Digital Forensics

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. The term digital forensics was first used as a synonym for computer forensics. Since then, it has expanded to cover the investigation of any devices that can store digital data.

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.The context is most often for the usage of data in a court of law

the role of digital forensics and its environment

Digital forensics is probably the most intricate step of the cybercrime investigation process, and often yields the strongest evidence in terms of prosecutable cases. Digital forensics as a field can be divided into two subfields: network forensics and host-based forensics. Network forensics focuses on the use of captured network traffic and session information to investigate computer crime. Host-based forensics focuses on the collection and analysis of digital evidence collected from individual computer systems to investigate computer crime. The four main phases of the digital forensic process include: collection, examination, analysis, and reporting. It is a digital forensics best practice to make a full bitstream copy of the physical volume. This usually entails physically removing the hard drives from the suspect system and attaching the drives to another system for forensic duplication. The

data must be unaltered and the chain of custody must be maintained.Documenting hardware configuration is a tedious but essential part of the forensic process.

The magnitude of documentation is in direct correlation to the number and types of devices being acquired. Examination consists of the methodical sifting and combing of data. It may consist of examining dates, metadata, images, document content, or anything else. Every cybercrime incident will involve at least some analysis of data retrieved from systems, whether it's only a few small files from a system or two or terabytes from many machines.

The digital forensic process has the following five basic stages:

1. Identification – the first stage identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.
2. Preservation – the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.
3. Collection – collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
4. Analysis – an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.

5. Reporting – firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.

Tools

Hardware

Hardware tools are designed primarily for storage device investigations, and they aim to keep suspect devices unaltered to preserve the integrity of evidence. A forensic disk controller or a hardware write blocker is a read-only device that allows the user to read the data in a suspect device without the risk of modifying or erasing the content. Conversely, a disk write-protector prevents the content in a storage device from being modified or erased. A hard-drive duplicator is an imaging device that copies all files on a suspect hard drive onto a clean drive; it can also duplicate data in flash drives or secured digital (SD) cards. A password recovery device employs algorithms, such as brute-force or dictionary attacks, to attempt to crack password-protected storage devices.

Software

Most forensic software applications are multipurpose and can perform various tasks in one application. Some applications are open source, which allow experienced programmers to modify the code to meet their specific needs and provide cost savings for law enforcement. Some can process multiple devices simultaneously or manage different operating systems. Some of the tools are :

A. **MemGator**

As the name indicates, MemGator is a memory interrogation tool that automates the extraction of data from memory files and complies a report on the extract data [26]. MemGator brings together a number of memory analysis tools such as the Volatility Framework and PTFinder into the one program. Data can be extracted in relation to memory details, processes, network connections, malware detection, passwords and encryption keys and the registry

b.First on Scene

FoS is a scripted code written in visual basic and it works along with other tools such as LogonSessions, FPort, PromiscDetect, and FileHasher to create an evidence log report. Log report is very important for forensic investigators during the investigation process.

C. **Galleta**

Galleta tool is specialized in inspecting cookies' files which are linked to browsing history. These files provide an idea on

which websites were recently visited and where they keep their traces in the form of cookies.

D. **Ethreal**

Ethreal is network security tool used for sniffing packet traffic on the network (incoming and outgoing). Although this tool is useful; however, it is fragile against encryption codes which deteriorate its performance.

E. **Pasco**

Pasco is a tool used extensively in analyzing browsers' contents and helps in identifying the conducted transaction based on the analyzed contents. The origin of the name comes from Latin language where Pasco means browse.

F. **Rifiuti**

This tool performs its action on recycle bin of the system to recover any recent deleted files. Rifiuti is an open source released under the liberal FreeBSD license [29].

G. **NMap**

Network Mapper or NMap is a network security tool that operates based on scanning a remote workstation for finding any open ports. NMap has the ability to hide its nature from the source workstation so that it won't cause any alert as a malware attack [30].

properties of digital evidence

There are 5 properties of digital forensic :

Admissible : Admissible is the most basic rule (the evidence must be able to be used) in court or otherwise. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

Authentic :If you can't tie the evidence positively with the incident, you can't use it to prove anything. You must be able to show that the evidence relates to the incident in a relevant way.

Complete :It's not enough to collect evidence that just shows one perspective of the incident. Not only should you collect evidence that can prove the attacker's actions, but also evidence that could prove their innocence. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in, and why you think they didn't do it. This is called exculpatory evidence, and is an important part of proving a case

Reliable:

The evidence you collect must be reliable. Your evidence collection and analysis procedures must not cast doubt on the evidences authenticity and veracity.

