412-79$^{\text{Q\&As}}$

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

QUESTION 1

The MD5 program is used to:

A. wipe magnetic media before recycling it

B. make directories on a evidence disk

C. view graphics files on an evidence drive

D. verify that a disk is not altered when you examine it

Correct Answer: D

QUESTION 2

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?

A. the Microsoft Virtual Machine Identifier

B. the Personal Application Protocol

C. the Globally Unique ID

D. the Individual ASCII String

Correct Answer: C

QUESTION 3

An Expert witness give an opinion if:

A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors

B. To define the issues of the case for determination by the finder of fact

C. To stimulate discussion between the consulting expert and the expert witness

D. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case

Correct Answer: A

QUESTION 4

When cataloging digital evidence, the primary goal is to:

A. Make bit-stream images of all hard drives

B. Preserve evidence integrity

C. Not remove the evidence from the scene

D. Not allow the computer to be turned off

Correct Answer: B

QUESTION 5

One way to identify the presence of hidden partitions on a suspect s hard drive is to:

A. Add up the total size of all known partitions and compare it to the total size of the hard drive

B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field

C. Examine the LILO and note an H in the partition Type field

D. It is not possible to have hidden partitions on a hard drive

Correct Answer: A

412-79 Practice Test 412-79 Study Guide 412-79 Exam Questions