Computer Forensics

Omveer Singh, GCFA
Additional Director / Scientist 'E'
(In-charge, Cyber Forensics Lab)

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

Agenda

- Cyber Crime Investigation
- Computer Forensics
- Digital Evidence
- Seizure of Digital Evidence
- Imaging of Digital Evidence
- Computer Forensics Tools & Toolkits
- Analysis of Digital Evidence
- Anti-Forensics
- References

Cyber Crime Investigation?

Most of the times, criminal leave some clues, traces or trails 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 finger print, a footprint, or a tool mark. Rather, here the evidence is in the form of electronic or digital data / files (0s & 1s; bits & bytes).

Computer Forensics …

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

Computer Forensics …

is the integration of identification, assessment, seizure, preservation, imaging, analysis of digital evidence to find out the relevant data and/or the root cause of the incident / crime.

Cyber Forensic Investigation Process

- Identification
  - Assessment
- Seizure / Acquisition
  - Imaging
  - Integrity verification
- Analysis
- Documentation
  - Report preparation for submission to LEA / Judiciary

Computer Forensic Investigation: 2 Roles

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

Role of a First Responder

- Essentially the first person noticing and reacting to the 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

First Responder's Toolkit

- Log Book
  - To record all actions /events with date & time chronologically
- Safe Boot / 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
- Tools to open CPU Cabinet, detach Hard Disk (multi screw driver set, etc)
- Multi-purpose mechanical toolset
- Anti-static covers
- Air bubbled PVC covers
- Marking labels
- Marking pen (permanent ink)

Digital Evidence

Digital Evidence

- Latent, like fingerprints or DNA
- Extremely fragile & resilient; can be altered, damaged or destroyed easily
- Can transcend borders with ease & speed (networked systems)
- Some of the common practices – curiosity may destroy digital evidence.
- Direct analysis will make it **unacceptable** in a court of law

Digital Evidence - Types

- **Volatile (Non-persistent)**

  Memory that loses its contents, if 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 / floppy disk / hard disk (magnetic storage), CD / DVD (optical storage), ROM (semiconductor storage; USB Thumb Drives – Flash Memory).

Volatile Data from a live system: Why so 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

Handling of Digital Evidence - at Crime Site

- 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

Computer Forensic Investigation ...

- Original digital evidence is imaged
- Analysis of the imaged digital evidence is carried out at the lab using tools as well as manually.
- Relevant information is searched from the digital evidence that may have significance in the case.
- Computer Forensics traditionally rely upon the data inadvertently left on the system by the SW application programs / tools.
- Investigator must be aware about the computer knowledge level of the suspected person

Imaging of Digital Evidence (Data Storage Media)

Legal Issues

- MAC details (time & date) 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 and court can not accept it as an admissible evidence.

Direct Analysis of Org. Digital Evidence : Strictly Forbidden

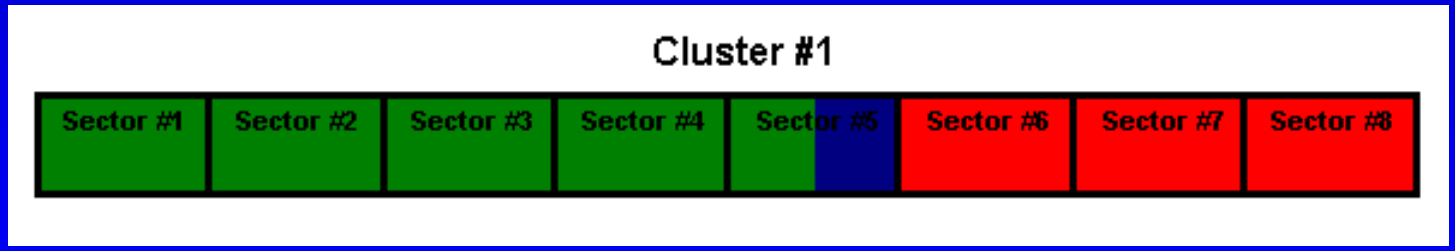
- Will change MAC (last Modified, last Accessed, Created) details (date & time) of a file
- Analysing a live file system / original evidence also changes the state of the evidence (MAC details)
- Any analysis on the original digital evidence makes it a tampered digital evidence
- Digital evidence will not be accepted by court and render it useless
- Solution – analyse a clone or image of the original digital evidence

