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.passapply.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 technique is used by JPEGs for compression?

A. ZIP

B. TCD

C. DCT

D. TIFF-8

Correct Answer: C

QUESTION 2

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall

B. Circuit-level proxy firewall

C. Application-level proxy firewall

D. Stateful firewall

Correct Answer: D

QUESTION 3

What does mactime, an essential part of the coroner\\'s toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

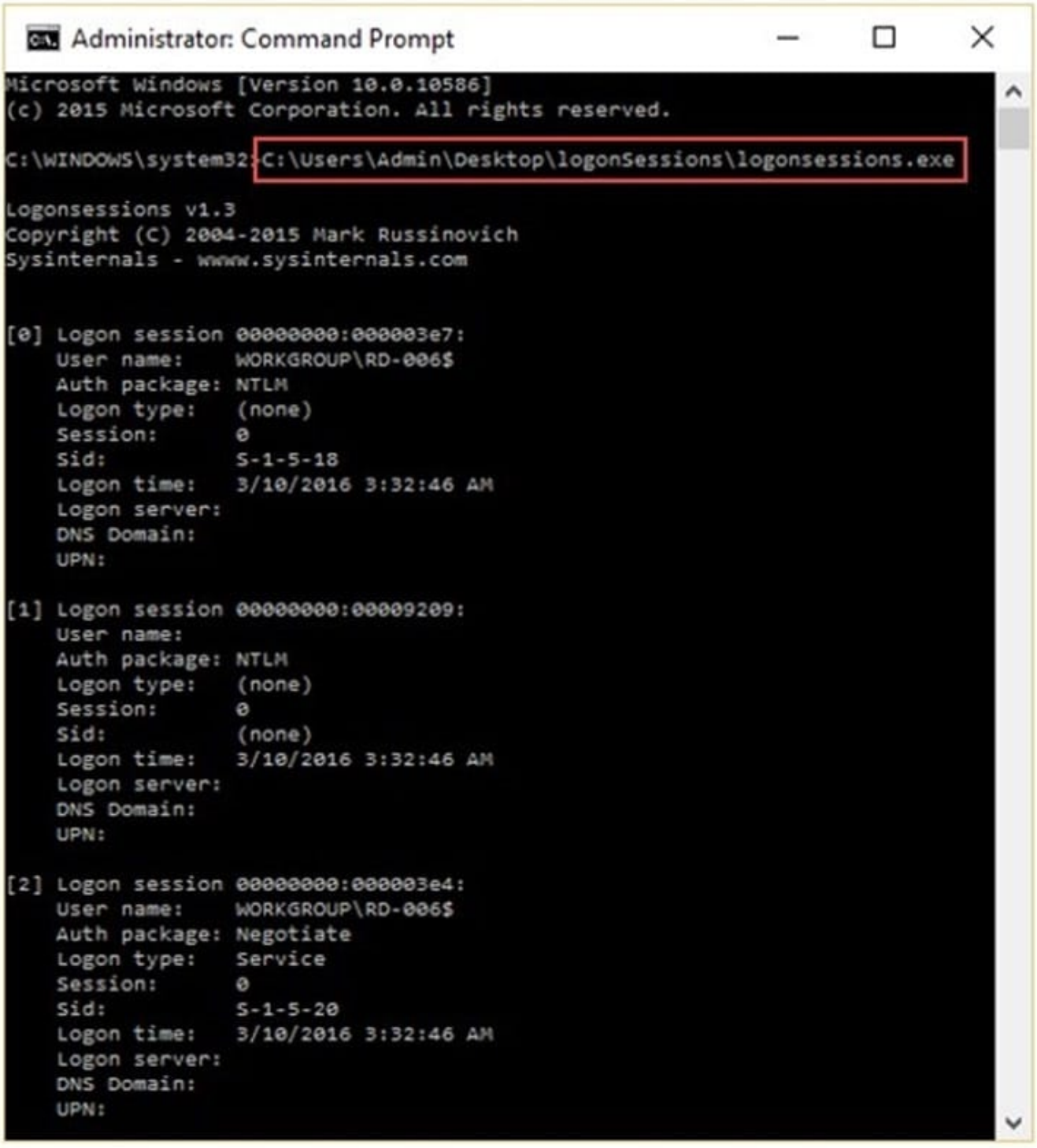
C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is too specific to the MAC OS and forms a core component of the toolkit

Correct Answer: A

QUESTION 4

What is the investigator trying to analyze if the system gives the following image as output?



A. All the logon sessions

B. Currently active logon sessions

C. Inactive logon sessions

D. Details of users who can logon

Correct Answer: B

QUESTION 5

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A. Routing Table

B. Firewall log

C. Configuration files D. Email Header

Correct Answer: D