Department of Cyber Security

R18

Code No: 156EW

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, March - 2024
CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS
(Computer Science and Engineering – Cyber Security)

Time: 3 Hours **Max. Marks: 75**

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	What is cyberterrorism?	[2]
b)	Define cybercrimes.	[3]
c)	What are the issues with software piracy?	[2]
d)	Define cyberstalking.	[3]
e)	What do you mean by data processing in eDiscovery?	[2]
f)	How to recover deleted cyber security pieces of evidence?	[3]
g)	How to do WINDOWS forensics?	[2]
h)	Differentiate cyber forensics and network forensics.	[3]
i)	What are the rules for handling digital evidence?	[2]
j)	What is the criminal procedure code for cybercrime?	[3]

PART – B

(50 Marks)

2.a) Discuss the nature and scope of cyber crimes in detail.
b) What is the importance of cyber security? [5+5]

OR

3. Summarize the different categories of cybercrimes with appropriate examples. [10]

4. Write short notes on the following:
a) White-collar crimes.
b) Viruses and malware code. [5+5]

OR

5. What are the roles and responsibilities of 'Law Enforcement'? Explain. [10]

6. Explain "Email Investigation, Email Tracking, IP tracking, and Email recovery". [10]

OR

7. How the encryption and decryption methods be influenced in cybercrime investigation? Explain. [10]

8. Discuss the following briefly:
   a) Digital Forensic Hardware tools
   b) Audio-video evidence analysis. [5+5]

OR

9. Write short notes on the following:
   a) Forensic ballistics
   b) Network forensics. [5+5]

10. Demonstrate the "Electronic Communication Privacy Act and Legal policies". [10]

OR

11. Explain the following in brief:
   a) Laws and ethics
   b) Digital Evidence controls. [5+5]

---ooOoo---

Code No: 156EW **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, July - 2023
CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS
(Computer Science and Engineering – Cyber Security)

Time: 3 Hours **Max. Marks: 75**

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	What are Botnets?	[2]
b)	Discuss briefly about property cyber-crime.	[3]
c)	Define mail bombs.	[2]
d)	List down the white collar crimes.	[3]
e)	How the emails are tracked?	[2]
f)	With an example, explain password cracking.	[3]
g)	Define digital forensic.	[2]
h)	Discuss about fingerprint recognition.	[3]
i)	What are the legal policies?	[2]
j)	Explain how digital evidences are controlled?	[3]

PART – B

(50 Marks)

2.	Describe in detail about the concept of nature and scope of cyber-crime.	[10]
	OR	
3.	How the Criminals Plan the Attacks? Explain with examples.	[10]
4.	With an example, explain about various methods used in password cracking.	[10]
	OR	
5.	Enumerate the guidelines for seizing digital evidence at the scene.	[10]
6.	List standard systems analysis steps to be applied when preparing for a forensic investigation case.	[10]
	OR	
7.	Explain the various process involved in recovering deleted evidences.	[10]
8.	Illustrate in detail about various computer forensic hardware tools.	[10]
	OR	
9.	What is the standard procedure used for network forensics? Explain.	[10]
10.	Illustrate about the challenges to Indian cyber laws in detail.	[10]
	OR	
11.	Elaborate in detail about the Amendments to the Indian IT ACT.	[10]

---ooOoo---

Code No: 156EW

R18

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, August/September - 2024
CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS
(Computer Science and Engineering – Cyber Security)

Time: 3 Hours **Max. Marks: 75**

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	Discuss briefly about the concept of phishing.	[2]
b)	What are the characteristics that define the nature of cyber-crime?	[3]
c)	What are white collar crimes in the context of cyber-crime?	[2]
d)	What constitutes unauthorized access to computers?	[3]
e)	What are the best practices for collecting digital evidence?	[2]
f)	Why is e-discovery important in cyber-crime investigations?	[3]
g)	What are the essential components of a forensic workstation?	[2]
h)	List the main components of a network forensic data visualize.	[3]
i)	What is the role of laws and ethics in digital investigation?	[2]
j)	Discuss about the IPC Act.	[3]

PART – B

(50 Marks)

2.a)	Explain the key differences between cybercrime and traditional crime.	
b)	Describe common social engineering techniques used by cyber criminals.	[5+5]
	OR	
3.a)	Describe the impact of cybercrime on individuals, businesses, and governments.	
b)	What measures can be taken to prevent and mitigate property cyber-crimes?	[5+5]
4.a)	Explain the steps involved in a typical computer intrusion attack.	
b)	What are the common methods used to distribute viruses and malicious code?	[5+5]
	OR	
5.a)	How can organizations protect against unauthorized access to their systems?	
b)	What steps should be taken immediately after a virus attack is detected?	[5+5]
6.	Explain the process of investigating E-mail crimes and violations.	[10]
	OR	
7.	Illustrate about digital evidence collection and data seizure activities in data recovery process in cybercrime scene.	[10]

8.a) How do forensic investigators ensure data integrity throughout the investigation process?

b) Describe the principles behind iris and fingerprint recognition in forensic identification. [5+5]

OR

9.a) How does photography assist in forensic ballistics and crime scene documentation?

b) Explain the role of video enhancement tools in forensic video analysis. [5+5]

10.a) How do international laws impact cybercrime investigations conducted across borders?

b) Explain the importance of using write blockers and forensic tools in evidence handling. [5+5]

OR

11.a) Explain the role of timestamps and digital signatures in evidence controls.

b) Explain the Criminal Procedure Code (CrPC) and its role in cybercrime investigations. [5+5]

---ooOoo---