Chapter 4- Digital Evidence (CO4)

**MCQ**

1. A valid definition of digital evidence is:

A. Data stored or transmitted using a computer

B. Information of probative value

C. Digital data of probative value

D. Any digital evidence on a computer

Ans: C

2. What are the three general categories of computer systems that can contain digital evidence?

A. Desktop, laptop, server

B. Personal computer, Internet, mobile telephone

C. Hardware, software, networks

D. Open computer systems, communication systems, and embedded systems

Ans: D

3. In terms of digital evidence, a hard drive is an example of:

A. Open computer systems

B. Communication systems

C. Embedded computer systems

D. None of the above

Ans: A

4. In terms of digital evidence, a mobile telephone is an example of:

A. Open computer systems

B. Communication systems

C. Embedded computer systems

D. None of the above

Ans: C

5. In terms of digital evidence, a Smart Card is an example of:

A. Open computer systems

B. Communication systems

C. Embedded computer systems

D. None of the above

Ans: C

6. In terms of digital evidence, the Internet is an example of:

A. Open computer systems

B. Communication systems

C. Embedded computer systems

D. None of the above

Ans: B

7. Computers can be involved in which of the following types of crime?

A. Homicide and sexual assault

B. Computer intrusions and intellectual property theft

C. Civil disputes

D. All the above

Ans: D

8. A logon record tells us that, at a specific time:

A. An unknown person logged into the system using the account

B. The owner of a specific account logged into the system

C. The account was used to log into the system

D. None of the above

Ans: C

9. Cyber trails are advantageous because:

A. They are not connected to the physical world.

B. Nobody can be harmed by crime on the Internet.

C. They are easy to follow.

D. Offenders who are unaware of them leave behind more clues than they otherwise

would have.

Ans: D

10. Private networks can be a richer source of evidence than the Internet because:

A. They retain data for longer periods of time.

B. Owners of private networks are more cooperative with law enforcement.

C. Private networks contain a higher concentration of digital evidence.

D. All the above.

Ans: C

11. Due to caseload and budget constraints, often computer security professionals attempt to limit

the damage and close each investigation as quickly as possible. Which of the following is NOT

a significant drawback to this approach?

A. Each unreported incident robs attorneys and law enforcement personnel of an opportunity

to learn about the basics of computer-related crime.

B. Responsibility for incident resolution frequently does not reside with the security

professional, but with management.

C. This approach results in under-reporting of criminal activity, deflating statistics that are

used to allocate corporate and government spending on combating computer-related crime.

D. Computer security professionals develop loose evidence processing habits that can make

it more difficult for law enforcement personnel and attorneys to prosecute an offender.

None of the above

Ans: B

12. The criminological principle which states that, when anyone, or anything, enters a crime scene

he/she takes something of the scene with him/her, and leaves something of himself/herself

behind, is:

A. Locard’s Exchange Principle

B. Differential Association Theory

C. Beccaria’s Social Contract

D. None of the above

Ans: A

13. The author of a series of threatening e-mails consistently uses “im” instead of “I’m.” This is

an example of:

A. An individual characteristic

B. An incidental characteristic

C. A class characteristic

D. An indeterminate characteristic

Ans: A

14. Personal computers and networks are often a valuable source of evidence. Those involved with

\_\_\_\_\_\_\_ should be comfortable with this technology.

A. Criminal investigation

B. Prosecution

C. Defense work

D. All of the above

Ans:

15. An argument for including computer forensic training computer security specialists is:

A. It provides an additional credential.

B. It provides them with the tools to conduct their own investigations.

C. It teaches them when it is time to call in law enforcement.

D. None of the above.

Ans: C

16. The digital evidence are used to establish a credible link between\_\_\_\_\_\_\_\_\_\_\_\_

A. Attacker and victim and the crime scene

B. Attacker and the crime scene

C. Victim and the crime scene

D. Attacker and Information

Ans: A

17. Digital evidences must follow the requirements of the \_\_\_\_\_\_\_\_\_\_\_

A. Ideal Evidence rule

B. Best Evidence rule

C. Exchange rule

D. All the mentioned

Ans: B

18. From the two given statements 1 and 2, select the correct option from a-d.

a. Original media can be used to carry out digital investigation process.

b. By default, every part of the victim’s computer is considered as unreliable.

