ISSN: 2410-7727

Cybercrime Types and Digital Forensic Tools : review

أنواع الجرائم السيبرانية وأدوات التحري الجنائي الرقمي: مراجعة

Abd AL-latif H. Abo-Torkhoma[1], *,

Gameil S.H. Ali[2],

Amat AL-latif H. Abo-Torkhoma[1],

Mufleh M. Abo-Torkhoma[1],

Mayasa M. Al-hossini[1],

Mohammed M. Al-ahwal[1],

Widad H. Al-wakif[1].

1Department of Information Technology, Sana'a University, Faculty of Education and Applied Sciences- Arhab.

2Medical Information Technology department, Faculty of Medical Technology,21 September University-for Medical and Applied Science, Sana'a, Yemen.

**Corresponding author: abdalaltifhezam2002@gmail.com1*

ISSN: 2410-7727

ISSN: 2410-7727

Cybercrime Types and Digital Forensic Tools : review

Abd AL-latif H. Abo-Torkhoma[1], *, Gameil S.H. Ali[2], Amat AL-latif H. Abo-Torkhoma[1], Mufleh M. Abo-Torkhoma[1], Mayasa M. Al-hossini1, Mohammed M. Al-ahwal[1], Widad H. Al-wakif[1].

1) 1Department of Information Technology, Sana'a University, Faculty of Education and Applied Sciences- Arhab.
2)Medical Information Technology department, Faculty of Medical Technology,21 September University-for Medical and Applied Science, Sana'a, Yemen.
**Corresponding author: abdalaltifhezam2002@gmail.com1*

ABSTRACT

Cyberspace driven by information systems and the internet is transforming our environment in extraordinary ways by enabling economic growth and providing new means by which people connect, interact and collaborate with one other. There is no denying that cyberspace has a good impact on communication, trade, business, and knowledge. Cybercrimes, on the other hand, are a negative aspect of cyberspace that undermines its peaceful use. Cybercrimes encompass any illicit actions carried out through cyberspace and its technological environs. Cybercrimes, in contrast to "traditional" crimes, pose a serious problem because the identity of the perpetrators may be false or concealed in a virtual space. To devise potential methods for the investigation and analysis of cybercrime, the notion of digital forensics was born. In this study, we criticize the notion of cybercrime and discuss its various forms, difficulties in digital forensics, and analytical techniques.

Keywords: digital forensics, tools, cybercrime types.

ISSN: 2410-7727

أنواع الجرائم السيبرانية وأدوات التحري الجنائي الرقمي: مراجعة

عبد اللطيف حزام، جميل حمزة، أمة اللطيف حزام،
مفلح محمد، مياسة محمد، محمد ماجد، وداد حسين.

1) قسم تكنولوجيا المعلومات، جامعة صنعاء، كلية التربية والعلوم التطبيقية. أرحب.
2) قسم تكنولوجيا المعلومات الطبية، كلية التكنولوجيا الطبية
جامعة 21 سبتمبر للعلوم الطبية والتطبيقية، صنعاء اليمن.

ملخص البحث:

يعمل الفضاء الإلكتروني المدفوع بأنظمة المعلومات والإنترنت على تحويل بيئتنا بطرق غير عادية من خلال تمكين النمو الاقتصادي وتوفير وسائل جديدة يتواصل من خلالها الناس ويتفاعلون ويتعاونون مع بعضهم البعض. لا يمكن إنكار أن الفضاء الإلكتروني له تأثير جيد على الاتصالات والتجارة والأعمال والمعرفة. ومن ناحية أخرى، تمثل الجرائم السيبرانية جانبا سلبيا للفضاء السيبراني يقيد استخدامه السلمي. تشمل الجرائم السيبرانية أي أعمال غير مشروعة تتم عبر الفضاء السيبراني وبيئته التكنولوجية. تشكل الجرائم السيبرانية، على النقيض من الجرائم "التقليدية"، مشكلة خطيرة لأن هوية مرتكبيها قد تكون مزيفة أو مخفية في الفضاء الافتراضي. ولابتكار أساليب محتملة للتحقيق في الجرائم الإلكترونية وتحليلها، وُلدت فكرة الطب الشرعي الرقمي. ننتقد في هذه الدراسة مفهوم الجريمة السيبرانية ونناقش أشكالها المختلفة، والصعوبات التي تواجه الطب الشرعي الرقمي، وتقنيات التحليل.

