COURSE TITLE	**CYBER CRIME INVESTIGATION & DIGITAL FORENSICS**
COURSE CODE	**01CC0601**
COURSE CREDITS	**4**

Objective:

1 This course aims to introduce the fundamentals of digital forensics and the process of computer forensic investigations, along with developing an understanding of digital evidence handling, first responder procedures, and the structure of storage media and file systems. It also focuses on exploring forensic techniques in Windows environments and analyzing digital data for investigation purposes, as well as studying network forensics, event logs, password cracking, and wireless attack forensics using appropriate tools and methodologies.

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

1 Apply digital forensic techniques and standard procedures to collect, preserve, and handle digital evidence from various systems while maintaining its integrity.

2 Implement appropriate forensic tools and methodologies to examine storage media, file systems, and digital artifacts in different investigation scenarios.

3 Analyze network data, system logs, and digital traces to reconstruct events and support cybercrime investigations effectively.

4 Evaluate forensic tools, techniques, and legal considerations to ensure accuracy, reliability, and admissibility of digital evidence.

5 Design and develop structured forensic investigation procedures and comprehensive reports for real-world cybercrime cases.

Pre-requisite of course: Basic understanding of computer hardware and operating systems (especially Windows and Linux). Familiarity with networking fundamentals, including TCP/IP and OSI models. Basic knowledge of file systems and data storage structures. Fundamental programming or scripting skills (e.g., Python, Bash) are helpful but not mandatory.

Teaching and Examination Scheme

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

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

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

Contents : Unit	Topics	Contact Hours
1	**Introduction to Digital Forensics and Computer Forensics Investigation Process** Introduction to Computer Forensics, Evolution of Computer Forensics,, Stages of Computer Forensic Process, Benefits of Computer Forensics, Uses of Computer Forensics, Objectives of Computer Forensics, Role of Forensic Investigator and Forensic Readiness, Introduction to Computer Crime Investigation, Assess the Situation, Acquire the Data, Analyze the Data, Report the Investigation	9
2	**Digital Evidence and First Responder Procedure and Understanding Storage Media and File System** What is Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types of Investigation,, Techniques of Digital Forensics,, Hard Disk Drive, Details of Internal Structure of HDD, Types of File Systems	8
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, Anatomy 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	12
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	8
5	**Logs and Event Analysis, Password Cracking, Wireless Attacks and Wireless Attack Forensics** Windows Registry, Windows Event Log File, Windows Password Storage, Application Password Crackers, Password Cracking Methods, Tools for Password Cracking, Introduction to Wireless Fidelity, Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection System, Introduction to Web Attack Forensics, Web Application Forensic Tools	8
Total Hours		**45**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** To acquire a forensic disk image of a storage device and verify its integrity using hash values. Tools: FTK Imager, Guymager	2
2	**Practical 2** To analyze a forensic image and identify potential digital evidence files. Tools: Autopsy	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
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
3	**Practical 3** To examine disk partitions and file systems (NTFS/FAT/EXT) from a forensic image. Tools: Autopsy, WinHex	2
4	**Practical 4** To recover deleted files from a storage device or forensic image. Tools: Recuva, Autopsy	2
5	**Practical 5** To perform file carving on unallocated disk space to retrieve hidden or deleted data. Tools: Autopsy, X-Ways Forensics	2
6	**Practical 6** To capture and analyze volatile memory (RAM) data for running processes and network connections. Tools: Volatility	2
7	**Practical 7** To analyze Windows Event Logs and system artifacts for user activity investigation. Tools: Event Viewer, Autopsy	2
8	**Practical 8** To capture and analyze network packets to identify suspicious traffic. Tools: Wireshark, Tcpdump	2
9	**Practical 9** To perform password cracking using dictionary and brute-force techniques. Tools: John the Ripper, Hashcat	2
10	**Practical 10** To analyze wireless network security and detect unauthorized access or attacks. Tools: Aircrack-ng, Kismet	2
Total Hours		**20**

Textbook :

1 Digital Forensics and Incident Response, Gerard Johansen, Packt Publishing, 2020

References:

1 Real Digital Forensics, Real Digital Forensics, Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Wesley, 2006

2 Forensic Computing: A Practitioner's Guide, Forensic Computing: A Practitioner's Guide, ony Sammes and Brian Jenkinson, Springer, 2004

3 Computer Forensics and Investigations, Computer Forensics and Investigations, elson, Phillips Enfinger, Steuart, -, -

4 Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7", Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7", Harlan Carvey, Amsterdam ; Boston : Syngress, 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	20.00	20.00

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 or class-room.

Supplementary Resources:

1. https://www.dfir.training
2. https://www.sans.org/cyber-security-courses/digital-forensics/
3. https://csrc.nist.gov/publications
4. https://forensics.wiki/
5. https://www.futurelearn.com/courses/introduction-to-cybersecurity

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

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