Logical copy / backup of Hard Disk

- Back up or copy of a hard disk – copies only active files from the original hard disk and not all the data areas
- So copy will not provide all the data areas of the hard disk (digital evidence) for analysis
  - Unallocated area (deleted files) will not be available
  - Swap files will not be available
  - File slack will not be available

File Slack

- Green : Space used by file for data storage (Sectors 1 to 5).
- Red : Unused sectors in the last cluster. File Slack or Slack Space (Sectors 6 to 8)
- Blue : RAM Slack (Sector 5)



(1 Cluster = 8 Sectors = 8 * 512 Bytes = 4096 Bytes = 4 KB;

i.e. min. size of a file in **NTFS** on a hard disk)

Logical Copy v/s Physical Copy

- **Logical copy**

  In a logical copy, the active directories and files only of a logical volume are copied. It does not capture other data that may be present on the media such as deleted files or residual data stored in the slack space.

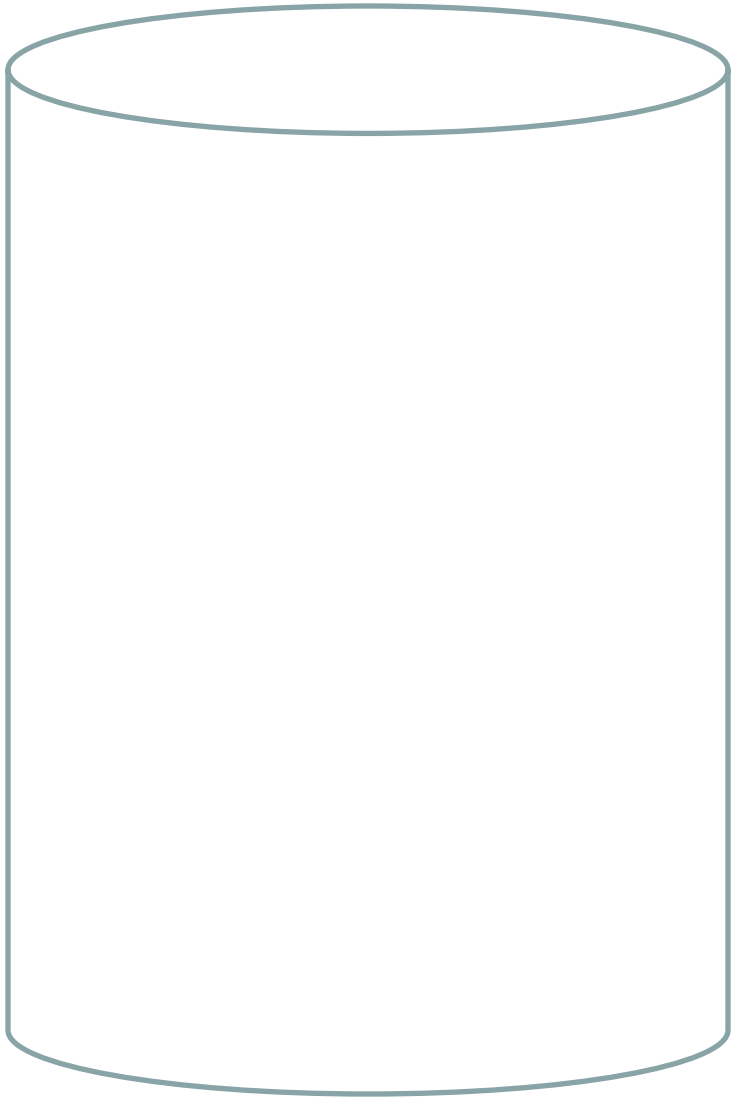
- **Physical copy (generally called forensic imaging, imaging, cloning or mirror image)**

  Generate a bit for bit copy of the original media; include free space and slack space.

