Chapter 2: Understanding Computer Investigations

TRUE/FALSE

1. Chain of custody is also known as chain of evidence.

   ANS: T PTS: 1 REF: 30

2. Employees surfing the Internet can cost companies millions of dollars.

   ANS: T PTS: 1 REF: 32

3. You cannot use both multi-evidence and single-evidence forms in your investigation.

   ANS: F PTS: 1 REF: 39

4. Many attorneys like to have printouts of the data you have recovered, but printouts can present problems when you have log files with several thousand pages of data.

   ANS: T PTS: 1 REF: 42

5. A bit-stream copy is a bit-by-bit duplicate of the original disk. You should use the original disk whenever possible.

   ANS: F PTS: 1 REF: 66

MULTIPLE CHOICE

1. The ____ is the route the evidence takes from the time you find it until the case is closed or goes to court.

   a. acquisition plan
   b. chain of custody
   c. evidence path
   d. evidence custody

   ANS: B PTS: 1 REF: 30

2. When preparing a case, you can apply ____ to problem solving.

   a. standard programming rules
   b. standard police investigation
   c. standard systems analysis steps
   d. bottom-up analysis

   ANS: C PTS: 1 REF: 32

3. The list of problems you normally expect in the type of case you are handling is known as the ____.

   a. standard risk assessment
   b. chain of evidence
   c. standard problems form
   d. problems checklist form

   ANS: A PTS: 1 REF: 33

4. The basic plan for your investigation includes gathering the evidence, establishing the ____, and performing the forensic analysis.

   a. risk assessment
   b. nature of the case
   c. chain of custody
   d. location of the evidence

   ANS: C PTS: 1 REF: 35

5. A(n) ____ helps you document what has and has not been done with both the original evidence and forensic copies of the evidence.

a. evidence custody form		c. initial investigation form

b. risk assessment form		d. evidence handling form

ANS: A		PTS: 1		REF: 36

6. Use ____ to secure and catalog the evidence contained in large computer components.

a. Hefty bags		c. paper bags

b. regular bags		d. evidence bags

ANS: D		PTS: 1		REF: 39

7. ____ prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab.

a. An antistatic wrist band		c. An antistatic pad

b. Padding		d. Tape

ANS: B		PTS: 1		REF: 39

8. ____ investigations typically include spam, inappropriate and offensive message content, and harassment or threats.

a. VPN		c. E-mail

b. Internet		d. Phone

ANS: C		PTS: 1		REF: 41

9. To conduct your investigation and analysis, you must have a specially configured personal computer (PC) known as a ____.

a. mobile workstation		c. forensic lab

b. forensic workstation		d. recovery workstation

ANS: B		PTS: 1		REF: 48

10. You can use ____ to boot to Windows without writing any data to the evidence disk.

a. a SCSI boot up disk		c. a write-blocker

b. a Windows boot up disk		d. Windows XP

ANS: C		PTS: 1		REF: 49

11. To begin conducting an investigation, you start by ____ the evidence using a variety of methods.

a. copying		c. opening

b. analyzing		d. reading

ANS: A		PTS: 1		REF: 51

12. A ____ is a bit-by-bit copy of the original storage medium.

a. preventive copy		c. backup copy

b. recovery copy		d. bit-stream copy

ANS: D		PTS: 1		REF: 52

13. A bit-stream image is also known as a(n) ____.

a. backup copy		c. custody copy

b. forensic copy		d. evidence copy

ANS: B PTS: 1 REF: 52

14. To create an exact image of an evidence disk, copying the ____ to a target work disk that's identical to the evidence disk is preferable.
a. removable copy
b. backup copy
c. bit-stream image
d. backup image

ANS: C PTS: 1 REF: 52

15. ____ from Technology Pathways is a forensics data analysis tool. You can use it to acquire and analyze data from several different file systems.
a. Guidance EnCase
b. NTI SafeBack
c. DataArrest SnapCopy
d. ProDiscover Basic

