sciendo

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

Atonbara Ombu
Charisma University, Providenciales, Turks and Caicos Island
atonbara-ombu@charisma.edu.eu

Abstract

Information and communication technologies (ICT) have changed every area of our lives. Cyberspace-related areas have reflected these shifts. Cyberspace has an undeniable positive impact on information, trade, industry, and communication. On the other hand, cybercrime is a dark side of the Internet that degrades its peaceful use. Any illegal activity carried out by or via cyberspace and its electronic environment is characterized as cybercrime. Unlike traditional crimes, cybercrimes present a real dilemma because the identities of criminals may be hidden in the virtual domain. Digital forensics has emerged to formulate possible ways for cybercrime investigation and analysis process. In this paper, we deplore the idea of digital forensics in the context of cybercrimes. An investigation of the positive impact of digital forensics in combating cybercrimes is discussed. In today's world of computers, any information can be made available within a few clicks for different endeavors. The information may be tampered with by changing the statistical properties and can be further used for criminal activities.

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

Paper type: Non-research article

Received: March 02, 2023
Accepted: June 12, 2023

Citation: Ombu, A., (2023), "Role of Digital Forensics in Combating Financial Crimes in the Computer Era", Journal of Forensic Accounting Profession, Vol. 3, No. 1, pp. 57 - 75

DOI: https://doi.org/10.2478/jfap-2023-0003

These days, cybercrimes are happening on an enormous scale and pose significant threats to the security of individuals, firms, industries, and even developed countries. Law enforcement agencies and investment institutions incorporate supportive examination policies, procedures, and protocols to address the complete investigation process to combat such crimes. This research paper entails a detailed review of several cybercrimes followed by various digital forensics processes involved in the cybercrime investigation. Various digital forensics tools with detailed explanations are discussed with advantages, disadvantages, challenges, and drawbacks.

1. Introduction

In the early days of digital forensics, interest and effort were focused on addressing stand-alone and network personal computers. As technology has developed, the focus has extended to include recovering evidence from any device with a digital processor or storage capability. As a result, digital forensics has moved from investigating computer-based crimes such as hacking to exploring all types of cybercrimes, including financial crimes (Mugisha, 2019). Digital forensics, forensic computing, and computer forensics are all words that are sometimes used interchangeably (Schatz, 2007). Computer forensics and forensic computing originally referred to the utilization of computer-related evidence in legal proceedings. Digital forensics and digital investigations are widely used to gather, examine, analyze, and present digital evidence in court (Hewling, 2013). Cyber/computer crimes have become prevalent in today's technologically driven culture. With the ongoing rise in the use and availability of digital devices and the digitization of previously-stored analog data, digital evidence in court cases is becoming increasingly important. Digital evidence differs from previous evidence given in court since it exhibits flaws such as being easily altered, improperly presented, and a general lack of familiarity with this type of evidence.

Without a doubt, the last few decades are representing a breakthrough in Information Communication Technology (ICT). The emergence of the Internet or cyberspace as a very effective communication medium has brought countless benefits. Most of our activities have moved from the physical world to the virtual world, where cyberspace is the keyword. For example, until the mid-1990s, the banking sector in most parts of the world was simple and reliable. However, since the development of information technology, the banking industry has experienced a paradigm shift (Jaleshgari, 1999). Banks established numerous platforms to increase their customer base by allowing transactions to be completed without much effort

(Vrancianu and Popa, 2010). It is realized in practical systems such as e-commerce, e-learning, e-banking, etc., which have tremendously facilitated and speeded up most transactions. The remaining sections of the study are divided into five sections: Digital Forensics in the Context of Cybercrime; Digital Forensic Investigation; Cybercrime, Globalization, and Global Economic Growth; The Tenets of Digital Forensics Investigation; and Cybercrime Investigations and Digital Forensics.

