# Eccouncil 312-49 Practice Questions

**Shared by Blair on 17-08-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

### Options:

A- logical
B- anti-magnetic
C- magnetic
D- optical

### Answer:

D

## Question 2

Question Type: MultipleChoice

An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

### Options:

A- They should pause the running instance
B- They should keep the instance running as it stores critical data
C- They should terminate all instances connected via the same VPC
D- They should terminate the instance after taking necessary backup

### Answer:

D

## Question 3

Question Type: MultipleChoice

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?

### Options:

A- ParentIDPrefix
B- LastWrite
C- UserAssist key
D- MRUListEx key



### Answer:

A

## Question 4

Question Type: MultipleChoice

Which option best should a computer forensics lab used for investigations have?

### Options:

A- isolation
B- restricted access
C- open access
D- an entry log



### Answer:

B

## Question 5

Question Type: MultipleChoice

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

### Options:

A- Copyright
B- Design patent
C- Trademark
D- Utility patent

### Answer:

D



## Question 6

Question Type: MultipleChoice

In a Linux-based system, what does the command ''Last -F'' display?

### Options:

A- Login and logout times and dates of the system
B- Last run processes
C- Last functions performed
D- Recently opened files

### Answer:

A



## Question 7

Question Type: MultipleChoice

SO/IEC 17025 is an accreditation for Which option best:

### Options:

A- CHFI issuing agency
B- Encryption
C- Forensics lab licensing
D- Chain of custody

### Answer:

C

## Question 8

Question Type: MultipleChoice

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?

### Options:

A- Physical theft
B- Copyright infringement
C- Industrial espionage
D- Denial of Service attacks

### Answer:

C

## Question 9

Question Type: MultipleChoice

Which of the following tool can reverse machine code to assembly language?

### Options:

A- PEiD

B- RAM Capturer
C- IDA Pro
D- Deep Log Analyzer

## Answer:

C



P2P exams