Believable :

The evidence you present should be clearly understandable and believable by a jury. There's no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if you present them with a formatted, human-understandable version, you must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether you've faked it.

recovering and preserving digital evidence

- Do not change the current state of the device
- Power down the device
- Do not leave the device in an open area or unsecured place
- Do not plug any external storage media in the deviceDo not copy anything to or from the device
- Take a picture of the piece of the evidence
- Make sure you know the PIN/ Password Pattern of the device
- Do not open anything like pictures, applications, or files on the devic
- Do not trust anyone without forensics training
- Make sure you do not Shut down the computer, If required Hibernate it

Recovery

DETECTING DELETED DATA

Many computer users, including criminals, believe that once they delete a file, it disappears from the hard disc. Even some experts believe that files are destroyed when recycle bin is emptied.

But things are not as simple as they think. Deleting files by tools of operating system simply removes the file indicators from the table of disc contents. This table is called differently in different types of file systems. The very term FAT abbreviated from File Allocation Table indicates the system of file storing.

FINDING HIDDEN DATA

Data hidden in a disc zone may be useful for investigation in many different ways. Some data remain present even after data deletion or disc repartitioning. Besides, there are many options for criminals with technical know-how how to hide data, mainly using a disc editor, stenography, encryption etc. Finding, recovery and reconstruction of hidden data can be a very time-consuming and tedious process, but in some cases it may produce evidence that will crack the case.

SLACK SPACE

Another option for hiding data is the slack space caused by file sizes that don’t exactly match the size of the clusters in which they are stored. Forensic experts are interested in this space particularly because of functions through which DOS and Windows operating systems use this slack to fill in the system’s memory (RAM

slack). All kinds of data can be found in this space, and some of them may be crucial for the investigation.

SHADOW DATA

Another option that may be examined is shadow data, created due to a difference in vertical and horizontal alignment of the magnetic heads. Namely, when accessing particular disc sector, the access points of head 1 and head 2 are not exactly the same, and this difference enables some data to remain present even after overwriting. Hence, it is sometimes possible (although very time consuming and expensive) to recover overwritten data.

STEGANOGRAPHY

Steganography implies hiding files within other files. This type of encryption is made possible through empty space or change in value of the least significant bit. The easiest way to explain stenographic methods is through data hidden within images. In this way the entire file may be hidden within different parts of the image. Hidden bits and their order can be detected by using a key to their correct order, meaning only someone who knows the code can successfully reconstruct the file. Surely, like any other code, this one might be cracked by several anti-steganography programs that can detect the presence of hidden files.

Advance Forensic Technology and Practices

DNA Phenotyping

While DNA gathered from a crime scene can be matched to a suspect by comparing samples, DNA can also be used to determine what a suspect physically looks like. DNA has 23 chromosomes that code outward appearance. Forensic scientists can sequence a DNA sample and provide investigators with identifying traits of the suspect, including hair, eye, and skin color. Newer techniques can also predict age and biological background.

Biosensors for Fingerprint Analysis

Like DNA, fingerprints found at a crime scene can be matched to a suspect by comparing them. However, fingerprints aren't always clear or readable. Forensic scientists can now use biosensors to analyze the minute traces of bodily fluids found in fingerprints to identify the suspect. Data that can be detected include age, medications, gender, and lifestyle. Biosensors can also be used on other bodily fluids found at a crime scene.

Immunochromatography

Immunochromatography is a method to test for diseases by dropping a small sample onto a prepared test strip. Results are relatively quick, and common tests that use this technique include COVID, HIV, and even pregnancy tests. In forensics, immunochromatography tests are used to detect substances in subjects' bodily fluids, such as drugs and medications.

A smartphone-based sensor has even been developed to evaluate a saliva sample through immunochromatography without needing to be in a lab.

Geolocating a Suspect or Victim using Stable Isotopes of Water

Isotopes vary from atom to atom and can have a unique signature. Recent forensic developments have found that scientists can determine where the sample could have originated by isolating the isotopes in a water sample found on a suspect or victim.

If there are several samples, the isotopes can even recreate the path that the subject took. Isotope detection through other methods can also be used to determine the number of people present.

Forensic Palynology

Forensic palynology is a relatively new area for forensic scientists. Palynology is the study of pollen, spores, grains, and seeds and can be used in forensics to identify a subject's location. Pollen and spores are minute and can be deposited on skin and clothes largely undetected. Scientists have not developed techniques to gather and compare these trace materials and use them as evidence.

Blockchain-Based Solutions: Cloud Forensics

Over 50 percent of personal and corporate data is now stored in the cloud, meaning on remote servers. As a result, digital forensic scientists have had to develop methods for collecting, analyzing, and evaluating data that has been collected from the cloud.