الكلمات المفتاحية: التحري الجنائي الرقمي، الأدوات، أنواع الجرائم الالكترونية.

I. INTRODUCTION

Computers are utilized in nearly every part of daily life, and they have become the standard in today's environment. They can be found in stores, banks, schools, streets, sports, and pockets, among other places. These computers and the internet are essential to modern life because they allow people to conduct daily business, market globally, and communicate with each other. These computer systems include a vast amount of data, including financial and personal data. In the 1980s, the phrase "cyberspace" first originated in the computer industry to refer to the "space of cyber," or more technically, a hypothetical network of computers where communication and

ISSN: 2410-7727

interaction occur [1, 2, 3]. More than half of those surveyed predicted that computer crimes would rise as computer networks expanded [4].

As a result, there has been an increase in computer crimes worldwide. Cybercrimes can happen when someone intentionally damages a computer or system by removing data that has been saved, illicitly extracting data, or even just viewing data. Cybercrime is a phrase that is used by a variety of persons, including computer professionals and legal firms. According to law firms, cybercrimes are any criminal activities involving a network and a computer or device.

Consequently, an investigator for the inquiry procedure becomes necessary the more harm there is. The word "forensic" is defined by the Oxford Dictionary as "relating to or denoting the application of scientific methods to the investigation of crime" in addition to having a legal connotation. The mainstay for resolving cybercrime matters can be thought of as the forensic sciences combined with rational thinking. Since forensic science has been effective in resolving several conventional cases, it can also be applied to computer crimes or cybercrimes. This approach, sometimes called computer forensics or digital forensics, makes use of systems analysis and investigations [5].

II. CYBERCRIME

Any illegal behavior involving a computer, network, or networked device is referred to as cybercrime. Although most cybercriminals steal to get money, some of them actively target computers or other devices to damage or disable them. Others disseminate malware, illicit data, photographs, and other items via computers or networks. Certain cybercrimes combine the two tactics of targeting computers and infecting them with a virus that spreads to other devices and occasionally even entire networks.

Money is one of the main effects of cybercrime. Cybercrime encompasses a wide range of financially motivated illegal activities, such as ransomware attacks, identity theft, email and internet fraud, and efforts to acquire credit card numbers, bank account information, or other payment card details. It is especially crucial to preserve backup data since hackers may target private or company information for theft and selling [6]. The following three categories represent how the U.S. Department of Justice (DOJ) classifies cybercrime [6]:

The U.S. Department of Justice (DOJ) divides cybercrime into the following three categories [6]:

1. Crimes against computing devices, such as those committed to obtaining access to networks.
2. Crimes that employ computers as weapons, such as launching denial-of-service (DoS) attacks.
3. Crimes where a computer is used as a tool for the commission of another crime, such as storing material that was obtained illegally on a computer.

ISSN: 2410-7727

Cybercrime takes many various forms, but most of it is done to benefit the offenders financially. Cybercriminals use a variety of strategies to get paid, but their motivations are always the same. Here are some instances of several attacks of cybercrime:

a. Cyber Extortion

A cyberattack or threat of a cyberattack combined with a demand for money to halt the attack is known as cyber extortion. One kind of cyber extortion is the ransomware assault. After gaining access to a firm's databases, the hacker encrypts all of the valuable documents and information held by the company, making the material inaccessible until a ransom is paid. Usually, this takes the shape of a cryptocurrency, like Bitcoin [7].

b. Crypto-jacking

A type of attack known as "crypto-jacking" involves using scripts to mine cryptocurrency in browsers without the consent of the user. The victim's PC may be infected with Bitcoin mining software as part of a crypto-jacking attack. However, many assaults rely on JavaScript code that, if the user has a tab or window open on the malicious website, does in-browser mining. Since the in-browser mining code is run when the impacted website loads, there is no need to install malware[22].

All crypto jacking works the same way in principle. Cryptomining malware runs stealthily in the background, hijacking the victim’s central processing unit (CPU) and graphics processing unit (GPU) to “mine” fresh bits of cryptocurrency by solving complex math problems that verify crypto transactions. Every time a piece of cryptocurrency is “minted,” it’s sent to the attacker’s crypto-wallet. Cryptomining malware is specifically designed to exploit a target’s computer resources, often through a browser or JavaScript. After getting infected with cryptominer malware through a link or other malicious source, the cryptojacking code embeds itself in your machine. The mining malware then runs a script to take control of your computer and start mining cryptocurrency [11]. Fig.1 shows how cryptojacking works.