Copying of Disk

Suspected disk (Source)

Sterile disk (Target)

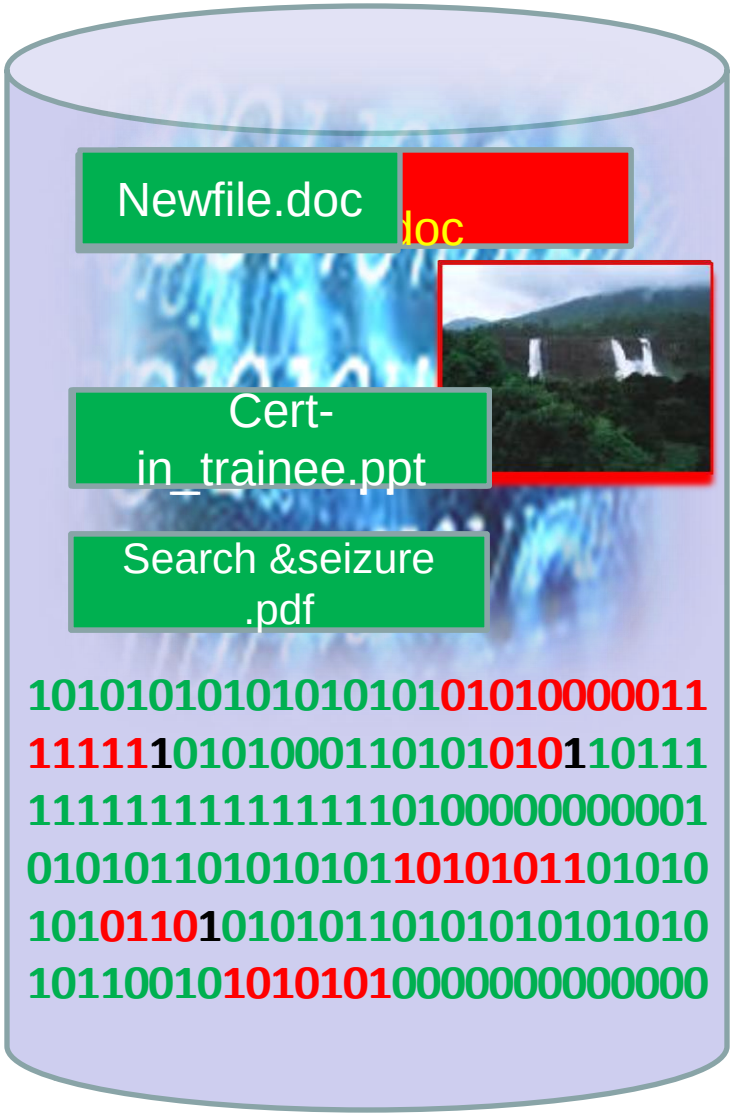


Active files

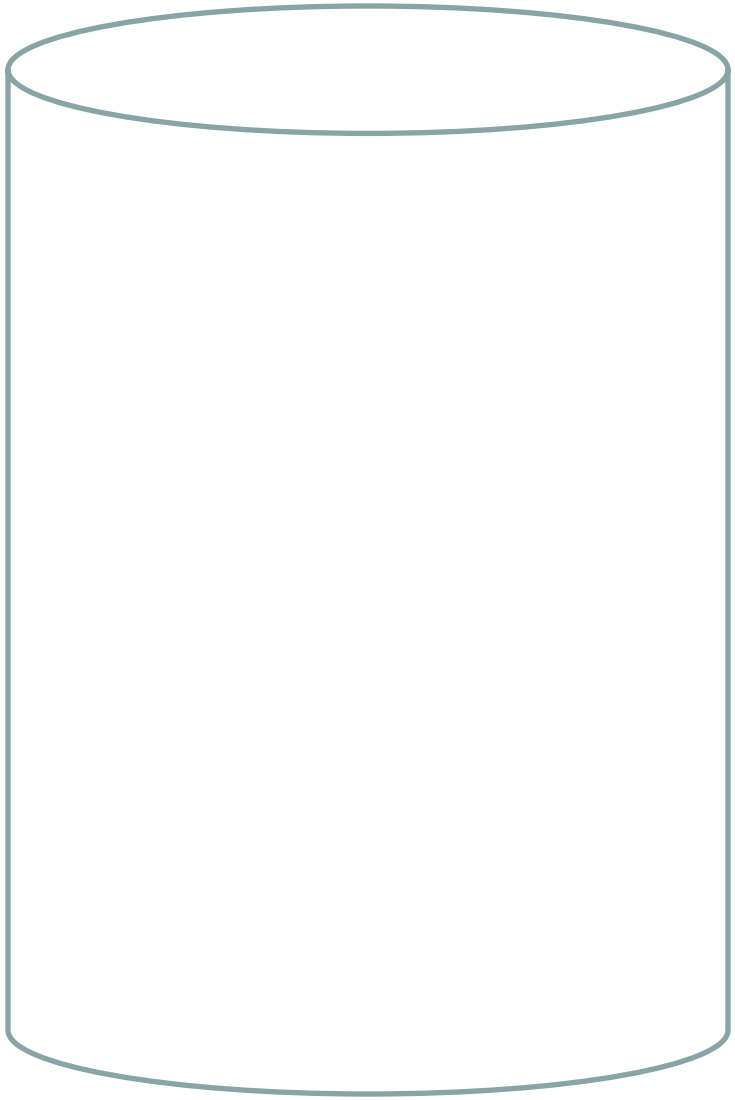
Deleted files

Imaging of the Disk

Suspected disk (Source)



Sterile disk (Target)



Active files

Deleted files

Advantage of having the image of org. Digital Evidence

- Analysing the image of the digital evidence will
  - Preserve the original evidence
  - Prevent inadvertent alteration of original evidence during examination
  - Cloned image may be created again if required

Computer Forensic Toolkits: imaging s/w with GUI

- TrueBack (C-DAC) - Freeware
- FTK Imager (AccessData) – Freeware
- Built-in feature of most of the computer forensic toolkits

Disk Write Blockers

- Prevent writing of data to the suspect original drive
- Ensure the integrity of the suspect original drive
- Software Write Blockers v/s Hardware Write Blockers


STABLEAU


DC IN A
USB 2.0
800
800
400
IDE
Power
IDE Detect
Host Detect
Write Block
Activity
DC
OUT

Best Practices for imaging

- Always ensure that the integrity & security of the org. evidence is maintained.
- Suspected org. evidence (hard drive) must be connected through a write blocker.
- The destination disk should be a freshly wiped (sterilised) disk, even if it is new.
- Entire disk imaging is better than partition (Volume) wise imaging.
- Every action should be documented.

Best Practices … (cont'd)

- Document the Make, Model, Serial No and Size of the hard disk into multiple forms like Chain of Custody, Seizure Note, etc as required
- Note down the size (or capacity) of the suspected (source) hard disk and always connect it through Hardware Write Blockers.
- Be cautious when you choose the SOURCE & DESTINATION hard disks in the Forensic Imaging software
- Always select the Forensic Image as RAW Image Type which could be acceptable by all – Freeware as well as Commercial Forensic S/w applications

Integrity of Digital Evidence?

