D Y PATIL
DEEMED TO BE
UNIVERSITY
NAVI MUMBAI

B.Tech in Cyber Security & Digital Forensics

D Y PATIL DEEMED TO BE UNIVERSITY

2025-2026

1. Name of the Program**:** **B. Tech in Cyber Security & Digital Forensic**
2. Proposed Year of commencement**:** **2025-2026**
3. Duration of the Proposed Program: **4 Years** Full time under graduate program comprising 8 (eight) semesters. Each year is divided in to 2 (two) semesters.
4. Degree Offered: **B. Tech Cyber Security & Digital Forensic**
5. Proposed Intake: **120**
6. Eligibility:

For National Students	Minimum 50% aggregate in PCM/PCB* or Physics & Mathematics with any Technical Vocational Subject. Physics, Mathematics & English are Compulsory subjects with Chemistry/Biotechnology* or Biology*/Technical Vocational Courses in 10+2/Class 12th or equivalent examination
For International Students	The eligibility criterion for all programs for international applicants is minimum 50% in the qualifying examination and having studied the pre-requisite subjects for admission in to the desired program.

Introduction of the Program:

With the increasing prevalence of cybercrimes and digital threats, the need for skilled professionals in digital forensics has become critical. The B.Tech. in Digital Forensics program addresses this growing demand by combining core concepts of computer science, cybersecurity, and criminal investigation. As businesses, governments, and individuals rely more on digital platforms, the ability to investigate cyber incidents, recover compromised data, and ensure digital security has gained immense importance. This program provides a robust foundation for students to understand and tackle cyber threats, preparing them to play a vital role in safeguarding digital infrastructures.

In today's digital age, cybercrime is one of the fastest-growing threats to global security, affecting industries, governments, and individuals alike. The B.Tech in Digital Forensics program is designed in response to the urgent need for experts who can investigate and prevent cybercrime, recover digital evidence, and protect sensitive data. As organizations increasingly depend on digital operations, the demand for trained professionals who can ensure the integrity of digital systems and solve cybercrime cases has never been higher, making this program highly relevant and essential.

Interdisciplinary Nature:

The B.Tech in Digital Forensics combines elements from computer science, law, and cybersecurity, offering a holistic approach to investigating cybercrimes. Students gain expertise in areas like ethical hacking, data recovery, cryptography, and digital law enforcement. This interdisciplinary curriculum prepares graduates to address complex challenges in both technical and legal domains of digital crime investigation.

P**rogram Objectives:**

- To equip students with a strong foundation in digital forensics, covering topics such as cybersecurity, ethical hacking, data recovery, and cryptography.
- To provide practical experience through advanced forensic tools and techniques for analyzing digital evidence and solving cybercrimes.

- To teach students the legal frameworks, ethical considerations, and regulations governing cyber investigations and digital evidence handling.
- To train students to critically analyze and respond to digital threats, system vulnerabilities, and cyber incidents using effective forensic methods.
- To encourage research in emerging areas of digital forensics and cybersecurity, promoting innovation in the detection and prevention of cybercrimes.
- To ensure graduates are ready for careers in cybersecurity, law enforcement, corporate IT security, and digital forensic consultancy, addressing the rising global demand for skilled professionals in this field.

Programme Outcomes

- **PO1: Apply Knowledge**: Use fundamental concepts of computer science, cybersecurity, and digital forensics to solve complex problems in cybercrime investigation.
- **PO2: Forensic Investigation Skills**: Demonstrate proficiency in digital forensic tools and techniques for detecting, analyzing, and responding to cyber incidents.
- **PO3: Legal and Ethical Competence**: Apply relevant legal frameworks, regulations, and ethical standards in handling digital evidence and conducting forensic investigations.
- **PO4: Problem-Solving and Critical Thinking**: Analyze and address cybersecurity challenges with a structured approach to prevent, detect, and mitigate cyber threats.
- **PO5: Communication and Collaboration**: Communicate digital forensic findings effectively to diverse audiences, including legal, law enforcement, and technical professionals.
- **PO6: Lifelong Learning and Adaptability**: Commit to continuous learning and staying current with emerging technologies, tools, and threats in the rapidly evolving field of digital forensics.

