THE RELEVANCE OF DIGITAL FORENSICS IN THE BATTLE AGAINST CYBERCRIME

Mamta Sakpal Research Scholar Department of CSE Vivekananda Global University, Jaipur, Rajasthan -303012
Dr. Sanjay Kumar Sinha Associate Professor Department of CSE Vivekananda Global University, Jaipur, Rajasthan -303012

ABSTRACT
The advent of ICT has revolutionized every facet of human existence. The domains associated with cyberspace have mirrored these changes. Information, commerce, business, and communication are all positively impacted by cyberspace. In contrast, cybercrime diminishes the Internet's otherwise benign use. Cybercrime refers to any unlawful conduct perpetrated using the Internet and its electronic infrastructure. Because cybercriminals' identities can be concealed in the virtual world, cybercrimes provide a significant challenge in comparison to traditional crimes. An emerging field known as digital forensics has the potential to revolutionize the way cybercrime investigation and analysis are conducted. We criticize the concept of digital forensics as it pertains to cybercrimes in this article. The article delves into the ways digital forensics might help fight cybercrimes. Nowadays, with the use of computers, any kind of information can be quickly and easily accessed for many purposes. Data can be compromised by altering statistical features and subsequently utilized for illicit purposes.

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

INTRODUCTION
Both standalone and networked personal computers were the primary targets of attention and research in the early stages of digital forensics. Now that more and more devices have digital processors or storage capabilities, the focus has shifted to include recovering evidence from any of these devices. So, digital forensics has expanded its scope to include all forms of cybercrime, including financial crimes, in addition to computer-based crimes like hacking (Mugisha, 2019). Some sources use the terms "digital forensics," "forensic computing," and "computer forensics" interchangeably (Schatz, 2007). The original meaning of computer forensics and forensic computing was the use of evidence pertaining to computers in court. It is common practice to collect, inspect, analyse, and present digital evidence in court through digital investigations and forensics (Hewling, 2013). In today's technologically advanced society, cybercrime and computer crimes have grown commonplace. As more and more people own and utilise digital devices, and as more and more analogue material is digitised, the significance of digital evidence in legal proceedings is growing. Digital evidence is different from earlier forms of evidence presented in court since it has shortcomings such being easily changed, being presented incorrectly, and people generally not being familiar with it.
There is no denying that ICT has made tremendous strides in the last several decades. Numerous advantages have resulted from cyberspace's (the Internet's) rise to prominence as a highly efficient communication channel. Nowadays, we spend much of our time in cyberspace, a virtual realm where most of our actions take place. As an example, most of the world's banking systems were straightforward and trustworthy up until the mid-1990s. A paradigm shift, however, has occurred in the banking business since the emergence of information technology (Jaleshgari, 1999). Because they made it easy for customers to make transactions, banks set up a plethora of platforms to attract more customers.
Specifically, Vrancianu and Popa (2010). Online technologies like e-commerce, e-learning, e-banking, etc., have made this a reality and greatly simplified and accelerated the majority of transactions. Digital Forensics in the Context of Cybercrime, Digital Forensic Investigation, Cybercrime, Globalisation, and Global Economic Growth, The Tenets of Digital Forensics Investigation, and Cybercrime Investigations and Digital Forensics make up the remaining sections of the study.

Digital Forensics in the Context of Cybercrime

Crimes committed by digital means are the purview of digital forensics. Even while a single computer system doesn't make up much of a crime scene, it could nonetheless have information or evidence that helps with the investigation. On the other hand, according to Rana et al. (2017), it can be described more technically as the process of locating, collecting, storing, analysing, and documenting digital evidence. The field of digital forensics investigates, analyses, and saves data found on any electronic device so that it can be used as evidence in legal proceedings. Cybercrimes, often called e-crimes, hi-tech crimes, or electronic crimes, involve malicious data extraction and deletion carried out by an individual with a basic or advanced understanding of computer systems. Crimes committed on, through, or in relation to the Internet are defined as such. Computer crimes include a wide range of activities, such as phishing, credit card fraud, bank robberies, illegal downloading, industrial espionage, child pornography, cyber-terrorism, scams, virus generation and distribution, and so on (Mugisha, 2019). According to Okutan and Cebi (2019), cybercrimes are illicit, immoral, or unauthorised actions carried out within a system that handles data processing or transfers data through the use of communication and computer technology. Another definition of cybercrime is any wrongdoing that makes use of computers or other electronic equipment, whether as an instrument or a target (Vadza 2011). Some examples of these crimes are defamation, hacking, fraud, theft, and laundering (Awoyemi et al., 2021).

