100 sample question TYBSc.CS sem-6 Cyber Forensics (USCS603)

1) The most common storage device for the personal computer is the:

   a)Flopy disk

   b)USB thumb drive

   c)Zip disk

   d)Hard disk drive

2) Computer forensics involves all of the following stated activities except:

   a)interpretation of computer data

   b)manipulation of computer data

   c)extraction of computer data

   d)preservation of computer data

3) The most popular software forensic tools include all of the following except:

   a)Forensic Autopsy®

   b)Forensics Toolkit®

   c)SMART®

   d)Quicken®

4) The area that begins at the end of the last sector that contains logical data and terminates at the end of the cluster is known as:

   a)RAM slack

   b)ROM slack

   c)File slack

   d)HDD slack

5) Areas of the disk that are not apparent to the user and sometimes not even to the operating system,is termed:

   a)latest data

   b)hidden data

   c)exceptional data

   d)missing data

6) There are three c's in computer forensics.Which is one of the three.

   a)control

b)chance

c)chaims

d)core

7) You are suppose to maintain three types of records.Which answer is not a record?

a)Chain of custody

b)Documentation of the crime scene

c)Searching the crime scence

d)Documnent ypur actions

8) Physical forensics discipline include which of the following?

a)Bloodstain

b)Eating

c)Searching

d)Watching

9) Which do you document an audio?

a)Write down information

b)Zoom in on evidence

c)close up images

d)your arrival time

10) 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

11) A valid definition of digital evidence is:

a. Data stored or transmitted using a computer

b. Information of probative value

c. Digital data of probative value

d. Any digital evidence on a computer

12) In terms of digital evidence, a hard drive is an example of:

a. Open computer systems

b. Communication systems

c. Embedded computer systems

d. None of the above

13) Computers can be involved in which of the following types of crime?

a. Homicide and sexual assault

b. Computer intrusions and intellectual property theft

c. Civil disputes

d. All of the above

14) A logon record tells us that, at a specific time:

a. An unknown person logged into the system using the account

b. The owner of a specific account logged into the system

c. The account was used to log into the system

d. None of the above

15) Cybertrails are advantageous because:

a. They are not connected to the physical world.

b. Nobody can be harmed by crime on the Internet.

c. They are easy to follow.

d. Offenders who are unaware of them leave behind more clues than they otherwise would have.

16) Private networks can be a richer source of evidence than the Internet because:

a. They retain data for longer periods of time.

b. Owners of private networks are more cooperative with law enforcement.

c. Private networks contain a higher concentration of digital evidence.

d. All of the above.

17) Personal computers and networks are often a valuable source of evidence. Those involved with _____ should be comfortable with this technology.

a. Criminal investigation

b. Prosecution

c. Defense work

d. All of the above

18) Computers can play the following roles in a crime:
    a. Target, object, and subject
    b. Evidence, instrumentality, contraband, or fruit of crime
    c. Object, evidence, and tool
    d. Symbol, instrumentality, and source of evidence
19) The following specializations exist in digital investigations:
    a. First responder (a.k.a. digital crime scene technician)
    b. Forensic examiner
    c. Digital investigator
    d. All of the above
20) The first tool for making forensic copies of computer storage media was:
    a. EnCase
    b. Expert Witness
    c. dd
    d. Safeback
21) One of the most common approaches to validating forensic software is to:
    a. Examine the source code
    b. Ask others if the software is reliable
    c. Compare results of multiple tools for discrepancies
    d. Computer forensic tool testing projects
22) An instrumentality of a crime is:
    a. An instrument used to commit a crime
    b. A weapon or tool designed to commit a crime
    c. Anything that plays a significant role in a crime
    d. All of the above
23) Contraband can include:
    a. Child pornography
    b. Devices or programs for eavesdropping on communications
    c. Encryption devices or applications
    d. All of the above

24) Stolen bank account information is an example of:

a. Hardware as contraband or fruits of crime

b. Information as contraband or fruits of crime

c. Information as an instrumentality

d. Information as evidence

25) A network sniffer program is an example of:

a. Hardware as contraband or fruits of crime

b. Hardware as an instrumentality

c. Information as an instrumentality

d. Information as evidence

26) In the course of conducting forensic analysis, which of the following actions are carried out?

