DiF Notes

Module 1

Digital Forensics Foundations

Digital forensics is the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law.

6 A's Of Digital Forensics

1. Assessment : The process of evidence assessment relates the evidential data to the security incident. There should be a thorough assessment based on the scope of the case.
2. Acquisition : The gathering and recovery of sensitive data during a digital forensic investigation is known as data acquisition. You must acquire evidence without modification or corruption. Do not tamper or spoil or contaminate the original evidence. The most common methods include Bit-stream disk-to-image files, Bit-stream disk-to-disk files and Logical acquisition.
3. Authentication : The examiner must make sure the recovered evidence is the replica or the same as the originally seized data. No forensic evidence recovery is complete without first authenticating it using such tools as MD5 to compare the original evidence with the recovered evidence.
4. Analysis : The data and evidence without any alterations. The forensic investigator’s work is to examine what is on the seized devices and to map relationships with other facts collected to aid the solving of the case. You cannot alter any data as such would be a biased action.
5. Articulation : Refers to the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.
6. Archival : Storage of the digital evidence in archives such that we can retrospectively interpret events represented on digital devices.

Digital Investigations and Computer evidence

Types of computer forensics

- Database forensics. The examination of information contained in databases, both data and related metadata.
- Email forensics. The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.
- Malware forensics. Sifting through code to identify possible malicious programs and analyzing their payload. Such programs may include Trojan horses, ransomware or various viruses.
- Memory forensics. Collecting information stored in a computer's random access memory (RAM) and cache.
- Mobile forensics. The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.
- Network forensics. Looking for evidence by monitoring network traffic, using tools such as a firewall or intrusion detection system.

Chain of custody

The chain of custody in digital cyber forensics is also known as the paper trail or forensic link, or chronological documentation of the evidence.

- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has not tampered.
- CoC demonstrates that the image has been under known possession since the time the image was created.
- Any lapse in the CoC nullifies the legal value of the image, and thus the analysis.
- Any gaps in the procession record like any time the evidence was left unattended in an open space or an unsecured location are problematic.

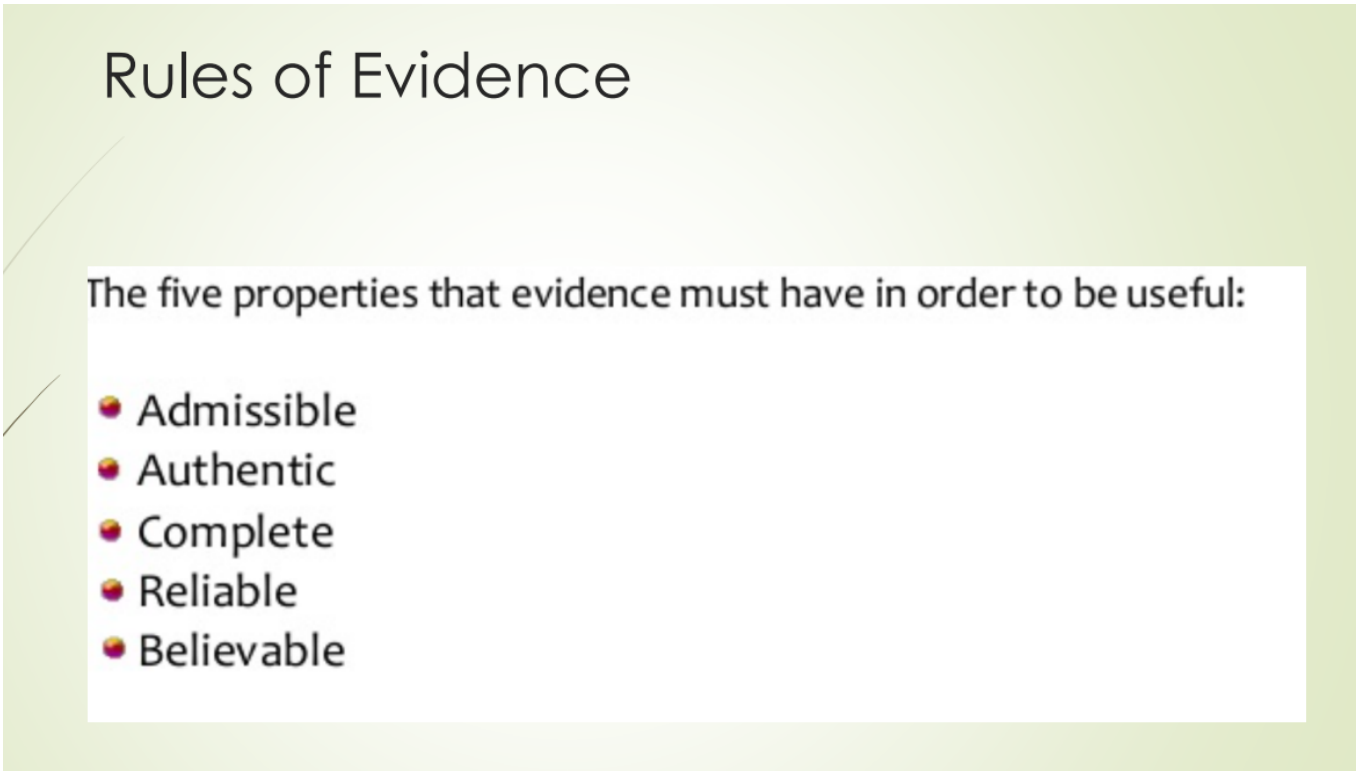
Steps in Preserving Digital Evidence

1. Do not change the current state of the device: If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
2. Power down the device: In the case of mobile phones, If it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping

or data overwriting due to automatic booting.

3. Do not leave the device in an open area or unsecured place: Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
4. Do not plug any external storage media in the device: Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
5. Do not copy anything to or from the device: Copying anything to or from the device will cause changes in the slack space of the memory.
6. Take a picture of the piece of the evidence: Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
7. Make sure you know the PIN/ Password Pattern of the device: It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry their job seamlessly.
8. Do not open anything like pictures, applications, or files on the device: Opening any application, file, or picture on the device may cause losing the data or memory being overwritten.
9. Do not trust anyone without forensics training: Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.
10. Make sure you do not Shut down the computer, If required Hibernate it: Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

Rules of evidence



Location of Evidence

Files Created by Computer Users

Files created by the user include document (e.g., Word; file extensions of either ".doc" or ".docx"), text, spreadsheet (e.g., Excel), image, graphics, audio, and video files. These files contain metadata (i.e., data about data).
Metadata can provide the following kinds of information:
• The name of the author of the document and the company the document belongs to
• The owner of the computer
• The date and time the document was created
• The last time the document was saved and by whom it was saved
• Any revisions made to the document
• The date and time the document was last modified and accessed
• The last time and date the document was printed

Files Protected by Computer Users

There are many different ways a user can protect his or her files:
• An individual can modify files or folders in the computer to look like something else.
• He or she can add a password to the file or folder and/or encrypt it to

ensure that no one will be able to see what is in the file or folder.
• An individual can make the file or folder invisible.
These same tactics are also used by criminals to hide evidence of their crimes.

- Renamed Files and Files with Changed Extensions : Individuals can hide files in plain sight by renaming or changing the file extensions
- Deleted Files : Evidence can be found in files deleted by a computer user; however, deleted files can typically be recovered by investigators. The first thing an investigator should do when searching for a deleted file is to check the Recycle Bin. When a file is deleted, it is moved to the Recycle Bin. More often than not, the files in the Recycle Bin will have been emptied (i.e., deleted) by the offender. When this occurs, any file that has been deleted from the Recycle Bin is removed from the file allocation table.
    - Depending on which Windows operating systems the investigator is dealing with, the file allocation table can be in the FAT, FAT32, or NTFS format.
    - Once a file is removed from the file allocation table, the space where the deleted file resided is marked as free space. In particular, when a file is deleted by the user, the operating system indicates that the space occupied by that file is now available for use by another file. However, the contents of the original file remain in that space until the space is overwritten with new data. Even if a file has been deleted and partially overwritten, it is still possible to recover the file fragment that has not been overwritten.
- Encrypted Files : To protect his or her files, an individual may use encryption to physically block third-party access to them, either by using a password or by rendering the file or aspects of the file unusable. Encryption basically scrambles the data and makes it unreadable. It does so by transforming plaintext into ciphertext, which is essentially gibberish. A decryption key is required to transform the ciphertext back into plaintext.
- Hidden Data: Steganography - Something that needs to be protected from prying eyes can be “camouflaged in sound, pictures, or other routine content in ways analogous to hiding a pebble on a shingle beach.” This technique is known as steganography (information hiding). Steganography seeks to make data and messages invisible by hiding them in various files.
    - To determine if an image contains steganography, an investigator usually makes a visual, side-by-side comparison of the original image and the processed image to identify any differences between them. Unfortunately, computer forensics investigators may not have this luxury; they often have only the processed image available, making visual detection of steganography extremely difficult. To find it,

investigators would basically need to know what they are looking for and in which type of file it is possibly hidden. With steganography, only those individuals with the appropriate software can see the hidden information

Files Created by the Computer

Files that are created by the computer may also have evidentiary value. Files that may assist a computer forensics specialist in his or her investigation include event logs, history files, cookies, temporary files, and spooler files.

- Event Logs : Event logs automatically record events that occur in a computer to provide an audit trail that can be used to monitor, understand, and diagnose activities and problems within the system.
- Application logs : These logs contain the events that are logged by programs and applications. Errors of these applications and programs are also recorded in this log.
- Security logs : These logs record all login attempts (both valid and invalid) and the creation, opening, or deletion of files, programs, or other objects by a computer user.
- Setup logs : These logs provide data on applications that are installed on a computer.
- System logs : These logs provide information on Windows system components. For example, they record any failure of a component to load during the startup process.
- Applications and services logs : These are new event logs in Windows 7. Instead of recording events that may affect the system as a whole, each log stores events from a single application or component.
- History Files
- Cookies: Cookies are files created by websites that are stored on a user's computer hard drive when he or she visits that particular website. As such, by viewing cookies, the investigator can determine which websites the user has visited. Certain cookies are used by websites to gather information about an individual's activities, interests, and preferences. Others are used to store credit card information, usernames, and passwords. Some cookies do both. The type of information an investigator finds depends on the cookies stored on the suspect's computer.
- Temporary Files : Some files are created by the computer unbeknownst to the user. Specifically, the operating system collects and hides certain information from the user.
- Spooler Files : As a default setting, most Microsoft Windows operating systems have print jobs "spool" to the hard drive before they are sent to the printer. Accordingly, a copy of the printed item is stored on the hard drive of the computer. This copy can be recovered and could provide vital evidence in the case under investigation.

Other Data Areas on Computers

- Unallocated space - space available because it was never used or because the information in it was deleted—may also contain important evidence of a crime or incident. Evidence may also be found in hidden partitions, bad clusters, and slack space.
- Hidden Partitions: Individuals may choose to hide drives or files when they share computers with others, especially if these files hold confidential and sensitive data (e.g., Social Security numbers, bank information, credit card data). It is a quite simple and easy way to hide data. Criminals, however, also use the hidden partition technique to hide evidence of their crimes.
- Slack Space and Bad Clusters: Certain programs (e.g., Slacker) exist that can help users hide files from computer forensics investigators in slack space. Specifically, the program breaks up the file that a user wants hidden and places parts of that file into the slack space of other files. Other areas of the computer that investigators should look at are clusters— that is, areas of the operating system where data are stored. In particular, bad clusters, which are not accessed and thus overlooked by the operating systems, should be examined. Criminals have been known to mark clusters as bad and hide data in them.

