J. B. INSTITUTE OF ENGINEERING AND TECHNOLOGY

Course Plan
For
Cmputer Forensics

III B. Tech(CSE)	I SEMESTER	ACADEMIC YEAR	2015-16

M. Ravi
Assistant Professor

WWW.JBIET.EDU.IN

J.B.Institute of Engg & Technology

Department of CSE

Syllabus

Subject Name : Computer forensics Subject Code : 56053

Class : B.Tech III-Isem

Sl.No	Unit No:	Details of the unit
01	**Unit I**	Computer forensics fundamentals: What is Computer forensics
		Use of Computer forensics in law Enforcement
		Computer forensics assistance to Human resources/ employment proceeding
		Computer forensics services
		Benefits of professional forensics methodology
		Steps taken by Computer forensics specialists
		Types of computer forensics technology
		Types of military computer forensics technology
		Types of Law Enforcement of computer forensics technology
		Types of business computer forensics technology
02	**Unit II**	Computer forensics Evidence capture
		Data recovery defined
		Data backup and data recovery
		The role of backup in data recovery
		Data recovery solution
		Evidence collection and data seizure
		Why collection evidence
		Collection options –obstacles
		Types of evidence, the rules of evidence

		Volatile evidence, general procedure
		Collection and archiving, methods of collection, artifacts
		Collection steps, controlling contamination
		The chain of custody
03	**Unit III**	Duplication and preservation of digital evidence
		Preserving the digital crime scene
		Computer evidence processing steps
		Legal aspects of collection and preserving Computer forensics evidence
		Computer image verification and authentication
		Special needs of evidential authentication
		Practical consideration, implementation
04	**Unit IV**	Computer forensics analysis and validation
		Determining what data to collect and analyze
		Validating forensic data, addressing data-hiding techniques
		Performing remote acquisitions
		Network forensics overview
		Performing the live acquisitions
		Developing the standard procedure for Network forensics, Using network tools
		Examining the honey net project
05	**Unit V**	Processing crime and incident scene
		Identifying digital evidence, collecting evidence in private sector incident scenes
		Processing law enforcement crime scene, preparing for research
		Securing the computer incident or crime scene
		Seizing digital evidence at the scene, storing digital evidence , obtaining a digital hash , reviewing a case
06	**Unit VI**	Current computer forensic tools
		Evaluating computer forensic tool needs, computer forensic software tools
		computer forensic hardware tools
		Validating and testing forensic soft wares
07	**Unit VII**	E-mail investigations , exploring the role of email investigation
		Exploring the role of client and server , investigating email crimes and violations
		Understanding email servers , using specialized email forensic tools

		Cell phone and mobile device forensics
		Understanding mobile device forensics
		Understanding acquisition procedure for cell phones and mobile devices
08	**Unit VIII**	Working with windows and dos systems
		Understanding file systems
		Exploring ms file structure
		Examining NTFS disks
		Understanding whole disk encryption
		Windows registry
		MS startup tasks
		MS dos startup tasks
		Virtual machines

Guidelines to Students

Where will this subject help?

.

Books / Material

Text Books (TB)

TB1: Computer forensics, computer crime investigation by john R Vacca.

TB2: Computer forensics and investigation by Nelson, Philips enfinger.

Suggested / Reference Books (RB)

RB1: Real digital forensics

RB2: Forensic compiling

RB3: Computer evidence collection and presentation.

J.B.Institute of Engg & Technology

Department of CSE

SUBJECT PLAN :

Subject Name : **Computer forensics** Subject Code : 56053

Class :B.Tech III-Isem Faculty Name : M.Ravi

Number of Hours / lectures available in this Semester / Year	

Unit	Topic	Total No. of Hours
I	Computer forensics fundamentals: What is Computer forensics	
	Use of Computer forensics in law Enforcement	
	Computer forensics assistance to Human resources/ employment proceeding	
	Computer forensics services	
	Benefits of professional forensics methodology	
	Steps taken by Computer forensics specialists	
	Types of computer forensics technology	
	Types of military computer forensics technology	
	Types of Law Enforcement of computer forensics technology	
	Types of business computer forensics technology	
II	Computer forensics Evidence capture	
	Data recovery defined ,Data backup and data recovery	
	The role of backup in data recovery, Data recovery solution	
	Evidence collection and data seizure	
	Why collection evidence, Collection options –obstacles	
	Types of evidence, the rules of evidence	