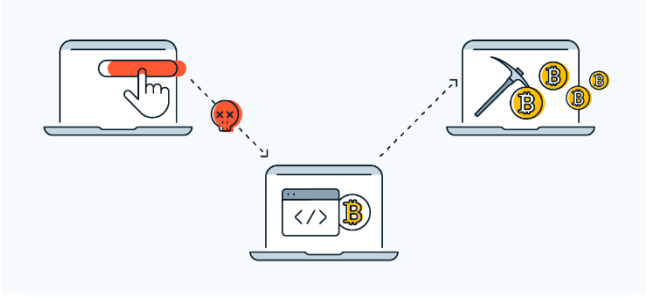

Fig1. Cryptojacking makes unauthorized use of third-party devices to mine cryptocurrency.

ISSN: 2410-7727

c. Identity theft

Identity theft is an attack where a hacker obtains access to a computer system to collect a victim's personal information. This information is then used to either steal the victim's identity or gain access to their credit card and bank accounts, among other valuable accounts. Cybercriminals purchase and trade identity information on dark net markets, including bank accounts and other account types including webmail, streaming video and music, online auctions, and more. Fig2. Illustrates an example of identity theft.

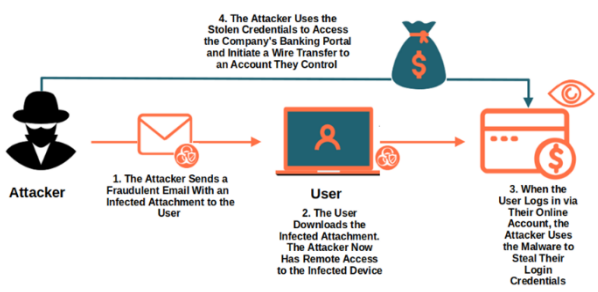

Fig2. An example of identity theft

d. Identity hackers

Information about a person's health is occasionally the target of identity thieves. The act of hackers breaking into a retailer's networks to take advantage of their customers' credit card numbers and/or banking information is known as credit card fraud. Stolen payment cards can be bought and sold in large quantities on dark web markets, with hacking organizations making money from sales to less experienced online thieves who take advantage of credit card fraud against individual accounts.

e. Cyberespionage

The act of a cybercriminal breaking into a government's or another organization's systems or networks to obtain sensitive data is known as cyberespionage. An attack may be motivated by philosophy or benefit. Any type of cyberattack to gather, change, or destroy data is considered cyber espionage. Other activities include using network-connected devices, like webcams or Closed-Circuit Television (CCTV) cameras, to spy on a specific individual or group and keeping an eye on communications via emails, texts, and instant messages [6].

ISSN: 2410-7727

In Fig3, the information collection phase includes the collection of search history, browser history, social media groups, and shared data after determining the target [6].

1. Detection: The exploration phase includes the examination of the target system infrastructure, the ports used, the active services, and the data-base used.
2. Vulnerability Scan: The vulnerability screening phase includes the determination of the hobbies and interests of the senior managers or authorized individuals working at the target.
3. Make Use of Vulnerability: Exploiting vulnerabilities is the process of infiltration through potential system vulnerabilities. It is defined as the ability to spoof (design fake e-mails and install malware through e-mail attachments) by utilizing the hobbies and interests or carelessness of the targeted individuals.
4. Goal Directed Activity: The goal-driven activities are defined as the attacker's communication with the system using remote access after in filtrating the target system.
5. Data Collection: The activities to collect information, documents, or other detected files are carried in this process by the attackers.
6. Delete Trackers: The removal of traces involves the process of not being caught after infiltrating the target system (e.g., closing antivirus pro-grams, deleting system logs, etc.).

f. Software piracy

The unauthorized duplication, transfer, and use of software for business or private benefit is known as software piracy. Intellectual property violations, copyright violations, and trademark infringements are frequently linked to this type of cybercrime.

