|  |
| --- |
| True / False |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. ​According to the National Institute of Standards and Technology (NIST), digital forensics involves scientifically examining and analyzing data from computer storage media so that it can be used as evidence in court.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | | *POINTS:* | 1 | | *REFERENCES:* | 4 | | *QUESTION TYPE:* | True / False | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:17 AM | | *DATE MODIFIED:* | 9/27/2014 4:16 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. All suspected industrial espionage cases should be treated as civil case investigations.​   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | | *POINTS:* | 1 | | *REFERENCES:* | 32 | | *QUESTION TYPE:* | True / False | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:50 AM | | *DATE MODIFIED:* | 9/27/2014 4:16 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. User groups for a specific type of system can be very useful in a forensics investigation.​   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | | *POINTS:* | 1 | | *REFERENCES:* | 9 | | *QUESTION TYPE:* | True / False | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:12 PM | | *DATE MODIFIED:* | 9/27/2014 4:16 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. Most digital investigations in the private sector involve misuse of computing assets.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | | *POINTS:* | 1 | | *REFERENCES:* | 17 | | *QUESTION TYPE:* | True / False | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:24 PM | | *DATE MODIFIED:* | 9/27/2014 4:16 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. If you turn evidence over to law enforcement and begin working under their direction, you have become an agent of law enforcement, and are subject to the same restrictions on search and seizure as a law enforcement agent.​   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | | *POINTS:* | 1 | | *REFERENCES:* | 18 | | *QUESTION TYPE:* | True / False | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:27 PM | | *DATE MODIFIED:* | 9/27/2014 4:17 PM | |

|  |
| --- |
| Multiple Choice |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. Signed into law in 1973, the \_\_\_\_\_\_\_ was/were created to ensure consistency in federal proceedings.   |  |  |  | | --- | --- | --- | |  | a. | Federal Proceedings Law | |  | b. | ​Federal Rules of Evidence | |  | c. | ​Federal Consistency Standards | |  | d. | ​Federal Proceedings Rules |  |  |  | | --- | --- | | *ANSWER:* | b | | *POINTS:* | 1 | | *REFERENCES:* | 3 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 12:56 AM | | *DATE MODIFIED:* | 9/27/2014 4:17 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Which amendment to the U.S. Constitution protects everyone's right to be secure in their person, residence, and property from search and seizure?​   |  |  |  | | --- | --- | --- | |  | a. | ​First Amendment | |  | b. | ​Second Amendment | |  | c. | ​Fourth Amendment | |  | d. | ​Fifth Amendment |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 3 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:26 AM | | *DATE MODIFIED:* | 9/27/2014 4:17 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Which Microsoft OS below is the least intrusive to disks in terms of changing data?​   |  |  |  | | --- | --- | --- | |  | a. | ​Windows 95 | |  | b. | ​Windows XP | |  | c. | ​Windows 7 | |  | d. | ​MS-DOS 6.22 |  |  |  | | --- | --- | | *ANSWER:* | d | | *POINTS:* | 1 | | *REFERENCES:* | 35 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 10:08 PM | | *DATE MODIFIED:* | 9/27/2014 4:17 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. \_\_\_\_\_\_\_ is not recommended for a digital forensics workstation.   |  |  |  | | --- | --- | --- | |  | a. | ​A text editor tool | |  | b. | ​A write-blocker device | |  | c. | ​An SCSI card | |  | d. | ​Remote access software |  |  |  | | --- | --- | | *ANSWER:* | d | | *POINTS:* | 1 | | *REFERENCES:* | 36 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 10:12 PM | | *DATE MODIFIED:* | 9/27/2014 4:18 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. ​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 |  |  |  | | --- | --- | | *ANSWER:* | a | | *POINTS:* | 1 | | *REFERENCES:* | 48 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 10:15 PM | | *DATE MODIFIED:* | 9/27/2014 4:19 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. If a police officer or investigator has sufficient cause to support a search warrant, the prosecuting attorney might direct him or her to submit a(n) \_\_\_\_\_\_\_.