

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Network Security and Forensics Practical
Course Code:	2ET2070107P
Pre-requisite Course:	Basic knowledge about computer networks and troubleshooting of network systems

Course Objectives:

The objective of this course is to learn and develop a Combines both the technical expertise and the knowledge required to investigate, detect and prevent network crimes.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
1	-	-	2	2	-	-	-	-	10	25	10	25	50

Course Contents:

Unit	Details	Contact Hours
1	a. Learn to install wine / virtual box or any other equivalent Software on the host os. b. Perform an experiment to grab a banner with telnet and perform The task using netcat utility c. Perform an experiment for port scanning with nmap, superscan Or any other software	8
2	Study of Computer Forensics and different tools used for forensic investigation a. Perform an experiment on active and passive finger Printing using xprobe2 and nmap. b. Performa and experiment to demonstrate how to sniff for router Traffic by using the tool wireshark. c. Perform an experiment how to use dumpsec.	8
3	Study of Computer Forensics and different tools used for forensic investigation a. Perform a wireless audit of an access point / router and Decrypt wep and wpa. b. Perform an experiment to sniff traffic using arp poisoning. c. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, symmetric crypto algorithm, hash and digital/pki Signatures	8
4	Network forensic investigation a. Computer Hacking & Network Intrusion b. Intellectual Property Theft c. Telecommunications Fraud	8

Reference Books:

1. Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom" by Lars Daniel and Larry E. Daniel
2. Digital Forensics with Kali Linux" by Shiva V. N Parasram

Course Outcomes:

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	I can compare and contrast tools used in network forensics and security applications.	Understanding (2)
CO2	I can provide technical arguments for the integrity of a certain piece of evidence.	Understanding (2)
CO3	I can create a timeline of events and identify linkage b/w subjects and objects for synthetic and real datasets.	Applying (3)
CO4	I can explain and process forensic datasets in a variety of formats.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3	PS O4
CLO1	H	M	M		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				

H: High, M: Medium, L: Low