Managing this data presents a number of security and privacy issues. To help protect the integrity of the data as well as maintain a custody chain, digital forensic scientists have begun to use blockchain technology as it is virtually impossible to tamper with.

Digital Vehicle Forensics

Vehicle forensics has typically been an area where investigators gather physical evidence, including fingerprints, fluid samples, and trace materials like dirt. Also, they can physically examine the car to determine how an accident, crash, or terrorist attack occurred.

However, as vehicles have become more technologically sophisticated, it has opened the field of digital vehicle forensics where scientists and investigators can gather data such as recent destinations, typical routes, personal data, and favorite locations.

Social Network Forensics

Over 3.6 billion people are on social networks, and this number is projected to increase to 4.5 by 2025. When social media first emerged, investigators and forensic scientists didn't have as much data to comb through. Now, the social media data for a particular subject can be daunting.

Recently, to help evaluate this data, scientists have developed models for analyzing the information gleaned from social networks. In order for automated data analysis to be accepted in court, it has to be based on models that are reproducible, explainable, and testable

FORENSIC BALLISTICS

Application of Ballistics for aiding law and legal agencies so as to maintain law and order in our society is referred to as FORENSIC BALLISTICS. It basically aims at identifying the offender and linking him/her to the scene of crime as well as

a weapon of offense. To achieve this purpose forensic ballistic expert performs the following tasks:-

1. Collection of all the physical evidence at the crime scene such as fired cartridges, wads, bullets or shots, firearms, clothes of the deceased and accused etc.
2. Analyzing the physical evidence collected.
3. Studying in detail the different types of marks found on the projectile as well as the cartridge case.
4. Analyzing and evaluating the projectile wounds (living target), impact of projectile (inanimate objects) and fate of the projectile after hitting the target.

The identification of the weapon of offense and linking it to the scene of crime as well as the offender/suspect is the primary aim of a forensic ballistic expert and this is carried out by ascertaining various aspects which are as follows:-

1. Nature of Crime (homicide, suicide, assault etc.)
2. Number of rounds fired from a single firearm and the total number of shooters.
3. Range from which firing took place.
4. Crime Scene Reconstruction
5. Distance between victim and offender
6. Identification of weapon of offense (aided by analysis of projectile injuries)

Photography : It is one of the most critical factors in any crime scene solving cases. Crime Scene photography or forensic photography is an important role depending on the crime scene as well as its a photo in the criminal justice system as a scene of crime evidence. In the 21st century all over the world, all respective forensic science authorities used high-resolution camera, lens and modern instrumentation technology to capture crime scene photographs. Evidence collection and preservation using digital forensic photography is a crucial aspect of a future legal proceeding. Crime scene photography allows us to capture essential aspects of the presented from the crime scene, including its scope, the focal points of the scene, and any physical or material evidence found at or from a result of it.[5] With the use of crime scene photography, the context of the crime scene can be represented through a series of photographs; aiming to tell the whole story. [5] Such photographs are used to capture the physical environment of the scene and its surroundings, in addition to physical evidence in situ and key areas of the crime scene. Crime scene photography is important to the overall documentation of a Crime Scene. Crime scene photography or forensic photography should be considered a main responsibility and duty of forensic photographers, investigators, as everything that is done later is rarely done without a proper photographic foundation. Crime scene Photographers must ensure their work is both ethical and honestly while capturing as much accurate information and detail as possible photographs of a Crime scene

Biometrics - Tool For Identification

Biometric is the science that deals with identification of individuals based on a person's physical and behavioral attributes. It is the most advanced technology

used in the modern world for identification of an individual via fingerprints, DNA, or iris. Basic perspective of biometric authentication is that every person can be accurately identified by his or her physical or behavioral traits. Biometric systems make use of fingerprint, hand geometry, iris, retina, face, hand-vein, facial thermograms, signature, or voice print to verify a person.

Fingerprint Scanning

Fingerprint recognition is a type of physical biometrics. For this authentication method, a fingerprint scanner is used to authenticate data.

Even with the variety of biometric systems, we can simply divide them into three types that work in three different ways: converting a fingerprint into a digital code with an optical sensor, saving conversion using a linear thermal sensor, and converting a fingerprint with a capacitive authentication sensor. Despite this variety, the only difference for the end-user is which manipulations are to be performed with the scanner, i.e., applying their finger (optical and capacitive) or guiding it through a sensor (thermal).

Advantages of Fingerprint Scanning:

- Fingerprints are unique identifiers specific to the individual.
- Most people are familiar with this authentication method.
- No need to remember complex passwords.
- Fingerprint scanners are relatively cheap and can even be bought on Amazon.