Incident Response and computer forensics

Incident Response Plan

1. Preparation : This stage is where the team develops the formal incident response capability; where they create an incident response process defining the organizational structure with roles and responsibilities; where they create procedures with detailed guidance in order to respond to an incident; where they select the right people with the appropriate skill set; where they define the criteria to declare an incident; where they define the right tools to handle an incident; where the team defines what they are going to report; and to whom is the team going to communicate.
2. Identification: This step is where the team verifies if an occasion has occurred, supported events observation, indicators, and search for deviations from traditional operations and for malicious acts or tries to and do damage. The protection mechanism in place can facilitate the team doing the identification. Incident handler team will use their experience to look at the signs and indicators. The observation might occur at network, host, or system level. It is where the team leverages the alerts and logs from routers, firewalls, IDS, SIEM, AV gateways, operating system, network

flows, and more. When distinguishing an occasion, the team is compelled to assess the impact and notify the suitable people or external parties. If there are reasons to believe that the team will engage law enforcement, it is where the team ensures chain of custody.

3. Containment: This stage consists of limiting the injury. Stop the bleeding. Stop the offenders/ attackers. It is where the team makes decisions on which strategy it will use to contain the incident bases on processes and procedures. It is where the team interacts with the home-based business owners and judges to finish off the system or disconnect the network or continue operations and monitor the activity. All depends on the scope, magnitude, and impact of the incident.
4. Eradication: After the success contained the incident, successive steps involve eliminating the reason for the incident. Within the case of a deadly disease incident, the demand is for eradicating the virus. On different complicated incident cases, the team would possibly have to be compelled to acknowledge and diminish ill-used susceptibilities. It's on this step that the team should determine how it was initially executed and apply the necessary measures to ensure it doesn't happen again.
5. Recovery: In this phase, restoring of a backup or reimaging of a system takes place. After successful restoration, it is very important to monitor it for a certain time period. Monitoring is important because the team wants to potentially identify signs that evaded detection.
6. Lessons learned: Follow-up activity is crucial. It is where the team can reflect and document what happened; where they can learn what failed and what worked; where the team identifies improvements for incident handling processes and procedures; where they write the final report.

Order of Volatility

When collecting evidence, you should always try to proceed from the most volatile to the least.
To determine what evidence to collect first, you should draw up an order of volatility—a list of evidence sources ordered by relative volatility.
An example an order of volatility would be:

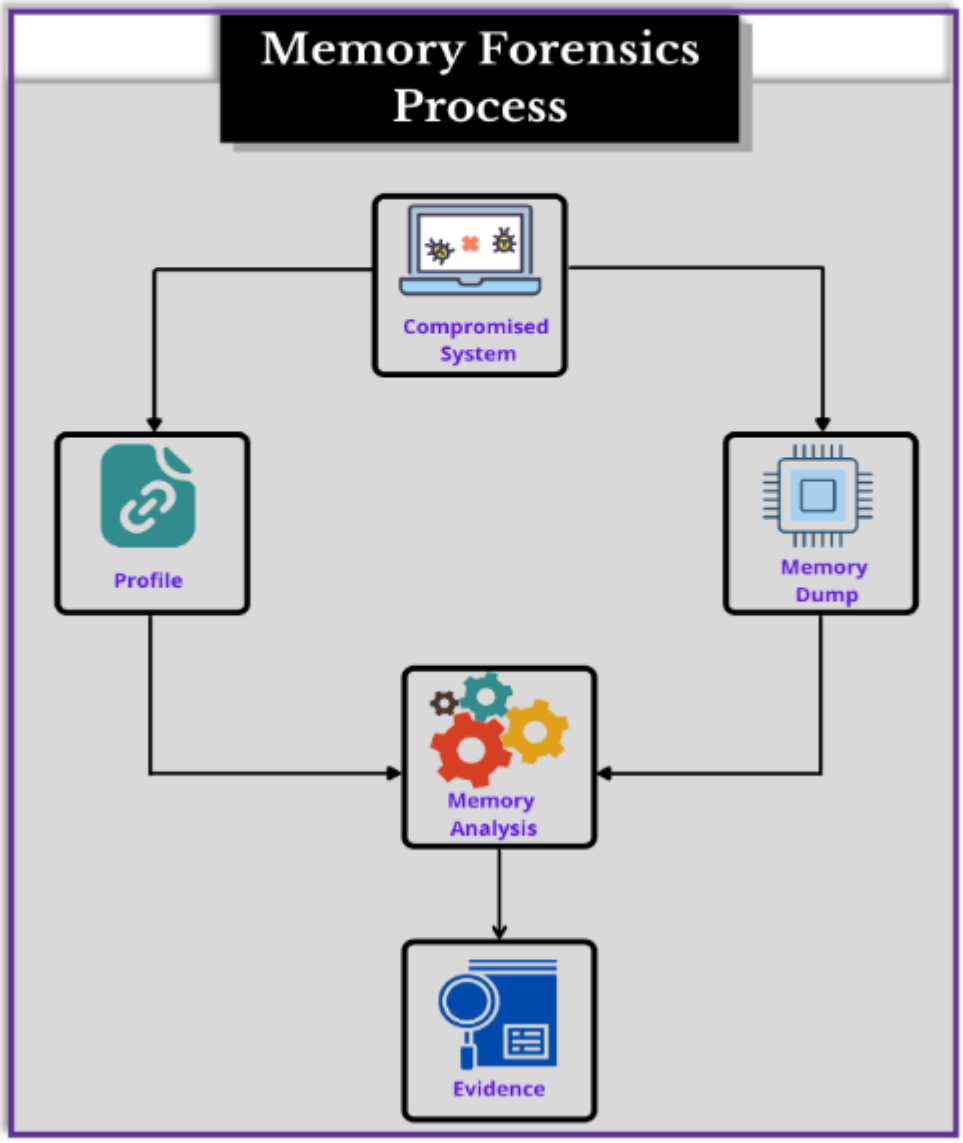
1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules

6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology

Memory Forensics

Memory Forensics

Memory Forensics is a budding field in Digital Forensics Investigation which involves recovering, extracting and analysing evidence such as images, documents, or chat histories etc from the structured volatile memory into non-volatile devices like Hard-drives or USB drives.



Memory Acquisition

- It is the method of capturing and dumping the contents of a volatile content into a non-volatile storage device to preserve it for further investigation.
- A ram analysis can only be successfully conducted when the acquisition has been performed accurately without corrupting the image of the volatile memory.
- In this phase, the investigator has to be careful about his decisions to collect the volatile data as it won't exist after the system undergoes a reboot.
- The volatile memory can also be prone to alteration of any sort due to the continuous processes running in the background.

> processes running in the background.
> - Any external move made on the suspect system may impact the device's ram adversely.

Memory Analysis

> Once the dump is available, we will begin with the forensic analysis of the memory using the Volatility Memory Forensics Framework which can be downloaded from here. The volatility framework support analysis of memory dump from all the versions and services of Windows from XP to Windows 10. It also supports Server 2003 to Server 2016. In this article, we will be analysing the memory dump in Kali Linux where Volatility comes pre-installed.

- Basic Volatility commands:
  - Typical command components: `#vol.py -f[image] --profile=[profile] [plugin]`
  - Display profiles,address spaces, plugins: `#vol.py --info`
  - imginfo : Info about image OS and architecture.
  - pslist : Basic process listings
  - psscane : Scan for hidden processes

IT Law

Indian Evidence Act 1872

The Indian Evidence Act contains rules and relevant issues regarding admissibility of evidence in courts of law in India.

- As per the Act, Evidence includes all documents including electronic records produced for the inspection of the Court. Such evidence is known as documentary evidence.
- Section 65 B of the Act deals with admissibility of Electronic records as Evidence. (It was inserted by Information Technology Act 2000)

Module 2

Image capturing and Information Extraction from Data

Imaging Process

Imaging is the process by which a duplicate copy of the entire hard drive is created. Once an exact copy of a suspect's hard drive has been made, the investigator must verify that it is an exact copy. An investigator verifies this by computing an MD5 hash algorithm for both the original hard drive and the copy. If the MD5 values are exactly the same, then the copy is an exact copy of the original drive. Hashing using the MD5 or SHA hash algorithm has a standard of certainty even higher than that of DNA evidence. Indeed, it has been validated by many courts.

According to NIST, the computer forensics tools that an investigator uses must meet the following requirements:

- Make a bitstream duplicate or an image of an original disk or partition
- Not alter the original disk in any way
- Log input and output errors and offer a resolution to fix such errors
- Keep correct documentation

Types of Images

Most IR teams will create and process three primary types of forensic images: complete disk, partition, and logical.

1. Complete Disk Image: The process for obtaining a "complete disk image" is intended to duplicate every addressable allocation unit on the storage medium.
2. Partition Image: Most forensic imaging tools allow you specify an individual partition, or volume, as the source for an image. A partition image is a subset of a complete disk image and contains all of the allocation units from an individual partition on a drive. This includes the unallocated space and file slack present within that partition.
3. Logical Image A logical image is less of an "image" and more of a simple copy, and it's the type of duplication we referred to previously as a "simple duplication." Although logical copies are typically the last resort and make most examiners cringe when they hear one is inbound, there are solid reasons why they are the duplication of choice.

Digital Forensic Imaging Methods

1. Copy and Paste Method
   A standard copy and paste process isn't the same as the processes used to carry out forensic imaging (copies). When a copy and paste is done from one hard drive to another, what's being copied are just the files visible to the user. All other additional

data that the hard drive uses to locate and access the hidden files is missing. Data such as file allocation tables (FAT) and the master boot records aren't copied. As such, if the seemingly duplicate drive created is used as a replacement to the original, the system won't boot and will be non-functional.

2. Disk Cloning Method
   Disk cloning creates a copy of the original drive and includes all the information that will enable the duplicate (cloned) drive to boot the operating system, accessing all the files as if it were the original. The disk cloning process creates what is known as a one-to-one copy. This duplicate is fully functional and in the event that it's swapped to replace the original drive, will work just like the original. The computer, when booted using the cloned drive, has its operations and data identical to the original drive.
3. Disk Imaging Method
   Disk Imaging is the process of copying a hard drive as a backup copy or an archive. The process entails copying all the data stored on the source drive, including data like the master boot record and table allocation information. This image, however, is a single file that can be stored in any storage device and not necessarily an identical hard drive. In the event that a restoration is necessary, the image will have to be applied to the hard drive. Unlike the cloned drive, system restore isn't possible by just copying the image file on the hard drive. A software imaging program will have to be employed to install and open the image on the hard drive. The backup device can therefore be used to store multiple image files, unlike the cloned drive where only a single clone can be stored on the duplicate drive.

Partial Volume Image

With the advent of inexpensive storage, the ability to store large amounts of data and information has become common. A 200GB hard drive is no longer expensive. Larger hard drives and more storage space can cause issues for an investigator who might be working onsite or during emergency cases. Although some utilities include newer technology that speeds up the imaging process, there are times when a full volume image simply isn't possible. Such times might include situations in which data is stored on a mainframe computer. Remember that full imaging will copy each sector of the original media, including hidden data, partially erased data, encrypted data, and unused space. A full image copy also takes longer to make, and it will use more space. The full imaging process is less bandwidth-efficient than partial imaging.

Working with Virtual Machines

In their many forms, virtual systems provide the same functionality as physical computers, OSs, applications, hardware, and software but without the possibility of failure. Why? Because all of their abilities—from booting up to shutting down—are just an imitation of what a real, tangible machine or system would do. And as such, they offer a tremendous opportunity for users to beat up different OSs, play around with suspicious applications, or hook up peripheral devices like USB flash drives without fear of negative consequences. If a problem comes up like a virus or a mismanagement of the network, a virtual system will behave just as a real system would. And as a result, they are the perfect tool for information security experimentation because they allow the user complete freedom to make mistakes, much like a child in a sandbox.

Virtualization is key to forensic investigations because it allows authorities to view the digital environment in exactly the same way the suspect did. Although this may not be appropriate for every situation, an intruder who compromises a virtual system can likely compromise the host machine as well.

There are two common types of investigative analysis involved in digital forensics: *live and dead*. The former happens while a machine is running and often focuses on things like open files, running processes, network connections, and volatile malware. In many cases, systems need to continue running for as long as possible to provide the insight authorities need to find evidence. Dead analysis, on the other hand, occurs while the machine is turned off and an identical image of the machine's storage media is created and analyzed for relevant findings. This reduces the possibility of source contamination and makes investigating static data from a system easier.

