Seat No. / Enrolment No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

Diploma Engineering – SEMESTER – 6 (NEW) – EXAMINATION – Winter-2024

Subject Code: 4360705 **Date: 27-11-2024**

Subject Name: Network Forensics

Time: 02:30 PM TO 05:00 PM **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make Suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Use of simple calculators and non-programmable scientific calculators are permitted**
5. **English version is authentic.**

			Marks
Q.1	**(a)**	Write the Full form of UDP, TCP, and DNS.	**03**
પ્રશ્ન. ૧	**(અ)**	UDP, TCP અને DNS નું પૂર્ણ નામ લખો.	**૦૩**
	(b)	Describe the steps for handling evidence in network forensics.	**04**
	(બ)	નેટવર્ક ફોરેન્સિકસમાં પુરાવાને હેન્ડલ કરવાનાં પગલાંઓનું વર્ણન કરો.	**૦૪**
	(c)	Write a difference between OSI and TCP/IP model.	**07**
	(ક)	OSI અને TCP/IP મોડલ વચ્ચેનો તફાવત લખો.	**૦૭**
		OR	
	(c)	Write a short note about LAN, MAN, and WAN.	**07**
	(ક)	LAN, MAN અને WAN વિશે ટૂંકી નોંધ લખો.	**૦૭**
Q.2	**(a)**	Define Network Forensics and its importance.	**03**
પ્રશ્ન. ૨	**(અ)**	નેટવર્ક ફોરેન્સિકસની વ્યાખ્યા લખી તેનું મહત્વ લખો.	**૦૩**
	(b)	Explain Proactive investigations in network forensics.	**04**
	(બ)	નેટવર્ક ફોરેન્સિકસમાં પ્રોએકટીવ ઈન્વેસ્ટીગેશન વિગતવાર સમજાવો.	**૦૪**
	(c)	Explain DNS Spoofing, ARP Poisoning, and Web Jacking network attack.	**07**
	(ક)	DNS સ્પૂફિંગ, ARP પોઈઝનિંગ અને વેબ જેકિંગ નેટવર્ક એટેક વિગતવાર સમજાવો.	**૦૭**
		OR	
Q.2	**(a)**	Write the advantages and disadvantages of Network Forensics.	**03**
પ્રશ્ન. ૨	**(અ)**	નેટવર્ક ફોરેન્સિકસના ફાયદા અને ગેરફાયદા લખો.	**૦૩**
	(b)	Explain Incident Response investigations in network forensics.	**04**
	(બ)	નેટવર્ક ફોરેન્સિકસમાં ઇન્સીડન્ટ રિસ્પોન્સ ઈન્વેસ્ટીગેશન વિગતવાર સમજાવો.	**૦૪**
	(c)	Define social engineering attack. Explain any three social engineering attacks in detail.	**07**
	(ક)	સોશિયલ એન્જીનીયરીંગ એટેકની વ્યાખ્યા લખો. કોઇપણ ત્રણ સોશિયલ એન્જીનીયરીંગ એટેકને વિગતમાં સમજાવો.	**૦૭**
Q.3	**(a)**	Explain how digital devices can be sources of evidence.	**03**
પ્રશ્ન. ૩	**(અ)**	ડિજિટલ ઉપકરણો પુરાવાના સ્ત્રોત કેવી રીતે બની શકે છે તે વિગતવાર સમજાવો.	**૦૩**
	(b)	Write a comparison between flow analysis and packet analysis in network forensics.	**04**
	(બ)	નેટવર્ક ફોરેન્સિકસમાં ફ્લો એનાલીસીસ અને પેકેટ એનાલીસીસ વચ્ચેની સરખામણી લખો.	**૦૪**
	(c)	List out Data Preservation Technique. Explain any two techniques in detail.	**07**

	(ક)	ડેટા પ્રિઝર્વેશન ટેકનીકની યાદી બનાવો અને કોઈપણ બે ટેકનીક વિગતમાં સમજાવો.	**૦૭**

