Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, July 2020

Course: Digital Forensics I	**Semester:** IV
Program: B.Tech - CSF	**Time:**02 hrs.
Course Code:CSSF3003	**Max. Marks:** 100

1. Multiple Choice: There are___searching options for ...

Question	There are _____searching options for keywords which FTK offers.
Answer	✓ 2 4 3 5

□

2. Multiple Choice:_____Search can locate items such as ...

Points: **1**

Question	_____Search can locate items such as text hidden in unallocated space that might not turn up in an indexed search.
Answer	Online Active ✓ Live Inline

□

3. Multiple Choice: FTK and other computer forensics prog...

Points: **0.5**

Question	FTK and other computer forensics programs use what option to tag and document digital evidence.
Answer	tracers

✓ bookmarks

hyperlinks

indents

□ 4. Multiple Choice: What is the default port number for A...

Points: **1**

Question	What is the default port number for Apache and most web servers?
Answer	20 27 ✓ 80 87

□ 5. Multiple Choice: Which is a popular tool used for disc...

Points: **0.5**

Question	Which is a popular tool used for discovering networks as well as in security auditing.
Answer	Ettercap Metasploit ✓ Nmap Burp Suit

□ 6. Multiple Choice: Which of the following deals with net...

Points: **1**

Question	Which of the following deals with network intrusion detection and real-time traffic analysis?
Answer	John the Ripper L0phtCrack ✓ Snort

Nessus

□ 7. Multiple Choice: Marking bad clusters data-hiding tech...

Points: **0.5**

Question Marking bad clusters data-hiding technique is more common with _____file systems.

Answer

NTFS

HFS

✓ FAT

Ext2fs

□ 8. Multiple Choice:__________is a password recovery and a...

Points: **1**

Question _________is a password recovery and auditing tool.

Answer

LC3

✓ LC4

Network Stumbler

Maltego

□ 9. Multiple Choice: "Make sure you always label any hardw...

Points: **1**

Question "Make sure you always label any hardware with the following, except;"

Answer

✓ Part number

case number

short discription of the hardware

your signature

Points: 0.5

□ 10. Multiple Choice: Packet sniffers examine which layers ...

Question	Packet sniffers examine which layers of the OSI model
Answer	Layers 2 and 4 Layers 4 through 7 ✓ Layers 2 and 3 all layers

Points: 1

□ 11. Multiple Choice: which of the following is not a type ...

Question	which of the following is not a type of volatile device?
Answer	Routing tables Main memory Log files ✓ Cached data

Points: 1

□ 12. Multiple Choice: Recovering pieces of a file is called...

Question	Recovering pieces of a file is called as.

Answer	✓ carving saving slacking rebuilding

□ 13. Multiple Choice: You are suppose to maintain three typ...

Points: 0.5

Question	You are suppose to maintain three types of records. Which answer is not a record?
Answer	Chain of custody Documentation of the crime scene ✓ Searching the crime scene Document your actions

□ 14. Multiple Choice: What happens when first securing the ...

Points: 1

Question	What happens when first securing the area?
Answer	Start looking for evidence ✓ Make sure that crime scene is safe Gather evidence make sure computer is ON

□ 15. Multiple Choice: The simplest way to access a file hea...

Points: 0.5

Question	The simplest way to access a file header is to use a(n)_____editor
Answer	✓ hexadecimal disk image text

□ Points: **1**

16. Multiple Choice:_________________is the central conce...

Question	_________________is the central concept in cyber forensics/digital forensics investigation
Answer	✓ Chain of custody Testifying Analysis Attribution

Points: **1**

□ 17. Multiple Choice: Which activity is not a part of analy...

Question	Which activity is not a part of analysis phase in forensics life cycle?
Answer	Determine significance Reconstruct fragments of data Recover Data ✓ Draw Conclusion

□ Points: **0.5**

18. Multiple Choice: Which is not a context involved in id...

Question	Which is not a context involved in identifying a piece of digital evidence
Answer	Physical Logical ✓ Electrical Legal

□ 19. Multiple Choice:_____hide the most valuable data at t...

Points: 1

Question	_____hide the most valuable data at the innermost part of the network.
Answer	✓ Layered network defense strategies Protocols Firewalls NAT

□ 20. Multiple Choice: The majority of digital cameras use t...

Points: 1

Question	The majority of digital cameras use the_____ format to store digital pictures.
Answer	✓ EXIF PNG TIFF GIF

Points: 0.5

□

21. Multiple Choice: ou begin any computer forensics case ...

Question	ou begin any computer forensics case by creating
Answer	✓ investigation plan
	evidence custody form
	risk assessment report
	investigation report

□ 22. Multiple Choice: "To find deleted files during a foren...