Tools

Forensic Toolkit

Forensic Toolkit (FTK) is a product sold by Access-Data. This software has many capabilities, including the ability to create images of hard drives, analyze the registry, scan slack space for file fragments, inspect emails, and identify steganography. Unlike other computer forensics tools on the market, FTK can crack passwords. This tool can also be used to decrypt files.

Encase

Encase is a computer forensics tool that is widely used by law enforcement agencies. It allows the user to create an image of a drive without altering its contents and calculates the hash value for further authentication. It can locate hidden drives or partitions within a drive, as well as other hidden files or media that some other programs would not be able

to discover. Encase can search multiple file locations and devices simultaneously. In doing so, it creates an index of what is found on the computer, such as emails and deleted files.

ILook

ILook is another tool that is used to forensically examine computer media. Its capabilities include imaging, advanced email analysis, and data salvaging (to recover files that have been deleted by the user). It is not available to the general public, but rather is provided to law enforcement agencies, government intelligence agencies, military agencies, and government, state, and other regulatory agencies with law enforcement missions.

E-fense Helix and Live Response

E-fense offers cybersecurity and computer forensics software such as Helix3Pro and Live Response. E-fense Helix3Pro software can be used on multiple operating systems (Windows, Macintosh, and Linux). This tool is carefully designed to ensure that data is not altered during the imaging process.
E-fense Live Response is a Universal Serial Bus (USB) key that is designed to be used by first responders, investigators, information technology professionals, and security professionals to collect nonvolatile and volatile data (which will be lost if the computer is shut down) from live running systems.

Extracting Information from Data

Windows File systems

1. FAT - A type of file allocation table that is used in the Windows 3.1, 95, 98, and ME operating systems. It consists of a boot sector, a file allocation table, and plain storage space to store files and folders.
2. FAT32 - A type of file allocation table that is used in the Windows 3.1, 95, 98, and ME operating systems.
3. NTFS - New Technology File System; the file allocation table used in the Windows NT, 2000, XP, 2003, 2008, Vista, and 7 operating systems. This file system supports many file properties, including encryption and access control.

Hidden Evidence

1. Deleted Files and Slack space: Recently deleted files leave slack space. The files are still there, but the area is marked unallocated. Those unallocated sectors are eventually overwritten, permanently “deleting” prior data in the sector.

2. Hiding data in HPA on disk : Host Protected Areas on disks are not visible to the operating system. Boot diagnostics, BIOS support, and other manufacturer tools are generally loaded there in the host protected area. Rootkits can write to that space, which makes them difficult to detect because the operating system and anti-virus cannot see those rootkits either.
3. Hiding data by marking sectors that contain data as “bad” and therefore unreadable by end user software
   This process forces the operating system to think a sector is bad, and therefore it will ignore it. It requires creating bad blocks on the file system where data is logically located to “hide” it. This is generally reversible by unmarking bad blocks and making them visible to the operating system.

Trace Evidence

Trace Evidence Analysis is the discipline of forensic science that deals with the minute transfers of materials that cannot be seen with the unaided eye. The handling and analysis of trace evidence requires care and specialized techniques.

Sniffer logs, malware Dlls, Open TCP ports etc are examples of trace evidence left behind by the intruder.

Registry Analysis

In early versions of Windows, specific system files used to stored information in directories consisting information about default or user customized application, security or software settings. Later, user settings and other relevant information were systematically encapsulated to a structured format known as the Windows Registry.

The Registry is a hierarchical database that stores low-level settings and other information for the Microsoft Windows Operating System and for applications that pick to utilize the registry. From the point of installation of operating system, registries are used. Kernel, Device Driver settings to the Hardware and User Interface all settings are stored in the windows registry.

For a Forensic analyst, the Registry is a treasure box of information. It is the database that contains the default settings, user, and system defined settings in windows computer. Registry serves as repository, monitoring, observing and recording the activities performed by the user in the computer. The Data is stored in the main folders in a Tree like structure which is called Hive and its subfolders are called KEYS and SUBKEYS where each component’s configuration is stored called VALUES.

Imp points about the Registry :

1. Original files that contain registry values are stored in the system directory itself.
2. Registry files are system protected and can not be accessed by any user unless administration access is provided.
3. For the investigation purpose, the forensic investigator analyzes registry files via tools such as Registry Viewer, Regshot, Registry Browser etc..
4. Trojans and Malware information can be found in the registries.

Registry Structure

Registry appears in a tree-like structure with five root folders, or “hives”.

1. HKEY_CLASSES_ROOT hive contains configuration information relating to which application is used to open various files on the system.
2. HKEY_CURRENT_USER − loaded user profile for the currently logged-on-user.
3. HKEY_LOCAL_MACHINE−contains a vast configuration information for the system, including hardware settings and software settings.
4. HKEY_USERS− contains all the actively loaded user profile for that system
5. HKEY_CURRENT_CONFIG−contains the hardware profile the system uses at startup.

Registry Forensics

You can track activity through inspecting the registry as follows −

1. Most Recent User list
   `(HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Explorer\RunMRU)`
   It contains with the information provided from the RunMRU key, an examiner can gain better understanding fo the user they are investigating and the application that is being used. In this above figure, you can see the user has opened cmd, Notepad, MSPaint etc.
2. USB Connection
   `(HKEY_LOCAL_MACHINE\SYSTEM\controlset001\Enum\USBSTOR.)`
   This key stores the contents of the product and device ID values of any USB devices that have ever been connected to the system.
3. Attached Hardware List − `( HKEY_LOCAL_MACHINE\SYSTEM|MountedDevices.)`
   This information can be useful to a forensic examiner as it shows any connected storage device has been recognized by the operating system. If the examiner notes a discrepancy between the physically attached devices and the ones reported here, it

can be an indication that some device was removed prior to the evidence being seized.

4. Malicious Software Running – `(HKEY_CURRENT_USER\Software\ )`
   This information will be quite informatic for Forensics Examiner as it could see the hacker used VPN such as CyberGhost which is used for being anonymous.
5. Recent Applications Used–
   `(HKEY_CURRENT_USER\SOFTWARE\Microsoft\Currentversion\Search\RecentApps)`
   By navigating to the said key will give information for last accessed applications list by the user.
6. Internet Explorer information
   `(HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs.)`
   Internet Explorer is the native Web browser in Windows operating system. It utilizes the Registry extensively in the storage of data, like many applications. From the said key, we can obtain such information.

File Carving

It is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originality created the file. It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation. It also called “carving,” which is a general term for extracting structured data out of raw data, based on format specific characteristics present in the structured data.
File carving is most often used to recover files from the unallocated space in a drive. Unallocated space refers to the area of the drive which no longer holds any file information as indicated by the file system structures like the file table. File carving is the process of reconstructing files by scanning the raw bytes of the disk and reassembling them. This is usually done by examining the header (the first few bytes) and footer (the last few bytes) of a file.
File carving is a great method for recovering files and fragments of files when directory entries are corrupt or missing.

File Carving Techniques:

1. Header-footer or header-“maximum file size” carving:
   Recover files based on known headers and footers or maximum file size
   If the file format has no footer, a maximum file size is used in the carving program, eg JPEG—”xFFxD8” header and “xFFxD9” footer
   PST—”!BDN” header and no footer

2. File structure-based carving
   This technique uses the internal layout of a file
   Elements are header, footer, identifier strings, and size information
3. Content-based carving
   Recovers files by analysing the contents of the scan area. The carving process includes identification, validation, and reassembling the fragmented portions of the files.

Internet Artifacts

Browser artifacts

1. Internet Explorer:
   IE has two primary areas where data of primary interest
   to forensic analysts are stored: in the index.dat "database" used by the Web browser and in the browser cache.
   - Index.dat :
     The index.dat file contains a record of accessed URLs, including search queries, Web mail accesses, and so on, and is often considered the primary source of forensic information when it comes to IE Web browser analysis. Various open source tools can be used to access and parse the contents of the index. dat file into a readable format. Perhaps one of the most well-known open source tools for parsing index.dat files is pasco from FoundStone.
   - Cookies, Favorites Cache :The browser's cache contains files that are cached locally on the system as a result of a user's Web browsing activity.
2. Chrome:
   Like Firefox, Chrome utilizes a variety of SQLite databases to store user data. We can access these data using any SQLite client, but will use the base command line sqlite3 program for most cases. "Cookies" is the SQLite database Chrome uses to store all cookies. Information stored in this database includes the creation time of the cookie, the last access time of the cookie, and the host the cookie is issued for.
   The "History" SQLite database contains the majority of user activity data of interest, divided among numerous tables.

Mail Artifacts:

1. PST:
   PST is the mail storage format used by Microsoft's Outlook email client. The PST file

provides a data storage format for storing emails on the user's computer system. Users of OutLook email clients may also have an OST file, which is for offline storage of email.

2. mbox and maildir:
   mbox and maildir are the two primary local mail storage formats used by Linux email clients. These formats are also supported by cross-platform mail clients, especially those with Unix. The older mbox format consists of a single flat file, containing numerous email entries, whereas the maildir format stores each email as a discreet file in a set of subdirectories.
   Because both of these formats are plain text, searching for specific key words quickly can be performed without the need for a dedicated email forensics utility.

Password Cracking

User and passwords in a windows system are stored in either of two places:
a) SAM(Security Account Manager)
The Security Account Manager (SAM) is a database file in Windows XP, Windows Vista and Windows 7 that stores users' passwords. It can be used to authenticate local and remote users. The SAM file cannot be moved or copied while Windows is running, since the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file, and will not release that lock until the operating system has shut down or a "Blue Screen of Death" exception has been thrown. However, the in-memory copy of the contents of the SAM can be dumped using various techniques (including pwdump), making the password hashes available for offline brute-force attack.

b) AD(Activity directory)
Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.

A password cracker recovers passwords using various techniques. The process can involve comparing a list of words to guess passwords or the use of an algorithm to repeatedly guess the password.

Techniques

1. Brute force: This attack runs through combinations of characters of a predetermined length until it finds the combination that matches the password.

2. Dictionary search: Here, a password cracker searches each word in the dictionary for the correct password. Password dictionaries exist for a variety of topics and combinations of topics, including politics, movies and music groups.
3. Malwares : Malware such as keyloggers, which track keystrokes, or screen scrapers, which take screenshots, are used instead.
4. Rainbow attack. This approach involves using different words from the original password in order to generate other possible passwords. Malicious actors can keep a list called a rainbow table with them. This list contains leaked and previously cracked passwords, which will make the overall password cracking method more effective.

Tools

1. Hashcat
   Hashcat is a password cracking tool used for **licit and illicit purposes**. Hashat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying
2. John the Ripper
   John the Ripper works by using the dictionary method favored by attackers as the easiest way to guess a password. It takes text string samples from a word list using common dictionary words or common passwords. It can also deal with encrypted passwords, and address online and offline attacks.
3. Brutus
   Brutus is a password cracking tool that can perform both dictionary attacks and brute force attacks where passwords are randomly generated from a given character. Brutus can crack the multiple authentication types, HTTP (Basic authentication, HTML Form/CGI), POP3, FTP, SMB and Telnet.
4. THC Hydra
   The tool is commonly used for fast network login hacking. It uses both dictionary and brute-force attacks to attack login pages. Brute-force attacks may raise alarms on the target's side if there are some security tools put in place, and thus hackers are extremely careful with the use of the tool.
5. RainbowCrack
   RainbowCrack is a computer program which generates rainbow tables to be used in password cracking. RainbowCrack differs from "conventional" brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password drastically.
6. Cain and Abel
   This password recovery software can recover passwords for Microsoft Windows user

accounts and Microsoft Access passwords. Cain and Abel uses a graphical user interface, making it more user-friendly than comparable tools. The software uses dictionary lists and brute-force attack methods.

7. Ophcrack
   This password cracker uses rainbow tables and brute-force attacks to crack passwords. It runs on Windows, macOS and Linux.

