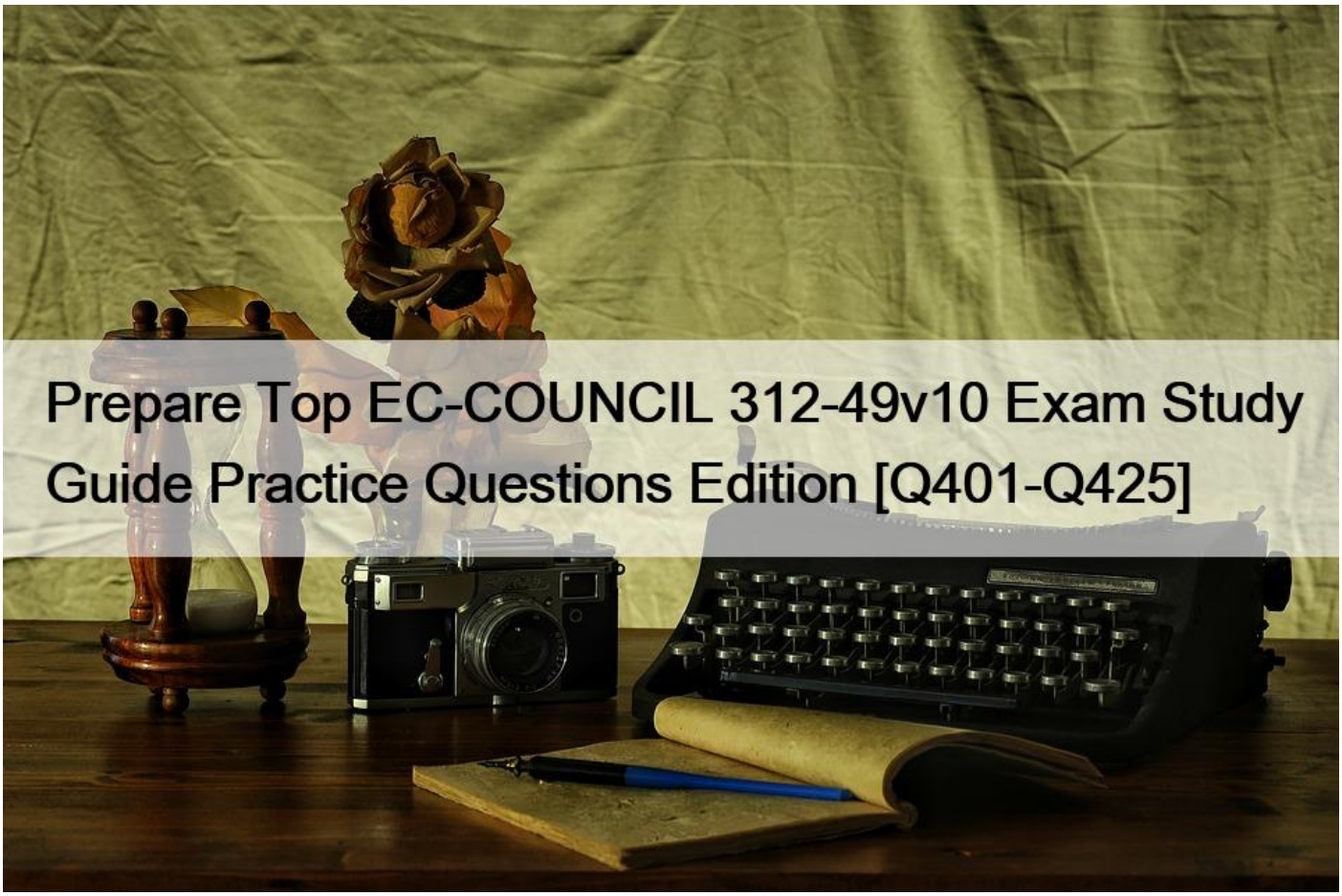
Prepare Top EC-COUNCIL 312-49v10 Exam Study Guide Practice Questions Edition [Q401-Q425



Prepare Top EC-COUNCIL 312-49v10 Exam Study Guide Practice Questions Edition
Go to 312-49v10 Questions - Try 312-49v10 dumps pdf

EC-COUNCIL 312-49v10 Exam Syllabus Topics:

TopicDetailsTopic 1- Database Forensics- Network Forensics- Windows ForensicsTopic 2- Defeating Anti-Forensics Techniques- Malware ForensicsTopic 3- Computer Forensics in Today's World- Investigating Web AttacksTopic 4- Computer Forensics Investigation Process- Dark Web Forensics- Mobile ForensicsTopic 5- Understanding Hard Disks and File Systems- Investigating Email Crimes

QUESTION 401

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

* the Microsoft Virtual Machine Identifier
* the Personal Application Protocol

* the Globally Unique ID
* the Individual ASCII String

QUESTION 402

Fill In the missing Master Boot Record component.