ANS: D PTS: 1 REF: 53

16. Forensics tools such as ____ can retrieve deleted files for use as evidence.
a. ProDiscover Basic
b. ProDelete
c. FDisk
d. GainFile

ANS: A PTS: 1 REF: 56

17. When analyzing digital evidence, your job is to ____.
a. recover the data
b. destroy the data
c. copy the data
d. load the data

ANS: A PTS: 1 REF: 56

18. ____ can be the most time-consuming task, even when you know exactly what to look for in the evidence.
a. Evidence recovery
b. Data recovery
c. Data analysis
d. Evidence recording

ANS: C PTS: 1 REF: 58

19. When you write your final report, state what you did and what you ____.
a. did not do
b. found
c. wanted to do
d. could not do

ANS: B PTS: 1 REF: 64

20. In any computing investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as ____.
a. checked values
b. verification
c. evidence backup
d. repeatable findings

ANS: D PTS: 1 REF: 64

21. After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and ____.
a. critique the case
b. repeat the case
c. present the case
d. read the final report

ANS: A PTS: 1 REF: 65

COMPLETION

1. When you are dealing with password protected files, you might need to acquire ____________________ or find an expert who can help you crack the passwords.

   ANS: password-cracking software

   PTS: 1 REF: 31

2. During the ____________________ design or approach to the case, you outline the general steps you need to follow to investigate the case.

   ANS: preliminary

   PTS: 1 REF: 32

3. A(n) ____________________ lists each piece of evidence on a separate page.

   ANS: single-evidence form

   PTS: 1 REF: 36

4. A(n) ____________________ is usually conducted to collect information from a witness or suspect about specific facts related to an investigation.

   ANS: interview

   PTS: 1 REF: 47

5. A(n) ____________________ is where you conduct your investigations and where most of your equipment and software are located, including the secure evidence containers.

   ANS:
   computer forensics lab
   data-recovery lab

   PTS: 1 REF: 48

MATCHING

Match each item with a statement below

a. FTK's Internet Keyword Search
b. Data recovery
c. Free space
d. Interrogation
e. Forensic workstation
f. Norton DiskEdit
g. MS-DOS 6.22
h. Multi-evidence form
i. Self-evaluation

1. an essential part of professional growth
2. extracts all related e-mail address information for Web-based e-mail investigations
3. process of trying to get a suspect to confess to a specific incident or crime
4. a type of evidence custody form
5. also known as a computer forensics workstation
6. is the more well-known and lucrative side of the computer forensics business
7. can be used for new files that are saved or files that expand as data is added to them

8. the least intrusive (in terms of changing data) Microsoft operating system
9. an older computer forensics tool

1.	ANS: I	PTS: 1	REF: 33
2.	ANS: A	PTS: 1	REF: 42
3.	ANS: D	PTS: 1	REF: 47
4.	ANS: H	PTS: 1	REF: 36
5.	ANS: E	PTS: 1	REF: 48
6.	ANS: B	PTS: 1	REF: 48
7.	ANS: C	PTS: 1	REF: 56
8.	ANS: G	PTS: 1	REF: 49
9.	ANS: F	PTS: 1	REF: 31

SHORT ANSWER

1. What should you do to handle evidence contained in large computer components?

   ANS:
   To secure and catalog the evidence contained in large computer components, you can use large evidence bags, tape, tags, labels, and other products available from police supply vendors or office supply stores. When gathering products to secure your computer evidence, make sure they are safe and effective to use on computer components. Be cautious when handling any computer component to avoid damaging the component or coming into contact with static electricity,which can destroy digital data. When collecting computer evidence, make sure you use antistatic bags.

   Be sure to place computer evidence in a well-padded container. Padding prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab. Save discarded hard disk drive boxes, antistatic bags, and packing material for computer hardware when you or others acquire computer devices.

