Chapter 3: The Investigator's Office and Laboratory

TRUE/FALSE

1. Performing a forensic analysis of a disk 200 GB or larger can take several days and often involves running imaging software overnight and on weekends.

   ANS: T PTS: 1 REF: 75

2. Requirements for taking the EnCE certification exam depend on taking the Guidance Software EnCase training courses.

   ANS: F PTS: 1 REF: 81

3. If damage occurs to the floor, walls, ceilings, or furniture on your computer forensics lab, it does not need to be repaired immediately.

   ANS: F PTS: 1 REF: 85

4. A good working practice is to use less powerful workstations for mundane tasks and multipurpose workstations for the higher-end analysis tasks.

   ANS: T PTS: 1 REF: 88

5. Computing systems in a forensics lab should be able to process typical cases in a timely manner.

   ANS: T PTS: 1 REF: 89

MULTIPLE CHOICE

1. A ____ is where you conduct your investigations, store evidence, and do most of your work.
   a. forensic workstation
   b. computer forensics lab
   c. storage room
   d. workbench

   ANS: B PTS: 1 REF: 74

2. Lab costs can be broken down into daily, ____, and annual expenses.
   a. weekly
   b. monthly
   c. bimonthly
   d. quarterly

   ANS: D PTS: 1 REF: 75

3. ____ are generated at the federal, state, and local levels to show the types and frequency of crimes committed.
   a. HTCN reports
   b. IDE reports
   c. Uniform crime reports
   d. ASCLD reports

   ANS: C PTS: 1 REF: 76

4. Windows hard disks can now use a variety of file systems, including FAT16, FAT32, ____, and Windows File System.
   a. NTFS
   b. ext3
   c. FAT24
   d. ext2

ANS: A PTS: 1 REF: 78

5. ____ was created by police officers who wanted to formalize credentials in computing investigations.
   a. HTCN
   b. NISPOM
   c. TEMPEST
   d. IACIS

   ANS: D PTS: 1 REF: 79

6. IACIS requires recertification every ____ years to demonstrate continuing work in the field of computer forensics.
   a. 2
   b. 3
   c. 4
   d. 5

   ANS: B PTS: 1 REF: 79

7. What HTCN certification level requires candidates have three years of investigative experience in any discipline from law enforcement or corporate or have a college degree with one year of experience in investigations?
   a. Certified Computer Crime Investigator, Basic Level
   b. Certified Computer Crime Investigator, Advanced Level
   c. Certified Computer Forensic Technician, Basic
   d. Certified Computer Forensic Technician, Advanced

   ANS: C PTS: 1 REF: 80

8. To preserve the integrity of evidence data, your lab should function as an evidence locker or safe, making it a ____ or a secure storage safe.
   a. secure workstation
   b. secure workbench
   c. protected PC
   d. secure facility

   ANS: D PTS: 1 REF: 82

9. The EMR from a computer monitor can be picked up as far away as ____ mile.
   a. 1/4
   b. 1/2
   c. 3/4
   d. 1

   ANS: B PTS: 1 REF: 83

10. Defense contractors during the Cold War were required to shield sensitive computing systems and prevent electronic eavesdropping of any computer emissions. The U.S. Department of Defense calls this special computer-emission shielding ____.
    a. TEMPEST
    b. RAID
    c. NISPOM
    d. EMR

    ANS: A PTS: 1 REF: 83

11. A secure storage container or cabinet should be made of ____ and include an internal cabinet lock or external padlock.
    a. gypsum
    b. steel
    c. wood
    d. expanded metal

    ANS: B PTS: 1 REF: 84

12. Floors and carpets on your computer forensic lab should be cleaned at least ____ a week to help minimize dust that can cause static electricity.
    a. once
    c. three times

b. twice
d. four times

ANS: A PTS: 1 REF: 85

13. One way to investigate older and unusual computing systems is to keep track of ____ that still use these systems.
a. AICIS lists
c. SIGs
b. uniform reports
d. Minix

ANS: C PTS: 1 REF: 89

14. A ____ plan also specifies how to rebuild a forensic workstation after it has been severely contaminated by a virus from a drive you're analyzing.
a. disaster recovery
c. configuration management
b. risk management
d. security

ANS: A PTS: 1 REF: 91

15. You should have at least one copy of your backups on site and a duplicate copy or a previous copy of your backups stored in a safe ____ facility.
a. in-site
c. off-site
b. storage
d. online

ANS: C PTS: 1 REF: 91

16. In addition to performing routine backups, record all the updates you make to your workstation by using a process called ____ when planning for disaster recovery.
a. configuration management
c. recovery logging
b. risk assessment
d. change management

