Hindi Vidya Prachar Samiti's

Ramniranjan Jhunjhunwala College

of Arts, Science & Commerce

(Empowered Autonomous College)

Affiliated to

UNIVERSITY OF MUMBAI

Program Code: RJCUCSDF

Syllabus for the

B.Sc Cyber Security & Digital Forensics (under NEP)

Course Codes: RJVSCCSDFP111

New Program to be started from the academic year 2026-2027

Preamble

The National Education Policy 2020 aims at imparting skill-based learning and caters to the multiple entry and exit facility for the students thus empowering them to acquire knowledge at their pace In the three-year UG program, the student has two exit options. Students also have the option for choosing the Honors program of four years study in a given discipline and later converting it to five year integrated PG degree program. As undergraduate student, he/she learns the core subject (Major), subject complementing the core subject (Minor), a course from other discipline (OEC or GEC) Vocational and Skill Enhancement course from the Major(VSEC). The remaining verticals under NEP 2020 are IKS (Indian Knowledge System), AEC (Ability Enhancement Course), VEC (Value Enhancement Course) and with progressive three years of UG, student also completes at different levels OJT (On Job Training), FP (Field Projects), CEP (Community Engagement Program) , RP (Research Project) which helps him/her in understanding their roots, application of the knowledge for the benefit of self and the society. Vertical CC (Co-curricular activities and activities related to yoga and human well-being) helps in preparing youth with good character and interpersonal relationships.

Vocational and Skill Enhancement Course (VSC) (Practical) – Introduction to Forensics Tools (Practical)

Course Code	Course Title	Course Type	Credits	Duration
• RJVSCCSDFP111	Introduction to Forensics Tools (Practical)	Value Added Skill (Practical)	2	60 Hours

Course Objectives

Sr. No.	Objective
1	Familiarize with open-source forensics tools for data acquisition.
2	Practice disk imaging and hash verification techniques.
3	Learn basic file recovery and timeline analysis.
4	Understand chain of custody in tool usage.

Practical Assignments

Practical No.	Task / Title	Description
1	Launch and Preview	Launch FTK Imager and create a logical drive preview of a sample folder; export as a basic evidence file (Tool: FTK Imager - GUI Export Wizard).
2	Physical Acquisition	Acquire a physical preview of a sample USB drive image; note the process time and file size (Tool: FTK Imager - Physical Drive Selection).
3	Hash Generation	Generate and display an MD5 hash for a sample evidence file; compare it to a pre-known good hash (Tool: FTK Imager - Verify Hashes feature).
4	Acquisition Log	Document a simple acquisition step-by-step in the tool's built-in notes; save as a PDF report (Tool: FTK Imager - Case Log/Report Export).
5	Evidence Import	Import a sample image into FTK Imager and browse the file tree without modifications (Tool: FTK Imager - Add Evidence Item).
6	Custom Export	Create a custom export of a folder structure from a preview image, including metadata like creation dates (Tool: FTK Imager - Export Files with Options).
7	Batch Verification	Verify hash integrity for a multi-file evidence set (e.g., 3-5 documents) and flag any mismatches (Tool: FTK Imager - Batch Hash Verification).
8	Log Entry Simulation	Simulate a quick acquisition log entry for a hypothetical device seizure, including who/what/when details (Tool: FTK Imager - Integrated Notes and Export).

9	Case Creation	Create a new case in Autopsy and add a sample disk image; explore the directory structure (Tool: Autopsy - New Case Wizard).
10	Deleted File Recovery	View and export a deleted text file from the sample image's unallocated space (Tool: Autopsy - File Types View and Export).
11	Timeline Report	Generate a basic timeline report for files modified in the last 7 days from the image (Tool: Autopsy - Timeline Module).
12	Browser Artifact Extraction	Extract and preview browser history artifacts from a user profile in the image (Tool: Autopsy - Keyword Search and Ingest Modules).
13	Incident Summary Report	Compile a simple incident summary report from viewed artifacts; include screenshots (Tool: Autopsy - Reports Generation).
14	Image Tagging and Export	Search for and tag image files (e.g., JPEGs) in a case; export tagged items to a folder (Tool: Autopsy - Keyword Search with Tagging).
15	Filtered Views	Build a filtered views of recent documents by file type and date; note any suspicious patterns (Tool: Autopsy - Views and Filters).
16	Basic Ingest Run	Run a basic ingest on a small image to auto-detect and highlight potential artifacts like URLs or emails (Tool: Autopsy - Ingest Manager with Default Modules).

CO–PSO Mapping

CO	**Outcome**	**Bloom's**	**PSO**
CO1	Demonstrate basic acquisition and hashing using a single GUI tool.	Apply (L3)	PSO1, PSO5
CO2	Explain and apply chain of custody in tool-based workflows.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO3	Implement simple file viewing and export on sample evidence.	Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze basic timelines for introductory incident insights.	Analyze (L4)	PSO1, PSO2, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Practical Digital Forensics (2019)	Richard Boddington / Packt Publishing
2	Digital Forensics for Legal Professionals (2012)	Larry Daniel, Lars Daniel / Elsevier
3	The Basics of Digital Forensics (2nd Ed., 2014)	Jason Luttgens, Matthew Pepe, Kevin Mandia / Syngress
4	Digital Forensics with Open Source Tools (2011)	Cory Altheide, Harlan Carvey / Syngress
5	File System Forensic Analysis (2005)	Brian Carrier / Addison-Wesley