digital forensic

by J J

Submission date: 14-Oct-2021 03:59PM (UTC-0400)
Submission ID: 1674026499
File name: Digital_Forensic_and_cybercrime.docx (29.49K)
Word count: 3408
Character count: 19622

Digital Forensic as Cybercrime Prevention Approach

12
Student's Name

Institutional Affiliation

Course Code and Number

Instructor's Name

Date

Digital Forensic as Cybercrime Prevention Approach

Abstract

Following the invention and widespread use of computers, forensics has advanced significantly as an area of law. As a result of widespread computer use and technical innovation, a slew of new crimes have evolved, including cybercrime, which necessitates extensive investigation and information gathering. The emergence of digital forensics has resulted in the development of several stages to explain the various features of the evidence. The procedure consists of the following steps: identification, acquisition, analysis, and storage of data as a form of proof. The old forensic system, which incorporated actual data, was the most well-known of the forensic systems. But the system is gradually evolving into a more complex one that includes the acquisition of digital evidence from technological devices. This is a significant step forward. The gaps in data storage, protection, and employee qualities in terms of knowledge are just a few issues that digital forensics aims to addresses.

Keyword; Forensics, Crimes, Digital Forensic, Forensic system, technological devices

Cybercrime

Cybercrime or fraud is a crime that takes advantage of faults in large and complex information systems like the internet in order to commit crimes against the public. The fast rise of E-Commerce and the prevalent reliance on online services for social interactions and financial transactions has generated the new potentials for many sorts of criminal activities, including fraud, on a worldwide scale. As a results of rampant profits and low expenses, cybercrime is quickly becoming the most expensive kind of crime globally. Criminal conduct in the digital age

is becoming a great threat in large businesses as well as national intelligence departments all over the world. The practices must be deterred by the use of more secure systems and user education, as well as new legislation and enforcement tactics.

People's personal information and data security are violated by cybercrime practices, including malware, hacking, financial fraud, and medical fraud as well as other offenses against persons that involve revealing personal information and images without their consent or permission(Drew and Farrell, 2018). Malware, hacking, medical fraud, financial fraud, and other offenses against persons include revealing personal information and images without their consent or permission. For example, cyber harassment, cyberbullying, and cyberstalking are all forms of cyberbullying. Both legitimate and illicit players regard data as a commodity, both online and offline, and this is true for both (Kleijssen and Perri, 2017).

As a result, data has been a primary target for cybercriminals in recent years. Data also plays an important role in the commission of many cybercrimes, principally since data is not effectively safeguarded and can be gained illegally by means of unauthorized access. Accidental disclosure of information, publication of data, unauthorized access to a database, or exceeding the authorized access to a database have all resulted in data breaches. Data breaches have occurred as a result of lost or stolen encrypted flash drives and other organization storage devices- primarily a smartphone or laptop, data security, inadequate system, flawed system, accidental disclosure of information. Cybercrime has been a problem that has adversely affected large business organizations and national intelligence (Pereira, 2016). Therefore, new forms of crime have evolved due to technological advancements, necessitating the use of sophisticated technologies. The innovation, sometimes known as digital forensics, is a multistep procedure

aimed at solving internet-related crimes. However, this procedure has faced numerous problems, and the necessity to combine computers and forensics has proven to be effective.

Cybercrime Literature

To begin with, Drew and Farrell (2019) argue that the rise of new methods of cybercrime practices demonstrates the ineffectiveness of traditional methods of police response to such crimes, as well as the incompetence of traditional methods of crime prevention. In the twenty-first century, Sharma et al. (2019), underline that cybercrime is frequently done in collaboration, making cybercrime a severe problem for the entire world community. Various sorts of crime fall under the umbrella term "cybercrime," including internet gambling, cyber slander, email, viruses, financial crime, cyber-pornography, Inter and email, and data forgery. The practices pose a large threat to people as well as business organizations.

As a result, numerous organizations worldwide are continually working to combat cybercrime, including government agencies, police departments, the Bureau of Cybercrime, and other similar groups (Sharma et al., 2017). On the other hand Tsakalidis et al. (2019) point out that cybercrime is frequently confused with other technology-related offenses, such as cyberterrorism and cyberwarfare, contradicting other opinions. According to Boes & Leukfeldt, law enforcement agencies play a critical role in the fight against cybercrime since they have access to sophisticated technology. In the meantime, one of the tactics for combating this type of crime is the development of partnerships with private institutions, which formalizes cooperation between public authorities and other stakeholders in the fight against crime (Boes & Leukfeldt, 2017).