a. Critical thinking

b. Fusion

c. Validation

d. All of the above

27) Having a member of the search team trained to handle digital evidence:

a. Can reduce the number of people who handle the evidence

b. Can serve to streamline the presentation of the case

c. Can reduce the opportunity for opposing counsel to impugn the integrity of the evidence

d. All of the above

28) Which of the following is not a type of cybercrime

a)Data theft

b)Forgery

c)Damage to data and system

d)Installing antivirus for protection

29) Which of the following are data compression technique?

a)LZW

b)Huffman coding

c)RLE

d)All of the above

30) _____ is the process of making an archival or back up copy of the entire contents of a hard drive.

A. Investigation

B. Disk imaging

C. Formatting

D .S/w Installation

31) A valid definition of digital evidence is:

a. Data stored or transmitted using a computer

b. Information of probative value

c. Digital data of probative value

d. Any digital evidence on a computer

32) In this phase from the collection data identify and extract the pertinent information using proper forensic tools.

a) Collection

b) Examination

c) Analysis

d) Reporting

33) What things are not recover while investigating the computer fraud:

a) Financial and asset record

b) Accounting software and files

c) Photos and diaries of the victim

d) Credit card data

34) This attack uses a killer packet to flood a system

a) DNS DoS attack

b) The Ping of death attack

c) SYN/LAND attack

d) Teardrop attacks

35) ____ types of evidence are collected in cyber forensic .

a) 5

b) 2

c) 3

d) 4

36) ODD stand for_____ in Cyber forensic.

a) Operation Data Directory

b) Open Data Duplicator

c) Open Data Device

d) Optional Device Driver

37) Wireshark is a _____ tool.

a) network protocol analysis

b) network connection security

c) connection analysis

d) defending malicious packet-filtering

38) Which of the following deals with network intrusion detection and real-time traffic analysis?

a) John the Ripper

b) LophtCrack

c) Snort

d) Nessus

39) In general how many key elements constitute the entire security structure?

a) 1

b) 2

c) 3

d) 4

40) According to the CIA Triad, which of the below-mentioned element is not considered in the triad?

a) Confidentiality

b) Integrity

c) Authenticity

d) Availability

41) CIA triad is also known as _____

a) NIC (Non-repudiation, Integrity, Confidentiality)

b) AIC (Availability, Integrity, Confidentiality)

c) AIN (Availability, Integrity, Non-repudiation)

d) AIC (Authenticity, Integrity, Confidentiality)

42) When integrity is lacking in a security system, _____ occurs

a) Database hacking

b) Data deletion

c) Data tampering

d) Data leakage

43) Data _____ is used to ensure confidentiality.

a) Encryption

b) Locking

c) Deleting

d) Backup

44) One common way to maintain data availability is _____

a) Data clustering

b) Data backup

c) Data recovery

d) Data Alterin

45) _____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

a) Network Security

b) Database Security

c) Information Security

d) Physical Security

46) From the options below, which of them is not a vulnerability to information security?

a) Flood

b) without deleting data, disposal of storage media

c) unchanged default password

d) latest patches and updates not done

47) Which of the following information security technology is used for avoiding browser-based hacking?

a) Anti-malware in browsers

b) Remote browser access

c) Adware remover in browsers

d) Incognito mode in a browser

48) The full form of EDR is _____

a) Endpoint Detection and recovery

b) Early detection and response

c) Endpoint Detection and response

d) Endless Detection and Recovery

49) Which of the following is not done in the gaining access phase?

a) Tunnelling

b) Buffer overflow

c) Session hijacking

d) Password cracking

50) Which of the below-mentioned penetration testing tool is popularly used in gaining access phase?

a) Maltego

b) NMAP

c) Metasploit

d) Nessus

51) A _____ can gain access illegally to a system if the system is not properly tested in scanning and gaining access phase.

a) security officer

b) malicious hacker

c) security auditor

d) network analyst

52) Which of the following is not a type of peer-to-peer cyber-crime?

a) Phishing

b) Injecting Trojans to a target victim

c) MiTM

d) Credit card details leak in deep web

53) Cyber-crime can be categorized into _____ types.

