Assignment: 9-19-2022

1. **What is digital forensics?**

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.

The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances.

2. **Why there is a need for digital forensic services?**

Digital Forensic services are often a critical component for the court of law cases that require analysis to understand how certain technology was used for malicious acts. Not only is it used as evidence but also as basis for improvement of digital security moving forward.

3. **Where does the ESI commonly store?**

ESI, electronically stored information, can be stored and accessed in many ways and places. We can store this information in physical devices such as hard drives, company servers, and the like. Another way can be through the cloud where information is stored at an offsite location.

4. **What are some circumstances in which digital forensics are applied or needed?**

One situation would be in a business setting to investigate policy or legal violations by an employee, contractor, or an outsider, and to investigate attacks on a physical or information asset.

5. **Specify some examples in order for you to be a properly trained, digital forensic examiner.**

Build your skillset in digital forensics. Having the technical skill to perform in this field is quite essential and to develop these skills must be your top priority. It is important to have adequate knowledge about operating systems, storage devices, cryptography, data privacy, critical thinking and most importantly, cryptography. Not only being aware of these concepts and also having the practice allows you to develop the necessary skills.

If you are confident enough, then take a step forward towards getting certification – these certifications not only boost your capabilities as a digital forensic examiner but also authenticates your expertise in the field. A lot of these certifications are listed and a short brief explanation is provided in question 10.

6. **What does digital forensic examination provide?**

A digital footprint is information about a person on a system, such as the websites they have visited, when they were active, and what device they were using. This information is provided through a digital forensic analysis. The detective will find the information necessary to crack the case by tracking the digital traces. It also offers information on passwords, deleted files, and the

origin of security breaches. After being gathered, the evidence is then archived and translated so that it can be presented in court or for further investigation by the police.

7. **What is the difference between digital forensics and data recovery?**

Digital forensics and data recovery are often used synonymously. However, these are two distinct concepts. The main distinctions between digital forensics and data recovery are the goal of the recovery and the intended use of the recovered data.

Data forensics is the analysis of digital data to find evidence of crimes, and it may be done on any type of computer system, including mobile devices. Data recovery is the process of removing damaged or lost contents from a storage device with the intention of restoring their usability.

8. **What should I do if I think evidence exists on a computer or other electronic media?**

These are protocols that I need to follow. First, I would gather information regarding the situation. I would prevent any further usage of the electronic device until evidence has been collected. I would then store this evidence securely and make sure it is not tampered with. If I am deemed unable to handle such evidence, to contact a computer forensic specialist would be my next move.

9. **What types of legal cases typically work? Do you specialize in a particular category, like white-collar crime or sexual offenses?**

Any major criminal investigation including rape, stalking, child abuse or exploitation, forgery, extortion, gambling, piracy, or terrorism may involve the use of digital evidence. Electronic crime, sometimes known as e-crime, such as child pornography or credit card fraud is frequently linked to digital proof. However, not just e-crime is increasingly prosecuted using digital evidence; other forms of crimes as well, if not all.

10. **Define and briefly explain the following**
    - **CISSP (Certified Information Systems Professional)**

is an independent information security certification granted by the International Information System Security Certification Consortium. Acquiring such a certificate is a big feat in a professional's life as it is awarded to individuals that prove they have what it takes to effectively design, implement, and manage a top-notch cybersecurity program.

    - **MCSE (Microsoft Certified Solutions Expert)**

focuses on the ability to design and build technology solutions, which may include integrating multiple technology products and span multiple versions of a single technology, whether on-premises or in the cloud. This validates that you have the skills needed to move your company to the cloud, increase user productivity and flexibility, reduce data loss, and improve data security for your organization.

    - **CEH (Certified Ethical Hacker)**

is a qualification given by EC-Council and obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system**.**

- **CFCE (Certified Forensic Computer Examiner)**

is a certification offered by the EC-Council that can be earned by proving one's understanding of evaluating the security of computer systems by searching for flaws and vulnerabilities in target systems while using the same skills and tools as a malicious hacker to evaluate the security posture of a target system.

- **CEECS (Certified Electronic Evidence Collection Specialist)**

was the first certification demonstrating competency in computer forensics. It is one of the most widely recognized non-tool certifications in computer forensics for current and former law enforcement personnel. This certification proves that one has adequate information on the proper procedures in detection, collection, documentation and preservation of all aspects of evidence.

