

# Network Forensics



**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

- Cyber Forensics
- Digital Evidence & Investigation Process
- Network Forensics
- Network Forensics Analysis Tools (NFAT)
- N/w Traffic Capturing & Analysis
- Digital Evidence Imaging, Analysis
- Computer Forensics Tools & Toolkits
- Log Files Analysis
- Internet & Email Analysis
- Anti-Forensics
- References

# Cyber Forensics

- The art of gathering evidence during or after a crime
  - Reconstructing the criminal's actions
  - Providing evidence for prosecution
- Forensics for computer networks is ***extremely*** difficult and depends completely on the quality of information you maintain

# Cyber Forensics

- Computer Forensics
- Mobile Forensics

## Handling the digital evidence

- Handle the original evidence as little as possible to avoid changing the data.
- Establish and maintain the chain of custody.
- Documenting everything that has been done.
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.

# Forensic Examination Process of Digital Evidence

- Acquisition
  - Imaging & Authentication
- Analysis
- Interpretation
- Presentation

## 4 Steps of Computer Forensics

- Acquisition
  - Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices
- Analysis
  - This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites

## 4 Steps of Computer Forensics

- Interpretation
  - Evaluating the information/data recovered to determine if and how it could be used against the suspect for employment termination or prosecution in court
- Presentation
  - This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technical staff/management, and suitable as evidence in a court of law

## Subcategories of Computer Forensic Analysis

- **Storage Media Analysis**
  - Examining storage media for evidence
- **Source Code Analysis**
  - Software Source Code Examination for malicious signatures
- **Network Analysis**
  - **Scrutinize network traffic and logs to identify and locate the suspicious system**

## Storage Media Forensics

- Storage Media Forensics is the process of acquiring and analyzing the data stored on some form of physical storage media.
  - includes recovery of hidden/deleted data/files.

## Storage media to be examined for finding/recovery of relevant evidence in :

- Office files
- Deleted files of all kinds
- Encrypted Files
- Compressed Files
- Hidden Files
- Hidden Partitions
- Bad File Extensions
- Cache files
- Registry
- Unallocated Space
- File Slack
- Meta data
- Recycle Bin
- Temp files
- Hidden Data in files

## Storage media to be examined for finding/recovery of relevant evidence in :

- Temp files
- Recycle Bin
- Email messages (deleted ones also)
- Web history
- Cookies
- Network Server files:
  - System history files
  - Web log files

## Source Code Forensics

- To examination Software Source Code for malicious signatures
- To determine software ownership or software liability issues.
  - Review of actual source code.
  - Examination of the entire development process, e.g., development procedures, documentation review, and review of source code revisions.

## What is Network Forensics?

- Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

## Network Forensics

- Scrutinising network traffic and logs to identify and locate the suspicious system
- Network forensics is the process of examining network traffic
  - After-the-fact analysis of transaction logs
  - Real-time analysis via network monitoring
    - Sniffers
    - Real-time tracing

# Network Forensics Analysis Tools (NFAT)

- NFATs must do the following:
  - Capture network traffic
  - Analyze network traffic according to user needs
  - Allow system users to discover useful and interesting things about the analysed traffic

# NFAT Tasks

- Traffic Capture
  - What is the policy?
  - What is the traffic of interest?
  - Internal/External?
  - Collect packets: tcpdump
- Traffic Analysis
  - Sessionising captured traffic (organise)
  - Protocol parsing and analysis
    - Check for strings, use expert systems for analysis
- Interacting with NFAT
  - Appropriate user interfaces, reports, examine large quantities of information and make it manageable

## NFAT v/s IDS, Firewall

- IDS attempts to detect activity that violates an organization's security policy by implementing a set of rules describing preconfigures patterns of interest
- Firewall allows or disallows traffic to or from specific networks, machine addresses and port numbers
- NFAT synergizes with IDSs and Firewalls :
  - Preserves long term record of network traffic
  - Allows quick analysis of trouble spots identified by IDSs and Firewalls

## Network based IDS (NIDS)

- Detect malicious activity by monitoring network traffic – DoS attacks, port scans, attempts to crack into computers
- Collect data from the network or a hub / switch
  - Reassemble packets
  - Look at headers
- Try to determine what is happening from the contents of the network traffic
  - User identities, etc inferred from actions

# Honeypots

- Network Forensics and Honeypot systems have the same features of collecting information about computer misuses
- Honeypot system can lure attackers and gain information about new types of intrusions
- Network forensics systems analyze and reconstruct the attack behaviors
- These two systems integrated together build a active self-learning and response system to profile the intrusion behavior features and investigate the original source of the attack.

