Project Πρακτικής Zelus, Παναγιώτης Κολλιόπουλος

Digital Forensics Process

- What is Digital Forensics?

Digital Forensics is the practice of identifying, acquiring, and analyzing electronic evidence. Today almost all criminal activity has a digital forensics element, and digital forensics experts provide critical assistance to police investigations. Digital forensic data is commonly used in court proceedings.
An important part of digital forensics is the analysis of suspected cyberattacks, with the objective of identifying, mitigating, and eradicating cyber threats. This makes digital forensics a critical part of the incident response process. Digital forensics is also useful in the aftermath of an attack, to provide information required by auditors, legal teams, or law enforcement.
Electronic evidence can be gathered from a variety of sources, including computers, mobile devices, remote storage devices, internet of things (IoT) devices, and virtually any other computerized system.

- Why Is Digital Forensics Important?

Digital forensics is commonly thought to be confined to digital and computing environments. But in fact, it has a much larger impact on society. Because computers and computerized devices are now used in every aspect of life, digital evidence has become critical to solving many types of crimes and legal issues, both in the digital and in the physical world.
All connected devices generate massive amounts of data. Many devices log all actions performed by their users, as well as autonomous activities performed by the device, such as network connections and data transfers. This includes cars, mobile phones, routers, personal computers, traffic lights, and many other devices in the private and public spheres.
Digital evidence can be used as evidence in investigation and legal proceedings for:

1. Data theft and network breaches: Digital forensics is used to understand how a breach happened and who were the attackers.
2. Online fraud and identity theft: Digital forensics is used to understand the impact of a breach on organizations and their customers.
3. Violent crimes like burglary, assault, and murder: Digital forensics is used to capture digital evidence from mobile phones, cars, or other devices in the vicinity of the crime.
4. White collar crimes (financially motivated, nonviolent or non-directly violent crime)

Digital forensics is used to collect evidence that can help identify and prosecute crimes like corporate fraud, embezzlement, and extortion.

- Steps of Digital Forensics

Identification

This is the initial stage in which the individuals or devices to be analyzed are identified as likely sources of significant evidence.

Preservation

It focuses on safeguarding relevant electronically stored information (ESI) by capturing and preserving the crime scene, documenting relevant information such as visual images, and how it was obtained.

Analysis

It is a methodical examination of the evidence of the information gathered. This examination produces data objects, including system and user-generated files, and seeks specific answers and points of departure for conclusions.

Documentation

These are tried-and-true procedures for documenting the analysis's conclusions, and they must allow other competent examiners to read through and duplicate the results.

Presentation

The collection of digital information, which may entail removing electronic devices from the crime/incident scene and copying or printing the device(s), is critical to the investigation.

- Objectives of Digital Forensics

Knowing the primary objectives of using digital forensics is essential for a complete understanding of what is digital forensics:

1. It aids in the recovery, analysis, and preservation of computers and related materials for the investigating agency to present them as evidence in a court of law
2. It aids in determining the motive for the crime and the identity of the primary perpetrator
3. Creating procedures at a suspected crime scene to help ensure that the digital evidence obtained is not tainted
4. Data acquisition and duplication: The process of recovering deleted files and partitions from digital media in order to extract and validate evidence
5. Assists you in quickly identifying evidence and estimating the potential impact of malicious activity on the victim
6. Creating a computer forensic report that provides comprehensive information on the investigation process
7. Keeping the evidence safe by adhering to the chain of custody

- Types of Digital Forensics

As digital data forensics evolves, several sub-disciplines emerge, some of which are listed below:

Computer Forensics

It analyzes digital evidence obtained from laptops, computers, and storage media to support ongoing investigations and legal proceedings.

Mobile Device Forensics

It entails obtaining evidence from small electronic devices such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.

Network Forensics

Network or cyber forensics depends on the data obtained from monitoring and analyzing cyber network activities such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

Digital Image Forensics

This sub-specialty focuses on the extraction and analysis of digital images to verify authenticity and metadata and determine the history and information surrounding them.

Digital Video/Audio Forensics

This field examines audio-visual evidence to determine its authenticity or any additional information you can extract, such as location and time intervals.

Forensic Data Analysis

This branch of forensics analyzes structured data. The data analysts are mainly involved in investigating financial crimes and fraud.

Database Forensics

Database forensic specialists investigate any access to a database and report any changes made in the data. Database forensics can be used to verify commercial contracts and to investigate large-scale financial crimes.

