

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Student Details ( Student should fill the content)** | | | | | | | | | |
| Name | |  | | | | | | | |
| Student ID (UWIC ID and ICBT ID) | | Cardiff Met ID : | | | | ICBT ID : | | | |
| **Scheduled unit details** | | | | | | | | | |
| Unit code | | CIS 7028 | | | | | | | |
| Unit title | | **Information Security and Document Management** | | | | | | | |
| **Assignment Details** | | | | | | | | | |
| Nature of the Assessment | | REPORT | | | | | | | |
| Topic of the Case Study | | GIVEN | | | | | | | |
| Learning Outcomes covered | | YES | | | | | | | |
| Word count | | 4000 Words | | | | | | | |
| Due date / Time | | 21st March 2021 | | | | | | | |
| Extension granted? (For Office use only) | | Yes | No |  | | | |  | |
|  | |  |  |  | | | |  | |
| **Declaration** | | | | | | | | | |
| I certify that the attached material is my original work. No other person’s work or ideas have been used without acknowledgement. Except where I have clearly stated that I have used some of this material elsewhere, I have not presented it for examination / assessment in any other course or unit at this or any other institution | | | | | | | | | |
| Signature | |  | | | | | Date |  | |
| **Result (Assessor use only)** | | | | | | | | | |
| Marks by 1st Assessor |  | Name & Signature of the 1st Assessor | | |  | | | | **Agreed Mark** |
| Marks by IV: |  | Name & Signature of the IV | | |  | | | |
| **For Office use only (hard copy assignments)** | | | | | | | | | |
| Receipt date |  | Received by | | |  | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Assignment Type & Title:** | | | |
| **For student use: *Critical feedback on the individual progression towards achieving the assignment outcomes*** | | | |
|  | | | |
| **For 1st Assessor use: Assessment feedback** | | | |
| **Strengths**  **Weaknesses** | | | |
| **Name & Signature of the Assessor :** |  | **Date :** |  |
| **Comments by the IV** | | | |

**THE ROLE OF DIGITAL FORENSIC IN SOLVING CYBER-CRIMES**

**Content**

**Introduction**

**Justification for selecting the topic**

**Literature review and analysis**

**Discussion and conclusion**

**References**

**Introduction**

Digital forensics is the application of scientific investigation techniques to digital crimes. Digital crimes and attacks happen in cyberspace. Cyberspace is the non-physical environment where people communicate through computer networks with the aid of internetworking devices. Cybercrimes threaten the smooth flow inside cyberspace at many levels. Cybercrimes are criminal activities that involve computers or other digital devices and target individual computers, computer networks, or any other digital device connected to a computer network. Carried out by individuals or organizations, it can be in the form of viruses, malware, identity theft, hacking, phishing emails, child pornography, ransomware, spreading hate, criticism or false information, illegal content, drug smuggling, and attacks to confidential content as well. Once a cybercrime has occurred authorities start the investigation process to identify the attackers and recover the resources. Considering the inquiry processes of a cybercrime, extracting the most relevant data from devices subjected to a security threat is a very important step in an investigation. Digital forensics comes into being in this situation. Digital forensic is a branch of forensic science that mainly focuses on the matter of extracting and recovering of right material from devices related to cybercrimes. Digital forensics is defined as, Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user (Vacca, 2005).

**Justification for selecting the topic**

As much as forensic science is important to tackle the complexities of a criminal investigation in the physical world, digital forensics is important to track down the criminals behind cybercrimes. Digital forensics is the scientific methodology that aims at presenting illegal digital artifacts to the court of law as evidence. With that, law enforcement, security experts, and academics pay great attention to the development of digital forensic as a science and practice. Hence, when discussing information security management, digital forensics is an integral part of the subject and it is very interesting to learn the process of cybercrime investigations. By choosing the topic of "The role of digital forensic in solving cyber-crimes" we are hoping to gain in-depth knowledge about the digital forensic process and widen the knowledge of cybercrimes too. We firmly believe that this knowledge we obtain by researching on the chosen topic can be a great asset in the future as an information security management professional in the field.