## N/w Traffic Capturing Systems - 1

- “***Catch-it-as-you-can***” systems, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.

## N/w Traffic Capturing Systems - 2

- **“Stop, look and listen”** systems, in which each packet is analysed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

## Tools for Network Traffic/Data Capturing/Monitoring

- Tcpdump
- Windump
- NetVCR (Niksun)
- Netintercept (Sandstorm)
- Network Flight Recorder (NFR)
- SilentRunner
- NetWitness .....and more

# Tools for Network Forensics

- Argus
- Tcpwrapper
- Nnstat
- Netflow
- Tripwire

## N/w Traffic Analysis

- Tcpcmdump + *strings*
- Iris Network Traffic Analyser
  - Session reconstruction
  - Data capturing
  - Network performance analysis
- Wireshark

## N/w Traffic Analysis (contd..)

- 'strings' to find text from traffic stream
- 'grep' to find specific words or phrases in the recovered strings
- get -> network's web traffic
- quit -> FTP control session / POP3 session / NNTP session
- privmsg -> IRC (internet relay chat) session
- TCP connection on port 23 with telnet commands -> telnet session
- TCP connection on port 23 with string 'YMSG' -> yahoo messenger session

## N/w Traffic Analysis will provide

- Contents of people's emails
- User ids & passwords (if plaintext, FTP, POP3 )
- Web pages viewed
- Contents of a person's shopping cart

# Analysis

- Examine log files
- Look for remotely controlled hostile programs (netbus, backorifice, etc)
- Look for possible hacker file sharing or communications programs (eggdrop, IRC, etc)

## Analysis (contd..)

- Look for privileged programs  
`find / -perm -4000 -print`
- Look for file system tampering  
(use tripwire or backups)
- Examine 'cron' and 'at' jobs
- Look for unauthorized services  
`netstat -a`  
check `inetd.conf`

## Analysis (contd..)

- Look for password file changes or new users
- Check system and network configurations
  - Pay close attention to filtering rules
- Look for unusual files
  - Depending on the size of your disks:  
`find / -print | more`
- Look at all your hosts, especially servers

## Backtracking

- Nowadays hackers are increasingly sophisticated about hiding tracks
  - The ones that are good, you won't catch
  - The ones that you can catch aren't worth catching
- Very few good tools for backtracking are available

## Hidden Directories

- Warez: Cute term for pirated software
- Warez are often hidden in FTP or web areas using weird directory names:
  - “...”
  - “ ” (space)
  - “normal ” (normal with space after it)
- Check FTP areas for new directories

## Finding Hacker -Prints

- Search suspected infected system for new files:
  - `find / -mtime -30 -print`
  - Use tripwire
  - Restore filesystems to a different disk and compare all the files (slow and painful!)

## Some hostile tools to look for

- nuke - icmp bomb program
- rootkit - trojans and patches
- cloak - log clearer
- zap - file date changer
- icepick - penetration test tool
- toneloc - wargames dialer

## Digital Evidence - Types

- **Volatile Storage (Non-persistent data)**  
Memory loses its contents, if power turned off. RAM (except the CMOS RAM used in BIOS) contents are volatile.
- **Non-volatile Storage (Persistent data)**  
No change in memory contents, if power turned off. Tape or disk (magnetic/optical storage), ROM are non-volatile.

