IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

Role of Digital Forensics in Combating Financial Crimes in the Computer Era

Ms. Juwariya Dalvi[1], Dr. Sachin Bhosale[2], Mrs. Pooja Devrukhkar[3]
Student, M.Sc.IT.[1]
Assistant Professor, Department of I.T[2,3]
I.C.S. College, Khed, Ratnagiri

Abstract: *Within the computer time, monetary violations have advanced in complexity and scope, requiring progressed techniques to examine and combat unlawful exercises. Computerized forensics plays a pivotal part in this scene by giving investigative techniques and devices to gather, analyze, and protect electronic prove related to budgetary violations. This paper investigates the multifaceted role of advanced forensics in tending to money related wrongdoings within the computer era.*

The integration of computerized innovations into budgetary frameworks has made unused openings for hoodlums, extending from advanced cyber-attacks to conventional extortion encouraged by advanced means. Digital forensics, as a teach, has developed as a crucial component within the battle against monetary violations. This paper analyzes the particular ways in which advanced forensics contributes to combating money related violations, including both proactive and responsive measures.

Proactively, computerized forensics includes the improvement of strong cybersecurity measures, chance evaluations, and proactive monitoring frameworks to identify and anticipate potential monetary violations. Reactively, it plays a urgent role within the consequence of an occurrence by conducting careful examinations, collecting electronic evidence, and supporting within the distinguishing proof and indictment of perpetrators.

The paper dives into the challenges confronted by computerized forensics experts within the energetic scene of monetary violations, counting issues related to security, encryption, and jurisdictional complexities. Besides, it investigates the advancing nature of budgetary violations, such as cryptocurrency-related offenses, and the adjustment of advanced forensics strategies to address these developing challenges.

Through case considers and real-world illustrations, this paper outlines the effectiveness of advanced forensics in revealing money related extortion, cash washing, and other illegal exercises. It highlights the intrigue nature of combating money related wrongdoings, emphasizing collaboration between law authorization, budgetary teach, and computerized forensics specialists.

Keywords: digital forensics, combating financial crimes, computer era.

I. INTRODUCTION

Within the early days of computerized forensics, intrigued and exertion were centered on tending to stand-alone and arrange individual computers. As innovation has created, the center has expanded to incorporate recouping prove from any gadget with a advanced processor or capacity capability. As a result, computerized forensics has moved from examining computer-based wrongdoings such as hacking to investigating all sorts of cybercrimes, counting money related violations (Mugisha, 2019). Advanced forensics, measurable computing, and computer forensics are all words that are some of the time utilized traded (Schatz, 2007). Computer forensics and legal computing initially alluded to the utilization of computer-related prove in legitimate procedures. Computerized forensics and computerized examinations are broadly utilized to accumulate, look at, analyze, and display computerized prove in court (Hewling, 2013). Cyber/computer violations have gotten to be predominant in today's innovatively driven culture. With the progressing rise within the utilize and accessibility of advanced gadgets and the digitization of previously-stored analog information, advanced prove in court cases is getting to be progressively critical. Advanced prove varies from past

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

prove given in court since it shows blemishes such as being effectively modified, despicably displayed, and a common need of nature with this sort of prove.

Without a question, the final few decades are speaking to a breakthrough in Data Communication Innovation (ICT). The rise of the Web or the internet as an awfully viable communication medium has brought endless benefits. Most of our exercises have moved from the physical world to the virtual world, where the internet is the catchphrase. For illustration, until the mid-1990s, the keeping money division in most parts of the world was straightforward and dependable. Be that as it may, since the advancement of data innovation, the managing an account industry has experienced a worldview move (Jaleshgari, 1999). Banks built up various stages to extend their client base by permitting exchanges to be completed without much exertion (Vrancianu and Popa, 2010). It is realized in down to earth frameworks such as e-commerce, e-learning, e-banking, etc., which have massively encouraged and speeded up most exchanges. The remaining segments of the study are separated into five areas: Advanced Forensics in the Setting of Cybercrime; Advanced Scientific Examination; Cybercrime, Globalization, and Worldwide Financial Development; The Fundamentals of Advanced Forensics Examination; and Cybercrime Examinations and Computerized Forensics.

