BOOK CHAPTER | *"Scrutinizing Bytes"*

Digital Forensics In Multimedia

Frey John Wisdom
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: frey.john.wisdom@gmail.com
Phone: +233242145354 /+233205479212

ABSTRACT

Digital forensics and multimedia forensics are rapidly growing disciplines where electronic information is extracted and interpreted using scientifically accepted and validated processes, to be used in and outside of a court of law. As personal computing and the internet becomes more widespread, these two fields are becoming increasingly important in law enforcement and cybercrime investigation.Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics which focuses on extracting and analyzing contents such as images, videos, and audio to produce forensic evidence from both regular computer systems and special multimedia devices, such as digital cameras, voice recorders etc. This paper seeks to shed some light on digital forensics in multimedia, methods of authentication and challenges.

Keywords: Forensics, Multimedia, Scrutiny, Analysis, Video, Voice, Data, Camera, Authentication

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Frey John Wisdom (2022): Digital Forensics In Multimedia
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 239-250
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P39

1. INTRODUCTION

Digital forensics is a branch of forensic science that focuses on the identification, preservation, examination and analysis of digital evidence, using scientifically accepted and validated processes, to be used in and outside of a court of law. Digital evidence is a component of nearly all criminal practices, and digital forensics expertise is crucial for law enforcement investigations. Digital evidence may be gathered from a variety of sources including computers, mobile phones, digital cameras, hard drives, CD-ROM, USB memory sticks, cloud computers, servers etc. The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution whiles utilizing sound forensic techniques to ensure the findings are admissible in court. Multimedia forensics is the science that aims to evaluate a digital asset by mainly studying it and extracting information that may be used to address and assist an investigation related to the circumstances outlined in that specific digital document.

Digital forensics faces some huge challenges when applied to multimedia data because multimedia content uses a mix of various forms data such as text, audio, images etc. and due to the wide adoption of mobile devices, high bandwidth and cheaper storage, this generates huge amounts of multimedia content all of which are free to store and share through the internet. This growth has pushed digital multimedia into the forefront of human activity and made it an integral part of everyday life as this content must also be secured from illegal use, unauthorized modification and/or destruction etc.

Digital Forensics is a branch of forensic science which involves the process of identifying, preserving, analyzing and presenting digital evidences using scientifically accepted and validated processes, to be used in and outside of a court of law. The first computer crimes were recognized in the 1978 Florida computers act and after this, the field of digital forensics grew pretty fast in the late 1980-90's. Its operation is based on investigating cybercrimes perpetrated in the cyberworld whiles focusing on the analysis of storage media, hardware, operating systems, networks and applications etc. with the aim of collecting, preserving, analyzing and the presentation of evidence from digital sources.

Computers have become smaller, faster, cheaper, easily accessible and even interconnected to other larger systems. Personal Computers (PCs), Supercomputers, Distributed client-server networks, laptops and smart phones etc. are used to transmit information over networks which means an increase in the use of digital information world-wide and each of these acts as a potential source of digital evidence. In general, privacy means allowing or rejecting access to information. The code of ethics needs the forensics professionals to preserve the privacy of the client. Based on the sensitivity concern and the needs of the result, the privacy of the client is required to be compromised for the proper event investigation cases. The digital forensic process is a conventional scientific and forensic method used in digital forensics analysis.

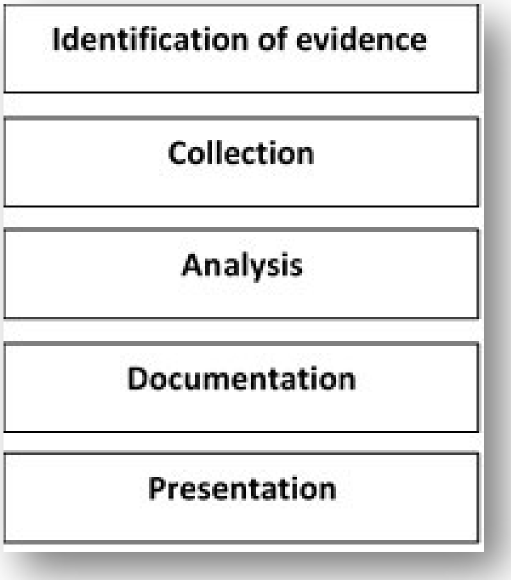

Fig 1: Steps in the Digital Forensic Investigation of Criminal Activities

Digital Forensic Investigation use Information Technology and related techniques to examine criminal activities and detect crime such as fraud, computer security breaches or the distribution of illegal content perpetrated using electronic systems. This makes multimedia data fundamentally essential in Digital Forensic Investigation of criminal activities. It consists of 5 steps;