Points: 1

Question	"To find deleted files during a forensic investigation on a Linux computer, you search for inodes that contain some data and have a link count of"
Answer	-1
	1
	✓ 0
	2

□ 23. Multiple Choice: Which field type refers to the volume...

Points: 1

Question	Which field type refers to the volume descriptor as a partition descriptor?
Answer	✓ Number 3
	Number 2
	Number 0
	Number 4

Points: 0.5

□

24. Multiple Choice: What must an investigator do in order...

Question	What must an investigator do in order to offer a good report to a court of law and ease the prosecution?
Answer	obfuscate the evidence Prosecute the evidence ✓ preserve the evidence authorize the evidence

□ 25. Multiple Choice: monitor network traffic and alerts on...

Points: 1

Question	monitor network traffic and alerts on suspicious activities
Answer	TCP Firewalls Switches ✓ NIDS/NIPS

□ 26. Multiple Choice: Stores web surfing log for an entire ...

Points: 1

Question	Stores web surfing log for an entire organization
Answer	Routers DHCP Servers ✓ Web proxies Firewalls

Points: 0.5

□ 27. Multiple Choice: Recovering and analyzing digital evid...

Question	Recovering and analyzing digital evidence from network resources
Answer	TCP port scan Protocol analysis Web proxies ✓ Network Forensics

Points: 1

□ 28. Multiple Choice: "Libraries: libpcap and WinPcap, Tool...

Question	"Libraries: libpcap and WinPcap, Tools: Wireshark, snort, nmap, ngrep, tcpdump"
Answer	Application servers ✓ Traffic acquisition software Active Acquisition Authentication Servers

Points: 1

□ 29. Multiple Choice: "Understand how a protocol works, how...

Question	"Understand how a protocol works, how to identify and dissect it; can use RFCs and standards to understands protocols"
Answer	✓ Protocol analysis Flow analysis Network Forensics Protocol identification

□ 30. Multiple Choice: Which of the following are the two ty...

Points: **0.5**

Question Which of the following are the two types of write protection?

Answer

Fast and slow

Windows and Linux

✓ Hardware and software

Forensic and non-forensic

□ 31. Multiple Choice: Validate your tools and verify your e...

Points: **1**

Question Validate your tools and verify your evidence with _____to ensure its integrity.

Answer

✓ hashing algorithms

steganography

watermarks

digital certificates

□ 32. Multiple Choice: "Regarding a trial, the term_____mea...

Points: **0.5**

Question "Regarding a trial, the term______means rejecting potential jurors."

Answer

voir dire

rebuttal

✓ strikes

venirema

□ 33. Multiple Choice: "To retrieve an Outlook Express e-mai...

Points: 1

Question	"To retrieve an Outlook Express e-mail header right-click the message, and then click_____to open a dialog box showing general information about the message."
Answer	✓ Properties Options Details Message Source

□ 34. Multiple Choice: EX01

Points: 0.5

Question	EX01
Answer	✓ EnCase Output Formats Different FTK Output Formats EEPROM Network Forensics

□ 35. Multiple Choice: gives us a road map to data on a disk...

Points: 1

Question	gives us a road map to data on a disk type of file system an OS used determines how data is stored on the disk
Answer	✓ file system Drive Slack EEPROM

SIM Cards

Points: **1**

□ 36. Multiple Choice:_____can help you determine whether a...

Question	_____can help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program.
Answer	Broadcast forensics ✓ Network forensics Computer forensics Traffic forensics

Points: **0.5**

□ 37. Multiple Choice:_____can be used to create a bootable...

Question	_____can be used to create a bootable forensic CD and perform a live acquisition.
Answer	✓ Helix Inquisitor DTDD Neon

Points: **1**

□ 38. Multiple Choice: A common way of examining network tra...

Question	A common way of examining network traffic is by running the______program.
Answer	Netdump lackdump

	Coredump
	✓ Tcpdump

□ 39. Multiple Choice: Recovering pieces of a file is called...

Points: 1

Question	Recovering pieces of a file is called as.
Answer	✓ carving
	saving
	slacking
	rebuilding

□ 40. Multiple Choice: Which tool is needed for a computer f...

Points: 1

Question	Which tool is needed for a computer forensics job?
Answer	Tooth brush
	✓ Latex Gloves
	Backup computer
	Sunlight

□ 41. Multiple Choice: What happens when first securing the ...