II. DIGITAL FORENSICS IN THE CONTEXT OF CYBERCRIME

Advanced Forensics is the department that bargains with the wrongdoings which happen over computers. Where a single computer framework constitutes a whole wrongdoing scene the slightest, it may contain a few prove or information that can be valuable within the examination. Be that as it may, in specialized terms, it can be characterized as the distinguishing proof, procurement, conservation, investigation, and documentation of any advanced prove (Rana et al., 2017). Computerized forensics collects prove from any computing gadget and explores, analyzes, and jam it as legitimately allowable prove in a court of law. Cybercrimes, too known as e-crimes, hi-tech violations, or electronic violations, are operations performed by an person who has a few or seriously information of the computer and its entire framework to extricate and erase the put away information illicitly. It is portrayed as a wrongdoing done on the Web, through the Web, or the utilize of the Web. Phishing, credit card fakes, bank thefts, unlawful downloading, mechanical surveillance, child explicit entertainment, capturing children through chat rooms, tricks, cyber-terrorism, the generation and spread of infections, and so on are all illustrations of computer wrongdoing (Mugisha, 2019). Cybercrimes allude to illicit, unscrupulous, and unauthorized behavior in a framework that forms data or exchanges information utilizing computer and communication innovations (Okutan and Cebi 2019). Cybercrime is additionally characterized as illegal or unsatisfactory acts committed utilizing electronic devices, counting computers, as a target or a instrument (Vadza 2011). These wrongdoings incorporate washing, burglary, fraud, hacking, fraud, and criticism (Awoyemi et al., 2021).

III. DIGITAL FORENSIC INVESTIGATION

Within the computer time, monetary violations have advanced in complexity and scope, requiring progressed techniques to examine and combat unlawful exercises. Computerized forensics plays a pivotal part in this scene by giving investigative techniques and devices to gather, analyze, and protect electronic prove related to budgetary violations. This paper investigates the multifaceted role of advanced forensics in tending to money related wrongdoings within the computer era.

The integration of computerized innovations into budgetary frameworks has made unused openings for hoodlums, extending from advanced cyber-attacks to conventional extortion encouraged by advanced means. Digital forensics, as a teach, has developed as a crucial component within the battle against monetary violations. This paper analyzes the particular ways in which advanced forensics contributes to combating money related violations, including both proactive and responsive measures.

Proactively, computerized forensics includes the improvement of strong cybersecurity measures, chance evaluations, and proactive monitoring frameworks to identify and anticipate potential monetary violations. Reactively, it plays a urgent role within the consequence of an occurrence by conducting careful examinations, collecting electronic evidence, and supporting within the distinguishing proof and indictment of perpetrators.

The paper dives into the challenges confronted by computerized forensics experts within the energetic scene of monetary violations, counting issues related to security, encryption, and jurisdictional complexities. Besides, it

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

investigates the advancing nature of budgetary violations, such as cryptocurrency-related offenses, and the adjustment of advanced forensics strategies to address these developing challenges.

Through case considers and real-world illustrations, this paper outlines the effectiveness of advanced forensics in revealing money related extortion, cash washing, and other illegal exercises. It highlights the intrigue nature of combating money related wrongdoings, emphasizing collaboration between law authorization, budgetary teach, and computerized forensics specialists.

IV. CYBERCRIME, GLOBALIZATION, AND GLOBAL ECONOMIC GROWTH

Globalization alludes to worldwide change or internationalization interlinked with the socio-economic, innovative, political, and social viewpoints through diverse stream mediums, counting individuals, sharing of information and data, rural-urban movement, and online exchanging of merchandise and administrations (Awoyemi et al., 2021). It includes the integration of distinctive social orders, social hones, economies, innovative advancements, and organization administration, driving to complex shared interrelatedness. Due to globalization, people, organizations, social orders, and governments from other nations communicate, collaborate, and coordinated. Globalization has helped advance in numerous ways in several parts of the world. It has encouraged get to to instruction, transportation, communication, wellbeing offices, importation and exportation, work openings, government income, and a tall standard of living for the individuals over the a long time. Exchange and innovation are two other segments of society that have been considerably affected by globalization. Data innovation progressions give modern procedures for taking an interest in around the world financial exercises by encouraging the movement of properties, assets, and cash and collaboration with far-flung accomplices. Be that as it may, cybercrime contains a noteworthy negative affect on society related with innovation.

V. THE TENETS OF DIGITAL FORENSICS INVESTIGATION

Courts utilize it broadly to help judges and attendants in criminal and respectful things. Any computerized information that builds up criminal behavior or offers a connect between an denounced and a casualty or an blamed and a wrongdoing is characterized as computerized prove. Prove alludes to thing/s that offer assistance frame a conclusion or judgment (Hewling, 2014). The computerized forensics examination handle includes recognizable proof, securing, conservation, examination and examination, and introduction (Harbawi and Varol, 2016).

