Cyber Forensics Solution Set

I. Choose the correct alternative and rewrite the entire sentence with the correct alternative.

1. DFRWS stands for **Digital Forensic Research Workshop**.
2. **Interrogation** is the process of trying to get a suspect to confess to a specific incident or crime.
3. The legal process leading to a trail with the purpose of proving criminal or civil liability is called **Litigation**.
4. **Allegation** is a charge made against someone or something before proof has been found.
5. **Lab manager** is not a role performed by the incident response team.
6. Data that doesn't contribute to evidence of a crime or violation is called **Innocent information**.
7. **Live** acquisition method is used where computers can't be shut down.
8. The process of determining how much risk is acceptable for any process or operation is called **Risk management**.
9. FAT stands for **File Allocation Table**.
10. The device that reads and writes data to disk drive is **Head**.
11. **dd** command in Linux is used to copy data from a disk drive.
12. Which is not a data acquisition tool? **Recuva**
13. Which of the following is a steganography tool? **S-Tools**
14. Which of the following is not an image file format? **.wav**
15. The goal of an investigation is to? **Discover the truth**
16. Investigative reconstruction is composed of three different forms. Which of the following is NOT one of those three forms? **Intentional**
17. Crime scenes fall into which two categories? **Primary and Secondary**
18. HFS (Hierarchical File Systems) volumes are divided into logical blocks of? **512 bytes**
19. The standard format of submitting documents electronically in federal court is in **Portable Document Format (PDF)** format.
20. Which of the following hold the highest value of evidence in the court? **Documentary**
21. Syslog uses **TCP** to transfer log messages in a clear text format.
22. Network **Administrators** maintain logs of the inbound and outbound traffic routers handle.
23. Law enforcement investigators need a **warrant** to remove computers from a crime scene and transport them to a lab.
24. Which antenna is used in wireless base stations and provides a 360 degree horizontal radiation pattern? **Omnidirectional antenna**
25. Unsolicited Bulk E-mails (UBI) are called **Spam emails**.
26. ASER stands for? **Advanced Stealth Email Redirector**
27. What are different numbering systems used from layout systems? **Decimal, Legal Sequential**

28. Which tool is used for examining any standard smart card reader? **SIMCon**
29. Rules that you internalize and use to measure your performance is called **Ethics**.
30. Which of the following is the current formatting standard for email? **MIME**

II. Attempt any one.

a. Explain the ways of maintaining professional conduct.

- The professional conduct as a computer investigation and forensics analyst is critical because it determines the credibility.
- Professional conduct includes ethics, morals, and standards of behaviour.
- As a professional, we must exhibit the highest level of ethical behaviour at all times.
- To do so, we must maintain objectivity and confidentiality during an investigation, expand the technical knowledge continuously, and conduct ourselves with integrity.
- Maintaining objectivity means we must form and sustain unbiased opinions of your cases.
- Avoid making conclusions about findings until we have exhausted all reasonable leads and considered the available facts.
- The ultimate responsibility is to find digital evidence to support or refute the allegation.
- We must ignore external biases to maintain the integrity of fact-finding in all investigations.
- We must also maintain an investigation's credibility by keeping the case confidential.
- Discuss the case only with people who need to know about it, such as other investigators involved in the case or someone in the line of authority asking for an update.
- In some instances, corporate case might become a criminal case as serious as murder. If an investigator talks about the digital evidence with others, the case could be damaged because of pre-trial publicity.
- When working for an attorney on an investigation, the attorney-work-product rule and attorney-client privilege apply to all communication.
- This means we can discuss the case only with the attorney or other members of the team working with the attorney. All communication about the case to other people requires the attorney's approval.
- In addition to maintaining objectivity and confidentiality, we can enhance professional conduct by continuing the training.
- We should stay current with the latest technical changes in computer hardware and software, networking, and forensic tools. We should also learn about the latest investigation techniques we can use in your cases.

- To continue the professional training, we should attend workshops, conferences, and vendor courses. We might also need to continue formal education.
- In addition to education and training, membership in professional organizations adds to the credentials.
- These organizations often sponsor training and offer information exchanges of the latest technical improvements and trends in computer investigations.
- Also, keep up to date with the most recent books and read as much as possible about computer investigations and forensics.
- As a computer investigation and forensics professional, we are expected to maintain honesty and integrity. We must conduct yourself with the highest levels of integrity in all aspects of the life.
- Any indiscreet actions can embarrass us and give opposing attorneys opportunities to discredit us during testimony in court or in depositions.

b. Explain the responsibilities of a technical advisor.

- Know aspects of the seized system
- Direct investigator handling sensitive material
- Help secure the scene
- Help document the planning strategy for search and seizure
- Conduct ad hoc trainings
- Document activities
- Help conduct the search and seizure

c. What is CSIRT? What is the need for CSIRT?