	Volatile evidence, general procedure	
	Collection and archiving, methods of collection, artifacts	
	Collection steps, controlling contamination	
	The chain of custody	
III	Duplication and preservation of digital evidence	
	Preserving the digital crime scene	
	Computer evidence processing steps	
	Legal aspects of collection and preserving Computer forensics evidence	
	Computer image verification and authentication	
	Special needs of evidential authentication	
	Practical consideration, implementation	
IV	Computer forensics analysis and validation	
	Determining what data to collect and analyze	
	Validating forensic data, addressing data-hiding techniques	
	Performing remote acquisitions	
	Network forensics overview	
	Performing the live acquisitions	
	Developing the standard procedure for Network forensics, Using network tools	
	Examining the honey net project	
V	Processing crime and incident scene	
	Identifying digital evidence, collecting evidence in private sector incident scenes	
	Processing law enforcement crime scene, preparing for research	
	Securing the computer incident or crime scene	
	Seizing digital evidence at the scene, storing digital evidence , obtaining a digital hash , reviewing a case	
VI	Current computer forensic tools	
	Evaluating computer forensic tool needs, computer forensic software tools	
	computer forensic hardware tools	
	Validating and testing forensic soft wares	
VII	E-mail investigations , exploring the role of email investigation	
	Exploring the role of client and server , investigating email crimes and violations	
	Understanding email servers , using specialized email forensic tools	
	Cell phone and mobile device forensics	
	Understanding mobile device forensics	
	Understanding acquisition procedure for cell phones and mobile devices	

VIII	Working with windows and dos systems	
	Understanding file systems	
	Exploring ms file structure	
	Examining NTFS disks	
	Understanding whole disk encryption	
	Windows registry	
	MS startup tasks, MS dos startup tasks	
	Virtual machines	

J.B.Institute of Engg & Technology

Department of CSE

LESSON PLAN :

Subject Name : **Computer forensics** Subject Code : 56053

Class : B.Tech III-Isem Faculty Name : M.Ravi

Unit I : COMPUTER FORENSIC FUNDAMENTALS

LEARNING OBJECTIVES: Deals with Fundamentals of Computer Forensic and Types in technology.

LECTURE PLAN:

Total no_ of classes: 11

Unit #	**Topic as per JNTU syllabus**	**Lesson #**	**Suggested Books ** (Refer the list**	**Question Bank**			**Hand outs**
				OQ	DQ	AQ	
Unit I	Computer forensics fundamentals	1	TB-1	1	1	A1	H1
	What is Computer forensics	1	TB-1		1		
	Use of Computer forensics in law Enforcement	1	TB-1				
	Computer forensics assistance to Human resources/ employment proceeding	1	TB-1				
	Computer forensics services	1	TB-1				
	Benefits of professional forensics methodology	1	TB-1				
	Steps taken by Computer forensics specialists	1	TB-1				

	Types of computer forensics technology	1	TB-1		2		
	Types of military computer forensics technology	1	TB-1				
	Types of Law Enforcement of computer forensics technology	1	TB-1				
	Types of business computer forensics technology	1	TB-1				

OBJECTIVE QUESTIONS :

1.

2.

DESCRIPTIVE QUESTIONS :

1.

2.

ASSIGNMENT QUESTIONS:

1. What is Computer forensics?
2. Explain types of Computer forensics technologies?

UNIT-II : COMPUTER FORENSIC EVIDENCE AND CAPTURE.

LEARNING OBJECTIVES: Deals with collection of Evidence and data seizure.

LECTURE PLAN:

Total No_ of Classes: 13

S.No	Name of the Topic	Reference book code	No. of classes required
1	Computer forensics Evidence and capture	TB-1	1
2	Data recovery defined	TB-1	1
3	Data backup and data recovery	TB-1	1
4	The role of backup in data recovery	TB-1	1
5	Data recovery solution	TB-1	1
6	Evidence collection and data seizure	TB-1	1
7	Why collection evidence	TB-1	1
8	Collection options –obstacles	TB-1	1

9	Types of evidence, the rules of evidence	TB-1	1
10	Volatile evidence, general procedure	TB-1	1
11	Collection and archiving, methods of collection, artifacts	TB-1	1
12	Collection steps, controlling contamination	TB-1	1
13	The chain of custody	TB-1	1

OBJECTIVE QUESTIONS :

1.
2.

