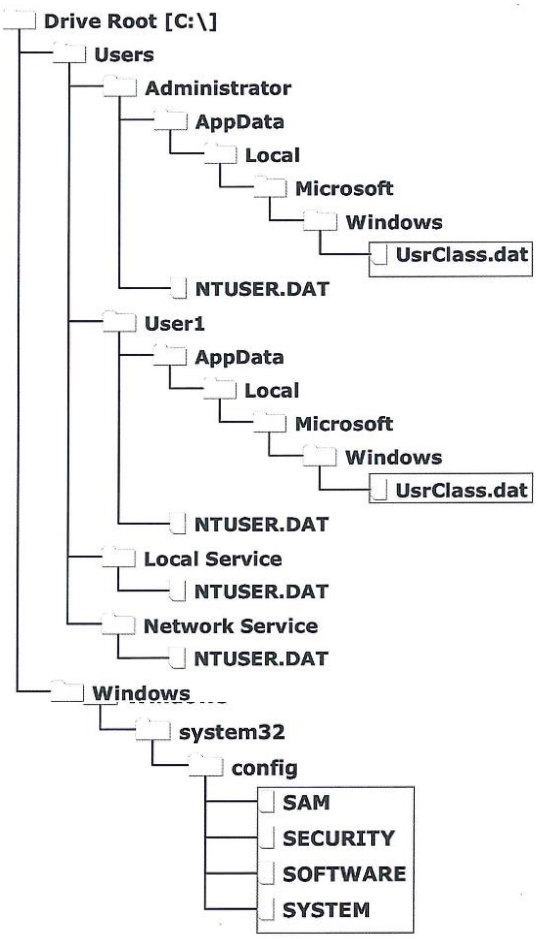


Figure: Directory Structure Windows 10

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.avi
LastWrite Time Sat Apr  2 23:40:19 2011 (UTC)
MRUListEx = 4294967295
  4294967295 =

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.azw
LastWrite Time Sat Apr  2 23:22:28 2011 (UTC)
MRUListEx = 0,4294967295
  0 = B003ODIZL6_EBOK.azw
  4294967295 =

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc
LastWrite Time Sun Apr  3 00:22:50 2011 (UTC)
MRUListEx = 1,0,4294967295
  1 = agenda5.doc
  0 = agenda4.doc
  4294967295 =

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
LastWrite Time Sat Apr  2 23:24:14 2011 (UTC)
MRUListEx = 1,2,0,4294967295
  1 = ahrendtHW4.docx

----------------------------------------
RecentDocs - recentdocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Sun Apr  3 00:38:25 2011 (UTC)
  14 = RegRipper032911
  13 = ripxp_instructions.txt
  6 = Practical
  9 = System_Rip.txt
  12 = Security_Rip.txt
  10 = Security_Rip.log
  3 = Downloads
  8 = agenda5.doc
  7 = Software_Rip.txt
  2 = RegRipper032911.zip
  1 = 1033
  0 = Blog.dotx
  11 = Pictures
  48 = captain_america_first_avenger_by_delta_seb-d39e1ps.jpg
  19 = IAAS 335
  21 = ahrendtHW4.docx
  47 = My Kindle Content
  46 = B003ODIZL6_EBOK.azw
  45 = SIFT Workstation 2.0 Distro Version
  44 = SIFT Workstation 2.0.vmdk
  43 = ahrendtHW5.docx
  27 = FreeBSD-8.2-RELEASE-i386-dvd1
  23 = FreeBSD-8.2-RELEASE-i386-dvd1.iso
  18 = ahrendtHW3.docx
  5 = agenda4.doc
  4 = readme.txt
  4294967295 =
```

Figure: Sample RegRipper Output

Timezones

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformtion

Windows NT based registries store a modified date for each registry key. These dates, like many of the dates encountered, are stored in Greenwich Mean Time (GMT). In order to convert these GMT times tolocal time, the registry's Time Zone Information needs to be determined.

TimeZone Values	Explanation
Bias	signed 4-byte value, standard offset to GMT (minutes)
StandardBias	signed 4-byte value, standard time adjustment (minutes)
StandardName	string value, time zone description — standard time
Standardstart	16-byte structure defining start date for standard time
DaylightBias	signed 4-byte value, daylight time adjustment (minutes)
DaylightName	string value, time zone description — daylight time
DaylightStart	16-byte structure defining start date for daylight time
ActiveTimeBias	signed 4-byte value, offset currently in effect (minutes)

Table: Timezone Values

The values ***Bias, Standard Bias*** and ***ActiveTimeBias*** are all 4 byte signed values measuring minutes behind GMT time. For example, the time zone -5 GMT would be stored [+300](minutes). The time zone +10 would be stored as [-600] minutes.

To calculate the local time, during standard time, use the formula:

Local Time = GMT - Bias - StandardBias

To calculate time local time, during daylight time, use the formula:

Local Time = GMT - Bias - DaylightBias

The **ActiveTimeBias** value is updated to reflect the current offset to GMT (eg.**Bias + DaylightBias**). This value will change after the trigger dates **StandardStart** and **DaylightStart**. These trigger dates are stored as a 16-byte structure, made up of six, two-byte values as follows: Year, Month, Day of Week, Day, Hour, Minute, Second and Milliseconds. These dates do not explicitly express a given date. Insteadthey express a rule for determining the date, e.g., Last Sunday in October at 2am.

Hardware Devices

There is a lot more to the Windows Registry than just program settings, cache and data. A lot of information about the system's hardware is stored in the registry as well, particularly for NT based registries. These hardware keys are located at HKLM\System\CurrentControlSet\Enum and therefore can be viewed or searched with Regedit or other registry viewing software. This can be a little problematic as the information is not laid out in a human friendly way.

A more effective method of viewing these keys is RB's Registered Device Manager, or RDM. The RDM Interface is just like the Device Manager function of Windows except that it shows all hardware registered with the system, not just the devices currently attached (Figure 5.69). With this feature this user can identify hardware devices such as a thumb-drive and determine when it was first attached to the system.

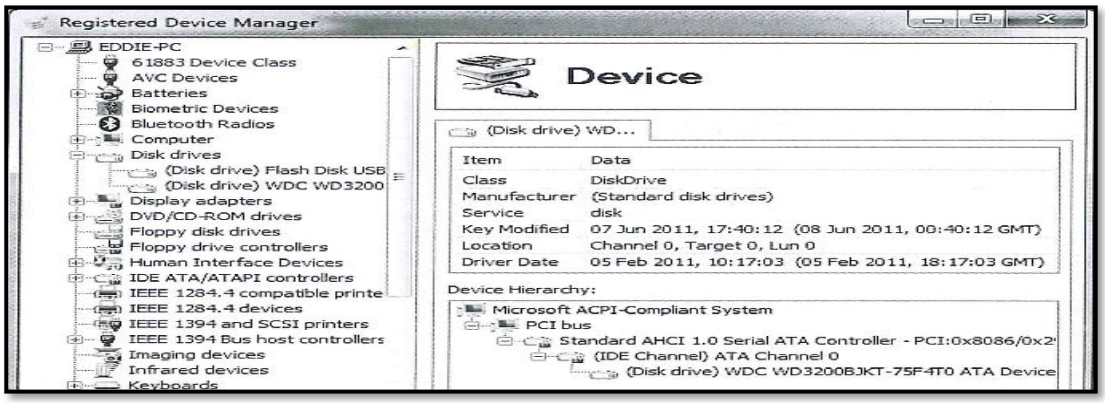


Figure: Registered Device Manager

Protected Storage — Pstore (Windows 7 and earlier only)

The Protected Storage System Provider, often referred to as PStore or PSSP, is an encrypted area of the Windows Registry devoted to storing passwords and also forms data from web pages. This

makes the PStore an excellent source of potential evidence. The suspect might have an encrypted container which cannot be opened using brute force (any time soon). But what if they are careless enough to use the same password elsewhere?

Each user on the system has its own PStore area of the registry located at:

Microsoft \Windows\Protected Storage System Provider

In order to decrypt the keys and values of the PStore, a third-party tool will be required. Most of the popular computer forensics suites have a function to decrypt the PStore. If you are running on a live machine or a restored copy of a machine, the free tool "Protected Storage PassView" can be run.

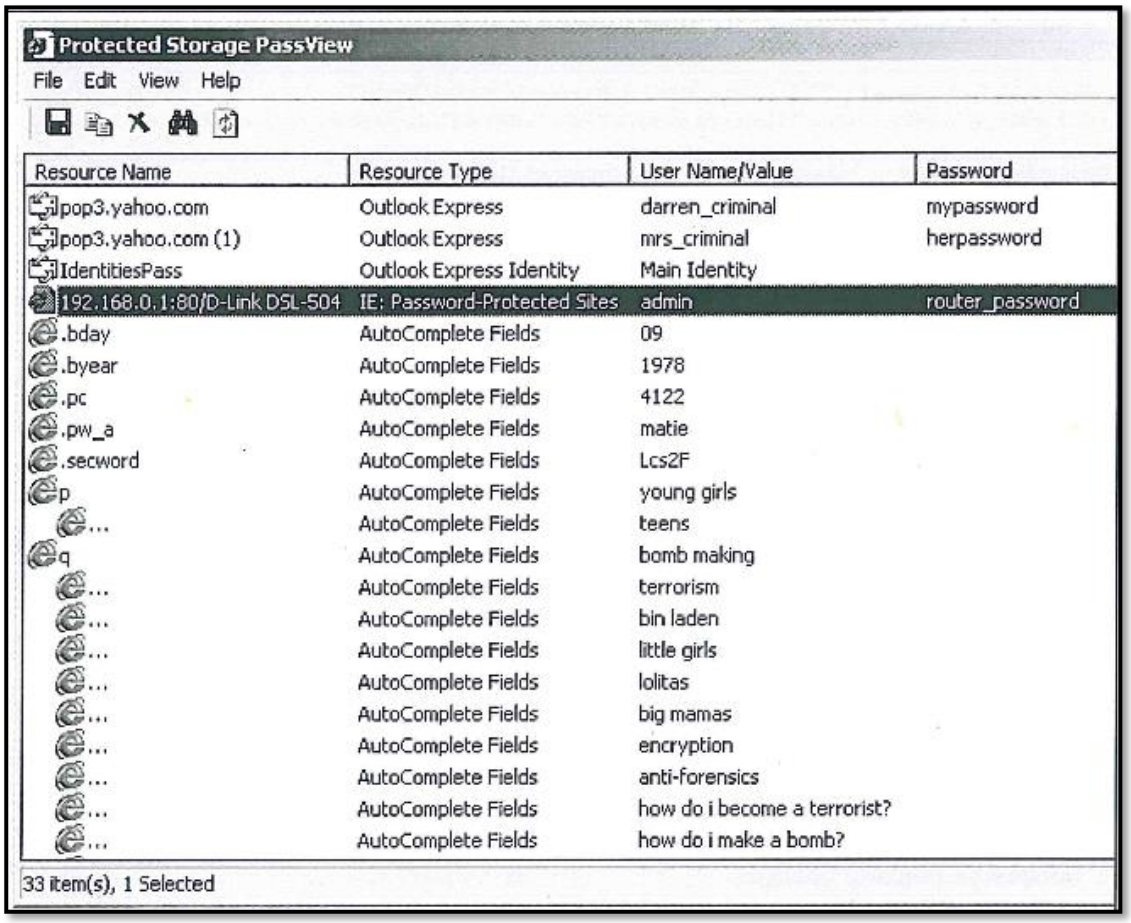


Figure: Protected Storage PassView

The Outlook Express usernames and passwords have been stored for two pop accounts. Also stored is the admin, password for a D-Link router. Note also how search terms entered into Internet Explorer can be stored too. Other passwords that can appear are FTP sites and password protected web sites such as adult sites.

The PSTORE has been depreciated in Windows Vista and Windows 7 and exists in a read-only capacity. DPAPI (Data Protection API) replaces PSTORE. For more information of DPAPI see: http://msdn.microsoft.com/en-usllibraryims995355.aspx

Security Identifiers (SIDs)

When examining an NT style registry, or even the file system it resides on, you will encounter Security Identifiers (commonly abbreviated SIDs). SIDs is an alphanumeric character string which is by a Windows Domain Controller during the log-on process. The SID uniquely identifies the user or group from all other users and groups on the network.

The following is an example of the SID S-1-5-12-4626982574-2357336844-2345214626-11114 broken down into its components:

Denotes a SID	Revision Level	Authority Valve	Domain or Computer Identifier	Relative ID RID
S	1	5	12-4626082574-2357336844-2345214626	1014

There are many fixed SIDs common to all systems. A few examples are listed below:

Security Identifier	Username	Account Description
S-1-5-18	System	Powerful service account used by the OS
S-1-5-19	Local Service	For running services locally
S-1-5-20	Network Service	For running services over the network.
S-1-5-21-domain-500	Administrator	System Admin's account with full control.
S-1-5-21-domain-501	Guest	A guest account - disabled by default

Table: SIDs common to all systems

When examining a regular system, the most important part of the SID to look at is the last portion of digits, the Relative ID (RID) It is important to be able to relate an identified SID/RID back to a user account name. The easiest way is as follows:

- Navigate to:

HKEY_LOCAL_MACHINE\Sam\SAM\Domains\Account \Users \Names

- Scroll through the usernames within this key. eg. Administrator, Guest whilst looking at the “Value Type" column.
- The value in the value type column is the Relative ID (RID) of that user.
- So, once the RID has been found the account name has been identified.

The subfolders in the Recycle Bin folder are named by SID with the respective RID. In the scenario where a deleted file of particular relevance is located within one of those sub folders, the first step will be to identify which user account the SID refers.

Windows 8 Registry Changes

The release of Windows 8 additional artifacts added to the Registry which contain items of interest to an examiner, which are carried over in Windows 10. The location and structure of the hive files remains the same but additional keys have been added in support of the User Interface.

Within each user's NTUSER.DAT file contained within their profile is a key which can identify typed URLs for Internet Explorer, along with the time this information was entered.

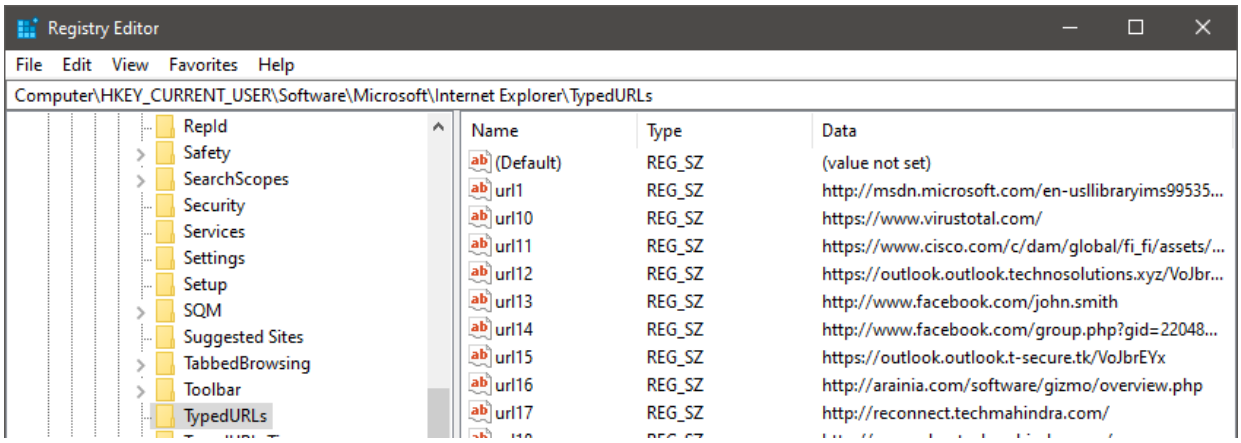


Figure : SID of User\Software\Microsoft\Internet Explorer\TypedURLs

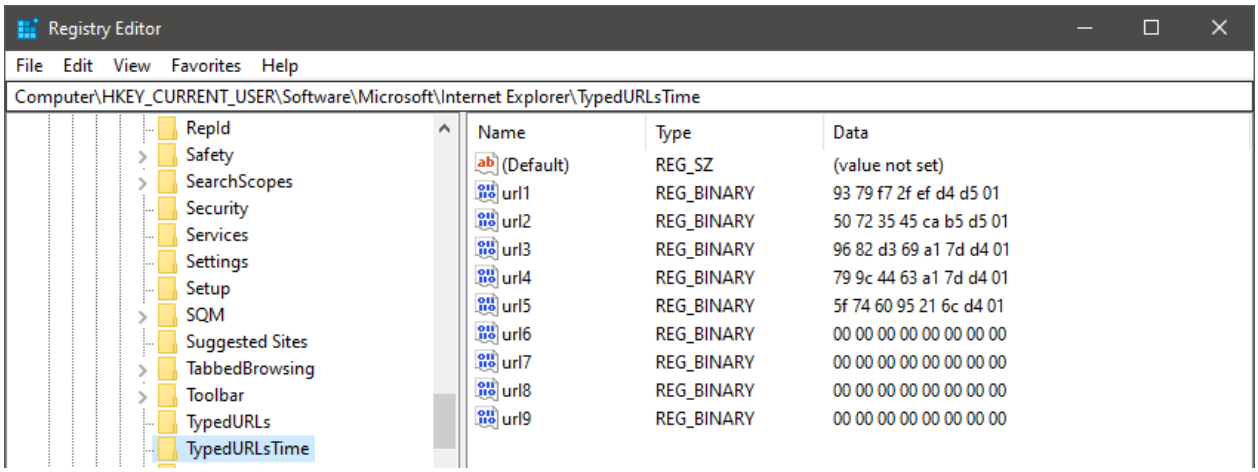


Figure : SID of User\Software\Microsoft\Internet Explorer\TypedURLs

This information is stored in Windows FILETIME format.

The SAM file contains the hive which lists each user's Internet User Name associated with their Windows Live account.

If the user has a "local" type of account, their Microsoft account used for the App store is found in the User's NTUSER.DAT file.

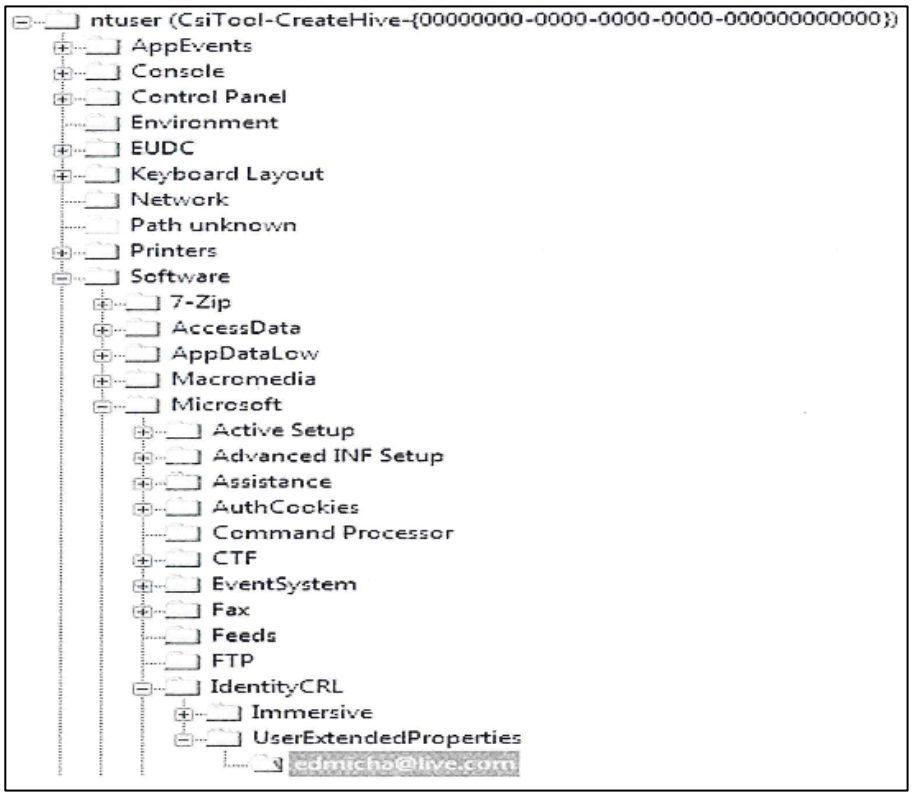


Figure : NTUSER.DAT file

The software key contains additional information about Metro applications installed on the system through the App store Microsoft has made available to Windows 8 users.

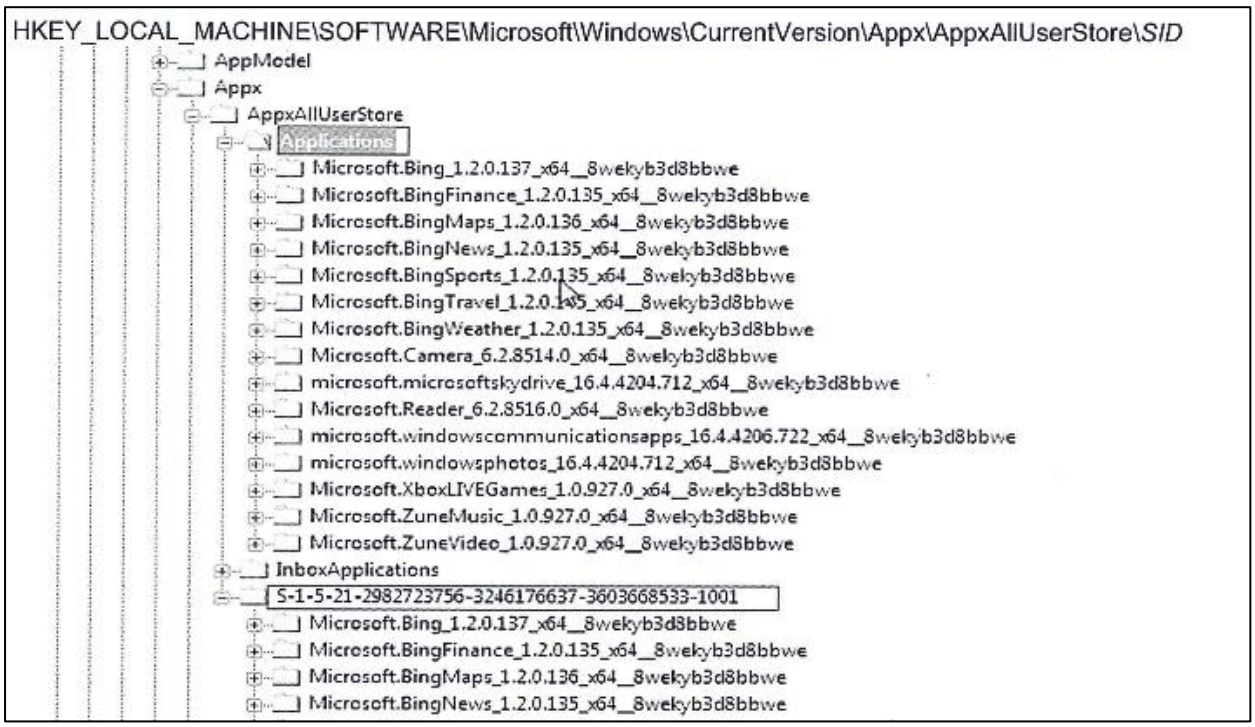


Figure : Information about Metro applications

Registry Keys & Values — Examples

HKLM\Software\Microsoft\Windows NT\currentVersion

- Registered Owner
- RegisteredOrganization
- Productid
- CurrentVersion
- CurrentBuildNumber
- ProductName
- InstallDate (UNIX time_t date format)

HKLM\System\CurrentControlset\control\Windows

- ShutdownTime (FILETIME date format)

HKLM\system\CurrentControlSet\Control\TimeZoneInformation

- ActiveTimeBias
- Bias
- DisableAutoDay1ightTimeset
- StandardName
- StandardBias
- standardstart
- DaylightName
- DaylightBias
- Daylightstart
  HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
  HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

These keys provide a listing of applications that start at boot

HKLM\Software\Microsoft\Windows\CurrentVersion\internet Settings\cache\Paths
HKLM\Software\Microsoft\Windows\CurrentVersion\internet Settings\Cache\Content
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Cookies
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\special Paths\Cookies
HKLM\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Cache\History
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\special Paths\History

HKLM\Software\Microsoft\Windows\CurrentVersion\internet Settings\URL History

- Daystokeep

HKLM\system\CurrentControlset\Services\Tcpip\Parameters\Interfaces\ [keyname]

- EnableDHCP (yes/no)
- IPAddress
- SubnetMask

- DhcpIPAddress
- DhcpSubnetMask
- DhcpServer
- LeaseObtainedTime (UNIX time_t date format)

HKLM\System\CurrentControlset\Control\Print\Printers\ [keyname]

- Name
- Port
- Printer Driver

HKLM\Software\Microsoft\Windows\CurcentVersion\Uninstal1\ [keyname]

- Add/Remove programs section - stores a record of each program installed on the computer.
- DisplayName
- Uninstallstring
- DisplayVersion
- InstallDate
- Publisher
- EstimatedSize
- InstallSourcenstallsource
- ModifyPath

HKCU\Control Panel\Desktop

- ScreenSaveActive
- ScreenSaverIsSecure
- ScreenSaveTimeOut
- wallpaper
- OriginalWallpaper
- SCRNSAVE.EXE

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Shows folder redirection e.g: A change of location for the My Documents folder.

HKCU\Software\Microsoft\MediaPlayer\Player\Settings

- SaveAsDir
- OpenDir

HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList

4.5 Volume Shadow Copy

During a Forensic analysis, it is quite common to have keyword search hits within a shadow copy file. It is also very common to find important Internet History evidence that has been backed up before the suspect tries to hide their tracks by clearing the Internet History in the browser. This section will explain how to retrieve the complete file.

Volume Snapshot Service mounts each snapshot as a hidden volume in the background. The content can be accessed by the examiner and relevant data can be located at the folder\file level, using a Windows Vista, 7, 8, 10 Ultimate, Pro, or Enterprise laboratory computer.

The suspect hard drive can either be connected to the computer via a write blocking device or can be virtually mounted if it is a forensic backup (*.E01, DD etc). Once mounted, the tool Shadow Explorer (www.ShadowExplorer.com) is a useful quick browsing tool, will show how many shadow copies are available on a specific volume and their dates, as was shown in Figure 52. The content of each snapshot can be browsed and content exported.

There are no differences in the process of access to shadow copies between Windows Vista/7 and Windows 8/10. However, there appears to be some changes made to the permissions in Windows 8/10 shadow copies, which prevent them being accessed from computer other than that which made the shadow copy. Fortunately, this should not represent too much of a problem, due to this feature being disabled by default in Windows 8/10.

1. With the suspect hard drive volume(s) mounted on a laboratory computer, open command prompt in Administrator mode.
2. Type in the command “vssadmin list shadows”. This command will list all the snapshots on each volume that the volume snapshot service can see, an example of the result is shown in Figure 5.75.

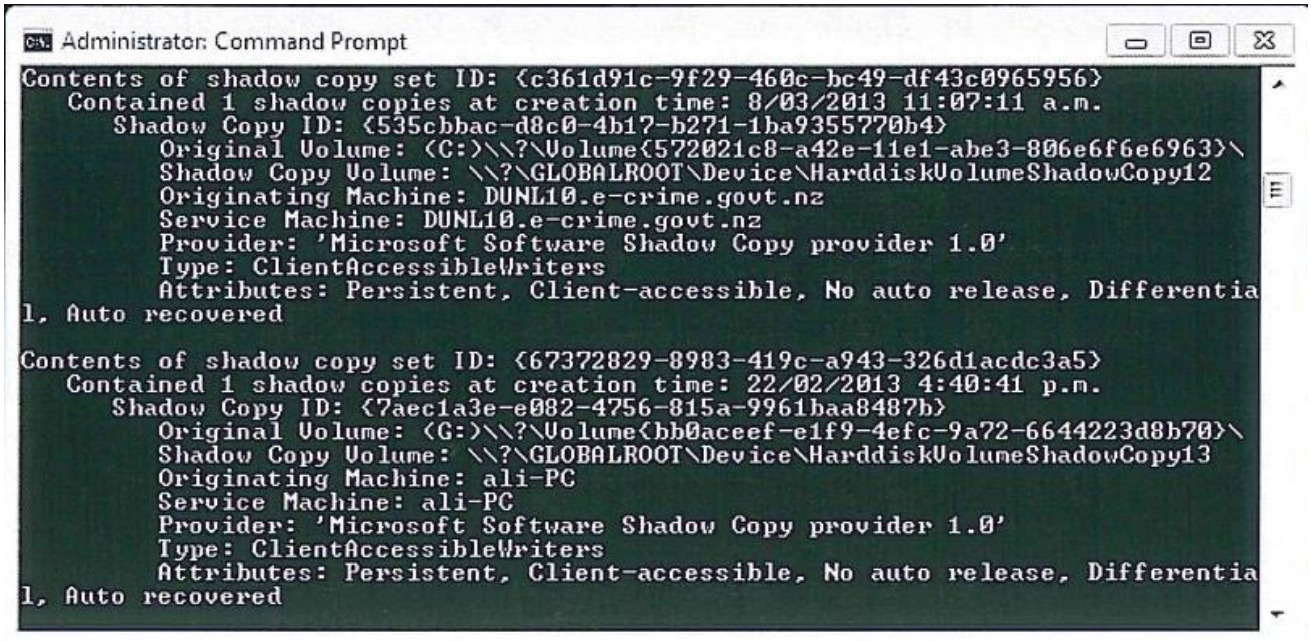


Figure : List of Mounted shadow copies

The list will show the identity of each snapshot, the date and time it was created, and the machine name (computer name) that created the snapshot. The date and machine name can be used to identify what volume snapshots may contain material that is relevant to the investigation.

If, during a forensic examination, a keyword search locates possible evidence within a snapshot, the Shadow Copy ID of that snapshot can be located at offset 0x90. The Shadow Copy ID is a GUID, as shown in third line for each shadow copy, Fig- 5.76.

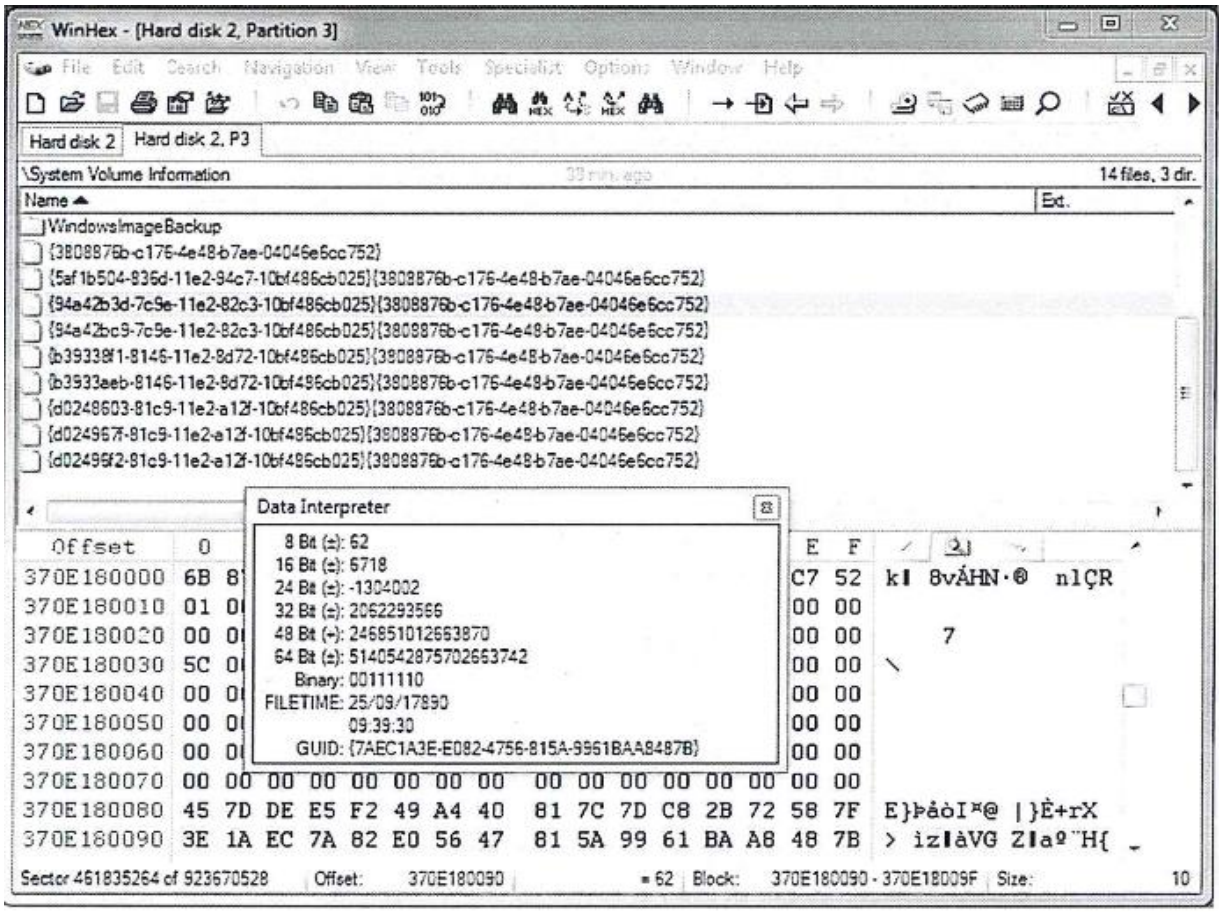


Figure : Shadow copy ID GUID

In the example shown in Figure 5.75, the snapshot file "{94a42b3d-7c9e-11e2-82c3-10bf486cb025}{3808876b-c176-4e48-b7ae-04046e6cc752}" has a Shadow Copy ID of {7AEC1A3E-E082-4756-815A-9961BAA8487B}. We then match that to the Shadow Copy ID from the list of shadows, to find where that shadow copy has been mounted as a volume - the Shadow Copy Volume field. In this case, it is \\? \GLOBALROOT\Device\HarddiskVolumeShadowCopy13.

A symbolic link to Shadows needs to be created. It is a good idea to give the symbolic link a name that matches the shadow copy number for easy reference. So, for ShadowCopy21, it would be easier to create a link that includes the number 21 and is in an easy to find location.

3. At the command prompt, type: "mklink /d C:\snapshot21 \\? \GLOBALROOT\Device\HarddiskVolumeShadowCopy13\"

This command will make a symbolic link to that snapshot, which will be C:\snapshot13, and can be seen in Windows Explorer. The trailing backslash must be present or the command will fail. Figure 5.77 shows the result from the executed command.

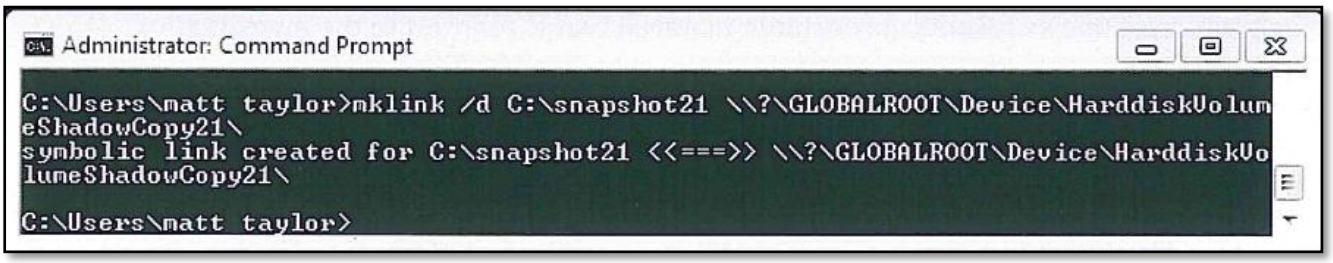


Figure : Symbolic Link Created

Figure 5.78 shows the result in Windows Explorer. If the link is shown in Explorer but cannot be accessed, it is most likely because the trailing backslash (\) was omitted.

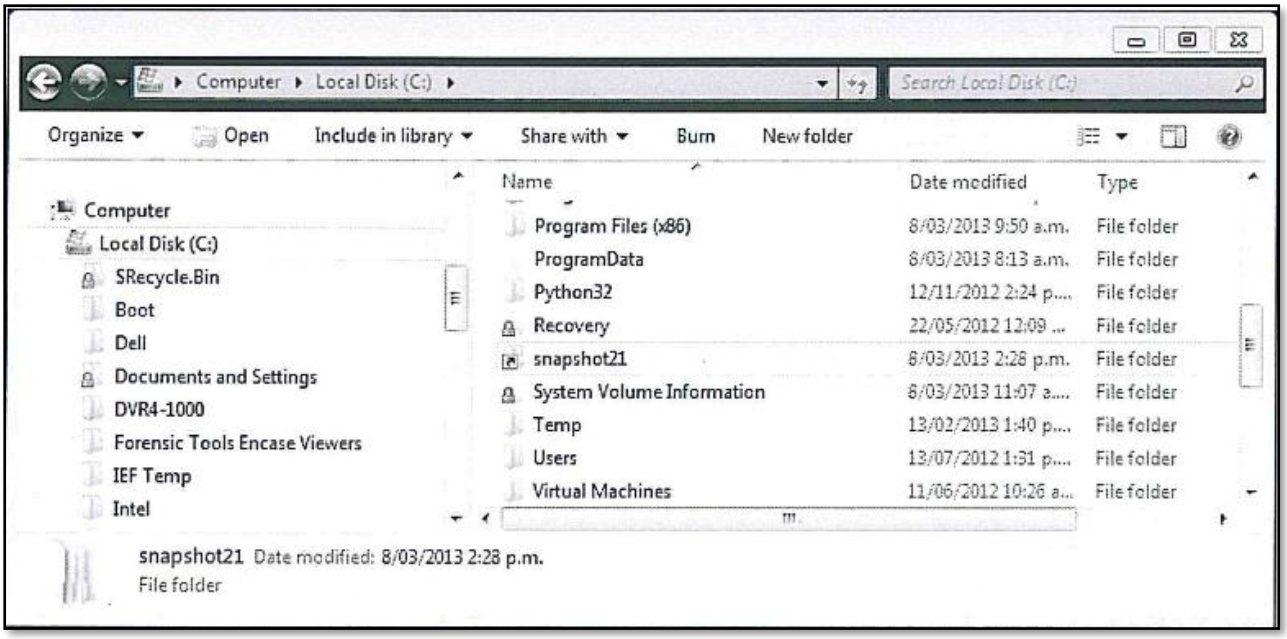


Figure : Symbolic Link to snapshot in windows explorer

It is possible to mount multiple snapshots at one time, using a “loop” command. (It is possible to mount all snapshots at once, but this is not recommended due to the risk of cross-contamination between evidential shadow copies and any laboratory computer shadow copies.)

The command is:

for /L %i in (start,1,stop) do mklink /d c:\rp%i

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy%i\

The start value is the first (lowest) shadow copy volume number that is to be mounted, and the stop value is the last (highest) in a sequential group. An example is shown in Figure 5.79.

