

# Cyber Forensics

**Lecture and Demonstration:** 10 Days

**Daily Classes** : 02 Hours

## 1. Introduction to Cyber Forensics

- What is Cyber Forensics
- Scope of Cyber Forensics
- Chain of Custody
- Expert Witness
- Ethics for Experts
- Evidence Storage

## 2. Investigation Basics

- Corporate Investigation vs Legal Investigation
- Why Corporate Investigation?
- Preparing for Investigation
- Validating data Under Linux
- Validating Data Under Windows

## 3. Memory Investigation

- Image Acquisition
- Evidence Analysis
- Evidence Analysis
- Data Recovery & Analysis
- Last Activity View

## 4. Network Investigation

- Internet History Analysis
- Network Acquisition
- Packet Analysis
- Evidence Hunt

## 5. Mobile Investigation (Santoku)

- Santoku Overview
- Android Rooting
- Image Acquisition
- Mobile Memory Analysis
- Evidence

## 6. Facebook Investigation

- Crimes on Facebook
- Information Gathering
- Facebook Log Request
- Evidence Collection

## 7. Whatsapp Forensics

- Introduction to End to End Encryption
- Whatsapp Memory Acquisition
- Recovering all Deleted Conversations
- Evidence Collection

## 8. Reporting

## 9. Practice & Doubts Sessions