Question 1: Explain the fundamental concept of digital forensics and its role in cybersecurity and law enforcement. How does digital forensics assist in investigating and analyzing digital evidence, and what types of incidents or crimes can it help address?

Answer: The fundamental concept of digital forensics is the practice of collecting evidence from computer systems to a standard that will be accepted in a court of law. Forensics investigations are most likely to be launched against crimes arising from insider threats, notably fraud or misuse of equipment, such as downloading or storing obscene material.

Question 2: Discuss the importance of preserving the integrity of digital evidence in the field of digital forensics. What procedures and best practices should digital forensic investigators follow to ensure that evidence is admissible in legal proceedings and remains untampered with?

Answer: This is a very important topic because the integrity of digital evidence, regarding digital forensics and investigations is of the upmost importance. If there is any altering to data during an investigation, a criminal could be found innocent when the crime has been committed and vice versa. There are several procedures that need to take place. Once the target disk has been safely attached to the forensics workstation, data, acquisitions are as follows: 1. Cryptographic has of the disk 2. Bit-by-bit copy 3. Second hash. 4. Copy is made. Preservation of media, the host devices and media are taken from the scene of the crime and should be labeled, bagged, and sealed, using tamper-evident bags.