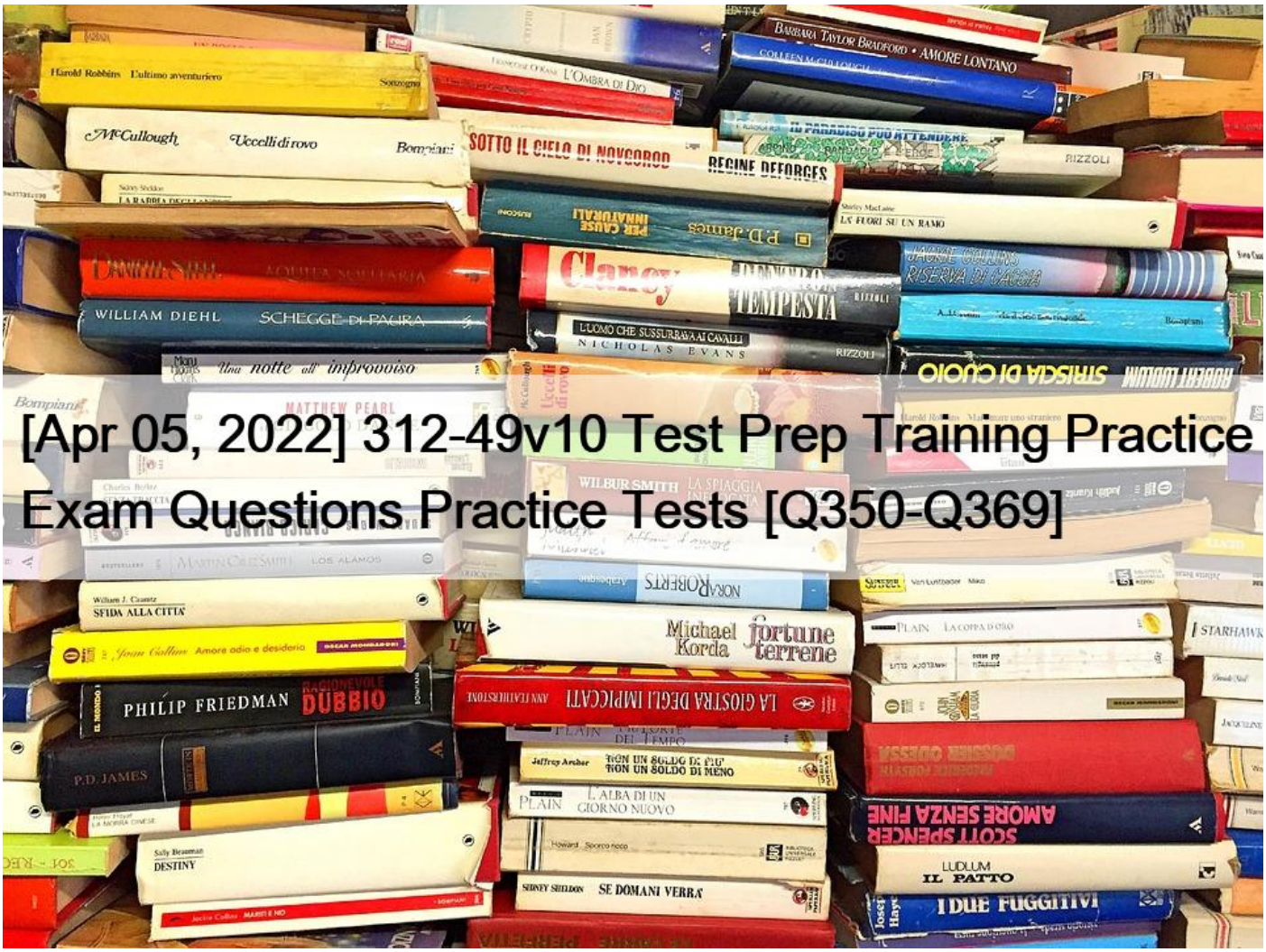
[Apr 05, 2022 312-49v10 Test Prep Training Practice Exam Questions Practice Tests [Q350-Q369



[Apr 05, 2022] 312-49v10 Test Prep Training Practice Exam Questions Practice Tests
Exam Questions Answers Braindumps 312-49v10 Exam Dumps PDF Questions

NO.350 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.

Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?
* All forms should be placed in an approved secure container because they are now primary evidence in the case.
* 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.
* 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.

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

NO.351 You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?
* Robust copy
* Incremental backup copy
* Bit-stream copy
* Full backup copy

NO.352 Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?
* Virtual Files
* Image Files
* Shortcut Files
* Prefetch Files

NO.353 Which of the following components within the android architecture stack take care of displaying windows owned by different applications?
* Media Framework
* Surface Manager
* Resource Manager
* Application Framework

NO.354 MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network.
* 48-bit address
* 24-bit address
* 16-bit address
* 32-bit address

NO.355 Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?
* network-based IDS systems (NIDS)
* host-based IDS systems (HIDS)
* anomaly detection
* signature recognition

NO.356 George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as “stealthy” as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?
* Nessus is too loud
* Nessus cannot perform wireless testing
* Nessus is not a network scanner
* There are no ways of performing a “stealthy” wireless scan

NO.357 As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through

penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization’s interest and your liabilities as a tester?
* Project Scope
* Rules of Engagement
* Non-Disclosure Agreement
* Service Level Agreement

NO.358 In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?
* The ISP can investigate anyone using their service and can provide you with assistance
* The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant
* The ISP can’t conduct any type of investigations on anyone and therefore can’t assist you
* ISP’s never maintain log files so they would be of no use to your investigation

NO.359 What does mactime, an essential part of the coroner’s toolkit do?
* It traverses the file system and produces a listing of all files based on the modification, access and change timestamps
* It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them
* The tools scans for i-node information, which is used by other tools in the tool kit
* It is too specific to the MAC OS and forms a core component of the toolkit

NO.360 Jacky encrypts her documents using a password. It is known that she uses her daughter’s year of birth as part of the password. Which password cracking technique would be optimal to crack her password?
* Rule-based attack
* Brute force attack
* Syllable attack
* Hybrid attack

NO.361 The process of restarting a computer that is already turned on through the operating system is called?
* Warm boot
* Ice boot
* Hot Boot
* Cold boot

NO.362 What malware analysis operation can the investigator perform using the jv16 tool?
* Files and Folder Monitor
* Installation Monitor
* Network Traffic Monitoring/Analysis
* Registry Analysis/Monitoring

NO.363 When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?
* Multiple access points can be set up on the same channel without any issues
* Avoid over-saturation of wireless signals
* So that the access points will work on different frequencies
* Avoid cross talk

NO.364 In Microsoft file structures, sectors are grouped together to form:
* Clusters

* Drives
* Bitstreams
* Partitions

NO.365 Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?
* The 10th Amendment
* The 5th Amendment
* The 1st Amendment
* The 4th Amendment

NO.366 Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk

80 heads/cylinder

63 sectors/track
* 53.26 GB
* 57.19 GB
* 11.17 GB
* 10 GB

NO.367 Which of the following tool can the investigator use to analyze the network to detect Trojan activities?
* Regshot
* TRIPWIRE
* RAM Computer
* Capsa

NO.368 Ivanovich, 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
* Application data
* Files and documents
* Slack space

NO.369 When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?
* on the individual computer’s ARP cache
* in the Web Server log files
* in the DHCP Server log files
* there is no way to determine the specific IP address

EC-COUNCIL 312-49v10 Exam Syllabus Topics:

TopicDetailsTopic 1- Understanding Hard Disks and File Systems- Investigating Email CrimesTopic 2- Data Acquisition and Duplication- Linux and Mac ForensicsTopic 3- Database Forensics- Network Forensics- Windows Forensics

Download Free EC-COUNCIL 312-49v10 Real Exam Questions:
https://www.topexamcollection.com/312-49v10-vce-collection.html]