Cyber Forensics: Introduction & First Responder

Omveer Singh, GCFA
Additional Director
(In-charge, Cyber Forensics Lab)

Cyber Forensics Lab
Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications & Information Technology
Government of India
New Delhi

Agenda

- Introduction
- Definition
- Categorisation
- Process of Investigation
- Computer Forensic Analysis
- Legal Issues
- First Responder
- 1st Responder's Toolkit
- References

Computer Forensics?

Most of the times, criminal leave some clues, traces or trail at the crime scene, which is searched by the investigator as the evidence to prove one's involvement.

In a case of cyber crime, the evidence being searched is not a bloodstain, a fingerprint, a weapon, a tool or a tool mark. Here the evidence is in digital form (0s & 1s; bits & bytes; files & folders).

a “trail” of electronic fingerprints ...

Sequence of relevant bits & bytes of data (may be hidden too) from the associated computer, called files, are searched and identified.

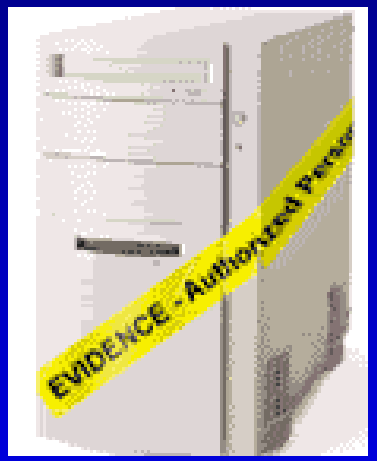
Investigator / Analyst analyse association of these files to the crime and link them together to reconstruct the chain of events

Computer Forensics …

- is seizing of evidence during or after a crime
  - to reconstruct the criminal's actions
  - to provide evidence for prosecution
- Forensic investigation of a cyber crime, carried out using a computer connected to internet, is complex and depends on the evidence found

Computer Forensics …

is the process of applying logical & analytical techniques to computers, networks, digital devices & files to discover or recover admissible evidence.



Computer Forensics ..

Computer Forensics is not just investigation of computers, it is essentially about:

- Correct process of investigation
  - Follow the rules of evidence
  - Imaging & integrity of evidence
  - Analyse the image of evidence
  - Clear and concise reporting of factual information
- Provision of expert testimony

Computer Forensics …

- Computer forensics is the integration of the assessment, identification, seizure, preservation, imaging, analysis of digital evidence to find the related data and/or the root cause of the incident / crime.
- Evidence is required for prosecution in a wide range of computer crimes and misuses
- Multiple methods of
  - Discovering data on computer system
  - Recovering deleted, encrypted, or damaged file information
  - Monitoring live activity
  - Detecting violations of corporate policy
- Information collected may assist in arrests, prosecution, termination of employment, and preventing future illegal activity

Computer Forensics …

- What constitutes a Digital Evidence?
  - Any information, subjected to human intervention or not, that can be extracted from a computer or data processing device.
  - Should be in human-readable format or be capable of being interpreted by a person with expertise in the subject.
- Examples of Forensic Investigation of Computers
  - To recover deleted emails
  - To investigate a suspected system for post employment termination
  - To recover evidence from a formatted hard disk
  - To investigate a suspected system, used by multiple users; e.g. cyber cafe

Cyber Forensics

- **Computer Forensics**
- Mobile Forensics

Subcategories of Computer Forensic Analysis

- Storage Media Analysis
  - Examining storage media for evidence
- Source Code Analysis
  - Software Source Code Examination
- Network Analysis
  - Scrutinize network traffic and logs

Storage Media Forensics

- Storage Media Forensics is the process of acquiring and analyzing the data stored in any form in a physical storage media.
  - includes recovery of hidden/ deleted data/ files
- Windows Registry Analysis

Source Code Forensics

- To analyse Software Source Code for malicious signatures
- To determine software ownership or software liability issues.
  - Review of actual source code.
  - Examination of the entire s/w development process, e.g., architecture, design, development strategy, modules, integration of modules, testing; review of documentation and source code revisions.

Network Forensics

- Network forensics is the process of analysing network traffic
  - After-the-fact analysis of transaction logs
  - Real-time analysis via network traffic capturing / monitoring
    - Sniffers
    - Real-time tracing
- Scrutinising network traffic and logs to identify and locate the suspicious system
- Log Analysis
- Web Access Analysis
- e-mail Analysis

Legal Authority

- Legal authority must be available with the First Responder / Investigation Officer to identify & seize the suspected system or digital device for imaging & analysis of the digital evidence.
  - Search warrant
  - Authorisation to seize the evidence
  - Two (min.) independent witnesses
    - To sign Evidence Seizure Note

Computer Forensics is not "Hacking"

Stick to the evidence left on the hard disk, and you should be on safe legal ground. Provided you have proper consent to search the hard drive.

