GUJARAT TECHNOLOGICAL UNIVERSITY

INFORMATION TECHNOLOGY (23)

DIGITAL FORENSIC

SUBJECT CODE: 272231

SEMESTER: II

Type of course: Elective

Prerequisite: NA

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)		PA (I)	
					PA	ALA	ESE	OEP		
3	2#	2	5	70	20	10	20	10	20	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	**Introduction to Software Forensics** Digital Forensic Definition, Software forensics, Objectives and object of software forensics, Identity, other objects of study, software forensic tools, the process, the products, finally,already,the tools, software forensic technology and practice, Content analysis, non-content analysis, legal considerations, Presentation in court, summary**.**	**6**	20
2	**The Players-Hackers, Crackers, Phreaks and other Doodz** Terminology, types of blackhats, motivation and rationales, general characteristics, blackhat products, other products, summary.	**4**	10
3	**Software code and analysis tools** The programming process,the products, the resulting objects, the analytical tools,forensics tools, summary.	**2**	5
4	**Advanced tools** Decompilation, desquirr, Dcc, Boomerang, Plagiarism, JPlag, YAP, Other approaches, summary.	**2**	10
5	**Law and Ethics-software forensics in court** Legal system, differences within common law,jurisdiction,evidence,types of evidence, rules of evidence, providing expert testimony,ethics,disclosure,blackhat motivation as a defense, summary.	**4**	10
6	**Computer virus and malware concept and background** History of computer virus and worms, malware definition and structure, virus structure, worm structure, Trojan structure, logic bomb structure, remote access Trojan structure, distributed denial of service structure, detection and antidetection techniques, detection technologies, stealth and antidetection measures, summary.	**6**	15
7	**Programming Culture and Indicators** User-interface, cultural features and "help", functions in programming style, program structure, programmer skill and objectives, development	**4**	15

	strictures, technological change. Summary.		
8	**Stylistic analysis and Linguistic Forensics** Biblical criticism, Shakespeare and other literature, individual identification and authentication, content analysis, noncontent analysis, the content/noncontent debate, noncontent matrics as evidence of authorship, additional indicators, summary.	**4**	10
9	**Authorship analysis** Problems, plagiarism detection versus authorship analysis, how can it work? , source code indicators, more general indicators, are it reliable? Summary.	**4**	5

Reference Books:

- Software Forensics by Robert M Slade McGrew Hill Publication

Course Outcome:

After learning the course the students should be able to:

Student will be enabled to learn basics of Software forensics and also securing and analyzing the software malcious content. Will be enabled to learn software forensic tools to digitally viable threats mitigations. Student also will learn structure of malicious code structure such as structure of Virus, trojen horse. Student will use this course for legal & Law and Ethics-software forensics required in court for Cyber crime litigation. Student will also learn Authorship analysis and IPR related terms such as copyright, patent related Problems resultions , plagiarism detection techniques

List of Experiments and Open Ended Problems:

(1) Software Forensic tools such as Drozer,Soot,Valgrind, memcheck
(2) Malware dataset analysis
(3) Malware Payload generation & it's mitigation techniques
(4) Analysing the Anti-malware tools and software against various malware data-set

Major Equipment:

(1) Malware Tools and Malware Libraries

(2) Digital Forensics Tools

List of Open Source Software/learning website:

(1) Drozer

(2) Soot

(3) Squid

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