Digital forensics in terms of its importance and role with respect to cybersecurity crimes and AI.

Alaa Mohammed Abd El-Wahed

Digital forensics in terms of its importance and role with respect to cybersecurity crimes and AI.

Alaa Mohammed Abd El-Wahed

Abstract:

Technology has played an important role in various aspects of life, in addition to its important role in societal development. However, the rapid development that we are witnessing has also led to the rapid development and multiplication of cybercrimes, and thus they have become a threat to both public and private security, but in different forms and mechanisms.

Thus, cybercrime is no longer as tainted by ambiguity as it used to be. It has become more familiar to governments and people as well, but with some differences in terms of the form of the crime and the mechanism of its implementation, for example, crimes of defrauding money and people, hacking websites, preventing unauthorized access, and furthermore, the protocols used in terms of violations of the Internet of Things (IOT). Additionally, there are various mechanisms for it, whether through malicious software, botnet software, hidden networks, etc.

What we will explain is the nature and branches of digital forensics in terms of their importance and role with regard to digital crime, in addition to the methodology of the digital forensic process in this type of crime and the mechanisms for dealing with digital investigations and crime scene inspection and the role of artificial intelligence (AI).

Keywords: Digital forensics; Importance and role of digital forensics; Branches of digital forensics; Digital investigations; crime scene inspection.

Introduction

There is no doubt that technology has revolutionized the way we work and communicate its impact on various sectors, and its role in shaping our future.

It has also become an integral part of our lives, permeating every aspect of society as the connected world consists of embedded systems that are attached to physical space and cloud systems through the Internet that provide various services; furthermore, its impact has never been more profound than it is nowadays.

With each passing time, the pace of technological innovation accelerates, shrinking our world in ways we never thought it could be, breaking down barriers, and enabling people to work together regardless of either their location or society.

Notwithstanding, there is the most important part that should not be overlooked with all this rapid pace of technological development, which is that there is a direct relationship between the development of technology and also the development of digital crime in its various forms, its mechanisms, and how such crimes are committed.

And here specifically comes the role of digital forensics with respect to cybercrimes and how to confront and deal with them from a practical and technical perspective.

I. Definition of the digital forensics

Digital forensics is one of the branches of forensic science, but with regard to violations occurring on or through the computer, which depend on a set of techniques and tools used to find digital evidence in the computer, then the concept later expanded to include all devices that may contain digital data, such as electronic guide sources.

Also, it is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.

Additionally, it is the application of computer technology to a matter of law where the evidence is stored either by or created by people or by technology as a result of human interactions. To illustrate, the data that has been created and recorded or stored manually or automatically due to a technological machine process requires such a machine to be programmed to create that data after being turned on directly or indirectly by the user.

Therefore from an evidentiary standpoint all the data acquired electronically are called an electronic evidence which can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, also without limitation there are some daily aspects that contain some type of digital evidence such as footprint, sending and receiving emails, taking pictures using digital cameras, using car GPS, etc.

Thus the main goal of digital forensics is to extract data from the electronic evidence, process it into actionably and present the findings for prosecution. All processes utilize sound forensic techniques to ensure that the findings are admissible in the court stage.

II. Importance and role of digital forensics

The importance of digital forensics lies in accessing electronic evidence that can support or refute a hypothesis, whether at the level of criminal or civil cases in terms of violations committed against individuals or their property or contractual disputes between commercial entities. There is a form of digital forensics called electronic discovery, and its content comes in the form of information stored electronically.

In conjunction with specialized tools in the field of digital forensic investigations, which provide tremendous insight into attack trends, digital forensics experts track and identify attackers, in addition to studying how they carry out criminal attacks, the tricks and tools used, and the path of threats and security from a legal standpoint. Therefore, its importance lies in law enforcement and criminalization, as actions have become more harmful than those that the law usually prohibits.

III. Branches of digital forensics

Digital forensics is comparatively new field compared to traditional forensic science. It began as computer forensics in the early 1990s and has expanded with the passage of new technology such as devices such as mobile phones, digital cameras, music devices, etc.