**Literature review and analysis**

Digital forensic investigators need the development of a proper methodology for the analysis of digital devices to capture significant evidence of a cybercrime. There are many models of investigation used by commercial and public services authorities. The fact that many digital forensic investigation models exist is a result of the dynamic and varied nature of cybercrimes occur in the context. Over the years it has not been possible to suggest one general model that fits all types of cybercrimes investigations. Various digital forensic methodologies have been developed over the years, some of which are extensions to previous models and some are original methods as well.

The first model of such was formed in 1995(Pollitt, 2007) which had four phases in total. The steps were Acquisition, Identification, Evaluation and Admission. This model guaranteed the legally admissible and scientifically reliable evidence in a court of law at the investigation. Notably, this approach is missing the preparation and dissemination stages of an investigation process compared to models that were later invented (Rahayu et al., 2008). In 2001 a non-profit volunteer organization, Digital Forensics Research Workshop (DFRWS) proposed a generic model that can be applied to most of the investigation processes. It has six phases namely, Identification, Preservation, Collection, Examination, Analysis and Presentation. DFRWS is considered to be the first large-scale consortium led by academia rather than law enforcement (Clint et al., 2002). Before that different law enforcement authorities defined processes for digital forensic investigation. In 2001, the United States Department of Justice published a model which comprises of four phases: Collection, Examination, Analysis and Reporting(Abdalla et al., 2007). This model has focused on abstracting the model from specific technologies and methodologies hence it is better at identifying core aspects of the investigation process. Also, it minimizes the distinction between computers and other electronic devices and attempts to build a more generalized process. Inspired by the 2001 DFRWS model, in 2002 abstract digital forensics model (ADFM) was proposed (Yusoff et al., 2011) which comprises nine phases namely, Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning Evidence. This was an extension of the DFRWS model and has three additional phases than DFRWS. This model is considered a more generic one with the capability of using various types of digital devices. In 2003 the Integrated Digital Investigation Process (IDIP) was invented(Carrier & Spafford, 2003) which has five major steps and each has its sub-steps as well. IDIP intended to integrate the various available processes into one combined model. The phases of IDIP are Readiness, Deployment, Physical Crime, Investigation, Review and Digital Crime Investigation. Based on IDIP in 2004, the Enhanced Digital Investigation Process Model (EDIP) was proposed with one specific phase called "Traceback" allowing the investigators to trace back to find the actual devices used for the crime. Stemming from their early models there have been many models proposed throughout the time. Considering that there does not exist a model that can assist a legal procedure of an investigation and that is generic and can be applied in different breach of trust situations, (Montasari et al., 2019) proposed the novel Standardised Digital Forensic Investigation Process Model (SDFIPM) in 2019. SDFIPM is reportedly the most recent methodology developed and documented in the area of forensic research. The usability of methodologies is mostly the focus of digital forensic researches yet the selection of the right tools and technologies is as important as choosing the right methodology for an inspection procedure.

Evidence of cybercrime can exist in different forms. Therefore, a forensic investigation includes examining network activity, file systems, peripheral devices, emails, etc. Until the 1990's most of the investigations carried out by examining the devices subjected to the crime with no or fewer tools in usage (Flandrin et al., 2014). Since the technologies of hardware and software developed to more complex levels, such analysis procedures were inefficient. The technological experts began developing tools to extract and examine evidence without harming the original data. These tools are used for different purposes; disk analysis, file analysis, data capture, network analysis, mobile device forensics, registry analysis, cloud forensics, audio/video analysis, artificial intelligence forensics, etc. Some tools can perform multiple of these jobs which introduces a trend in digital forensic tools development, to produce wrappers that encompass hundreds of technologies and different functionalities into one tool. Digital forensic tools can be hardware or software. Hardware tools are mostly for storage device investigations. Such as hard driver duplicators or write blockers, are used to preserve the original evidence intact while the storage evidence is examined separately. Software tools are often multi-purpose and got the ability to be adjusted by programmers suitable for the incident being investigated. Forensic tools are used in disk image acquisition and analysis processes. These tools are used to retrieve hidden content, recover deleted content, report generating, recovering geographical locations, extracting logs, perform registry analysis, crack passwords of storage devices, etc. Apart from generic all-purpose tools, there is a need for tools that are specific to certain operating systems. And some operating systems have built-in support for forensic investigations such as Kaali Linux-BackTrack, CAINE Linux and Gentoo Linux-Pentoo (Offensive Security, 2013). Among the vast range of these technologies, choosing the right tool for the job is also challenging.

