

Cybercrime Unmasked: Investigating Cases and Digital Evidence

Hamza Azam¹, Mohammad Irfan Dulloo^{1*}, Muhammad Hassan Majeed¹, Janelle Phang Hui Wan¹,
Lee Tong Xin¹ and Siva Raja Sindiramutty¹

¹ School of Computer Science, Taylor's University, Subang Jaya, Selangor, Malaysia

*Corresponding author

Abstract

The advent of rapid digital technology has opened doors to a new domain for criminal activities, commonly termed as computer crimes. Stringent penalties have been instituted by various countries and institutions to combat these offenses executed through computers or networks. Central to investigating these crimes is digital evidence, pivotal in the realm of digital forensics. The digital forensics process comprises five critical phases: acquisition, preservation, analysis, reconstruction, and presentation. Its core aim is to locate and present digital evidence in court, aiding in determining the culpability of individuals involved in computer crimes. This discipline encompasses specialized fields such as data recovery, conversion, erasure, file identification, encryption, decryption, and IP address tracing to apprehend culprits. This paper conducts a thorough examination of the digital forensics stages using sample cases that elucidate five distinct computer crimes. It delves into evidence origins, collection methods, and preservation techniques utilized in the investigation. Once this meticulous process is completed, the digital forensics team compiles documented findings for presentation in a court of law.

Keywords: Computer crime; Cybercrime; Digital evidence; Digital forensics.

1. Introduction

A. Definition of Computer Crime and Digital Evidence

Computer Crime, also referred to as cybercrime, involves individuals with a profound understanding of computer systems who seek to exploit technology for their personal gain, engaging in malicious activities with the aim of victimizing users in the online realm (Hope, 2023; Alferidah & Zaman, 2020, Almrezeq et al., 2021). In recent times, the evolution of Information and Communications Technology (ICT) has made

electronic devices an indispensable aspect of our daily lives. These devices have ushered in numerous advantages for humanity, prompting substantial investments. However, some individuals, known as cybercriminals, have exploited technological progress, giving rise to new forms of digital-era crimes. The enhanced accessibility of ICT and the internet has made cybercriminals more proactive, leading to a surge in computer crimes (Shalaginov et al., 2017; Annadurai et al., 2022).

The examination of these computer crimes falls under the domain of digital forensics. In the field of digital forensics, electronic data serves as the basis for evidence, commonly referred to as digital evidence. Investigators can build cases against cybercriminals by tracing their digital footprints through meticulous audit trails. Moreover, it is of paramount importance to assess the reliability and authenticity of digital evidence to ensure its admissibility in a court of law, as digital evidence is susceptible to manipulation. Consequently, it is imperative to employ appropriate authentication methods to ascertain the trustworthiness and legitimacy of digital evidence (Abiodun, 2018; Chaurasiya et al., 2023).

B. Cybersecurity Law and Confidentiality Integrity and Availability (CIA)

Cybersecurity law refers to a set of legal regulations and measures designed to protect information technology systems and users from various threats and risks in the digital realm (Allahrakha, 2023). It aims to ensure the security and privacy of digital data and the safety of individuals and organizations online. The primary objective of cybersecurity laws is to compel companies and organizations to strengthen their cybersecurity measures, policies, and practices (Bongiovanni et al., 2022; Elijah et al., 2019). These laws are put in place to mitigate the growing cyber threats and vulnerabilities that exist in the online environment. Many countries around the world have enacted cybersecurity laws to safeguard the interests of their citizens, businesses, and governments in the digital space (Mishra et al., 2022). These laws may vary in scope and specific requirements, but they generally share the common goal of enhancing cybersecurity.

Confidentiality, Integrity, and Availability (CIA), these are the three core principles of information security, often referred to as the CIA triad (Chitadze, 2023, Gaur et al., 2022, Gaur et al., 2021, Gouda et al., 2022). They are fundamental concepts that guide the design and implementation of cybersecurity measures and policies. This principle is focused on ensuring that sensitive and private information is kept secret and only accessible to authorized individuals or systems. It aims to prevent unauthorized access, disclosure, or exposure of sensitive data. Measures to achieve confidentiality include encryption, access controls, and data classification. Integrity ensures that data remains accurate and reliable (M. Ali et al., 2023, Hamid et al., 2019). It involves protecting data from being altered or tampered with by unauthorized parties. Data integrity measures can include checksums, digital signatures, and version control to detect and prevent unauthorized changes (Shukla et al., 2022; Humayun et al., 2020). Availability ensures that information and IT systems are accessible and operational when needed. This means that users should have timely access to data and services without interruption (Nasiri et al., 2019, Humayun et al., 2020a, Hussain et al., 2019, Nanglia et al., 2022, Nawaz et al., 2021). Availability is maintained through redundancy, disaster recovery plans, and measures to prevent and mitigate service disruptions. In the context of cybersecurity law, these principles are often mandated by legal regulations. For example, laws may require organizations to protect the confidentiality of customer data, maintain the integrity of financial records, and ensure the availability

of critical services. Compliance with these principles is essential not only for legal reasons but also for maintaining trust and security in the digital environment. Cybersecurity professionals and organizations work to balance these three principles, considering the specific needs and risks associated with their systems and data.

C. Importance of Protecting CIA

Cybersecurity is fundamentally rooted in the principle of the CIA, making it of paramount importance in the realm of cybersecurity. According to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the core essence of cybersecurity revolves around upholding the principles of confidentiality, integrity, and availability (Ian Cornelius, 2020). It is imperative for every organization to prioritize the protection of these facets of information.

Several methods are employed to achieve the critical CIA principle. These methods encompass the implementation of various security controls, the enforcement of appropriate guidelines, policies, and standards, and the initiation of training programs. To attain cybersecurity objectives, numerous organizations, including the National Institute of Standards and Technology (NIST), the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), and the Internet Engineering Task Force (IETF), have instituted cybersecurity programs. These frameworks share the primary goal of preserving the CIA triad.

Effectively addressing cybersecurity is a complex endeavor, underscoring the necessity for organizations to implement robust cybersecurity guidelines and frameworks to counter the escalating malicious threats (Grispos, 2019; Humayun et al., 2021).

D. Scope of the discission

The scope of this paper encompasses an in-depth exploration of cybercrime and digital evidence, with a primary focus on various facets of cybercrimes such as cyberbullying, data theft, ransomware, phishing, and identity theft. In the introductory section, we establish the definitions of computer crime and digital evidence, highlighting the significance of cybersecurity laws and the principles of Confidentiality, Integrity, and Availability (CIA) in safeguarding digital information. Emphasizing the importance of protecting CIA, we set the stage for a comprehensive investigation into these critical aspects of cybercrime. Each subsequent section delves into a specific cybercrime category, providing a detailed examination of sample cases within the respective domain. For each case, we explore the sources of evidence, how evidence is collected, and the crucial measures taken to ensure the protection of this evidence. By addressing these different types of cybercrimes and their associated digital evidence, this paper aims to shed light on the methods, challenges, and best practices in investigating and combating cybercriminal activities. Through a holistic analysis of these cases and evidence management, we contribute to a better understanding of the complexities and nuances within the realm of cybercrime, ultimately advancing our knowledge and strategies for addressing this ever-evolving threat. In the conclusion, we synthesize the key findings and insights derived from the

various sections, offering a cohesive summary of the investigative processes, and highlighting the overarching significance of protecting Confidentiality, Integrity, and Availability in our digital landscape. This paper serves as a valuable resource for legal professionals, law enforcement, cybersecurity experts, and anyone interested in comprehending the intricacies of cybercrime and digital evidence.

2. Cyberbullying (Computer Crime #1)

Cyberbullying, often referred to as the use of information technology tools to threaten, harass, victimize, or bully individuals or groups, is a significant issue in the digital age (Martellozzo & Jane, 2017; Jayakumar et al., 2021). It is formally defined as "the use of information and communication technologies (ICT) to enable deliberate, recurrent, and abusive behavior by an individual or a group with the intent to harm others." Examples of cyberbullying include sending or uploading obscene content or employing modern technology to inflict gratuitous cruelty on victims. The widespread availability of the internet and internet-accessible devices has resulted in a substantial increase in online communication (Lee et al., 2023; Khan et al., 2022). Consequently, the number of reported cases of cyberbullying is on the rise. The growing number of young people and teenagers using the internet makes them particularly vulnerable to cyberbullying, as they may lack the ability to distinguish between right and wrong behavior, making it challenging for them to recognize if they are being victimized (Zainudin et al., 2016; Khan et al., 2022a).

Cyberbullying encompasses various specific activities, including flaming, denigration, harassment, flooding, masquerade, trolling, and cyberstalking (Yi & Zubiaga, 2023; Kumar et al., 2022, Kumar et al., 2015;). In the context of this computer crime, we will discuss the specifics of cyberstalking, as it is closely related to the sample case discussed in the following section.

Cyberstalking, in essence, involves the use of the internet and internet-accessible devices by criminals or stalkers to pursue and harass someone online (Mišev et al., 2023; Ponnusamy et al., 2020). Online harassment and abuse are also associated with cyberstalking. Cyberstalks employ multiple methods, such as following a person, sending harassing messages or phone calls, tracking victims on social media platforms, and various other means to make the targeted individual feel threatened or unsafe (Steinmetz, 2019; Prabakar et al., 2023). The key factor enabling cybercriminals to engage in cyberstalking is the anonymity the internet provides, allowing them to conceal their identity while stalking their victims (Keswani, 2017; Priyadarshini et al., 2021).

A. Sample Case

The tragic case of Brandy Vela underscores the severe consequences of cyberbullying and online harassment. Vela took her own life on November 29, 2016, by inflicting a self-inflicted wound to her chest. The blame for this tragedy was directed at cyberbullies and abusers who impersonated Vela on Facebook and dating sites. These malicious individuals created fake profiles on social media platforms, including Facebook, where they published intimate pictures and her mobile number. Following this, Vela's mobile phone was inundated with abusive calls and text messages. The torment did not cease even after Vela's death, as threatening pictures were posted on her Facebook tribute page with the intent of harassing her (Cbsnews.com, 2017; Hassan, 2016).