- Digital data is vulnerable to intentional or unintentional alteration
- Integrity of digital evidence is required to be maintained through out the investigation and prosecution
- For verification of integrity, the digest of data (evidence / file), called hash value, is calculated by a well-defined mathematical hash function
- MD5 (128 bit / 32 Hexits), SHA-1 (160 bit / 40 Hexits)

Analysis of the Image of Digital Evidence

Computer Forensic Tool Kits

- Analysis is carried out using various tools and toolkits
- Toolkit provides integrated Graphical User Interface (GUI) to the set of tools used in toolkit
- Ease of use, follows the steps in sequence
- Investigator need not bother about tools & their usage syntax, results & documentation

Toolkit Features

- Imaging
- Integrity/Authentication through hash value
- Deleted files Recovery
- Identification of
  - Files with bad extension
  - Files with used Slack Space
  - Encrypted / compressed files
- Display of file contents
- Display of file contents in hex format
- Report preparation

Computer Forensic Tool Kits

- CyberCheck Suite (C-DAC) : Commercial
- EnCase (Guidance) : Commercial
- FTK (AccessData) : Commercial
- Helix : Freeware
- Autopsy (GUI) + Sleuth Kit : Freeware
- TCT (The Coroner's Toolkit) : Freeware
- Knoppix STD : Freeware
- ProDiscover Forensics: Commercial
- X-Ways Forensics: Commercial
- F-Response: Commercial

At CERT-In we have all these above.

… and there are many more available

Analysis of the Image of the Digital Evidence

- Image is uploaded to the forensic toolkit and processed
- Toolkit provide complete structure of the file system / data on the image including the deleted / password protected / encrypted / compressed / bad extension files
- Various options are selected as per requirements, e.g. list of keywords from the files