2. Digital Forensics in the Context of Cybercrime

Digital Forensics is the branch that deals with the crimes which happen over computers. Where a single computer system constitutes an entire crime scene the least, it may contain some evidence or information that can be useful in the investigation. However, in technical terms, it can be defined as the identification, acquisition, preservation, analysis, and documentation of any digital evidence (Rana et al., 2017). Digital forensics collects evidence from any computing device and investigates, analyzes, and preserves it as legally admissible evidence in a court of law. Cybercrimes, also known as e-crimes, hi-tech crimes, or electronic crimes, are operations performed by an individual who has some or intensive knowledge of the computer and its whole system to extract and delete the stored data illegally. It is described as a crime done on the Internet, through the Internet, or the use of the Internet. Phishing, credit card frauds, bank robberies, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber-terrorism, the production and spread of viruses, and so on are all examples of computer crime (Mugisha, 2019). Cybercrimes refer to illegal, unethical, and unauthorized behavior in a system that processes information or transfers data using computer and communication technologies (Okutan and Cebi 2019). Cybercrime is also defined as unlawful or unacceptable acts committed using electronic devices, including computers, as a target or a tool (Vadza 2011). These crimes include laundering, theft, fraud, hacking, forgery, and defamation (Awoyemi et al., 2021).

The idea of digital forensic sciences is based on an electronic environment or cyberspace crime scene. In this regard, it is likely to need the know-how to be able to analyze the crime scene. Analysis of cyberspace crime scenes aims at identifying the puzzle pieces that solve the electronic crime. Therefore, the first thing that should be considered is the evidence likely to be in the digital form. Digital evidence can be defined as any form of data in electronic systems, such as documents, audio, videos, browsing history, social media activities, logs, e-banking, and credit card transactions. The digital evidence maybe also in the form of e-signature or online shopping. The ubiquity of computer systems, dependency on electronic devices, and cyberspace create various forms and lots of digital evidence that can be traced. Digital evidence may be generated by: Open computer systems include internal or external storage, input and output devices, and peripheral devices. Communication systems: including traditional and mobile phones, wireless devices, routers, cyberspace, and any network. Embedded computer systems: portable devices, smart cards, tablets, and any other device with an embedded computer.

3. Digital Forensic Investigation

A Digital Forensic Investigation, as defined by Homem (2018), involves the reconstruction of events using digital evidence to understand, prove, disprove or remediate criminal or otherwise malicious actions within a digital environment or crime scene, as it may be. A digital environment could include computing devices related to businesses, governments, healthcare providers, individuals, or other organizations. Hence, reconstruction of events is used to make crucial decisions involving potentially critical computing infrastructure and often sensitive data to the stakeholders involved. The goal of digital forensics is to follow the standardized investigation process while documenting any evidence that is stored in digital form, which may indicate to the person responsible for the crime. The investigators use various techniques and forensic applications to search hidden folders, retrieve deleted data, decrypt the data, restore damaged files, etc. Examples of outcomes of decisions could include initiating remediation measures that may be costly and appropriating the actions to a culprit (an individual, organized group, or national or state actor) leading to incarceration. Outcomes of decisions could also include reputation damage, loss of jobs, business or sensitive data, and even far-reaching effects such as destabilizing economies, governments, and international relations (Mimoso, 2017). Therefore, digital evidence and the digital investigation process must be reliable and trustworthy to make trustable decisions, as the consequences can be devastating. The need for integrity and trust in the data and the process is often termed forensic soundness (Casey, 2007). For evidence to be considered reliable and valid in a court of law, the forensic investigator is required to understand and be able to clarify the process of how the evidence was forensically collected, which makes it almost as important as identifying the evidence in the first place (James & Gladyshav, 2013).

4. Cybercrime, Globalization, and Global Economic Growth

Globalization refers to global transformation or internationalization interlinked with the socio-economic, technological, political, and cultural aspects through different flow mediums, including people, sharing of data and information, rural-urban migration, and online trading of goods and services (Awoyemi et al., 2021). It involves the integration of different societies, cultural practices, economies, technological innovations, and institutional governance, leading to complex mutual interrelatedness. Due to globalization, individuals, organizations, societies, and governments from other countries communicate, collaborate, and integrate. Globalization has aided progress in different ways in different parts of the world. It has facilitated access to education, transportation, communication, health facilities, importation and exportation, employment opportunities, government revenue, and a high standard of living for the people over the years. Trade and technology are two other sectors of society that have been substantially influenced by globalization. Information technology advancements provide new techniques for participating in worldwide economic activities by facilitating the movement of properties, resources, and money and collaboration with far-flung partners. However, cybercrime has a significant negative impact on society associated with technology. The tech world has undergone an immense digital transformation to attain a digital economy in real-world applications such as innovative learning, smart/precision farming, smart governance, and smart cities (McAfee and Brynjolfsson, 2012; Constantiou and Kallinikos, 2015). Moreover, various data-intensive economic sectors, such as telecommunication and information technology, manufacturing, banking, investment, and health in advanced economies, have managed to apply Big Data to digitalize their economies.

