1.A forensic image of a suspect’s laptop is taken at the scene. Later, this image is transferred to a secure forensic lab for analysis. What steps should be taken to properly maintain the chain of custody of this evidence, and why is this process critical in digital investigations?

2.Hackers attempt to shut down a city’s power grid by infecting its servers with malware. The attack threatens public safety and national security.Under which section of the IT Act would this act fall? , Suggest two ways law enforcement agencies could respond to such a situation.

3.(A)Investigators arrive at a crime scene where a server is currently running critical applications. Turning it off might result in loss of volatile data.Explain whether you would perform live system forensics or dead system forensics in this case, and why.

(B)Once the evidence is collected, how would you use hashing techniques to ensure that the data remains unaltered during the investigation?

4.An employee of a bank leaks customers’ credit card details to a hacker group. Many customers suffer financial losses.Which provision of the IT Act deals with this violation? What kind of compensation or penalty could be imposed on the bank?

5. During a cybercrime investigation, you find an external hard drive connected to the suspect’s workstation. You also notice multiple USB drives lying on the desk.Explain how you would document this scene and these items to ensure that the evidence can later be presented in court. Provide at least two types of documentation you would create.

6.You are part of a digital forensics team called to investigate a suspected insider attack at a corporate office. Several computers may contain evidence of data theft.Describe the first three steps you would take upon arriving at the scene to ensure that evidence is preserved and not contaminated.

7. A person creates a fake job portal and tricks hundreds of job seekers into paying a registration fee online. Later, the website vanishes, and the money is stolen.Identify which section of the IT Act, 2000 applies here. What punishment can the offender face?