S.No	**TWO CREDIT COURSE - NEED ANALYSIS SHEET**	
1.	**Name of the Course**	14IT2A0 - Malware Analysis
2.	**Name of the Industry**	Symantec, Chennai
3.	**Name of the SIG associated with**	Information Security and Management
4.	**Motivation for offering the course**	In Outcome Based Education (OBE), Information Security and Management SIG has Programme core courses like ***OBE - UG core/elective courses*** In Outcome Based Education (OBE), Information Security and Management SIG has Programme core courses like • *Information Systems (Semester 2)* • *Network Security (Semester 5)* • *Network Management and Security Lab (Semester 5)* • *Information Storage and Management (Semester 6)* Programme Elective courses like • *Information Theory and Coding* • *Computer Forensics* • *Cloud Security* • *Applied Cryptography* • *Ethical Hacking* • *Digital Watermarking and Steganography* *Information Security Auditing and Management* Tools and methodologies used to perform malware analysis on executables found on Windows / Linux systems using hands-on approach has to be introduced to the students

4.1	**Feedback** **(If yes, Details of the feedback as per the annexure I)**	
	From Recruiter	-
	From Employer	-
	From Alumni	-
	From Academic Council members	Yes, Syllabus reviewed and passed in Academic Council Meeting on 30.05.2015
	From Board of Studies members	Yes, Syllabus reviewed and passed in Board of Studies Meeting on 18.04.2015
	From Senior students	Yes
	From current students	-
	From Performance Assessment Committee	-
	From Department Advisory committee	-
4.2	**Faculty participation in Seminar/FDP (If yes, details)**	
	At higher learning institutes	-
	At Industry	Title: Ethical Hacking and Countermeasures Venue: IntelleSecure, Bangalore (5 days training - 15,16,17,23,14 August, 2014), 15-08-2014 to 24-08-2014

5.	**Outcomes expected**	
	Technology transfer	-
	Student Internship	Yes, started working on this proposal
	Placement	-
	Organizing FDP/seminar at TCE	Yes, Workshop on "Ethical Hacking"
	Collaborative research/consultancy projects	-
	Faculty as Trainee/Trainer in the Industry	-
	Joint publications	-
	Setting up of Lab/Infrastructure	Yes, discussing with the expert to enhance the resources in Cyberforensics Lab

Thiagarajar College of Engineering
Department of Information Technology
B.TECH INFORMATION TECHNOLOGY
2016-17 (Even Semester)
Nominal Roll

Sem/Year: VI/III
Sub code/Name: 14IT2A0/Malware Analysis

S.No	Reg.No	Name
1	14IT01	Abinaya G.C
2	14IT02	Aishwarya R
3	14IT04	Akila M
4	14IT06	Akshaya P
5	14IT07	Amala Richu A
6	14IT08	Amirtharaj. R.S
7	14IT09	Antony Rishanth S
8	14IT10	Aparna A
9	14IT11	Aravind Lal. T.S
10	14IT12	Arockia Ajan L
11	14IT13	Ashik Abdul Rahuman P
12	14IT15	Balaji P
13	14IT16	Balakrishnam Nivedha
14	14IT17	Balamurugan M
15	14IT18	Buvaneswari. M
16	14IT20	Deepika R
17	14IT22	Dhanasekaran V
18	14IT23	Dhivya V
19	14IT24	Divyalakshmi J
20	14IT30	Guhanjeeva J
21	14IT32	Hema Iniya B
22	14IT33	Hemasharani A
23	14IT34	Jagannath T
24	14IT41	Karthickkumar R
25	14IT42	Karthickraj P
26	14IT44	Karthikairaja A
27	14IT47	Krishna Veni N
28	14IT49	Malarvizhi K
29	14IT50	Maneksha B
30	14IT55	Meenakshi G
31	14IT56	Mirnalini A
32	14IT57	Muthu S

Thiagarajar College of Engineering
Department of Information Technology
B.TECH INFORMATION TECHNOLOGY
2016-17 (Even Semester)
Nominal Roll

Sem/Year: VI/III
Sub code/Name: 14IT2A0/Malware Analysis

S.No	Reg.No	Name
33	14IT58	Mythili S
34	14IT61	Neethi M.S
35	14IT65	Nithya P
36	14IT66	Nivedita Shree M
37	14IT81	Ramya R
38	14IT84	Reshma Kris M
39	14IT88	Santhini K
40	14IT93	Selva Pradeesha A
41	14IT94	Selvakumar D
42	14IT104	Suryaprakasam M.C
43	14IT105	Sushmitha S
44	14IT119	Divya J
45	14IT120	Goutham M.S
46	14IT121	Jeyasri N
47	14IT122	Karthika P
48	14IT127	Priyachandrika B
49	14IT133	Sindhuja R
50	14IT134	Sugapriya S
51	14IT135	Suriya Priya A

HoD - IT

COURSE SCHEDULE

1	Subject Code	14IT2A0
2	Subject Name	Malware Analysis
3.	Date and Duration of the Programme	March 11,12,25 & 26, 2017 & 4 - Days Programme.
4.	Contents covered in Day 1	**Introduction** Malware – Definition, Types, Goals. Malware Analysis – Definition, Requirements, Essentials, Goals and Objectives. **Dynamic Analysis** PE structure, Tools for malware analysis, Procedure to protect the host, Procedure to analyze a file and giving reputation, Analyze DLL files, Network traffic analysis, Creating YARA rules. **Analyzing Non-PE files** File structures of non-PE file, Importance of non-PE files
5.	Contents covered in Day 2	**Analysing Non-PE files** Tools to analyse non-PE files, Analysis of Microsoft document file, PDF files, Flash files. **Static Analysis** Importance of PE structures, Packers, Compilers, Crypters, Tools for static analysis, Debuggers, Disassemblers, packing and unpacking a malware.
6.	Contents covered in Day 3	**Static Analysis** Introduction to virustotal, Hashing, Need of Antivirus, Working principle of Antivirus, Create signature for a malware to support antivirus. **Web Exploits analysis** Severity of web exploits, Why & How web exploits carried on, Tools to analyse web exploits, Environment setup, Exploit kit analysis, Vulnerabilities used in Exploit kits, Vulnerabilities used to create exploit kits.

7.	Contents covered in Day 4	**Hands-On Practice** FakeAV malware, ZeroAccess Rootkit, Ransomware for trainees, DLL malware samples, Trojan.RATdll file for trainees, Microsoft document file embedded with malware, PDF file embedded with malware, Static analysis of a malware sample (PlugX rat), Web exploits, and YARA rules creation.