Chapter 1: Computer Forensics and Investigations as a Profession

TRUE/FALSE

1. By the 1970s, electronic crimes were increasing, especially in the financial sector.

   ANS: T PTS: 1 REF: 6

2. To be a successful computer forensics investigator, you must be familiar with more than one computing platform.

   ANS: T PTS: 1 REF: 8

3. Computer investigations and forensics fall into the same category: public investigations.

   ANS: F PTS: 1 REF: 10

4. The law of search and seizure protects the rights of all people, excluding people suspected of crimes.

   ANS: F PTS: 1 REF: 11

5. After a judge approves and signs a search warrant, it's ready to be executed, meaning you can collect evidence as defined by the warrant.

   ANS: T PTS: 1 REF: 15

MULTIPLE CHOICE

1. The FBI ____ was formed in 1984 to handle the increasing number of cases involving digital evidence.
   a. Federal Rules of Evidence (FRE)
   b. Department of Defense Computer Forensics Laboratory (DCFL)
   c. DIBS
   d. Computer Analysis and Response Team (CART)

   ANS: D PTS: 1 REF: 2

2. ____ involves recovering information from a computer that was deleted by mistake or lost during a power surge or server crash, for example.
   a. Data recovery
   b. Network forensics
   c. Computer forensics
   d. Disaster recovery

   ANS: A PTS: 1 REF: 4

3. ____ involves preventing data loss by using backups, uninterruptible power supply (UPS) devices, and off-site monitoring.
   a. Computer forensics
   b. Data recovery
   c. Disaster recovery
   d. Network forensics

   ANS: C PTS: 1 REF: 4

4. The ____ group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime.
   a. network intrusion detection
   c. incident response

b. computer investigations
d. litigation

ANS: B PTS: 1 REF: 5

5. By the early 1990s, the ____ introduced training on software for forensics investigations.
a. IACIS
c. CERT
b. FLETC
d. DDBIA

ANS: A PTS: 1 REF: 6

6. In the Pacific Northwest, ____ meets monthly to discuss problems that law enforcement and corporations face.
a. IACIS
c. FTK
b. CTIN
d. FLETC

ANS: B PTS: 1 REF: 8

7. In a ____ case, a suspect is tried for a criminal offense, such as burglary, murder, or molestation.
a. corporate
c. criminal
b. civil
d. fourth amendment

ANS: C PTS: 1 REF: 11

8. In general, a criminal case follows three stages: the complaint, the investigation, and the ____.
a. litigation
c. blotter
b. allegation
d. prosecution

ANS: D PTS: 1 REF: 12

9. Based on the incident or crime, the complainant makes a(n) ____, an accusation or supposition of fact that a crime has been committed.
a. litigation
c. blotter
b. allegation
d. prosecution

ANS: B PTS: 1 REF: 13

10. In a criminal or public case, if you have enough information to support a search warrant, the prosecuting attorney might direct you to submit a(n) ____.
a. blotter
c. litigation report
b. exhibit report
d. affidavit

ANS: D PTS: 1 REF: 14

11. It's the investigator's responsibility to write the affidavit, which must include ____ (evidence) that support the allegation to justify the warrant.
a. litigation
c. exhibits
b. prosecution
d. reports

ANS: C PTS: 1 REF: 14

12. The affidavit must be ____ under sworn oath to verify that the information in the affidavit is true.
a. notarized
c. recorded
b. examined
d. challenged

ANS: A PTS: 1 REF: 14

13. Published company policies provide a(n) ____ for a business to conduct internal investigations.

a. litigation path
b. allegation resource
c. line of allegation
d. line of authority

ANS: D PTS: 1 REF: 16

14. A ____ usually appears when a computer starts or connects to the company intranet, network, or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will.
a. warning banner
b. right of privacy
c. line of authority
d. right banner

ANS: A PTS: 1 REF: 16

15. A(n) ____ is a person using a computer to perform routine tasks other than systems administration.
a. complainant
b. user banner
c. end user
d. investigator