In response to this tragic incident, law enforcement acted. Two suspects in the case, Andres Arturo Villagomez (A.A.V), aged 21, and Karinthya Sanchez Romero (K.S.R), aged 22, both from Galveston, Texas, were arrested on March 16, 2017. According to the police report, Villagomez and Romero were dating at the time of their arrest. Investigators, after examining data on Brandy Vela's mobile phone and social media accounts, obtained search warrants for the suspected individuals. The suspects' electronic devices were seized in compliance with guidelines outlined in "Electronic Crime Scene Investigation: A Guide for First Responders." Subsequent investigative procedures adhered to the guidelines set by the National Institute of Justice (NIJ) and the Technical Working Group for the Examination of Digital Evidence (TWGEDE).

Priority	Suspect	Connection	Charge
1	Karinthya Sanchez Romero	Villagomez's girlfriend	-Stalking -Online impersonation
2	Andres Arturo Villagomez	Vela's Ex-boyfriend	Unlawful disclosure or promotion of intimate visual material

Figure 1: Sample case

The following sections will discuss possible sources of evidence in such cyberbullying crimes, explain how to collect evidence from these sources, and detail methods to protect the gathered evidence.

B. Source of Evidence

In cases of cyberbullying, primary data sources often revolve around electronically stored data on image files, which can be acquired from seized computer storage devices such as hard disk drives. The electronically stored data may encompass a variety of elements, including deleted or undeleted files, browser cache, slack space, renamed files, and removable media. When identified suspects are involved in these cases, their devices can be seized and examined under the authority of a search warrant. One common objective in such examinations is to reconstruct any form of conversation or communication between the suspect and the victim. This effort can aid in identifying the motive behind the wrongful actions, understanding the relationship between the parties involved, and grasping the context within which the cyberbullying took place.

In the case of Brandy Vela's suicide, a search warrant was obtained to confiscate all digital media, leading to the seizure of personal devices belonging to both suspects. There were no removable or portable storage media devices found, and it was confirmed that both suspects were the sole owners and users of their personal devices following interviews with their friends and family. The potential sources of evidence in this case were the mobile phones and laptops of both suspects. Karinthya's devices included her Dell Latitude D-630 Laptop and Apple iOS7 Phone, while Andres had a Lenovo ThinkPad SL510 Laptop and a

Samsung Galaxy S5 Phone. The operating system, model, and serial numbers for all four devices were also recorded (Nye, 2017).

C. Collection of Evidence

In cases of cyberbullying, it is indeed crucial to thoroughly understand the unique context of each case before proceeding with the analysis of collected evidence. The initial step involves a comprehensive review of the case documentation, carefully examining all image files. This process helps in uncovering the events and interactions that may have led to the incident's development. The activities of both the victim and the perpetrator are subject to meticulous analysis through the reconstruction of various forms of communication, including emails, phone calls, text messages, or any digital trails like images, videos, and documents. The creation of a timeline can aid in reconstructing the sequence of events.

In the sample case, before any data collection commenced, separate media were prepared, with working directories established to store any relevant evidentiary files and data during the collection process. The forensic analysis of the seized devices was conducted using specialized tools. AccessData FTK Imager was utilized to analyze the images of both laptops, and EnCase Mobile Investigator was employed for the examination of the mobile phones. During the logical extraction process, three key elements were targeted for extraction: the file system, which provides insight into file structure, file names, and timestamps; pertinent information to locate case-relevant data through file headers, content, and extensions; and unallocated space to recover files like images and messages relevant to the case. To ensure the extraction of only case-relevant information, primary methods such as timeframe analysis and data hiding analysis were employed.

Several types of files were discovered that directly related to the case, including a summary of text messages in which Romero used a fake account to harass Vela, explicit photos of Vela, and other relevant evidence (Nye, 2017). This meticulous approach to evidence collection and analysis is critical in building a comprehensive understanding of the case and its surrounding context.

D. Protection of Evidence

Maintaining the integrity of collected evidence is a critical stage in any forensic investigation, especially in cases involving electronic data. Preserving the integrity of evidence is essential to ensure that it is not altered or tampered with in any way, particularly when it must be presented in a court of law. This is typically achieved through the use of cryptographic techniques and cryptographic algorithms to prevent any unauthorized alteration of the collected evidence. Physical protection is also of paramount importance, as the evidence must be transported from the crime scene to the laboratory and potentially to the court. Proper sealing and secure handling are essential to prevent any damage or interference with the digital evidence (Varol and Ülgen Sönmez, 2017).

In the sample case, the processing of the evidence was conducted at an accredited forensics laboratory in Houston, Texas, which adhered to professional guidelines for preserving collected evidence. The evidence was securely stored in a mechanical locker equipped with a biometric scanner, allowing only authorized individuals to access the room. This locker also protected the evidence from electromagnetic interference, which is crucial since the evidence is in digital format and can be easily damaged. To authenticate the evidence, the relevant files found during the collection and analysis stage were fingerprinted using

cryptographic algorithms such as MD5 and SHA-1. These cryptographic hashes, along with descriptions and file paths, were used to verify the integrity of the evidence (Nye, 2017). This rigorous approach to evidence preservation and protection ensures that the evidence remains untampered and can be relied upon in legal proceedings.

2. Data Theft (Computer Crime #2)

Data theft, in the realm of computer crime, is a malicious act in which unauthorized individuals or entities gain access to and steal sensitive, confidential, or valuable information stored on computers, servers, or other digital devices (Belmabrouk, 2023; R.Sujatha et al., 2022). This crime involves the unlawful acquisition, copying, or dissemination of data, often for financial gain or to harm individuals or organizations. Data theft can take various forms, and it poses significant threats to privacy, security, and the integrity of digital information (Almaghrabi & Bugis, 2022; Saeed et al., 2023, Sennan et al., 2021, Shafiq et al., 2021, S Verma 2021). One common method of data theft is hacking. Cybercriminals use various techniques, such as exploiting software vulnerabilities or using malware like viruses, trojans, or ransomware to infiltrate computer systems (Ayele et al., 2023; Shah et al., 2022, Sharma et al., 2022). Once inside, they can exfiltrate sensitive data, including personal information, financial records, trade secrets, or intellectual property. Another method involves social engineering, where attackers manipulate individuals or employees into disclosing confidential information, such as passwords or account credentials (Syafitri et al., 2022). Phishing emails and deceptive phone calls are commonly used tactics for this type of data theft.

Data theft can also occur through physical means, such as theft of laptops, external hard drives, or other storage devices (I. Lee, 2022; Shah et al., 2022a, Lim et al., 2019, Lim et al., 2021). In these cases, criminals aim to gain access to the data stored on these devices, either for resale or for leveraging the information against the owner. The motivations behind data theft can vary. Some criminals seek to profit by selling stolen data on the dark web, while others may use it to commit identity theft, financial fraud, or corporate espionage (Jung et al., 2022; Taj & Zaman, 2022, Jhanjhi et al., 2018). In some cases, hacktivists or nation-state actors engage in data theft to advance political or ideological agendas, causing harm on a larger scale. To combat data theft, individuals and organizations employ various security measures, including encryption, strong password policies, regular software updates, and employee training to recognize and thwart phishing attempts. Legal frameworks and regulations, such as the General Data Protection Regulation (GDPR) and the Computer Fraud and Abuse Act (CFAA), provide a basis for prosecuting data thieves and protecting individuals' and organizations' data. In summary, data theft in the context of computer crime involves the unauthorized access and acquisition of valuable or sensitive information through various means, including hacking, social engineering, or physical theft. The consequences of data theft can be severe, ranging from financial loss and identity theft to reputational damage and legal penalties. As technology continues to advance, the importance of safeguarding data and combatting data theft remains a critical aspect of modern cybersecurity.

A. Sample Case

In the scenario described, where a former employee joins a competitor, and shortly thereafter, a significant number of major clients shift to the competitor, it does indeed raise suspicions of potential data theft. To investigate whether the employee was involved in stealing company information (data theft), a digital forensic analysis of the employee's previous computer is a logical step to take.

Digital forensics involves a systematic examination of digital devices and data to identify any unauthorized access, data theft, or other cybercrimes. By scrutinizing the employee's computer, the forensic team can search for evidence of any actions that may have contributed to the loss of major clients. This could involve looking for evidence of unauthorized access to sensitive company information, the copying of proprietary data, or any unusual or suspicious activities related to client lists or company data. Performing a digital forensic analysis is a methodical approach to uncovering any wrongdoing and ensuring the protection of a company's valuable information. It can help determine whether the employee was indeed involved in data theft and provide the necessary evidence to take appropriate actions, such as legal measures or the protection of sensitive company data (Palavalli, 2021).

B. Source of Evidence

In the above sample case, the forensic team examined the following:

Use of USB Devices

When a user connects a USB device to their computer or laptop, an alert is generated, indicating the installation of the device driver (software required to run the device). Subsequently, a popup window appears, explaining how the user can interact with the newly connected device. This process may seem routine for the average computer user, but for forensic examiners, it provides essential information. Each time these windows appear, multiple system and registry files are generated to record the use of USB devices, which the forensic team can utilize to collect relevant evidence.

LNK Files

LNK files, which are shortcut files linked to applications, folders, and files on the user's computer, or on removable media, are automatically created by Windows every time a user opens a file. These files can offer valuable insights to forensic teams.

Jump Lists

Jump Lists contain crucial information, including details like the file path, the application used to access a resource, the date and time of use, and specifics about the drive from which the resource was accessed.

Windows Event Logs and Timeline

Windows Event logs provide users with a centralized location to access important information related to applications and system activities. Meanwhile, Windows Timeline maintains a record of all activities performed on the system (Palavalli, 2021).

C. Collection of Evidence

The forensic team conducted an analysis of USB devices that had been connected to the employee's computer. They scrutinized the date and time of each USB device connection, collecting information on the device's name, manufacturer, the assigned drive letters, and the Windows user profile associated with each device. This comprehensive examination allowed the forensic team to gain insights into how the USB devices were utilized in conjunction with the employee's computer.

