GUJARAT TECHNOLOGICAL UNIVERSITY

SUBJECT NAME: DIGITAL FORENSICS
SUBJECT CODE: 3715908
M.E. 1st SEMESTER

Type of course: Elective

Prerequisite: Cybercrime and Information warfare, Computer Networks

Rationale:

- Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
- Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
- Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools.
- E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	**Digital Forensics Science:** Forensics science, computer forensics, and digital forensics. **Computer Crime:** Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics	**8**	16%
2	**Cyber Crime Scene Analysis:** Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.	**7**	14%
3	**Evidence Management & Presentation:** Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.	**8**	18%
4	**Computer Forensics:** Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case, **Network Forensics:** open-source security tools for network forensic analysis, requirements for preservation of network data.	**12**	24%

5	**Mobile Forensics:** mobile forensics techniques, mobile forensics tools. **Legal Aspects of Digital Forensics:** IT Act 2000, amendment of IT Act 2008.	**8**	18%
6	Recent trends in mobile forensic technique and methods to search and seizure electronic evidence	**5**	10%
	Total	**48**	100%

Reference Books:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. Dr. Nilakshi Jain and Dr. Dhananjay Kalbande, Digital Forensic, Wiley Press John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

Course Outcome:

After completion of course, students would be able to:

- Understand relevant legislation and codes of ethics
- Computer forensics and digital detective and various processes, policies and procedures
- E-discovery, guidelines and standards, E-evidence, tools and environment.
- Email and web forensics and network forensics

List of Experiments:

1. To study detail working of boot process the operating system (Windows, Linux).
2. To study a case for digital evidence collection, retrieval and presentation of cybercrime incidence.
3. To track the details of the computer in past using Last Activity view tool
4. To perform data recovery of deleted files using Recuva in Windows.
5. To perform password cracking using any password cracking tool.
6. To perform detail inspection of different file formats using Hex editor
7. To perform data extraction from android phone using AFLogical tool.
8. To perform forensics on whatsapp using Whatsapp Extractor.
9. To perform OS Backdoor using set toolkit.
10. To perform Email Spoofing using SMTP servers.

List of Open Source Software/learning website:

Kali Linux, Wireshark, Recuva, Last Activity tool, AFLogical, Whatsapp Extractor, Free Hex Editor