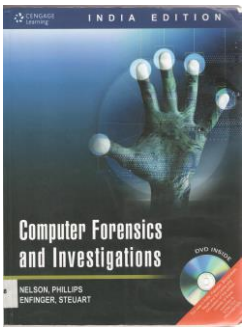
# Birla Institute of Technology & Science, Pilani
# Hyderabad Campus

Department of Computer Science and Information Systems

Sumer Term 2014-2015 Course Handout (Part II)

**Date**: 22nd May 2015

In addition to part-I (General handout for all courses appended to the timetable) this portion gives further specific details regarding the course:




**COURSE NO. : CS F404**
**Room: G203 (M/T/W/Th 4th hr)**

## Computer Crime and Forensics

**Instructor In-Charge**: **Chittaranjan Hota (hota@hyderabad.bits-pilani.ac.in)**

### Scope and Objectives:

Computer crimes include a wide range of crimes like network administrators hacking into the computers of current or former employees, major credit-card theft, drug trafficking, money laundering, e-mail harassment, fraud rings, and cyber terrorism etc. Computer crimes are generally handled using preventive and detective techniques. Computer crime detection is generally known as computer forensics whereas computer crime prevention is done by using computer and network security mechanisms. Computer forensics is the process of identification, seizure, acquisition, authentication, analysis, documentation and storage of digital evidence involved in computer crimes. With the dramatic rise in computer crimes in recent times using PCs, mobile devices, networks, and other peripheral devices, the demand for computer forensics experts have also risen. In this course, we will start with examining few Computer Crimes in India and abroad in recent times. Then we will discuss storage formats for digital evidence, best acquisition method, processing crime and incident scenes, understanding registry files, startup tasks, virtual machines etc. We will also discuss what data to collect and analyze, performing remote acquisitions, network forensics, e-mail investigations, and mobile device forensics. The course will also include experiments or labs like Make evidence tags and logs; Seize a computer (lockdown lab); Cloning a disk; Recovering, Analyzing, and Documenting Digital Evidence etc. Tools like ProDiscover Basic, WinHex, Registry viewer and FTK Imager, DiskExplorer etc. will be used to get a hands-on on the concepts covered in this course.

### TEXT BOOK

[T1] Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009.

### REFERENCE BOOKS

[R1] Angus M.Marshall, Digital forensics: Digital evidence in criminal investigation, John –Wiley and Sons, 2008.

[R2] Debra Littlejohn Shinder, Michael Cross, Scene of the Cybercrime**:** Computer Forensics Handbook, 2nd Edition, Syngress Publishing, Elsevier, 2008.

[R3] Chuck Easttom, and Det.Jeff Taylor, Computer crime, Investigation, and the Law, Course Technology (Cengage Learning), 2011.

[R4] Warren G. Kruse, Jay G. Heiser, Computer forensics: Incident Response Essentials, AW, 2001.

[R5] Eoghan Casey, Digital evidence and Computer crime, 3rd edition, Academic Press, 2011.

[R6] Kevin Mandia, Chris Prosise, Matt Pepe,, Incident Response and Computer Forensics, Tata McGraw Hill, 2006.

**PLAN OF STUDY:**

| Sl. No. | TOPIC | CHAPTER Ref | Lect.s |
|---|---|---|---|
| 1. | Introduction to Computer Crime: Identity theft, Cyber Stalking, etc. | R3(Ch.1) | 1 |
| 2. | Understanding Computer Forensics. | T1(Ch.1) | 1 |
| 3. | Conducting an Investigation and Completing the case. | T1 (Ch.2) | 1 |
| 4. | Review of Computer Networks: Hardware and Software. | Class notes | 2 |
| 5. | Working with Windows and DOS: Microsoft file structure, NTFS disks. | T1(Ch.6) | 1 |
| 6. | Working with Windows and DOS: Disk encryption, Windows registry, Startup tasks, and Virtual machines. | T1(Ch.6) | 1 |
| 7. | Linux boot processes and disk structures. | T1(Ch.8) | 1 |
| 8. | Data acquisition: Determining best acquisition method, Using acquisition tools, Validating data acquisitions. | T1(Ch.4) | 2 |
| 9. | Identifying digital evidence, securing a crime scene, storing digital evidence, and obtaining a digital hash. | T1(Ch.5) | 2 |
| 10. | Computer Forensics Tools: Software tools, ProDiscover, EnCase, FTK, Open source tools, etc. | T1(Ch7) | 2 |
| 11. | Addressing data hiding techniques. | T1(Ch.9) | 1 |
| 12. | Performing remote acquisitions. | T1(Ch.9) | 1 |
| 13. | Recognizing Graphics files, Understanding data compression. | T1(Ch.10) | 2 |
| 14. | Network forensics overview, Performing live acquisitions. | T1(Ch.11) | 1 |
| 15. | Exploring the Role of E-mail, and Chats in Investigations. | T1(Ch.12) | 1 |
| 16. | Investigating E-mail crimes and violations, Password cracking, using E-mail forensics tools. | T1(Ch.12) | 2 |
| 17. | Understanding Mobile device forensics. | T1(Ch.13) | 1 |
| 18. | Guidelines for Report writing, Generating Report findings with forensics software tools. | T1(Ch.14) | 1 |
| 19. | Advanced topics: Forensics in Embedded systems, and Critical infrastructures (Smart grids, distributed forensics). | Class notes | 1 |

**EVALUATION SCHEME**:

| Sl. No. | Component & Nature | Duration | Weightage | Date and Time |
|---|---|---|---|---|
| 1. | Assignments (take home) | * | 20% | * |
| 2. | Test I (Closed Book) | 1hr | 20% | 10/06/2015 (11.00 to 12.00 n) |
| 3. | Test II (Closed Book) | 1hr | 20% | 27/06/2015 (11.00 to 12.00n) |
| 4. | Compre. Exam (Part Open) | 3 hrs | 40% | 15/07/2015 (F106) |

**Note:** All course notices will be displayed on the Computer Sc. Dept. Notice Board.
**Chamber Consultation Hour**: Would be announced in the class.

**Instructor-In-Charge**