ANS: C PTS: 1 REF: 16

16. Without a warning banner, employees might have an assumed ____ when using a company's computer systems and network accesses.
a. line of authority
b. right of privacy
c. line of privacy
d. line of right

ANS: B PTS: 1 REF: 16

17. In addition to warning banners that state a company's rights of computer ownership, businesses should specify a(n) ____ who has the power to conduct investigations.
a. authorized requester
b. authority of line
c. line of right
d. authority of right

ANS: A PTS: 1 REF: 18

18. Most computer investigations in the private sector involve ____.
a. e-mail abuse
b. misuse of computing assets
c. Internet abuse
d. VPN abuse

ANS: B PTS: 1 REF: 19

19. Corporations often follow the ____ doctrine, which is what happens when a civilian or corporate investigative agent delivers evidence to a law enforcement officer.
a. silver-tree
b. gold-tree
c. silver-platter
d. gold-platter

ANS: C PTS: 1 REF: 20

20. Your ____ as a computer investigation and forensics analyst is critical because it determines your credibility.
a. professional policy
b. oath
c. line of authority
d. professional conduct

ANS: D PTS: 1 REF: 21

21. Maintaining ____ means you must form and sustain unbiased opinions of your cases.
a. confidentiality
b. objectivity
c. integrity
d. credibility

ANS: B PTS: 1 REF: 21

COMPLETION

1. _____ involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.

   ANS: Computer forensics

   PTS: 1 REF: 2

2. The _____ to the U.S. Constitution (and each state's constitution) protects everyone's rights to be secure in their person, residence, and property from search and seizure.

   ANS: Fourth Amendment

   PTS: 1 REF: 2

3. The term _____ refers to large corporate computing systems that might include disparate or formerly independent systems.

   ANS: enterprise network environment

   PTS: 1 REF: 4

4. When you work in the _____ group, you test and verify the integrity of standalone workstations and network servers.

   ANS: vulnerability assessment and risk management

   PTS: 1 REF: 5

5. The _____ provides a record of clues to crimes that have been committed previously.

   ANS: police blotter

   PTS: 1 REF: 13

MATCHING

Match each item with a statement below:

a. Computer forensics
b. Network forensics
c. Litigation
d. Xtree Gold
e. Case law
f. HTCIA
g. Affidavit
h. Industrial espionage
i. Line of authority

1. the legal process of proving guilt or innocence in court
2. recognizes file types and retrieves lost or deleted files
3. investigates data that can be retrieved from a computer's hard disk or other storage media

4. sworn statement of support of facts about or evidence of a crime that is submitted to a judge to request a search warrant before seizing evidence
5. allows legal counsel to use previous cases similar to the current one because the laws don't yet exist
6. specifies who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence
7. organization that exchanges information about techniques related to computer investigations and security
8. yields information about how a perpetrator or an attacker gained access to a network
9. involves selling sensitive or confidential company information to a competitor

1. ANS: C PTS: 1 REF: 5
2. ANS: D PTS: 1 REF: 6
3. ANS: A PTS: 1 REF: 3
4. ANS: G PTS: 1 REF: 14
5. ANS: E PTS: 1 REF: 8
6. ANS: I PTS: 1 REF: 16
7. ANS: F PTS: 1 REF: 9
8. ANS: B PTS: 1 REF: 3
9. ANS: H PTS: 1 REF: 15

SHORT ANSWER

1. Briefly describe the triad that makes up computer security.

   ANS:
   Investigators often work as a team to make computers and networks secure in an organization. The computer investigations function is one of three in a triad that makes up computing security. In an enterprise network environment, the triad consists of the following parts:
   * Vulnerability assessment and risk management
   * Network intrusion detection and incident response
   * Computer investigations

   PTS: 1 REF: 4

2. Briefly describe the main characteristics of public investigations.

   ANS:
   Public investigations involve government agencies responsible for criminal investigations and prosecution. Government agencies range from local, county, and state or provincial police departments to federal regulatory enforcement agencies. These organizations must observe legal guidelines such as Article 8 in the Charter of Rights of Canada, the Criminal Procedures Act of the Republic of Namibia, and U.S. Fourth Amendment issues related to search and seizure rules.

