1. Write at least one page summary of the history and evolution of computer forensics

Computer forensics is a new profession involving the convergence of digital evidence and the law. There is a process of identifying, preserving, and analysing data and technological elements for the purpose of using as the evidence in court. Computer forensic scientist analyse the data from personal computers, laptops, cell phones, servers, tapes, digital assistants along with the other types of media available.

As most experts say, the computer forensic field began to develop more than 30 years ago. In United States, law enforcement and military investigators were the first to notice criminals more technical. The government experts were responsible in response to suspected security breaches. The experts were responsible to protect important, private, and certainly confidential information have conducted forensic examinations to not only to investigate a specific breach that were possible. But to understand and analyse so that they could be able to prevent future violations. Information security on the other hand focuses on data and asset protection. We can see that computer forensics and Information security have come together.

The computer forensic filed hyped up in the following decades and it is still a hot topic to this day. At the local state, and federal levels, there is a strong presence of information security and computer forensics in military and law enforcements. Both private and public companies have followed the trend, hiring in-house computer forensic and information security experts. In substitute, contracting those experts or departments as needed. We can also see that, private sector has only recently recognised the need for computer forensics testing in civil legal disputes, leading to the eDiscovery boom.

The field of computer forensics is seen expanding day by day. The forensic agencies, private investigators and boutique companies are all accumulating experience and knowledge in this field. We can see powerful and newer software tools and solutions being developed by the software companies. In addition, law enforcement and the military continue to identify and further educate their members in responding to technology-related crime.

Computer forensics arose because of several factors, the most important of which is that computers are everywhere. Nowadays, finding a home without at least one computer is extremely difficult. Investigators who work in computer forensics deal with more than simply computers. Computer forensics investigates a variety of technological devices. Observe how many individuals are talking on the phone, using iPods, PDAs, and texting while you stroll down the street. Computer forensic professionals examine all these electronic devices.

1. Find 3 recent examples of crimes where a computer is used to commit a crime (last 2 years)

A criminal activity that either targets or uses a computer, a computer network or a networked device can be called as cybercrime. In 2020, 4.2 billion dollars losses were recorded. Examples:

* After an alleged ransomware attack on its IT systems, parts of the UK website of Brazilian-owned cosmetics and beauty company Avon remain unavailable after more than a week. The attack is believed to have harmed the back-end systems used by the company's well-known sales reps in nations other than the United Kingdom, including Poland and Romania, which are currently operational. People have been unable to place orders with the company as a result of this. On June 9, 2020, Avon notified the US Securities and Exchange Commission (SEC) of the breach, stating that it had experienced a "cyber event" in its IT environment, which had disrupted systems and impacted operations.
* According to a study by the litigation firm Griffin Law, customers of Lloyds Bank are being targeted by a sophisticated phishing scam. Approximately 100 Lloyds Bank clients have reported receiving forged correspondence purporting to be from Lloyds, one of England and Wales' largest banks. The cyber attackers used the bank's official logo and branding to send these malicious communications to consumers in the form of SMS texts or emails, notifying them that their bank account had been hijacked. The email scam is seemingly legitimate and uses Lloyds branding with the subject header: “Alert: Document Report – We noted about security maintenance.”

The message, which has spelled errors and some Chinese characters, claims that the recipient’s bank account has been compromised, stating:

“Your Account Banking has been disabled, due to recent activities on your account, we placed a temporary suspension until you verify your account.”

* Cyber Gangster Demand Payment from Travelex after Sodinokibi attack foreign exchange company Travelex is facing demands for payment to decrypt critical computer files after it was hit by one of the most sophisticated ransomware attacks, known as Sodinokibi, which disabled its IT systems on New Year’s Eve.