The team also gathered LNK files, which are invaluable for tracking deleted or moved files on the computer. In this specific case, LNK files were crucial in establishing whether data had been removed from the computer, supporting the claim of data theft. Even in the absence of files on the computer, LNK files associated with those files provided the forensic team with vital information. Additionally, the forensic team collected Jump Lists, which were instrumental in reviewing recently used files and the applications used to access or modify them. The forensic examiner meticulously reviewed the Windows Timeline to track various activities, such as opened folders, accessed files, and web page history. Windows Defaults maintain a chronological record of activities within the last 30 days. Furthermore, the team examined the Windows Events Log to assess general information, system activities, errors, and warnings.

Upon analyzing the evidence collected, the team reached the conclusion that the employee had connected a USB device to the computer after the date of their resignation with the intent to pilfer highly sensitive and crucial information pertaining to the company's strategy. LNK files played a pivotal role in this investigation, revealing that confidential data was located on the D: drive following the employee's resignation. Moreover, the D: drive had been assigned to the USB device on the exact date when the confidential files were created (Palavalli, 2021).

D. Protection of Evidence

To ensure the protection of evidence throughout the entire investigation, there are several key practices and protocols that should be followed:

Secure Storage: It is of utmost importance that the evidence is stored in a secure and controlled area. The forensic team should maintain a documented record detailing the location of the evidence, who has access to it, and when and why the evidence is moved.

Media Protection: Any external media devices, such as USB drives or external HDDs, connected to the evidence should not be unplugged or tampered with during the investigation.

No Data Copying: Data should neither be copied to nor from the investigating device to avoid any potential contamination or tampering of the evidence.

Photographic Documentation: The forensic examiners should take photographs of the evidence device from all sides. This visual documentation can serve as an additional layer of protection.

Drive Imaging: Before commencing the investigation, it is essential to create an image of the evidence. This process involves duplicating the entire drive. Forensic analysis should be conducted on the duplicate image rather than the original media, preserving the integrity of the original evidence.

Hashing Algorithms: Apply hashing algorithms such as MD5 and SHA-1 to the evidence. This step is crucial for verifying the integrity of the evidence and ensuring it has not been tampered with during the investigation.

Chain of Custody (CoC): Maintain a detailed Chain of Custody record. This record should document the collection and transfer of evidence from the client to the forensic team. It should include information about who handled the evidence, when it was transferred, and the reasons for any transfers. Signatures, along with date and time stamps, should also be included to create a clear audit trail (Garg, 2020).

By adhering to these best practices, the forensic team can safeguard the integrity and security of the evidence, ensuring that it remains admissible and reliable throughout the investigation process.

3. Ransomware (Computer Crime #3)

What's a ransomware?

Ransomware is a criminal act in which malware is utilized to target a victim's files, typically by locking them out of their computer or encrypting their files, rendering them inaccessible (Al-rimy, Maarof, and Shaid, 2018). Essentially, at this stage, the user's files are effectively hijacked. To regain access to their affected files or system, the victim is usually required to pay a ransom, a specific sum of money, to the attackers. This type of attack is notorious for its high success rate, as victims often feel compelled to pay to retrieve their files, driven by the fear of data loss or system downtime. Moreover, ransomware is unlike other forms of malware; it's challenging to remove, and cracking the encryption to unlock the files is nearly impossible. Various encryption techniques are employed, including Client Asymmetric Encryption, Server Asymmetric Encryption, and Symmetric Encryption, among others. Some specific algorithms used include RSA, DSA, AES, and more.

Companies facing such situations often conduct a cost-benefit analysis, comparing the value of the hijacked data with the ransom demand. In most cases, paying the ransom is the easiest and most effective way to resolve the situation, a fact supported by statistics. A recent survey of approximately 300 IT company decision-makers revealed that 83% of victims opted to pay the requested ransom (Greig, 2022). The ransom amount varies significantly, ranging from a few hundred dollars to several hundred thousand dollars, depending on the value of the files and the victim's significance. There are two primary types of ransoms: Locker Ransomware and Crypto Ransomware. Locker Ransomware infiltrates a system, effectively locking the entire system and blocking access. On the other hand, Crypto Ransomware employs encryption to render specific files on the system inaccessible. These encrypted files can only be accessed with the use of a decryption key (Ransomware Encryption Techniques, 2022).

How are ransomware spread?

Ransomware is malicious software designed to encrypt a victim's data and demand a ransom for its decryption (Kara & Aydos, 2022, Kaur et al., 2021). Ransomware spreads through various methods, primarily exploiting vulnerabilities and human behaviors. One common avenue is phishing emails, where attackers send deceptive messages containing infected attachments or links. Clicking on these links or downloading attachments can trigger the ransomware installation (Chaithanya & Brahmananda, 2021). Another method involves exploiting software vulnerabilities. Cybercriminals search for weaknesses in operating systems or applications and use these vulnerabilities to deliver ransomware payloads, often through drive-by downloads from compromised websites (Datta, 2022). Moreover, ransomware can propagate through malicious downloads and infected software. When users visit untrustworthy websites or download compromised software, ransomware may sneak onto their systems. Additionally, some ransomware strains employ worms or self-propagation mechanisms to target vulnerable networked devices, enabling rapid infection across interconnected systems. Remote desktop protocol (RDP) exploitation is another vector; attackers exploit weak or default credentials to access systems remotely, then deliver ransomware payloads (Haber et al., 2022). Lastly, there are cases where attackers compromise legitimate websites, injecting them with malicious code that distributes ransomware to visitors (Teichmann, 2023). Ultimately, understanding these propagation methods is crucial in implementing effective cybersecurity measures to prevent ransomware attacks. Regular software updates, employee training, and robust security practices are key components of defense against ransomware threats.

How is the ransom paid?

Ransom payments in ransomware attacks are typically made in cryptocurrencies like Bitcoin, Ethereum, or Monero (Berry, 2022). These digital currencies offer a degree of anonymity and are difficult to trace, making them the preferred method for cybercriminals. The process typically involves the following steps:

- 1. Contact with the Attacker:** After encrypting the victim's files, the ransomware displays a ransom note on the victim's computer or network, providing instructions on how to make the payment (Connolly & Borrión, 2022). In some cases, victims may receive an email with payment details.
- 2. Setting up a Wallet:** The victim must create a digital wallet to hold the cryptocurrency required for the ransom (Darmawansyah et al., 2023). There are numerous online platforms and software wallets available for this purpose.
- 3. Purchasing Cryptocurrency:** If the victim doesn't already have the required cryptocurrency, they must acquire it. This can be done through cryptocurrency exchanges or peer-to-peer platforms using traditional currency.
- 4. Transferring the Ransom:** Once the victim has the necessary cryptocurrency, they transfer the specified amount to the wallet address provided by the attacker. This transaction is recorded on the blockchain, but the identities of the sender and receiver remain pseudonymous.
- 5. Receiving the Decryption Key:** In many cases, once the ransom is paid, the attacker provides the decryption key to unlock the victim's files. There is an element of trust involved, as there's no guarantee that the attacker will uphold their end of the bargain.

It's important to note that paying the ransom is not recommended, as it does not guarantee the recovery of data, and it fuels the criminal enterprise. Law enforcement agencies and cybersecurity experts generally

advise victims to report the attack and seek other means of data recovery, such as backups and decryption tools.

A. Sample Case

The specific case we have chosen to focus on is the WannaCry Virus. This ransomware attack occurred on May 12, 2017, and lasted for four days, impacting approximately 230,000 users worldwide. The primary targets of this virus were machines running Microsoft Operating Systems, particularly Windows. WannaCry propagated through a vulnerability in Windows known as EternalBlue, which had been developed in the United States. The Shadow Brokers, a hacking group, had publicly disclosed EternalBlue about a year before the WannaCry attack. However, Microsoft had released a security update several months prior to protect users from this vulnerability. Those who had not updated their systems were the ones most severely affected. The virus spread rapidly across the globe, affecting regions from Asia to America. Upon infecting the victim's machine, WannaCry encrypted the user's files and demanded a ransom in Bitcoin for the data to be accessible again. This type of ransomware is classified as crypto ransomware because it utilizes encryption to lock the user's files and data. Microsoft ultimately mitigated the attack by releasing a patch update for its Windows machines a week later. The aftermath of the WannaCry attack was devastating. In the UK, numerous surgeries and hospital activities were disrupted, and the estimated cost of the attack reached approximately £90 million. The virus is reported to have spread to 150 countries, resulting in approximately \$4 billion in losses worldwide.

This attack stands out as one of the most impactful ransomware attacks ever carried out on a global scale. Protecting yourself from such attacks involves several measures. Firstly, exercise caution when opening emails, as the virus can be disseminated via email attachments. Secondly, avoid plugging unknown USB flash drives into your device without conducting a proper scan. Lastly, always ensure that your operating system is up to date with the latest patches released by the manufacturer. While there are various methods to protect against ransomware, these are some of the most common and effective ones.

B. Source of Evidence

In the real world, when a crime occurs, a forensic team is typically dispatched to investigate the crime scene. Similarly, in the case of a computer virus like WannaCry, similar protocols are applied. Here, we are specifically focusing on the WannaCry virus, and the forensic team conducted several analyses on infected devices to gather crucial information about the virus's source and other pertinent details. To conduct these analyses, the team needed to collect evidence, and in this section, we will delve into where this evidence is collected. In our case, the forensic team primarily utilized the physical hard drive of an infected system to obtain the necessary information. This choice is grounded in the fact that when an infection occurs, the virus tends to reside and potentially replicate itself on the victim's hard disk. Therefore, the primary source for collecting all the evidence, including the affected files, is indeed the hard disk, as it contains all the relevant data (Priyanka, 2019).

C. Collection of Evidence

Moving on to the next phase, which involves collecting evidence for analysis. In this section, we will explore the techniques and tools used by forensic experts to gather and prepare evidence for examination.

In the case of the WannaCry virus, experts utilized an open-source tool called FTK Imager to create an image of the hard disk and employed Autopsy for analyzing the affected files. This image proves invaluable for analysis, resembling a snapshot of the entire operating system and its contents. The image was captured in the Standard E01 format. Given that the source of evidence is the PC's hard drive, we can utilize the Digital Intelligence FRED kit to access the image and acquire the necessary information.

