

Computer Forensics – Basics, First Responder, Collection of Evidence

Omveer Singh

Joint Director / Scientist ‘D’

omveer@cert-in.org.in

Indian Computer Emergency Response Team (CERT-In)

Department of Information Technology

Ministry of Communications & Information Technology

Government of India

New Delhi

Agenda

- Computer Forensics
- First Responder
- Computer Forensics Tools
- Volatile data collection
- Digital Evidence Handling at Crime Site
 - Best Practices & Guidelines
- Disk Imaging
- References

Some Cyber Crimes

- Bank Accounts / Demat Accounts with online transaction facility – login user id & password compromised
- Payment Card (credit / debit / ATM / Prepaid Smart) frauds
- Net Extortion
- Phishing
- Vishing
- Nigerian Advance Fee Scam : “4-1-9” Fraud
- Lottery Advance Scams
- Money laundering and unlawful Banking transactions.

Computer as the instrument of crime

The processes of the computer and not the contents of computer files, facilitate the crime.

- Fraudulent use of automated teller machine (ATM) cards and accounts
- Theft of money from accrual, conversion, or transfer account
- Credit card frauds
- Fraud from computer transactions (stock transfers, sales, or billings) and
- Telecommunications fraud.

Cyber Forensics

- **Computer Forensics**
- Network Forensics
- Mobile Forensics

Subcategories of Cyber Forensic Analysis

- Media Analysis
 - Examining physical media for evidence
- Code Analysis
 - Review of software for malicious signatures
- Network Analysis
 - Scrutinize network traffic and logs to identify and locate the suspicious system

Computer Forensics – why?

- Some of the common practices may destroy digital evidence. Direct analysis will make it **unacceptable** in a court of law - tempered evidence

Digital Evidence is -

- Latent, like fingerprints or DNA
- Extremely fragile & resilient, can be altered, damaged or destroyed easily
- Can transcend borders with ease & speed (networked systems)

Computer Forensics : Definition

Computer Forensics is the use of scientifically derived, proven and legally acceptable methods towards the identification, seizure, preservation, retrieval, validation, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources and processed electronically for the purpose of facilitating the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations.

Computer Forensics

- Analysis of evidence is carried out virtually at any physical location (lab).
- Search for some direct information from the evidence that may have significance in the case.
- Computer Forensics traditionally rely upon the data inadvertently left on disk by the SW application programs / tools.

Computer Forensics - Objectives

- To identify the digital evidence (should be acceptable in a court of law)
- To investigate and analyse the digital evidence & find the relevant data / documents
- To reconstruct the chain of events
- To identify the computer & user responsible for the crime.

Computer Forensics - Process

For investigation of Financial frauds, we do the following:

- **Identify**
- **Collect**
- Authenticate
- **Preserve**
- **Analyse**
- Interpret

the digital evidence and **document** the findings for preparing the report and reconstruct the chain of events

Computer Forensics – Myths & Realities



- Myth :
 - Investigation can identify the person, who carried out the cyber crime.
- Reality :
 - No, investigation will only identify the system & user-id through which the cyber crime was performed.
- Solution :
 - Follow security policy strictly(Login id & Password)
 - Have physical access controls
 - Have video recording & monitoring facility for the systems with critical importance

Computer Forensic Investigation – 2 roles

- First Responder
 - record the site scene
 - collect volatile evidence
 - image the disks (non volatile evidence)
 - contain intrusion
 - protect
 - preserve
 - transport for analysis
- Digital Evidence Computer Forensics Examiner (Investigator)

Duties of First Responder

To coordinate with –

- Law enforcement Agencies (Police)
- Organisation, management
- Forensic Investigator
- Court of Law

First Responder's Toolkit

- Log Book
 - To record all actions /events with date & time chronologically
- Safe Boot CD / Floppy
- Digital camera (or cellphone with digicam)
- Tools for
 - Imaging of media (non volatile data collection)
 - Volatile data collection

Documentation – Incident Profile

- How was the incident detected?
- What is the scenario of the incident?
- What time did the incident occur?
- Who or what reported the incident?
- What hardware & software are involved?
- Who are contacts for the involved personnel?
- How critical is the suspicious computer?

