Certified Incident Handler (ECIH)

1. Consistency in the investigative report is more important than the exact format in the report to eliminate uncertainty and confusion.

A. True

B. False

Answer(s): A

---

2. The Electronic Serial Number (ESN) is a unique __________ recorded on a secure chip in a mobile phone by the manufacturer.

A. 16-bit identifier

B. 24-bit identifier

C. 32-bit identifier

D. 64-bit identifier

Answer(s): C

---

3. Event correlation is a procedure that is assigned with a new meaning for a set of events that occur in a predefined interval of time.
Which type of correlation will you use if your organization wants to use different OS and network hardware platforms throughout the network?

A. Same-platform correlation

B. Cross-platform correlation

C. Multiple-platform correlation

D. Network-platform correlation

Answer(s): B

---

4. The Recycle Bin is located on the Windows desktop. When you delete an item from the hard disk, Windows sends that deleted item to the Recycle Bin and the icon changes to full from empty, but items deleted from removable media, such as a floppy disk or network drive, are not stored in the Recycle Bin.
What is the size limit for Recycle Bin in Vista and later versions of the Windows?

A. No size limit

B. Maximum of 3.99 GB

C. Maximum of 4.99 GB

D. Maximum of 5.99 GB

Answer(s): A

---

5. The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:

A. Maximize the investigative potential by maximizing the costs

B. Harden organization perimeter security

C. Document monitoring processes of employees of the organization

D. Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

Answer(s): D

---

6. First responder is a person who arrives first at the crime scene and accesses the victim's computer system after the incident. He or She is responsible for protecting, integrating, and

preserving the evidence obtained from the crime scene.
Which of the following is not a role of first responder?

A. Identify and analyze the crime scene

B. Protect and secure the crime scene

C. Package and transport the electronic evidence to forensics lab

D. Prosecute the suspect in court of law

Answer(s): D

---

7. Smith, an employee of a reputed forensic Investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry key Smith will check to find the above information?

