Seat No.: ________ Enrolment No. 2010

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. DFIS

Semester – I – January - 2024

Subject Code: CTMSDFIS S1 P1 **Date: 11.01.24**

Subject Name: Computer Forensics

Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. Write down each question on a separate page.
2. Attempt all questions.
3. Make suitable assumptions wherever necessary.
4. Figures to the right indicate full marks.

			Marks
Q.1		**Attempt any three.**	
	(a)	With a neat diagram explain the different components of the CPU.	08
	(b)	Explain the process control block and what type of information it maintains.	08
	(c)	Explain the Volume Boot Record and GPT, and what type of data it holds.	08
	(d)	i. Convert the decimal number 450 into the hexadecimal representation. ii. Convert the decimal number 456 into binary representation.	08
Q.2		**Attempt any three.**	
	(a)	Explain with examples Little Endian and Big Endian.	08
	(b)	Explain Basic and Dynamic disks and what type of operations can be performed on them.	08
	(c)	Write a short note on Lockard's principle from the digital forensic perspective with an example.	08
	(d)	Explain Master Boot Record with a neat diagram	08
Q.3		**Attempt any three.**	
	(a)	Explain different branches of digital forensics.	08
	(b)	How do you preserve the data on a live system? Write the steps.	08
	(c)	Write down the guidelines for digital evidence collection and archiving	08
	(d)	Explain MAC OS extended file system and compare it with HFS.	08
Q.4		**Attempt any two.**	
	(a)	With a neat diagram briefly explain Windows 10 architecture.	07
	(b)	With a neat diagram explain NTFS file system and compare it with FAT.	07
	(c)	List out five registry data types and its values.	07

Q.5		**Attempt any two.**	
	(a)	Explain data carving and its types in detail	07
	(b)	Write a note on syslog. What type of information do you get from it?	07
	(c)	What are the Registry Hives in Windows OS explain in detail?	07

--- End of Paper---

Seat No.: ________ Enrolment No.___________

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics an Information Security - Semester - I - Jan-2024

Subject Code: CTMSDFIS SI P2 **Date: 12/01/2024**
Subject Name: Cyber Security Audit and Compliance
Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

Marks

Q.1 **Attempt any three.**

(a) What are the auditing standards of ISO/IEC 27001/2? **08**

(b) Define terms with Example or Scenario **08**
I)Policies, ii)Framework, iii)Rules, iv)Laws.

(c) Differentiate between **08**
I.
Audit and Assessment.
II.
Difference Between Compliance Audit and Financial

(d) Explain Business Continuity Planning and life Cycle of BCP. **08**

Q.2 **Attempt any three.**

(a) Discuss IT audit Approaches for Change Management. **08**

(b) What systems does an audit cover? Explain steps involved in a security audit. **08**

(c) Discuss one Case study based on the importance of the audit. **08**

(d) What is risk analysis and risk response? Give example. **08**

Q.3 **Attempt any three.**

(a) IT audit Approaches for Vendor and Third-Party Management. **08**

(b) What Are Controls and Why Are They Important? **08**

(c) Explain Disaster Recovery & planning of DR. **08**

(d) Discuss System/Application in IT Domain. **08**

Q.4 **Attempt any two.**

(a) Expand and elaborate the following terms **07**
I. HIPAA, **II.** GDPR and **III.** PCIDSS.

(b) Explain threat analysis in assessing IT security. **07**

(c) Discuss Risk Assessment and Mitigation. **07**

Q.5

Attempt any two.

(a) Explain Remote Access in IT Domains for audit. 07

(b) Draw Structure of the standard of ISO 270001. 07

(c) Write short note on Gramm-Leach-Bliley Act. 07

--- End of Paper---

Seat No.: ________ Enrolment No.________

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics and Information Security
Semester – I – January - 2024

Subject Code: CTMSDFIS SI P3 **Date: 16-01-2024**
Subject Name: Incident Response Management
Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

Marks

Q.1 **Attempt any three.**

(a) Illustrate the need and goals of an incident response. 08

(b) What is malware and its various types? Explain about botnet identification. 08

(c) There is an incident occurred in a windows-based computer system. What investigation you will do? What different windows-based artefacts should be analyzed and why? 08

(d) Discuss about Log with their formats and types in detail. 08

Q.2 **Attempt any three.**

(a) One Albania, the second-largest mobile operator in Albania with 1.36 million subscribers, confirmed in a Facebook post that it dealt with a cybersecurity incident on Christmas day. 08
The hackers in a Telegram post claimed to have stolen data from the organizations. "The amount of data collected is enormous. Expect the worst to happen," the hackers warned. Apparently, the hacker group has a publicly accessible website where similar messaging is published. Explain the possible cyberattack(s) and methodology used by the criminal.

(b) State the developin skills of Incident Response Team members. 08

(c) Discuss Base Scoring of CVSS. 08

(d) Write a detailed note on Incident Handling Process. 08

Q.3 **Attempt any three.**

(a) What are various costs of an incident? Explain them in detail. 08

(b) Write a detailed note on report writing. 08

(c) During Ukraine Blackout (2016) cyber incident following details were observed technically by E-ISAC and SANS ICS team: 08

- Spear phishing to gain access to the business networks of the oblenergos
- Identification of BlackEnergy 3 at each of the impacted oblenergos
- Theft of credentials from the business networks
- The use of virtual private networks (VPNs) to enter the ICS network
- The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
- Serial-to-ethernet communications devices impacted at a firmware level
- The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs
- Utilizing UPS systems to impact connected load with a scheduled service outage
- Telephone denial-of-service attack on the call center

Explain the loss of C-I-A & A-A-A triad & type(s) of information warfare with justified reasons.

