Computer Forensics: Digital Evidence & its Seizing

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

- Digital Evidence
- Legal issues
- Volatile & Non-volatile Digital Evidence
- Volatile Data Collection Process
- Acquisition of RAM data
- Handling of Digital Evidence at site of Crime
- References

Digital Evidence

Digital Evidence

- Latent, like fingerprints or DNA
- Extremely fragile & resilient; can be easily altered, damaged or destroyed
- Can cross borders with ease & speed (networked systems)
- Some of the common practices – curiosity may destroy digital evidence.
- If analysed directly, it will loose its integrity and will not be **admissible** in any court

Digital Evidence should be -

1. **Admissible,** conform to legal requirements
2. **Authentic,** relevant to the case
3. **Complete**, & not just extracts
4. **Reliable -** collected & handled appropriately
5. **Believable** & understandable

Legal Issues

- MAC details of the files as digital evidence in the seized original hard disk (hence its image too) must be earlier than the noticing / reporting of criminal incident as well as the date & time of its seizure.
- If it is not so, digital evidence will be diagnosed as a tampered evidence and court can not accept it as an admissible evidence.

Sources of Digital Evidence:

- Hard Drive(s)
- CD, DVDs
- USB Mem. Devices
- Mag. Tapes
- RFID Tags
- PDAs
- Smart Cards
- Web pages
- Voice mail
- e-Diary
- Scanner, Printer
- Fax, Photocopier M/c
- Digital Phone Set
- iPods
- Cellphone
- DigiCam
- Config'n settings of digital devices

Digital Evidence - Types

- **Volatile (Non-persistent)**

  Memory that loses its contents, as soon as power is turned off; e.g. Data stored in RAM (semiconductor storage)

  (System BIOS: CMOS RAM - battery powered)

- **Non-volatile (Persistent)**

  No change in contents, even if power is turned off; e.g. Data stored in a tape / hard disk (magnetic storage), CD / DVD (optical storage), data cards, USB Thumb Drives – Flash memory).

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 from a live system: Why it is so much important?

- Current running state & system configuration details
- Activities performed / in progress
- Root cause of the incident
- Timeline of the incident
- Time, date, user responsible for the incident
- Network connection details
- Once system is shutdown / rebooted, volatile data is lost for ever

Tools for acquisition of Physical Memory (RAM) Dump

- dd (fau)

  [ex C:\>dd if=\\.\PhysicalMemory of=e:\ramdump.img conv=noerror]
- Win32DD, Win64DD
- WinEN (Helix 3)
- Nigilant32
- **FTK Imager** (AccessData)
  - Easiest to use (GUI), freeware

Digital Evidence: Volatile Active System Information

- System Profile
- System Date & Time
- Command history
- System Uptime
- Running Processes
- Open files
- Start up files
- Files accessed
- Clipboard data
- Logged in users
- DLLs or shared libraries