- Identification of evidence:
  Before any digital forensic examination begins, the scope of actions must be identified. The best sources of potential electronic evidence that will need to be accessed for collection needs to be identified so that no essential evidence which might affect the case is missed, cost can be estimated in advance and the scope of the case can be adjusted to fit actual needs, potential sources of evidence identified later will have smaller impact in cost increases etc.
- Collection:
  The crime scene is not limited to the physical location of digital devices used in cybercrime. The cybercrime scene also includes the digital devices that potentially hold digital evidence, and spans multiple digital devices, systems, and servers. The crime scene is secured when a cybercrime is observed, reported, and/or suspected. The first responder (discussed in Cybercrime Module 5 on Cybercrime Investigations) identifies and protects the crime scene from contamination and preserves volatile evidence by isolating the users of all digital devices found at the crime scene
- Analysis:
  This involves analyzing the collected digital evidences and any other related source of information relevant in tracing the criminal and the possible path used to breach into the system.
- Documentation:
  Proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. during the digital investigative process is essential to support decision maker (i.e., the legal, administrative etc.) in processing of decisions and serve as a guide to analyze other future forensic occurrences and make it admissible in the law court.
- Presentation:
  This stage entails presenting all the digital evidences and documentations in court in order to prove that the digital crime was committed and identify the criminal(s) involved.

There are several branches of digital forensics. These include but are not limited to;

Media forensics:
It is the branch of digital forensics that deals with the identification, collection, analysis and presentation of audio, video and image evidences during a digital investigation process.

Cyber forensics:
It is the branch of digital forensics that deals with the identification, acquisition, analysis, and presentation of digital evidences during a cybercrime investigation.

Mobile forensics:
It is a branch of digital forensics that entails the identification, collecting, analysis, and presentation of digital evidences during the investigation of a crime committed using a mobile device such as a phone, GPS device, tablet, or laptop.

Software forensics:

It is the branch of digital forensics that deals with the identification, collecting, analysis, and presentation of digital evidences during the investigation of a software-related crimes only.

2. MULTIMEDIA Forensics

Multimedia forensics is a set of techniques used to analyze multimedia signals such as audio, video, and images. It aims to but not limited to:

- Disclose the history of digital content.
- Identifying the data acquisition device that generated it.
- Validating the content's integrity.
- Retrieving data from multimedia signals.

When applied to the field of multimedia, digital forensics experienced challenges, since multimedia data combines audio, video, images, and text. Online users generate a massive amount of data that outstrips the forensic professionals' ability to efficiently examine and interpret it as a result of the widespread usage of mobile devices, cheaper storage, and fast bandwidth etc. This expansion has significantly propelled digital multimedia to the forefront and made it an essential component of cyber forensics.

Methods of Multimedia Authentication

Since Internet content is not only limited to text, but also comes in many different forms, the forensic approaches developed to analyze it must also vary in scope. The goal is to analyze images, text, audio, and video to produce logical Forensic evidence.

Multimedia Forensics' operations are divided into two main approaches: Active Image Authentication and Passive Image Authentication.