```
C:\>for /l %i in (2,1,3) do mklink /d c:\shadow%i \\?\GLOBALROOT\Device\Harddisk
VolumeShadowCopy%i\

C:\>mklink /d c:\shadow2 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\
symbolic link created for c:\shadow2 <<===>> \\?\GLOBALROOT\Device\HarddiskVolum
eShadowCopy2\

C:\>mklink /d c:\shadow3 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\
symbolic link created for c:\shadow3 <<===>> \\?\GLOBALROOT\Device\HarddiskVolum
eShadowCopy3\
```

Figure : Loop command for multiple shadow copies

4. Create a forensic backup of the Snapshot using FTK Imager.

a. The Source is Contents of a Folder.
b. Browse to the snapshot reparse point created (snapshot##).

The content of the mounted snapshot is viewed with FTK Imager in Figure.

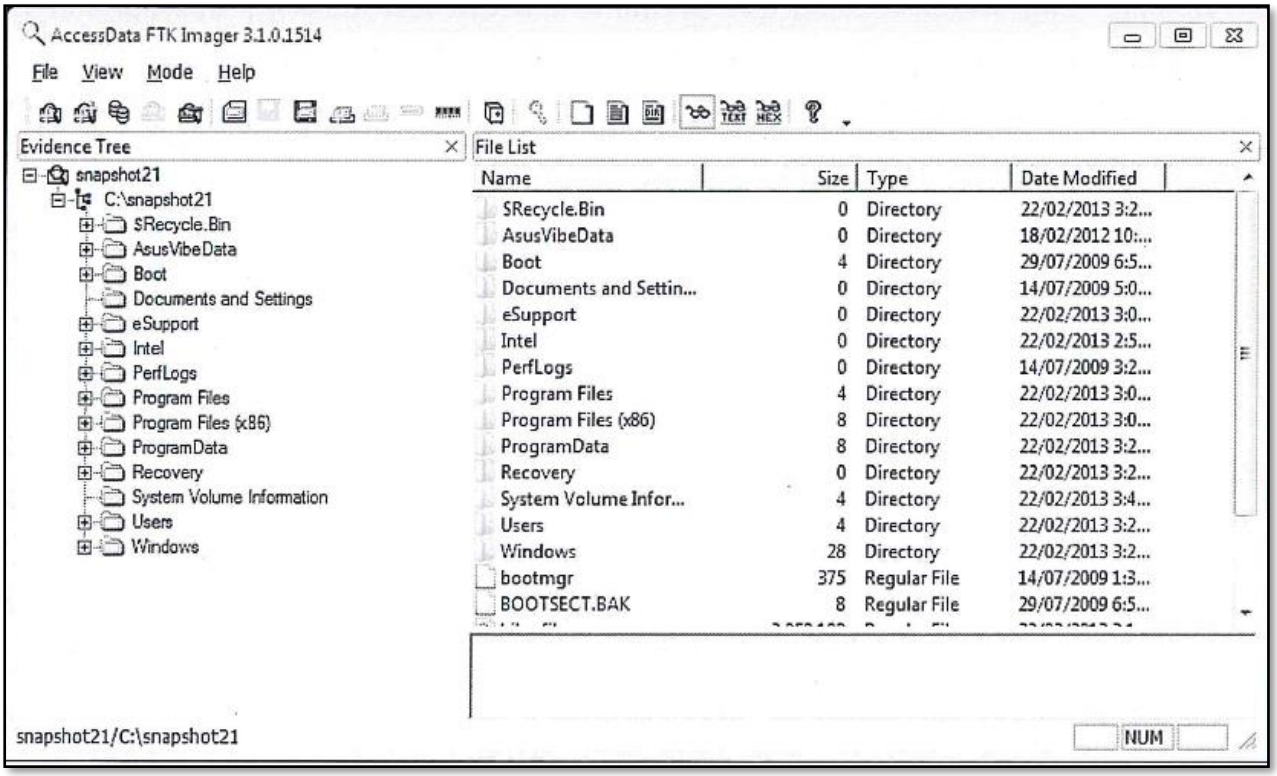


Figure : Snapshot in FTK

5. Browser Forensics

5.1 Browser

A browser is a software application which is used to access, retrieve and display content on the World Wide Web, which includes web pages, images, video and other files. It is a client/server model where, the browser is the client run on a computer or mobile device that contacts the Web server and requests information.

Analyzing web browser artifacts is a important part of any computer forensic investigation, as it can effectively determine the source of compromise orthe user's previous activities.

5.2 Forensics and its Importance

Internet applications installed on Windows can give important information about user actions performed previously on computer. For instance, a web browser is the only way to access the Internet, and criminals may use it to commit crimes related to the Internet or to target other users online. Internet users use web browsers to socialize, purchase online items, or to send e-mails and browse the web contents, among other things. This fact makes web browsers the preferred target for malicious actors to steal confidential information like account credentials.

What information does a browser store on an Operating System?

- Cache
- Website History
- Search Performed
- Online files executed and/or downloaded
- Cookies
- User Login

What is Browser cache?

Cache is the portion of a computer hard disk space where a browser temporarily stores recently visited webpage to speed up browsing. If the user tries to go back to those pages, the browser displays the stored pages instead of downloading them again. A web cache stores copies of documents passing through it. The browser includes entire web pages, images, CSS, audio, video etc.

Bookmarks and Favicons

Bookmarks can also prove helpful in identifying the behavior of the person and find out what kind of sites he frequents to.

Private Browsing Mode or Incognito mode – Is it really private?

Chrome's incognito mode cannot control, just like Internet Explorer's "InPrivate" mode, is what ends up in RAM and the pagefile.sys file (virtual RAM). It leaves lots of important artifacts in memory and in the pagefile.sys file.

Thumbnail Forensics

A thumbnail is an exact miniature copy of a picture file. It is used for previewing actual picture in Windows Explorer.They are stored by Windows Operating system to increase the preview of the image files faster.

Thumbs.db is a file created by Windows when thumbnail view is used. It is a hidden file which is not viewed by most users and not updated when files are moved from a folder which images have passed through or deleted. This gives a secondary chance that someone will leave behind at least partial evidence of an image in their Windows folders.

Thumbs.db no longer exists in Vista/7 as individual files. This data has been moved to a centralized database located in

\Users\<username>\AppData\Local\Microsoft\Windows\Explorer

Windows 8 and above stores thumbs.db and centralized cache of those at the same location. Tools like thumbcache_viewer and thumbs_viewer can be used look at thumbs.db file and the centeralized files like thumbcache_32.db, thumbcache_96.db, thumbcache_256.db and thumbcache_1024.db

5.3 Artefacts Location of Internet Explorer/ Edge

IE comes preinstalled with all versions of Windows. Its main registry key is locatedat HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer.

Browser Cache Location:

In Windows Vista, and Windows 7:

C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files

In **Windows 8**, and above:

C:\Users\username\AppData\Local\Microsoft\Windows\INetCache

The Index.dat file of Internet Explorer is hidden on your computer that contains list of all of the Web sites that you have ever visited. Every URL, and every Web page is listed there. To access it, go to the following location:

C:\Users\username\AppData\Local\Microsoft\Windows\TemporaryInternet Files\Content.IE5

Download History:

C:\Users\<username>\AppData\Local\Microsoft\Windows\History

Bookmarks and Fevicons :

C:\Users\<user_name>\Favorites

a) Microsoft Edge Web Browser

Microsoft Edge is the replacement of the Internet Explorer browser and the default browser for Windows 10. This is a lightweight web browser that integrates with the Cortana feature available in Windows 10, allowing a user to complete many tasks (e.g., open web pages, conduct online searches) using voice commands only.

Edge browser database is located at:

\Users\<UserName>\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\

MicrosoftEdge\User\Default\DataStore\Data\nouser1\xxxx-xxx\DBStore\spartan.edb

Microsoft Edge cache content is stored at:

\Users\<UserName>\AppData\Local\Packages\Microsoft.MicrosoftEdge_*****\

AC\#!001\MicrosoftEdge\Cache

Microsoft Edge stores its browsing history location:

\Users\<UserName>\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

The last browsing session of Microsoft Edge is stored at:

\Users\<UserName>\AppData\Local\Packages\Microsoft.MicrosoftEdge_****\AC\

MicrosoftEdge\User\Default\Recovery\Active

5.4 Artefacts Location of Google Chrome

Browser Cache Location:

C:\Users\<user_name>\AppData\Local\Google\Chrome\User Data\Default\Cache\

Download History:

C:\Users\<user_data>\AppData\Local\Google\Chrome\UserData\Default\HistoryProvider Cache

Bookmarks and Fevicons :

C:\Users\<user_name>\AppData\Local\Google\Chrome\User Data\Default\

- Bookmarks
- Favicons

5.5 Artefacts Location of Mozilla Firefox

Firefox is a free, open source web browser developed by Mozilla; it is considered amongthe most used web browsers in the world. Firefox stores its web history, download history, andbookmarks in a central database file named places.sqlite. This file exists within yourFirefox profile.

Browser Cache Location:

C:\Users\<USER_NAME>\AppData\Local\Mozilla\Firefox\Profiles\<SOMENAME.default-SOMENUMBERS>\

Download History:

C:\Users\<user_name>\AppData\Roaming\Mozilla\Firefox\Profiles\<some string>.default-<some numbers>\downloads.sqlite

Bookmarks and Fevicons :

C:\Users\<user_name>\AppData\Roaming\Mozilla\Firefox\Profiles\<some string>.default-<some numbers>\places.sqlite

5.6 Extracting and Analyzing SQLite File

Firefox stores its web history, download history, and bookmarks in a central database file named **places.sqlite**. This file exists within Firefox profile. It can be accessed by pressing the Windows key and typing the following:

%APPDATA%\Mozilla\Firefox\Profiles\

In the search box, Firefox profile will appear in the search result as a folder; click to access it.

The following window appears with whole content.

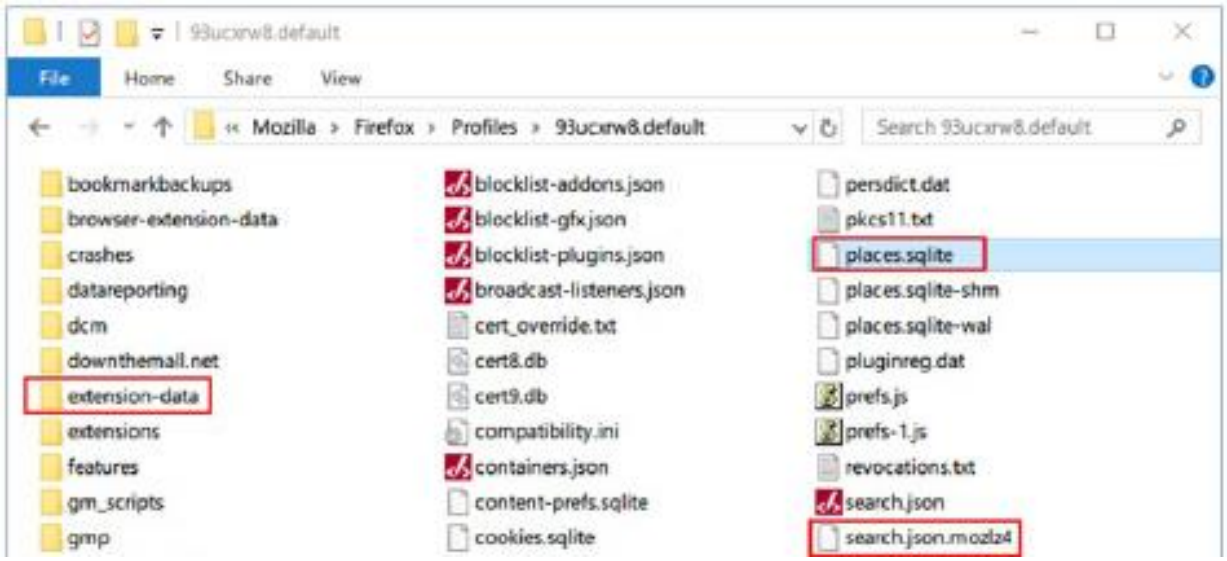


Figure: Sqlite Files

1. **places.sqlite**: Holds bookmarks, visited web sites, and download history.

The following tools can be used to retrieve information from the places.sqlite database file:

- DB Browser for SQLite (http://sqlitebrowser.org).
- MZHistoryView (www.nirsoft.net/utils/mozilla_history_ view.html). Displays list of previously visited web sites from the places.sqlite database.

2. **cookies.sqlite**: Stores cookies planted by web sites you already visited (cookies are usually used to save login usernames and passwords of previously visited web sites and/or to store web site preferences where applicable).

The following tools can be used to retrieve information from cookies.sqlite database file:

- MZCookiesView (www.nirsoft.net/utils/mzcv.html). Displays all cookies stored in a Firefox cookie file; The report generated can also be exported into a text, XML, or HTML file.
- DB Browser for SQLite.
- formhistory.sqlite: Stores your search keywords used in Firefox search bar and your searches entered into web forms.
- key4.db and logins.json: Here is where Firefox saves passwords. (Older versions of Firefox use the name key3.db for
- PasswordFox (www.nirsoft.net/utils/ passwordfox.html) can be used to display all usernames and passwords.

6. Servers

6.1 Introduction

A computer programme or apparatus that offers a service to another computer programme and its user, also known as the client, is referred to as a server. The actual computer that a server programme runs on in a data centre is also frequently referred to as a server. It's possible the device serves as a dedicated server or serves other functions.

A server programme responds to requests from client programmes, which may be operating on the same computer or on different machines, in the client/server programming model. Depending on the application, a computer may act as both a client and a server to other programmes requesting services from it.

Working

A physical machine, a virtual computer, or software that provides server services can all be referred to as servers. Depending on how the word "server" is employed, there are many different ways that a server might operate.

6.2 Physical and Virtual Servers

A physical server is a machine that runs server software.

A virtual server is a computerized simulation of a physical server. A virtual server has its own operating system and applications, just like a physical server. These are kept apart from any other virtual servers that could be running on the actual server.

A lightweight software component known as a hypervisor must be installed on a physical server in order to create virtual machines. To make the physical server capable of acting as a virtualization host is the hypervisor's responsibility. The virtualization host makes one or more virtual machines accessible to the actual server's hardware resources, including CPU time, memory, storage, and network bandwidth.

Administrators can assign particular hardware resources to each virtual server through an administrative console. Because numerous virtual servers can run on a single physical server rather than each workload requiring a separate physical server, this significantly reduces the cost of hardware.

Figure: Servers

6.3 Server Software

An operating system and an application are the two essential software parts that any server must have. The server application is run on the operating system as a platform. It grants access to the hardware resources underneath and offers the dependency services needed by the application.

The operating system also gives clients a way to communicate with the server application. The server's IP address and fully qualified domain name, for example, are assigned at the operating system level.

- Desktop Computers Vs. Servers

Desktop computers and servers have a number of commonalities as well as distinctions. The vast majority of servers are built around X86/X64 CPUs and are capable of running the same software as a desktop computer. Contrary to the majority of desktop PCs, real servers frequently have several CPU sockets and error-correcting memory. Additionally, in comparison to most desktop PCs, servers often support a far higher memory capacity**.**

Manufacturers of server hardware build servers to handle redundant components since they frequently conduct mission-critical workloads. There are servers that come with redundant network ports and redundant power supply. With the help of these backup parts, a server can keep running even when a crucial component break.

In terms of form factor, server hardware differs from desktop hardware. Modern desktop computers frequently come in the form of towers that can fit under a desk. Even while few companies still sell tower servers, the majority of servers are made to be rack mounted. Depending on how much rack space they take up, these rack mount systems are referred to as having a 1U, 2U, or 4U form factor. For example, a 2U server uses twice as much rack space as a 1U server.

A desktop computer's operating system and a server's operating system are two additional significant differences. A desktop operating system might be able to carry out some server-like tasks, but it is neither intended nor authorized to replace a server operating system. Desktop operating systems like Windows 10 are available.

Hyper-V, Microsoft's virtual machine platform, is a feature of some Windows 10 editions. Although Hyper-V can be run on both Windows 10 and Windows Server, the Hyper-V version that comes with Windows Server is intended for running production virtual servers, whereas the Hyper-V hypervisor in Windows 10 is primarily intended for use in development.

6.4 Types of Server

- **Web Servers:** An application that serves up requested HTML files or pages is known as a web server. Web browser serves as the client in this scenario.
- **Application Server:** A computer program that creates the business logic for an application software in a distributed network.
- **Proxy Server:** A program that serves as a go-between for a client or user who is requesting a service from another server and an endpoint device such a computer.

- **E-mail Server:** A program that accepts receiving emails from local users (users on the same domain) and remote senders and routes outgoing emails for delivery.
- **Virtual Server:** An application operating on a shared server that is set up such that each user feels as though they have full control over the server.
- **Blade Server:** A server chassis that holds numerous server blades—thin, modular electronic circuit boards. Each blade is a separate server that is frequently devoted to a single application.
- **File Server:** A computer that manages and stores data files centrally so that other computers on the same network can access them.
- **Policy Server:** A security component of a policy-based network that provides authorization services and facilitates tracking and control of files.
- **Database Servers:** A database or databases are hosted on this server. Database queries are executed by client programs to read data from or publish data to the server-hosted database.
- **Print Server:** One or more network-attached printers, or print devices as some server providers refer to them, are accessible to users through this server. The print jobs that users submit are placed in a queue on the print server. Depending on the job type or the person who submitted the print job, certain print servers can prioritise the jobs in the print queue.

7. RAID Configuration

7.1 Introduction

Using RAID technology, data storage can be made more efficient and/or reliable. The acronym refers for either Redundant Array of Independent Drives or, more formally and less frequently, Redundant Array of Inexpensive Disks. A RAID system has two or more parallel-operating discs. These can be hard drives, but an increasing number of people are using SSD technology instead (Solid State Drives). There are various RAID levels, each of which is best suited for a certain circumstance.

An independent controller card (a hardware RAID controller) may house the software necessary to carry out RAID functionality and manage the discs, or it may just be a driver. Some Windows versions, including Windows Server 2012 and Mac OS X, include software RAID capabilities. Hardware RAID controllers are more expensive than pure software RAID controllers, but they also perform better, especially with RAID 5 and 6.

RAID-systems can be used with a number of interfaces, including SATA, SCSI, IDE, or FC (fiber channel.) There are systems that use SATA disks internally, but that have a FireWire or SCSI-interface for the host system.

7.2 RAID Level 0- Stripping

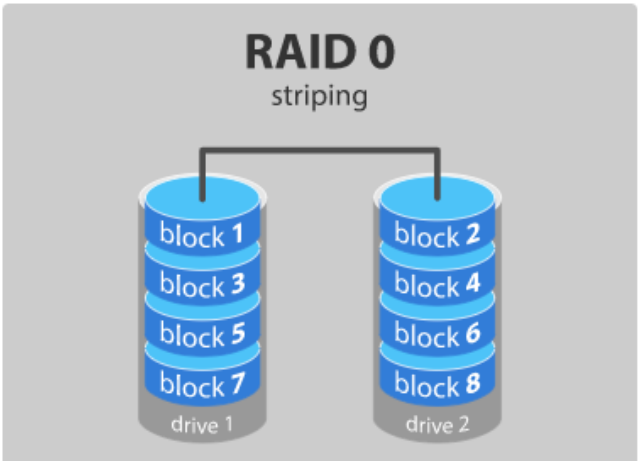


Figure: RAID 0

In a RAID 0 system, data is divided into blocks and written across all of the array's devices. This provides better I/O speed by employing many drives (at least 2) concurrently. Using numerous controllers, ideally one per disc, can improve this speed even more.

Advantages:

- Great performance is provided by RAID 0 for both read and write operations. The overhead of parity controls does not exist.
- There is no overhead because all storage space is being used.
- The technology is simple to use.

Disadvantages:

- Failure-tolerant RAID 0 is not. All of the data in the RAID 0 array is lost if one drive fails. Mission-critical systems shouldn't use it.

7.3 RAID Level 1-Mirroring

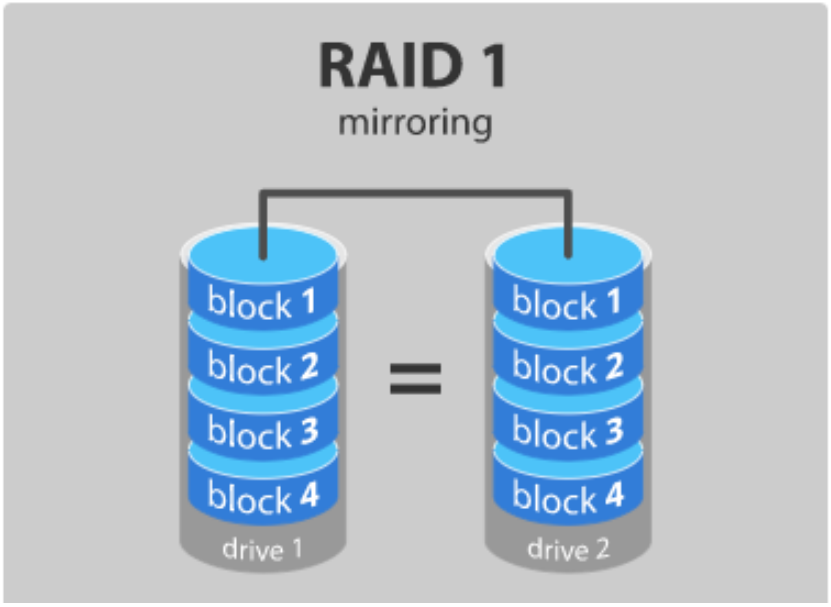


Figure: RAID 1

Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives). In the event of a drive failure, the controller continues to operate and retrieve data using either the data drive or the mirror drive. For a RAID 1 array, you require at least two discs.

Advantages:

- RAID 1 provides fast read and write speeds that are on par with a single disc.
- Data only has to be moved to the new drive in the event that a drive fails rather than being rebuilt.
- It is quite easy to use RAID 1 technology.

Disadvantages:

- The key drawback is that since all data is written twice, the effective storage capacity is just half of the overall drive capacity.
- A hot swap of a failing drive is not always possible with software RAID 1 solutions. Therefore, replacing the faulty drive requires shutting down the computer to which it is linked. This could not be appropriate for servers that are being accessed concurrently by multiple users. These systems frequently employ hardware controllers that enable hot swapping.

7.4 RAID Level 5 – Striping with parity

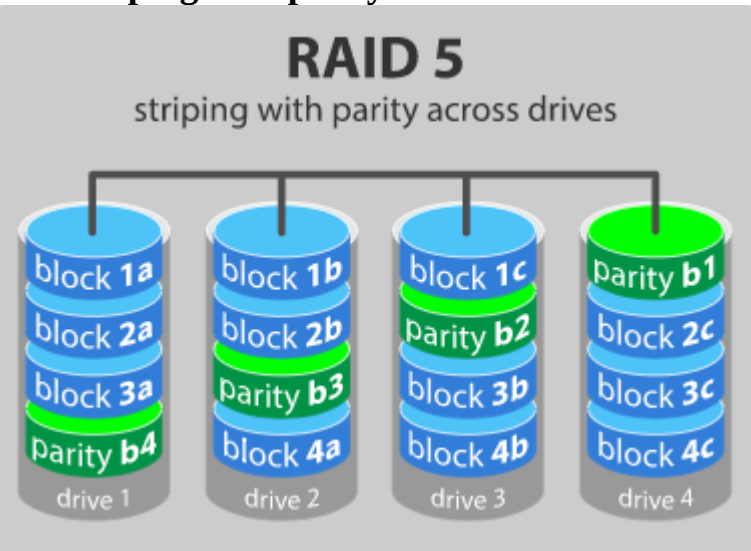


Figure: RAID 5

The most popular secure RAID level is RAID 5. At least three drives are needed, however up to sixteen can be used. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written. The parity data are distributed over all drives rather than being written to a single fixed disc. If one of the other data blocks' data is no longer available, the computer can recalculate it using the parity data. In other words, a RAID 5 array may survive a single disc failure without losing data or the ability to access data. Although software can be used to implement RAID 5, a hardware controller is advised.

Advantages:

- Write data transactions take a little longer than read data operations to complete (due to the parity that has to be calculated).
- Even when the failed drive is being replaced and the storage controller rebuilds the data on the replacement drive, if a drive fails, you may still access all of your data.

Disadvantages:

- Drive failures have an effect on throughput, although this is still acceptable.
- This technology is sophisticated. Depending on the load on the array and the speed of the controller, rebuilding the data when a 4TB disc fails and needs to be replaced could take a day or more. During that time, if another disc fails, the data are permanently gone.

7.5 RAID Level 6 – Stripping with double parity

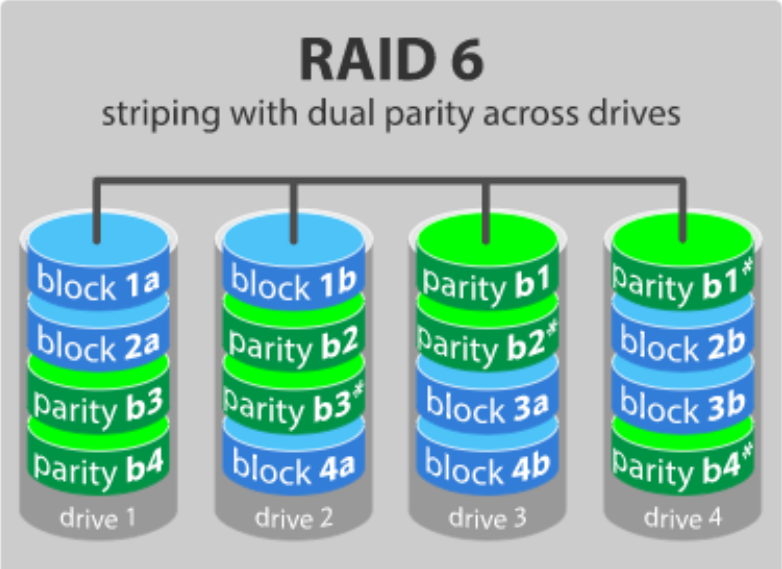


Figure: RAID 6

Similar to RAID 5, but RAID 6 writes the parity data to two discs. That means it needs at least 4 drives and is capable of handling 2 drives failing at once. Of course, there are extremely little odds that two drives will fail simultaneously. It takes hours or even more than a day to rebuild the swapped drive in a RAID 5 system, however, if a drive dies and is replaced by a new drive. During that time, if another drive fails, you still lose all of your data. The RAID array will even survive that second failure with RAID 6

- Advantages:
  - Read data operations occur very quickly, just like with RAID 5.
  - If two drives fail, you still have access to all data, even while the failed drives are being replaced. So, RAID 6 is more secure than RAID 5.
- Disadvantages:
  - Due to the additional parity data that must be calculated, write data transactions take longer than RAID 5 transactions. One report I read showed a 20% decrease in writing performance.
  - Throughput is impacted by drive failure; however, this is still acceptable.
  - This technology is sophisticated. It can take a while to rebuild an array once a drive fails.

8. MAC OS Forensics

8.1 Introduction

Professionals and enthusiasts in industries including photography, music creation and editing, video processing, and web development are huge fans of Mac. Siri, a voice assistant provided by Apple Inc., improves user experiences on Mac.

Apple frequently extols the virtues of its better hardware. An SSD is used in place of an HDD in Mac computers. Modern processors and other motherboard components are present.

Apple initially had a very small market share, but over time, it has experienced a considerable increase in its numbers thanks to its ardent fan base and tech enthusiasts.

8.2 Mac OS X

The operating system for Apple was introduced as Mac OS X, with the letter "X" standing for the number 10. Compared to Macintosh, Mac OS X had an entirely separate code base. It is based on the NeXTSTEP operating system code base. The core of the operating system is Darwin, an open source software. Apart from that, new applications were added like iTunes and GarageBand. Apple also offered additional online services such as iCloud products. This system brought a number of new capabilities to provide a more stable and reliable platform than its predecessor.

This included preemptive multitasking and memory protection to improve the system's ability to run multiple applications simultaneously without them interrupting or corrupting each other

8.3 File System

The first Macintosh computer, which was released in 1984, used the HFS (Hierarchical File System) file system. After 13 years, the HFS+ (Hierarchical File System plus) file system was released. It was a significant update to the Mac's file system and quickly took over as the default file system. Apple replaced the HFS+ file system in 2016 along with the release of macOS High Sierra and the Apple File System (APFS). The main feature of this file system, which is suited for SSDs in macOS, is encryption. Snapshot, copy-on-write information, space sharing, quick directory scaling, cloning for files and directories, automated safe-save, and better file system foundations are just a few of the new capabilities offered by Apple File System.

Some general characteristics of Apple File System are the following:

- In contrast to the HFS+ file system, the Apple File System supports sparse files, a type of computer file that makes an effort to use file system space more effectively when the file itself is partially empty.
- • HFS+ supports 1-second timestamp granularity while APFS only supports timestamp granularity down to 1-nanosecond intervals.
- 64-bit inode numbers are supported by APFS, enabling more secure data storage and supporting over 9 quintillion files on a single volume.
- HFS+ allows for 32-bit file IDs.
- Because APFS allows for the cloning of files and directories, the operating system can create effective file copies on the same volume without using up extra storage space.
- In order to create a read-only instance of the file system, APFS supports the snapshot feature, which records the state of a system.
- APFS uses the metadata "copy-on-write" scheme to make sure that updates to the file system are safe from crashes.

- TRIM operations are supported by both APFS and HFS+.
- Using multiple logical drives in a single container, where free space is accessible to all volumes inside of that container, APFS enables space sharing.
- APFS allows for complete disc encryption. For each volume in a container, a user can select no encryption, single-key encryption, or multi-key encryption models. Depending on the hardware, it uses the AES-XTS or AES-CBC encryption technique. Even when a device's physical security is breached, the multi-key encryption model ensures user data integrity.

8.4 Forensic Artifacts

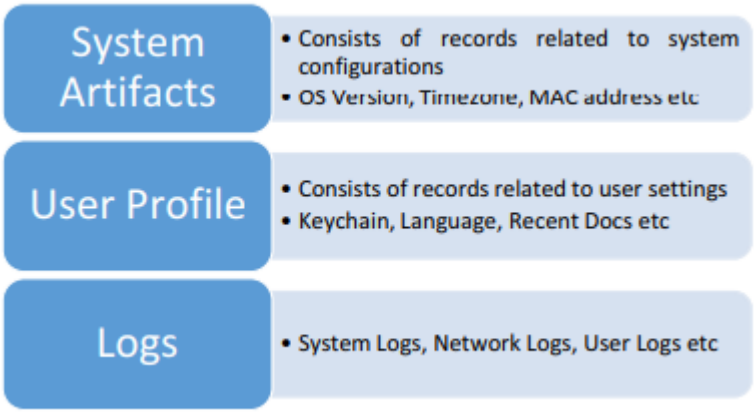


Figure: MAC Artifacts

The term "artifacts" refers to useful items or areas within a computer system that store information about various activities carried out by a user on the system. These artefacts vary from one operating system to another. Forensic investigators working with macOS may find various artifacts useful, including system artifacts, user profile artifacts, and logs.

8.5 System Artifacts

System artifacts are records that describe the configurations of the system, such as the OS version, MAC address, time zone, etc. The location where you can find these logs is indicated here.

OS Version	• /System/Library/CoreServices/SystemVersion.plist
MAC Address	• /private/var/log/daily.out
Timezone	• /Library/Preferences/.GlobalPreferences.plist
Language	• /Library/Preferences/.GlobalPreferences.plist
Start-up	• /Library/LaunchAgents/
Folders	• /Library/LaunchDaemons/
	• /System/Library/LaunchAgents/
	• /System/Library/LaunchDaemons/

8.6 User Profiles

These files contain data related to user activity on a system. Analysis of these files helps to track user activity and associate user profiles with system events

User Folder (Default)	• Desktop files -- ~/Desktop/ • Download folder -- ~/Downloads/ • Library -- ~/Library/ • Document folder -- ~/Documents/ • Deleted files -- ~/.Trash/
Recent folders	• ~/Library/Preferences/com.apple.finder.plist
DOCK – Persistent apps	• ~/Library/Preferences/com.apple.dock.plist
Recent Documents	• ~/Library/Preferences/com.apple.recentitems.plist
Safari Browsing History	• /username/Library/Safari/History.plist
Apple Mail	• Desktop/Library/Mail
USB devices	• /private/var/log/system.log

8.7 Keychain

The Keychain is a significant forensic artefact in Mac forensics. MacOS has a unique Keychain is a password management system that keeps track of sensitive data like passwords, certificates, and any other secure entities, including user credentials.

The operating system credentials used by MacOS are stored in a Keychain file. additionally, one more file for every system user. Keychain stores and encrypts the All other entities' secure notes and passwords are in plain text.

System keychain contains –

- Apple ID and Password
- Wi-Fi passwords
- VPN, FTP, and SSH passwords
- Passwords to iTunes backup
- Passwords to social networks
- iWork document passwords
- AirPort and TimeCapsule passwords
- Passwords to mail accounts
- Passwords to social networking websites

Keychain files are located at:

/Library/Keychains/ /System/Keychains/

8.8 Logs

Like any other operating system, Mac also stores logs of system and user activity. These logs are used for Timeline analysis. Logs are also used to check evidence integrity.

System Logs	• /private/var/log/asl/YYYY.MM.DD.U[XX].asl • /private/var/log/DiagnosticMessages/YYYY.MM.DD.asl • /private/var/log/system.log • /private/var/log/zzz.log
Shutdown Logs	• /private/var/log/com.apple.launchd/launchd- shutdown.system.log
Network Status	• /private/var/log/daily.out
Bootup Time	• /private/var/log/System.log (find 'BOOT_Time')
Filesystem Logs	• ~/Library/Logs/fsck_hfs.log
VMWare Logs	• /Library/Logs/VMWare

8.9 Information to Collect During MacBook Forensics Investigation

We would require the following information at the time of seizing the devices:

- Case Background/Bring Your Own Device (BYOD) policy – if any type of evidence needs to be acquired and analyzed.
- Details such as make, model, capacity, etc., and also decryption key/ password or decrypt the hard drive before/after handing it over for the imaging.
- Admin username and password, FileVault Password, or Recovery Key (if enabled) for unlocking the device.
- Original charger of the device.
- iCloud Credentials /Apple Id and Password (for extraction of recovery key from iCloud).
- In case of some of the latest MacBooks, as there is only one USB C port, we will have to carry a multiport adapter that can be connected to it to have the access to plug in the USB hard drive and charge it.
- Disable the secure boot and enable booting from external media on Apple T2-based MacBook devices before handover.
- Ask for the file system (HFS, HFS+, APFS) of the machine.

9. Linux Forensics

9.1 Introduction

The Linux operating system can be very helpful to a forensic investigator, despite not being utilized as frequently as Windows systems in forensic investigations. Not only will this section detail how to carry out forensics with a Linux system as a target, but also why using a Linux system in certain situations can be advantageous additional investigations.

9.2 Types of Linux Distribution

With the help of developers from all over the world, Linus Torvalds developed the free, UNIX-based operating system Linux. It is available in a variety of versions, or distributions, such as Red Hat, SUSE, Debian, and Ubuntu. Each edition is distinct, having particular advantages and disadvantages of its own.

The three main categories of Linux distributions are:

- Desktop distributions, which come with popular applications and a graphical user interface and are appropriate for home use.
- Server or enterprise distributions that can be used as a home server but are primarily used for business applications.
- Live-CD operating systems that are installed on bootable storage media An operating system that can be booted from a CD called a "live CD" is loaded into RAM and operates separately and externally from the target computer.

9.3 File System in Linux

Linux treats its devices as files, stored in /dev. Most Linux distributions share a basic directory structure, with files organized in the following directories:

- /bin: Common commands
- /boot: Files needed at boot time, including the kernel images that are pointed to by LILO or GRUB
- /usr: Local software, libraries, games, etc.
- /var: Logs and other variable files
- /dev: Interface files that allow the kernel to interact with hardware and the file system
- /home: Directories for each user on the system, containing user-specific personal and configuration files
- /mnt: Mount points for external, remote, and removable file systems
- /etc: Administrative configuration files and scripts
- /root: The root-user home directory
- /sbin: Administrative commands and process-control daemons
- /lib: Basic system libraries
- /opt: Optional and third-party software In order to find system information, the following commands can be used:

- uname -a: returns the computer name and Linux version
- ls -l: returns the list of files in the current directory
- ls -ul [filename]: returns the access time of the file
- netstat -s: returns protocol information

For storing files and directories, UNIX and Linux both use a tree-based, or hierarchical, structure. A UNIX disc structure contains. A forward slash (/) designates the root directory, which is the topmost directory. In a root directory, there are several subdirectories exist within these directories.

9.4 Linux Forensics

Linux has a number of simple utilities for imaging and basic disk analysis, including the following:

- dd: Copies data from an input file or device to an output file or device
- sfdisk and fdisk: Determines the disk structure
- grep: Searches files for instances of an expression or pattern
- md5sum and sha1sum: Create and store an MD5 or SHA-1 hash of a file or list of files (including devices)
- file: Reads file header information in an attempt to ascertain its type, regardless of name or extension Copyright © by All rights reserved. Reproduction is strictly prohibited Figure 6-1 This is a typical Linux file structure.
- xxd: Command-line hex dump tool
- ghex and khexedit: Gnome and KDE (X Window interfaces) hex editors

9.5 Acquisition through Kali Linux

1. Booting Kali Linux USB on a Computer
2. Let's begin by launching Kali and locating dcfldd. Access dcfldd by going to Kali Linux -> Forensics -> Forensic Imaging Tools. As can be seen below, it will be the fifth option on the menu.

Figure : Imaging Tools in kali

3. Start "Dcfldd"

A help screen similar to the one below will appear when we click on the dcfldd.

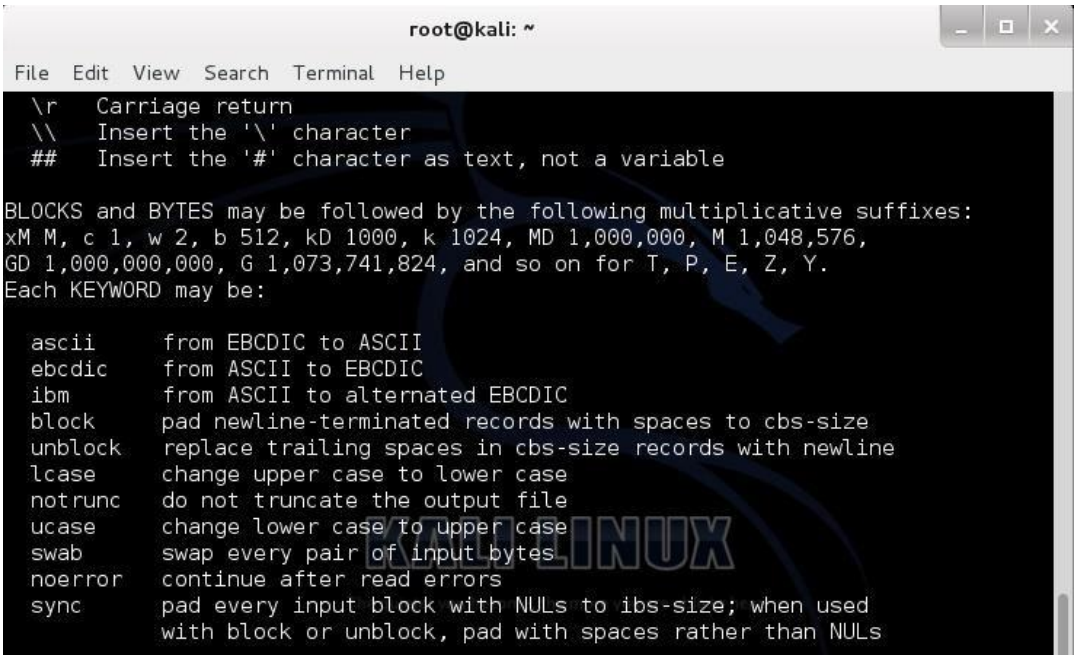


Figure : Dcfldd

We utilise a syntax for dcfldd that is quite similar to dd but has additional options for forensic capture.

4. Attach destination hard disk storage to store the image from suspect hard drive
