1) Forensic Accounting is defined as:
   a. The practice of applying defined financial ratios to investigate a company's financial health.
   b. The use of law enforcement to subpoena financial records to determine unlawful actions.
   c. The application of investigative and analytical skills for the purpose of resolving financial issues in a manner that meets standards required by courts of law.
   d. The investigatory arm of the Securities and Exchange Commission.

2) If your actions are the result of misleading, intentional actions or inaction (including misleading statements and the omission of relevant information to gain an advantage, then you have committed:
   a. Perjury.
   b. Contempt.
   c. Treason.
   d. Fraud.

3) When the auditor tests the documents by keeping them side by side then it is known as
   a. Test of impossibility
   b. Test of absurdity
   c. Juxtaposition test
   d. None of the above

4) As per the study of ACFE, following category of individuals commit highest frauds (in monetary terms)
   a. Low level management
   b. Mid level management

c. Senior level management
d. All of the above

5) _____ are the elements of fraud
a. The individual must know that the statement is untrue
b. There is an intent to deceive the victim
c. The victim relied on the statement & The victim is injured financially or otherwise
d. All of the above

6) A type of fraud where forged emails, forged websites are used to defraud the user are known as
a. E frauds
b. Forgery
c. Phishing
d. None of the above.

7) _____ happens when the fraudster avails multiple loans for the same property simultaneously for a total amount in excess of the actual value of the property.
a. Phishing
b. Window dressing
c. Shot gunning
d. Skimming

8) Pressure, opportunity & _____ are the aspects of a fraud triangle.
a. Rationalization
b. Creation
c. Commitment
d. None of the above

9) A _____ is termed as an indication of a danger or a warning signal
a. Red flag
b. Green flag
c. Amber flag
d. White flag

10) A _____ is a flag which denotes a "too good to be true scenario".
a. Red flag
b. Green flag
c. Amber flag
d. White flag

11) Significant increase in working capital borrowing as a percentage of turnover is a
a Red flag
b. Green flag
c. Amber flag
d. White flag

12) A case where an employee doesn't take travel advance but always pays from his pocket is a
a. Red flag
b. Green flag
c. Amber flag
d. White flag

13) Analysing non verbal cues is important for a forensic auditor while
a. Interviewing a suspect
b. Interrogating a suspect
c. a & b both
d. None of the above

14) A model categorizing known frauds which lists about 49 different individual fraud schemes grouped by categories and sub categories is known as
a. Fraud triangle
b. Fraud square
c. Fraud model
d. Fraud tree

15) When the fraudster is able to give a personal justification of dishonest actions, it is known as
a. Pressure

b. opportunity
c. rationalization
d. All of the above

16) Various frauds in banking sector are:
a. Appraisal fraud
b. Mortgage fraud
c. Shot gunning
d. All of the above

17) Fraudsters may alter cheques to change the name or the amount on the face of cheques. This is called
a. Phishing
b. Forgery
c. Disbursement fraud
d. Skimming

18) Ratio analysis is one of the key aspects which a forensic auditor has to look at.
a. Correct
b. Incorrect

19) The principle of 3D vision includes
a. Time dimension analysis
b. Space dimension analysis
c. Both a & b
d. None of the above

20) "Fraud is a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank" is a definition given by:
a. SEBI
b. RBI
c. ICAI
d. ACFE

21) Which of the following is a method used to embezzle money a small amount at a time from many different accounts?
   a. Data diddling
   b. Pretexting
   c. Spoofing
   d. Salami technique

22) Payment to vendors who are not on approval list is a
   a. Management red flag
   b. Red flag in purchase
   c. Red flag in payroll
   d. Red flag in AR

23) Theft of an employer's property which was not entrusted to employee will be defined as:
   a. Lapping
   b. Larceny
   c. Check Kitting
   d. None of the above

24) Weakness in internal control environment will lead which kind of fraud-
   a. Employee Red Flag
   b. Management Red Flag
   c. General Red Flag
   d. None of above

25) _____ is the practice of concealing a file, message, image, or video within another file, message, image, or video.
   a. Imaging
   b. Encryption
   c. Steganography
   d. Data hiding

26) The basic principles used in identifying red flags are:
   a. Distrust the obvious
   b. 3 D vision

c. Inverse logic
d. All of the above

27) The purpose of the Red Flags Rule is:
a. To detect the warning signs – or "red flags" – of identity theft in day-to-day operations
b. Take steps to prevent the crime
c. Mitigate the damage it inflicts.
d. All of the above

28) Which among the following are the three payroll fraud schemes
a. Ghost employees
b. Falsifying wages
c. Falsifying commission
d. All of the above

29) Stealing money from one customer's account and crediting it into another customer's account is known as:
a. Larceny
b. Skimming
c. Lapping
d. None of the above

30) Which of the following scheme referes to the falsification of personnel or payroll records, causing paychecks to be generated to someone who does not actually work for the victim company?
a. Falsified Salary scheme
b. Record alteration scheme
c. Ghost employee scheme
d. Inflated commission scheme

31) The main difference between forgery and cheating is that
a. In cheating, the deception is in writing whereas in forgery it is oral
b. Deception can be described as merely the means whereas, the end being forgery
c. In cheating the deception is oral while in forgery it is in writing
d. None of the above

32) Why Do People Commit Financial Statement Fraud

a. To conceal true business performance
b. To preserve personal status/control
c. To maintain personal income/wealth
d. All the above

33) The interrelationship among auditing, fraud examination, and financial forensics is:

a. Established and maintained by legal structures and justice processes
b. Constant even while social and cultural pressures are exerted on it
c. Cased on the SOX Act and SAS 99
d. Dynamic and changes over time

34) Financial statement fraud is easiest to commit in organizations that:

a. have democratic leadership.
b. have a large internal audit department.
c. have a board of directors comprised primarily of outsiders.
d. have complex organizational structures.

35) The process by which several bidders conspire to split contracts up and ensure each gets a certain amount of work is called

a. Bid pooling
b. Fictitious suppliers
c. Kickback payments
d. Bidding agreements

36) Which of the following types of organizations typically use Forensic Accountants?

a. Publicly held corporations.
b. Private/non-profit corporations.
c. Federal/State Agencies.
d. All of the above.

37) Red Flag procedures must be implemented by individual departments. That means:

a. The procedures just have to be written and accessible to everyone.

b. The procedures have to be written and everyone needs to be trained to use them.

c. The procedure & policy will be drafted

d. A & B Both

38) _____ can be described as the use of that stolen *identity* in criminal activity to obtain goods or services by deception

a. Identity fraud

b. Deception

c. Theft

d. None of the above

39) White collar crimes are the ones which damage the organisation:

a. Many times

b. Many times & in huge amounts

c. Less times

d. Less times but in huge amounts

40) The Fraud Exposure Rectangle includes:

a. Rationalization

b. Perceived pressure

c. Relationships with others

d. All of the choices are included in the Fraud Exposure Rectangle

41) Motivation for Financial Statements Fraud can be:

a. Increasing stock prices

b. Maximising management bonus

c. Pressure on management to perform

d. All of the above

42) Management & directors, relationship with others, organization & industry, financial results & operating characteristics are components of:

a. Fraud Tree

b. Fraud Exposure Rectangle

c. Fraud Triangle

d. None of the above

43) Relationship of the management with auditors, bankers, lawyers, regulatory authorities etc is to be checked while analyzing

a. Management & Directors
b. Relationship with Others
c. Organisation & Industry
d. Financial Results & Operating Characteristics

44) _____ among the following is an example of red flag.

a. Very friendly, but self centered and egoistic
b. Unfriendly and an introvert
c. Surly and angry but good in work
d. Very slow in work that he/she is used to doing for years together

45) Introduction, rapport, questioning, summary & close are elements of:

a. Interview
b. Investigation
c. Interrogation
d. None of the above

46) Voice Analysis can detect?

a. Temperament of a person during the interview
b. Whether person is lying
c. Whether he is telling the facts
d. All of the above

47) All of the following are methods that organization can adopt to proactively eliminate fraud opportunities EXCEPT:

a. Accurately identifying sources and measuring risks
b. Implementing appropriate preventative and detective controls
c. Creating widespread monitoring by employees
d. Eliminating protections for whistle blowers

48) Professional Skepticism refers to

a. An alert Mind
b. A questioning Ming
c. A & B Both
d. None of the above

49) Weak internal controls in an organization will affect which of the following elements of fraud?

a. Motive
b. Opportunity
c. Rationalization
d. None of the above

50) If a company wishes to improve detection methods, they should do all of the following except:

a. Use forensic accountants
b. Conduct frequent audits
c. Conduct surprise checks
d. All of the above improve detection of fraud

51) Fraudulent financial reporting is most likely to be committed by whom?

a. Line employees of the company
b. Outside members of the company's board of directors
c. Company management
d. The company's auditors

52) Confrontational Interviews and recording of any interviews should be done

a. With the advice of legal counsel only if there is need to prosecute the fraudster later.
b. With the advice of legal counsel to get proper legal guidance to protect the interviewer, the Company, Directors/Management and prosecute the fraudster later if needed.
c. Without the advice of legal counsel since the confidentiality of strategy is compromised.
d. Without the advice of legal counsel since they have no role to play till the fraud is established.

53) _____ is an equitable remedy designed to deter future violations of the securities laws and to deprive defendants of the proceeds of their wrongful conduct.

a. Disgorgement
b. Penalty

c. Insider information
d. Proceedings

54) When individually any financial items/ transactions are not much relevant, however if used wisely together to commit a fraud, it is known as:

a. Combined fraud
b. Gunpowder effect
c. Lapping
d. None of the above

55) The term "razor" used in the Theory of Occam's razor signifies

a. Shaving off illegal data
b. Shaving of backdated data
c. Shaving off unnecessary data
d. None of the above.

56) Disaster situation, incomplete information, disorderliness are:

a. Red flags at macro level
b. Red flags at micro level
c. Green flags at macro level
d. Green flags at micro level

57) Orphan funds, excess knowledge, close nexus with vendors etc are:

a. Red flags at macro level
b. Red flags at micro level
c. Green flags at macro level
d. Green flags at micro level

58) While conducting an interview, as a general rule,

a. One person should be interviewed at a time
b. Two persons should be interviewed at a time
c. Three persons should be interviewed at a time
d. None of the above.

59) Types of questions that could be asked in an interview could be

a. Open ended
b. Closed ended
c. Leading
d. All of the above

60) A type of question wherein the Interviewer provides an answer within the question is know as:

a. Open ended
b. Closed ended
c. Leading
d. All of the above

61) A question which requires a narrative response is known as _____ question:

a. Open ended
b. Closed ended
c. Leading
d. All of the above

62) A question which requires a yes/ no answers is known as _____ question:

a. Open ended
b. Closed ended
c. Leading
d. All of the above

63) In cases where the interviewee in constantly denying the charges against him,

a. Detain him in a room
b. Present partial evidences
c. Make a direct accusation
d. None of the above.

