Absolutely — here is a complete viva preparation package for Cyber Forensics & Investigation, with orally answerable, clear, confident, crisp explanations (not too long, not too short).

This will prepare you 100% for viva.

I will cover:

✔ Top 60 Viva Questions & Answers (Unit-wise + mixed)

✔ Practical/Tool-based Viva Q&A

✔ Scenario-based Viva Q&A

✔ Short definitions (very important)

✔ Tricky questions examiners often ask

🌟

FULL VIVA PREPARATION – CYBER FORENSICS & INVESTIGATION

🔵

SECTION 1 – BASIC & CORE VIVA QUESTIONS

1. What is Digital Forensics?

Digital forensics is the scientific process of identifying, collecting, preserving, analyzing, and presenting digital evidence that can be used in court or investigations.

---

2. What are the main goals of digital forensics?

- Preserve evidence
- Recover hidden/deleted data
- Reconstruct events
- Identify attacker or suspect
- Support legal proceedings

---

3. What are the phases of digital forensic investigation?

1. Identification
2. Preservation
3. Acquisition
4. Examination
5. Analysis
6. Reporting
7. Presentation (Court)

---

4. What is chain of custody? Why important?

Chain of custody is the documented record of evidence handling from seizure to court.

It proves evidence was not altered and ensures legal admissibility.

---

5. What is the difference between public-sector and private-sector investigations?

- Public sector: crime-based, requires warrants, police handle it.
- Private sector: corporate cases, HR violations, no warrants needed.

---

6. What is a forensic image?

A sector-by-sector, bit-by-bit exact copy of a digital device created without modifying the original.

---

7. Which formats are used for forensic images?

- RAW (.dd)
- E01 (EnCase)
- AFF (Advanced Forensic Format)

---

8. What is evidence hashing?

Hashing creates a digital fingerprint (MD5/SHA-256) of data.

If original and copy match → evidence is unchanged.

🔵

SECTION 2 – DATA ACQUISITION VIVA QUESTIONS

9. What is data acquisition?

The process of safely copying digital evidence without modifying the original.

10. What is live acquisition?

Collecting data from a running computer (RAM, active connections, encryption keys).

11. What is dead (static) acquisition?

Collecting evidence after powering off the system, typically using write blockers.

12. When do we use live acquisition?

- When system is ON
- When encryption is enabled
- When RAM evidence is required
- Ongoing attacks

13. What is a write blocker?

A device/software that prevents any write operation to the evidence disk.

14. Name data acquisition tools.

FTK Imager, EnCase Imager, dd, dc3dd, X-Ways, Cellebrite.

15. What is RAID acquisition?

Acquiring evidence stored across multiple disks in RAID.

Requires imaging all disks and reconstructing array.

🔵

SECTION 3 – CRIME SCENE PROCESSING VIVA QUESTIONS

16. What is digital evidence?

Any data stored or transmitted in digital form with legal value.

---

17. What is the first step at a digital crime scene?

Secure and isolate the device; prevent remote access.

---

18. Why do we photograph the scene?

To document the original state of evidence before touching anything.

---

19. What is covert surveillance?

Secret monitoring using spyware, keyloggers, or hidden cameras.

---

20. How do you store digital evidence?

- Evidence bag
- Tamper-proof seal

- Labeled
- Stored in secure evidence locker

🔵

SECTION 4 – FORENSIC TOOLS VIVA QUESTIONS

21. What is FTK Imager used for?

Creating forensic images, previewing files, extracting RAM.

---

22. What is EnCase Imager?

A forensic acquisition tool generating E01 images with metadata.

---

23. What are hardware forensic tools?

Write blockers, forensic duplicators, imaging docks, PC-3000.

---

24. What is file carving?

Recovering files based on headers/footers without file system metadata.

---

25. What is signature-based recovery?

Recovering deleted images using magic numbers (JPEG FF D8 FF).