Encryption and Bit-locker

1. Software Encryption:
   Process of keeping data safe using the software. In this, the software is generally installed in the host computer that encrypts and decrypts data. It is more cost-effective for smaller companies. In this, the password is the key that one needs to have access to data. It usually shares processing resources with all other programs or processes on the system that might have an impact on the performance of all other functions of the system.
   Examples: LastPass, BitLocker, VeraCrypt, DiskCryptor, etc., are some software encryption tools that are best to use to keep valuable data safe and secure.
2. Hardware Encryption:
   Process of keeping data safe using a dedicated and separate processor. It is more cost-effective for larger companies because it does not require any additional software installation. In this, password, biometrics such as fingerprints can be used to have access to data. It provides much greater throughput capacity and speed in a large-scale environment. It also includes faster algorithm processing, tamper-proof or tamper-resistant key storage, and protection against unauthorized code.
   Examples: Wireless access point or wireless base station, Credit card point-of-sale-device, network bulk encrypts, etc.
3. Hybrid Encryption:
   The final type of encryption is a hybrid software/hardware encryption such as Windows BitLocker. The hybrid encryption uses software to encrypt but can be tied to a specific hardware configuration as well.
   Hardware and hybrid encryption techniques make use of a TPM (Trusted Platform Module) chip, which can tie a machine‟s hard drive, at a hardware level, to the TPM chip on the motherboard.

BitLocker helps prevent unauthorized access to data on lost or stolen computers by a combination of protection methods. Primary methods that are used: Encrypting the Windows operating system volume on the hard drive and verification of boot components

and configuration data. BitLocker can be used with or without a TPM chip. However, a BitLocker enabled system without a TPM chip is limited to only encrypting the Windows operating system volume. The system cannot perform verification of any boot components, as a TPM chip is required to compute and safely store such measurements.

Forensics Acquisition Tools

Disk analysis: Autopsy/the Sleuth Kit

Autopsy and the Sleuth Kit are likely the most well-known forensics toolkits in existence. The Sleuth Kit is a command-line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI-based system that uses The Sleuth Kit behind the scenes.
The tools are designed with a modular and plug-in architecture that makes it possible for users to easily incorporate additional functionality. Both tools are free and open-source, but commercial support and training are available as well.

Image creation: FTK imager

Autopsy and The Sleuth Kit are designed to examine disk images of hard drives, smart phones and so on. The benefit of analyzing an image (rather than a live drive) is that the use of an image allows the investigator to prove that they have not made any modifications to the drive that could affect the forensic results.
Autopsy does not have image creation functionality, so another tool needs to be used. While the majority of the AccessData Forensics Toolkit items are paid tools, its FTK Imager is a free product. This can be used to create disk images that can then be analyzed using Autopsy/The Sleuth Kit.

Memory forensics: volatility

Tools like The Sleuth Kit focus on the hard drive, but this is not the only place where forensic data and artifacts can be stored on a machine. Important forensic information can be stored in RAM, and this volatile memory must be collected quickly and carefully to be forensically valid and useful.
Volatility is the most well-known and popular tool for analysis of volatile memory. Like The Sleuth Kit, Volatility is free, open-source and supports third-party plugins. In fact, the Volatility Foundation holds an annual contest for users to develop the most useful and innovative extension to the framework.

Module 3

Network Forensics

Stand-Alone Versus Networked Devices

- Stand-alone computer:
  - A computer that is not connected to another computer or network.
  - More secure than those connected to a network, because they are less prone to attacks by malicious software.
- Networked computer:
  - A computer that is connected to one or more computers in a manner that allows them to share data, software, and hardware.
  - Networked computers are more vulnerable to attacks by hackers and malicious software.

Computer Networks

Types of Computer Networks

- LAN (Local area network):
  - The simplest type of computer network, which connects computers within a small area and provides these systems with the ability to share resources.
  - normally used to connect computer systems within a building.
- WAN (Wide area network):
  - A network that connects computers in different locations.
- MAN (Metropolitan area network):
  - A network that is restricted to a particular city or town.
- CAN (Campus area network):
  - A computer network that connects computer systems in a particular area.

Network Configuration

- Peer-to-peer networking configuration:
  - A network in which each peer (or computer) manages authentication and access to its own resources.
- Server-based network configuration:

- A network in which different servers manage authentication and access to resources from a database (directory).
- Network administrator:
  - The individual responsible for managing a server-based network.
- Access control systems:
  - Systems used to restrict access to protectednetwork resources.
- Access control list:
  - Rules that define network security policies and govern the rights and privileges of users of a specific system.

Network Forensics

- The use of scientifically proven techniques to investigate computer networks.
- Network forensics seeks to capture, analyze, and preserve network traffic (i.e., data in a network).
  - This traffic consists of packets, units of data transmitted over the network.
  - Each packet contains a header and a body.
    - The header is located at the beginning of the packet and includes information on the source address, destination address, total number of packets, and the specific packet's position within a sequence of packets (e.g., packet 1 of 3).
    - The body includes the content (i.e., data) that the packet is delivering.
- To put it briefly, network forensics is about monitoring. It checks the network for any anomalies (or malicious activity). If such anomalies are detected, it tries to determine the nature of the attack or intrusion within legal and/or corporate policy constraints.

Network Components

- MAC address:
  - A media access control (MAC) address is a unique identifier that is used to connect to the network.
  - Associated with a particular network interface card (NIC) or network adapter.
  - Used to identify the NIC or adapter on LANs.
  - Consists of a 12-digit hexadecimal number.
  - Although MAC addresses can be retrieved from the Address Resolution Protocol (ARP) table, they can easily be changed by software. The NIC can also be easily removed and replaced.

- How Do You Find the MAC Address of a Computer?
    1. Click on the Start menu.
    2. Type “cmd” in the Run text box.
    3. Once in the command prompt window, type “ipconfig/all”.
    - Other information that can be retrieved from this utility includes the IP address of the computer user and the Domain Name System (DNS) server that the particular computer is using.
- Network interface card:
    - A network interface card is a device that is installed in or attached to a computer system, which enables the computer to transmit and receive data on a network.
- Address Resolution Protocol (ARP):
    - It is a protocol that is used to map an IP address to the unique physical address of a computer - the MAC address.
- Hub:
    - A device that connects computers and sends data (packets) between the networked computers through all of its ports.
- Switch:
    - A more efficient and intelligent version of a hub that sends each packet only to the port that it is supposed to travel through
- Router:
    - A device that connects two networks and routes data between them.

Attacks on Network Components

- MAC Address Spoofing:
    - A type of computer attack in which the offender poses as an approved network device.
    - An offender spoofs a MAC address.
    - Routers deal exclusively with IP addresses and, as such, are unaffected by MAC address spoofing.
    - The same cannot be said about switches, as they deal solely with MAC addresses.
- ARP poisoning:
    - A type of attack in which the offender causes the network devices to update their ARP tables with false information so that the offender could redirect traffic and launch attacks.

    - An offender sends a poisoned ARP packet, which contains an IP address and a request for a MAC address for the corresponding IP address. If the network device has the IP address assigned to it, it sends its MAC address in response to the request. The poisoned ARP request causes the network devices to update their ARP tables with the false information, which “poisons” them.
- MAC flooding:
    - A type of computer attack in which numerous ARP requests are sent requesting multiple MAC addresses, which eventually overwhelms the resources of network switches.
    - As a result, switches enter fail-open mode, which causes them to function as hubs and send the incoming traffic through all their ports.
- Man-in-the-Middle Attack:
    - A type of computer attack in which the offender hijacks a TCP connection between a client and a server, and eavesdrops on their communication.

Where Can Network-Related Evidence Be Found?

- The type of evidence that can be retrieved from networks includes full content data (i.e., the entire contents of packets) and session data (i.e., traffic data).
- File server:
    - A computer that handles requests from other computers on the network for data that are stored on one or more of the server’s hard drives.
    - File servers hold the data that all the computers on the network can use. In addition, they may contain logs of emails, instant messages, and Internet activities.
- Dynamic Host Configuration Protocol (DHCP):
    - A protocol that allows a server to dynamically assign IP addresses to networked computers.
    - When a computer on the network starts up, it requests an IP address from the DHCP server. DHCP server logs may, therefore, link an IP address to a particular computer at a specific date and time.
- Peripheral devices, such as network printers, scanners, and copiers, may also contain data vital to an investigation.
- Router:
    - If a router is hacked, an offender can bypass existing firewalls and intrusion detection systems, attack the network and router, disable the router, redirect traffic to any destination desired, and record all outgoing and incoming traffic.

    - Access control lists can be used to prevent attackers from gaining access to the network through this means. With these lists, routers can be configured to allow or block certain IP addresses from traversing them.
    - In addition, tools such as tracert (also known as traceroute) can determine the route a packet used to travel across the network—that is, the routers the packet traversed to reach its destination.
    - Evidence in routers is found in the configuration files.
    - In addition to the nonvolatile data (NVRAM) stored in them, routers contain volatile data (DRAM/SRAM) that may be vital to an investigation.
- Live Analysis:
    - Retrieves data from a running system, which will be lost once a device is powered down. This type of investigation is performed inlieu of traditional forensic analysis when the circumstances of the case warrant the live collection of data.
    - When conducting live analysis, an investigator must choose between maintaining the integrity of the contents of the hard drive (i.e., ensuring that the contents remain unaltered) and acquiring live volatile data, which will be lost if the device is rebooted or shut down.
    - Examples of volatile information that will be lost if the system is powered down include the following:
        - NIC configuration settings
        - Running processes and services
        - Open sources, ports, and connections
        - List of users currently logged on
        - Active sessions
        - Shared drives
        - Files opened remotely
    - Live analysis must be performed on a router if volatile data are sought as evidence. To minimize alteration of the contents of the hard drive, the software that is used to perform the live analysis should already be installed in the target system in anticipation of the event, and the metadata should not be changed.
    - To perform live analysis, the router should be accessed through its console port. An investigator should record the entire session and all volatile data. Both the time on the router and the actual time should be documented as well.
- Firewalls:

    - A firewall is used to block incoming network traffic based on certain predetermined criteria.
    - Firewalls contain detailed logs that hold a wealth of information pertinent to network forensics investigations.
        - For example, these logs retain data about the network traffic that was blocked and allowed in, any attempted intrusions, and attacks that the firewall recognized.
        - Firewall logs also include information about hardware failures, successful and unsuccessful connection attempts, users added to the system, and any permissions changed.
- Backdoors:
    - A backdoor can be created to hide evidence of the offender's unauthorized access to the system. One tool widely used by hackers for this purpose is a rootkit. Rootkits are installed after an offender has gained full (root) access to a system.
    - Evidence of the rootkit may be found once the system is brought offline, as this software needs a live system to run its program and conceal its presence.
- Keyloggers:
    - Keyloggers can be installed either in person or remotely (e.g., via Trojan horse) on a computer and have the ability to record every keystroke of a user.
    - Given that keyloggers can capture all the data that a user inputs into a computer, a wealth of information can be retrieved from them if they have been installed on a system.
- Sniffers:
    - A sniffer is a device that is used to capture network traffic.
    - Depending on the size and activity of the network, sniffers may collect an enormous amount of data.For this reason, investigators should narrow the scope of their search of these logs.
    - Network traffic can reveal data about the source, destination, and content of communications.
    - Wireshark is an example of a sniffer program that captures network traffic in real time and records it. This tool is not designed to alert authorities of any suspicious activity, so it is not considered a form of intrusion detection. Instead, it is designed to troubleshoot network problems and is used to perform both live and offline analysis of captured network data.
- Honeypots:

    - An intrusion detection/prevention system that lures offenders away from valuable network resources and can help capture new and unknown attacks.
    - Honeynet - A collection of honeypots that is used to mimic a more complex environment.
    - Monitoring of these mechanisms can provide detailed insight as to how a specific exploitation occurred.
- Intrusion Detection Systems:
    - A computer security system that is intended to detect attacks on systems and to detect the unauthorized use of such systems, networks, and related resources.
    - Two types of IDS - Signature based and Pattern based
    - Although both types of IDS are effective in detecting most forms of network attacks and intrusions, human analysis of network traffic is also required to identify incursions. In particular, network administrators should review encrypted traffic and traffic from entrusted sources.
    - An example of an IDS is Snort, which is the most popular of these tools in use today. Snort is designed to identify anomalies by inspecting network traffic. This program uses its analytical abilities to identify suspicious activity and alert the appropriate authorities (e.g., network administrator) of the observation of such activity. Snort can be configured to function as both an intrusion detection system and an intrusion prevention system (IPS).
    - An IDS produces one of four results:
        - True positive: An actual attack or intrusion occurs, and authorities are alerted to its presence.
        - True negative: Network activity is normal. No attack or intrusion occurs, and no alarm is raised.
        - False positive. The IDS reads an activity as an attack or intrusion when, in fact, it is not. (It is either a legitimate activity or no activity at all.)
        - False negative: In this case, the IDS misses an actual intrusion or attack.

