UNIT 1

INTRODUCTION

1.1) Computer Roles in Crime

The need for computer forensic expertise in law enforcement is growing as digital crime increases exponentially. There are many law enforcement agencies such as your local police force, The FBI as well as countless other agencies who rely on computer forensics to catch criminals.

The role of computer forensics in crime is just going to increase in demand because the need for assistance in retrieving information that can be used as evidence is getting more difficult for law enforcement. Now more than ever this growing field of study demands IT professionals who are experts at this type of data retrieval for law enforcement.

The number one profession for 2015 according to Forbes Magazine is IT professionals and this is just for general types of IT positions. IT expertise in law enforcement is not only a critical position but also one that changes the face of law enforcement with technique and expertise to solve cases and make a real difference.

Computer forensics is quickly becoming used for many different areas of criminal investigations and there is now a methodology that is used. Computers have been widely known for being used in committing crime but now the tables have turned and forensics has the edge using computer forensics to catch criminals who believe they do not leave an imprint when committing certain crimes.

➢ Collecting Criminal Evidence

The role of computer forensics in crime has advanced to evidentiary admission in a court of law. This is very important in how the evidence is maintained and collected and it has become quite a precise process in law enforcement. Demand is high for expertise in computer forensics.

The FBI uses IT professionals to gain serious evidence in their investigations and these crimes can be simple or hacking, espionage and even bank fraud. The FBI now uses computer forensics as a standard tool to investigate crime. Using devices such as mobile phones, tablets, and hard drives to collect the evidence needed to prove premeditation in some cases.

Computer forensics is the new frontier of criminal investigation for these agencies and it is growing daily. As technology enhances so do the crimes associated with using technology in criminal activity.

Computer forensics is widely known for catching criminals in various types of fraud. However, investigators are now using computer forensics to catch murderers, and access encrypted data daily that will stand as evidence in a court of law.

➢ Computer Forensics Tools and Tasking

Those who decide to enter this vocation are considered investigators. They will investigate encrypted files and using the "live box" method along with many other great new types of software used in the latest techniques available. Information technology professionals who choose this profession are considered in a class by themselves.

Many of the tasks included in this particular part of criminal investigation are recovering deleted files, deleted passwords and checking for breeches of security for cyber-crime. Once the evidence is collected it must be contained and translated for lawyers, judges and juries to examine.

While one might think that recovering fraud data is the main task of computer forensics this is just simply not true anymore. The origin of computer forensics began this way as most of the cases solved in the beginning were of this type. However, The BTK Killer was also caught and evidence was used in his court trial from computer forensics discovered in a search of his home.

Computer forensics goes back as far as floppy discs? Yes it certainly does and now police use their computers for everything from searches to warrants and as technology grows so will the ways criminals hide their activities. There does not seem to be a ceiling on technology and the ways it is investigated.

➢ Cold Case Files Solved Using Computer Forensics

Law Enforcement agencies are also using computer forensics to reopen and solve cold case files. This is a great advantage as technology grows so do the ways to collect the information from old hard drives to solve crimes that have gone unsolved for years.

The role of computer forensics in crime is increasing as databases are being introduced to hold case files for law enforcement. The simple gathering and organization of old forensics

from unsolved cases have brought forward details that investigators might have missed in initial investigations. These innovations are helping to change the face of criminal investigation.

1.2) Processing and the Phases of Forensics Investigation

Pollitt has proposed a methodology for dealing with digital evidence investigation so that the results with be scientifically reliable and legally acceptable.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

It comprises of 4 distinct phases.

Figure 1:

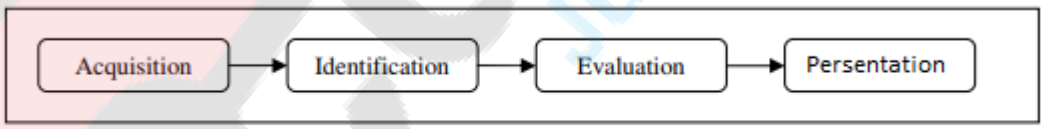


Figure 1: Computer Forensic Investigative Process

Computer Forensic Investigative Process In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority.

It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human.

The Evaluation phase comprise of the task to determine whether the components indentified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence.

In the final phase, presentation, the acquired & extracted evidence is presented in the court of law.

The process of digital forensics can be broken down into three categories of activity: acquisition, analysis, and presentation.

Acquisition

Refers to the collection of digital media to be examined. Depending on the type of examination, these can be physical hard drives, optical media, storage cards from digital cameras, mobile phones, chips from embedded devices, or even single document files. In any case, media to be examined should be treated delicately. At a minimum the acquisition process should consist of creating a duplicate of the original media (the working copy) as well as maintaining good records of all actions taken with any original media.

Analysis

Refers to the actual media examination—the "identification, analysis, and interpretation" items from the DFRWS 2001 definition. Identification consists of locating items or items present in the media in question and then further reducing this set to items or artifacts of interest. These items are then subjected to the appropriate analysis. This can be file system analysis, file content examination, log analysis, statistical analysis, or any number of other types of review. Finally, the examiner interprets results of this analysis based on the examiner's training, expertise, experimentation, and experience.

Presentation

Refers to the process by which the examiner shares results of the analysis phase with the interested party or parties. This consists of generating a report of actions taken by the examiner, artifacts uncovered, and the meaning of those artifacts. The presentation phase can also include the examiner defending these findings under challenge.

1.3) Different types of digital forensics

Digital forensics is a constantly evolving scientific field with many sub-disciplines. Some of these sub-disciplines are:

- **Computer Forensics –**

The purpose of computer forensics is to obtain evidence from various computer systems, storage mediums or electronic documents.

The identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.

Throughout the course of our investigations we can obtain a wide range of information including: system and file transfer logs; internet browsing history; email and text communication logs; hidden, deleted, temporary and password-protected files; sensitive documents and spreadsheets, and many more.

- **Network Forensics –**

The purpose of Network forensics is to monitor and analyse computer network traffic, including LAN/WAN and internet traffic, with the aim of gathering information, collecting evidence, or detecting and determining the extent of intrusions and the amount of compromised data.

The monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.

1. **Mobile Devices Forensics –**

The recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.

This can include call and communications data such as call logs, test messages and in-app communication via WhatsApp, WeChat, etc, as well as location information via inbuilt GPS or cell site logs.

2. **Digital Image Forensics –**

The extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.

3. **Digital Video/Audio Forensics –**

The collection, analysis and evaluation of sound and video recordings.The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.

4. **Memory forensics –**

The recovery of evidence from the RAM of a running computer, also called live acquisition.

5. Forensic data analysis

During Forensic Data Analysis, we work closely with Certified Fraud Examiners to examine structured data in order to discover and analyse patterns of fraudulent activities resulting from financial crime.

6. Database forensics

Database forensics is concerned with the forensic study of databases and their metadata. During our investigations we can use information from database contents, log files and in-RAM data to create timelines or recover pertinent information.

In practice, there are exceptions to blur this classification because the grouping by the provider is dictated by staff skill sets, contractual requirements, lab space, etc. For example:

- Tablets or smartphones without SIM cards could be considered computers.
- Memory cards (and other removable storage media) are often found in smartphones and tablets, so they could be considered under mobile forensics or computer forensics.
- Tablets with keyboards could be considered laptops and fit under computer or mobile forensics.

The science of digital forensics has a seemingly limitless future and as technology advances, the field will continue to expand as new types of digital data are created by new devices logging people's activity. Although digital forensics began outside the mainstream of forensic science, it is now fully absorbed and recognised as a branch of forensic science.

1.4) Forensic evidence

Evidence usable in court, specially the one obtain by scientific methods such as ballistics , blood test, and DNA test.

Obviously the main aim of any investigation is to recover some form of digital evidence, objective data that is relevant to the examination. On top of that the investigator might be asked to make some form of analysis of that evidence; either to form an expert conclusion, or to explain the meaning of the evidence.
Computers are used for committing crime, and, thanks to the burgeoning science of digital evidence forensics, law enforcement now uses computers to fight crime.

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other place s. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. In 2005, for example, a floppy disk led investigators to the BTK serial killer who had eluded police capture since 1974 and claimed the lives of at least 10 victims.

In an effort to fight e-crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure. Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems.

1.5)Introduction to Digital Forensics and it uses

Digital Forensics This book is a "short and sweet" introduction to the topic of Digital Forensics, covering theoretical, practical and legal aspects. The first part of the book focuses on the history of digital forensics as a discipline and discusses the traits and requirements needed to become an forensic analyst. The middle portion of the book constitutes a general

guide to a digital forensic investigation, mostly focusing on computers. It finishes with a discussion of the legal aspects of digital forensics as well as some other observations for managers or other interested parties.

Digital forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. Computer forensics follows a similar process to other forensic disciplines, and faces similar issues.

Uses of digital forensics

- **Criminal prosecutors**
  Rely on evidence obtained from a computer from a computer to prosecute suspeets and use as evidence.
- **Civil litigation**
  Personal and business data discovered on a computer can be used in fraud divorce , harassment, or discrimination cases
- **Insurance companies**
  Evidence discovered on computer can be used to modify costs (fraud, workers compensation, arson, etc)
- **Private corporation**
  Obtained evidence from employee computers can be used as evidence in harassment, fraud and embezzlement cases.
- **law enforcement officials**
  Rely on computer forensics to backup search warrants and post- seizure handling
- **Individual/private citizens**
  Obtain the services of professional computer forensic specialists to supports claims of harassment, abuse or wrongful termination from employment.

1.6) Introduction of cyber crime

Cyber Crimes and Cyber Laws- Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security etc…

Cyber Forensics Investigation- Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking.

Cyber Security- Introduction to Cyber Security, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team, Reporting Cyber crime, Operating System Attacks, Application Attacks, Reverse Engineering & Cracking Techniques and Financial Frauds.

Computer crime refers to criminal activity involving a computer. The computer may be used in the commission of a crime or it may be the target.

Net-crime refers to criminal use of the Internet. Cyber-crimes are essentially a combination of these two elements and can be best defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

In its most simple form, cyber-crime can be defined as any illegal activity that uses a computer as its primary means of function. The U.S. Department of Justice broadens this definition to include any illegal activity that uses a computer for the storage of evidence. The term 'cyber-crime' can refer to offenses including criminal activity against data, infringement of content and copyright, fraud, unauthorized access, child pornography and cyber-stalking.

There are two main categories that define the make up of cyber-crimes.

Firstly those that target computer networks or devices such as viruses, malware, or denial of service attacks.

The **second** category relate to crimes that are facilitated by computer networks or devices like cyber-stalking, fraud, identity-theft, extortion, phishing (spam) and theft of classified information.

UNIT 2
DATA RECOVERY

2.1) Encrypted Data Recovery

Are you unable to access your encrypted business critical data? Do not worry! Stellar Encrypted Data Recovery services can help you to get your data back in a readable form.
Stellar has proven capabilities to recover data from encrypted hard disk or any other storage media device. With Our in-house Research & Development team along with data recovery experts, Stellar has in-depth knowledge about various encryption algorithms used by most of the popular third-party encryption software.
Encryption is used to protect your confidential business data from unauthorized access. However, sometimes even the authorized person with a valid password can't access the data because of issues with encryption or if something goes wrong with the media device.

One may get any of these errors due to a problem with encryption or while decrypting your data carrier.

- Fatal Error
- Decrypt Error
- Media not encrypted
- SafeBoot Error/ SafeBoot corrupted
- Blue Dump (An unusual blue screen of death)
- SG kernel halted (On SafeGuard encryption) etc.

What is Data Encryption?

Data encryption, using any third party encryption software is used to make data non-readable to any unauthorised person. The encryption software uses mathematical calculations and algorithms that transform plaintext into cyphertext. The recipient of an encrypted message uses a key which triggers the algorithm mechanism to decrypt the data, turning it into the original plaintext version while displaying on the computer screen.

Stellar can efficiently recover your data by following Third Party Encryption software:

- Safeboot
- SafeGuard
- Pointsec
- EPST
- PGP
- CREDANT
- Windows encryption

Dos & don'ts while decrypting data:

- Don't decrypt the encrypted data on your own if the drive has bad sectors, or else, you will lose data beyond the scope of recovery.
- Always ensure the health of the hard drive before trying decryption.
- Don't decrypt your valuable data if you are not sure, that the decryption key you have is the correct one. Multiple usages of the wrong key can encrypt or lock the encrypted data, making data recovery virtually impossible.

Contact encrypted data recovery experts immediately, once you recognise the problem with the data.

Stellar's systematic and scientific process ensures safe recovery of your data from the encrypted hard drive:

Analysis:

At Stellar, our **encryption data recovery professionals**, first of all, analyse the data loss/inaccessibility problem to follow right data recovery approach. In case of the physically damaged media device, We use a controlled environment of **CLASS 100 Clean Room.**

Ensure Data Safety through Cloning

For the security of data as well as the state of original media, we make the clone of the source media.

Encrypted Data Recovery:

With our cutting-edge data recovery tools and techniques, we first recover the data in the encrypted form and then decrypted. To decrypt the data, the experts at Stellar would need details of encryption software used and its necessary files along with the password.
Be it a case of forgotten password or corruption of the encryption algorithm, our R & D experts have in-depth knowledge to decrypt the data into its original form successfully.

Definitions:

Encryption is a method of turning meaningful information (known as the plaintext) into an obscured format (the ciphertext) by means of an algorithm (cipher). Encryption algorithms use a key to obscure the data (encryption) and to recover the plaintext (decryption). Good modern algorithms make it infeasible to recover the plaintext from the ciphertext without obtaining the decryption key, and so to protect encrypted data only the key needs to be kept secret. They also make the ciphertext indistinguishable from random data, which can make the use of encryption difficult to prove. For these reasons, encryption is one of the best methods for concealing information and is increasingly used by criminals as a method for hiding their files. It is also used by ordinary people and organisations to minimise the risks of personally identifiable information getting into the wrong hands when, for example,

a laptop is stolen (Casey & Stellatos, 2008). The terms password and key will be used interchangeably to mean either the key to decrypt the data or a password which unlocks a readily-available decryption key.

Full disk encryption (FDE) is when a whole hard drive or the entirety of a particular volume has been encrypted. This can be done using software or hardware. Software such as BitLocker, available on Windows Vista and Windows 7 Ultimate and Enterprise editions, will encrypt everything apart from the Master Boot Record (which it boots from). Hardware based methods can encrypt the disk completely, and are currently supported by a number of hard drive companies including Hitachi and Seagate. Both methods require a password on machine boot-up to decrypt the hard drive. When turned off, the whole hard drive is seemingly filled with random data, and without knowing the password is virtually impossible to decrypt. Hardware which assists FDE includes the Trusted Platform Module (TPM) – a secure cryptoprocessor that can secure encryption keys. Many new laptops have the TPM chip built in, and it can be used by FDE software such as BitLocker as one of the methods of identification. File encryption involves encrypting files within an operating system rather than entire disks or volumes. It can mean encryption of single files, such as an encrypted Microsoft Word document, or encryption of entire folder, for example with Windows Encrypted File System (EFS).

What is Decryption ?

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

2.2) Recovery deleted file

If you ever unintentionally deleted a file, you may have been able to retrieve it from the Recycle Bin. Or, if it was past that stage and the file was really important, you may have used System Restore. You may even have looked for recovery software.

But what's actually happening when you delete and recover those files? And are they ever truly gone? We examine the steps a forensic analyst would use to both recover deleted files and permanently delete those they want gone forever.

Deleting a file in Windows

When you send a file to the Recycle Bin, nothing happens to the file itself. The only change is in a pointer record that showed the location of the file before you deleted it. This pointer now shows the file is in the Recycle Bin. Taking the removal one step further, which can be achieved by emptying the Recycle Bin or using Shift + Delete, this pointer record is now what gets deleted.

So Windows will no longer "know" the physical location of the file. And the physical space it occupies on the hard disk is now free and ready to be used for a different objective. But it's not immediately overwritten. This is by design. The data that was in the file is still in that same location until the operating system uses that physical location for a different purpose.

How does that help us?

Let's for the sake of this article assume that System Restore or another backup method was not enabled, because if it were, that would the second method to try and get those important files back. The problem is that with System Restore, we sometimes dread the other changes that may be undone in the process of using it. Especially if the last usable restore point is an old one.

Knowing how the deletion procedure in Windows works can help us if and when we want to recover important deleted files. You should realize that every change you make after deleting that file diminishes the chance of getting it back in one piece. Defragmenting, for example, re-arranges a lot of the physical locations that files are in and can overwrite the "freed-up" space.

The mere act of looking for recovery software, downloading it, and installing it, may be the very thing that renders the file unrecoverable.

This is where forensic analysts come into play. While most home users wouldn't perform many more tasks to find deleted files than mentioned above, forensic analysts will take the drive that they want to examine out of operation and slave it on another system, creating an exact snapshot image of all the data contained on the drive. This method allows them to examine the data without making any changes to the drive. And if they make changes to the copy, there is no harm done, as they can make a new copy from the original.

What if I really want my files to be deleted?

Deleting a file may erode it or make space for other files, but is it ever truly 100 percent gone? For example, are there effective ways of deleting the content of a hard drive when you sell your computer? Well, the short answer is "No." There is no method of deletion that I would trust 100 percent. There are professional recovery tools that claim they will be able to recover files even when the drive has been re-partitioned and re-formatted.

What a forensic analyst might do is to overwrite a whole hard disk and fill every addressable block with zeroes (ASCII NUL bytes). There are secure drive erase utilities for this purpose

that can reach a high efficiency rate when used several times on the same drive. At this point, there is no way of recovering overwritten data.

There is software that can erase specific files and folders by overwriting them. Take note that this procedure could turn out to be useless if you have any type of automatic backup system in place, which is recommended given the current number of ransomware threats that are out there.

And if you want to keep on using a drive, but don't want anyone else to have access to your important files, we would advise you to use encryption. You can encrypt specific data or the whole drive to prevent uninvited eyes from opening them.

There are important differences between deleting, erasing, and overwriting. When it comes to recovering and deleting files, think like a forensic analyst. If you want to be able to recover a deleted file, the method you use will be very different from wanting to make a file virtually disappear. Choose wisely and you'll better protect your data in the long run.

2.3) Identifying False Images And Steganography Methods For Media Data Including Text, Image And Audio Data 2

2.3.1) Identifying False Images

Eyes and Positions

Because eyes have very consistent shapes, they can be useful for assessing whether a photograph has been altered.

A person's irises are circular in reality but will appear increasingly elliptical as the eyes turn to the side or up or down

(*a*).One can approximate how eyes will look in a photograph by tracing rays of light running from them to a point called the camera center

(*b*).The picture forms where the rays cross the image plane (*blue*). The principal point of the camera—the intersection of the image plane and the ray along which the camera is pointed—will be near the photograph's center.

My group uses the shape of a person's two irises in the photograph to infer how his or her eyes are oriented relative to the camera and thus where the camera's principal point is located

(*c*). A principal point far from the center or people having inconsistent principal points is evidence of tampering

(*d*).The algorithm also works with other objects if their shapes are known, as with two wheels on a car.

The technique is limited, however, because the analysis relies on accurately measuring the slightly different shapes of a person's two irises. My collaborators and I have found we can reliably estimate large camera differences, such as when a person is moved from one side of the image to the middle. It is harder to tell if the person was moved much less than that.

Send in the Clones

Cloning- the copying and pasting of a region of an image—is a very common and powerful form of manipulation.

This image is taken from a television ad used by George W. Bush's reelection campaign late in 2004. Finding cloned regions by a brute-force computer search, pixel by pixel, of all possible duplicated regions is impractical because they could be of any shape and located anywhere in the image. The number of comparisons to be made is astronomical, and innumerable tiny regions will be identical just by chance ("false positives"). My group has developed a more efficient technique that works with small blocks of pixels, typically about a six-by-six-pixel square (*inset*).

For every six-by-six block of pixels in the image, the algorithm computes a quantity that characterizes the colors of the 36 pixels in the block. It then uses that quantity to order all the blocks in a sequence that has identical and very similar blocks close together. Finally, the program looks for the identical blocks and tries to "grow" larger identical regions from them block by block. By dealing in blocks, the algorithm greatly reduces the number of false positives that must be examined and discarded.