5. Type “fdisk -l” command to view if the destination hard drive storage is attached to suspect notebook or workstation.
6. Now, to create the image's MD5 and capture a bit-by-bit image of the hard disc, type:

   dcfldd if=/dev/sda hash=md5 of=/media/diskimage.dd bs=512 noerror

- **if=/dev/sda** is the input device, in this case /dev/sda.
- **hash=md5** tells the command to calculate an MD5 hash of the image that we can use to assure the image integrity.
- **of=/media/diskimage.dd** is the file that the disk image will go, in this case on an external device mounted at /media.(Destination)
- **bs=512** tells the command we want to transfer the image 512 bytes at a time.
- **noerror** tells the command that in the case of error continue to do the data transfer, but write zeros where the error occur.

Note: Linux doesn't offer drive names with a single letter as Windows does, which is something we should be aware of. Hard drives in Linux are distinguished by a hd identifier, such as had, hdb, etc. It is sd, sba, sdb, etc. for SCSI (small computer system interface).

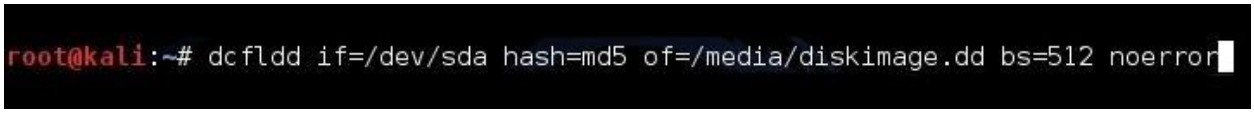


Figure 1 dcfldd command

This will create a bit-by-bit identical image of the hard drive and send it to our external drive with a filename of "diskimage.dd", 512 bytes at a time.

7. Type “ls” command to check if the image and md5 file is created
8. Type command “cat diskimage.md5” to view the hash value.

2. Digital Payment Fraud

1. Digital Payment Methods

In this era of the connected world, there are many ways to send and receive payments and they grow rapidly. Like in earlier day cash is the only way to pay, then comes to cheque, drafts, money order, etc. And as payment system evolved with internet and devices the fraudsters also evolved with the same path having advanced techniques to dupe the customers as well as banks. In this chapter, we will discuss various payment channels available by which one can perform the transaction, and also explained their threat vectors.

1.1 Internet Banking

Internet banking, also known as virtual banking, e-banking or online banking in a channel through which organization or an individual can perform various online transactions remotely. To perform online transaction user needs online banking username, password and transaction password. By using online banking facility users can pay online utility bills, recharge and perform different online transactions including Fund Transfer.

Figure : Internet Banking

Fund Transfer can be done using any one of these methods like RTGS, NEFT or IMPS.

- **RTGS:** Real Time Gross Settlement (RTGS) is a real-time settlement of funds transfers individually on an order by order basis. Real-time processing of instructions, rather than at the later point of time. Gross Settlement means the instruction for fund transfers executed individually. RTGS payment system is meant primarily for large value transaction. The minimum amount value allowed in RTGS in 2 lakh and no upper limit is there in this type of transactions. This service is available in branch time only as depending on the bank.
- **NEFT:** National Electronic Fund Transfer is a payment system which facilitating one-to-one funds transfer nation-wide. In this organization, firms, individuals and corporate having an account with any bank- branch can transfer funds to any other bank branch which participated in this Scheme. Presently, NEFT operates in hourly batches - there are twelve settlements from 8 am to 7 pm on weekdays (Monday through Friday) and six settlements from 8 am to 1 pm on Saturdays.
- **IMPS:** Immediate Payment Service offers an instant, 24X7, interbank electronic fund transfer service accessible through Internet banking or mobile phones. It allows any time fund transfer.

Parameters	NEFT	RTGS	IMPS
Full form	National Electronic Funds Transfer	Real-Time Gross Settlement	Immediate Mobile Payment Services
Minimum Transfer	₹ 1	₹ 2 Lakh	₹ 1
Transaction Time	Within 1-2 hours	Real-time, within a few minutes	Instant, within a few seconds
Payment mode	Online and Offline	Online and Offline	Online
Timings	365 days 24*7	365 days 24*7	365 days 24*7

Figure : Transaction Methods

Threat Vector:

- Internet Banking lures many of attacks like phishing, smishing, and vishing.
- An attacker can steal a username password using different technique and perform a transaction on behalf of the user.
- The transaction can be easily done if no two-factor authentication is enabled

1.2 POINT OF SALE

A point of sale (PoS) is the place where sales are made. On a macro level, a PoS may be a mall, a market or a city. On a micro level, retailers consider a PoS to be the area where a customer completes a transaction, such as a checkout counter. It is also known as a point of purchase.

Figure : POS

1.3 Near Field Communication (NFC)

Near field communication, abbreviated NFC is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over an NFC compatible PoS device to send information without needing to touch the devices together or go through multiple steps setting up a connection.

Example: HDFC PayZapp, Samsung pay and ICICI bank Pockets 'Touch & Pay' Feature, this Touch & Pay feature on Pockets app simply lets the user tap his/her smartphone at an NFC (Near Field Communication) enabled merchant terminal and make the payment through your linked ICICI Bank Debit/Credit Card.

Working of NFC: In the case of near field communication all the account details, are provided in the form of field(waves), so no physical card is required.

Figure : Payment via NFC

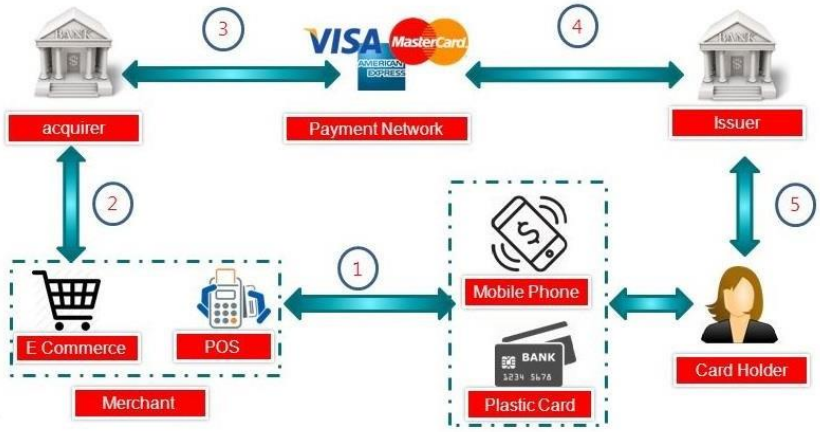


Figure : NFC/Plastic Card (Payment Authorization Steps)

Threat Vector:

- NFC communication protocol used by service providers may be vulnerable to interception, eavesdropping, and manipulation.
- An attacker can carry out data corruption by transmitting valid frequencies of the data spectrum that can interfere with the data transmission and can even block the flow of information from an NFC device.

1.4 Quick Response Code (QR code)

QR (Quick Response) Code is a square-shaped barcode that stores information about the product, link or information. By scanning one can download, locate websites, offer and perform financial transactions like paying for shopping, movie, and food bills payment. QR code requires a special application which scans and converts it to readable form, often most of the smartphones inbuilt have these feature.

There are different types of QR codes are there and they store a large amount of data as compared to simple barcodes. Nowadays QR codes are an instant way to scan and connect or purchase any item.

Bharat QR code developed by National Payment Corporation of India and collaborated with MasterCard, American Express and Visa apart from RuPay. Bharat QR code is rolled out so quickly because of its zero initial investment, as it is integrated with all payment gateway and Point of Sale (POS) devices.

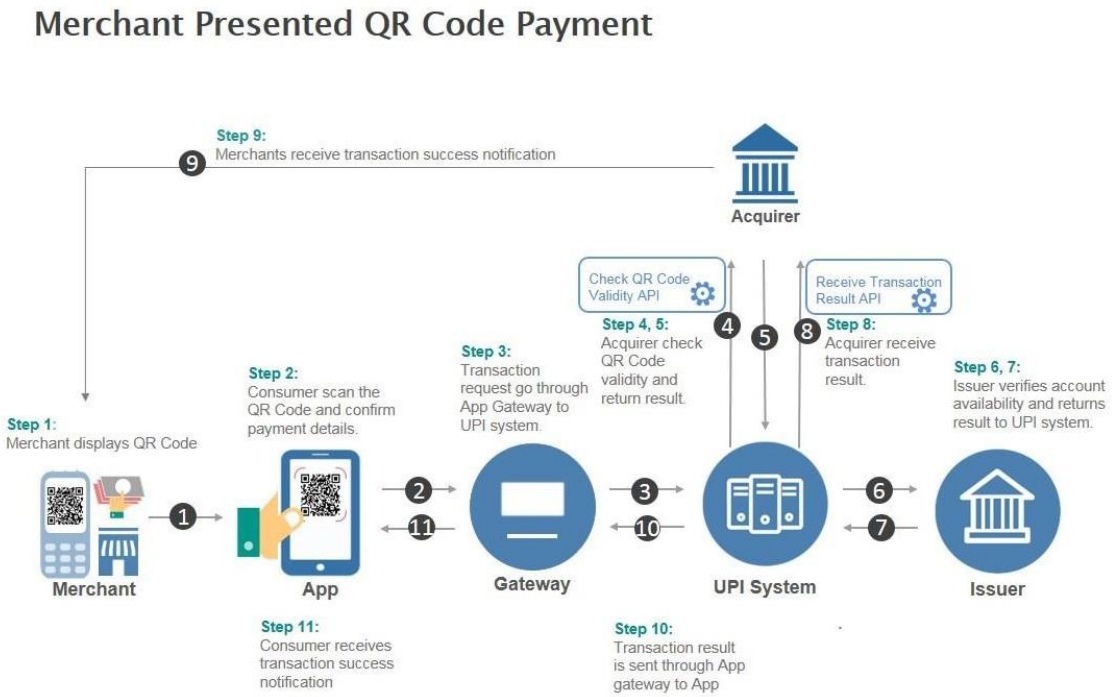


Figure : QR code Payment

Threat Vectors

- Attackers generating a QR code for a shortened URL, redirecting to the phishing or malicious site.
- Victims may be lured into scanning a QR code, looking same as a genuine brand, stealing their sensitive information, or to a malicious site that will exploit the mobile device.
- Criminals can easily craft malicious QR codes and affix them over genuine codes which may result in victims making payment to the spoofed party, not the real service provider.

Once a case related to QR payment fraud cybercrime gets registered, the investigation officer needs to collect a lot of information from various sources in order to identify the suspect computer that is involved in the commission of a crime and the criminals who are behind the commission of the crime. Therefore, intelligence gathering is one of the major task in the course of the investigation. The investigating officer will be having very few inputs, using that he has to collect the maximum amount of details about the criminals or suspects. Here comes the use of various information gathering techniques.

1.5 UPI (Unified Payment Interface)

National Payment Corporation of India has created a set of standard API specification to enable easier online payments. Its API supports Windows, iOS, and Android platform, Bank can extend its application and integrate with this API to start sending and receiving payments. It provides interoperability and compatibility across all other payment standards developed by the NPCI. And it supports "peer to peer" request and schedule payment, which can be later on paid by the end user as per convenience.

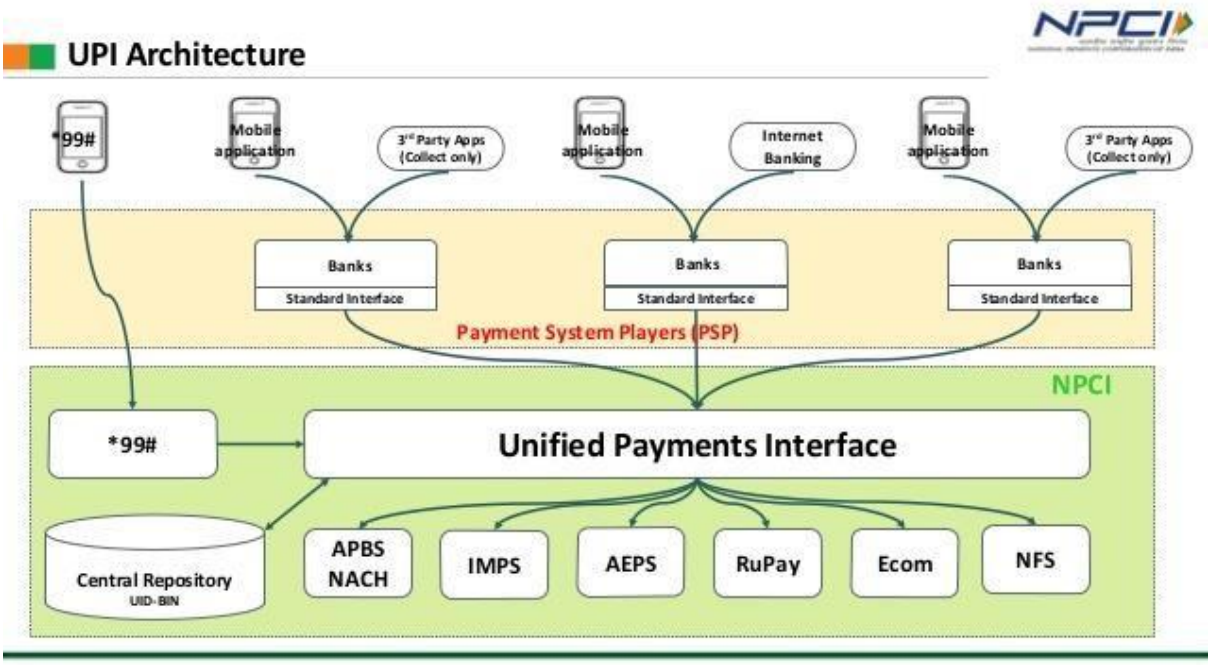


Figure : UPI Architecture

Threat Vectors:

- As these API can be integrated on any application, the developer should practice secure coding habits to eliminate vulnerabilities of application.

1.6 Mobile Wallets (E-wallets)

A mobile wallet which is also known as a virtual wallet that allows the user to carry financial transaction on their mobile devices. These wallets have the credit card or debit card which enrolled with it for payment mechanism. User can load amount from their bank account and use it directly from this wallet wherever it required.

Mobile wallets are categorized into these categories:

- **Open Wallet:** Allows a user to buy goods and services, withdraw cash at ATMs or banks and transfer funds. These services can only be jointly launched with a bank. Additionally, it allows its users to send money to any mobile number bank account.
  Examples: M-PESA by Vodafone, ICICI Bank pockets, and ITZ Cash Card
- **Closed Wallet:** Amount of money is locked with the merchant to place an order, use in case of a cancellation or return of the order, or gift cards.
  Example: Flipkart e-wallet
- **Semi-closed Wallet:** It does not permit cash withdrawal or redemption, but allows users to buy goods and services at the listed merchants.
  Example: Paytm Wallet, Mobikwik

Figure: Working of Mobile wallet

Threat Vectors:

- Fake apps appearing to be banking apps
- Malware infecting the mobile device, compromising the legitimate use of the device and stealing credentials, etc.
- Phishing and Vishing attacks specifically targeting the mobile device
- SMS based authentication like OTP for the online transaction using two-factor authentication can be performed using SIM swap-based attacks.

1.7 AADHAAR ENABLED PAYMENT SYSTEM (AEPS)

AEPS is a bank led model which allows online interoperable financial transaction at PoS (Point of Sale / Micro ATM) through the Business Correspondent (BC)/Bank Mitra of any bank using the Aadhaar authentication.

Figure : AEPS

1.8 Mobile Money Transfer (Telecom Based)

These types of the transaction doesn't require the data transmission for doing any transaction. This includes balance enquiry, statement of the bank- last transactions, funds transfer, ticket booking, etc. Using the SMS or platform based USSD (Unstructured Supplementary Service Data) or IVR (Interactive Voice Response) based systems.

1.9 Banking Cards (Debit / Credit / Cash / Travel / Others)

Banking cards offer consumers more security, convenience, and control than any other payment method. The wide variety of cards available – including credit, debit and prepaid – offers enormous flexibility, as well. These cards provide two-factor authentication for secure payments e.g PIN and OTP. RuPay, Visa, MasterCard are some of the examples of card payment systems.

Threat Vectors:

- Card trapping: This is a trap that retains the card when you insert it in the machine and the card is retrieved later.
- Shoulder surfing: While the victim is doing a transaction at ATM, or feeling from with details, the bystander tries to get the details from behind or by side. Later he can reveal details like PIN, date of birth, etc.
- Skimming: This technique involves attaching a data skimming device in the card reader slot to copy information from the magnetic strip when one swipes the card.
- Shimming: This technique involves attaching a card shimming thin layer strip into the chip-based card reader, and it will collect the details of the card and later on fraudster can use this data to make new magnetic strip based card.

1.10 Mobile applications

Mobile applications are developed by a specific bank for their customers. Customers can use these applications to perform a various online activity related to their account, this includes balance enquiry, transferring money to their beneficiary accounts and receive money. These apps provide more features than telecom-based services and support instant banking. These apps should be developed and tested with secure app development practices to ensure the security of customer data and money.

Threat Vectors:

- Fake Apps: The attacker may build a fraudulent application of mobile banking and palaces it over popular market stores like apple store and play store, which users download and be the victim of the trap. And the attacker seeks all the user details.
- Abuse: By doing abuse attack the attacker can take over the business logic of applications and use this logic to automate the different scams like auto booking of items during sale periods.
- Access violations: These occur when an attacker or legitimate user takes advantage of weaknesses in the authentication or authorization policies of the app.
- Rooted Device: Usage of rooted devices may help criminals to easily bypass the security and steal user information using malicious application.

1.11 UNSTRUCTURED SUPPLEMENTARY SERVICE DATA (USSD)

The innovative payment service *99# works on Unstructured Supplementary Service Data (USSD) channel. This service allows mobile banking transactions using basic feature mobile phone, there is no need to have mobile internet data facility for using USSD based mobile banking. It is envisioned to provide financial deepening and inclusion of underbanked society in the mainstream banking services.

Figure : USSD

*99# service has been launched to take the banking services to every common man across the country. Banking customers can avail this service by dialling *99#, a “Common number across all Telecom Service Providers (TSPs)” on their mobile phone and transact through an interactive menu displayed on the mobile screen. Key services offered under *99# service include, interbank account to account fund transfer, balance enquiry, mini statement besides host of other services. *99# service is currently offered by 51 leading banks & all GSM service providers and can be accessed in 12 different languages including Hindi & English as on 30.11.2016 (Source: NPCI). *99# service is a unique interoperable direct to consumer service that brings together the diverse ecosystem partners such as Banks & TSPs (Telecom Service Providers).

1.12 BANKS PRE-PAID CARDS

Prepaid Credit Cards are issued by banks and financial institutions and can be used for transactions in a very similar way as a credit card. Prepaid credit cards come loaded with funds and works using a very simple process. Unlike normal credit cards, which functions on borrowed credit from the bank, customers can make purchases using the funds available on the prepaid card. Similar to gift cards, purchases can be made until funds are available in the card.

Figure: Bank pre-paid cards

The biggest advantage of a prepaid credit card is that customers can make purchase transactions without incurring any debts and paying huge interests. Also, there is always the limit that has to be adhered to, as purchases have to be made only up to the amount available in the prepaid card.

1.13 MICRO ATMS

Micro ATM meant to be a device that is used by a million Business Correspondents (BC) to deliver basic banking services. The platform will enable Business Correspondents (who could be a local kirana shop owner and will act as 'micro ATM') to conduct instant transactions.

The micro platform will enable function through low cost devices (micro ATMs) that will be connected to banks across the country. This would enable a person to instantly deposit or withdraw funds regardless of the bank associated with a particular BC. This device will be based on a mobile phone connection and would be made available at every BC. Customers would just have to get their identity authenticated and withdraw or put money into their bank accounts. This money will come from the cash drawer of the BC. Essentially, BCs will act as bank for the customers and all they need to do is verify the authenticity of customer using customers' UID. The basic transaction types, to be supported by micro ATM, are Deposit, Withdrawal, Fund transfer and Balance enquiry.

Figure :Micro ATM

1.14 TERMINOLOGY RELATED TO DIGITAL PAYMENT

- **MMID:** A 7-digit unique number provided by bank that allows user for immediate payment services.
- **VPA, UPI Address:** Virtual Private Address, a unique identifier that helps UPI to track a person's account.
- **QR Code:** QR based code that contains a VPA of sender/receiver.
- **UPI PIN:** A secret passcode that is validated by NPCI irrespective of any UPI Application

- **PSP:** Payment Service Provider Apps/banks. PSPs may have banking licenses (Ex. If UPI Id is pmcares@sbi, PSP is State Bank of India.
- **Transaction number:** A reference number generated by the UPI application on successful transaction.
- **Collect Request:** A request sent by the person who wants to get money. A person who receives a collect request needs to enter PIN to complete the payment.
- **P2P:** Transaction between person to person. No merchant involvement. A friend sending money to another friend for personal dealing.
- **P2M:** Transaction from buyer to Merchant. Merchants typically are payment gateway like razor pay, cc avenues etc

2. Fraud related to Digital Payment

2.1 ATM/debit/credit card Frauds

The ATM cards are widely used for money withdrawals, shopping on the online site, paying money at the Point of sale machines, etc. Credit cards, debit cards, and smart cards are some of the examples of the ATM cards. As the use of ATM cards is increasing day by day, it poses a great amount of risk and frauds caused by the misuse of these cards. Fraudster performs various techniques in order to get the details of the ATM and uses the credential to do the fraudulent transactions.

Modus operandi:

- Commission of ATM frauds has two key aspects: firstly, getting access to the card or the data stored on the card and secondly getting the pin of the card. A criminal can get these through various methods. Some of them are discussed below.

a) Stealing cards:

One of the ways a fraudster can get access to the ATM card of the victim is by stealing it and use the card to perform fraudulent transactions. To get the PIN, the thief might shoulder surf or guess a weak password, such as a birthdate.

For stealing the card details attacker inject the small script to capture card related information, it is also known as a form of hacking.

Figure : Stealing Card information

b) Card skimming:

The ATM cards generally have a magnetic strip on it, which contains some of the electronic data which is used to authenticate when

we use the ATM card to perform for any kind of payment. Fraudsters install ATM skimmers to the ATM machines or the POS machines, which scan the electronic data present in the magnetic strip as the victim perform the transactions on the ATM machine or the POS machine.

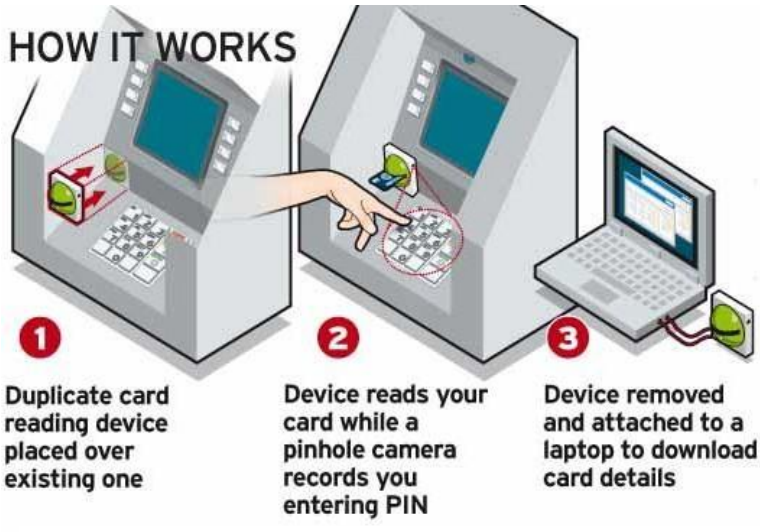


Figure : Working of Card Skimming

c) Card shimming:

The emergence of chip-enabled cards was supposed to help eliminate vulnerability to identity theft and fraud because those cards could not be "skimmed." But fraudsters are persistent, and they've found a way to lift information from chip cards using this new technique called "shimming,"

Fraudsters insert a paper-thin device, or "shim," enabled with a microchip and flash storage directly into the dip-and-wait slot on card readers that accepts chip-enabled cards.

The shim then copies and saves the information from a credit card or debit card. While the information from the chip can't be used to clone another chip card, it can be employed to create a version of the card featuring a magnetic strip —and plenty of retailers, especially online, still accept such cards.

Figure : Shimming module

d) Buying card details from internet

There are a lot of websites available on the internet as well as on the Dark web where people sell the ATM card details of various users which were gained by hacking into the bank's database or by posting a fraudulent website and getting the credentials from it.

All the above-mentioned techniques are used to get the details of the ATM card. From here on the fraudster can use the details to do some online transactions or he can make duplicate ATM cards by embedding the electronic data onto the empty cards with the magnetic strip.

Investigation:

1. On receiving the complaint, the first step an IO need to do is to block the ATM card temporarily by calling the corresponding bank, so that the fraudster is not allowed to make any other transactions.
2. If the fraudster does any online transaction using the ATM card then the IO can contact the online portal on which the transaction was made asking for the IP address of the system used to make transaction along with the personal details of the person, which are collected by the portal.
3. Suppose the fraudster transferred the money to some different account, then IO has to identify the account to which the amount was transferred from the victim's bank statement and proceed to the bank asking for KYC documents of the account holder.
4. In case the fraudster has used a duplicate ATM card and performed any kind of withdrawals at any of the bank ATMs, IO can proceed by asking the bank the statement of the victim account and identify the location of the ATM machine from where the withdrawal occurred and take out the CCTV footage for the respective duration and identify the fraudster.

2.2 OTP Frauds

As a measure to increase the security of the electronic transactions that are happening through the internet and various payment applications, the concept of multi factor authentication was introduced in all the electronic transactions. One of the most common techniques used in the multi-factor authentication of the financial transactions in electronic form is the One Time Password (OTP). In this process, the user authentication is performed by sending a OTP from the payment portal to the mobile number attached to the account of the user.

In the OTP frauds, the OTP generated by the payment portal is captured or taken by the fraudster from the user by adopting various techniques. One of the most common techniques used by them is by calling the user and asking them to share the OTP in the pretext that they require this for unlocking the card/attaching the Aadhar/approval of loan and so on. Also, there are techniques by which the user's mobile is infected with malware that can forward the OTP automatically to the fraudsters or a mechanism by which fraudsters can read or access the OTP delivered to the mobile of the user.

Modus operandi:

The fraudster calls the victim saying he was making some online registration and had entered the phone number of the victim by mistake since the two numbers were similar. And asks the victim to share the code received on the phone, so that he could complete the registration. Whereas the fraudster is actually trying to reset to online bank account of his target using the One Time Password (OTP).

Investigation:

- The crime committed by stealing the OTP and using it for doing fraudulent financial transactions is considered to be Identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
- The investigation of these cases has to be proceeded on the basis of the calls received from the fraudster if he/she has called and taken the OTP. The IO has to take the CDR and customer identity details of the owner of the SIM and proceed with investigation. But, in most of the cases it is found that the SIM cards used by the fraudster for these purposes are not registered using genuine name and addresses. In such case, we need to further the investigation of the case by

analyzing the call details of the IMEI traces, tower locations and other information that can be collected in this regard.

- If the fraudster used the OTP that he has stolen for making a bank transaction or changing the password of online banking services, then we need to request the bank for the details of the accounts into which money was withdrawn or transferred. Once we identify the account particulars, we will continue the investigation in this line. If no transaction was done but they have changed the password of the online account, immediately bank need to be alerted to block the transactions from the account temporarily. Then, we proceed to collect the details of the IP address of the machine that is used to make those changes in the profile or password of the account.
- Once, we receive the IP address of the device that is used to make the fraudulent online transactions, we can find out the ISP, who has allocated the IP address. Then we would approach the ISP for collecting the details (name, physical address, mobile and email attached, the location from which device was connected to the internet etc) of the person on whose name this IP was allocated.
- These are some of the ways by which we identify the suspect device that was used to do the transaction.
- Now it is the task of the IO to proceed and seize the device.
- Once the device is seized, acquire the data from the device forensically and analyse for collecting evidences such as the web sites visited, details of credit cards if he/she has stored on it and other relevant digital evidences required for proving the involvement of the device in the commission of the offence.
- After that, IO has to collect required evidences for connecting the suspect to the suspect device. This can be done by collecting all the circumstantial evidences related to the commission of the offence.

2.3 Job Frauds

Figure : job frauds

Many of us would have received messages in our mobile phones requesting us to apply for job with working from home and payment of good salaries. We would have seen lot of advertisements that were received in our mail box or posted on social media sites. Though we cannot tell that all these are frauds, job frauds using electronic media would look something like this. There can be a website where in fraudster could ask all the persons to register with all the personal information of people and they can collect lot of information, they can collect some money promising them placements in lucrative positions in prime companies. If people are defrauded by using these techniques through online platforms, they are considered to be job frauds. In this kind of frauds, scammers trick victims into

handing over your money by offering you a 'guaranteed' way to make fast money or a high- paying job for little effort.

Modus operandi:

The fraudster would post recruitment advertisements over social media site or send personal e-mails to the victim asking them to pay some fees as a deposit to secure the job.

Investigation:

1. In all such cases, the IO can take leads from various places and proceed for investigation of the cases. These include

I. If the victim received communication from the fraudster through email, collect the details of the email id, take the copy of the email along with the header following proper established procedures. Collect the details of the persons who were contacted by the victim and collect their KYC details. If the victim paid money through any bank account, collect KYC details of the account holder and investigate. To find the origin of the email and locate the user of the e-mail account, the procedure to be followed is explained in the e-mail investigation unit.

II. If a website is being run by the fraudster for advertising or registration for jobs and other purposes, then find the details of the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact etc. collect the details of the owners of the domain name as well following procedures mentioned in the 'internet investigation' unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.

2.4 Hacking of Bank Accounts

Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer user. If one can get access to the credentials of the account holders of different banks, we know that they can use them to do the transactions online or otherwise. So, it is a practice that fraudsters collect the details of the bank account by hacking the bank servers, payment gateways, user machines that are being used for doing online transactions, e-commerce sites, etc. For the purpose of hacking, fraudsters may make use of any vulnerable services running on the victim's machine or send any kind of malicious program that infects the victim's machine.

Modus operandi:

- Fraudsters take advantage of the software vulnerability present in user system or in the bank application to fetch the login credentials and perform the fraudulent transactions.

a) Using Key-Loggers

Key-Logger is a piece of software which once installed on any system, it tracks or logs all the keystrokes made by the victim using the keyboard and sends this data to the fraudster. Whenever a user enters his/her credentials in the key-logger infected machine, the fraudster receives the credentials sitting in a remote location.

Fig.: Hardware Keylogger

b) Using Malware

Malware is nothing but a software program, which, when running on a computer, it makes the system perform the tasks that an attacker wants it to do.

- **PoS RAM scraping malware**
  This malware infect the point of sale (PoS) machines and capture the credit/debit card information stored in the RAM and send it to the fraudster who is sitting in some remote location.
- **ATM malware**
  These types of malware infect the ATM machines and perform some unusual activities such as stopping the ATM machine to dispense or dispense all the money that is available inside the ATM when the fraudster give some instruction to the ATM.
- **Malware infecting bank's server**
  These types of malware infect the bank servers and send the database of the user details, user credentials, etc to the fraudster who is sitting in some remote location.

Investigation:

1. Whenever a case related to stealing of the bank account credentials of a person through the process of hacking is reported, police officer need to register an FIR as per sections 43(a), 43(b), 43(g) r/w 66, 66C of IT Act and sections 379, 406, 420, 467, 468, 471 of IPC, whichever is relevant.
2. We then need to identify the computer that was hacked for stealing the account details. We know that, when a computer system is hacked/compromised, there is a significant amount of evidence that will be available in the form of logs in the computer as well as the network it is connected to. IO should collect the bit-by-bit copy of the infected/ compromised system. From the image acquired, an IO should extract the logs and analyze them in order to identify the IP address and the details of the fraudster. We need to analyze the machine to find out all the other information that the fraudster has stolen.
3. If we get to know the vector used by the fraudster such as email, social media, website, etc, we can collect further details about the activities performed by the fraudster by investigating the

respective platforms. The processes to be followed by the IO for investigating the platforms are discussed in the other units in detail.

2.5 Identity Theft

In this kind of frauds, the fraudster uses various techniques in order to get the personal information of the victim such as login credentials of Internet banking; ATM pins, etc and uses this personal information of the victim to perform fraudulent transactions causing financial loss to the victim. Fraudster performs identity theft in the following ways:

a) Phishing

Phishing is an attempt made by the fraudsters, where he sends the link of the page of a fake bank website to the victim either by mail/SMS or over social media sites in order to steal the personal information of the victim such as Customer ID, PIN, Credit/Debit Card number, Card expiry date, CVV number, etc. In recent years, phishing has emerged as one of the biggest threats to individuals and to the economy as well.

Modus operandi:

1. In these cases, fraudsters normally create a fake website that looks similar to a banking website or an e-commerce website and sends a link to the victim by email/SMS asking them to enter the credentials to verify the account status or change the password, etc. Once the victim enters the credentials in that site, the fraudster receives those credentials and uses it to perform fraudulent transactions.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. The IO should collect the URL which was received by the victim and identify the location of the phishing website. We would also collect the details such as the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact, etc. We have to collect the details of the owners of the domain name as well following procedures mentioned in the 'internet investigation' unit. The evidence of the existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.

b) Smishing

Smishing involves obtaining the personal information of the victim using SMS text messages or tricking a user into downloading a Trojan horse, virus or other malware onto their cell phone or another mobile device.

Modus operandi:

In Smishing, the fraudster sends an SMS to the victim with Link asking the victim to go to the link and register for securing their account or verifying the credentials with the bank server as a security check-up.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. As the victim receives the message via SMS, IO can proceed to investigate based on the SMS received from them. An IO has to take the CDR and customer identity details of the owner of the SIM and proceed with the investigation. But, in most of the case, it is found that the SIM cards used by the fraudster for these purposes are not registered using genuine name and addresses. In such cases, we need to further the investigation of the case by analyzing the call details of the IMEI traces, tower locations and other information that can be collected in this regard.

c) Vishing

Unlike traditional phishing attacks where the fraudster uses fake emails or link manipulation to get the information from the victim, vishing is when a fraudster tries the call the victim in order to get the information from the victim. There are a number of techniques used, e.g., a concern that one of your accounts may be vulnerable, a threat that you have not paid a bill, an offer of a reward or prize.

Modus operandi:

The Victims receive a call from the fraudster saying that they are the representatives from the banks/E-commerce sites and asking them to reveal the banking credentials so that they can verify the account.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. As the fraudster communicates with the victim by calling him/her, IO can precede the investigation by taking the CDR and customer identity details of the owner of the SIM.

d) SIM Cloning

This has mushroomed after OTP became mandatory for banking and card transactions. The fraudster gets hold of victim account details and identity proof to get a duplicate SIM after getting original SIM deactivated, and uses this SIM card to perform all transactions.

Modus operandi:

Fraudster approaches a victim's mobile service provider with a victim's fake identity proof and, claiming loss of handset or SIM damage, seeks a duplicate SIM card. Following verification, the

original SIM is deactivated and a new one is issued to the fraudster. He then initiates financial transactions from a victim bank account, details of which he had earlier stolen, and receives payment confirmation requests on the duplicate SIM. Since the original SIM has been deactivated, the victim remains unaware of the fraudulent transactions he makes.

Investigation:

These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.

2.6 Fake Mobile Banking Apps

Once installed, these apps will steal the personal details of the customers, like user-id, password, PIN, Credit/Debit Card details and most probably sell them in the black market. They also install malware application for accessing the OTP and removing SMS from the inbox.

Modus operandi:

Once installed, most of these apps ask for the users' bank account details, debit/credit cards, name, address and phone numbers. They ask for these details so that the app can fetch the current bank balance.

Other apps are even asking for Aadhar, PAN Card details from the users. Once the information is submitted, the details are sent to a command center, without any verification. Most of the apps are sending data to a common command center, which signifies the role of an organized gang of hackers.

Investigation:

These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.

2.7 Credit Card Fraud

Credit cards are commonly being used for online booking of airline and railways tickets and for other e-commerce transactions. Although most of the e- commerce websites have implemented strong security measures (such as SSL, secure web servers, etc.), the instances of credit card frauds are increasing.

The victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites, online gambling transactions, etc.).

Modus operandi:

Petrol pump attendants, workers at retail outlets, hotel waiters, etc. note down the information of the credit cards used for making payment at these establishments. This information is sold to the cybercriminals (also known as carders) that misuse it for online frauds.

Investigation:

1. The websites, where the credit cards are misused, should be examined carefully. Sometimes criminals set up bogus e-commerce websites to misuse the credit card information.
2. The co-operation of the website operators is required to obtain the IP addresses used to make fraudulent transactions. Once these IP addresses are obtained, a WHOIS search will reveal the Internet Service Provider.
3. The ISP can provide the end user details. The suspect's computer can be examined using WinHex and all relevant evidence can be extracted.
4. Sometimes the investigation may lead to a cybercafé or other public computer. In this situation
5. Conventional investigation can be used (e.g. photographs of the suspects can be shown to the
6. Cyber café manager). In case physical goods are delivered pursuant to the fraud, the address should be investigated.
7. These crimes are considered as a denial of service, the penal provisions for this crime are covered under Section 43 and 66 of the Information Technology Act 2000 and section 420 of Indian Penal Code.

2.8 Denial of Service

A Denial-of-Service (DoS) attack is an attempt to make a system/application or network resource unavailable to its users for their intended purposes, such as to interrupt or suspend services of a host connected to the Internet. A successful DoS attack directly affects the availability of a network system (server, system, platform, etc.)

Most of the DoS attacks are "Distributed Denial of Service" attacks (DDoS attacks). A DDoS attack is an attack in which multiple computer systems attack a target, such as a server, website or another network resource, and potentially causes a denial of service for users of the targeted resource.

Modus operandi:

In these cases, the attacker sends the requests to banking service from different systems which would lead to the banking system not serve legitimate user's requests. Attackers are using online botnet servers to perform these types of attack.

Investigation:

These crimes are considered as a denial of service, the penal provisions for this crime are covered under Section 43 (e), (f) and(g) of the Information Technology Act 2000.

2.9 Insurance Frauds

Figure : Insurance frauds

Insurance fraud occurs when individuals deceive an insurance company, agent or other person to try to obtain money to which they are not entitled. It happens when someone puts false information on an insurance application and when false or misleading information is given or important information is omitted in an insurance transaction or claim.

There are two types of insurance frauds:

- **Hard Fraud:**

Someone deliberately fakes an accident, injury, theft, arson or other loss to collect money illegally from insurance companies.

- **Soft Fraud:**

Normally honest people often tell "little white lies" to their insurance company. Many people think it's just harmless fudging. But soft fraud is a crime.

Modus operandi:

Fraudster furnish false documents and manipulation in citing the cause of death as part of the adopted by to claim insurance benefits.

Ex:

- Billing for services that were not provided
- Performing medically unnecessary services
- Altering claim forms, medical documentation, etc.
- Billing for a service that costs

Investigation:

- IO has to verify each document of the insurance carefully and identify fraudulent claim which the fraudster is trying to claim

2.10 Payment Gateway Frauds

A payment gateway is a service which acts as a middle man when a buyer wants to make the payment to the seller. Payment gateways provide a secure medium/channel for making the transaction. These gateways transmit the transaction details such as the banking credentials, whether there is sufficient balance for the transaction to proceed etc. Just like in the physical world, where we use Point of sale machines to make the payment to the seller, we use payment gateways to make the online transactions and complete the payment. Some of the payment gateways are Bill Desk, CC Avenue, and Citrus etc

Modus operandi:

Fraudster creates a fake payment gateway web page which looks and behaves similar to the genuine payment gateway website and sends it to the victim. The victim thinking the fake website sent by the fraudster as genuine enters his credentials. The fraudster receives those credentials and performs the fraudulent transactions.

Investigation:

- These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
- Identify the phishing page and then find the details of the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact etc. Collect the details of the owners of the domain name as well following procedures mentioned in the 'internet investigation' unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.
- Suppose the fraudster has used the credentials to make any transaction on the payment gateway, IO can get the transaction id from the victim, which can be obtained from the bank statement. Then the IO can request the details such as for what purchase did the fraudster made the transaction from the E-commerce website and request the details such as IP address, bank account etc of the fraudster from the payment gateway.

2.11 Digital Wallets related frauds

Figure : Digital Wallets

As the online mode of payments has increased to make cashless transactions, multiple ways to make the payments has also increased. One such mode of payment is digital wallets/Virtual wallets/mobile wallets. Similar to the physical wallets we use in our daily life, digital wallets act as a container where we can store your digital information about various credit/debit card, load money from your bank account to the digital wallets and get coupons etc. Using these digital wallets, one can pay the bills, book tickets on various platforms, transfer fund from one account to other etc., providing convenience to the user by not allowing him/her to stand in long queues to pay the bills. Digital wallets allow user to pay these bills from anywhere in the world connected to the internet There are many applications like PayTM, Freecharge wallet, SBI buddy, ICICI pockets, Mobikwik, PayUMoney etc which provide the digital wallets service.

Modus operandi:

In these kinds of frauds, the fraudster creates fake mobile wallet apps and uploads it to the internet for people to download. People over the internet thinking the fake mobile wallet app as genuine app download and try to use it for transactions giving away their credential. The fraudster receives those credentials and performs the fraudulent transactions.

Investigation:

- These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
- On receiving the complaint, we would identify the fake app that is being hosted and then find the details of the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact etc. Collect the details of the owners of the domain name as well following procedures mentioned in the 'internet investigation' unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.

2.12 QR Code Scan fraud

- Fraudster sends QR code to victim and asks them to scan it to receive money.
- QR codes are meant to send money. Victim scans the QR, enters PIN and money is debited

Figure : QR code fraud

2.13 CASE STUDIES

❖ **Case Study 1 Cosmos Bank Cyber Attack**

In August 2018, the personal data of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities. Hackers managed to siphon off over INR 94 crore through a malware attack on the server of Pune-based Cosmos Bank and cloning thousands of the bank's debit cards over a period of two days.

The fraudulent transactions were carried out on August 11 and August 13 and the malware attack by the hackers originated in Canada. While cloning the cards and using a "parallel" or proxy switch system, the hackers self-approved the transactions and withdrew over INR 80.5 crore in about 15,000 transactions. The malware attack was on the switch, which is operative for payment gateways of Visa and Rupay debit cards.

Investigation: These crimes are considered as identity theft, the penal provisions for this crime are covered under Section 43, 65, 66(C) and 66(D) of the Information Technology Act 2000.

❖ **Case Study 2 Cyber-Heist: The $951m Raid on Bangladesh's Central Bank**

In early 2016, a criminal gang penetrated the security systems of Bangladesh Bank with malware that cloned legitimate transactions. On February 4, the malware sent 35 withdrawal requests through the international SWIFT system to the New York Federal Reserve, where the Bangladeshi central bank had money on deposit.

The fraudsters attempted to steal a total of $951m. Thirty of the orders, worth

$850m, were blocked by the New York Fed, but the gang succeeded in having

$101m transferred to banks in Sri Lanka and the Philippines before their activities were noticed, thanks to a spelling mistake in one of the transfer requests. Subsequently, $20m was recovered from a Sri Lankan bank, but officials were too late to stop the remaining $81m from disappearing.

The gang involved is thought to have consisted of between 20 and 40 members with a range of skills and including financial and banking experts, hackers and software engineers. Had it not been for one slip-up, their audacious attempt to steal almost $1bn might have succeeded – a prospect that has caused huge concern among banks and their institutional customers, which keep large sums on deposit to pay staff and suppliers.

❖ **Case Study 3 Union Bank of India Heist**

In July 2016, the malware in the attachment stole Union Bank's Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes and initiated a transfer of the money to an account in Citigroup in New York. SWIFT is a global network which links financial institutions to send and receive transactions. The report added that Union Bank traced the money and blocked the transaction. Using a phishing email, hackers accessed the credentials to execute a fund transfer, swindling USD171 million.

❖ **Case Study 4 Tesco Bank Suffers UK's First Mass Account Theft**

In November 2016, the bank owned by UK supermarket group Tesco suffered a huge online security breach in which a total of £2.5m was removed from 20,000 of its 136,000 current accounts and suspicious activity was discovered on a further 20,000.

The robbery happened over a weekend, while bank staff were absent, and there has been no official explanation of exactly how the thefts were executed. However, experts suggested that hackers had identified a weakness in the Tesco Bank website and exploited it to steal thousands of customers'

account details that were then used to make online purchases. On discovering the fraud, Tesco temporarily blocked online payments by its current account customers while continuing to allow them to use cards for cash withdrawals, chip and pin, and bill payments.

❖ **Case Study 5 Android Malware Installs Fake Apps On Smartphones**

In June 2017, security organization FireEye reported that they had identified malware that installs fake versions of eight popular apps including Facebook, WhatsApp, Uber, Google Play and Viber on victims' smartphones.

They are sent a text message saying: "We have not been able to deliver your order. Please check your shipping information here", followed by a link. Once the victim clicks the link, it installs the malware, which waits for the user to open one of the targeted apps.

The malware then overlays a fake interface on top of the legitimate app and attempts to trick victims into divulging their online banking information. The phishing texts were first seen in Denmark, where 130,000 victims were tricked into clicking the link. The malware is thought to have spread to the UK, Germany, Luxembourg, Spain, Sweden, Norway, the Netherlands, Italy, Greece, and Turkey.

❖ **Case Study 6 Wannacry Ransomware Campaign**

The ransomware attack in India with several thousand computers getting locked down by ransom-seeking hackers. The ransomware, known as WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRYt. A total of 16 U.K. organizations have been affected by the ongoing attack, including the National Health Service (NHS), which was forced to reject patients, cancel operations, and reschedule appointments due to WannaCry. Also, systems in Russia, Ukraine, India, and Taiwan. Infections are also spreading through the United States. The malware is notable for its multi-lingual ransom demands, which support more than two-dozen languages. Ransom between $300 to $600 is being demanded. There is code to 'rm' (delete) files in the virus, it seems to reset if the virus crashes.

❖ **Case study 7 stolen dongle used in an attempt to crack 'strong authentication'**

In one recent Swiss case involving a corporate client of a bank, 10 employees had the authority to issue payments in the name of the corporation but only three normally did so. One of the remaining seven staff had his dongle stolen but since he was not among the group that normally issued payments, he did not immediately notice the theft.

The thief waited eight months before attempting to initiate a transaction using the stolen dongle, but his attempt raised a flag and was blocked. However, the case highlights the need to check whether the person attempting to issue payment is one of the normal users of the system or part of a wider group that has the authority to do so.

3. Virtual currencies and Crypto currencies

There are various innovative money payment systems in the market today, many of which are built on platforms like the mobile phone, the Internet, and the digital storage card. These alternative payment systems have seen encouraging or even continued growth, from the likes of PayPal, Google Pay(Tez), Paytm, Phonepay, Airtel Money, Vodafone M-Pesa, and others.

Beyond payment systems that are based on fiat currency, the growing use of digital currency allows for faster, more flexible, and more innovative payments and ways in financing goods and services. In this chapter we will look at different types of currencies with their examples.

3.1 Virtual currencies

Virtual currency is a type of digital currency which is only available in electronic form and it is not physically present. It require specified software, mobile application or a digital wallet. Virtual currency is considered to be a subset of the digital currency group, which also includes crypto currencies.

Examples are frequent flyer programs by various airlines, Payback points, SBI Rewardz, Microsoft Points, Nintendo Points, Facebook Credits and Amazon Coin.

To prevent fraud and manipulation, every user of a crypto currency can simultaneously record and verify their own transactions and the transactions of everyone else. The digital transaction recordings are known as a “ledger” and this ledger is publicly available to anyone. With this public ledger, transactions become efficient, permanent, secure and transparent.

3.2 Crypto currencies

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Crypto currencies use decentralized control as opposed to centralized digital currency and central banking systems.

To prevent fraud and manipulation, every user of a crypto currency can simultaneously record and verify their own transactions and the transactions of everyone else. The digital transaction recordings are known as a “ledger” and this ledger is publicly available to anyone. With this public ledger, transactions become efficient, permanent, secure and transparent.

With public records, crypto currencies don’t require to trust a bank to hold money. They don’t require you to trust the person you are doing business with to actually pay you. Instead, you can actually see the money being sent, received, verified, and recorded by thousands of people. This system requires no trust. This unique positive quality is known as “trustless”.

The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain that serves as a public financial transaction database.

Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency. Other examples of crypto currencies are Ethereum, Ripple, Litecoin, and NEO.

3.3 Blockchain

Blockchain is technology for creating permanent, secure digital recordings that don't rely on any single person or group. Blockchains can record any information, though the first example was created to record bitcoin transactions.

Imagine the blockchain as a book of records. Each page in that book, is a block, and can record anything. Blocks are created one after the other, chained to each other creating what we know as the blockchain.

Multiple blockchain records are maintained simultaneously by many unrelated individuals and their computers, making it cloud storage on steroids. Updates are seen immediately and manipulation is extremely difficult/impossible. This positive quality known of many people keeping their own copies of the blockchain is known as "distributed".

There are hundreds of blockchains created by many groups to records all sorts of information including art, medical records, computer information and much more.

But if a blockchain is not distributed among many individuals and instead run by one government, organization, group or person, then it is not at a blockchain at all. A centralized system like that is simply a database.

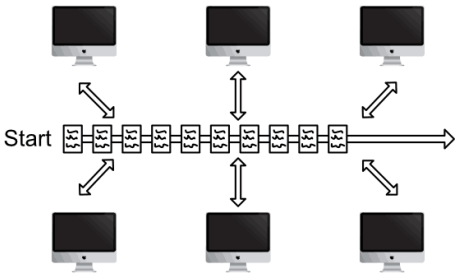


Figure : Blockchain Decentralized architecture

3.4 Types of Virtual Currencies

a) Bitcoin

Bitcoin introduced a decentralized currency system based on a peer- to-peer network where currency is not issued per se; instead it is mined with advanced computers by cracking difficult math-based equations. Bitcoin can be called the trendsetter, as its success has spurred the launch of many other virtual currencies (there are more than 150 cryptocurrencies). The currencies inspired by Bitcoin are collectively called altcoins and have tried to present themselves as improvised and modified versions of Bitcoin.

The challenges in using virtual currency is that these systems are capable of facilitating tax evasion or illegal activities because of the anonymity factor which is built into the system. As a result, Bitcoin is a preferred mode by hackers for ransomware.

These currencies are easier to mine, but involve greater risk in terms of lesser liquidity, acceptance and value retention. Here are five digital currencies picked from the lot

b) Litecoin

Litecoin, the second largest cryptocurrency in the world was launched in the year 2011. It was created by Charlie Lee, a MIT graduate and former Google engineer and can be described as the second-in command to Bitcoin. Litecoin is based on an open source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer grade. Litecoinhas a faster block generation rate and well as more rewards per block as compared to Bitcoins.

c) Darkcoin

Darkcoin is a more secretive version of Bitcoin. Though Bitcoins are anonymous when compared to traditional money, there is still a record of all transactions ever carried out in a ledger “blockchain” which can reveal a lot of information. Darkcoin offers more anonymity as it works on a decentralized mastercode network that makes transactions almost untraceable. Launched in January 2014, Darkcoin has an increasing fan following in a short span of time. This cryptocurrency was created and developed by Evan Duffield and can be mined using a CPU or GPU.

d) Peercoin

Peercoin, also referred to as PPCoin, Peer-to-Peer Coin and P2P Coin, was created by software developers Sunny King (a pseudonym) and Scott Nadal. It was launched in August 2012 and was the first digital currency to use a combination of proof-of-stake and proof-of-work. The coins are initially mined through the commonly-used proof-of-work hashing process but as the hashing difficulty increases over time, users are rewarded with coins by the proof-of-stake algorithm, which requires minimal energy for generating blocks. This means that over time, the network of Peercoin will consume less energy. Peercoin is an inflationary currency since there is no fixed upper limit on the number of coins.

e) Dogecoin

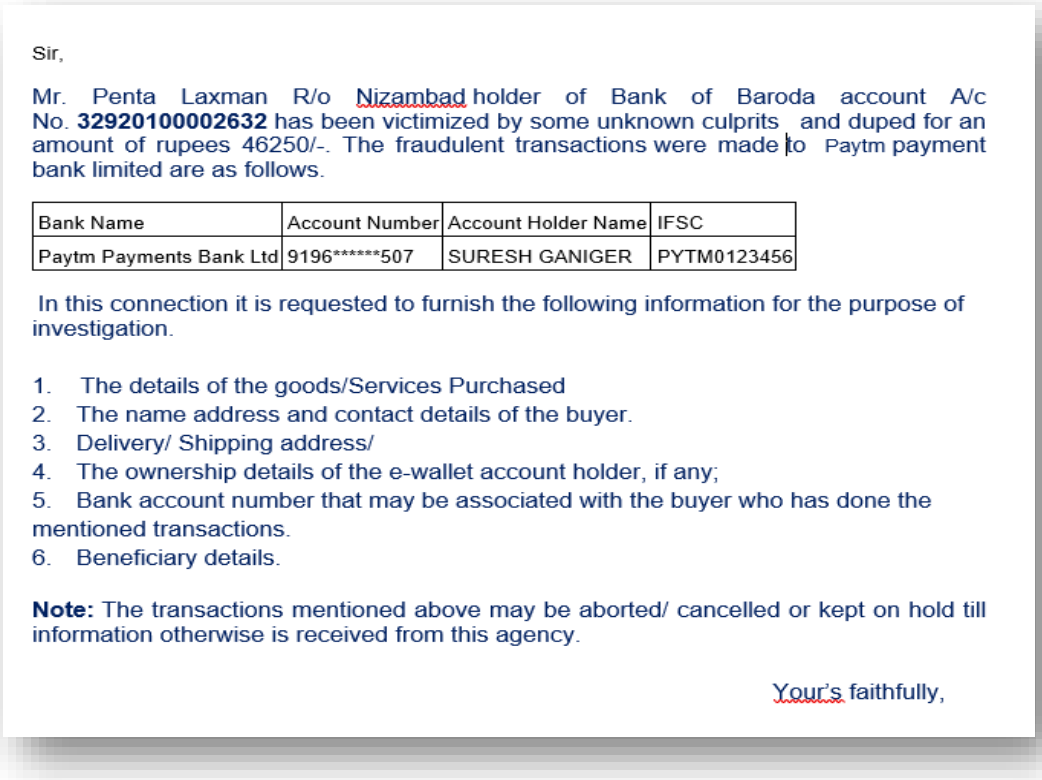
Dogecoin is another currency from the family of cryptocurrencies that recently turned a year old (launched in December 2013). Dogecoin, which has a ShibuInus (a bread of a Japanese dog) as its logo, was created by Billy Markus and Jackson Palmer. Dogecoin presents itself broadly based on the Bitcoin protocol, but with modifications. It uses scrypt technology as a proof-of-work scheme. It has a block time of 60 seconds (1 minute) and the difficulty retarget time is four hours. There is no limit to how many Dogecoin can be produced i.e. the supply of coins would remain uncapped. Dogecoin deals with large numbers of coin that are lesser in value individually, making the currency more accessible with a low entry barrier and fit for carrying out smaller transactions.

f) Primecoin

Primecoin is an altcoin with a difference. Developed by Sunny King (who also developed Peercoin), its proof-of-work is based on prime numbers, which is different from the usual system of hashcash used by most cryptocurrencies based on the Bitcoin framework. It involves finding special long chains of prime numbers (known as Cunningham chains and bi-twin chains) and offers greater security and mining ease to the network. These chains of prime numbers are believed to be of great interest in mathematical research.

4. Notice Formats

4.1 Notice to Paytm



Sir,

Mr. Penta Laxman R/o Nizambad holder of Bank of Baroda account A/c No. **32920100002632** has been victimized by some unknown culprits and duped for an amount of rupees 46250/-. The fraudulent transactions were made to Paytm payment bank limited are as follows.

Bank Name	Account Number	Account Holder Name	IFSC
Paytm Payments Bank Ltd	9196******507	SURESH GANIGER	PYTM0123456

In this connection it is requested to furnish the following information for the purpose of investigation.

1. The details of the goods/Services Purchased
2. The name address and contact details of the buyer.
3. Delivery/ Shipping address/
4. The ownership details of the e-wallet account holder, if any;
5. Bank account number that may be associated with the buyer who has done the mentioned transactions.
6. Beneficiary details.

Note: The transactions mentioned above may be aborted/ cancelled or kept on hold till information otherwise is received from this agency.

Your's faithfully,

4.2 Notice to bank

LOGO

Cr.No.391/2018-CCPS
Jedcherla **Date: 12-08-2021**

Notice U/Section 91 Criminal Procedure Code

The above cited case is being investigated by this agency where in the online fraudsters offered fake jobs On false pretexts like consultation, processing charges accused duped Rs.1,60,000/- to the victim. In this regard victim approached to local Police station basing on the complaint case registered in Cr.No.391/2018 U/s 420,406,419 IPC and 66- IT Act 2008. During the course of investigation it came to light that the following indusind bankaccount number belongs to fraudster A/c No.**157*****78949**.

Therefore it is requested to furnish the following information for the purpose of investigation.

1. Customer application forms including ID / Address proofs submitted.
2. Account transactions statement from starting to till date
3. Accessing IP Log details of the online transactions if any.
4. Footage of recent ATM withdrawals.
5. Linked-up mobile number.

Early action would be highly appreciated

Inspector of Police,
Cyber Crime PS,
place.

To

Senior Vice President,
Banking Operations IndusInd Bank Ltd.
701/801 Solitaire Corporate Park, 167

5. RBI Guidelines

5.1 Limited Liability of customer in unauthorized transaction

According to RBI circular no DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 available from

https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15D620D2C4D2CA4A33AABC928CA6204B19.PDF

In any unauthorized transaction liability of customer will be calculate according to the above guidelines. The guideline includes online/ Remote payment e.g. Internet Banking, Mobile Banking, Card Not Present and Prepaid payment instruments. These guidelines also made mandatory to send SMS/ Email alert in any type of transaction; SMS/Email alerts shall be mandatory to be sent to customers. The customer must notify the bank as soon as possible in case of any unauthorized transactions. Summary of the circular is as mentioned

Liability of the customer:

Sr. No	Zero Liability of customer	Limited liability if customer
1.	Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).	In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.
2	Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within **three working days** of receiving the communication from the bank regarding the unauthorised transaction.	In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of **four to seven working days** after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in picture below, whichever is lower

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer's liability (₹)
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
Beyond 7 working days	As per bank's Board approved policy

Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

Please go through to the detail circular for more detail:

https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15D620D2C4D2CA4A33AABC928CA6204B19.PDF

5.2 Limiting Liability of Customers in Unauthorized Electronic Payment Transactions in Prepaid Payment Instruments (PPIs) issued by Authorized Non-banks

Customer liability in case of unauthorized electronic payment transactions through a PPI		
S. No.	Particulars	Maximum Liability of Customer
(a)	Contributory fraud / negligence / deficiency on the part of the PPI issuer, including PPI-MTS issuer (irrespective of whether or not the transaction is reported by the customer)	Zero
(b)	Third party breach where the deficiency lies neither with the PPI issuer nor with the customer but lies elsewhere in the system, and the customer notifies the PPI issuer regarding the unauthorized payment transaction. The per transaction customer liability in such cases will depend on the number of days lapsed between the receipt of transaction communication by the customer from the PPI issuer and the reporting of unauthorized transaction by the customer to the PPI issuer -	
	i. Within three days#	Zero
	ii. Within four to seven days#	Transaction value or ₹10,000/- per transaction, whichever is
	iii. Beyond seven days#	As per the Board approved policy of the PPI issuer

(c)	In cases where the loss is due to negligence by a customer, such as where he / she has shared the payment credentials, the customer will bear the entire loss until he / she reports the unauthorized transaction to the PPI issuer. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the
(d)	PPI issuers may also, at their discretion, decide to waive off any customer liability in case of unauthorized electronic payment transactions even in cases of customer Negligence.

The provision of these direction will be applicable to all authorized non-Bank PPI issuers. This notification DPSS.CO.PD.No.1417/02.14.006/2018-19, dated January 04, 2019, covers all PPI's. All remote/ online transactions done via PPI's platform, limited customer liability is mentioned below.

For detailed guidelines please go through to the RBI guideline available from *https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT101746BAE75BB964EB1AD2E5BB6DC3FE5DC.PDF*.