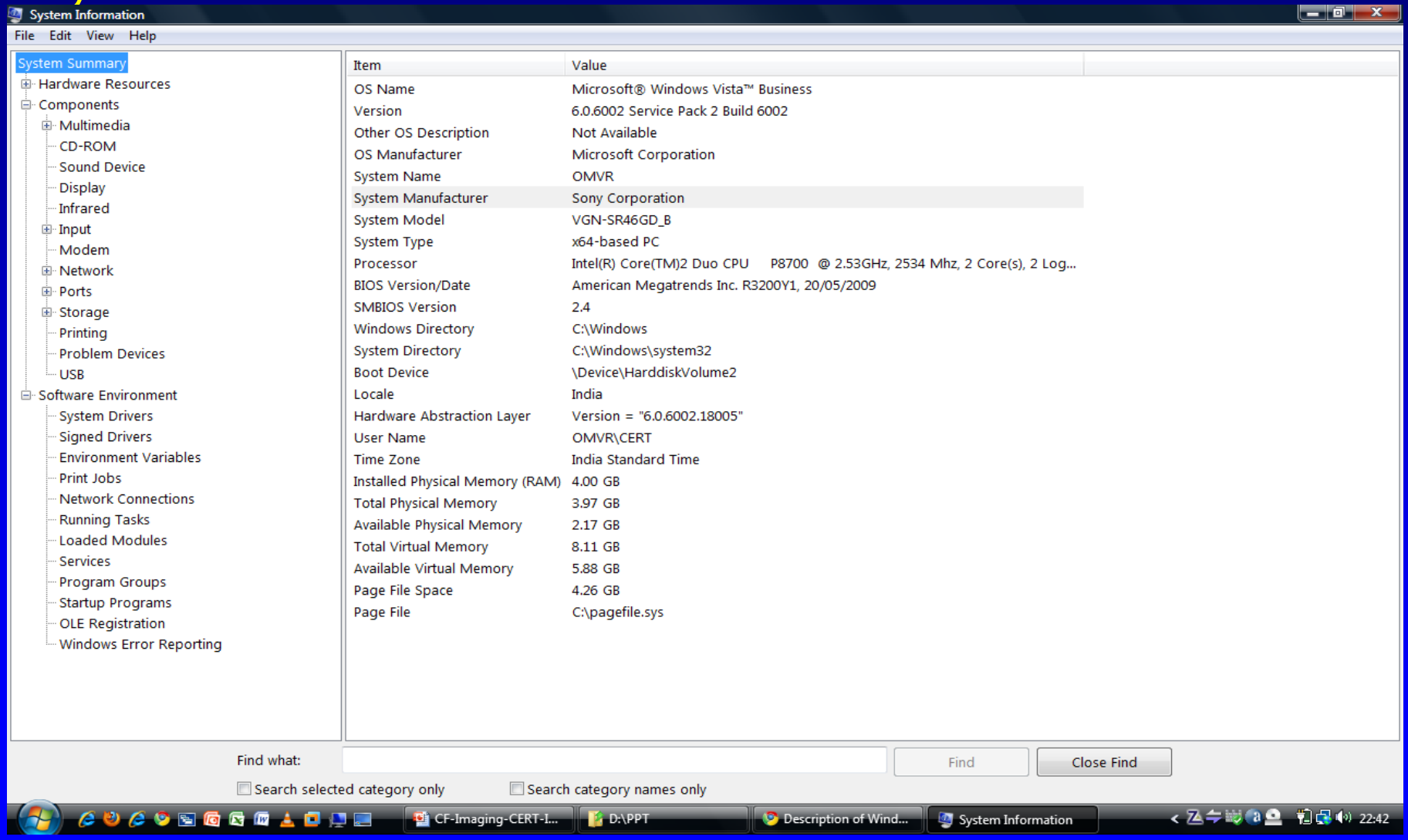
System Profile by ‘Systeminfo’ (Win)

(Tool: msinfo32.exe in DOS mode)

- Date of OS installation
- System Uptime
- Registered Owner
- BIOS Version
- System Directory
- Log-on Server
- N/w Interface Card(s) installed

System Information

Click: Start → Programs → Accessories → System Tools → System Information



Digital Evidence: Volatile N/w connectivity Information

- State of N/w connection
- Open connections
- Open ports
- Routing information
- N/w interface
- ARP Cache

System Time v/s Std. Time

- Always compare suspected system time with the standard time; is there any time difference?
- Difference, if noticed, must be recorded
- Same process must be carried out for the other associated systems and servers providing the logs
- Photograph the system monitor showing the system time along with a watch having standard time
- By the above, reconciliation of access logs from the servers and suspected system will be easier

Digital Evidence may be in form of …

- Email messages (deleted too)
- 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
- Web/e-Mail Server access logs
- Domain access logs

Volatile Data Collection Process

- Collect system uptime, incident's date & time, and command history from the suspicious system.
- Run forensic tools or OS commands, to know date and time of actions to establish a timeline / trail of events.
- Document all forensic collection activities including s/w tools / commands used in logbook.
- Collect all types of volatile information from system and network.
- End the forensic collection by recording the used commands along with date and time of use.

Scenario 1:
If computer is in ON state, then -

1. Must have the RAM dump using tools (will be used to extract user-ids & passwords)
2. Note the System H/w, N/w configuration
3. Note the Processes / Applications running
4. Note the documents / files – open / being accessed or accessed after system up
5. Note Network connectivity details
6. Pull the power chord (laptop – remove battery) to power OFF the system
7. Now follow as given in Scenario 2

Scenario 2:
If computer is already OFF, then -

- Disconnect all the Hard Disks, except CD/DVD Drive (to boot from it)
- Label the connections (for later restoration)
- Ensure that any of the connected drives is not having any CD, DVD or USB Drives, etc
- Power ON the system and enter into BIOS?
- Photograph the monitor showing BIOS
- Document the boot sequence
- Change the boot sequence to “boot from CD/DVD”; and note it.