When the algorithm is applied to the image from the political ad, it detects three identical regions (red, blue and green).

Camera Fingerprints

Digital retouching rarely leaves behind a visual trace. Because retouching can take many forms, I wanted to develop an algorithm that would detect any modification of an image. The technique my group came up with depends on a feature of how virtually all digital cameras work.

A camera's digital sensors are laid out in a rectangular grid of pixels, but each pixel detects the intensity of light only in a band of wavelengths near one color, thanks to a color filter array (CFA) that sits on top of the digital sensor grid. The CFA used most often, the Bayer array, has red, green and blue filters arranged as shown below.

Each pixel in the raw data thus has only one color channel of the three required to specify a pixel of a standard digital image. The missing data are filled in—either by a processor in the camera itself or by software that interprets raw data from the camera—by interpolating from the nearby pixels, a procedure called demosaicing. The simplest approach is to take the average of neighboring values, but more sophisticated algorithms are also used to achieve better results. Whatever demosaicing algorithm is applied, the pixels in the final digital image will be correlated with their neighbors. If an image does not have the proper pixel correlations for the camera allegedly used to take the picture, the image has been retouched in some fashion.

My group's algorithm looks for these periodic correlations in a digital image and can detect deviations from them. If the correlations are absent in a small region, most likely some spot changes have been made there. The correlations may be completely absent if image-wide changes were made, such as resizing or heavy JPEG compression. This technique can detect changes such as those made by Reuters to an image it released from a meeting of the United Nations Security Council in 2005 (*above*): the contrast of the notepad was adjusted to improve its readability.

A drawback of the technique is that it can be applied usefully only to an allegedly original digital image; a scan of a printout, for instance, would have new correlations imposed courtesy of the scanner.

2.3.2) Steganography Methods For Media Data Including Text, Image And Audio Data

Steganography Methods

Steganography is technique and art of hiding a secret message in carrier file so the existence of the secret messages cannot be known.

If anyone knew the existence of the secret message with its carrier file then steganography is failed. This paper will be discussing the various types and techniques of steganography on text, image, audio, and video as a media.

Steganography is not a new term but has been used thousands of years ago. This is a technique for allowing two or more people to silently communicate with each other by hiding any secret message on a media cover. Files used as media can be text, audio, image or digital video formats.

TYPES OF STEGANOGRAPHY METHODS

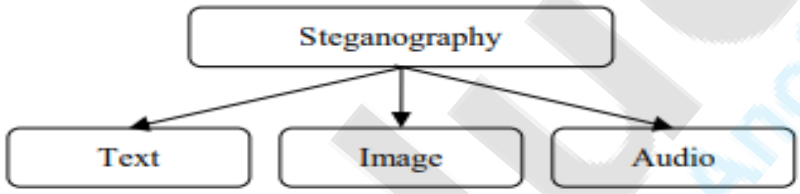


Fig.1 Steganography types diagram

Text Steganography:

It hides the text behind some other files, changing the format of an existing text within a file, to change the words within the text or to generate random character sequences. Basically here we use a text file as a cover media to embed the secret information. It is more vulnerable to attack as it can be easy for an attacker to detect the pattern,

Text steganography its self is has this following three categories such as :

a. Format Based Methods, in this method text data is embedded in the carrier text by changing the format of the cover text itself.

b. Linguistic Methods, in this method just doing analysis the linguistic.

c. Random and Statistical generation methods, generating its carrier text according to the statistical and embedding the information in random sequence of characters.

Text steganography is the most difficult kind of steganography because a text file lacks a large scale redundancy of information in comparison to other digital medium like image, audio and video. Many languages are use to hide data like Persian, Arabic, Hindi, English etc.There is characteristic of English language such as inflexion, use of periphrases and fixed word order. Conversion means that with minimum change of the word will make the relationship of the words into a sentence may be indicated.

Image Steganography:

The process of concealment of information into the carrier image in the absence of degradation in the image and make the image robust enough to not let the users who have nothing to do with this information cannot access it. The secret message is embedded into a carrier image as a noise because human eyes can not detect a difference between the original image and stego image.

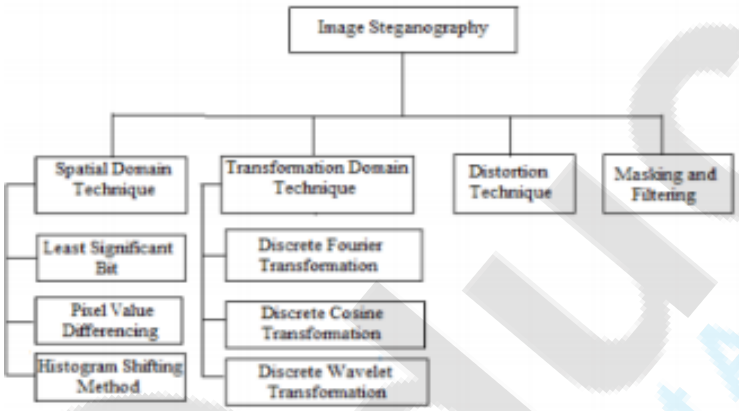


Figure 2: Image steganography techniques [15]

a. Spatial Domain Technique.

For hiding the data some bits are directly changed into the image pixel values bitwise also include, the intensity of pixels and noise manipulation. There are many ways to perform embedding file in Spatial Domain, the easiest is Least Significant Bit (LSB).

b. Transformation Domain Technique.

This technique has a threat like an image processing operations (compression, docking and enhancement) to this technique, because of that transformation domain is hides the secret message in the significant area in the carrier image

c. In the transformation domain

The first thing to do is convert the image from spatial domain into transformation domain and then the secret message is embedded into carrier image. These techniques hide data by mathematical functions

d. Distortion Technique

The information is embedded and store in signal distortion. This technique requires knowledge and carefulness in looking different between the original carrier image and stego image after information embeds during process of decoding.

e. Masking and Filtering

The image with 24bit of size or greyscale type is usually applying masking and filtering technique and using different applications to hide a message. Hiding information by marking the image, this technique is similar to paper watermark, this technique imparts information in a more significant image area than just hiding in the noise level.

For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results: (00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden.

Audio Steganography:

Human Auditory System(HAS) is more sensitive than Human Visual System(HVS), that is one of the reasons that makes embedding message in audio file in any different method is more difficult than other formats

These are the most common method that uses for embedding process in audio file:

a. LSB Coding

b. Parity Coding

c. Echo Data Hiding

In Audio steganography, there is some format that can use as a cover media for embedding the file such as MP3, WAV, MIDI etc.

There are various techniques of audio steganography:

a. LSB Coding: The least significant byte of carrier file is replaced with the bytes of the secret message. Generally why the rightmost bit is chosen for the replacement, because considered as the LSB as it has the least impact on the quality of file.

b. Parity Coding: The parity bit of the cover file is checked for similarity, if similarity exists then no action will be done and if the dissimilarity exists then any bit LSB will be slightly changed (cover file or secret message) to make parity equal.

c. Echo Data Hiding: The information is inserted by adding an echo sound to the cover file. Embedding data is expressed in terms of decay rate, initial amplitude and delay.

a) The initial amplitude is used to determine the original data sound.

b) Decay rate is useful for determination of echo function to be made.

c) The Offset function is used to determine the distance between the original speech signals with the echo that has been made.

UNIT 3
DIGITAL EVIDENCE CONTROLS

3.1)Uncovering attacks that evade detection by event viewer and task manager

For the last twenty years intruders have made unauthorized access to corporate, educational, government, and military systems a routine occurrence. During the last ten years structured threats have shifted their focus from targets of opportunity (any exposed and/or vulnerable asset) to targets of interest (specific high-value assets). The last five years have shown that no one is safe, with attackers exploiting client-side vulnerabilities to construct massive botnets while pillaging servers via business logic flaws.

Despite twenty years of practical experience trying to prevent compromise, intruders continue to exploit enterprises at will. While they may not be successful attacking any specific asset (unless inordinate resources are applied), in aggregate intruders will always find at least one viable avenue for exploitation. The maxim that "prevention eventually fails" holds for any enterprise of sufficient size, complexity, and asset value to attract an intruder's attention. The threshold has fallen to the point where a single home PC is now considered "worthy" of the same sorts of attacks levied against multibillion-dollar conglomerates.

In a world where the adversary eventually breaches some aspect of a target's protective measures, what's an enterprise security manager to do? The answer is simple:

1) detect compromise as efficiently as possible;

2) respond to incidents as quickly as possible; and

3) investigate using digital forensics as effectively as possible.

This article will provide several ways to think about this issue and implement computer incident detection, response, and forensics capabilities to support your enterprise.

Incident Detection

Incident detection has suffered from a variety of misconceptions and miscommunications during its history. One of these has been the narrow way in which most operators view the detection process. I recommend thinking of incident detection in terms of three "orders."

First order incident detection is the traditional way to apply methods to identify intrusions. First order detection concentrates on discovering attacks during the reconnaissance (if any) and exploitation phases of compromise. Reconnaissance is the process by which an intruder learns enough about the target to effect intrusion. Exploitation is the process of abusing, subverting, or breaching a target, thereby imposing the intruder's will upon the asset. Almost all security products that seek to detect and/or "prevent" attacks monitor activity during these stages of the compromise lifecycle.

Second order incident detection moves beyond reconnaissance and exploitation to the final three stages of compromise: reinforcement, consolidation, and pillage. Reinforcement is the process by which an intruder leverages the unauthorized access gained during exploitation in order to build a more stable platform for repeated re-entry. Downloading and installing a remote access Trojan program is a classic reinforcement activity. Consolidate is the act of controlling a compromised asset using the means installed during reinforcement. Pillage is the execution of the intruder's ultimate plan, which could be pivoting on the target to attack another system, exfiltrating sensitive information, or any other nefarious plan the intruder may wish to execute. Second order detection focuses on identifying any of these final three phases of compromise, which can be highly variable and operate at the discretion of the intruder.

Third order incident detection occurs outside the realm of the five phases of compromise by concentrating on post-pillage activities. Whereas first- and second-order detection is done at the enterprise, either by watching hosts, network traffic, logs, or possibly even sensitive data, third order detection takes place outside the enterprise. Third order detection seeks to discover indications that preventative and detection mechanisms have failed by finding the consequences of an intrusion. Looking for these sorts of signs could take the form of searching for, and finding, private company documents on peer-to-peer networks, or intruder-operated botnet servers, or a competitor's release of a product uncannily similar to your company's own. Each of these events indicate a breach or policy violation occurred, yet none may have been detected by conventional means. Third order detection is a powerful way to determine if the formal detection mechanisms operated by an organization's security team make any difference in the real world.

A complementary way to think about detection takes the form of six maturity levels. Using the ideas below, you can determine how advanced your detection initiative may be.

Level 0. No primary detection method exists. No formal data sources are used. No actions are taken, since this "blissful ignorance" hides the fact that the enterprise could be (and probably is) severely compromised.

Level 1. Customers, peer organizations, and users are the primary detection methods. No data sources beyond those provided by the aforementioned parties are available. The predominate reaction is to form an ad-hoc team to fight fires on a repeated basis.

Level 2. Customers, peer organizations, and users are still the primary detection methods. However, the organization has some data store from which to draw conclusions -- once the enterprise knows it must look for clues. Reaction involves more fire fighting, but the officers aren't quite as blind as they were at level 1 thanks to the availability of some logs.

Level 3. The **Computer Incident Response Team (CIRT)** is discovering incidents in concert with the parties listed at levels 1 and 2. Additional data sources augment those aggregated at level 2. The CIRT develops some degree of formal capability to detect and respond to intrusions.

Level 4. The CIRT is the primary means for detecting incidents. All or nearly all of the data sources one could hope to use for detection, response, and forensics are available. The CIRT exercises regularly and maintains dedicated personnel, tools, and resources for its mission.

Level 5. The CIRT is so advanced in its mission that it helps prevent incidents by identifying trends in the adversary community. The CIRT recommends defensive measures before the enterprise widely encounters the latest attacks. The CIRT operates a dedicated security intelligence operation to stay in tandem or even ahead of many threat agents.

Incident detection natually leads to incident response, where actions are taken to contain, eradicate, and recover from intrusions.

Incident Response and Forensics

Twenty years ago incident responders were taught to locate a potentially compromised computer and literally, physically, "pull the plug." The idea was to eliminate the possibility that an intruder occupying a compromised system could notice a normal shutdown and implement techniques to evade detection. Incident responders also worried that intruders might have planted rogue code that started cleanup routines upon initiation of a shutdown command.

Following the abrupt removal of the power cord, incident responders would duplicate the hard drive (usually 40MB -- if it had a hard drive at all in 1988!) and scrutinize the duplicate for evidence of malfeasance. Despite the small hard drive size, this process took time, physical locality (to acquire the hard drive), and expertise.

In 2008, and really for the last decade, the situation has been vastly different. Pulling the plug has been a discredited strategy for years. The major problem with abruptly removing power is the removal (heroic freezing efforts to the contrary) of volatile evidence from system RAM. System RAM is the place where computers store much of the data that incident responders care about, like running processes, active network connections, and so on. Most of that sort of high-value information is not stored on the hard drive, so it perishes when power disappears.

For example, do you remember the Slammer worm mentioned previously? Slammer was completely memory-resident. Remove the power and Slammer disappears. Unless an intruder takes steps to entrench himself on a system (in the reinforcement stage), sometimes a simple reboot is enough to remove him (at least temporarily). If the original vulnerability persists, re-exploitation may quickly follow. For a certain category of stealth-minded intruders, reliance on re-exploitation is the preferred means to maintain a low-profile network presence.

The question of who pulls the plug, and when it could happen, is also paramount in 2008. Most important systems run in data centers built for uptime and redundancy. Pulling the plug isn't a normal operation, and even getting to the server in question can be an adventure. Furthermore, few asset owners would consent to having their money-making systems abruptly removed from operation. Some managers are willing to tolerate

compromise because losing a production host is considered the greater risk (never mind that hacker -- we need to make money!).

Given these realities, incident response in 2008 is now a different animal. Often a system suspected of being compromised is on another continent, in the hands of a user who may not even speak the same language as the security team. Hard drives are routinely 80-160GB on laptops and more than 500GB on servers, with storage area networks and related systems easily exceeding any investigator's ability to duplicate. With such huge volumes of data to analyze, it makes more sense to concentrate on the 4GB of virtual memory present on 32-bit systems.

Incident responders are increasingly relying on live response, or the collection and analysis of system RAM for indicators of compromise. Live response activities have been used for the last eight to ten years by professional investigators in high-end cases, but modern realities are forcing most security pros to add the techniques to their repertoire. Current tools usually push an agent or executable to a remote system, capture or parse memory, and communicate the results to a central location. There an expert human or, in some cases, a series of programs reviews the evidence for signs of malware or unusual activity.

In addition to remote retrieval and analysis of memory, incident responders and forensic investigators are trying to avoid duplicating the entire hard drive of target computers. Increasingly it is just not technically possible or cost effective to do so. Judges, agents, and investigators who were taught that only a "bit for bit copy" was a "forensically sound copy" will have to wake up to the expansive nature of today's digital environment. Why copy a 2-terabyte RAID array on a server if cursory analysis reveals that a small set of files provides all of the necessary evidence to make a sound case? Expect greater use of "remote previews" during incident response and select retrieval of important files for forensic analysis.

In addition to focusing on just the material that matters, modern incident response and forensic processes are more rapid and effective than historical methods. When hard drives were 40MB in size, it was feasible for a moderately skilled investigator to fairly thoroughly examine all of the relevant data for signs of wrongdoing. With today's volume of malicious activity, hard drive size, and efforts to evade investigators (counter- and anti-forensics, for example), live response with selective retrieval and review are powerful techniques.

3.2) Memory Acquisition

Techniques used to extract volatile memory images from target systems are defined as either hardware-based or software-based solutions. Software-based solutions rely on the operating systemin order to perform memory capture. Hardware-based solutions in contrast, directly access the volatile memory of the target system. To date, hardware-based solutions for memory acquisition have been considered the most reliable as it is difficult to obtain a complete and accurate memory snapshot from software.

In order to measure the efficacy of acquisition techniques, Schatz suggests several criteria. These are:

- **The fidelity and reliability of the generated image**

- **The availability of the mechanism (software or hardware) used to capture the image.**

The fidelity and reliability criteria ensure that the image obtained is a "precise copy of the host's memory". In particular these criteria dictate that the resultant memory image should be trustworthy (i.e. the capture process is not interfered with by malware or other actors). Schatz suggests that if the result is not guaranteed to be trustworthy there should be no memory capture at all. This is because if the memory image contains misinformation as a result of tampering, the information gained from its analysis is likely to add confusion to an investigation.

The availability criteria stipulates that the technique must work on arbitrary computers and/or devices — essentially meaning that the method be operating system agnostic and not require specialised techniques.

Vömel and Freiling suggest slightly different criteria used to measure efficacy for an acquisition technique: atomicity and availability. The availability factor extends Schatz's definition, stating that a technique that is characterised by a high availability does not make any assumptions about particular pre-incident preparatory measures and can be applied without knowledge of the execution environment and without requiring that any pre-configurations exist prior to its execution. The atomicity of a technique reflects the demand to produce an accurate and complete image of a host's volatile storage, which encompasses the fidelity and reliability requirements put forth by Schatz.

The remainder of this section will analyse a variety of memory acquisition techniques, using the factors of atomicity and availability as a basis for discussion. For reference, an ideal acquisition method would be characterised as both highly atomic and highly available. Section 3.1 discusses hardware-based acquisition methods.

Hardware-Based Techniques

This section describes hardware-based techniques for memory sample acquisition. It is structured as follows:

Dedicated Hardware

Dedicated hardware techniques are those that involve the installation of a physical device in order to assist investigators in acquiring a memory image from a target system. Carrier and Grand's Tribble is an example of one such device. It is a Peripheral Component Interconnect (PCI) card that enables the capture of physical memory using Direct Memory Access (DMA) at the push of a button.A major advantage of a device such as Tribble is that it is able to obtain a precise copy of physical memory without any interaction with the operating system running on the target machine. As such, it will bypass any subverted processes or memory structures running on the host machine.The Tribble device itself must be installed prior to an investigation. When it is activated, the host machine is suspended to prevent any malicious code being executed during memory imaging. Once the memory dump is completed control is returned to the host operating system.

Until recently hardware devices such as Tribble were characterised as producing accurate and concise (highly atomic) memory images. This was based upon the assumption that as dedicated hardware does not rely on the operating system on the target machine it is able to produce a true picture of a system's memory. This includes any malware or rootkits that may be resident only in the system's volatile memory. However, Vömel and Freiling discuss recent experiments that show that the northbridge chipset of motherboards is able to be reprogrammed to provide a subverted view of the system's memory, allowing regions to be swapped in and out with both software and hardware processes alike oblivious to the substitution. Although it is currently unlikely, investigators will need to consider that the hardware itself has been compromised when taking a memory snapshot. This means that while hardware-based acquisition techniques generally produce highly atomic memory images, it is not necessarily always the case.

Dedicated hardware solutions for memory acquisition generally have low availability. For instance Tribble requires that the PCI card be installed in the system prior to use.Such devices are not designed to be part of a first responder's triage toolkit, but assume that they will most likely be installed on critical infrastructure where high-stakes intrusions may occur. Dedicated hardware devices may also be used in a honeypot to facilitate learning about the tools and tactics utilised by attackers .

Hardware Bus

A hardware bus facilitates data transfer between components (such as PCI) or between devices (such as USB or FireWire) within computer architectures. Memory acquisition techniques have been developed to exploit the use of the FireWire hardware bus to access the volatile memory of a system.These approaches initially targeted Mac OS X and Linux-based systems, although they have also been shown to work on Windows operating systems. FireWire-based approaches have shown to be quite popular primarily because the bus provides DMA by design. As such, several proof-of-concept applications able to extract raw physical memory from a system through the FireWire bus have been developed.

