

*"The Incident Response & Computer Forensics workshop was excellent"*

**Manish Patil**  
 Manager, Information Security  
 Oracle India

*"The Incident Response & Computer Forensics workshop was perfect and excellent"*

**Meenakshi Sundaram**  
 Tech Specialist (Risk & Compliance)  
 Wipro Technologies

## ▾ About the course

The CHFI course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law. The best tools used in the forensic trade will be taught during this course, including software, hardware and specialized techniques. It is no longer a matter of "will your organization be compromised (hacked)?" but, rather, "when?" If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

## ▾ Program Benefits

1. What should one do when there is a suspicion of a computer-based crime?
2. What tools and techniques are most likely to yield the right set of clues?

3. How should the investigation be carried out such that it can be presented in a court of law?
4. Full one day Hands-on practice with the world's leading forensics tool - Encase Forensic Edition 5.04



Each trainee will be provided with fully-configured machines with all the tools and test images loaded into them.

5. Helps you prepare for EC-Council's CHFI and SANS GCFA
6. Participants can appear for the CHFI certification exams and are required to pass the online Prometric tests.
7. Become an NII Certified Forensics Professional (NCFP)

## ▾ Who should attend?

- Police and other law enforcement personnel
- Defense and Military personnel, e-Business Security professionals, Systems administrators
- Legal professionals, Banking, Insurance and other professionals, Government agencies
- IT Managers/Auditors and financial fraud examiners
- Chief Security Officers and Chief Technology Officers
- Students and Professionals seeking a career in computer forensics and cyber crime investigations
- Security and Network Administrators

## 📄 Course Outline

### DAY 1

1. Computer Forensics in Today's World
2. Law and Computer Forensics
3. Computer Investigation Process
4. First Responder Procedure
5. CSIRT
6. Computer Forensic Lab
7. Understanding File Systems and Hard Disks
8. Understanding Digital Media Devices

### DAY 2

1. Windows, Linux and Macintosh Boot Processes
2. Windows Forensics
3. Linux Forensics
4. Data Acquisition and Duplication
5. Computer Forensic Tools
  - ☞ Part I- Software Forensics Tools
  - ☞ Part II- Hardware Forensics Tools

### DAY 3

1. Forensics Investigations Using Encase
2. Recovering Deleted Files and Deleted partitions
  - ☞ Part I: Recovering Deleted Files
  - ☞ Part II: Recovering Deleted Partitions
3. Image Files Forensics
4. Steganography
5. Application Password Crackers
6. Network Forensics and Investigating Logs

### DAY 4

1. Investigating Network Traffic
2. Investigating Wireless Attacks
3. Investigating Web Attacks
4. Router Forensics
5. Investigating DoS Attacks
6. Investigating Internet Crimes
7. Tracking E-mails and Investigating E-mail Crimes

### DAY 5

1. Investigating Corporate Espionage
2. Investigating Trademark and Copyright Infringement
3. Investigating sexual harassment incidents
4. Investigating Child Pornography
5. PDA Forensics
6. iPod Forensics
7. Blackberry Forensics
8. Investigative Reports
9. Becoming an Expert Witness
10. Closing Discussions

## 📄 Tools Used

- Encase Forensic edition
- Helix Bootable CD
- The SleuthKit and Autopsy Browser
- The Coroner's Toolkit
- Tcpdump
- Snort
- Tcpsstat
- Argus
- Tcpflow
- Tcpsrc
- Ethereal
- Neotrace
- Smartwhois
- Peid
- NetAnalysis
- Web Historian
- Bintext
- IDA freeware
- FTK- Forensic Toolkit
- Email Recovery Tools
- Data Recovery Tools
- Password Recovery Tools
- Registry Analyzing Tool
- Hard Disk Write Protection Tools
- Plagiarism Detection Tool
- Mail Detective Tools

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

## ↘ Workshop Facilitator

### KUSH WADHWA

Encase Certified Examiner (EnCE),  
Certified Computer Examiner (CCE),  
Certified Ethical Hacker (CEH),  
Red Hat Certified Engineer (RHCE),  
B.E. (Electronics & Communications)

Kush Wadhwa is an experienced professional in the field of Information Security focused on the niche area of Digital Forensics. He is an acclaimed expert in Incident Response and Computer Forensics standards and methodology having handled projects related to forensics cases of many multinational clients. He has carried out many digital forensics projects related to financial frauds, child pornography, company policy violation, data mining, keyword searching. He has also executed many projects in the areas of penetration testing, System and Server Audits, Intrusion Detection, Mail Servers setup (Qmail), and iptables implementation.

He has also published many articles for NII's Computer Forensics blog [Checkmate](#) and has also authored articles on Digital Forensics tools. He has also created an open source tool for Linux Incident Response called LINReS (LINReS is a Live Response script designed to run on suspect / compromised Linux systems)

Kush is an Information Security Analyst with NII Consulting.

## ↘ Course Fee

Fee is INR 32,000/- per participant inclusive of meals and training material.

*The fee includes training material and handouts, working lunch and refreshments on all training days. This program is non-residential. Service Tax Regn No.: ST/MUM/DIV-III/STC/167/06*

*PAN: AGOPJ4732E*

## ↘ Schedule & Venue

Duration: 5 Days. 20<sup>th</sup> Aug - 24<sup>th</sup> Aug 2007

Venue: Suba Galaxy, Andheri East

Timings: 10:00 am to 6:00 pm

## ↘ Enquiries

All enquiries can be directed to:

**Ketan Shah**

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

*Mobile: +91 9322 580 963*

*Email: [ketan.shah@niiconsulting.com](mailto:ketan.shah@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 10 days 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 their clients include the UN World Food Programme, Capgemini, 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>