Program: BE **Computer** Engineering

Curriculum Scheme: Revised **2012**

Examination: **Final** Year Semester **VIII**

Course Code: **CPE8034** and Course Name: **Digital Forensics**

Time: 1hour Max. Marks: 50

==============================================================================

Note to the students:- All the Questions are compulsory and carry equal marks .

|  |  |
| --- | --- |
| Q1.  | Which of the following is not a type of cyber crime? |
| Option A: | Forgery |
| Option B: | Installing antivirus for protection |
| Option C: | Data theft |
| Option D:  | Damage to data and systems |
|  |  |
| Q2. | Which of the following is the type of software that has self-replicating software that causes damage to files and system?  |
| Option A: | Viruses |
| Option B: | Trojan horses |
| Option C: | Bots |
| Option D: | Worms |
|  |  |
| Q3. | \_\_\_\_\_\_\_\_\_\_\_ is a discipline that combines elements of law and computer science to collect and analyze information from various electronic gadgets that are admissible in the court of law.  |
| Option A: | Cyber crime |
| Option B: | Cyber forscience |
| Option C: | Cyber forensics |
| Option D: | Ethical hacking |
|  |  |
| Q4. | Digital Forensics entails \_\_\_\_\_.  |
| Option A: |  Accessing the system's directories viewing mode and navigating through the various systems files and folders  |
| Option B: |  Undeleting and recovering lost files  |
| Option C: | Identifying and solving computer crimes  |
| Option D: | The identification, preservation, recovery, restoration and presentation of digital evidence from systems and devices |
|  |  |
| Q5. | The main objective of the cyber forensics is to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Option A: |  Collect data in the manner acceptable for a court |
| Option B: | Produce the gadgets in the court |
| Option C: | Check what is the process going on in the network  |
| Option D:  | Collect database from the system administrator |
|  |  |
| Q6. | Which of the following software tools is NOT used for data recovery? |
| Option A: | WinHex (X-Ways) Forensic |
| Option B: | EnCase |
| Option C: | FTK |
| Option D:  | Safeback |
|  |  |
| Q7.  | The standard Windows environment supports all of the following file systems EXCEPT\_\_\_\_\_\_\_\_ |
| Option A: | FAT16 |
| Option B: | ext2 |
| Option C: | FAT32 |
| Option D:  | NTFS |
|  |  |
| Q8.  | 1. What is called as the process of creation a duplicate of digital media for purpose of examining it?
 |
| Option A: | Acquisition |
| Option B: | Steganography |
| Option C: | Live analysis |
| Option D:  | Hashing |
|  |  |
| Q9. | Unlike the standard DOS/Windows environments, the UNIX environment has the capability of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, thereby preventing the contents of evidentiary media from being changed. |
| Option A: | Encrypting all data on the media |
| Option B: | Copying the contents of the media |
| Option C: | Warning the examiner of an impending write |
| Option D:  | Mounting storage media as Read-Only |
|  |  |
| Q10.  | 1. What are the three general categories of computer systems that can contain digital evidence?
 |
| Option A: | Desktop, laptop, server |
| Option B: | Personal computer, Internet, mobile telephone |
| Option C: | Hardware, software, networks |
| Option D:  | Open computer systems, communication systems, embedded systems |
|  |  |
| Q11.  | According to the text, the most common mistake that prevents evidence seized from being admitted is: |
| Option A: | Uninformed consent |
| Option B: | Forcible entry |
| Option C: | Obtained without authorization |
| Option D:  | Warning the examiner of an impending write |
|  |  |
| Q12.  | The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as: |
| Option A: | Chain of custody |
| Option B: | Due diligence |
| Option C: | Field notes |
| Option D: | Authenticity |
|  |  |
| Q13. | Direct evidence establishes a: |
| Option A: | Fact |
| Option B: | Assumption |
| Option C: | Error |
| Option D:  | Line of inquiry |
|  |  |
| Q14.  | Evidence contained in a document provided to prove that statements made in court are true is referred to as: |
| Option A: | Inadmissible evidence |
| Option B: |  Illegally obtained evidence |
| Option C: |  Hearsay evidence |
| Option D:  | Direct evidence |
|  |  |
| Q15. | Although it was not designed with evidence collection in mind, \_\_\_\_\_\_\_can still be useful for examining network traffic |
| Option A: | CHKDSK |
| Option B: | EnCase |
| Option C: |  FTK |
| Option D:  | Wireshark |
|  |  |
| Q16.  | Analysis of digital evidence includes which of the following activities? |
| Option A: | Seizure, preservation, and documentation |
| Option B: | Experimentation, fusion, and correlation |
| Option C: | Recovery, harvesting, and reduction |
| Option D:  | Arrest, interviewing, and trial |
|  |  |
| Q17. | Which of the following is NOT an information gathering process? |
| Option A: | Scanning the system remotely |
| Option B: | Studying security audit reports |
| Option C: | Attempting to bypass logon security |
| Option D: | Examining e-mail headers |
|  |  |
| Q18. | If a criminal reconfigures his computer with someone else’s IP address to conceal his identity, the local router would have an entry in its \_\_\_\_\_\_ showing that criminal’s actual Mac address associated with somebody else’s IP address |
| Option A: | CMOS |
| Option B: | ARP table |
| Option C: | Host table |
| Option D:  | BOOTP |
|  |  |
| Q19.  | 1. Which of following is a not unethical norm for Digital Forensics Investigation?
 |
| Option A: | To respect the privacy of others |
| Option B: | Uphold any relevant evidence |
| Option C: | Declare any confidential matters or knowledge. |
| Option D:  | Distort or falsify education, training, credentials. |
|  |  |
| Q20. | Forensic analysis involves the following: |
| Option A: | Assessment, experimentation, fusion, correlation, and validation |
| Option B: | Seizure and preservation |
| Option C: | Recovery, harvesting, filtering, organization, and search |
| Option D: | Identification , Examination, Preservation |
|  |  |
| Q21. | Generating a plan of action and obtaining supporting resources and materials falls under which step in the digital investigation? |
| Option A: | Examination and analysis |
| Option B: | Preparation |
| Option C: | Survey/identification |
| Option D:  | Preservation |
|  |  |
| Q22.  | Governments hired some highly skilled hackers. These types of hackers are termed as \_\_\_\_\_\_\_  |
| Option A: | Government Hackers |
| Option B: | Special Hackers |
| Option C: | Cyber Intelligence Agents |
| Option D:  | Nation / State sponsored hackers |
|  |  |
| Q23. | CFAA stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Option A: | Cyber Fraud and Abuse Act |
| Option B: | Computer Fraud and Abuse Act |
| Option C: | Cyber Fraud Activity Act |
| Option D:  | Cyber Fraud Activity Analysis |
|  |  |
| Q24.  | The US introduced \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in 2003. |
| Option A: | Spam act |
| Option B: | Cyber act |
| Option C: | Can spam act |
| Option D:  | Phishing act |
|  |  |
| Q25. | Information Technology act in India was amended in the year \_\_\_\_\_\_\_\_\_\_\_\_  |
| Option A: | 2008 |
| Option B: | 2009 |
| Option C: | 2010 |
| Option D:  | 2000 |