A. UserAssist Key

B. MountedDevices key

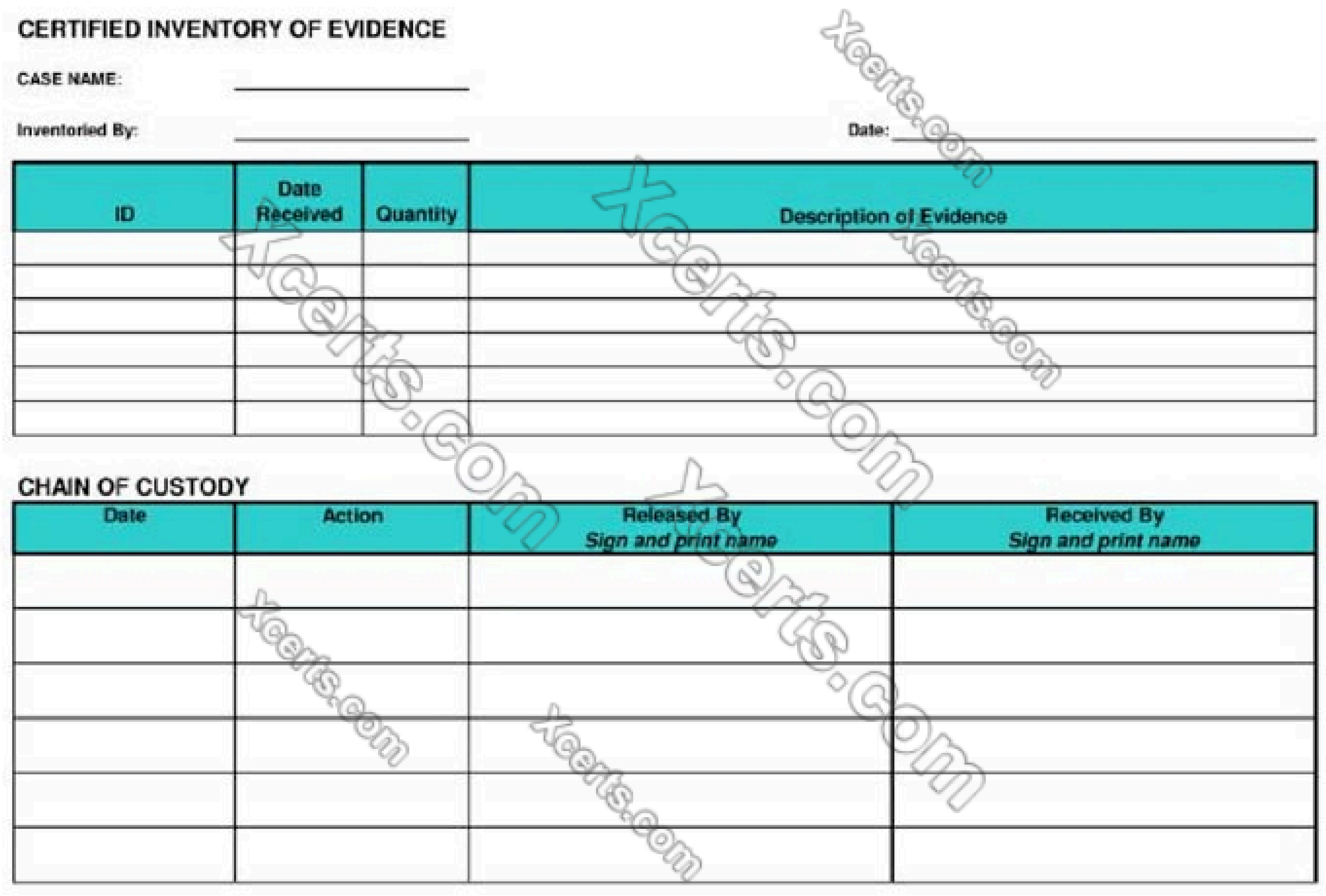
C. RunMRU key

D. TypedURLs key

Answer(s): C

---

8. What document does the screenshot represent?



CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: ____________________

Inventoried By: ____________________ Date: ____________________

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By *Sign and print name*	Received By *Sign and print name*

A. Chain of custody form

B. Search warrant form

C. Evidence collection form

D. Expert witness form

Answer(s): A

---

9. Which of the following commands shows you all of the network services running on Windows-based servers?

A. Net start

B. Net use

C. Net Session

D. Net share

Answer(s): A

---

10. Data compression involves encoding the data to take up less storage space and less bandwidth for transmission. It helps in saving cost and high data manipulation in many business applications.
Which data compression technique maintains data integrity?

A. Lossless compression

B. Lossy compression

C. Speech encoding compression

D. Lossy video compression

Answer(s): A

---

11. Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

A. Sample banners are used to record the system activities when used by the unauthorized user

B. In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring

C. The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken

D. At the time of seizing process, you need to shut down the computer immediately

Answer(s): D

---

12. Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

A. True

B. False

Answer(s): A

---

13. Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11i

Answer(s): A

---

14. Hash injection attack allows attackers to inject a compromised hash into a local session and use the hash to validate network resources.

A. True

B. False

Answer(s): A

---

15. Which of the following standard is based on a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

A. Daubert Standard

B. Schneiderman Standard

C. Frye Standard

D. FERPA standard

Answer(s): C

---

16. Injection flaws are web application vulnerabilities that allow untrusted data to be Interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?

A. SQL Injection

B. Password brute force

C. Nmap Scanning

D. Footprinting

Answer(s): A

---

17. Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Graph-based approach

B. Neural network-based approach

C. Rule-based approach

D. Automated field correlation approach

Answer(s): D

---

18. Which of the following commands shows you the NetBIOS name table each?

A. nbtstat -n

B. nbtstat -c

C. nbtstat -r

D. nbtstat -s

Answer(s): A

---

19. What is a bit-stream copy?

A. Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk

B. A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition

C. A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition

D. Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk

Answer(s): A

---

20. Which of the following is not a part of disk imaging tool requirements?

A. The tool should not change the original content

B. The tool should log I/O errors in an accessible and readable form, including the type and location of the error

C. The tool must have the ability to be held up to scientific and peer review

D. The tool should not compute a hash value for the complete bit stream copy generated from an image file of the source

Answer(s): D