Network Forensics Analysis Tools

- Network forensics analysis tool:
    - A tool that is used to capture, record, and analyze computer network traffic, or is intended for use in a networked computer environment.
- Two types of network forensics analysis tools may be distinguished:
    - “Catch it as you can” tools:

        - Within the network, packets that traverse certain points are captured and stored.
        - Analysis of this recorded traffic is subsequently done in batch mode (i.e., all at once).
        - Such a system requires a significant amount of storage space for the data.
    - "Stop, look, and listen" tools:
        - Unlike the "catch it as you can" tools, large amounts of storage are not required because packets are analyzed in a rudimentary manner and only certain types of data are stored for further analysis.
- NetWitness:
    - A network forensics analysis tool that proactively detects threats and alerts authorities as to their presence; it also captures network traffic data and provides real-time analysis of it.
- NetIntercept:
    - A network forensics analysis tool that captures and archives network data for analysis at a later date and time, and is used to detect spoofing.
    - This tool also has data mining capabilities; that is, it can sort and sift through vast quantities of data to find valuable information.
- NetDetector:
    - A network forensics analysis tool that engages in continuous, real-time surveillance of a network.
- OmniPeek:
    - A network forensics analysis tool that allows an investigator or network administrator to see every part of the network in real time, and capture and store network traffic.
- SilentRunner:
    - A network forensics analysis tool that can capture, analyze, and visualize computer network activity by uncovering misuse, intrusion attempts, and abnormal activity.
- NetworkMiner:
    - A network forensics analysis tool (sniffer) that is used to capture network traffic.
- PyFlag:
    - An advanced network forensics analysis tool that can be used to analyze disk images and large volumes of log files, and can reconstruct webpages viewed by a user.
- ProDiscover:

    - A network forensics tool that can remotely acquire drive images in a live environment and securely investigate and extract network evidence from running systems.

The Pros and Cons of Conducting Investigations on Networked Computers

- Benefits
    - Real-time surveillance of network activity
    - Stored network traffic data from devices is usually available
    - High probability that backups of data are conducted regularly (so that data required for an investigation are likely to be available)
    - Centralized data storage on servers
- Drawbacks
    - Jurisdiction issues may arise for large networks
    - Data can be remotely erased and easily hidden
    - It is difficult to secure multiple computers at various sites
    - It is difficult to isolate and secure servers at multiple sites

Special Issues When Conducting Investigations in a Networked Environment

- The primary purpose of a network forensics investigation is to find evidence of a crime, incident, or policy violation. During the investigation, an investigator specifically looks for the following:
    - Network access around the time of the incident
    - Access to the network at unusual times or from unusual locations
    - Repeated failed attempts to access the network
    - Evidence of port scanning or probing the network that preceded an incident
    - Data transfers that occurred after the incident (e.g., a large volume of outgoing traffic after the incident may indicate theft of data)
    - Detection of malicious software or exploitation methods
- An investigator must not forget to look for or at encrypted data and hidden network traffic.
- In a corporate environment, the daily audit logs of corporations should be reviewed as part of the investigation, as they could reveal information about user logon and

logoff, websites accessed, and documents viewed.

Preliminary Analysis

- A preliminary analysis must first be conducted to determine whether an actual incident occurred.
- If an incident has not occurred, the investigator must determine if the activity under investigation was the result of employee (or user) negligence or mistake.
- If an incident has, in fact, occurred, all relevant evidence must be collected. The organization's security policies (e.g., ACLs) and security settings (e.g., access control and signatures) of network devices (e.g., IDS, firewalls, routers, and switches) should be evaluated. These policies and settings should also be reviewed to determine if any changes were made to them as part of the offender's attempt to gain access to the network or to execute an attack. Moreover, these policies and settings should be evaluated to determine whether an offender made any additional changes to secure future access to the system.
- Indeed, the router, firewall, and IDS logs can reveal any attempted or realized attack and intrusion.
- When IDS alerts occur, the network administrator will analyze the anomaly to determine whether a policy violation, intrusion, or attack has occurred.
- If any of these events are observed, the investigation will continue. If not, the alert will be ignored and it will be considered a false alarm.

Documentation and Collection

- The entire incident scene and all related devices must be photographed. In a networked computer environment, photographs of all network and phone cables connected to the computer (or computers) of interest in the investigation should be taken.
- The investigator should also photograph both ends of the cable (or cables) to prove that a computer was connected in a specific manner (to a certain network and phone line) when he or she first arrived at the scene.
- Depending on the nature of the intrusion or the attack, certain parts of the system may need to be isolated from the network. Disconnecting systems is usually not a feasible option for corporations. An investigator can disconnect and seize such devices when permission to do so has been obtained from corporate authorities. Additionally, the investigator can disconnect networked computers if he or she has a search warrant specifying the seizure of such devices. Accordingly, an investigator can

disconnect computers from a networked environment and collect them based on the circumstances of the case and the investigator's legal authority to do so.

- The evidence and related devices that can be legally seized should be thoroughly documented and collected. The investigator must ensure that he or she logs the location of evidence and the network devices of interest to the investigation, including the serial numbers, model numbers, MAC addresses, and any IP addresses of these devices.
- The scope of the investigation must be clearly established. This step, in turn, facilitates a comprehensive and methodical approach to conducting a network forensics investigation. Initial network traffic should be obtained (at the very least, photographed and documented in notes) as soon as possible (after an incident has occurred) to prevent the loss or change of volatile data. For each network device seized, an investigator must determine the order of volatile data and collect it accordingly.

Analysis and Preservation

- From the data obtained during the investigation, the investigator must develop a timeline for the incident.
- Investigations of networked devices and traffic data can help determine which IP address (or IP addresses) successfully compromised the system on a specific date and time. If systems have been compromised, investigators can look at the http sessions, which include data about the requests and transfers of files across the network. Specifically, these sessions can reveal information about any files downloaded.
- Network traffic data can provide proof that a suspect performed a specific action (e.g., misused company resources by viewing pornographic websites on company time). Traffic data captured by network forensics analysis tools must be correlated with other information (e.g., data retrieved from computer events logs, browser history, and so on). The captured network traffic data can then be used as evidence in legal and administrative proceedings.
- As with other forms of evidence, the original captured network traffic data must be kept intact.
- The electronic evidence obtained must be cryptographically hashed using forensically sound procedures. The appropriate network forensics analysis tools should be employed to ensure that evidence is not altered during the acquisition of data. The tool chosen must be able to deal with different log data formats and handle a vast amount of data that requires significant memory space.

Module 4

E-mail Forensics

The Importance of Email Investigations

- Many cybercrimes have involved the use of emails, either as the means with which to commit the crime or as evidence of the crime.
- In respect to the former, emails may be sent, for example, to extort money from the recipient. A case in point is the crime committed by Oleg Zezev. Zezev sent an email to Michael Bloomberg, the president and chief executive officer of Bloomberg, Inc. (a multinational financial data company), in an attempt to extort $200,000 from him. Specifically, in the email to Bloomberg, Zezev stated that he would inform the media and Bloomberg's customers that Zezev had gained unauthorized access to Bloomberg's computer system, where confidential customer information was retained, if Bloomberg did not pay him the money.
- One well-known case involving the use of evidence from emails was the Enron scandal. According to the FBI, during the Enron investigation, agents "collected over four terabytes … of data, including email from over 600 employees." In these emails, FBI agents found numerous remarks and jokes from employees about their shredding of thousands of crucial auditing materials under the direction of their supervisors at Arthur Andersen.

Email: The Basics

- Two types of email systems exist:
  - Client/server email:
    - The client is the computer that sends or receives messages; the server stores any messages received until they are retrieved by the user.
    - In client/server systems, emails are downloaded to a user's computer.
  - Web-based email:
    - With a web-based system, email accounts are accessed through a Web browser and emails are stored in the email service provider's server.
    - A few well-known examples of web-based systems are Yahoo, Gmail, and Hotmail.
- To communicate with one another, email systems use a variety of protocols:
  - SMTP:

        - Simple Mail Transfer Protocol; the protocol used to send email across the Internet or across a network.
        - It is a TCP/IP Protocol.
    - Post Office Protocol 3 (POP3):
        - Used to read email.
        - It is designed to store emails in a single mailbox until they are downloaded by the user.
        - designed in such a way as to delete emails on the server immediately after they have been downloaded. However, a user or an administrator may opt to save emails on a server for a set period of time. As such, these servers should not be overlooked by investigators when they are seeking emails that have already been downloaded by the user.
    - Internet Message Access Protocol (IMAP):
        - used to retrieve and read emails.
        - more powerful protocol than POP3
        - Emails can be received and stored on the server.
        - IMAP affords users with the opportunity to create and manage multiple folders within which to store emails on the server.
    - In summary, an email is sent with SMTP, an email handler receives this message, and it is then read using POP3 or IMAP.
- Email Address:
    - An email address is used to identify the email box that the message should be sent to.
    - It is made up of two parts: the username and the domain name.
    - The characters on the left side of the @ symbol comprise the username—that is, the mailbox where the message should be sent.
    - The characters on the right hand side of the @ symbol are the domain. The domain name is an identifying label by which computers on the Internet are known.

Parts of an Email:

- An email primarily has two parts: the body and the header.
- The body contains the actual message.
- Email header:

    - The part of an email that provides identifying information for both sender and receiver of the message.
    - There are two versions of an email header: the condensed and full versions.
    - With the condensed version of the email header, four basic fields of header information are provided:
    - From: This field consists of the sender's address. The name of the sender may also be included (whether real or fake). The investigator should keep in mind that the email address of the sender may be faked. SMTP does not verify email headers, so the suspect may disguise (or spoof) his or her address to make it look like another individual sent the email.
    - To: This field consists of the recipient's address. The name of the recipient may also be included. This address can also be faked or spoofed.
    - Subject: Sometimes this field may be left blank. The investigator must also keep in mind that this field may contain misleading information.
    - Date: This field includes the date, day of the week, time and time zone, such as GMT (Greenwich Mean Time), UTC (Coordinated Universal Time), ADT (Atlantic Daylight Time), and CST (Central Standard Time), to name a few. This field is recorded by the computer where the message was sent. It may not be accurate if the sender's clock was set incorrectly (either intentionally or accidentally).
- X-Originating-IP:
    - The X-Originating-IP field reveals the IP address of the computer from which the email was originally sent. The IP address is a unique identifier that is assigned to a computer by service providers when it connects to the Internet.
- Received:
    - A header field that provides information on the recipient of an email, and sometimes on the sender of the email.

Received Field

Received: by mail-gy0-f180.google.com with SMTP id 13so4018650gyg.25 for <marika.filipopoulou@yahoo.com>; Wed, 09 Jun 2010 07:40:46 -0700 (PDT).

    - What information does this field reveal to the user? It indicates that the server "mail-gy0-f180.google.com" received the message on June 9, 2010, at 7:40:46 A.M. Pacific Daylight Time (PDT) via SMTP. Depending on the email system, the Received field may also include the IP address of the sender.