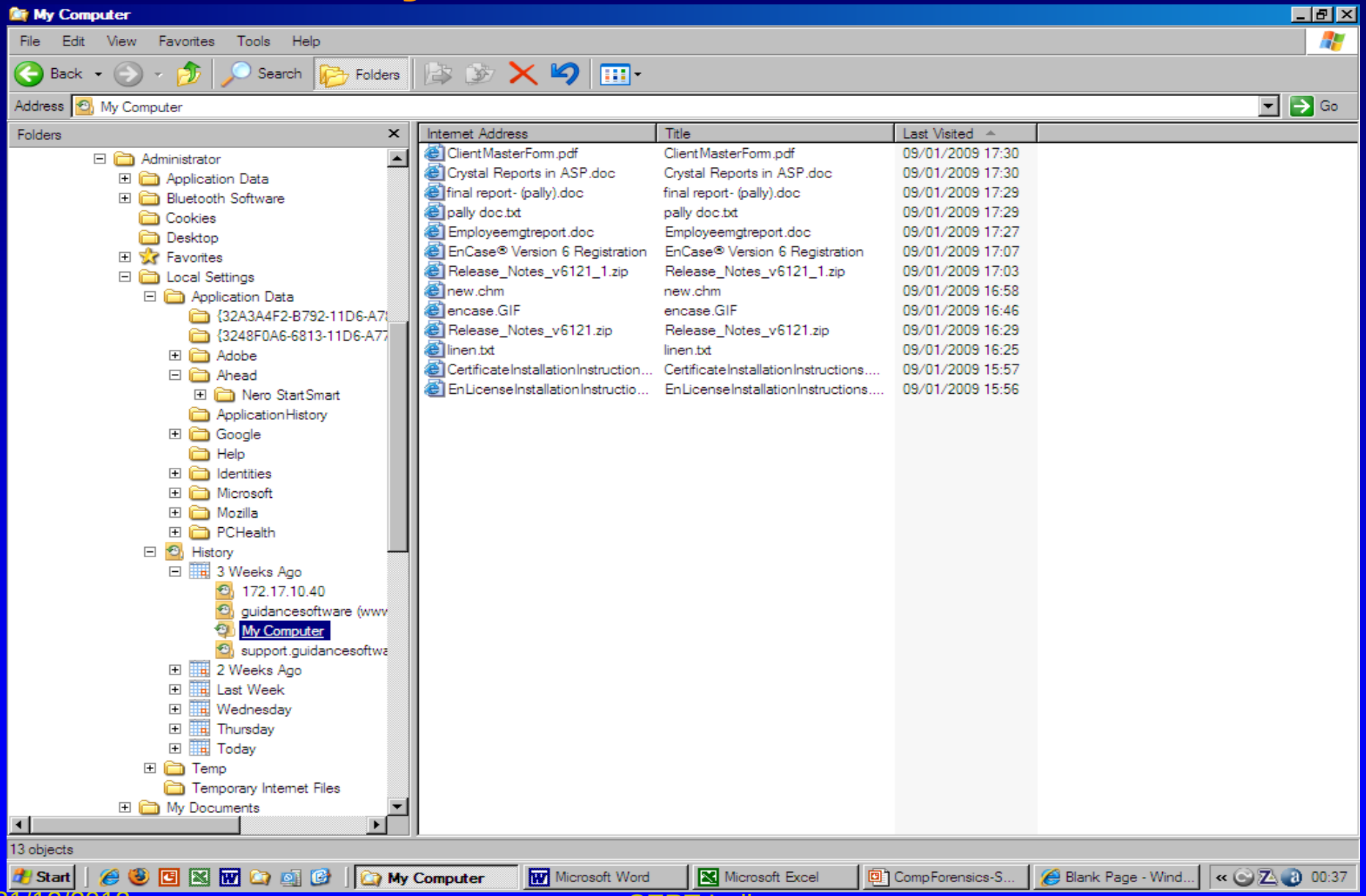
Timeline

- Files on the hard disk are sorted according to MAC times in decreasing order
- Based on the estimation of time taken to carry out the cyber crime, files are manually looked into
- Sequence of the tools run are noted
- List of the files edited / read / uploaded are noted
- These files are analysed for any hidden or encrypted information

