| Department of Information Technology | | LP: Sub Code<br>Rev. No: 00<br>Date: 12.11.2019 |
|---|---|---|
| ~~B.E~~/B.Tech/~~M.E/M.Tech~~ : IT | Regulation: 2016 | |
| PG Specialisation : -- | | |
| Sub. Code / Sub. Name : IT16013 / Cyber Forensics | | |
| Unit : I | | |

**Unit Syllabus: INTRODUCTION**
The Scope of Computer Forensics - Windows Operating and File Systems –Handling Computer Hardware – Anatomy of Digital Investigation.

**Objective:**
Students will understand the fundamentals of Computer Forensics and computing Investigations.

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 1 | The Scope of Computer Forensics – Introduction – Types of Computer Forensics Evidence Recovered – What skills must a computer Forensics Investigator Possess? | 2- Ch 1; pg 1-11 | BB/LCD |
| 2 | The importance of computer forensics – A History of computer forensics – Training and Education | 2- Ch 1; pg 12-24 | BB/LCD |
| 3 | Windows Operating and File Systems – Physical and Logical Storage – File Conversion and Numbering Formats – Operating Systems | 2- Ch 2; pg 32- 49 | BB/LCD |
| 4 | Windows Registry – Microsoft Windows features | 2- Ch 2; pg 50- 72 | BB/LCD |
| 5 | Handling Computer Hardware – Hard Disk Drives – Cloning a PATA or SATA Hard disk | 2- Ch 3; pg 80- 92 | BB/LCD |
| 6 | Removable memory | 2- Ch 3; pg 93- 108 | BB/LCD |
| 7 | Anatomy of Digital Investigation – A Basic Model for Investigators | 1- Ch 1; pg 1 -8 | BB/LCD |
| 8 | Understanding the scope of the Investigation | 1- Ch 1; pg 8 -13 | BB/LCD |
| 9 | The Art of Documentation | 1- Ch 1; pg 13 -20 | BB/LCD |
| **Content beyond syllabus covered (if any):** | | | |

* Session duration: 50 minutes

Sub. Code / Sub. Name: IT16013 / Cyber Forensics

Unit : II

**Unit Syllabus : INVESTIGATIVE SMART PRACTICES**

Forensics Investigative Smart Practices –Time and Forensics –Incident closure

**Objective:** Students will understand the fundamentals of Computer Forensics and computing Investigations.

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 10 | Forensics Investigative Smart Practices - The Forensic process – | 3- Ch 10; pg | LCD |
| 11 | Forensic Investigative smart practices - Time | 3- Ch 10; pg | LCD |
| 12 | Time and Forensics - What is time? - Network Time Protocol – Timestamp data – Keeping track of time | 3- Ch 11; pg | LCD |
| 13 | Clock models and time bounding: The foundations of Forensic time – MS-DOS 32 -bit Timestamp: Date and Time | 3- Ch 11; pg | LCD |
| 14 | Date Determination – Time Determination – Time Inaccuracy | 3- Ch 11; pg | LCD |
| 15 | Incident closure – Forensic Investigative smart practices | 3- Ch 12; pg | LCD |
| 16 | Investigation – Communicative Findings Characteristics of a good Cyber forensic report contents | 3- Ch 12; pg | LCD |
| 17 | Retention and Curation of Evidence | 3- Ch 12; pg | LCD |
| 18 | Investigation Wrap – up and Conclusion Investigator's role as an expert witness summary | 3- Ch 12; pg | LCD |
| **Content beyond syllabus covered (if any):** | | | |

* Session duration: 50 mins

Sub. Code / Sub. Name: IT16013 / Cyber Forensics

Unit : III

**Unit Syllabus :**

## LAWS AND PRIVACY CONCERNS

Laws Affecting Forensic Investigations –Search Warrants and Subpoenas–Legislated Privacy Concerns –The admissibility of Evidence –First Response and Digital Investigator

**Ob**jecti**ve:** Students will recognize the legal underpinnings and critical laws affecting forensics.

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 19 | Laws Affecting Forensic Investigations – Constitutional Implications – of Forensic Investigation – The right to privacy – The expert witness - | 1- Ch 2; pg 23 -31 | LCD |
| 20 | Search Warrants and Subpoenas – Distinguishing between warrants and Subpoenas – What is a search and when is it legal? - basic elements of obtaining a warrant | 1- Ch 3; pg 35- 42 | LCD |
| 21 | The plain view doctrine – The Warrantless search - Subpoenas | 1- Ch 3; pg 43- 50 | LCD |
| 22 | Legislated Privacy Concerns – General Privacy – Financial Legislation | 1- Ch 4; pg 55 - 61 | LCD |
| 23 | Privacy in Health Care Education – Privileged Information | 1- Ch 4; pg 62 - 66 | LCD |
| 24 | The admissibility of Evidence – What makes evidence admissible? – keeping evidence authentic | 1- Ch 5; pg 71- 83 | LCD |
| 25 | Defining the scope of the search – when the constitution doesn't apply | 1- Ch 5; pg 84- 88 | LCD |
| 26 | First Response and Digital Investigator-Forensics and Computer Science – Controlling the scene of the crime | 1- Ch 5; pg 91- 99 | LCD |
| 27 | Handling evidence | 1- Ch 5; pg 100-108 | LCD |
| **Content beyond syllabus covered (if any):** | | | |

* Session duration: 50 mins

Sub. Code / Sub. Name: IT16013 / Cyber Forensics
Unit : IV

**Unit Syllabus : DATA ACQUISITION AND REPORT WRITING**

Data Acquisition –Finding Lost Files –Document Analysis –Case Management and Report Writing –Building a Forensics Workstation.

