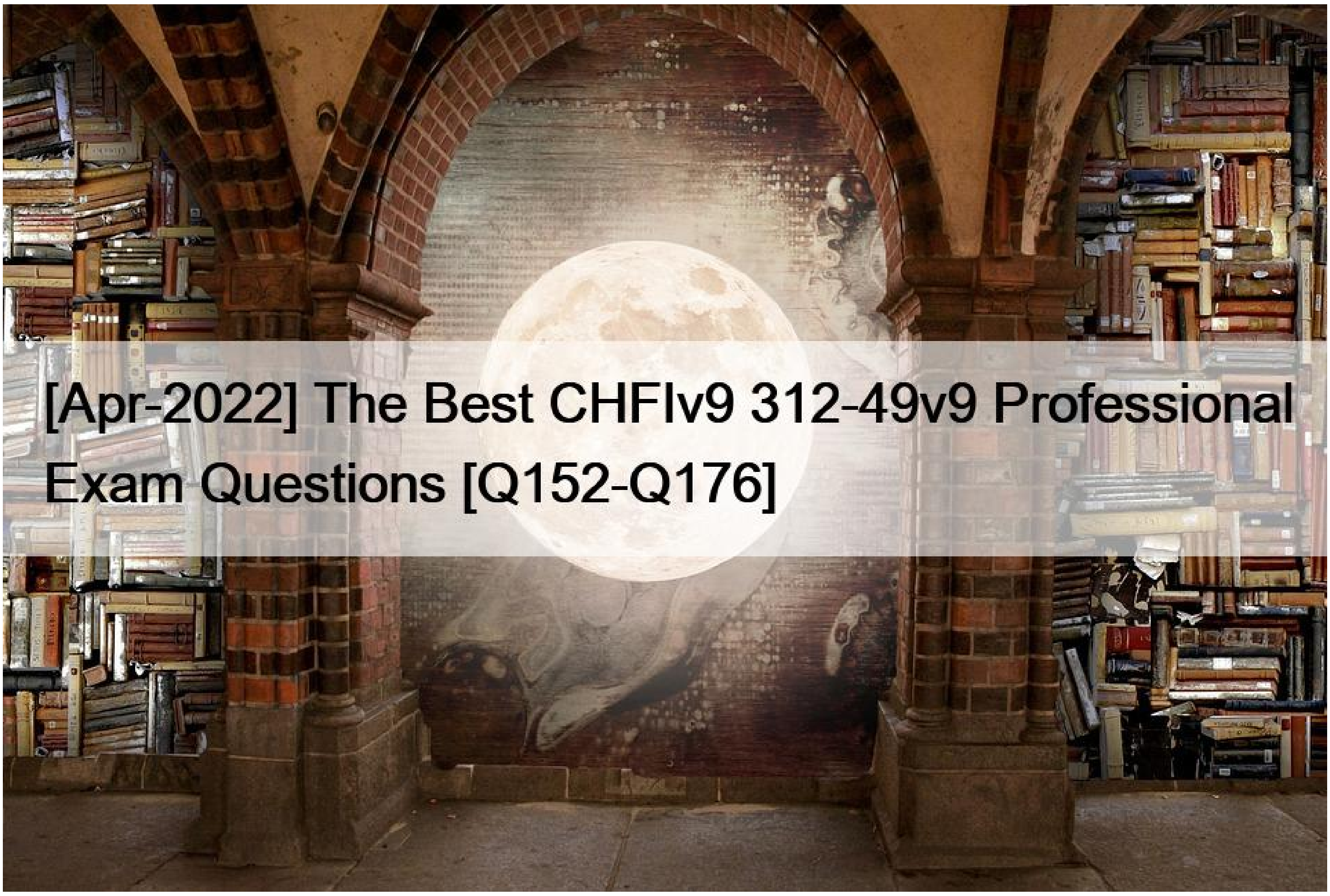
[Apr-2022 The Best CHFIv9 312-49v9 Professional Exam Questions [Q152-Q176



[Apr-2022] The Best CHFIv9 312-49v9 Professional Exam Questions
Try 100% Updated 312-49v9 Exam Questions [2022]

EC-COUNCIL 312-49v9 Exam Syllabus Topics:

TopicDetailsTopic 1- Operating System ForensicsTopic 2- Defeating Anti-Forensics TechniquesTopic 3- Understanding Hard Disks and File SystemsTopic 4- Investigat

NO.152 Jvanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

* Swap space
* Files and documents
* Application data
* Slack space

NO.153 You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company.

