GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)

Semester - VI

Course Title: Network Forensics

(Course Code: 4360705)

Diploma Programme in which this course is offered	Semester in which offered
Computer Science & Engineering	6th semester

1. RATIONALE

This course provides a foundational understanding of computer networks, emphasizing protocols, structures, and networking necessity. Exploring various network types and components ensures a comprehensive grasp of critical elements. Transitioning to the OSI model and TCP/IP protocol suite establishes a conceptual framework for network structures. The course introduces Network Forensics, addressing myriad threats and vulnerabilities. Students gain hands-on digital forensics skills through evidence identification, data acquisition, and preservation techniques. Inclusion of wireless network fundamentals and security challenges anticipates evolving technologies, addressing legal and privacy aspects, and future trends like blockchain, AI, and IoT forensics, prepares students for the dynamic field's ethical, legal, and technological dimensions.

2. COMPETENCY

The purpose of this course is to help the student to attain the following industry identified competency through various teaching-learning experiences:

- Demonstrate comprehensive ability in network forensics process and its legal aspects.

3. COURSE OUTCOMES (COs)

The practical exercises, the underpinning knowledge, and the relevant soft skills associated with this competency are to be developed in the student to display the following COs:

a) Identify the significance and principles underlying networking concepts and protocols.

b) Demonstrate the application of network forensics in addressing different types of network attacks and vulnerabilities.

c) Describe the principles and methodologies involved in conducting network forensics analysis.

d) Comprehend wireless basics, authentication types, and attacks on wireless networks.

e) Describe the legal challenges, privacy laws, and future trends in network forensics.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme(In Hours)			Total Credits (L+T/2+P/2)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	CA	ESE	CA	ESE	
3	-	2	4	30	70	25	25	150

(*): Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

***Legends: L**-Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** -Practical; **C** – Credit, **CA** - Continuous Assessment; **ESE** -End Semester Examination.*

5. SUGGESTED PRACTICAL EXERCISES

The following practical outcomes (PrOs) are the subcomponents of the COs. These PrOs need to be attained to achieve the COs.

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
1	Execute Basic TCP/IP utilities and commands. (eg: ping, ipconfig, tracert, arp, tcpdump, whois, host, netstat, nslookup, ftp, telnet etc...)	I	2
2	Design and implement small network using bus, star, mesh and hybrid topology with IP address scheme (eg. packet Tracer)	I	2
3	Simulate the configuration of DHCP (eg. packet Tracer)	I	2
4	Simulate the configuration of DNS (eg. packet Tracer)	I	2
5	Study different types of vulnerabilities of Web Applications and Networks.	II	2
6	Study Wireshark tool for Network Packet Capturing.	III	4
7	Analysis of Internet Protocol using Wireshark.	III	2
8	Analysis of TCP Protocol using Wireshark.	III	2
9	Analysis of DHCP Protocol using Wireshark.	III	2
10	Analysis of DNS Protocol using Wireshark.	III	2
11	Study different authentication techniques in Wireless Networks.	IV	2

12	Study different attacks on Wireless Networks.	IV	2
13	Study application of Artificial Intelligence in Network Forensics.	V	2
	Total		**28**

Note

i. *More* ***Practical Exercises*** *can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.*

ii. The following are some ***sample*** *'Process' and 'Product' related skills (more may be added/deleted depending on the course) that occur in the above listed* ***Practical Exercises*** *of this course required which are embedded in the COs and ultimately the competency..*

S. No.	**Sample Performance Indicators for the PrOs**	**Weightage in %**
1	Regularity	20
2	Problem Analysis	20
3	Development of the Solution	20
4	Testing of the Solution	20
5	Mock viva test	20
Total		**100**

6. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

This major equipment with broad specifications for the PrOs is a guide to procure them by the administrators to usher in uniformity of practical in all institutions across the state.

S. No.	**Equipment Name with Broad Specifications**	**PrO. No.**
1	Hardware: Computer System with latest configuration and laptops	Al l
2	Software: Wireshark, Cisco Packet Tracer, Linux, Windows	

7. AFFECTIVE DOMAIN OUTCOMES

The following ***sample*** Affective Domain Outcomes (ADOs) are embedded in many of the above-mentioned COs and PrOs. More could be added to fulfill the development of this competency.

a) Follow ethical & safety practices.
b) Work as a leader/a team member.
c) Follow standard configuration.
d) Motivation and Attitude towards learning

The ADOs are best developed through the laboratory/field based exercises. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

i. 'Valuing Level' in 1st year
ii. 'Organization Level' in 2nd year.
iii. 'Characterization Level' in 3rd year.

8. UNDERPINNING THEORY

Only the major Underpinning Theory is formulated as higher-level UOs of Revised Bloom's taxonomy in order development of the COs and competency is not missed out by the students and teachers. If required, more such higher-level UOs could be included by the course teacher to focus on the attainment of COs and competency.

