University of Mumbai (UoM)

Programme: M.Sc. (Information Technology)

Subject: Computer Forensics

Class and Semester: Part II and IV

Class: M.sc(IT)-II Sem IV Subject: Computer Forensics

1. An argument for including computer forensic training computer security specialistsis:
   a. It provides an additionalcredential.
   b. It provides them with the tools to conduct their owninvestigations.
   c. It teaches them when it is time to call in lawenforcement.
   d. None of theabove.

2. Computers can play the following roles in a crime:
   a. Target, object, andsubject
   b. Evidence, instrumentality, contraband, or fruit ofcrime
   c. Object, evidence, andtool
   d. Symbol, instrumentality, and source ofevidence

3.The first US law to address computer crimewas:
a.Computer Fraud and Abuse Act (CFAA)
b.Florida Computer Crime Act
c.Computer AbuseAct
d. None of theabove

4.The following specializations exist in digitalinvestigations:
a.First responder (a.k.a. digital crime scenetechnician)
b.Forensicexaminer
c.Digitalinvestigator
d.all of the above

5.The first tool for making forensic copies of computer storage mediawas:
a.EnCase
b.ExpertWitness
c.dd
d.Safeback

6.One of the most common approaches to validating forensic software isto:
a.Examine the sourcecode
b.Ask others if the software isreliable
c.Compare results of multiple tools fordiscrepancies

d.Computer forensic tool testingprojects

7.An instrumentality of a crimeis:

a.An instrument used to commit acrime

b.A weapon or tool designed to commit acrime

c.Anything that plays a significant role in acrime

d.All of the above

8.Having a member of the search team trained to handle digitalevidence:

a. Can reduce the number of people who handle theevidence

b. Can serve to streamline the presentation of thecase

c. Can reduce the opportunity for opposing counsel to impugn the integrity of the evidence

d. All of the above

9.An attorney asking a digital investigator to find evidence supporting a particular line of inquiry is an exampleof:

a.Influencing theexaminer

b.Duediligence

c.Quid proquo

d.Voir dire

10.A digital investigator pursuing a line of investigation in a case because that line of investigation proved successful in two previous cases is an exampleof:

a.Logicalreasoning

b.Commonsense

c.Preconceived theory

d.Investigator'sintuition

11.A scientific truth attempts to identify roles that are universally true. Legal judgment, on the other hand, has a standard of proof in criminal prosecutionsof:

a.Balance of probabilities

b.Beyond a reasonable doubt

c.Acquittal

d.None of theabove

12.Regarding the admissibility of evidence, which of the following is not aconsideration:

a.Relevance

b.Authenticity

c.Bestevidence

d.Nominallyprejudicial

13.Log files are used by the forensicexaminer to____________.

a. Associate system events with specific useraccounts

b. Verify the integrity of the filesystem

c. Confirm loginpasswords

d. Determine if a specific individual is the guiltyparty

14.Standard operating procedures (SOPs) are important becausethey:

a. Help individuals avoid commonmistakes

b. Ensure that the best available methods areused

c. Increase the probability that two forensic examiners will reach the same conclusions when they examine theevidence

d. All of the above

15.The goal of an investigation is to:

a.Convict thesuspect

b.Discover thetruth

c.Find incriminatingevidence

d.All of theabove

16.An investigation can be hindered by thefollowing:

a.Preconceivedtheories

b.Improperly handledevidence

c.Offender concealmentbehavior

d.All of the above

17.When you have developed a theory, what can you do to confirm that your hypothesis is correct?

a.Predict, based on your hypothesis, where artifacts should belocated

b.Perform experiments to test results and rule out alternateexplanations

c.Conclude, based on your findings, whether the evidence supports thehypothesis

d.All of the above

18.Which of the following is NOT a class characteristic of files on magneticmedia:

a.Extension (e.g., .jpg,.exe)

b. Date-time stamp (e.g., 02/28/2004 03:00 PM)

c. Name (e.g.,encase.exe)

d. Directorystructure

19.Which of the following would be considered an individualcharacteristic?

a.The originating IP address in a network packet or e-mailheader

b.A scratch on the glass of a flatbed scanner or digital cameralens

c.Date-time stamps of files on a disk or entries in adatabase

d.All of theabove

University of Mumbai (UoM)

Programme: M.Sc. (Information Technology)

Subject: Computer Forensics

Class and Semester: Part II and IV

20.When digital photographs containing child pornography are found on a home computer, investigators can assertthat:

a.Someone in the house transferred the photographs onto the computer from a disk or theInternet.

b.Someone in the house took the photographs with a digital camera and transferred them directly onto thecomputer.

c.Someone gained unauthorized access to the computer via the Internet and transferred the photographs onto thecomputer.

d.None of the above.