2 /42

0806E490

Candidate's Seat No :_____

M.Sc Sem.-2 Examination

P - 408

Cyber Security & Forensics

June 2022

Time : 2-00 Hours] **[Max. Marks : 50**

Question-1 Answer the following questions(Any Six, each carry 7 Marks)		**[42 Marks]**
A	What is continuity of evidence?	
B	What are the four stages of the computer forensic process?	
C	What are the different phases of the investigation process? Explain with the help of a diagram.	
D	Explain the data acquisition process in detail.	
E	What is digital evidence? What is its role in the investigation process? Give examples of some common digital evidence.	
F	What is the chain of evidence and chain of custody? Explain.	
G	What is volatile data? What is the order of volatility of digital evidence? Explain.	
H	What is the evidence custody form? What information does it contain? Explain in detail.	
I	How is registry information important in windows forensics?	
J	Explain in detail – The corporate Espionage case.	
K	What is a file system? Why it is used?	
L	Explain in detail Cyber Pornography Case.	
M	State and explain various network components and their forensic importance.	
N	What are IDS and IDPS?	
O	Describe the major types of web attacks in brief.	
P	List and describe at least 4 email attacks.	
Question-2 Answer the following questions: (Any Eight, Each carry 1 mark)		**[08Marks]**
a	Enlist any two types of tools used in Forensic Investigation.	
b	IDS stands for	
c	Logs can originate from only one source in a computer. (State true or false)	
d	Cybercrime is any crime that involves a computer and a network. (State true or false)	
e	List the types of Malwares.	
f	Maintain digital copies of evidence, printouts of evidence, and the chain of custody for all evidence, in case of legal action. .(State true or false)	
g	What do you mean by MBR?	
h	BIOS stands for.	
i	An HDD records data by magnetizing a thin film of _____ material on a disk. (a) Magnetic (b) Ferromagnetic (c) Iron (d) Cylinder	
j	Physical level formatting is also known as high-level formatting. (True or False)	
k	The Microsoft Windows versions that are currently in use are _____ and _____.	
l	Tools like reg and regedit helps in to get _____ via important keys.	
m	Major forensics areas in windows are _____ and _____ information	

P.T.O.

IE490-2

n	_____is a utility for DOS and Microsoft Windows that adds command history.	
o	A Group of sectors forms a cluster. (state true or false)	
p	When a file is deleted, the file system removes the file logically i.e. it removes all the meta-data and stamps related to the file. (state true or false)	
q	System time, logged users, open files, network information and drives that are mapped to shared folders are examples of non-volatile information in windows. (state true or false)	
r	Modem, hub, bridge or switches are _____ in a data communication.	
s	Enlist OSI Model layers.	
t	_____ is the creation of email messages with a forged sender address.	
u	List any 3 components of the E-mail header.	
v	A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. (state true or false)	

— X —