Compared to dedicated hardware, hardware bus acquisition techniques are much more highly available. This is because hardware bus ports such as FireWire are quite common across both portable and desktop computers. However, Vidstrom illustrates that when FireWire methods of acquisition access the Upper Memory Area (UMA) region of memory they can cause random system crashes. This decreases the reliability and atomicity of the results of this hardware bus approach. Other researchers have also found that the memory images captured through FireWire are often corrupt (i.e. missing data). As such, hardware bus approaches can have low atomicity.

Software-Based Techniques

This section describes software-based techniques for memory sample acquisition. It is structured as follows:

Virtualization

Virtualisation provides isolated and reliable emulated system environments (Virtual Machines (VMs)) that execute within a host computer.VMs are monitored to ensure proper management, sharing and restriction to the available hardware resources. Each VM is equipped with a virtual processor, memory, graphics adapters, network and IO interfaces and may run in parallel with many other VMs.

An important characteristic of VMs, is that they are capable of having their execution paused or suspended. The state of the machine is temporarily frozen and its virtual memory is saved to a harddisk on the underlying host. In the case of VMWare-based VMs, all of this volatile memory datails stored to a .vmem or .vmss file located in the working directory of the guest machine4. As such, the entire memory contents of such VMs can be acquired by simply suspending then copying this generated snapshot of main memory.

Within an environment that makes use of virtualisation, memory acquisition is both highly atomic and readily available. This makes virtualisation-based approaches a highly useful testing ground for both memory analysis and memory acquisition techniques. Any techniques developed to acquire memory can do a bit-by-bit comparison of the data they captured with the .vmem file of the VM. This can help to verify and validate the technique that has been developed.

Crash Dumps

Windows operating systems can be configured to write memory dumps to a file when the system unexpectedly stops working.In the case of a critical system failure the system state is frozen and the main memory as well as relevant CPU information are saved in the system root directory for later examination.These dump files can then be examined with Microsoft's Debugging Tools for Windows or manually analysed. For a memory forensics investigation, a responder may force the generation of a software crash dump by interrupting key system services using a third-party application, or by editing the registry to enable Right-Ctrl+ScrollLock+ScrollLock crash dumps.This technique is only suitable to limited situations as the Windows registry must be modified in order to enable the manual crash dump technique. Furthermore, crash dumps can override parts of the system page file, which can decrease the total amount of evidence available.

User-Mode Applications

It is an extremely challenging task to atomically read physical memory using a user-mode application. Early attempts were able to access the \\.\Device\PhysicalMemory address to gain DMA on a Windows system. However, due to security reasons user-mode access to this object was restricted in Windows Server 2003 and later. As such this technique is no long viable for memory acquisition and researchers have had to develop new techniques for acquisition, commonly involving the execution of another process on the target system.

PMDump was developed to help investigators analyse the memory space of a target system. This tool only extracts the address space of a single process from volatile memory. This has the advantage of completing execution much more quickly and only capturing the memory

space of a process of interest.However, tools such as this must also run as a process within the operating system meaning that they modify the volatile memory of the system from which they are capturing process memory space. Furthermore, PMDump requires the process ID of the process the user wishes extract data from. This is not useful in the situation where the process has hidden itself from the operating system, such as in the case of rootkits.

A key advantage of user-mode applications is that they are characterised by a high level of availability. Such tools can be executed from an external USB flash drive to minimise system impact and be designed such that they will run on most Windows-based operating systems.The primary disadvantages of pure software based approaches is that by the very nature of being a software program, it must be loaded into volatile memory to execute. As such, user-mode applications are not atomic when they acquire memory from a target system. Furthermore, as these applications rely on functions provided by the operating system they are vulnerable to subversion by malicious software. For instance, a rootkit may deny direct access to physical memory and return a modified representation during image generation. As such, the overall atomicity of such techniques is questionable especially in the case of acquiring memory from a target system that may be running malware.

Kernel-Mode Applications

In order to mitigate the shortcomings of user-mode applications, software vendors and researchers are increasingly focusing on developing kernel-mode applications and drivers that can be used to create forensic copies of volatile memory. These techniques are utilised in some freely available tools, such as Memory DD, Windows Memory Toolkit (Community Edition) and Memoryze.
Commercial software vendors have also developed some alternatives. These include Guidance
Software's WinEN (Part of EnCase 6.11 and higher), GMG Systems' KnTDD and Fast Dump Pro from HB Gary.

Kernel-mode applications still suffer from the inherent weaknesses that affect user-mode applications. Even if an application is a kernel-mode driver, it still modifies memory as Windows will create new process and thread structures when it is executed. Such techniques are also susceptible to compromised operating system functionality as per user-mode applications. Furthermore, kernel-based approaches suffer from availability issues as they require the investigator to have administrator privileges to install a driver-based approach onto the system itself prior to utilising it, or to execute a process that requires elevated user privileges. It could be argued that in practice this might not be an issue, due to the common practice of Windows users having administrative privileges.

Operating System Injection

A novel approach to help overcome the inherent issues with software-based approaches to memory acquisition was developed by Schatz in their proof of concept tool called BodySnatcher. The approach injects an independent operating system into the kernel of the target machine. The target machine's native kernel execution is then frozen such that BodySnatcher can then provide an atomic snapshot of the machine's volatile data. A

strength of the tool is that it does not matter if the target operating system has been subverted, as BodySnatcher only relies on its own tool set. Although the technique shows promise as it produces atomic snapshots of memory, its availability is low due to a reliance on specific hardware platforms. In addition, the technique is limited to single processor execution. As a result the acquisition of memory also takes a great deal of time.

Cold Booting Technique

Halderman et al. present a novel approach to the acquisition of volatile memory. Their approach is based on the observation that information is not erased from volatile memory immediately after powering off a machine and may be recovered for a non-trivial amount of time.Halderman et al. present three methods for acquiring volatile memory contents,based on this phenomena of memory remanence. The first and most simple approach is to reboot the machine and launch a custom kernel with a small memory footprint that gives access to residual memory. The second is to briefly cut power, restore power and then launch the custom kernel. The second approach deprives the operating system of any opportunity to scrub the contents of RAM. The third attack involves cutting the power of the target machine and translating the RAM modules to a second computer which is configured to extract their state. This third approach denies the original Basic Input/Output System (BIOS) and computer hardware any chance to clear the memory.

UNIT 4
NETWORK FORENSICS

4.1) Attacks

Network security starts with authorization, commonly with a username and a password. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations. If this authorized, a firewall forces to access policies such as what services are allowed to be accessed for network users. So that to prevent unauthorized access to system, this component may fail to check pote ntially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion detection system (IDS) helps, to detect the malware. Today anomaly may also monitor the network like wire shark traffic and may be logged for audit purposes and for later on high-level analysis in system.Communication between two hosts using a network may be uses encryption to maintain privacy policy.

The world is becoming more interconnected of the Internet and new networking technology. There is a so large amount of personal, military, commercial, and government information on networking infrastructures worldwide available. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.The network security is analyzed by researching the following:

- History of network security
- Internet architecture and security aspects of the Internet
- Types of network attacks and security methods
- Security for internet access in networks
- Current development in the network security hardware and software

Network Security

System and Network Technology is a key technology for a wide variety of applications. It is a critical requirement in current situation networks, there is a significant lack of security methods that can be easily implemented. There exists a “communication gap” between the developers of security technology and developers of networks. Network design is a developed process that is depends on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing network security. It offers modularity, ease-of-use, flexibility, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. In contrast to secure network design is not a well- developed process. There isn’t a methodology to manage the complexity of security requirements. When considering about network security, it should be emphasized that the complete network is secure. It does not only concern with the security in the computers at each end of the communication chain. When transferring from one

node to another node data the communication channel should not be vulnerable to attack. A hacker will target the communication channel, get the data, and decrypt it and re-insert a duplicate message. Though securing the network is just as important as securing the computers and encrypting the message. While developing a secure network, the following needs to be considered.

- **Confidentiality**
  It means that the non-authenticated party does not examine the data
- **Integrity**
  It is a guarantee that the data which is received by the receiver has not been change or Modified after the send by the sender.

Types of Attacks

Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses, etc. Attacks to network from malicious nodes.

Attacks can be categories in two:

"Passive" when a network intruder intercepts data traveling through the network, and, **"Active"** in which an intruder initiates commands to disrupt the network's normal operation.

Active attack

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

Spoofing
When a malicious node miss-present his identity, so that the sender change the topology

Modification
When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

Wormhole
This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network

Fabrication
A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices.

Denial of services
In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the

network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

Sinkhole

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack [1]

Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring.

Traffic analysis

In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

Eavesdropping

This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

Monitoring

In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

Advance attacks

Black hole attack

Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. So that a malicious fake route is create.

Rushing attack

In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver.

Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

Replay attack

It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time,an attacker can intercept the password.

Byzantine attack

A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

Location disclosure attack

Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

4.2)Email forensics

E-mail has emerged as the most important application on Internet for communication of messages, delivery of documents and carrying out of transactions and is used not only from computers but many other electronic gadgets like mobile phones. Over a period of year's e-mail protocols have been secured through several security extensions and producers, however, cybercriminals continue to misuse it for illegitimate purposes by sending spam, phishing e-mails, distributing child pornography, and hate emails besides propagating viruses, worms, hoaxes and Trojan horses. Further, Internet infrastructure misuse through denial of service, waste of storage space and computational resources are costing everyInternet user directly or indirectly. It is thus essential to identify and eliminate users and machines misusing e-mail service. E-mail forensic analysis is used to study the source and content of e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. to collect credible evidence to bring criminals to justice.

E-mail system comprises of various hardware and software components that include sender's client and server computers and receiver's client and server computers with required software and services installed on each. Besides these, it uses various systems and services of the Internet. The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required.

An e-mail communication between a sender 'Alice' having e-mail address 'alice@a.com' and recipient 'Bob' having e-mail address 'bob@b.com' is shown in figure 1.
'Alice' composes an e-mail message on her computer called client for 'Bob' and sends it to her sending server 'smtp.a.org' using SMTP protocol. Sending server performs a lookup for

the mail exchange record of receiving server 'b.org' through Domain Name System (DNS) protocol on DNS server 'dns.b.org'. The DNS server responds with the highest priority mail exchange server 'mx.b.org' for the domain 'b.org'. Sending server establishes SMTP connection with the receiving server and delivers the e-mail message to the mailbox of 'Bob' on the receiving server. 'Bob' downloads the message from his mailbox on receiving server to local mailbox on his client computer using POP3 [2] or IMAP [3] protocols. Optionally, 'Bob' can also read the message stored in his server mailbox without downloading it to the local mailbox by using a Webmail program.

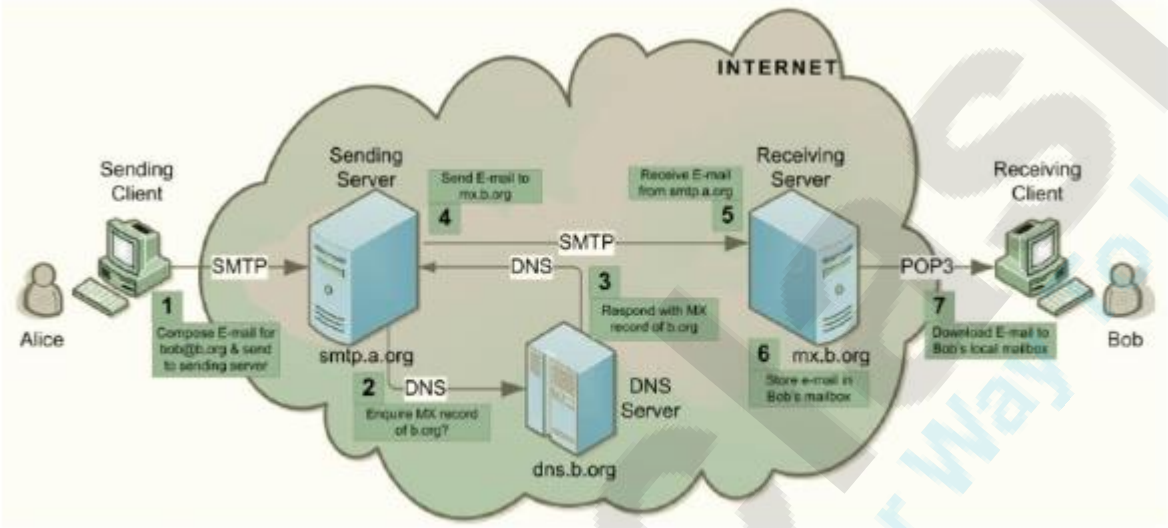


Figure 1: E-mail communication between a sender 'Alice' and recipient 'Bob'

E-MAIL FORENSIC INVESTIGATION TECHNIQUES

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.
Various approaches that are used for e-mail forensic and are briefly defined below:

Header Analysis

Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.

Bait Tactics

In bait tactic investigation an e-mail with http: "<img src>" tag having image source at some computer monitored by the investigators is send to the sender of e-mail under investigation

containing real (genuine) e-mail address. When the e-mail is opened, a log entry containing the
IP address of the recipient (sender of the e-mail under investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the e-mail under investigation) is using a proxy server then IP address of the proxy server is recorded.
The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server's log is unavailable due to some reason, then investigators may send the tactic e-mail containing a) Embedded Java Applet that runs on receiver's computer or b) HTML page with Active X Object. Both aiming to extract IP address of the receiver's computer and e-mail it to the investigators.

Server Investigation

In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries. Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e-mail and server logs only for some limited periods and some may not co-operate with the investigators. Further, SMTP servers which store data like credit card number and other data pertaining to owner of a mailbox can be used to identify person behind an e-mail address.

Network Device Investigation

In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of co-operation by ISP's or failure to maintain chain of evidence.

Software Embedded Identifiers

Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital information about the senders e-mail preferences and options that could help client side evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message.

Sender Mailer Fingerprints

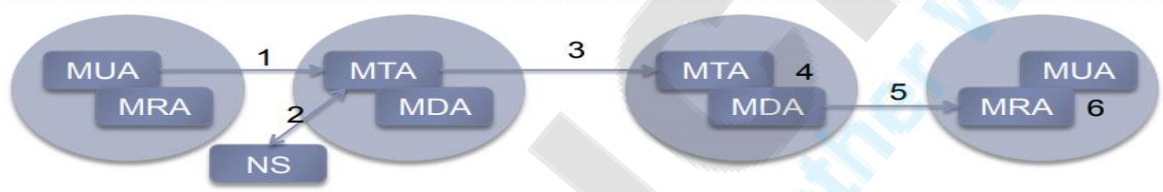
Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e-mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information about the

client computer of the sender can be used to help investigators devise an effective plan and thus prove to be very useful.

Email Forensic Tools

1. **eMail TrackerPro**
2. **EmailTracer**
3. **Adcomplain**
4. **Aid4Mail Forensic**
5. **AbusePipe**
6. **AccessData's FTK**
7. **EnCase Forensic**
8. **FINALeMAIL**
9. **Sawmill-Group Wise**
10. **Forensics Investigation Toolkit(FIT)**
11. **Paraben (Network) E-mail Examiner**

Typical actors in an email flow



- MUA – Mail User Agent
  - E.g. thunderbird, outlook
- MTA – Mail Transfer Agent
  - E.g sendmail, qmail
- MDA – Mail Delivery Agent
  - E.g procmail
- MRA – Mail Retrieval Agent
  - POP/IMAP client
- NS – Name Server
  - DNS server

1. MUA implements smtp client to smtp server
2. MTA solves address using MX record in NS
3. MTA contacts MTA though SMTP
4. Receiving MTA delivers the email to MDA
5. MRA uses IMAP/POP/MAPI to retrieve from MDA
6. MUA presents mail to user

A mail message from Author to Receiver that traverses through aMUA, aMSA, hMSA, MTA (outbound), MTA (Inbound), hMDA, rMDA, rMailServ and rMUA is considered as good mail by the Sender Policy Forum (SPF).

Mails following through other paths are either fully or partially non-SMTP based or uses non-standard transfer modes which are often suspected to contain viruses and spam. Delivery Status Notification (DSN) messages are generated by some components of MHS (MSA, MTA, or MDA) which provide information about transfer errors or successful deliveries and are sent to MailFrom addresses.

Message Disposition Notification (MDN) messages are generated by rMUA which provide information about post-delivery processing are sent to Disposition-Notification-To address.

Out Of Office (OOO) messages are sent by rMDA to return address. The functions and roles of various components shown in the architecture are discussed below.

Message/Mail User Agent (MUA): It works for user actors and applications as their representative within e-mail service. A MUA that works on behalf of Author is called Author MUA (aMUA) and the one that works on behalf of Receiver is called Receiver MUA (rMUA).aMUA creates messages and performs initial submission via Mail Submission Agent (MSA). Besides this, it can also perform creation and posting time archiving in its Message Store.rMUA processes received mail that includes generation of user level disposition control messages, displaying and disposing of the received message and closing or expanding the user communication loop by initiating replies and forwarding new messages. A Mediator performs message re-posting and as such it is a special MUA. For bulk sending services and automatic responder (serving out of office notifications), MUA can be automated. The identity fields relevant to MUA are: From, Reply-To, Sender, To, CC and BCC.

All Mail User Agent (MUA) nodes are software packages that run on client computers and allow end users to compose, create and read e-mail. Some MUAs may be used to send e-mail to the receiving MTAs directly or indirectly. 'Microsoft Outlook', 'Microsoft Outlook Express', 'Lotus Notes', 'Netscape communicator', 'Qualcomm Eudora', 'KDE KMail', 'Apple Mail', and 'Mozilla Thunderbird' are examples of MUAs. Several Web-based e-mail programs and services (known as Webmail) such as 'AIM Mail', 'Yahoo Mail', 'Gmail', and 'Hotmail' which integrate e-mail clients and servers behind a Web server are also used as MUAs.

Message/Mail Store (MS): It serves as a long term message store for MUA which can be located on a remote server or on the machine running MUA. Messages can be organized in a MS in different ways. The MUA accesses the MS either by a local mechanism or by using POP or IMAP.

Message/Mail Submission Agent (MSA): Mail Submission Agent (MSA) accepts the message submitted by the aMUA for posting. It enforces the policies of the hosting ADMD and the requirements of Internet standards before posting the message from an Authors environment to the MHS. These include adding header fields such as Date and Message-ID and expanding an address to its formal Internet Mail Format (IMF) representation. The hMSA is responsible for transiting the message to MTA. The identity fields relevant to MSA are: HELO/EHLO, ENVID, MailFrom, RcptTo, Received, and SourceAddr. The responsibilities of MUA and MSA may be integrated in a single Agent.

Message/Mail Transfer Agent (MTA): A Message Transfer Agent (MTA) relays mail for one application-level "hop". MTA nodes are in effect postal sorting agents that have the responsibility of retrieving the relevant Mail eXchange (MX) record from the DNS Server for each e-mail to be send and thus map the distinct e-mail addressee's domain name with

the relevant IP address information. DNS is a distributed directory database that correlated domain names to IP addresses. MTAs can also be used to compose and create e-mail messages. 'Sendmail', 'Postfix', 'Exim', and 'Exchange Server', are examples of MTAs. A receiving MTA can also perform the operation of delivering e-mail message to the respective mailbox of the receiver on the mail server and thus is also called Mail Delivery Agent (MDA). Unlike typical packet switches (and Instant Messaging services), MTAs are expected to store messages in a manner that allows recovery across service interruptions, such as host-system shutdown. The offered degree of robustness and persistence by MTAs can vary. An MTA can perform well established roles of Boundary MTAs (Onbound or Inbound) or Final MTAs. The identity fields relevant to MTAs are: HELO/EHLO, ENVID, MailFrom, RcptTo, Received, and SourceAddr.

Message/Mail Delivery Agent (MDA): Both hMDA and rMDA are responsible for accepting the message for delivery to distinct addresses. hMDA functions as a SMTP server engine and rMDA performs the delivery action. The identity fields relevant to MDA are: Return-Path and Received.

Relays: SMTP-Relays are the nodes that perform e-mail relaying. Relaying is the process of receiving e-mail message from one SMTP e-mail node and forward it to another one. They are like packet switches or IP routers and make routing assessments to move the message closer to the Recipients. They also add trace information and have all roles of MTA's.