There are experts in every field of digital forensics, and it is difficult to find an expert who specializes in all of its fields because digital forensics has a very broad scope, so it shall be divided into several branches to facilitate and clarify the information that each branch may contain as an example, but not be limited to.

Accordingly, the branches of digital forensics can be divided and reviewed as follows:

- Computer Forensics

Computer forensics is a scientific method of investigation and analysis techniques used to gather and preserve evidence from computing devices, networks, and components in a way that is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Computer forensics, also referred to as computer forensic science, is basically data recovery compliant with legal guidelines, making the information admissible in legal proceedings.

Therefore, as it is a technique in order to gather and preserve the information in the form of evidence to be suitable for presentation in a court of law, it starts with the collection of information in a way that maintains its integrity, and then such data shall be analyzed to determine if it was changed, how it was changed, and who made such changes.

Furthermore, it is not only tied to a crime; such a process is also used for data recovery processes to gather data from a crashed server, failed drive, reformatted operating system (OS), or system crash in order to retrieve the data that was previously lost.

Most well-known types are such as database forensics which is the examination of information in databases and related metadata, Email forensics which depends on the recovery and analysis of emails and other information in email platforms, In addition to malware forensics sifting through code to identify possible malicious programs and analyzing their payload such programs may include Trojan horses, ransomware or various viruses.

- Device Forensics

A branch of digital forensics deals with gathering digital evidence available on different types of devices. Sound forensic techniques and a systematic approach are needed. Device forensics is the solution to the issue. Such different types of devices, for instance, are smart phones and tablets, PDAs, disks, printers, scanners, cameras, fax machines, and digital music devices such as iPods, etc.

Clarification of the aforementioned examples as follows:

 Disk forensics: It is the science of extracting forensic information from digital storage media. For instance, computers usually have disks such as hard disk (IDE/SCSI), CDs, DVDs, floppy Disk, USB devices, FireWire devices, flash drives, etc.

 Printer forensics: It is all about the printed materials which are frequently used as a direct accessory by terrorists and criminals. Additionally, printed materials could be utilized for terrorist or illegal actions.

 In both situations, law enforcement and other legal authorities will benefit greatly from being able to identify the device or type of device that printed the content. For instance, counterfeiters frequently employ color laser and inkjet printers after digitally scanning cash to create fake notes.

Fake passports and other documents are created using the same techniques.

Consequently, it's critical to determine not just the printer model that was used, but also the exact printer that was used. As a result, even though two counterfeit bills are made on the same printer, they may be distinguished from one another.

 Scanner forensics: Since digital cameras and scanners are among the acquisition equipment that produce a significant amount of the digital picture data that is already available. Scanners are employed to capture hardcopy art in more controlled circumstances, whereas cameras allow for the digital reproduction of natural scenes. Non-intrusive scanner model identification is essential for a forensic approach, and it can be further extended to validate scanned images.

A robust scanner identifier should be able to identify the make and model of the scanner that was used to capture each unique scanned image based only on samples of scanned images. Based on the statistical characteristics of scanning noise, a proposal for such a scanner identification is made. Several approaches, such as image noise reduction, wavelet analysis, and neighborhood prediction, can be used to scan the noise in the images. From each characterization, statistical information can be extracted.

Further, the same approach can be extended to digital cameras and other imaging devices.

- PDAs forensics:

Personal digital assistants, or PDAs, are gaining a lot of popularity in the modern world. They are more than just electronic devices that store addresses, appointments, and personal data these days. In addition to the typical personal information management functions, modern PDAs are hybrid devices that integrate wireless, Bluetooth, infrared, WiFi, mobile phones, cameras, global positioning systems, rudimentary computing skills, the Internet, etc.

It is more difficult to investigate crimes involving PDAs than those involving regular PCs. This is primarily due to the fact that these gadgets require batteries, are smaller, and use volatile memory to store data. As long as its battery lasts long enough, a PDA is never truly off.