5.1. Identification of the Digital Evidence

The first step involves the identification of any digital evidence which might be present at the crime scene. Evidence can include computers, pen drives, hard disks, or any electronic device to store digital data (Rana et al., 2017). and storage devices such as hard disks, pen drives, compact discs, digital video discs, and other peripheral devices capable of storing digital data.

5.2. Acquisition

The procurement comes after the recognizable proof step. Once the prove is recognized, it must be obtained within the most suitable way where the judgment of the prove remains intaglio. The sub-steps to take after amid the securing of the examination can be seizing the crime scene and forensically securing the information put away within the found gadgets for encourage examination. The two sources of prove: unstable and non-volatile information have distinctive securing strategies. Once the things or information of intrigued have been recognized, advanced securing starts.

5.3. Preservation

The acquired evidence should be kept the way it was acquired in the first place. Keeping digital evidence is done via a well-formulated chain of custody to preserve the evidence from intended and unintended alteration to its contents. Read-only copies of acquired evidence should also be precautionary during the forensic acquisition.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

5.4.Examining and Analyzing

Evidence examining is done to categorize the digital evidence and the tools used to analyze it. For instance, evidence extracted from an email contains different data and metadata than data extracted from an image. Once the evidence has been examined, the analysis step starts by identifying the methods, tools, and skills needed for extracting vital information that can be used in a court of law. This step is essential and relies much on the forensic examiner's experience and skills.

5.5. Presentation

The ultimate step within the computerized measurable examination handle is when the inspector ought to give a report, and documentation, on how the scientific handle was done, what sort of instruments and strategies were utilized, lawful conventions and approaches taken after forensics discoveries, and important enunciations. The report ought to be composed in an justifiable and express dialect, reliable with the conclusions, and precise in its introduction.

VI. TYPES OF CYBERCRIME

Cybercrimes may be against individuals, property, government, or organizations. Cybercrime against individuals includes cyber pornography, in particular, child pornography, invasion of privacy, cyberbullying or harassment of individuals via email spoofing, stalking, hacking, credit card frauds, password sniffing, and defamation.

Illegal Data Acquisition (Data Espionage)

Computer systems frequently contain sensitive information. Offenders can try to obtain this information from practically anywhere globally if the computer system is connected to the Internet. Trade secrets are increasingly being obtained via the Internet. Data espionage is appealing because of the worth of sensitive information and the ability to access it remotely. One example is "phishing," which has lately emerged as a significant cybercrime and describes attempts to get sensitive information (such as passwords) by impersonating a trustworthy person or organization (such as a financial institution) in an official electronic contact. For instance, the Internet, online banking, and e-payments have exposed end users to online crimes (Lavorgna and Sergi, 2014; Oruç and Tatar, 2017).

6.1.System Interference

Attacks on computer systems are subject to the same problems as attacks on computer data. More companies are implementing Internet services into their manufacturing processes, owing to the advantages of 24-hour availability and global accessibility

6.2.Computer Worms

Worms on computers are a type of malware (like computer viruses). They self-replicate computer programs that cause network disruption by launching multiple data-transfer processes. They can impact computer systems by interfering with their smooth operation, utilizing system resources to duplicate themselves via the Internet, or generating network traffic that can cause some services to become unavailable (such as websites). Denial of service attacks target individual computer systems, but computer worms often affect the entire network without affecting specific computer systems.

6.3.Denial of Service Attack

Denial of service attack prevents users from accessing computer resources. Offenders can restrict people from accessing a computer system, checking emails, reading the news, booking a trip, or downloading files by flooding it with more demands than the computer system can handle. Several denials of service assaults were attempted against well-known companies such as CNN, eBay, and Amazon in 2000. Similar assaults on government and commercial websites in the United States of America and South Korea were reported in 2009.

As a result, certain services were unavailable for several hours, if not days.

6.4.The Use of Virtual Currencies

The need for anonymous payment systems has led to virtual payment systems and virtual currencies allowing anonymous transactions. Virtual currencies may not require identification or authentication, making it difficult for law

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

enforcement to track money flows back to criminals. When criminals make anonymous payments, it is tough to follow them.