- A team of trained professionals
- CSIRT members detect incidents at early stages and make reports to prevent further incidents
- CSIRT protects and secures critical information of an organization
- It secures organization’s data, hardware, and critical business policy
- It provides training on security awareness, intrusion detection, and penetration testing
- Documents and develops program
- It strengthens organization’s security
- Decreases the response time during any future security breach
- <u>Need for CSIRT</u>
  1. CSIRT provides rapid response to maintain the security and integrity of the systems
  2. Experienced in handling compromised network/systems.
  3. Being in a network of likeminded professionals, the CSIRT team members get to know the vulnerabilities firsthand

iv. CSIRT helps in deploying systems that follow the security policy of the organization

III. Attempt any one.

a. What are the recommendations for evidence locker combinations and evidence locker padlock?

- Recommendation for evidence locker combination
  - There must be equal security to both combination of container and content of the container
  - Destroy old combination after the new combination is created
  - Only authorized personnel must change the combination
  - Lock combination must be changed after every six months and when an authorized personnel leaves the company
- Recommendation for evidence locker padlock
  - Custodian for distributing the keys
  - Sequential number for every duplicate key
  - Record the listing of the assigned key
  - Monthly audit to ensure no key is lost
  - Inventory of all keys must be maintained
  - Locks and keys must be changed annually
  - Master key must not used for several keys

b. Explain any six file systems.

- Ext
  - First filesystem for the Linux operating system to overcome certain limitations of the Minix file system
  - Quickly replaced by the second extended file system
- Ext2
  - Standard filesystem with improved algorithms used on the Linux operating system for a number of years
  - Not a journaling file system
- Ext3
  - Journalled filesystem used in the GNU/Linux operating system
  - Can be mounted and used as an Ext2 filesystem
  - Can use file system maintenance utilities (like fsck) for maintaining and repairing alike Ext2 filesystem
- ZFS
  - Used in Sun Microsystems Solaris
  - Uses 128-bit addressing to perform read/write operation referred to as a "giga- terabyte" (a zettabyte)
  - Any modification to this filesystem will never increase its storage capacity
- FAT

    - 16 bit file system developed for MS-DOS
    - Used in consumer versions of Microsoft Windows till Windows Me
    - Considered relatively uncomplicated and became popular format for devices like floppy disks, USB devices, Digital cameras, flash disks
- NTFS
    - NTFS has three versions
        - v1.2 (v4.0) found in NT 3.51 and NT 4
        - v3.0 (v5.0) found in Windows 2000 and
        - v3.1 (v5.1) found in Windows XP and Windows Server 2003
    - Newer versions added extra features like quotas introduced by Windows 2000. In NTFS, anything such as file name, creation date, access permissions and even contents is written down as metadata
- HFS
    - Developed by Apple Computer to support Mac Operating System
    - Traditionally used by floppy and hard disks but now also used by CD-ROMs
- UFS
    - Derived from the Berkeley Fast File System (FFS) that was originally developed at Bell Laboratories from first version of UNIX FS
    - All BSD UNIX derivatives including FreeBSD, NetBSD, OpenBSD, NeXTStep, and Solaris use a variant of UFS
    - Acts as a substitute for HFS in Mac OS X

c. Explain following data acquisition tools: AccessData FTK, SafeBack, Encase.

- **AccessData FTK**
    - FTK Explorer acquires data that can help the investigator understand how other forensic tools in Windows work
    - This tool was first designed to examine disks and bit-stream disk- to-image files created by using other forensic software
    - FTK Explorer can make bit-stream disk-to-image copies of evidence disks
    - This tool allows the investigator to acquire the evidence disk from a logical partition level or a physical drive level
- **SafeBack**

    - SafeBack is also a MS-DOS data acquisition tool and can perform a CRC-32 calculation for each sector copied to ensure data integrity
    - SafeBack creates a log file of all transactions it performs
    - Functions:
    - Creates disk-to-image files
        - –Copies data from a source disk to an image on a tape drive
        - –Copies data from a partition to an image file
        - –Compresses acquired files to reduce the volume save-set sizes
- **Encase**
    - The Encase tool delivers advanced features for computer forensics and investigations
    - It is the primary data acquisition tool that is used by forensic investigators
    - Provides tools to conduct investigations with accuracy and efficiency
    - Data can be acquired by:
        - Disk to disk
        - Disk to network server drive
        - Parallel port with a laplink cable to the forensics workstation's disk drive

IV. Attempt any one.

a. Explain any six image file format.