Additionally, together with the aspects of personal information management that are standard. Technology is frequently a "double-edged sword," and as Pereira (2005) notes in his piece, it "breeds crime." PDAs are not an exemption either. Their small size and integrated features are the key reasons they are becoming more and more involved in electronic crimes. In their computer crime report, the Federal Bureau of Investigation (FBI, 2005) has brought attention to the increased number of crimes employing portable devices.

Nevertheless, the digital music device has become a technology that the cyber forensic community should be interested in due to its high storage capacities and PDA functions.

The advent of the digital music revolution has also led to the widespread use of digital music devices. The capacity of some hard drive-based devices can reach up to 60GB. Developers have expanded and added features like a calendar and contact book with this much audio storage capacity (Apple iPod, audio, and more).

These devices can hold papers and photos in addition to music, as they are essentially portable hard drives.

The type of evidence found in PDA is extremely erratic. It is easily modifiable and imperceptibly harmed. To gather such evidence and guarantee its acceptance in a court of law, good forensic practices and a methodical approach are required.

- Smart phones forensics:

Numerous types of evidence can be retrieved by mobile device forensics, such as call records, SMS/MMS messages, app data, browsing history, GPS position data, and multimedia files. The methods of extraction vary from physical and logical extraction through the use of forensic technologies such as Oxygen Forensics, Cellebrite UFED, and XRY, to manual examination.

While logical extraction retrieves files via the device's operating system to provide an organized view of the data, physical extraction offers a bit-by-bit copy of the full memory, possibly retrieving deleted objects and buried data.

The diverse range of operating systems (iOS, Android, etc.), multiple device models, and frequently updated software provide particular issues for smartphones and tablets. Investigators also face challenges when dealing with sophisticated security mechanisms like biometric locks, encryption, and protected containers. Cloud data associated with these devices adds another layer of complexity.

- Memory Forensics

A memory dump is a snapshot capture of computer memory data from a particular moment in time. It is sometimes referred to as a core dump or system dump. Important forensic information regarding the condition of the system prior to an occurrence, like a crash or security breach, may be found in a memory dump. Memory dumps include RAM data that can be used to determine the reason for an occurrence as well as other important information.

Memory forensics is the process of extracting raw data from system memory, including RAM, cache, and system registers, and evaluating it in preparation for additional research.

Memory forensics may provide special insights into system activity that occurs during runtime, such as open network connections and recently run commands or processes. Critical information about threats or assaults is frequently only present in system memory; examples include encrypted keys, chat messages, network connections, account credentials, active processes, inserted code pieces, and non-cacheable browsing history.

Since all programs, malicious as well as not, must load into memory in order to run, memory forensics is essential for detecting attacks that would otherwise be obscured.

The analysis of the memory image file using sophisticated software capable of parsing and interpreting the data structures and artefacts in the memory is the next stage in memory forensics. A few of the most widely used memory analysis tools are the Sleuth Kit, Rekall, and Volatility.

These tools are capable of a wide range of functions, including file extraction, password recovery, registry dumps, operating system identification, and malware signature scanning.

It can be challenging for traditional network and endpoint security tools to detect malware that is directly written in the RAM of your computer. Conventional security systems are generally capable of analyzing input sources such as email, CD/DVD, USB drives, network, and keyboards; however, they are not able to examine volatile data that is kept in memory. These systems are good choices for defending against external hard drives, network storage, BIOS, and ROM malware. However, attacks that upload malware to memory locations designated for permitted programs could nonetheless put your data in execution at risk. Memory forensics and behavioral analysis features that can detect malware, rootkits, and zero days in your system's physical memory are now standard on the most advanced business security systems.

The physical memory of your system can yield priceless threat knowledge, which memory forensics tools can also acquire.

A few instances of physical memory artefacts are as follows:

 Passwords and Usernames: Data that users enter to access their accounts may be kept in the physical memory of your computer.

 Programs that have been decrypted: Any harmful file that is encrypted and executed must first decrypt itself in order to function. Threat identification and attribution are made easier with the help of this threat intelligence.