1. Find 3 recent examples of crimes where a computer is the victim of a crime or an attack. (Last 2 years)

* According to persons familiar with the incident, CNA Financial Corp., one of the largest insurance companies in the United States, paid $40 million in late March to restore control of its network following a ransomware attack. According to two people involved with the incident who asked not to be identified because they weren't authorized to discuss the matter publicly, the Chicago-based business paid the hackers roughly two weeks after a wealth of company data was taken and CNA officials were locked out of their network. A CNA representative stated the corporation followed the law in a statement.
* In March 2021, London-based Harris Federation suffered a ransomware attack and forced the "temporary" disabling of the devices and messaging systems of all 50 secondary and elementary academies. level it operates. As a result, more than 37,000 students were unable to access their courses and correspondence.
* On Sunday night, a cyber-attack on Nine Entertainment's North Sydney offices, which halted publishing and broadcasting at the country's largest media firm, remained unresolved, raising fears that its consequences could last for day. Channel Nine's capacity to broadcast from its Sydney studios was hampered by the ransomware assault, which forced the company to relocate its operations to Melbourne.

1. Briefly describe the triad that makes up computer security.

The CIA triad represents the functions of your information system. Your information systems include both your computer systems and your data. The CIA security triad is comprised of three functions:

• Confidentiality. A system’s ability to ensure that only the correct, authorized user/system/resource can view, access, change, or otherwise use data.

* Integrity. A system’s ability to ensure that the system and information is accurate and correct.
* Availability. A system’s ability to ensure that systems, information, and services are available the vast majority of time

Secrecy, in the insecure definition, is the ability to keep anything hidden. We can hang drapes or hang curtains on windows in the actual world. We can enlist the help of a friend to keep it a secret. Technology and privacy go hand in hand. At the level of personal use, where we utilize VPN or encryption to protect our privacy, this can play out differently. We may turn off appliances in our homes that are always listening. However, privacy is compromised in corporate security when an unauthorized individual can access, obtain, and/or edit your files.

Because your company needs to protect its competitive advantage, or intangible assets that make it stand out from the competitors, confidentiality is crucial

Integrity in computer systems refers to the accuracy and validity of the system's output. This is known as data dependability in the data world. Can you rely on the outcomes of your data and computer system? Integrity is a function that you want to protect when securing an information system. You don't want bad actors or human mistake to jeopardize the integrity of your computer systems and your bottom line, whether intentionally or unintentionally. Because your company needs to protect its competitive advantage, or intangible assets that make it stand out from the competitors, confidentiality is crucial.

The term "availability" is commonly used in the IT industry to refer to the availability of resources to support your services. In terms of security, availability denotes that the appropriate personnel have access to your data systems. It will not be available if a user with privileged access does not have access to his dedicated computer. Because it can be hacked, availability is a major security concern. An attack on your availability can prevent users from accessing some or all of your services, leaving you to clean up the mess and manage downtime on your own.

1. Briefly describe the main characteristics of public-sector investigations

There are two distinct characteristics: Public and private. The characteristics of public sector are:

* Public investigations usually involve criminal cases and government agencies; private or corporate investigations, however, deal with private companies, nonlaw-enforcement government agencies, and lawyers.
* They must observe legal guidelines such as Article 8 in the Charter of Rights of Canada, the Criminal Procedures Act of the Republic of Namibia, and U.S. Fourth Amendment issues related to search and seizure rules.
* These agencies range from local, county, and state or provincial police departments to federal regulatory enforcement agencies.
* Public investigations involve government agencies responsible for criminal investigations and prosecution.

1. Briefly describe the main characteristics of private-sector investigations

* They rely on a more automated, software approach to the business rather than a singular scientific focus of solving one or a few legal cases.
* They are usually conducted in the civilian sphere cases, a civil case may escalate into a criminal case and a criminal case may be reduced to a civil case. If you follow good forensic procedures, evidence is found during your investigation can easily switch between civil and criminal cases.
* In the private sector, consulting firms seek to help victims and solve cases just as public sector investigators do, but they also create forensic tools for their clients and provide support services when needed