Points: 0.5

Question	What happens when first securing the area?
Answer	Start looking for evidence
	✓ Make sure that crime scene is safe

Gather evidence

make sure computer is ON

□ 42. Multiple Choice: manages investigations and conducts f...

Points: 1

Question	manages investigations and conducts forensics analysis of systems suspected of containing evidence
Answer	Digital Forensics What are public-sector investigations ✓ describe digital investigations describe private-sector investigations

□ 43. Multiple Choice: "e-mail harassment, falsification of ...

Points: 0.5

Question	"e-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage"
Answer	What is an evidence custody form ✓ What kinds of crimes are private sector crimes? What are write blocker devices? What is a bit-stream copy?

□ 44. Multiple Choice: A method that uses two independent pi...

Points: 1

Question	A method that uses two independent pieces/processes of information to identify a user is known as

Answer		Authentication through encryption
		Password-method authentication
		Two-method authentication
	✓	Two-factor authentication

□ 45. Multiple Choice: Which of the following is the first w...

Points: 1

Question	Which of the following is the first web browser?	
Answer	✓	Nexus
		Netscape Navigator
		Internet Explorer
		Mosaic

□ 46. Multiple Choice: "E-mail messages are distributed from...

Points: 0.5

Question	"E-mail messages are distributed from one central server to many connected client computers, a configuration called_____."	
Answer	✓	client/server architecture
		central distribution architecture
		client architecture
		peer-to-peer architecture

□ 47. Multiple Choice: "In cyber ceime, what is the target o...

Points: 1

Question	"In cyber ceime, what is the target of attacker "

Answer

Hardware

Tools

Machines

✓ Data

□ 48. Multiple Choice: IT Act -2000 discusses--

Points: 1

Question IT Act -2000 discusses--

Answer

Various laws

✓ civil offence of data theft and the process of adjudication

punishment

civil and cyber crimes

□ 49. Multiple Choice: Sec 75 of IT Act deals with

Points: 0.5

Question Sec 75 of IT Act deals with

Answer

"common computer parlance like access , computer resource , computer system "

"coverage cell phones, personal digital assistance or such other devices"

authentication of electronic record

✓ Law for an offence or contravention committed outside of India

□ 50. Multiple Choice: Digital Signature is included in whic...

Points: 1

Question Digital Signature is included in which IT act

Answer

✓ ITA2008

ITA 2000

ITAA 2004

ITAA1984

□ 51. Multiple Choice: The essence of this Section 43 deals in

Points: 1

Question	The essence of this Section 43 deals in
Answer	✓ civil liability Criminality third party data analysis punishment

□ 52. Multiple Choice: Chapter IX of IT act is titled as

Points: 0.5

Question	Chapter IX of IT act is titled as
Answer	Offences Punishment ✓ Code of conduct cyber procedures

□ 53. Multiple Choice: Why RAID was developed?

Points: 1

Question	Why RAID was developed?
Answer	to store the data to estimate the losses in the data ✓ to minimize data loss caused by a disk failure to compute the reasons of disk failures

□ 54. Multiple Choice: Remote acquisition tools vary in

Points: 1

Question	Remote acquisition tools vary in
Answer	Capabilities and speed ✓ configurations and capabilities Features and storage types and networks things

□ 55. Multiple Choice: Why validation of data is important?

Points: 2

Question	Why validation of data is important?
Answer	Ensure authenicity ✓ ensures the integrity Ensure positivity ensure repudiation

□ 56. Multiple Choice: which tool is used to acquire RAID di...

Points: 1

Question	which tool is used to acquire RAID disks at the physical level

Answer	X-Ways Forensics R-Tools Technologies EnCase ✓ Technologies Pathways ProDiscover

Points: 1

□ 57. Multiple Choice: "hexadecimal editors offer many featu...

Question	"hexadecimal editors offer many features not available in computer forensics tools, such as"
Answer	✓ hashing specific files or sectors sector discovery hashing and encryption fragmentation and hash tables

Points: 1

□ 58. Multiple Choice: ProDiscover s .eve files contain meta...

Question	ProDiscover s .eve files contain metadata that includes
Answer	data tables misc values encyption key values ✓ hash value

Points: 1

□ 59. Multiple Choice: What is the most significant legal is...

Question	What is the most significant legal issue in computer forensics?
Answer	Preserving Evidence Seizing Evidence ✓ Admissibility of Evidence Discovery of Evidence