1. Which of the following is a hacking technique in which cyber criminals create fictitious web pages or domains to deceive or obtain more traffic.

- Mimicking
- Spamming
- Website Duplication
- Pharming

2. Computer evidence is like any other evidence. It must be

- Authentic
- Accurate
- Complete
- All of the Above

3. The legal aspects of a computer forensics investigation center primarily on the following two main issues:

- The requirements that need to be met in order for evidence to be successfully presented in court and, of course, not considered legally admissible
- The requirements that need to be met in order for evidence to be successfully presented in court and, of course, considered legally admissible
- The right of the investigator to avoid the possibility of not incurring legal action against himself or the organization for whom he is conducting the investigation
- The acceptance of the investigator to avoid the possibility of incurring legal action against himself or the organization for whom he is reviewing

4. What is meant by the term 'cyber-crime'?

- Any crime that uses computers to jeopardise or attempt to jeopardise national security
- The use of computer networks to commit financial or identity fraud
- The theft of digital information
- Any crime that involves computers and networks

5.Which of the following is not a type of cyber crime?

- Data theft
- Forgery
- Damage to data and systems
- Installing antivirus for protection

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

- Open computer systems
- Communication systems
- Embedded computer systems
- None of the above

7.A valid definition of digital evidence is:

- Data stored or transmitted using a computer
- Information of probative value
- Digital data of probative value
- Any digital evidence on a computer

8.A logon record tells us that, at a specific time:

- An unknown person logged into the system using the account
- The owner of a specific account logged into the system
- The account was used to log into the system
- None of the above

9. Private networks can be a richer source of evidence than the Internet because:

- They retain data for longer periods of time
- Owners of private networks are more cooperative with law enforcement.
- Private networks contain a higher concentration of digital evidence
- All of the above.

10.Computers can play the following roles in a crime

- Target, object, and subject
- Evidence, instrumentality, contraband, or fruit of crime
- Object, evidence, and tool
- Symbol, instrumentality, and source of evidence

1. Pharming
2. All of the Above
3. The requirements that need to be met in order for evidence to be successfully presented in court and, of course, considered legally admissible
4. Any crime that involves computers and networks
5. Installing antivirus for protection
6. Open computer systems
7. Digital data of probative value
8. The account was used to log into the system
9. All of the above
10. Evidence, instrumentality, contraband, or fruit of crime

1.One of the most common approaches to validating forensic software is to:

- Examine the source code
- Ask others if the software is reliable
- Compare results of multiple tools for discrepancies
- Computer forensic tool testing projects

2.What can you do to determine the number of sectors on a hard drive larger than 8GB? *

- Use a UNIX tool like hdparm
- Use a Windows tools like EnCase
- Check the drive manufacturer's website for the specific drive
- All of the above

3 The following are some helpful tips that you can follow to help preserve data for future computer forensic examination, except:

- Do not turn on or attempt to examine the suspect computer. This could result in destruction of evidence
- Identify all devices that may contain evidence.
- Run all in-house computers.
- Quarantine all in-house computers.

4.For a strategy of deterrence to work the following must hold, except:

- The incident must not be well defined.
- The identity of the perpetrator must be unambiguous.
- The will and ability to carry out a deterrence strike must be believed.
- The perpetrator must have something of value at stake.

5 Just as perpetrators such as hackers and crackers have done to wired networks, they can assault WLANs through the same methods, except

- Unauthorized access points
- Data interception
- Denial-of-service (DoS) attacks
- Authorized access points

6.Because the Internet is built upon the TCP/IP protocol, many hacker attacks will seek to exploit the TCP ports of these servers with public IP addresses. A number of common ports are scanned and attacked, except

- FTP (21)
- Telnet (23)
- SMTP (25)
- INS (53)

7.Forensic investigators perform the following, except:

- Detect the extent of a security breach.
- Recover found data.
- Recover lost data
- Determine how an intruder got past security mechanisms.

