COURSE TITLE	**DIGITAL FORENSICS AND INCIDENT RESPONSE**
COURSE CODE	**01CY0213**
COURSE CREDITS	**4**

Objective:

1 This course aims to equip students with comprehensive knowledge and practical skills in digital crime investigation, including techniques for evidence collection and analysis using various tools. It covers critical areas such as analyzing Windows systems, networks, Wi-Fi, and web applications in the context of cybercrime. Students will also gain an understanding of the technical aspects of criminal activities, the legal procedures for reporting cyber incidents, and how to effectively present findings in a court of law.

Course Outcomes: After completion of this course, student will be able to:

1 Demonstrate a comprehensive understanding of cyber threat intelligence concepts, including types of threat intelligence and their applications.

2 Acquire skills in analyzing malware and other indicators of compromise (IOCs).

3 Apply threat intelligence to enhance proactive threat detection and response capabilities within an organization.

4 Critical Thinking and Problem-Solvingto analyze and interpret complex cyber security incidents and threats and apply critical thinking skills to prioritize and respond to incidents based on their severity and potential impact.

5 Recognize the importance of continuous learning and adaptation in response to evolving cyber threats.

Pre-requisite of course: Fundamental Knowledge of Cybersecurity, OS basic knowledge, Critical Thinking and Analytical Skills.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Digital Forensics** Introduction to computer forensics,, Evolution of computer forensics- Stages of Computer forensic process,Benefits of computer forensics-uses ofcomputer forensics, objectives of computer forensics, ole of Forensic Investigator,Forensic Readiness., Computer Forensics Investigation Process, Introduction to Computer Crime Investigation, Assess the situation – Aquire the data, Analyze the data, Report the investigation Understanding of FTK Imager and Autopsy	10

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
2	**Digital Evidence and First Responder Procedure** What is digital Evidence?, First Responder toolkit- Issues facing computer forensics, Types of Investigation- Techniques of Digital Forensics, Understanding Storage Media and File System, Hard Disk Drive,Details of Internal Structure of HDD – The booting process, File system,Common file systems,Types of file systems	9
3	**Windows Forensics** Introduction to Windows Forensics, Background and need for Windows forensics, Major forensic areas in Windows, Volatile Information ,Non-Volatile Information, Recovering deleted files and partitions, natomy of a disc drive,Data organization in Windows, Retrieving deleted files,Retrieving cache files, Retrieving files in unallocated space, Slack space- swap space,file carving , Event Logs	8
4	**Network Forensics** Introduction,Network Components and their Forensic Importance, Host, Node, Router, Switch, Hub, NIC -OSI Model – TCP /IP Layers, Forensic Information from Network, Log Analysis, Forensic Tools, Understanding the Usage of Wireshark ,SPLUNK and NMap	9
5	**Logs and Event Analysis** Windows Registry,, Windows event log file,Windows password storage, Password Cracking Application Password Crackers, Password cracking methods, Tools for Password Cracking, Wireless Attacks, Introduction- Wireless Fidelity – Wireless Security, ireless Attacks Detection Techniques, Wireless Intrusion Detection System, Wireless Attack Forensics: Introduction , Web Attack Forensics ,Web Application Forensic Tools	10
Total Hours		**46**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical - 1** Capture Active data of device using FTK Imager in order to understand Live memory Forensic	2
2	**Practical - 2** Make the Forensic Image of any Physical device using Autopsy and FTK Imager in order to understand bit by bit copy and Raw images Detecting	2
3	**Practical - 3** Use OSINT Framework in order to understand Investigation Process of Username and how it helpful in digital forensic process	2
4	**Practical - 4** Use OSINT Framework in order to understand Investigation Process of Domain Analysis and how it helpful in digital forensic process	2

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
5	**Practical - 5** Use OSINT Framework in order to understand Email Forensic	2
6	**Practical - 6** Use Autopsy Forensic tool to understand live forensic investigation (Ex. Pen-drive Image Analysis)	2
7	**Practical - 7** Use FTK Imager Forensic tool for recovering deleted file and how it helpful in forensic investigation	2
8	**Practical - 8** Use sysinternal tool suite to understand the inner working mechanism of the window machine process to identify and analyze illicit process	2
9	**Practical - 9** Use different plugin paly software to identify the malicious activities form the windows machine to understand the acquisition phase	2
10	**Practical - 10** Use Forensic Methodology for Extracting Browser Artefacts in order to understand browser forensic investigation	2
Total Hours		**20**

Textbook :

1 Digital Forensics and Incident Response: Fundamentals and Practices, Johansen, Packt Publishing, Limited, 2020

References:

1 Practical Incident Response: An Introduction to Enterprise Incident Response, Practical Incident Response: An Introduction to Enterprise Incident Response, Phil Beyer and Chris Childers, McGraw-Hill second edition, 2003

2 The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Michael Hale Ligh, Andrew Case, Jamie Levy, and Aron Walters, Wiley (John Wiley & Sons), 2014

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	0.00	30.00	30.00	30.00	10.00

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Instructional Method:

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1. “Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, Fourth Edition” by Harlan Carvey
2. “Incident Response & Computer Forensics, Third Edition” by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)