64) Things to be avoided during an interview include:

a. Threatening
b. Detaining the person
c. Negotiating
d. All of the above

65) Among the following which would be red flags for payroll?

a. Overtime charged during a slack period
b. Large number of write offs
c. Unjustified transactions
d. All of the above

66) The most cost effective way to minimize the cost of fraud is:

a. Prevention
b. Detection
c. Investigation
d. Prosecution

67) An act of unintentional mistake is known as

a. Fraud
b. Deception
c. Error
d. Forgery

68) While conducting a an interview, the interviewer analyses:

a. Verbal clues
b. Non verbal clues
c. Both a & b
d. None of the above

69) An employee not taking a single holiday during the entire year is

a. Red flag at macro level
a. Red flag at micro level
b. Green flag
c. None of the above

70) Excessive competition in the market leads to

a. Rationalisation
b. Opportunity
c. Pressure

d. None of the above

71) Lack of rotation of duties will come under _____ component of a fraud triangle

a. Rationalisation
b. Opportunity
c. Pressure
d. None of the above

72) Recording a suspect's interview will help in

a. Gathering evidence in the case
b. Taking e notes instead of handwritten notes
c. Assist you in case the interviewee changes his/ her statement at a later stage
d. All of the above

73) Which of the following entities are/ were involved in frauds

a. Enron
b. Tyco International
c. WorldCom
d. All of the above

74) Having excess stock as compared to that recorded in books of accounts is a

a. Red flag
b. Amber flag
c. Green Flag
d. None of the above

75) Excessive payment to consultants & auditors is an example of

a. Red flag
b. Amber flag
c. Green Flag
d. None of the above

76) Reporting of identified frauds is covered as per

a. SA 240

b. Sec 143(12) of Companies Act 2013
c. CARO, Clause x
d. All of the above.

77) Section 143(12) deals with reporting frauds committed by
a. Officers of the company
b. Employees of the company
c. Third parties
d. Only a & b

78) As per the study of ACFE, following category of individuals commit highest frauds (in monetary terms)
a. Low level management
b. Mid level management
c. Senior level management
d. All of the above

79) _____ are the elements of fraud
a. The individual must know that the statement is untrue
b. There is an intent to deceive the victim
c. The victim relied on the statement & The victim is injured financially or otherwise
d. All of the above

80) The principle of 3D vision includes
a. Time dimension analysis
b. Space dimension analysis
c. Both a & b
d. None of the above

81) The basic principles used in identifying red flags are:
a. Distrust the obvious
b. 3 D vision
c. Inverse logic
d. All of the above

82) Why Do People Commit Financial Statement Fraud

a. To conceal true business performance
b. To preserve personal status/control
c. To maintain personal income/wealth
d. All the above

83) White collar crimes are the ones which damage the organisation:

a. Many times
b. Many times & in huge amounts
c. Less times
d. Less times but in huge amounts

84) Areas which are difficult to corroborate is perceived as _____ by a fraudster

a. Pressure
b. Opportunity
c. Rationalisation
d. Threat

85) Excessive related party transactions are considered as

a. Red flag
b. Amber flag
c. Green Flag
d. None of the above

86) Things to be avoided during an interview include:

e. Threatening
f. Detaining the person
g. Negotiating
h. All of the above

87) Among the following which would be red flags for payroll?

e. Overtime charged during a slack period
f. Large number of write offs
g. Unjustified transactions
h. All of the above

88) The most cost effective way to minimize the cost of fraud is:

e. Prevention
f. Detection
g. Investigation
h. Prosecution

89) Satyam case was filled with

a. Ghost employees
b. Fake sales
c. Inflated Cash & bank balances
d. All of the above

90) A forensic auditor can get opportunities in

a. Banking sector
b. Insurance Sector
c. Both a & b
d. None of the above

91) Auditor's responsibility relating to fraud in financial statements is covered in:

a. SA 200
b. SA 240
c. SA 250
d. SA 299

92) A type of question wherein the Interviewer provides an answer within the question is know as:

a. Open ended
b. Closed ended
c. Leading
d. All of the above

93) The concealment of the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses is known as

a. Slicing
b. Spoofing
c. Money Laundering

d. All of the above

94) A red flag indicates that the alert is
a. New
b. Old
c. Follow up
d. Outdated

95) Existence of orphan funds comes under _____ component of a fraud triangle
a. Rationalisation
b. Opportunity
c. Pressure
d. None of the above

96) An entity running on an auto pilot mode can be perceived as _____ by a fraudster.
a. Rationalisation
b. Opportunity
c. Pressure
d. None of the above

97) When individually any financial items/ transactions are not much relevant, however if used wisely together to commit a fraud, it is known as:
a. Combined fraud
b. Gunpowder effect
c. Lapping
d. None of the above

98) While conducting an interview, as a general rule,
a. One person should be interviewed at a time
b. Two persons should be interviewed at a time
c. Three persons should be interviewed at a time
d. None of the above.

99) Examples of few simple forensic audit tests are

a. Test of absurdity
b. Test of impossibility
c. Juxtaposition test
d. All of the above

100) Good traits of a forensic auditor are:
a. Maintaining professional skepticism
b. Being a good observer
c. Using multiple cues to analyze any area
d. All of the above.

1. What is the objective of using CAAT

a. Data Mining

b. Data Analysis

c. Data Analytics

d. Data Wrangling

Answer: C

2. Which functionality is NOT present in CAAT

a. Comparison

b. Statistics

c. Monetary unit

d. Split

Answer: D

3. Which of the following is not the outcome of joining two databases

a. Complete join

b. Partial join using look-up field

c. Selective join using look-up field

d. Merging

Answer: C

4. …… refers to collection of information pertinent to project

a. Data gathering

b. Data exporting

c. Data embedding

d. Data importing

Answer: A

5. Development costs for a computer based information system include/s

a. Salaries of the system analysis

b. Cost of converting and preparing data

c. Cost of testing and documenting

d. All A, B, C

Answer: D

6. Which of the following is NOT a sampling technique provided in CAAT

a. Attribute

b. clustered

c. Random

d. Monetary unit

Answer: B

7. developing a logical flow of fraud detection it is a good idea to

a. develop a physical flow

b. develop a system flow chart

c. determine the contents of all data stores

d. find out user's preferences

Answer: A

8. A data store in a CAAT represents

a. a sequential file

b. a disk store

c. a repository of data

d. a random access memory

Answer: C

9. Which of the following is not a criticism of the use of CAAT

a. It reinforces the idea that code-and-retrieve is the only way to conduct qualitative analysis

b. It results in the fragmentation of data and a loss of narrative flow

c. It may not be suitable for focus group data

d. It is not very fast or efficient at retrieving sections of data

Answer: D

10. Which of the following is a disadvantage of using CAAT in different types of projects

a. It makes the process of qualitative data analysis more transparent

b. It is faster and more efficient than analysing by hand

c. It involves learning skills that are specific to each program

d. It helps you to map out the relations between ideas and themes in the data

Answer: C

11. Which of the following is a kind of search that can be carried out in CAAT

a. Boolean

b. Proximity

c. Wildcard

d. All of above

Answer: D

12. Which of the following is not the capability of CAAT in statistics?

a. Probability

b. Correlation

c. Trend Analysis

d. Time Series

Answer: A

13. Which of the following is not a valid Benford test in CAAT

a. First two digit

b. Last two digit

c. First three digit

d. Last three digit

Answer: D

14. Which characteristics of data is not preserved in CAAT

a. Integrity

b. Source format

c. Indexed order

d. Originality

Answer: B

15. Which of the below is not an advantage of using CAAT

a. The audit team may not require the knowledge or training needed to understand the results of the CAAT

b. Independently access data stored on a computer without dependence on the client

c. Test the reliability of client software

d. Increase the accuracy of audit tests

Answer: A

16. Which of the below is a PRIMARY limitation of using CAAT

a. Potential incompatibility with the client's computer system

b. The audit team may not have sufficient IT skills and knowledge to create the complex data extracts and programming required

c. Client permission and cooperation may be difficult to obtain

d. The audit team may not have the knowledge or training needed to understand the results of the CAATs

Answer: C

17. Which of the following are two broad categories of CAAT

a. Audit software and exception reporting module of clients software

b. Audit software and test data

c. BI tools and Integrated test facility

d. Test data and embedded audit software in SAP/ERP

Answer: B

18. Of the following which is the specific purpose for which CAAT is used:

a. Sampling

b. File management

c. Report generation

d. Log maintenance

Answer: D

19. CAAT is used for which of the following type of data analytics

a. Cognitive analysis

b. Predictive analysis

c. Diagnostic analysis

d. Prescriptive analysis

Answer: C

20. CAAT performs following functions:

a. Data Presentation

b. Data queries

c. Data Stratification

d. Data Extraction

Answer: A

1. Which of the file systems for Microsoft system provides the most security?
   a. NTFS
   b. FAT
   c. FAT32
   d. FAT16

2. The chain of custody should be able to answer the following questions *except*:

   a. Who collected the evidence?
   b. How and where is the evidence stored?
   c. Who took possession of the evidence?
   d. Who created the chain of custody document?

3. The different ways in which the network can be attacked *except*?
   a. availability
   b. confidentiality
   c. integrity
   d. durability

4. Where do routers reside in relationship to the OSI model?
   a. Layer 1

b. Layer 2
c. Layer 3
d. Layer 4

5. The term is used to describe espionage conducted for commercial purposes on companies and governments, and to determine the activities of competitors:
   a. company espionage
   b. corporate espionage
   c. government espionage
   d. business espionage

6. What is the main motive behind corporate spying?
   a. personal relations
   b. disgruntled employees
   c. easy money
   d. all of the above

7. The major technique used for corporate spying is :
   a. social engineering
   b. dumpster diving
   c. phone eavesdropping
   d. all of the above

8. An Internet standard protocol that is used to synchronize the clocks of client computers is called:
   a. Network Time Protocol (NTP)
   b. Time Sync Protocol (TSP)
   c. Server time Protocol (STP)
   d. Client time Protocol (CTP)

9. The process of tracking unauthorized activity using techniques such as inspecting user actions, security logs, or audit data is called:
   a. Intrusion Prevention
   b. Intrusion Detection

c. Host Detection
d. Host Prevention

10. The unique 48-bit serial number assigned to each network interface card, providing a physical address to the host machine is called:
    a. MAC
    b. NAC
    c. IAC
    d. HAC

11. A record of the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence is called:
    a. Chain of Evidence
    b. Chain of History
    c. Chain of Custody
    d. Chain of Forensics

12. An attack that overloads a system's resources, either making the system unusable or significantly slowing it down, is called:
    a. Denial-of-service attack
    b. Network Denial attack
    c. Resource Denial attack
    d. Server down attacks

13. The wilful act of stealing someone's identity for monetary benefits is called:
    a. Data Theft
    b. Privacy Theft
    c. Identity Theft
    d. Person Theft

14. When did both the houses of the Indian Parliament passed the Information Technology Bill in 2000?
    a. Jan 2000
    b. Mar 2000
    c. May 2000
    d. Aug 2000

15. In February 2016, which Bank of Bangladesh suffered a major cyber-attack losing millions of dollars?
    a. EBL Bank
    b. United Commercial Bank
    c. Grameen Bank
    d. Bangladesh Bank

16. Which section of IT Act 2000 hands out Punishment for Sending Offensive Messages through Communication Service etc.?
    a. Sec 66A
    b. Sec 66B
    c. Sec 66C
    d. Sec 66D

17. Which section of IT Act 2000 deals with Cyber Terrorism?
    a. Sec 66A
    b. Sec 66B
    c. Sec 66C
    d. Sec 66F

18. The administrators of the DDoS marketplace webstresser.org were arrested on 24 April 2018 as part of which global Operation?
    a. Operation Power Zero
    b. Operation Power Off
    c. Operation Power On
    d. Operation Power Global

19. IoT stands for:
    a. Internet of Tech
    b. Internet of Times
    c. Internet of Tomorrow
    d. Internet of Things

20. As per global study, most cyber-attacks on corporates are performed by:
    a. Outsiders
    b. Insiders
    c. Vendors
    d. Unknown Hackers