On the other hand, Donalds and Osei-Bryson, (2019) say that in order to achieve such cooperation, it is required to build a common understanding of cybercrime and a classification of the offenses included by this concept. At the same time, not only does the issue of general understanding of cybercrime continue to be relevant, but so does the problem of determining the metrics that are appropriate for the assessment by the competent authorities of the threat and harm posed by cybercrime, as well as the impact of cybercrime on national and human.

As Hosch Tsakalidis et., (2019) points out that technological advancement provide room to new criminal opportunities, but they do not automatically result to new sorts of crime. "For the sake of defense, it should be noted that cybercrimes are simply extensions of previously existing unique unlawful actions." In the words of Hosch Tsakalidis et al., (2019), cybercrime encompasses a wide variety of behaviors that include trafficking child pornography, committing fraud to trafficking child pornography, stealing identities, intellectual property and infringing on an individual's privacy. Levi, 2017 identifies software piracy as a serious challenge that the technology industry is currently dealing with. Kleijssen and Perri, (2017) added to the assertion by stating that piracy and intellectual property are among the most pressing problems of professionals. Along with the destruction and extension of cyberspace, two forms of accessing information dominated the mass market – piracy and streaming – and continue to do so now.

Cybercrime Solution

With the advancement of technology, digital forensics has become increasingly significant and well-known. Traditional forensics relied on tangible evidence such as hair to be collected and examined to discover criminal conduct. To the extent that it is applicable to the subject of law, forensic science can provide insight. For a long time, it was based on two frames:

direct individualization, such as classic fingerprint detection on the crime scene, and non-direct individualization, such as the use of paint as a form of evidence in criminal investigations. Digital forensics is the process of extracting data from digital devices and storing it in a digital format (Edmond et al., 2017). The word is extensively used in the context of gathering, identifying, and analyzing digital evidence obtained through the use of electronic devices.

Digital forensics and cybersecurity are inextricably linked; cybersecurity would be less effective if it did not have access to the information provided by digital forensics. When digital forensics discovers information via various cases, cybersecurity uses that information to devise ways to avoid digital forensic investigations from occurring in the future; cybersecurity is fundamentally preventative in nature (Patil and Meshram, 2016). In a similar vein, digital forensics exists as a result of failed or ineffective cybersecurity strategies. The ability to recognize both and understand how they are interconnected is critical to maintaining your information's privacy and security. Digital forensic benefits individuals and business organizations in the following ways.

Preventing Hackers and Hijackers from Stealing Sensitive Information

Because of the information discovered by digital forensics companies, they can design equipment that prohibits hackers from accessing networks, websites, and other devices in the first place. Hackers and hijackers are proficient at infiltrating a people or business's device or network. Besides, the forensics has congregated information that cyber security may use to prevent hackers from infiltrating a device or network in the first place. Cyber security software can detect and safeguard vital data based on trends discovered in how hackers and hijackers

steal, erase, or exploit information (Oparnica, 2016). Cyber security software can also continuously scan networks to ensure that no outside parties are present.

Prevention of Virus that Leads to Breaching of Sensitive Information

When it comes to digital forensics' impacts on cyber security, antivirus software is likely one of the most significant advantages. Digital forensics has discovered how viruses gain access to a device or network; often, a hacker will transmit an incorrect email or file to infect the device or network. As a result of this information, antivirus software may pay close attention to any emails or files that are being delivered. A similar approach can be used with software that has been generated from digital forensic material. This software can detect spyware and malware, and it can typically remove it before any information is exploited or erased.

Digital Forensic aid in Recovering Stolen Information

When it comes to digital investigations, commercial data breaches, or just the everyday life of a citizen whose identity has been stolen digitally, recovering lost information is critical to a successful outcome. When information is lost or corrupted, digital forensics recovers it using sophisticated tools and methodologies to present it in a legal proceeding. However, digital forensics has enabled cyber security to develop methods of recovering data if a person needs to do so, but there is no court case to do so. It is a branch of cyber security known as disaster recovery (Xiao et al., 2019). It is aimed to safeguard networks, notably those associated with a business, from being attacked by a cyber attacker. When a cyber assault occurs, disaster recovery (DR) plans are developed that include step-by-step techniques for restoring service to affected

networks. As a result, an emergency plan is already in place, and information will be kept in multiple networks and servers to make a recovery as simple as possible.

Digital forensic identify areas of vulnerability.

