Uka Tarsadia University

B. Tech.

CSE / CSE (CC) / CE (SE)

Semester VII

Program Elective - V

MALWARE ANALYSIS AND FORENSICS

CY6013

EFFECTIVE FROM July-2024

Syllabus version: 1.00

Subject Code	Subject Title
CY6013	Malware Analysis and Forensics

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 introduce basic concepts of malware analysis and forensics.
- To employ static, dynamic, and reverse engineering methods for malware identification, analysis and classification.
- To understand operating system forensics, network and email forensics.

Course outcomes:

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

CO1: Understand the basic concepts of malware analysis and forensics.
CO2: Understand the classification and analysis of malware in the field of malware analysis and forensics.
CO3: Describe malware analysis and mitigation.
CO4: Understand operating system forensics in malware analysis and forensics.
CO5: Understand network and email forensics.
CO6: Analyze malware forensics in malware analysis and forensics.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction:** Introduction to malware, Types of malware, Malware behavior and capabilities, Host-based malware detection, Advanced malware analysis techniques, Malware intelligence and threat hunting, Machine learning and artificial intelligence in malware analysis and detection.	6
	Unit – II	
2	**Malware Analysis and Classification:** Cyber physical systems, Types of cyber physical systems, Levels of cyber physical system architecture, Detecting malware in cyber physical systems, Malware detection methods, Malware classification – Static, dynamic and hybrid malware, Machine learning approach.	8

Unit – III		
3	**Malware Analysis and Mitigation:** Static malware analysis tools, Dynamic malware analysis tools, Hybrid malware analysis tools, Malware mitigation tools.	8
Unit – IV		
4	**Operating System Forensics:** Windows malware – Digital evidence in windows, File system, Windows forensics tools, Linux malware – Forensic process for Linux systems, Linux distributions used for forensic analysis, Linux forensics tools, Android malware – Android operating system, Manual extraction, Physical acquisition, iOS malware – iOS operating system, iOS forensics tools.	8
Unit – V		
5	**Network and Email Forensics:** Network forensics overview, Forensic footprints, Seizure of networking devices, Network forensic artifacts, ICMP attacks, Network forensic analysis tools, Email anatomy, Protocols used in email communication, Email crimes, Email forensics.	8
Unit – VI		
6	**Malware Forensics:** Types of malware, Malware analysis, Tools for analysis, Challenges, Malware as a service, Case study: Android malware analysis, Case study: Windows malware analysis of data stealing malware, Case study: Ransomware.	7

Sr. No.	Malware Analysis and Forensics (Practicals)	Hours
1	Install FlareVM on VirtualBox.	6
2	Perform static malware analysis techniques.	6
3	Perform dynamic malware analysis techniques.	6
4	Analyze Malware Traffic using iNetSim.	6
5	Malware code analysis with IDA.	6

Text books:

1. S.L. Shiva Darshan, M.V. Manoj Kumar, B.S. Prashanth and Y. Vishnu Srinivasa Murthy, “Malware Analysis and Intrusion Detection in Cyber-Physical Systems”, 2023, IGI Global.
2. Niranjan Reddy, “Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations”, 2019, Apress.

Reference book:

1. Abhijit Mohanta and Anoop Saldanha, "Malware Analysis and Detection Engineering", 2020, Apress.

Course objectives and Course outcomes mapping:

- To understand the basic concepts of Malware analysis and forensics: CO1.
- To understand malware analysis and classification, malware analysis and mitigation, operating system forensics: CO2, CO3, CO4.
- To understand network and Email forensics, malware forensics: CO5, CO6.

Course units and Course outcomes mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction	✓					
2	Malware Analysis and Classification		✓				
3	Malware Analysis and Mitigation			✓			
4	Operating System Forensics				✓		
5	Network and Email Forensics					✓	
6	Malware Forensics						✓

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 team work: 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		✓		✓	✓	✓