21. The write-blocker that sits between evidence drive & forensic workstation is called:
    a. Software Write Blocker
    b. Hardware Write Blocker
    c. Hybrid Write Blocker
    d. Forensic Write Blocker

22. The write-blocker that is built into a computer forensic suite or OS configured is called:
    a. Software Write Blocker
    b. Hardware Write Blocker
    c. Hybrid Write Blocker
    d. Forensic Write Blocker

23. The process of making a partition visible to an OS is called:
    a. Partitioning
    b. Mounting
    c. Loading
    d. Plugging

24. The process of changing the caller ID to any number other than the calling number is called:
    a. Caller ID Tagging
    b. Caller ID Changing
    c. Caller ID Spoofing

d. Caller ID Rigging

25. A specific type of phishing attack that appears to come from a trusted source is also known as:
    a. Target Phishing
    b. Spear Phishing
    c. Knife Phishing
    d. Sword Phishing

26. A general term for any encrypted overlay network that you can only access with specific types of software, or authorization, or protocols, or ports, is called:
    a. Underground
    b. Darkweb
    c. Unknown Web
    d. HardWeb

27. A system that is attractive to an attacker and serves no other purpose than to keep attackers out of critical systems and observe their attack methods, is known as:
    a. Honeypot
    b. Honeytoken
    c. Sandbox
    d. Sandtrap

28. An Internet protocol designed for accessing e-mail on a mail server is:
    a. POP
    b. ICMP
    c. IMAP
    d. TCP

29. An Internet protocol used to retrieve e-mail from a mail server is:
    a. POP

b. ICMP
c. IMAP
d. TCP

30. A set of duplicate data that is stored in a temporary location to allow rapid access for computers to function more efficiently, is known as:
    a. Boot Record
    b. Metadata
    c. Swap
    d. Cache

31. A service provided by a server in which the server assigns a client machine an IP address upon request, is called:
    a. TCP
    b. IP
    c. DHCP
    d. ICMP

32. In asymmetric key cryptography, the private key is kept by:
    a. Sender
    b. Receiver
    c. sender and receiver
    d. all the connected devices to the network

33. This is the inclusion of a secret message in otherwise unencrypted text or images.
    a. Masquerade
    b. Steganography
    c. Spoof
    d. Hashing

34. When a user needs to provide message integrity, what options may be best?
    a. Send a digital signature of the message to the recipient
    b. Encrypt the message with a symmetric algorithm and send it
    c. Encrypt the message with a private key so the recipient can decrypt with the corresponding public key
    d. **Create a checksum, append it to the message, encrypt the message, then send to recipient**.

35. What kind of hacker uses hacking to send social, religious, and political, etc messages, usually, done by hijacking websites and leaving a message on the hijacked website?
    a. Hacktivist
    b. Phone phreaker
    c. White hat hacker
    d. Grey hat hacker

36. What kind of hacker gains access to systems with a view to fix the identified weaknesses?
    a. Black hat hacker
    b. Purple hat hacker
    c. White hat hacker
    d. Grey hat hacker

37. What kind of program allows the attacker to control the user's computer from a remote location?
    a. Virus
    b. Trojan Horse
    c. Malware
    d. Keylogger

38. What is the art of exploiting the human elements to gain access to un-authorized resources?
    a. Ethical Hacking
    b. Social Engineering
    c. Caller ID Spoofing
    d. Reverse Engineering

39. How many numbers of bits are used by IPv6?
    a. 64
    b. 32
    c. 24
    d. 128

40. How many numbers of bits are used by IPv4?
    a. 64

b. 32
c. 24
d. 128

41. Which service runs on port 21?
    a. HTTP
    b. HTTPS
    c. FTP
    d. SMTP

42. Which service runs on port 80?
    a. HTTP
    b. HTTPS
    c. FTP
    d. SMTP

43. Which service runs on port 443?
    a. HTTP
    b. HTTPS
    c. FTP
    d. SMTP

44. What can be used to intercept packages as they are transmitted over the network?
    a. MAC flooding
    b. Active Sniffing
    c. Passive Sniffing
    d. Network Sniffing

45. Which attack is used to crash Web Server?
    a. SQL Injection
    b. ARP poisoning
    c. DOS attack
    d. Cross Site Scripts

46. This attack involves eavesdropping on a network and capturing sensitive information?
    a. Man-in-the-Middle

b. Sniffing
c. DoS Attack
d. SQL Injection

47. Which of the following best describes a distributed denial-of-service attack?
    a. A DoS against an entire subnet, affecting multiple systems
    b. A DoS against multiple systems across an enterprise network
    c. DoS against similar systems in different target networks
    d. A DoS carried out by multiple systems

48. Passwords no longer provide adequate authentication to online services because:
    a. People typically choose simple and easy to guess passwords
    b. People share passwords
    c. People reuse passwords across multiple accounts
    d. All of the above

49. This authentication process allows a user to enter one name and password to access multiple applications.
    a. RADIUS
    b. security ID
    c. SSO
    d. user profile

50. What best describes metadata?

    a. Data that is important to the investigation
    b. Data about data
    c. Data that is hidden
    d. Operating system data

51. What type of encryption uses a different key to encrypt the message than it uses to decrypt the message?

    a. private key
    b. asymmetric

c. symmetric
d. secure

52.Which of the following are the two types of write protection?

a. Fast and slow
b. Windows and Linux
c. Hardware and software
d. Forensic and non-forensic

53.What is Digital Forensic?

a. Process of using scientific knowledge in analysis and presentation of evidence in court.
b. The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.
c. A process where we develop and test hypotheses that answer questions about digital events.
d. Use of science or technology in the investigation and establishment of the facts or evidence in a court of law

54.Which of the following is NOT focus of digital forensic analysis?

a. Authenticity
b. Comparison
c. Proving
d. Enhancement

55.Which of the following is FALSE?

a. The digital forensic investigator must maintain absolute objectivity
b. It is the investigator's job to determine someone's guilt or innocence.
c. It is the investigator's responsibility to accurately report the relevant facts of a case.
d. The investigator must maintain strict confidentiality, discussing the results of an investigation on only a "need to know" basis.

56.What do you do to a computer that is turned off?

a. Turn it on
b. Leave it off
c. Start typing
d. Flip the switch

57. What should you do if the computer is turned on?
a. Shut it down
b. Unplug it
c. Start typing
d. Log the user off

58. What happens when first securing the area?
a. Start looking for evidence
b. Make sure that the crime scene is safe
c. Gather evidence
d. Make sure computer is on

59. A system for locating phones by determining its distance from 3 different towers.
a. Arson Can
b. Cell site
c. Dead spots
d. Triangulation

60. Which of the following is NOT a service level for the cloud?
a. Platform as a service
b. Infrastructure as a service
c. Virtualization as a service
d. Software as a service

61. Which is not a valid method of deployment for a cloud
a. community
b. public
c. targeted
d. private

62. Which password recovery method uses every possible letter, number, and character found on a keyboard?

a. rainbow table
b. dictionary attack
c. hybrid attack
d. **brute-force attack**

63. Validate your tools and verify your evidence with ____ to ensure its integrity.
    a. hashing algorithms
    b. watermarks
    c. steganography
    d. digital certificates

64. E-mail administrators may make use of ???, which overwrites a log file when it reaches a specified size or at the end of a specified time frame
    a. log recycling
    b. circular logging
    c. log purging
    d. log cycling

65. The ___ tool is an updated version of BackTrack, and contains more than 300 tools, such as password crackers, network sniffers, and freeware forensics tools
    a. Kali Linux
    b. Ubuntu
    c. OSForensics
    d. Sleuth Kit

66. The ___ command line program is a common way of examining network traffic, which provides records of network activity while it is running, and produce hundreds of thousands of records
    a. netstat
    b. ls
    c. ifconfig
    d. tcpdump

67. What method below is NOT an effective method for isolating a mobile device from receiving signals?
    a. placing the device into a plastic evidence bag
    b. placing the device into a paint can, preferable one previously containing radio-wave blocking paint

c. placing the device into airplane mode
d. turning the device off

68. One of the most noteworthy e-mail scams was 419, otherwise known as the?
a. Nigerian Scam
b. Lake Venture Scam
c. Conficker virus
d. Iloveyou Scam

69. What is a search query that can help identify some of the individuals and/or companies associated with a given domain name, including the registrant, when the domain was created, etc.
a. Email
b. Google
c. Whois
d. Cookies

70. What is a small text file that is deposited on a user's computer by a web server? They are used to track sessions as well as remember a user's preferences for a particular web site.
a. Browser
b. Spoofing
c. Whois
d. Cookies

71. What is responsible for mapping domain names to specific IP address?
a. Static web page
b. Message ID
c. Dynamic web page
d. Domain Name Server

72. What is used primarily as a means to share files?
a. Peer-to-Peer
b. Browser
c. Web Cache
d. Cookies

73. Which system is Base 16 that use 0-9 A, B, C, D, E, F can go 0-15?
    a. Octal
    b. Decimal
    c. Binary
    d. Hexadecimal

74. What option below is an example of a platform specific encryption tool?
    a. GnuPG
    b. TrueCrypt
    c. BitLocker
    d. Pretty Good Privacy (PGP)

75. Within a computing investigation, the ability to perform a series of steps again and again to produce the same results is known as ???
    a. repeatable findings
    b. reloadable steps
    c. verifiable reporting
    d. evidence reporting

76. Which of the following scenarios should be covered in a disaster recovery plan?
    a. damage caused by lightning strikes
    b. damage caused by flood
    c. damage caused by a virus contamination
    d. all of the above

77. The passwords are typically stored as one-way _____ rather than in plaintext?
    a. hex values
    b. variables
    c. hashes
    d. stack spaces

78. What program serves as the GUI front end for accessing sleuth kit's tools?
    a. detectiveGUI
    b. autopsy
    c. kde
    d. smart

79. Which term describes rooms filled with extremely large disk systems that are typically used by large business data centers?
    a. storage room
    b. server farm
    c. data well
    d. storage hub

80. What is the purpose of the reconstruction function in a forensics investigation?
    a. re-create a suspect's drive to show what happened during a crime or incident
    b. prove that two sets of data are identical
    c. copy all information from a suspect's drive, including information that may have been hidden
    d. generate reports or logs that detail the processes undertaken by a forensics investigator

81. Which option below is not a recommendation for securing storage containers?
    a. the container should be located in a restricted area
    b. only authorized access should be allowed, and it should be kept to a minimum
    c. evidence containers should remain locked when they aren't under direct supervision
    d. rooms with evidence containers should have a secured wireless network

82. What is the name of the Microsoft solution for whole disk encryption?
    a. drivecrypt
    b. truecrypt
    c. bitlocker
    d. FileVault

83. What is the name of the Mac solution for whole disk encryption?
    a. drivecrypt
    b. truecrypt
    c. bitlocker
    d. FileVault

84. What virtual machine software supports all Windows and Linux OSs as well as Macintosh and Solaris, and is provided as shareware?
    a. KVM
    b. Parallels
    c. Microsoft Virtual PC
    d. VirtualBox

85. In a ___ attack, the attacker keeps asking your server to establish a connection, with the intent of overloading a server with established connections
    a. smurf
    b. SYN flood
    c. spoof
    d. ghost

86. A Nibble is made of:
    a. 4 bits
    b. 8 bits
    c. 12 bits
    d. 16 bits

87. A computer network that spans a relatively large geographical area and consists of two or more interconnected local area network (LAN)?
    a. Network Share
    b. Wide Area Network (WAN)
    c. Local Area Network (LAN)
    d. Cloud Network