6.5.Copyright - Related Offences

The distribution of information is one of the essential tasks of the Internet. Companies utilize the Internet to disseminate product and service information. Successful organizations may encounter piracy issues on the Internet analogous to those faced by brick and mortar businesses. Counterfeiters may exploit brand image and corporate design to promote counterfeit products by replicating logos and products and attempting to register the domain associated with that company. Copyright breaches may be a legal issue for companies that distribute products directly over the Internet. Their products are available for download, copying, and distribution.

6.6.Trademark - Related Offences

Copyright breaches are related to trademark violations, a prominent part of global trade. Trademark violations have become online, with differing degrees of illegality under various national penal codes. Trademarks in criminal operations to mislead users and domain namerelated offenses are the most severe offenses. A company's positive reputation is frequently tied to its trademarks. Domain-related offenses such as cybersquatting, which is the illegal process of registering a domain name identical or similar to a product or company trademark, are another issue related to trademark violations. Most of the time, offenders want to sell the domain to a corporation for a high price or use it to sell items or services that deceive people by claiming to be associated with the trademark.

6.7.Identity Theft

There are three phases to the crime of identity theft. The perpetrator acquires identity related information in the first phase. Interaction with identity-related information occurs in the second phase before the information is used in criminal offenses. The third phase is the use of identity-related details about a criminal offense. As a result, the culprits are more concerned with the capacity to exploit the data in illicit activities than with the data itself. Falsification of identification documents or credit card fraud are examples of similar crimes. Finally, the criminals can utilize social engineering to encourage the victim to reveal personal information. Recently, scammers have developed sophisticated social engineering tactics to manipulate consumers and steal confidential information (such as bank account information and credit card data).

The sort of information that the perpetrators want varies. Social security and passport numbers, date of birth, address and phone numbers, and passwords are the most critical pieces of information. Financial account information, including social security numbers, is a favorite target for identity thieves.

6.8. Cyber Laundering

Money laundering is changing thanks to the Internet. Traditional money-laundering strategies still have advantages for larger quantities, but the Internet has significant benefits. Online banking services allow you to complete several international financial transactions swiftly. The Internet has assisted in the reduction of reliance on physical monetary transactions. Wire transfers replaced the transportation of hard cash as the first step in reducing physical dependence on money, but tighter rules to detect suspicious wire transfers have driven criminals to invent other methods. In the fight against money laundering, detecting suspicious transactions is based on the obligations of the financial institutions participating in the transfer. Money laundering can be broken into placement, layering, and integration.

6.9. Cyber-Attacks Targeted at Financial Institutions

Cyber risk is defined as "operational risks to information and technology assets that have implications for information or information systems' confidentiality, availability, or integrity" Cyber-attacks can harm businesses by compromising the three primary pillars of data security: confidentiality, integrity, and availability. Confidentiality difficulties arise when private information within a company is leaked to third parties, such as data breaches. Integrity issues, including fraud, are related to the misuse of systems. The three cyber-attack forms directly affect the targets. Firms cannot operate due to business disruptions, resulting in revenue loss.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

While the long-term consequences of data breaches, including reputational damage and litigation costs, take longer to manifest. Because financial institutions rely on their customers' trust, the risk of losing confidence due to cyber-attacks could be substantial. Business disruptions are most likely to have direct short-term contagion effects on the financial system than fraud or data breaches, affecting only the targeted firm in the short-term (Bouveret, 2018).

VII. COUNTRIES WITH HIGH CYBER RISK EXPOSURE

Cyber risk is a significant threat to the financial sector in all countries. The International Telecommunication Union (ITU), a United Nations institution, publishes a global cybersecurity index. The cybersecurity index considers various aspects, such as legal, technological, and organizational structures and capacity building and cooperation (ITU, 2017). For the time being, the cost of cybercrime is around 0.8 percent of global GDP or $600 billion, according to research by McAfee and the Center for Strategic and International Studies
(CSIS).

VIII. CYBERCRIME INVESTIGATIONS AND DIGITAL FORENSICS

Through the recognizable proof of computer-based and computer-assisted wrongdoing, advanced forensics has gotten to be an fundamental instrument within the fight against cybercrime. Security pros and law requirement organizations exploring cybercrime confront critical obstacles due to today's gigantic sums of information, shifted data, and communication innovations, and borderless cyberinfrastructures. Exploring cybercrime can happen over national borders, purviews, and lawful frameworks.

