Computer Hacking Forensic Investigator (CHFI-V10)

1. The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

A. Hierarchical File System (HFS)

B. New Technology File System (NTFS)

C. Global File System (GFS)

D. File Allocation Table (FAT

Answer(s): B

---

2. You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.

A. All forms should be placed in an approved secure container because they are now primary evidence in the case.

B. All forms should be placed in the report file because they are now primary evidence in the case.

C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.

D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.

Answer(s): D

---

3. In forensics.______are used lo view stored or deleted data from both files and disk sectors.

A. Hash algorithms

B. Host interfaces

C. Hex editors

D. SI EM tools

Answer(s): C

---

4. Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?

A. Create another VM by using the snapshot

B. Recommend changing the access policies followed by the company

C. Delete the snapshot from the source resource group

D. Delete the OS disk of the affected VM altogether

Answer(s): C

---

5. A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be Identified as______.

A. Cluster space

B. Slack space

C. Swap space

D. Sector space

Answer(s): B

---

6. What is the location of the binary files required for the functioning of the OS in a Linux system?

A. /bin

B. /run

C. /sbin

D. /root

Answer(s): A

---

7. Which of the following tool captures and allows you to interactively browse the traffic on a network?

A. Security Task Manager

B. ThumbsDisplay

C. Wireshark

D. RegScanner

Answer(s): C

---

8. Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

A. 25 50 44 46

B. ff d8 ff

C. 50 41 03 04

D. d0 0f 11 e0

Answer(s): B

---

9. James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA.

A. Fifth Amendment of the U.S. Constitution

B. Third Amendment of the U.S. Constitution

C. Fourth Amendment of the U.S. Constitution

D. First Amendment of the U.S. Constitution

Answer(s): A

---

10. Rule 1002 of Federal Rules of Evidence (US) talks about_____

A. Requirement of original

B. Admissibility of duplicates

C. Admissibility of original

D. Admissibility of other evidence of contents

Answer(s): A

---

11. In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

A. filecache.db

B. sigstore.db

C. install.db

D. config.db

Answer(s): D

---

12. What information do you need to recover when searching a victim's computer for a crime committed with specific e-mail message?

A. Username and password

B. Firewall log

C. E-mail header

D. Internet service provider information

Answer(s): C

---

13. Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

A. FATKit

B. CacheInf

C. Belkasoft Live RAM Capturer

D. Coreography

Answer(s): C

---

14. What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

A. Check the disk for Slack Space

B. Check the disk for connectivity errors

C. Repairs logical file system errors

D. Check the disk for hardware errors

Answer(s): C

---

15. Adam Is thinking of establishing a hospital In the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

B. Payment Card Industry Data Security Standard (PCI DSS)

C. Electronic Communications Privacy Act

D. Data Protection Act of 2018

Answer(s): A

---

16. Which of the following statements is true with respect to SSDs (solid-state drives)?

A. Faster data access, lower power usage, and higher reliability are some of the m<ijor advantages of SSDs over HDDs

B. SSDs cannot store non-volatile data

C. Like HDDs. SSDs also have moving parts

D. SSDs contain tracks, clusters, and sectors to store data

Answer(s): A

---

17. Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

A. WIN-DTRAI83202Xrelay-bin.index

B. WIN-DTRAI83202X-bin.nnnnnn

C. WIN-DTRAI83202Xslow.log

D. relay-log.info

Answer(s): C

---

18. Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away.

A. Computers on his wired network

B. 2.4Ghz Cordless phones

C. Satellite television

D. CB radio

Answer(s): B

---

19. Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

A. Web application attack

B. IDS attack

C. APT

D. Network attack

Answer(s): D

---

20. Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

A. Frye

B. IOCE

C. SWGDE & SWGIT

D. Daubert

Answer(s): D