88. "A sender and receiver share a single, common key to encrypt and decrypt the message" is called?
    a. Anti-Forensics

b. Swap Partition
c. Public-Key Encryption
d. Symmetric-Key Encryption

89. A basic unit of communication over a digital network is called?
a. Payload
b. Packets
c. BIOS
d. Carrier

90. The practice of examining large databases in order to generate new information?
a. Tunneling
b. Sandboxing
c. Degaussing
d. Data Mining

91. "A network of personal computers, each of which acts as both client and server, so that each can exchange files and email directly with every other computer on the network. "?
a. Peer-to-Peer Network
b. Local Area Network
c. Hypervisor
d. Brute-Force Attack

92. "An efficient, isolated duplicate of a real machine." Is called?
a. Visualization
b. File Carving
c. Data Mining
d. Virtual Machine (VM)

93. Using a very large magnet to destroy the magnetic data on the disk?
a. Sandboxing
b. Tunneling
c. Degaussing
d. Data Mining

94. This assumes that the password is a dictionary word or some variant of one. The tool simply does a replacement of the password until it finds the one that fits?
    a. Metadata
    b. Brute-Force Attack
    c. Network Share
    d. Dictionary Attack

95. "A process of allowing an unknown executable to run in a specially prepared and instrumented environment, so that its capabilities and actions can be observed"?
    a. Degaussing
    b. Sandboxing
    c. Spoofing
    d. Tunneling

96. A computer virus that replicates and spreads itself is also known as?
    a. virus
    b. worm
    c. bot
    d. zombie

97. What describes an examination of a system while it is still running?
    a. live analysis
    b. crackers
    c. hackitvists
    d. steganography

98. People who would like to be hackers but don't have much technical expertise?
    a. hackitvists
    b. rootkit
    c. crackers
    d. script kiddies

99. The process of keeping track of all upgrades and patches you apply to your computer's OS and applications is called
    a. Configuration Management
    b. Hardware Management

c. Software Management
d. Server Management

100. Which one is a Network forensics tool?
a. EnCase
b. Autopsy
c. nMap
d. Volatility

101. Which one is a Data Capture forensics tool?
a. EnCase
b. Wireshark
c. nMap
d. Volatility

102. Which one is a RAM forensics tool?
a. EnCase
b. Autopsy
c. nMap
d. Volatility

MCQs on CAAT

1. What is the objective of using CAAT

a. Data Mining

b. Data Analysis

c. Data Analytics

d. Data Wrangling

Answer: C

2. Which functionality is NOT present in CAAT

a. Comparison

b. Statistics

c. Monetary unit

d. Split

Answer: D

3. Which of the following is not the outcome of joining two databases

a. Complete join

b. Partial join using look-up field

c. Selective join using look-up field

d. Merging

Answer: C

4. …… refers to collection of information pertinent to project

a. Data gathering

b. Data exporting

c. Data embedding

d. Data importing

Answer: A

5. Development costs for a computer based information system include/s

a. Salaries of the system analysis

b. Cost of converting and preparing data

c. Cost of testing and documenting

d. All A, B, C

Answer: D

6. Which of the following is NOT a sampling technique provided in CAAT

a. Attribute

b. clustered

c. Random

d. Monetary unit

Answer: B

7. developing a logical flow of fraud detection it is a good idea to

a. develop a physical flow

b. develop a system flow chart

c. determine the contents of all data stores

d. find out user's preferences

Answer: A

8. A data store in a CAAT represents

a. a sequential file

b. a disk store

c. a repository of data

d. a random access memory

Answer: C

9. Which of the following is not a criticism of the use of CAAT

a. It reinforces the idea that code-and-retrieve is the only way to conduct qualitative analysis

b. It results in the fragmentation of data and a loss of narrative flow

c. It may not be suitable for focus group data

d. It is not very fast or efficient at retrieving sections of data

Answer: D

10. Which of the following is a disadvantage of using CAAT in different types of projects

a. It makes the process of qualitative data analysis more transparent

b. It is faster and more efficient than analysing by hand

c. It involves learning skills that are specific to each program

d. It helps you to map out the relations between ideas and themes in the data

Answer: C

11. Which of the following is a kind of search that can be carried out in CAAT

a. Boolean

b. Proximity

c. Wildcard

d. All of above

Answer: D

12. Which of the following is not the capability of CAAT in statistics?

a. Probability

b. Correlation

c. Trend Analysis

d. Time Series

Answer: A

13. Which of the following is not a valid Benford test in CAAT

a. First two digit

b. Last two digit

c. First three digit

d. Last three digit

Answer: D

14. Which characteristics of data is not preserved in CAAT

a. Integrity

b. Source format

c. Indexed order

d. Originality

Answer: B

15. Which of the below is not an advantage of using CAAT

a. The audit team may not require the knowledge or training needed to understand the results of the CAAT

b. Independently access data stored on a computer without dependence on the client

c. Test the reliability of client software

d. Increase the accuracy of audit tests

Answer: A

16. Which of the below is a PRIMARY limitation of using CAAT

a. Potential incompatibility with the client's computer system

b. The audit team may not have sufficient IT skills and knowledge to create the complex data extracts and programming required

c. Client permission and cooperation may be difficult to obtain

d. The audit team may not have the knowledge or training needed to understand the results of the CAATs

Answer: C

17. Which of the following are two broad categories of CAAT

a. Audit software and exception reporting module of clients software

b. Audit software and test data

c. BI tools and Integrated test facility

d. Test data and embedded audit software in SAP/ERP

Answer: B

18. Of the following which is the specific purpose for which CAAT is used:

a. Sampling

b. File management

c. Report generation

d. Log maintenance

Answer: D

19. CAAT is used for which of the following type of data analytics

a. Cognitive analysis

b. Predictive analysis

c. Diagnostic analysis

d. Prescriptive analysis

Answer: C

20. CAAT performs following functions:

a. Data Presentation

b. Data queries

c. Data Stratification

d. Data Extraction

Answer: A

21. In an audit of Journal Vouchers (JVs) how will you derive for potential duplicate JVs booked on the same date to the same head of account combination for round sum amounts?

a. Direct Extraction

b. Duplicate key Detection

c. Publish PDF

d. All of the above

Answer: D

22. In the audit of JVs how will you identify JV narrations containing key words like 'adjustment', accommodate' and others?

a. Manage Project

b. Gap Detection

c. Search

d. Go To

Answer: C

23. You are required to pick up random JVs per cost centre within the JV file so that all cost centres are covered in the review. Which function will assist you with the same?

a. Stratification - Numeric

b. Stratified Random Sampling - Character

c. Pivot Table

d. Stratified Random Sampling - Numeric

Answer: B

24. How will you capture JVs booked on Saturday/Sundays with an all numeric narration (non-standard narrations)?

a. Field Statistics

b. Criteria

c. Save As Selected

d. All of the above

Answer: D

25. Which function will you apply in IDEA to look for a sudden drop in the count of month ending JVs for accruals?

a. Pivot Table

b. Top Records Extraction

c. Control Total

d. Find Next

Answer: A

26. In a data file of Goods and Service Tax (GST) levy and payment how will you check for product sales within State A but where Inter State GST has been incorrectly levied and paid

a. Export

b. Print

c. Direct Extraction

d. Field Manipulation

Answer: C

27. In the GST data file, you need to re-compute the Central and State GST levied and paid on the Invoice value to check whether the application system is correctly computing the same. How will you perform this in IDEA?

a. Modify Field

b. Append Field

c. Remove Field

d. Hide Field

Answer: B

28. You are presented with the GST data file from the GSTIN portal which contains GST returns filed by your Vendors over the last year. You need to reconcile the portal file with your GST data file to identify entries in the portal file based on Vendor Code and Vendor Invoice Number not in your GST data file. How will you set about doing this in IDEA?

a. Join

b. Append Database

c. Stratification

d. Systematic Sampling

Answer: A

29. You are required to match the Vendor Code wise total of Inter State GST levies for the current month from your data with the portal data to identify Vendor wise mismatches on Inter State GST. Which function in IDEA will assist?

a. Criteria

b. Compare - CORRECT ANSWER

c. Send Email

d. Summarization

Answer: B

30. In your GST data how will you check for the Vendor Invoice number containing special characters other than numbers and letters in IDEA?

a. Data - Append - use @split

b. Data - Append - use @left

c. Data - Append - use @strip

d. Data - Append - use @age

Answer: C

31. You are required to allocate a single Digital Advertisement Expense bill for 12 months to various branch locations based on the number of walk in customers in each branch. You have a file with 275 branches and the total walk in count (footfall) per branch for 12 months. Which function in IDEA will you apply for the Expense allocation branch wise

a) Key Value Extraction

b) Append Databases

c) Append Field

d) Gap Detection

Answer: C

32. How will you go about identifying in IDEA specific branches having a rising footfall but falling Digital Advertisement Expense allocation or vice - versa

a) Trend Analysis

b) Correlation

c) Duplicate Key Exclusion

d) Search

Answer: B

33. How will you identify branches having a total footfall of 100 customers and below in the entire 12 month's period and below using IDEA

a) Publish to PDF

b) Create Project

c) Stratification

d) Summarization

Answer: D

34. Which function in IDEA will you apply to identify the 25 branches having the highest Digital Advertisement Expense allocation

a) Bottom Records Extraction

b) Top Records Extraction

c) Group Records

d) Indexed Extraction

Answer: B

35. To capture manipulation in footfall data for any given branch how will you identify in IDEA branches having the same footfall for 12 months

a) Duplicate Key Exclusion

b) Import

c) Save As

d) Duplicate Key Detection

Answer: D

36. You have been provided with an online content - TV Serial, Movie Streaming website data file with the following key fields -

- Customer Number
- Plan Reference
- Date of Visit (DD-MMM-YY Format)
- Time of Visit (HH:MM:SS Format)
- Online Content Duration in Standard Minutes
- Actual State Time of Viewing (HH:MM:SS Format)
- Actual Stop Time of Viewing (HH:MM:SS Format)
- Standard Stop Time of Viewing (HH:MM:SS Format)
- Content Unique Serial Number
- Genre - Comedy, Horror, Action, Family Drama
- Category - Serial, Movie
- IP Number of Streaming Device
- Buffering Speed - Low, Medium, High

A. How will you identify Customers who have stopped watching content before the Standard End Time for a Serial/Movie owing to Low Buffering Speed

a) Join

b) Export Databases

c) Direct Extraction

d) Save As

Answer: C

B. Which function in IDEA will you apply to identify the top content watching Customer's based on count of Serial's watched per day

a) Direct Extraction

b) Summarization

c) Top Records Extraction

d) All of the Above

Answer: D

C. How will you report on Customers watching content from multiple devices on the same date like Tablets, Smart Phones, Laptops etc.