6. Various Organizations

6.1 CERT-IN

CERT-IN (Computer Emergency Response Team – India, government-mandated information technology (IT) security organization) has been taking important initiatives in strengthening cyber-security by providing proactive & reactive services as well as guidelines, threat intelligence and assessment of preparedness of various agencies across the sectors, including the financial sector.

The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country. CERT-In was created by the Indian Department of Information Technology in 2004 and operates under the auspices of that department. According to the provisions of the Information Technology Amendment Act 2008, CERT-In is responsible for overseeing administration of the Act.

6.2 CERT-Fin

Government of India announced its intention to set up a Computer Emergency Response Team for the Financial Sector (CERT-Fin). Ministry of Finance set up a working group to work closely with all financial-sector regulators and stakeholders on issues of cyber security. The working group report was put in public domain by MoF, soliciting public comments.

It is recommended in the Working Group report that CERT-Fin, will collect, analyze and disseminate information on cyber incidents in the financial sectors. It will forecast and send alerts on cyber security incidents. It will also take emergency measures on cyber security incidents. It will coordinate responses and activities for cyber incidents and issue guidelines, advisories, and white papers relating to vulnerabilities and information security.

CERT-Fin will monitor efforts in the financial sector towards maintaining modern cyber security architecture, developing awareness among regulated entities and the public in general. It will also create awareness on security issues through dissemination of information on its website and operate a 24x7 incident response help desk. It will also provide incident prevention and response services as well as quality management services and will carry out functions similar to CERT-In, which operates at the national level, for priority cyber security in financial sector. CERT-Fin will offer policy suggestions for strengthening financial sector cyber security to all the stakeholders, including regulators and the government.

It is expected that CERT-Fin will make a significant contribution towards improving the cyber resilience of the Indian Financial Sector.

6.3 ReBIT

Reserve Bank Information Technology Pvt Ltd (ReBIT) has been set up by the Reserve Bank of India (RBI), to take care of the IT requirements, including the cyber security needs of the Reserve Bank and its regulated entities. ReBIT will focus on IT and cyber security (including related research) of the financial sector and assist in IT systems audit and assessment of the RBI regulated entities; advise, implement and manage internal or system-wide IT projects (both the existing & the new) of the Reserve Bank as mutually decided between the Reserve Bank and ReBIT.

ReBIT will act as a catalyst for innovation, big systems and new ideas apart from having the capability to guide the regulated entities in the IT areas of their operations as also for the RBI's IT related functions and initiatives. Given the need for inter-operability and cross- institutional cooperation, ReBIT will effectively participate in setting up of standards to strengthen Reserve Bank's role as regulator.

6.4 NCPI

The National Payments Corporation of India (NCPI) functions under the Reserve Bank of India (RBI) and the Indian Banks' Association (IBA). NPCI was founded in 2008 as a not-for-profit organization. It aims to create nationwide standards for business and retail payments across India, which is why its services are all geared towards achieving this goal.

What are the services that NPCI provides?

Through various FinTech innovations, the NPCI has contributed to India's current payment ecosystem in a big way. The following are some of its prominent services:

- **UPI**

United Payments Interface)UPI) is a real-time payment solution that links bank accounts with UPI platforms on mobile phones. It eliminates the need for a third- party wallet and enables the direct transfer of money from one bank account to another. Currently, UPI services are integrated with over 120 banks. Consumers can also use UPI for P2P transfers to family and friends.

- **Bharat Interface for Money (BHIM)**

BHIM is an app that runs on UPI. It allows users to easily make payments by using just a registered mobile number or a virtual payment address (VPA). Though BHIM is not as widely used as some of its competitors like Google Pay, it offers avast scope for financial inclusivity for citizen across India. This is because BHIM can be operated offline and does not require a smartphone. BHIM leverages NPCI's *99# facilities–more on that below.

- ***99# or USSD services**

NPCI's *99# services run on USSD, which stands for Unstructured Supplementary Service Data. These services aim to bring traditional and newer banking solutions to citizens of India who may not have smartphones, internet or even traditional bank accounts. It aims to leverage as much of mobile banking as possible and works on low-value remittances so that more citizens can become integrated and familiar with banking services.

- **RuPay**

Now a part of the government's Jan Dhan Yojna, RuPay is another big initiative of the NPCI that has influenced the way the average citizen makes financial decisions. RuPay is essentially a more affordable version of international debit and credit cards. These cards are issued as prepaid cards, debits cards and credit cards, as per the customer's requirements. As of now, over 300 million RuPay cards are in circulation across India. More and more consumers are using RuPay for PoS and E- commerce transactions too.

- **IMPS**

IMPS stands for Immediate Payment Service. This system works around the clock and offers the ability to transfer funds instantly. It is because of IMPS that current innovations like UPI are possible. Unlike NEFT and RTGS, IMPS does not rely on traditional banking hours nor does it adhere to public holidays. With payments occurring through smartphones, all consumers need is the beneficiary's mobile number to initiate the process. Of course, other payment details such as bank account number and IFSC codes can also be used to conduct an IMPS transaction.

- **BBPI**

BBPI stands for Bharat Bill Payment Interface. Recognizing how vital bill payments are to the retail payments industry, NPCI developed BBPI to facilitate the same. According to data released by the RBI, Rs. 6,223 billion is generated by India's top 20 cities for bill payments alone. Over 70% of these bill transactions occurred through cash. BBPI is all set to function as the single platform that consolidates payments for bill payers and aggregators. So far, the NPCI has launched the pilot project for this platform. Only time will tell how widely it is accepted by vendors and consumers alike.

6.5 IDBRT

Institute for Development & Research in Banking Technology (IDRBT) is a banking research institute established in 1996 by Reserve Bank of India (RBI). It is located in Hyderabad, India. RBI established IDRBT with the aim of providing the operational service support in information technology to banks and financial institutions. The first phase of reforms in the Indian financial sector precipitated the need for an apex-level institute for implementing banking technology and technology absorption in the Indian banking and financial sector. IDRBT is also an academic institution that offers a range of academic and research programmes, designed specifically to meet both the existing and emerging requirements of the Banking and Financial Sector in India.

IDRBT also offers consultancy in banking technology and related areas to banks and financial institutions. Consultancy is taken up not only for solutions offered by the Institute but also in the various routine facets of I.T. in banking. Some of the areas of consultancy are security technologies, IT strategy, technology planning and upgrades, networking, electronic payment systems, information systems audit, IT infrastructure audit, information security policy, data warehousing, data mining, risk management, customer relationship management and beyond-core banking.

Appendix

1. Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions
2. Master Direction - Information Technology Framework for the NBFC Sector

Picture Resources

Figure	Resource
Payment via NFC	Adobe Stock
UPI Architecture	NPCI
Working of Mobile Wallets	Securing India's Digital Payment Frontiers by DSCI
Stealing Card information	Adobe Stock
Working of Card Skimming	https://www.kaskus.co.id/thread/55dc1341947868e93c8b4568/mengenal-modus-kejahatan-skimming-teknik-penipuan-kartu-atm/?med=go_mlt&ref=postlist-21
Shimming module	Pintereset.com
Hardware Keylogger	https://www.lawweb.in/2014/02/hardware-keylogger-in-cyber-cafe.html

3. OSINT and Social Media Analysis

1. OSINT

1.1 Introduction to OSINT

Open Source Intelligence can be defined as the retrieval, extraction and analysis of information from publicly available sources. Each of these three processes is the subject of ongoing research resulting in specialized techniques. Today the largest source of open source information is the Internet.

Most newspapers and news agencies have web sites with live updates on unfolding events, opinions and perspectives on world events are published. Most governments monitor news reports to feel the pulse of public opinion, and for early warning and current awareness of emerging crises. The phenomenal growth in knowledge, data and opinions published on the Internet requires advanced software tools which allow analysts to cope with the overflow of information. Malicious use of the Internet has also grown rapidly particularly on-line fraud, illegal content, virtual stalking, and various scams. These are all creating major challenges to security and law enforcement agencies. The alarming increase in the use of the Internet by extremist and terrorist groups has emerged. The number of terrorist linked websites has grown from about 15 in 1998 to some 4500 today.

These sites use slick multimedia to distil propaganda whose main purpose is to 1) enthuse and stir up rebellion in embedded communities 2) instill fear in the "enemy" and fight psychological warfare. Anonymous communication between terrorist cells via bulletin boards, chat rooms and email are also prevalent.

Open-Source Intelligence (OSINT) refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).

a) Scope of Open Source Intelligence

- In today's world, internet has become a core part of a human life, where one can share information, opinions and ideas as well as post photos, videos on various social media platforms.
- As lot of information is being uploaded onto the internet every day, it becomes essential for a Law Enforcement officer to collect every possible information that available on the internet.
- Information on the internet can be collected from various sources like social media sites, Online news websites, search engines, various government etc.
- Generally, information about an individual or an organization is provided in two ways.
  - One, where an individual given by himself and
  - Second, information is given out by third party such as company for which the individual is working for or from the government website.

b) Need of Open Source Intelligence for Law Enforcement Agencies

- Once a case related to cybercrime gets registered, the investigation officer needs to collect a lot of information from various sources in order to identify the suspect computer

that is involved in the commission of crime and the criminals who are behind commission of the crime.

- Therefore, intelligence gathering is one of the major tasks in the course of investigation. The investigating officer will be having very few inputs, using that he has to collect maximum amount of details about the criminals or suspects. Here comes the use of various information gathering techniques.

1.2 Preparations to be done before performing OSINT

As all the activities performed over the internet can have traces, criminal can get trace of Law Enforcement Officer. It is required that the officer needs to take some precautionary steps in order to reduce the traces and makes the process more secure.

Necessary precautions must be taken for two main reasons. First is to maintain anonymity over the internet and the second is to protect the systems used for gather information.

While performing the OSINT, systems having the government ip address should not be used. It suggested to use certain services like proxies and VPN's which provide anonymity over the internet.

The collected data should be organized in a systematic manner. The data can be arranged based on the type of data, Subject (Organization) or based on the region as this will help the next officer who gets access to the data when transfer takes place.

➢ Undercover Accounts

Whenever we are performing the OSINT, we must make sure that we do not use our original social media accounts, email-ids, and mobile numbers in order to access the information. It is advisable to create some undercover accounts on various sites such as Facebook, Gmail, Twitter and other things. This ensures that the identity of the officer is protected over internet.

➢ Using Anti-viruses

- One must ensure using anti-virus software when performing the Open Source Intelligence because during the process, we may download some files from unauthorized websites which may pose a potential threat to our systems.
- Few of the anti-virus software's are:
    - Mcafee
    - Kaspersky
    - Avast
    - 360 total etc.

➢ Adblocker

- Most websites today are enabled with service to display ads on their page. When we access those websites, it creates an uncertainty about the content displayed on the page. To hide these ads from getting displayed, we can use a service known as ad blockers, which we can install in our browsers as a plugin.

- Few popular ad-blockers are:
  - Ublock origin
  - AdBlock plus

➢ No Script

- "No script" is another add-on or extension that we can add to our browsers which blocks any malicious scripts from running when we visit various websites.

➢ Virtual Machines

- A Virtual Machine is a software that allows us to run other operating systems within your current computer system.
- In virtual machines, the operating system actually running on your computer is called the host and any operating systems running inside VMs are called guests
- OSINT Operation more effective way by using virtual machines, because when you use your normal desktop and if you are accessing any website of any person, he may get notified or get alert saying that someone is trying to get data of this.
- So, if we use virtual machines, it may not get such kind of suspicious things. Virtual machines are basically a computer inside another computer.
- Some of the virtual machine software's are:
  - Virtual Box
  - VM Ware
  - Hypervisor

1.3 OSINT on E-mail Address

We can use the e-mail address to search for a person over the internet.

➢ People Search using pipl.com

Pipl.com is an online search engine, which can be used to find the information about an individual by using the email address, social media username or phone number.

- Go to the website "**pipl.com**" and enter the email id and click search.

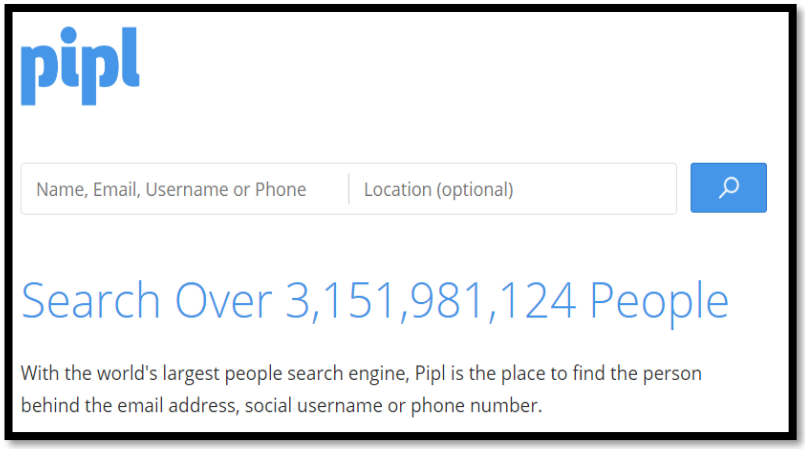


Figure: Pipl tool

- The output when we search for email id on pipl.com is shown below.

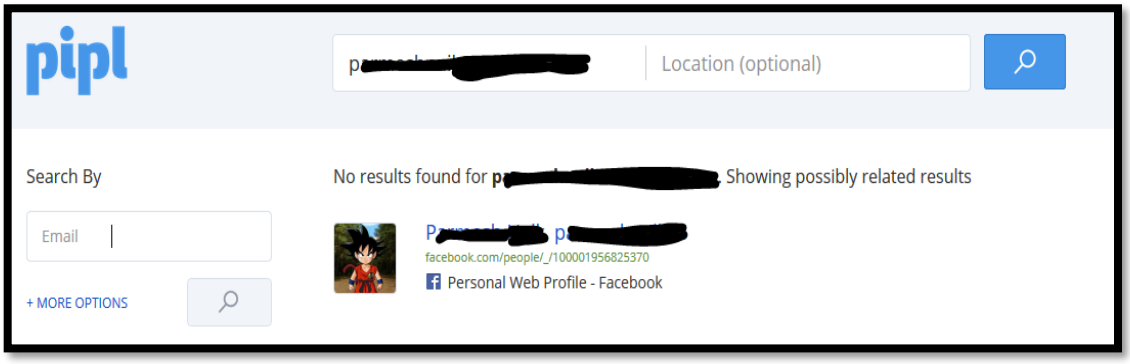


Figure: Pipl tool search

➢ Facebook password reset

Facebook provides option for resetting the password using the E-mail/Phone number/username/ full name. If we know the phone number, we can go to the password reset page of Facebook and enter the phone number in the given field. If any Facebook account is linked with this number, that account would be shown. This way we will get the full name and photos of owner of that number.

- Go to "**Facebook.com**" and click the "**Forgot your account**".

Enter the mobile number of the person and then select search.

Figure : Facebook forgot Password

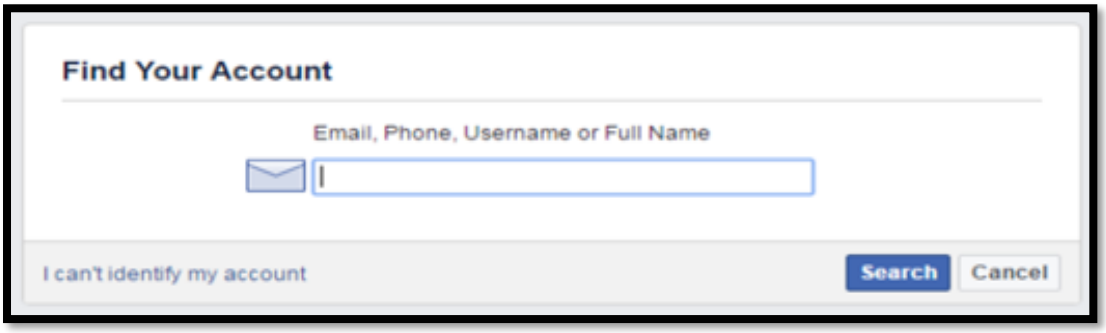


Figure: Facebook forgot password 2

- Once we click the search button, Facebook will display the Facebook profile belonging to that mobile number.

Figure: facebook reset password

➢ **Gmail Compose message**

- Another way of identifying the user of an unknown email-id is to compose a mail and enter the email-id in the "To" field and then hover over the email-id. This will display the picture of the user as shown below

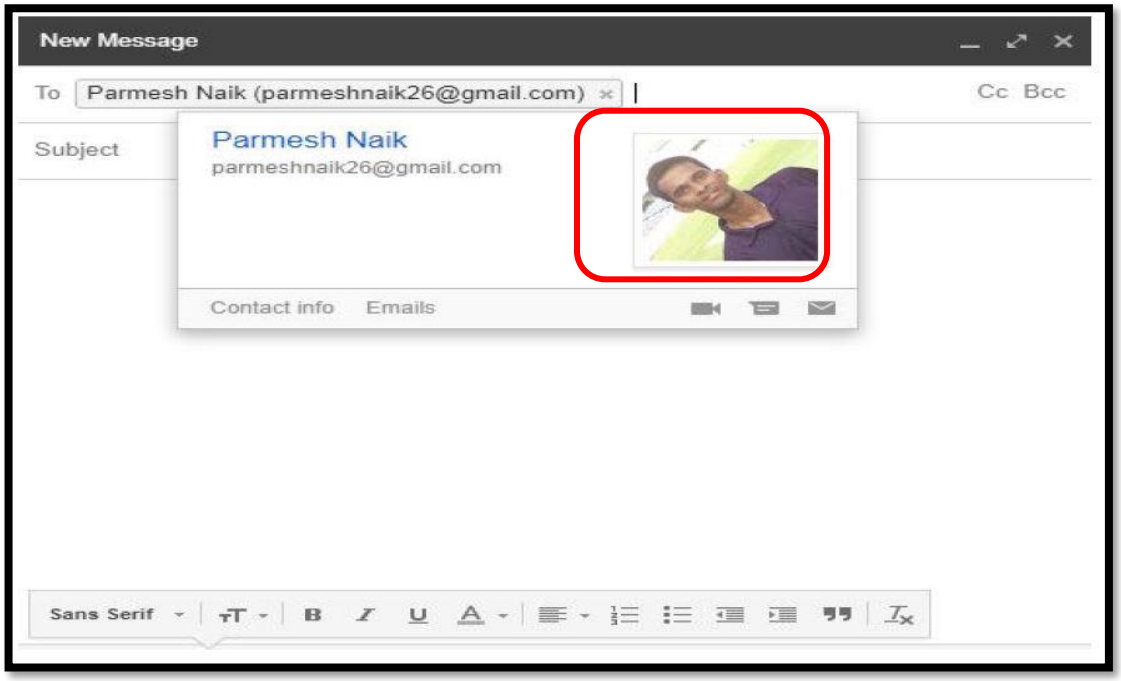


Figure: Gmail mail compose

1.4 OSINT on Name

There are websites that specialize in people search which can be done providing a real name, username, email or phone number.

- https://www.spokeo.com
- https://thatsthem.com
- https://www.beenverified.com
- https://www.fastpeoplesearch.com
- https://www.truepeoplesearch.com
- https://www.familytreenow.com
- https://people.yandex.ru

People search websites allow to opt out, but after people remove themselves from listings, new search services appear with their records in them. The reason for that is the same dataset is bought and used by different services. Some companies own those datasets and even if on one of their websites a person removes the listing, on the new domain the old data is repopulated again so the previously removed profile reappears in the search. Consequently, if people did a pretty good at cleaning their stuff up you just have to wait for a new database to appear. One of the methods to find people that opted out is to go the people search service, find a unique paragraph, do a quoted Google search on it and find all of the domains that the company owns. There are chances that information your target removed from site A is now on-site B.

2. OSINT over search engines

2.1 Understanding how Search engines works

Search engines allow users to search the internet for content using keywords. Although the market is dominated by a few, there are many search engines that people can use. When a user enters a query into a search engine, a search engine results page (SERP) is returned, ranking the found pages in order of their relevance. How this ranking is done differs across search engines.
Search engines often change their algorithms (the programs that rank the results) to improve user experience. They aim to understand how users search and give them the best answer to their query. This means giving priority to the highest quality and most relevant pages.

2.2 Various kinds of search engines available on internet

- **Google**

Google is the most popular search engine on the planet. Their search engine routinely owns above 90% of the market, resulting in approximately 3.5 billion of individual searches on their platform every day. While notoriously tight-lipped about how their algorithm works, Google does provide some high-level context about how they prioritize websites in the results page.
New websites are created every day. Google can find these pages by following links from existing content they've crawled previously, or when a website owner submits their sitemap directly. Any updates to existing content can also be submitted to Google by asking them to recrawl a specific URL. This is done through Google's Search Console.

Figure : Google search

- **Bing**

Bing is an internet web search engine developed, owned and operated by Microsoft. Bing was launched in 2009 as a rebranded version of Microsoft's earlier search engines, MSN Search, Windows Live Search and Live Search.

Figure : Bing search

- **Duck Duck GO**

DuckDuckGo is a bit of a maverick in the search engine market but is gaining headway as the go-to search engine for anyone concerned about their data privacy. While they have a proprietary web, crawler called DuckDuckBot to scour web-page content, much of the information DuckDuckGo shows on their results page is compiled from 400+ additional third-party sources, including Bing, Yahoo, and Wikipedia.

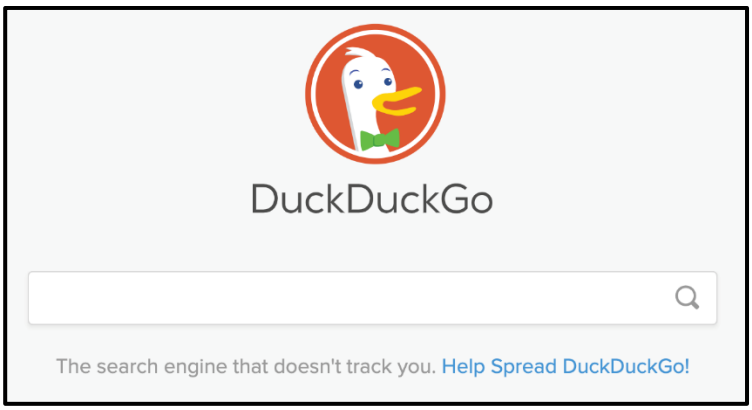


Figure : Duck Duck go search

Unlike Google and Bing, DuckDuckGo does not capture personal information on their users, including past search history and IP address. This dedication to privacy in some ways makes their algorithm work harder to provide personalized results.

- **Yandex**

Yandex is a Russian company that is best known for its Yandex search engine. This is a search engine that was originally started in Russian at yandex.ru, but now has a global English version at yandex.com.

Yandex functions mostly like the other popular search engines. You type in a search phrase, hit enter and then you see a search results page with a bunch of blue links, URLs, and descriptions. Depending on the search query, you may also see images, videos, and other types of search results.

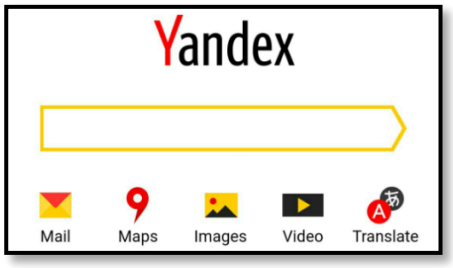


Figure : Yandex search

2.3 Using operators on Google Search

It provides various advanced search options using which, one can do effective search and filter out unwanted results. It also has mechanism by which one can design custom search queries in google to get desired search results.

A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website. Google dorking, also known as Google hacking, can return information that is difficult to

locate through simple search queries. That description includes information that is not intended for public viewing but that has not been adequately protected.

Google Operators:

a) Explicit Search:

For instance, if we want to search exact name of a person or a string, we need to write it in " ". If you want to filter out unwanted results of narrow down the search, we can add the occupation, city or college of target.

Let's say you're searching on Google for content about Sachin Tendulkar. Instead of just typing Sachin Tendulkar into the Google search box, you will likely be better off searching explicitly for the phrase. To do this, simply enclose the search phrase within double quotes.

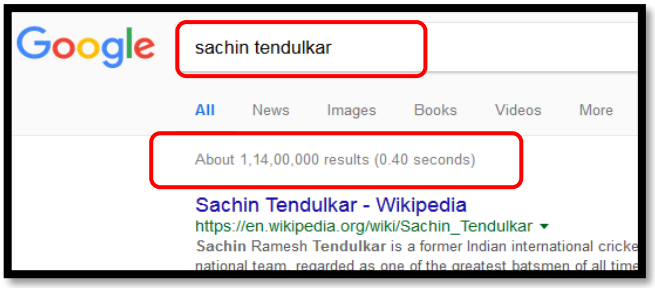


Figure : Google Explicit Search

- When we search for the name without quotes, Google is search for the word **Sachin** separately and **Tendulkar** separately. That is the reason it is giving more results in the above scenario.
- But when we search for same name by adding quotes around it, the results decrease in number because it searches for the exact phrase which is present in the quotations.

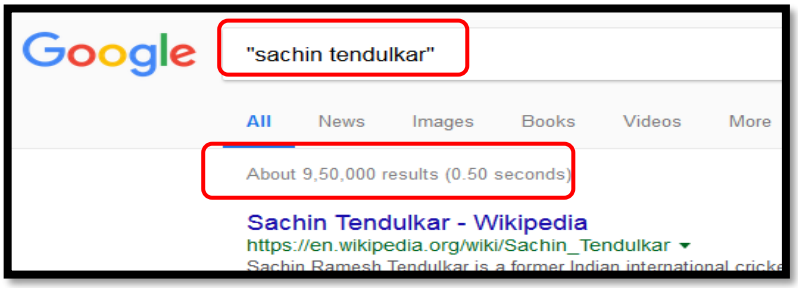


Figure : Google Explicit Search

b. Intitle

This Google operator allows one to search for pages with specific text in their HTML title. So intitle: "login page" will help a person scour the web for login pages.

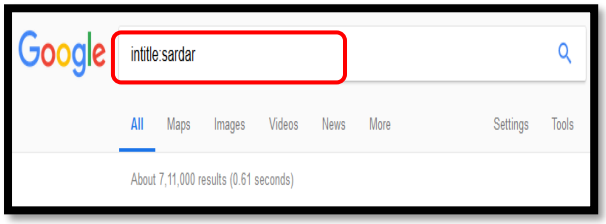


Figure : Intitle operator

- The query "**Intitle: Sardar**" will search "**Sardar**" in all Google cache pages and gives the results according to page rank.
- If we look at the results, it will show all websites having "**Sardar**" in their title of the webpage.

Figure :Intitle operator result

C. Inurl

This Google operator allows a person to search for pages based on the text contained in the URL (i.e. "login.php").

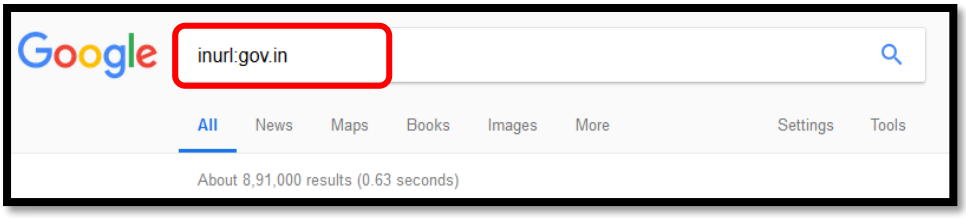


Figure : Inurl operator

- The query "**Inurl: gov.in**" will search for all Google pages which contains "**.gov.in**" **in** the URL of the website.
- If we look at the results, it will show all websites having "**.gov.in**" in their URL of the webpage.

Figure : Inurl operator result

- Similarly we can search for "**.in**", "**.com**", "**.nic.in**" and various other kinds of domain names in order fetch better results from the Google search engine.

d. Intext

This Google operator searches the entire content of a given page for keywords supplied by the person.

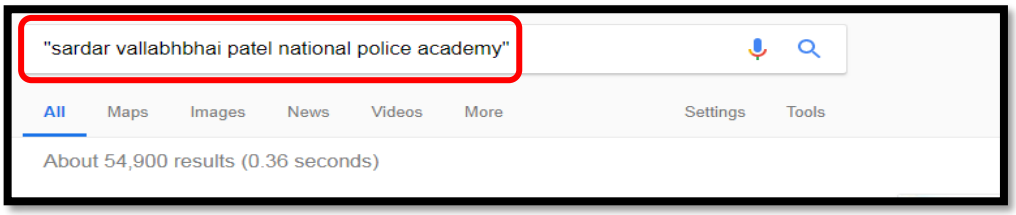


Figure : Intext Operator

Without this operator, there are **54,900** results are there, and with operator only **196** results we have. So, using these operators we can reduce the search results and find relevant information.

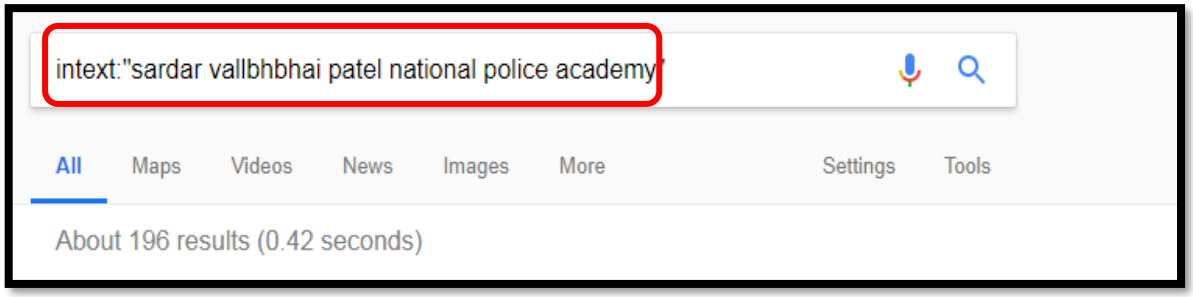


Figure : Intext Operator 2

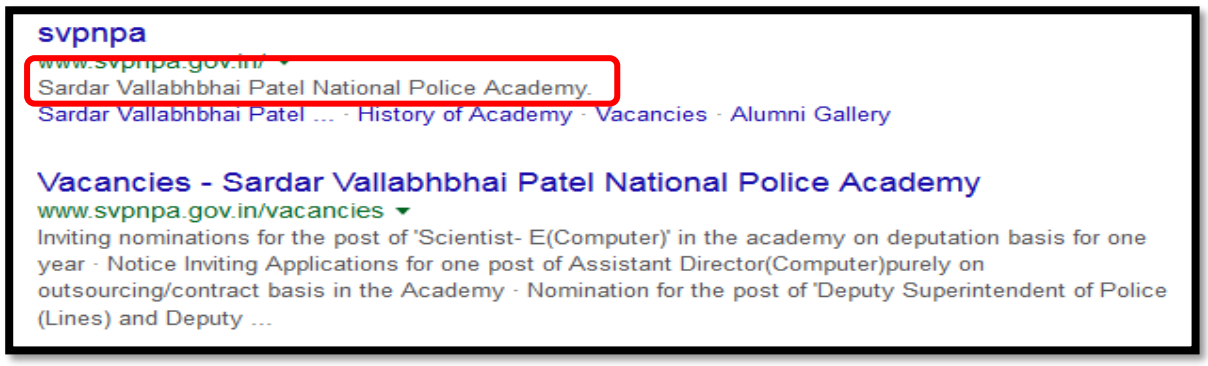


Figure : Intext Operator Result

e. Site

This Google operator allows the user to search for any query on a specific website.

Let us assume, we want to search for the name" Narendra panwar**"** on the website **www.svpnpa.gov.in**. The Google query would look something as shown below.

Figure : Site Operator

- This search provided only 3 results, which we tried to search for the keyword "**Narendra panwar**" on the website **www.svpnpa.gov.in**.
- Suppose if we want to search for hashtags on **twitter.com**, then we can use the following query.

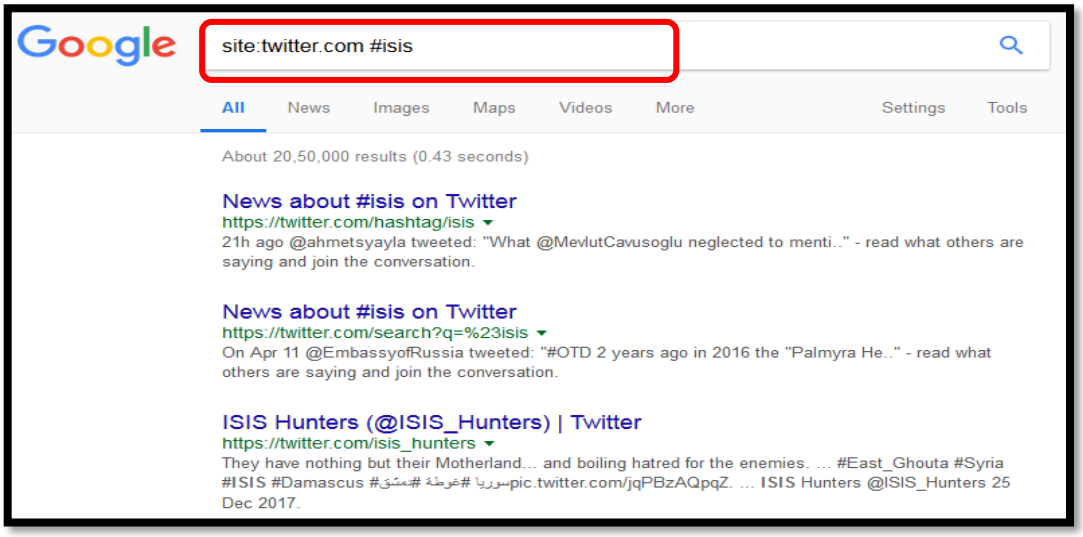


Figure : Site Opearator Result

f. Filetype

This Google operator helps a person narrow down search results to specific types of files such as PHP, PDF, or TXT file types.

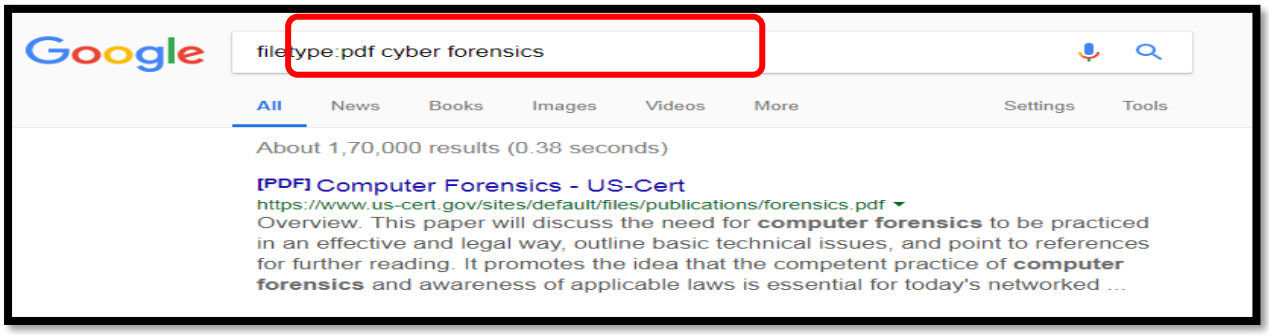


Figure : filetype operator

When we use "**filetype:pdf cyber forensics**" keyword, Google displays all the pdf files which contains the word "**cyber forensics**" available on the internet.

Figure : filetype operator result

In the above picture, we are combining "site" operator and "filetype" operator together, this keyword is used to search all pdf documents in svpnpa.gov.in website which are having cyber forensics keyword in it.
There are various other Google operators which we can use to narrow down our searches and get the desired results as fast as possible.
Below is some additional Google operator which we can make use of.

- **allinurl** – similar to the previous operator, but only returns matches for URLs that meet *all* the matching criteria.
- **ext** – very similar to filetype, but this looks for files based on their file extension.
- **allintext** – similar to the previous operator, but requires a page to match *all* of the given keywords.
- **Site** – limits the scope of a query to a single website.
- **Cache** - cache dork will show the cached version of the site or page of the specified site.
- **Link** - It will restricts results to sites containing links to the specified location.
- **Inanchor** - It will restrict results to sites containing links with the specified phrase in their descriptions. Unanchored dork will show all the sites which contains links with specified word or phrase.

Most of the operators can be used in combination, the most notable exceptions being the allintitle, allinurl, allinanchor, and Allintext operators. Advanced Google searchers tend to steer away from these operators, opting to use the intitle, inurl, and link operators to find strings within the title, URL, or links to pages, respectively. Allintext, used to locate all the supplied search terms within the text of a document, is one of the least used and most redundant of the advanced operators. Filetype and site are very powerful operators that search specific sites or specific file types.

2.4 Google advanced search

Google also provide advanced search option, where we can narrow down search results. To use google advanced search. follow the steps

Step 1: Go to google.com

Figure : Google Advance Search

Step 2: Type a string which you want to search

Step 3: Click on settings button

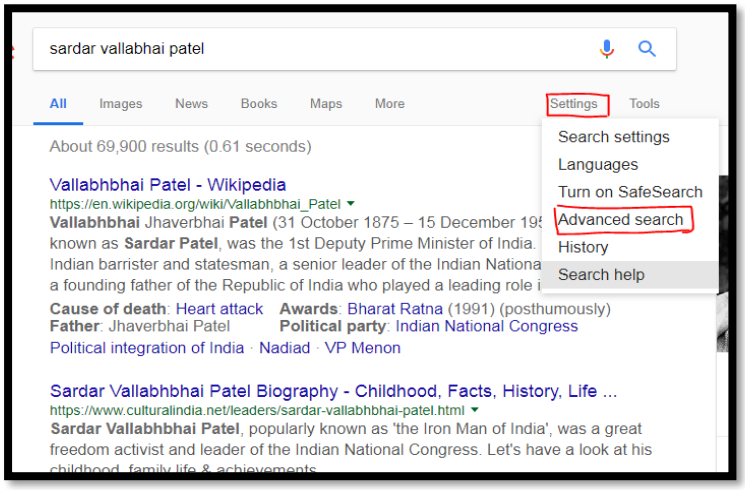


Figure : Google Advance Search Result

2.5 Carrot search

Carrot Search is an Open Source Search Results Clustering Engine. It can automatically organize small collections of documents (search results but not only) into thematic categories.

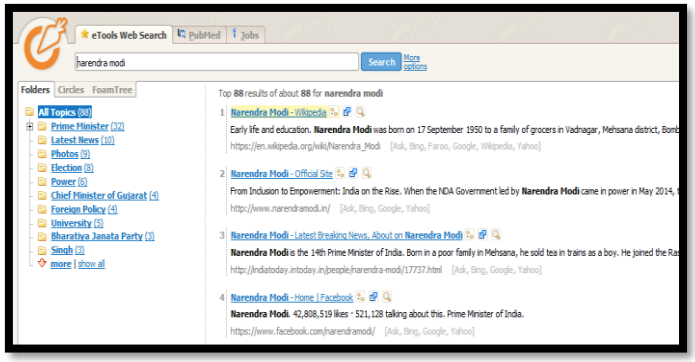


Figure : Search results in carrot search engine

It can automatically cluster small collections of documents, e.g. search results or document abstracts, into thematic categories.

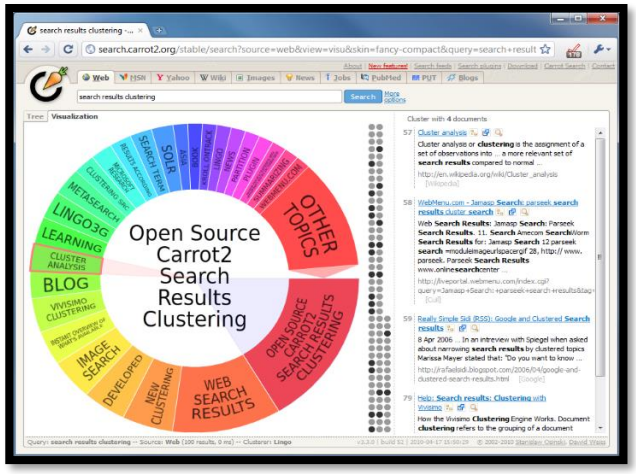


Figure: Clustered results in Carrot search engine

3. OSINT on Social Media

3.1 Introduction

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing, and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social circulation, and wikis are among the different types of social media.

Social media changes constantly – Twitter, now one of the most popular social media platforms, didn't even exist ten years ago. And the dynamics of social media use can be complicated. Different social media platforms are more popular among different demographic or geographic groups. Agencies should not simply think of social media as a venue to obtain evidence of a crime, but also as a tool for gathering intelligence. The intelligence can be useful for a variety of law enforcement functions, including counterterrorism, gang enforcement, policing protests, and monitoring drug trends.

The number of social media sites is astounding and ever-increasing. Some of the more popular applications include Facebook, Instagram, Kik, Snapchat, Tagged, Twitter, Myspace, Vine, LinkedIn, Flickr, Vimeo, Google+, Tumblr, Skype, Stickam, YouTube, Sina Weibo, Craigslist, Bebo, Sony PlayStation Network, Xbox Live!, iMessage, mIRC, Viber, Wickr, Vibe, WhatsApp, TigerText, Yahoo Messenger, AIM, Omegle, WeChat, and ooVoo. Investigators will need to determine a user's username and password for most of these services to obtain more information on a specific user.

Several resources can help agencies data mine and analyse information from social media websites. One useful site is Media Sonar, which is an application that provides location-based social media investigations' platform for law enforcement. Another is Sociospyder, which is software available exclusively to law enforcement and intelligence agencies that "mines open-source intelligence (OSINT) from Facebook, Twitter, LinkedIn, YouTube, and Google+."

- **Facebook** is a popular free social networking website that allows registered users to create profiles, upload photos, and videos, send messages, and keep in touch with friends, family, and colleagues. According to statistics from the Nielsen Group, Internet users within the United States spend more time on Facebook than any other website.
- **Twitter** is a free microblogging service that allows registered members to broadcast short posts called tweets. Twitter members can broadcast tweets and follow other users' tweets by using multiple platforms and devices.
- **Google+** (pronounced Google plus) is Google's social networking project, designed to replicate the way people interact offline more closely than is the case in other social networking services. The project's slogan is "Real-life sharing rethought for the web."
- **LinkedIn** is a social networking site designed specifically for the business community. The goal of the site is to allow registered members to establish and document networks of people they know and trust professionally.
- **Pinterest** is a social curation website for sharing and categorizing images found online. Pinterest requires brief descriptions but the main focus of the site is visual. Clicking on an image will take you to the original source, so, for example, if you click on a picture of a pair of shoes, you might be taken to a site where you can purchase them. An image of blueberry pancakes might take you to the recipe; a picture of a whimsical birdhouse might take you to the instructions.

- **Instagram** is a free online program and social network that enables users to take, edit and share photos with other users via Instagram's own platform, email, and social media sites including Twitter, Facebook, Tumblr, Foursquare, and Flickr.
- **YouTube** is a free video-hosting website that allows members to store and serve video content. YouTube members and website visitors can share YouTube videos on a variety of web platforms by using a link or by embedding HTML code.
- **WhatsApp** Messenger is a cross-platform instant messaging application iPhone, BlackBerry, Android, Windows Phone, and Nokia smartphone users to exchange text, image, video, and audio messages for free.

3.2 Sentiment Analysis using Open Source Tools

Sentiment Analysis is the process of 'computationally' determining whether a piece of writing is positive, negative or neutral. It's also known as opinion mining, deriving the opinion or attitude of a speaker.

Why sentiment analysis?

- **Business**: In marketing field companies use it to develop their strategies, to understand customers' feelings towards products or brand, how people respond to their campaigns or product launches and why consumers don't buy some products.
