Program: BE Information Technology Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VI

Course Code: ITDLO6023 and Course Name: Digital Forensics

Time: 1 hour Max. Marks: 50

==

Note to the students:- All the Questions are compulsory and carry equal marks.

Q1.	Digital Forensics entails ______.
Option A:	a) Accessing the system's directories viewing mode and navigating through the various systems files and folders
Option B:	b) Undeleting and recovering lost files
Option C:	c) Identifying and solving computer crimes
Option D:	d) The identification, preservation, recovery, restoration and presentation of digital evidence from systems and devices
Q2.	Which of the following is not a rule of digital forensics?
Option A:	a) An examination should be performed on the original data
Option B:	b) A copy is made onto forensically sterile media. New media should always be used if available.
Option C:	c) The copy of the evidence must be an exact, bit-by-bit copy
Option D:	d) The examination must be conducted in such a way as to prevent any modification
Q3.	In terms of digital evidence, a hard drive is an example of:
Option A:	a) Open computer systems
Option B:	b) Communication systems
Option C:	c) Embedded computer systems
Option D:	d) Open computer systems, communication systems, embedded systems
Q4.	Computers can play the following roles in a crime:
Option A:	a) Target, object, and subject
Option B:	b) Evidence, instrumentality, contraband, or fruit of crime
Option C:	c) Object, evidence, and tool
Option D:	d) Symbol, instrumentality, and source of evidence
Q5.	What is the most significant legal issue in computer forensics?
Option A:	a) Preserving Evidence
Option B:	b) Seizing Evidence
Option C:	c) Admissibility of Evidence
Option D:	d) Discovery of Evidence
Q6.	Which of following is not general ethical norm for Investigator?
Option A:	a) To contribute to society and human being.
Option B:	b) Uphold any relevant Evidence.

Option C:	c) To be honest and trustworthy.
Option D:	d) To honor confidentially.
Q7.	Which term refers for modifying a computer in a way which was not originally intended to view Information?
Option A:	a) Metadata
Option B:	b) Live analysis
Option C:	c) Hacking
Option D:	d) Bit Copy
Q8.	Phone company records are an example of:
Option A:	a. Hardware as contraband or fruits of crime
Option B:	b. Information as contraband or fruits of crime
Option C:	c. Information as an instrumentality
Option D:	d. Information as evidence
Q9.	The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:
Option A:	a. Chain of custody
Option B:	b. Field notes
Option C:	c. Interim report
Option D:	d. Voir dire
Q10.	The process model whose goal is to completely describe the flow of information in a digital investigation is known as:
Option A:	a. The Physical Model
Option B:	b. The Staircase Model
Option C:	c. The Evidence Flow Model
Option D:	d. The Subphase Model
Q11.	The crime scene preservation process includes all but which of the following:
Option A:	a. Protecting against unauthorized alterations
Option B:	b. Acquiring digital evidence
Option C:	c. Confirming system date and time
Option D:	d. Controlling access to the crime scene
Q12.	In the case where digital investigators dealing with distributed systems need to collect data from remote sites, the following procedure is recommended:
Option A:	a. Notify personnel at the remote sites to leave everything as is, and arrange for travel to the remote locations
Option B:	b. Notify personnel at the remote sites to shut down all systems and send the hard drives to the forensic lab
Option C:	c. Utilize remote forensics tools to acquire data from the remote sites' RAM as well as the hard drives
Option D:	d. USB bracelets
Q13.	Which of the following is not a safety consideration for a first responder?
Option A:	a. Additional personnel to control those present at the crime scene
Option B:	b. Protection against ELF emanations from monitors
Option C:	c. Proper tools for disassembling and reassembling computer cases
Option D:	d. Protective gloves and eyewear

Q14.	Why is the first step to secure the physical crime scene by removing everyone from the immediate area?
Option A:	a. To prevent them from contaminating evidence
Option B:	b. To prevent them from asking questions about the case before they can be interviewed
Option C:	c. To give them time to fill out a personal information survey
Option D:	d. To keep them from blocking the view when photographs are being taken
Q15.	The process of evaluating available evidence objectively, independent of the interpretations of others, to determine its true meaning is referred to as:
Option A:	a. Equivocal forensic analysis
Option B:	b. Investigative reconstruction
Option C:	c. Threshold assessment
Option D:	d. Behavioral imprints
Q16.	The type of report that is a preliminary summary of findings is known as:
Option A:	a. SITREP
Option B:	b. Threshold Assessment report
Option C:	c. Full investigative report
Option D:	d. Field notes
Q17.	In crimes against individuals the period leading up to the crime often contains the most important clues regarding the relationship between the offender and the victim.
Option A:	a. 24-hour
Option B:	b. 48- hour
Option C:	c. 60-minute
Option D:	d. 15-minute
Q18.	Modus operandi (MO) is a Latin term that means:
Option A:	a. Seize the data
Option B:	b. Ways and means
Option C:	c. Operator error
Option D:	d. A method of operating
Q19.	One reason not to put too much trust into those who run the company's computers is that:
Option A:	a. There has always been an antagonism between system administrators and law enforcement.
Option B:	b. They are typically too busy to take the time to answer your questions.
Option C:	c. They are usually not authorized to answer questions.
Option D:	d. They may be the offenders.
Q20.	It is unwise to rely only on a recovered IP address because:
Option A:	a. An IP address may change many times during a session.
Option B:	b. Offenders can change their IP address.
Option C:	c. By changing the system time, the contents of log files containing IP addresses can be falsified.
Option D:	d. IP addresses only exist in system memory.

Q21.	It is important to gather as many sources of supporting evidence as possible because:
Option A:	a. The more evidence, the stronger the case.
Option B:	b. No amount of supporting evidence can prove conclusively that an individual was in a specific place at a specific time.
Option C:	c. The volume of evidence produced dictates the strength of the alibi.
Option D:	d. Creating an alibi on a network could take months of work.
Q22.	Victimology can help determine:
Option A:	a. Why the victim was selected
Option B:	b. What victim behavior caused the offense
Option C:	c. To what extent the victim was at fault
Option D:	d. The offender’s modus operandi
Q23.	An offender’s choice of location, tools, and actions taken are referred to as:
Option A:	a. MO
Option B:	b. Motivation
Option C:	c. Crime scene characteristics
Option D:	d. Signature behaviors
Q24.	The most common approach to salvaging deleted data on Macintosh systems is to:
Option A:	a. Use EnCase to recover the files.
Option B:	b. Use the Catalog utility.
Option C:	c. Use file carving techniques.
Option D:	d. There is currently no solution to recovering deleted files from a Macintosh.
Q25.	The fact that with modern technology, a photocopy of a document has become acceptable in place of the original is known as:
Option A:	a. Best evidence rule
Option B:	b. Due diligence
Option C:	c. Quid pro quo
Option D:	d. Voir dire