Following are some criteria that can be considered while selecting a digital forensic/cybersecurity tool.

Level of expertise: The level of skill and knowledge requires to use the tool is important and specific to the investigator. Some tools need basic skills while some need expert knowledge and skills. Therefore, assessing one's skills before the investigation will help to select the most powerful tool needed for the job.

The output of the tool: Some tools return raw data while some tools return reports or processed data. Depending on the tool the output varies. Hence, when choosing the tool, it is necessary to consider the type of output the tool will return and the job that is needed to be performed.

Cost: In the context of cybersecurity-related technology there are commercial tools as well as open-source tools. Since a digital forensic investigation has cost concerns as selecting the tool suitable to the budget is important. Finding the most suitable tool involves considering the trade-off between cost and features the tool offers.

Functionality: Some tools are used for database investigations while some are for network activity investigations. The functionality of tools varies in great degrees and some tools might be able to perform multiple tasks as well. Hence, when selecting a tool, it is needed to consider the focus of a tool regarding the task we need to perform.

Peripheral devices: While some tools can perform the job alone some need additional devices to complete the task. With budget constraints and the level of expertise available, it is needed to consider the possibility of using additional tools.

Despite all the tools, technologies, and methodologies used, cybercriminals and attackers are always in search of ways to breach the security of the internet. The practice of ubiquitous computing, cloud computing, the internet of things (IoT), the rise of social media platforms and related services, advancements in artificial intelligence technologies have inspired the attackers to find new ways of cybercrimes. Cloud computing is immensely popular at present due to the vast number of services it provides. The cloud platform is considered as a cost-effective platform that offers services such as software as a service (SaaS), platform as a service (PaaS), security as a service (SECaaS), database as a service (DBaaS) and integration as a service (IaaS). It also has private, public and hybrid models. Cloud is mostly famous among companies for its high scalability, support for business continuity and automatic updates. However, before using this technology, users consider the increasing number of cybercrimes in the cloud platforms as a challenge to their businesses. Cloud forensics is the sub-section of network forensics where the crimes that occur in cloud platforms are handled. Security analysts concern with cloud forensic as a challenge due to several reasons. Unlike traditional forensics, where the investigator has full access to crime scenes and devices, the devices and processes of the cloud environment are out of reach and distributed among several places geographically and virtually. The fact that big data is deficient to handle and the lack of existing tools and technologies specific to the cloud are the major concerns of authorities. The investigator has to rely on the cloud service provider to carry out the investigations. Since SaaS is software offered as a service, users get to access the software from a web browser. PaaS is a platform of development tools, operating systems, middleware, etc. where customers can rely on to build applications on top of that. Therefore, SaaS and PaaS both fall short in process monitoring and network monitoring from the perspective of the cloud consumer. Besides all the challenges, cloud forensics has become a prominent trend among forensic investigators in digital forensics due to the ability to use distributed processing, computing power, and scalability of the cloud for the use of inquiring processes.

The invention and development of social media platforms have influenced the daily activities of people around the world by making such platforms one of the main sources of socialization. A humongous amount of data is daily posted and published with little to no concern of how they can affect the security of the social and private lives. Among this information are sensitive personal data as well. This lets the attackers use these platforms to extract confidential data and exploit them in their favor. The attacks can be the denial of service (DoS), distributed denial of service (DDoS), or retrieving cookies data attack. Even though these social media platforms ensure the data is encrypted, there are an ample number of vulnerabilities exists due to users’ lack of knowledge in technical aspects behind the scene. Hence, the term social media forensics is also a hot topic among digital forensic investigators. Social media forensics is about retrieving electronic evidence from social networking platforms and, analyzing and preserving the information to present in the court of laws. Due to the vast amount of information present in social networks, it is easy to trace back the evidence but as much as the potential it has, there are also a considerable number of challenges posed by smartphones. As smartphones are quickly getting updated evidence tends to get erased faster. The frequent release of OSs for smartphones has become a challenge to investigators as the tools and technologies for forensic investigations are not that sophisticated and updated.