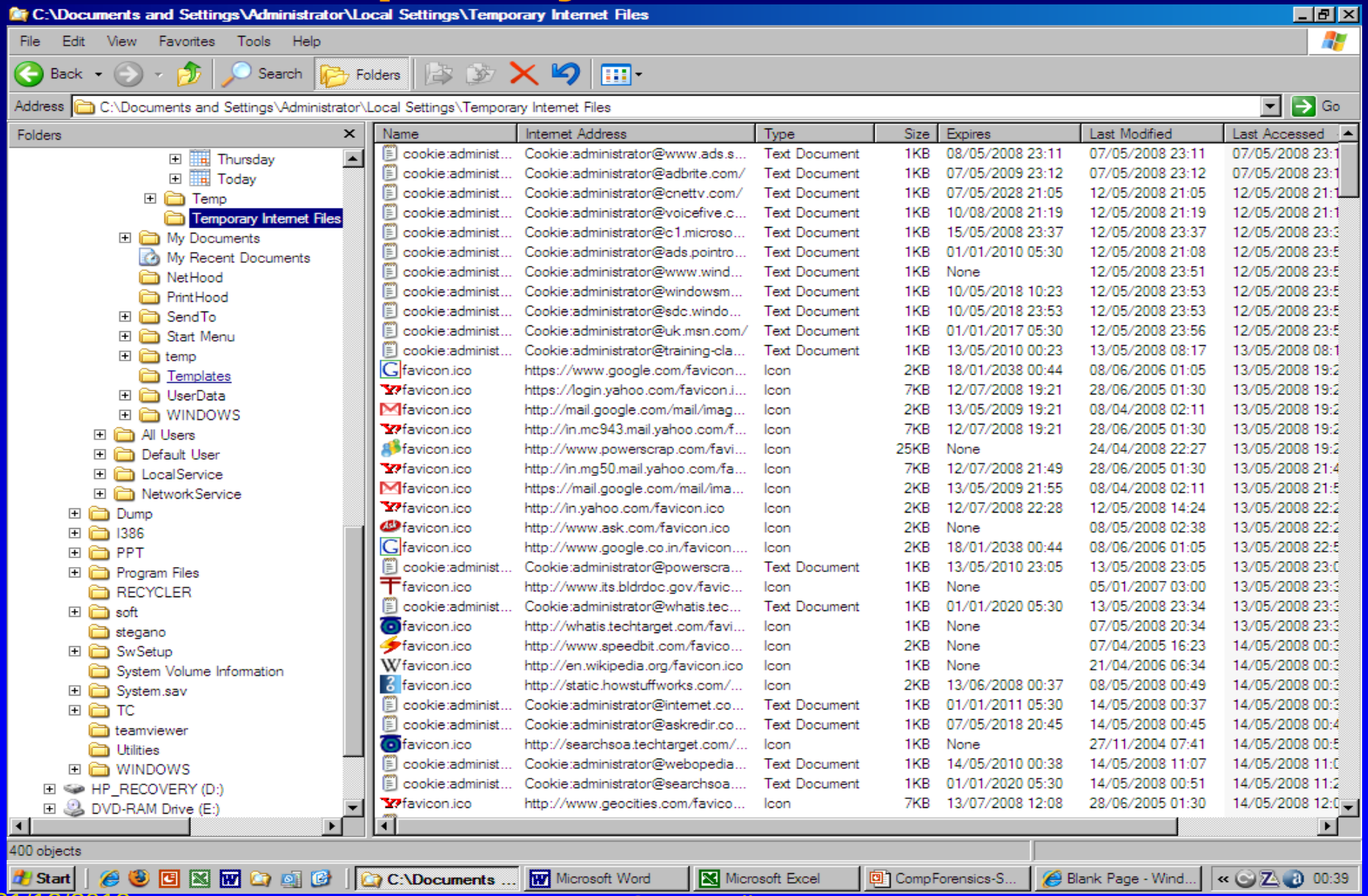
Internet Usage Analysis

- Internet Access details from the system
- Internet Access Logs from ISP
- Internet Websites browsed, date, time & duration
- Proxy websites used to hide the details of the websites visited?

History of websites visited



Temporary Internet Files



e-Mail Analysis

- When sending a message, it is not cached into the system hard disk (web based emails)
- Analysis of email as an evidence:
  - identifying the source system domain, IP Address
  - Recipient & sender of a message (spoofed?)
  - date/time of sending email
  - Message / contents
  - email headers
  - email server access logs
  - Internet access logs from ISP
- Recovery of deleted e-mails
- Locate the source of e-mail & its sender

Windows Registry

- Provide a wealth of information
- Located in /SystemRoot/System32/config
- Organised in 5 sections – termed ‘Hives’
  - HKEY_CLASSES_ROOT (HKSC, file name-OLE-streams)
  - HKEY_CURRENT_USER (HKCU, sid-user-desktop)
  - HKEY_LOCAL_MACHINE (HKLM, configuration, memory, last boot)
  - HKEY_USERS (HKU, all user account profiles)
  - HKEY_CURRENT_CONFIG (HKCC, running image)
- Each hive has keys and subkeys, which contain a value entry
- Each value entry has a name, data type and value

Windows Registry Analysis

Information from windows registry:

- System Configuration
- Devices connected to the System (USB)
  - Plug & play
- User ids & Passwords
  - Programs, e-mails, websites
- Personal Settings and Browser Preferences
- Websites visited
  - Date, time, queries
- Recently Accessed Files
- Programs Installed / Executed

Anti-Forensics

- Tools on RAM
- Diskless PC (RAM only)
- Disk Sanitisers - Wipe
- Compressed files (with password)
- Encrypted files (with password)
  - PGP
  - Digital Signature
- Steganography

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!