**Objective:** Students will recognize the legal underpinnings and critical laws affecting forensics.

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 28 | Data Acquisition- Order of Volatility – Memory and Running Processes – Acquiring media | 1- Ch 7; pg 111- 127 | LCD |
| 29 | Finding Lost files- File recovery | 1- Ch 8; pg 131- 141 | LCD |
| 30 | The deleted file – data carving | 1- Ch 8; pg 141- 148 | LCD |
| 31 | Document Analysis – File identification – understanding metadata | 1- Ch 9; pg 151- 171 | LCD |
| 32 | Mining the temporary files – identifying alternate hiding places of data | 1- Ch 9; pg 172-182 | LCD |
| 33 | Case Management and Report Writing – Managing a case – | 1- Ch 17; pg 379-388 | LCD |
| 34 | Writing reports | 1- Ch 17; pg 389-392 | LCD |
| 35 | Building a Forensics Workstation– What is a forensic workstation? – Commercially available forensic workstations | 1- Ch 19; pg 423-428 | LCD |
| 36 | Building a Forensics Workstation from scratch | 1- Ch 19; pg 429-239 | LCD |

**Content beyond syllabus covered (if any):**

* Session duration: 50 mins

Sub. Code / Sub. Name: IT16013 / Cyber Forensics

Unit :V

**Unit Syllabus : TOOLS AND CASE STUDIES**

Tools of the Digital Investigator-Licensing and Certification –Case Studies: E-mail Forensics –Web Forensics –Searching the Network –Excavating a Cloud –Mobile device Forensics.

**Objective:** Students will apply the tools and methods to uncover hidden information in digital systems.
Students will learn about current licensing and certification requirements to build the career in digital forensic.

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 37 | Tools of the Digital Investigator – Software tools – Working with "Court-Approved" tools | 1- Ch 18; pg 395-412 | LCD |
| 38 | Hardware tools – nontechnical tools | 1- Ch 18; pg 413-420 | LCD |
| 39 | Licensing and Certification – Digital Forensic Certification- Vendor – Neutral Certification Programs - Vendor – Neutral Specific Programs – Digital Forensic Licensing Requirements | 1- Ch 20; pg 441-453 | LCD |
| 40 | Case Studies: E-mail Forensics – Email technology – Information Stores – the Anatomy of an E-mail – An approach to Email analysis | 1- Ch 10; pg 185-209 | LCD |
| 41 | Web Forensics –Internet Addresses – Web browsers – Web servers – Proxy servers | 1- Ch 11; pg 213-242 | LCD |
| 42 | Searching the Network- An eagle's eye view – Initial response – Proactive collection of evidence – Post – incident Collection of evidence – Router and switch forensics | 1- Ch 12; pg 247-274 | LCD |
| 43 | Excavating a Cloud - What is cloud computing? – Shaping the cloud – the implications of cloud forensics – on virtualization – Constitutional issues | 1- Ch 13; pg 277-302 | LCD |
| 44 | Mobile device Forensics – Challenges of mobile device forensics – how cell phone works – data storage on cell phones | 1- Ch 14; pg 307-316 | LCD |
| 45 | Acquisition and storage –legal aspects of mobile device forensics | 1- Ch 14; pg 317-323 | LCD |
| **Content beyond syllabus covered (if any):** | | | |

* Session duration: 50 mins

Sub Code / Sub Name: IT16013 / Cyber Forensics

**TEXT BOOKS:**

1. Michael Graves, —Digital Archaeology: The Art and Science of Digital Forensics, Addison-Wesley Professional, 2014.
2. Darren R. Hayes, —Practical Guide to Computer Forensics Investigation, Pearson, 2015.

**REFERENCES:**

3. Albert J. Marcella and Frederic Guillossou, —Cyber Forensics: From Data to Digital Evidence,Wiley, 2015.
4. Bill Nelson, Amelia Phillips and Christopher Steuart, —Guide to Computer Forensics

| | Prepared by | Approved by |
|---|---|---|
| Signature | | |
| Name/ | Dr G.SUMATHI<br>KIRUBA WESLEY | Dr.V.VIDHYA |
| Designation | Assistant Professor | HOD-IT i/c |
| Date | 12/11/19 | 12/11/19 |
| Remarks *: | | |
| Remarks *: | | |

* If the same lesson plan is followed in the subsequent semester/year it should be mentioned and signed by the Faculty and the HOD