

COURSE STRUCTURE

Course Code	CET4033B			
Course Category	Professional Core			
Course Title	Digital Forensics and Investigation			
Total Teaching Hrs and Credits	Lectures	Tutorial	Laboratory	Credits
	02 hrs/week	--	02 hrs/week	2+1=03

Pre-requisites

- Computer Networks, Information Security

Course Objectives:

1. To explore the investigative aspect of digital crimes
2. To understand computer forensics
3. To learn tools used in digital forensics
4. To learn basic programming for digital forensics

Course Outcomes:

On completion of course, students should be able to

1. Develop awareness of computer forensics
2. Conduct effective investigation of digital crimes
3. Analyze and use digital forensics tools for efficient investigation
4. Employ digital forensics applications in real world

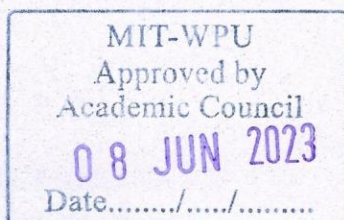
Course Contents:

1. Introduction to Digital Forensics
2. Evidence Collection
3. Windows and Linux Forensics
4. Security Tools
5. Case Study and Scenarios

Laboratory Exercises:

1. Explore various computer forensic application programs for recovering deleted files and or deleted partitions and demonstrate any one such tool.
2. Write a program in C++ /Python to analyze an email header.
3. Write a program for identifying tampering in either image or voice data. Use big data as input.
4. Install a suitable Digital Forensics framework (such as Encase) and perform investigation. Generate the various reports and analyze the same.
5. Write a Java/Python program to monitor and analyze Network Forensics, also perform investigation of various logs
6. Perform installation and employ any Android Mobile Forensics Open Source Tools for real time investigation of mobile forensics
7. Develop a C++/Java program for Log Capturing using a wireless router. Perform suitable event correlation and analysis of network traffic.
8. Demonstrate Forensics Case Investigation using Autopsy

Dr. Dinesh Seth
Dean



Learning Resources:

Text Books:

1. Digital Evidence & Computer Crime, Eoghan Casey Bs Ma Ac, Elsevier-Academic Press, Third Edition, ISBN 13: 978-0123742681, ISBN 10 : 0123742684
2. Computer Forensics Jump Start- Michel G. Solomen, Diane Banet and Neil Broom

Reference Books:

1. Hacking Exposed- Computer Forensics Chris Davis, Aaron Phillipp and Davidcowen. Ma-Graw Hill
2. Forensics and Investigative accounting- D Larry Crumbley, Laster E. Heitger and G. Stevenson smith.

Supplementary Reading:

Code Hacking- Richard Conway and Julian Cordingley

Web Resources:

<https://www.forensicfocus.com/>

<https://www.youtube.com/watch?v=F7mH5vz1qEI&featur=yotu.be>

Web links:

<http://www.cca.gov.in/>

<https://www.verisign.com/>

<https://meity.gov.in/content/information-technology-act-2000>

MOOCs:

<https://swayam.gov.in/NPTEL>

<https://nptel.ac.in/noc/>

<https://www.edx.org/course/computer-forensics>

Pedagogy:

1. Power Point Presentation
2. Video Lectures
3. Flipped Classroom Activity

Assessment Scheme:

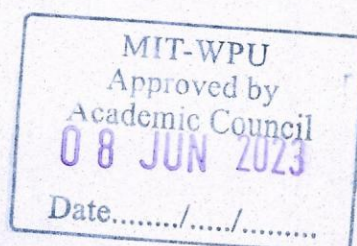
Class Continuous Assessment: 30 Marks

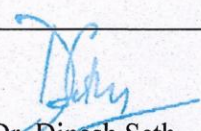
Assignments	Mid Term Exam	Active learning	Total
5 Marks	15 Marks	10 Marks	30 Marks

Laboratory Continuous Assessment: 30 Marks

Practical	Problem based Learning/ Tool Demo	Oral	Total
10 Marks	10 Marks	10 Marks	30 Marks

Term End Examination: 40 Marks




Dr. Dinesh Seth
Dean

Syllabus: Theory

Module No.	Contents	Workload in Hrs
		Theory
1	Introduction Digital Forensics Introduction to Digital Forensics, Locard's Principle of Exchange in Digital Forensics, Branches of Digital Forensics, Principles of Digital Forensics, Phases of digital/computer forensics investigation, Identification of digital evidences, necessary documentations such as Chain of Custody, pre-acquisition forms etc., Digital evidence handling at crime scene as per standards, Collection/Acquisition and preservation of digital evidences, Processing & analysis, Compilation of findings & Reporting. Code Hacking- Input Validation, Buffer Overflow Attacks, SQL Injection, Cross Site Scripting , Ethical hacking of operating Systems, Ethical hacking of web, email and mobile Phones	08
2	Evidence Collection Challenges in dealing with Digital Evidence Defining levels of certainty in Digital Evidence, Computer Forensics: Incident Response Secrets and solutions, Investigations – Covert and remote operations, Search and seizure of digital evidence, Data Acquisition and disk imaging, Special Forensics Scenarios : Email Forensics Investigation, Data storage Forensics, Forensic Investigation of mobile devices, Forensic investigation of Wi-Fi Environment	08
3	Windows and Linux Forensics Understanding registry concept in various operating systems, Log analysis with respect to standalone machine and server which includes system logs, kernel logs, event logs etc. Windows Forensics: Locate and Gather Evidence, File Slack and its Investigations, Interpret the Windows Registry, Internet Traces, System State Backups, File System Description in Linux, Linux Directories, The Challenges in Disk Forensics with Linux, Linux Forensics Tool: SMART for Linux Forensics	08
4	Security Tools Open Source Tools (Forensics tools Suites) TCT (The Coroners Toolkit), TSK (The Sleuth Kit), FTK (Forensics Tool Kit), EnCaseMaresware. Security Software: Antivirus, Email Security, Identify and Access Management, Incidence response policies, Incidence reporting Forensics & Intrusion Detection, and Prevention. Case Study and Scenarios IP Thefts, Corporate Frauds, Digital Frauds, Cyber Crimes, Cyber Porn, Cyber Stalking, Consumer and credit Card Fraud, Online and Digital Fraud-Phishing Attacks, Spare Attack and other Incident.Forensic analysis of Multimedia Files, CCTV Footage analysis, Different Steganalysis tools and techniques	08

Dr. Dinesh Seth
Dean



Laboratory:

Module No.	Contents	Workload in Hrs
		Lab
1.	Write a program in C++ /Python to analyse an email header.	04
2.	Perform installation and employ any Android Mobile Forensics Open Source Tools for real time investigation of mobile forensics	02
3.	Write a Java/Python program to monitor and analyse Network Forensics, also perform investigation of various logs.	02
4.	Write a program for identifying tampering in either image or voice data. Use big data as input.	02
5.	Develop a C++/Java program for Log Capturing using a wireless router. Perform suitable event correlation and analysis of network traffic.	02
6.	Explore various computer forensic application programs for recovering deleted files and or deleted partitions and demonstrate any one such tool.	02
7.	Install a suitable Digital Forensics framework (such as Encase) and perform investigation. Generate the various reports and analyse the same.	04
8.	Demonstrate Forensics Case Investigation using Autopsy	04

MIT-WPU
Approved by
Academic Council
Date...../...../.....

Signature

Signature
Dr. Dinesh Seth
Dean