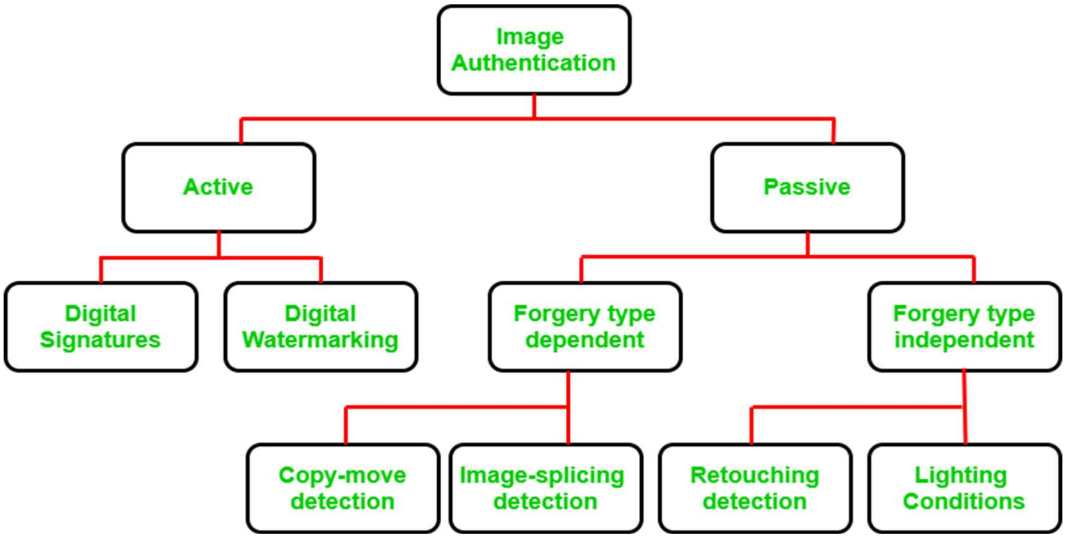

Fig 2: Components of Multimedia Forensics
Source: www.geeksforgeeks.org/multimedia-forensics

i. Active Image Authentication:

A known authentication code is embedded in the image at the time of image generation or sent with the image to access its integrity at the receiving end in this technique. Verifying this code validates the image's originality.

Drawbacks of Active image authentication:

- Because the authentication code must be embedded in the image during recording using special equipment, prior knowledge of the image is required.
- This method necessitates the creation of a digital watermark or digital signature precisely when the image is recorded, limiting its ability to handle specially equipped digital devices.
- Because the majority of images on the Internet today lack a watermark or a digital signature, this image authentication method has been forced to consider additional techniques.

Digital Watermarking and Digital Signatures are the two categories of Active Authentication.

a. Digital Watermarking: This is a technique where a digital watermark is embedded into the image during the acquisition or processing stages.
b. Digital Signatures: Digital signatures embed some secondary information into the image that is typically obtained from the image at the acquisition end.

ii. Passive Image Authentication:

Passive authentication, also known as image forensics, makes use of the only image with no prior information to determine the image's integrity. Passive authentication is based on the assumption that, while tampering with the image may not leave a visible trace, it is likely to change the underlying statistics. This means that digital forgeries can affect the image's underlying properties and quality even if no physical evidence is left behind.

Passive techniques are further classified into *Forgery-type dependent* and *Forgery-type independent techniques*.

a. Forgery-type dependent;

These are intended to detect only specific types of forgeries, such as copy-move and image-splicing, which vary depending on the type of forgery performed on the image.
It is further divided into two categories: image-splicing detection and copy-move detection.

- Copy-move detection:
  Because of the ease with which it can be performed, copy-move is the most popular photo tampering technique. It entails copying some regions of an image and moving them to another region of the image. Because the copied region is part of the same image, the dynamic range and color remain consistent with the rest of the image.

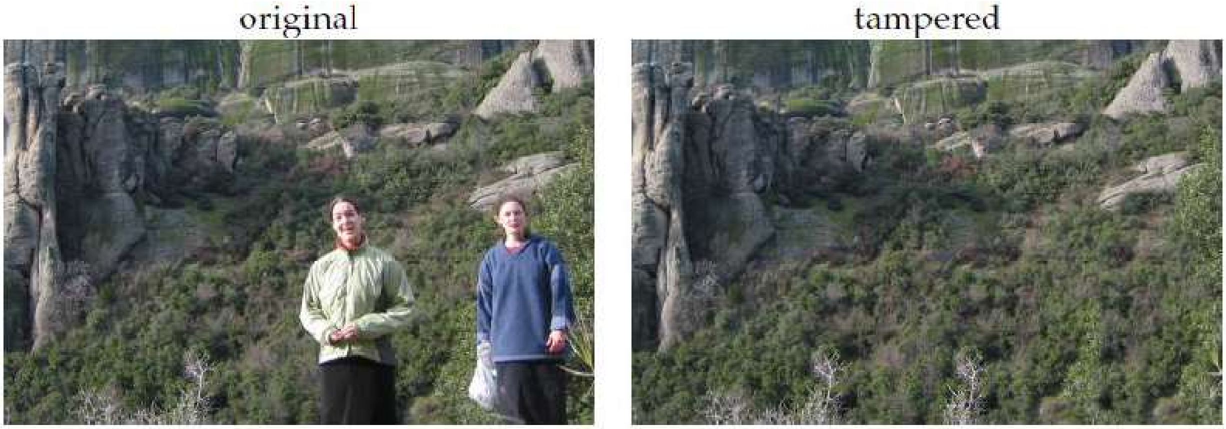

Fig 2: Original and Tampered Images
Source: Image source: https://www.geeksforgeeks.org/multimedia-forensics