- **Politics**: In political field, it is used to keep track of political view, to detect consistency and inconsistency between statements and actions at the government level. It can be used to predict election results as well!
- **Public Actions**: Sentiment analysis also is used to monitor and analyse social phenomena, for the spotting of potentially dangerous situations and determining the general mood of the blogosphere.

a) Sentiment Analysis with Talkwalker

Talkwalker's Free social search monitors every conversation about your brand, hashtags and competition on social media.

After we login to the Talkwalker portal, we would search for the word "Taylor swift", we would see as follows

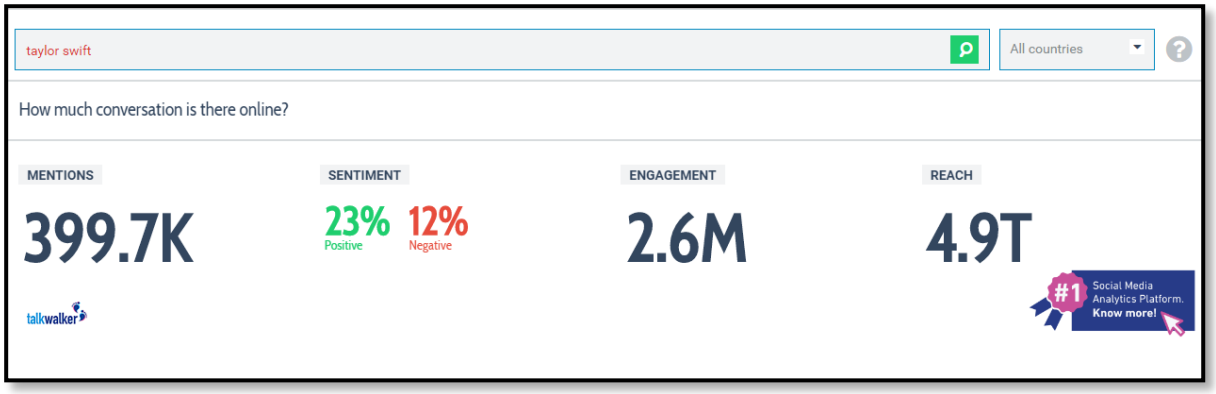


Figure : Talkwalker

As we can see, the sentiment about "Taylor swift" is 23% positive and 12% negative

In Talkwalker, we can also see who is talking about "Taylor swift" in various countries and also analyze based on the gender.

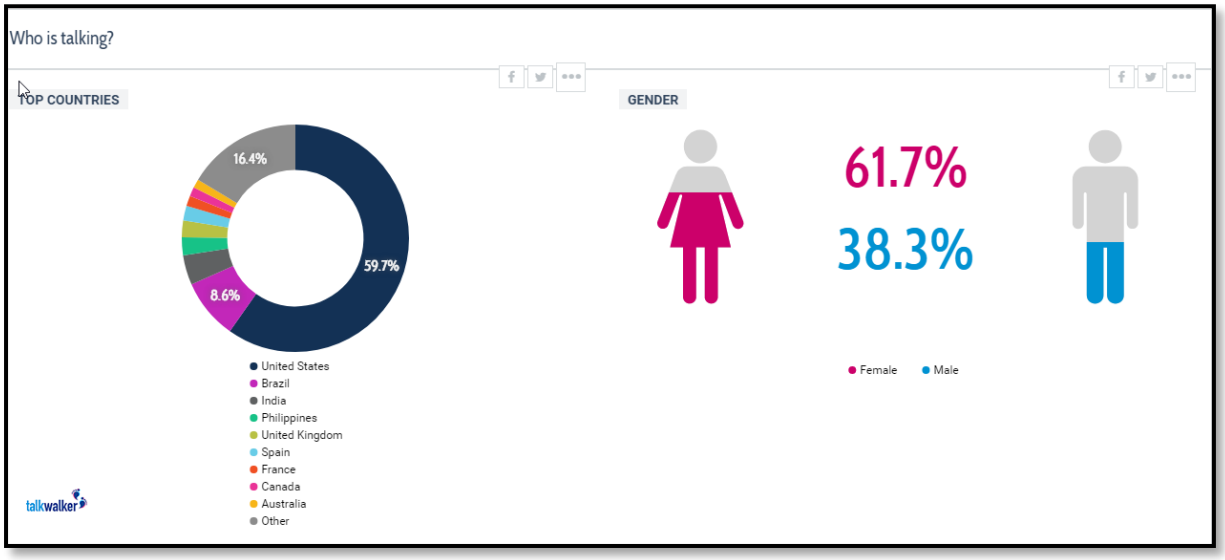


Figure : Talkwalker

If we scroll down to the bottom of the page, we'd be able to see each post and the sentiment associated with it denoted by a green (positive), yellow (neutral) or red(negative) flag.

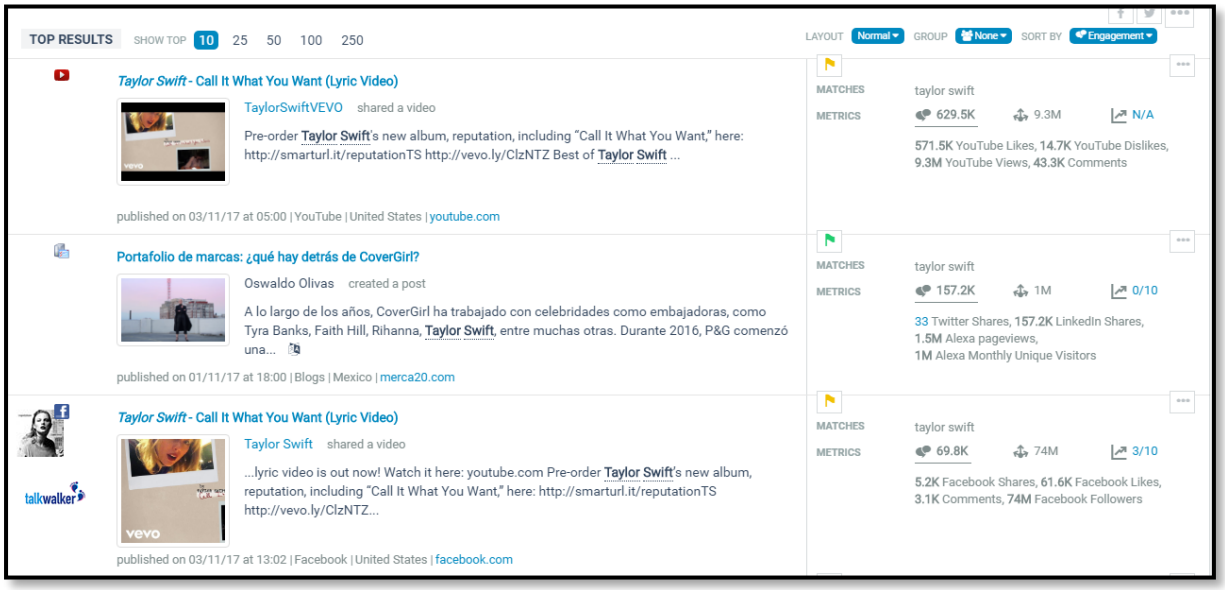


Figure : Talkwalker

As we can see that the first and third posts and neutral and the second is positive.

b) Hashtag Analysis using manual queries and Automated Queries on Social Media

➢ Twitter Advanced Search (twitter.com/search-advanced)

This page will allow for the search of specific people, keywords, and locations. The problem here is that the search of a topic is often limited to the previous seven to ten days. Individual profiles should display Tweets as far back as you are willing to scroll through. This can be a good place to search for recent data, but complete archives of a topic will not be displayed. The following explains each section.

- **All of these words**: The order of wording is ignored here, and only the inclusion of each of the words entered is enforced.

- **This exact phrase**: Every Twitter search takes advantage of quotes to identify exact word placement. Optionally, you can conduct the search here to get precise results without quotes.
- **Any of these words:** You can provide multiple unique terms here, and Twitter will supply results that include any of them. This search alone is usually too generic.
- **None of these words**: This box will filter out any posts that include the chosen word or words.
- **These Hashtags**: This option will locate specific posts that mention a topic as defined by a Twitter hashtag. This is a single word preceded by a pound sign (#) that identifies a topic of interest, this allows users to follow certain topics without knowing user names of the user submitting the messages.
- **From these accounts**: This section allows you to search for Tweets from a specific user. This can also be accomplished by typing the user name into the address bar after the Twitter domain, such as twitter.com/ndcrtc. This will display the user's profile including recent Tweets.
- **To these accounts**: This field allows you to enter a specific Twitter user name. The results will only include Tweets that were sent to the attention of the user. This can help identify associates of the target and information intended for the target to read.
- **Mentioning these accounts**: While these messages might not be in response to a specific user, the target was mentioned. This is usually in the form of using Anyone mentioning me within a Tweet may start it with @SVPNPA.
- **Near this place**: This field allows for the input of a zip code or city name. The default 15 miles setting would produce Tweets posted from within 15 miles of the perimeter of the zip code supplied. In a moment, I will explain a more effective search technique for location.
- **From this date**: The final option allows you to limit a search to a specific date range. We will do this manually in just a moment.

To perform advanced search on twitter, go to https://twitter.com/search-advanced.

We would get a page which looks as shown below.

Figure : Twitter Advance Search 1

- We can search for hashtags, people on the twitter, tweets based on the location and tweets in between specific dates.
- If we want to search for the word "**Metro**" in all the tweets, then we can enter the word in the "All of these words" search box and click search.
- This would display all the tweets containing the word "**Metro**" in it.

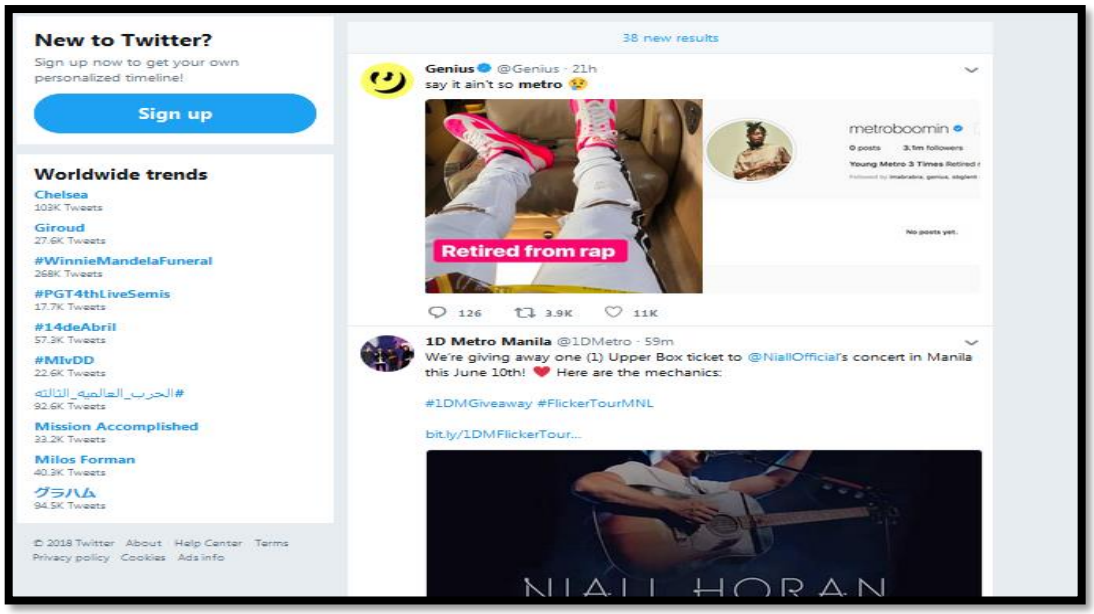


Figure : Twitter Advance Search 2

- Suppose we want to for tweets containing a specific hashtag. Then we can enter the word in the "These hashtags" search box and click search.
- This would display all the tweets containing the hashtag "**#isis**" in it.

Figure : Twitter Advance Search 3

- If we want to search for the hashtag "**Metro**" in all the tweets that were made from Hyderabad, then we can enter the word in the "All of these words" search box and enter "Hyderabad" in the places section and click search.
- This would display all the tweets containing the word "**Metro**" in all the tweets that were made from Hyderabad.

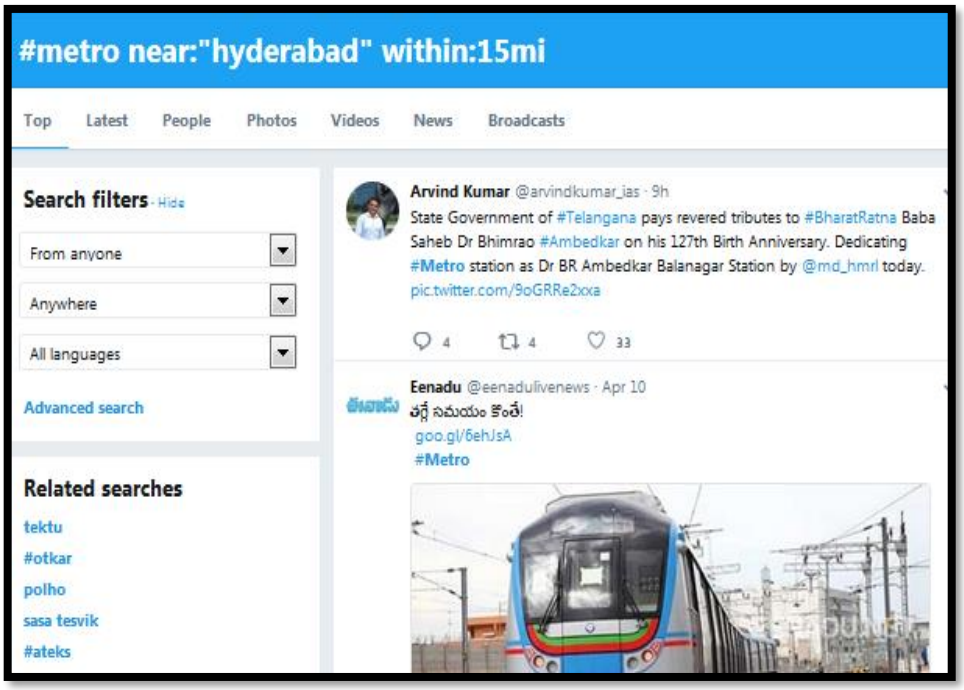


Figure : Twitter Advance Search 4

- If we want to search for the hashtag "**Metro**" in all the tweets that were made within a specific time period, then we can enter the word in the "All of these words" search box and select the duration within which the tweets are required in the "From this date" section and click search.
- The output would be the tweets within the specified duration as shown below

Figure : Twitter Advance Search 5

3.3 Location based Social Media Content Analysis

If you are investigating an incident that occurred at a specific location and you have no known people involved, Twitter will allow you to search by GPS location alone. The Twitter Advanced Search allowed us to search by zip code, but that can be too broad. The following specific search on any Twitter page will display Tweets known to have been posted from within one kilometer of the GPS coordinates of 43.430242, -89.736459.

geocode:43.430242, -89.736459, 1km

There are no spaces in this search. This will be a list without any map view. They will be in order chronologically with the most recent at top. The "1km" indicates a search radius of one kilometer.

This can be changed to 5,10, or 25 reliably. Any other numbers tend to provide inaccurate results. You can also change "km" to "mi" to switch to miles instead of kilometers. If you want to view this search from the address bar of the browser, the following page would load the same results.

https://twitter.com/search?q=geocode:43.430242,-89.736459,1km

You can add search parameters to either of these searches if the results are overwhelming. The following search would only display Tweets posted at the listed GPS coordinates that also mention the term "fight". Notice that the only space in the above search is between "km" and "fight".

geocode:43.430242,-89.736459,1km "fight"

It would be inappropriate to finish this section without a discussion about the lack of geo-enabled Tweets. Several years prior, this search would have been highly productive, as an alarming number of Twitter users were unknowingly sharing their locations with every post. Today, it is the opposite. The default option for Twitter is NOT to share location. A user must enable this option in order to appear within these search results. In my experience, catching a criminal from a location-enabled Tweet is extremely rare. However, we should be aware of the possibility.

3.4 OSINT using multiple websites and Web Applications

a) First Follower (socialrank.com/firstfollower**)**

It may be beneficial to know the first follower of your target on Twitter. This will likely be the person that introduced the target to Twitter and can often identify a former associate. If you want only this one piece of information, First Follower will usually give you the result. However, we have found that you must often click the search option several times before the result is displayed.

b) One Million Tweet Map (onemilliontweetmap.com)

This service only displays the most recent one million Tweets on an international map. They do not have access to every Tweet available, often referred to as the "firehose", but they offer new Tweets every second. We would never rely on this map for complete data about a location. However, monitoring a large event can provide live intelligence in an easily viewed format. We recommend using a mouse scroll wheel to zoom into your location of interest. Once you are at a level that you can see single Tweets, you can click any of them to see the content. The page will automatically refresh as new information is posted.

c) Followerwonk (followerwonk.com)

The second website that we use for group Twitter analysis is Followerwonk. This service offers more options than Twiangulate and will let you compare up to three users. The second tab at the top of the page, titled "Compare Users", will allow you a more thorough search. We can see that the first and second subject do not have any people in common that they follow on Twitter. This can indicate that they may not know each other in real life, or that they simply have different tastes in the people that they find interesting. However, the first and third subjects have 79 people in common that they follow on Twitter. This is a strong indication that they know each other in real life and have friends in common. Clicking on the link next to this result will display the identities of these people

This default search on Followerwonk is a good start. A more valuable search is to analyze the people that follow these users. The previous example identified people that our targets followed. This will often include celebrities, businesses, and profiles that probably have no impact on your investigation. However, the people that follow your targets are more likely to be real people that may have involvement in your investigation

3.5 Keyword monitoring on Social media Platforms

There are approximately 500 million tweets a day. That's a lot of information to get through, but TweetDeck makes it a lot easier to monitor trends, follow hashtags, and perform live searches. This is a useful tool for security professionals, as it allows us to monitor for events in real time, such as cyber-attacks, vulnerabilities being released, or even tracking malicious actor's activity.

a) Twilert

Twilert is a tool that, like Warble, emails you tweets based on search terms. We'll get real-time emails with tweets about your brand, competitors, hashtags, or any search term you provide.

Some of the features offered by Twilert are:

- Twilert tells you when someone is talking about your brand on Twitter.

- You decide what to search for
- Twilert listens for your chosen search terms

Twilert is easy to use tool, we just need to Sign up, set up our alerts and we are good to go. There are 3 different plans, but for all small agencies and business, the pro plan is the best, costing $19 per month. This is our Twilert account page. You can see that we have a couple of alerts set to show up at 3pm every day.

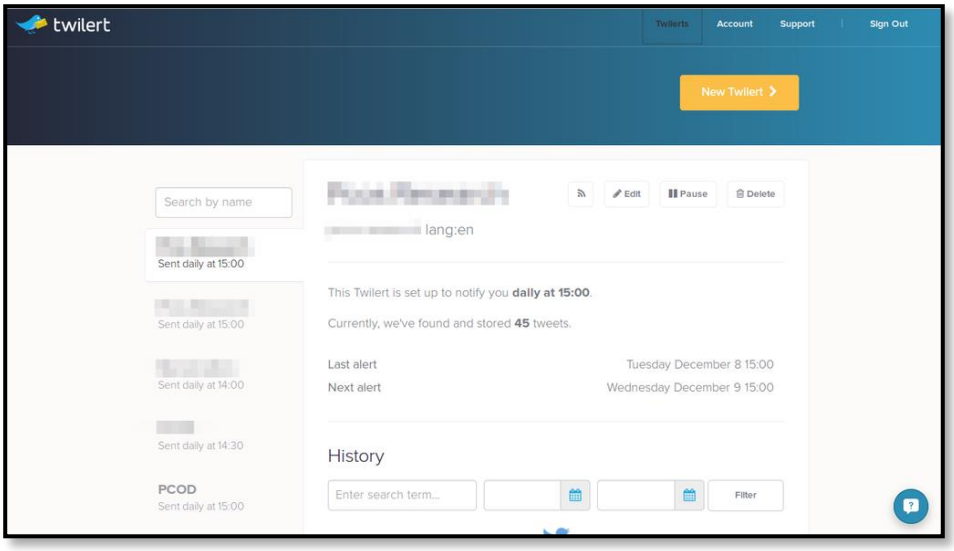


Figure : Twilert

Setting up a new alert is easy. Simply click the top right-hand yellow button and we will be taken to this page

Assuming we want to be informed every time the word ‘cars’ comes up on twitter

There are 4 different categories that search terms can be refined with. Filter by

- Word – exact phrase, something or other, exclude, hashtag
- User – from: user, to: user, mentioning @user
- Location – area on map, in: language
- Misc – 🙂 positive, 😦 negative, ? question, retweets, links, verified.

For my example, I have chosen to be alerted when there are **POSITIVE** new tweets related to **CARS**, in **ENGLISH**

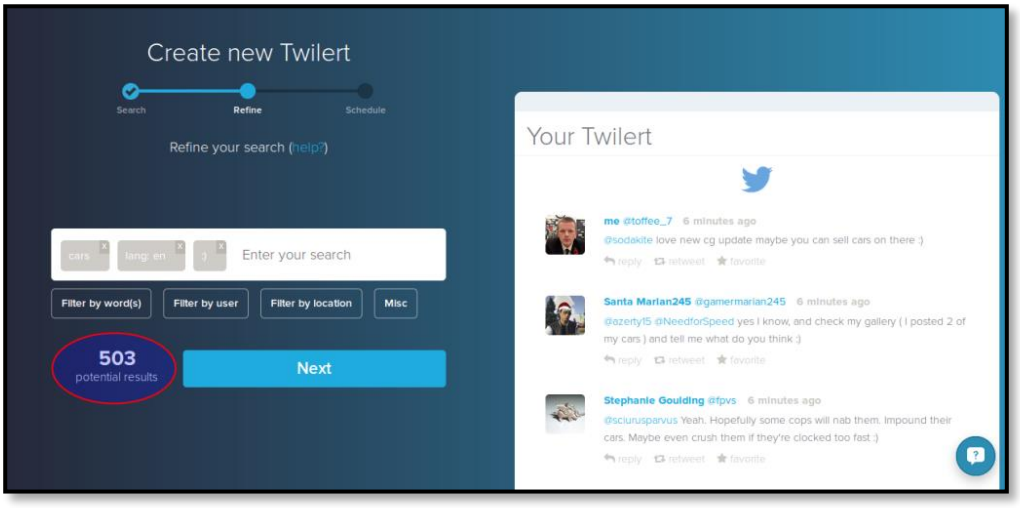


Figure : Twilert Result

As we can see, the initial number of tweets related to cars was a staggering 216000. However, putting multiple filters brought down that number to 503 tweets only.

The next page will ask us to name the alert and set if you want to be alerted hourly, daily, weekly or in real time and if we would prefer your alerts in html or plain text format.

4. OSINT on Mobile numbers

Most of the times, we receive complaints from the victim saying that they have received a call or message from an unknown number trying to harass or threaten them. It becomes important for an investigating officer to get the details about the mobile number as soon as possible. Below are some effective ways by which we can gather more information using the mobile number.

4.1 Verifying mobile service provider

As a law enforcement agency, we need to know the service provider of a given mobile number which can be used to get the CDR of the suspect and other subscriber details. For that reason, we will see how we can get the service provider details from the mobile number.

- In order to identify the service provider, first we will go to the website called as freecarrierlookup.com.

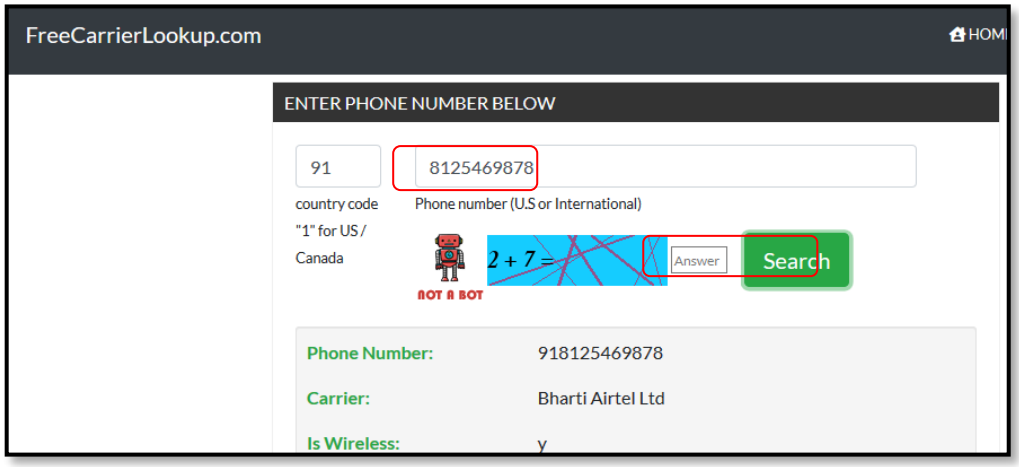


Figure : freecarrierlookup

- Now we will enter the unknown mobile number of the person. And once we enter the number, it will suggest the mobile service provider. In the example shown in the above screenshot, the number belongs to Airtel.
- After that, in order to verify the service provider, we need to go to the recharge website of the suggested service provider and enter the mobile number to confirm validity of the information from **Free carrier lookup**. In the above example, we would cross check the details from the Freecharge with Airtel mobile recharge website as suggested and try to recharge this mobile number. Enter the mobile number and add some random amount and click proceed to confirm. As we click, we will get a confirmation saying that this number belongs to Airtel. By this way we can confirm that this mobile number is an Airtel number now.
- In case of non-Airtel mobile number, if you try to recharge on its recharge website. It gives an error saying “subscriber number does not exist”.

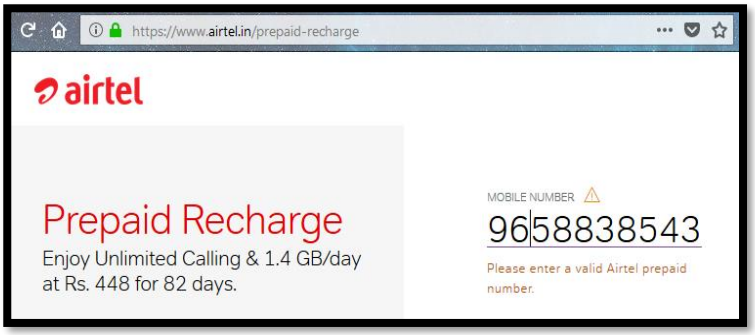


Figure : freecarrierlookup result

- Above mentioned procedure can be applied on various service providers such as BSNL, Reliance and Idea etc.

4.2 Reverse number lookup

- **Truecaller**

Another technique to get the details of the service provider of a number is by using a website called **truecaller.com**.

Truecaller is a mobile application, which is a worldwide number lookup service. Which means, by this app you can find the name of the user of any Mobile number as saved in the contacts of the person who has installed this app without making a call to that number.

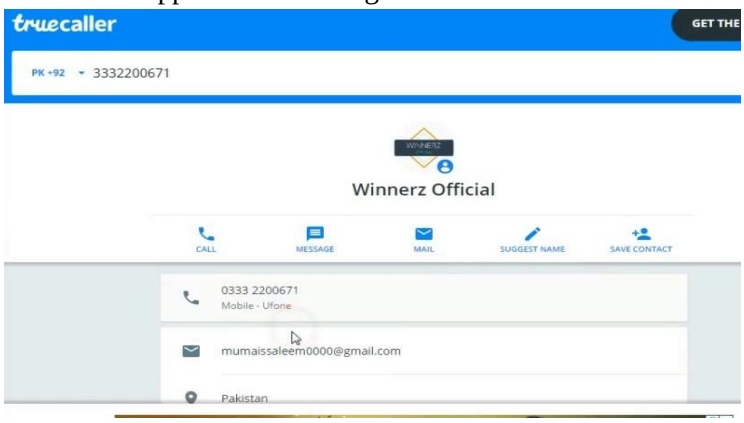


Figure : Truecaller search

Truecaller has collection of all the contacts (mobile phonebook) of its users (People who use this app) from all around the world and the public phone directories.

When a person downloads and starts using Truecaller, this app uploads all the contacts of that person to its database. So, when you search a number on Truecaller, it shows the name used by someone for saving the number in his/her phonebook.

In the process of investigation, when the officer comes across an unknown number, this service can be utilized to find out the name of the user. It has to be understood that the data on this app need not be correct always. Many times, we get the names of the persons as their nick names that are used to save the contact.

Here first we need to sign in with the Google account. And then once we enter the mobile number in the search box, it will give the name and service providers of the owner of the mobile number.

- **Facebook password reset**

Facebook provides option for resetting the password using the E-mail/Phone number/username/ full name. If we know the phone number, we can go to the password reset page of Facebook and enter the phone number in the given field. If any Facebook account is linked with this number, that account would be shown. This way we will get the full name and photos of owner of that number.

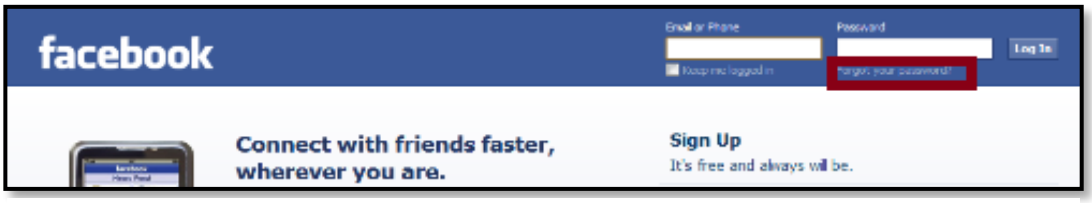


Figure : Facebook forgot password

- Go to "**Facebook.com**" and click the "**Forgot your account**".

- Enter the mobile number of the person and then select search.

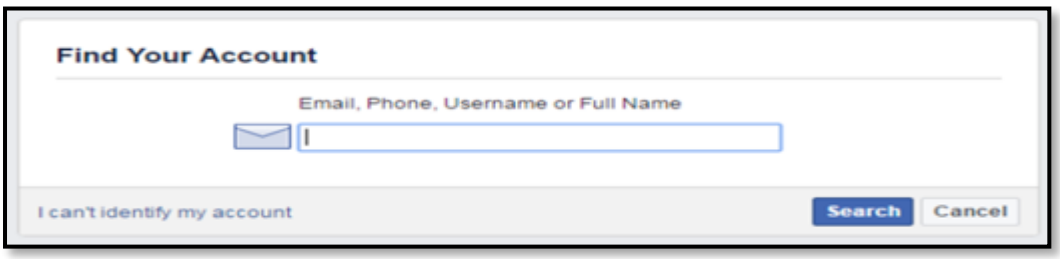


Figure : Facebook reset password

- Once we click the search button, Facebook will display the Facebook profile belonging to that mobile number.

Figure : Facebook Password Reset

➢ **Pipl.com**

Pipl.com is an online search engine, which can be used to find the information about an individual by using the email address, social media username or phone number.

- Go to the website "**pipl.com**" and enter the mobile number and click search.

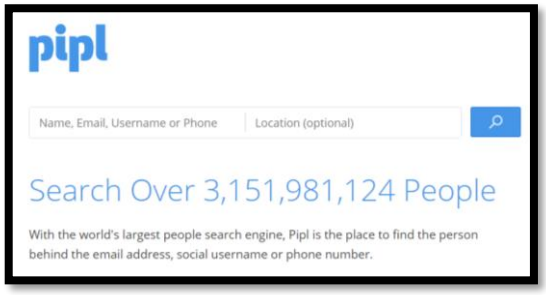


Figure : Pipl search

- The output when we search for mobile number on pipl.com is shown below.

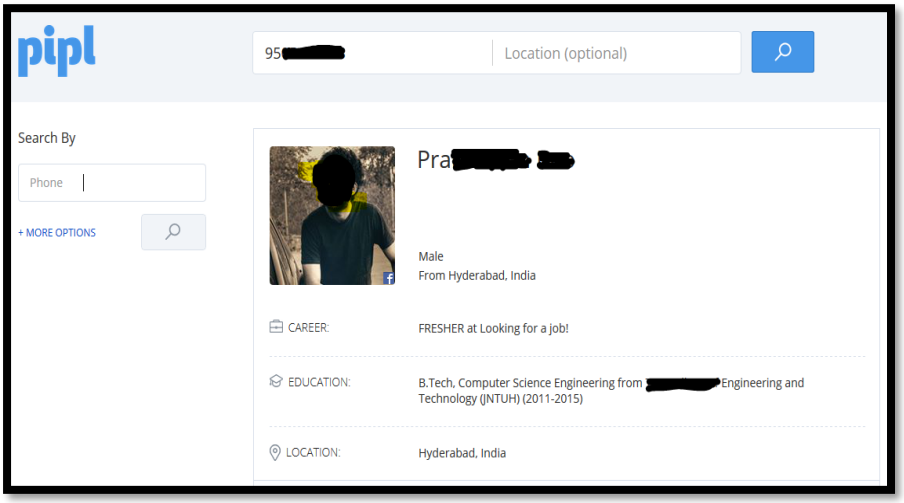


Figure : Pipl search result

5. Gathering information from mobile apps

a) **Eyecon** - is a program which automatically adds photos to your contacts and arranges your favorite messengers for fast and simple access. Bright intuitive list of contacts will allow you to gather icons of the most popular application in one page. With the help of this contact finder you will see a photo and name of someone calling directly during the call.

Figure : Eyecon

b) **WhatsApp Contacts**

One more way to find the identity on the owner of the unknown mobile number is to save the suspect's number to a smartphone in which WhatsApp is installed. If the number is having WhatsApp account, then the user profile can be viewed. This method is possible only if the user has set the privacy settings to public.

Figure : WhatsApp Contacts

c) Additional Resources

Explaining how to enter a telephone number into every reverse phone search website is unnecessary. Instead, I present the additional resources that I have found helpful in my investigations. They are listed in order of most benefit to least.

- Advanced Background Checks (advancedbackgroundchecks.com/phone)
- Nuwber (nuwber.com/phone)

- Sync.me (sync.me)
- Search Bug (searchbug.com/peoplefinder/phone-search.aspx)
- OK Caller (okcaller.com) That's Them (thatsthem.com) 411 (411.com)
- Reverse Genie (reversegenie.com/reverse_phone)
- Super Pages (wp.superpages.com)
- Yahoo (people.yahoo.com)
- Free Phone Tracer (freephonetracer.com)
- Fone Finder (fonefinder.net)
- Mobile Phone No (mobilephoneno.com) Skip Ease (skipease.com/reverse) IvyCall (ivycall.com)
- Numpi (numpi.com)

6. Using Online maps for information gathering and recce

6.1 Overview of Online maps

The presence of online satellite images is not news anymore. Most of you have already "Googled" your own address and viewed your home from the sky. This view can get surprisingly detailed when using the zoom feature. Alleys, sheds, and extended driveways that are hidden from the street are now visible thanks to this free service. Many tactical units will examine this data before executing a search warrant at a residence.

Aerial maps are helpful for viewing the location of exiting doors, escape routes, stairs, and various obstructions. The rapidly growing availability of the Street View option now gives us more data.

6.2 Introduction to various online map services

- **Google Maps (maps.google.com)**

In 2014, Google made several changes to their online maps service. They introduced a new feature with Street View that made the default view full screen. This eliminates the Google search bar, side menu, browser menus, and any other items from blocking a larger view. Additionally, Google streamlined the entire Maps experience to make everything easier to use. Unfortunately, they also eliminated many of the features that were beneficial to researchers and investigators. Fortunately, they have re-enabled some of these missing features. The following basics of Google Maps are now default for all users.

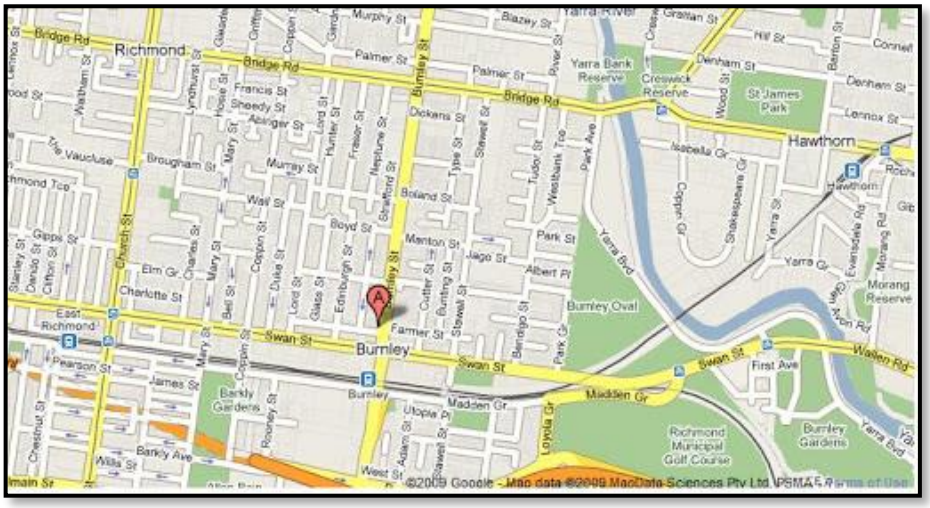


Figure : Google maps

- **Search Bar**: The Google Maps search bar can now accept practically any type of input. A full address, partial address, or GPS coordinates will immediately present you with a mapped view. Company names and types of businesses, such as "cafe" will highlight locations that may be of interest. This search field is the first stop. Attempt any search relevant to your investigation and you may be surprised at how accurate Google is. We can collapse this entire menu by clicking the left arrow next to the search field. This will return you to a full screen view of the map.

- **Satellite/Earth View**: The lower left area of any map will offer a satellite and earth view. The satellite view is a direct view from the sky looking almost straight down. The Earth view is similar, but offers the tilt option. While in the earth view, click on the small icon to the right of the map that appears similar to four small squares. This will shift the view 45 degrees and a second click will shift an additional 45 degrees. A third click returns to the standard satellite view. The rotation icon above this button allows you to rotate your view for the desired result. While satellite views of maps are now well-known, we see continuous enhancements that are not advertised. A satellite view of your target location is always vital to every investigation.

➢ Zoom Earth (zoomearth.com)

This multiple satellite imagery website presents views from NASA, Bing, and ArcGIS. Occasionally, the ArcGIS data is more recent than Google or Bing. The smooth interface will easily provide a comparison of the available images for any location. One advantage of Zoom Earth is the ability to view satellite images in true full-screen mode. This allows creation of full- screen captures without branding, menus, or borders. This could be more appropriate for live demonstration instead of a standard Google or Bing window.

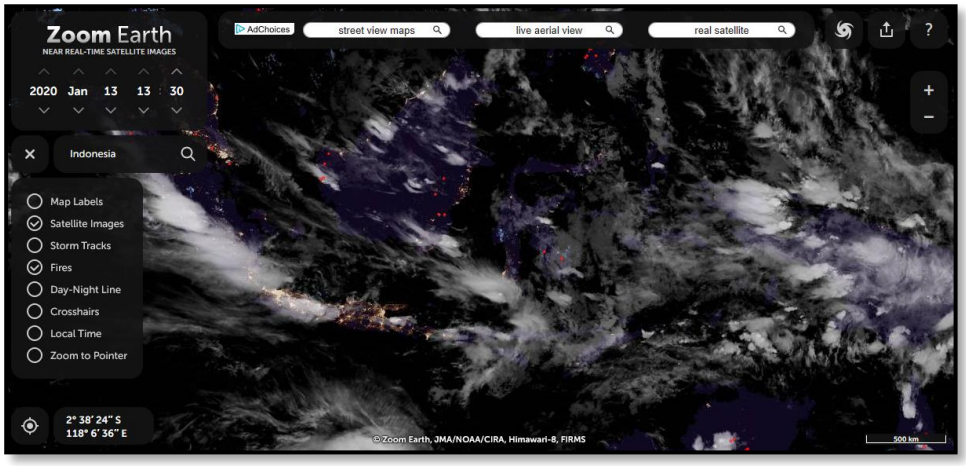


Figure : Zoom Earth

➢ Google Earth

Google maps is an online website. Google Earth is a standalone application that takes the Google Map data to another level. With this application, we have access to many mapping tools. These tools can import data from spreadsheets and help you visualize the content. In order to maintain the scope of open source intelligence, we will focus on only a few specific tools. Within the application, the first step is to display your location of interest. This can be accomplished by typing the address or GPS coordinates in the upper left search field. When you see your target location and have set the zoom to an appropriate level, you are ready to start adding layers. By default, you will only see the satellite imagery of the location. The menu on the left possesses options for adding new content to this view. The last box in this menu is titled "Layers". Inside of this menu are several data sets that can be enabled and disabled by the checkbox next to each. The following details will explain the layers of interest

Photos - Digital images uploaded through social networking sites Panaramio and 360cities
Roads - Text layer of road names
3D Building - Alternative 3D view of some locations
Gallery - User submitted content including YouTube videos

Figure : Google Earth

7. OSINT on Multimedia files

7.1 Introduction to metadata

When an original document is found online, it is obviously important to analyze the visible content of the file. This includes the file name, written text, and an original location of the document. Digging deeper will expose more information. There is data embedded inside the document that cannot be seen by simply looking at the content of the file. This data is called metadata and can be very valuable to any type of investigation. This data can often include the computer name the document was created on, the user name of the computer or the network, the software version used, and information about the network to which the computer is connected. The best way to view all this information is to use a software solution which will be discussed later in the book. It is also possible to view this "hidden" information online through a web browser.

Several online sites will allow you to upload documents for analysis. To do this, click the "browse" button on the pages detailed below. This will enable a file explorer that will allow you to select the document that you want analyzed. The result often identifies a created and modified date, the original tide, three applications used to create the document, and a user name. A further search of this user name through the previously discussed techniques could produce a wealth of information about the author of the document. The following websites allow you to upload a locally stored document or submit a URL of a file for analysis. Please use caution with this technique. If the document is already posted online, there is very little risk of allowing a URL analysis. However, a locally stored file that has never been on the internet may require a second thought If the content is sensitive, you may not want to upload to any service. If the file contains classified information, you could be jeopardizing your clearance. In these situations. If this is not a concern the following work well.

7.2 Identifying metadata in Various multimedia files

Thanks to cameras on every data cellular phone, digital photograph uploads are extremely common among social network users. These images can create a whole new element to the art of open source intelligence analysis. Now, we will identify various photo sharing websites as well as specific search techniques. Later, photo metadata will be explained that can uncover a new level of information including the location where the picture was taken, the make, model and serial number of the camera, original uncropped views of the photos, and even a collection of other photos online taken with the same camera. After reading this information, you should question if your online photos should stay online

7.3 Jeffrey's Exif Viewer

Jeffrey's Exif Viewer the online standard for displaying Exif data. The site will allow analysis of any image found online or stored on a drive connected to your computer. The home page provides two search options. The first allows you to copy and paste an address of an image online for analysis. Clicking "browse" on the second option will open a file explorer window that will allow you to select a file on your computer for analysis. The file types supported are also identified on this page. The first section of the results will usually provide the make and model of the camera used to capture the image. Many cameras will also identify the lens used, exposure settings, flash usage, date and time of capture, and file size.

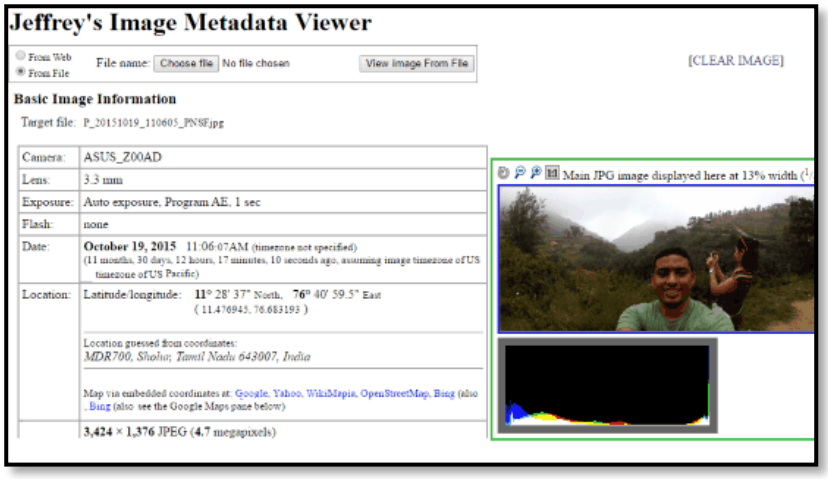


Figure :Jeffrey's Exif Viewer

Scrolling down the analysis page will then identify many camera settings that probably provide little information to the researcher. These include aperture information, exposure time, sharpness, saturation, and other image details. Mixed in with this data is the serial number field. This is most common in newer SLR cameras and will not be present in less expensive cameras. These cameras usually identify the make, model, and serial number of the camera inside every photo that they capture. A serial number of a camera associated with an image can be valuable data. This can help an analyst associate other photos found with a target's camera. If an "anonymous" image was found online that included a serial number in the Exif data, and another image was found of a target of the investigation, these two photos can be analyzed. If the serial number as well as make and model of camera match, there is a good likelihood that the same camera took both images. It is important to know that this data can be manipulated, though. Using software such as Exif Tool, a user can modify this data. While this is not a popular tactic to use, it is still possible. The difficult part of this is finding photos only knowing the serial number.

In order to find the exif data of an image, visit website http://exif.regex.info/exif.cgi

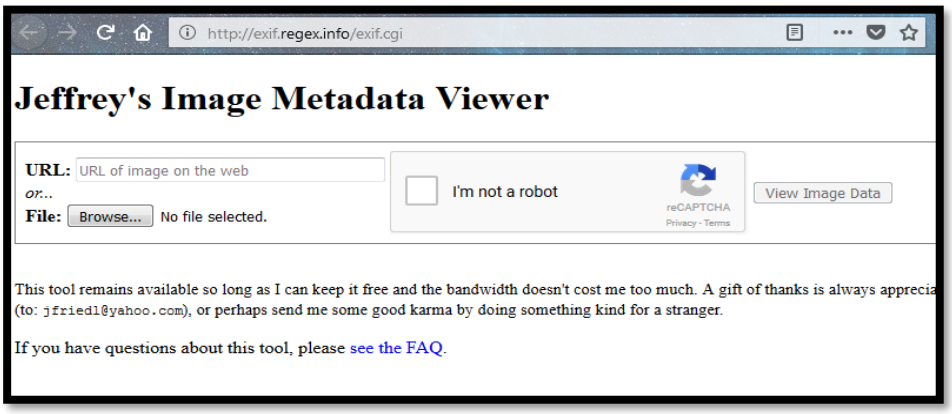


Figure : Jeffrey's Exif Viewer

7.4 Introduction to reverse image search

Advancements in computer processing power and image analysis software have made reverse image searching possible on several sites. While a standard search online involves entering text into a search engine for related results, a reverse image search provides an image to a search engine for analysis. The results will vary depending on the site used. Some will identify

identical images that appear on other websites. This can be used to identify other websites on which the target used the same image. If you have a photo of a target on a social network, a reverse analysis of that photo may provide other websites on which the target used the same image on. These may be results that were not identified through a standard search engine.

Occasionally, a target may create a website as an alias, but use an actual photo of himself. Unless you knew the alias name, you would never find the site. Searching for the site by the image may be the only way to locate the profile of the alias. Some reverse image sites go further and try to identify other photos of the target that are similar enough to be matched. Some will even try to determine the sex and age of the subject in the photo based on the analysis of the image. This type of analysis was once limited to expensive private solutions. Now, these services are free to the public.

We can use the picture itself to search in the internet instead of keywords. Using this way, we can find out websites where same images has been uploaded or being used. This method can also be used to find out where this image has been uploaded first and where similar images are located on internet.

- **TinEye**

Using TinEye, we can search by image or perform what we call a reverse image search. We can do that by uploading an image, or searching by URL. We can also simply drag and drop your images to start your search.

TinEye constantly crawls the web and adds images to its index. Today, the TinEye index is over 27.3 billion images. Using TinEye, we can identify the website which first uploaded a specific viral image. And we can also list all the websites in which the image is available.

website www.tineye.com

Figure : Tineye

8. OSINT using Government websites

8.1 Information from National Voters Service Portals

The National Voters Portal (http://www.nvsp.in/) is a place where you can search for the people who are listed in voters list in India.

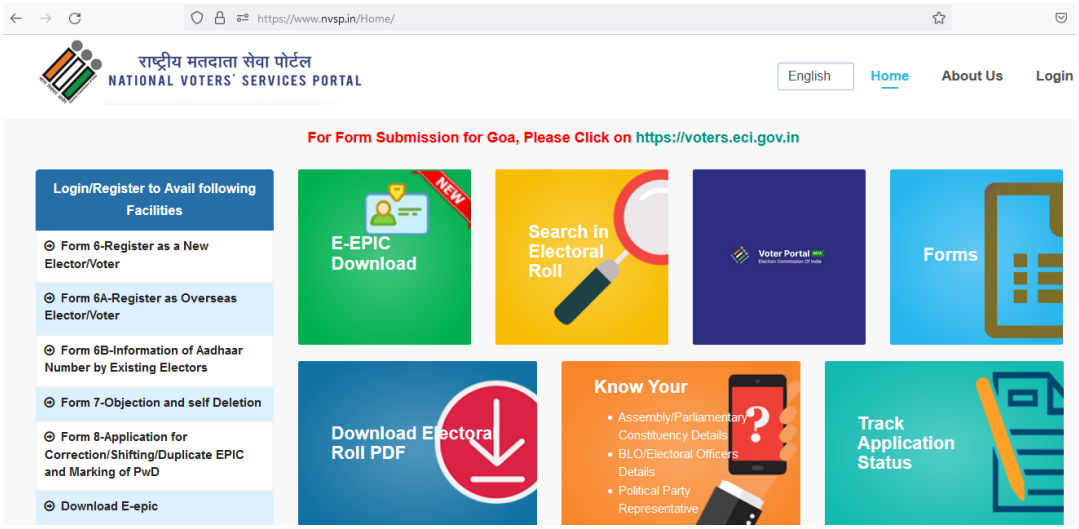


Figure : National Voters Portal Home Page

We can search with the name/state/district/constituency name/fathers name etc. In case we know the suspects name we can search on this portal. If the name is a common name in India, we will get thousands of results. We can filter it by state/district/constituency name/fathers name etc.

8.2 Information from Ministry of Road Transport & Highways

Motor vehicle departments will have the details of all the vehicles and driving license issued by them. At any point of investigation, if we get a vehicle number or license number, we can search for the details of owner.

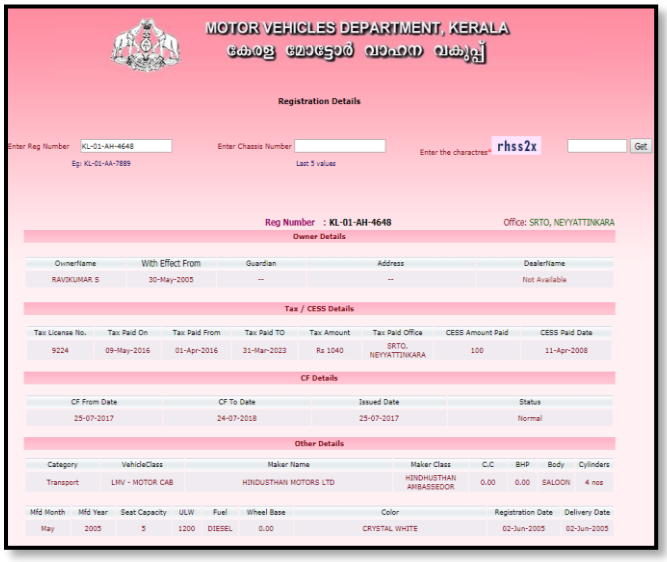


Figure : Motor Vehicle Dept Kerala

9. OSINT using Automated tools

9.1 Recon-ng

Recon-ng is a full-featured web reconnaissance framework written in Python. Complete with independent modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which OSINT research can be conducted quickly and thoroughly. This utility provides automation to many of the redundant tasks that OSINT examiners find themselves performing on a daily basis. If you would like to install it within your own Linux environment, everything you need is at

https://bitbucket.org/LaNMaSteR53/recon-ng/wiki/Usage%20Guide.

Recon-ng does not possess many online tutorials. Instead of trying to summarize how the program functions. Upon executing Recon-ng from the dock, a large portion of red text will appear followed by a default Terminal prompt. The red text indicates that you have not applied any API keys. At this prompt, let's begin with the help command. Typing help reveals the following commands and explanations.