First Responder's Log Book

- Timeline of events
- Audit trail during collection of evidence
- Who is performing the forensic collection?
- History of executed forensic tools and commands
- Generated output from forensic tools & commands
- Date & time of executed commands & tools
- Expected system changes or effects due to use of tools

Computer Forensically Sound

Manners :

- Date & time of all the systems on LAN should be synchronised with the standard local time & internet time server.
- System users should not be given privilege / right to modify date & time.

Tools for -



- Volatile data collection
- Non-volatile data (digital evidence) collection
- Listing running Software / processes on system
- Imaging the Digital Evidence
- Checking the integrity of Digital Evidence
- Analysis of Digital Evidence's Image
- Network configuration details
- System Hardware configuration details
- User's details
- Analysis of Log Files
- Discovery / Cracking of Passwords

Digital Evidence - Types

- **Volatile storage / Non-persistent data**

Memory that loses its contents when the power is turned off. RAM (except the CMOS RAM used for the BIOS) contents are volatile.

- **Non-volatile storage / Persistent data**

data stored on tape or disk (magnetic / optical storage), ROM; no change in contents, if power turned off.

Volatile Digital Evidence

(may be in main memory)

Order of Volatility :

1. Registers & Cache
2. Routing tables
3. ARP Cache
4. Process Table
5. Kernel statistics & modules
6. Main memory (RAM)
7. Temporary System files
8. Secondary Memory
9. Router Configuration
10. Network Topology

Volatile Data Collection Tools

- systeminfo.exe (win): system profile
- psinfo.exe (dos) : sw installed
- cat (linux) : system profile
- uname (linux) : machine's profile
- Psuptime (win) : system uptime info
- Net statistics (win) : system uptime info
- Uptime, w (linux) : user uptime info

Tools for Running Processes

- Netstat -ab : process & pid info
- Listdlls.exe <process> : cmd line & dll(s)
- Pslist <process> : duration of process
- Pslist -me <process> : virtual memory usage
- Pulist : active processes (running)
- Pmdump : active process memory dump

Tools for Running Processes

- Task Manager (Win)
- Process Explorer (Sysinternals)
- ps (Linux)

Check for rogue processes ?

Svchost1.exe

Svch0st.exe

Some useful Tools

- Msconfig
- Autoruns, autorunsc
- Ls (linux)
- Chkconfig -- list (linux)
- Inittab (linux) : run level
- Netusers
- PsLoggedOn (win) : local/remote logged users

Tools for network user details

- Net user : local / remote users
- NTLast <session> : login attempts logs
- Who -all : all local+remote logged users
- Last : history of logged on users
- Lastlog : last login time
- Cat /etc/passwd : user a/c info

Tools for HW Config'n

- Fport (win) : open ports
- Netstat -anb (win) : TCP/IP connections
- Net share (win) : network shares
- Netstat -anp (linux)
- Ifconfig (linux) : NIC config'n
- Netstat -r (win) : routing info'n
- Arp -a : IP Addr, MAC Addr of NIC
- Netstat -rn (linux) : routing info'n

At the Computer Crime Site - 1

- Seize the suspected system
- Label all the connecting cables and have photographs of the suspected system, its connectivity & crime site
- Identify the Evidence & Authenticate it through 32/64 bit Hash (CRC, MD5 checksum)
- Consult with the case investigator
- Interact with SA, users & employees
- Explore the remote storage locations
- Explore all the potential digital evidences
- Capture accurate bit image of the seized Hard Disks (org. evidence)