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
Unit - I Basics of Networking Concepts andProtocols	1.a Describe basic concept of Internetworking and its components	1.1. Basics of Computer Networks- Definition ofNetwork, Need of Networks, Protocol. 1.2. Types of Networks- LAN, MAN, WAN 1.3. Network Components- Twisted Pair Cable, Coaxial cable, Fiber Optic Cables, Network Interface Card, HUB, Switch, Router 1.4. OSI model and TCP/IP protocol suite 1.5 Introduction Network Protocols- IP, TCP, UDP, DHCP, DNS
Unit - II Introduction to Network Forensics andNetwork Threats	2.a Explain Network Forensics and its importance 2.b Explain Network threats and vulnerabilities 2.c Explain Types of Network Forensics Investigations	2.1 Overview of Network Forensics: Definition, Process of Network Forensics, Importance,Advantages and Disadvantages, Applicationof Network Forensics. 2.2 Network threats and vulnerabilities: Types of network attacks- eavesdropping, spoofing, modification, Cross-site scripting, DNS Spoofing, Routing Table Page Poisoning, ARP Poisoning, Web Jacking. Social Engineering Attacks and its types. 2.3 Types of network forensics investigations: Incident Response and Proactive Investigations

Unit - III Network Forensics Analysis	3.a Describe the process of evidence handling 3.b Explain data acquisition methods 3.c Explain data preservation techniques 3.d Explain Network Traffic Analysi smethods	3.1 Identifying sources of evidence- Digital devices, Network traffic, Cloud environments, Steps for handling evidence. 3.2 Data acquisition methods- Network traffic capture, Log file analysis, Memory acquisition, List Packet capture tools 3.3 Introduction to Data Preservation Technique- Write-blocking, Data encryption, Data hashing, Metadata preservation 3.4 Network Traffic Analysis Methods- Flow analysis, Packet analysis, Deep packet inspection (DPI), Network behavior analysis
Unit - IV	4.a Describe Wireless Networks and security challenges	4.1 Introduction to Wireless Networks: Basics of wireless (IEEE 802.11) communication and security challenges.
Wireless Network Forensics	4.b Explain Attacks on Wireless Networks	4.2 Types of Authentications: WEP, WPA and WPA-2 Encryption. 4.3 Attacks on Wireless networks: Man-in-the-middle (MITM), Brute-Force, Evil Twin, Rogue access points, Phishing, Wireless Jamming (Denial-of-Service Attacks), Wireless Eavesdropping.
Unit - V Legal Aspectsand Future Trends	5.a Explain Legal challenges, Digital Personal Data Protection Act, 2023 5.b Explain the future trends in network forensics	5.1 Legal challenges in network forensics: Authorization, Privacy, Data Preservation, Disclosure, Cross-Border Investigations. 5.2 Digital Personal Data Protection Act,2023: Introduction, Data, Data Fiduciary, Data Principal, Data Processor, Personal Data Breach, Need of DPDP, Key Features of DPDP 5.3 Future Trends: Role of Artificial intelligence in Intrusion Detection, Role of Artificial intelligence in network forensics, Introduction to Internet of Things (IoT) forensics, components and challenges

***Note**: The UOs need to be formulated at the 'Application Level' and above of Revised Bloom's Taxonomy' to accelerate the attainment of the COs and the competency.*

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	**Unit Title**	**Teaching Hours**	**Distribution of Theory Marks**			
			R Level	**U Level**	**A Level**	**Total Marks**

I	**Basics of Networking Concepts andProtocols**	06	04	04	02	10
II	**Introduction to Network Forensics andNetwork Threats**	08	06	06	02	14
III	**Network Forensics Analysis**	10	04	08	08	20
IV	**Wireless Network Forensics**	10	04	08	04	16
V	**Legal Aspects and Future Trends**	08	06	04	00	10
Total		**42**	**24**	**30**	**16**	**70**

Legends: *R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)*
Note*: This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from the above table.*

10. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related ***co-curricular*** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct followingactivities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

a) Undertake micro-projects in teams
b) Give a seminar on any relevant topics.
c) Students are encouraged to register themselves in various MOOCs such as: Swayam, edx, Coursera, Udemy etc to further enhance their learning.
d) Prepare charts to explain use/process of the identified topic.
e) Arrange visits to cybersecurity operations centers or relevant facilities, providing students with exposure to professional network forensic environments.
f) Organize workshops where students can interact with network forensic experts, participate in live demonstrations, and ask questions to deepen their understanding.
g) Form small groups for collaborative projects, such as creating a network forensic analysis report for a specific scenario or designing a network security solution.
h) Use simulation tools to create controlled network security scenarios, challenging students to identify and respond to security incidents.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainmentof the various outcomes in this course:

a) Massive open online courses (***MOOCs***) may be used to teach various topics/subtopics.
b) Guide student(s) in undertaking micro-projects.
c) Diagnosing Essential Missed Learning concepts that will help students.
d) ***'L' in section No. 4*** means different types of teaching methods that are to be employed by teachers to develop the outcomes.
e) About ***20% of the topics/sub-topics*** which are relatively simpler or descriptive

in nature is to be given to the students for ***self-learning***, but to be assessed using different assessment methods.