TIFF

i. TIFF stands for Tagged Image File Format.
ii. Developed in 1986
iii. It's a data compression technique for monochrome and color images
iv. They occupy less space
v. Eg., images downloaded from internet

PICT

i. Supported by Macintosh
ii. Used for storing bit-mapped images

BMP

i. Developed by Microsoft
ii. Can save monochrome as well as color images
iii. Eg., wallpapers on computers, images created in paint brush also saved as bmp.
iv. Quality good
v. Occupy more memory space

ESP

i. File format of post script and is device independent
ii. Images can be readily be transferred from one application to another

JPEG

i. JPEG stands for Joint Photographic Expert Group.
ii. Uses compression algorithms
iii. Compressed images
iv. Occupy little space
v. Uses lossy compression, results in some loss of original data
vi. Quality not too good

GIF

i. GIF stands for Graphics Interchange Format.
ii. GIF is a raster file format designed for relatively basic images that appear mainly on the internet.
iii. Each file can support up to 8 bits per pixel and can contain 256 indexed colors.
iv. GIF files also allow images or frames to be combined, creating basic animations.

b. What is application password cracking? Explain any five application password cracking tools.

- Programs that attempt to determine the password and gain access by decrypting or disabling the normal password protection.
- A technique of trying to identify encrypted passwords.
- Brute force attack is when every single combination of characters is attempted.
- A dictionary attack is when a file of dictionary words is loaded to run against the user accounts.
- A hybrid attack is when combinations of characters are added to dictionary words.
- Guessing is when the attacker attempts to guess the user password using well-known defaults or information they have about the user.
- A rainbow attack uses the time-memory trade-off technique and generates a table of all possible hash values, and this table is searched to find the matching value and crack the password.
- Cain and Abel has a password cracking capability that can de used against Windows systems.
- LCP works by auditing and recovering passwords on Windows systems.
- Ophcrack is a tool that uses the rainbow-cracking technique.
- John the Ripper is a fast auditing tool that can crack both Windows and UNIX/Linux passwords.
- Brutus is a fast remote password cracker tool that works on Windows.
- Rock XP allows you to retrieve your XP product key used from your Windows installation.
- Use strong passwords for privileged user accounts.
- Practice principle of least privilege and least services.
- Change your password on a regular basis.
- Never use a dictionary word to include other languages.
- Use a mixture of character sets.

- Choose a pass phrase or saying to make a password strong and easy to remember.

c. **Explain the following steganography tools: Image Hide, Snow.exe, Camera/Shy.**

- **Image hide**
    - ImageHide is a steganography program which hides loads of text in images
    - Does simple encryption and decryption of data
    - Even after adding bytes of data, there will not be any increase in image size
    - Image looks the same to normal paint packages
    - Loads and saves to files and gets past all the mail sniffers
- **Snow.exe**
    - Snow is a whitespace steganography program and is used to conceal messages in ASCII text by appending whitespace to the end of lines
    - Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built in encryption is used, the message cannot be read even if it is detected
- **Camera/Shy**
    - Camera/Shy works with Windows and Internet Explorer and lets users share censored or sensitive information buried within an ordinary gif image
    - The program lets users encrypt text with a click of the mouse and bury the text in an image. The files can be password protected for further security
    - Viewers who open the pages with the Camera/Shy browser tool can then decrypt the embedded text on the fly by double-clicking on the image and supplying a password

V. Attempt any one.

a. **What is a router? What is the role of a router?**

- Routers can be hardware or software devices that route data from a local area network to a different
- network. Routers are responsible for making decisions about which of several paths network
- (or Internet) traffic will follow. If more than one path is available to transmit data, the
- router is responsible for determining which path is the best path to route the information.
- Routers also act as protocol translators and bind dissimilar networks. Routers limit physical broadcast traffic as they operate at layer 3 of the

OSI model. Routers typically use either link state or hop count based routing protocols to determine the best path.

- Routers are found at layer three of the OSI model. This is known as the networking layer.
- The network layer provides routing between networks and defines logical addressing, error handling, congestion control, and packet sequencing. This layer is concerned primarily with how to get packets from network A to network B. This is where IP addresses are defined. These addresses give each device on the network a unique (logical) address.
- Routers organize these addresses into classes, which are used to determine how to move packets from one network to another. All types of protocols rely on routing to move information from one point to another.

b. Explain Denial-of-Service attack.

- Denial-of-service (DoS) attacks fall into three categories:
  - o **Destruction**. Attacks that destroy the ability of the router to function.
  - o **Resource consumption**. Flooding the router with many open connections simultaneously.
  - o **Bandwidth consumption**. Attacks that attempt to consume the bandwidth capacity of the router's network.
- DoS attacks may target a user or an entire organization and can affect the availability of target systems or the entire network. The impact of DoS is the disruption of normal operations and the disruption of normal communications. It's much easier for an attacker to accomplish this than it is to gain access to the network in most instances. Smurf is an example of a common DoS attack. Smurf exploits the Internet Control Message Protocol (ICMP) protocol by sending a spoofed ping packet addressed to the broadcast address and has the source address listed as the victim. On a multiaccess network, many systems may possibly reply. The attack results in the victim being flooded in ping responses.

c. Explain wireless penetration testing.