Post-processing operations such as blurring are used in copy-move detection to reduce the effect of border irregularities between the two images.

- **Image-splicing detection:**
  The image-splicing method involves combining two or more images and significantly altering the original image to create a forged image. It should be noted that when merging images with different backgrounds, it can be difficult to make the border and boundaries indistinguishable. Image-splicing detection is a difficult task that requires the following techniques:
- A variety of methods are used to investigate composite regions.
- The presence of abrupt changes between different regions that are combined to create a composite image and their backgrounds provides valuable traces to detect splicing in the image under consideration.

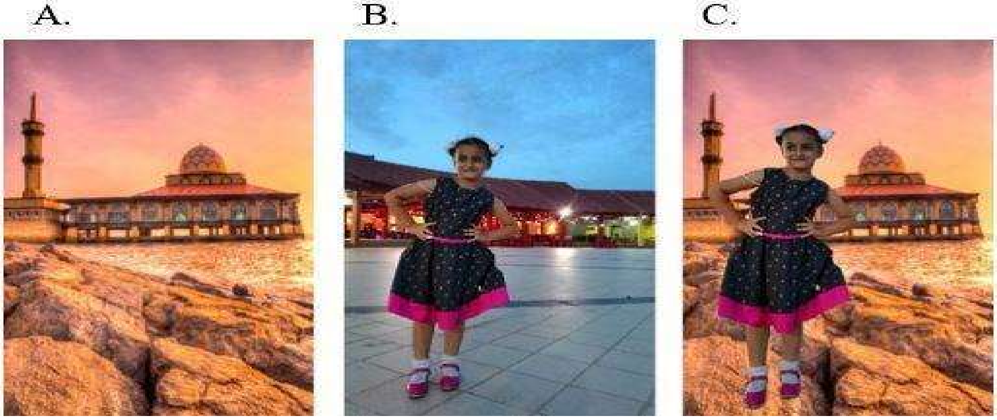

Fig 3: Detecting Splicing In The Image Under Consideration.
Source: https://www.geeksforgeeks.org/multimedia-forensics

b. Forgery-type independent;
These methods detect forgeries regardless of the type of forgery, but based on artifact traces left during the re-sampling process and lighting inconsistencies. It is further classified into two categories.:

a) Retouching detection:
This technique is most commonly used for commercial and aesthetic purposes. Retouching is typically used to enhance or minimize image features, or to create a convincing composition of two images that necessitates the rotation, resizing, or stretching of one of the images. The following techniques are used to detect image retouching:

Locate the blurring, enhancements, color changes, and illumination changes in the forged image. If the original image is available, detection is simple; however, blind detection is difficult.