The concept of a cybercrime scene or electronic environment is foundational to digital forensic sciences. To that end, expertise in analysing crime scenes is likely to be required. Finding the missing parts of the electronic criminal puzzle is the goal of cybercrime scene analysis. Consequently, evidence most likely to exist in digital form should be taken into account first. Any information stored in an electronic system, including but not limited to documents, audio, video, social media activity, logs, e-banking, and credit card transactions, can be considered digital evidence. Electronic signatures or purchases made via a website might likewise constitute digital proof. Computer systems' pervasive**ness, reliance on electronic** devices, cyberspace, and a deluge of tracable digital evidence all contribute in different ways. Any number of open computer systems, including storage (both internal and external), I/O devices, and peripherals, can produce digital evidence. "Systems for communication" encompass not only landlines and cell phones but also wireless devices, routers, the Internet, and any kind of network. Mobile gadgets, smart cards, tablets, and anything else that has a built-in computer are considered embedded computer systems.

Digital Forensic Investigation

According to Homem (2018), a digital forensic investigation is one that rebuilds events within a digital environment or crime scene using digital evidence in order to analyse, verify, disprove, or remedy illegal or otherwise malicious conduct. Business, government, healthcare, individual, and other organization-related computing equipment could all be part of a digital ecosystem. Therefore, important decisions involving potentially vital computer infrastructure and frequently private data are based on event reconstruction. Following the established protocol of an investigation and recording any evidence kept in digital form that can point to the perpetrator is what digital forensics is all about. In order to repair corrupted files, decode data, find hidden folders, recover deleted data, etc., investigators utilise a variety of methods and forensic applications. Costly repair efforts may be initiated and attributed to a culprit (an individual, an organisation, a national or state entity), resulting to jail, as an example of a possible outcome of a decision. Decisions can have far-reaching consequences, such as destabilising economies, governments, and international relations; they can also harm reputations, lead to the loss of employment, businesses, or sensitive data; and so on (Mimoso, 2017). The stakes are too high for anything less than trustworthy digital evidence and an inquiry that uses it to make judgements. Forensic soundness refers to the requirement for data and process integrity and trustworthiness (Casey, 2007). Just as crucial as identifying the evidence itself is the forensic investigator's ability to comprehend and explain the process of forensic collection if the evidence is to be deemed credible and valid in a legal setting (James & Gladyshav, 2013).

Cybercrime, Globalization, and Global Economic Growth

The term "globalisation" describes the process by which various flow media connect socioeconomic, technical, political, and cultural elements with internationalisation on a global scale. components, such as individuals, information and data exchange, movement from rural areas to urban centres, and online commerce (Awoyemi et al., 2021). It entails the intricate interdependence of various civilizations, cultural traditions, economic systems, technical advancements, and institutional governance. People, groups, and governments from all over the world are able to connect, work together, and integrate as a result of globalisation. In various regions of the globe, globalisation has contributed to advancement in distinct methods. Over the years, it has helped people get to and from school, communicate with one another, use healthcare services, import and export goods, get jobs, pay taxes, and generally live well. Another area where globalisation has had a significant impact is in trade and technology. New methods of collaborating with faraway partners and transferring assets, resources, and money have emerged as a result of developments in information technology, which allow more people to take part in global economic operations. But society suffers greatly from cybercrime's detrimental effects on technology. According to McAfee and Brynjolfsson (2012) and Constantiou and Kallinikos (2015), the IT sector has experienced a massive digital transformation in order to achieve a digital economy in real-world applications including smart cities, smart governance, smart agriculture, and innovative learning. Furthermore, in developed economies, numerous data-intensive industries have successfully utilised Big Data to digitise their operations, including healthcare, banking, manufacturing, information technology, and telecommunications.

According to Okutan and Cebi (2019), cybercrimes are immoral, unlawful, or unauthorised actions carried out by a system that handles data processing or transfers data through the use of computer and communication technology. Computers and other electronic equipment can be used as tools or targets in illegal or undesirable ways; this is known as cybercrime (Vadza, 2011). Computer systems and networks, as well as the data and programmes stored within them, are vulnerable to cyber assaults, which aim to change, disrupt, deceive, diminish, or destroy them. From the mere defacement of a website to the theft of data and intellectual property, espionage on target systems, and even the disruption of essential services, cyber assault weapons can produce a wide range of results. Although cybercriminals' goals may vary, they often have the means to launch coordinated operations. Individuals, businesses, financial institutions, areas, and even countries might fall victim to their schemes of deceit, theft, and robbery (Mugisha, 2019). Along with the revolution in communication and social exchange, processes of global connection have also made it easier for criminal actions to occur on a worldwide scale. Many terms have been used to describe this phenomena; some examples are cybercrime, web crime, digital criminality, and e-crime (Wall, 2007).

