Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: A **200 level** number requested**.**
2. Course Title: **Digital Forensics**
3. No. of Lectures per week: 0 (L), Tutorial: 1 (T), Laboratory: 3 (P), Additional Hours: 3 (A),
   Credits (3*L+2*T+P+A): 08 Duration of Course: Full Semester
4. Proposing Department/IDP : WSAIS
   Other Departments/IDPs which may be interested in the proposed course: CSE
   Other faculty members interested in teaching the course: Somitra Sanadhya, Manindra Agrawal
5. Proposing Instructor: DUGC (WSAIS)
6. Course Description:

A) Objectives: The objective of this practical-based course is to impart hands-on training in the digital, network, mobile forensics, VM forensics, and memory forensics, and in the proper analysis and reporting of digital evidence using standard forensic tools and techniques.

B) Contents: **(for 13 weeks of labs, tutorials, and additional work)**

S. No	Type	Broad Title	Topics	Tools	Duration
1	**Theory**	**Digital Forensics Process & Chain of Custody**	Digital Forensics Investigation Lifecycle: Identification, Preservation, Collection, Examination, Analysis, Reporting Search and Seizure Process, Chain of Custody and legal importance Admissibility of Digital Evidence Overview of Indian IT Act (relevant sections), and Relevant Section of BSA	Manual documentation and Autopsy, VMware/VirtualBox	1 Hour
	Practical		**Lab 1: Digital Forensics Lab Setup & Evidence Handling** • Windows & Kali VM setup, host-only network, snapshots, tool installation, • Chain of custody documentation, • Evidence handling simulation		3 Hour

2	**Theory**	**Disk Acquisition & Imaging Techniques**	Storage media fundamentals. Logical vs Physical vs Live vs Dead Acquisition and Importance of Write Blockers. Forensic image formats (RAW, E01, AFF).	FTK Imager, dd, dc3dd	1 Hour
	Practical		**Lab 2: Forensic Disk & Live Data Acquisition** • Disk/USB acquisition, • Live acquisition, • Image integrity verification.		3 Hour
3	**Theory**	**Hashing & Evidence Integrity Verification**	Importance of hashing in forensics and Hash algorithms (MD5, SHA-1, SHA-256).	Hashcalc/ md5sum/ SHA-1 and 256sum	1 Hour
	Practical		**Lab 3: Evidence Hash Generation & Integrity Validation** • Generating hashes for original media, • Hash comparison and validation and Maintaining evidence integrity		3 Hour
4	**Theory**	**Disk Structure & File System Identification**	Disk Geometry, MBR/GPT, MFT, partitions, file system identification and corruption scenarios.	Sleuth Kit & Autopsy	1 Hour
	Practical		**Lab 4: Partition & File Metadata Analysis** • Partition analysis, hidden/damaged partitions, • file metadata & timestamps		3 Hour
5	**Theory**	**File System Forensics (NTFS, FAT, EXT)**	Common File Systems & Usage, Key File System Components (FAT,NTFS,EXT), File system metadata, timestamps, journaling and allocation strategies.	Sleuth Kit & Autopsy	1 Hour
	Practical		**Lab 5: File System Analysis & Timeline Reconstruction** • File system identification, • Directory analysis, • Metadata & timeline correlation		3 Hour
6	**Theory**	**Deleted Data & File Carving**	Deletion mechanisms, slack/unallocated space, anti-forensic	Autopsy & Foremost & Scalpel	1 Hour

	Practical		**Lab 6: Deleted File Recovery & Basic File Carving** • Recycle Bin recovery, unallocated space analysis, carving, wiping detection		3 Hour
7	**Theory**	**Advanced File Carving & Fragment Recovery**	Fragmented files, header/footer limitations and validation of carved files.	Scalpel, Binwalk, PhotoRec, Exif Tool	1 Hour
	Practical		**Lab 7: Advanced File Carving & Fragment Reconstruction** • Manual carving, fragmented file recovery, anti-forensic detection		3 Hour
8	**Theory**	**Windows OS Artifact Forensics**	Windows activity artifacts, Categories of Windows Artifacts, user behaviour traces and execution artifacts.	Autopsy, RegRipper	1 Hour
	Practical		**Lab 8: Windows Registry & User Activity Forensics** • Registry, Prefetch, • LNK, USB artefacts, • Event logs, • User activity		3 Hour
9	**Theory**	**Volatile Memory (RAM) Forensics**	Volatile data importance, Types of Volatile data, Order of Volatility (OOV), memory acquisition challenges and live analysis risks.	Volatility	1 Hour
	Practical		**Lab 9: Live Memory Acquisition & Analysis** • RAM capture, process, • Network & credential artefacts		3 Hour
10	**Theory**	**Network Forensics and malware traffic exercise**	What is Network Forensics, Network evidence types, Live vs Dead Network Forensics, packet vs log analysis.	Wireshark & tcpdump	1 Hour
	Practical		**Lab 10: Network Traffic Capture & Analysis** • Traffic capture, • PCAP analysis, • DNS, HTTP/HTTPS forensics		3 Hour
11	**Theory**	**Virtual Machine & Cloud Artifact Forensics**	W hy VM & Cloud Forensics is Different VM disk formats (VMDK, VDI), snapshots andcloud artifact fundamentals.	Autopsy & qemu-img	1 Hour

	Practical		**Lab 11: VM Disk & Snapshot Forensic Analysis** • VM disk analysis, snapshot investigation and VM timeline reconstruction. Hypervisor & Host Artefacts.		3 Hour
12	**Theory**	**Mobile Device Forensics**	Mobile file systems, Types of Mobile Acquisition: logical vs physical extraction and app artifacts. Mobile Forensic Challenges	ADB & Autopsy	1 Hour
	Practical		**Lab 12: Logical Mobile Acquisition & App** • Logical acquisition, • App data, location, deleted data & caches		3 Hour
13	**Theory**	**Integrated Forensic Case Investigation**	Evidence correlation, forensic reporting and expert testimony basics.	Autopsy & Manual	1 Hour
	Practical		**Lab 13: End-to-End Digital Forensic Case Investigation** • Integrated disk, • Memory, • Network, • Mobile • VM analysis, • Final report		3 Hour 3 Hour

C) Pre-requisites:

- Working knowledge of Windows and Linux OS
- Basic networking concepts
- Familiarity with virtual machines
- Introductory cyber security knowledge

D) Short summary for including in the Courses of Study Booklet: This course provides hands on training to the students on the concepts and techniques of digital forensics and preserving evidence. The students will be able to analyze operating systems and memory artifacts, examine the same, and prepare simple forensic reports.

7. Recommended books:
   • Tools which will be used are already listed in the weekly description.

Dated: 13 August 2026; Proposer: DUGC, WSAIS

Dated: ; DUGC Convener (WSAIS):_____

The course is approved / not approved

_____

Chairperson, SUGC

Dated:_____