```
Add         Adds records to the database
Back        Exits the current context
Delete      Deletes records from the database
Exit        Exits the framework
help        Displays this menu
keys        Manages framework API keys
load        Loads specified module
pdb         Starts a Python Debugger session
query       Queries the database
record      Records commands to a resource file
reload      Reloads all modules
resource    Executes commands from a resource file
search      Searches available modules
set         Sets module options
shell       Executes shell commands
show        Shows various framework items snapshots Manages workspace snapshots spool   Spools output to a file
unset       Unsets module options
use         Loads specified module
workspaces  Manages workspaces
```

Figure : Recon-ng Commands

Typing show modules will reveal the current functions available. Think of a module as a "resource". Just like Twitter is a website resource that we can use through a web browser, "twitter_mentions" is a specific resource that we can use in Recon-ng. The following modules were available at the time of this writing. We will use some of these during the instruction.

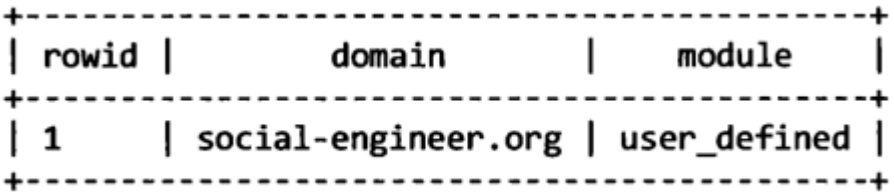
```
[recon-ng][default] > show modules