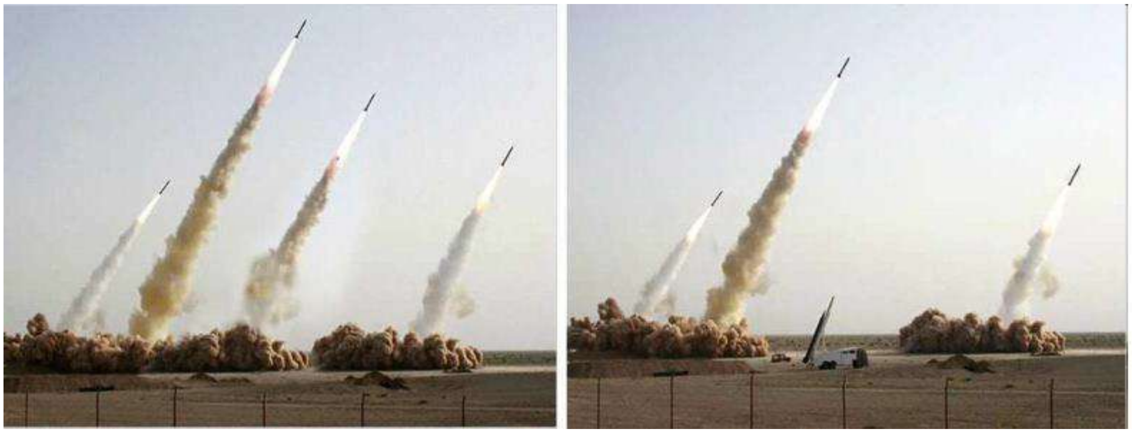

Fig 4: Locating Enhancements and Blurring
Source: https://www.geeksforgeeks.org/multimedia-forensics

b) Lighting Conditions:
Images taken in various lighting conditions are combined during tampering. Combining photographs makes matching the lighting conditions extremely difficult. This inconsistency in lighting in the composite image can be used to detect image tampering.

Digital Fingerprints
Although cryptographic tools and access control mechanisms ensure the secure delivery of multimedia content over the Internet. However, this security is lost once the content is delivered to the end user and safely decrypted. Digital fingerprinting has emerged to address this post-delivery issue by identifying end-users who have authorized access to plaintext but use it for unauthorized purposes. The Digital Fingerprinting process entails investigators tracing the illegal use of multimedia content using a unique identifying information known as a "Fingerprint" that is embedded in the content prior to distribution.

YouTube is using this technology to scan files and compare the digital fingerprints found to a database of copyrighted material to see if any intellectual property is being violated. Digital fingerprints are technically encoded strings of binary digits generated by mathematical algorithms; they are as distinct as a person's analog fingerprints.

With the rapid advancement of computer technologies over the last decade, technology use has been classified as both good and bad. While some people use technology to create things that benefit humanity, criminals use it to achieve their own goals. One of the main issues is that as soon as a technology for identifying and investigating criminals is developed, another technique for hiding criminals is developed. Today, forensics officers face a massive challenge.

- Digital forensics is a method of identifying computer-related crimes. When it comes to conducting investigations, however, digital forensics faces a few major challenges.
- The challenges of digital forensics can be divided into three categories, according to Fahdi, Clarke, and Furnell (2013).
- Technical difficulties, such as different media formats, encryption, steganography, anti-forensics, and live acquisition and analysis
- Legal issues, such as jurisdictional concerns, privacy concerns, and a lack of standardized international legislation.
- Resource constraints, such as data volume and the time required to acquire and analyze forensic media.

3. TECHNICAL CHALLENGES

What follows are identifiable technical challenges

- Unlike many other types of physical evidence, digital evidence is simple to alter, remove, or conceal, possibly without leaving traces that could lead to the criminal's identification. As a result, anti-forensics has become a significant challenge for digital forensics.
- According to Rekhis and Boudriga (2010), anti-forensic techniques are classified into the following categories.
- Encryption
- Steganography
- Covert Channel
- Data hiding in storage space
- Residual Data Wiping
- Tail Obfuscation
- Attacking the tools
- Attacking the investigators

Encryption

Encryption, according to TechTerms (2014), is the process of scrambling information so that it can only be decoded and read by someone with the correct decoding key. On a compromised system, encryption is used to conceal or render evidence unreadable. According to Balogh and Pondelic (2011), in 2007, US Customs discovered child pornography on Canadian citizen and legal US resident Sebastian Boucher's laptop. The laptop was confiscated as evidence, and he was charged with smuggling pornography across borders. The issue arose when investigators attempted to open the incriminating drive Z and discovered that it was a Pretty Good Privacy encrypted container.

Despite the fact that a forensic duplicate of the hard drive was created after the notebook was shut down, the examiner was unable to open the encrypted container. Attackers employ a variety of encryption methods, and in order for the data to be usable, investigators must decrypt the encrypted data. It takes time, and the encrypted data cannot always be decrypted.