The following steps were undertaken to obtain the required evidence from the Windows image (Priyanka, 2019):

Step 1: Launch FTK Imager.exe and navigate to the File Menu.

Step 2: Select the Create Disk Image Option.

Step 3: Choose the source of evidence (in our case, the physical hard drive).

Step 4: Specify the source drive.

Step 5: Select the desired format (in our case, E01).

Step 6: Input the necessary information and configure options like the destination path and image name.

Step 7: Proceed to the Create Image option to initiate the image creation process.

You can observe a sample of the created image file in Figure 1 below.

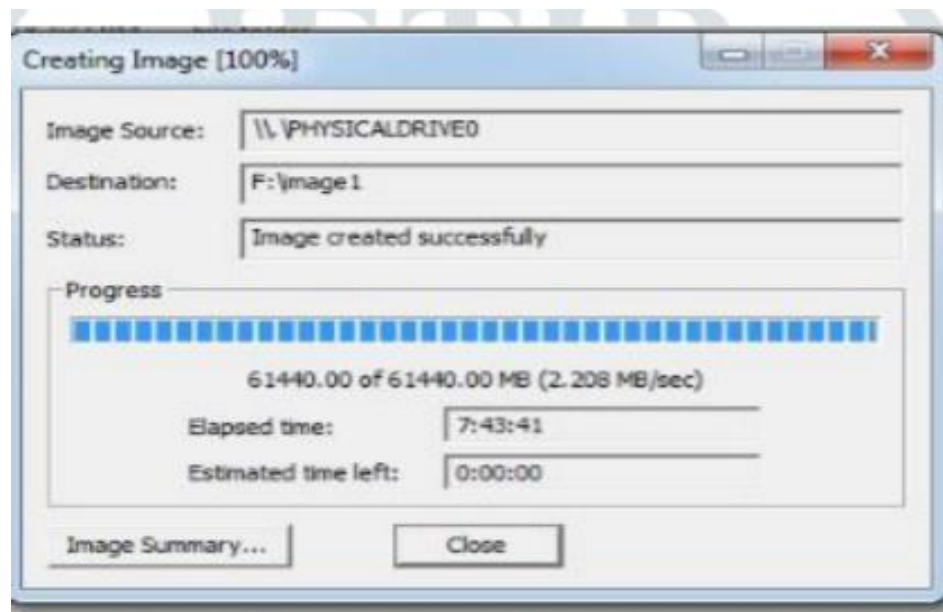


Figure 1: (Priyanka, 2019)

Following the procedures in FTK Imager, forensic experts successfully acquired a preserved image of the Windows device. Subsequently, they employed the Autopsy tool for the analysis of this image. Autopsy offered them the capability to access all files within the hard drive, regardless of whether they had been deleted or not. In our specific case, the experts identified that the infected files were encrypted, identifiable

by the .WNCRY file extension. These files remained inaccessible to the user and could only be decrypted by the attacker once the ransom was paid (Priyanka, 2019).

D. Protection of Evidence

In this section, we will delve into the preservation of evidence, specifically focusing on the steps taken and tools utilized to safeguard the evidence related to the WannaCry virus on a system. To enable forensic experts to investigate this virus, the FTK Imager tool was once again employed to preserve the evidence. This involved using the imaging method to create a duplicate of the hard disk and safeguard the data. Additionally, the volatile memory of the infected system was captured, allowing experts to obtain information about all running processes and the activities occurring on the computer during the attack.

The following steps were employed in the FTK Imager tool to capture the volatile memory and, thus, protect the evidence (Priyanka, 2019):

Step 1: When launching FTK Imager, navigate to the File Menu.

Step 2: Select the Capture Memory option.

Step 3: Specify the destination path for the dump file.

Step 4: Provide a filename for the dump file, and the memory capture process will commence.

A visual representation of the preservation and collection of volatile memory can be observed in Figure 2.

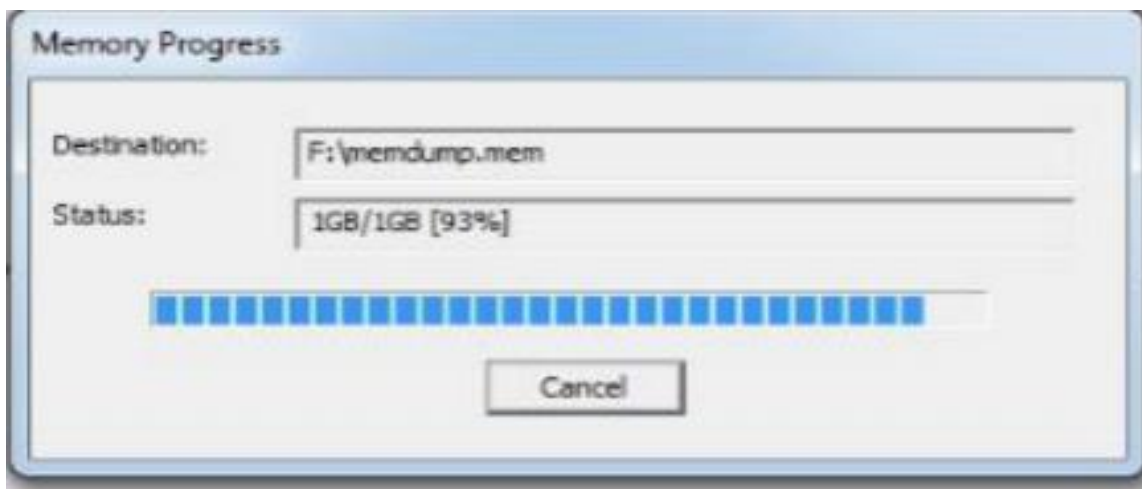


Figure 2: (Priyanka, 2019)

In addition to the methods mentioned in the articles, there are some proposed techniques that were not explicitly stated but are presumed to have been employed. These methods encompass actions such as disconnecting the power cord or shutting down a laptop to maintain it in its most recent state. Furthermore, experts likely documented the condition of the device and digitally isolated it as part of their forensic procedures.

4. Phishing (Computer Crime #4)

Phishing is a widely recognized cyberattack, which can be defined as the act of sending deceptive emails, falsely claiming to represent a legitimate organization, with the intention of tricking the recipient into divulging their personal information (Alkhalil et al., 2021). Typically, the attacker targets large organizations or government networks when launching phishing attacks. This choice is motivated by the fact that such entities employ a considerable number of individuals, and on average, around 5% of employees may become victims of phishing cyberattacks. The attacker usually conceals their true identity to lure the victim into opening the fraudulent email (Alabdan, 2020). Once the victim takes the bait and clicks on a malicious link within the email, malware and viruses are installed into the software system. As a result, the software system becomes compromised, potentially leading to the exposure of sensitive information and data. Such an attack can have devastating consequences, including the risk of identity theft.

How does phishing works?

Phishing commonly takes place via email, where an attacker sends a deceptive email that closely resembles a legitimate one, aimed at deceiving the recipient (Carroll et al., 2022). Email phishing operates on the principle of quantity, as the attacker typically dispatches thousands of fraudulent emails, hoping that some recipients will take the bait (Morovati, 2019, Muthukkumar et al., 2022, Muzammal et al., 2021). These emails often claim to be from a reputable bank and include a link that prompts the victim to update their banking information (Barker, 2020, Basavaraju et al., 2022). To enhance the illusion of legitimacy and boost their chances of success, attackers frequently incorporate bank logos and signatures within the email content. Furthermore, they employ tactics to induce a sense of urgency, such as threatening the recipient with account expiration or placing them on a countdown timer if they fail to transfer the money promptly. This strategy is designed to instill fear in the victim, prompting them to swiftly comply and transfer the money to the attacker.

Spear phishing

Another form of phishing is known as spear phishing, which is designed to target specific individuals or organizations (Burns et al., 2019). This type of phishing demands a high level of cybersecurity expertise from the attacker. To begin, the attacker must conduct research on a target company to determine if it possesses substantial financial resources. Subsequently, the attacker will select an employee responsible for managing the company's finances. Following this, the attacker will gain access to the company's recent project invoices and replicate the organization's standard email template. The fraudulent email will include a link to a password-protected internal document, which is the stolen invoices. Ultimately, the attacker will send this email to the targeted employee to obtain full access to the company's sensitive information and credentials.

A. Sample Case

One of the notable phishing incidents in recent times was the OCBC bank phishing case in Singapore. In December 2021, approximately 420 OCBC bank customers fell victim to SMS phishing scams. The

scammers impersonated OCBC staff by sending SMS messages containing phishing content along with links that directed recipients to fake websites. Despite OCBC's efforts to alert domain hosts to take down these phishing websites, it proved insufficient to thwart the scammers.

According to the Singapore police, most victims received similar phishing messages, which claimed issues with their bank accounts. The content of these SMS messages prompted bank customers to click on a provided link to address the supposed account problems. Upon clicking the link, customers were redirected to a counterfeit website and asked to enter their bank account details, including usernames and passwords. This provided an opportunity for the scammers to access the victims' bank accounts and transfer funds to overseas accounts (TODAY, 2022). Ultimately, the scammers succeeded in pilfering hundreds of thousands of dollars from the bank customers by the end of December. The total amount lost was estimated to be around USD 2.7 million during the Christmas week from December 24 to 26. Prior to this incident, OCBC bank had been working closely with the police to educate customers about SMS phishing through their online banking platforms and social media. Unfortunately, despite these efforts, the scammers managed to bypass the bank's security measures. In response, OCBC bank deployed approximately 100 staff members to combat the scams by shutting down mule accounts. However, the scammers persistently created new mule accounts to funnel the stolen money. Consequently, recovering the victims' funds once they had been transferred to overseas banks proved to be a daunting task. Nevertheless, OCBC bank decided to reimburse customers who had fallen victim to the recent phishing attack.