Gateway: Gateway nodes are used to convert e-mail messages from one application layer protocol to other. Gateway nodes named GWSMTP, B accept SMTP protocol based e-mails and transfer them with protocols other that SMTP and GWA, SMTP performs the inverse process at incoming and outgoing interfaces. Gateway nodes GWA,B do not use SMTP either for incoming or outgoing interfaces. A process called Proxy may be done at these nodes when incoming and outgoing interfaces use same protocols.

Web Server (WebServ): These nodes are the e-mail Web servers that provide the Web environment to compose, send and read an e-mail message.

Mai Server (MailServ): They represent e-mail servers providing users mail access service using IMAP or POP3 protocols. They can also provide an internal interface to a Web server for HTTP based e-mail access. The e-mail nodes establish connections with one or more nodes on specific ports for possible email flow between them using a particular protocol. SMTP is an application layer protocol for TCP/IP based Internet infrastructure which sets conversational and grammatical rules for exchanging e-mail between computers. The most commonly-used protocols for e-mail retrieval by client programs are Post Office

Protocol Version 3 (POP3) and Internet Message Access Protocol (IMAP). Table 4, lists the protocols used in e-mail flow between two possible e-mail nodes.

Client Protocols

Post Office Service	Protocol	Characteristics
Stores only incoming messages	POP	Investigation must be at the workstation.
Stores all messages	IMAP MS' MAPI Lotus Notes	Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.
Web-based send and receive	HTTP	Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation

Local Image Storage

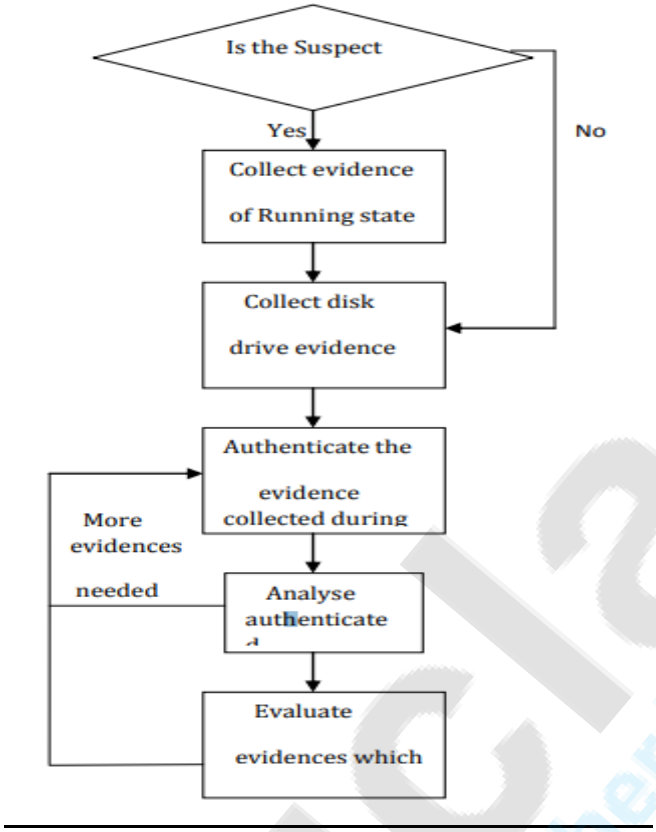
E-Mail Client	Extension	Type of File
AOL	.abi	AOL6 organizer file
	.aim	Instant Message launch
	.arl	Organizer file
	.bag	Instant Messenger file
Outlook Express	.dbx	OE mail database
	.dgr	OE fax page
	.email	OE mail message
	.eml	OE electronic mail
Outlook	.pab	Personal address book
	.pst	Personal folder
	.wab	Windows address book

Commonly used Ports in Email Commuunication

Port No	Protocols/Services	Description
25	SMTP SMTP e-mail server	Simple Mail Transfer Protocol - core Internet protocol used to transfer from client to server (MUA to MTA) and server to server (MTA to MTA)
110	POP3 POP e-mail server	Post Office Protocol allows clients (MUA's) to retrieve stored e-mail
143	IMAP IMAP(4) e-mail server	Internet Message Access Protocol provides a means of managing e-mail messages on a remote server and retrieve stored e-mail
465	SMTPS WSMTP (SSMTP) protocol over TLS|SSL	SMTP via SSL encrypted connection (Unofficial)
993	IMAPS SSL encrypted IMAP	IMAP via SSL encrypted connection
995	POP3S SPOP SSL encrypted POP	POP via SSL encrypted connection
587	MSA	Outgoing Mail (Submission)
80	HTTP	Webmail
443	HTTPS	Secure Webmail

Table 5: Commonly used Ports in E-mail Communication

4.3) Procedure of Computer Forensics



Computer Forensics is a four step process:-

- **Acquisition**

Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices

- **Authentication**

The authentication of the evidence is the process of ensuring that the evidence has not been altered during the acquisition process. In other words, authentication shows that the no changes to the evidence occurred during the course of the investigation. Any changes to the evidence will render the evidence inadmissible in a court. Investigators authenticate the hard drive evidence by generating a checksum of the contents of the hard drive. The algorithms most commonly used to generate these checksums are MD5 and SHA.

- **Analysis**

The most time consuming step in computer forensics investigation is the analysis of the evidence.It is in the analysis phase that evidence of wrongdoing is uncovered by the investigator.

- **Evaluation**

Evaluating the information/data recovered to determine if and how it could be used again the suspect for employment termination or prosecution in court.

THE SOURCE OF DIGITAL EVIDENCE

Digital Evidences come from the target system host data and network data. The main information on a host of evidence comes from some cases as follows.

- System log files
- Data and program files
- Swap files
- Temp files
- Free disk space and system buffers.

Evidence on the network data from some cases as follows.

- Firewall Logs
- Intrusion Detection System logs
- Network communication link records
- Information on network devices

Forensics Analysis

Forensic Analysis with Windows versus UNIX

Windows environment offers few utilities that can be employed by forensic investigators, such utilities like Ms-config help to track system events, other utilities can be used in monitoring user accounts and other user related activities, the Windows operating system does not offer much when it comes to forensic investigations, most of the applied utilities are third party applications that ride on the Windows platform, the operating system itself has little or nothing to offer for investigation, however, the third party applications like FTK and Winhex are considered great choices when it comes to digital analysis, they offer a user friendly environment for analysis even for non professional computer users, they offer appealing GUI and finally Windows based forensic applications actually deliver.

On the other hand, Forensic investigations under the Unix platform is something that can be left for the professionals, first, personally speaking, the UNIX environment appears more professional than the Windows environment, the command line gives it that look, one has to learn a great deal of commands before working with Unix, and that explains the advantage the Windows environment has over UNIX on popularity.

For Forensic Investigation, UNIX offers special commands that can actually aid the work of an investigator, most of these commands are shipped with the Unix OS, they are good and also easy to use for people that can find their way around it. UNIX has various commands that can give full details of user events with Date-Time stamp results, these commands can easily be obtained with usage options by typing the Man command at the Command line.

The Problem with UNIX

However, there are serious concerns with investigations under the UNIX environment, Unix is an Open Source operating system, which makes most of the command files available for use and rewrite, a clever instigator can alter these files to give false results during investigations, the Open Source nature of Unix makes it available for developers to re-engineer the files to suit their purposes, as a result of all these possibilities, the investigation of digital crime under Unix environment is thereby difficult to handle, an investigator should have a clean Unix environment for investigation and acquisition of digital evidence.

Attack on Windows vs UNIX

Attacks on Windows platform can be easily managed, Windows have a unique file system - the FAT file system, also available for Windows is the NTFS file system, deleted files on Windows platform are transferred to the unallocated space and slack spaces on the hard drive, this makes the investigation of attacks related to Windows environment a straight forward procedure once the right tool is acquired, Windows also have log files which contain user log activities and a config file, together with a system restore point that monitors various changes in the Windows environment.

Attacks on Unix environments are a little bit complex to handle, one thing to note is the Unix file system, UNIX OS employs the UFS file system and the ext2 file system, ext2 files are represented as inodes, which are referenced by IO operations to display file contents, unlike Windows file system, Unix file system does not implement slack file system, during file deletion, rather Unix file system makes a note to notify the system that the given Inode is ready for reuse, but however keeps the data there waiting to be overwritten.

Though Unix was developed with networking at heart, there are different attacks that can happen to Unix environment without the consent of the system user, these is mainly possible due to the Open Source nature of the Unix platform, it gives developers and hackers alike the opportunity to study and re-engineer the Operating System, an example is the notorious Suid bit shell attack, in which a Trojan program transfers a shell program to a user accessible directory, and then gives the shell program a permission that makes it executable by the user. UNIX attacks are considerably difficult to trace due to the nature of the environment.

Tools To Recover Data on Windows

- **Drivespy**

It is a forensic DOS shell. It is designed to emulate and extend the capabilities of DOS to meet forensic needs. It includes A built in Sector (and Cluster) Hex Viewer which can be used to examine DOS and Non-DOS partitions.

- **Encase**

It is a computer forensics product which is used to analyze digital media (for example in civil/criminal investigations, network investigations, data compliance and electronic discovery). The software is available to law enforcement agencies and corporations. It includes tools for data acquisition, file recovery, indexing/search and file parsing. Special training is usually required to operate the software.

- **Ilook**

The ILook Investigator Forensic Software is a comprehensive suite of computer forensics tools used to acquire and analyze digital media. It provides the list of allocated and unallocated files and works with compressed zip files.

Tools To Recover Data on UNIX

- **The Coroner' Tool Kit:**

A coroner's means government official who Investigates human death or determines cause of death. The Coroner's Toolkit is a set of tools for post-mortem analysis of a UNIX system. It is designed to discover data or programs which may not be visible to the operating system through the normal file interfaces.

- **The Sleuth Kit**

The Sleuth Kit (TSK) is a library and collection of UNIX and Windows-based tools and utilities to allow for the forensic analysis of computer systems. The seulth kit's tools allow us to examine the layout of disks and other media. It supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools.

Network Forensic Analysis using Tools

Network forensic analysis is the process of monitoring the networks traffic by the system administrator. Using this analysis the system administrator will gather the information about the anomalous traffic. IDSs and Firewalls are also used to store the network traffic for long term analysis.

Similar to other computer forensic tasks recovering and analyzing the evidences which are gathered from the network resources must be done perfectly because it has to be produced in court for legal prosecution. Forensic investigators must follow a framework for doing the investigation process. The step by step approach is discussed below:

- Preparation Phase
- Detection Phase
- Collection Phase
- Preservation and protection Phase
- Examination and analysis Phase
- Investigation and attribution Phase
- Presentation and review Phase

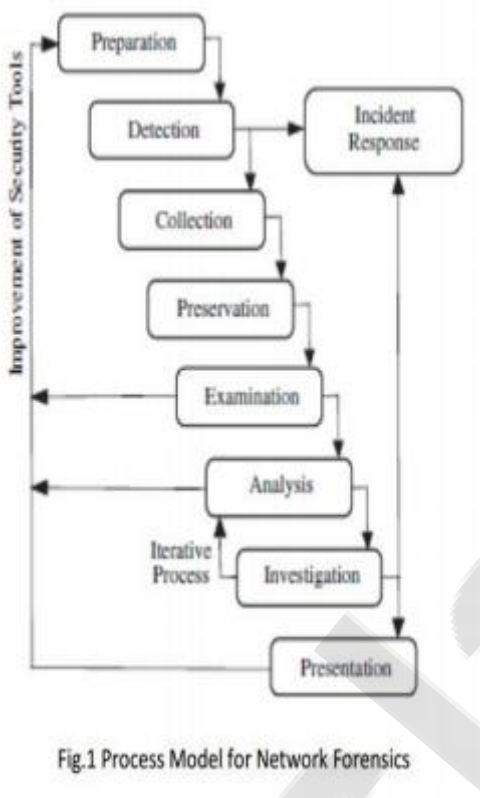


Fig.1 Process Model for Network Forensics

- **Preparation Phase:**

  Since many instruments need to be put out (IDPSs, firewalls, packet analysers) on different points on the network, In this phase is it will ensure the authenticity of the users those who are entering in the network.

- **Detection Phase:** The tools which are deployed in the network will give an alarm or indicate if any security violation is made by the intruders. The traffic is validated quickly in order to assess the attack.
- **Incident Response Phase:** In this phase the attack is identified and the organization will take legal action.
- **Collection phase:** This is the most difficult phase because traffic in the network is very fast to gather the information to trace. It is must to use reliable hardware and software tools to collect maximum no of evidences with minimum impact on the network. Preservation phase: This phase is maintaining the chain of custody of the recovered data. It is must to keep the original data in safe with hashing value; this will give the integrity of the data. Analysis is done in the duplicate copy.
- **Examination phase:** This phase examines previous phase. This is done in a carefully planned way so no key information is lost. All hidden or changed data done by attacker needs to be uncovered. Reduction of high book data is necessary in order to identify the least information holding the highest probable event that proves something.

- **Analysis phase:** Collected event or objects that prove something is analyzed in order to find clearly stated indicator of an invasion.Also, stastical analysis and data mining is performed to search for data and to match it to attacking model. The attacking patterns are put together and rebuilt to understand the purpose and way(s) of doing things of the attack. Investigation Phase: This phase uses information gathered through analysis phase, and Concentrates on identifying attacker, which is the hardest part of analysis phase. Attacker may use many different ways of doing things to hide their plans/desires or their identity, such as IP spoofing or stepping stone attack. Actual approach in Investigation phase depends on attack type.
- **Presentation Phase:** This the final stage in processing model. Well-thought-out paperwork that proves, along with making a statement with explanations are presented in readable and understandable format. Everything that has been did needs to be presented in accordance to related laws and security policy, along with recommendations on how to prevent future attacks.

UNIT 5

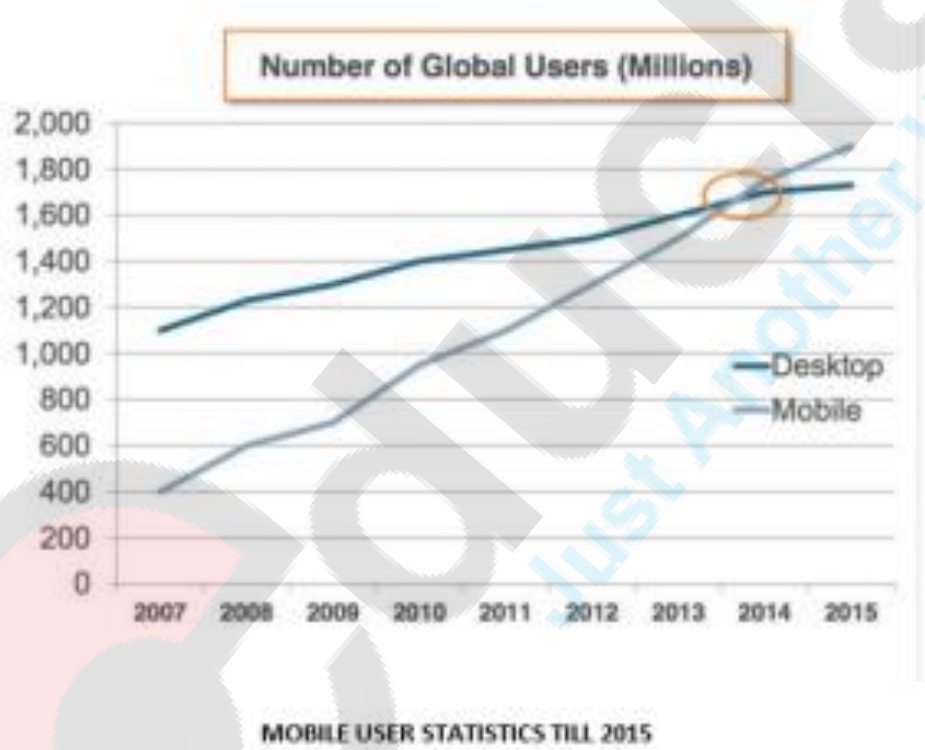
MOBILE PHONE AND ANDROID FORENSICS

5.1) CRIME and Mobile Phone:

Why is mobile a tool of crime?

The creativity and Innovation of the great master Sir Martin Cooper has made a drastic change in the current generation of the world's most interactive beings. Mobile phones in today's world have completely replaced a personal computer or a laptop and is made smart for people to do things faster and smarter. Mobile Phones have changed the history of the technological world by bringing in a combination of techniques, to fulfill the basic necessity of today's generation.

The Mobile phone has become a key role-playing component in the life of a common man. Starting from 16 to 60's without any age limit, the present generation has carved a everlasting path in the skilled growth of the mobile industry creating a boom in the electronics sector. The usage of mobile devices paved a path for the successful growth in the electronic industry.



MOBILE USER STATISTICS TILL 2015

Ever since the usage of Mobile Phones carved a booming path in common man's life, It made it easy for the cyber criminals to use mobile as a medium or tool of attack. When growth of technology created a good impact in the life of a common man, The same technological growth was used to tamper the life of a common man.

Types of mobile phone related crimes

1. Vishing :

Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

- **Purpose :**
- To extract sensitive information from the victim, by means of social engineering.
- Cheating by personation.
- Identity theft

2. Smishing :

Smishing is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device. smishing is short for “SMS phishing.”
Just like phishing, smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again just like phishing, the smishing message usually asks for your immediate attention.
In many cases, the smishing message will come from a “5000” number instead of displaying an actual phone number. This usually indicates the SMS message was sent via email to the cell phone, and not sent from another cell phone.

Purpose :

- To steel sensitive data from the victim's mobile by using a malware.
- Act of Social Engineering.
- To track the victim's device by sending a malware to the device

3. Lottery Scams:

A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing (sometimes including a large check) explaining that "You have won!" a large sum of money in a lottery.

- **Purpose :**
- To make the victim believe that he has won a lottery and extract sensitive information from him.

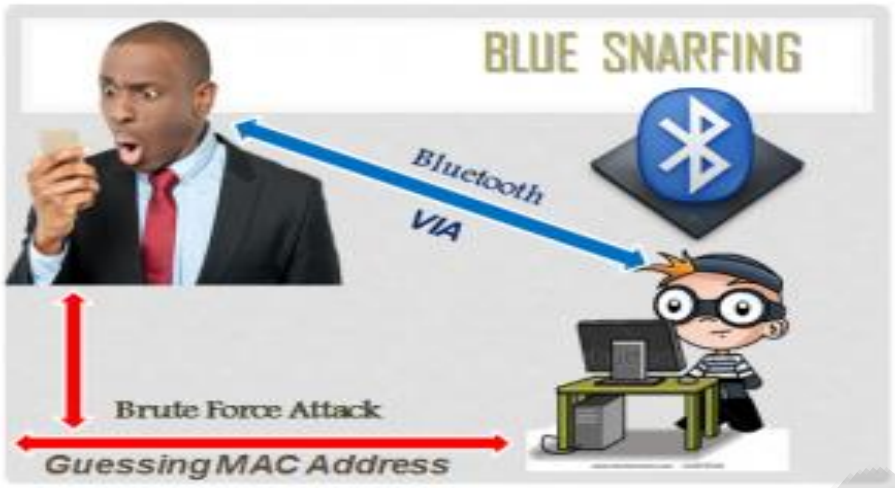
4. The Blue Bugging :

This attack involves the virtual takeover of the victim's phone by performing a backdoor mechanism. A backdoor is generally performed by a developer in the case of troubleshooting a problem, but this mechanism is also performed by attackers to gain access into the victim's device by bypassing the security mechanism.

5. Blue Jacking:

It is a milder version of Blue bugging, it involves sending anonymous, unwanted messages to other users with Bluetooth-enabled mobile phones. A Bluejacker uses a feature originally intended for exchanging contact details or Electronic-Business cards. The attacker adds a new entry in the address book, types in a message and sends it via Bluetooth

6.) Blue Snarfing :



Bluesnarfing is the theft of data from a Bluetooth phone. The attacker, just by running the right software on their laptop, can discover the nearby phone, connect to it without confirmation and download confidential data. Even by turning off the Bluetooth a potential victim cannot be safe from being Bluesnarfed. As a device in hidden state may also be Bluesnarfable by guessing the device's MAC address via a brute force attack.