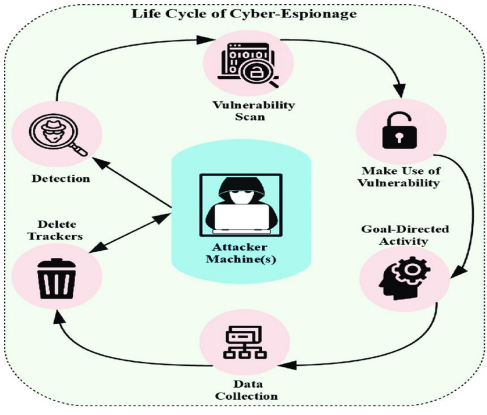

Fig3. Life cycle of cyber-Espionage

ISSN: 2410-7727

III. TYPES OF CYBERCRIME

In this section, the different types of cybercrimes with their explanations and some known cases of them are explained [22].

Table 1. Types of Cybercrime

Type of Cybercrime	Explanation	Known Case
Unauthorized Access	gaining access to data or information that they are not permitted to view or obtain It is.[1]	ignorant cybercrime, committed by anyone from professional hackers to university students.[5]
Identity Theft	someone who is performing or claiming to be someone else.[1]	Identity theft affects a lot of social networks, including Facebook and Twitter.
Denial of Service (DoS)	Sending too many requests at once overloads a computer system and prevents it from fulfilling regular requests.[5]	DoS affects large companies. Hackers typically demand money or a ransom.[1]
Phishing	attracting or seducing people to obtain their financial or personal information, then exploiting them. Some hackers refer to this as social engineering, though. [5]	The purpose of the cloned LinkedIn website was to steal user credentials.
Fraud	modifying or manipulating another person's financial information to gain an advantage.[5]	It's a form of deceit. Workers at an Indian bank connected to Citibank in New York were detained on suspicion of embezzling thousands of dollars.
Cyber Terrorism	Social media and the internet are used by terrorist organizations as a	The terrorist from Christchurch utilized Facebook to publicize his

ISSN: 2410-7727

	platform to propagate anti-government ideologies and terrorist agendas.	atrocity after using the internet to send a message to the prime minister's office.
Intellectual Property Theft	It can be defined as the stealing of any property or material that is copyrighted.	Yahoo filed a case in an Indian court against Akash Arora for using 'yahooindia.com' as a domain name that resembles the website 'yahoo.com'
Spoofing	A person takes up another person's identity to penetrate the system or to shift the blame onto that person.	Scam can be near to this. An Indian executive pretended as a girl and cheated a UAE man through the internet.
Malware	Like viruses, worms, Trojans, and spyware. They capture critical information like IDs, passwords, usernames, and keystrokes. etc.	There are a ton of malware and malicious apps on the internet.
Spamming	sending unsolicited emails to many email addresses. Numerous might be produced automatically.	These spasms affect everyone on the internet. The hardest affected are businesses.

IV.DIGITAL FORENSIC

A subfield of forensic science called "digital forensic science" is dedicated to the recovery and analysis of data from digital devices used in cybercrime. The phrase "computer forensics" was superseded by the term "digital forensics."

It now includes looking at any gadget that can store digital data. Although the Florida Computer Act was passed the following year and the first computer crime was recognized in 1978, it wasn't until the 1990s that the term "computer crime" gained widespread recognition. Digital forensics policies around the world did not change until the early 21st century [8].

ISSN: 2410-7727

V. CHALLENGES FOR DIGITAL FORENSICS

Digital forensics has six primary obstacles, which are as follows:

a. High speed and volumes

The availability and commercialization of digital information have made gathering, storing, and processing large amounts of data for forensic reasons more difficult than it was ten years ago.

b. An explosion of intricacy

Evidence is now dispersed among several real and virtual spaces, such as cloud services, online social networks, and network-attached storage devices, rather than being confined to a single host. Consequently, more knowledge, resources, and time are required to accurately and fully replicate the evidence. Partial automation of some tasks has drawn criticism from the digital investigation group, which claims that it might quickly reduce the inquiry's effectiveness.

c. Development of standards

It is further stated that the investigation of cutting-edge cybercrime can necessitate collaborative data processing or the use of outsourced storage and computation. Therefore, developing appropriate standard formats and abstractions would be crucial for the field of digital forensics.

d. Privacy-preserving investigations

These days, a lot of people share various aspects of their lives online, mostly on social media pages or online social networks. Sadly, collecting data to identify and replicate an attack will compromise users' privacy and is linked to further problems when utilizing cloud storage.

e. Legitimacy

Validity with some functions being delegated to outside parties or complexity shifting at the border (as in fog computing) (as in platform-as-a-service frameworks), modern infrastructures become more virtualized and sophisticated.

f. Rise of anti-forensic techniques

The complexity of modern infrastructures is increasing due to virtualization, with some services being delegated to outside parties or complexity shifting at the border (like in fog computing) (like in platform-as-a-service frameworks).

