Program: BE Information Technology Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VI

Course Code: ITDLO6023 and Course Name: Digital Forensics

==

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

Q1.	Digital forensics is all of them except:
Option A:	a) Extraction of computer data.
Option B:	b) Preservation of computer data.
Option C:	c) Manipulation of computer data
Option D:	d) Interpretation of computer data
Q2.	What is the most significant legal issue in computer forensics?
Option A:	a) Preserving Evidence
Option B:	b) Seizing Evidence
Option C:	c) Discovery of Evidence
Option D:	d) Admissibility of Evidence
Q3.	In _____ phase investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location
Option A:	a) Preservation phase
Option B:	b) Survey phase
Option C:	c) Documentation phase
Option D:	d) Reconstruction phase
Q4.	What are the three general categories of computer systems that can contain digital evidence?
Option A:	a) Desktop, laptop, server
Option B:	b) Personal computer, Internet, mobile telephone
Option C:	c) Hardware, software, networks
Option D:	d) Open computer systems, communication systems, embedded systems
Q5.	In terms of digital evidence, the Internet 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
Q6.	There are three c's in computer forensics. Which is one of the three?
Option A:	a) Control
Option B:	b) Chance
Option C:	c) Chains
Option D:	d) Core
Q7.	Which of following is a not unethical norm for Digital Forensics Investigation?
Option A:	a) Uphold any relevant evidence.

Option B:	b) Declare any confidential matters or knowledge.
Option C:	c) Distort or falsify education, training, credentials.
Option D:	d) To respect the privacy of others.
Q8.	The ability to recover and read deleted or damaged files from a criminal's computer is an example of a law enforcement specialty called?
Option A:	a) Robotics
Option B:	b) Simulation
Option C:	c) Computer Forensics
Option D:	d) Animation
Q9.	The first step in applying the scientific method to a digital investigation is to:
Option A:	a. Form a theory on what may have occurred
Option B:	b. Experiment or test the available evidence to confirm or refute your prediction
Option C:	c. Make one or more observations based on events that occurred
Option D:	d. Form a conclusion based on the results of your findings
Q10.	The Coroner's Toolkit and The Sleuth Kit are examples of open source
Option A:	a. Hard drive repair tools
Option B:	b. System administrator tools
Option C:	c. Forensic examination tools
Option D:	d. Network management tools