This issue, combined with the endless sum and assortment of information, amazingly heterogeneous data and communication innovations, and complex current hardware/software systems, make critical deterrents, especially in computerized forensics (Caviglione et al., 2017). Advanced scientific examinations are broadly utilized by law requirement to analyze electronic media, and businesses are progressively utilizing them as portion of their occurrence reaction strategies (Al Fahdi et al., 2013). Verifiably, as it were a minor rate of casualties and examiners have been influenced by e-crime or computer-related crime. In any case, this is often changing, and computerized prove in formal examinations is getting to be commonplace. Electronic prove will without a doubt be seized, protected, and inspected in any open or private investigation. As a result, advanced prove handling must be coordinates into the complete examination.

IX. CONCLUSION

In spite of the fact that wrongdoing has continuously existed in human civilization, the strategies by which it is committed are ceaselessly advancing and extending. Offenders advantage from the changing nature of innovation by having modern implies and instruments to commit wrongdoings. Already, criminal examinations depended on physical prove, the examination of the wrongdoing scene, the addressing and recording of witnesses, and the addressing and recording of suspects. Today's criminal agents must acknowledge the plausibility that the prove they must look at is electronic or computerized (Macdermott et al., 2018). Not at all like the ordinary 'physical' scene, the wrongdoing scene may comprise of a computer framework, cleverly and small-scale advanced gadgets, or organize traffic/logs. Computer-generated log records, metadata, or surfing history may be utilized as "witnesses" in these circumstances. Fingerprints can be utilized to appear who was using a specific weapon, but how can we know who was at the console when the wrongdoing was committed? In this field, legal phonetics is progressively being utilized to help examinations by distinguishing members inside a discussion, deciding thought processes and behaviors, and making a timeline of events. Cybercrime is on the rise due to innovative headways and our developing network to the Web and gadgets in our day by day lives. These headways, combined with the namelessness given by the Web, give an motivating force for offenders, coming about in a surge in computer and cybernetics-related violations. Because the namelessness of the Web can make a sense of partition, offenders habitually feel confined from their violations or are ignorant of the results of their acts. Agreeing to a overview by the Office for National Insights, there were around 3.6 million events of extortion and two million cases of computer abuse in 2017. (Casciani, 2017).

Government frameworks, colossal organizations, small-to-medium businesses, eCommerce, online managing an account, and imperative foundation are getting to be more defenseless to cybercrime. In spite of the fact that

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

inspirations change, cybercrime for benefit is considerable, much more so than the recognition of non-economic attacks. Still, it is distant less so with respect to the number of endeavors or archived cases. Harm to one's notoriety, money related misfortune, and repercussions on information secrecy, judgment, and accessibility are noteworthy concerns.

The wide assortment of gadgets that can be utilized to commit a wrongdoing and the number of gadgets of intrigued to be recognized, accumulated, and analyzed at a wrongdoing scene postures a significant trouble from an investigative angle. The innovative complexity and capacity capability of gadgets contrast. Since businesses are progressively utilizing cloud administrations in their day-to-day operations and utilizing expansive capacity gadgets and the rise of keen gadgets, computerized legal examinations including such frameworks will require more complex computerized prove collecting and examination (Taylor et al., 2010). Whereas defining measures for managing with electronic or computerized prove, other supporting disciplines must too rise to help examiners in this unused world and ensure that they know appropriate cybercrime action.

REFERENCES

[1]. Anderson, R. C., Barton, R., Böhme, M. J., van Eeten, M., Levi, T. M. & Savage, S. (2013). Measuring the Cost of Cybercrime. In Böhme, R. (Ed.), The Economics of Information Security and Privacy. Springer.

[2]. Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). Challenges to digital forensics: A survey of researchers and practitioners attitudes and opinions. 2013 Information Security for South

[3]. Africa - Proceedings of the ISSA 2013 Conference, pp. 1–8.

[4]. http://doi.org/10.1109/ISSA.2013.6641058

[5]. Adams, R. B. (2012). The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice. Journal of Digital Forensics, Security and Law, 8(4), pp. 25–48.

[6]. Adams, R. B. (2013). The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. [Doctoral dissertation, Murdoch Unversity]. Retrieved from: http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf

[7]. Casey, E. (2007) What Does "Forensically Sound" Really Mean? Digital Investigation, 4(2), pp. 49–50. doi: 10.1016/j.diin.2007.05.001.

[8]. Choo, K. R. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. Computers &Security 30(8), pp. 719-731.