a) 4

b) 2

c) 3

d) 6

54) …… is a technique for anonymous communication where messages are encapsulated in layers.

a) AAAA

b) SMTP

c) Web Shell

d) Onion Routing

55) …… meaning how long piece of information lasts on a system

a) Order of volatility

b) DDOS

c) Honeypot

d) honeystick

56) ……. Is a file generated records of past events consist of timestamp

a) Log files

b) Memory files

c) reports

d) Meta data

57) ……. is a suite of tools created by Sysinternals

a) Browserhistory

b) Encase

c) FTK

d) pstools

58) …… is a computer or network setup to tempt an attacker to do the activity

a) Order of volatility

b) DDOS

c) Honeypot

d) honeystick

59) Computer forensics involves _____

a) obtaining and analyzing digital information

b) analysis of network traffic

c) protect evidences

d) all of the above

60) AFF stands for _____

a) Advanced Forensics Format

b) Analysis Forensics Format

c) Access Forensics Format

d) Acquire Forensics Format

61) In case of ----------, the evidence is collected from a system where the microprocessor is running.

a) live acquisition

b) static acquisition

c) sparse acquisition

d) none of the above

62) …… is a global system for translating IP addresses to human-readable domain names.

a) TLD

b) Web Shell

c) Whois

d) DNS

63) You begin any computer forensics case by creating a(n) ____.

a) investigation plan

b) risk assessment report

c) evidence custody form

d) investigation report

64) …… are found most commonly in GSM devices and consist of a microprocessor and 16 KB to 4 MB EEPROM.

a) Sim cards

b) SDD cards

c) MMC cards

d) SD cards

65) What are the three general categories of computer systems that can contain digital evidence?
a. Desktop, laptop, server
b. Personal computer, Internet, mobile telephone
c. Hardware, software, networks
d. Open computer systems, communication systems, embedded systems

66) In terms of digital evidence, a mobile telephone is an example of:
a. Open computer systems
b. Communication systems
c. Embedded computer systems
d. None of the above

67) In terms of digital evidence, a Smart Card is an example of:
a. Open computer systems
b. Communication systems
c. Embedded computer systems
d. None of the above

68) In terms of digital evidence, the Internet is an example of:
a. Open computer systems
b. Communication systems
c. Embedded computer systems
d. None of the above

69) Computers can be involved in which of the following types of crime?
a. Homicide and sexual assault
b. Computer intrusions and intellectual property theft
c. Civil disputes
d. All of the above

70) Due to caseload and budget constraints, often computer security professionals attempt to limit the damage and close each investigation as quickly as possible. Which of the following is NOT a significant drawback to this approach?

a. Each unreported incident robs attorneys and law enforcement personnel of an opportunity to learn about the basics of computer-related crime.
b. Responsibility for incident resolution frequently does not reside with the security professional, but with management.

c. This approach results in under-reporting of criminal activity, deflating statistics that are used to allocate corporate and government spending on combating computer-related crime.

d. Computer security professionals develop loose evidence processing habits that can make it more difficult for law enforcement personnel and attorneys to prosecute an offender.

71) The author of a series of threatening e-mails consistently uses "im" instead of "I'm." This is an example of:
   a. An individual characteristic
   b. An incidental characteristic
   c. A class characteristic
   d. An indeterminate characteristic
72) An argument for including computer forensic training computer security specialists is:
   a. It provides an additional credential.
   b. It provides them with the tools to conduct their own investigations.
   c. It teaches them when it is time to call in law enforcement.
   d. None of the above.
73) cloned mobile telephone is an example of:
   a. Hardware as contraband or fruits of crime
   b. Hardware as an instrumentality
   c. Information as contraband or fruits of crime
   d. Information as evidence
74) Digital photographs or videos of child exploitation is an example of:
   a. Hardware as contraband or fruits of crime
   b. Hardware as an instrumentality
   c. Hardware as evidence
   d. Information as contraband or fruits of crime
75) Computer equipment purchased with stolen credit card information is an example of:
   a. Hardware as contraband or fruits of crime
   b. Hardware as an instrumentality
   c. Hardware as evidence
   d. Information as contraband or fruits of crime
76) A printer used for counterfeiting is an example of:
   a. Hardware as contraband or fruits of crime
   b. Hardware as an instrumentality
   c. Hardware as evidence
   d. Information as contraband or fruits of crime
77) Phone company records are an example of:
   a. Hardware as contraband or fruits of crime
   b. Information as contraband or fruits of crime
   c. Information as an instrumentality
   d. Information as evidence
78) According to the text, the most common mistake that prevents evidence seized from

being admitted is:
a. Uninformed consent
b. Forcible entry
c. Obtained without authorization
d. None of the above