Cybercrimes refer to illegal, unethical, and unauthorized behavior in a system that processes information or transfers data using computer and communication technologies (Okutan and Cebi, 2019). Cybercrime is also defined as unlawful or unacceptable acts committed using electronic devices, including computers, as a target or a tool (Vadza, 2011). Cyber attacks are deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and programs resident in transiting these systems or networks. Cyber attack weapons can generate outcomes that range from the simple defacing of a website to stealing data and intellectual property, espionage on target systems, and even disrupting critical services. Cybercriminals have different motives, but they can command the resources to create attacks to achieve their desired results. They may commit fraud, identity theft, stealing money, and robbery against individuals, corporations, banks, regions, and nations (Mugisha, 2019). Processes of global connectivity that have seen a revolution in communication and social exchange also facilitate criminal activities on a planetary scale. This phenomenon has been variously conceptualized as web crime, digital criminality, e-criminality, or, at its most generic, cybercrime (Wall, 2007). "Significantly, this project was developed because computers were being utilized to conduct crimes more and more," Kuchta (2000) writes in his history of computer forensics. Because of the nature and widespread use of the technology, connectivity has resulted in various security vulnerabilities and will continue to do so. As networks and other technologies, particularly the Internet, evolve rapidly, cybercrime has become more prevalent worldwide (Hewling, 2010).

5. The Tenets of Digital Forensics Investigation

Courts utilize it extensively to assist judges and jurors in criminal and civil matters. Any digital data that establishes criminal behavior or offers a link between an accused and a victim or an accused and a crime is defined as digital evidence. Evidence refers to thing/s that help form a conclusion or judgment (Hewling, 2014). The digital forensics investigation process involves identification, acquisition, preservation, examination and analysis, and presentation (Harbawi & 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). Harbawi and Varol (2016) also stated that "before any investigation step, identifying relevant digital elements that can be used for data acquisition should be done. These elements include computers, mobile phones, personal digital assistants, tablets, or any other electronic device containing and storing digital information, 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 acquisition comes after the identification step. Once the evidence is identified, it needs to be acquired in the most appropriate manner where the integrity of the evidence remains intact. The sub-steps to follow during the acquisition of the investigation can be seizing the crime scene and forensically acquiring the data stored in the found devices for further investigation. The two sources of evidence: volatile and non-volatile data have different acquisition methods. Once the items or data of interest have been identified, digital acquisition initiates. Here, the acquisition is made by seizing electronic devices found or attached to the crime scene and forensically acquiring (copying) the data found in their memory for investigation purposes (Harbawi and Varol, 2016).

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.

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 final step in the digital forensic investigation process is when the examiner should provide a report, and documentation, on how the forensic process was done, what type of tools and methods were used, legal protocols and policies followed forensics findings, and relevant articulations. The report should be written in an understandable and explicit language, consistent with the conclusions, and accurate in its presentation.

6. 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. Offenders utilize various methods to access their victims' computers, including software that scans for open ports or bypasses security barriers and social engineering. Cybercriminals collect information by phishing and spoofing, where the imposter uses the victim's information without their consent. Phishing refers to sending unnecessary emails to corporate clients of different institutions by manipulating them to share their personal account information via fake websites (Hassan et al. 2012). 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. If perpetrators succeed in blocking computer systems from functioning correctly, victims may suffer significant financial damages. Physical attacks on the computer system can be used to carry out attacks. Offenders who get access to the computer system can destroy hardware. The financial losses incurred by computer system attacks are frequently significantly more than the cost of computer hardware for very profitable e-commerce enterprises. Computer worms and denial-of-service (DoS) attacks are examples of remote attacks on computer systems.

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 enforcement to track money flows back to criminals. When criminals make anonymous payments, it is tough to follow them. When criminals employ anonymous currencies, law enforcement can identify suspects through money transfers is limited.

