Unit 1:

1. Data recovery is distinct from computer forensics. Make the same argument.
2. What are the computer security triad aspects
3. What is the purpose of maintaining professional conduct ? -
4. Are company policies different from warning banners? Justify and How are warning banners different for guests over the employees? -15
5. Explain the different digital forensics aspects of the case ? -pg 13
6. Briefly explain the possible circumstances in an corporate setup - pg 17
7. Explain the legal aspects of criminal investigation ? pg 12
8. Discuss are the approaches in assessment of any investigation ? pg 30-31
9. What are the specific steps in gathering evidence ? pg 33
10. Explain
    i. The steps to perform while gathering evidence - pg 46
    ii. What are essential for configuring a forensic workstation? Pg 45
11. Define
    1. the prerequisites for internet abuse investigation,
    2. procedure for email abuse
    3. And guidelines for media leak investigation,
    4. The parameters to be considered for industrial investigation
12. What is the purpose of maintaining professional conduct ? (19)
13. What are the specific steps in gathering evidence ? pg 33
14. What is the purpose of maintaining professional conduct ?
15. While conducting an investigation
    i. how do you acquire and store the evidence (46)
    ii. Required configurations for a forensic workstation? Pg 45
16. How do you analyse your evidence using Pro Discover ? (51)
17. For employee termination cases, what types of investigations do you typically encounter?

Unit 2:

1. Define :– Bit stream image, MBR,cluster, police blotter
    a. search warrant, VCN, ZBR,Litigation
    b. search and seizure, RAM slack and file slack.
2. For a typical 1TB HDD with 512 bytes of sectors, and considering it has 255 heads and 63 sectors per track, How do you calculate the number of cylinders on the disk drive ?
3. Explain the unique features of NTFS and FAT ?
4. Explain MFT and its attributes. MS DOS startup tasks ?
5. Explain the organization of Windows Registry ?

2,3,4,5,9

6. cs1: In 2014, **Sony Pictures Entertainment** suffered a devastating hack that resulted in the leak of **confidential company data.** This data were **publicly released** by a group calling themselves "Guardians of Peace." The leaks included embarrassing personal emails between Sony executives, private film scripts, and sensitive company information
7. As an investigation officer, briefly describe the steps on how would you go ahead with the case // Email investigation
8. Explain the organization of Windows Registry ?
9. Explain MFT and what are the functions of a data run's field components in an MFT record?
10. Explain NTFS in detail

Unit 3

1) Cs2: Ahead of the release of **Season 3 of "The Witcher"**, spoilers about key plot points were leaked online. This leak involved unauthorized disclosure of details about major plot twists, character deaths, and the direction of the story. As an investigation officer, briefly describe the steps on how would you go ahead with the case ? // internet or media abuse
2) Differentiate live imaging and dead imaging along with four methods of data acquisition methods ?
3) How do you update a Windows registry for a USB device
4) List the digital evidence storage formats ? (100), What are two advantages and disadvantages of the raw format?
5) Steps involved in updating windows registry (106)
6) Explain on how would you, Capturing an Image of a suspect drive using FTK imager (124)
7) Briefly explain RAID, and what are two concerns when acquiring data from a RAID server?
8) How do you validate your data acquisition (126)
9) How do you perform, ProDiscover and Runtime Software acquire data remotely over a network ? (139)
10) Explain lossy and lossless compression ? (104)
11) What is the most critical aspect of computer evidence?

Unit 4:

1. Explain the two hashing algorithms commonly used for forensic purposes.
2. Explain the following: (May or may not get the same, refer to the summary and keywords at the end of the chapter for every unit)

i. keyed hash set,
ii. non keyed hash set,
iii. limiting phrase
iv. plain view doctrine
v. sniffing

3. When you are processing the evidence, list out the steps to create image files
4. Why are technical advisors important ? Also mention their responsibilities towards any investigation?
5. List out the steps involved while processing a crime scene
6. Brief out the steps involved in a computer search and seizure
7. The general tasks you perform in any computer forensics case
8. Remote Acquisitions tools

Unit 5:

1) basic steps for all computer forensics investigations
2) Using FTK for search and report functions.
3) Explain a few Data-Hiding Techniques
4) Brief note on **Bit-Shifting, Using Steganography** Data-Hiding Techniques
5) How do you perform a remote acquisition using HDHOST and DiskExplorer ?
6) Analyse and briefly explain the most critical aspects of computer forensics
7) Comment, Under what all purposes can you use steganography?
8) A drive you're investigating contains several password-protected files and other files with headers that don't match the extension. Write a report describing the procedures you need to follow to retrieve the evidence. Identify the mismatched file headers to extensions and discuss techniques you can apply to recover passwords from the protected files.
9) Write your analysis on Bitmap and Raster Images ?
   Understanding Bitmap and Raster Images
10) Differentiate between Lossless and Lossy Compression
   Lossless and Lossy Compression
11) Repairing Damaged Headers
12) Using Steganalysis Tools
13) Copyright laws don't apply to Web sites.Comment ?
14) You're investigating a case involving an employee who's allegedly sending inappropriate photos via e-mail in attachments that have been compressed with a zip utility. As you examine the employee's hard disk, you find a file named Orkty.zip, which you suspect is a graphics file.
When you try to open the file in an image viewer, a message is displayed indicating that the file is corrupt.
Write a report explaining how to recover Orkty.zip for further investigation.

15) Remote Acquisitions with Runtime Software
16) Email header and email analysis
17) To retrieve an Outlook email header
18) Virtual machine forensics