Consent

- Who can provide consent for a search?
  - Spouse, Parent, Business owner / partner
- Get it in Writing
  - Affidavits as per format

Affidavit

Affidavit by _____ for the Consent given to search a personal computer.

Undersigned appeared personally before the Auth Commissioner and duly sworn as follows:

1. I, _____ Son of _____ am a resident of _____ _____ _____ _____
2. I have hired Mr./Ms. _____ of M/s _____, <City>, to conduct a computer forensics examination of a hard disk from a personal computer, which is in my possession.
3. I have consented to a search by Mr. _____ of all data contained on the hard drive.
4. I attest that the computer hard disk which I have consented to have searched is material property; to which I have had unrestricted access.
5. I acknowledge that I have been informed that state and federal laws require Mr. _____ to notify law enforcement authorities of any suspected child pornography or evidence of criminal activity found on a computer during his examination.

DEPONENT

Computer Forensic Investigations: 2 Roles

- First Responder
  - record the crime site scene
  - collect volatile evidence
  - seize system / hard disk, etc
  - image the hard disk (?)
  - contain intrusion (if any)
  - preserve, protect, pack, seal the evidence
  - send to lab for analysis
- Computer Forensic Analyst (Investigator) of Digital Evidence

Role of a First Responder

- Essentially the first person noticing and reacting to the cyber security incident / cyber crime
- Responsibilities:
  - Determine the severity of the incident
  - Collect as much information about the incident as possible
  - Document all the findings
  - Share this collected information to determine the root cause

Duties of First Responder

To coordinate with –

- Law Enforcement Agencies (Police)
- Suspected User(s), Witnesses, System Admin, Management
- Forensic Investigator
- Court of Law

Valuable information through user interview

- System configuration
- S/w applications, tools installed
- Encryption ?
  - Methodology, tools used & key
- Login id(s) & password(s)

First Responder's Toolkit

- Log Book
  - To record all actions /events with date & time chronologically
- Safe Boot CD / USB
  - Forensic Live CD (e.g. Helix)
- Digital camera
- S/w Tools for
  - Volatile data collection
  - Imaging the hard disk, etc
  - System H/w & S/w configuration details

Tools ...

- Laptop (Forensic Workstation)
- RJ-45 Crossed LAN cable
- Multi-purpose mechanical toolset to open CPU Cabinet and detach Hard Disk (multi screw driver set, etc)
- Anti-static covers
- Air bubbled PVC covers
- Marking labels with permanent ink marking pen

First Responder's Log Book

- Timeline of events
- Entries with date & time during collection of evidence
- Who is performing the seizure / forensic acquisition of digital evidence?
- History of executed forensic tools and commands
- Generated output from forensic tools & commands
- Date & time of executed tools & commands
- Expected system changes or effects due to use of tools

General Tasks at Crime Site by First Responder

- Photograph the crime scene along with the suspected system
- Photograph the suspected systems front & rear view
- Document the system details, as available; e.g. Make, model, S. No., Inventory No. of CPU Cabinet; if these details are on a metallic plate, then photograph (zoomed) it
- When CPU cabinet is opened, photograph the inside view closely

General Tasks at Crime Site by First Responder

- Photograph hard drive connectivity to mother board, document its interface
- On detaching the hard drive, photograph it closely showing readable view of hard drive details
- Document hard drive details in Log Book and Evidence Seizure Note
- Document the professional level and area of expertise of suspected users

Common Mistakes ?
by First Responder

- Shutting down, rebooting or switching off-
- Not recording H/w configuration details from -
- Not recording OS, S/w Applications installation details from -
- Not documenting the data (digital evidence) collection process from –

the suspicious computer system

Cyber Forensic Investigation Process

- Identification
- Seizure / Acquisition
  - Imaging
  - Integrity verification
- Analysis
- Documentation
  - Report preparation