DESCRIPTIVE QUESTIONS :

1.
2.

ASSIGNMENT QUESTIONS:

1. Explain Computer forensics Evidence and capture?
2. Describe types and rules of evidence?

UNIT-III : DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE

LEARNING OBJECTIVES: which deals about how to collect evidence and verification,authentication.

LECTURE PLAN:

Total No_ of Classes: 10

S.No	Name of the Topic	Text/Reference book code	No. of classes required
1	Duplication and preservation of digital evidence	TB-1	1
2	Preserving the digital crime scene	TB-1	1
3	Computer evidence processing steps	TB-1	1
4	Legal aspects of collection and preserving Computer forensics evidence	TB-1	2
5	Computer image verification and authentication	TB-1	2
6	Special needs of evidential authentication	TB-1	2
7	Practical consideration, implementation	TB-1	1

OBJECTIVE QUESTIONS :

1.
2.

DESCRIPTIVE QUESTIONS :
1.
2.

ASSIGNMENT QUESTIONS:
1. In Detail Legal aspects of collection and preserving Computer forensics evidence?
2. What is Image Verification and Authentication?

UNIT-IV : COMPUTER FORENSICS ANALYSIS AND VALIDATION

- **LEARNING OBJECTIVES:** Deals with data validation and network forensics.

LECTURE PLAN:
Total No_ of Classes: 10

S.No	Name of the Topic	Text/Reference book code	No. of classes required
1	Computer forensics analysis and validation		1
2	Determining what data to collect and analyze		1
3	Validating forensic data, addressing data-hiding techniques		2
4	Performing remote acquisitions		1
5	Network forensics overview		1
6	Performing the live acquisitions		1
7	Developing the standard procedure for Network forensics, Using network tools		2
8	Examining the honey net project		1

OBJECTIVE QUESTIONS :

1.
2.

DESCRIPTIVE QUESTIONS :
1.
2.

ASSIGNMENT QUESTIONS:
1. Write a short notes on Validating forensic data, addressing data-hiding techniques?
2. Give an overview on Network forensics?

UNIT-V: PROCESSING CRIME AND INCIDENT SCENES

- ❖ **LEARNING OBJECTIVES:** Deals with collecting and identifying digital evidence

LECTURE PLAN:
Total No_ of Classes: 08

S.No	**Name of the Topic**	**Text/Reference book code**	**No. of classes required**
1	Processing crime and incident scene	TB2	1
2	Identifying digital evidence, collecting evidence in private sector incident scenes	TB2	2
3	Processing law enforcement crime scene, preparing for research	TB2	1
4	Securing the computer incident or crime scene	TB2	1
5	Seizing digital evidence at the scene, storing digital evidence	TB2	2
6	obtaining a digital hash , reviewing a case	TB2	1

OBJECTIVE QUESTIONS :
1.
2.

DESCRIPTIVE QUESTIONS :

1.
2.

ASSIGNMENT QUESTIONS:
1. How to identify Digital Evidence?
2. Explain about Seizing digital evidence at the scene?

UNIT-VI: CURRENT COMPUTER FORENSIC TOOLS

- ❖ **LEARNING OBJECTIVES:** Learns about what are the tools needed for computer forensic.

LECTURE PLAN:
Total No_ of Classes: 06

S.No	**Name of the Topic**	**Text/Reference book code**	**No. of Lecture classes required**
1	Current computer forensic tools	TB-2	1
2	Evaluating computer forensic tool needs, computer forensic software tools	TB-2	2
3	computer forensic hardware tools	TB-2	1
4	Validating and testing forensic soft wares	TB-2	2

OBJECTIVE QUESTIONS :
1.
2.

DESCRIPTIVE QUESTIONS :
1.
2.

ASSIGNMENT QUESTIONS:
1. Give a brief note on different tools?
2. Validating and testing forensic soft wares?

UNIT-VII: E-MAIL INVESTIGATIONS

- ❖ **LEARNING OBJECTIVES: D**eals with E-mail investigations.

