University of Mumbai

Examination June 2021

Examinations Commencing from 1st June 2021

Program:Information Technology
Curriculum Scheme: Rev2016
Examination: TE Semester VI
Course Code: ITDLO6023 and Course Name: Digital Forensics

Time: 2 hour   Max. Marks: 80

==

==

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	Which among the following is not a valid Forensic Container Format?
Option A:	EWF/E01
Option B:	AFF
Option C:	AFD
Option D:	AFN
2.	Which among the following is not a Mail Forensic Tool.
Option A:	AbusePipe
Option B:	Aid4Mail Forensic
Option C:	EmailTracer
Option D:	WEFA
3.	Which Forensic Tool is used for Full Content Network Monitoring?
Option A:	TCPDUMP
Option B:	WINDUMP
Option C:	IDS
Option D:	Firewall
4.	Which type of IDS basically acts as or works like a Sniffer who observes all the traffic in the Network?
Option A:	Host Based IDS
Option B:	Network Based IDS
Option C:	Knowledge Based IDS
Option D:	Behavior Based IDS
5.	Can you help decide on the RAID level to use – we are a media house and we use lot of graphics/video applications – we need large throughputs for videos to get played without any jitter and since we are in publishing business we can't afford downtimes.Even if there is any downtime we would like our data to be quickly reconstructed and enable us to continue with out work in less time
Option A:	Raid 5
Option B:	Raid 10
Option C:	Raid 6
Option D:	Raid 01

6.	Which method uses stochastic properties of the computer system to investigate activities lacking digital artifacts?
Option A:	Steganography
Option B:	Stochastic forensics
Option C:	Both A and B
Option D:	None of the above
7.	You are suppose to maintain three types of records. Which answer is not a record?
Option A:	Chain of custody
Option B:	Documentation of the crime scene
Option C:	Searching the crime scene
Option D:	Document your actions
8.	Volatile data resides in ?
Option A:	Registries
Option B:	Ram
Option C:	Cache
Option D:	All of the above
9.	Which of the following deals with network intrusion detection and real-time traffic analysis?
Option A:	John the Ripper
Option B:	L0phtCrack
Option C:	Snort
Option D:	Nessus
10.	Wireshark is a ______________ tool.
Option A:	network protocol analysis
Option B:	network connection security
Option C:	connection analysis
Option D:	defending malicious packet-filtering
11.	The first part of a complete URL is the ___________ needed to access the web resource.
Option A:	Location
Option B:	Address
Option C:	Name
Option D:	Protocol
12.	Unsolicited commercial emails are known as __________
Option A:	Junk
Option B:	Hoaxes
Option C:	Hypertext
Option D:	Spam
13.	In Linux “Dotfiles” are
Option A:	Hidden Files
Option B:	Driver Files
Option C:	System Files
Option D:	Library Files

14.	Cryptography is used to transform message to make them secured and immune from ______.
Option A:	Idle
Option B:	Attack
Option C:	Congestion
Option D:	Defend
15.	Which of the following Protocols use both TCP & UDP?
Option A:	FTP
Option B:	Telnet
Option C:	DNS
Option D:	HTTP
16.	Deleted files is a common technique used in computer forensics is the recovery of deleted files.
Option A:	TRUE
Option B:	FALSE
Option C:	Can be True or False
Option D:	Cannot Say
17.	Which of the following techniques are used during computer forensics investigations?
Option A:	Cross-Drive Analysis
Option B:	Live Analysis
Option C:	Deleted Files Recovery
Option D:	All of the above
18.	And IDS can be used to monitor and filter network traffic. From the viewpoint of detection, which main IDS types can be distinguished?
Option A:	Anamoly based and Heuristic based
Option B:	Signature based and knowledge based
Option C:	Behavior based and knowledge based
Option D:	Anamoly based and Behavior based
19.	For what purpose “Volatility” Tool is used?
Option A:	To extract data from RAM Dumps
Option B:	To capture RAM Dumps
Option C:	To capture Volatile Data
Option D:	To extract data from Non Volatile Data.
20.	is a password recovery and auditing tool.
Option A:	LC3
Option B:	LC4
Option C:	Network Stumbler
Option D:	Maltego

Q2	
A	**Solve any Two** **5 marks each**

i.	*Explain Difference between Ethical Hacking and Unethical Hacking.*
ii.	*Explain Steps of Ethical Hacking in detail.*
iii.	*Explain types of Computer Forensics.*
B	**Solve any One** **10 Marks each**
i.	*Explain types of Evidences and write Rules of Evidence.*
ii.	*Explain how Evidence handling is done in Digital Forensics.*

Q3	
A	**Solve any Two** **5 marks each**
i.	*Explain how Routers can be used as Response Tools.*
ii.	*Explain Intrusion Detection System and types of IDS's*
iii.	*Explain the phases after detection of an Incident.*
B	**Solve any One** **10 Marks each**
i.	*Explain all the steps of Investigating Windows System.*
ii.	*Explain various guidelines of Writing a Report.*