# *CSE 3156: Digital Forensics Workshop*

| | | | |
|---|---|---|---|
| | **ITER, SIKSHA 'O' ANUSANDHAN**<br>**(Deemed to be University)** | | **LESSON PLAN** |
| Programme | **B.Tech.** | Academic Year | **2024-25** |
| Department | **Cybersecurity** | Semester | **5** |
| Credit | **4** | Grading Pattern | **5** |
| Subject Code | **CSE 3156** | | |
| Subject Name | **Digital Forensics Workshop** | | |
| Weekly Course Format | **0L-8P** | | |
| Subject Coordinator (s) | **Dr. Bharat Jyoti Ranjan Sahu & Dr. Rourab Paul** | | |

## Text Books(s):

(1) Digital Forensics with Kali Linux by Parasam, $3^{rd}$ Edition, Packt Publishing

| | | |
|---|---|---|
| **Course Outcomes** | Students will be able to | |
| | **CO1** | Understand the fundamental concepts and methodologies of digital forensics, including file systems and data acquisition. |
| | **CO2** | Develop proficiency in using Kali Linux, netdiscover, and nmap for network discovery and device identification. |
| | **CO3** | Gain hands-on experience with forensic tools like Autopsy, Xplico, and Wireshark for analyzing digital evidence. |
| | **CO4** | Perform memory forensics using the Volatility framework and analyze malware and ransomware artifacts. |
| | **CO5** | Investigate automated forensic analysis with tools such as magicrescue, Scalpel, and PcapXray for data recovery and network traffic analysis. |
| | **CO6** | Conduct online PCAP analysis and use platforms like shodan.io and packettotal.com to assess network security vulnerabilities. |

# *CSE 3156: Digital Forensics Workshop*

| Sl.No. | Lessons/Topics to be covered | Book Reference (sections) | Mapping with COs | Home Work/ Assignments/ Quizzes |
|---|---|---|---|---|
| **1** | Introduce the grading pattern, credit, classes and lab session of the course. Motivation behind the course. Introduction to Digital Forensics | **2** | **CO1** | |
| **2** | Kali Linux Installation and familiarization, Basic Commands | **1** | **CO2** | |
| **3** | Understanding File systems and Storage Media: history of storage media, File system and Operating System, DATA states and metadata | **6** | **CO1** | |
| **4** | Incident Response and Data Acquisition, Hashing, DFIR Chain of Custody (CoC) | **7** | **CO1** | |
| **5** | Different Hash Commands in Kali Linux, MD5, SHA256, hash commands in python environment and examples | **7** | **CO2** | **Assignments 1** |
| **6** | Evidence Acquisition and Preservation with dc3dd and Guymager | **8** | **CO1** | |
| **7** | dc3dd and dd Examples, dd and dc3dd commands in python environment and examples | **8** | **CO1** | |
| **8** | Image acquisition, Guymager, FTK Imager | **8** | **CO1** | **Assignments 2** |
| **9** | Introduction to File Recovery and Data Carving Forensic test images, foremost | **9** | **CO5** | |
| **10** | foremost in python environment and examples | **9** | **CO5** | |
| **11** | bulk_extractor, explore bulk_extractor in python environment and examples | **9** | **CO5** | |
| **12** | magicrescue and Scalpel, magicrescue and Scalpel in python environment and examples | **9** | **CO5** | **Assignments 3** |
| **13** | Introduction Memory Forensics and analysis, Introducing the Volatility Framework | **10** | **CO4** | |
| **14** | Setup dependencies of Volatility in Kali Linux, memory dump using volatility | **10** | **CO4** | **Quiz 1** |
| **15** | Image and OS verification, process identification and analysis, pstree plugin, modscan plugin, envars plugin using volatility | **10** | **CO4** | |

| Sl.No. | Lessons/Topics to be covered | Book Reference (sections) | Mapping with COs | Home Work/ Assignments/ Quizzes |
|---|---|---|---|---|
| **16** | hivelist plugin, password dumping using volatility | **10** | **CO4** | |
| **17** | volatility in python environment and examples | **10** | **CO4** | **Assignments 4** |
| **18** | Introduction artifact malware and ransomware analysis, introduction p0f | **11** | **CO4** | |
| **19** | Identifying devices and operating systems with p0f, p0f in python environment and examples | **11** | **CO2** | |
| **20** | Information gathering and fingerprinting with Nmap | **11** | **CO2** | |
| **21** | nmap in python environment and examples | **11** | **CO2** | |
| **22** | Linux Explorer swap digger, Password dumping with mimipenguin | **11** | **CO4** | **Quiz 2** |
| **23** | PDF malware analysis, Examining Firefox artifacts with pdgmail | **11** | **CO4** | |
| **24** | Malicious file analysis using Hybrid | **11** | **CO4** | |
| **25** | Ransomware analysis using volatility, pslist plugin | **11** | **CO4** | **Assignments 5** |
| **26** | Introduction to autopsy, autopsy forensic browser, Automated Digital Forensic Suites, Introduction and setup Autopsy 4 | **12** | **CO3** | |
| **27** | Analyzing Directories & recovering deleted files & Artifacts with Autopsy 4 | **12** | **CO3** | **Assignments 6** |
| **28** | Autopsy 4 GUI Features, analyzing directories and recovering deleted files and artifacts with Autopsy 4 | **13** | **CO3** | |
| **29** | Introduction to Network Discovery Tools, introduction netdiscover | **14** | **CO2** | |
| **30** | netdiscover in python environment | **14** | **CO2** | **Quiz 3** |
| **31** | Introduction to nmap, nmap in python environment | **14** | **CO2** | |
| **32** | nmap to find additional hosts and device on a network, nmap to fingerprint host details | **14** | **CO2** | |
| **33** | shodan.io to find devices including firewalls, CCTV and servers | **14** | **CO6** | **Assignment 7** |

| **Sl.No.** | **Lessons/Topics to be covered** | **Book Reference (sections)** | **Mapping with COs** | **Home Work/ Assignments/ Quizzes** |
|---|---|---|---|---|
| **34** | Introduction to Xplico, Packet capture analysis with Xplico | **15** | **CO3** | |
| **35** | Automated web traffic analysis with Xplico | **15** | **CO3** | |
| **36** | Automated SMTP traffic analysis with Xplico | **15** | **CO3** | **Quiz 4** |
| **37** | Introduction to Network Forensic Analysis, capturing Packet with Wireshark and explore different features of Wireshark | **16** | **CO3** | |
| **38** | Different filters and command to analyze network traffic using Wireshark | **16** | **CO3** | |
| **39** | Packet Capture and analysis with PcapXray | **16** | **CO6** | |
| **40** | Online PCAP analysis using packettotal.com | **16** | **CO6** | **Assignment 8** |
| **41** | Project | **NA** | **CO1-CO6** | **Project** |
| **42** | Project | **NA** | **CO1-CO6** | **Project** |
| **43** | Project | **NA** | **CO1-CO6** | **Project** |