Prasanja:

1. Sto ne e princip na digitalnata forenzika
   -Testiranje

2. Pribiranje na podatoci vo izvoren kod spaga vo?
   -Fizicki sloj

3. Kaj digitalnata forenzika terminot atribucija se koristi za da odgovori na prasanjeto
   -Koj bil odgovoren

4. C skala (S skala) obezbeduva metod za
   -Bezbednost(sigurnost)

5. Sto ne e del od pribiranje I pregled na podatoci
   -Procenka na izvor

6. Kaj elektronskoto otkrivanje pokraj identifikacija I sobiranje na podatoci sto od navedenoto e kriterium koj e potrebno da se proveri za podatocite
   -Releventnost

7. Prva faza kaj elektronsko otkrivanje
   -Upravuvanje so informacii

8. Spored EDRM koi dva cekora se vo edna faza
   -Zacuvuvanje I sobiranje na informacii

9. Edna od glavnite celi vo fazata na obrabotka na podatocite e
   -Transformacija na informacii

10. Sto od navedenoto ne e del od procesor na procenka na opsegot (Scope assesment)
   -Identifikacija na informacii

11. Which one of the following acts states that individuals have a right to respect for the privacy of their e-mails
   -Human rights act

12. Which **two** of the following show why it is important to conduct an investigation on a copy of the data instead of the original
   -To allow investigation to be replicated , to prevent any aspect of the investigation from tampering with the original evidence

13. At which stage of the digital forensics process would a write-blocker be used?
   -Acquisition

14. Applying preservation techniques during data acquisition can help to identify which of the following?
   -Running programs

15. Which **two** of the following software tools could be used during the analysis phase of the digital forensics process?
   hex editor , network packet analyser

16. Which **three** of the following statement s describes forensic readiness?

-How prepared a digital forensic investigator is to present their evidence in a court of law
-A machine which has been imaged for the forensic purposes
-How prepared an ogranisation is to respond an incident

17. Which one of the following files could be retrieved during browser forensics?
-index.dat

18. Which one of the following acts allows certain organisations to get access to an individuals sent and received text messages?
-Regulation of investigatory powers act

19. Which **three** of the following are benefits of forensic readiness?
-Forensic readiness reduces the costs of a digital forensic investigation
-Forensic readiness makes it easier for organisations to gather evidence
-Forensic readiness ensures that as much evidence as possible is available

20. Which **two** of the following are the role of the reporting stage of the digital forensic process?
-The report descibes the investigation so that it can be understood by a non technical person
-The report describes the evidence which was obtained from the investigation

21. Which **two** of the following statements describing the steps in the digital forensic process are true?

-The steps must be completed in the order of accusation , analysis and reporting – there are guildelines explaining how the steps should be completed

22. The Regulation of Investigatory Powers Act 2000, allows organisations to access digital communication, ISPs, Businesses and individual communications and storage
-True

23. Why was the Computer Misuse Act of 1990 introduced?
-To stop people from accessing unauthorised information

24. The most relevant part of the **Human Rights Act** in relation to Digital Forensics is...
-The right to privacy

25. It is the responsibility of who to supervise the execution of a warrant and the security of the site and potential evidence.
-Lead investigator

26. An investigation can only be carried out when
-There is a suspicion that a crime has been commited

27. Which one of the following acts states that individuals have a right to respect for the privacy of their e-mails
-Himan rights act

28. A Digital Forensic examiner will be expected to hold at least which **two** of the following:
-Certified forensic investigation practitioner, degree in digital forensic

29. Which of the following is the correct order of the Digital Forensic examination process?
-Acquisition , analysis, reporting

30. Charachteristics of true evidence are: believeable, admissible, reliable, complete , authentic
-Believeable : Must produce result that are clear and easy to understand, even among the most non-technical members of a jury
-Admissible : If the evidence you uncover will not stand up in court, you have wasted your time and possibly allowed a guilty party to go unpunished
-Reliable : There should be no question about the truth of the investigator's conclusions
-Complete : Investigator should approach the case with no preconceived notions about someone's guilt or innocence
-Authentic : It must be directly related to the incident being investigated

31. Which is false:
- It is the investigator's job to determine someone's guilt or innocence.

32. The forensic database includes in the Digital Forensic application.
-YES

33. Which of the following is NOT the focus of digital forensic analysis?
-Prooving

34. Which of the following represents the step of the scientific method

I- Develop a hypothesis based on evidence

II- Calculate the hash value of the evidence

III- Test the hypothesis to look for additional evidence

IV-make imaging of the original evidence

- I and III are correct

35. What is Digital Forensic?

-The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, a chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation

36. What is the Primary Objective of Digital Forensic for Business and Industry

-Availibility of service

37. Which of the following holds the highest value of evidence in the court?

-Real

38. What are the difficulties in handling Digital Evidence?

Easy to destroy and hard to get

39. Which World organization accredited labs in the world of forensics?
-ACSLD