Email Forensics

Email forensics analysts retrieve relevant data from email. This information can be the senders' and receivers' identities, the content of the messages, timestamps, sources, and metadata. Email forensics tools are widely used when a company is suspected of email forgery.

Malware Forensics

The specialists in this branch detect, analyze, and investigate different malware types to trace suspects and reasons for the attack. They also evaluate the damage caused by the attack and determine the code of the malware.

Memory Forensics

This type of digital forensics is also called live acquisition. It retrieves the data from RAM. The recent development in cybercrime technology enables hackers to leave no traces on hard drives. In such cases, memory forensics helps to track down the attack.

Wireless Forensics

Wireless forensics uses specific tools and methodologies to analyze and investigate traffic in a wireless environment. This type of analysis is crucial when computer crimes or cyberattacks are committed through the breach of security protocols in wireless networks.

Disk Forensics

Specialists in disk forensics retrieve and recover data from hard drives and other physical storage devices, such as memory cards, servers, flash drives, and external USB sticks. Disk forensics analysts make sure any data relevant to the case is recovered, analyzed, and presented as evidence.

- Challenges Faced by Digital Forensics

  Digital forensics experts use forensic tools to collect evidence against criminals, and criminals use the same tools to conceal, modify, or remove traces of their criminal activity. It is known as the anti-forensics technique and is considered one of the key issues digital forensics faces. This branch of forensic science also deals with certain legal, technical, and resource challenges.

1. Extracting data from locked, or destroyed computing devices is one of the challenges that digital forensic investigators face.
2. Ensuring data integrity throughout an investigation.
3. Rapid Technological Development:

   As an example, there are currently eight different operating systems for mobile devices, and their versions are regularly updated. It makes it challenging to develop standard methods of digital forensic analysis.

4. Availability:

   PC’s, mobile phones, tablets, game consoles, GPS devices, and other types of electronic devices are no longer a luxury for the average person.

5. Availability of Hacking Tools:

   The Internet contains information, how-to’s, software, and tools for hackers. Anybody can get access to this type of resource effortlessly.

6. Big Data Era:

   Terabytes of information can now be found even on personal hard drives. Excessive volumes of data make its analysis and preservation a challenging issue.

7. Admissibility:

   The procedure of preserving and presenting electronic evidence is a complex process. It leads to some evidence being rejected by the court.

- Advantages of Digital Forensics

The following are some advantages of digital forensics:

Enables Digital Evidence Analysis

Computer forensics uses investigation and analysis techniques to collect and preserve evidence from a specific computing device to present it in court.

Aids in the Identification of Criminals

Law enforcement officers can frequently track down suspects and piece evidence together to prosecute them by analyzing data on computers and other digital devices.

It Is Capable of Recovering Deleted Data

One advantage of using computer forensics to recover deleted data is that it is relatively simple to do. Most of the time, all you need is the right software and a little know-how.

Enlightens on How Crimes Are Committed

Computer forensics can shed light on how crimes are committed by analyzing digital evidence.

It Has the Potential to Be Used to Prevent Future Crimes

Law enforcement can better target their investigative efforts if they understand how criminals use computers to commit crimes.

- Disadvantages of Digital Forensics

The following are some disadvantages of digital forensics:

Prolonged Procedure

Computer forensics is a lengthy process. Data collection and analysis can take days or weeks.

Requires Specialized Knowledge and Skills

Computer forensics is a process that collects, examines, and reports digital evidence using specialized skills and knowledge.

Can Be Costly

Computer forensics can be costly because it requires specialized equipment and software and is frequently performed by a specialist.

Obtaining Evidence May Necessitate a Court Order

Obtaining the evidence may necessitate a court order. It means there could be a delay in getting the evidence, giving the perpetrator time to destroy or tamper with it.

Evidence Can Be Easily Destroyed or Manipulated

One of the most severe issues with computer forensics is the ease with which evidence can be destroyed or tampered with. Even if investigators successfully recover deleted files or damaged hard drives, there is no guarantee that the evidence has not been tampered with.

- When Is Digital Forensics Used in a Business Setting?

In the context of an organization, digital forensics can be used to identify and investigate both cybersecurity incidents and physical security incidents. Most commonly, digital evidence is used as part of the incident response process, to detect that a breach occurred, identify the root cause and threat actors, eradicate the threat, and provide evidence for legal teams and law enforcement authorities.
To enable digital forensics, organizations must centrally manage logs and other digital evidence, ensure they retain it for a long enough period, and protect it from tampering, malicious access, or accidental loss.