Disadvantages of Fingerprint Scanning:

- Injuries, temporary or permanent, can interfere with scans.
- It is a technology that can be bypassed with methods that copy and replicate fingerprints. It's hard to copy one's fingerprint, but it's not impossible.
- It can be bypassed by using someone else's finger while they are asleep or unconscious.

Voice Recognition

Voice is a feature as inherent to each person as their fingerprints or face. The fact that so many companies worldwide use phones for communication offers an excellent opportunity for the use of this biometric authentication method. Moreover, voice recognition is very convenient for users and requires minimum effort on their side.

Voice biometric authentication technology is widely used in several areas directly related to processing users' voices, such as in call centers. Adoption of this biometric technology allows for speeding up of the service, making the work of agents easier, and helping them become more efficient. This technology can have many different use cases such as security systems, credit card verification, forensic analysis, and teleconferencing, etc. In larger projects, especially when the need to protect confidential information is great, voice identification can be applied with another authentication method such as fingerprint scanning.

Advantages of Voice Recognition:

- No need to remember and then use a password while being authenticated.
- Voice is a natural way of communication and interaction between people.
- It saves time for both users and agents, especially when using passive voice biometrics.

- The voice is a unique feature that is extremely hard to falsify.
- It's a widely used method that is familiar to users.

Disadvantages of Voice Recognition:

- Users may not understand how their data is stored and have privacy-related concerns.
- Noisy places may prevent successful authentication.
- Severe respiratory illness may decrease the success rate of authentication.

Iris Recognition

Iris scanning technology was first proposed in 1936 by ophthalmologist Frank Bursch (source). In the early 1990s, John Dufman of Iridian Technologies patented an algorithm for detecting differences in the iris. At the moment, this biometric authentication method is one of the most accurate and is performed with the help of dedicated iris scanners.

This is how the technology works: First, the pupil is located, followed by detecting the iris and eyelids. Next, unnecessary parts such as eyelids and eyelashes are excluded to leave only the iris part, which is divided into blocks and converted into numerical values representing the image. Finally, matching with previously collected data is performed using the same methods to verify identity.

Advantages of Iris Recognition:

- Iris is an internal organ that is well protected against damage by a highly transparent and sensitive membrane. Thus, it's unlikely for minor injuries to influence scanning devices.

- The iris is an invariant organ with a high level of randomness between individuals.
- No need to memorize complicated passwords.

Disadvantages of Iris Recognition:

- This technology is relatively new and still requires improvements.
- It is a method that requires a short distance between the device and the user's eye.
- In low light conditions, the chances of iris recognition are really poor.

Facial Recognition

Facial recognition is the automatic localization of a human face in an image or video. If necessary, facial recognition technology can be used to confirm a person's identity based on the available data - an image of someone’s face stored in a database as mathematical code. Interest in this technology is high because this method can be applied in videoconferencing.

Advantages of Facial Recognition:

- Requires little interaction with the device.
- It is widely used and people are used to this type of technology.
- Highly effective when combined with other biometric methods.
- No need to memorize complex passwords.

Disadvantages of Facial Recognition:

- Lighting changes can affect the system's performance.

- Facial expressions may change the system's perception of the face.
- The use of facial accessories may make it difficult to recognize the user.
- It may cause embarrassment for some users to have to look at their phone often to unlock it.

Forensic Voice Recognition & Audio Enhancement

Forensic speech analysis covers a number of areas including identifying whether a recording has been tampered with, deciphering unclear speech, unraveling speech codes and designing voice line ups for the purposes of suspect elimination and speaker identification. It forms part of our Digital Forensics services.

Audio authentication Investigating whether audio has been edited or tampered with using electronic and metadata analysis and establishing a chain of custody.

Speech decoding Deciphering unclear speech into intelligible transcripts. This includes decoding voice disguise, dialects, fast speech, speech affected by speaker fatigue, stress or intoxication.Speech decrypting Unraveling speech codes.Voice line-ups Akin to visual line-ups for the purposes of suspect elimination.Speaker identification Utilization of fine-grained phonetic analysis to determine probability of speaker’s identity.

Validation of digital evidences

Validating digital evidence requires verification of relevant parts of the digital domain where the evidence is created, processed and transferred, including the evidence file itself, application and operating programmes and the hardware platform. While techniques of digital forensics aid in preserving and locating potential evidence from a crime scene, the extent to which this may be trusted and used as evidence in a particular legal argument still needs to be determined. We suggest that validation of digital evidence, a difficult task for the investigator, poses an even greater challenge to legal practitioners when constructing legal arguments.It is important that digital forensic examiners formally validate digital forensic tools in order **to demonstrate that the tools are accurate and reliable**. It is also important that examiners consider the limitations of tools, particularly tools not explicitly designed with digital forensic investigation in mind.