[9]. Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security Privacy, 15(6), pp. 12–17. http://doi.org/10.1109/MSP.2017.4251117

[10]. Dorrell, D. D., & Gadawski, G. A. (2012). Financial forensics body of knowledge. John Wiley & Sons.

[11]. Du, X., Le-Khac, N., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. ArXiv, abs/1708.01730.

[12]. Eling, M. & Wirfs, J. H. (2016). Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class.I.VW HSG Schriftenreihe59(59), University of St.Gallen, Institute of Insurance Economics (I.VW-HSG).

[13]. European Central Bank. (2018, February 23). A Euro Cyber Resilience Board for pan-

[14]. European Financial Infrastructures. Retrieved from:

[15]. https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html

[16]. Homem, I. (2018). Advancing Automation in Digital Forensic Investigations [Doctoral Dissertation, Stockholm University, Department of Computer and Systems Sciences].

[17]. Hewling, M. (2010). Digital Forensics: The UK Legal Framework [Masters dissertation, University of Liverpool].

[18]. Harbawi, M., & Varol, A. (2016). The role of digital forensics in combating cybercrimes. 2016 4th International Symposium on Digital Forensic and Security (ISDFS), pp. 138-142.

[19]. Hassan, A., Lass, F., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the way out. ARPNJ Science and Technology 2(7), pp. 626-631.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

[20]. United Nations. International Telecommunication Unit (ITU). (2017). Global Cybersecurity Index(GCI) 2017.

[21]. James, J., & Gladyshev, P. (2013). Challenges with Automation in Digital Forensic Investigations. ArXiv, abs/1303.4498.

[22]. Jaleshgari, R. (1999). Document Trading Online. Information Week755(136).

[23]. Kuchta K. J., (2000). Computer Forensics Today's Law, Investigations and Ethics Available from: http://www.liv.ac.uk/library/ohecampus/

[24]. Mugisha, D. (2019). Role and Impact of Digital Forensics in Cybercrime Investigations. International Journal of Cyber Criminology 47(3). Retrieved from:

[25]. https://www.researchgate.net/publication/331991596_role_and_impact_of_digital_forensics_ in_cyber_crime_investigations.

[26]. Mimoso, M. (2017). Maersk Shipping Reports $300M Loss Stemming from Not Petya Attack.

[27]. Threat Post - The Kaspersky Lab Security News Service.Retrieved from: https://threatpost.com/maersk-shipping-reports-300m-lossstemming-from-notpetyaattack/127477/

[28]. Macdermott, Á., Baker, T., & Shi, Q. (2018). IoT Forensics: Challenges For The IoT Era. In 9th IFIP International Conference on New Technologies Mobility and Security (NTMS) (pp. 1–5). Paris, France. http://doi.org/10.1109/NTMS.2018.8328748

[29]. McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. Harvard Business Review 90(10), pp. 1-9.

[30]. McAfee & CSIS (2018). The Economic Impact of Cybercrime - No Slowing Down.

[31]. Mac Dermott, A. M., Baker, T., Buck, P., Iqbal, F., & Shi, Q. (2019). The Internet of Things: Challenges and Considerations For Cybercrime Investigations And Digital Forensics. International Journal of Digital Crime and Forensics(IJDCF) 12(1), pp. 1-13.

[32]. Mocas, S. (2004). Building Theoretical Underpinnings for Digital Forensics Research. Digital Investigation1(1), pp. 61–68. http://doi.org/10.1016/j.diin.2003.12.004

[33]. Okutan, A., & Cebi, Y. (2019). A framework for Cyber Crime Investigation. Procedia Computer Science 158, pp. 287–294.

[34]. Oruc, E., & Tatar, C. (2017). An investigation of factors that affect internet banking usage based on structural equation modelling. Computational Human Behavior 66, pp. 232–235.

[35]. Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence1(3), pp. 1–12.

[36]. Rogers, M. (2006). DCSA: A Practical Approach to Digital Crime Scene Analysis. In Tipton, H. F. & Krause , M. (Eds.), Information Security Management Handbook. Auerbach Publications.

[37]. Schatz, B. (2007). Bodysnatcher: Towards Reliable Volatile Memory Acquisition By Software. Digital Investigation4, pp. 126-134.

[38]. Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer Law & Security Review26(3), pp. 304–308.

[39]. http://doi.org/10.1016/j.clsr.2010.03.002

[40]. Vrancianu, M., & Popa, L. A. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. The Amfiteatru Economic Journal, 1228: pp. 388403.

[41]. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.