5.2) Evidence:

Evidence is something tangible that proves a fact. Digital evidence is evidence in electronic form. It can take a variety of forms (media, information, transaction) and can come from many sources (computers, smartphones, wearables, printers, home routers).

Before collecting evidence, the digital forensics examiner must ensure that he has the **legal authority** to identify, collect, and preserve digital evidence. The constant challenge of digital forensic examination is its **fragility**. Digital evidence loses its value if it is not properly collected, preserved, and protected.

Depending on data persistency and volatility, digital evidence can be classified from less fragile to very fragile. Volatile data is stored in main device memory; network connections can be altered or eliminated rapidly. Persistent data stored on device media can still be tampered with or overwritten.

These technical issues combined with legal missteps can affect the admissibility of digital evidence. **Admissible** is the most basic attribute of digital evidence. Admissible evidence must be properly collected and relevant to a case in order to be used in court and a judge, jury, or tribunal may use it in order to decide a case. In order for digital evidence to be admissible, it must be also authentic and reliable.

A forensic examiner must be able to show that the evidence, in its original state, relates to the incident in a relevant way. The **authenticity** of the evidence is proved by demonstrating its provenance. Evidence that is not **reliable** is not admissible.

Evidence collection and analysis procedures must be trusted on the evidence's authenticity and veracity. The **validity** of evidence is meant by proving that a tool used in forensic examination meets standards and to ensure its correctness. Finally, the presented evidence and its source should be clearly understandable and believable to a jury. The **credibility** is established by demonstrating the tools used to collect and preserve evidences, the guidelines used, and the controlling standards.

5.3) Forensics procedures:

When a compromise of security or a unauthorized/illegal action associated with a computer is suspected, it is important that steps are taken to ensure the protection of the data within the computer and/or storage media.

The initial response to a computer security incident may be more important than later technical analysis of the computer system because of the actions taken by incident response team members. Actions taken by the incident response team impact subsequent laboratory examinations of the computer and/or media. Of most importance is that the first responder act appropriately.

In the event of a suspected computer incident, care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, opening a file changes it. From a legal sense, it is no longer the original evidence and may be inadmissible in any subsequent legal or administrative proceedings.

The activities/procedures for securing a suspected computer incident scene include

- Securing the scene
- Shutting down the computer
- Labelling the evidence
- Documenting the evidence
- Transporting the evidence
- Providing chain-of-custody documentation

Securing the scene

The entire work area, office, or cubicle is a potential crime scene, not just the computer itself. The work area should be secured and protected to maintain the integrity of the scene and the storage media. While waiting for the official incident responder, no one should be allowed to touch the computer, to include shutting the computer down or exiting from any programs/files in use at the time or remove anything from the scene. All individuals at a scene should be known and briefly interviewed to determine their access to the computer and work area before asking them to leave.

Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system. It is important to remember that that the data present within the storage media is potential evidence and should be treated accordingly. Any attempts to retrieve data by unqualified individuals should be avoided as these attempts could either compromise the integrity of the files or result in the files being inadmissible in legal or administrative proceedings.

Procedure for previewing and taking BitStream Backup

1. Photograph the Scene
2. If the computer is ON then photograph the screen and note down the names of programs being run.
3. Do not switch off the computer. Simply pull the power cord from behind the back of the computer.
4. Open the computer and inspect the inside for unusual connections or configuration.
5. Disconnect the Power cables to all the storage hard drives
6. Switch on the suspect computer and run the CMOS Setup routine to ensure that the computer is set to boot from floppy drive. For entering into the CMOS Setup, most of the systems will flash the correct key on the screen as the system boots. If not, the following setup keys are common:
    - Compaq Computers F10
    - IBM Computers F1
    - Some PC Clones Del
    - OR F2
    - OR Ctrl-Alt-Esc
    - OR Ctrl-Alt-Enter
7. Make sure that the computer is set the Boot Sequence from floppy drive. Exit the BIOS Setup, by saving the changes. Switch off the system.
8. Insert the BitStream Software Booting floppy into the floppy drive. Switch on the computer. Make sure system is booting with floppy.
9. Power off the computer and reconnect the disk drive power cables.

For Previewing

1. Remove the parallel port cable from the computer and connect the cable from the kit brought by the team.
2. Connect the other end of the cable to the PC or Notebook PC brought by the team which contains the analysis software.
3. Run the BitStream Software from the floppy, and make sure all the storage devices are shown and all are locked by default.
4. Run the server mode
5. Switch ON the Analysis Computer (PC bought by the team) and it as client.
6. Use the Analysis Software to see the content of the suspect disk.

For Bitstream Copy

1. Connect the destination disk (bought by the team) to the free IDE port / connector and connect power cable to the destination HDD.
2. Turn ON the computer and allow the computer to boot from the floppy drive.
3. Run the BitStream Software from the floppy, and make sure all the storage devices are shown and all are locked by default.
4. Take the media hash of the suspect computer hard disk and note it down. This may take hours.

5. Unlock the destination disk
6. After taking the media hash value start the BitStream copying. This process will take long time to complete. Please ensure that the power will not be disturbed during this operation.
7. After copying is over, switch off the computer. Remove the destination disk connected to it.
8. Disconnect the suspect hard disk from the computer. Note down its make, model no, serial number and any noticeable things on the hard disk
9. Pack the suspect hard disk in a Packing Box, seal it using tapes and get it signed by the witnesses.

Documentation

Detailed notes should be maintained during all aspects of the scene processing. This not only includes the usual who, what, where, when but overall observations of the scene. A evidence/property document should contain entries with a description of the items (model and serial number), any visible markings present on the item, the condition of the item, the manner it was marked for evidence and the location from within the scene it was seized. Every item of evidence has its own characteristics, but should be identified in a manner it can be easily identified at a later date. Items should be collected as found and documented.

Handling and Transportation

Diskettes have fragile magnetic media. If they are packed loosely and allowed to strike each other repeatedly during transit, the media could be damaged and the data lost.

Hard disks should not be subjected to shocks. When transporting a CPU, devices, or media, they should not be placed in a vehicle trunk or area where there will be drastic changes in temperature.

5.4) Files present in sim card:

A smart card, also known as an Integrated Circuit Card (ICC), is a micro-controller based access module. It is a physical/logical entity and can be either a Subscriber Identity Module (SIM) or a Universal Integrated Circuit Card (UICC). Originally, the ICC defined for 2G networks was the SIM. In 3G networks, the SIM may also be a logical entity (application) on a 3G UICC thereby making it functionally the same as a 2G SIM. The Universal Subscriber Identity Module (USIM) is a logical application running on a UICC smart card, which normally only accepts 3G Universal Mobile Telecommunications Service (UMTS) commands. A USIM can have multiple phone numbers assigned to it, thus allowing one phone to have multiple numbers. If the USIM and SIM applications reside on the same UICC, they cannot be active at the same time.

SIM Technology and Functionality

SIMs are found in GSM, iDEN, and Blackberry handsets and are also used by satellite phone networks such as Iridium, Thuraya, and Inmarsat. Under the GSM framework, a cell phone is termed a Mobile Station, consisting of a SIM card and a handset (Mobile Equipment–ME). One very important and functional feature of a SIM card is that it can be moved from one GSM compatible phone to another, thereby transferring all of the subscriber's information.

The first SIM cards were about the size of a credit card. As cell phones began to shrink in size, the mini-SIM (about one-third the size of a credit card) was developed. Today an even smaller version, the micro-SIM, is available. Each of these three iterations varies in physical size and the functionality supported. Normally, a SIM card provides functionality for both the identification and authentication of the subscriber's phone to its network; contains storage for phone numbers, SMS, and other information; and allows for the creation of applications on the card itself. The basic functions are illustrated in Figure 1.

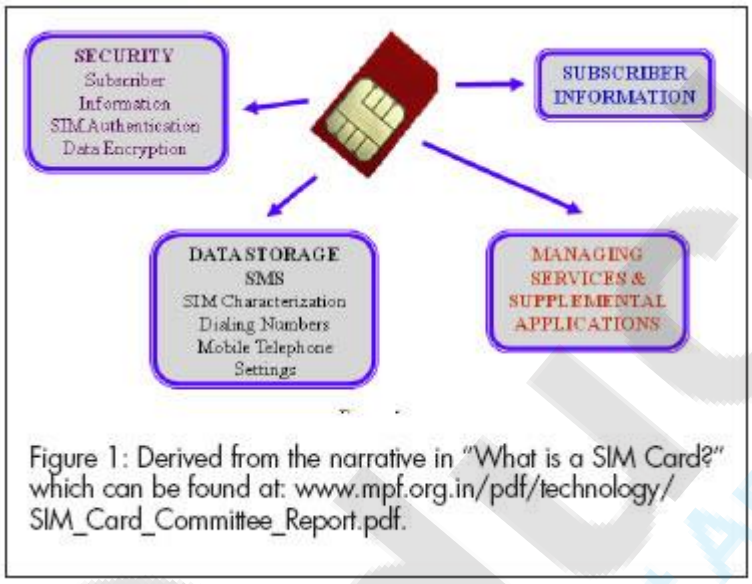


Figure 1: Derived from the narrative in "What is a SIM Card?" which can be found at: www.mpf.org.in/pdf/technology/SIM_Card_Committee_Report.pdf.

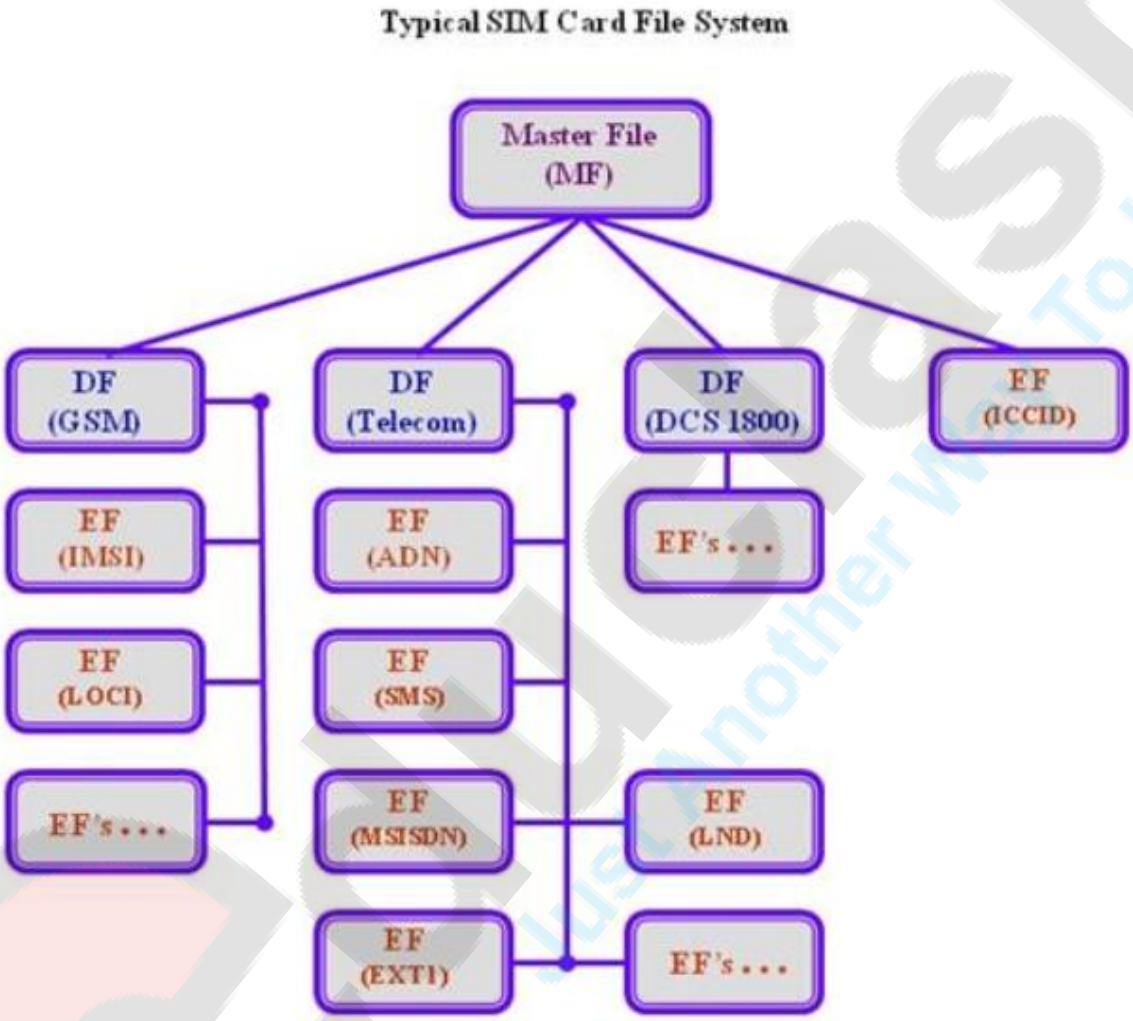
SIM Structure

SIMs contain both a processor (CPU) and an operating system which is either native (proprietary, vendor specific) or Java Card (a subset of the Java programming language). SIMs also have Electrically Erasable Programmable Read Only Memory (EEPROM), Random Access Memory (RAM) for controlling program execution, and persistent Read Only Memory (ROM) which stores user authentication, data encryption algorithms, the operating system, and other applications. Communication between the SIM card and the handset is via a serial interface.

A SIM card also contains a hierarchical file system which resides in EEPROM. The file structure consists of a Master File (MF), which is the root of the file system, Dedicated Files (DFs), and Elementary Files (EFs). Dedicated Files are subordinate directories under the MF, their contents and functions being defined by the GSM11.11 standards. Three are usually present: DF (DCS1800), DF (GSM), and DF (Telecom). Also present under the MF is EF (ICCID). Subordinate to each of the DFs are supporting EFs which contain the actual data. The EFs under DF (DCS1800) and DF (GSM) contain network related information and the

EFs under DF (Telecom) contain the service related information. A typical SIM card file system is shown in Figure 2.

While all the files have headers, only the EFs contain data. The first byte of the header identifies the file type. Headers contain the security and meta-information related to the structure and attributes of the file, such as length of record. The body of the EFs contains information related to the application(s). Files can be either administrative or application specific and access to stored data is controlled by the operating system.



SIM Card File Structure

SIM cards incorporate simple hierarchical file structures with certain classes of files used to organize and secure larger groups of files, providing directory-like functionality. Each file has a descriptor byte indicating the file's type, and a location byte that distinguishes individual files. Files can be elementary files, dedicated files or master files. Table 1 hosts the different file types and the associated header numbers [6]. The Master File (MF) is a unique file present on all SIM cards. The MF acts as the root directory, and usually has a small number of elementary (data) files, with most files on the SIM card contained in directory like objects called dedicated files (DFs). An Elementary File (EF) is a container for data, either in

records or as a simple byte stream. Records can only be accessed in one of two modes for a given EF: "linear-fixed" mode, i.e., each record is accessed as a sequential list (appropriate for contact lists), and "circular" mode, i.e., access is based on recency using a queue (appropriate for call lists).

Table 1. SIM card file types.

Descriptor Byte (Hexadecimal)	File Type
3F	Master File (MF)
2F, 4F, 6F	Elementary File (EF)
5F, 7F	Dedicated File (DF)

Table 2. Important SIM card files.

File Name/Location	Description
3F00 7F10 6F3A	Abbreviated Dialing Numbers
3F00 7F10 6F3C	Short Message Service storage
3F00 7F10 6F40	Mobile Subscriber ISDN
3F00 7F20 6F21	International Mobile Subscriber Identity

5.5) Device Data:

Nearly two-thirds of the U.S. population use mobile or cell phones. Even consumer purchases of these phones are constantly increasing with the phone memory capacities being constantly increased by manufacturers. Thus, allowing users to secretly take photos, record conversations or video. Some organizations offer the consumer private investigation services to extract cell phone data revealing immoral activities such as marital infidelity.

However, the most common use of mobile phone forensics is by law enforcement. Digital data trails are easily left by mobile phones, so criminals must beware. Just as computer information is never truly deleted, the same applies to mobile phone information.

Because of the development of mobile phone forensics, law enforcement can more readily identify pedophiles, stalkers or harassers through mobile phone forensics. Persons experiencing medical emergencies also benefit from these forensics. For example, state or local agencies may automatically link addresses to their mobile phones, especially useful when cell phones are used to report emergencies.

For investigators in particular, a wide array of challenges can occur during the process of

mobile-phone evidence gathering. Such hurdles can include formidable file systems within mobile phones, one-of-a-kind operating systems, a plethora of network systems and network providers. Nevertheless, patented cables and connectors also add to the challenge. Proper training of such investigators can combat some of the mobile phone complexities, but it is however, difficult to keep up with the fluidity and uniqueness of mobile phone technologies.

Mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. Developing an understanding of the components and organization of cell phones is a prerequisite to understanding the criticalities involved when dealing with them forensically. Similarly, features of cellular networks are an important aspect of cell phone forensics, since logs of usage and other data are maintained therein. Cell phone forensics include the analysis of both SIM and phone memory, each requires separate procedure to deal with.

5.6) External memory dump and evidences in memory card:

5.6.1) Memory Dump

A memory dump is a process in which the contents of memory are displayed and stored in case of an application or system crash. Memory dump helps software developers and system administrators to diagnose, identify and resolve the problem that led to application or system failure.

Memory dump is also known as core dump, and blue screen of death (BSOD) in Windows-based computers.

Memory dump primarily identifies a problem or error within the operating system or any installed application within the system. Typically, memory dump provides information about the last state of the programs, applications and system before they were terminated or crashed.

This information consists of memory locations, program counters, program state and other related details. It is displayed on-screen and also creates a system log file for viewing/referencing later. After memory dump, the computer is generally unavailable or inaccessible until it's rebooted. Memory dump can also be caused by memory leak, when the system is out of memory and can no longer continue its operations.

THE IMPORTANCE OF MEMORY FORENSICS

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments, and internet history which is non-cacheable. Any program – malicious or otherwise – must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

As attack methods become increasingly sophisticated, memory forensics tools and skills are in high demand for security professionals today. Many network-based security solutions like firewalls and antivirus tools are unable to detect malware written directly into a computer's physical memory or RAM. Security teams should look to memory forensics tools and specialists to protect invaluable business intelligence and data from stealthy attacks such as fileless, in-memory malware or RAM scrapers.

5.6.2)Evidence in memory card:

Memory card forensics plays a vital role during investigation of any digital storage device. With the advent of modern technology, experts have possibilities to carve artifacts from mobile phones, digital cameras, MP3 & many more.

Memory card is a sort of small data storage medium that is widely used within portable devices to store digital information like *pictures & media files, audio, video, text* and many more. The page describes the complete memory card forensics including analysis and recovery of data from corrupted memory card.

During investigation, the primary goal of techies should be to recover data before it is overwritten or damaged. Since the technology has changed to a new phase, it is obvious that criminals have also used these innovations to perform their illegitimate activities. Therefore, proper collection of information is essential.

From an investigative viewpoint, artefacts recovered from a memory card can provide crucial information about the suspect. Some are listed below: -

- Details about the call logs -received, dialled & missed calls.
- Stored contact numbers.
- Sent, received or deleted text/multimedia messages.
- Images, video, audio and MMS.
- Web Browser History.
- Database of desktop-based or web-based email clients.

NOTE: – Apart from the above-listed artifacts, there are number of other evidences that play a very crucial role in investigation.

Compared with some past year's statistics of memory card forensics investigation; there has been a significant growth in number of crimes. Another important aspect that must be addressed while conducting memory card

forensic analysis is to keep it out from the slot so that the data is not manipulated or removed during the process of recovering evidence from corrupted memory card.

5.7) Android Forensics Fundamentals:

Forensics Strategies for Android Devices

There are four primary ways to approach forensics on an Android device. They are:

- SD Card analysis
- Logical acquisition
- Physical acquisition
- Chip-off

Before exploring these techniques, a brief discussion on the challenges of mobile phone forensics is warranted. A fundamental goal in digital forensics is to prevent any modification of the target device by the examiner. However, mobile phones lack traditional hard drives which can be shutdown, connected to a write blocker, and imaged in a forensically sound way. The end result is that Android forensic techniques, short of chip-off, do alter the device. Examiners must use their discretion when examining a mobile device and if the device is modified, they must explain how it was modified and, as important, why that choice was made.