B. Source of Evidence

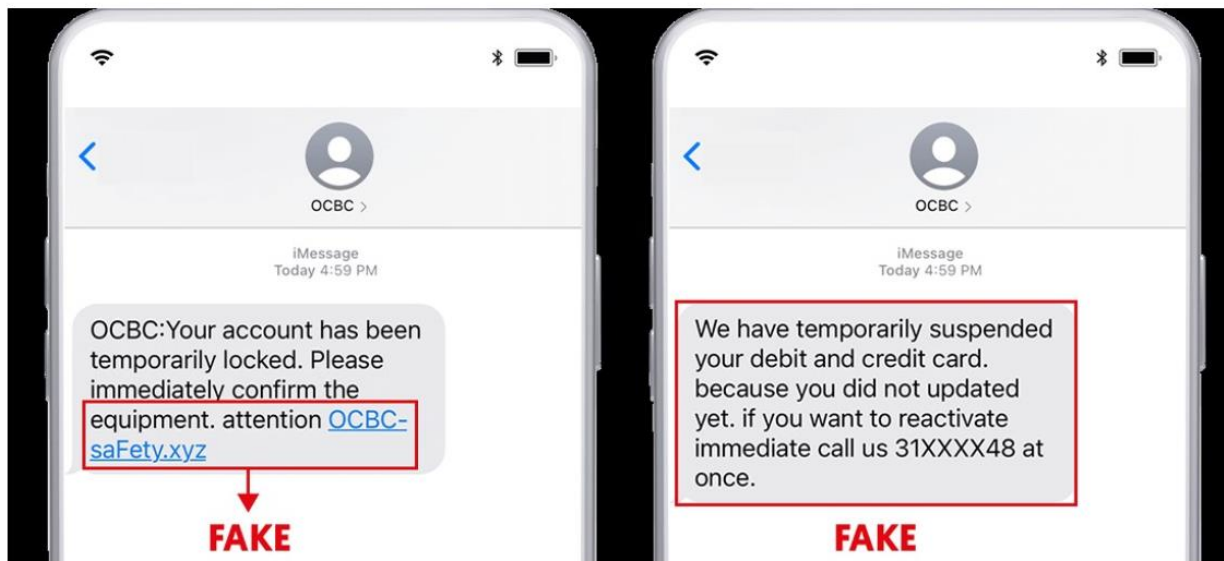


Figure 3: Source of evidence of phishing in OCBC bank

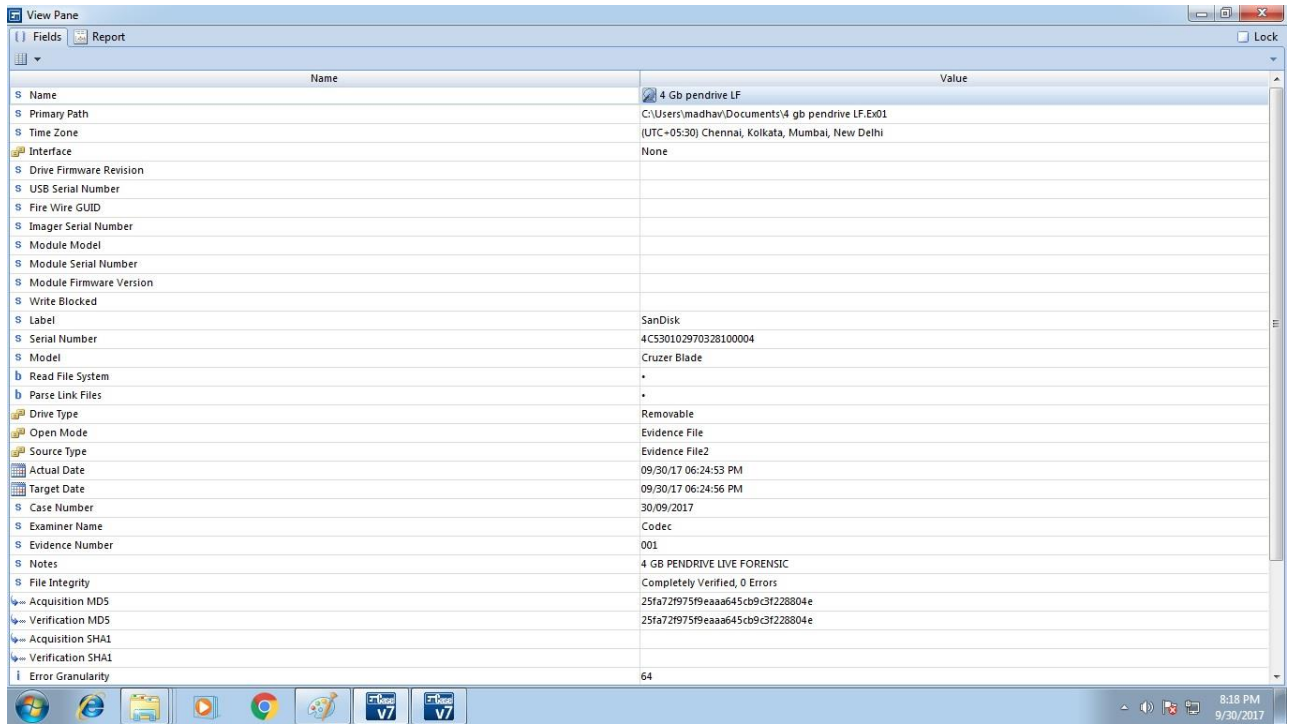
The diagram provided above illustrates the evidence of a phishing incident that occurred with OCBC bank customers. In this case, the scammers posed as bank staff using a spoofing technique to replicate a legitimate sender's name, such as 'OCBC,' in SMS messages. This made the SMS messages appear as if they originated from the legitimate source, which is OCBC bank.

Mobile devices lack the capability to distinguish between legitimate and fake SMS messages because the names and contact numbers of the fake SMS are concealed. As a result, these deceptive SMS messages become intermingled with authentic bank communications in the same message thread. Recipients of these unsolicited SMS messages with 'OCBC' headers found content related to issues with their credit cards or bank accounts. These messages typically included a link for the recipient to click on to address the purported bank issues. When clicked, the link directed the recipient to a counterfeit website, which requested personal bank details, including the bank account PIN number. Upon entering this sensitive information, the scammer gained direct access to the victim's bank account and swiftly transferred the money out. Unfortunately, the victim remained unaware of the scam until they received an unauthorized transaction notification from OCBC bank. Only then did they realize they had been scammed (Ocbc.com, 2020).

C. Collection of Evidence

Next, it is crucial to identify the appropriate forensic tools for investigating phishing scams. In this context, the chosen forensic tool is EnCase. The decision to utilize EnCase is driven by its exceptional capabilities in delving deep into the evidence of phishing incidents, surpassing many other tools available in the market. EnCase stands out due to its compatibility with multiple operating systems, file systems, and even mobile devices. Furthermore, it boasts robust decryption capabilities akin to McAfee, which aids in identifying and unlocking password-encrypted files found in SMS phishing links. This forensic software tool is purposefully designed from the perspective of an investigator, facilitating efficient analysis and compilation of phishing evidence until a conclusive resolution is reached, enabling the case to be closed. EnCase generates an evidence file that includes essential components such as headers, checksums, and data blocks. Subsequently, the computer forensic investigator inputs the relevant information for the ongoing investigation. Moreover, encase performs MD5 hash calculations to inscribe in the evidence file, making it a permanent element of the documentation for the phishing case. The tool also automatically verifies CRC values and recomputes the hash value when the evidence file is incorporated into the case.

Here are the steps that has been carried out to obtain the evidence from the phishing scam SMS messages by using EnCase:



Name	Value
Name	4 Gb pendrive.LF
Primary Path	C:\Users\madhav\Documents\4 gb pendrive LF.Ex01
Time Zone	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Interface	None
Drive Firmware Revision	
USB Serial Number	
Fire Wire GUID	
Imager Serial Number	
Module Model	
Module Serial Number	
Module Firmware Version	
Write Blocked	
Label	SanDisk
Serial Number	4CS30102970328100004
Model	Cruzer Blade
Read File System	.
Parse Link Files	.
Drive Type	Removable
Open Mode	Evidence File
Source Type	Evidence File2
Actual Date	09/30/17 06:24:53 PM
Target Date	09/30/17 06:24:56 PM
Case Number	30/09/2017
Examiner Name	Codec
Evidence Number	001
Notes	4 GB PENDRIVE LIVE FORENSIC
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	25fa72f975f9eaaa645cb9c3f228804e
Verification MD5	25fa72f975f9eaaa645cb9c3f228804e
Acquisition SHA1	
Verification SHA1	
Error Granularity	64

Figure 4: Example of an evidence file that has been created (codecnetworks, 2017)

- 1) Add the phishing website link to the case and then click 'Process'.
- 2) A dialog will pop out from the EnCase Processor Options for you to choose the options needed.
- 3) Choose the option carefully and not too many to avoid taking up too much processing time.
- 4) Click on the right pane to choose your option.
- 5) You can double click on the module's name to see additional options available.
- 6) Next click 'Ok' to start the processing. There is a progress bar located at the bottom of the right corner to view the processing details.
- 7) After completing the process, run the Case Analyzer EnScript to add the processed data into the report.
- 8) Choose the data that is needed then click 'Save Report'.
- 9) If you want to customize the report, click 'Manage Saved Reports'.
- 10) Click 'View Report' to see the final version.

D. Protection of Evidence

This stage is critical for maintaining the integrity of the collected evidence. Safeguarding the phishing evidence is of utmost importance. Let's outline the steps necessary to protect and preserve the evidence of the OCBC bank phishing scams: Select the Appropriate Forensic Tool for Drive Imaging: The first step involves the use of a suitable forensic tool for drive imaging, which is essential for duplicating the drive.

Drive imaging is employed to maintain the original evidence intact for the investigation. An effective tool for this purpose is X-Ways Imager. Notably, X-Ways Imager offers the advantage of being usable from a USB device without the need for installation. It operates by directly installing itself into a temporary folder, consuming approximately 45 MB of drive space (X-Ways Software Technology AG, 2022).

Employ Hash Values to Verify File Integrity: Computer forensic specialists use hash values to verify the integrity of files. Hash values generate MD5 and Sha-1 checksums, which are critical for preserving the evidence to be presented in court. Given that data is inherently volatile, even slight alterations can lead to changes in the hash values. These hash values may not be visible within a standard file explorer but can be accessed using specialized software, such as HashMyFiles (Guru99, 2020).