​   |  |  |  | | --- | --- | --- | |  | a. | exhibit | |  | b. | ​verdict | |  | c. | ​affidavit | |  | d. | ​memo |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 13 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 10:33 PM | | *DATE MODIFIED:* | 9/27/2014 4:19 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. \_\_\_\_\_\_\_ describes an accusation of fact that a crime has been committed.   |  |  |  | | --- | --- | --- | |  | a. | ​Attrition | |  | b. | ​Attribution | |  | c. | ​Allegation | |  | d. | ​Assignment |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 12 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 10:39 PM | | *DATE MODIFIED:* | 9/27/2014 4:19 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. \_\_\_\_\_\_\_ is not one of the functions of the investigations triad.   |  |  |  | | --- | --- | --- | |  | a. | ​Digital investigations | |  | b. | ​Data recovery | |  | c. | ​Vulnerability/threat assessment and risk management | |  | d. | ​Network intrusion detection and incident response |  |  |  | | --- | --- | | *ANSWER:* | b | | *POINTS:* | 1 | | *REFERENCES:* | 5 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:11 PM | | *DATE MODIFIED:* | 9/27/2014 4:20 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. In what year was the Computer Fraud and Abuse Act passed?​   |  |  |  | | --- | --- | --- | |  | a. | ​1976 | |  | b. | ​1980 | |  | c. | ​1986 | |  | d. | ​1996 |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 12 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:17 PM | | *DATE MODIFIED:* | 9/27/2014 4:29 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. ​The \_\_\_\_\_\_\_ is not one of the three stages of a typical criminal case.   |  |  |  | | --- | --- | --- | |  | a. | ​complaint | |  | b. | investigation | |  | c. | civil suit | |  | d. | prosecution |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 12 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:20 PM | | *DATE MODIFIED:* | 9/27/2014 4:30 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. ​After a judge approves and signs a search warrant, the \_\_\_\_\_\_\_ is responsible for the collection of evidence as defined by the warrant.   |  |  |  | | --- | --- | --- | |  | a. | ​Digital Evidence Recorder | |  | b. | ​Digital Evidence Specialist | |  | c. | ​Digital Evidence First Responder | |  | d. | ​Digital Evidence Scene Investigator |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 13 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:30 PM | | *DATE MODIFIED:* | 9/27/2014 4:31 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. The \_\_\_\_\_\_\_ is responsible for analyzing data and determining when another specialist should be called in to assist with analysis.   |  |  |  | | --- | --- | --- | |  | a. | ​Digital Evidence First Responder | |  | b. | ​Digital Evidence Specialist | |  | c. | ​Digital Evidence Analyst | |  | d. | ​Digital Evidence Examiner |  |  |  | | --- | --- | | *ANSWER:* | b | | *POINTS:* | 1 | | *REFERENCES:* | 13 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:35 PM | | *DATE MODIFIED:* | 9/27/2014 4:37 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. The sale of sensitive or confidential company information to a competitor is known as \_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | ​industrial sabotage | |  | b. | ​industrial espionage | |  | c. | ​industrial collusion | |  | d. | ​industrial betrayal |  |  |  | | --- | --- | | *ANSWER:* | b | | *POINTS:* | 1 | | *REFERENCES:* | 14 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:39 PM | | *DATE MODIFIED:* | 9/27/2014 4:37 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. Which option below is not a standard systems analysis step?