

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Student Details ( Student should fill the content)** | | | | | | | | | | | |
| Name | | | | |  | | | | | | |
| Batch number | | | | | Intake 17 | | | | | | |
| Student ID | | | | | Cardiff Met ID :20188240 | | | | | ICBT ID :**CL/MSCIT/17/35** | |
| **Scheduled unit details** | | | | | | | | | | | |
| Unit code | | | **CIS 7028** | | | | | | | | |
| Unit title | | | **Information Security Management - Assignment** | | | | | | | | |
| **Assignment Details** | | | | | | | | | | | |
| Nature of the Assessment | | | | | | Report | | | | | |
| Topic of the Case Study | | | | | |  | | | | | |
| Learning Outcomes covered | | | | | |  | | | | | |
| Word count | | | | | | 800 | | | | | |
| Due date / Time | | | | | | **07th March 2021** | | | | | |
| **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 |  | | | Rp POP eceived by | | |  | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name |  | | | | |
| Batch Number | Intake 17 | | | | |
| Student ID | Cardiff Met ID :20188240 | | ICBT ID :**CL/MSCIT/17/35** | | |
| **Assignment Type & Title:** | | | | | |
| **For student use: *Critical feedback on the individual progression towards achieving the assignment outcomes*** | | | | | |
|  | | | | | |
| **For 1st Assessor use: Assessment feedback** | | | | | |
|  | | | | | |
| **Name & Signature of the Assessor :** | |  | | **Date :** |  |
| **Comments by the IV** | | | | | |

**Topic: The role of digital forensic in solving cyber-crimes**

**Introduction**

With the inventions and advancements of technology related to computer science and networking, digitization of businesses and services has increased in both public and private sectors. In addition, individuals have also become dependent on internet and related technologies for most of the day-to-day activities. While we cannot question the positive impacts of digitization on human lives, the dark side of cyberspace security has also expanded in leaps and bounds. Cybersecurity Ventures, the leading cyber security magazine and a trusted source for cybersecurity facts and statistics, expects cybercrimes to make a damage of $6 trillion to world economy by 2021(Morgan, 2021). It is also mentioned that the frequency of cyber-attacks will increase to 1 per 11 seconds in the year of 2021. With such increase of cyber-criminal activities, the demand for investigations and jurisdiction procedures has also become a major concern of governments and organizations. Cyberspace, cybercrimes and digital forensics are the main considerations related to this field and hence will be defined in the following further more.

**Background of the study**

Cyberspace is described as an infinite artificial world where humans navigate in information-based space (Benedikt, 1992). It is the non-physical environment where people communicate through computer networks with the aid of other peripheral devices like internet connectivity adapters, processors and controllers. Cybercrimes are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT) (Mcguire & Dowling, 2013). 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. There are attacks that are targeted on devices and networks as well as individual humans behind the devices. The targeted attacks are mostly carried out to extract information from individuals or a single source while un-targeted attacks are carried out to harm many devices, services and individuals. Attackers could be of different types. Hacker groups, scammers, religious or political groups, amateur script writers and advanced persistent threat agents are different types of such attackers.

As a response to these threats, number of precautionary measures have been taken in different levels. Anti-malware is one of such programs to combat the battel against software-based malware and viruses. Even though these anti-malware products are successful in performing their job, malware is only a one way of cybercrimes. Upgrading the rules and legislations should also be a major part of this battle as the speed of technological advancement is exceeding the pace of upgrades in jurisdiction systems. Considering the inquiry processes, extracting the most relevant data from devices subjected to a security threat is a very important step in an investigation of a cybercrime. Digital forensic is a branch of forensic science mainly focuses on this matter of extracting and recovering of right material from devices related to cybercrimes. Digital forensics can be simply defined as the process of identifying, uncovering, preserving, retrieving and analysing of digital evidences using scientifically proven methods, tools and formulas that facilitate the reconstruction and retrieval of these digital evidences in a way that ensures the admissibility of the retrieved evidence in the court of law; which imposes the existence of a computer based or cyberspace-based crime scene and the needed technical investigation skillset (Harbawi & Varol, 2016).

As much as forensic science is important to tackle the complexities of a criminal investigation in physical world, digital forensics is important to track down the criminals behind cybercrimes. Hence, when discussing about information security management, digital forensics is an integral part of the subject and furthermore it is very interesting to learn the process of cybercrime investigations. By choosing the topis of “The role of digital forensic in solving cyber-crimes” we are hoping to gain an 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 future as an information security management professional in the field.

**Outline of the final report**

This report discusses the role of digital forensics in solving cybercrimes in a well-organized manner dividing the report into subsections describing different aspects of the subject areas comprehensively. In order to consider the interconnection between digital forensics and cybercrimes the introduction section includes the definitions of cyberspace, cybercrime, digital forensics and a background information of these subject areas. The following paragraph describes cybercrimes, what they are, the different types and characteristic traits of cybercrimes as well. The overall process of digital forensics needs to be studied to understand how a cybercrime investigation is carried out. Therefore, the report comprises a superficial description of digital forensic process step by step. The technological advancements and tools used in digital forensics and cybercrime investigations will be discussed in the following sections of the report. In the pragmatic usage, due to dynamic and volatile nature of internetworking technologies digital forensic faces multiple challenges combating the cybercrimes. The next section aims to provide a detailed explanation of such obstructions which could hinder the performance of the tools, technologies and processes related to digital forensic discussed above. Following up, the coordination, interconnection and the roleplay of digital forensic in cybercrime investigation is briefly considered as the conclusion the of the study.

**References**

Benedikt, M. (Ed.). (1992). *Cyberspace: First Steps* (New edition). The MIT Press.

Harbawi, M., & Varol, A. (2016). *The role of digital forensics in combating cybercrimes*. 138–142. https://doi.org/10.1109/ISDFS.2016.7473532

Mcguire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence Research Report 75 Chapter 1: Cyber-dependent crimes*. Undefined. /paper/Cyber-crime%3A-A-review-of-the-evidence-Research-75-Mcguire-Dowling/5e089b9bac3cdba577724cf0cd23f648a4f952d9

Morgan, S. (2021). *CYBERCRIME FACTS AND STATISTICS*. 19.