Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441108
NAAC Accredited with A+ Grade
(An Autonomous Institute Affiliated to RTM Nagpur University, Nagpur)

Programme: B.Tech Second Year (CSE- Data Science)

Semester		Course Code		Course Name	
III		BDS32324		Digital Forensic	
Teaching Scheme		**Examination Scheme (Th)**		**Examination Scheme (P)**	
Theory (Th)	3Hrs/week	**CT-I**	15	-	-
Practical (P)	0	**CT-II**	15	-	-
Total Credits	**4**	**CA**	10	-	-
Duration of ESE: 3 Hrs		**ESE**	60	-	-
		Total Marks	**100**	-	-

Pre-Requisites:

Course Outcomes:

CO1	Understand Digital Forensics fundamentals – principles, methodologies, and best practices for identifying, collecting, and analyzing digital evidence.
CO2	Identify advanced forensic tools – Autopsy, FTK Imager, EnCase.
CO3	Learn Drone Forensics and UAV investigations.
CO4	Examine Mobile Forensics skills by working with storage media using industry-standard tools.
CO5	Discuss Network Forensics and Cybercrime Investigations.

Course Content

Unit I	**Introduction to Digital Forensic** - Definition of Computer Forensics, Cyber Crime, Evolution of Computer Forensics, Objectives of Computer Forensics, Roles of Forensics Investigator, Forensics Readiness, Steps for Forensics Readiness Planning. **Computer Forensic Investigation Process** - Computer Forensics Investigation Process - Assessment Phase, Acquire the Data, Analyze the Data, Report the Investigation
Unit II	**Digital Evidence and First responder Procedure** - Digital Evidence, Digital Evidence Investigation Process, First Responders Toolkit, Issues Facing Computer Forensics. **Types of Investigation** - Types of Investigation, Techniques in digital forensics. **Storage Media** - The Booting Process, LINUX Boot Process, Mac OS Boot Sequence, Windows 10 Booting Sequence.
Unit III	**Windows Forensics** – Introduction to Windows Forensics, Volatile Information, Recovering Deleted Files and Partitions. **Digital Forensics Road Map** – Static Data Acquisition from Windows using FTK Imager, FTK Imager Installation, Kali Linux Installation, RAM Dump Analysis using Volatility, Static Data Acquisition from Linux OS. **Digital Forensics Tools** – Recovering Deleted Files and Partitions, Overview of EnCase Forensics, Deep Information Gathering Tool (Dmitry), Computer Forensics using Autopsy and FTK Imager.
Unit IV	**Introduction to Network Forensics** – Network Components, OSI Internet Layers, Forensic Importance, Tools: Wireshark and TCPDUMP. **Network Analysis and Forensic Tools** – Packet Sniffing and Analysis using Ettercap and Wireshark, Packet Capture using TCPDUMP, Wireshark Packet Analyzer, Website Penetration using WHOIS and nslookup.

Unit V	**Application Password Cracking** – Introduction to Password Cracking, John the Ripper, Rainbow Tables, PDF File Analysis, Remote Imaging using E3 Digital Forensics. **Wireless and Web Attacks** – Wi-Fi Packet Capture and Password Cracking using Aircrack-ng, Web Attacks, Website Copier (HTTrack), SQL Injection, Site Report Generation (Netcraft), Vulnerability Analysis (Nikto), Wayback Machine, Dmitry, Image Metadata Extraction using ImageMagick.
Text Books	
1	Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, John R. Vacca, Charles River Media, 2005.
2	Cyber Law Crimes, Barkhs and U. Rama Mohan, Third Edition, 2017, Asia LawHouse.
3	Drone and UAV Forensics – A Hands-on Approach, Dr. Nitesh Tiwari, Dr. Shekhar Yadav, Dr. V.K. Giri. S.K. Katariya & Sons.
4	Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools, Nipun Jaswal, Packt Publishing Limited.
Reference Books	
1	Mobile Forensics: The Comprehensive Guide to Mobile Forensics (Cyber Crime Forensics Investigator), Vijay Gupta Book, Kindle Edition.
2	Mastering Network Forensics: A practical approach to investigating and defending against network, Nipun Jaswal.
3	Digital Forensic: The Fascinating World of Digital Evidences, Nilakshi Jain (Author), Dhananjay R. Kalbande, Wiley.
Useful Links	
1	Basics of Forensic Science & Criminalistics by Prof. Devasish Bose | Department of Criminology & Forensic Science, https://onlinecourses.swayam2.ac.in/cec25_ge11/preview
2	NPTEL course in Digital Forensics by Dr. Jeetendra Pande, Uttarakhand Open University, Haldwani https://onlinecourses.swayam2.ac.in/nou25_cs19/preview