- The Received field provides the domain name and/or the IP address of the sender of the email. Both can be used to trace the email back to the offender. If an IP address is not available, a request can be made to the domain to retrieve further information on the user.
- Multiple Received Fields:
  - The Received field allows the computer forensics investigator to trace the email from the user's mailbox back to the mailbox it originated from.

Multiple *Received* Fields[11]

Received: from 127.0.0.1 (EHLO vms173013.mailsrvcs.net) (206.46.173.13) by mta109.mail.ac4.yahoo.com with SMTP; Thu, 03 Jun 2010 20:06:58 -0700

Received: from vms170003.mailsrvcs.net ([unknown] [172.18.12.133]) by vms173013.mailsrvcs.net (Sun Java(tm) System Messaging Server 7u2-7.02 32bit (built Apr 16 2009)) with ESMTPA id <0L3G00G2DZB94Y5A@vms173013.mail-srvcs.net> for marika.filipopoulou@yahoo.com; Thu, 03 Jun 2010 22:06:47 -0500 (CDT)

Received: from 70.19.46.22 ([70.19.46.22]) by vms170003.mailsrvcs.net (Verizon Webmail) with HTTP; Thu, 03 Jun 2010 22:06:45 -0500 (CDT)

  - As the message travels across the Internet, it passes through a series of routers on the way to the recipient. Each router adds code with the IP addresses and timestamp to the header.
  - To determine where the email was sent from, an investigator must start at the bottom.
  - If the email traveled across several servers, then each mail server will be added on top of the existing Received header field.
  - Multiple Received field headers can also reveal whether a sender tried to send the email with a false IP address. To make this determination, the investigator compares the sending location listed next to the word "by" in each Received field header and the receiving location listed next to the word "from" in the Received field header below it. If they do not match, the sender as used a fake IP address.
- Return Path:
  - Indicates where the email should be returned if it fails to reach the recipient.

    - If the email address provided in the From field does not match the email address listed in the Return-Path, then the user should suspect that the address provided in the From field has been faked or spoofed.
- Message ID:
    - The Message ID field consists of the name of the server and a unique string that the sending email server assigned to the message.
    - This number can be used to track the message (along with timestamp information) on the originating email server in the logs held by ISPs.
- Received-SPF:
    - A header field used for spam-filtering purposes.

> **Excerpts from the Full Email Header**
>
> **Example 1**
>
> Received-SPF: pass (mta1077.mail.re4.yahoo.com: domain of smtpreturnpath@skysiteonline.com designates 208.184.87.85 as permitted sender)
>
> **Example 2**
>
> Received-SPF: neutral (google.com: 92.247.202.229 is neither permitted nor denied by domain of uufas1247@spectrumnet.bg)
>
> **Example 3**
>
> Received-SPF: fail (mta1019.mail.re4.yahoo.com: domain of bestmeds1@hatfuel.ru does not designate 198.185.97.95 as permitted sender)

    - The function of this header field is as follows: The receiver of an email makes an SPF query, which checks to see whether the sending server is allowed to send an email for the sender's domain. If the result of the query is "fail,", the email should be rejected and not delivered.
    - SPF specification does not mandate that rejection occur, so many times receivers will see such messages delivered to their mailboxes (albeit typically to their spam folders).
- Authentication-Results:
    - A header field that decides and/or makes a recommendation to the user as to the validity of the origin of the message and the integrity of its content.

Authentication-Results Header

Authentication-Results: mta1032.mail.ac4.yahoo.com from=gmail.com; domainkeys=pass (ok); from=gmail.com; dkim=pass (ok)

- MIME-Version:
  - The MIME-Version field indicates that the message that was sent was composed in compliance with RFC 1341, Multipurpose Internet Mail Extensions (MIME).

Another Excerpt from the Full Email Header

MIME-version: 1.0
Content-type: multipart/mixed;
boundary="——=_Part_834179_1894254106.1275620805664"
X-Mailer: Verizon Webmail

  - The MIME protocol standardizes headers and body of emails.
  - MIME uses headers to inform the system which type of processing is required to re-create the message. Non-MIME messages may not always be recognized, so the system may not be able to interpret the message.
- Content-Type:
  - A header field that indicates the type of data included in an email message, such as text, image, audio, video, and multipart.
- X-Mailer:
  - A header field that specifies the email system used to send a message.

How to Conduct an Email Investigation

Obtaining the Email

- The first step in an email investigation is to make an evidentiary copy of the digital evidence. The copy of the email must include the header information and any attachments.
- Even if the email on the receiving end has been deleted, a copy of it will still reside in the sent folder of the suspect's email program.

- Assume that the suspect deletes the copy of the email that is in his or her sent folder. Even in this scenario, a computer forensics investigator can still find a copy of the email attachment in the computer's hard drive or the backup tape of a network server.
- Other places where emails can be found include temporary files and in the unallocated space if the temporary files have been erased.

Searching the Email for Evidence

- a computer forensics investigator can search the body and headers of the email and email server log files for potential evidence.
- An investigator should also check, if applicable, attachments, individuals who have received copies of the email as secondary recipients (i.e., carbon copies (CC) or blind carbon copies (BCC)), individuals to whom the message was forwarded, and the original message to which the email under investigation represents a response.
- The investigator should examine both the condensed and full versions of the header.
    - In these headers, the most reliable and most important information to an investigation is the IP address. The PING command can be used to validate IP addresses found in the email header.

Verifying the Owner of an IP Address

- The Internet Assigned Numbers Authority (IANA) is responsible for coordinating the general pool of IP addresses and providing them to Regional Internet Registries (RIRs).

- RIRs administer and register IP addresses in a defined region. Several RIRs exist:

    1. American Registry for Internet Numbers (ARIN) - North America
    2. African Network Information Center (AfriNIC) - Africa
    3. Asia Pacific Network Information Center (APNIC) - Asia Pacific
    4. Latin American and Caribbean Internet Addresses Registry (LACNIC) - Southern America
    5. Regional Internet Registry for Europe (RIPE) - Europe, the Middle East, and parts of Central Asia.

- A query tool on ARIN's website, known as WHOIS, allows a user to find out the contact and location information of the owner of an IP address.

- In summary, after determining the originating IP address, the investigator should use a query tool to retrieve the name and contact information of the ISP that assigned the IP address in question. Once this ISP is located, the investigator should draft a subpoena or search warrant—whatever is required for the particular situation—for ISP records pertaining to the email message and its sender. Generally, a search warrant is needed to view the contents of a computer. By contrast, data on ISP servers requires only a subpoena.As the final step in the email investigation process, the investigator secures and documents the evidence.

Problems Encountered by Computer Forensics Investigators

- Criminals use different techniques with which to communicate undetected online. They may also seek to avoid detection by changing their IP or email addresses.
- In other cases, criminals may use proxy servers to hide or mask their IP addresses. If an individual uses a proxy server (i.e., a server that acts as an intermediary for client requests for resources from other servers when accessing a website), the user's identity is not revealed because the proxy server provides its own identity when it retrieves the website for the user.
- Criminals may also use anonymous remailers to communicate undetected.
- A criminal may intentionally bounce (or route) his or her communication through numerous intermediate computers all over the world before arriving to the target computer. To find the criminal, the investigator will have to identify each router or bounce point through which the message traveled to eventually find the email's point of origin. This is likely to be a slow process, as investigators may have to retrieve data from each point pursuant to a subpoena, court order, or search warrant (depending on which location in the world the message bounced to) to trace the message back to the computer from which it originated.
- Criminals may attempt to evade detection by setting up a foreign POP3 or IMAP email account and then accessing this account by using certain web based systems such mail2web.com. With this approach, the mail is stored in and accessed from a foreign account, so that the criminal never uses publicly available electronic communications services or public communications networks.

- Criminals have tried to avoid detection by accessing the Internet from Internet cafés or library computers.
- Piggybacking:
  - In this approach, when surveillance is being performed, information that needs to be passed on to a third party undetected can be attached to a legitimate object.
- Steganography:
  - With steganography, only those individuals with the appropriate software can see the hidden messages.
- Terrorists may also hide messages in spam. Several tools are available online that allow terrorists and other criminals to do so. For instance, spammimic is a program that turns email messages into spam. This program is designed to encode the email to appear as spam. The spam is then decoded by the recipient to reveal the original message.
- Some other Methods :
  - Blocking moves:
    - individuals “physically block access to the communication or, if unable or unwilling to do that, to render it (or aspects of it such as the identity, appearance, or location of the communicator) unusable.”
  - Encryption
  - Pizzini
    - Small slips of paper, either tiny handwritten or typewritten notes
    - used for high level communications to evade fax or phone taps.
  - Tor:
    - An anonymous Internet communication system that provides individuals (and organizations) the ability to share information and communicate over public networks without compromising their privacy.

Module 5

Mobile Forensics

Role of Mobile Devices

- Mobile phone technology has been (and is being) used, for example, by criminals—such as terrorists—to communicate undetected.

- Both mobile phones and PDAs(personal data assistants) have been used in crimes. Nowadays, the majority of PDAs also function as mobile phones. Consequently, their use in illicit activities has been increasing. Mobile phones and PDAs may be involved in an investigation in various ways.
- They may be the target of an attack. Mobile phones and PDAs are increasingly becoming the targets of attacks by hackers and malicious software.
- Mobile devices may provide evidence of a crime or incident. Today's mobile devices have vast storage capacities—and, therefore, may contain very valuable information to an investigation. The types of information normally retrieved from PDAs and mobile phones for use in an investigation include, but are not limited to:
    - PIM data. Personal information manager (PIM) information includes:
        - A memo pad, personal notes, diary, and/or a journal
        - A calendar, datebook, and/or events list that contain appointments and reminders
        - A "to-do list," which records tasks that a user needs to accomplish
        - The numbers dialed, the numbers from which calls were received, missed calls, and the dates and times of these calls.
        - Contacts listed in the phone book.
        - Text messages.
    - Instant messages (IMs)
        - SMS messages
        - MMS messages, which can include text and image, video, and/or sound
        - Enhanced multimedia messages (EMS), which can be used, for example, to send ringtones
        - Email and Internet data.
    - Image, sound, or audio files. Photographs, audio recordings, and video clips can be stored on a memory card.
    - Applications
    - Subscriber identifiers. These identifiers are used to authenticate the user to the network and to verify the services tied to the account.
    - Other data. The personal identification number (PIN) and financial information (e.g., credit and debit card numbers) of the mobile phone or PDA user can also be retrieved, including data from the user's voice mail account.
    - If a person (including an investigator) enters the wrong PIN three consecutive times, he or she will be locked out of the user's phone. To unlock access to the phone after incorrectly typing in the PIN in this manner, the investigator must

type in the personal unlock key (PUK). The PUK is unique to each subscriber identity module (SIM) card. The SIM card stores information identifying the subscriber to a particular network. An investigator must ensure that he or she does not enter the wrong PUK 10 times. If this occurs, the SIM card will be rejected. If the SIM card is rejected, the only way to use the phone is to request another SIM card. Certain phones may also ask for a second personal unlock key (PUK2) after a user has inserted the PUK as a means of enhancing security.

- The integrated circuit card identifier (ICCID), which is imprinted on the SIM card, can be used by the service provider operator to trace the SIM card back to the number that it was assigned to. The mobile subscriber integrated services digital network number (MSISDN) on the SIM card also provides the real number of a Global System for Mobile Communications (GSM) mobile phone. The MSISDN consists of the country code, national destination code, and subscriber number, in that order.
- SIM cards are used in GSM devices. Their equivalent in Universal Mobile Telecommunications Systems (UMTS) is the Universal Integrated Circuit Card (UICC). UMTS runs the Universal Subscriber Identity Module (USIM) application, which is a component of the UMTS 3G network. The USIM stores data that identify a mobile phone user as well as his or her subscriber data, contacts, preferences, and so on.
- Voice mail access numbers and passwords can also be obtained from mobile phones and PDAs. Voice mail may contain information that is vital to an investigation. Messages in the voice mail system are held by the network, but the storage space for such messages is finite.
- Information retrieved from a mobile phone should be verified with the service provider. In particular, the SIM and the international mobile equipment identifier (IMEI) are used to identify mobile phones and match them to subscribers. An IMEI number may be requested when a service provider wants to determine whether a mobile phone has been stolen. However, IMEIs can easily be manipulated by users, and manufacturers might assign these numbers multiple times. Most service providers do not use IMEI numbers to identify mobile phone users, but instead use the international mobile subscriber identity (IMSI) number assigned by the provider and stored on the customer's chip (SIM) card.
- Location data can also be retrieved from mobile devices.
- The GPS functionality included in most mobile phones and PDAs enables the pinpointing of the location of the user to within a few feet. GPS navigation

systems can record the user's home address, work address, and other areas to which the individual traveled.
    - Majority of PDAs and mobile phones have digital picture and video capabilities, images or recordings of a crime, evidence, victims, or accomplices can be stored on it.