...cont’d

Scenario 2:
If computer is already OFF, then -

- Save the BIOS & shutdown the system
- Restore all the drive connections
- Connect another hard disk to system disk controller card as a destination drive for storing the image of system hard disk
- Insert a bootable CD/DVD, having tools for imaging and password recovery; and boot the system
- System is ready for imaging the hard disk
- RAM dump is irrelevant in this case
- Document all your actions

Volatile Data Collection Tools

Windows

- COFEE (given by Microsoft to LEAs only; Computer Online Forensic Evidence Extractor)
- systeminfo : system profile
- psinfo -s : s/w installed
- Psuptime : system uptime info
- Net statistics : system uptime info
- WFT (win forensic toolchest)

Linux

- cat : system profile
- uname : machine's profile
- Uptime, w : user uptime info

Tools (Win) for Running Processes

- Netstat –ab : process & pid info
- Listdlls <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

Some Useful Tools

Windows

- Msconfig
- Autoruns, autorunsc
- Netusers
- PsLoggedOn : local/remote logged users

Linux

- Autoruns, autorunsc
- Ls
- Chkconfig – list
- Inittab : run level
- Netusers

Tools for network user details

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

Tools for HW Config'n

Windows

- Fport : open ports
- Netstat –anb : TCP/IP connections
- Net share : network shares
- Netstat –r : routing info'n
- Arp –a : IP Addr, MAC Addr of NIC

Linux

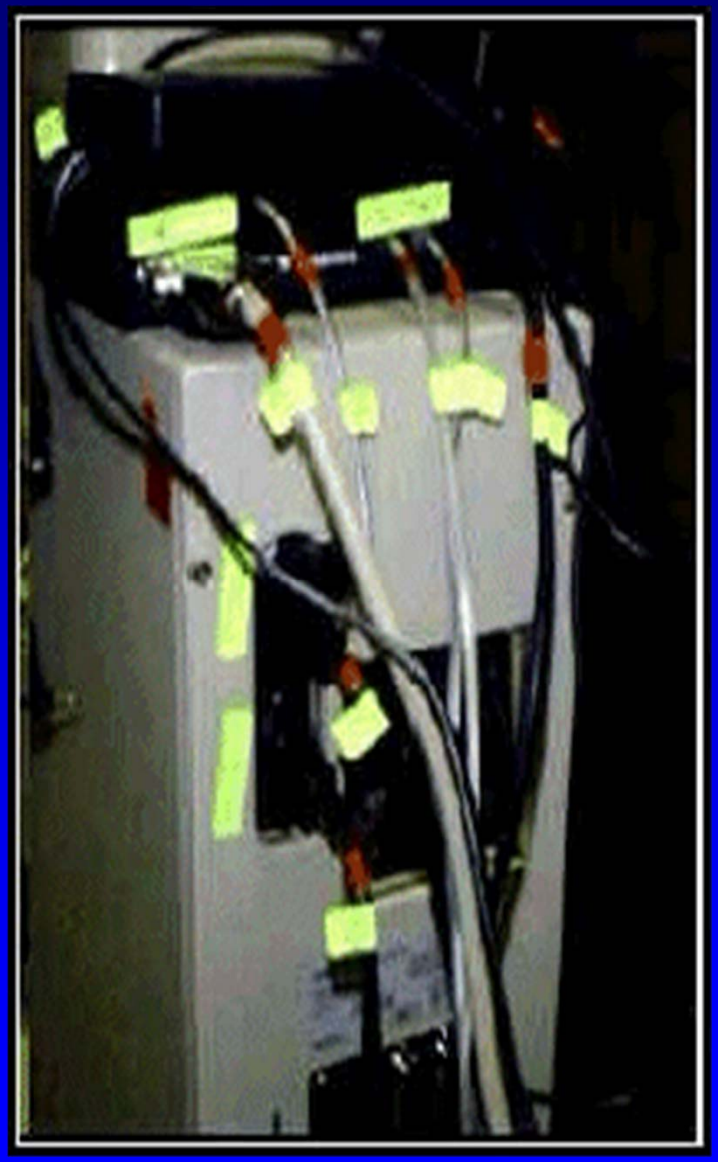
- Netstat –anp
- Ifconfig : NIC config'n
- Arp –a : IP Addr, MAC Addr of NIC
- Netstat –rn : routing info'n

Digital Evidence Handling at Crime Site

- Document the Crime Scene - OS (Ver.), BIOS date & time (and difference, if any), H/w & S/w Configuration, IP / MAC address
- Computer System : shutdown / power off ?
- Identify Evidence & Authenticate through a Hashing Algo. (MD5)
- Always make the bit-stream copy (forensic image) of the seized storage media

Digital Evidence Handling at Crime Site (contd ..)

- Label all the connecting cables and photograph them
- Document the chain of custody
- Preserve the evidence before packing for transportation
- Securely pack & transport the Evidence to lab



Digital Evidence Handling at Crime Site (contd ..)

- Store the seized org. evidence in a protected storage (Air bubbled PVC, antistatic bag)
- Transfer the Computer System to a secure location

"Best Practices for Seizing Electronic Evidence Ver. 3" may be downloaded from -

http://www.forwardedge2.usss.gov/pdf/bestPractices.pdf

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!