- **CHFI (Computer Hacking Forensic Investigator)**

is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. This proves that one is knowledgeable and competent in the process of detecting hacking attacks and properly extracting evidence and prosecute cybercriminals.

- **CCFE (Certified Computer Forensics Examiner)**

program is designed to train Cyber Crime and Fraud Investigators whereby students are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation.

- **Ence (encase Certified Examiner)**

This program certifies professionals in the public and private sectors in using Opentext EnCase Forensic. Professionals who hold an EnCE certification have mastered computer investigation techniques and the usage of EnCase software during difficult computer tests. EnCE certification shows that an investigator is a competent computer examiner and is recognized by both the law enforcement and corporate worlds as a mark of in-depth understanding of computer forensics.

**11. What are the possible risks if one doesn’t consult a computer forensics expert at the start of an event?**

Delaying contact with a computer forensics professional raises the likelihood that the evidence be altered. The evidence is more likely to be lost the longer it is utilized since the operating system randomly overwrites data on the hard disk. As a result, delaying the hiring of a digital forensics expert corrupts sensitive and personal files in addition to destroying evidence. The best action to

do at the beginning of the incident is to take a picture of the computer to gather evidence away from the compromised device.

**12. If the evidence exists, is it okay for an in-house technology expert before calling on outside experts?**

When trying to find the perpetrators of a cybercrime, businesses may unintentionally delete evidence. You only get one shot to acquire the evidence you'll need to back up your assertion. They tamper with the evidence when Human Resources sends in IT personnel who are not familiar with reliable forensic procedures. Even while the internal IT team is quite knowledgeable about their working environment and the technologies used there, computer forensic investigations are best performed by outside experienced individuals. Due to the very nature of the forensic analysis process, the need to preserve evidence, and the strict chain-of-custody rules enforced by courts, computer forensic investigations must be carried out by outside organizations with authorized forensic technology and trained to adhere to forensic protocols.

Most internal IT professionals are concerned about recovering from catastrophic data loss and mission-critical data. In the collection and storage of data that the operating system has rendered invisible, they lack specialized understanding. Even the most well-intentioned technology expert risks damaging sensitive data stored on a computer if the operating system does not recognize it. Even the simple act of turning on the computer or scrolling through files can corrupt the data you're looking for. System dates can be changed, data can be overwritten, and evidence can be tampered with. The bottom line is that in-house technology experts should only perform such under the condition that outside experts are out of reach or as a last resort.

**13. What makes a collection procedure forensically sound?**

Without altering the data or its metadata, forensically sound data collection is the process of collecting data for eDiscovery. To be deemed forensically sound, a data collection technique must be defendable, which means consistent, repeatable, and well-documented. With a forensically sound data collecting approach, a thorough explanation of each step taken in gathering electronically stored data should be provided. It should be necessary to authenticate the process or provide proof that the data collected was used by the litigant and was not changed from its original state. The entire data collection procedure must be precise and explainable for the data to hold up under scrutiny in a court of law.

**14. What are the proper procedures if you think that the organization’s computer contains important evidence?**

A thorough, well-thought-out plan for gathering evidence is a crucial aspect of a successful computer forensic investigation. There must be extensive documentation before, during, and after the acquisition process; particular information, such as all hardware and software specifications, any systems employed in the investigation process, and the systems under investigation, must be recorded and archived. Policies pertaining to maintaining the integrity of prospective evidence are particularly applicable at this stage.

The removal of storage devices physically, the use of controlled boot discs to retrieve sensitive data and guarantee operation, and following the proper measures to copy and transfer evidence to the investigator's system are all general criteria for evidence preservation. Evidence gathering must be done in a planned and legal manner. Given the intricacy of most cybersecurity

investigations, it is very important for computer forensics to be able to establish and validate the chain of evidence while pursuing a legal case.

### 15. What is the process of a typical digital forensic examination?

**Identification**: The first step identifies prospective sources of pertinent data and evidence (devices), as well as important data custodians and their locations.

**Preservation** is the process of protecting a crime or incident scene, taking pictures of the area, and recording all pertinent details about the evidence and how it was obtained in order to preserve pertinent electronically stored information (ESI).

**Collection** is the act of gathering digital data that might be important to the investigation. Removal of the electronic device(s) from the crime or incident scene and subsequent imaging, copying, or printing of the contents are examples of collection.