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 name-related offenses are the most severe offenses. A company's positive reputation is frequently tied to its trademarks. Brand names and trademarks are used fraudulently in various activities, including phishing. Millions of emails imitating emails from real organizations are sent out to internet users containing 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. Fraud and Computer-Related Fraud

Computer-related fraud is one of the most common crimes on the Internet because it allows offenders to hide their identities through automation and software tools. Automation will enable criminals to profit handsomely from minor offenses. Offenders utilize one approach to ensure that each victim's financial loss is minimal. Victims of "little" losses are less inclined to devote time and effort to reporting and investigating crimes. Online auction fraud and advanced fee fraud are two of the most popular types of fraud.

6.8. Online Auction Fraud

The lack of physical contact between sellers and purchasers can exploit criminals who conduct crimes using auction sites. Due to the difficulty in discriminating between legitimate users and criminals, auction fraud is one of the most common forms of cybercrime. Offering non-existent products for sale and seeking payment before delivery are the two most popular tactics: purchasing goods and asking for delivery without intending to pay. As a result, auction houses have implemented safeguards such as the feedback/comments system. Buyers and sellers submit feedback after each transaction for other users to use as neutral information on the reliability of sellers and buyers. On the other hand, criminals have retaliated by using third-party accounts to get beyond this protection. In the "account takeover" scam, criminals attempt to get legitimate users' user names and passwords to buy or sell products fraudulently, making identifying the perpetrators more difficult.

6.9.Fraudulent Payment in Advance

In advance fee fraud, criminals send emails to recipients requesting their assistance in moving vast sums of money to third parties, promising them a share if they agree to complete the transfer using their accounts. The perpetrators then urge them to either give bank account data directly or transfer a small amount to authenticate their bank account data - respondents may be willing to suffer a slight but guaranteed loss in exchange for a significant but unlikely win). They will never hear from the criminals again once they have transferred the funds. Offenders may utilize their bank account information for fraudulent purposes if they send it. Thousands of targets, according to evidence, respond to emails. According to recent studies, advance fee frauds are still on the rise in both the number of victims and total losses, despite multiple information campaigns and initiatives.

6.10. Computer-Related Forgery

The alteration of digital documents is referred to as computer-related forgeries. Creating a paper that appears to come from a reputable organization, changing electronic photographs, or altering text documents are examples of the crime. Phishing relies heavily on the fabrication of emails. Phishing aims to induce people to reveal personal or confidential information. Offenders frequently send out emails that appear to be from reputable financial institutions that the target uses. The emails are crafted to make it difficult for recipients to recognize them as spam. The email requests that the recipient divulge and verify sensitive information. Many victims heed the suggestion and reveal information that allows criminals to perform internet transfers and other transactions.

6.11.Identity Theft

The criminal act of falsely obtaining and utilizing another person's identity is identity theft. The increased usage of digital information has provided new opportunities for criminals to obtain identity-related information. As a result, the transition from industrialized to information societies has significantly impacted the growth of identity theft crimes. Identity-related data is becoming increasingly important in business and social interactions. A "good name" and solid personal relationships dominated business and daily activities in the past. Face-to-face identification has become increasingly complex with the shift to internet commerce. As a result, identity-related information has become vital for persons engaging in social and commercial interactions. Non-face-to-face transaction needs, such as trust and security, now dominate the economy, not only e-commerce enterprises. The usage of payment cards with a personal identification number (PIN) for grocery purchases is an example.

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. An identity thief can use this information to commit financial cybercrime. Cybercriminals use various methods to steal people's bank information and money (Choo, 2011). The findings of an empirical study conducted by Anderson et al. (2012) revealed that financial institutions such as banks had suffered billions of dollars in losses globally and provided details of direct and indirect losses, criminal revenue, and indirect costs as a result of cybercrime in the banking sector around the world.

6.12.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. When it comes to placing vast sums of money, the Internet may not provide any real benefits. However, offenders in the layering (or masking) phase will find the Internet particularly beneficial. Money-laundering investigations are even more complicated when money-launderers utilize online casinos to stack their transactions. Money transfer regulation is currently weak, and the Internet allows criminals to make cheap and tax-free cross-border money transactions.

