Uka Tarsadia University

B. Tech.

CSE / CSE (CC) / CE (SE)

Semester VII

Program Elective - V

CYBER FORENSICS AND INVESTIGATION

CY6012

EFFECTIVE FROM July-2024

Syllabus version: 1.00

Subject Code	Subject Title
CY6012	**Cyber Forensics and Investigation**

Teaching Scheme				**Examination Scheme**				
Hours		**Credits**		**Theory Marks**		**Practical Marks**		**Total Marks**
Theory	Practical	Theory	Practical	Internal	External	Internal	External	
3	2	3	1	40	60	20	30	150

Objectives of the course:

- To understand the basic concepts of cyber forensics.
- To understand data acquisition process, processing crime and incident scenes, and current digital forensics tools used in cyber forensics.
- To understand digital forensics analysis and validation, analyze reporting and investigations prepared during forensics investigation.

Course outcomes:

Upon completion of the course, the student shall be able to,

CO1: Understand the basic concepts of cyber forensics.
CO2: Understand data acquisition process in cyber forensics.
CO3: Describe processing crime and incident scenes.
CO4: Apply a variety of current digital forensics tools used in cyber forensics.
CO5: Understand digital forensics analysis and validation.
CO6: Analyse reporting and investigations prepared during forensics investigation.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction to Cyber Forensics:** Digital forensics, Preparing for digital investigations, Maintaining professional conduct, Preparing a digital forensics investigation, Procedures for private-sector high-tech investigations, Understanding data recovery workstations and software, Conducting an investigations, Forensics lab accreditation requirements, Requirements for a digital forensics lab, Forensic workstation.	6
	Unit – II	
2	**Data Acquisition:** Formats for digital evidence, Best acquisition method, Acquisition tools, Validating data acquisitions, RAID data acquisitions, Remote network acquisition tools, Other forensics acquisition tools.	8

Unit – III		
3	**Processing Crime and Incident Scenes:** Identifying digital evidence, Collecting evidence, Preparing for a search, Securing a digital incident, Seizing digital evidence, Storing digital evidence, Obtaining a digital hash, Reviewing a case.	8
Unit – IV		
4	**Current Digital Forensics Tools:** Evaluating digital forensics tool, Software tools, Hardware tools, Validating and testing forensics software, Recovering graphics files.	7
Unit – V		
5	**Digital Forensics Analysis and Validation:** Determining what data to collect and analyze, Validating forensic data, Addressing data-hiding techniques, Virtual machine forensics, Live Acquisitions, Network forensics, E-mail, and Social media investigations.	8
Unit – VI		
6	**Reporting and Investigations:** Understanding the importance of reports, Guidelines for writing reports, Generating report findings with forensics software tools, Preparing for testimony, Testifying in court, Preparing for a deposition or hearing, Preparing forensics evidence for testimony.	8

Sr. No.	Cyber Forensics and Investigation(Practicals)	Hours
1	Create a forensic image using FTK imager/EnCase imager.	4
2	Perform data acquisition from a suspect device using various techniques and tools commonly employed in digital forensics investigations.	4
3	Solve forensic case study using encase investigator or autopsy.	4
4	Using Wireshark, capture and analyze network packets.	2
5	Monitor and manage processes on your computer using Sysinternals process explorer.	4
6	Perform email forensics on a Gmail account.	4
7	Perform forensics analysis of cell phones and mobile devices.	4
8	Conduct a forensic analysis of web browser artifacts to uncover evidence of online activities and reconstruct user browsing behavior.	4

Text book:

1. Bill Nelson, Amelia Phillips and Christopher Steuart, “Guide to Computer Forensics and Investigations”, 7th Edition 2024, Cengage Learning.

Reference book:

1. Darren R. Hayes, “A Practical Guide to Computer Forensics Investigations”, 2015, Pearson.

Course objectives and Course outcomes mapping:

- To understand the basic concepts of Cyber Forensics: CO1.
- To understand data acquisition, processing crime and incident scenes, current digital forensics tools used in cyber forensics and investigation: CO2, CO3, CO4.
- To understand digital forensics analysis and validation, reporting and investigations in cyber forensics and investigation: CO5, CO6.

Course units and Course outcomes mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction Cyber Forensics	✓					
2	Data Acquisition		✓				
3	Processing Crime and Incident Scenes			✓			
4	Current Digital Forensics Tools				✓		
5	Digital Forensics Analysis and Validation					✓	
6	Reporting and Investigations						✓

Programme outcomes:

PO 1: Engineering knowledge: An ability to apply knowledge of mathematics, science, and engineering.

PO 2: Problem analysis: An ability to identify, formulates, and solves engineering problems.

PO 3: Design/development of solutions: An ability to design a system, component, or process to meet desired needs within realistic constraints.

PO 4: Conduct investigations of complex problems: An ability to use the techniques, skills, and modern engineering tools necessary for solving engineering problems.

PO 5: Modern tool usage: The broad education and understanding of new engineering techniques necessary to solve engineering problems.

PO 6: The engineer and society: Achieve professional success with an understanding and appreciation of ethical behavior, social responsibility, and diversity, both as individuals and in team environments.

PO 7: Environment and sustainability: Articulate a comprehensive world view that integrates diverse approaches to sustainability.

PO 8: Ethics: Identify and demonstrate knowledge of ethical values in non-classroom activities, such as service learning, internships, and field work.

PO 9: Individual and teamwork: An ability to function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO 10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give/receive clear instructions.

PO 11: Project management and finance: An ability to demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO 12: Life-long learning: A recognition of the need for, and an ability to engage in life-long learning.

Programme outcomes and Course outcomes mapping:

Programme Outcomes	Course Outcomes					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1	✓					
PO2		✓	✓	✓	✓	✓
PO3			✓		✓	
PO4		✓		✓		✓
PO5						✓
PO6	✓			✓	✓	
PO7						
PO8	✓			✓	✓	
PO9						✓
PO10	✓		✓			✓
PO11						
PO12		✓		✓	✓	✓