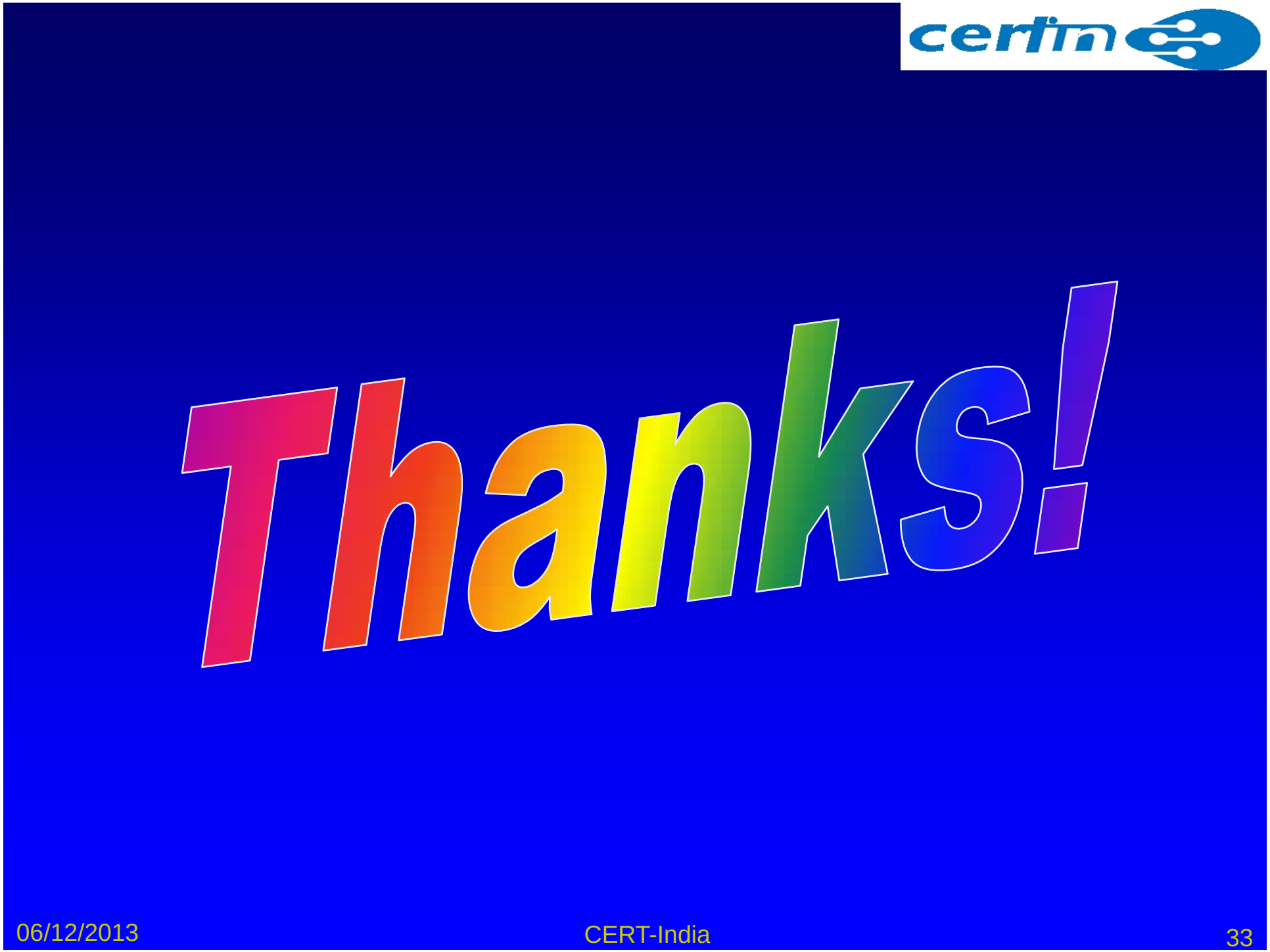
References

- “Electronic Fingerprints – computer evidence comes of Age” by Michael R. Anderson
- “Electronic Crime Scene Investigation – A Guide for First Responders” by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- “Forensic Examination of Digital Evidence : A guide for Law Enforcement” by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- “Forensics – Tools”; http://www.forinsect.de/index.html
- Training Material on Information Security by Carnegie Mellon University, Pitsburgh, USA

References (contd..)

- Collecting Electronic Evidence After a System Compromise" by Matthew Braid, SANS Security Essentials.
- "Computer Forensics – An Overview" by Dorothy A. Lunn, SANS Institute; http://www.giac.org/practical/gsec/Dorothy_Lunn_GSEC.pdf
- "Manual for Investigation of Computer Related Crimes" by Ashok Dohare
- Course Contents : SANS SEC508

Questions?


Thanks!