	National Institute of Technology Meghalaya An Institute of National Importance	CURRICULUM

Programme	**Bachelor of Technology in Computer Science and Engineering**	Academic Year of Regulation	**2018-19**
Department	**Computer Science and Engineering**	Semester	**VIII**

Course Code	Course Name	Credit Structure				Marks Distribution			
		L	T	P	C	INT	MID	END	Total
CS 420	Cyber Forensics and Analysis	**3**	**0**	**0**	**3**	**50**	**50**	**100**	**200**

Course Objectives		Course Outcomes		
	This course introduces the knowledge in various robot structures and their workspace.		CO1	Able to acquire knowledge about the basic concepts used in Cyber Forensics and Analysis.
	This course illustrate digital investigation and digital evidence		CO2	Able to interpret the computer forensics
	This course illustrates with File System Analysis & file recovery.		CO3	Able to implement with forensics tools
	This course explains the information hiding & steganography time, registry & password recover.		CO4	Able to analyse and validate forensics data.
	This course familiarize with the Email & database forensics and Memory acquisition.		CO5	Able to analyse and identify the vulnerabilities in a given network infrastructure.

No.	COs	Mapping with Program Outcomes (POs)												Mapping with PSOs		
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
1	CO1	**-**	**1**	**-**	**1**	**-**	**-**	**-**	**-**	**2**	**-**	**-**	**-**	**3**	**-**	**3**
2	CO2	**1**	**1**	**-**	**1**	**-**	**-**	**-**	**-**	**2**	**-**	**-**	**-**	**2**	**-**	**2**
3	CO3	**1**	**2**	**3**	**1**	**2**	**-**	**-**	**-**	**0**	**-**	**-**	**-**	**2**	**3**	**2**
4	CO4	**-**	**2**	**3**	**-**	**2**	**2**	**3**	**-**	**2**	**-**	**-**	**1**	**2**	**3**	**2**
5	CO5	**-**	**2**	**3**	**-**	**2**	**2**	**-**	**-**	**2**	**-**	**-**	**1**	**3**	**3**	**3**

SYLLABUS

No.	Content	Hours	COs
I	**Introduction to Cyber forensics:** Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analysing Malicious software. Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques – Incident and incident response methodology – Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. – Forensics Technology and Systems -Understanding Computer Investigation – Data Acquisition.	10	CO1 CO2
II	**EVIDENCE COLLECTION AND FORENSICS TOOLS** Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools. Introduction to Cyber forensics: Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analysing Malicious software.	08	CO2 CO3
III	**ANALYSIS AND VALIDATION** Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition –Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics	08	CO2 CO3
IV	**ETHICAL HACKING** Introduction to Ethical Hacking – Foot printing and Reconnaissance – Scanning Networks -Enumeration – System Hacking – Malware Threats – Sniffing	05	CO4 CO3 CO4
V	**ETHICAL HACKING IN WEB** Social Engineering – Denial of Service – Session Hijacking – Hacking Web servers – Hacking Web Applications – SQL Injection – Hacking Wireless Networks – Hacking Mobile Platforms.	05	CO4 CO5
	Total Hours	36	

Essential Readings

1. Computer Forensics and Investigations, By Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, Cengage Learning, India Edition, 2016.
2. Cyber Forensics, By Dejey & S. Murugan, Oxford University Press, 2018.
3. Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, By Joakim Kävrestad, Springer International Publishing, 2018

Supplementary Readings

1. Computer Forensics, By John R.Vacca, Cengage Learning, 2005
2. Computer Forensics and Cyber Crime: An Introduction, By Marjie T.Britz, 3rd Edition, Pearson, 2013.
3. Ethical Hacking and Penetration Testing Guide, By Rafay Baloch , CRC Press, 2015