# ECCouncil

## Exam EC1-349

### ECCouncil Computer Hacking Forensic Investigator

**Version: 7.3**

**[ Total Questions: 306 ]**

## Topic break down

| Topic | No. of Questions |
|---|---|
| Topic 1: Volume A | 75 |
| Topic 2: Volume B | 231 |

## Topic 1, Volume A

### Question No : 1 - (Topic 1)

Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?computer fraud. What is the term used for Jacob? testimony in this case?

**A.** Justification
**B.** Authentication
**C.** Reiteration
**D.** Certification

**Answer: B**

### Question No : 2 - (Topic 1)

Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

**A.** IT personnel
**B.** Employees themselves
**C.** Supervisors
**D.** Administrative assistant in charge of writing policies

**Answer: C**

### Question No : 3 - (Topic 1)

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.

**A.** Magnetic
**B.** Optical
**C.** Anti-Magnetic
**D.** Logical

**Answer: B**

**Question No : 4 - (Topic 1)**

Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to findThese 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather? responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused. In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples?desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

**A.** Grill cipher
**B.** Null cipher
**C.** Text semagram
**D.** Visual semagram

**Answer: A**

**Question No : 5 - (Topic 1)**

Which is a standard procedure to perform during all computer forensics investigations?

**A.** With the hard drive in the suspect PC, check the date and time in the system CMOSWith the hard drive in the suspect PC, check the date and time in the system? CMOS
**B.** With the hard drive removed from the suspect PC, check the date and time in the system CMOSWith the hard drive removed from the suspect PC, check the date and time

in the system? CMOS
**C.** With the hard drive in the suspect PC, check the date and time in the File Allocation Table
**D.** With the hard drive removed from the suspect PC, check the date and time in the system RAMWith the hard drive removed from the suspect PC, check the date and time in the system? RAM

**Answer: B**

**Question No : 6 - (Topic 1)**

The offset in a hexadecimal code is:

**A.** The 0x at the beginning of the code
**B.** The 0x at the end of the code
**C.** The first byte after the colon
**D.** The last byte after the colon

**Answer: A**

**Question No : 7 - (Topic 1)**

How often must a company keep log files for them to be admissible in a court of law?

**A.** All log files are admissible in court no matter their frequency
**B.** Weekly
**C.** Monthly
**D.** Continuously

**Answer: D**

**Question No : 8 - (Topic 1)**

What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

**A.** Every byte of the file(s) is given an MD5 hash to match against a master file

**B.** Every byte of the file(s) is verified using 32-bit CRC
**C.** Every byte of the file(s) is copied to three different hard drives
**D.** Every byte of the file(s) is encrypted using three different methods

**Answer: B**

**Question No : 9 - (Topic 1)**

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

**A.** One
**B.** Two
**C.** Three
**D.** Four

**Answer: B**

**Question No : 10 - (Topic 1)**

When using an iPod and the host computer is running Windows, what file system will be used?

**A.** iPod+
**B.** HFS
**C.** FAT16
**D.** FAT32

**Answer: D**

**Question No : 11 - (Topic 1)**

The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?

**A.** Detection

**B.** Hearsay
**C.** Spoliation
**D.** Discovery

**Answer: D**

## Question No : 12 - (Topic 1)

What does the acronym POST mean as it relates to a PC?

**A.** Power On Self Test
**B.** Pre Operational Situation Test
**C.** Primary Operating System Test
**D.** Primary Operations Short Test

**Answer: A**

## Question No : 13 - (Topic 1)

When examining a file with a Hex Editor, what space does the file header occupy?

**A.** The first several bytes of the file
**B.** One byte at the beginning of the file
**C.** None, file headers are contained in the FAT
**D.** The last several bytes of the file

**Answer: A**

## Question No : 14 - (Topic 1)

Why should you never power on a computer that you need to acquire digital evidence from?

**A.** When the computer boots up, files are written to the computer rendering the data nclean?When the computer boots up, files are written to the computer rendering the data ?nclean
**B.** When the computer boots up, the system cache is cleared which could destroy evidence

**C.** When the computer boots up, data in the memory buffer is cleared which could destroy evidenceWhen the computer boots up, data in the memory? buffer is cleared which could destroy evidence
**D.** Powering on a computer has no affect when needing to acquire digital evidence from it

**Answer: A**

**Question No : 15 - (Topic 1)**

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

**A.** Cracks every password in 10 minutes
**B.** Distribute processing over 16 or fewer computers
**C.** Support for Encrypted File System
**D.** Support for MD5 hash verification

**Answer: B**

**Question No : 16 - (Topic 1)**

You are working in the Security Department of a law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is a possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?fake email to the attorney that appears to come from his boss. What port do you send the email to on the company? SMTP server?

**A.** 10
**B.** 25
**C.** 110
**D.** 135

**Answer: B**

**Question No : 17 - (Topic 1)**

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file?its contents. The picture? quality is not degraded at all from this process. What kind of picture is this file?

**A.** Raster image
**B.** Vector image
**C.** Metafile image
**D.** Catalog image

**Answer: B**

**Question No : 18 - (Topic 1)**

You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

**A.** 70 years
**B.** The life of the author
**C.** The life of the author plus 70 years
**D.** Copyrights last forever

**Answer: C**

**Question No : 19 - (Topic 1)**

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

**A.** Typography
**B.** Steganalysis
**C.** Picture encoding
**D.** Steganography

**Answer: D**

**Question No : 20 - (Topic 1)**

What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?

**A.** Compressed file
**B.** Data stream file
**C.** Encrypted file
**D.** Reserved file

**Answer: B**

## Question No : 21 - (Topic 1)

To check for POP3 traffic using Ethereal, what port should an investigator search by?

**A.** 143
**B.** 25
**C.** 110
**D.** 125

**Answer: C**

## Question No : 22 - (Topic 1)

You are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect house after aYou are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect? house after a warrant was obtained and they located a floppy disk in the suspect bedroom. The disk contains several files, but they appear to be passwordwarrant was obtained and they located a floppy disk in the suspect? bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you could use to obtain the password?

**A.** Limited force and library attack
**B.** Brute force and dictionary attack
**C.** Maximum force and thesaurus attack
**D.** Minimum force and appendix attack

**Answer: B**