6.13.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" (Cebula and Young) (2010). Cyber risk shares feature with property and liability risk and catastrophic and operational risk (Eling and Wirfs, 2016) compared to risk categories covered by insurance. 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. Finally, business disruptions are tied to availability difficulties (Bouveret, 2018). The three cyber-attack forms directly affect the targets: Firms cannot operate due to business disruptions, resulting in revenue loss.

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).

7. 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). The new analysis replaces a popular 2014 report estimated worldwide losses at nearly

$500 billion, or 0.7 percent of global income. To put these figures in context, they exceed the income of practically every country but a few. When you compare the cost of cybercrime to the global internet economy, which was $4.2 trillion in 2016, cybercrime may be considered a 14 percent growth tax. As a worldwide economic scourge, cybercrime ranks third, behind government corruption and narcotics, for the following reasons:

Everyone is affected: Personal data has been stolen or compromised for about two-thirds of persons who utilize online services (over two billion people).

Low-Risk, High-Reward: The chances of being arrested or going to jail are slim. None of the perpetrators of the most high-profile security breaches have been charged. Although law enforcement authorities are increasing their efforts, many cybercriminals operate outside their territories. The report credits the $100 billion increase in cybercrime to cybercriminals' swift adoption of new technology and the ease they engage in cybercrime. A growing number of cybercrime centers and top-tier cybercriminals' are developing financial sophistication.

Europe, North America, and Central Asia, East Asia and the Pacific, South Asia, Latin America and the Caribbean, Sub-Saharan Africa, the Middle East, and North Africa are all included in the report. The paper's conclusions reveal that the cost of cybercrime varies by region, based on each nation's level of cybersecurity maturity, which is assessed using the following key indicators: legal measures, capacity building, technical standards, organizational measures, and cooperation. The findings were divided into top-tier countries with developed digital economies and cybersecurity, mid-tier countries evolving their digital and cybersecurity, and bottom-tier countries with developing digital economies and cybersecurity. As one might imagine, wealthier countries experience more cybercrime losses. Those in the middle are the most brutal hit.

Brazil is the second most common source of cyberattacks and the third most frequently targeted country.

Germany is home to the European Union's most advanced underground internet economy.

Japan: Previously immune to cybercrime due to a language barrier and a lack of money laundering infrastructure, the country is now seeing an uptick, particularly in assaults on banks.

Online fraud and cybercrime account for approximately half of all crimes in the United Kingdom, with over 5.5 million offenses reported yearly. The United Arab Emirates is the world's second-most targeted country, with annual cybercrime costs estimated at $1.4 billion.

8. Cybercrime Investigations and Digital Forensics

Through the identification of computer-based and computer-assisted crime, digital forensics has become an essential instrument in the battle against cybercrime. Security specialists and law enforcement organizations investigating cybercrime face significant hurdles due to today's massive amounts of data, varied information, and communication technologies, and borderless cyberinfrastructures. Investigating cybercrime can occur across national borders, jurisdictions, and legal systems. This problem, combined with the vast amount and variety of data, extremely heterogeneous information and communication technologies, and complex current hardware/software frameworks, create significant obstacles, particularly in digital forensics (Caviglione et al., 2017). Digital forensic investigations are widely used by law enforcement to analyze electronic media, and businesses are increasingly using them as part of their incident response procedures (Al Fahdi et al., 2013). Historically, only a tiny percentage of victims and investigators have been affected by e-crime or computer-related crime. However, this is changing, and digital evidence in formal investigations is becoming commonplace. Electronic evidence will undoubtedly be seized, preserved, and examined in any public or private investigation. As a result, digital evidence processing must be integrated into the whole investigation.

When conducting a digital forensics-based investigation, a digital forensics process model or digital forensic methodology provides a framework for procedures and processes to be followed (Mac Dermott, 2019). Many models have been presented to speed up the investigative process or tackle issues during forensic investigations (Du, X., Le-Khac, N. A., & Scanlon, 2017). These features and terms establish research and tool development principles (Mocas, 2004). The investigator determines a model or methodology for crime scene processing and evidence confiscation. Different models include the same fundamental steps (detect, secure, analyze, and present), but each pays extra attention to distinct stages. For example, Adams (2013) advocates allocating significant time for pre-planning and pre-investigative phases in the Advanced Data Acquisition Model (ADAM) technique. The Advanced Data Acquisition Model was created to solve the flaws noted in a previous review study (Adams, 2012), which revealed that none of the currently available models suit the requirements of researchers and practitioners.