Since areas of weakness are never obvious, numerous cyber attackers can certainly access information, without encountering any difficulties. Digital forensic services assemble information that can be used to identify cyber security weaknesses in a network or website, as well as the locations of those weaknesses. Cyber security software can then be programmed to pay particular attention to and correct the areas of weakness or vulnerability identified. An area that is particularly prone to vulnerability and weakness is the password aspect of a network or a particular account (Philomin et al., 2020). Online hackers normally access devices by steering background research on a person or corporation and critically guess their password. It is important that any password does not contain any information that has a significant personal meaning, such as personal name. It is crucial to keep passwords secure in a business setting; this is especially true in the case of sensitive information. Digital forensic investigators have discovered that a major problem among business owners is that many employees have access to data and information that they do not need. It makes it possible for data breaches and cyber-attacks to take place within a company.

Gaps Addressed by Digital Forensic

- Compared to external auditors, digital forensic has the ability to reduce or even eliminate sample risk is the most significant benefit that forensic accountants have.

- Digital forensic aid in the comparison of relevant types of data from several systems or sources to present a more complete picture.
- It also makes it easy to have the capacity to quickly and readily trend pertinent data over long periods ((Oparnica, 2016). Major changes in trending lines can then be investigated further, to identify false positives and potential danger factors.
- The rapid detection and extraction of specific risk criteria from the full data population to conduct additional analysis.
- Tests are conducted to determine whether the control environment and policies in place are effective by detecting features that contradict the rules.
- The identification of trends that were previously unknown to company staff, consultants, and forensic accountants.

Digital Forensics Critics and Limitations

Despite the various positive impacts of digital forensics, it faces different critics based on its challenges and limitations. According to Asquith and Horsman, (2019) the digital forensics has technical issues that limit its effectiveness in the field of criminology. As technology progresses, so do crimes and criminals, who progress along with the technology. Forensic tools are used by digital forensic experts to collect evidence against criminals, while criminals use such tools to conceal, alter or remove evidence for crimes. In digital forensics, the process is known as the anti-forensics technique. It is a major limitation in the field of digital forensics. The various anti-forensics technics include data hiding in storage space as well as a covert channel. According to Patil and Meshram, (2016) criminals typically conceal large portions of data inside the storage medium in an indistinguishable format by utilizing system commands and software

tools to do this. On the other hand, a covert channel is a communication protocol that allows an attacker to circumvent intrusion detection systems and conceal data transmitted across a network connection. The attacker employed it in order to conceal the existence of a connection between himself and the hacked system.

Another critic is that digital forensic is limited due to resource challenges, including volume replications and changes in technology. As the rate of crime rises, the amount of data generated rises, and the task of analyzing such vast amounts of data falls on the shoulders of digital forensic experts. Because digital evidence is more sensitive than physical evidence, it is more likely to be lost than physical evidence. Forensic professionals employ various skills to verify the authenticity of data in order make the investigation process as efficient and effective as possible. However, dealing with these instruments is a task poses a challenge with the technique.

The rapid changes in technology such as application software, hardware and operating systems are making it more difficult to read digital evidence (Asquith and Horsman, 2019). This is because new version software's are not supported by older versions, and software developing companies have not provided any backward compatible's, which has implications for legal proceedings. Additionally, even though electronic documents are secure, their confidentiality, availability, and integrity are easily compromised. When the internet and wide-area of networks combined, they result to a large network that enable data to flow across physical borders. Because of the affluence with which information can be shared and the availability of electronic documents as well as the volume of data has increased, making it more difficult to identify original and pertinent information.

Implications

Based on the study, cybercrime is a crime that is increasing growing owing to the increased technological advancement. For several years, cybercrime has been on the rise. As more and more people conduct business and live their lives online, fraudsters are taking advantage of this growing trend to steal from people and businesses (Boes and Leukfeldt, 2017). You may anticipate hackers to be feeling the heat as a result of breakthroughs in cybersecurity, the development of best practices, security awareness initiatives, more regulation, and collaboration between businesses and the government to combat the problem. In an attempt to solve this problem, digital forensics can be used to address the increasing cybercrime practices. Government, business organizations, and individuals can utilize digital forensics to prevent hackers from stealing their sensitive information. The government can use digital forensics to protect national intelligence from getting into the hands of enemies.

Further, digital forensics can be used to recover stolen information from a suspected compromised system in the context of a digital forensic investigation. Digital forensic can be incorporated in criminal investigations when the nature of the intrusion is unclear, such as when a zero-day exploit is used, However, the root cause must be fully understood, either to ensure that the exploited vulnerability is properly remediated or to provide evidence to support a legal proceeding. Criminal investigations relating to cybercrime can incorporate digital forensic to aid in investigations. In certain cases, only a thorough and rigorous investigation will reveal the nature of an intrusion. The circumstances of the intrusion, such as those involving the theft of PII in jurisdictions where one or more data breach disclosure laws are in effect, may also necessitate the conduct of a forensic inquiry.