OR

Q.3	**(a)**	Explain the concept of metadata preservation.	**03**
પ્રશ્ન. ૩	**(અ)**	મેટાડેટા પ્રિઝર્વેશન કોન્સેપ્ટ વિગતવાર સમજાવો.	**૦૩**
	(b)	Define Deep Packet Inspection (DPI). Explain its role in network forensics.	**04**
	(બ)	ડીપ પેકેટ ઇન્સ્પેક્શન (DPI) ની વ્યાખ્યા લખો અને નેટવર્ક ફોરેન્સિક્સમાં તેના રોલ વિષે વિગતવાર સમજાવો.	**૦૪**
	(c)	List out Data acquisition methods. Explain any two methods in detail.	**07**
	(ક)	ડેટા એક્વિઝીશન પધ્ધતિઓની યાદી બનાવો. અને કોઈપણ બે પધ્ધતિઓને વિગતવાર સમજાવો.	**૦૭**
Q.4	**(a)**	Write a short note on WPA.	**03**
પ્રશ્ન. ૪	**(અ)**	WPA પર ટૂંકી નોંધ લખો.	**૦૩**
	(b)	Describe key components of wireless network.	**04**
	(બ)	વાયરલેસ નેટવર્કના મુખ્ય કમ્પોનન્ટો નું વર્ણન કરો.	**૦૪**
	(c)	Explain Man-in-the-middle, Phishing and Wireless Eavesdropping attack in wireless network.	**07**
	(ક)	વાયરલેસ નેટવર્કમાં મેન-ઇન-ધ-મિડલ, ફિશિંગ અને વાયરલેસ ઇવેસ્ડ્રોપિંગ એટેક વિગતવાર સમજાવો.	**૦૭**

OR

Q.4	**(a)**	Write a short note on WPA-2.	**03**
પ્રશ્ન. ૪	**(અ)**	WPA-2 પર ટૂંકી નોંધ લખો.	**૦૩**
	(b)	Describe the security challenges in wireless networks.	**04**
	(બ)	વાયરલેસ નેટવર્ક્સમાં સિક્યુરિટીના ચેલેન્જીસ નું વર્ણન કરો.	**૦૪**
	(c)	Explain Evil Twin, Wireless jamming and Brute-Force attack in wireless network.	**07**
	(ક)	વાયરલેસ નેટવર્કમાં એવિલ ટ્વીન, વાયરલેસ જામિંગ અને બ્રુટ-ફોર્સ એટેક વિગતવાર સમજાવો.	**૦૭**
Q.5	**(a)**	Write a short note on WEP.	**03**
પ્રશ્ન. ૫	**(અ)**	WEP પર ટૂંકી નોંધ લખો.	**૦૩**
	(b)	Explain the Role of Artificial intelligence in network forensics.	**04**
	(બ)	નેટવર્ક ફોરેન્સિકમાં આર્ટીફિસિયલ ઇંટેલિજન્સની ભૂમિકા વિગતવાર સમજાવો.	**૦૪**
	(c)	Describe the components and challenges of IoT forensics.	**07**
	(ક)	IoT ફોરેન્સિક્સના કમ્પોનન્ટો અને ચેલેન્જીસ નું વર્ણન કરો.	**૦૭**

OR

Q.5	**(a)**	Explain Rogue access points attack in wireless network.	**03**
પ્રશ્ન. ૫	**(અ)**	વાયરલેસ નેટવર્કમાં Rogue એક્સેસ પોઈન્ટ એટેક વિગતવાર સમજાવો.	**૦૩**
	(b)	Define Data Processor and Personal Data Breach in the context of the DPDP Act, 2023.	**04**
	(બ)	DPDP એક્ટ, 2023ના સંદર્ભમાં ડેટા પ્રોસેસર અને પર્સનલ ડેટા બ્રિચ ની વ્યાખ્યા કરો.	**૦૪**
	(c)	List out Legal challenges in network forensics. Explain any three challenges in detail.	**07**
	(ક)	નેટવર્ક ફોરેન્સિક્સમાં કાનૂની ચેલેન્જીસ ની યાદી બનાવો અને કોઈપણ ત્રણ ચેલેન્જીસ ને વિગતવાર સમજાવો.	**૦૭**

****