​   |  |  |  | | --- | --- | --- | |  | a. | ​Determine a preliminary design or approach to the case. | |  | b. | ​Obtain and copy an evidence drive. | |  | c. | ​Share evidence with experts outside of the investigation. | |  | d. | ​Mitigate or minimize the risks. |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 22-23 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:50 PM | | *DATE MODIFIED:* | 9/27/2014 4:38 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. A chain-of-evidence form, which is used to document what has and has not been done with the original evidence and forensic copies of the evidence, is also known as a(n) \_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | ​single-evidence form | |  | b. | ​multi-evidence form | |  | c. | ​evidence custody form | |  | d. | ​evidence tracking form |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 25 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:53 PM | | *DATE MODIFIED:* | 9/27/2014 4:38 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. ​An evidence custody form does not usually contain \_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | ​the nature of the case | |  | b. | ​a description of evidence | |  | c. | ​vendor names for computer components | |  | d. | ​a witness list |  |  |  | | --- | --- | | *ANSWER:* | d | | *POINTS:* | 1 | | *REFERENCES:* | 25-27 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 12:01 AM | | *DATE MODIFIED:* | 9/27/2014 4:39 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What tool, currently maintained by the IRS Criminal Investigation Division and limited to use by law enforcement, can analyze and read special files that are copies of a disk?​   |  |  |  | | --- | --- | --- | |  | a. | ​AccessData Forensic Toolkit | |  | b. | ​DeepScan | |  | c. | ​ILook | |  | d. | ​Photorec |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 8 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 1:05 PM | | *DATE MODIFIED:* | 9/27/2014 4:42 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. The term \_\_\_\_\_\_\_ describes a database containing informational records about crimes that have been committed previously by a criminal.   |  |  |  | | --- | --- | --- | |  | a. | ​police ledger | |  | b. | ​police blotter | |  | c. | ​police blogger | |  | d. | ​police recorder |  |  |  | | --- | --- | | *ANSWER:* | b | | *POINTS:* | 1 | | *REFERENCES:* | 12 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 3:56 PM | | *DATE MODIFIED:* | 9/27/2014 9:56 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. \_\_\_\_\_\_\_ must be included in an affidavit to support an allegation in order to justify a warrant.   |  |  |  | | --- | --- | --- | |  | a. | ​Verdicts | |  | b. | ​Witnesses | |  | c. | ​Exhibits | |  | d. | ​Subpoenas |  |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | | *REFERENCES:* | 13 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 3:59 PM | | *DATE MODIFIED:* | 9/27/2014 9:57 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. ​After the evidence has been presented in a trial by jury, the jury must deliver a(n) \_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | ​exhibit | |  | b. | ​affidavit | |  | c. | ​allegation | |  | d. | ​verdict |  |  |  | | --- | --- | | *ANSWER:* | d | | *POINTS:* | 1 | | *REFERENCES:* | 13 | | *QUESTION TYPE:* | Multiple Choice | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 4:02 PM | | *DATE MODIFIED:* | 9/27/2014 9:57 PM | |

|  |
| --- |
| Completion |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. In 1987, the \_\_\_\_\_\_\_\_\_\_\_\_ was introduced with an external EasyDrive hard disk with 60 MB of storage.​   |  |  | | --- | --- | | *ANSWER:* | Mac SE​ | | *POINTS:* | 1 | | *REFERENCES:* | 8 | | *QUESTION TYPE:* | Completion | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:21 AM | | *DATE MODIFIED:* | 9/27/2014 9:57 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Typically, the \_\_\_\_\_\_\_\_\_\_\_\_\_ requires a bootable DVD or USB flash drive that runs an independent OS in a suspect computer's RAM, with the goal of preserving data during an acquisition.   |  |  | | --- | --- | | *ANSWER:* | ​software write-blocker | | *POINTS:* | 1 | | *REFERENCES:* | 36 | | *QUESTION TYPE:* | Completion | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:58 AM | | *DATE MODIFIED:* | 9/27/2014 9:58 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. ​A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence.   |  |  | | --- | --- | | *ANSWER:* | line of authority​ | | *POINTS:* | 1 | | *REFERENCES:* | 14 | | *QUESTION TYPE:* | Completion | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:16 PM | | *DATE MODIFIED:* | 9/27/2014 9:59 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ notifies end users that the organization owning the computer equipment reserves the right to inspect or search computer systems and network traffic at will.   |  |  | | --- | --- | | *ANSWER:* | warning banner​ | | *POINTS:* | 1 | | *REFERENCES:* | 15 | | *QUESTION TYPE:* | Completion | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:32 PM | | *DATE MODIFIED:* | 9/27/2014 10:11 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. When conducting a digital forensics analysis under \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ rules for an attorney, you must keep all findings confidential.​   |  |  | | --- | --- | | *ANSWER:* | attorney-client privilege (ACP)​ | | *POINTS:* | 1 | | *REFERENCES:* | 31 | | *QUESTION TYPE:* | Completion | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 10:03 PM | | *DATE MODIFIED:* | 9/27/2014 10:12 PM | |