f) With respect to ***section No.10***, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.

g) Utilize multimedia resources such as videos, interactive simulations, and virtual labs to cater to diverse learning styles and enhance understanding.

h) Implement regular quizzes, assessments, and progress checks to ensure ongoing comprehension and engagement throughout the course.

i) Invite guest speakers who are experts in network forensics to share their experiences, insights, and practical tips with students.

j) Encourage students to analyze and solve problems based on actual incidents.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-project are group-based. However, in the fifth and sixth semesters, it should be preferably be ***individually*** undertaken to build up the skill and confidence in every student to become problem solver so that s/he contributes to the projects of the industry. In special situations where groups have to be formed for micro-projects, the number of students in the group should ***not exceed three.***

The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain a dated work diary consisting of individual contributions in the project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than ***16 (sixteen) student engagement hours*** during the course. The student ought to submit a micro-project by the end of the semester to develop the industry oriented COs.

A suggestive list of micro-projects is given here. This has to match the competency and the COs. Similar micro-projects could be added by the concerned course teacher:

Project 1 : Conducting a security assessment on a LAN/Wi-Fi network.

Project 2 : Evaluation of Network Forensic Tools.

Project 3 : Research and prepare brief presentations on future trends in network forensics (malware analysis, blockchain impact, AI integration, IoT forensics).

Project 4 : Study the Digital Personal Data Protection Act (2023) regulations andconduct a seminar on their impact on network forensics.

Project 5 : Simulate a network attack scenario (e.g., Man-in-the-Middle attack) in a controlled environment.

Project 6 : Research a real-world legal case related to network forensics and Present the case, highlighting the legal and ethical considerations.

Project 7 : Construct a small-scale network, implement different components, and assess their performance under diverse conditions.

13. SUGGESTED LEARNING RESOURCES

S. No.	Title of Book	Autho r	Publication with place, yearand ISBN
1	Learning Network Forensics	Samir Datt	PACKT Publications, Year:2016 ISBN: 9781782174905

2	Digital Forensic: The FascinatingWorld of Digital Evidences	Nilakshi Jain, Dhananjay R.Kalbande	WILEY Publications, ISBN: 9788126565740
3	Network Forensics	Ric Messier	Wiley, ISBN: 9781119328285
4	Network Forensics: Tracking Hackersthrough Cyberspace	Sherri Davidoff, Jonathan Ham	Pearson
5	Hands-On Network Forensics	Nipun Jaswa	PACKT PublicationsISBN 9781789344523

14. SOFTWARE/LEARNING WEBSITES

a. https://www.lucidchart.com/blog/cloud-computing-basics
b. https://www.forcepoint.com/cyber-edu/cloud-security
c. https://forensicscontest.com/
d. https://www.sans.org/in_en/
e. https://nptel.ac.in/
f. https://www.udemy.com/
g. https://www.cybrary.it/

15. PO-COMPETENCY-CO MAPPING

Semester VI	Network Forensics (Course Code: 4360705)						
	POs and PSOs						
Competency & Course Outcomes	**PO 1 Basic & Discipline specific knowledge**	**PO 2 Problem Analysis**	**PO 3 Design/ development of solutions**	**PO 4 Engineering Tools, Experimentation & Testing**	**PO 5 Engineering practices for society, sustainability & environment**	**PO 6 Project Management**	**PO 7 Life-long learning**
Competency Demonstrate comprehensive ability in network forensics process and its legal aspects.							
Course Outcomes CO a) Identify the significance and principles underlying networking concepts and protocols.	3	1	2	2	-	1	2
CO b) Demonstrate the application of network forensics in addressing different types of	3	2	2	-	-	1	2

network attacks and vulnerabilities.							
CO c) Describe the principles and methodologies involved in conducting network forensics analysis.	3	2	2	3	-	3	2
CO d) Comprehend wireless basics, authentication types, and attacks on wireless networks.	3	2	2	2	-	2	2
CO e) Describe the legal challenges, privacy laws, and future trends in network forensics.	3	-	-	-	2	-	2

Legend: ‘**3**’ for high, ‘**2**’ for medium, **‘1’** for low or **‘-’** for the relevant correlation of each competency, CO, with PO/ PSO

16. COURSE CURRICULUM DEVELOPMENT COMMITTEEGTU Resource Persons

Sr. No.	Name and Designation	Institute	Email
1	Smt. Manisha P. MehtaHOD, Computer	Government Polytechnic, Himmatnagar	manishamehtain@gmail.com
2	Mr. Punit Saswadkar Lecturer (Computer)	Government Polytechnic, Gandhinagar	psgpg20@gmail.com
3	Mr. Naresh A. Patel Lecturer (Computer)	K. D. Polytechnic, Patan	napcool37@gmail.com