312-49Q&As

ECCouncil Computer Hacking Forensic Investigator (V9)

Pass EC-COUNCIL 312-49 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/312-49.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

A. Disk deletion

B. Disk cleaning

C. Disk degaussing

D. Disk magnetization

Correct Answer: C

QUESTION 2

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri\\'s duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company\\'s switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri\\'s computer

B. Poison the switch\\'s MAC address table by flooding it with ACK bits

C. Crash the switch with a DoS attack since switches cannot send ACK bits D. Enable tunneling feature on the switch

Correct Answer: A

QUESTION 3

What must be obtained before an investigation is carried out at a location?

A. Search warrant

B. Subpoena

C. Habeas corpus

D. Modus operandi

Correct Answer: A

QUESTION 4

What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch

B. Dalvik

C. Zygote

D. AirPlay

Correct Answer: A

QUESTION 5

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest

B. Root

C. You cannot determine what privilege runs the daemon service

D. Something other than root

Correct Answer: D

QUESTION 6

What file structure database would you expect to find on floppy disks?

A. NTFS

B. FAT32

C. FAT16

D. FAT12

Correct Answer: D

QUESTION 7

Which of the following statements is incorrect when preserving digital evidence?

A. Verify if the monitor is in on, off, or in sleep mode

B. Turn on the computer and extract Windows event viewer log files

C. Remove the plug from the power router or modem

D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

Correct Answer: B

QUESTION 8

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"

B. intitle:"exchange server"

C. locate:"logon page"

D. outlook:"search"

Correct Answer: A

QUESTION 9

How many bits is Source Port Number in TCP Header packet?

A. 16

B. 32

C. 48

D. 64

Correct Answer: A

QUESTION 10

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. digital attack

B. denial of service

C. physical attack

D. ARP redirect

Correct Answer: B

QUESTION 11

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times

B. a new log file is created everyday

C. a new log file is created each week

D. a new log is created each time the Web Server is started

Correct Answer: A

QUESTION 12

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display

B. Perform data acquisition without disturbing the state of the systems

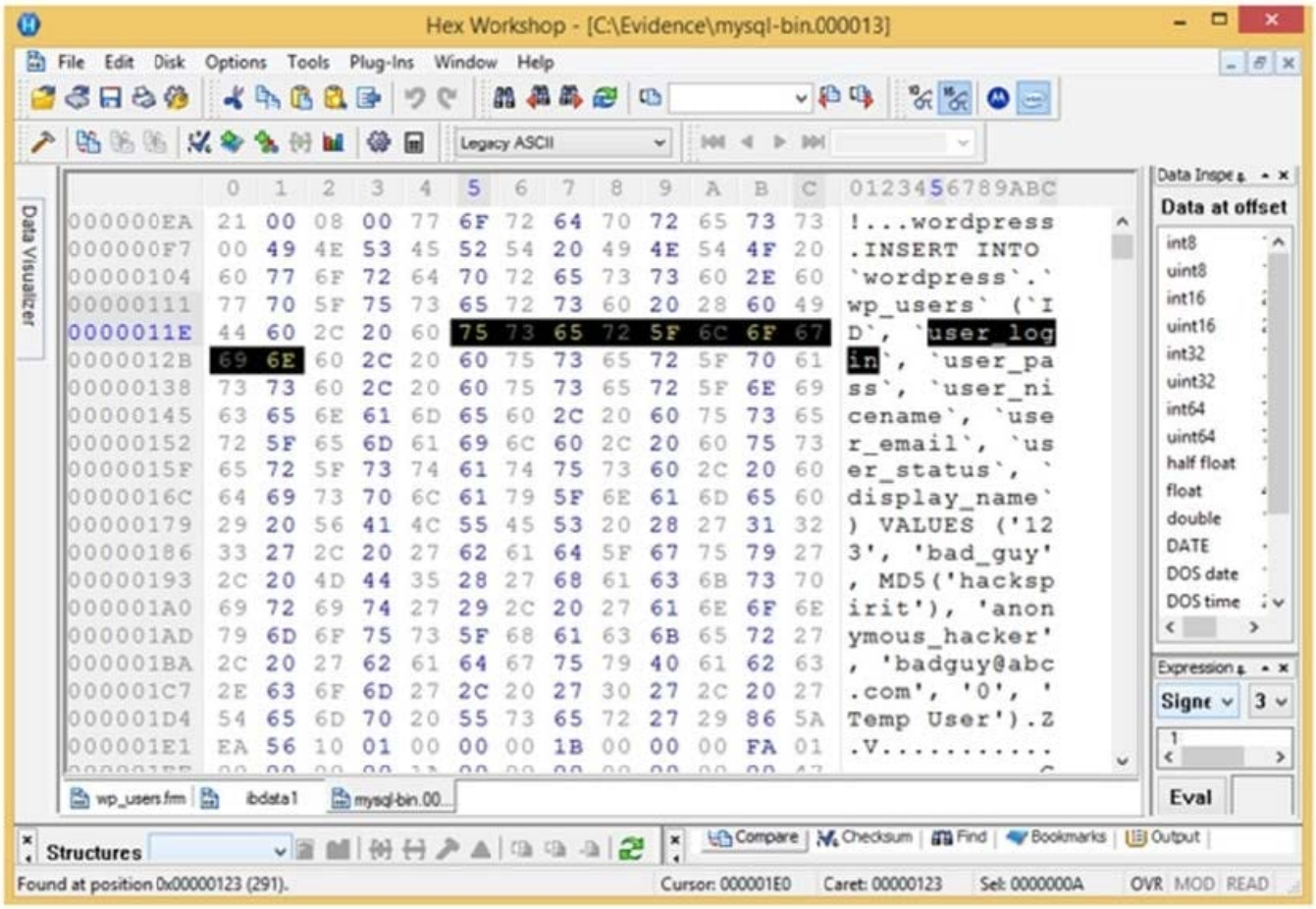
C. Open the systems, remove the hard disk and secure it