SD Card Analysis

Nearly every Android device comes with an external SD Card for storing data. Upon receiving and securing an Android device (as you would any other mobile device), an examiner should remove the SD Card and process it in the standard way. The card is formatted with a FAT32 file system.

Logical Analysis

The logical acquisition of an Android device is the technique we recommended first. This technique involves copying a small (~25k) Android Forensics application to the device, running the application, and then removing it from the device. An application, written by viaForensics and distributed for free to law enforcement and government agencies charged with digital forensic responsibilities, currently acquires the following information:

1. Browser history
2. Call Logs
3. Contact Methods
4. External Image Media (meta data)
5. External Image Thumbnail Media (meta data)
6. External Media, Audio, and Misc. (meta data)
7. External Videos (meta data)
8. MMS
9. MMSParts (includes full images sent via MMS)
10. Organizations
11. People
12. SMS
13. List of all applications installed and version
14. Contacts Extensions
15. Contacts Groups

16. Contacts Phones
17. Contacts Settings

And new data sources are being developed weekly. The data is written to an SD Card the examiner placed into the device. The files are currently written as CSV, however we will likely change this to an XML format. Also, there are some challenges when interpreting this data and we are currently developing viaExtract, a reporting application for the data. The application will be released in the next few months and sold at significant discount to active law enforcement.

If you are active law enforcement, you can register for free access at viaforensics.com/wiki/doku.php using your agency e-mail address. After verification, your access will be enabled, generally within 24 hours. It should be noted that several commercial platforms have support for a logical acquisition of Android devices however they are typically limited to basic information.

Physical Analysis

In some cases, a more significant analysis is required. To this end, we have developed a technique to physically acquire a "dd" image from support Android devices (currently any Android 1.5 devices and Motorola Droid 2.0 and 2.01). This technique requires root privileges on the device and can yield a significant amount of information.

This technique will provide a forensic image of the various user data partitions. These partitions use the open source file system YAFFS2 (Yet Another Flash File System 2) and is one of the significant challenges with the Android platform.

YAFFS2 was built specifically for the growing NAND memory devices and has a number of important features which address the stringent needs of this medium. It is a log-structured file system, provides built in wear-leveling and error correction, is fast, and has a small footprint in RAM. However, since its usage was limited prior to Android, no commercial forensic product supports the file system.

For the brave, you can download the YAFFS2 source code, grab a forensic image of a partition, open it up in your favorite hex editor and start digging. However, we are making progress in the development of some tools. The tools allow an examiner to forensically acquire the NAND data (you cannot use dd for this…we've developed a special nanddump program for this purpose), mount the image in Linux (using nandsim) and extract the data. Traditional techniques such as file carving and strings also work. However, the real potential is in the development of a program which will provide a "point-in-time" version of any file on the YAFFS2 file system; this is a very fortunate (for the forensic examiner) byproduct of YAFFS2 being a log-structured file system.

Chip-off

For those with full lab facilities, there is always the option of using chip-off techniques on the NAND memory. The scope of this is well beyond this article…but those of you who have such facilities certainly need to read about it!

5.8) DATA EXTRACTION TECHNIQUES

Mobile forensics

Majorly deals with the hand-held devices and smart devices to collect the digital evidence and to analyse the data and to fetch the results of various apps installed, user data, browser history and more. As per the Netmarketshare reports approximately Android covers 52% of the market globally followed by IOS with 40% then windows with 3%, blackberry with 2% and others with 3%.
Mobile Forensics involves the below process.

- Intake
- Identification
- Preparation
- Isolation
- Acquisition / Processing
- Verification
- Reporting
- Presentation
- Archiving

Forensic artifacts varies from operating system to operating system as the architecture differs from device to device. To collect the digital evidence from a smart phone below are the **commonly used types of extraction techniques used by major forensic tools.**

1. Physical Collection
2. Logical Collection
3. File System Extraction

1) Physical Collection:

Physical extraction extracts the information from the device by accessing its flash memory. It creates a bit-by-bit copy of the device. Physical collection supports deleted file extraction.

Types of Physical Acquisitions:

Most of the devices in the market doesn't support physical extraction unless the user has the root privileges, to overcome such challenges extraction is performed by using two techniques:

JTAG - Joint Test Action Group

JTAG (Joint Test Action Group) involves using advanced data acquisition methods at the hardware level, which is done by connecting to specific ports on the device and transfer the data. Analyst must have proper training and experience prior to attempting JTAG as the device may be damaged if handled improperly.

Chip-off

Chip-off, is another type of physical acquisition where in the flash chips would be removed from the device to extract the data. This type of acquisition usually damages the device.

Logical Collection:

The best and preferred method is physical extraction, however due to the wide range of devices present in the market the second preferred method is logical extraction. Logical extraction extracts the information which is accessible and not from the unallocated space. It extracts data without root access however having root access on a device can allow examiner to acquire more data. The data is extracted based on the application programming interface.

Types of Logical Extraction:

i. Agent Based Extraction

In this extraction an agent will be pushed in to the device and extracts the data then uninstall the agent and its traces. The extraction method from device to device and operating system to operating system differs as the architecture is different.

ii. Data Extraction using ADB commands

ADB (Android Debug Bridge) is a command line tool which is used to communicate with the device to retrieve the information, it can extract the data which is on device having root access to the device provides you more information than as a normal user. ADB shell uses USB debugging mode. If the device is locked and USB debugging is not enabled ADB commands will not able to fetch the results. In most of the cases Application data is stored as a SQLite database. In any type of extraction these dBs are parsed altogether and report is generated.

3) File system Extraction

It is used to acquire the data stored in the allocated space, unlike physical extraction it only captures the application specific entries in the database to recover the deleted items.

Below table gives an overview of collection methods in mobile forensics.

Physical	Logical	File system
Bit-By-Bit image of the device	Active content (User accessible)	Active content with application support
Includes deleted data	Does not include deleted data	Partially recovers deleted data
Captures call logs, sms, mails, Application data and Images, music and videos	Captures only active content like contacts, call logs, Images, music and videos	Captures contacts, call logs, Images, music, videos, and Application data

Mobile Artifacts:

As mentioned in the above extractions every operating system has their own architecture to store the artifacts below is the details of different artifacts these artifacts locations varies from device to device and version of the Operating System to Operating System.

Android

Artifacts	Location
Call Logs	Com.android.providers.contact/contacts2.db
SMS	Com.android.providers.telephony/mmssms.db
Internet History	Com.android.browser
Whatsapp database	/data/data/com.whatsapp/databases
Mail	/data/com.google.android.gm/databases/mailname.db

Windows

Artifacts	Location
Call Logs	Users\WPCOMMSERVICES\APPDATA\Local\UserData\phone
SMS	Users\WPCOMMSERVICES\APPDATA\Local\Unistore\store.vol.
InternetHistory	Users\DefApps\APPDATA\INERNETEXPLORER\INetCache\
Whatsapp Database	/sdcard/Whatsapp/Databases/msgstore.db
Mail	/private/User/Mail

IOS

Artifacts	Location
Call Logs	/private/var/mobile/callhistory
SMS	/private/var/mobile
Internet History	/private/var/mobile/Library
Whatsapp	/var/mobile/applications/sid/chatstorage.sqlite
Mail	/Library/Mail/

Challenges:

Smart device is an important piece of evidence when it comes to corporate frauds, financial frauds, civil and criminal litigations. Any corporate having a BYOD policy provide users an flexibility to configure MDM (Mobile Device Management) services, and

corporate policy defines that the asset can be seized if it is required in any investigation of the incident happened.
The major challenges in mobile forensics are:

- To acquire and analyse the digital data of a new device released in the market because of continuous changes or upgrades of the architecture.
- Cloud storage of phone memory in recent devices like One Drive, ICloud, Google Drive – JTAG / Chip-off as mentioned above can be used as an option to retrieve the data.
- Recent mobiles come with an option to encrypt the phone data which will not be able to decrypt by usin any of the former techniques

5.9) Screen Lock bypassing techniques

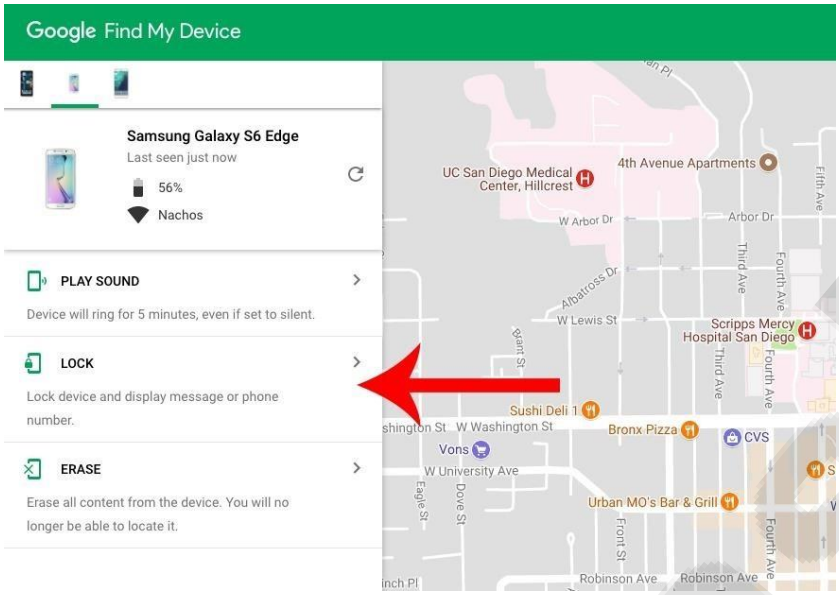
If you somehow forgot the pattern, PIN, or password that locks your Android device, you might think you're out of luck and are destined to be locked out forever. These security methods are hard to crack by design, but in many cases, it's not entirely impossible to break into a locked device.

There are several different ways to hack a locked Android smartphone or tablet, but unfortunately, there's not a one-size-fits-all method. So below, I'll go over 7 of the most effective methods, and hopefully one will help you get back into your device.

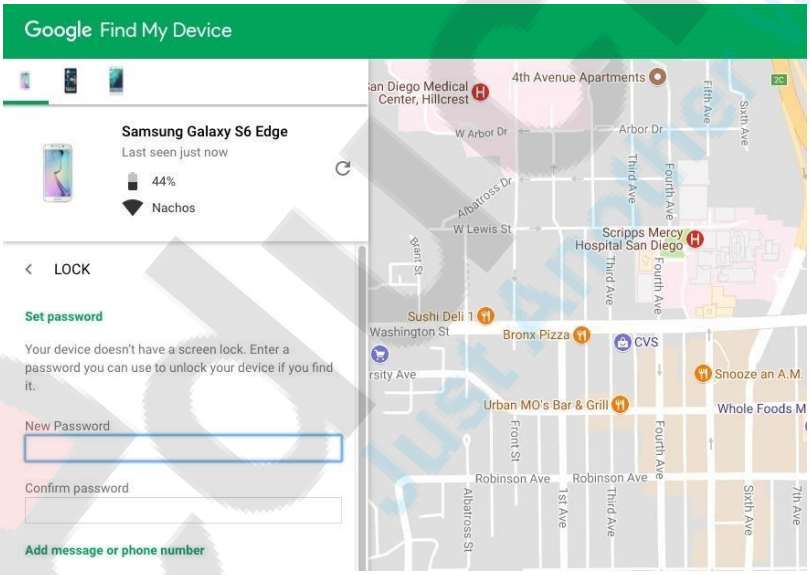
Method 1Use Google's 'Find My Device' Website

For most Android phones and tablets, a built-in service called Find My Device is your best bet. As long as you're logged into your Google account, you can use any device or computer to access the service, which is available at this link.
From our testing, we've noticed that this method does not work on Android 8.0 or higher. But as long as your phone is running Android 7.1.1 Nougat or lower, it should do the trick.

As counterintuitive as it may sound, start by clicking the "Lock" button once Find My Device gets a fix on your phone. If the service is having trouble finding your device, click the refresh button next to your phone's name a few times, and it should make the connection within 5 attempts if your phone is compatible.



After clicking the "Lock" button, you'll be prompted to enter a new password, which will replace the pattern, PIN, or password that you forgot. Type the new password twice to confirm your choice, then click the "Lock" button.



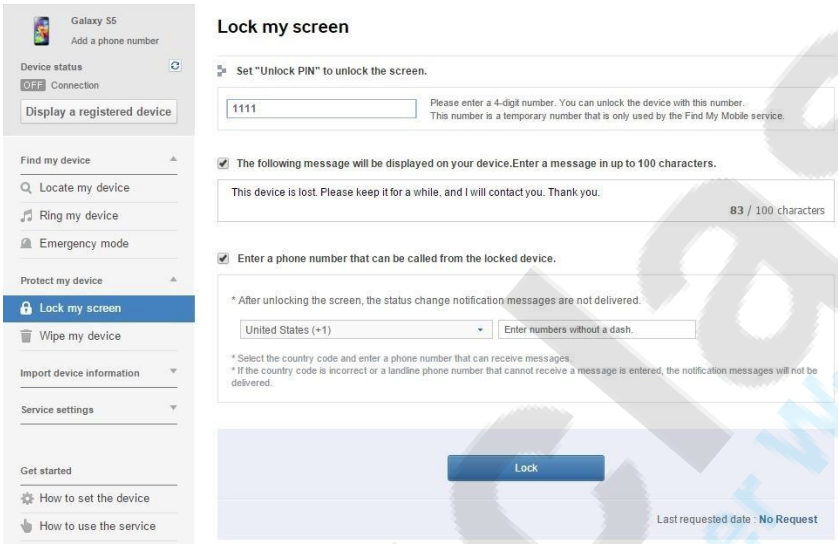
From here, it can take up to 5 minutes for the password to change over, but when it does, you should be able to enter the new password to unlock your device.

Method 2Use Samsung's 'Find My Mobile' Service

If you have a Samsung device, a similar service called Find My Mobile should be the first thing you try. Start by heading to this link from any web browser, then log into your Samsung account. If you never set up a Samsung account,

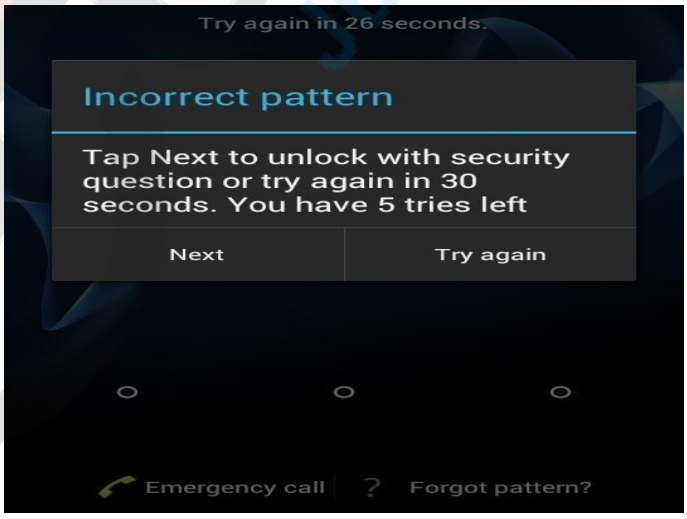
this method will not work, unfortunately. Also, some carriers, like Sprint, lock out this service, which is something to keep in find.

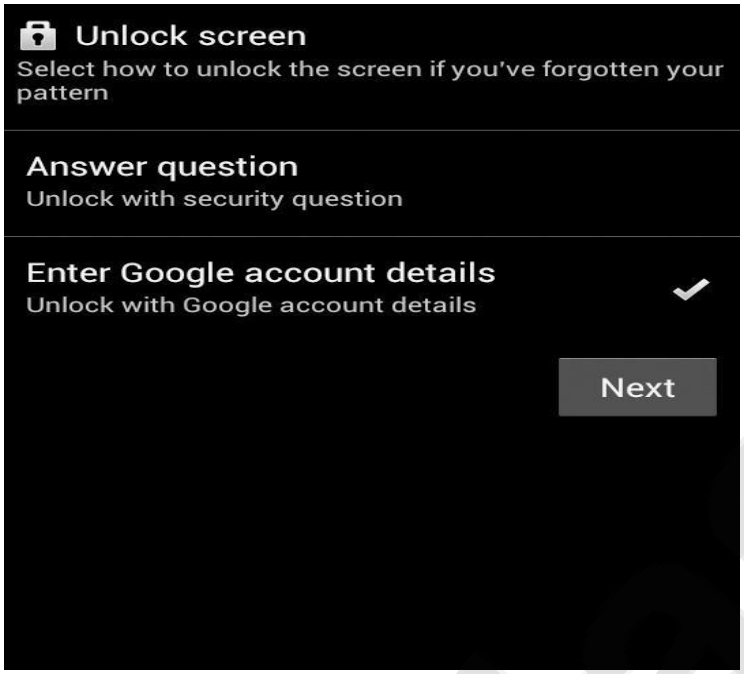
Once you've logged into your Samsung account, click the "Lock my screen" button in the left-hand pane. From here, enter a new PIN in the first field, then click the "Lock" button near the bottom of the screen. Within a minute or two, your lock screen password should be changed to the PIN you just entered, which you can use to unlock your device.



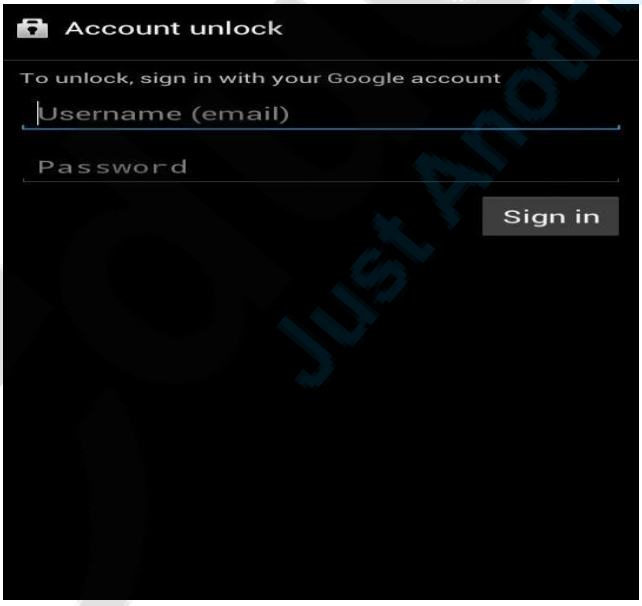
Method 3Use the 'Forgot Pattern' Feature

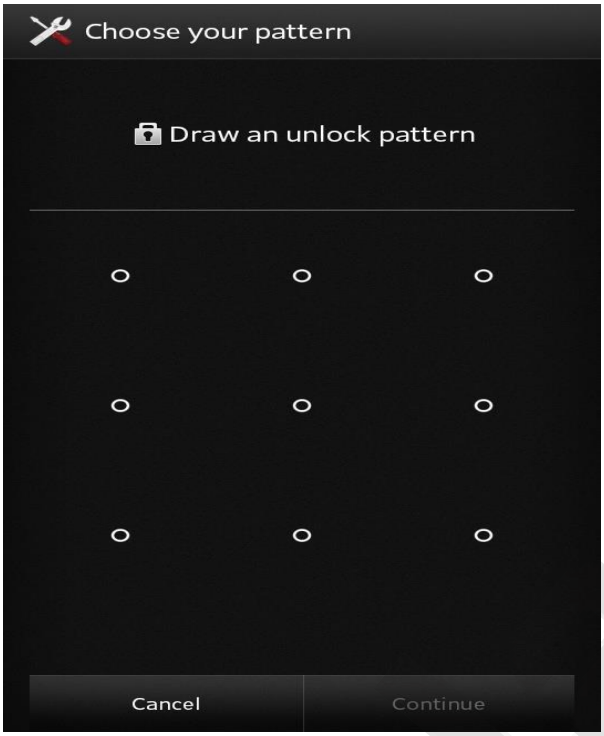
If your device is running Android 4.4 or lower, try using the "Forgot Pattern" feature. After 5 failed unlock attempts, you'll see a message that says "Try again in 30 seconds." While this message is showing, tap the button at the bottom of the screen that says "Forgot Pattern."