LECTURE PLAN:
Total No_ of Classes: 08

S.No	Name of the Topic	Text/Reference book code	No. of classes required
1	E-mail investigations , exploring the role of email investigation	TB-2	1
2	Exploring the role of client and server , investigating email crimes and violations	TB-2	2
3	Understanding email servers , using specialized email forensic tools	TB-2	2
4	Cell phone and mobile device forensics	TB-2	1
5	Understanding mobile device forensics	TB-2	1
6	Understanding acquisition procedure for cell phones and mobile devices	TB-2	1

OBJECTIVE QUESTIONS :

1.
2.

DESCRIPTIVE QUESTIONS :

1.
2.

ASSIGNMENT QUESTIONS:

1. Explain the role of email investigation
2. Give deatil notes on Cell phone and mobile device forensics?

UNIT VIII: WORKING WITH WINDOWS AND DOS SYSTEMS

- ❖ **LEARNING OBJECTIVES:** Learns about the working with Windows and DOS System.

LECTURE PLAN:
Total No_ of Classes: 10

S.No	Name of the Topic	Text/Reference book code	No. of classes required
1	Working with windows and dos systems	TB-2	2
2	Understanding file systems	TB-2	1
3	Exploring ms file structure	TB-2	1
4	Examining NTFS disks	TB-2	1
5	Understanding whole disk encryption	TB-2	1
6	Windows registry	TB-2	1
7	MS startup tasks	TB-2	1
8	MS dos startup tasks	TB-2	1

9	Virtual machines	TB-2	1

OBJECTIVE QUESTIONS :

1.

2.

DESCRIPTIVE QUESTIONS :

1.

2.

ASSIGNMENT QUESTIONS:

1. Explain Working with windows and dos systems?

2. Examine NTFS disks?

DEPARTMENT OF CSE

INDIVIDUAL TIME TABLE

NAME OF THE FACULTY*:*

Period	1	2	3	4		5	6	7
Day/Time	9.10-10.00	10.00-10.50	10.50-11.40	11.40-12.30	L U N C H	01.00-1.50	1.5 0-2.40	2.40-3.30
Mon								
Tue								
Wed								
Thu								
Fri								
Sat								

Name of the Subject:

Total no of theory classes :

Total no of practical classes :

Total no of classes :

J. B.Institue of Engineering & Techology
Batch/I SEM (I-MID DESCRIPTIVE)
BRANCH: CSE
SUB:

TIME: 60 MINUTES **Marks: 10**

SECTION-A & B

Answer any TWO of the following: **(2x5=10M)**

1. xxxxxxxxxxxxxxx

a) xxxxxxxxxxxx

b) xxxxxxxxxxx
c) xxxxxxxxxxxxxxxxxx

2. xxxxxxxxxxxxxxxxxx
    a) xxxxxxxxxxxxxxxx
    b) xxxxxxxxxxxxxxx
    c) xxxxxxxxxxxxx

3. xxxxxxxxxxxxxxxxxxx?

4. xxxxxxxxxxxxxxxs? xxxxx?

Marks for Internal Theory Examination

ROLL.NO	NAME OF THE STUDENT	I MID (Des+Obj+Assign))	II MID Des+Obj+Assign))

Computer forensics: QUESTION BANK 1 (Descriptive)-DQ1

1) What is Computer forensics?
2) Explain types of Computer forensics technologies?
3) Explain Computer forensics Evidence and capture?
4) What is Image Verification and Authentication?

Computer forensics: QUESTION BANK 2 (Objective)-OQ1

1. When handling computers for legal purposes, investigators increasingly are faced with four main types of problems, except:

A. How to recover data from computers while preserving evidential integrity
B. How to keep your data and information safe from theft or accidental loss
C. How to securely store and handle recovered data
D. How to find the significant information in a large volume of data
E. How to present the information to a court of law and to defense during disclosure

2. In order for a double tier approach to work it is necessary to have:

A. A defined methodology
B. Civil control
C. A breach of contract
D. Asset recovery
E. Tort, including negligence

3. Criteria for equipment in the double tier approach results in the following except:

A. Simple to use
B. Quick to learn
C. Totally reliable
D. Robust and durable
E. Legally operable

4. A computer forensics specialist is the person responsible for doing computer forensics. The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system. These results in the following steps except:

A. Protects the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction

B. Discovers all files on the subject system. This includes existing normal files, Deleted yet remaining files, hidden files, password-protected files, and encrypted files

C. Recovers all (or as much as possible) of discovered deleted files

D. Reconstructs system failure

E. Reveals (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system