---

26. What is thumbnail recovery?

Recovering small preview images stored in thumbcache even after deletion.

🔵

SECTION 5 – ANALYSIS & VALIDATION VIVA QUESTIONS

27. What is forensic validation?

Ensuring evidence and analysis are accurate using hashes, repeatability, and cross-tool verification.

---

28. What is steganography?

Hiding data inside media like images or audio.

---

29. What is metadata?

Information describing a file: timestamps, EXIF data, author, GPS.

---

30. What are data-hiding techniques?

Steganography, encryption, obfuscation, ADS, hidden partitions.

---

31. What is EXIF data?

Metadata in images containing camera model, GPS, date/time.

---

32. What is timeline analysis?

Arranging events chronologically to understand sequence of activities.

🔵

SECTION 6 – VM & NETWORK FORENSICS VIVA QUESTIONS

33. What is VM forensics?

Analyzing virtual machine artifacts like VMDK, snapshots, logs, memory dumps.

---

34. Why criminals use VMs?

Easy to erase, multiple identities, portable, isolated from host.

---

35. What is network forensics?

Capturing and analyzing network traffic for evidence.

---

36. Name network forensic tools.

Wireshark, tcpdump, NetworkMiner.

---

37. What is a live network capture?

Real-time packet capture of network traffic.

🔵

SECTION 7 – EMAIL & SOCIAL MEDIA FORENSICS VIVA QUESTIONS

38. What evidence do we recover from emails?

Headers, timestamps, IP addresses, attachments, routing info.

39. What is email header analysis?

Examining “Received From” fields to trace sender, path, and authenticity.

40. What tools are used for email recovery?

Magnet AXIOM, MailXaminer, FTK.

🔵

SECTION 8 – REPORTING & COURTROOM VIVA QUESTIONS

41. What is a forensic report?

A formal document presenting findings, tools used, evidence, and conclusions.

---

42. What are qualities of a good forensic report?

Clear, objective, reproducible, structured, legally sound.

---

43. What is a fact witness?

Describes what they saw/did during investigation.

---

44. What is an expert witness?

Provides opinions based on forensic expertise.

---

45. What is cross-examination?

Opposing lawyer questions you to test credibility.

---

46. What is deposition?

A pre-trial statement under oath, without court judge.

---

47. How should you answer in viva/court?

Calmly, clearly, factually — no assumptions.

🔵

SECTION 9 – SCENARIO-BASED VIVA QUESTIONS

48. System is ON and logged into banking portal. What do you do?

Perform live acquisition → capture RAM, network connections, session info.

---

49. Suspect HDD is encrypted. What acquisition is used?

Live acquisition to capture encryption keys from RAM.

---

50. A photo is deleted. How to recover?

Use signature-based carving or thumbnail extraction.

---

51. A company network is under attack. What to collect first?

Volatile data → RAM, network traffic, active sessions.

---

52. USB was connected to suspect PC. How do you confirm?

Check Windows registry entries:

USBSTOR, MountedDevices.

🔵

SECTION 10 – SUPER SHORT DEFINITIONS (VERY IMPORTANT)

These are asked in almost every viva:

53. Digital Evidence

Data with legal value.

54. Hashing

Creating a unique fingerprint of data.

55. Forensic Imaging

Exact copy of digital evidence.

56. Volatile Data

Data lost after power off.

57. Non-Volatile Data

Permanent storage data.

58. Write Blocker

Prevents writing to evidence.

59. Steganography

Hiding data in media.

60. ADS (Alternate Data Streams)

Hidden NTFS file streams.

🌟

Want COMPLETE VIVA MASTER LIST (150+ Q&A)?

I can prepare:

✔ All Units combined viva booklet (PDF style)

✔ Only tough viva questions

✔ Only definitions viva

✔ Only tool-based viva (FTK, EnCase, X-Ways)

✔ Rapid-fire Q&A for oral exam

Just tell me what format you want!