5. Identity Theft (Computer Crime #5)

What Is Identity Theft?

Identity theft is a pervasive and damaging crime where an individual's personal information is unlawfully obtained and used for fraudulent purposes (Jamal & Zain, 2022). This stolen information typically includes a person's name, Social Security number, credit card details, and other sensitive data. Perpetrators can use this data to commit various crimes, such as financial fraud, tax evasion, or opening new accounts in the victim's name. The consequences of identity theft can be severe. Victims may face financial losses, damage to their credit score, and legal troubles resulting from the fraudulent activities committed in their name (DeLiema et al., 2021). Additionally, the emotional toll and the time required to rectify the damage can be overwhelming. Common methods of identity theft include phishing scams, data breaches, and physically stealing personal documents (Burnes et al., 2020). Safeguarding personal information through strong passwords, encryption, and vigilant monitoring of financial accounts can help prevent identity theft. In the event of a breach, quick action is crucial, involving reporting the theft to law enforcement, credit bureaus, and financial institutions to minimize the damage. In the digital age, where personal information is constantly shared and stored online, understanding, and taking proactive measures against identity theft is essential to protect one's financial and personal well-being (Javaid et al., 2023).

How Does It Happen?

In the realm of cybersecurity, identity thieves have become increasingly sophisticated over the years (How Does Identity Theft Happen? n.d.). One of the most common methods they employ is known as social engineering (Imperva, 2022). Social engineering involves multiple stages, starting with the collection of information about the intended victim. Weak security credentials are often targeted as points of entry. Subsequently, the perpetrator manipulates the victim, creating a deceptive story and establishing trust. Following this, the attacker seeks to extract sensitive information from the victim after gaining their trust. Once this information is obtained, the attacker concludes the interaction and eliminates all traces without arousing suspicion. Additionally, phone scams are a notorious tactic employed by identity thieves. In this scenario, the perpetrator poses as a representative from a reputable institution, often a bank, during a phone call. Victims who are not vigilant may unknowingly disclose private information such as bank account numbers and passwords, resulting in financial losses.

A. Sample Case

In the year 2017, Roman Seleznev, a notorious Russian hacker and the son of a Russian politician, received the longest sentence in the history of the United States for hacking-related charges—27 years in prison. This hacker was responsible for an astonishing \$169 million in credit card fraud, alongside involvement in approximately 400 point-of-sale (POS) hacks that impacted over 3,700 financial institutions and 500 businesses worldwide (Sheridan, 2017). The journey began in the early 2000s when Roman Seleznev, known by the handle 'nCux,' started selling stolen information on the dark web. By 2005, the United States Secret Service (USSS) detected his criminal activities and initiated intelligence gathering. In 2009, when sufficient evidence pointed to Seleznev as the man behind 'nCux,' he mysteriously disappeared, frustrating the USSS (Sheridan, 2017).

During the same year, Seleznev resurfaced under new aliases, 'Track2' and 'Bulba.' These aliases were active on Carder.su, a platform where credit card details and personal data were traded. Under these aliases, he achieved 'trusted seller' status on the platform, alerting the USSS to his long-standing presence in the industry. The USSS reopened its investigation in May 2010. In approximately one year, Seleznev once again engaged in hacking multiple restaurants, pilfering customers' credit card information from POS devices. In January 2012, Seleznev returned to Russia to close his online shop following injuries sustained in a terrorist incident in April 2011. The USSS continued tracking him until 2013 when Seleznev adopted a new alias, '2PAC.CC.' During this period, other hackers sought him out for stolen credit cards and data to resell (Sheridan, 2017).

In 2014, Seleznev was apprehended at the Maldives airport by local police. He was subsequently handed over to USSS agents and transported to Guam, a U.S. territory, before being transferred to a federal prison in Washington, D.C. Eventually, Seleznev pleaded guilty to orchestrating the theft of personal data, credit card fraud, and bank fraud charges.

B. Source of Evidence

When Roman Seleznev was apprehended at the Maldives airport, the USSS seized his devices, believing they held a treasure trove of information from his vacation. The confiscated devices included a laptop, a computer bag, an Apple iPad, a Samsung mobile phone with an installed SIM card, and an Apple iPhone with a SIM card found in Seleznev's pants (Sheridan, 2017). These devices are of utmost importance due to the wealth of information they may contain. Forensic tools can be employed to recover data from these devices. This data can be used to demonstrate the existence of files that were previously stored on the medium but have since been deleted or altered. In addition, operating systems can record supplementary information, such as the connection of peripherals, the attachment of USB flash storage devices or other external storage media, and the periods during which the computer was in use. Furthermore, there may be instances where it's necessary to establish the absence of a specific object on a storage medium to uncover evidence regarding how a device was used, its intended purpose, the user, and the timing of its use.

C. Collection of Evidence

The use of various data analysis tools for searching forensic images of specified devices is essential. Agents and analysts can conduct precise and focused searches to identify evidence without the need for time-consuming manual sorting through potentially irrelevant documents that might be mixed with criminal evidence in some cases. However, there are situations where such approaches may not yield the requested evidence, requiring law enforcement to undertake more extensive searches to uncover materials falling within the scope of the warrant. Only procedures, techniques, and protocols that are reasonably expected to locate, identify, segregate, and/or duplicate the materials allowed to be seized will be employed. These strategies, techniques, and protocols include the utilization of a 'hash value' library to filter out common operating system files that do not require further examination. The evidence sought by the USSS does not possess specific recognized hash values, making it impossible for others to discover the items on the seized devices using any hash value library.

D. Protection of Evidence

To examine Electronically Stored Information (ESI) in a forensically sound manner, law enforcement professionals with the requisite expertise strive to generate a comprehensive forensic image of the confiscated device. The outcome of this forensic image should be both feasible and appropriate. It's crucial to note that law enforcement will only image the data physically present on or within the confiscated devices. Creating an image of the seized devices will not grant access to any data physically stored elsewhere. However, if the seized devices had been previously linked to other devices in different locations, they may contain data from those remote sources. This approach is designed to ensure that no trace of Seleznev will have the opportunity to destroy the seized evidence.

6. Conclusion

In conclusion, we have observed how different forensic tools and methods are applied in various situations for forensic analysis. We've also gained insights into some well-known tools such as FTK Imager, EnCase, Autopsy, and others. Our intention has been to enhance your understanding of how evidence is sought, collected, preserved, and analyzed. As we are aware, technology is a field that evolves rapidly, and this is equally true in the realm of forensics. The field of computer forensics faces certain challenges, and improvements in the process can enhance the success rate of investigations. Some of these enhancements include utilizing hash values during the imaging process to verify image authenticity and prevent a compromised investigation. It's also crucial to maintain a chain of custody to track who is in possession of the evidence and its transfer. Lastly, collecting and analyzing evidence as promptly as possible is essential, as the risk of evidence deterioration increases over time. We trust that these findings and improvements will provide you with a better understanding of the concept of digital forensics, the procedures involved, and how investigations can be made more successful.

References

- [1] Abidin, M. A. Z., Nawawi, A. H., & Salin, A. S. a. P. Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security*, **27**(1), 81–100. <https://doi.org/10.1108/ics-04-2018-0043> (2019).
- [2] Abiodun, O. I. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. https://www.researchgate.net/publication/326847672_Digital_Forensics_Review_of_Issues_in_Scientific_Validation_of_Digital_Evidence (2018).
- [3] Alabdan, R. Phishing Attacks Survey: Types, vectors, and technical Approaches. *Future Internet*, **12**(10), 168. <https://doi.org/10.3390/fi12100168> (2020).
- [4] Alferidah, D. K., & Zaman, N. *Cybersecurity Impact over Bigdata and IoT Growth*. <https://doi.org/10.1109/icci51257.2020.9247722> (2020).
- [5] Almrezeq, N. Cyber security attacks and challenges in Saudi Arabia during COVID-19. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, **12**(10), 2982-2991 (2021).
- [6] Ali, M. et al. A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. *Alexandria Engineering Journal*, **64**, 749–760. <https://doi.org/10.1016/j.aej.2022.10.056> (2023).
- [7] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. Phishing Attacks: a recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, **3**. <https://doi.org/10.3389/fcomp.2021.563060> (2021).
- [8] Allahrakha, N. *Balancing cyber-security and privacy: Legal and ethical considerations in the digital age*. <https://lida.hse.ru/article/view/17666> (2023).
- [9] Almaghrabi, N. S., & Bugis, B. A. Patient confidentiality of Electronic Health Records: A recent review of the Saudi literature. *Dr. Sulaiman Al Habib Medical Journal*, **4**(3), 126–135. <https://doi.org/10.1007/s44229-022-00016-9> (2022).
- [10] Al-rimy, B., Maarof, M., & Shaid, S. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, **74**, 144-166. DOI: 10.1016/j.cose.2017.11.015 (2018).
- [11] Annadurai, C. et al. Biometric Authentication-Based Intrusion Detection Using Artificial Intelligence Internet of Things in Smart City. *Energies*, **15**(19), 7430. <https://doi.org/10.3390/en15197430> (2022).
- [12] Ayele, Y. Z., Chockalingam, S., & Lau, N. Threat actors and methods of attack to social robots in public spaces. In *Lecture Notes in Computer Science*, 262–273. https://doi.org/10.1007/978-3-031-35822-7_18 (2023).