VI. DIGITAL FORENSICS TOOLS

This section explains various digital forensics packages or programs that are commonly used in forensic investigations.

ISSN: 2410-7727

1. Computer Forensics tools

Computer forensics means the use of investigation and analytical techniques to collect evidence from a specific computing device and store it in order to present this evidence in a courtroom. The purpose of computer forensics is to conduct a systematic investigation and maintain a recorded chain of evidence in order to determine exactly what occurred on a computing device and who was accountable for it.

The tools are often used to recover lost data, break passwords, Decryption, analyze the registry entries, and build physical file data types. We summarized the computer forensic tools in Table 2, which lists the advantages, and disadvantages for each tool.

Table 2. computer forensic tools

Tools	Advantages	Disadvantages
EnCase	Authenticate Identifying threats friendly GUI Disk imaging Data and password recovery Decryption Data carving Protocol support like HTTP/POP Memory acquisition [9] Hash databases Remote data collection and processing [9]	Paid software Static analysis Can't detect timestamp forgery attack [12]
FTK Forensic toolkit	Detect missing data [9] Support multi languages [9] Search data [9] Friendly GUI Decryption [9] Memory dump analyze [10] Password recovery [10]	Don't support protocol such as HTTP/POP [11] Can't give report [13] Support only window

ISSN: 2410-7727

	Data recovery [10] Hash databases Email analyze [9]	
DFF	Open source Carry out data carving. Conduct memory dump analysis. Support data recovery. Perform disk imaging. Provide real-time alerts. Perform static and live analysis conduct decryption.	Don’t conduct password recovery Don’t conduct email analysis No incident response

2. Mobile forensic tools

Specialized technologies are available to assist investigators in retrieving deleted information, analyzing, and preserving evidence that may emerge during an investigation of illegal activities. These applications are utilized by a wider range of groups than only investigators. These tools may be beneficial to the common individual for their personal purposes and forensic analysis. [17]

Mobile forensic tools aid in the unlocking and extraction of data from a phone, whether it be an Android or an iPhone. These mobile forensics tools allow you to access critical

information saved on a variety of cell phones. Call records, chats, text messages, documents, graphics, photographs, emails, app data, and other information can be obtained from a suspect's Smartphone.

We summarized the mobile forensic tools in Table 3, which lists the advantages, and disadvantages for each tool.

ISSN: 2410-7727

Table 3. Mobile forensic tools

Tools	Advantages	Disadvantages
Oxygen Forensic [11]	Disable Screen Lock Breaking passwords and pins Application data Give GPS data Cloud data Support GUI Detect Malware Backup and image import [14]	Paid software Need full course training. [10].
Mobile Edit [21] [10]	Phone extractor, data analyzer Report generator GUI Deleted data recovery Live update Password and PIN breaker Cloud support	Not free Not authenticate
Andriller	Breaking screen lock patterns, PINs, and Passwords. Decrypting encrypted databases and files. Automatically extracting data from encrypted database. Unpacking of android backups.[15]	Not free tool. Python needs. [10]
XRY	High quality fast and secure extraction data Quick logical and physical file extracting Evidence safe and reliable at all times Support GUI [16]	Not free tool

ISSN: 2410-7727

3. Network Forensic tools

Network Forensics refers to a subtype of digital forensics. It encompasses the analysis and inspection of every traffic that traverses a network or network system. Network forensics is crucial to the incident handling and post-event investigative processes of an organization [18]. Numerous network forensic tools are commercially available along with open-source tools.

These tools were not developed for just any particular organization. While selecting tools from an organizational and investigator perspective, there are some criteria, critical factors, and goals to consider. We summarized the network forensic tools in Table 4, which lists the advantages, and disadvantages for each tool.