According to Kuchta (2000), who traces the history of computer forensics, the field evolved in response to the increasing criminal use of computers. There are a number of security holes that have arisen and will persist as a result of connectivity due to the characteristics and extensive use of the technology. Worldwide, cybercrime has been on the rise because to the fast evolution of networks and other technologies, especially the Internet (Hewling, 2010).

The Tenets of Digital Forensics Investigation

Judges and jurors in both civil and criminal cases rely on it heavily. Data stored digitally that proves criminal activity or connects a suspect to a crime or a victim is called digital evidence. According to Hewling (2014), evidence is everything that can be used to draw a conclusion or make a judgement. The steps of a digital forensics inquiry include discovery, collection, storage, analysis, and presentation (Harbawi & Varol, 2016).

Recognising the Digital Documents

Finding any digital evidence that may be lying around the crime scene is the first order of business. Any digital data storage device, such as a computer, pen drive, hard drive, or any other electronic device, can be used as evidence (Rana et al., 2017). In their 2016 publication, Harbawi and Varol

emphasised the importance of identifying relevant digital elements that can be used for data acquisition prior to any investigation. These elements encompass a wide range of electronic devices, including computers, mobile phones, personal digital assistants, tablets, and storage devices like hard discs, pen drives, compact discs, digital video discs, and other peripheral devices with the ability to store digital data.

Acquisition
Digital acquisition begins with the identification of items or data of interest. In this step, electronic devices found or attached to the crime scene are seized and their memory data is forensically acquired (copied) for investigational purposes. The next step is to acquire the evidence in the most appropriate manner while preserving its integrity. The acquisition of the crime scene and the data stored in the found devices are sub-steps in the acquisition of the investigation. The methods for acquiring volatile data differ from those for non-volatile data.

Preservation
Digital evidence is safeguarded from intentional and accidental changes to its contents through a well-established chain of custody. As an additional precautionary measure during forensic acquisition, read-only copies of the acquired evidence should be maintained.

Investigating and Assessing
Forensic examiners rely heavily on their experience and expertise to identify the methods, tools, and skills necessary to extract vital information that can be used in a court of law from digital evidence. After evidence has been examined, it is categorised according to its type. For example, data extracted from an email contains different data and metadata than data extracted from an image.

Presentation
At the end of a digital forensic investigation, the examiner is responsible for writing a report that details the procedures followed, the tools and methods used, the legal protocols and policies that were based on the forensic findings, and any pertinent articulations. The report should be presented accurately, use clear and understandable language, and be consistent with the conclusions.

Cybercrime Categories
Cybercrimes can target individuals, property, governments, or organisations. Cyber bullying and harassment of individuals can take many forms, including email spoofing, stalking, hacking, credit card fraud, password sniffing, defamation, and cyber pornography, especially child pornography.

Data Espionage: The Illegal Acquiring of Information Computer systems often hold sensitive information. Cybercriminals can access this data remotely through various methods, such as social engineering, software that scans for open ports, and spoofing, where the imposter uses the victim's information without their consent. In particular, phishing involves sending unnecessary emails to corporate clients of different institutions in an effort to manipulate them into sharing sensitive information.
Internet, online banking, and e-payments have exposed end users to online crimes (Lavorgna and Sergi, 2014; Oruç and Tatar, 2017), which is a serious form of cybercrime that aims to obtain sensitive information (like passwords) by impersonating a trustworthy person or organisation (like a financial institution) in an official electronic contact.

Interference with System
There are similar issues with attacks on computer systems as there are with attacks on computer data. With the benefits of 24/7 availability and global accessibility, more and more companies are integrating Internet services into their manufacturing processes. If attackers are able to prevent computer systems from working properly, victims could incur substantial financial losses. Offenders can destroy

hardware by physically attacking the computer system. Financial losses from computer system attacks often exceed the cost of computer hardware for highly profitable e-commerce businesses. Examples of remote attacks on computer systems include denial-of-service (DoS) attacks and computer worms.

