# EC0-349<sup>Q&As</sup>

Computer Hacking Forensic Investigator

## Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/ec0-349.html**

**100% Passing Guarantee**
**100% Money Back Assurance**

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

**Instant Download** After Purchase

**100% Money Back** Guarantee

**365 Days** Free Update

**800,000+** Satisfied Customers

**QUESTION 1**

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. RIM Messaging center

B. Blackberry Enterprise server

C. Microsoft Exchange server

D. Blackberry desktop redirector

Correct Answer: C

**QUESTION 2**

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. BPG

D. OSPF

Correct Answer: D

**QUESTION 3**

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

A. 143

B. 25

C. 110

D. 125

Correct Answer: C

**QUESTION 4**

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

Correct Answer: D

QUESTION 5

If you plan to startup a suspect\\'s computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect\\'s hard drive by booting to the hard drive.

A. deltree command

B. CMOS

C. Boot.sys

D. Scandisk utility

Correct Answer: C