With the advancement in embedded systems and network technologies, the Internet of Things (IoT) has entered human lives and making it upgraded and updated as never before.

IoT is a network of many interconnected digital objects embedded with software or sensors

to achieve a common goal and share data, services, or instructions to offer services to humans and devices. (Mahmoud et al., 2015). It is a system where devices can interconnect with each other and with humans to perform tasks and share information with humans and other applications. Starting from the 1990s the number of devices that are connected has been increasing in leaps and bounds. According to Gartner report (Hung, 2017) by 2020, the number of interconnected devices was 20 billion. Some practical applications of IoT include wearables, traffic monitoring, smart homes, smart cities, fleet management, smart farms, smart grid and energy savings, and many more. One thing that is specific to IoT is seamless connectivity and massive data transfer which along brings massive data breaches and cybersecurity threats. IoT forensics is a branch of digital forensics that investigates devices, sensors, and data stored in various platforms connected and subjected to cybercrimes. Smart TVs, smartphones, tablets, wearables, smart appliances, smart speakers, Smart meters, toys, laptops, personal computers, and commercial security systems are some of the devices that are part of IoT-related applications. Connecting traditionally dumb devices with limited computational resources and memory, to an intelligent network raised several questions related to security and privacy. IoT forensics is multifaceted and more complex than traditional digital forensics as it involves a varied range of devices. No methodology can be used broadly in the investigation process. Hence, the challenges in IoT forensics are different from other forensic investigations. The variance of the IoT devices in question, data preserved in multiple devices, proprietary hardware and software within the IoT devices are the major challenges of such. IoT forensics is considered a combination of cloud forensics, digital device forensics, and network forensics (Alenezi et al., 2019). Along with their unique challenges of the three areas IoT forensics has unique challenges due to its novelty and lack of forensic tools.

Considering all the trends and applications mentioned above, it is evident that digital forensic tools, technologies, and methodologies play a crucial role in cybercrime investigations. The usual procedure in an investigation is to follow a common workflow and use a known methodology. Cybercriminals are aware of these methodologies and tools used in an investigation. So, they have invented and use anti-forensic methodologies to mislead the investigations. Use of encryption, onion routing, obfuscation, spoofing, tunneling, and steganography to destruct, hide or hamper evidence and eliminating the sources of the evidence is the most common such anti-forensic techniques used by attackers. Recently, anti-forensics have caught the attention of researchers and is considered a growing area of study. Still, the knowledge obtained by researchers is insufficient to develop techniques to fight against anti-forensics (Alenezi et al., 2019). So, the governments and private sectors must come together and share the experience and plans to develop this subject area furthermore.

**Discussion and conclusion**

The findings of the literature review have established that the area of digital forensic studies has been growing and the related tools and technologies are expanding. Yet many challenges and threats need to be discussed and classified. The most prominent challenge digital forensics faces are the huge and fast growth of technologies related to internet security. Big data, encryption algorithms and techniques, and the existence of various forensic tools are the main challenges in digital forensics at present (Alghamdi, 2020). The development of encryption services and techniques has made the encryption algorithms more complex. Hence backtracking and conducting cryptanalysis has become difficult. Cryptography also helps the attackers to hide their identity in crimes. And this makes the investigators' job harder and slower. Distributed data management techniques have lowered access and control over digital evidence of cybercrimes. The challenges in digital forensics can be of two types, operational and personnel challenges. Operational challenges are in the form of detection, prevention and incident response. While the on-site infrastructure of a company makes it easier to manage intrusion detection, data loss prevention and incident management, a company based on a cloud platform faces challenges in all these areas due to distributed nature of resources.