 Open Clipboard or Window Contents: This can contain copied or pasted data, chat or instant messaging conversations, form field contents, and email contents.

- Multimedia Forensics

One area of forensics that collaborates closely with computer forensics is multimedia forensics. As though The area of forensics known as computer forensics is concerned with using investigative methods to remove and preserve evidence from digital devices that are turned over to legal authorities. Comparatively, multimedia forensics examines the evidence that has been extracted. To preserve the evidence's integrity, identify its

source, and verify its authenticity, the analysis comprises a scientific assessment of the digital data.

By removing and analyzing the digital fingerprints on digital evidence using cutting-edge software that facilitates authentication and scientific analysis, multimedia forensics works to prevent and detect criminal activity. Unsettlingly, digital evidence such as photos, audio files, and video recordings—is not always verified when it comes to its use in criminal investigations. These evidences are frequently altered by criminals in a variety of ways to change the original source's substance and sway an investigation. Verifying and validating the presented evidence is therefore a crucial precondition. The field of multimedia forensics employs instruments to enable the scrutiny, verification, and improvement of digital evidence.

Enhancing low-quality photos and videos to identify the suspect at the crime scene is another significant problem multimedia specialists must overcome. The examination of the 2011 Mumbai serial bomb attack case serves as a case study in this regard. This is a well-known illustration of the difficulties that modern multimedia forensic specialists encounter. The crime scene yielded the CCTV footage that was turned over to the legal system for the investigation. It contained the car thought to be transporting the explosive material responsible for the explosion. The multimedia forensic specialists faced a significant hurdle in identifying the license plate from the made available public CCTV material. Nevertheless, the multimedia forensic specialists were unable to improve the license plate due to the extremely low-quality footage and awkward camera placement. However, the additional physical characteristics of the suspected vehicles were examined and reported by the Multimedia experts.

Multimedia forensic specialists utilize a wide range of advanced techniques these days to analyzes digital evidence. Tools like FTK Imager, Gold Wave, Multi speech, Computerized Speech Lab, Acustek, Audacity, etc. are frequently used for audio recordings that are submitted as evidence.

The tools are used for a number of tasks, such as separating the region of interest in audio samples, utilizing histograms and LPC charts for analysis and authentication, and assisting in the comparison of the extracted hash values from the source with the submitted evidence to see if any changes have been made. The authentication of the evidence can also be ascertained through the use of metadata analysis and Hex value comparison.

For the examination of other digital evidence like images and videos, tools like Amped Five, Amped Authenticate, Kinesense, MIDAS, Adobe Photoshop, Brief Cam, Pinnacle, Clear ID, etc. are commonly used. In the case of video footage provided for the examination, the video clip is converted into frames and then analyzed. The enhancement and correction of the image are achieved by applying a variety of filters, adjusting brightness, contrast, motion deburring, field stabilization, etc. Gradient variation differences, histogram analysis, and video error level analysis are done by the experts to determine the authenticity of the evidence.

- Network Forensics

A subfield of digital forensics called "network forensics" is dedicated to the observation and examination of network traffic. In order to confirm how an attack occurred, a procedure like this one involves collecting and analyzing raw network data as well as methodically observing and monitoring network activity. Using tools like Wireshark or tcpdump, investigators can capture network packets in real-time or from preserved records. These packets can be analyzed to find malicious network anomalies, suspicious activity, or data exfiltration. While servers may hold databases, user data, and website logs, network devices also keep log files that serve as a record of network occurrences.

Network address translation (NAT), proxies, VPNs, and anonymizing networks like Tor make it difficult to track and attribute specific network activities to specific users. Handling the massive amount of data and extracting pertinent information presents another difficulty. Moreover, evidence may be dispersed throughout several networked devices, necessitating a coordinated inquiry.

Typically, packet-level traffic interceptions are used to retain data for subsequent analysis or to filter data in real-time. In contrast to other branches of digital forensics, network data is frequently unstable and infrequently recorded, leading to a reactive approach within the field. These kinds of technologies are frequently used by security experts to investigate network breaches, not only to prove the attacker's guilt but rather to figure out how the attacker got in and close the gap.