a) Duplicate Key Exclusion

b) Duplicate Key Detection

c) Gap Detection

d) Field Manipulation

Answer: A

D. To identify Customers who use the Streaming site only less than 3 times a month which Function in IDEA will help

a) Add Comments

b) Summarization

c) Stratification

d) Set Working Folder

Answer: B

F. To report on which Serial and Genre has minimum viewership online per month how will you use IDEA

a. Summarization

b. Bottom Records Extraction

c. Export Databases

d. All of the Above

Answer: D

Q. No.	Question - Suggested Answer
1	Forensic Accounting is essentially ……
	a) Accounting in a way to detect fraud
	b) Auditing in a way to gather evidence
	c) Investigating in a way to get different evidence
	d) Combination of accounting, auditing, and investigative skills to gather evidence usable in a court of law
2	What is the AutoComplete feature of Excel?
	a) It automatically completes abbreviated words
	b) It completes text entries that match an existing entry in the same column
	c) It completes text and numeric entries that match an existing entry in the same column
	d) It completes text entries that match an existing entry in the same worksheet
3	A circular reference is ……
	a) Geometric modeling tool
	b) A cell that points to a drawing object
	c) A formula that either directly or indirectly depends on itself
	d) Always erroneous
4	Which of the following is a correct order of precedence in formula calculation?
	a) Multiplication and division exponentiation positive and negative values
	b) Multiplication and division, positive and negative values, addition and subtraction
	c) Addition and subtraction, positive and negative values, exponentiation
	d) All of above
5	You want to track the progress of the stock market on a daily basis. Which type of chart should you use?
	a) Pie Chart
	b) Bar Chart
	c) Line Chart
	d) Column Chart
6	Except for the …… function, a formula with a logical function shows the word “TRUE” or “FALSE” as a result.

	a) IF
	b) AND
	c) OR
	d) NOT
7	Which function will calculate the number of workdays between 6/9/2017 and 8/12/2018?
	a) Workday
	b) Date
	c) Networkdays
	d) All of the above
8	_____ is an interactive data summarisation tool in Excel.
	a) CONSOLIDATE
	b) PIVOTTABLE
	c) SUBTOTAL
	d) POWER QUERY
9	_____ is done to identify the missing items in a sequence or series.
	a) Gap Testing
	b) Relative Size factor Analysis
	c) Fuzzy Logic Matching
	d) Sort
10	Which of the following errors will not be traced by Error Checking?
	a) Inconsistent manner of defining formulas
	b) Errors like #N/A, #REF! etc.
	c) Numbers stored as text
	d) Error in the logic of defining the formula
11	Which of the following functions is totally irrelevant for performing aging analysis?
	a) IF Function
	b) AND Function
	c) TODAY Function
	d) LEFT Function
12	In order to prevent identity thieves from finding personally identifiable information by looking through your trash, you should:
	a) Put your sensitive documents in your neighbors trash bin.
	b) Shred, or otherwise destroy all account statements, account applications, cancelled checks or other documents or information that contain personally identifiable information.
	c) Never throw out any sensitive information. Keep it in a safe place within your home.
	d) Take your sensitive information directly to the dump.
13	You're exposing yourself to potential credit card fraud if you:
	a) Sign your cards as soon as they arrive.

	b) Leave cards or receipts lying around.
	c) Void incorrect receipts.
	d) Carry your cards separately from your wallet, in a zippered compartment, a business card holder, or another small pouch.
14	Which of the following are not recommended security practices when setting up a wireless network in your home?
	a) Place your router in a secure location in your home.
	b) Change the name of your router from the default.
	c) Change your router's pre-set password.
	d) Turn on the encryption feature of your wireless routers.
15	Which of the following is not considered to be "personally identifiable information"?
	a) Credit card numbers
	b) Vehicle registration plate number
	c) Name of the school you attend or your workplace
	d) Date of birth
16	Which of the following is a characteristic that asset hiders generally look for in the financial vehicles they use to conceal assets?
	a) Transparency
	b) Inaccessibility
	c) Liquidity
	d) None of the above
17	Which of the following is a step in the general process for tracing illicit transactions?
	a) Selecting a response team
	b) Building a financial profile
	c) Implementing litigation hold procedures
	d) Establishing reporting protocols
18	When determining a subject's net worth for asset-tracing purposes, all assets should be valued at current market value to eliminate any question about estimates.
	a) True
	b) False
19	Sachin is currently being prosecuted for financial statement fraud for allegedly intentionally over-reporting earnings. Although Sachin did over-report income, he did not do so on purpose. Under these facts, which of the following defenses, if any, would likely benefit Sachin as a defense?
	a) Mistake
	b) Ignorance
	c) Duress

	d) All of the above
20	Akbar works as a cashier in an antiques store. Since the merchandise lacks barcodes, he has to enter the prices manually. One customer purchased a piece of furniture that cost Rs. 2500 and paid in cash. Akbar recorded the sale at Rs. 2000 and pocketed the Rs. 500 bill. What type of fraud did Akbar commit?
	a) A cash larceny scheme
	b) Lapping of receivables
	c) An unrecorded sales (skimming) scheme
	d) An understated sales (skimming) scheme
21	Amar, a fraud examiner, is conducting textual analytics on emails sent to and from specific employees that his client has identified as fraud suspects. He is using the Fraud Triangle to come up with a list of fraud keywords to use in his search. Which of the following words found in email text might indicate a fraudster is rationalizing his actions?
	a) Write off
	b) Deserve
	c) Override
	d) Quota
22	If an information thief has long range interest in monitoring of a company, he might place a spy in that target company as a permanent employee. This employee is known as …….
	a) Sleeper
	b) Mole
	c) Detective
	d) Insider Spies
23	The existence of the following might indicate presence of Ghost Employees:
	a) Employees with no withholding
	b) No employees with same address
	c) No employye with same PAN
	d) No employee with same account number
24	In Health Care Fraud, …….. reimbursement occurs when providers receive payment for each service rendered.
	a) Capitation
	b) Fee for Service
	c) Episode of Care
	d) None of the above
25	Which of the following are the best for a comprehensive investigation ……
	a) Data vouching, trend analysis
	b) Trend analysis and tests of logic and absurdities
	c) Data vouching and tests of impossibilities

	d) All of the above to the extent possible in every case
26	Luhn's algorithm is …….
	a) A tool to find out valid credit card numbers
	b) A tool to find out invalid debit card numbers
	c) A tool to find valid or invalid debit cards/credit cards
	d) None of the above
27	Which of the following is not an indication of Money laundering?
	a) Use of third party cheque for making purchases
	b) Lump sum payment made by wire transfer
	c) Willingness to provide normal information
	d) Request to borrow maximum cash value of a single premium policy soon after paying for the policy.
28	An employee has duty to cooperate during internal investigation irrespective of nature of investigation.
	a) True
	b) False
29	Which situation will not give rise to sanctions for failing to preservce evidence include intentionally or accidentally?
	a) Erasing computer file relevant to unanticiapated litigation
	b) Destroying physical evidence relevant to existing litigation
	c) Losing documents relevant to anticipated litigation
	d) Failing to suspend routine destruction of electronic data relevant to existing litigation
30	……. refers to defamatory statements in writing.
	a) Slander
	b) Human Rights
	c) Libel
	d) Breach of Privacy
31	To establish libility for public disclosure of private facts, the plaintiff must prove following elements:
	(i) The defendant made public statements about another party's private life.
	(ii) The statements were not of public concern.
	(iii) The statements would be highly offensive to a reasonable person.
	a) (i) only
	b) (i) and (ii) only
	c) All of the above
	d) None of the above

32	…… software gives investigators the ability to image a drive and preserve it in a forensic manner.
	a) Stego Suite
	b) Forensic Toolkit (FTK)
	c) Recovery Toolkit
	d) Encase Forensic
33	Which is not a process for tracing illicit transactions?
	a) Collect Information
	b) Profile the subject
	c) Interview the subject
	d) Review information for leads
34	Fraud Assessment questioning is a non-accusatory interview technique used as a part of normal audit.
	a) True
	b) False
35	Following employee can be exempted from Fraud Awareness Training program -
	a) Top Level staff
	b) Middle Level Staff
	c) Lower Level Staff
	d) None of the above
36	……. is the impression a writing instrument leaves on sheets of paper below the sheet that contains the original writing.
	a) Indented Writing
	b) Freehand Forgeries
	c) Autoforgeries
	d) Imitator style
37	To avoid smudging and contamination, fraud examiners should use …… when handling latent finger print evidence.
	a) Protective Gloves
	b) Acid free paper envelopes
	c) Dusting powder
	d) None of the above
38	While interviewing, Amar, forensic auditor, locks the door of interview room. This can be claimed as ……. by the interviewee.
	a) Human Right Violation
	b) Actual Imprisonment
	c) False Imprisonment

	d) True Imprisonment
39	While doing interview, Amar, forensic auditor, was doing covert recording of interview process. It helps Amar to deny the recording when asked without taking ownership of recording.
	a) True
	b) False
40	…… is a defence mechanism that protects an individual from items that would cause anxiety by prevneting the items from becoming concious.
	a) Etiquette
	Ego Threat
	c) Depression
	d) Repression
41	Amar, a Certified Fraud Examiner, has obtained an oral confession from Vijay, a fraud suspect. Amar wants to probe Vijay for additional details. Which of the following is the most appropriate question Amar should ask Vijay to find out if there are any remaining proceeds that can be used to reduce losses?
	a) "Did you spend everything?"
	b) "What do you have left?"
	c) "Is there anything left?"
	d) "It's all gone, isn't it?"
42	Amar, a Certified Fraud Examiner, is conducting an admission-seeking interview of Vijay, a fraud suspect. Amar has a great deal of documentary evidence that he plans on using to diffuse Vijay's alibis. The proper technique for using the evidence is for Amar to display it all at once so that Vijay will be demoralized by the overwhelming amount of evidence.
	a) True
	b) False
43	In interview situations, it is sometimes recommended that the interviewer shake hands with the respondent. What is the purpose of this?
	a) Social courtesy
	b) Professional courtesy
	c) To establish the interview purpose
	d) To break down psychological barriers
44	Forensic analysis can be performed directly on suspect devices because doing will not alter or damage digital evidence.
	a) True

	b) False
45	Which is not a Red Falg associated with Fictitious Revenue?
	a) An unusually large amount of long overdue accounts receivable
	b) Rapid growth or unusual profitability
	c) Significant sales to entities whose substance not known
	d) Inventory totals appear forced
46	Vijay, a manager at a major company, is suspected of financial statement fraud. During an admission-seeking interview with Vijay, the investigator states: "A lot of employees count on the company doing well. I know you only did this to help the company succeed. Isn't that right?" This technique is known as:
	a) Genuine need
	b) Extrinsic rewards
	c) Altruism
	d) Depersonalizing the victim
47	Vijay, a fraud suspect, has confessed to Amar, a Fraud Examiner, that he has embezzled funds. Amar is unsure whether Vijay had an accomplice. Which of the following is the most appropriate question concerning accomplices?
	a) "Who else knew about this besides you?"
	b) "Was anyone else involved?"
	c) "Did someone else know?"
	d) "We have evidence someone else is involved. Who is it?"
48	Which of the following is a good practice for taking notes during an interview?
	a) Slow down the interview process if necessary to take accurate notes.
	b) Avoid making notes regarding opinions or impressions about a witness
	c) Write down verbatim all responses given by the subject during the interview.
	d) Make any necessary additions to interview notes within several weeks of the interview
49	During the introductory phase of the interview, the interviewer should avoid terms such as:
	a) Investigation
	b) Review
	c) Inquiry
	d) All of the above
50	Whenever possible, make a list of questions to be asked during the interview. It helps in maintaing the flow of interview.
	a) True
	b) False