- Before performing any tests on a production system, ensure that management and the owner of the system have agreed to the penetration tests. A search warrant is required for forensic analysis on any equipment the owner does not authorize you to test.
- You can detect wireless access points using Nmap's OS fingerprinting techniques. These scans can be scripted for scheduled coverage of a large network. Nessus, a vulnerability scanner, can also be used to detect wireless access points on the wired network. To do so, you can use plugin #11026, which identifies WAPs by TCP/IP fingerprint, HTTP, FTP, and SNMP responses.
- Improperly configured rogue access points can leave your network open to attackers. Wireless IPS/IDS systems can be used to monitor the network and shut down these rogue access points by suppressing the

wireless signal or shutting off the port to the switch once a rogue access point is detected.

- Wireless packet analyzers such as Kismet and Airodump-ng can be used to detect wireless networks and determine their security. They can also capture wireless network traffic that can be used later for encryption key cracking or viewing plaintext network data.
- Wireless packet injection allows attackers to generate traffic that can be used by tools to crack wireless encryption. Wireless cards must support packet injection for it to be successful.
- With enough data, WEP keys can be broken using brute force techniques, while WPA-PSK can only be cracked using dictionary attacks. This is why it is so important to use complex encryption keys.

VI. Attempt any one.

a. What should be included in written preliminary report?

- Anything that we write down as part of the examination for a report is subject to discovery from the opposing attorney.
- Therefore, a written preliminary report is considered a high-risk document because opposing counsel can demand discovery on it.
- If we a preliminary report, don’t destroy it before a final resolution of the case or any discovery issue related to the report.
- Destroying the report could be considered destroying or concealing evidence; among lawyers, this action is called **spoliation.**
- For written preliminary reports include the same information we would supply in an informal verbal report.
- First, restate the assignment to confirm with the client that the work we have done is focused correctly. Next, summarize what has been accomplished.
- Identify the systems we have examined, what tools we have used, and what we have seen.
- State evidence preservation or protection processes we have used.
- The following list shows additional items to include in the report:
  - Summarize the billing to date and estimate costs to complete the effort.
  - Identify the tentative conclusion (rather than the preliminary conclusion).
  - Identify areas for further investigation and obtain confirmation from the attorney on the scope of the examination.

b. What are e-mail servers? Explain their role in forensic investigations.

- An e-mail server is loaded with software that uses e-mail protocols for its services and maintains logs that we can examine and use in the investigation.
- To investigate e-mail abuse, we should know how an e-mail server records and handles the e-mail it receives.
- Some e-mail servers use databases that store users’ e-mails, and others use a flat file system.
- All e-mail servers can maintain a log of e-mails that are processed.

- Some e-mail servers are set up to log e-mail transactions by default; others must be configured to do so.
- Most e-mail administrators log system operations and message traffic to recover e-mails in case of a disaster, to make sure the firewall and e-mail filters are working correctly, and to enforce company policy.
- However, the e-mail administrator can disable logging or use circular logging, which overwrites the log file when it reaches a specified size or at the end of a specified time frame.
- The only way to access the log file information is from a backup file, which many e-mail administrators create before a log file is overwritten.
- These e-mail logs are usually formatted in plain text and can be read with a basic text editor, such as Notepad or vi.
- Administrators usually set e-mail servers to continuous logging mode.
- They can also log all e-mail information in the same file, or use one log file to record, for example, date and time information, the size of the e-mail, and the IP address.
- These separate log files are extremely useful when we have an e-mail header with a date and time stamp and an IP address, and we want to filter or sort the log files to narrow the search.
- In addition to logging e-mail traffic, e-mail servers maintain copies of clients' e-mail, even if the users have deleted messages from their inboxes.
- Some e-mail servers don't completely delete messages until the system is backed up. Even if the suspect deletes the e-mail, sometimes the e-mail administrator can recover the e-mail without restoring the entire e-mail system.
- With other systems, however, the e-mail administrator must recover the entire e-mail server to retrieve one deleted message.
- This process is similar to deleting files on a hard drive; the file is marked for deletion, but it's not truly deleted until another piece of data is written in the same place.
- E-mail servers wait to overwrite disk space until the server has been backed up.
- If we have a date and time stamp for an e-mail, the e-mail administrator should be able to recover it from backup media if the message is no longer on the e-mail server.

c. What are the ethics to be followed while presenting as expert witness to a court?

- Be professional, polite and sincere in testimony
- Always pay tribute to the jury
- Be enthusiastic during testimony
- Keep the jury interested in speech
- Be aware and prepare for the possible rebuttal questions especially from the opposing counsel
- Avoid overextending opinions
- Develop repetitions into details and descriptions for the jury
- Augment your image with the jury by following a formal dress code