VII SEMESTER – Skill Oriented Course	L	T	P	C
	1	-	2	2
CYBER SECURITY TOOLS LAB				

Course Objective:

1. To get practical exposure to Cyber Security threats and Forensics tools.

Course Outcomes:

1. Get the skill to identify cyber threats/attacks.
2. Get the knowledge to solve security issues in day-to-day life.
3. Able to use Autopsy tools
4. Perform Memory capture and analysis
5. Demonstrate Network analysis using Network miner tools

List of Experiments:

1. Perform an Experiment for port scanning with nmap
2. Set up a honey pot and monitor the honey pot on the network
3. Install Jscript/Cryptool tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures.
4. Generate minimum 10 passwords of length 12 characters using openSSL command
5. Perform practical approach to implement Foot printing - Gathering target information using Dmitry-Dmagic, UA tester
6. Work with sniffers for monitoring network communication (Wireshark).
7. Using Snort, perform real-time traffic analysis and packet logging.
8. Perform email analysis using the Autopsy tool.
9. Perform Registry analysis and get boot time logging using process monitor tool
10. Perform File type detection using Autopsy tool
11. Perform Memory capture and analysis using FTK imager tool
12. Perform Network analysis using the Network Miner tool

Text Books:

1. Real Digital Forensics for Handheld Devices, E.P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

Reference Books:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C.H. Malin, E. Casey and J.M. Aquilina, Syngress, 2012.