ANS: A PTS: 1 REF: 91

17. For labs using high-end ____ servers (such as Digital Intelligence F.R.E.D.C. or F.R.E.D.M.), you must consider methods for restoring large data sets.
a. RAID
c. WAN
b. ISDN
d. TEMPEST

ANS: A PTS: 1 REF: 91

18. ____ involves determining how much risk is acceptable for any process or operation, such as replacing equipment.
a. Risk configuration
c. Configuration management
b. Change management
d. Risk management

ANS: D PTS: 1 REF: 92

19. Computing components are designed to last 18 to ____ months in normal business operations.
a. 24
c. 36
b. 30
d. 42

ANS: C PTS: 1 REF: 92

20. In the ____, you justify acquiring newer and better resources to investigate computer forensics cases.
a. risk evaluation
c. configuration plan
b. business case
d. upgrade policy

ANS: B PTS: 1 REF: 92

21. By using ____ to attract new customers or clients, you can justify future budgets for the lab's operation and staff.
    a. pricing
    b. marketing
    c. budgeting
    d. changing

    ANS: B PTS: 1 REF: 94

COMPLETION

1. The _____ provides guidelines for managing a forensics lab and for acquiring official crime-lab certification.

   ANS:
   American Society of Crime Laboratory Directors (ASCLD)
   American Society of Crime Laboratory Directors
   ASCLD
   ASCLD (American Society of Crime Laboratory Directors)

   PTS: 1 REF: 74

2. The lab _____ sets up processes for managing cases and reviews them regularly.

   ANS: manager

   PTS: 1 REF: 74

3. For daily work production, several examiners can work together in a large open area, as long as they all have _____ level of authority and access need.

   ANS: the same

   PTS: 1 REF: 82

4. _____ Chapter 5, Section 3 (*http://nsi.org/Library/Govt/Nispom.html*) describes the characteristics of a safe storage container.

   ANS:
   NISPOM
   National Industrial Security Program Operating Manual
   NISPOM (National Industrial Security Program Operating Manual)
   National Industrial Security Program Operating Manual (NISPOM)

   PTS: 1 REF: 83

5. A(n) _____ plan ensures that you can restore your workstations and file servers to their original condition if a catastrophic failure occurs.

   ANS: disaster recovery

   PTS: 1 REF: 91

MATCHING

Match each item with a statement below

a. FireWire
b. Guidance Software
c. Business case
d. F.R.E.D.C.
e. ASCLD/LAB
f. SIG
g. MAN
h. Norton Ghost
i. Disaster recovery plan

1. sponsors the EnCE certification program
2. a high-end RAID server from Digital Intelligence
3. a plan you can use to sell your services to your management or clients
4. stands for Metropolitan Area Network
5. tool for directly restoring files
6. addresses how to restore a workstation you reconfigured for a specific investigation
7. ruled by the IEEE 1394B standard
8. can be a valuable source of support for recovering and analyzing uncommon systems
9. certification program that regulates how crime labs are organized and managed

1. ANS: B PTS: 1 REF: 81
2. ANS: D PTS: 1 REF: 91
3. ANS: C PTS: 1 REF: 92
4. ANS: G PTS: 1 REF: 88
5. ANS: H PTS: 1 REF: 91
6. ANS: I PTS: 1 REF: 91
7. ANS: A PTS: 1 REF: 92
8. ANS: F PTS: 1 REF: 89
9. ANS: E PTS: 1 REF: 74

SHORT ANSWER

1. What are the duties of a lab manager?

   ANS:
   The lab manager sets up the processes for managing cases and reviews these procedures regularly. Besides performing general management tasks, such as promoting group consensus in decision making, maintaining fiscal responsibility for lab needs, and encouraging honesty among staff members, the lab manager plans updates for the lab, such as new hardware and software purchases.

   The lab manager also establishes and promotes quality-assurance processes for the lab's staff to use, such as what to do when a case arrives, including logging evidence, specifying who can enter the lab, and establishing guidelines for filing reports. To ensure the lab's efficiency, the lab manager also sets reasonable production schedules for processing work.

   PTS: 1 REF: 74

2. Provide a brief explanation of how to plan a lab budget.

   ANS:

Lab costs can be broken down into daily, quarterly, and annual expenses. The better you understand these expenses, the better you can delegate resources for each investigation. Using a spreadsheet program helps you keep track of past investigation expenses. From past expenses, you can extrapolate expected future costs. Remember, expenses for a lab include computer hardware and software, facility space, and trained personnel. When creating a budget, start by estimating the number of computer cases your lab expects to examine and identifying the types of computers you're likely to examine, such as Windows PCs or Linux workstations.