Conclusion

Cybercrime is a serious problem that is increasing every day. Malicious cyber activity endangers the safety of the general public as well as our national and economic security. Online hackers involve themselves in cybercrime to steal money and identities from victims that are not aware. The cyber thief can use other people's identities to: take out loans, accrue debt, incur credit, and leave without leaving a trace in the process. The process of rehabilitating one's own identity can take several years. In addition, a virus can destroy someone's files, and a lost database can result in receiving unwanted sales calls from third-party vendors. As a result, the formation of an organization's personnel is jeopardized. In an attempt to address the problem, digital forensics has evolved widely to safeguard important information. Forensics prevents hackers from accessing personal information from computers and smartphones. Moreover, digital forensic aid in recovering stolen information, preventing the virus to computers that leak information, and identifying vulnerability areas.

Nevertheless, Because of the broad breadth of digital forensics, the employment of numerous tools and methodologies and the differences in their methods of operation raises a slew of gaps and challenges for the resource and technical experts to contend with. Some of the most common challenges include luck of acquisition, a lack of appropriate strategies for the collection of information, rapid technological change, and the various ways of presenting of electronic evidence, big data, anti-forensic techniques by criminals, and free online tools for investigation and others. These challenges point to the need for new legislation and amendments to existing legislation and patches to existing technologies.

References

Asquith, A., & Horsman, G. (2019). Let the robots do it!–Taking a look at Robotic Process Automation and its potential application in digital forensics. *Forensic Science International: Reports*, *1*, 100007.

Edmond, G., Towler, A., Growns, B., Ribeiro, G., Found, B., White, D., ... & Martire, K. (2017). *Thinking forensics: Cognitive science for forensic practitioners. Science & Justice, 57(2), 144-154.*

Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. *?yber-Physical Security: Protecting Critical Infrastructure at the State and Local Level , 3*(1), 185-203.

Donalds, C., & Osei-Bryson, K.M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*(1), 403-418.

Drew, J.M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research , 19*(6), 537-549.

Kleijssen, J., & Perri, P. (2017). *Cybercrime, evidence and territoriality: Issues and options. In Netherlands Yearbook of International Law 2016 (pp. 147-173). TMC Asser Press, The Hague.*

Kavallieros, D., Chalanouli, C., Kokkinis, G., Panathanasiou, A., Lissaris, E., Leventakis, G., Giataganas, G., & Germanos, G. (2018). Searching for crime on the web: Legal and ethical perspectives. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security.*

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, and Law. Social Change, 67*(1), 3-20.

Oparnica, G. (2016*). Digital evidence and digital forensic education. Digital Evidence & Elec. Signature L. Rev., 13, 143.*

Patil, D. N., & Meshram, B. B. (2016). *Digital forensic analysis of ubuntu file system. Int. J. Cyber Secure. Digit. Forensics, 4(5), 175-186.*

Pereira, B. (2016). The fight against cybercrime: From the abundance of the standard has its perfectibility. *Revue Internationale de Droit Economique, 30*(3), 387-409.

Philomin, S., Singh, A., Ikuesan, A., & Venter, H. (2020). Digital forensic readiness framework for smart homes. In *International Conference on Cyber Warfare and Security* (pp. 627-XVIII). Academic Conferences International Limited.

Sharma, P., Doshi, D., & Prajapati, M.M. (2017). Cybercrime: Internal security threat. *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government.*

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers and Security, 29*(1), 45-72.

Xiao, J., Li, S., & Xu, Q. (2019). Video-based evidence analysis and extraction in digital forensic investigation. *IEEE Access*, *7*, 55432-55442.

digital forensic

ORIGINALITY REPORT

17%	9%	3%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.abacademies.org Internet Source	3%
2	Submitted to University of Westminster Student Paper	3%
3	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	2%
4	Submitted to University of Teesside Student Paper	1%
5	C DAY. "Intrusion Prevention and Detection Systems", Computer and Information Security Handbook, 2009 Publication	1%
6	www.unodc.org Internet Source	1%
7	unina.stidue.net Internet Source	1%
8	Submitted to University Tun Hussein Onn Malaysia Student Paper	1%

9	Submitted to University of Lancaster Student Paper	1 %
10	amp.itweb.co.za Internet Source	1 %
11	Submitted to University of Waikato Student Paper	<1 %
12	www.coursehero.com Internet Source	<1 %
13	www.crimrxiv.com Internet Source	<1 %
14	"Cybercrime in Context", Springer Science and Business Media LLC, 2021 Publication	<1 %
15	cradpdf.drdc-rddc.gc.ca Internet Source	<1 %
16	Christopher Day. "Intrusion Prevention and Detection Systems", Elsevier BV, 2013 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

digital forensic

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14