From here, choose "Enter Google account details" (depending on your device, you may go directly to this option), then enter your primary Gmail account and password. Google will either send you an email with your unlock pattern, or you can change it right then and there.

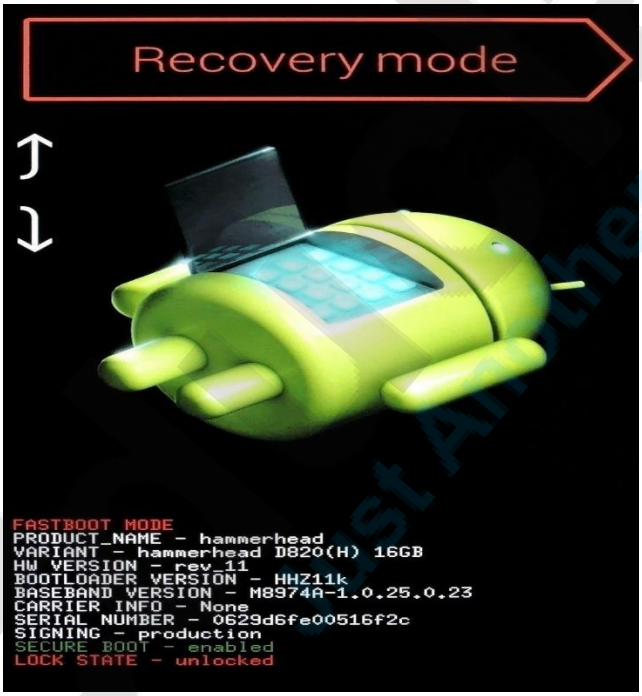




Method 4Perform a Factory Reset

If you're more concerned with getting into your phone than you are with preserving any data stored on it, a factory reset should work in many scenarios. But due to a new anti-theft feature called Factory Reset Protection, you'll need to know your Google account password to use this method if the phone was released in 2016 or later.

The process will vary depending on your device type, but for most phones, start by powering the device completely off. When the screen goes black, press and hold the volume down and power buttons simultaneously, which will bring up Android's bootloader menu. From here, press the volume down button twice to highlight the "Recovery mode" option, then press the power button to select it.



Next, hold the power button down and tap the volume up button once, then your phone should enter recovery mode. From here, use the volume buttons to highlight the "Wipe data/factory reset" option, then press the power button to select it. When the process is finished, select the "Reboot system now" option and you should no longer be locked out of your phone.

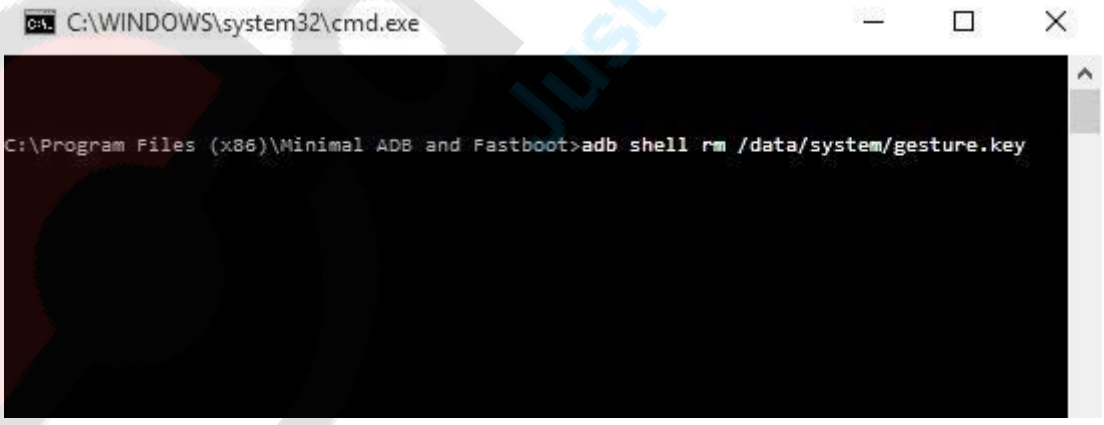
If it's a newer phone, you'll be prompted to log in with the Google account and password that were previously used on the device before it was reset. As long as you know this information (and you should), it's just a matter of logging back into your Google account to regain access to your phone at this point.

Method 5 Use ADB to Delete the Password File

This next option will only work if you've previously enabled USB debugging on your phone, and even then, it will only work if you've allowed the computer you're using to connect via ADB. But if you meet those requirements, it's a perfect way to unlock your device. However, note that models with encryption enabled by default may not be compatible with this workaround.

Start by connecting your phone to your computer with a USB data cable, then open a command prompt window in your ADB installation directory. From here, type the following command, then hit *Enter*.

- **adb shell rm /data/system/gesture.key**

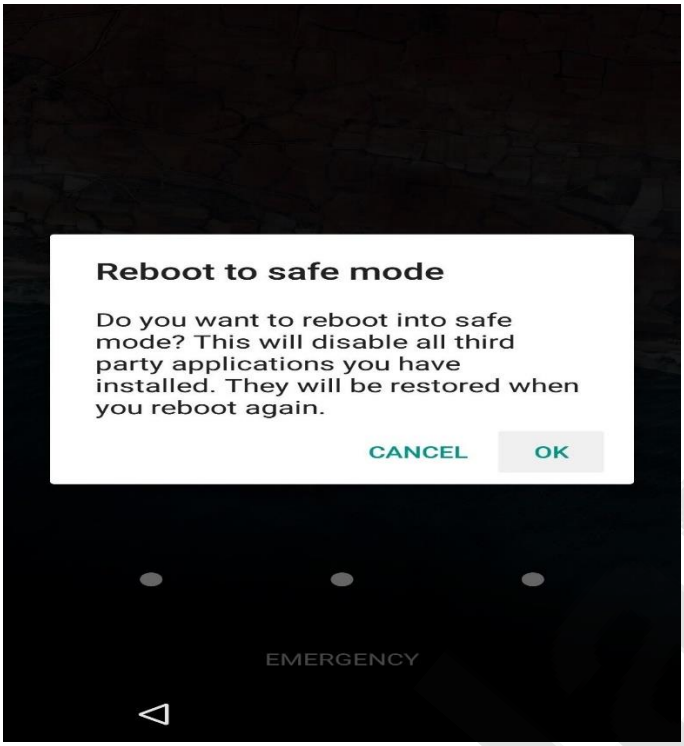


Next, reboot your phone and the secure lock screen should be gone, allowing you to access your phone. But this is only temporary, so make sure to set a new pattern, PIN, or password before you reboot again.

Method 6Boot into Safe Mode to Bypass Third-Party Lock Screen

If the lock screen you're trying to bypass is a third-party app rather than the stock lock screen, booting into safe mode is the easiest way to get around it.

For most phones, you can boot into safe mode by bringing up the power menu from the lock screen, then long-pressing the "Power off" option. From here, choose "OK" when asked if you'd like to boot into safe mode, and when the process finishes, your third-party lock screen app will be temporarily disabled.

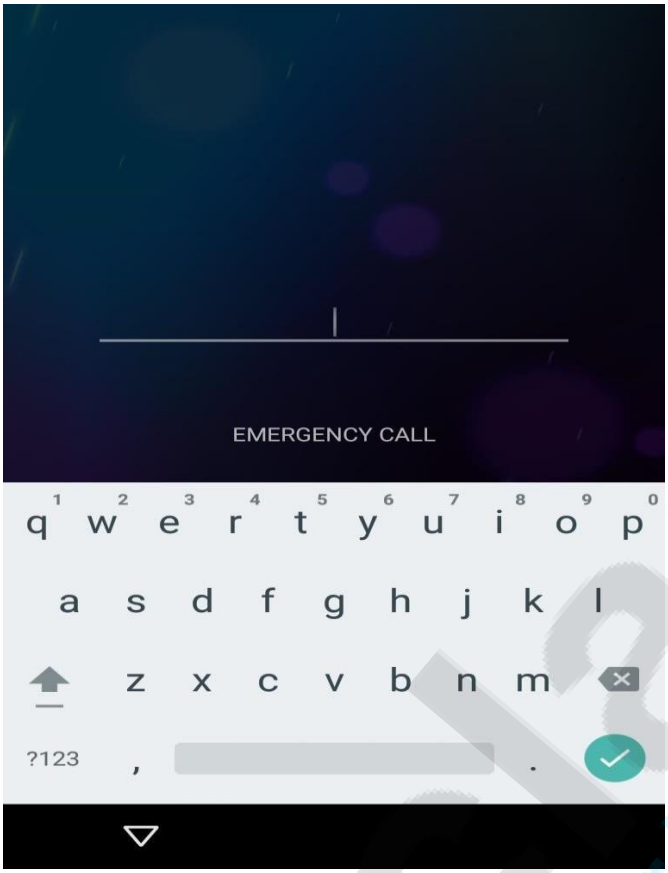


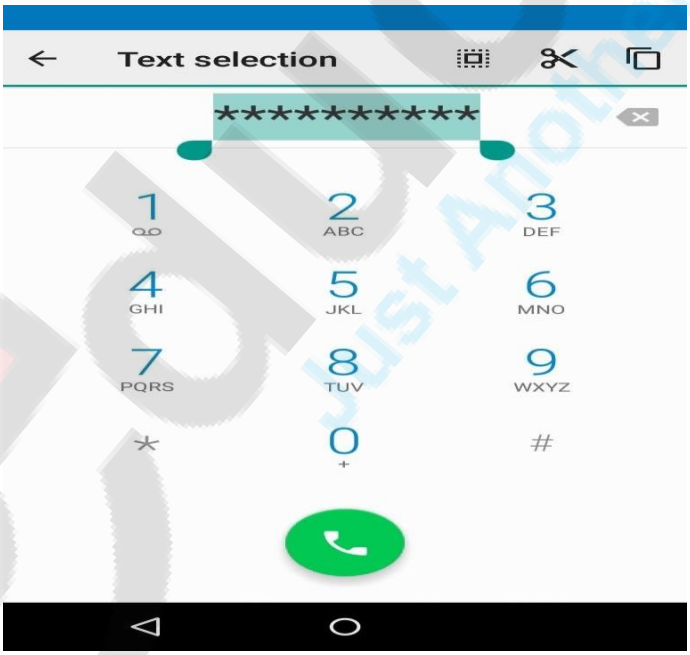
From here, simply clear data on the third-party lock screen app or uninstall it, then reboot your phone to get back out of safe mode. When you get back up, the troublesome lock screen app should be gone.

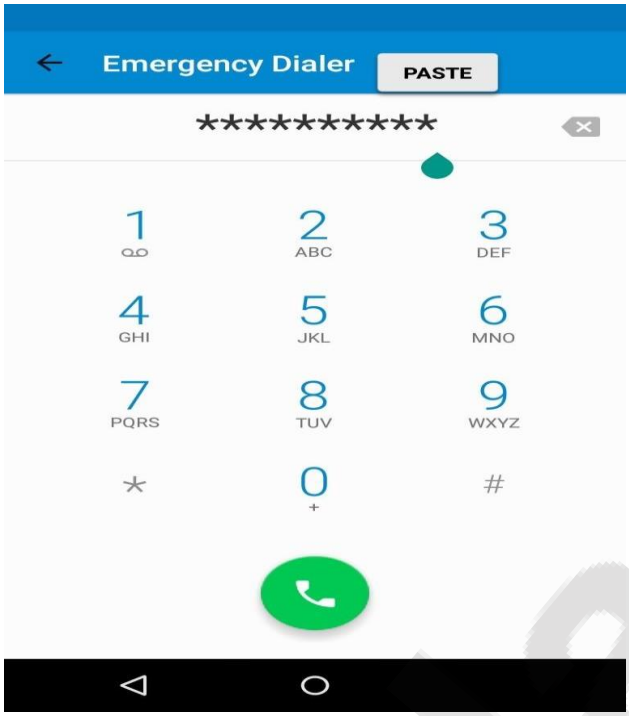
Method 7Crash the Lock Screen UI

Finally, if your device is encrypted and running Android 5.0-5.1.1, there's a way to get around the password lock screen. This method won't work on any other type of secure lock screen, but it's a lifesaver if you forgot your password.

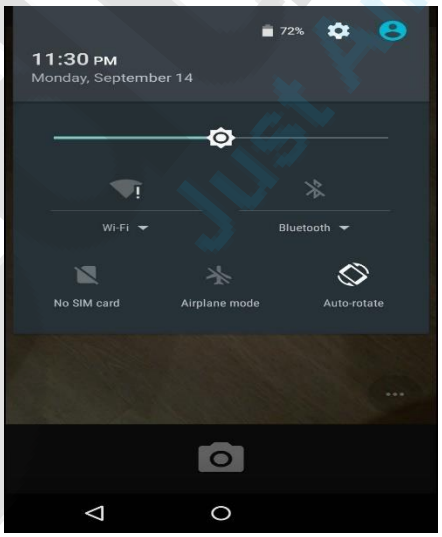
First, tap the "Emergency Call" option on your lock screen, then use the dialer interface to enter 10 asterisks. From here, double-tap the field to highlight the entered text and choose "Copy," then paste it into the same field to essentially double the amount of entered characters. Repeat this same process of copying and pasting to add more characters until double-tapping the field no longer highlights the characters.


EMERGENCY CALL
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123


Text selection
1 2 ABC 3 DEF
4 GHI 5 JKL 6 MNO
7 PQRS 8 TUV 9 WXYZ
0 +



Next, head back to the lock screen and open the camera shortcut. From here, pull down the notification shade and tap the Settings icon, then you'll be prompted to enter a password. Long-press the input field and choose "Paste," then repeat this process several more times. Eventually, after you've pasted enough characters into the field, your lock screen will crash, which will allow you to access the rest of your phone's interface.




72%
11:30 PM
Monday, September 14
Wi-Fi
Bluetooth
No SIM card
Airplane mode
Auto-rotate
a s d f g h j k l
z x c v b n m
?123
EMERGENCY CALL


69%
11:33 PM
Monday, September 14
Wi-Fi
Bluetooth
No SIM card
Airplane mode
Auto-rotate
PASTE
a s d f g h j k l
z x c v b n m
?123
EMERGENCY CALL

UNIT 6

COUD FORENSICS

Types of Cloud Architectures

Before going any further into Cloud forensics, it is important to have a proper understanding of basic Cloud concepts:

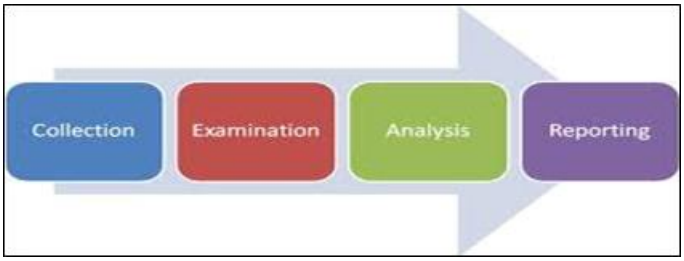
There are three options of service models that define your Cloud architecture:

- **Infrastructure as a service (IaaS)** delivers basic computer infrastructure (typically a platform virtualization environment) as a service, along with raw storage space and networking capabilities.
- **Platform as a service (PaaS)** is the delivery of an entire computing platform and solution stack as a service, including all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet. This allows the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities.
- **Software as a service (SaaS)** may be understood as "on-demand software." In this model, software and any associated data are hosted centrally and usually accessed by users using a thin client, such as a web browser over the Internet.

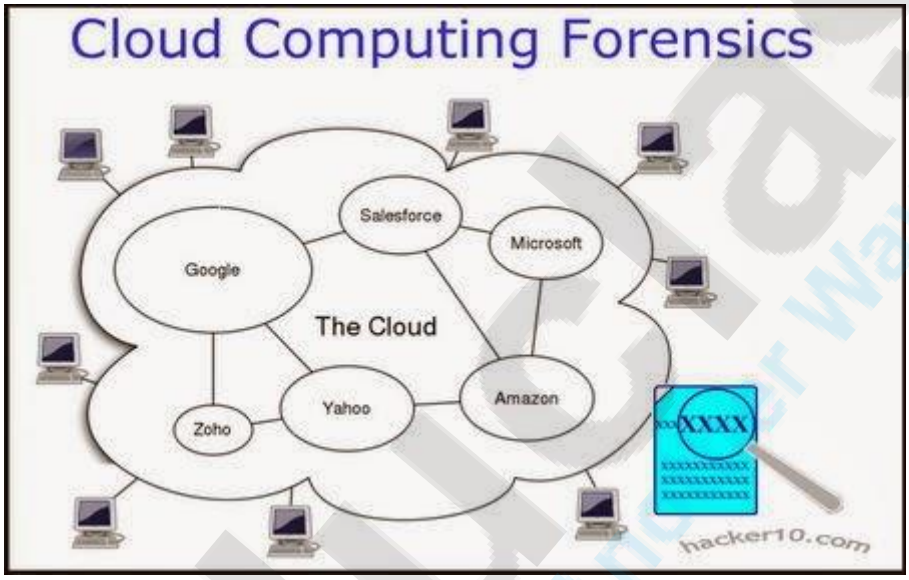
Types of Clouds

Once you have chosen your architecture, the next step is defining your deployment option. There are four basic Cloud types:

- **Public Cloud:** This is the most common type of Cloud offered by big players such as Amazon Web Services (AWS) and Google. In a public Cloud, the infrastructure is made available to the general public, so you will be sharing resources with other companies.
- **Private Cloud:** In this deployment option, the Cloud infrastructure is operated solely for a single organization. Think of it as your basic datacenter (located on-premise or off-premise) using Cloud technology and concepts. You may choose to manage it directly or even have a third party controlling it.
- **Community Cloud**: A community deployment means that the Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. Either managed directly by the organizations or by a third party, it may be located on-premise or off-premise. For instance, this is a good option for highly regulated industry (e.g., healthcare) that does not want or need to build a private environment, but may not be able to use a public Cloud.
- **Hybrid Cloud**: As its name suggests, this delivery option combines two or more Clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load-balancing between Clouds).



Cloud computing is said to be a game changing technologies in the recent history of computing. Unfortunately, due to its young age, cloud companies don't have yet any process that allows for a set procedure on how to investigate or go about cloud issues. Due to this absence, they have no means of ensuring the robustness and suitability of cloud services when it comes to supporting investigations of criminal activity.



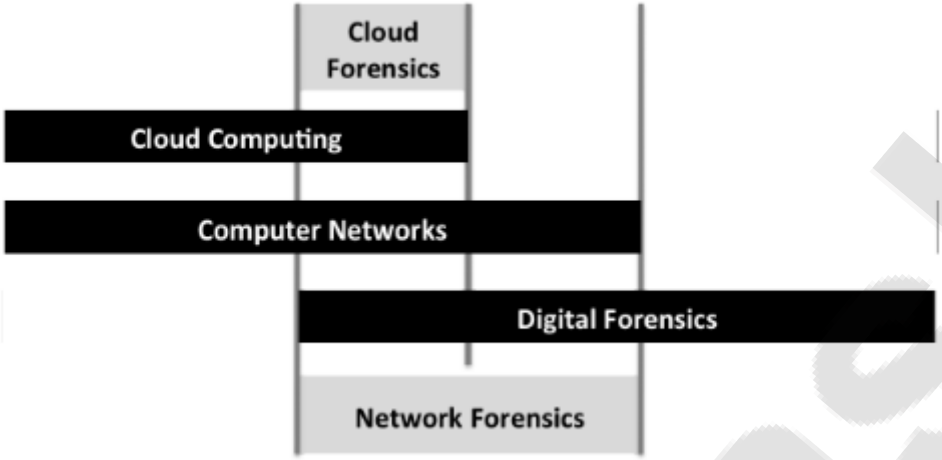
6.1) Cloud Forensics

Cloud forensics is a cross discipline of cloud computing and digital forensics. Cloud computing is a shared collection of configurable networked resources (e.g., networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law.

Cloud forensics is a subset of network forensics. Network forensics deals with forensic investigations of networks. Cloud computing is based on broad network access. Therefore, cloud forensics follows the main phases of network forensics with techniques tailored to cloud computing environments.