Current models have been criticized for being too detailed (Reith et al., 2002), too broad (Rogers, 2006), or too complex in various ways (Selamat et al., 2008). In contrast, Macdermott et al. (2018)'s Computer Forensics – Secure, Analyze, Present (CFSAP) breaks down the four essential parts of computer forensics (identification, preservation, analysis, and presentation) into three simple steps:

1) Secure (identify sources of digital evidence, preserve digital evidence).
2) Analyze (forensic analysis of digital evidence: extract, process, interpret).
3) Present (Presentation of digital evidence, expert opinion, and testimony).

Framework for Reliable Experimental Design (FRED) focuses on the techniques that support reverse engineering of digital data structures and the process of reliably retrieving and understanding digital content. The suggested framework is intended to serve as a resource for individuals working in digital forensics, both in industry and academia, to support and create research best practices (Horsman, 2018). The three fundamental steps of any strategy are evidence collecting, analysis, and presentation, but the emphasis and attention given to additional stages might vary. You may have to pay attention to other stages or change your strategy. Standardization and transparency in digital forensic research procedures are required to provide adequate peer evaluation of practices, secondary data interpretation, and the capacity to judge the veracity of findings presented in addition to knowledge (Horsman, 2018). Following a generic process, the model is insufficient to deal with the various types of cybercrime and the wide range of instances law enforcement encounters.

Conclusion

Although crime has always existed in human civilization, the methods by which it is committed are continually evolving and expanding. Criminals benefit from the changing nature of technology by having new means and tools to commit crimes. Previously, criminal investigations relied on physical evidence, the examination of the crime scene, the questioning and recording of witnesses, and the questioning and recording of suspects. Today's criminal investigators must accept the possibility that the evidence they must examine is electronic or digital (Macdermott et al., 2018). Unlike the typical 'physical' scene, the crime scene could consist of a computer system, intelligent and small-scale digital devices, or network traffic/logs. Computer-generated log files, metadata, or surfing history could be used as "witnesses" in these circumstances. Fingerprints can be used to show who was wielding a particular weapon, but how can we know who was at the keyboard when the crime was committed? In this field, forensic linguistics is increasingly being utilized to aid investigations by identifying participants within a conversation, determining motives and behaviors, and creating a timeline of occurrences. Cybercrime is on the rise due to technological advancements and our growing connectivity to the Internet and devices in our daily lives. These advancements, combined with the anonymity provided by the Internet, provide an incentive for criminals, resulting in a surge in computer and cybernetics-related crimes.

Because the anonymity of the Internet can create a sense of separation, criminals frequently feel detached from their crimes or are unaware of the consequences of their acts. According to a survey by the Office for National Statistics, there were around 3.6 million occurrences of fraud and two million cases of computer misuse in 2017. (Casciani, 2017). Government systems, huge organizations, small-to-medium businesses, eCommerce, online banking, and vital infrastructure are becoming more vulnerable to cybercrime. Although motivations vary, cybercrime for profit is substantial, much more so than the perception of non-economic attacks. Still, it is far less so regarding the number of attempts or documented cases. Damage to one's reputation, financial loss, and repercussions on data confidentiality, integrity, and availability are significant concerns.

The wide variety of devices that can be used to commit a crime and the number of devices of interest to be recognized, gathered, and analyzed at a crime scene poses a substantial difficulty from an investigative standpoint. The technological complexity and storage capability of devices differ. Because businesses are increasingly using cloud services in their day-to-day operations and using large storage devices and the rise of smart devices, digital forensic investigations involving such systems will require more complex digital evidence collecting and analysis (Taylor et al., 2010). While formulating standards for dealing with electronic or digital evidence, other supporting disciplines must also emerge to aid investigators in this new world and guarantee that they know proper cybercrime activity.

References

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.

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 Africa - Proceedings of the ISSA 2013 Conference*, pp. 1–8. http://doi.org/10.1109/ISSA.2013.6641058

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.

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

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *International Monetary Fund (IMF) Working Paper* 2018/143, pp. 1-29.