8.A printer used for counterfeiting is an example of:

- Hardware as contraband or fruits of crime
- Hardware as an instrumentality
- Hardware as evidence
- Information as contraband or fruits of crime

9.One of the most common approaches to validating forensic software is to:

- Examine the source code
- Ask others if the software is reliable
- Compare results of multiple tools for discrepancies
- Computer forensic tool testing projects

10. The following specializations exist in digital investigations:

- First responder (a.k.a. digital crime scene technician)
- Forensic examiner
- Digital investigator
- All of the above

1. Computer forensic tool testing projects
2. All of the above
3. Run all in-house computers.
4. The incident must not be well defined.
5. Authorized access points
6. INS (53)
7. Recover found data.
8. Hardware as an instrumentality
9. Computer forensic tool testing projects
10. All of the above

1. CDMA Uses which transmission techniques

- Voice Data Packets
- Patterns
- 12 Bits Packet
- Data Analog to Digital Data Packets

2."SICAR" is a system software is used for the identification of

- Cartridge
- Case Bullet
- Shoe Impression
- Tyre Impression

3.Which of the following software's are used for data retrieval from mobile phones

- MOBILedit
- UFED(cellebrite)
- Susteen secure view
- Elcomsoft Software Ampedfive

4.The "agent" application extract which type of data from a mobile device?

- Only computing
- Data Both Physical and Logical Data
- Physical data
- Logical Data

5.In mobile Forensics, BTS Stands for

- Base Transceiver station
- Basic Transceiver station
- Basic Transmission service
- Basic Transceiver service

6.In mobile Telecommunication, 3GPP stands for

- Third Generation protocol project
- Third generation partnership protocol
- Third generation partnership Project
- Third Generation of password protocol

7.Which of the following are the tools for a software-based manual examination of mobile evidence?

- Snaphit
- eHub Creator
- Screen Hunter
- ForensicFIT

8.Non Removable SIMs is also called:

- NR-SIM
- Patent SIM
- Closed SIM
- eSIM

9.What is the full form of SOP in cell device Forensic

- set operational procedure
- Standard of Preservation

- Safety Operational Procedure
- Standard Operating Procedure

10.In a humid environment, a mobile device is found and has a fungus layer on it. Which of the following fungus layer has the most damaging effect on the mobile phone?

- Black Fungus
- All are harmless to electronic devices
- Green Fungus
- White Fungus

1. Analog to Digital Data Packets
2. Shoe Impression
3. All of the above
4. Both Physical and Logical Data
5. Base Transceiver station
6. Third generation partnership Project
7. Screen Hunter
8. eSIM
9. Standard Operating Procedure
10. Black Fungus

1. What is the Full Form of a VLR

- Visual Location Router
- Visited Local Reseller
- Visual Local Registry
- Visitor Location Registry

2. PEM stands for _______.

- Public Encryption Mail
- Privacy Enhanced Mail
- Privacy Enhanced Message
- Public Encryption Message

3. In ________ acquisition, the data acquisition method captures only specific files of interest to the case or specific types of files, such as Outlook PST files.

- Live
- Sparse
- Logical
- All of these

4. The set of procedures, policies and guidelines that commence at the detection of an incident is the __________.

- computer forensics
- digital forensics
- incident response
- investigation

5. Which of the following is not a part of an incident response?

- Identification
- Investigating
- Entrapment
- Repairing

6. Your system has been acting strangely since you downloaded a file from a colleague. Upon examining your antivirus software, you notice that the virus definition file is missing. Which type of virus probably infected your system?

- Polymorphic virus
- Retrovirus
- Worm
- Armored virus

7. You've discovered that an expired certificate is being used repeatedly to gain logon privileges. Which type of attack is this most likely to be?

- Man-in-the-middle attack
- Back door attack
- Replay attack
- TCP/IP hijacking

8. As security in the enterprise increases,

- ease of use increases and functionality decreases.
- functionality increases and ease of use decreases
- ease of use decreases and functionality increases.
- functionality decreases and ease of use decreases.

9. Which form of communication is a real-time, text-based communication type used between two or more people who use mostly text to communicate?

- a) Weblogs
- b) Wikis
- c) Instant messaging
- d) Podcasting

10. ____________ recording the system time and date.

- ls
- date and time
- rdate
- w

1. Visitor Location Registry
2. Privacy Enhanced Mail
3. Sparse
4. incident response
5. Entrapment
6. Retrovirus
7. Replay attack
8. ease of use decreases and functionality increases.
9. c) Instant messaging
10. date and time