Faculty of Engineering and Technology
First Year Master of Technology (Cyber Security)
In Effect from Academic Year 2019-20

Subject Code : 1ET2070104	**Subject Title:** Cyber Forensic and Incident Response
Pre-requisite :	Fundamentals of Cryptography and Linux

Course Objective:
The course centers around the techniques for ID, safeguarding, and extraction of electronic proof, evaluating and examination of system and host framework interruptions, examination and documentation of data assembled, and arrangement of master tribute proof. The course will likewise give hands on experience on different scientific apparatuses and assets for framework.

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
				Theory		Practical		
Lecture	Tutorial	Practical	Credit	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	Total
2	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Crime Incident and Incident Response**	**4**	**15**
	Introduction to Crime Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident.		
2	**Initial Response and Forensic Duplication**	**6**	**25**
	Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system - Forensic Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive.		
3	**Storage And Evidence Handling**	**5**	**25**
	File Systems-FAT,NTFS - Forensic Analysis of File Systems - Storage Fundamentals-Storage Layer, Hard Drives Evidence Handling-Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure.		
4	**Network and Internet Forensics**	**3**	**20**
	Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud.		
5	**Systems Investigation And Ethical Issues**	**4**	**15**
	Data Analysis Techniques - Investigating Live Systems (Windows &Unix) - Investigating Hacker Tools - Ethical Issues – Cybercrime.		

Review Presentation: The student is expected to refer at least two peer reviewed journal papers related to this domain/subject. The student is expected to identify issues/challenges and emerging trends in the domain/subject. Student is supposed to explore various video lectures (E.g. NPTEL) available in the domain/subject. Student is required to make a review-presentation on the work carried out for the same.
Recommended sites for journal papers are (1) dl.acm.org (2) springer.com (3) sciencedirect.com (4) elsevier.com (5) ieeexplore.ieee.org (6) scholar.google.co.in (7) scopus.com or others of similar repute.

Course Outcome:
After successful completion of the course, student will be able to:

- Plan and get ready for all phases of an examination - recognition, starting reaction
- Investigate web server attacks, DNS attacks and router attacks and also can learn the importance of evidence handling and storage .
- Monitor network traffic and detect illicit servers and covert channels.

List of References:

1. Kevin Mandia, Chris Prosise, "Incident Response and computer forensics",Tata McGrawHill, 2006.
1. Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999.
2. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001.
3. Skoudis. E., Perlman. R. Counter Hack: "A Step-by-Step Guide to Computer
4. Attacks and Effective Defenses", .Prentice Hall Professional Technical Reference. 2001.
5. Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information From a Computer", Paladin Press, 2000.
6. Bill Nelson,Amelia Philips and Christopher Steuart, "Guide to computer forensics and investigations", course technology, Cengage Learning; 4 thedition, ISBN: 1-435-49883-6, 2009.

E-Resources / Web Links:

- https://nptel.ac.in/courses/106106178/7

List of Experiments:

Note: The experiment list provided beneath is for reference only. The course teacher may change/formulate it as per his/her methodology and requirement.

Practical List

1. Installation of BackTrack Linux and various tools.
2. Installation of Kali Linux and various tools.
3. Exploration of various tools available in Backtrack linux
4. Exploration of various tools available in Kali linux