Casciani, D. (2017, January 19). Cybercrime and fraud scale revealed in annual figures. *BBC News*. Retrieved from: http://www.bbc.co.uk/news/uk-38675683

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

Constantiou, I., & Kallinikos, J. (2015). New Games, New Rules: Big Data and the Changing Context of Strategy. *Journal of Information Technology 30*(1), pp. 1-32.

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

Cebula, J. J. & Young, L. R. (2010). *A taxonomy of Operational Cyber Security Risks, (CMU/SEI-2010-TN-028).* Software Engineering Institute, Carnegie Mellon University.

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

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

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.*

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

European Central Bank. (2018, February 23). *A Euro Cyber Resilience Board for pan-European Financial Infrastructures.* Retrieved from: https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html

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

Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A Research Framework To Ensure The Dependable Interpretation Of Digital Data For Digital Forensics. *Computers and Security 73*, pp. 294–306. http://doi.org/10.1016/j.cose.2017.11.009

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

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.

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.

United Nations. International Telecommunication Unit (ITU). (2017). *Global Cybersecurity Index (GCI) 2017.*

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

Jaleshgari, R. (1999). Document Trading Online. *Information Week 755*(136).

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

Lavorgna, A., & Sergi, A. (2014). Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies. *International Journal of Law, Crime and Justice 42*(1), pp. 16-32.

Mugisha, D. (2019). Role and Impact of Digital Forensics in Cybercrime Investigations. *International Journal of Cyber Criminology 47*(3). Retrieved from: https://www.researchgate.net/publication/331991596_role_and_impact_of_digital_forensics_in_cyber_crime_investigations.

Mimoso, M. (2017). Maersk Shipping Reports $300M Loss Stemming from Not Petya Attack. *Threat Post - The Kaspersky Lab Security News Service. Retrieved from:* https://threatpost.com/maersk-shipping-reports-300m-lossstemming-from-notpetya-attack/127477/

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

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

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

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.

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

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

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.

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

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.

Schatz, B. (2007). Bodysnatcher: Towards Reliable Volatile Memory Acquisition By Software. *Digital Investigation 4*, pp. 126-134.

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *International Journal of Computer Science and Network Security 8*(10), pp. 163–169.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review 26*(3), pp. 304–308. http://doi.org/10.1016/j.clsr.2010.03.002

Vrancianu, M., & Popa, L. A. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. *The Amfiteatru Economic Journal*, 1228: pp. 388-403.

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

Sažetak

Informacijske i komunikacijske tehnologije (IKT) promijenile su svako područje naših života. Područja koja se odnose na sajber prostor odraz su ove promjene. Sajber prostor ima neosporan pozitivan uticaj na informacije, trgovinu, industriju i komunikaciju. S druge strane, sajber kriminal je mračna strana interneta koja degradira njegovu miroljubivu upotrebu. Svaka nezakonita aktivnost koja se provodi putem sajber prostora i njegovog elektronskog okruženja okarakterizirana je kao sajber kriminal. Za razliku od tradicionalnih zločina, sajber kriminal predstavlja pravu dilemu jer identitet kriminalaca može biti skriven u virtuelnom domenu. Digitalna forenzika se pojavila kako bi formulisala moguće načine za istragu i proces analize sajber kriminala. U ovom radu raspravlja se o istraživanju pozitivnog uticaja digitalne forenzike na borbu protiv sajber kriminala. U današnjem svijetu računara, bilo koja informacija može biti dostupna u nekoliko klikova za različite poduhvate. Informacije se mogu mijenjati promjenom statističkih svojstava i mogu se dalje koristiti za kriminalne aktivnosti. Današnjih dana, sajber kriminal se dešava u ogromnim razmjerima i predstavlja značajnu prijetnju sigurnosti pojedinaca, firmi, industrija, pa čak i razvijenih zemalja. Agencije za provođenje zakona i investicione institucije uključuju prateće politike, procedure i protokole za ispitivanje kako bi se bavili kompletnim istražnim procesom u borbi protiv takvog kriminala. Ovaj istraživački rad uključuje detaljan pregled nekoliko vrsta sajber kriminala praćenih raznim digitalnim forenzičnim procesima uključenim u istragu istog. Različiti digitalni forenzični alati sa detaljnim objašnjenjima su razmatrani sa prednostima, nedostacima i izazovima.

Ključne riječi: *digitalna forenzika, borba protiv finansijskog kriminala, kompjuterska era.*