1. Master boot code

2. Partition table

3._____
* Boot loader
* Signature word
* Volume boot record
* Disk signature

QUESTION 403

What is kept in the following directory? HKLMSECURITYPolicySecrets
* Cached password hashes for the past 20 users
* Service account passwords in plain text
* IAS account names and passwords
* Local store PKI Kerberos certificates

QUESTION 404

How many possible sequence number combinations are there in TCP/IP protocol?
* 1 billion
* 320 billion
* 4 billion
* 32 million

QUESTION 405

What happens lo the header of the file once It Is deleted from the Windows OS file systems?
* The OS replaces the first letter of a deleted file name with a hex byte code: E5h
* The OS replaces the entire hex byte coding of the file.
* The hex byte coding of the file remains the same, but the file location differs
* The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

QUESTION 406

What is the size value of a nibble?
* 0.5 kilo byte
* 0.5 bit
* 0.5 byte
* 2 bits

QUESTION 407

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?
* Cross Examination
* Direct Examination
* Indirect Examination
* Witness Examination

QUESTION 408

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?
* Cloud as an Object
* Cloud as a Tool
* Cloud as an Application
* Cloud as a Subject

QUESTION 409

Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?
* Place PDA, including all devices, in an antistatic bag
* Unplug all connected devices
* Power off all devices if currently on
* Photograph and document the peripheral devices

QUESTION 410

A master boot record (MBR) is the first sector (“sector zero”) of a data storage device. What is the size of MBR?
* Depends on the capacity of the storage device
* 1048 Bytes
* 4092 Bytes
* 512 Bytes

QUESTION 411

A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.
* Mere Suspicion
* A preponderance of the evidence
* Probable cause
* Beyond a reasonable doubt

QUESTION 412

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?
* A text file deleted from C drive in sixth sequential order

* A text file deleted from C drive in fifth sequential order
* A text file copied from D drive to C drive in fifth sequential order
* A text file copied from C drive to D drive in fifth sequential order

QUESTION 413

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:
* Type Allocation Code (TAC)
* Integrated Circuit Code (ICC)
* Manufacturer Identification Code (MIC)
* Device Origin Code (DOC)

QUESTION 414

Which of the following is NOT a graphics file?
* Picture1.tga
* Picture2.bmp
* Picture3.nfo
* Picture4.psd

QUESTION 415

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?
* Kernel ring buffer information
* All mail server message logs
* Global system messages
* Debugging log messages

QUESTION 416

The MD5 program is used to:
* wipe magnetic media before recycling it
* make directories on an evidence disk
* view graphics files on an evidence drive
* verify that a disk is not altered when you examine it

QUESTION 417

Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?
* PUB.EDB
* PRIV.EDB
* PUB.STM
* PRIV.STM

QUESTION 418

Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?
* Azure CLI
* Azure Monitor
* Azure Active Directory
* Azure Portal

QUESTION 419

Which “Standards and Criteria” under SWDGE states that “the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure”?
* Standards and Criteria 1.7
* Standards and Criteria 1.6
* Standards and Criteria 1.4
* Standards and Criteria 1.5

QUESTION 420

One way to identify the presence of hidden partitions on a suspect’s hard drive is to:
* Add up the total size of all known partitions and compare it to the total size of the hard drive
* Examine the FAT and identify hidden partitions by noting an H in the partition Type field
* Examine the LILO and note an H in the partition Type field
* It is not possible to have hidden partitions on a hard drive

QUESTION 421

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?
* The year the evidence was taken
* The sequence number for the parts of the same exhibit
* The initials of the forensics analyst
* The sequential number of the exhibits seized

QUESTION 422

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?
* Volume Boot Record
* Master Boot Record
* GUID Partition Table
* Master File Table

QUESTION 423

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?
* Keep the device powered on
* Turn off the device immediately
* Remove the battery immediately
* Remove any memory cards immediately

QUESTION 424

To which phase of the computer forensics investigation process does “planning and budgeting of a forensics lab” belong?

* Post-investigation phase
* Reporting phase
* Pre-investigation phase
* Investigation phase

QUESTION 425

Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

* SOX
* HIPAA 1996
* GLBA
* PCI DSS

Free CHFI v10 312-49v10 Exam Question:
https://www.examslabs.com/EC-COUNCIL/CHFI-v10/best-312-49v10-exam-dumps.html]