|  |
| --- |
| Matching |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ​   |  |  |  |  | | --- | --- | --- | --- | | a. | ​Authorized requester | b. | ​Bit-stream image | | c. | ​Digital Evidence First Responder (DEFR) | d. | Digital Evidence Specialist (DES)​ | | e. | ​Inculpatory evidence | f. | Line of authority​ | | g. | ​Search and seizure | h. | Single-evidence form​ | | i. | ​Verdict | j. | Warning banner |  |  |  | | --- | --- | | *REFERENCES:* | 51-52 | | *QUESTION TYPE:* | Matching | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/27/2014 4:35 PM | | *DATE MODIFIED:* | 8/14/2014 3:35 PM | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 31. A professional who secures digital evidence at the scene and ensures its viability while transporting it to the lab   |  |  | | --- | --- | | *ANSWER:* | c | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 32. ​In a private-sector environment, the person who has the right to request an investigation, such as the chief security officer or chief intelligence officer   |  |  | | --- | --- | | *ANSWER:* | a | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 33. ​The legal act of acquiring evidence for an investigation   |  |  | | --- | --- | | *ANSWER:* | g | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 34. The decision returned by a jury   |  |  | | --- | --- | | *ANSWER:* | i | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 35. ​The order in which people or positions are notified of a problem; these people or positions have the legal right to initiate an investigation, take possession of evidence, and have access to evidence   |  |  | | --- | --- | | *ANSWER:* | f | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 36. ​An expert who analyzes digital evidence and determines whether additional specialists are needed   |  |  | | --- | --- | | *ANSWER:* | d | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 37. ​A form that dedicates a page for each item retrieved for a case; it allows investigators to add more detail about exactly what was done to the evidence each time it was taken from the storage locker   |  |  | | --- | --- | | *ANSWER:* | h | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 38. ​Text displayed on computer screens when people log on to a company computer; this text states ownership of the computer and specifies appropriate use of the machine or Internet access   |  |  | | --- | --- | | *ANSWER:* | j | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 39. ​Evidence that indicates a suspect is guilty of the crime with which he or she is charged   |  |  | | --- | --- | | *ANSWER:* | e | | *POINTS:* | 1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 40. The file where the bit-stream copy is stored   |  |  | | --- | --- | | *ANSWER:* | b | | *POINTS:* | 1 | |

|  |
| --- |
| Subjective Short Answer |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 41. What is the difference between an interview and an interrogation?​   |  |  | | --- | --- | | *ANSWER:* | ​An interview is conducted to collect information from a witness or suspect about specific facts related to an investigation, whereas an interrogation is the process of trying to get a suspect to confess to a specific incident or crime. | | *POINTS:* | 1 | | *REFERENCES:* | 34 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:55 AM | | *DATE MODIFIED:* | 10/2/2014 11:20 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 42. Basic report writing involves answering the six Ws. What are they?​   |  |  | | --- | --- | | *ANSWER:* | The six Ws are who, what, whe​n, where, why, and how. | | *POINTS:* | 1 | | *REFERENCES:* | 49 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 8:17 AM | | *DATE MODIFIED:* | 10/2/2014 11:21 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 43. ​What is the difference between a Digital Evidence First Responder (DEFR) and a Digital Evidence Specialist (DES)?   |  |  | | --- | --- | | *ANSWER:* | ​A Digital Evidence First Responder (DEFR) has the skill and training to arrive on an incident scene, assess the situation, and take precautions to acquire and preserve evidence. A Digital Evidence Specialist (DES) has the skill to analyze the data and determine when another specialist should be called in to assist with the analysis. | | *POINTS:* | 1 | | *REFERENCES:* | 13 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/30/2014 7:14 PM | | *DATE MODIFIED:* | 10/2/2014 11:21 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 44. ​Why is confidentiality critical in a corporate environment during and after an investigation of a terminated employee?   |  |  | | --- | --- | | *ANSWER:* | Agreements may exist to ensure the confidentiality of the reasons for termination, or the termination may be represented as a resignation or a layoff in exchange for no bad references. Disseminating the information could make the company liable for breach of contract.​ | | *POINTS:* | 1 | | *REFERENCES:* | 19 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 7/31/2014 11:44 PM | | *DATE MODIFIED:* | 10/2/2014 11:22 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 45. Why is it important to maintain specific temperature and humidity ranges within a forensics lab?​   |  |  | | --- | --- | | *ANSWER:* | Without proper temperature and humidity control, computer components and magnetic media can be damaged.​ | | *POINTS:* | 1 | | *REFERENCES:* | 28 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 12:04 AM | | *DATE MODIFIED:* | 10/2/2014 11:22 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 46. What must be done if data is found in the form of binary files, such as CAD drawings?​   |  |  | | --- | --- | | *ANSWER:* | The program that originally created the binary files must be used to examine the data.​ | | *POINTS:* | 1 | | *REFERENCES:* | 31 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 12:13 AM | | *DATE MODIFIED:* | 10/2/2014 11:22 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 47. Why is it important to have a well-defined policy, especially when investigators and forensics examiners are involved?​   |  |  | | --- | --- | | *ANSWER:* | ​Well-defined policies give computer investigators and forensics examiners the authority to conduct an investigation. Policies also demonstrate that an organization intends to be fair-minded and objective about how it treats employees and state that the organization will follow due process for all investigations. | | *POINTS:* | 1 | | *REFERENCES:* | 14-15 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 4:07 PM | | *DATE MODIFIED:* | 10/2/2014 11:23 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 48. Why must all evidence that is collected be treated with the highest level of security and accountability, even if the evidence is regarding an internal abuse investigation within an organization?   |  |  | | --- | --- | | *ANSWER:* | The evidence must be protected because any civil investigation can become a criminal investigation. | | *POINTS:* | 1 | | *REFERENCES:* | 18 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/1/2014 4:21 PM | | *DATE MODIFIED:* | 10/2/2014 11:23 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 49. What questions should someone consider prior to assisting in an interview or interrogation?   |  |  | | --- | --- | | *ANSWER:* | The following questions should be considered prior to assisting with an interview or interrogation:  ​• What questions do I need to ask the suspect to get the vital information about the case? • Do I know what I’m talking about, or will I have to research the topic or technology related to the investigation? • Do I need additional questions to cover other indirect issues related to the investigation? | | *POINTS:* | 1 | | *REFERENCES:* | 34 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/2/2014 12:48 PM | | *DATE MODIFIED:* | 10/2/2014 11:23 PM | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50. What is a bit-stream image?​   |  |  | | --- | --- | | *ANSWER:* | A bit-stream image is a file containing a bit-stream copy of all data on a disk or disk partition, and is usually referred to as an "image," "image save," or "image file."​ | | *POINTS:* | 1 | | *REFERENCES:* | 38 | | *QUESTION TYPE:* | Subjective Short Answer | | *HAS VARIABLES:* | False | | *DATE CREATED:* | 8/2/2014 12:57 PM | | *DATE MODIFIED:* | 10/2/2014 11:24 PM | |