Vendor:EC-COUNCIL

Exam Code:312-49V10

Exam Name:ECCouncil Computer Hacking Forensic
Investigator (V10)

Version: Demo

QUESTION 1

A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect\\'s available information but without any success. Which of the following tool can help the investigator to solve this issue?

A. Cain and Abel

B. Xplico

C. Recuva

D. Colasoft\\'s Capsa

Correct Answer: A

QUESTION 2

First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

A. System administrators

B. Local managers or other non-forensic staff

C. Forensic laboratory staff

D. Lawyers

Correct Answer: C

QUESTION 3

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL

B. Surface Manager

C. Media framework

D. WebKit

Correct Answer: A

QUESTION 4

Which is not a part of environmental conditions of a forensics lab?

A. Large dimensions of the room

B. Good cooling system to overcome excess heat generated by the work station

C. Allocation of workstations as per the room dimensions

D. Open windows facing the public road

Correct Answer: D

QUESTION 5

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?

A. Copyright

B. Design patent

C. Trademark

D. Utility patent

Correct Answer: D

QUESTION 6

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

A. Civil Investigation

B. Administrative Investigation

C. Both Civil and Criminal Investigations

D. Criminal Investigation

Correct Answer: B

QUESTION 7

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

A. Civil litigation testimony

B. Expert testimony

C. Victim advocate testimony

D. Technical testimony

Correct Answer: D

QUESTION 8

How will you categorize a cybercrime that took place within a CSP\\'s cloud environment?

A. Cloud as a Subject

B. Cloud as a Tool

C. Cloud as an Audit

D. Cloud as an Object

Correct Answer: D

QUESTION 9

Physical security recommendations: There should be only one entrance to a forensics lab

A. True

B. False

Correct Answer: A

QUESTION 10

Which of the following tool is used to locate IP addresses?

A. SmartWhois

B. Deep Log Analyzer

C. Towelroot

D. XRY LOGICAL

Correct Answer: A

QUESTION 11

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix

B. Nikto

C. Snort

D. Kismet

Correct Answer: C

QUESTION 12

Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot

records, or memory with a known and trusted baseline?

A. Signature-Based Detection

B. Integrity-Based Detection

C. Cross View-Based Detection

D. Heuristic/Behavior-Based Detection

Correct Answer: B

Reference: https://info-savvy.com/anti-forensics-techniques-rootkits/