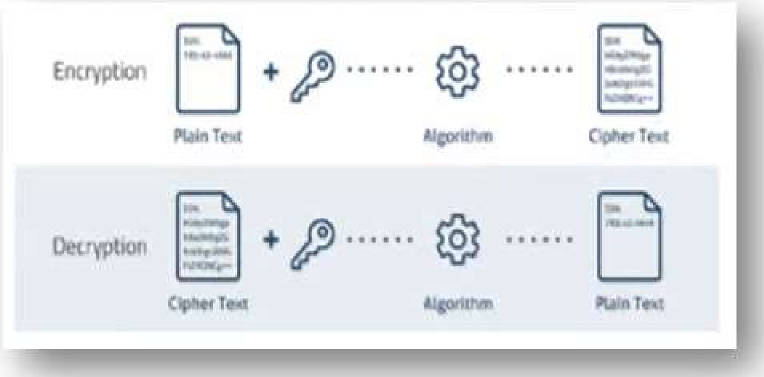

Fig 5: The Encryption and Decryotion Process
Source:www.forensicfocus.com

Steganography

"Steganography is an encryption technique that, when combined with cryptography, provides an extra-secure method of protecting data." Janssen (2014) states that Steganography is a technique for concealing data within a file carrier without altering its appearance. This steganography is used by attackers to conceal their hidden data (payloads) within the compromised system. When investigating computer crimes, the investigator must locate hidden data in order to reveal the information for future use.

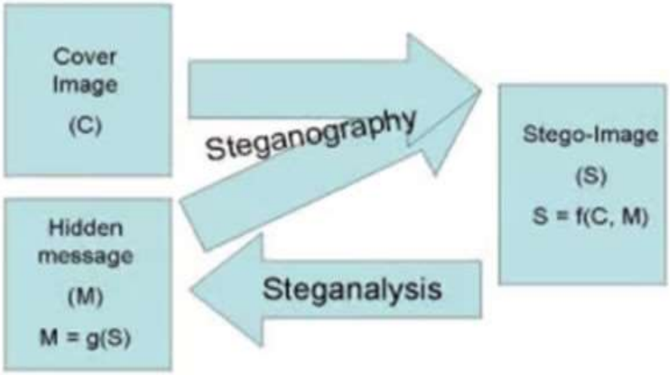

Fig 5: The Steganographic Process
Source:www.forensicfocus.com

Covert Channel

Convert channel in communication protocols to hide data across the network and potentially bypass intrusion detection techniques. Typically, a network protocol is chosen and its header is modified in order to leak messages between attackers, taking advantage of the fact that only a few fields of the header are modified during transmission." Rekhis and Boudriga (2010). Attackers use covert channels to keep a hidden connection between themselves and the compromised system. It is less distinguishable.

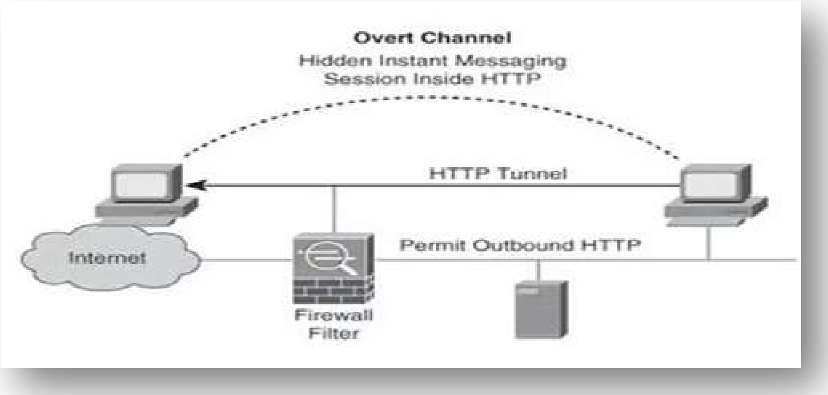

Fig 5: Covert Channel Scenario
Source:www.forensicfocus.com

Attackers conceal data in storage areas, rendering it invisible to standard system commands and programs. It complicates and lengthens the investigation, and it can also cause data corruption. One of the most common methods for concealing data in storage is the use of a rootkit. Malware authors, according to Microsoft (2014), use rootkits to hide malware inside victims' computers. Rootkits are difficult to detect, and most computer users do not know how to remove them. User mode rootkits, according to Kassner (2008), are capable of concealing "processes, files, system drivers, network ports, and even system services."