Worms on Computers

Computer worms, like viruses, are malicious programmes that replicate themselves and disrupt networks by launching multiple data-transfer processes. They can disrupt computer systems in various ways, such as by stealing system resources to copy themselves online or by creating so much network traffic that some services, like websites, become unavailable. While denial-of-service attacks target specific computers, worms typically impact the entire network without affecting any particular computers.

Attack on Service Denial

In 2000, several denial of service assaults were attempted against well-known companies like CNN, eBay, and Amazon. Similar assaults on government and commercial websites in the US and South Korea were reported in 2009. As a result, certain services were unavailable for several hours, if not days. A denial of service attack essentially prevents users from accessing computer resources, such as checking emails, reading the news, booking trips, or downloading files.

The Application of Digital Currency

Virtual payment systems and virtual currencies have emerged in response to the desire for anonymous payment systems. Since virtual currencies do not necessarily require authentication or identification, they provide a challenge for law enforcement agencies in their efforts to trace financial transactions. getting back to the offenders. It's hard to track down criminals who use anonymous currencies since it limits the ability of law enforcement to identify suspects through money transfers.

Infractions Concerning Copyrights

Companies use the Internet to spread information about their products and services. However, just like brick-and-mortar businesses, successful organisations may face piracy issues on the Internet. For example, counterfeiters may try to register a domain associated with a company's name by replicating its logo and products. Copyright breaches can be a legal problem for companies that distribute their products directly over the Internet. Their products can be downloaded, copied, and distributed.

Offences Relating to Trademarks

Copyright violations are associated with trademark violations, which are a significant aspect of international trade. The severity of trademark violations varies across national penal codes, but the most serious ones include using trademarks in criminal operations to deceive users and domain name-related offences. Trademarks and brand names are often used fraudulently in a variety of contexts, such as phishing, where millions of emails posing as legitimate organisations are sent to internet users, containing trademarks. Another problem with trademark violations is cyber squatting, the unlawful process of registering a domain name that is identical or confusingly similar to a product or company's trademark.

Computers Fraud

Online auction fraud and advanced fee fraud are two of the most common forms of computer-related fraud. Because of the ease with which fraudsters can hide their identities using automation and software tools, these criminals are able to make a tidy profit from relatively small offences. Moreover, they employ a strategy to make sure that each victim's financial loss is minimal, so victims of "little" losses are less likely to report and investigate the crime.

Fraud in Online Auctions

Because of the difficulties in distinguishing between real and fraudulent transactions, cybercriminals can take advantage of the anonymity of online auctions by preying on the fact that buyers and sellers do not physically interact.
One of the most prevalent types of cybercrime is auction fraud. The most common tactics used in this type of fraud are offering products that do not exist for sale and asking for payment before delivery. To combat this, auction houses have put safeguards in place like the feedback/comments system, where users can rate the reliability of sellers and buyers based on the feedback submitted after each transaction. However, criminals have found a way to circumvent this system by using third-party accounts. One such scam is the "account takeover" scam, in which criminals try to obtain the login credentials of legitimate users in order to buy or sell products fraudulently, making it harder to identify the culprits.

Premature Fraudulent Payment
In advance fee fraud, fraudsters contact victims via email, promising a share if they help them transfer large sums of money to a third party. The victims are then pressured to either provide their bank account details directly or send a small amount to verify their account. The victims are left with no contact from the criminals after they have transferred the funds, and the criminals may use the victims' bank account information for other fraudulent purposes. Thousands of victims fall for this

Forgery in the Computer Age
The forgery of digital documents is called computer-related forgeries. Examples of this type of crime include creating a paper that looks like it came from a reputable organisation, changing electronic photographs, or altering text documents. One tactic used in phishing is the fabrication of emails. In phishing, the goal is to get people to reveal sensitive information. For example, scammers will often send emails that look like they came from a reputable financial institution that the target us