- [13] Babu, C. V. S., Suruthi, G., & Indhumathi, C. Malware forensics. In *Advances in information security, privacy, and ethics book series*, 285–312. <https://doi.org/10.4018/978-1-6684-8666-5.ch013> (2023).
- [14] Basavaraju, P. H., Lokesh, G. H., Mohan, G., Jhanjhi, N. Z., & Flammini, F. Statistical channel model and systematic random linear network coding based qos oriented and energy efficient uwsn routing protocol. *Electronics*, **11**(16), 2590 (2022).
- [15] Barker, R. The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management*. <https://doi.org/10.4102/sajbm.v51i1.1941> (2020).
- [16] Belmabrouk, K. Cyber criminals and data privacy measures. In *Advances in information security, privacy, and ethics book series*, 198–226. <https://doi.org/10.4018/979-8-3693-1528-6.ch011> (2023).
- [17] Berry, H. S. The Evolution of Cryptocurrency and Cyber Attacks. *2022 International Conference on Computer and Applications (ICCA)*. <https://doi.org/10.1109/icca56443.2022.10039632> (2022).
- [18] Bongiovanni, I., Gale, M., & Slapničar, S. Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, **121**, 102840. <https://doi.org/10.1016/j.cose.2022.102840> (2022).
- [19] Burnes, D., DeLiema, M., & Langton, L. Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, **17**, 101058. <https://doi.org/10.1016/j.pmedr.2020.101058> (2020).
- [20] Burns, A. C., Johnson, M. E., & Caputo, D. D. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, **29**(1), 24–39. <https://doi.org/10.1080/10919392.2019.1552745> (2019).
- [21] Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. *SN Computer Science*, **3**(2). <https://doi.org/10.1007/s42979-022-01069-1> (2022).
- [22] Cbsnews.com. Texas couple charged in alleged cyberbullying that led to teen's suicide. [online] Available at: <https://www.cbsnews.com/news/texas-couple-charged-in-alleged-cyberbullying-that-led-to-teens-suicide/> [Accessed 18 Jan. 2022] (2017).
- [23] Chaithanya, B. N., & Brahmananda, S. H. Detecting ransomware attacks distribution through phishing URLs using machine learning. In *Springer eBooks*, 821–832. https://doi.org/10.1007/978-981-16-3728-5_61 (2021).

- [24] Chaurasiya, S. K., Biswas, A., Nayyar, A., Jhanjhi, N. Z., & Banerjee, R. DEICA: A differential evolution-based improved clustering algorithm for IoT-based heterogeneous wireless sensor networks. *International Journal of Communication Systems*, **36**(5). <https://doi.org/10.1002/dac.5420> (2023).
- [25] Chitadze, N. Basic principles of information and cyber security. In *Advances in human and social aspects of technology book series*, 193–223. <https://doi.org/10.4018/978-1-6684-5760-3.ch009> (2023).
- [26] codecnetworks. How to Creating Image & Data Extraction of Digital Device ? < Blogs. [online] Blogs. Available at: <https://www.codecnetworks.com/blog/digital-forensic-tool-encase/> [Accessed 28 Jan. 2022] (2017).
- [27] Connolly, L. Y., & Borrión, H. Reducing ransomware Crime: Analysis of victims' payment decisions. *Computers & Security*, **119**, 102760. <https://doi.org/10.1016/j.cose.2022.102760> (2022).
- [28] Darmawansyah, A., Djunaedi, D., & Kristiawanto, K. Legal protection of cryptocurrency users against cybercrime attacks. *Journal of Social Research*, **2**(7), 2393–2401. <https://doi.org/10.55324/josr.v2i7.1256> (2023).
- [29] Datta, P. Cybersecurity threats: Malware in the code. In *Springer eBooks*, 155–170. https://doi.org/10.1007/978-3-030-96929-5_10 (2022).
- [30] DeLiema, M., Burnes, D., & Langton, L. The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, **5**(4). <https://doi.org/10.1093/geroni/igab043> (2021).
- [31] Elijah, A. V., Abdullah, A., Zaman, N., Supramaniam, M., & Abdullateef, B. N. Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study. *International Journal of Advanced Computer Science and Applications*, **10**(9). <https://doi.org/10.14569/ijacsa.2019.0100969> (2019).
- [32] Garg, R. Digital Evidence Preservation - Digital Forensics. <https://www.geeksforgeeks.org/digital-evidence-preservation-digital-forensics/> (2020).
- [33] Gaur, L., Zaman, N., Bakshi, S., & Gupta, P. Analyzing Consequences of Artificial Intelligence on Jobs using Topic Modeling and Keyword Extraction. In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*. <https://doi.org/10.1109/iciptm54933.2022.9754064> (2022).
- [34] Gaur, L et al. Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. *Human-Centric Computing and Information Sciences*, **11**, NA (2021).
- [35] Gaur, L. et al. Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. *Computers and Electrical Engineering*, **95**, 107374 (2021).

- [36] Gouda, W., Sama, N. U., Al-Waakid, G., Humayun, M., & Jhanjhi, N. Z. Detection of skin cancer based on skin lesion images using deep learning. In *Healthcare* **10**(7), 1183. MDPI (2022).
- [37] Greig, J. 83% of ransomware victims paid ransom: Survey. ZDNet. <https://www.zdnet.com/article/83-of-ransomware-victims-paid-ransom-survey/> (2022).
- [38] Grispos, G. Cybersecurity: Practice. [Link](<https://www.researchgate.net/publication/337011>) (2019).
- [39] Grispos, G. Cybersecurity: Practice. https://www.researchgate.net/publication/337011424_Cybersecurity_Practice (2019).
- [40] Guru99. 15 BEST Computer (Digital) Forensic Tools & Software in 2022. [online] Available at: <https://www.guru99.com/computer-forensics-tools.html> [Accessed 28 Jan. 2022] (2020).
- [41] Haber, M. J., Chappell, B., & Hills, C. Attack vectors. In *Apress eBooks*, 117–219. https://doi.org/10.1007/978-1-4842-8236-6_6 (2022).
- [42] Hamid, B., Jhanjhi, N. Z., Humayun, M., Khan, A., & Alsayat, A. Cyber security issues and challenges for smart cities: A survey. In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) 1-7. IEEE (2019).
- [43] Hassan, C. Bullied teen killed herself in front of family. [online] CNN. Available at: <https://edition.cnn.com/2016/12/14/health/teen-suicide-cyberbullying-continues-trnd/index.html> [Accessed 18 Jan. 2022] (2016).
- [44] Hope, C. What is computer crime? Computer Hope. <https://www.computerhope.com/jargon/c/compcrim.htm> (2023).
- [45] Humayun, M., Niazi, M., Zaman, N., Alshayeb, M., & Mahmood, S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, **45**(4), 3171–3189. <https://doi.org/10.1007/s13369-019-04319-2> (2020).
- [46] Humayun, M., Zaman, N., Hamid, B., & Ahmed, G. Emerging Smart Logistics and Transportation Using IoT and Blockchain. *IEEE Internet of Things Magazine*, **3**(2), 58–62. <https://doi.org/10.1109/iotm.0001.1900097> (2020).
- [47] Humayun, M., Zaman, N., Talib, M. N., Shah, M. H., & Suseendran, G. Cybersecurity for Data Science: Issues, Opportunities, and Challenges. In *Lecture notes in networks and systems*, 435–444. Springer International Publishing. https://doi.org/10.1007/978-981-16-3153-5_46 (2021).
- [48] Hummer, D., & Byrne, J. M. *Handbook on crime and technology*. Edward Elgar Publishing, 2023.

- [49] Hussain, K., Hussain, S. J., Jhanjhi, N. Z., & Humayun, M. SYN flood attack detection based on bayes estimator (SFADBE) for MANET. In 2019 International Conference on Computer and Information Sciences (ICCIS) 1-4. IEEE (2019).
- [50] Ian Cornelius, W. *Cybersecurity using risk management Strategies of U.S. government health organizations - ProQuest*. Pro Quest. <https://www.proquest.com/docview/2479424341?pq-origsite=gscholar&fromopenview=true> (2020).
- [51] Jamal, N., & Zain, J. M. A review on nature, cybercrime and best practices of digital footprints. 2022 *International Conference on Cyber Resilience (ICCR)*. <https://doi.org/10.1109/iccr56254.2022.9995834> (2022).
- [52] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, **1**, 100016. <https://doi.org/10.1016/j.csa.2023.100016> (2023).
- [53] Jayakumar, P., Brohi, S. N., & Zaman, N. Artificial Intelligence and Military Applications: Innovations, Cybersecurity Challenges & Open Research Areas. *Preprint.org*. <https://doi.org/10.20944/preprints202108.0047.v1> (2021).
- [54] Johansen, A. 4 Lasting Effects of Identity Theft. Lifelock.com. <https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft#:~:text=Criminals%20can%20open%20new%20accounts,to%20get%20identity%20theft%20protection> (2021).
- [55] Jhanjhi, N. Z., Almusalli, F. A., Brohi, S. N., & Abdullah, A. Middleware power saving scheme for mobile applications. In 2018 *Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 1-6. IEEE (2018).
- [56] Jung, B. R., Choi, K., & Lee, C. Dynamics of Dark Web Financial Marketplaces: An Exploratory study of underground fraud and scam business. *International Journal of Cybersecurity Intelligence and Cybercrime*. <https://doi.org/10.52306/xmhn2624> (2022).
- [57] KAGAN, J. Identity Theft. [online] Investopedia. Available at: <<https://www.investopedia.com/terms/i/identitytheft.asp#:~:text=Identity%20theft%20is%20the%20crime,making%20unauthorized%20transactions%20or%20purchases.>> [Accessed 24 January 2022] (2021).
- [58] Kara, İ., & Aydos, M. The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems With Applications*, **190**, 116198. <https://doi.org/10.1016/j.eswa.2021.116198> (2022).