Mobile Phones and PDAs Versus Other Electronic Devices

- Many electronic devices, such as computers, laptops, mobile phones, and PDAs, are similar in that they read and write data using some kind of storage medium.
- Both mobile phones and PDAs contain memory similar to that of a hard drive of a computer, which provides for nonvolatile and volatile storage of data.
- Consider, for instance, the SIM and USIM smart cards contained in most mobile phones.
- These phones typically have a microprocessor and three types of memory: random access memory (RAM), read-only memory (ROM), and electrically erasable programmable read-only memory (EEPROM).
- Memory cards could also be used to store the data from PDAs and mobile phones. For example, a micro secure digital (SD) memory card, which is a removable card, can be used to store data.
    - Other types of memory cards that can be used in mobile phones and PDAs include the following devices:
        - MultiMedia Card (MMC): a form of nonvolatile computer storage
        - Memory sticks: used to store data from portable electronic devices
        - TransFlash: similar to a micro SD card (and, in fact, was an earlier version of it)
        - CompactFlash (CF): provides mass storage for these devices
    - Fortunately, these memory cards are "normally formatted with a conventional filesystem (e.g., FAT) and can be treated similarly to a disk drive, imaged and analyzed using a conventional forensic tool with a compatible media adapter that supports an integrated development environment (IDE) interface.
- Forensically, these electronic devices are also similar because they rely on an operating system for their functioning. There are numerous makes and models of mobile phones and PDAs on the market, which differ significantly in respect to their specifications (e.g., processing capacity, storage size, and other capabilities, such as

phone, texting, and other features) and the types of operating systems they use (e.g. Macintosh, Linux, or a particular version of Windows).

- Some of the most common operating systems of PDAs are identified here:
  - PalmOS. Palms are PDAs that run on the Palm operating system. Sony and Palm are among the manufacturers that use this operating system.
  - Windows CE. Pocket PCs are PDAs that use the Windows CE operating system. Usually, Compaq, Casio, and Hewlett-Packard PDAs run this operating system.
  - Other PDAs have proprietary operating systems. For example, BlackBerry PDAs run on the RIM BlackBerry operating system.
- PDAs are primarily used as organizers and are intended to link up with computers. Given this interrelationship, the file structures of PDAs and computers are compatible. This similarity enables the investigator to easily access PDA files, because they are essentially computer files residing on a different device.
- A device that has both mobile phone and PDA capabilities is known as a smartphone.
- The operating systems of smartphones vary.
  - Like PDAs, smartphones can run on Windows CE and Palm OS. BlackBerry smartphones have their own proprietary operating system.
  - Apple Computer's iPhone also has its own operating system.
  - Moreover, the Motorola Droid runs on the Google Android 2.0 operating system, whereas the Symbian operating system is used for smartphones from Nokia, Samsung, and Panasonic (to name a few).
  - Android is a mobile operating system based on a modified version of the Linux kernel and other open-source software, designed primarily for touchscreen mobile devices such as smartphones and tablets.
  - iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that powers many of the company's mobile devices, including the iPhone; the term also includes the system software for iPads.

Which Tools Can Be Used to Retrieve Evidence?

- Given that each manufacturer may use its own proprietary operating system, and that each device may operate in a completely different manner from other devices offered by the same manufacturer, it is nearly impossible to develop an all-inclusive forensics tool to deal with the many different makes and models of mobile phones, PDAs, and smartphones on the market from various manufacturers.
- PDA Forensics Tools

- PDA forensics tools are chosen for use in an investigation based on their ability to successfully meet the following demands:
  - Acquire the contents of the device
  - Retrieve information associated with PIM applications (e.g., calendar, “to-do list”) •
  - Locate graphic, text, video, and audio files
  - Identify websites visited and obtain emails exchanged
  - Find and display fields acquired from the device
  - Locate data in compressed, archived, and formatted files
  - Recover deleted, misnamed, and hidden file
  - Retrieve files from a removable memory card
  - Acquire data after a hard reset is performed
  - Obtain the user’s password to acquire the contents of the device in question
- Encase:
  - Incompatible with PDAs running Pocket PC. Instead, it is used to acquire data from PDAs with Palm operating systems (OS).
  - This tool also facilitates investigations of Linux-based PDAs.
  - With Encase, “a complete physical bit-stream image of Palm OS devices is created and this bit-stream image is checked with the already obtained existing CRC (Cyclical Redundancy Checksum) values.
  - A report of the analyses performed and the results of these analyses can also be provided using this tool.
- Palm dd
  - Used to acquire data from a Palm device with a Palm operating system that is running in console mode.
  - This tool does not have report, bookmarking, and search capabilities.
  - The files that are “created from pdd can be imported into a forensic tool, such as Encase, to aid analysis; otherwise the default tool is a hex editor.”
  - Although this tool can image the memory of the device, it does not provide hash values for the data that are acquired.
- PDA Seizure
  - The PDA Seizure tool can be used to extract data from PDAs running the Windows CE, Pocket PC, or Palm operating systems.
  - This tool can image RAM and ROM and works in a Windows environment.
  - Unlike the pdd, PDA Seizure can provide hash values for acquired information.

        - This toolkit is oriented toward PDAs without mobile phone functions, as it does not include features such as the ability to acquire SIM data.
    - POSE
        - If an investigator uses Palm Operating System Emulator (POSE), he or she can view the data in the same manner that the user of the PDA did.
        - That is, the POSE interface allows an investigator to work on the device and access items (e.g., menus, calendars) on it as if he or she was working on the original device.
    - Pilot-Link
        - Incompatible with PDAs running Pocket PC; rather, it is used to acquire data from PDAs with Palm OS.
        - It was "developed for the Linux community to allow information to be transferred between Linux hosts and Palm OS devices. It runs on several other desktop operating systems besides Linux, including Windows and Mac OS."
    - Duplicate Disk
        - Functions in a similar manner to pdd in that it creates a bit-by-bit image of the contents of the PDA.
        - It is compatible with a Linux-based PDA.
        - If this forensics tool is used incorrectly, it could delete or overwrite parts of the content that are stored on the device.
- Mobile Phone Forensics Tools:
    - The information located on a mobile phone will depend on several factors:
        - Capabilities of the mobile phone
        - Modifications made to the phone by a communications service provider
        - Services that the user has subscribed to and utilizes
        - Modifications made to the phone by the user
    - According to the NIST, mobile phone forensics tools are chosen for an investigation based on their ability to successfully meet the following demands:
        - Acquire the contents of the device
        - Obtain subscriber data
        - Recover location data (e.g., the place where the device was last used)
        - Retrieve information associated with PIM applications (e.g., a phonebook)
        - Find numbers dialed, numbers from which calls were received, missed calls, and deleted calls

    - Locate SMS, MMS, and EMS messages sent, received, saved as drafts, and deleted
    - Obtain information on Web applications (e.g., Internet sites browsed)
    - Acquire sent, received, saved, and deleted emails and IMs
    - Find graphic, text, video, and audio files
    - Locate data in compressed, archived, and formatted files
    - Recover deleted, misnamed, and hidden files
    - Retrieve files from a removable memory card
    - Acquire data after a hard reset is performed
    - Recover data from a device after its power has been completely
    - drained
    - Locate the password for the device to access its contents
- Cell Seizure:
    - Paraben's Cell Seizure product targets certain models of GSM, TDMA (time division multiple access), and CDMA (code-division multiple access) phones.
    - This forensics tool can acquire, search, bookmark, and examine data from the mobile phone device and report the results of the analyses performed.
- .XRY:
    - The .XRY forensics tool retrieves a wealth of stored data from certain models of GSM phones.
    - In addition, this tool creates an encrypted file of the data acquired from the mobile phone device and enables the investigator to inspect, search, and provide a report of the analyses conducted.
    - An additional important feature of this tool is that it protects the data from accidental or intentional deletion and overwriting.
- Oxygen Phone Manager:
    - The Oxygen Phone Manager forensics tool is compatible with numerous mobile phones and smartphones (Nokia, Samsung, Siemens, Ericsson, and Panasonic models, to name a few) and is widely used by law enforcement and government agencies.
    - The Oxygen Forensic Suite 2010 can be used on more than 1,550 mobile phones, smartphones, and PDAs with diverse operating systems.
    - An additional feature of this forensics tool is that it can extract geographic positioning data from the device.
- MOBILedit!:

        - The MOBILedit! forensics tool is also widely used by law enforcement, government agencies, and forensic investigators. It can acquire, search, and examine data from virtually all mobile phones on the market.
        - It also generates an extensive report of the results that can be electronically stored or printed.
- SIM Cards:
    - To extract SIM card information in a forensically sound manner, an investigator can use any of the following tools:
        - Mobile phone forensics tools
        - SIM card readers
        - Tools from the manufacturer
    - SIM Forensics Tools:
        - Certain SIM tools have been designated for forensic purposes, such as Cell Seizure, GSM.XRY, and MOBILedit! Forensic. These tools can recover data from a variety of SIM cards, including those inserted in handsets. Other tools can analyze only external SIM cards.
        - One of the latter tools is SIMIS, which can both securely acquire data from the SIM card and use cryptographic hashes to protect the integrity of the data.
        - Another tool, ForensicSIM, can clone the SIM card and examine it without altering the contents of the original device.
        - SIM Card Seizure:
            - This tool can perform a complete acquisition and analysis of the data on a SIM card.
            - It can also recover deleted data from the SIM card by searching unallocated space on this device.
            - Finally, SIM Card Seizure can calculate hash values, perform search functions, and bookmark data.
    - SIM Card Readers:
        - SIM card readers enable users to back up the data on their mobile phone devices. Numerous SIM cards readers are available on the market.
            - eg Dekart SIM reader, SIMGuard, SIMClone, SIMScan, SIMMaster, SIMCopy, SIMTools.
        - The integrity of the data that are extracted using these tools, however, cannot (and has not) been established.
    - Manufacturer-Provided Tools:

        - A vast number of manufacturer tools are available that are “designed to back up, restore, synchronize, or transfer data to and from their phones and domestic computers.”
        - Such tools are not forensically sound and their use could alter the data in the device.
- Popular Forensics Tools for Mobile Phones, PDAs, and Smartphones:
    - CellDEK:
        - CellDEK is widely used in investigations, as it can extract a wealth of information from the majority of mobile phones, PDAs, and smartphones on the market, while preserving the integrity of the data.
        - According the Logicube website, this tool is compatible with approximately 1,700 mobile phones and PDAs (including BlackBerry PDAs).
        - It also supports iPhones, iPods, and handheld navigation devices (e.g., GPS devices from Garmin, TomTom, and iPAQ).
    - Device Seizure:
        - Paraben’s Device Seizure also acquires and examines data from PDAs, mobile phones, smartphones, and navigation devices.
        - In particular, according to its website, it can be used on PDAs with various operating systems (e.g., BlackBerry, Windows CE, Symbian, and Pocket PC) and on more than 1,000 models of mobile phones.
        - Similarly to CellDEK, this tool preserves the integrity of the evidence it extracts from these devices.

