# RealValidExam

## Try before you buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

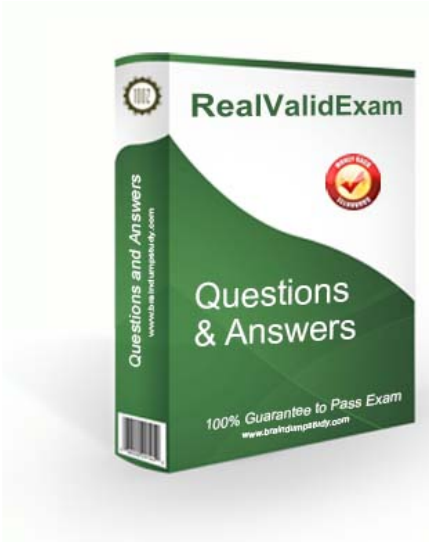
## Choose an exam to sample

Select a vendor...

Select an exam...

Your email address

Download Now




### QUALITY AND VALUE

RealValidExam Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

### TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

### EASY TO PASS

If you prepare for the exams using our RealValidExam testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

### TRY BEFORE BUY

RealValidExam offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.realvalidexam.com

100% real and valid exam dumps can ensure you pass at the first attempt

**Exam** : **312-49v9**

**Title** : ECCouncil Computer Hacking Forensic Investigator (V9)

**Vendor** : EC-COUNCIL

**Version** : DEMO

**NO.1** During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:
**A.** Inculpatory evidence
**B.** Terrible evidence
**C.** Mandatory evidence
**D.** Exculpatory evidence
***Answer:*** D

**NO.2** When should an MD5 hash check be performed when processing evidence?
**A.** Before the evidence examination has been completed
**B.** On an hourly basis during the evidence examination
**C.** After the evidence examination has been completed
**D.** Before and after evidence examination
***Answer:*** D

**NO.3** 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 medi a. 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?
**A.** Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
**B.** Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
**C.** Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media
**D.** Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
***Answer:*** B

**NO.4** Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?
**A.** ATM
**B.** UDP
**C.** OSPF
**D.** BPG
***Answer:*** C

**NO.5** When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

**A.** FF D8 FF E0 00 10
**B.** FF 00 FF 00 FF 00
**C.** FF FF FF FF FF FF
**D.** EF 00 EF 00 EF 00
***Answer:*** A

**NO.6** You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?
**A.** make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
**B.** sign a statement attesting that the evidence is the same as it was when it entered the lab
**C.** there is no reason to worry about this possible claim because state labs are certified
**D.** make an MD5 hash of the evidence and compare it to the standard database developed by NIST
***Answer:*** A

**NO.7** In which registry does the system store the Microsoft security IDs?
**A.** HKEY_CURRENT_USER (HKCU)
**B.** HKEY_CURRENT_CONFIG (HKCC)
**C.** HKEY_CLASSES_ROOT (HKCR)
**D.** HKEY_LOCAL_MACHINE (HKLM)
***Answer:*** D

**NO.8** Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?
**A.** SOX
**B.** FISMA
**C.** GLBA
**D.** HIPAA
***Answer:*** B

**NO.9** What is the default IIS log location?
**A.** SystemDrive\logs\LogFiles
**B.** %SystemDrive%\inetpub\logs\LogFiles
**C.** SystemDrive\inetpub\LogFiles
**D.** %SystemDrive\logs\LogFiles
***Answer:*** B

**NO.10** Which of the following file system is used by Mac OS X?
**A.** HFS+

**B.** NFS
**C.** EFS
**D.** EXT2
***Answer:*** A

**NO.11** Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate Americ a. What crime should Julie focus on?
**A.** Denial of Service attacks
**B.** Copyright infringement
**C.** Physical theft
**D.** Industrial espionage
***Answer:*** D

**NO.12** Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?
**A.** FISMA
**B.** HIPAA
**C.** SOX
**D.** GLBA
***Answer:*** C

**NO.13** Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?
**A.** Parameter/form tampering
**B.** Directory traversal
**C.** Unvalidated input
**D.** Security misconfiguration
***Answer:*** B

**NO.14** Windows identifies which application to open a file with by examining which of the following ?
**A.** The File extension
**B.** The file attributes
**C.** The file signature at the beginning of the file
**D.** The file Signature at the end of the file
***Answer:*** A

**NO.15** When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a

Blackberry device?
**A.** Blackberry Enterprise server
**B.** Blackberry desktop redirector
**C.** RIM Messaging center
**D.** Microsoft Exchange server
***Answer:*** D

**NO.16** Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?
**A.** Social Validation
**B.** Reciprocation
**C.** Friendship/Liking
**D.** Scarcity
***Answer:*** B

**NO.17** An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?
**A.** Ping of death
**B.** Nmap scan
**C.** Smurf
**D.** Fraggle
***Answer:*** A

**NO.18** A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?
**A.** Class A
**B.** Class D
**C.** Class C
**D.** Class B
***Answer:*** C

**NO.19** Which of the following tools is not a data acquisition hardware tool?
**A.** Triage-Responder
**B.** F-Response Imager
**C.** UltraKit
**D.** Atola Insight Forensic

***Answer:*** B

**NO.20** Which component in the hard disk moves over the platter to read and write information?
**A.** Spindle
**B.** Head
**C.** Actuator Axis
**D.** Actuator
***Answer:*** B

**NO.21** 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?
**A.** Place PDA, including all devices, in an antistatic bag
**B.** Photograph and document the peripheral devices
**C.** Unplug all connected devices
**D.** Power off all devices if currently on
***Answer:*** B

**NO.22** What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?
**A.** CF memory
**B.** SM memory
**C.** SD memory
**D.** MMC memory
***Answer:*** A

**NO.23** Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?
**A.** *IMEI#
**B.** #*06*#
**C.** *#06#
**D.** #06#*
***Answer:*** B

**NO.24** While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?
**A.** No particular field
**B.** Judging the character of defendants/victims

**C.** Legal issues
**D.** Technical material related to forensics
***Answer:*** A

**NO.25** What must an investigator do before disconnecting an iPod from any type of computer?
**A.** Disjoin the iPod
**B.** Join the iPod
**C.** Mount the iPod
**D.** Unmount the iPod
***Answer:*** D

**NO.26** Which of the following components within the android architecture stack take care of displaying windows owned by different applications?
**A.** Media Framework
**B.** Application Framework
**C.** Surface Manager
**D.** Resource Manager
***Answer:*** B

**NO.27** On Linux/Unix based Web servers, what privilege should the daemon service be run under?
**A.** Guest
**B.** You cannot determine what privilege runs the daemon service
**C.** Something other than root
**D.** Root
***Answer:*** C

**NO.28** Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?
**A.** He should contact the network operator for a Temporary Unlock Code (TUK)
**B.** He can attempt PIN guesses after 24 hours
**C.** He should contact the network operator for Personal Unlock Number (PUK)
**D.** Use system and hardware tools to gain access
***Answer:*** C

**NO.29** Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?
**A.** Enumerate all the users in the domain

**B.** Send DOS commands to crash the DNS servers
**C.** Perform DNS poisoning
**D.** Perform a zone transfer
***Answer:*** D

**NO.30** NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:
**A.** NTFS has lower cluster size space
**B.** FAT is an older and inefficient file system
**C.** NTFS is a journaling file system
**D.** FAT does not index files
***Answer:*** A