At the Computer Crime Site - 2

- Explore the e-mail accounts / addresses, e-mail aliases, network configuration & users, system logs, ISP, user ids & passwords
- Record OS (Ver.), System date & time (also difference, if any), H/w & S/w Configuration, IP / MAC address
- Power off the Computer System by pulling the power cable
- Never shutdown system before collecting volatile evidence
- Proceed the data collection from volatile to non-volatile evidence
- Never run any application on the suspected system
- Record the chain of custody in the log register
- To preserve, always keep the org. evidence in a magnetically shielded evidence storage bag

At the Computer Crime Site - 3

- To preserve, always keep the org. evidence in a magnetically shielded evidence storage bag
- Securely pack the Evidence & transport it to lab
- Never work on the original evidence
- Always record all the actions & investigative activities chronologically in Log Book
- Maintain the integrity of original evidence by its minimum handling
- Transfer the suspected Computer System & org. evidence to a sealed & secure location
- “Best Practices for Seizing Electronic Evidence Ver. 2.0” may be downloaded from -

<http://www.fletc.gov/training/programs/legal-division/continuing-legal-education-training-program-cletp/cletp-downloads/bestpractices.pdf>

Collection – Places to look for Electronic Evidence

- Floppy Disks
- Hard Disk(s)
- CDs
- DVDs
- Zip Drives
- Backup Tapes
- USB Storage
- PDAs
- Flash Drives
- Voice mail
- Electronic Calendars
- Scanner
- Photocopier
- Fax/Phone/Cellular
- iPods
- Cellphone

Supplementary Evidence at the crime site

- ❑ Portable / Removable Storage Media
 - Relevant files
 - Relevant deleted files
 - Log files from other systems/servers
- ❑ Record the -
 - Testimonial Evidence by a witness
 - Hearsay Evidence by a indirect witness

Relevant data may be recovered from ...

- Email messages
(deleted ones also)
- Office files
- Deleted files of all kinds
- Encrypted Files
- Compressed Files
- Temp files
- Recycle Bin
- Web history
- Cache files
- Cookies
- Registry
- Unallocated Space
- Slack Space
- Network Server files:
 - System history files
 - Web log files

File Slack Space

- RAM slack (blue) and file slack (red)



- File is green

Digital Evidence Handling :

Some Guidelines

- Trust none - Verify all & everything
- Never rely on a single tool. Use multiple tools to cross-validate the results
- Follow the organisation's Security Policy
- Always backup the discovered information
- Never exceed your knowledge
- Always remember that you are required to testify in a court of law
- Ensure that your actions are repeatable

Digital Evidence

It is always ensured that the digital evidence is :

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable

(called '5 Rules')

Disk (digital evidence) Imaging

- Integrity & security of the org. evidence
- Bit by bit copy; no change in the sequence & location of data – exact replica, but may stored in a different type of media
- Usually done by copying sector by sector
- Forensically sound copy of org. of the evidence
- Above means – swap file, unallocated space & file slack is also copied
- Time consuming process

Disk Imaging Tools

- dd (linux)
- dd (win)
- SafeBack (win)
- SnapBack DatArrest
- Drive Image Pro
- R-Drive Image
- FTK's built-in feature

It is better to use HW imaging equipments

Disk Imaging

Linux - Creating a disk images :

```
#dd if=/dev/sda1 of=usbdrive.img
```

Demonstration

DOS - Creating a disk images :

```
C:\>dd if=\\.\G: of=C:\GDrive.img --progress
```

Demonstration

Integrity of Evidence

Proof of Integrity of the digital evidence image -

Tool : md5sum.exe

(win, linux)

> md5sum <filename>

Demonstration

Processing Evidence from Computer Crime Site

- Start the Lab Evidence Log
- Mathematically authenticate the Data
- Generate Bit stream backup (image) of all crime scene computer hard drives & media
- Proceed with the Forensic Examination

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>
- “Collecting Electronic Evidence After a System Compromise” by Matthew Braid, SANS Security Essentials.

References (contd..)

- “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
- HoneyNet Project Website –
Computer Forensics Challenges