Mobile Forensics Process Steps

1. Seizure - Use Airplane Mode, Phone Jammer or Faraday box/bag.
2. Acquisition
3. Examination & Analysis

Mobile Device Investigations

- The investigator must document the location, make, model, serial number, identifying marks (if any), and condition of the electronic device (on, off, standby) to be seized.
- If the device is on, the investigator must write down all the information projected on the display of the electronic device and its current battery charge in his or her notebook.

- The screen of the mobile device (if on) and other related evidence should also be photographed.
- Forensic protocol dictates that if mobile devices (mobile phones, smartphones, and PDAs) are discovered during an investigation, they must be left in the state that they were found. If the device is off, it should remain off. If the device is turned on, the data in it may be modified. If the device is found on, the device should remain on. These devices are powered by battery; they must be charged to ensure that they remain on. As such, an investigator should ensure that the "on" state is maintained by powering the devices with, for example, a battery pack.
- The investigator cannot know how long a device has been on and how long the battery will last without power. In fact, the battery life among mobile devices varies according to their make and model.
- The phone will consume more power if it is blocked from connection to the mobile network, because it will continually attempt to connect to it. Thus the battery can be depleted much faster if the device is isolated from the mobile phone network. Moreover, some mobile phones will reset or clear network data after a predetermined number of failed attempts to connect to the network—and this data may be critical to the investigation.
- Accordingly, investigators must familiarize themselves with mobile devices for the following purposes:
    - Prevent the devices from losing power
    - Help them better understand how to handle the devices
    - Avert any data loss
- The investigator must have external batteries with him or her that can be attached to the mobile device to prevent power loss. If the battery of the device is depleted or the investigator turns the device off, volatile data will be lost. Moreover, an investigator may be locked out of the phone and be required to enter a PIN (which he or she may not have or know) when the device is turned back on.
- If a mobile device such as a PDA is in a cradle (an instrument connected to the computer that allows data to be transferred from the PDA), a different procedure should be followed. In particular, the investigator must remove the connection of the device to the computer. By doing so, the investigator will prevent any further communication between the PDA and the computer, thereby blocking any data from being modified in the mobile device.
- Investigators must remember that mobile devices that remain on are susceptible to damage. That is, data in these devices can be remotely modified and/or deleted if they are powered on. If the device is turned on, newly transmitted messages may

destroy existing messages that are stored on it. Forensic protocol dictates that Faraday bags be used to prevent any electronic signals from entering or exiting the mobile device.

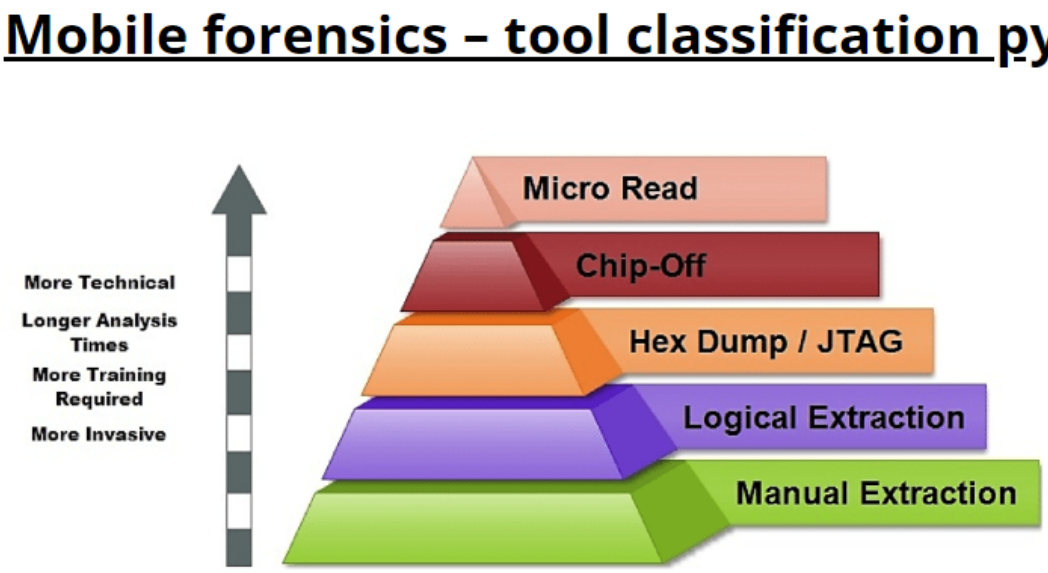
- When collecting mobile phone, PDA, or smartphone evidence, investigators should look for memory and SIM cards. The suspect may have hidden such items. Given their small size, these cards may be easily overlooked by investigators. In addition to those items, the cradle and all synchronization and power cables associated with the mobile device should be seized, labeled, packaged, and transported back to the forensic laboratory (if available). All peripheral devices, cloning equipment, and instruction and informational manuals related to the electronic devices (if present) should also be seized. All of the seized devices must be handled very carefully to avoid any destruction or tampering of the evidence.
- The evidence stored on the mobile device (PDAs, mobile phones, and smartphones) will depend on its make and model. All storage devices can have deleted files or fragments recovered using a forensic procedure. Recovery depends on the time a manufacturer allotted for the retention of this information on a specific device. For instance, iPhones tend to retain data longer than any device on the market. Other makes and models of mobile phones may store data for approximately 12 months before the data is overwritten—though this storage time depends on the frequency with which the devices are used. Other forms of evidence may be accessible from the service provider. Again, the availability of this data depends on the retention practices of the specific service provider. If unsure of such information, the investigator can review informational booklets on the mobile phone, visit the phone company website to review the capabilities of the phone, and contact the manufacturer. If a particular mobile phone is supported by forensic software, an investigator can use the tool to acquire the data stored in it.
- When conducting an investigation, the analyst must ensure that the mobile device is properly connected to a forensic workstation (i.e., computer) before acquiring data from it.
- The investigator must also make sure that no modifications are made to the original contents of the device; doing so may render the evidence inadmissible in court.
- Missing SIM Card:
    - What should an investigator do if a SIM card is missing (and he or she cannot find it at the crime scene)?
    - The specific steps to be taken will depend on the forensic tool used.
    - Suppose an investigator is using the .XRY forensic tool.
    - If a SIM card is missing from a phone, the following tasks should be performed:

1. The phone should be connected to the host workstation.
2. The last IMSI should be recovered.
3. The IMSI should be typed into the .XRY program and copied to a clone card.
4. After the insertion of the cloned card into the phone, data can be securely acquired from the device.

- Depending on the device, data may also be archived online or on the suspect's desktop or workplace computer. Indeed, Bluetooth (i.e., short range, wireless communication) technology affords users the opportunity to synchronize and transfer the data on their mobile devices to their home and work computers and laptops. Bluetooth technology can also be used to synchronize and transfer the data on the user's mobile devices to other mobile devices.
- Furthermore, new makes and models of mobile devices are offering users the ability to store the contents of their devices on the Internet. For instance, Verizon's Kin One and Kin Two models enable users to sort, share, and store all the contents of their phones online. Palm Pre also requires users to create a Palm Profile (complete with username and password), which saves their data and applications online for backup purposes. One feature of the Palm Profile is that it allows a user to erase personal data remotely. With this feature, users may remotely access the data stored online to erase any incriminating evidence if they believe they are under investigation. The availability of such areas of remote storage further complicates the work of a forensic investigator.
- Kill Switches in Mobile Phones and Smartphones:
  - Kill switches are no longer limited to automobiles, where they have long been used to prevent motor vehicle theft. Such techniques are now being used in communications technology, albeit for different reasons—for example, to remotely delete applications that violate the terms of service for users' phones. In addition, they may be used by individuals and service providers to wipe the contents of a mobile device when a phone has been lost or stolen.
  - Microsoft has added to the remote access capabilities of its users' phones by introducing Digital Manner Policies (DMP)–enabled devices. DMP devices could set users' phones to vibrate when individuals enter certain buildings or board a flight. They could also prevent users from using certain services and applications on their phones, such as taking photographs, in specific facilities. With this technology, someone else will have control over what is done with a user's phone in specific designated areas.

Non-invasive vs. invasive forensics

- No matter what your actual mobile forensic method is, it is imperative to create a policy or plan for its execution and follow all its steps meticulously and in the proper sequence.
- Not following the protocol may entail grave consequences.
- One should start with non-invasive forensic techniques first as they tend to endanger a device's integrity to a lesser degree. Be careful with built-in security features – "for example, collecting a physical image before a logical image on certain devices can completely wipe a phone of all data, as can attempting to access a locked device and making too many password attempts."



Non-Invasive Methods

- Manual extraction
  - The forensic examiner merely browses through the data using the mobile device's touchscreen or keypad. Information of interest discovered on the phone is photographically documented.
  - It is not possible to restore deleted data this way.
- Logical extraction
  - This approach involves instituting a connection between the mobile device and the forensic workstation using a USB cable, Bluetooth, Infrared or RJ-45 cable. Following the connecting part, the computer sends command requests to the device, and the device sends back data from its memory.
  - The majority of forensic tools support logical extraction, and the process itself requires short-term training.

    - On the downside, however, this technique may add data to the mobile device and may alter the integrity of the evidence. Also, deleted data is rarely accessible.
- JTAG method
    - JTAG is a non-invasive form of physical acquisition that could extract data from a mobile device even when data was difficult to access through software avenues because the device is damaged, locked or encrypted. The device, however, must be at least partially functional (minor damages would not hinder this method).
    - The process involves connecting to the Test Access Ports (TAPs) on a device and instructing the processor to transfer raw data stored on connected memory chips. This is a standard feature that one could come across in many mobile phone models, which provides mobile phone manufactures a low-level interface outside the operating system.
    - Digital forensic investigators take an interest in JTAG, as it can, in theory, allow direct access to the mobile device's memory without jeopardizing it. Despite that fact, it is a labor-intensive, time-consuming procedure, and it requires advance knowledge (not only of JTAG for the model of the phone under investigation but also of how to arrange anew the resulting binary composed of the phone's memory structures).
- Hex dump
    - Hex dump is another method for physical extraction of raw information stored in flash memory. It is performed by connecting the forensic workstation to the device and then tunneling an unsigned code or a bootloader into the device, each of them will carry instructions to dump memory from the phone to the computer. Resulting image is fairly technical—in binary format—and it requires a person having the technical education to analyze it. Furthermore, the examiner comes into possession of an abundant amount of data, since deleted data can be recovered, and, on top of that, the entire process is inexpensive.

Invasive methods

- Typically, they are longer and more complex. In cases where the device is entirely non-functional due to some severe damage, it is very likely the only way to retrieve data from the device might be to manually remove and image the flash memory chips of the device. Even if the device or item is in good condition, circumstances may require the forensic expert to acquire the chip's contents physically.
- Chip-off

    - A process that refers to obtaining data straight from the mobile device's memory chip. According to the preparations pertinent to this level, the chip is detached from the device and a chip reader or a second phone is used to extract data stored on the device under investigation.
    - Challenging because of the wide variety of chip types existing on the mobile market.
    - The chip-off process is expensive, training is required, and the examiner should procure specific hardware to conduct de-soldering and heating of the memory chip.
    - Bits and bytes of raw information that is retrieved from the memory are yet to be parsed, decoded, and interpreted. Even the smallest mistake may lead to damages to the memory chip, which, in effect, would render the data irrevocably lost.
    - Consequently, experts advise having recourse to chip-off when:
        1. other methods of extraction are already attempted,
        2. it is important to preserve the current state of device's memory,
        3. the memory chip is the only element in a mobile device that is not broken.
    - The whole process consists of five stages:
        1. Detect the memory chip typology of the device
        2. Physical extraction of the chip (for example, by unwelding it)
        3. Interfacing of the chip using reading/programming software
        4. Reading and transferring data from the chip to a PC
        5. Interpretation of the acquired data (using reverse engineering)
- Micro read
    - This method refers to manually taking an all-around view through the lenses of an electron microscope and analyzing data seen on the memory chip, more specifically the physical gates on the chip.
    - In a nutshell, micro read is a method that demands utmost level of expertise, it is costly and time-consuming, and is reserved for serious national security crises.