

Incident Response and Digital Forensics Workshop



↘ About the course

The term cyber-crime no longer refers only to hackers and other external attackers. Almost all every case of financial fraud or employee misuse 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 Digital Forensics (IRDF)**.

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



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 CHFI
- 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 Digital Forensics

Defining the Forensics Process

Digital Forensics Essentials - Learning the ropes

The 6 A's –

- Assessment
- Acquisition
- Authentication
- Analysis
- Articulation
- Archival

Preserving “Chain of Custody”

Investigative Guidelines

Disk-based Forensics vs. Network-based Forensics

Analysis of the Indian IT Act 2000

Disk-based Forensics - Data Acquisition and Analysis Case Study

Forensically sound evidence collection

Imaging using **Encase®** and **Helix®**
Conducting Physical And Logical Analysis
Recovering Deleted Files

Day II

Real-Life Scenarios - System-based Forensics

System Intrusion case study - Windows Box
0w3nd

Computer Intrusion case study - Linux Box
0w3nd

Deconstructing rootkits

Reverse Engineering unknown binaries and bots

Internet misuse case study - Browser Forensics

Day III

Real-Life Scenarios - Network-based Forensics

Network Intrusion – Web Server Hacked
Network Intrusion – Denial of Service Attack
Network Intrusion – ex-employee mischief
Digging deep into the cyber world - Email Tracing case study

Forensics for PDA and hand-held devices

Defeating anti-forensic measures – disk wiping, formatting, hiding partitions, anonymizers, etc.

Documenting the Investigation

Closing discussion

Read our e-zine on Computer Forensics –
Checkmate!

<http://www.niiconsulting.com/checkmate>

Visit us at www.niiconsulting.com

↘ Workshop Facilitators

K. K. Mookhey CISA, CISSP

K.K. Mookhey is the Founder and Principal Consultant of NII Consulting, a leading provider of information security services and solutions. KK has provided security consulting services to industry leaders across various segments all over the world - including the US, Middle East and the Asia Pacific region.

He has been a speaker at many leading security conferences. He has presented at BlackHat USA 2004, Network+Interop 2005 & many other conferences

His workshops on Database Security and other related topics such as Windows, Unix, Oracle and MS SQL Server Security, Ethical Hacking, Intrusion Detection/Analysis and Incident Handling have been attended by many delegates including HSBC, Citigroup, BNP Paribas, Pfizer, Reserve Bank of India, and many others.

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.

↘ 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.

↘ Schedule & Venue

2nd-4th March 2006

Time: 1000 – 1800 hours

The Mirador, New Link Chakala, Andheri (E),
Mumbai - 400 099.

↘ Enquiries

All enquiries can be directed to:

Benifer Lewis

Tel: +91 22 5620 2628 / +91 22 2839 2628

Mobile: + 91 98671 80193

Email: benifer@nii.co.in

↘ 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.