D. Switch off the systems and carry them to the laboratory

Correct Answer: A

QUESTION 13

Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



A. A user with username bad_guy has logged into the WordPress web application

B. A WordPress user has been created with the username anonymous_hacker

C. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database

D. A WordPress user has been created with the username bad_guy

Correct Answer: D

QUESTION 14

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

A. Computer Forensics Tools and Validation Committee (CFTVC)

B. Association of Computer Forensics Software Manufactures (ACFSM)

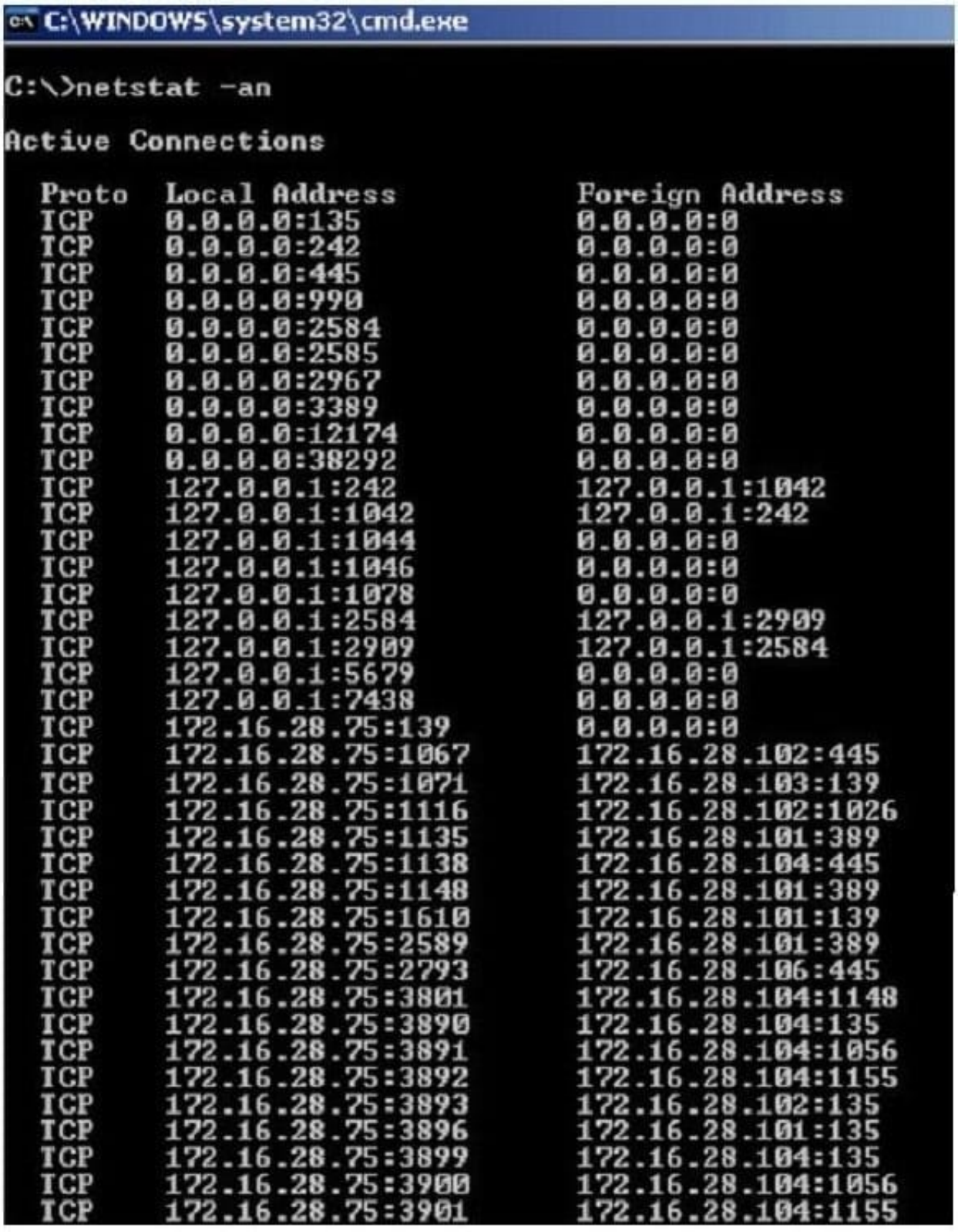
C. National Institute of Standards and Technology (NIST)

D. Society for Valid Forensics Tools and Testing (SVFTT)

Correct Answer: C

QUESTION 15

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.



He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

A. Those connections are established

B. Those connections are in listening mode

C. Those connections are in closed/waiting mode

D. Those connections are in timed out/waiting mode

Correct Answer: B