(b) Discuss any realworld cyber incident case study with all facts and technical findings. **08**

Q.4 **Attempt any two.**

(a) Discuss various signs of an incidents with 5 examples each. **07**

(b) What do you mean by network monitoring? How to analyze network data? **07**

(c) How can you collect live data for the investigation and what kind of measures should be considered? **07**

Q.5 **Attempt any two.**

(a) How can you collect live Microsoft events? What can you do afterwards for generating an incident alert? Discuss the process technically. **07**

(b) Explain Incident Response Team with it's various structure and dependencies. **07**

(c) Explain basics of windows registry. **07**

--- End of Paper---

Seat No.: ________

Enrolment No. 2010

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics and Information Security
Semester – I – January - 2024

Subject Code: CTMSDFIS S1 P4
Subject Name: Python & Scripting
Time: 11:00 AM to 2:00 PM

Date: 17/01/2024

Total Marks: 100

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three.**	
	(a)	What do you mean by permissions? Also briefly explain the different command used for permissions.	**08**
	(b)	Write short note on file system tree and its navigation in Linux.	**08**
	(c)	Explain the following commands Linux with examples: (i) ls, (ii) cat, (iii) ln, (iv) wc	**08**
	(d)	What do you mean by links in Linux? Briefly explain its types and related commands.	**08**
Q.2		**Attempt any three.**	
	(a)	Explain if elif and case statements with suitable examples.	**08**
	(b)	Explain the following Linux commands with examples: (i) read, (ii) grep, (iii) bg, (iv) yum	**08**
	(c)	Explain following networking commands – (i) ping, (ii) netstat, (iii) wget, (iv) traceroute, (v) ifconfig, (vi) ftp, (vii) ssh, (viii) route	**08**
	(d)	Explain different types of i/o redirects and expansion in bash shell with proper syntax and suitable examples.	**08**
Q.3		**Attempt any three.**	
	(a)	Write a python program for sorting a one-dimensional arrays.	**08**
	(b)	What is list data type in Python? How it is differ from tuple data type? Demonstrate the use of any five methods of the list.	**08**
	(c)	What do you mean by regular expressions? Explain the special sequence characters and quantifiers used in regular expressions.	**08**
	(d)	Explain following control statements with examples in Python: break, continue, pass, return	**08**
Q.4		**Attempt any two.**	
	(a)	Explain OS module of python with suitable examples.	**07**

	(b)	Explain sys module of python with suitable examples.	07
	(c)	Explain socket programming in python	07
Q.5		**Attempt any two.**	
	(a)	List out different variables in Powershell and explain any two in detail with example.	07
	(b)	Explain various looping statements in Powershell with examples.	07
	(c)	Explain comparison and logical operators in Powershell.	07

--- End of Paper---

Seat No.: ________ Enrolment No. 2010

NATIONAL FORENSIC SCIENCES UNIVERSITY

MSc Digital Forensics and Information Security

Semester – I – January - 2024

Subject Code: CTMSDFIS S1 P5 **Date: 10.01.2024**

Subject Name: INTRODUCTION TO FORENSIC SCIENCE AND CYBER LAWS

Time: 2:00 PM to 5:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

S. No. **Marks**

Q.1 **Attempt any three.**

(a) Describe about various computer storage devices and list out the volatile vs non-volatile memory difference. **08**

(b) What is Interpol/FBI, explain its role in international criminal investigations. **08**

(c) Explain the scope of any four type of analysis undertaken in Forensic Biology division. **08**

(d) What is IPC, explain the sections 299, 300, 375 & 377. **08**

Q.2 **Attempt any three.**

(a) Discuss Sec-66 of IT Act, 2000 with appropriate case-study. **08**

(b) Write a note on establishment of Fingerprint Bureau. **08**

(c) Explain about the various objectives of punishment. **08**

(d) Explain any four basic principles as followed in forensic science citing relevant illustrations. **08**

Q.3 **Attempt any three.**

(a) Define the following: **08**

i) Criminalistics
ii) Physical evidence
iii) Law
iv) Mobile Laboratory

(b) Explain what are the primary and secondary functions of court of law. 08

(c) Explain the role of any four techniques with their tools used for forensic investigations. 08

(d) Explain the scope of any four type of analysis undertaken in Forensic Biology division. 08

d) what are the diff services Provided by forensic science lab.

Q.4 **Attempt any two.**

(a) Differentiate between Cognizable and Non-cognizable offences. 07

(b) What is a State/Central Forensic Science Laboratory, explain its hierarchical setup with diagrammatic representation. 07

(c) Write a note on significance of forensic science in a society. 07

Q.5 **Attempt any two.**

(a) What is NIA, explain its role as an allied organization to forensic science. 07

(b) Discuss the difference between Civil and Criminal Justice. 07

(c) You are given a digital evidence for analysis, prepare a report of analysis for the same. 07

--- End of Paper---