Program Structure:

The B.Tech. in Digital Forensics program equips students with the skills to investigate cybercrimes, recover digital evidence, and ensure data security. Combining cybersecurity, ethical hacking, and legal frameworks, the curriculum provides hands-on training in advanced forensic tools and techniques. Graduates will be prepared for careers in cybersecurity, law enforcement, and IT security, addressing the growing demand for digital forensics experts.

Credit hours:

Credit hour distribution for B. Tech in Digital Forensic Studies course spread across eight semesters with a total of 168 credits.

Course Descriptions, Credit Hours, and Learning Outcomes:

Semester 1: **(22 credits)**

1. Technical English (5 credits)
2. Mathematics (5 credits)
3. Engineering Physics (5 credits)
4. Elective 1(4 credits)
5. Elective 2 (3 credits)

Semester 2: (22 credits)

1. Engineering Chemistry (5 credits)
2. Environmental Science (5 credits)
3. Fundamentals of Networking (5 credits)
4. Elective 1(4 credits)
5. Elective 2(3 credits)

Semester 3: (22 credits)

1. Cyber Criminology and Cyber Crime (5 credits)
2. Digital Systems (5 credits)
3. Elective 1(4 credits)
4. Elective 2(4 credits)
5. Elective 3(4 credits)

Semester 4: (22 credits)

1. Computer Organization and Architecture (5 credits)
2. Fundamentals of Information Security and Cryptography (5 credits)
3. Elective 1(4 credits)
4. Elective 2(4 credits)
5. Elective 3(4 credits)

Semester 5: (20 credits)

1. Statistics for Computer Engineers (5 credits)
2. Fundamentals of Digital Forensics (5 credits)
3. Elective 1(4 credits)
4. Elective 2(3 credits)
5. Elective 3(3 credits)

Semester 6: (20 credits)

1. Advanced Networking (5 credits)
2. Elective 1(5 credits)
3. Elective 2(4 credits)
4. Elective 3(3 credits)
5. Elective 4(3 credits)

Semester 7: (20 credits)

1. Advanced Digital Forensics (5 credits)
2. Elective 1(5 credits)
3. Elective 2(4 credits)
4. Elective 3(3 credits)
5. Elective 4(3 credits)

Semester 8: (20 credits)

1. Project or Internship

1. Examination and Evaluation:

EVALUATION PATTERN:

The performance of the learner will be evaluated in two components. The first component will be a Continuous Assessment with a weightage of 40% of total marks per course. The second component will be a Semester end examination with a weightage of 60% of the total marks per course. The allocation of marks for the Continuous Assessment and Semester end Examinations is as shown below:

Details of Continuous Assessment (ICA): 40% of the total marks per course:

Continuous Assessment details: Total 50 Marks

Component 1 (CA -1) Assignment 25marks

Component 2 (CA -2) Class Tests 25 marks

Details of Semester End Examination: 60% of the total marks per course.

Duration of examination will be Three hours. (Total Marks: 100)

Paper Pattern:

Total Five questions will be asked.

Q.1 is compulsory. Solve any THREE from remaining FOUR questions.

Each Question carries 15 marks each.

Note: 15 marks questions can be sub-divided as per the length/ level of difficulty of the question.

EVALUATION PATTERN FOR INTERNAL COMPONENT:

10 MARKS

Q1) Fill in the Blanks (5marks)

Q2) Practical/ Theory / Concept based question (5marks)

Career Paths:

A B. Tech in Digital Forensic opens up a wide range of exciting and in-demand career paths. Here are some of the most trending and promising career options that you can pursue after completing your degree:

- Digital Forensics Analyst
- Cybersecurity Specialist
- Ethical Hacker/Penetration Tester
- Malware Analyst
- IT Security Consultant
- Law Enforcement Digital Forensics Expert
- Cybercrime Investigator
- Information Security Auditor