

Branch Name:	Bachelor of Technology (Computer Engineering & Information Technology)
Program Code:	ET103
Course Title:	Malware analysis, Digital forensics, and Cyber Law
Course Code:	2ET1030606T
Pre-requisite Course:	Basic Understanding of Windows and Linux operating systems, Malware and Networking, Web and OS security attacks, High Level & Low Level Programming.

Course Objectives:

- Learn to build and utilize a sandbox environment for malware analysis
- Apply various tools to Identify the vulnerabilities and to perform Malware analysis
- To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
- To understand how to examine digital evidences such as the data acquisition, identification analysis.
- Develop a foundational understanding of cyber law principles, including international regulations, legal frameworks, and their application in digital environments.
- Identify and classify various types of cyber-crimes such as hacking, malware attacks, identity theft, and online fraud.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	SEE		CCA		SEE		CCA						
	L	T	P	Total	Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Malware Analysis Fundamentals: Assembling a toolkit for effective malware analysis, examining static properties of suspicious programs, performing behavioral analysis of malicious Windows executable, performing static and dynamic code analysis of malicious Windows executable, interacting with malware in a lab to derive additional behavioural characteristics.	09	20
2	Reversing Malicious Code: Understanding core x86 assembly concepts to perform malicious code analysis, Identifying key assembly logic structures with a disassembler, following program control flow to understand decision points during execution, recognizing common malware characteristics at the Windows API level (registry manipulation, key logging, HTTP communications, droppers), Extending assembly knowledge to include x64 code analysis Examining Self-Defending Malware: How malware detects debuggers and protects embedded data, unpacking malicious software that employs process hollowing, Bypassing the attempts by malware to detect and evade the analysis toolkit, Handling code misdirection techniques, including SEH and TLS Callbacks, unpacking malicious executable by anticipating the packer's actions	09	20
3	Computer forensics: fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues. Understanding Computing Investigations – Procedure for corporate High-Tech investigations, understanding data recovery work station and software, conducting and investigations. Data acquisition- understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools. Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case.	09	20

4	Introduction to Cyber Forensics: Definition and importance of cyber forensics. Role of digital evidence in legal proceedings. 3. Challenges in cyber forensics investigations. Digital Evidence Collection: Legal aspects of digital evidence: admissibility and authenticity. Techniques and tools for digital evidence collection. Chain of custody and preservation of digital evidence	09	20
5	Overview of IT Act 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.	09	20

Textbooks:

1. Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press
2. Warren G. Kruse II and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.
3. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., “Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006, ISBN: 0-619-21706-5.
4. Vacca, J. R. (2005): Computer forensics: computer crime scene investigation. Hingham, MA: Charles River Media.
5. V. K. Ahuja, Intellectual Property Rights in India (Lexis Nexis, Butterworths, Wad hwa, Nagpur, 2015).
6. Alka Chawla, Copyright and Related Rights: National and International Perspectives (Macmillan India Ltd., Delhi, 2007).
7. Alka Chawla, Law of Copyright: Comparative Perspectives India (LexisNexis, Butterworths, New Delhi, 2013).

Reference Books:

1. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.
2. Gogolin, G. (Ed.), (2021): Digital forensics explained, CRC Press
3. K. Kumar, “Cyber Laws: Intellectual property & E Commerce, Security”, 1st Edition, Dominant Publisher, 2011.
4. Reverend Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition, Jones & Bartlett
5. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	The concept of malware analysis.	1.Remembering 2. Understanding
COL2	The basics of Digital forensics, applicability of DF for Law enforcement agencies. Cyber law in India, Types of Digital forensics technology, Digital evidence collection and handing, Computing Device Forensics Hardware & software. To be well-trained as next-generation computer crime investigators.	1.Remembering 2. Understanding 4. Analyze
COL3	The Mobile Phone Forensics & recent developments, Smart phone Operating Systems, Logical v/s Physical extraction, Mobile phone forensics tools	1.Remembering 2. Understanding
COL4	Students will demonstrate a comprehensive understanding of cyber law principles, including legal frameworks, regulations, and their application in	1.Remembering

	digital environments. Ability to identify and Analyze various types of cyber-crimes, understanding their methodologies, impacts, and legal implications	2.Understanding
COL5	Know how to apply forensic analysis tools to recover important evidence for identifying computer crime.	2.Understanding

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H		H		H											
CLO2	H		H		M		M		L	L	L					
CLO3	M		M		M		M		L	L	L					
CLO4	M		M		M		L									
CLO5	M		M		M		L									

H: High, M: Medium, L: Low

Reference University:

1. Sage University
2. Rastriy Raksha University
3. MRCET
4. APJ Abdul Kalam Technological University
5. IIT Kanpur
6. Gitam University