The lack of universal standards to assess the digital forensic processes is another operation challenge that needs attention. Without a standard, various criminal cases are analyzed in different methodologies and which makes it harder to find a proper way of legally responding to situations around the globe. Lack of well-trained staff is the major concern related to personnel challenges. The shortage of well-trained forensic investigators is mainly because digital forensic needs tech-savvy professionals with good analytical skills and certified qualifications to deliver valid proofs to the court of law (Alghamdi, 2020). Along with challenges, some opportunities can be identified within the tools and technologies discussed in the literature review section to make the digital forensic process easier, safe, and efficient. Intrusion detection systems (IDS) are one of such. IDS can detect intrusion attempts, policy violations, or any malicious activity of that sort. (Alghamdi, 2020). Hence IDSs are excellent tools for digital forensic investigators to reveal security breaches in systems. There are some prominent advantages of IDS for forensic investigations which can be used as opportunities to aid the process of forensic investigation. With an efficient IDS, forensic investigators can determine what type of attack has happened as it can detect unauthorized data access, malicious network activities, and security breaches in general separately. IDS can activate the incident response in a problematic situation. It helps to gather and preserve live intrusion data that can later help in forensic analysis.

As mentioned in the literature review, the humongous amount of data being preserved and produced every day has become a challenge to digital forensic investigations. The traditional methods of analyzing data are inefficient in the context of big data. The role of artificial intelligence (AI) comes to attention at this point. With the limited resources and time constraints, digital forensic processes are unable to produce useful output in a realistic time frame. With aid of Machine Learning and other big data-related processing, digital forensics can tackle most of such problems in a realistic time frame. In addition to that AI brings the capability of systems to conduct investigations before (preventive) and after (reactive) the attacker break in using machine learning and pattern recognition-related knowledge.

Analyzing all the facts and points mentioned above, it can be seen that the methodologies, tools, and techniques used in digital forensics to combat the battle against cyber-crimes have developed and are expected to expand more in the future. Alongside the development of digital forensic technologies, attackers have become more aware of the area of digital forensic analysis processes and are inventing various anti-forensic methods to fight against the security of the systems. With the expansion of knowledge in computer science and the increased awareness of security breaches more and more novel approaches such as AI are adopted into the science of digital forensics with aim of designing globally accepted methodology for conducting investigation processes. To understand the role of digital forensics in solving cyber-crimes, this report has discussed the different methodologies, tools, recent trends, challenges, and opportunities for the growth of the subject comprehensively.

**References**

Abdalla, S., Hazem, S., & Hashem, S. (2007). *Guideline Model for Digital Forensic Investigation*. 23.

Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., & Wills, G. (2019, May 2). *IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions*. https://doi.org/10.5220/0007905401060115

Alghamdi, M. I. (2020). Digital forensics in cyber security—Recent trends, threats, and opportunities. *Periodicals of Engineering and Natural Sciences (PEN)*, *8*(3), 1321–1330. https://doi.org/10.21533/pen.v8i3.1463

Carrier, B. D., & Spafford, E. (2003). Getting Physical with the Digital Investigation Process. *Int. J. Digit. EVid.*

Clint, M. R., Reith, M., Carr, C., & Gunsch, G. (2002). *An Examination of Digital Forensic Models*.

Flandrin, F., Buchanan, W., Macfarlane, R., Ramsay, B., & Smales, A. (2014, September 1). *Evaluating Digital Forensic Tools (DFTs)*. https://doi.org/10.13140/2.1.3293.6004

Hung, M. (2017). *Gartner Insights on How to Lead in a Connected World*. 29.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 336–341. https://doi.org/10.1109/ICITST.2015.7412116

Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). *The Standardised Digital Forensic Investigation Process Model (SDFIPM)* (pp. 169–209). https://doi.org/10.1007/978-3-030-11289-9\_8

Offensive Security. (2013). *Kali Linux Has Been Released! | Offensive Security*. https://www.offensive-security.com/kali-linux/kali-linux-released/

Rahayu, S., Robiah, Y., & Sahib, S. (2008). *Mapping Process of Digital Forensic Investigation Framework*. *8*.

Vacca, J. R. (2005). *Computer forensics: Computer crime scene investigation* (2nd ed). Charles River Media.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science & Information Technology (IJCSIT)*, *3*. https://doi.org/10.5121/ijcsit.2011.3302