THIRD-YEAR DIPLOMA COMPUTER ENGINEERINGSYLLABUS

Semester: 6TH

Course Code: 002204672 **Type of Course:** PEC-LC-3

Course Name: Network Forensics Lab

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

COURSE OBJECTIVE(S): This course provides a foundational understanding of computer networks, emphasizing protocols, structures, and networking necessity. 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.

TEACHING & EXAMINATION SCHEME:

Teaching Scheme (Hrs/Week)				Examination Scheme					
Theory	Tutorial	Practical	Credit	SEE		CA			Total
				Th	Pr	MSE	PLE	LA	
0	0	2	1	00	25	00	00	25	50

Th: Theory; Pr: Practical; FA: Final Assessment; CAT: Continuous Assessment Theory; CAP: Continuous Assessment Practical;

*TOTAL Practical Hours: No. of Practical Hrs/Week*15 = 60*

LIST OF PRACTICALS: *(sample for 2 hrs/week)*15 weeks*

Sr. No.	Content	Unit No.	Time Duration
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	4
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
09	Analysis of DHCP Protocol using Wireshark.	III	2

THIRD-YEAR DIPLOMA COMPUTER ENGINEERINGSYLLABUS

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	**30**

Text Book(s):

Title of the Book	Author(s)	Publication
Network Forensics	d k thakar ,h k patel	Atul prakashan

Reference Book(s):

Title of the Book	Author(s)	Publication
Learning Network Forensics	Samir Datt	PACKT Publications, Year: 2016 ISBN: 9781782174905
Network Forensics	Ric Messier	Wiley, ISBN: 9781119328285
Network Forensics: Tracking Hackers through Cyberspace	Sherri Davidoff, Jonathan Ham	Pearson

Web Material Link(s):

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

Equivalent/Corresponding Course on NPTEL (SWAYAM):

Nill

PRACTICAL EVALUATION:

Sr. No.	Activity	Marks	Weightage
1	Semester End Examination (External Practical)	30	60%
2	Continuous Assessment Practical (CAP)	20	40%
	Semester End Examination (External Practical)		
1(a)	Lab Experiment/Exercise		30%
1(b)	Viva-voce		20%
1(c)	Certified Record		10%
	Continuous Assessment Practical (CAP)		
2(a)	Day to day Laboratory Work & Attendance		15%

2(b)	Submission of Laboratory Work/Journal		10%
2(c)	Exam		15%

* For 4 Credit Subjects

1 Credit = 25 Marks
Theory: 3 Credits = 75 Marks
Practicals: 1 Credit = 25 Marks
SEE Evaluation will be of 100 marks and converted to 50 Marks (75 Th + 25 Pr)
CA Evaluation will be of 100 Marks and converted to 50 Marks. (75 Th + 25 Pr)

Distribution of Marks for Theory Evaluation as per Bloom's Taxonomy Level:

Level	Remember	Understand	Apply	Analyse	Evaluate	Create
% Weightage	20%	25%	20%	15%	10%	10%

COURSE OUTCOMES:

CO1	Identify the significance and principles underlying networking concepts and protocols.
CO2	Demonstrate the application of network forensics in addressing different types of network attacks and vulnerabilities.
CO3	Describe the principles and methodologies involved in conducting network forensics analysis.
CO4	Comprehend wireless basics, authentication types, and attacks on wireless networks.
CO5	Describe the legal challenges, privacy laws, and future trends in network forensics.