   PTS: 1 REF: 39

2. What is required to conduct an investigation involving Internet abuse?

   ANS:
   To conduct an investigation involving Internet abuse, you need the following:
   * The organization’s Internet proxy server logs
   * Suspect computer’s IP address obtained from your organization’s network administrator
   * Suspect computer’s disk drive
   * Your preferred computer forensics analysis tool (ProDiscover, FTK, EnCase, X-Ways Forensics, and so forth)

   PTS: 1 REF: 40

3. What is required to conduct an investigation involving e-mail abuse?

   ANS:
   The following list is what you need for an investigation involving e-mail abuse:
   * An electronic copy of the offending e-mail that contains message header data; consult with your e-mail server administrator
   * If available, e-mail server log records; consult with your e-mail server administrator to see whether they are available

* For e-mail systems that store users’ messages on a central server, access to the server; consult with your e-mail server administrator
* For e-mail systems that store users’ messages on a computer as an Outlook .pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it
* Your preferred computer forensics analysis tool, such as Forensic Toolkit or ProDiscover

PTS: 1 REF: 41|42

4. What are the differences between computer forensics and data recovery?

ANS:
In data recovery, you don’t necessarily need a sterile target drive when restoring the forensics image. Typically, the customer or your company just wants the data back. The other key difference is that in data recovery, you usually know what you’re trying to retrieve. In computer forensics, you might have an idea of what you’re searching for, but not necessarily.

Be aware that some companies that perform computer investigations also do data recovery, which is the more well-known and lucrative side of the business.

PTS: 1 REF: 48

5. Describe some of the technologies used with hardware write-blocker devices. Identify some of the more commonly used vendors and their products.

ANS:
There are many hardware write-blockers on the market. Some are inserted between the disk controller and the hard disk; others connect to USB or FireWire ports. Several vendors sell write-blockers, including Technology Pathways NoWrite FPU; Digital Intelligence Ultra- Kit, UltraBlock, FireFly, FireChief 800, and USB Write Blocker; WiebeTECH Forensic DriveDock; Guidance Software FastBloc2; Paralan’s SCSI Write Blockers; and Intelligent Computer Solutions (*www.ics-iq.com*) Image LinkMaSSter Forensics Hard Case.

PTS: 1 REF: 49

6. What are the items you need when setting up your workstation for computer forensics?

ANS:
With current computer forensics hardware and software, configuring a computer workstation or laptop as a forensic workstation is simple. All that’s required are the following:
* A workstation running Windows XP or Vista
* A write-blocker device
* Computer forensics acquisition tool
* Computer forensics analysis tool
* A target drive to receive the source or suspect disk data
* Spare PATA or SATA ports
* USB ports

PTS: 1 REF: 50

7. What additional items are useful when setting up a forensic workstation?

ANS:
Additional useful items include the following:
* Network interface card (NIC)

* Extra USB ports
* FireWire 400/800 ports
* SCSI card
* Disk editor tool
* Text editor tool
* Graphics viewer program
* Other specialized viewing tools

PTS: 1 REF: 50

8. What items are needed when gathering the resources you identified in your investigation plan?

ANS:
You need the following items:
* Original storage media
* Evidence custody form
* Evidence container for the storage media, such as an evidence bag
* Bit-stream imaging tool; in this case, the ProDiscover Basic acquisition utility
* Forensic workstation to copy and examine your evidence
* Securable evidence locker, cabinet, or safe

PTS: 1 REF: 51

9. Describe the process of creating a bit-stream copy of an evidence disk.

ANS:
To create an exact image of an evidence disk, copying the image to a target disk that's identical to the evidence disk is preferable. The target disk's manufacturer and model, in general, should be the same as the original disk's manufacturer and model. If the target disk is identical to the original, the size in bytes and sectors of both disks should also be the same. Some software tools that acquire images can accommodate a target disk that's a different size than the original.

PTS: 1 REF: 52

10. Mention six important questions you should ask yourself when critiquing your work.

ANS:
Ask yourself assessment questions such as the following:
* How could you improve your performance in the case?
* Did you expect the results you found? Did the case develop in ways you did not expect?
* Was the documentation as thorough as it could have been?
* What feedback has been received from the requesting source?
* Did you discover any new problems? If so, what are they?
* Did you use new techniques during the case or during research?

PTS: 1 REF: 65