Residual Data wiping

When an attacker uses a computer to accomplish his goal, a few hidden processes (e.g. temporary files, command history) are running without the attacker's knowledge. However, an astute attacker can avoid this risk by erasing the tracks left by his process and making the system function as if it had never been used for such a purpose. According to Lee's 2013 article, Jake Davis, 20 years old, "was convicted of computer hacking for his role in the notorious group LulzSec." Furthermore, according to Lee (2013), he was "forbidden from creating encrypted files, securely wiping any data, or deleting his internet history."

Tail Obfuscation – attacking the tools

The most common technique, according to Rekhis and Boudriga (2010), is the obfuscation of the source of the attack. In this case, the attacker uses false information to mislead the investigator (e.g., false email headers, changing file extensions). As a result, the investigator may occasionally overlook data with forensic value.

Resource Challenges

The volume of data involved in the case may be substantial depending on the scenario. In that case, the investigator must go over all of the collected data to gather evidence. The investigation may take longer. Because time is a factor, it becomes yet another significant challenge in the field of digital forensics.Because the data stored in volatile memory is ephemeral, user activities in the volatile memory are overwritten. As a result, investigators can only analyze recent information stored on volatile memory. This reduces the data's forensic value in the investigation. When gathering data from a source, an investigator must ensure that no data is altered or overlooked during the investigation, and the data must be well secured. Damaged data sources cannot be easily used in investigations and this makes it a major problem when an investigator discovers a valuable source that cannot be used.

Legal Challenges

Any organization or victim values privacy as well. In many cases, the computer forensics expert may be required to share data or compromise privacy in order to discover the truth. A private company or an individual user may generate a large amount of private information in their daily operations. As a result, asking an investigator to examine their data may expose their personal information.According to Casey (2011), during an investigation into the notorious online Wonderland Club in 2000, Grant argued that all evidence found in his home should be suppressed because investigators had failed to prove that he was the person involved in the illegal online activities in question. The prosecution, on the other hand, presented sufficient corroborating evidence to prove their case.

It becomes difficult when the investigator 'accidentally' discovers or discovers facts related to the crime but is not permitted to use these against the attacker due to privacy concerns. This has an impact on the entire investigation process and limits the investigator to a certain extent. According to Bui, Enyeart, and Luong (2003), because of the wealth of information gathered from forensic investigations, ethical considerations should be examined. To ensure data integrity, data should be collected and stored carefully and legally. As Bui, Enyeart, and Luong (2003) point out, it is critical to respect the privacy of suspects and victims. Furthermore, Bui, Enyeart, and Luong (2003) stated that investigators must be well-versed in a variety of laws and "statutes that govern electronic evidence collection, including the fourth amendment to the United States Constitution."

4. CONCLUSION

The more images and videos continue to flood the Internet, the more difficult it becomes to protect the information through forensic investigations. As online multimedia content grows, it becomes important for the users and creators to understand the legal boundary of the virtual world.

REFERENCES

1. Handbook of Digital Forensics of Multimedia Data and Devices | IEEE eBooks | IEEE Xplore. (n.d.). Retrieved May 23, 2022, from https://ieeexplore.ieee.org/book/7394656
2. An Introduction to Challenges in Digital Forensics - Forensic Focus. (n.d.). Retrieved May 23, 2022, from https://www.forensicfocus.com/articles/an-introduction-to-challenges-in-digital-forensics/
3. Digital forensics. (n.d.). Retrieved May 23, 2022, from https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics
4. Cyber Forensic Security on Multimedia Communication. (n.d.). Retrieved May 23, 2022, from https://shodhganga.inflibnet.ac.in/handle/10603/287112
5. Computer Forensics: Multimedia and Content Forensics - Infosec Resources. (n.d.). Retrieved May 23, 2022, from https://resources.infosecinstitute.com/topic/computer-forensics-multimedia-content-forensics/
6. Multimedia Forensics - GeeksforGeeks. (n.d.). Retrieved May 23, 2022, from https://www.geeksforgeeks.org/multimedia-forensics/
7. Digital Forensics in Information Security - GeeksforGeeks. (n.d.). Retrieved May 23, 2022, from https://www.geeksforgeeks.org/digital-forensics-in-information-security/
8. An example of image splicing (A) and (B) The genuine images (C) The... | Download Scientific Diagram. (n.d.). Retrieved May 23, 2022, from https://www.researchgate.net/figure/An-example-of-image-splicing-A-and-B-The-genuine-images-C-The-resulted-image_fig3_316667407