A. a and b both are true

B. a is true and b is false

C. a and b both are false

D. a is false and b is true

Ans: B

19. The evidences or proof can be obtained from the electronic source is called the \_\_\_\_\_\_\_\_\_\_\_

A. digital evidence

B. demonstrative evidence

C. Explainable evidence

D. substantial evidence

Ans: A

20. Which of the following is not a type of volatile evidence?

A. Routing tables

B. Main memory

C. Log files

D. Cached data

Ans: C

21. The evidence must be usable in the court which is called as\_\_\_\_\_\_\_

A. Admissible

B. Authentic

C. Complete

D. Reliable

Ans: A

22. Photographs, videos, sound recordings, X-rays, maps drawing, graphs, charts is a a type of

\_\_\_\_\_\_\_\_\_\_\_\_\_

A. Illustrative evidence

B. Electronic evidence

C. Documented evidence

D. Explainable evidence

Ans: A

23. Email, hard drives are examples of \_\_\_\_\_\_\_\_\_\_\_\_

A. Illustrative evidence

B. Electronic evidence

C. Documented evidence

D. Explainable evidence

Ans: B

24. Blood, fingerprints, DNA these are examples of\_\_\_\_\_\_\_\_\_\_\_\_

A. Illustrative evidence

B. Electronic evidence

C. Documented evidence

D. Substantial evidence

Ans: D

25. When an incident takes place, a criminal will leave a hint evidence at the scene and remove a

hint from the scene which is called as \_\_\_\_\_\_\_\_\_\_\_\_

A. Locard’s Exchange principle

B. Anderson’s Exchange principle

C. Charles’s Anthony principle

D. Kevin Ashton principle

Ans: A

26. Which is not procedure to establish a chain of custody?

A. Save the original materials.

B. Take\photos of physical evidence.

C. Don’t take screenshots of digital evidence content.

D. Document date, time, and any other information of receipt.

Ans: C

27. Which is not related with digital evidence?

A. Work with the original evidence to develop procedures.

B. Use clean collecting media.

C. Document any extra scope.

D. Consider safety of personnel at the scene.

Ans: A

28. Which is example of non-volatile memory.

A. Flash memory

B. Registers and Cache

C. Process table

D. Arp cache

Ans: A

29.\_\_\_\_\_\_\_\_\_ is known as testimonial.

A. Oath affidavit

B. DNA samples

C. Fingerprint

D. Dried blood

Ans: A

30.The process of ensuring that providing or obtaining the data that you have collected is similar

to the data provided or presented in a court is known as\_\_\_\_\_\_\_\_\_\_\_

A. Evidence validation

B. Relative evidence

C. Best evidence

D. Illustrative evidence

Ans: A

31.When cases got to trial your forensics examiner play one of \_\_\_\_ role.

A. 2

B. 4

C. 3

D. 5

Ans. A

32.Types of digital evidence

A. Eye witness

B. Picture and video

C. Paper work

D. None of the above

Ans B

33.Rule of evidence is also known as \_\_\_\_\_\_\_\_\_\_

A. Law of witness

B. Law of litigation

C. Law of evidence

D. All of the above

Ans. C

**True or False Questions**

1. Digital evidence is only useful in a court of law.

A. True

B. False

Ans: B

2. Attorneys and police are encountering progressively more digital evidence in their work.

A. True

B. False

Ans: A

3. Video surveillance can be a form of digital evidence.

A. True

B. False

Ans: A

4. All forensic examinations should be performed on the original digital evidence.

A. True

B. False

Ans: B

5. Digital evidence can be duplicated exactly without any changes to the original data. A. True

B. False

Ans: B

6. Computers were involved in the investigations into both World Trade Center attacks. A. True

B. False

Ans: A

7. Digital evidence is always circumstantial.

A. True

B. False

Ans: B

8. Digital evidence alone can be used to build a solid case.

A. True

B. False

Ans: B

9. Computers can be used by terrorists to detonate bombs. A. True

B. False

Ans: A

10. The aim of a forensic examination is to prove with certainty what occurred. A. True

B. False

Ans: B

11. Even digital investigations that do not result in legal action can benefit from principles of

forensic science.

A. True

B. False

Ans: A

12. Forensic science is the application of science to investigation and prosecution of crime or to

the just resolution of conflict.

A. True

B. False

Ans: A

c) cost

d) None of these

11. Digital evidence may be in the form\_\_.

a) Cookies

b) Registry

c) Slack Space

d) all of the above

12.To meet requirements of judging and to withstand or face any challenges, it is essential to

follow the \_\_\_\_procedure.

a) Investigation

b) evidence-handling

c) organizational

d) None of these

13.\_\_\_\_are everywhere in today's world, helping people communication locally and globally

with ease.

a) Digital devices

b) Digital evidence

c) Internet

d) none of these

14.The \_\_\_or true writing or recording must be confessed in court to prove it's contents without

any expectations.

a) Best

b) digital

c) original

d) None of the above