Personal Data Theft
Identity theft is the unlawful acquisition and use of another person's personal identification information. With the proliferation of digital information, The rise of information societies has dramatically affected the incidence of identity theft. In the past, people relied on their "good name" and strong personal relationships to conduct business and go about their daily lives. However, with the advent of online shopping, face-to-face identification has become more difficult, making identity-related data crucial for people interacting in social and commercial contexts. Trust and security, which are non-face-to-face transaction needs, now rule the economy, and not just in e-commerce. One example is the use of PIN-enabled payment cards for grocery shopping.
There are three stages to the crime of identity theft. In the first stage, the criminal obtains information related to their identity. In the second stage, they interact with this information before using it for criminal purposes. In the third stage, they use the details of their identity for a criminal offence. Consequently, the criminals care more about their ability to use the data for illicit purposes than the data itself. Similar crimes include credit card fraud and the falsification of identification documents. Lastly, the criminals can use social engineering to trick victims into revealing personal information. Scammers have recently developed advanced social engineering tactics to manipulate consumers and steal confidential data.
Identity thieves target financial account information, including social security numbers, in order to commit financial cybercrime. Cybercriminals use various methods to steal people's bank information and money (Choo, 2011). An empirical study by Anderson et al. (2012) revealed that financial institutions like banks had suffered billions of dollars in losses globally. The study also provided details of direct and indirect losses, criminal revenue, and indirect costs as a result of cybercrime in the banking sector around the world. The type of information that perpetrators seek varies, but the most critical pieces of data are passwords, social security numbers, dates of birth, addresses, phone numbers, and social security numbers.

Online Fraud

Online banking services enable you to complete several international financial transactions swiftly. The Internet has helped reduce 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 up the cost of money laundering. Traditional money-laundering strategies still have advantages for larger quantities, but the Internet has sig

As a result, criminals are forced to come up with new strategies. In the fight against money laundering, the responsibility of the financial institutions involved in the transfer determines whether suspicious transactions can be identified. The three stages of money laundering—placing, layering, and integration—make the Internet particularly useful for offenders in the layering phase. Investigations into money laundering become even more complex when criminals use online casinos to stack their transactions. Regulators are currently lacking in their oversight of money transfers, and the Internet enables criminals to conduct cheap and tax-free cross-border money transactions.

Attacks on Financial Institutions via Cyberspace

Cyber risk is described as "operational risks to information and technology assets that have implications for information or information systems' confidentiality, availability, or integrity" (Cebula and Young) (2010). When it comes to insurance-covered risks, cyber risk is similar to property and liability risk as well as catastrophic and operational risk (Eling and Wirfs, 2016). Cyber-attacks can hurt businesses because they compromise the three main pillars of data security: availability, confidentiality, and integrity. When private information within a company is leaked to third parties, as in a data breach, it is considered a confidentiality issue. The misuse of systems is associated with integrity issues, such as fraud. Lastly, business disruptions are tied to availability difficulties (Bou).

Since financial institutions depend on their customers' trust, the risk of losing confidence due to cyber-attacks could be substantial. Business disruptions, on the other hand, are more likely to have direct short-term contagion effects on the financial system, affecting only the targeted firm in the short-term, as opposed to the longer-term consequences of data breaches, such as reputational damage and litigation costs (Bouveret, 2018).

Digital Forensics and Cybercrime Investigations

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 cyber infrastructures. 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.

Computer Forensics - Secure, Analyse, Present (CFSAP) by Macdermott et al. (2018) simplifies the four cornerstones of computer forensics—identification, preservation, analysis, and presentation—into three straightforward steps, in contrast to existing models that have been deemed either overly detailed (Reith et al., 2002), overly broad (Rogers, 2006), or overly complex (Selamat et al., 2008).

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.

Cybercrime is on the rise, affecting government systems, large organisations, small and medium businesses, eCommerce, online banking, and vital infrastructure. While the reasons behind cybercrime vary, the impact of financial attacks is significant compared to non-economic attacks. However, when it comes to the number of attempts or documented cases, the damage to one's reputation, financial loss, and ramifications on data confidence are far more significant.

The sheer variety of devices that can be used for criminal purposes, along with the sheer volume of devices that need to be identified, collected, and examined at a crime scene, presents a significant challenge from an investigative perspective. The technological sophistication and storage capacity of these devices vary. With the increase of cloud services, big storage devices, and smart devices in businesses, digital forensic investigations involving these systems will necessitate more intricate digital evidence collection and analysis (Taylor et al., 2010). As we establish standards for dealing with electronic or digital evidence, additional disciplines will emerge to assist investigators in this evolving landscape and ensure that they are well-versed in cybercrime regulations

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 surveyof 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. *20164th 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 spectrumof Italian criminal associations and their different attitudes in the financial crisis and in the useof 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. *ProcediaComputer 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.* AuerbachPublications.
- 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 ofE-Banking Services Consumers Interests. *The Amfiteatru Economic Journal*, 1228: pp. 388- 403.