- Phases of Digital Forensics

The following are the phases of digital forensics:

Phase I - Initial Response

The first response is the action taken immediately following a security incident. The nature of the incident heavily influences it.

Phase II - Seizure and Search

During this phase, the professionals look for the devices used in the crime. These devices were then carefully seized to extract information from them.

Phase III - Gather Evidence

Following the search and seizure phase, professionals collect data using the acquired devices. They have well-defined forensic methods for handling evidence.

Phase IV: Protect the Evidence

The forensic team should have access to a secure location where they can store the evidence. They determine whether the information gathered is correct, authentic, and accessible.

Phase V - Data Collection

Data acquisition is when Electronically Stored Information (ESI) from suspected digital assets is retrieved. It aids in gaining insights into the incident, whereas an improper process can alter the data, jeopardizing the evidence's integrity.

Phase VI - Data Analysis

The accountable staff scans the acquired data to identify the evidentiary information that can be presented to the court during data analysis. This phase involves examining, identifying, separating, converting, and modeling data to convert it into useful information.

Phase VII - Evidence Evaluation

The evidence assessment process connects the evidential data to the security incident. Based on the scope of the case, a thorough assessment should be performed.

Phase VIII - Reporting and Documentation

It is the post-investigation phase, which includes reporting and documenting all findings. In addition, the report should contain sufficient and acceptable evidence following the court of law.

Phase IX - Testify as an Expert Witness

Forensic investigators should approach the expert witness to confirm the evidence's accuracy. An expert witness is a professional who investigates a crime to obtain evidence.

- Types of digital evidences

Digital evidence is any sort of data stored and collected from any electronic storage device. Digital evidence can also be retrieved from wireless networks and random-access memory. There are many types of electronic evidence and methodologies of their retrieval, storage, and analysis. The types of electronic evidence include but are not limited to the following examples:

1. Media files (photo, video, audio)
2. User account data (usernames, passwords, avatars)
3. Emails (content, senders’ and receivers’ information, attachments)
4. Web browser history
5. Phone calls (video, audio)
6. Databases
7. Accounting program files
8. Windows registry system files

9. RAM system files
10. Any type of digital files (text files, spreadsheets, PDF files, bookmarks, etc.)
11. Records from networking devices
12. ATM transaction logs
13. GPS logs
14. Electronic door logs
15. CCTV cameras records
16. Hidden and encrypted data
17. Printer, fax, and copy machine logs
18. Computer backups.

- Digital Forensic Techniques

Digital forensics involves creating copies of a compromised device and then using various techniques and tools to examine the information. Digital forensics techniques help inspect unallocated disk space and hidden folders for copies of encrypted, damaged, or deleted files. Here are common techniques:

Reverse Steganography

Cybercriminals use steganography to hide data inside digital files, messages, or data streams. Reverse steganography involves analyzing the data hashing found in a specific file. When inspected in a digital file or image, hidden information may not look suspicious. However, hidden information does change the underlying hash or string of data representing the image.

Stochastic Forensics

Stochastic forensics helps analyze and reconstruct digital activity that does not generate digital artifacts. A digital artifact is an unintended alteration of data that occurs due to digital processes. Text files, for example, are digital artifacts that can content clues related to a digital crime like a data theft that changes file attributes. Stochastic forensics helps investigate data breaches resulting from insider threats, which may not leave behind digital artifacts.

Cross-drive Analysis

Cross-drive analysis, also known as anomaly detection, helps find similarities to provide context for the investigation. These similarities serve as baselines to detect suspicious events. It typically involves correlating and cross-referencing information across multiple computer drives to find, analyze, and preserve any information relevant to the investigation.

Live Analysis

Live analysis occurs in the operating system while the device or computer is running. It involves using system tools that find, analyze, and extract volatile data, typically stored in RAM or cache. Live analysis typically requires keeping the inspected computer in a forensic lab to maintain the chain of evidence properly.

Deleted File Recovery

Deleted file recovery, also known as data carving or file carving, is a technique that helps recover deleted files. It involves searching a computer system and memory for fragments of files that were partially deleted in one location while leaving traces elsewhere on the inspected machine.