## Order of Volatility of Digital Evidence

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

## Tools for Volatile Data Collection

- `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 useful information

- 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 to know System H/w Config'n

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

# Tools for discovery of Password

- Asterisk Logger
- AsterWin IE
- Network Password Recovery
- Protected Storage PassView
- Passware
- MessenPass (for IM)
- Mail PassView (e-mail)
- Brute Force
- AccessData FTK
- Rainbow Tables

## Disk (digital evidence) Imaging

- Maintain integrity & security of the org. evidence – use write protection
- 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, win)
- SafeBack (win)
- SnapBack DatArrest
- Drive Image Pro
- R-Drive Image
- FTK's built-in feature

It is better to use HW imaging equipments

# Log Files Analysis

Essential to reconstruct the chain of events:

- Victim system's log files (Event Logs)
- Web Server (IIS / Apache Logs), Mail Server Logs
- IDS / IPS, Firewall, Router log files
- Log files of the system used for crime
- Access log details of the system used for crime  
- from ISP
- SysLog Server Logs

## Handling of Log Files - as Evidence

- Must not be modifiable
  - Copy to a protected media (only once writable)
  - Bit-stream copy to Optical media
- Must be complete
  - All superuser access
  - Login and logout details
  - Attempts to use any controlled services
  - Attempts to access critical resources
  - E-mail details
- Appropriate retention

## Log Files

- Windows Hosts – Event logs
- Linux Hosts – Syslog
- Web server - IIS logs
- Web server – Apache logs
- IDS / IPS logs

## Tools for analysis of log files

- Dmpevt
  - Web historian
  - Swatch
  - Log Parser
  - Excel (MS Office)
- .....and many more

## Internet Forensics

- Internet or Web forensics is the process of piecing the information together - where and when a user has been on the Internet.
- Temporary Internet Files
- History of websites visited
- Cookies
- User activity recreation

# Email Forensics

- Email forensics is the study of source and content of electronic mail as evidence.
  - identifying the source system, location & actual sender
  - recipient of a message
  - date/time of sending email.
  - Often email is very incriminating.
- e-Mail Headers
- deleted emails

# Spoofer Emails

are sent using –

- Open relays / proxies
- Compromised systems
- Self owned email servers
- Email Anonymiser services
- Temporary accounts
- Hijacked accounts

## Tools to Trace the origin of Spoofed Email

- Nslookup
- Whois (Domain/IP)
- Traceroute
- SamSpade etc.

## They are coming from .... ?

- Use tcpdump / whois / syslog to see where they are coming in from
- Run 'finger' against remote system
  - If 'finger' is working on attacker system you may be able to correlate activity with times of attack and user idle time
  - Usually attacker will be using a stolen account on remote machine
- Check NIC registry for attacker domain and *telephone* the site technical contact
  - Remember: your communications are compromised
- Check for possible caching locations
  - DNS Cache
    - ipconfig /displaydns
  - ARP Cache
    - arp -a

## Security Issues

- Handling encrypted traffic
- Avoiding detection & circumvention
- Protecting sensitive data revealed by analysis

# Computer Forensic Tool Kits (FTK)

- Provides integrated Graphics User Interface (GUI) to the set of tools used in FTK
- Ease of use, follows the steps in sequence
- Investigator need not bother about tools & their usage syntax, results & documentation

## Some Computer Forensic Tool Kits

- CyberCheck Suite (C-DAC)
- EnCase (Guidance)
- FTK (AccessData)
- Helix
- Autopsy (GUI) + Sleuth Kit
- TCT (The Coroner's Toolkit)
- Knoppix STD
- ProDiscover

## Anti-Forensics : Challenges ?

- Rootkits based cyber crimes
- Tools on RAM (Diskless)
- Disk sanitisers (Wipe, Cipher)
- Compressed files with password
- Encrypted files with password
- Steganography

## References

- “Network Forensics: Tapping the Internet” by Simson Garfinkel (O'Reilly Network)
- “Lecture #14 - Network Forensics” by Bhavani Thuraisingham (University of Texas)
- “Experimentation in Network Forensics” by Naveen K Kumashi, et al (C-DAC, Bangalore)
- “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](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
- “File System Forensic Analysis” by Brian Carrier (Addison Wesley)