51	if the interviewer has reason to believe that the respondent is being deceptive, he should begin asking ……..
	a) Direct Questions
	b) Closing Questions
	c) Admission seeking Questions
	d) Assessment Questions
52	Which of the following is not the objective of Introductory questions ?
	a) Establish Rapport
	b) Establish Interview Theme
	c) Observe reactions
	d) Reconfirm Facts
53	What is your digital footprint?
	a) A scanned image of your foot
	b) All the information online about a person that is stored online.
	c) A photograph of your shoe
	d) Having a blog, facebook or twitter page
54	We use Cryptography term to transforming messages to make them secure and immune to ……..
	a) Change
	b) Idle
	c) Attacks
	d) Defend
55	Confidentiality with asymmetric-key cryptosystem has its own ……..
	a) Entities
	b) Data
	c) Problems
	d) Translator
56	In a _____ scheme, the fraudster leave malware infected USB flash drive in places where people will find them easily.
	a) Baiting
	b) Pharming
	c) Malware
	d) Malicious Insider
57	Why would a hacker use a proxy server?
	a) To create a stronger connection with the target.
	b) To create a ghost server on the network.
	c) To obtain a remote access connection.

	d) To hide malicious activity on the network.
58	What type of attack uses a fraudulent server with a relay address?
	a) NTLM (NT LAN Manager)
	b) MITM (Man-in-the-middle)
	c) NetBIOS (Network Basic Input/Output System)
	d) SMB (Server Message Block)
59	Which phase of hacking performs actual attack on a network or system?
	a) Reconnaissance
	b) Maintaining Access
	c) Scanning
	d) Gaining Access
60	Social engineering is one of the most successful attack methods of cybercriminals. What is regarded as a form of social engineering?
	a) Cryptoware
	b) Denial of Service (DOS) attack
	c) Phishing
	d) Spam
61	Biometrics become ever more important as a means to verify the identity of users. Which feature of biometrics represents a major consideration for organizations that want to implement it?
	a) The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are equal.
	b) The way users swipe their tablet or smartphone can be used as a behavioral mechanism for biometrics.
	c) The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are within acceptable levels.
	d) Face recognition cannot be used as a biometric mechanism, because it is very inaccurate.
62	Digital certificates represent an important component in any Public Key Infrastructure (PKI). What should never be included in a digital certificate?
	a) The digital signature of the certificate authority (CA) that has issued the digital certificate.
	b) The private key of the party to whom the digital certificate is tied.
	c) The identity of the party that owns the digital certificate.
	d) The start and end date of the period, in which the digital certificate is valid.
63	What is the purpose of a Denial of Service attack?
	a) Exploit a weakness in the TCP/IP stack
	b) To execute a Trojan on a system
	c) To overload a system so it is no longer operational
	d) To shutdown services by turning them off

64	How is IP address spoofing detected?
	a) Installing and configuring a IDS that can read the IP header
	b) Comparing the TTL values of the actual and spoofed addresses
	c) Implementing a firewall to the network
	d) Identify all TCP sessions that are initiated but does not complete successfully
65	Phishing is a form of ……
	a) Spamming
	b) Identify Theft
	c) Impersonation
	d) Scanning
66	Keyloggers are a form of ……..
	a) Spyware
	b) Shoulder surfing
	c) Trojan
	d) Social engineering
67	Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?
	a) User-based
	b) Computer-based
	c) Human-based
	d) Web-based
68	SQL injection is an attack in which …… code is inserted into strings that are later passed to an instance of SQL Server.
	a) Non malicious
	b) Clean
	c) Redundant
	d) Malicious
69	Which of the following is a proper acquisition technique?
	a) Disk to Image
	b) Disk to Disk
	c) Sparse Acquisition
	d) All of the above
70	Which duplication method produces an exact replica of the original drive?
	a) Bit-Stream Copy
	b) Image Copy
	c) Mirror Copy
	d) Drive Image
71	What should you do if the computer is turned on?

	a) Shut it down
	b) Unplug it
	c) Start typing
	d) Log the user off
72	What happens when first securing the area?
	a) Start looking for evidence
	b) Make sure that the crime scene is safe
	c) Gather evidence
	d) Make sure computer is on
73	The risk of contamination of evidence is controlled and/or minimised by ……..
	a) Minimising the number of people handling the evidence.
	b) Storing packages in a dedicated secure area.
	c) Opening each package in an area other than where it was originally sealed.
	d) Using chain of custody labels.
74	Corroborative evidence is ……..
	a) Evidence that links an individual with a particular location.
	b) Evidence that associates an individual with another individual.
	c) Evidence that refutes other evidence.
	d) Eidence that supports other evidence.
75	What is the most significant legal issue in computer forensics?
	a) Preserving Evidence
	b) Seizing Evidence
	c) Admissibility of Evidence
	d) Discovery of Evidence
76	As a good forensic practice, why would it be a good idea to wipe a forensic drive before using it?
	a) No need to wipe
	b) Chain of Custody
	c) Different file and operating systems
	d) Cross-contamination
77	SQL Injection is ……
	a) Physical Threat
	b) Application Threat
	c) Malicious Code
	d) Mobile Code
78	Cyber Forensic Investigation Process consists of …….
	a) Imaging - Copy - Analysis - Communication.
	b) Imaging - Cloning - Documenting - Communication.

	c) Identification - Preservation - Collection - Analysis - Communication.
	d) Searching - Extracting - Imaging - Cloning - Analysis.
79	Signature forgery can best be spotted by ……
	a) Juxtaposition and Comparison of signatures on two documents
	b) Juxtaposition and Comparison of a signature on a document with specimen signature
	c) Juxtaposition and comparison of signatures on several documents
	d) Any of the above
80	When a hash function is used to provide message authentication, the hash function value is referred to as ……
	a) Message Field
	b) Message Digest
	c) Message Score
	d) Message Leap
81	The main difference in MACs and digital signatures is that, in digital signatures, the hash value of the message is encrypted with a user's public key.
	a) True
	b) False
82	In which the database can be restored up to the last consistent state after the system failure?
	a) Backup
	b) Recovery
	c) Both
	d) None
83	Most backup and recovery commands in …….. are executed by server sessions.
	a) Backup Manager
	b) Recovery Manager
	c) Backup and Recovery Manager
	d) Database Manager
84	Which of the following is not a recovery technique?
	a) Deferred update
	b) Immediate update
	c) Two-phase commit
	d) Recovery management
85	Failure recovery and media recovery fall under .....
	a) Transaction recovery
	b) Database recovery

	c) System recovery
	d) Value recovery
86	……. means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services.
	a) Cyber Stalking
	b) Pornography
	c) Web Hijacking
	d) Hacking
87	……. register domain name identical to popular service provider's name. So as to attract their users and get benefit from them.
	a) Cyber squatters
	b) Phishing Attack
	c) Identity Theft
	d) Cyber Defamation
88	…… involves changing data prior or during input into a computer.
	a) Forgery
	b) Cyber Defamation
	c) Email spoofing
	d) Data diddling
89	As per ……., the auditor's report should state whether the company has adequate Internal Financial Control system in place and the operating effectiveness of such controls.
	a) Section 134
	b) Section 137
	c) Section 143
	d) Section 177
90	Fraud reporting should be done to Central Govt. in ……
	a) Form ADT-1
	b) Form ADT-2
	c) Form ADT-3
	b) Form ADT-4
91	……. dealing with compensation for failure to protect data.
	a) Section 41
	b) Section 43-A
	c) Section 65
	d) Section 66
92	Section 66E deals with ……
	a) Sending offensive messages
	b) Cheating by personation

	c) Privacy violation
	d) Cyber terrorism
93	……deals with publishing or transmitting obscene material in electronic form.
	a) Section 43
	b) Section 65
	c) Section 66
	d) Section 67
94	Section 75 of Indian Evidence Act, 1872 deals with ……
	a) Public Documents
	b) Private Documents
	c) Certified copies of Public Documents
	d) Proof of other official documents
95	A witness who is unable to speak is called …….
	a) Deaf Witness
	b) Dumb Witness
	c) Hostile Witness
	d) Unreliable Witness
96	Entries in the books of accounts regularly kept in the course of business are admissible under section 34 of Evidence Act
	a) If they by themselves create a liability
	b) If they by themselves do not create a liability
	c) Irrespective of whether they themselves create a liability or not
	d) Either (a) or (b)
97	Amar, a Forensic Auditor, has obtained an oral confession from Vijay, a fraud suspect. Vijay confessed to committing fraud, and he admitted to smuggling drugs in an unrelated case. How should Amar handle these admissions in Gamma's written confession?
	a) Amar should omit the information concerning the drug smuggling
	b) Amar should take separate statements for each of the unrelated crimes
	c) Amar should include both crimes in the same statement
	d) None of the above
98	Amar, a Fraud Investigator, is investigating Vijay, who is active on an online social networking site in which he voluntarily shares information about himself. Amar wants to search and extract information from Vijay's social network profile. Which of the following is the most accurate statement about the privacy of information Vijay shared through his social network profile?
	a) To search for information that Vijay posted and made available to the public through his social network profile, Amar must provide Vijay notice before hand.
	b) To access any information posted on Vijay's social network profile, Amar must obtain some type of legal order from the jurisdiction in which Vijay resides.

	c) The Privacy of Social Networks Treaty is an international law that makes it illegal for Amar to seek the login credentials from Vijay's social networking account.
	d) Amar could be liable for violating Vijay's privacy rights if he hacks or breaks into areas of the social networking site Vijay has designated as private
99	What is Mutual Legal Assistance (MLA)?
	a) A process by which countries request and provide assistance in law enforcement matters
	b) A letter whereby a criminal defendant requests that the government release exculpatory information
	c) A formal request by the courts of one country seeking judicial assistance from the courts of another country
	d) A formal request by the government of a country seeking information from a defendant residing in another country
100	In most common law jurisdictions, for a document to be admitted into evidence, it must be properly _____ that is, the party offering the document must produce some evidence to show it is, in fact, what the party says it is.
	a) Validated
	b) Marked
	c) Certified
	d) Authenticated

1. **The warehouse supervisor in ABC Ltd. has stolen ₹ 5 lakhs worth of inventory over the last year. He has made no effect to conceal his theft in any of the inventory records. During as analytical review of the financial statements, which of the following red flag might the auditor find that would indicate the inventory theft?**

   a) The percentage change in cost of goods sold was significantly higher than the percentage change in sales.
   b) The percentage change in sales was significantly higher than the percentage change in cost of goods sold.
   c) Sales and cost of goods sold moved together.
   d) None of the above.

2. **When circumstantial evidence is offered to prove that a subject has more income available than can be accounted for from legitimate sources, the subject often responds with which of the following defences?**

   a) The subject has no taxable income.
   b) The subject's excess funds were deobligated.
   c) The subject incurred substantial debts.
   d) The subject's excess funds were received as gifts.

3. **Which of the following statement concerning public records is most accurate?**

a) Public records are the primary source of individual health information
b) Public records are those maintained by public companies
c) Public records are valuable for obtaining background information on individuals
d) Public records are useful for searching banking records

4. **SQL injection is an attack in which …… code is inserted into strings that are later passed to an instance of SQL Server.**

a) Non malicious
b) Clean
c) Redundant
d) Malicious

5. **Section 66F of the Information Technology Act deals with ……**

a) Sending offensive messages
b) Cheating by personation
c) Privacy violation
d) Cyber terrorism

6. **Which of the following is a method in which contractors can inflate labour costs in negotiated contracts?**

a) Use higher wage personnel to perform work at lower rates.
b) Subcontract to affiliated companies at inflated rates.
c) Account for learning curve cost reductions.
d) Use valid cost schedules.

7. **Which of the following is the most appropriate type of question for fraud examiners to ask during interviews to confirm facts that are already known?**

a) Open
b) Leading
c) Complex
d) Narrative

8. **Which of the following activities are included in the bid evaluation and award phase of procurement involving open and free competition?**

a) The procuring employees issue the solicitation document.

b) The procuring employees develop the bid specifications.
c) The procuring employees assess the bids or proposals.
d) The procuring employees perform their contractual obligations.

