1a. Phishing is an instance where fraudulent mails, text and phone calls are sent to users in order to trick them into sending confidential information such as passwords and credit card numbers.

b.Hacking is breaking into a system or computer to have unauthorized access into the computer systems so that they can manipulate and disrupt operations .

c. Malware attacks is basically when malicious software such as viruses are created mainly to disrupt or damage a computer system.

d. Cyber stalking is when someone uses the internet to harass an individual . This involves sending or spreading false messages across about an individual or the stalker can send harmful messages to someone.

e. Identity theft involves the acts of using someone else’s personal information to be engage in fraudulent acts without the person’s knowledge.

2a. There are several repercussions that can arise from computer crimes that directly affect the forensic processes that are the focus. Forensic investigators deal with issues including important data encryption, digital evidence tampering, and the introduction of malware to change or destroy data as criminals become more skilled in their methods. Investigations may be hampered by these actions, making it more challenging for forensic specialists to locate relevant data, pinpoint the offenders, and guarantee the accuracy of digital evidence.

b. Computer crimes can jeopardize digital data integrity, which makes it difficult for forensic specialists to thoroughly examine and evaluate the evidence. Cybercriminals may conceal their activity using complex strategies, which makes it challenging for forensic tools to find and analyze the evidence. The accuracy and dependability of forensic investigators’ conclusions must be ensured, and they must constantly update their methods and instruments to keep ahead of cyber dangers.

c.The integrity and validity of the information may be difficult to maintain due to cybercriminals’ attempts to change or remove data, modify evidence that has been stored. Tight security controls and procedures need to be in place to prevent unauthorized access and tampering with the evidence repository in order to address these risks. To guarantee the dependability and credibility of the forensic evidence kept in these repositories, access limits, encryption, and routine backups are essential.

3.First and foremost you need to begin with chain case study. This is mainly about keeping a precise record of each piece of evidence to ensure integrity.

Also you need to make sure that the investigation going on complies with all legal standards.

Moreover it is very essential that you create an accurate documentation. This means you should keep a record of all proceedings, results, conclusion and all findings.

Finally the evidence obtained should be kept safe. This will help the investigation to be very credible.