IV. Methodology of digital forensic process

The following steps are necessary according to the digital forensics process methodology:

1- Identification is the process that recognizes an event based on its indications and categorizing it. Even while this is not directly related to forensics, it nevertheless matters because it affects various other steps.

2- Preparation includes getting tools, techniques, search warrants, authorizations for monitoring, and management support.

3- Approach strategy: dynamically formulating an approach based on potential impact on bystanders and the specific technology in question. The goal of the strategy should be to maximize the collection of untainted evidence while minimizing the impact on the victim.

4- Preservation: keeping digital and physical evidence distinct from one another, safe, and preserved. This includes restricting access to the digital device or enabling the usage of other electromagnetic devices within an affected radius.

5- Collection: utilizing established protocols take physical scene notes and replicate digital evidence.

6- Examination: a thorough, systematic search of the suspected crime's relevant evidence. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis.

7- Analyze: establish relevance, piece together data fragments, and make conclusions based on the evidence found. To support a crime theory, research and analysis may need to be done multiple times. The difference between analysis and is that more individuals can work on this instance because it might not demand highly technical expertise to complete.

8- Presentation: give a summary of the conclusions and an interpretation of them. This should be stated using abstract terminology and written for a lay audience. Every abstracted term needs to make reference to the particulars.

9- Returning evidence: making sure that tangible and digital property is given back to the proper owner and figuring out what illegal evidence needs to be destroyed and how. Not an explicit forensics step, mind you, but this is a rarely addressed feature of any methodology that seizes evidence.

V. Artificial intelligence in case of digital investigation and crime scene inspection

The safety of all parties involved must come first while examining a crime scene and all processes must be solid from a procedural and technical aspect in order to prevent damage to digital evidence or to challenging its validity procedurally. The inspection team is required to record and take pictures of the crime scene, the evidence's sources, and the actual evidence.

The Chain of Custody, a procedure that represents how digital evidence is obtained and preserved throughout the investigation process and until it is presented, must be used to document digital evidence once it has been collected otherwise the evidence might be contested and rejected in the court of law stage.

The chain of custody form shall contain every each detail about the collected evidences such as who was involved in the operation and their responsibilities, as well as the date and time of the evidence's acquisition, the case number, and the evidence numbers.

In addition to the legal and technical procedures followed for the safety of the crime scene and how to deal with evidence, there is also a greater benefit if artificial intelligence (AI) is used as a tool at the crime scene, as follows:

- Analysis of the data and its accessibility to support the investigation.

- Addressing challenges with a clear scope and case technique.

- Recognizing patterns.

- Clearly articulating the thought process.

- Forensic science frequently involves lowering the proportion of false positive or false-negative results during analysis.

- Formally organizing knowledge representation, which will aid the legal community in finding prompt and accurate solutions.

- Having a performance evaluation that is well-structured.
- Knowledge discovery and data mining.

Additionally, it could be very difficult to identify an individual in a big crowd. Also, even while it might be very easy for a person to make a mistake, it might be difficult to prove in court. But facial recognition technology has simplified everything. This innovative technology is being used by law enforcement agencies worldwide to identify individuals both online and offline. For example, you may feed suspect photographs into machine learning software to train it to identify the suspects across millions of web pages. Think about how tough it would be to search through all of these websites manually for the person that you are looking for. This is particularly beneficial while researching the "Dark Web" where many criminals hide and unlawful activity occurs.

However, AI technology can also be useful for tasks such as identifying patterns in emails and messages, recognizing the numerous components of a single image, and comparing new data with different kinds of pre-existing data stored in system databases. It can also assist investigators in drawing links between suspect information and criminal records that are already accessible, as well as notify them of any previous criminal behavior the suspect in question may have been connected to.