**Analysis** is the thorough, methodical examination of all available information about the occurrence under investigation. The results of the investigation are data items discovered in the information gathered; they could be user- and system-generated files. The goal of analysis is to reach conclusions about the evidence.

**Reporting**: first, reports are based on tried-and-true methods, and second, other qualified forensic investigators ought to be able to replicate the same findings.

### 16. When should I consider using computer forensics?

Results can be obtained using computer forensics in both civil and criminal cases generally. Employee internet abuse, computer misuse, computer-related fraud, data theft, industrial espionage, purposeful disclosure of company data, damage assessment and containment following a computer hack (incident response), and any cybercriminal activity in which a computer, tablet, or mobile phone has been used are examples of what it can cover.

### 17. Can anybody recover my lost data?

You may be able to recover lost data from a hard drive damage by removing the hard drive from the computer and connecting it to another computer to see if any files are not damaged. If the hard drive is entirely corrupted, you can try to retrieve data using data recovery software.

Lost data is just data that the file management system cannot locate in its storage. It is hardly ever “lost forever” or deleted forever unless you clear it from the recycle bin. Even in this stage, file recovery services can still recover data.

### 18. Can data be recovered from SMS applications?

Yes, it is possible. There are multiple recovery apps that help you recover information in SMS applications but then again, you are placing your information into the hands of 3rd party companies. Messages from these applications can be recovered as long as they have not been overwritten.

**19. What are the procedures to do if you were hacked?**

- If they haven't already been compromised, change your passwords right away.
- If you notice anything strange, alert your family and people you can trust.
- If you notice any strange expenditure, get in touch with your bank for assistance.
- Contact digital forensic examiners if anything escalates further.

**20. What are the proper ways to achieve a more secure password?**

- Never use your password to access personal information.
- Make your passwords longer
- Steer clear of using the same passwords across other accounts.
- Include both uppercase and lowercase characters, numbers, and symbols.
- To make it easier to remember complex passwords, try using a passphrase.

**21. I am not a big target, why should I be concerned with security?**

Hackers don't necessarily always choose their targets. The vast majority of cyber-attacks affect everyday people or even small businesses not because they are high-value targets, but because they are easy to attack. Security, no matter who you are, is a vital aspect of any system – especially in the digital world. Remember, your personal information, intellectual property, critical business data, and even reputation is at stake when don't assure yourself the protection you need online.

**22. Is it possible to recover data from a hard drive that has been damaged?**

It actually depends on the situation. Yes, files can be recovered from a failed/corrupted hard drive by using a skilled data recovery service. There are multiple recovery software available but you are putting your responsibility unto a 3rd party service. If the hard drive is logically damaged, there is a chance that data can be recovered using Disk Management Utility available on Operating Systems. However, if your system cannot detect the hard drive then this makes the situation more complicated and therefore, it would be difficult to recover data from it.

**23. Can blockchain be hacked?**

One might think that blockchain technology is virtually impossible to hack. That may have been the case a few years ago when it was first introduced to the world. That is no longer the case. Lately, hackers have been getting away with billions worth of cryptocurrency by attacking unique vulnerabilities of blockchains.

Phishing and Malware attacks make up the majority of blockchain hacks which take advantage of gullible targets. End users, when uneducated and don't take security seriously, are the main sources of weakness for blockchain technology.

There is a unique attack on blockchain called 51% attack which is an attack on a blockchain by a group of miners who control more than 50% of the network's mining hash rate. Attackers with majority network control can interrupt the recording of new blocks by preventing other miners from completing blocks.

24. **What can I do in order to prevent being hacked?**

There are multiple ways to prevent yourself from being hacked - a combination of these methods would prove to be ideal. First way to protect your online account is to set up a unique password (this should be standard). Second, setup two-factor authentication on your account so you have the ability to prove you are trying to login.

Another way is to never open links that redirect you to a website (especially on emails). Always visit the website by typing it into the address bar. Lastly, would be very ideal, to create your own file and store your information there – then you encrypt your login information for safekeeping (that is if you are willing to learn encryption).

**25. I just found a USB lying around outside my office, is it okay to insert it into my computer?**

My advice is do not insert the USB into any computing device. Don’t even bother picking it up because that is a great and easy way to get hacked. You take a chance of getting malware into your computer when this USB drive is plugged in. Cybercriminals often leave USB sticks lying around for malicious purposes.