  Discovery
  ---------
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter

  Import
  ------
    import/csv_file
    import/list

  Recon
  -----
    recon/companies-contacts/bing_linkedin_cache
    recon/companies-contacts/jigsaw/point_usage
    recon/companies-contacts/jigsaw/purchase_contact
    recon/companies-contacts/jigsaw/search_contacts
    recon/companies-contacts/linkedin_auth
    recon/companies-multi/github_miner
    recon/companies-multi/whois_miner
    recon/contacts-contacts/mangle
    recon/contacts-contacts/unmangle
    recon/contacts-credentials/hibp_breach
    recon/contacts-credentials/hibp_paste
    recon/contacts-domains/migrate_contacts
    recon/contacts-profiles/fullcontact
    recon/credentials-credentials/adobe
    recon/credentials-credentials/bozocrack
    recon/credentials-credentials/hashes_org
    recon/domains-contacts/pgp_search
    recon/domains-contacts/whois_pocs
    recon/domains-credentials/pwnedlist/api_usage
    recon/domains-credentials/pwnedlist/domain_ispwned
    recon/domains-credentials/pwnedlist/leak_lookup
    recon/domains-credentials/pwnedlist/leaks_dump
    recon/domains-hosts/bing_domain_web
    recon/domains-hosts/builtwith
    recon/domains-hosts/shodan_hostname
    recon/domains-hosts/ssl_san
    recon/domains-hosts/threatcrowd
    recon/domains-vulnerabilities/punkspider
    recon/domains-vulnerabilities/xssed
    recon/domains-vulnerabilities/xssposed
    recon/hosts-domains/migrate_hosts
    recon/hosts-hosts/freegeoip
    recon/hosts-hosts/ipinfodb
    recon/hosts-hosts/ssltools
    recon/hosts-locations/migrate_hosts
    recon/hosts-ports/shodan_ip
    recon/locations-locations/geocode
    recon/locations-locations/reverse_geocode
    recon/locations-pushpins/flickr
    recon/locations-pushpins/instagram
    recon/locations-pushpins/picasa
    recon/locations-pushpins/shodan
    recon/locations-pushpins/twitter
    recon/locations-pushpins/youtube
    recon/netblocks-companies/whois_orgs
    recon/netblocks-hosts/shodan_net
    recon/netblocks-ports/census_2012
    recon/netblocks-ports/censysio
    recon/ports-hosts/migrate_ports
    recon/profiles-contacts/dev_diver
    recon/profiles-contacts/github_users
    recon/profiles-profiles/profiler
    recon/profiles-profiles/twitter_mentioned
    recon/profiles-profiles/twitter_mentions
    recon/profiles-repositories/github_repos
    recon/repositories-profiles/github_commits
    recon/repositories-vulnerabilities/gists_searc
    recon/repositories-vulnerabilities/github_dork

  Reporting
  ---------
    reporting/csv
    reporting/html
    reporting/json
    reporting/list
    reporting/proxifier
    reporting/pushpin
```

Figure : Recon-ng modules

Before we can conduct any research within this program, we must create a workspace. A workspace is a container that will isolate your work from one investigation to another. Think of a workspace as a case file. You may have a stack of cases on your desk, each with its own folder. All of your work on a case stays within the folder associated. Workspaces are similar. You should create a new workspace for each investigation. They can be deleted later or preserved for additional work. You can type **workspaces list** at any time to see the currently used workspaces. For now, we will create a new workspace titled OSINT by executing a command of workspaces **add OSINT**.

After creation, you will automatically begin using the new workspace. If you have created more than one workspace, such as one titled OSINT2, you can switch to it by typing workspaces **select OSINT2**. You might have a workspace for every target suspect or a single workspace for an entire case. Each situation will be unique. Now that you have a space created, we can begin.

The **show** command followed by a type of data will identify any stored content that will be used during an investigation. Typing **show domains** should reveal **no data returned** since we have not added any target domain names to our workspace. Therefore, let's add a domain name for our investigation by typing **add domains social-engineer.org**. Repeating the show domains command should now reveal the following.



rowid	domain	module
1	social-engineer.org	user_defined

We have now added this domain into our system, and any module associated with domains that we execute will include this target. You could add every domain of interest and execute searches across all at once. Typing **add domains cnn.com** will make for a great example for the next option. Once you have your domains loaded, you may want to identify related web hosts. A domain, such as cnn.com, may have several unique host addresses that may be beneficial. Since I have already stored two domains in my system, typing **use recon/domains-hosts/bing_domain_web** will load a module ready to search across both. However, this command alone takes no action. After providing this command, you must type run and strike the enter key. This command checks the Bing search engine for hosts connected to the domains social-engineer.org and cnn.com. The result identified over 70 unique hosts, including the following.

[*] [host] internationaldesk.blogs.cnn.com (<blank>)
[*] [host] crossfire.blogs.cnn.com (<blank>)
[*] [host] reliablesources.blogs.cnn.com (<blank>)
[*] [host] lightyears.blogs.cnn.com (<blank>)
[*] [host] commercial.cnn.com (<blank>)
[*] [host] collection.cnn.com (<blank>)

We can replicate this type of search on Google to make sure that we are not missing any hosts that could be valuable by typing use **recon/domains-hosts/google_site_web**, striking the enter key, typing **run**, and striking the enter key again. This notifies us 35 total (15 new) hosts found, which indicates Bing found more hosts than Google, and Google found 15 hosts that we did not have in our collection from Bing. Since Recon-ng can parse out duplicates, we should have a list of unique hosts with a combined effort from both Google and Bing. Typing show **hosts** will display all of them.

We still have two domains stored in our workspace, but we may want to scan for additional options that we have not considered. There are many top-level domains (TLDs) aside from .com & .org. Executing **use recon/domains-domains/brute_suffix** and then run will scour the various TLDs such as .net, .tv, and others. After completion, typing **show domains** again will display our updated set of target addresses ready for further searching. In this example, we were notified that over 200 additional domains were located, mostly connected to cnn.com. These included numerous foreign versions and options such as cnn.org and cnn.photos. These are all new leads that should be analyzed later. We could now repeat our previous module execution of **use recon/domains-hosts/bing_domain_web** and likely grow our list of hosts substantially**.**

This is a good time to pause and consider what is happening here. As we find data, Recon-ng stores it and applies it to our searches. As those searches reveal more data, that content is added to our workspace. Every time we conduct a new search, or repeat a previous search, all of the

stored data is applied, even the new content found recently. This prevents us from documenting everything that we locate because Recon-ng is keeping good notes for us. This can allow us to collect an amount of data otherwise impossible to manage manually. Let's move on to individual contacts.

Typing **show contacts** will display any contacts stored within the current workspace. You likely do not have any, so let's add some. Typing **use recon/domains-contacts/pgp_search** will use the recon module PGP search feature. It will scan all of the stored domains that we have located and search for any email addresses associated with public PGP keys within those domains. Typing **run** and striking enter executes the process, while submitting **show contacts** afterward displays the results. The following is the partial output with 33 new email addresses identified. Each of these addresses are now stored in your workspace, ready for the next round of research.

rowid	first_name	middle_name	last_name	email
1	Christopher		Hadnagy	logan@social-engineer.org
2	barsuk			barsuk@cnn.com
3	Tristan		Helmich	tristan.helmich@cnn.com
4	Paul	P	Murphy	paul.p.murphy@cnn.com
5	Guy		Incognito	Huzudra@cnn.com
6	bob			hello@cnn.com
7	Jose		Pagliery	Jose.Pagliery@cnn.com
8	D	Ian	Hopper	ian.hopper@cnn.com
9	Scott	John	Anderson	scott.anderson@cnn.com

One of the most powerful email search options available is the Full Contact API. Hopefully, you have already obtained a free trial API key. If not, one can be requested at dashboard.fullcontact.com/register. In my examples, we will replace my actual Full Contact API key with XXX. We can load the Full Contact module by typing **use recon/contacts-profiles/fullcontact and** then run. You should receive an error message since you have not added any API keys to your copy of Recon-ng. At any time, you can type keys list and see any stored keys. Typing **keys add fullcontact_api** XXX will add your key for future use. Executing run again should now make the module function. Recon-ng is now searching all of the stored contacts through the Full Contact database. This will identify associated social networks. After completion, we were notified that 35 new profiles were added to my workspace and 8 new contacts were found. Basically, Recon-ng extracted all information it could from Full Contact and populated our database. The following is a small portion of the details available by typing **show contacts.**

Below is a portion of the social network profiles added to our database. We obtained this by typing **show profiles** and striking enter.

username	resource	url
logan@social-engineer.org	Facebook	https://www.facebook.com/chris.hadnagy
107828765414608142723	GooglePlus	https://plus.google.com/10714608142723
chrishadnagy	Gravatar	https://gravatar.com/chrishadnagy
christopherhadnagy	LinkedIn	linkedin.com/in/christopherhadnagy

Let's reflect on how this can be beneficial. Assume that you are investigating a website. Recon-ng has now identified people associated with the domain; email addresses connected to the people; and social network profiles created by the email accounts. Magnify this by tens or hundreds of subjects, and you have an easy way to replicate several hours of work. In another scenario, you are investigating a list of potential email addresses connected to a case. Entering these into Recon-ng allows you to execute your searches across all accounts. The effort to check one address is the same to check thousands. Now that we have a few profiles in our database, let's find more.

Typing **use recon/profiles-profiles/profiler** and striking enter loads the profiler option. Typing run executes the process which attempts to identify additional online services that possess accounts with the same user name as those in your database. After executing during this example, we typed show profiles which revealed the following partial output. This action added several additional profiles of our target Again, imagine how much time this could save if you had dozens of user names obtained through Recon-ng or added manually.

```
logan@social-engineer.org VideoLike videolike.org/video/logan@social-engineer.org
chrishadnagy              Klout     klout.com/chrishadnagy
chrishadnagy              VideoLike videolike.org/video/chrishadnagy
```

Now that we have several user names of targets in our workspace, we should consider searching within Twitter for any content of interest. We could navigate to Twitter, assume our suspect is chrishadnagy, and look for people mentioning him with to: chrishadnagy. Alternatively, we can ask Recon-ng to conduct this task for every user name we have collected. Typing **use recon/profiles-profiles/twitter_mentions** loads the module and typing run executes the process. You should immediately receive an error since you do not have a valid Twitter API key configured within Recon-ng. The process is identical to the Full Contact requirement, and the following commands will get you started. You can obtain your own Twitter API key and "secret" at apps.twitter.com.

keys add twitter_api xxx

keys add twitter_secret xxx

Repeating the run command executes the process, but nothing was found during this demonstration. Since we know that his Twitter user name is humanhacker, we can type the following to manually add that user name to our database. Note that you will be prompted for each response.

```
add profiles
username (TEXT): humanhacker
resource (TEXT): twitter
url (TEXT): https://twitter.com/humanhacker
category (TEXT): social
notes (TEXT): manual
```

We can replicate the same process for Flickr, but we must first add my Flickr API key, represented by "XXX". The following commands will add your Flickr API key, load the Flickr "pushpin" module; execute the script; and display the pushpins created.

```
keys add flickr_api XXX
use recon/locations-pushpins/flickr
run
show pushpins
```

The output of these commands included thousands of photos posted to Flickr that were geo- tagged within the area of the target location. If you encounter errors stating that your API keys are invalid after entering and running a script, simply exit Recon-ng and relaunch. This is a known bug. Now that we have several pushpins created, let's create the report. The following commands load the reporting module; display the stored location coordinates; set our latitude for the report; set our longitude for the report; define our radius as one kilometer; and execute the process.

```
use reporting/pushpin
show locations
set LATITUDE 41.9474536
set LONGITUDE -87.6561341
set RADIUS 1
run
```

Upon completion, your browser should launch two tabs. The first is a text listing of the Tweets and images located, and the second is an interactive map of the area. Clicking on any pushpin displays the associated details. Figures display the pages created during this demonstration. While an entire book could be written about the possibilities with Recon-ng, let's conduct one last example to illustrate another way to use the program. If you have not already done so, type exit to close the window, then relaunch Recon-ng. The following commands will display your current workspaces; delete the previous example; and create a new space titled email.

```
workspaces list
workspaces delete location
workspaces add email
```

In this example, we want to manually add a contact, and you may want to add several targets. Typing add contacts launches the contact dialogue. The following displays the prompts received and the target details that we entered. Note that all fields are optional.

```
first_name (TEXT): Bart
middle_name (TEXT):
last_name (TEXT): Lorang
email (TEXT): lorangb@gmail.com
title (TEXT):
region (TEXT):
country (TEXT):
```

The following commands display the contacts; load the Have we Been Pwned (HIBP) credential breach module; and execute the script. The response received is identical to what you would see on the HIBP website, and is displayed after the commands below. The power with this method is that you could load hundreds or thousands of email addresses into Recon-ng and execute a search on all of them simultaneously.

```
show contacts
use recon/contacts-credentials/hibp_breach
run

lorangb@gmail.com Seen in the Bitly breach that occurred on 2014-05-08.
lorangb@gmail.com Seen in the Dropbox breach that occurred on 2012-07-01.
lorangb@gmail.com Seen in the LinkedIn breach that occurred on 2012-05-05.
lorangb@gmail.com Seen in the MySpace breach that occurred on 2008-07-01.
lorangb@gmail.com Seen in the tumblr breach that occurred on 2013-02-28.
```

In the Bitly breach that occurred on 2014-05-08. In the Dropbox breach that occurred on 2012-07-01. In the Linkedln breach that occurred on 2012-05-05. In the MySpace breach that occurred on 2008-07-01. In the tumblr breach that occurred on 2013-02-28.

We can take this type of search to another level. Pastebin are often used to store user credentials after they are stolen from online services during illegal breaches. Recon-ng possesses a Paste module which will locate any pastes which contain the target email addresses, and also download the entire paste document to a text file. The following commands load the module and then execute it.

use recon/contacts-credentials/hibp_paste

run

In our example, there were no pastes that included the single email address that we have stored in our contacts. We could add more addresses through the method explained earlier, but that may be overkill for many scenarios. There is an easier way to define an email address as our target and immediately execute a search. The following commands set the source of our search as the generic email address ofbobl2@gmail.com, and re-execute the script. Setting this source tells Recon-ng to ignore the contacts in our database, and only focus on this single address. This type of specification of a single source works well across several modules of the application.

set source bobl2@gmail.com run

The results display the paste files that include this email within them. The raw text files for each identified paste is saved in the "recon-ng" folder within the Home folder on the Buscador desktop. In one of these files, we can see the type of data exposed in these breaches. The following text was copied from one of the raw text files obtained. The content was slightly modified to protect the privacy of these users. The first column depicts the user number within the web service that was compromised; the second column displays the user name; the third column displays an encrypted representation of the users' passwords; and the final column confirms the email address.

9.2 Cree.py (ilektrojohn.github.com/creepy)

In its early years, it was an extremely valuable tool that was launched during almost every Twitter investigation. Today, its power has been crippled by Twitter's strict enforcement of their API limits. However, there is still value here for specific investigations. Creepy is an application created to display a Twitter user's location on a map, or Twitter users that have posted from a specific location.

This is determined by the GPS data stored within a Twitter post This can identify places visited by a target with the date and time that they were present. The program previously allowed searching of any combination of Twitter user names, Instagram user names, Flickr user IDs, or locations. However, it currently only works with Twitter data, as Instagram and Flickr have blocked the application by changing their own API rules.

Before attempting a search, click on "Edit" in the menu and then 'Plugins Configuration". The Twitter plugin will ask you to log into your account and will guide you through the API setup process.

Look for the button tided "Run Configuration Wizard". Create a new project and enter the user name of your target Select the networks that you want to search and click "Search" to find the accounts. Any accounts identified will be displayed below. Click "Add to Targets" to select the accounts desired. Continue this process until you have added any accounts of your target Accept the default options and click "Next" and "Finish" to start the query.

The application will identify posts that contain GPS information from the selected accounts. It will then map out each post on an embedded Google map. The column on the right will display all of the geo-located posts in chronological order. You can double-click any of them to see additional information. The map will change so that the center marker is the location of the chosen message.

The lower right window will display the message and a link to the original source. The latest version will allow you to enter multiple targets from numerous accounts. Each project will automatically be saved within the application and available to you with the next launch. You can right-click any project to delete it. The program allows you to export a project to a standard CSV file or a Google Maps KML file. The KML option allows you to open the analysis within Google Maps.

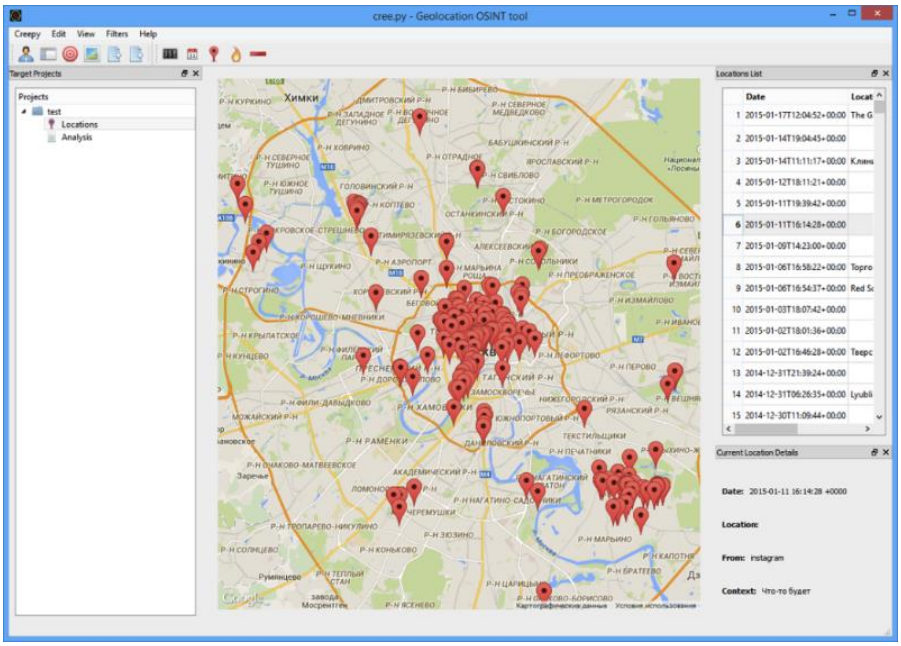


Figure : Cree.py

10. Miscellaneous

10.1 Wireless Recces

➢ WiGLE

WiGLE (or Wireless Geographic Logging Engine) is a website for collecting information about the different wireless hotspots around the world. Users can register on the website and upload hotspot data like GPS coordinates, SSID, MAC address and the encryption type used on the hotspots discovered. In addition, cell tower data is uploaded and displayed**.**

WiGLE is an open source network observation, positioning, and display client from the world's largest queryable database of wireless networks. Can be used for site-survey, security analysis, and competition with your friends. Collect networks for personal research or upload to https://wigle.net. WiGLE has been collecting and mapping network data since 2001, and currently has over 350m networks. WiGLE is *not* a list of networks you can use.

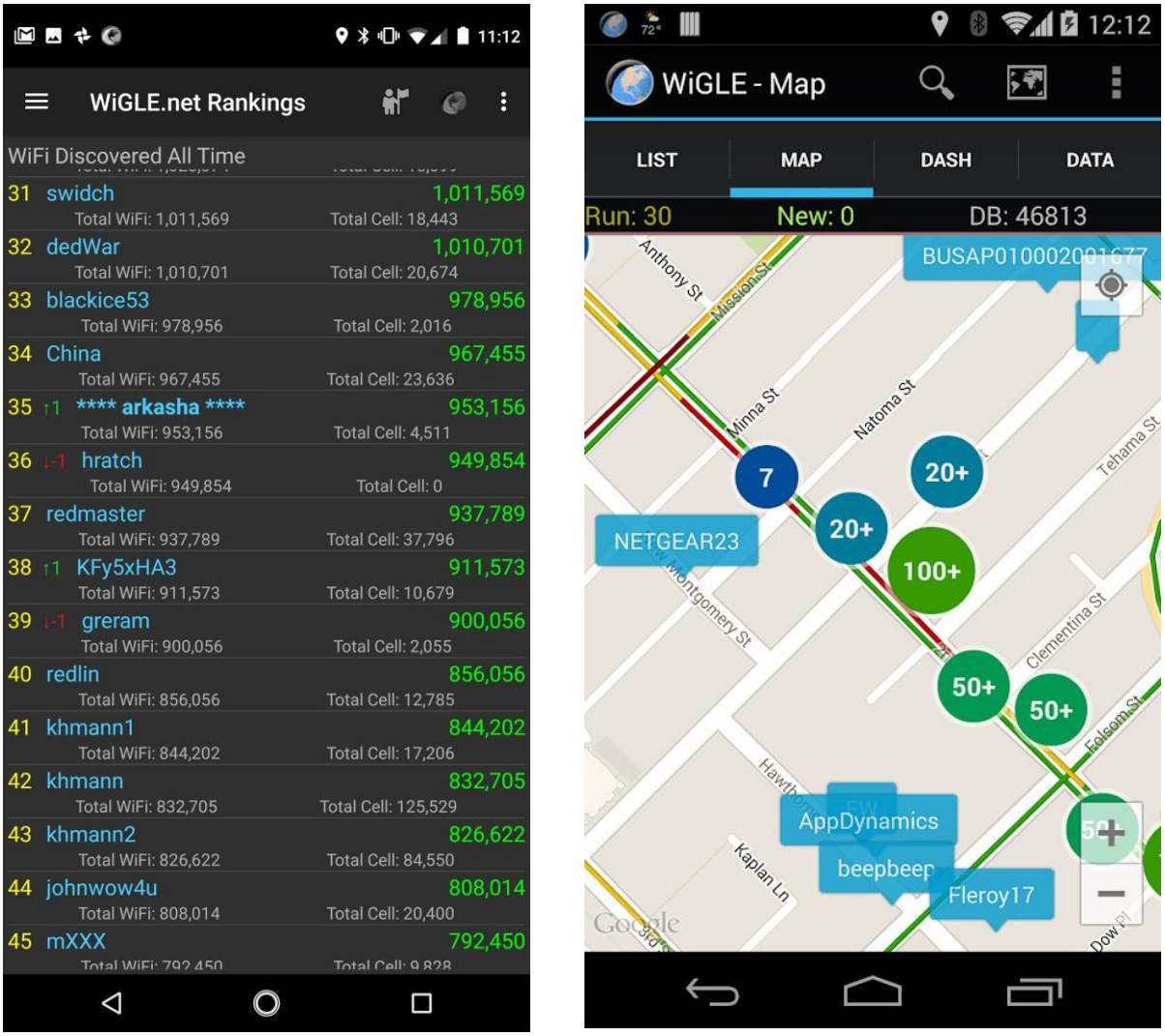


Figure : WiGLE

Features of WiGLE:

- Uses GPS to estimate locations of observed networks

- Observations logged to local database to track your networks found
- Upload and compete on the global WiGLE.net leaderboard
- Real-time map of networks found, with overlays from entire WiGLE dataset
- Free, open source, no ads (pull requests welcome at https://github.com/wiglenet/wigle-wifi-wardriving)
- Export to CSV, KML files on SD card (to import into Google Maps/Earth)
- Bluetooth GPS support through mock locations
- Audio and Text-to-Speech alerting and "Mute" option to shut off all sound/speech

➢ inSSIDer

With inSSIDer you can inspect your Wi-Fi and surrounding networks, scan and filter hundreds of nearby access points, troubleshot the competing access points and clogged Wi-Fi channels and more.

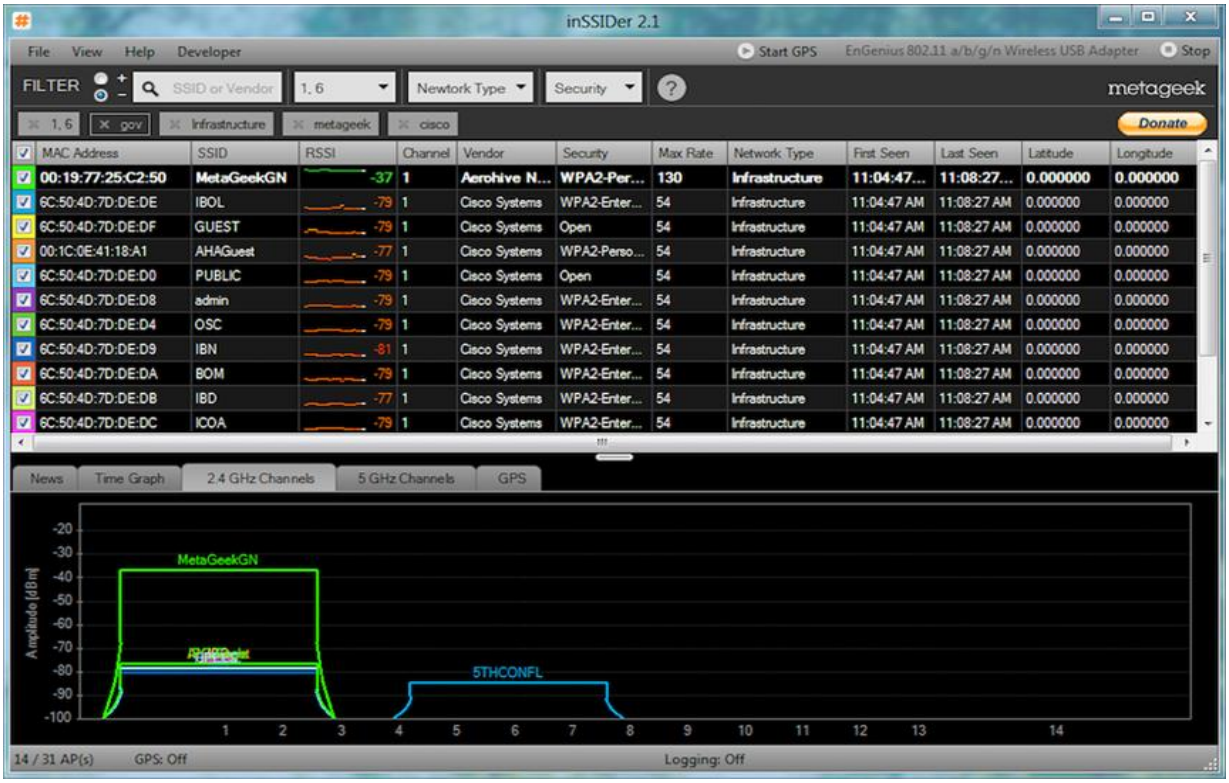


Figure : inSSIDer

Features:

- Inspect your Wi-Fi and surrounding networks
- Scan and filter hundreds of nearby access points
- Troubleshoot competing access points and clogged Wi-Fi channels
- Sort results by MAC Address, SSID, Channel, RSSI, Time Last Seen
- Export Wi-Fi and GPS data to a KML file in Google Earth

10.2 Monitoring websites for keyword

➢ Google Alerts (google.com/alerts)

When you have exhausted the search options on search engines looking for a target, you will want to know if new content is posted. Checking Google results every week on the same target to see if anything new is out there will get mundane. Utilizing Google Alerts will put Google to work on locating new information. While logged into any Google service, such as Gmail, create a new Google Alert and specify the search term, delivery options, and email address to which to send the alert.

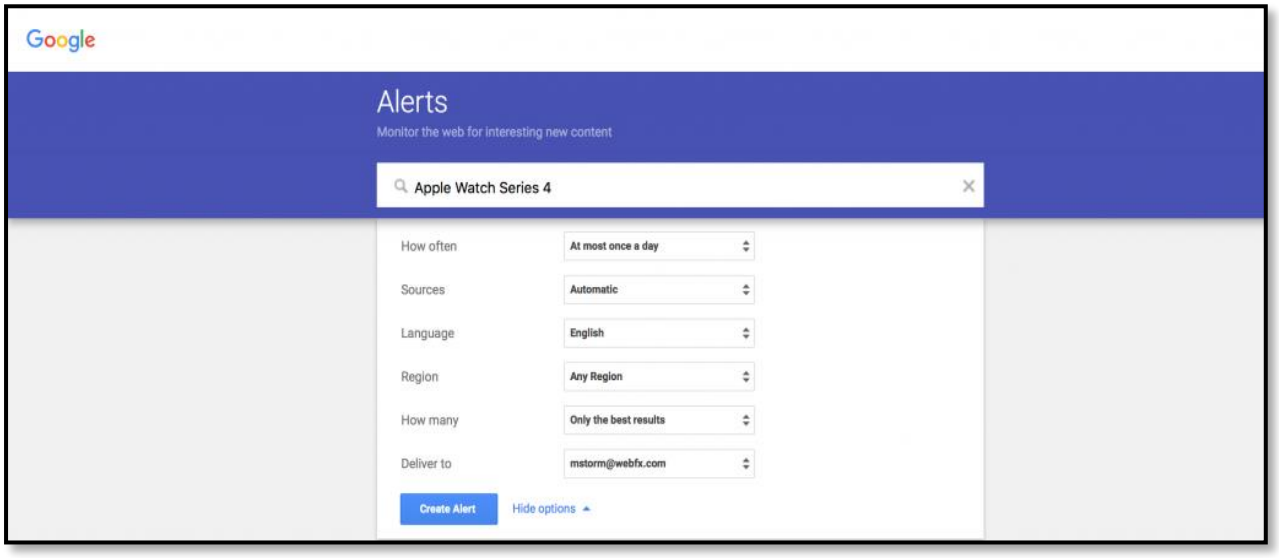


Figure : Goole Alerts

In one of my alerts, Google will send an email daily as it finds new websites that mention “Open Source Intelligence Techniques” anywhere in the site. Another one of my alerts is for my personal website. I now receive an email when another site mentions or links to my website. Parents can use this to be notified if their child is mentioned in a website or blog. Investigators that are continuously seeking information about a target will find this beneficial.

Volume - I

- Overview of Cybercrimes
- Information Gathering
- Crime Scene Management
- IP, Website and E-mail Investigation
- Communication Device Based Investigation
- Investigation of Financial Frauds
- Social Media Investigation
- Windows & Network Forensics

Volume - II

- Mobile Phone Investigation & Forensics
- IPDR and VoIP Investigation
- Cyber Security & Framework

Volume - III

- Disk Forensics
- Operating System Forensics (Windows, Linux & Mac)
- Browser Forensics
- Servers and RAID configuration
- Investigation of Digital Payment Frauds
- Virtual currencies and Crypto currencies
- Open-Source Intelligence

Volume - IV

- Malware and network forensics
- Dark web and cryptocurrency
- Advance Digital Forensics

Volume - V

- Trending Modus Operandi of Cybercrimes
- Acquaintance to Web Server and technology
- Investigation of E-Mails
- Cyber Law and Admissibility of Digital Evidence
- Digital crime Scene management
- Social media Monitoring and Sentiment Analysis
- Dark Web & Cryptocurrency Investigation
- New Technologies (Cloud, Metaverse, IoT) Investigation & Challenges