60612100– Kiberxavfsizlik injiniringi ta’lim yo‘nalishi 4-bosqich talabalari uchun Raqamli kriminalistika asoslari fanidan yakuniy nazorat savollari(Ingliz tili guruhi uchun)

1. Explain the concept of digital forensics in detail, including its main objectives, tasks, and its role in modern information security.

2. Describe the stages of digital evidence collection and analyze potential errors at each stage along with ways to prevent them.

3. Classify types of digital crimes and explain the methodologies used to investigate them with examples.

4. Analyze the main learning objectives of a digital forensics course and the competencies developed through it.

5. Explain methods for preserving digital evidence and ensuring its integrity.

6. Describe the key tools and methods used in forensic analysis within the Windows operating system.

7. Explain key concepts in digital forensics such as chain of custody, hashing, and imaging with examples.

8. Analyze the advantages and disadvantages of conducting forensic investigations in a CLI environment.

9. Categorize modern digital forensic tools and compare their functionalities.

10. Explain the structure of Linux file systems and how they are analyzed in digital forensics.

11. Describe forensic imaging methods and explain their importance in evidence collection.

12. Explain the methods and algorithms used in graphic file recovery.

13. Explain the features of the macOS file system (APFS) and its importance in forensic investigations.

14. Describe the stages of digital forensic analysis and examination in detail.

15. Explain the role of log files in detecting digital crimes and methods for analyzing them.

16. Analyze the specific characteristics and challenges of performing forensic analysis in virtual machines.

17. Explain the process of live data acquisition and justify its importance.

18. Describe the concept of network forensics and the tools used in this field.

19. Explain the process of email forensics, including key artifacts and investigation methods.

20. Analyze investigation techniques used in social media and their legal implications.

21. Describe the concept of mobile device forensics and the main tools used.

22. Explain the challenges and specific characteristics of conducting forensics on IoT devices.

23. Describe the main challenges and solutions in cloud forensics.

24. Explain the structure and requirements of writing digital forensic reports.

25. Analyze the role and responsibilities of an expert witness in digital investigations.

26. Discuss ethical and legal issues in digital forensics.

27. Explain the process of presenting digital evidence in court step by step.

28. Explain the general digital forensics process model (identification, preservation, analysis, presentation).

29. Describe the importance of Windows Registry analysis and methods for examining registry data.

30. Compare disk forensics and memory forensics.

31. Explain the concept of file system metadata and its role in digital forensics.

32. Analyze the process of deleted file recovery and its technical challenges.

33. Compare the capabilities of digital forensic tools such as Autopsy, FTK, and EnCase.

34. Explain how network packet analysis (pcap) can be used to detect cybercrimes.

35. Describe the role of tools like Wireshark in digital forensics.

36. Explain the importance of log and traffic analysis in detecting network attacks.

37. Explain mobile device file systems (Android/iOS) and methods for their forensic analysis.

38. Describe the process of recovering and analyzing SIM card and mobile application data.

39. Analyze the role of mobile devices in digital crimes with examples.

40. Explain the challenges of collecting and preserving data in cloud forensics.

41. Describe methods for identifying and recovering evidence in virtual environments.

42. Analyze the advantages and disadvantages of automated digital forensic tools.

43. Explain steganography and its significance in digital forensics.

44. Describe forensic analysis of multimedia files (images, videos, audio).

45. Explain methods for detecting image and video manipulation.

46. Analyze the relationship between incident response and digital forensics.

47. Explain the concept of timeline analysis in digital investigations.

48. Describe anti-forensics techniques and countermeasures.

49. Compare disk imaging and cloning techniques in digital forensics.

50. Explain the role and working principles of hash functions in forensics.

51. Describe the challenges of performing forensic analysis on RAID systems.

52. Explain how Windows Event Logs can be analyzed to detect cybercrimes.

53. Describe methods for analyzing registry and system artifacts.

54. Explain how forensic investigations can be conducted using CLI tools.

55. Explain how email header analysis can be used to identify the source of a message.

56. Analyze the role of social engineering in digital crimes.

57. Describe methods for monitoring and analyzing internet traffic.

58. Explain scientific and technical approaches to writing digital forensic reports.

59. Describe the process of testifying as an expert in court and defending digital evidence.

60. Analyze future trends in digital forensics, including AI, IoT, and cloud technologies.