GUJARAT TECHNOLOGICAL UNIVERSITY

Subject Name: Cyber Forensics
Subject Code: 3735101

Semester: III

Type of course: M.E. Computer Engineering (IT systems and Network Security)

Prerequisite:

- Sound Knowledge of Security
- Understanding of Cyber Laws
- Understanding of Different Operating System Management

Rationale: NA

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) ESE	PA (I)	
3	0	2#	4	70	30	30	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	What is Cyber Forensics?	2	4
2	Traditional "post-mortem" forensics	2	4
3	Cyber-crime & Cyber, Taxonomy of Computer Crime scene	2	4
4	Computer Forensics Involves , Preservation, Goals of Forensics Analysis	2	4
5	Cyber forensics Procedures	2	4
6	Forensic duplication	2	4
7	Incident Notification Checklist	2	4
8	Slight diversion	2	4
9	Encoding And Encryption Computer Forensics	2	4
10	Cyber Forensics Tools and Utilities, Forensic Acquisition Utilities (FAU)	2	4
11	Concealment Techniques, Forensic Implications	2	4
12	Digital Forensics Laboratory, Forensics Implications	2	4
13	Privacy and Cyber Forensics	2	6
14	Forensic value and corporate Exposure	2	6
15	Cyber Forensics and the Law, Cyber Forensics and the Investigating Criminal Behaviour	3	6
16	Electrically Stored Information and Cyber Forensics		

Reference Books: - Cyber Forensic Concepts and Approaches, B.Ravi Kumar Jain/ ICFAI, University Press

- CYBER SECURITY**:** Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole, Sunit Bel

Course Outcome:

After learning the course the students should be able to:

- Trace Back the Intrusion/Hacking.
- Investigate the scenario based cases.
- Recovering the Information from Digital media.
- Responding to the Cyber Crime
- Preserving and Creating controlled environment for Digital evidence.

List of Experiments: (with Open Ended Problems)

- Make a disk image using FTK or similar imaging tool.
- Install any hex editor tool and Analyse the metadata of file
- Fetch Windows Registry based artefacts
- Browser Forensics, collect the data related with History, Cache, and User Profiles etc. of any of the Browser and make a report over it.
- Create a RAM memory Dump and analyse with any of the Forensic tool and list down the processes ran by computer in that Dump.
- Hashing the files and analyse if MACB is changed it affect the value of hashing or not?
- Image metadata analysis
- Microsoft office files metadata analysis.
- Event Log interpretation and reporting the incident as per Timeline.
- Perform the mirroring of sample hard disk.
- Perform the creation of encryption of disk and decryption of the disk.
- Perform the taking raw dump image of live system.
- Perform the raw image dup from network.
- Perform the Hex creation and reading the Hex dump of the evidence file.

Major Equipments:

- Access Data FTK toolkit
- Win Hex
- EnCase Toolkit
- VMWare-Workstation
- Linux (Kali/Fedora)
- Network Simulators

List of Open Source Software/learning website:

- DD Toolkit
- Coffee Toolkit
- Data Recovery Toolkit

Review Presentation (RP): The concerned faculty member shall provide the list of peer reviewed Journals and Tier-I and Tier-II Conferences relating to the subject (or relating to the area of thesis for seminar) to the students in the beginning of the semester. The same list will be uploaded on GTU website during the first two weeks of the start of the semester. Every student or a group of students shall critically study 2 papers, integrate the details and make presentation in the last two weeks of the semester. The GTU marks entry portal will allow entry of marks only after uploading of the best 3 presentations. A unique id number will be

generated only after uploading the presentations. Thereafter the entry of marks will be allowed. The best 3 presentations of each college will be uploaded on GTU website