As well as above Artificial intelligence (AI) can also help with the establishment of an online repository all the data acquired during digital forensic investigations. Because storage capacity on USB, hard drives, optical media, and flash drives has been increasing exponentially, it is getting challenging for forensic science investigators to store and evaluate all this data. Artificial intelligence (AI) is showing potential as an effective tool for storing, analyzing, and using this data legally.

VI. Case studies on the role of artificial intelligence in digital forensics

Law enforcement authorities have a severe dilemma as a result of the increase in digital evidence, particularly in cases involving Indecent Images of Children (IIOC).

Consequently, model-based reasoning (MBR) and data-driven model (DDM) age categorization are the two main types of artificial intelligence (AI) that can be applied in digital forensic procedures.

Artificial intelligence (AI) can be broadly classified into two approaches: (i) model-based reasoning (MBR) approaches, which evaluate sensory input in relation to a predetermined understanding of how it can be used to achieve desired outcomes (often referred to as action-based AI); and (ii) data-driven model (DDM) approaches, which process the data itself to identify meaning. AI is defined as "the science and engineering of making intelligent machines, especially intelligent computer programs." DDM techniques are generally applied to applications that need to analyses or sort data in order to find new insights or significant elements.

Adopting AI has a lot of potential advantages for digital investigations, such in the case of IIOC investigations two approaches are obtainable as follows:

 The first is a DDM strategy that involves machine learning to classify images according to the age of the individuals, regardless of the kind of case being looked at, digital forensic procedures require the analysis of computer files. Files that contain images, for instance, will be examined in accordance with their visual contents. Determining the age of the individuals in images is a popular investigative task related to IIOC investigations. Since cases suspected of involving IIOC content are likely to involve large numbers of images, this is a difficult task for a human investigator. Therefore, there is a strong incentive to explore the use of DDM AI approaches, such as Machine Learning, to predict an individual's age in an image.

In order to accurately predict the age of recently taken images, algorithms utilizing supervised machine learning were used in experimental work to learn the link between 316K images and their known ages. The algorithm demonstrated that it could accurately classify images into the child (<18 years old) and adult (≥18 years old) groups in 90% of cases. Additionally, each image is analyzed in less than 0.5 seconds, which is a significant speed increase over human analysis.

- The second is an MBR prioritizing approach that optimizes a multi-stage investigation for handling multiple cases at once, creating a model to explain the application and the actions that can be implemented is a step in MBR approaches. The actions that can be implemented to modify the model's description in order to accomplish a goal can then be automatically determined by an algorithm.

The modelling and optimization of the various activities required in IIOC investigations is one instance of an MBR approach in practice.

The investigative actions can be modelled using MBR techniques in terms of actions that are relevant to each task, and sensory input can be utilized to determine which task is most appropriate to accomplish. In cases when computer resources are restricted, information about any significant findings can also be used to priorities case investigations. For instance, it would be preferable to process cases where discoveries are being made in order to meet prosecution limits more quickly if there are only five PCs available for case inquiry at any given moment. Five case studies were empirically analyzed, and the results showed a 36% reduction in processing time and a

26% reduction in the amount of time required to discover IIOC content.

VII. Conclusion

Artificial Intelligence (AI) applications are quickly surpassing all other applied science fields in significance. It is also helpful to forensic science if our system does not entirely depend on it, particularly with regard to digital crimes. Furthermore, forensic science calls for a high degree of specialization; artificial intelligence (AI) is limited to usage as a support tool in this area. Artificial intelligence (AI) can help digital forensics tools analyses the evidence and simplify the process for forensics specialists to review the data and reach precise findings to identify the crime scene as that a large volumes of data can be processed efficiently, saving the investigator time, and more quickly identifying any information pertinent to the casein addition to the behavioral predictive analysis through the use of DDM approaches. Pre-analyzing current security concerns while taking prior threats into account and maintaining threat recordings to upgrade the system for future use could also be beneficial. The research has demonstrated the significance and function of digital forensics in relation to cybersecurity crimes and artificial intelligence (AI) algorithms, which are currently being used in a number of digital forensics specialties.