- Digital Forensics Tools

Digital forensic tools were developed to examine data on a device without causing damage to it. Digital forensic tools can also assist ICT (information and communication technology) managers in proactively identifying risk areas. Digital forensic tools are currently classified as digital forensic open-source tools, digital forensic hardware tools, and various others.
Popular instruments include:

1. Forensic disc controllers: enable the investigator to read the data from a target device while preventing it from being modified, corrupted, or erased.
2. Hard-drive duplicators: enable the investigator to copy data from a suspect thumb drive, hard drive, or memory card to a clean drive for analysis.
3. Password recovery devices: crack password-protected storage devices using machine learning algorithms.
4. File viewers and file analysis tools work to extract and analyze separate files.
5. Registry analysis tools get the information about a user and their activities from the Windows registry.
6. Internet and network analysis tools provide detailed information about traffic and monitor user’s activity on the Internet.
7. Email analysis tools are designed to scan email content.
8. Mobile device analysis tools help extract data from the internal and external memory of mobile devices.
9. Mac OS analysis tools retrieve metadata from Mac operating systems and provide disk imaging.
10. Database forensics tools can analyze and manipulate data and provide reports of activities performed.

Here are some of the most popular digital investigation tools:

The **Sleuth Kit** allows forensic specialists to utilize a collection of command-line tools, access a C library, and analyze disk images and recover files.

Xplico is a network forensic analysis tool (NFAT) that helps reconstruct the data acquired using other packet sniffing tools like Wireshark. It is free and open-source software that uses Port Independent Protocol Identification (PIPI) to recognize network protocols. The tool is built on four key components: Decoder Manager, IP Decoder, Data Manipulators, and Visualization System.

FTK Imager is an acquisition and imaging tool responsible for data preview that allows the user to assess the device in question quickly. The tool can also create forensic images (copies) of the device without damaging the original evidence.

OSForensics lets you extract forensic evidence from computers quickly with high performance file searches and indexing. Identify suspicious files and activity with hash matching, drive signature comparisons, e-mails, memory and binary data.

Free Hex Editor Neo is an extremely fast and flexible binary editor optimized for large files. A full “basic” editing command set is supported by the editor: you can modify data, insert data, delete data and change file's size. In addition, advanced editing commands, such as Fill and Insert File are provided.

Bulk_extractor is a C++ program that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. The results are stored in feature files that can be easily inspected, parsed, or processed with automated tools.

Volatility allows forensic specialists to rapidly list kernel modules from an 80GB system, perform virtual machine introspection and use a customizable web interface.

Cellebrite UFED (Universal Forensic Extraction Device) allows forensic specialists to employ data collection capabilities in the lab, at a remote location and in the field; retrieve cloud tokens and app data; and overcome mobile encryption challenges and password/PIN locks.

Medusa allows forensic specialists to use multiple services that allow remote authentication, explore a supported list of services for brute-forcing and save its service module as a .mod file.

Hashcat allows forensic specialists to test mixed device types within one system, use distributed cracking networks and conduct automatic performance tuning.

Webinspect allows forensic specialists to test the dynamic behavior of web applications for security vulnerabilities; conduct simultaneous crawl testing at various levels, from professional to novice; and use centralized program management features.

- DD command
  When using the command-line in Ubuntu, you may need to copy a file from one place to another. You might also want to make sure that the data is accurately copied. For example, say you want a backup of your disk and you want to make sure that it is accurately backed up. To perform this action, you can use the dd (Data Dump) command-line utility available in many Linux distributions, such as Ubuntu and Fedora. The dd tool is a built-in command-line utility, and you do not need to install it before using this tool. The basic purpose of this command is to transfer data from one drive to another while also making sure that the data itself is not changed. The ability of this tool to accurately move data from one device to another makes it a popular tool for backing up your data. Without md5sum, the dd tool only transfers data from drive to drive, but if you use the dd tool with md5sum, then you can ensure that the data transfer will not be corrupted.

Open source forensic tools ανά κατηγορία:

1. GitHub - mesquidar/ForensicsTools: A list of free and open forensics analysis tools and other resources

Forensic tools ανά κατηγορία:
Computer Forensics Tools & Techniques Catalog - Home (nist.gov)
Disc image software:
14 Best Disk Image Software In 2023 [Updated List] (softwaretestinghelp.com)
Open source disc imaging software:
9 Useful Free and Open Source Disk Imaging Software (goodfirms.co)