

# Incident Response and Computer Forensics Workshop



NII  
Consulting

www.niiconsulting.com

## ➤ About the course

The term cyber-crime no longer refers only to hackers and other external attackers. With the ever increasing importance of computers in our daily life there is an exponential rise in the rate of computer crime such as, financial frauds, unauthorized access, employee misuse, identity theft, etc. Each and every case of fraud involves a very strong element of computer-based evidence.

NII Consulting has been providing professional computer forensics services to clients for the past four years. It now brings together its consolidated expertise into a three-day hands-on workshop on **Incident Response and Computer Forensics (IRCF)**.

The entire workshop is driven by hands-on exercises and case studies to ensure that all aspects have a real-life scenario-based approach.

## ➤ Key Benefits

This program addresses the key questions of:

- ❑ What should one do when there is a suspicion of a computer-based crime?
- ❑ What tools and techniques are most likely to yield the right set of clues?
- ❑ How should the investigation be carried out such that it can be presented in a court of law?



Each person will be provided with fully-configured laptops with all the tools and test images loaded onto it

- ❑ Hands-on practice with the worlds' leading forensics tool - Encase
- ❑ Helps you prepare for the SANS GCFA and EC-Council's CHF1
- ❑ Become a NII Certified Forensics Professional (NCFP)

## ➤ Who should attend?

- Auditors and financial fraud examiners
- Chief Security Officers and Chief Technology Officers
- Professionals seeking a career in computer forensics and cyber crime investigations
- Security and Network Administrators

## ➤ Course Outline

### Day I: Computer Crime - Case Studies

#### Threat Scenarios

Hacking Incidents  
Financial Theft  
Theft of Identity  
Corporate Espionage  
Email Misuse  
Pornography

#### Introduction to Incident Response and Computer Forensics

Pre- Incident Preparation  
Detection of Incidents  
Initial response phase  
Response Strategy Formulation  
Evidence Collection and analysis

- Defining Evidence
- Forensically sound evidence collection
- Evidence Handling
- Host Vs Network-based evidence
- Online Vs Offline Response

#### Digital Forensics - Putting on the Gloves

- The 6 A's

- The Investigative Guidelines
- Disk-based Forensics Vs Network-based Forensics

Reporting the Investigation

## Introduction to Network Forensics

Network Devices

Introduction to Log Analysis

Analyzing Snort and Firewall Logs

Analyzing Apache, IIS, Squid Logs

Using Tcpdump, Snort, Tcpdstat, argus, tcpflow, tcptrace

## Day II: Evidence Collection

### Introduction to Live response

The Do's and the Don'ts

Windows Live Response

Linux Live Response using LINReS

### Data Acquisition/Disk Imaging

Learning the rope - the essentials

Risk Imaging using Linux ( dd, sdd, dcfldd) and Netcat

Disk Imaging using Encase, Helix Bootable disk

### Forensic Analysis of the Evidence

Computer Intrusion case study - Windows Box 0w3nd

Computer Intrusion case study - Linux Box 0w3nd

Case Studies Continue

## Day III: Forensics Analysis Continued

### Internet misuse - Browser Forensics

Understanding Browser history artifacts

Using WebHistorian

Using Netanalysis

### Digging deep into the cyber world - Email and Website tracing

Using SmartWhois

Using Neotrace

### Windows Registry Forensics

Understanding Registry structure

Understanding MRU lists

Understanding UserAssist

## Malicious Binary Analysis

Using IDA freeware

Using strings.exe

Using BinText

Using Regmon, Tcpmon

Using Peid

## Documenting the Investigation

A peek into the Indian Cyber Law

Closing discussion

### Tools Used

- Encase Forensic edition
- Helix Bootable CD
- The SleuthKit and Autopsy Browser
- The Coroner's Toolkit
- Tcpdump
- Snort
- Tcpdstat
- Argus
- Tcpflow
- Tcptrace
- Ethereal
- Neotrace
- Smartwhois
- Peid
- NetAnalysis
- Web Historian
- Bintext
- IDA freeware

### Workshop Facilitator

**Chetan Gupta** GCFA, CIW Certified Security Analyst

Chetan Gupta has varied experience in the field of Information Security with a focus on the niche area of Digital Forensics. He is

well-versed with the Incident response and Computer Forensics standards and methodology, has a good understanding of the Indian Cyber law & has handled forensics cases of many multinational clients.

Chetan is a SANS GIAC Certified Forensics Analyst (GCFA).

Chetan has also been an invited speaker at the Cyber Safety Week, Bombay Chartered Accountants Society, and many other academic institutes & has presented on topics related to Incident Response, Computer Forensics, and Digital Forensics & Cyber Crime.

He has published articles in [ForensicFocus](#) and the NII Computer Forensics e-zine [Checkmate!](#)

#### ↳ Course Fee

**INR 15,000/- per participant**

*Fee includes Tuition, Refreshments, Lunch, Course Materials and Certificate.*

#### ↳ Schedule & Venue

**24<sup>th</sup> -26<sup>th</sup> August 2006**

**Time: 10:00 - 18:00 hours**

Residency Hotel, Suren Road, Andheri(E),  
Mumbai - 400 093.

#### ↳ Enquiries

All enquiries can be directed to:

**Benifer Lewis**

**Tel:** +91 22 4005 2628 / +91 22 2839 2628

**Email:** [benifer.lewis@niiconsulting.com](mailto:benifer.lewis@niiconsulting.com)

#### ↳ Registration & Payment

Workshop enrolment will only be confirmed upon the receipt of the completed registration form and payment. For assurance of availability, your registration will have to reach us 1 week prior to the workshop. All cheques must be made payable to:

**Network Intelligence India Pvt. Ltd.**

Upon receipt of the cheque, a confirmation note stating workshop details will be sent to the participants by email.

#### ↳ About NII Consulting

NII Consulting is an information security consulting firm. We offer services such as Security Assessments, Information Risk Management, Regulatory Compliance, Security Implementation, Forensics, and Training. Some of our clients include the UN World Food Programme, Capgemini Ernst & Young, Dubai Financial Markets, Saudi Telecom, Reliance Mutual Fund, Prudential ICICI, Tata Interactive Services, and many others. For more details on the services that we offer visit:

<http://www.niiconsulting.com/services.html>

NII also has its proprietary security auditing software, AuditPro™ which does a comprehensive policy-based assessment of Windows, Unix, Oracle, MS SQL and Cisco routers.



**N I I**  
**Consulting**

[www.niiconsulting.com](http://www.niiconsulting.com)