PTS: 1 REF: 75

3. What are the four levels of certification offered by HTCN?

ANS:
Certified Computer Crime Investigator, Basic Level
Certified Computer Crime Investigator, Advanced Level
Certified Computer Forensic Technician, Basic
Certified Computer Forensic Technician, Advanced

PTS: 1 REF: 80

4. What are the minimum requirements for a computer investigation and forensics lab?

ANS:
Small room with true floor-to-ceiling walls
Door access with a locking mechanism
Secure container, such as a safe or heavy-duty file cabinet with a quality padlock
Visitor's log listing all people who have accessed your lab

PTS: 1 REF: 82

5. Illustrate a proper way of disposing materials on your computer investigation lab.

ANS:
Maintain two separate trash containers, one to store items unrelated to an investigation, such as discarded CDs or magnetic tapes, and the other for sensitive material that requires special handling to ensure that it's destroyed. Using separate trash containers maintains the integrity of criminal investigation processes and protects trade secrets and attorney-client privileged communications in a private corporation. Several commercially bonded firms specialize in disposing of sensitive materials. Your lab should have access to these services to maintain the integrity of your investigations.

PTS: 1 REF: 85

6. Give a brief explanation of a computer forensics lab auditing process.

ANS:
To make sure security policies and practices are followed, conduct routine inspections to audit your lab and evidence storage containers. Audits should include, but aren't limited to, the following facility components and practices:
-Inspect the lab's ceiling, floor, roof, and exterior walls at least once a month, looking for anything unusual or new.
- Inspect doors to make sure they close and lock correctly.
- Check locks to see whether they need to be replaced or changed.
- Review visitor logs to see whether they're being used properly.
- Review log sheets for evidence containers to determine when they have been opened and closed.

- At the end of every workday, secure any evidence that's not being processed on a forensic workstation.

PTS: 1 REF: 86

7. Briefly outline the process of selecting workstations for a police computer investigation lab.

ANS:
For small, local police departments, the majority of work involves Windows PCs and Apple Macintosh systems. The computer forensics lab of a small police department can be limited to one multipurpose forensic workstation with one or two basic workstations.

As a general rule, there should be at least one law enforcement computer investigator for every 250,000 people in a geographic region. For example, if your community has 1,000,000 people, the regional computer forensics lab should have at least four computer investigators. Each investigator should have at least one multipurpose forensic workstation with one general-purpose workstation.

PTS: 1 REF: 89

8. What peripheral devices should be stocked in your computer forensics lab?

ANS:
In addition to workstations and software, all labs should have a wide assortment of cables and spare expansion slot cards. Consider stocking your computer forensics lab with the following peripheral devices:
* 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster
* Ribbon cables for floppy disks
* Extra SCSI cards, preferably ultra-wide
* Graphics cards, both Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP)
* Extra power cords
* A variety of hard drives (as many as you can afford and in as wide a variety as possible)
* At least two 2.5-inch adapters from notebook IDE hard drives to standard IDE/ATA drives, SATA drives, and so on
* Computer hand tools, such as Phillips and flathead screwdrivers, a socket wrench, and a small flashlight

PTS: 1 REF: 90

9. Discuss the use of a laptop PC as a forensic workstation.

ANS:
Recent important advances in hardware technology offer more flexibility to computer forensics. You can now use a laptop PC with a FireWire (IEEE 1394B standard), USB 2.0, or PCMCIA SATA hard disks to create a lightweight, mobile forensic workstation. Improved throughput speeds of data transfer on laptops also make it easier to create bit-stream copies of suspect disk drives.

However, laptops are still limited as forensic workstations. Even with improved data transfer rates, acquiring data with a data compression-imaging tool such as EnCase or SafeBack creates a bottleneck. The processor speed determines how quickly you can acquire an image file of a hard disk. The faster the CPU on your laptop (or other PC), the faster the image is created in a compressed mode.

PTS: 1 REF: 92

10. What are the questions you need to ask when planning the justification step of a business case?

ANS:
Before you can start, you need to justify to the person controlling the budget the reason a lab is needed. This justification step requires asking the following questions:
* What type of computing investigation service is needed for your organization?
* Who are the potential customers for this service, and how will it be budgeted—as an internal operation (police department or company security department, for instance)—or an external operation (a for-profit business venture)?
* How will you advertise your services to customers?
* What time-management techniques will you use?
* Where will the initial and sustaining budget for business operations come from?

PTS: 1 REF: 94