- [59] Kaur, M. et al. FANET: Efficient routing in flying ad hoc networks (FANETs) using firefly algorithm. In *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2021*, 483-490. Springer Singapore (2021).
- [60] Keswani, M. Cyber Stalking: A Critical Study. <https://www.investopedia.com/terms/i/identitytheft.asp#:~:text=Identity%20theft%20is%20the%20crime,making%20unauthorized%20transactions%20or%20purchases> (2017).
- [61] Khan, A., Jhanjhi, N. Z., & Humayun, M. The Role of Cybersecurity in Smart Cities. In *Cyber Security Applications for Industry 4.0*, 195-208. Chapman and Hall/CRC (2022).
- [62] Khan, A., Jhanjhi, N. Z., & Sujatha, R. Emerging Industry Revolution IR 4.0 Issues and Challenges. In *Cyber Security Applications for Industry 4.0*, 151-169. Chapman and Hall/CRC (2022).
- [63] Kumar, V., Malik, N., Singla, J., Zaman, N., Amsaad, F., & Razaque, A. Light Weight Authentication Scheme for Smart Home IoT Devices. *Cryptography*, **6**(3), 37. <https://doi.org/10.3390/cryptography6030037> (2022).
- [64] Kumar, T., Pandey, B., Mussavi, S.H.A. & Jhanjhi, N.Z. "CTHS based energy efficient thermal aware image ALU design on FPGA." *Wireless Personal Communications* **85**, 671-696 (2015).
- [65] Learning Center. What is Social Engineering | Attack Techniques & Prevention Methods | Imperva. [online] Available at: <<https://www.imperva.com/learn/application-security/social-engineeringattack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps.>> [Accessed 24 January 2022] (2022).
- [66] Lee, H. Y., Yoon, Y. J., Choi, Y. J., & Ham, Y. Factors Associated with Korean American Women's Health-Related Internet Use: Findings from Andersen's Behavioral Model. *Journal of Immigrant and Minority Health*. <https://doi.org/10.1007/s10903-023-01540-y> (2023).
- [67] Lee, I. Analysis of insider threats in the healthcare industry: A text mining approach. *Information*, **13**(9), 404. <https://doi.org/10.3390/info13090404> (2022).
- [68] Lim, M., Abdullah, A., Jhanjhi, N.Z. & Supramaniam, M. "Hidden link prediction in criminal networks using the deep reinforcement learning technique." *Computers*, **8**(1) (2019).
- [69] Lim, M., Abdullah, A., & Jhanjhi, N. Z. Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. *Journal of King Saud University-Computer and Information Sciences*, **33**(10), 1202-1210 (2021).

- [70] Martellozzo, E., & Jane, E. A. *Cybercrime and its Victims*. <https://doi.org/10.4324/9781315637198> (2017).
- [71] Medium. Ransomware encryption techniques. [online] Available at: <<https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9>> [Accessed 21 January 2022] (2022).
- [72] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, **120**, 102820. <https://doi.org/10.1016/j.cose.2022.102820> (2022).
- [73] Morovati, K. *Detection of Phishing Emails with Email Forensic Analysis and Machine Learning Techniques*. Document - Gale Academic OneFile. <https://go.gale.com/ps/i.do?id=GALE%7CA609412264&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=23050012&p=AONE&sw=w&userGroupName=anon%7E78f224bc&aty=open-web-entry> (2019).
- [74] Muthukkumar, R. et al. A genetic algorithm-based energy-aware multi-hop clustering scheme for heterogeneous wireless sensor networks. *PeerJ Computer Science*, **8**, e1029 (2022).
- [75] Muzammal, S. M., Murugesan, R. K., & Jhanjhi, N. Z. Introducing mobility metrics in trust-based security of routing protocol for internet of things. In *2021 National Computing Colleges Conference (NCCC)*, 1-5. IEEE (2021).
- [76] Nawaz, A. Feature engineering based on hybrid features for malware detection over Android framework. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, **12**(10), 2856-2864 (2021).
- [77] Nasiri, S., Sadoughi, F., Tadayon, M. H., & Dehnad, A. Security Requirements of Internet of Things-Based Healthcare System: a Survey Study. *Acta Informatica Medica : AIM : Journal of the Society for Medical Informatics of Bosnia & Herzegovina : Časopis Društva Za Medicinsku Informatiku BiH*, **27**(4), 253. <https://doi.org/10.5455/aim.2019.27.253-258> (2019).
- [78] Nanglia, S., Ahmad, M., Khan, F.A. & Jhanjhi, N.Z. "An enhanced Predictive heterogeneous ensemble model for breast cancer prediction." *Biomedical Signal Processing and Control* **72**, 103279 (2022).
- [79] Nye, R. DIGITAL FORENSICS REPORT EVIDENCE ANALYSIS IN CASE #90033. [online] Available at: https://www.rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt_by_ryan_nye.pdf [Accessed 19 Jan. 2022] (2017).

- [80] Ocbc.com. OCBC-SMS-PHISHING-SCAMS. [online] Available at: <https://www.ocbc.com/group/media/release/2021/ocbc-sms-phishing-scams> [Accessed 28 Jan. 2022] (2020).
- [81] Palavalli, V. Employee Theft Investigation: a Digital Forensics Case Study. [online] Percipient. Available at: <https://percipient.co/employee-theft-investigation-a-digital-forensics-case-study/> [Accessed 25 January 2022] (2021).
- [82] Ponnusamy, V., Zaman, N., & Humayun, M. Fostering Public-Private Partnership. In *Advances in electronic government, digital divide, and regional development book series*, 237–255. IGI Global. <https://doi.org/10.4018/978-1-7998-1851-9.ch012> (2020).
- [83] Prabakar, D. et al. Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City. *Sustainability*, **15**(7), 6031. <https://doi.org/10.3390/su15076031> (2023).
- [84] Priyadarshini, I. et al. Exploring Internet Meme Activity during COVID-19 Lockdown Using Artificial Intelligence Techniques. *Applied Artificial Intelligence*, **36**(1). <https://doi.org/10.1080/08839514.2021.2014218> (2021).
- [85] Priyanka, S. Digital Forensic Analysis of Ransomware Infected Windows System. *JETIR*, **6**(5), 13. <https://www.jetir.org/papers/JETIR1905197.pdf> (2019).
- [86] R. Sujatha, G. Prakash & Jhanjhi, N.Z. *Cyber Security Applications for Industry 4.0*, Chapman and Hall/CRC Cyber-Physical Systems Series, CRC Press, ISBN 1032066202, 9781032066202, 244 (2022).
- [87] Saeed, S., Almuhaideb, A. M., Kumar, N., Zaman, N., & Zikria, Y. B. (Eds.). *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*. IGI Global. <https://doi.org/10.4018/978-1-6684-5284-4> (2023).
- [88] Saluja, S. Identity theft fraud- major loophole for FinTech industry in India. *Journal of Financial Crime*. <https://doi.org/10.1108/jfc-08-2022-0211> (2022).
- [89] Sennan, S. et al. Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. *Transactions on Emerging Telecommunications Technologies*, **32**(8), e4171 (2021).
- [90] Shah, I. A., Jhanjhi, N. Z., Amsaad, F., & Razaque, A. The Role of Cutting-Edge Technologies in Industry 4.0. In *Cyber Security Applications for Industry 4.0*, 97-109. Chapman and Hall/CRC (2022).

- [91] Shah, I. A., Zaman, N., & Larajib, A. Cybersecurity and Blockchain Usage in Contemporary Business. In *Advances in information security, privacy, and ethics book series*, 49–64. IGI Global. <https://doi.org/10.4018/978-1-6684-5284-4.ch003> (2022).
- [92] Shafiq, M. et al. Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN. *Computers, Materials & Continua*, **67**(3) (2021).
- [93] Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. Machine learning approaches for load balancing in cloud computing services. In *2021 National Computing Colleges Conference (NCCC)* 1-8. IEEE (2021).
- [94] Shalaginov, A., Johnsen, J. W., & Franke, K. Cyber crime investigations in the era of big data. *Conference: 2017 IEEE International Conference on Big Data (Big Data)*. <https://doi.org/10.1109/bigdata.2017.8258362> (2017).
- [95] Sharma, U. et al. eds. *Cyber-Physical Systems: Foundations and Techniques*. John Wiley & Sons, 2022.
- [96] Sheridan, K. Inside the Investigation and Trial of Roman Seleznev. Dark Reading. <https://www.darkreading.com/threat-intelligence/inside-the-investigation-and-trial-of-roman-seleznev> (2017).
- [97] Shukla, P. K., Aljaedi, A., Pareek, P. K., Alharbi, A. R., & Jamal, S. S. AES based white box cryptography in digital signature verification. *Sensors*, **22**(23), 9444. <https://doi.org/10.3390/s22239444> (2022).
- [98] Verma, S. et al. "Intelligent Framework Using IoT-Based WSNs for Wildfire Detection," in *IEEE Access*, **9**, 48185–48196, doi: 10.1109/ACCESS.2021.3060549 (2021).
- [99] Steinmetz, K. F. Y. M. *Cybercrime and society*. Yar, Majid - Steinmetz, Kevin F. - SAGE Publications Ltd - Torrossa. <https://www.torrossa.com/en/resources/an/5017913> (2019).
- [100] Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, **10**, 39325–39343. <https://doi.org/10.1109/access.2022.3162594> (2022).
- [101] Taj, I., & Zaman, N. Towards Industrial Revolution 5.0 and Explainable Artificial Intelligence: Challenges and Opportunities. *International Journal of Computing and Digital Systems*, **12**(1), 285–310. <https://doi.org/10.12785/ijcds/120124> (2022).
- [102] Teichmann, F. Ransomware-Angriffe im Kontext der generativen künstlichen Intelligenz – eine experimentelle Studie. *International Cybersecurity Law Review*. <https://doi.org/10.1365/s43439-023-00094-x> (2023).

[103] TODAY. OCBC phishing scam: “Goodwill payouts” for 30 victims to date, all cases to be “reviewed and validated thoroughly.” [online] Available at: <https://www.todayonline.com/singapore/ocbc-phishing-scam-goodwill-payouts-30-victims-date-all-cases-be-reviewed-and-validated-thoroughly-1792411> [Accessed 28 Jan. 2022] (2022).

[104] Varol, A. and Ülgen Sönmez, Y. Review of Evidence Collection and Protection Phases in Digital Forensics Process. [online] Available at: <https://asafvarol.com/makaleler/SonmezVarol-ISCTURKEY20172.pdf> [Accessed 19 Jan. 2022] (2017).

[105] Yi, P., & Zubiaga, A. Session-based cyberbullying detection in social media: A survey. *Online Social Networks and Media*, 36, 100250. <https://doi.org/10.1016/j.osnem.2023.100250> (2023).

[106] Zainudin, N. M., Zainal, K. H., Hasbullah, N. A., Wahab, N. A., & Ramli, S. A review on cyberbullying in Malaysia from digital forensic perspective. *2016 International Conference on Information and Communication Technology (ICICTM)*. <https://doi.org/10.1109/iciutm.2016.7890808> (2016).