79) If, while searching a computer for evidence of a specific crime, evidence of a new, unrelated crime is discovered, the best course of action is:
a. Abandon the original search, and pursue the new line of investigation
b. Continue with the original search but also pursue the new inquiry
c. Stop the search and obtain a warrant that addresses the new inquiry
d. Continue with the original search, ignoring the new information

80) The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:
a. Chain of custody
b. Field notes
c. Interim report
d. None of the above

81) When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally, and:
a. Whether chain of custody was maintained
b. Whether there are indications that the actual digital evidence was tampered with
c. Whether the evidence was properly secured in transit
d. Whether the evidence media was compatible with forensic machines

82) The fact that with modern technology, a photocopy of a document has become acceptable in place of the original is known as:
a. Best evidence rule
b. Due diligence
c. Quid pro quo
d. Voir dire

83) Evidence contained in a document provided to prove that statements made in court are true is referred to as:
a. Inadmissible evidence
b. Illegally obtained evidence
c. Hearsay evidence
d. Direct evidence

84) Business records are considered to be an exception to:
a. Direct evidence
b. Inadmissible evidence
c. Illegally obtained evidence
d. Hearsay evidence

85) Which of the following is not one of the levels of certainty associated with a particular finding?
a. Probably
b. Maybe
c. Almost definitely

d. Possibly

86) Direct evidence establishes a:
   a. Fact
   b. Assumption
   c. Error
   d. Line of inquiry

87) What is IMSI stands for-----
   a) International Mobile Subscriber Identity
   b) Internet Mobile Subscriber Identifier
   c) Internet Message Subscriber Identifier
   d) International Message Supply Identity

88) The IMSI value is associated with
   a) SIM card
   b) Mobile device
   c) Wi-Fi
   d) network

89) How Many digits are in the string of IMSI numbers?
   a) 15
   b) 17
   c) 18
   d) 16

90) Which of the following is not the part of the IMSI number of SIM
   a) Mobile Country Code
   b) Mobile Network Code
   c) Mobile Check Digit
   d) Mobile Station Identification Number

91) ICCID value is stored on
   a) Mobile device only
   b) SIM cards
   c) Wifi
   d) Mobile Atom Processor

92) What is the length of the ICCID number?
   a) 18
   b) 16
   c) 22
   d) Both19 or 20

93) There are _____ major ways of stealing email information.
   a) 2
   b) 3
   c) 4
   d) 5

94) Which of them is not a major way of stealing email information?
   a) Stealing cookies
   b) Reverse Engineering
   c) Password Phishing
   d) Social Engineering

95) _____is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.
   a) Email security
   b) Email hacking
   c) Email protection
   d) Email safeguarding

96) _____ is a famous technological medium for the spread of malware, facing problems of spam, & phishing attacks.
   a) Cloud
   b) Pen drive
   c) Website
   d) Email

97) Which of them is not a proper method for email security?
   a) Use Strong password
   b) Use email Encryption
   c) Spam filters and malware scanners
   d) Click on unknown links to explore

98) The stored cookie which contains all your personal data about that website can be stolen away by _____ using _____ or trojans.
   a) attackers, malware
   b) hackers, antivirus
   c) penetration testers, malware
   d) penetration testers, virus

99) If the data stored in the _____ is not encrypted, then after cookie stealing, attackers can see information such as username and password stored by the cookie.
   a) Memory
   b) Quarantine
   c) Cookies
   d) hard drive

100) Which of the following is a non-technical type of intrusion or attack technique?
   a) Reverse Engineering
   b) Malware Analysis
   c) Social Engineering
   d) Malware Writing