9. **In MS-Excel, what is the correct way to refer the cell C5 on Worksheet named "Report" from Worksheet named "Sales Data"?**

a) =[Sales Data]!C5
b) =$C$5
c) ='Sales Data'!C5
d) ="Sales Data"!$C$5

10. **Act of obtaining information of a higher level of sensitivity by combining information from lower level of sensitivity is called?**

a) Aggregation
b) Data mining
c) Inference
d) Polyinstantiation

11. **Bars, restaurants, and nightclubs are favourite businesses through which to launder funds because:**

a) It is easy to match the cost of providing food, liquor, and entertainment with the revenues they produce.
b) They charge relatively low prices for services.
c) Sales are generally in cash.
d) All of these choices are correct.

12. **…… may not contain in Excel Formula.**

a) Text Constant
b) Mixed Reference
c) Circular Reference
d) All of the above

13. **In …… fraud scheme, Procurement official acts above or below normal scope of duties in awarding or administering contract.**

a) Bribes and Kickbacks
b) Manipulation of Bids
c) Split Purchases
d) Unnecessary Purchases

14. **Suppose you suspect there is a Ghost Employee scheme taking place in your organisation and you want to compare the payroll records to the employee master**

file. Which data analysis technique would you use to match these two data records?

a) Compliance verification
b) Correlation analysis
c) Join function
d) Gap Testing

15. All of the followings are hashing algorithms except …….

a) SHA
b) MFT
c) HAVAL
d) MD2

16. Common fraud schemes involving ATMs include all of the following Except:

a) Counterfeit ATM cards
b) Employee manipulation
c) Unauthorised access to PINs and account codes
d) Credit data blocking

17. In ……. Scheme, the company that initially conned a consumer contacts that consumer and offers to help retrieve the lost money. However, the investigation requires an upfront fee and the consumer is swindled again.

a) Retrieval
b) Double Hustle
c) Advance Fee
d) Scavenger

18. …….. can act as a "National Focal Point" for gathering information on threats and facilitating the Central Government's response to computer based incidents.

a) Intelligence Bureau
b) CBI
c) CERT-IN
d) Cyber Cell

19. …….. is a method of using software to extract usable information from unstructured data.

a) Linguistic Analytics
b) The Fog Index
c) Textual Analytics
d) Benford's Law

20. **Amar, a Fraud Investigator, is investigating Vijay, who is active on an online social networking site in which he voluntarily shares information about himself. Amar wants to search and extract information from Vijay's social network profile. Which of the following is the most accurate statement about the privacy of information Vijay shared through his social network profile?**

a) To search for information that Vijay posted and made available to the public through his social network profile, Amar must provide Vijay notice before hand.
b) To access any information posted on Vijay's social network profile, Amar must obtain some type of legal order from the jurisdiction in which Vijay resides.
c) The Privacy of Social Networks Treaty is an international law that makes it illegal for Amar to seek the login credentials from Vijay's social networking account.
d) Amar could be liable for violating Vijay's privacy rights if he hacks or breaks into areas of the social networking site Vijay has designated as private

21. **Which of the following is typically the most effective way to document chain of custody for a piece of evidence?**

a) An affidavit signed by the forensic auditor swearing to the evidence's contents
b) Photographs of the evidence that clearly show what the evidence is and where it was originally found
c) A memorandum with the custodian of the evidence when the evidence is received
d) A video recording of the forensic auditor explaining the process used to collect the evidence.

22. **…… is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.**

a) Steganography
b) Computer Forensics
c) Both (a & b)
d) None of the above

23. **Because Digital evidence is different from tangible evidence, the rules regarding its admissibility in court are very different from the rules governing the admissibility of tangible evidence.**

a) True
b) False

24. **Building a business case can involve which of the following?**

a) Procedures for gathering evidence
b) Testing software
c) Protecting trade secrets
d) All of the above

25. A fraud scheme in which an accountant fails to write down obsolete inventory to its current fair market value has what effect on the company's current ratio?

a) The current ratio will be artificially inflated.
b) The current ratio will be artificially deflated.
c) It is impossible to determine.
d) The current ratio will not be affected.

26. Which of the following is a legal element that must be shown to prove a claim for fraudulent misrepresentation of material facts?

a) The defendant acted negligently.
b) The victim failed to exercise due care in relying on the representation.
c) The defendant had a duty to disclose the information.
d) The defendant made a false statement.

27. Mr. Ram has been retained by an attorney to testily as an expert witness at Mr. Mallya's trial. Coincidentally. Mr. Ram also met Mr. Mallya while attending a university many years earlier. The attorney is compensating Mr. Ram for his services. Which of the following statements concerning conflicts of interest is MOST ACCURATE?

a) Mr. Ram should not serve as an expert witness because he is being compensated, which is a conflict of interest.
b) Mr. Ram should not serve as an expert witness because he knew Mr. Mallya from attending the university, which is a conflict of interest
c) Mr. Ram can serve as an expert witness because there are not conflicts of interest in this case.
d) Mr. Ram can only serve as an expert witness if he is able to objectively evaluate and present the case issues.

28. Following are Red Flag Indicators of Phantom Vendors, except –

a) Invoiced goods or services cannot be located or verified
b) No employee Identification Number (EIN) provided
c) Invoice has an unusual or unprofessional appearance
d) Bid prices drop when a new bidder enters the competition

29. What is the most critical aspect of computer evidence?

a) Validation of digital evidence
b) Security of digital evidence
c) Collection of digital evidence
d) List of digital evidence

30. Keeping track of the amount of paper generated is one of the biggest challenges in forensic audit. Which of the following is generally NOT a recommended practice when organizing evidence?

a) Make a key document file
b) Segregate documents by witness
c) Establish a database early on
d) File all papers chronologically

31. Which of the following statements about how Forensic Auditors should approach fraud examinations is CORRECT?

a) In most examinations, Forensic Auditors should start interviewing the suspect and then work outward.
b) if an individual appears to be involved in the fraud scheme, he should be interviewed first.
c) Fraud examinations should begin with general information that is known, starting at the periphery, and then move to the more specific details.
d) All of the above.

32. Mr. Ram, Forensic Auditor, determines that a document that purports to be the original writing of a famous author created fifty years ago, is actually made from paper created no more than 2 years ago. Which of the following best describes the document?

a) An Auto forgery
b) An Anachronism
c) An Indented Writing
d) None of the above

33. In asymmetric key cryptography, the private key is kept by ……

a) Sender
b) Receiver
c) Sender and Receiver both
d) All the connected devices to the network

34. When gathering information for a fraud investigation, virtually all helpful documentary evidence will come from internal sources.

a) True
b) False

35. Which of the followings is an example of simple substitution algorithm?

a) Rivest, Shamir, Adleman (RSA)
b) Data Encryption Standard (DES)
c) Blowfish
d) Caesar cipher

36. Mr. Ram, Forensic Auditor, is conducting an admission seeking interview. Which of the following strategies should Mr. Ram follow in his attempt to obtain a confession?

a) Imply that time is of the essence to pressure the subject into confessing.
b) Conduct the interview in a firm, yet compassionate manner.
c) Minimise sympathy and maximise the perception of wrongdoing.
d) Avoid potential liability by making the accusation in the presence of outsiders.

37. Mr. Shyam is on the boards of two companies that compete in the highway construction industry. Paul does not disclose this conflict, and he does not step down from the board of either company. If Mr. Shyam's acts are discovered and he is sued for violating his fiduciary duties, under what theory is the suit most likely to be filed?

a) Violating the duty of fair competition
b) Violating the duty to disclose
c) Violating the duty of loyalty
d) Violating the duty of care

38. Which of the following is an information security goal that an e-commerce system should strive to provide its users and asset holders?

a) Non repudiation
b) Exactness
c) Access authority
d) System reliability

39. What effect would improperly recording an expenditure as a capitalised asset rather than as an expense have on the financial statement?

a) Expenses would be overstated, giving the appearance of poor financial performance.
b) Net income would be falsely understated, lowering the company's tax liability.
c) Assets would be falsely overstated, giving the appearance of a stronger company.

d) None of the above

40. Sending offensive messages through communication service, causing annoyance etc. through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered under ..... of the Information Technology Act.

a) Section 66A
b) Section 66D
c) Section 66E
d) Section 66F

41. As per DOT, using spoofed call service is illegal as per the ……

a) Indian Telegraph Act, Sec 25(c).
b) Indian Penal Code Act, Sec 25(c).
c) Indian IT Act, Sec 25(c).
d) Indian Telecommunication Act, Sec 25(c).

42. From a legal perspective, which rule must be addressed when investigating a computer crime?

a) Search and seizure
b) Data protection
c) Engagement
d) Evidence

43. When a forensic investigator is seizing a running computer for examination, he can retrieve data from the computer directly via its normal interface if the evidence needed exists only in the form of volatile data.

a) TRUE
b) FALSE

44. In Interview situations, …… is defined as a "relation marked by harmony, conformity, accord or affinity."

a) Norming
b) Rapport
c) Active Listening
d) Calibration

45. Which of the following is a recommended method for organising and presenting information in a fraud examination report?

a) By the order in which the information was discovered
b) By party
c) Chronologically
d) All of the above

46. What is the advantage of using a tape backup system for forensic acquisitions of large data sets?

a) Tape backup system is more secure
b) Magnetic Tapes are condensation resistance
c) Magnetic Tapes are useful for long-term storage of data at infinite scale
d) Writing large data to Magnetic Tapes is faster as compared to other media

47. During the introductory phase of the interview, the interviewer should avoid terms such as:

a) Investigation
b) Review
c) Inquiry
d) All of the above

48. In IDEA, Query can be written in …….

a) Formula Editor
b) Query Editor
c) Equation Editor
d) None of the above

49. …….. refers to any statistical process used to analyse data and draw conclusions from the findings.

a) Data Analysis
b) Data Mining
c) Big Data
d) None of the above

50. Which of the following is not a component of "chain of evidence"?

a) Location evidence obtained.
b) Time evidence obtained.
c) Who discovered the evidence.
d) Identification of person who left the evidence.

51. In interviews, …… communication involves the use of volume, pitch, voice quality to convey meaning.

a) Kinetic

b) Chronemic
c) Paralinguistic
d) Proxemic

52. Which of the following best describes Social Engineering?

a) A method for gaining unauthorised access to a computer system in which an attacker bypasses a system's security through the use of an undocumented operating system and network functions.
b) A method for gaining unauthorised access to a computer system in which an attacker hides near the target to obtain sensitive information that he can use to facilitate his intended scheme.
c) A method for gaining unauthorised access to a computer system in which an attacker deceives victims into disclosing information or convinces them to commit acts that facilitate the attacker's intended scheme.
d) A method for gaining unauthorised access to a computer system in which an attacker searches through large quantities of available data to find sensitive information that he can use to facilitate his intended scheme.

53. Which of the following is true for the Statistical sampling of data?

a) The auditor should not be restricted to explicit numbers as to materiality or risk.
b) The auditor needs to employ professional subjective judgment.
c) Allows the auditor to maintain professional judgment in regard to audit risks and materiality.
d) There is a unique issue where there is a need for a less rigid standardized approach.

