GUJARAT TECHNOLOGICAL UNIVERSITY

COMPUTER ENGINEERING (SYSTEMS & NETWORK SECURITY)(56)
CYBER FORENSICS
SUBJECT CODE: 2745603
M.E. 4TH SEMESTER

Type of course: Major Elective - V

Prerequisite: Basic knowledge of Networking, File Structures, Operating System, Information Security

Rationale:
To understand the major concepts of Cyber Forensics, and to educate the students for learning of how to avoid becoming victims of cyber crimes. The subject and the course content will help to the student who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security and to gain experience of doing independent study and research in the field of cyber security and cyber forensics.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
3	2#	0	4	70	30	30	0	10	10	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	**Introduction to Cyber Forensics:** Definition of Cyber forensics? Its importance in Cyberspace, Relation between Cyber Crime-Cyber Forensics and Cyber Security, Classification of Cyber Forensics, Goals of Cyber Forensics, Forensic Investigation process, Benefits of professional forensic methodology. Case Study: Investigation of any Attack like phishing or stalking.	6	15
2	**Pre-Investigation Assessment :** Preliminary Review of the Scene of offence: Evaluation, Preliminary Interviews, Incident Response, Incident Response Team, Pre-Investigation Technical Assessment	4	10
3	**Standard Operating Procedures for Investigation** Steps for digital crime scene investigation, Evidence Collection Procedures from live systems and Switched-off Systems, Types and Rules of Evidence, Forensic Duplication, Documenting of Evidence, Chain of Custody	6	30
4	**Investigation Tools and Utilities** Drive Imaging, Memory Dump creation and analysis, Data Recovery Tools, and Introduction to Deleted-Hidden-Encrypted file Recovery, Formatted Partition Recovery, Time line analysis of file modification and file access, Recover Temporary Files or Cache Files, Open Source Forensic Tools.	10	25
5	**Building Forensics Laboratory**	4	10

	Laboratory Standards, Evidence Security, Portable Forensics Lab		
6	**Cyber Crime Laws** Cyber Crime and Information Technology Act, Laws/Guidelines relating to International Investigation	4	10

Reference Books:

1. Nina Godbole, Sunit Belapur, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Publications, April, 2011
2. Albert J. Marcella, Jr. Doug Menendez "CYBER FORENSICS: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes", Auerbach Publications
3. Robert Jones, "Internet Forensics: Using Digital Evidence to Solve Computer Crime", O'Reilly Media, October, 2005
4. Cyber Forensics Concepts and Approaches, B. Ravi Kumar Jain/ICFAI, University Press

Course Outcome:
After learning the course the students should be able:

1. Realize the activities carried using forensic technologies in detection of cyber crime.
2. Introduce a novel methodology of performing cyber forensics or system forensics.
3. Assess how the digital evidences will be handled in any crime scene

List of Tutorials:

1. Make a disk image using FTK or similar imaging tool.
2. Install any hex editor tool and Analyze the metadata of file
3. Fetch Windows Registry based artifacts
4. Browser Forensics, collect the data related with History, Cache, User Profiles etc. of any of the Browser and make a report over it.
5. Create a RAM memory Dump and analyze with any of the Forensic tool and list down the processes ran by computer in that Dump.
6. Hashing the files and analyze if MACB is changed it affect the value of hashing or not?
7. Image metadata analysis
8. Microsoft office files metadata analysis.
9. Event Log interpretation and reporting the incident as per Timeline.

Major Equipment: Desktop, Laptop.

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.