Table 4. Network forensic tools

Tools	Advantages	Disadvantages
Wireshark [19]	The best sniffer-developed tools as freeware capture network traffic and analysis. It support most of the operating systems. It has several filters and customization options. Life capture and offline analysis. Support VoIP analysis.	Can't support log management[11]
Nmap [20] [10]	Graphical (GUI) Free tool Portable Detect packet spoofing, Detect open port Intrusion detection system (IDS)[21]	A DOS or network slowdown is triggered when weak devices are scanned[10]
Xplico [22][11]	Support protocols HTTP/SIP/UDP/POP[22] Intrusion detection[11] Network security monitoring [11] Offline analysis [11] GUI[11] Support IPV4 and IPV6 [11] FTP and web login extraction [11]	Can't display filters[11]

ISSN: 2410-7727

	Output data and information in SQLite Database or MySQL database and/or files[22]	

VII. CONCLUSION

In conclusion, our study reflects the importance of confronting the challenges posed by the world of cybercrime, from understanding its different types to developing effective tools for digital forensics. It is clear that cybercrime represents a major threat to cyber safety, as perpetrators can have hidden or fake identities in virtual space, making it difficult to track them and hold them accountable. In this paper, we reviewed the various forms of cybercrime and the importance of digital forensics in confronting them. We also highlighted the tools and techniques used in digital forensics and the challenges they face. Progress in this area remains essential to ensure the security and safety of cyberspace, and to enhance the ability of authorities to effectively confront digital crimes.

ISSN: 2410-7727

References

[1] Thomas J. Hol, Adam M. Bossler, t, Kathryn C. Seigfried-Spellar (2017)"Cybercrime and Digital Forensics: An Introduction". Routledge; Second Edition

[2] Casey, E.: Digital Evidence and Computer Crime, 2nd Edition, Elsevier Academic Press, 2004.

[3] Kshetri, N.(2010) The Global Cybercrime Industry. Berlin, Heidelberg: Springer Berlin Heidelberg.

[4] Harbawi, M, Varol, A. "The role of digital forensics in combating cybercrimes." Digital Forensic and Security (ISDFS), 2016 4th International Symposium on. IEEE, 2016.

[5] Thomas J. Hol, Adam M. Bossler, t, Kathryn C. Seigfried-Spellar (2017)"Cybercrime and Digital Forensics: An Introduction". Routledge; Second Edition.

[6] Ilker Kara, (2021) "Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study" DOI:10.1080/08874417.2021.2004566

[7] Tanimoto, S., Kakuta, T., Sato, H. and Kanai, A., 2015. A Study of Cost Structure Visualization for Digital Forensics Deployment. 2015 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence.

[8] G. Pangalos, C. Ilioudis and I. Pagkalos, 2010. The importance of Corporate Forensic Readiness in the information security framework. IEEE.

[9] Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017, September). A study on digital forensic tools. 2017 IEEE

International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI).

[10] Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and edge computing-based computer forensics: Challenges and open problems. In Electronics (Switzerland) (Vol. 10, Issue 11). MDPI AG.

[11] andhi, I., Narwal, B., & Goel, N. (n.d.).2020, A Walkthrough of Digital Forensics and its tools.

ISSN: 2410-7727

[12] Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations? Science & Justice, 61(2).

[13] L. Carvajal, C. Varol, and L. Chen, "Tools for collecting volatile data: A survey study," 2013 Int. Conf. Technol. Adv. Electr. Electron. Comput. Eng. TAEECE 2013, no. May 2019, pp. 318–322, 2013, doi: 10.1109/TAEECE.2013.6557293

[14] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," Int.J.Adv. Comput. Sci. Appl., vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.

[15] Arista Yuliani, V., & Riadi, I. (2019). Forensic Analysis WhatsApp Mobile Application on Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework. International Journal of Cyber-Security and Digital Forensics, 8(3), 223–231.

[16] Ferreira, S., Antunes, M., & Correia, M. E. (2021). Exposing Manipulated Photos and Videos in Digital Forensics Analysis. Journal of Imaging, 7(7), 102.

[17] Best Mobile Forensic Tools For iPhone & Android: 2021 Reviews - Cybericus", Cybericus, 2022. [Online].

[18] Sachdeva, S., Raina, B. L., & Sharma, A. (2020). Analysis of Digital Forensic Tools. Journal of Computational and Theoretical Nanoscience, 17(6), 2459–2467.

[19] "Download," Wireshark · Go Deep. Available: https://www.wireshark.org/. [Accessed: 20-Dec-2021].

[20] Nmap. Available: https://nmap.org/ . [Accessed: 21-May-2024].

[21] S. Liao et al., "A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments," 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2020, pp. 64-71, doi 10.1109/CyberC49757.2020.00020.

[22] Saad Subair, Derar Yosif, Abdelgader Ahmed, and Christopher Thron(2022)" Cyber Crime and Digital Forensics: A Pragmatic Framework for Sudanese Courts".