54. In MS-Excel, a function inside another function is called ……

a) Complex function
b) Multiple function
c) Nested function
d) Mixed function

55. What does MFT stand for?

a) Master Folder Table
b) Master Format Table
c) Master File Table
d) Master FAT Table

56. A utility designed to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a file or entire disk is called …….

a) Brute-Force Scripting
b) Bit locker
c) Hashing Algorithm
d) Binary Sniffing

57. For employee expense reimbursement request, electronic receipts are preferred to paper receipts because they are more difficult to alter or forge.

a) True
b) False

58. When a caller ID display a phone number different from that of the telephone from which the call was placed is called ……

a) Cellular Fraud
b) Caller ID Phishing
c) Caller ID Spoofing
d) Unethical Hacking

59. While examining a document, a fraud examiner notices some very faint indented writings that might aid the examination if revealed. Which of the following would be the forensic auditor's best course of action in analysing these indented writings?

a) Performing the pencil shading method
b) performing the pencil scratching method
c) Applying a few drops of liquid and observing the liquid's flow in the indentations
d) Employing an expert to use an electrostatic detection apparatus

60. During an interview, Mr. Shyam, an employee at ABC Ltd, confesses to Mr. Ram, Forensic Auditor, that he has been embezzling money from the company. Which of the following pieces of information does Mr. Ram NOT have to obtain from Mr. Shyam?

a) Information about involvement of other employees
b) A statement from Mr. Shyam that his conduct was an accident
c) An estimate of the amount of money Mr. Shyam embezzled.
d) The approximate date Mr. Shyam started embezzling the money.

61. …… was designed to protect against accidental errors, such as a digit mistyping.

a) Relative Size Factor
b) Luhn algorithm
c) Benford's Law
d) None of the above

62. In MS-Excel, while splitting Text String in a column with Text to Columns, the data in original column can be retained.

a) True
b) False

63. What is the health care industry concerned about the potential effect of the Electronic Data Interchange (EDI) on fraudulent activity?

a) Only a few types of health care transactions can be process by EDI.
b) The tools required to detect EDI fraud are difficult to use.
c) The efficiency of EDI allows for more vendors and thus more claims to process.
d) All of the above.

64. Which of the following statement is True regarding a fictitious refund scheme?

a) The victim company's inventory is understated.
b) The amount of cash in the register balances with the register log.
c) Inventory is returned to the store.
d) All of the above.

65. Where is the data for roaming phones stored?

a) HLR (Home Location Register)
b) GSM (Global System for Mobile communications)
c) BTS (Base Transceiver Station)
d) VLR (Visitor Location Register)

66. Which of the following is a method that investigators can use to detect steganography?

a) Analysing files on a computer system for structural oddities that suggest manipulation.
b) Determining whether the statistical properties of files deviate from the expected norm.
c) Looking for visual anomalies in jpeg, bmp and other image files.
d) All of the above.

67. When searching regulatory securities records for information on a publicly traded company, which of the following information is least likely to be found?

a) Major events that are of interest to investors
b) Identity of the company's officers and directors
c) Identity of major owners of the company
d) The complete books and records of the company

68. **Forensic Auditor visited a project site and discovered a road of sub-standard quality. The road was built 50 percent narrower than specifications and lacked road surfacing. Nevertheless, the contract was paid in full. It is ……. Type of Fraud.**

a) Product substitution
b) Substandard work
c) Deviation from specifications
d) Failure to deliver

69. **Offences related to infringements of copy rights are extraditable offences.**

a) True
b) False

70. **Mr. Ram, Forensic Auditor, conducted an interview of Shyam, the controller of the ABC Ltd. Mr. Ram asked the following question: "Since you were here when the controls were developed, can you tell me how they came about?" This kind of question is called .....**

a) Complex Question
b) Controlled Answer Technique
c) Double Negative Question
d) Open Question

71. **Which of the following is NOT a type of physical access control device that can be used to control access to physical objects?**

a) Biometric systems
b) Profiling software
c) Electronic access cards
d) Locks and keys

72. **What part of a cloud implementation provides the virtual servers with access to resources?**

a) Hypervisor
b) Resource monitor
c) Resource auditor
d) Virtual Manager

73. A Forensic Auditor is deciding whether to conduct a traditional or a covert examination for a suspected fraud. Which of the following factors would be most favourable to conducting a covert examination?

a) There are sufficient details at the present time to apprehend the suspect.
b) The Forensic Auditor would like to determine who is responsible for known losses occurring in a certain area.
c) The Forensic Auditor finds it important to collect information in a direct manner from people possessing it.
d) The Forensic Auditor has several avenues through which he can obtain the necessary information.

74. Before powering off a computer system, a computer crime investigator should record contents of the monitor and ……...

a) save the contents of the spooler queue.
b) backup the hard drive.
c) dump the memory contents to a disk.
d) collect the owner's boot up disks.

75. Which of the two key functions is included in IDEA to identify exceptions, irregularities, anomalies and errors?

a) Error Detection & Duplicate Detection
b) Anomalies Detection & Exception Detection
c) Anomalies Detection & Duplicate Detection
d) Gap Detection & Duplicate Detection

76. Which of the following types of transactions is most likely to use a Person-to-person (P2P) payment system?

a) A person paying for movie tickets at an automated kiosk.
b) A person buying groceries at the supermarket.
c) A company using a bank's online payment system to make a loan payment.
d) A person buying a book on an online auction site.

77. Which of the following statement best describes the function of metasearch engines such as Sputtr, Dogpile and Mamma?

a) Metasearch engines contain links to websites that are sorted into categories
b) Metasearch engines send user requests to several search engines and aggregate the results for display
c) Metasearch engines narrow searches to only those search engines that achieve the best results
d) None of the above

78. **Which of the following facts would best support the defence of a law enforcement officer against an allegation of entrapment?**

a) The officer acted without malice
b) The officer acted based on a tip from a reliable source
c) The officer acted based on his suspicion of fraud
d) All of the above

79. **Which of the following evidence collection method is most likely accepted in a court case?**

a) Provide a full system backup inventory.
b) Create a file -level archive of all files.
c) Provide a mirror image of the hard drive.
d) Copy all files accessed at the time of the incident.

80. **What is the punishment for hacking of computers?**

a) Three year imprisonment or 10 lakh rupees penalty or both
b) Life Imprisonment
c) Three year imprisonment or 5 lakh rupees penalty or both
d) Three year imprisonment or 2 lakh rupees penalty or both

81. **Which of the following refers to investments that are designed to yield a tax benefit to the investor?**

a) Tax shelters
b) Tax havens
c) Secrecy jurisdictions
d) Money laundering havens

82. **Which of the following is a limitation of Benford's Law?**

a) Benford's Law can only be applied to data sets listed in currency amounts.
b) Benford's Law cannot be applied to data sets with non-natural numbers.
c) Benford's Law only works on data sets with assigned numbers.
d) Benford's Law applies best to data sets with three digit numbers.

83. **Mr. Ram, Forensic Auditor, is undertaking a data analysis engagement to identify potential fraud at ABC Ltd. Which of the following lists the most appropriate order in which he should conduct the steps involved in the data analysis process?**

I. Cleanse and normalise the data
II. Build a profile of potential frauds
III. Analyse the data
IV. Obtain the data
V. Monitor the data

a) IV, I, III, V, II
b) II, IV, III, I, V
c) II, IV, I, III, V
d) IV, II, I, V, III

84. A Forensic Auditor discovers that Mr. Shyam, a fraud suspect, has made dozens of cash deposits over the last few months into a bank account. None of the deposits have been Rs. 50,000 or more, and none of them have been below Rs. 45,000, either. The currency reporting threshold for cash deposits at financial institutions in the jurisdiction is Rs. 50.000. Based on this information, which of the following schemes is Mr. Shyam most likely committing?

a) Cash Transactions Fraud
b) Suspicious Transaction Fraud
c) Smurfing
d) Channel Stuffing

85. Pharming differs from Phishing in that in a pharming scheme:

a) The attacker delivers the solicitation via telephones using Voice over Internet Protocol instead of email.
b) The attacker delivers the solicitation message via SMS instead of email.
c) The attacker does not have to rely on having the user click on a link in an email to direct him to malicious website that is imitating a legitimate website.
d) The attacker has to rely on having the user click on a link in an email to direct him to the malicious website that is imitating a legitimate website.

86. A virus that changes as it spreads is called what?

a) Multipartite
b) Armored
c) Changeling
d) Polymorphic

87. Which of the following functions does a Benford's Law analysis help to achieve?

a) Measuring the relationship between items on financial statements by expressing accounts as percentages.
b) Extracting usable information from unstructured text data.
c) Identifying duplicate payments
d) Identifying fictitious numbers.

88. …….. is a powerful test for detecting errors.

a) Relative Size Factor
b) Luhn algorithm

c) Benford's Law
d) None of the above

89. The encoding step of a …… system identifies redundant bits and then replaces a subset of them with data from a secret message.

a) Phishing
b) Steganographic
c) SQL Injection
d) Key Logging

90. Which of the following methods might be used to conceal a sham loan transaction in which the loan officer receives part of the proceeds (kickback)?

a) Letting the loan go into arrears
b) Charging off the loan as a bad loan
c) Digging the loan on the books
d) Turning the loan over to a collection agency

91. Following are part of Planning Phase in Data Analysis Process, except:

a) Understand the data
b) Build a profile of potential frauds
c) Obtain the data
d) Determine whether predication exists

92. Which of the following is an example of the Array Formula in MS-Excel?

a) =IF(A2:D4=3,MAX(A5:A10))
b) =IF(A2>=3,MAX(A5:A10))
c) =IF(A2<=3,MAX(A5:A10))
d) None of the above

93. Which of the following is TRUE concerning the volatility of digital evidence?

a) Even the integrity of digital evidence has been violated through alteration or destruction, it can be restored easily.
b) The failure to preserve the integrity of digital evidence could result in evidence being deemed inadmissible in a legal proceeding
c) Digital evidence is less volatile than tangible evidence because data cannot be altered or destroyed easily than tangible information
d) None of the above

94. Which of the following situation is often present in real estate fraud schemes?

a) A false appraisal report
b) No expert assistance at closing
c) The services of an arm's length representative

d) All of the above

95. Which of the following is one of the objectives on which the international Organization of Securities Commissions (IOSCO) Objectives and Principles of Securities Regulation are based?

a) Enhancing the financial system's growth
b) Ensuring that markets are fair, efficient, and transparent
c) Harmonizing securities laws and standards across the globe
d) Eliminating market risk

96. In MS-Excel, which of the following function would you use to compare two text strings in a database?

a) EXACT
b) MATCH
c) VLOOKUP
d) All of the above

97. Which of the following attack targets an application's backend database?

a) Phishing
b) Evading detection
c) URI Hacking
d) SQL Injection

98. Suppose that a forensic auditor is going to testify at trial about an examination report for a complex case, and the report contains summaries of the key documents that were created by someone other than the forensic auditor. Which of the following best describes what the forensic auditor should know about the documents underlying the summaries?

a) The forensic auditor must have read and analysed every document in the case.
b) The forensic auditor should conduct a complete review of the documents underlying the summaries.
c) The forensic auditor does not need to review the documents underlying the summaries.
d) The forensic auditor only needs to review some of the documents underlying the summaries for quality assurance.

99. In MS-Excel, you can group non-contiguous worksheets with ……

a) Group button on the standard toolbar
b) Ctrl key and the mouse
c) Shift key and the mouse
d) None of the above

100. Which of the following is a type of information that can be obtained from the deep web?

a) An old version of a web page that has since been updated.
b) Websites without any links pointing to them.
c) An archived version of a web page that is no longer online.
d) Web content indexed by standard search engines.