Cloud computing is an evolving paradigm with complex aspects. Its essential characteristics have dramatically reduced IT costs, contributing to the rapid adoption of cloud computing by business and government. To ensure service availability and cost-effectiveness, CSPs maintain data centers around the world. Data stored in one data center is replicated at multiple locations to ensure abundance and reduce the risk of failure. Also, the segregation of duties between CSPs and customers with regard to forensic responsibilities differ according to the service models being used.

Likewise, the interactions between multiple tenants that share the same cloud resources differ according to the deployment model being employed.



6.2) Cloud crime

We extend the definition of computer crime by Casey (2000) to cloud crime. Cloud crime is any crime that involves cloud computing. The Cloud can be the object, subject or tool of crimes. The Cloud is the object of the crime when the CSP is the target of the crime and is directly affected by the criminal act, e.g. DDOS (Distributed Denial of Service) attacks targeting part(s) of the Cloud or even the entire cloud. The Cloud is the subject of the crime when it is the environment where the crime is committed, e.g., unauthorized modification or deletion of data residing in the Cloud, identity theft of users of the Cloud. The Cloud can also be the tool used to conduct or plan a crime, e.g., evidence related to the crime can be stored and shared in the Cloud and a Cloud that is used to attack other Clouds is called a dark Cloud.

6.3.1) Usage of cloud forensics

There are various usages of cloud forensics. We summarize them as follows:

(1) Investigation

• Investigation on cloud crime and policy violation in multi-jurisdictional and multi-tenant cloud environments

• Investigation on suspect transactions, operations and systems in the Cloud for incident response

• Event reconstruction in the Cloud

• Providing admissible evidence to the court

• Collaboration with law enforcement in resource confiscation

(2) Troubleshooting

• Locating data file and hosts virtually and physically in cloud environments.

• To determine the root cause for single events or trends spanning multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.

• Tracing an event and assessing the current state of an event in the Cloud

• Resolving functional issues in cloud applications and cloud services

• Resolving operational issues in cloud systems

• Security incident handling in the Cloud

(3) Log Monitoring

• Collecting, analyzing and correlating log entries across multiple systems in the Cloud, assisting in auditing, due diligence, regulatory compliance and other efforts

(4) Data and System Recovery

• Recovering data in the Cloud, that has been accidentally or intentionally deleted or modified

• Recovering encrypted data in the Cloud, when the encryption key has been lost.

• Recovering systems from accidental damage or attacks

• Acquiring data from the Cloud that are being redeployed, retired or need to be sanitized

(5) Due Diligence/Regulatory Compliance

• Helping organizations exercise due diligence and comply with requirements such as protecting sensitive information, maintaining certain records for audit purposes, notifying impacted parties when protected information is exposed, etc.

6.3.2) Challenges

In order to establish a forensic capability for cloud organizations in all three-dimensions defined above, we are facing enormous challenges. In the technical dimension, we have very limited tools and procedures in all five major components that we emphasize in this paper. In the legal dimension there is currently no agreement among cloud organizations on collaborative investigation, and no terms and conditions are present in SLAs on segregation of duties between CSP and cloud customer. International cyber law and policies must progress to help resolve the issues surrounding multi-jurisdiction investigations.

1. **Challenges in forensic data collection**

In all combinations of cloud service and deployment models, the cloud customer faces the challenge of decreased access to forensic data. Access to forensic data varies dependent on the cloud model; IaaS customers enjoy relatively easy access to all data required for a forensic investigation, while SaaS customers may have little to no access to data required. Decreased access to forensic data

means the cloud customer generally has no control or knowledge over the exact physical location of their data, and may only be able to specify location at a higher level of abstraction, typically as an object or container identified. CSPs intentionally hide the location of data from customers to facilitate data movement and replication. Moreover, there is a lack of appropriate terms of use in the SLA (Service Level Agreement) to enable general forensic readiness in the Cloud. Many CSPs do not provide services or interfaces for the customers to gather forensic data. For example, SaaS (Software as a Service) providers may not provide access to the IP logs of clients accessing content; IaaS (Infrastructure as a Service) providers may not provide forensic data such as recent VM (Virtual Machine) and disk images. In the Cloud, the customers have decreased access to relevant log files and metadata in all levels as well as a limited ability to audit the operations of the network of their CSP and conduct real-time monitoring on their own networks.

2. **Challenges in elastic, static and live forensics**

The proliferation of endpoints, especially mobile endpoints, is a challenge for data discovery and evidence collection. The impact of crimes and the workload of investigation can be exacerbated in cloud computing simply because of the sheer number of resources connected to the Cloud. Time synchronization is crucial to the audit logs that are used as source of evidence in the investigation. Accurate time synchronization has been always an issue in network forensics, and is made all the more challenging in a cloud environment as timestamps must be synchronized across multiple physical machines spread in multiple geographical regions, between cloud infrastructure and remote web clients including numerous end points. Similar to time synchronization, unification of log formats has been a traditional issue in network forensics and the challenge is exacerbated in the Cloud because it is extremely difficult to unify the log formats or make them convertible to each other from the massive resources available in the Cloud. Furthermore, proprietary or unusual log formats of one party can become major roadblocks in joint investigations.

In computer forensics, recovered deleted data is an important source of evidence, so it is in the Cloud. In AWS (Amazon Web Service) the right to alter or delete the original snapshot is explicitly reserved for the AWS account that created the volume. When item and attribute data are deleted within a domain, removal of the mapping within the domain starts immediately, and is also generally complete within seconds. Once the mapping is removed, there is no remote access to the deleted data. Storage space occupied by the data elements deleted is made available for future write operations and it is likely that storage space will be overwritten by newly stored data. However, some deleted data might be still present in the snapshot after deletion (Amazon, 2010). A simple challenge is: how to recover deleted data, identify the ownership of deleted data, and use deleted data as sources of event reconstruction in the Cloud?

3. **Challenges in evidence segregation**

In the Cloud, different instances running on the same physical machine are logically isolated from each other via hypervisor. An instance's neighbours have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. On the physical level system audit logs of shared resources and other forensic data are shared among multiple tenants. Currently, the provisioning and de-provisioning technologies still need to be much improved in the Cloud (CSA, 2009), and it remains a challenge for the CSP and law enforcement to

keep the same segregating in the whole process of investigation without breaching the confidentiality of other tenants sharing the same infrastructure and ensure the admissibility of the evidence.

Another issue is that the easy-to-use feature of cloud models results in a weak registration system, facilitating anonymity that is easy to be abused and making it easier for cloud criminals to conceal their identities and harder for investigators to identify and trace suspects as well as segregate evidence.

Moreover, encryption is used in the Cloud to separate data hosting of the CSPs and data usage of the cloud customers and most of the major CSPs encourage customers to encrypt their sensitive data before uploading to the Cloud if encryption is not provided by the CSP by default (Amazon, 2010; Force.com, 2010; Google, 2010). Unencrypted data in the Cloud can be considered lost from a strict security perspective. A chain of separation is required to segregate key management from the CSP hosting the data and needs to be standardized in contract language. Agreement has to be made among the law enforcement, the cloud customer and the CSP on granting access to keys of forensic data, otherwise evidence can be easily compromised when encryption key is destoryed.

4. **Challenges in virtualized environments**

Cloud computing claims to provide data and compute redundancy by replicating and distributing resources. However in reality most CSPs implement instances of a cloud computer environment in a virtualized environment. Instances of servers run as virtual machines, monitored and provisioned by a hypervisor. The hypervisor in a Cloud is analogous to a kernel in the traditional operating system. Attackers will aim to focus their attacks against the hypervisor; compromise of the hypervisor amplifies any attack as many compute resources rely on its security. For law enforcement and cloud investigators, however, there is a huge lack of policies, procedures and techniques on hypervisor level to facilitate investigation.

In the Cloud, mirroring data for delivery by edge networks, its redundant storage in multiple jurisdictions and the lack of transparent real-time information about where data is stored introduces difficulties for investigation. Investigators may unknowingly violate regulations, especially if clear information is not provided about the jurisdiction of storage (ENISA,2009). The CSPs cannot provide tools for the customer to locate at a given time, or trace at a given period of time, precisely and physically the multiple locations of a piece of data across all the geographical regions where the Cloud resides. Furthermore, the distributed nature of cloud computing forces a stronger international collaboration between law enforcement and industry, in cases such as confiscating “a Cloud” since the agency of a single nation cannot manage it when the physical servers are spread across different countries.

5. **Challenges in internal staffing**

Today most cloud organizations are dealing with investigations with traditional network forensic tools and staffing, or are simply neglecting the issue. The major challenge in establishing a cloud forensic organizational structure is the lack of forensic expertise and relevant legal experience. The deep-rooted reasons for this challenge, which is also a challenge for the whole discipline of digital

forensics, are firstly, the relative slow progress of forensic research compare to the rapidly evolving technology and secondly, the slow progress of relevant laws and international regulations.

With only a decade of research and development, the discipline of digital forensics is still in its infancy, new forensic research areas in non-standard systems (Beebe, 2009), such as cloud computing, need to be explored, techniques need to be developed, regulations need to catch up, law advisors need to be trained, staff need to be equipped with new knowledge and skills to deal with the new grounds for cyber crimes created by the rapid rise of new models such as cloud computing.

6. **Challenges in external chain of dependency**

As mentioned in the organizational dimension of cloud forensics, CSPs and most cloud applications often have dependencies on other CSPs. For example, a CSP providing an email application (SaaS) may depend on a 3rd party provider to host log-files (PaaS), who in turn may rely on a partner to provide infrastructure to store log files (IaaS). Although many predict the industry is moving towards federated or integrated Cloud in the near future, today every CSP has a different approach to solving this problem. Correlation of activities across CSPs is a big challenge.

Investigation in the chain of dependencies between CSPs may depend on the investigations of each one of the links in the chain and level of complexity of the dependencies. Any interruption or corruption in the chain or a lack of coordination of responsibilities between all the parties involved can lead to problems. Currently threre are no tool, procedure, policy or agreement regarding cross-provider forensic investigations.

7. **Challenges regarding SLA**

Important terms regarding forensic investigations are not included in the SLA at the moment. This is because there is a lack of customer awareness, a lack of CSP transparency and a lack of international regulations. Most cloud customers are still not aware of the potential issues that might rise regarding forensic investigations in the Cloud and their significance. The consequence is that they might end up not knowing anything at all about what has happened in the Cloud in cases when their data is lost in criminal activities and has no right to claim any compensation. CSPs are not willing to ensure transparency to the customers regarding forensic investigations because they either do not know how to investigate cloud crimes themselves or the methods and techniques they are using are likely to be problematic in the highly complex and dynamic multi-jurisdiction and multi-tenancy cloud environment. The progress of any law and regulations including law and regulations of cyber crimes is very slow, while cloud computing is rapidly emerging as a new battlefield of cyber crimes for hackers who are equipped by the most updated techniques, investigators, law enforcement and various cloud organizations.

8. **Challenges regarding Multi-Jurisdiction and multi-tenancy**

The legal challenges of multi-jurisdiction and multi-tenancy concern the differences among legislations in all the countries (states) the Cloud and its customers reside in. The differences between jurisdictions affects on issues such as what kind of data can be accessed and retrieved in

the jurisdiction(s) where the physical machine(s) from which data is accessed and retrieved, how to conduct evidence retrieval without breaching privacy or privilege rights of tenants according to the privacy policis and regulations in the organizations and specific jurisdiction where multiple tenants' data is located, what kind of evidence is admissible to the court in the specific jurisdiction, what kind of chain of custody is needed in the evidence preservation in the jurisdiction(s) where forensic data has passed during an investigation in the Cloud. Multi-jurisdiction issues also concern lack of legislative mechanism that facilitates collaboration between industry and law enforcement around the world, in cases such as resource seizure, cloud confiscation, evidence retrieval, data exhchange between countries, etc.

Cloud Storage

Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service is available to users over a network, which is usually the internet. It allows the user to store files online so that the user can access them from any location via the internet. The provider company makes them available to the user online by keeping the uploaded files on an external server. This gives companies using cloud storage services ease and convenience, but can potentially be costly. Users should also be aware that backing up their data is still required when using cloud storage services, because recovering data from cloud storage is much slower than local backup.

6.4) Popular Cloud Storage Options

1) **Dropbox**

- **Collaboration:** Dropbox gives users the capability of sharing entire folders with other Dropbox account users, which allows updates to be viewable by all collaborators. Users can download shared documents directly from Dropbox's web interface without having to install the Dropbox desktop client. Storing files in the Dropbox "Public" folder allows links to files to be sent to Dropbox and non-Dropbox users; however non-Dropbox link recipients must download the file to access/edit it, and any changes or revisions made to the file by the link-recipients will not be reflected in the Dropbox version of the file.
- **Mobile App Support:** Documents are easily accessible through phone and tablets using the Dropbox mobile app.
- **Storage:** Dropbox offers 2GB of free storage.
- **Strengths:** Primarily in its ease of use. Very intuitive interface—for example, sharing folders is available by simply right-clicking the file or folder on the desktop, and choosing Sharing. You can also determine how fast files are synced in Preferences (right-clicking the Dropbox icon). You can also recover deleted files in Dropbox easier than some other options.
- **Weaknesses:** Lowest amount of free storage of the offerings reviewed in this document. Also, when inviting users to share files/folders, the email invitation must be sent to the email address that is associated with the users' Dropbox account.

2) **Google Drive**

- **Collaboration:** Users of Google Drive documents must have a Google Drive account. All updates and editing by collaborators will be synced to Google Drive. For documents that you have permission to access, you can receive notifications when changes are made. You can share files with people by sending them a link to your file.
- **Mobile App Support:** Google Drive has an Android app which gives you the ability to share the files on your Android device using your Drive account. You can also share any file from Drive with your phone contacts.
- **Storage:** Google Drive offers 5GB of free storage.
- **Strengths:** Has built-in document editor so that programs such as Microsoft Word are not required to be installed on computer in order to edit document. Allows comments to be left on any files stored.
- **Weaknesses:** Sharing not as easy and intuitive as Dropbox—must use the Google Drive web application to set it up. Also no ability to set preferences on syncing speed.

3) Microsoft SkyDrive

- **Collaboration:** Colleagues can access SkyDrive files without having to sign up for a SkyDrive account. You can also update documents simultaneously online with colleagues.
- **Mobile App Support:** SkyDrive offers both a Window's phone app and an iOS (iPhone/iPad) app. This allows users to view and share as well as edit and update files via phone or tablet. SkyDrive files can also be opened using third party iOS apps, such as Pages and Keynote.
- **Storage:** SkyDrive offers 7GB of free space.
- **Strengths:** Offers the most storage for free of the options reviewed in this document. Like Google Drive, you can edit documents within the browser, without having to open up a client application like Microsoft Word.
- **Weaknesses: –** Skydrive is somewhat less user friendly than Dropbox and Google Drive.

4) Box

- **Collaboration:** You can share content with both colleagues that do have Box accounts, and those who don't. Like Dropbox, you can create a shared folder and invite Box account colleagues for ongoing sharing. You can receive email notifications when files are uploaded, downloaded, or added. You can also set passwords for important files and set time limits for user access to certain files. You have more control over user access to files and documents because security levels can be defined. Box is geared more towards businesses and enterprises, but it is also available for personal use.
- **Mobile App Support:** Users can view, edit, create and share content on-the-go. You can find files fast with built-in search. It allows you to save files you create or edit in other apps to your Box account. You can also upload files from your phone or tablet to Box as well as save files from Box onto your mobile device for offline access.
- **Storage:** Box offers 5 GB of free storage.

- **Strengths:** You can store larger file sizes. Box is organized and user friendly, you can create and organize several layers of folders for all of your documents and data. You can use tagging as a way to keep track of your folders and files. Tags allow you to mark and sort related files that may not be located in the same section of your Box. Box offers the highest security options. Content management tools.
- **Weaknesses:** Box doesn't do file-syncing from the computer to box.com as simply as other services do. There is a desktop component called Box Sync, but it's available only to Business and Enterprise account holders for a fee.

Advantages of Cloud Storage

- **Usability** – All cloud storage services reviewed in this topic have desktop folders for Mac's and PC's. This allows users to drag and drop files between the cloud storage and their local storage.
- **Bandwidth** – You can avoid emailing files to individuals and instead send a web link to recipients through your email.
- **Accessibility** – Stored files can be accessed from anywhere via Internet connection.
- **Disaster Recovery** – It is highly recommended that businesses have an emergency back-up plan ready in the case of an emergency. Cloud storage can be used as a back-up plan by businesses by providing a second copy of important files. These files are stored at a remote location and can be accessed through an internet connection.
- **Cost Savings** – Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.

Disadvantages of Cloud Storage

- **Usability** – Be careful when using drag/drop to move a document into the cloud storage folder.This will permanently move your document from its original folder to the cloud storage location. Do a copy and paste instead of drag/drop if you want to retain the document's original location in addition to moving a copy onto the cloud storage folder.
- **Bandwidth** – Several cloud storage services have a specific bandwidth allowance. If an organization surpasses the given allowance, the additional charges could be significant. However, some providers allow unlimited bandwidth. This is a factor that companies should consider when looking at a cloud storage provider.
- **Accessibility** – If you have no internet connection, you have no access to your data.
- **Data Security** – There are concerns with the safety and privacy of important data stored remotely. The possibility of private data commingling with other organizations makes some businesses uneasy.
- **Software** – If you want to be able to manipulate your files locally through multiple devices, you'll need to download the service on all devices.

Local Storage	
Advantages	**Disadvantages**

• The user has complete control over access to your files and therefore it is really secure in comparison to an online storage where you don't know where your data is stored and who has access to your data. • The data can be accessed easily and quickly. • The user does not require an internet connection to access the document.	• Have to constantly keep backup of data to prevent loss. • The user is completely responsible for the safety of the data. • The user is competely responsible for the safety of the data. • It is more difficult to share your data with others. • Takes up more storage space if you store locally.

Evaluation

Local storage is at great advantage because the data is more secure, the user has complete access an internet connection is not required however in the 21st century the disadvantages of local storage outweight the benefits. This is because in the world of work people are required to work collaboratively and share the work and therefore it is easier to do this with a hosted storage.

UNIT 7

REAL FORENSIC CASE AND ITS TOOLS

INTRODUCTON TO SOME FORENSICS TOOLS

1) HELIX

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification. For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly complete. The Helix tool is very robust and free of charge. Helix can be run as an operating system, it can be run from command line and it also has a windows GUI. Helix allows for the analysis of a live system. Many corporate systems use Windows and the Windows GUI is a perfect way to get started in practicing forensics. In this document you will find simple laboratories to follow so that you may familiarize yourself with the Helix tool using the Windows GUI and get started in the practice of computer forensics.

2)FTK

UNMATCHED SPEED AND STABILITY

FTK uses distributed processing and is the only forensics solution to fully leverage multi-thread/multi-core computers. While other forensics tools waste the potential of modern hardware solutions, FTK uses 100 percent of its hardware resources, helping investigators find relevant evidence faster.

FASTER SEARCHING

Since indexing is done up front, filtering and searching are completed more efficiently than with any other solution. Whether you're investigating or performing document review, you have a shared index file, eliminating the need to recreate or duplicate files.

DATABASE DRIVEN

FTK is truly database driven, using one shared case database. All data is stored securely and centrally, allowing your teams to use the same data. This reduces the cost and complexity of creating multiple data sets.

3)Autopsy

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

Easy to Use

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the intuitive page for more details.

Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX.

See the Features page for more details. Developers should refer to the module development page for details on building modules.

There is currently a Autopsy Module Writing Contest going on right now before OSDFCon 2016. Start writing modules for cash prizes.

Fast

Everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder. See the fast results page for more details.

Cost Effective

Autopsy is free. As budgets are decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis, that other commercial tools do not provide.

4) FIRE

FIRE is a portable bootable cdrom based distribution with the goal of providing an immediate environment to perform forensic analysis, incident response, data recovery, virus scanning and vulnerability assessment.

Also provides necessary tools for live forensics/analysis on win32, sparc solaris and x86 linux hosts just by mounting the cdrom and using trusted static binaries available in /statbins.