   PTS: 1 REF: 10|11

3. Briefly describe the main characteristics of private investigations.

   ANS:

Private or corporate investigations deal with private companies, non-law-enforcement government agencies, and lawyers. These private organizations aren't governed directly by criminal law or Fourth Amendment issues, but by internal policies that define expected employee behavior and conduct in the workplace. Private corporate investigations also involve litigation disputes. Although private investigations are usually conducted in civil cases, a civil case can escalate into a criminal case, and a criminal case can be reduced to a civil case. If you follow good forensics procedures, the evidence found in your investigations can easily make the transition between civil and criminal cases.

PTS: 1 REF: 11

4. What questions should an investigator ask to determine whether a computer crime was committed?

ANS:
In a criminal case, a suspect is tried for a criminal offense, such as burglary, murder, or molestation. To determine whether there was a computer crime, an investigator asks questions such as the following: What was the tool used to commit the crime? Was it a simple trespass? Was it a theft, a burglary, or vandalism? Did the perpetrator infringe on someone else's rights by cyberstalking or e-mail harassment?

PTS: 1 REF: 11|12

5. What are the three levels of law enforcement expertise established by CTIN?

ANS:
To differentiate the training and experience law officers have, CTIN has established three levels of law enforcement expertise:
* *Level 1*—Acquiring and seizing digital evidence, normally performed by a street police officer.
* *Level 2*—Managing high-tech investigations, teaching investigators what to ask for, and understanding computer terminology and what can and can't be retrieved from digital evidence. The assigned detectives usually handle the case.
* *Level 3*—Specialist training in retrieving digital evidence, normally performed by a data recovery or computer forensics expert, network forensics expert, or Internet fraud investigator. This person might also be qualified to manage a case, depending on his or her background.

PTS: 1 REF: 13

6. What are some of the most common types of corporate computer crime?

ANS:
Corporate computer crimes can involve e-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage, which involves selling sensitive or confidential company information to a competitor. Anyone with access to a computer can commit these crimes.

PTS: 1 REF: 15

7. What is embezzlement?

ANS:
Embezzlement is a common computer crime, particularly in small firms. Typically, the owner is busy and trusts one person, such as the office manager, to handle daily transactions. When the office manager leaves, the owner discovers that some clients were overbilled or others were not billed at all, and money is missing. Rebuilding the paper and electronic trail can be tedious. Collecting enough evidence to press charges might be beyond the owner's capabilities.

PTS: 1 REF: 15

8. Briefly describe corporate sabotage.

   ANS:
   Corporate sabotage is most often committed by a disgruntled employee. The employee decides to take a job at a competitor's firm and collects critical files on a disk or thumb drive before leaving. This type of crime can also lead to industrial espionage, which increases every year.

   PTS: 1 REF: 15

9. What text can be used in internal warning banners?

   ANS:
   Depending on the type of organization, the following text can be used in internal warning banners:
   * Access to this system and network is restricted.
   * Use of this system and network is for official business only.
   * Systems and networks are subject to monitoring at any time by the owner.
   * Using this system implies consent to monitoring by the owner.
   * Unauthorized or illegal users of this system or network will be subject to discipline or prosecution.

   PTS: 1 REF: 17

10. Mention examples of groups that should have direct authority to request computer investigations in the corporate environment.

    ANS:
    Examples of groups that should have direct authority to request computer investigations in the corporate environment include the following:
    * Corporate Security Investigations
    * Corporate Ethics Office
    * Corporate Equal Employment Opportunity Office
    * Internal Auditing
    * The general counsel or Legal Department

    PTS: 1 REF: 18