The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject&#8217;s computer. You inform the officer that you will not be able to comply with that request because doing so would:
* Violate your contract
* Cause network congestion
* Make you an agent of law enforcement
* Write information to the subject&#8217;s hard drive

NO.154 Which part of the Windows Registry contains the user&#8217;s password file?
* HKEY_LOCAL_MACHINE
* HKEY_CURRENT_CONFIGURATION
* HKEY_USER
* HKEY_CURRENT_USER

NO.155 Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?
* ParentIDPrefix
* LastWrite
* UserAssist key
* MRUListEx key

NO.156 What type of file is represented by a colon (:) with a name following it in the Master File

Table (MFT) of an NTFS disk?
* Compressed file
* Data stream file
* Encrypted file
* Reserved file

NO.157 The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks.

Which of the following would that be?
* Any data not yet flushed to the system will be lost
* All running processes will be lost
* The /tmp directory will be flushed
* Power interruption will corrupt the pagefile

NO.158 Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?
* Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
* Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
* Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
* Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

NO.159 Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully.

Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices.

How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?
* Two
* One
* Three
* Four

NO.160 Jones had been trying to penetrate a remote production system for the past two weeks.

This time however, he is able to get into the system. He was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?
* A system using Trojaned commands
* A honeypot that traps hackers
* An environment set up after the user logs in
* An environment set up before an user logs in

NO.161 Who is responsible for the following tasks?
* Non-forensics staff
* Lawyers
* System administrators
* Local managers or other non-forensic staff

NO.162 In General, ___________________ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.
* Network Forensics
* Data Recovery
* Disaster Recovery
* Computer Forensics

NO.163 Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?
* APIPA
* IANA
* CVE
* RIPE

NO.164 You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong.

When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

* ARP Poisoning
* DNS Poisoning
* HTTP redirect attack
* IP Spoofing

NO.165 Jason is the security administrator of ACMA metal Corporation. One day he notices the company&#8217;s Oracle database server has been compromised and the customer information along with financial data has been stolen.

The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.

Which organization coordinates computer crimes investigations throughout the United States?
* Internet Fraud Complaint Center
* Local or national office of the U.S. Secret Service
* National Infrastructure Protection Center
* CERT Coordination Center

NO.166 When an investigator contacts by telephone the domain administrator or controller listed by a whois lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?
* Title 18, Section 1030
* Title 18, Section 2703(d)
* Title 18, Section Chapter 90
* Title 18, Section 2703(f)
1 8 U.S.C. S 1029 Fraud and Related Activity in Connection with Access Devices

1 8 U.S.C. S 1030 Fraud and Related Activity in Connection with Computers

1 8 U.S.C. S 2703 Required Disclosure of Customer Communications Records

1 8 U.S.C. S 2703(d) Requirements for Court Order

1 8 U.S.C. S 2703(f) Requirement to Preserve Evidence

NO.167 Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format.

SAM file in Windows is located at:
* C:windowssystem32configSAM
* C:windowssystem32conSAM
* C:windowssystem32BootSAM
* C:windowssystem32driversSAM

NO.168 What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 server the course of its lifetime?
* forensic duplication of hard drive
* analysis of volatile data
* comparison of MD5 checksums
* review of SIDs in the Registry
Not MD5: MD5 checksums are used as integrity checks

User accounts are assigned a unique SID, and the SID are not reused.

NO.169 A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?
* Border Gateway Protocol
* Root Internet servers
* Gateway of last resort
* Reverse DNS

NO.170 To check for POP3 traffic using Ethereal, what port should an investigator search by?
* 143
* 25
* 110
* 125

NO.171 Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?
* Sectors
* Interface
* Cylinder
* Heads

NO.172 You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?
* The registry
* The swapfile
* The recycle bin
* The metadata

NO.173 Printing under a Windows Computer normally requires which one of the following files types to be created?
* EME
* MEM
* EMF
* CME

NO.174 Which US law does the interstate or international transportation and receiving of child pornography fall under?
* §18. U.S.C. 1466A
* §18. U.S.C 252
* §18. U.S.C 146A
* §18. U.S.C 2252

NO.175 Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?
* Events history
* Previously typed commands
* History of the browser
* Passwords used across the system

NO.176 You have been asked to investigate the possibility of computer fraud in the finance department of a company.

It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?
* The registry
* The swap file
* The recycle bin
* The metadata

312-49v9 Exam Questions Get Updated [2022 with Correct Answers: https://www.vceprep.com/312-49v9-latest-vce-prep.html]