Open Source Forensic Investigation Tools

By

Kasun De Zoysa & K. C. Hewage

UCSC

isif asia

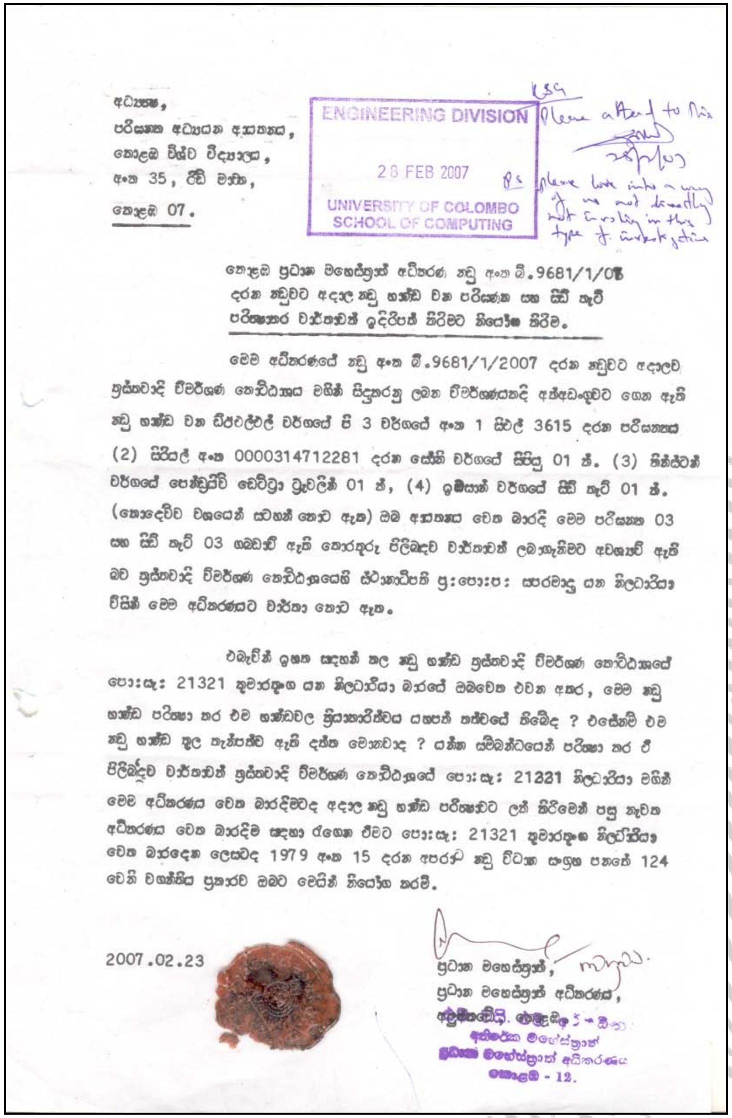
Centre for Digital Forensic

UCSC

isif asia

Our Role

- Police
- CID
- Customs
- Bribery and Corruption
- Judicial Services
- Victims



අධ්‍යක්ෂ,
පරිගණක අධ්‍යයන ආයතනය,
කොළඹ විශ්ව විද්‍යාලය,
අංක 35, රීඩ් මාවත,
කොළඹ 07.

ENGINEERING DIVISION
28 FEB 2007
UNIVERSITY OF COLOMBO
SCHOOL OF COMPUTING

KSG
Please attend to this
28/2/07

PS
please look into a way if we not directly not involving in this type of investigation

කොළඹ ප්‍රධාන මහේස්ත්‍රාත් අධිකරණ නඩු අංක බී.9681/1/07
දරන නඩුවට අදාල නඩු භාණ්ඩ වන පරිගණක සහ සීඩී තැටි
පරීක්ෂාකර වාර්තාවක් ඉදිරිපත් කිරීමට නියෝග කිරීම.

මෙම අධිකරණයේ නඩු අංක බී.9681/1/2007 දරන නඩුවට අදාලව ත්‍රස්තවාදී විමර්ශණ කොට්ඨාශය මගින් සිදුකරනු ලබන විමර්ශණයකදී අත්අඩංගුවට ගෙන ඇති නඩු භාණ්ඩ වන ඩිජිටල්වල් වර්ගයේ පී 3 වර්ගයේ අංක 1 සීඑල් 3615 දරන පරිගණකය (2) සීරියල් අංක 0000314712281 දරන සෝනි වර්ගයේ සීපියු 01 ක්. (3) කිංස්ටන් වර්ගයේ පෙන්ඩ්‍රයිව් ඩෙටිට්‍රා ට්‍රැවලින් 01 ක්, (4) ඉමේෂන් වර්ගයේ සීඩී තැටි 01 ක්. (කොදෙව්ව වශයෙන් සටහන් කොට ඇත) ඔබ ආයතනය වෙත බාරදී මෙම පරිගණක 03 සහ සීඩී තැටි 03 ගබඩාවී ඇති තොරතුරු පිලිබඳව වාර්තාවක් ලබාගැනීමට අවශ්‍යවී ඇති බව ත්‍රස්තවාදී විමර්ශණ කොට්ඨාශයෙහි ස්ථානාධිපති ප්‍ර:පො:ප: සපරමාදු යන නිලධාරියා විසින් මෙම අධිකරණයට වාර්තා කොට ඇත.

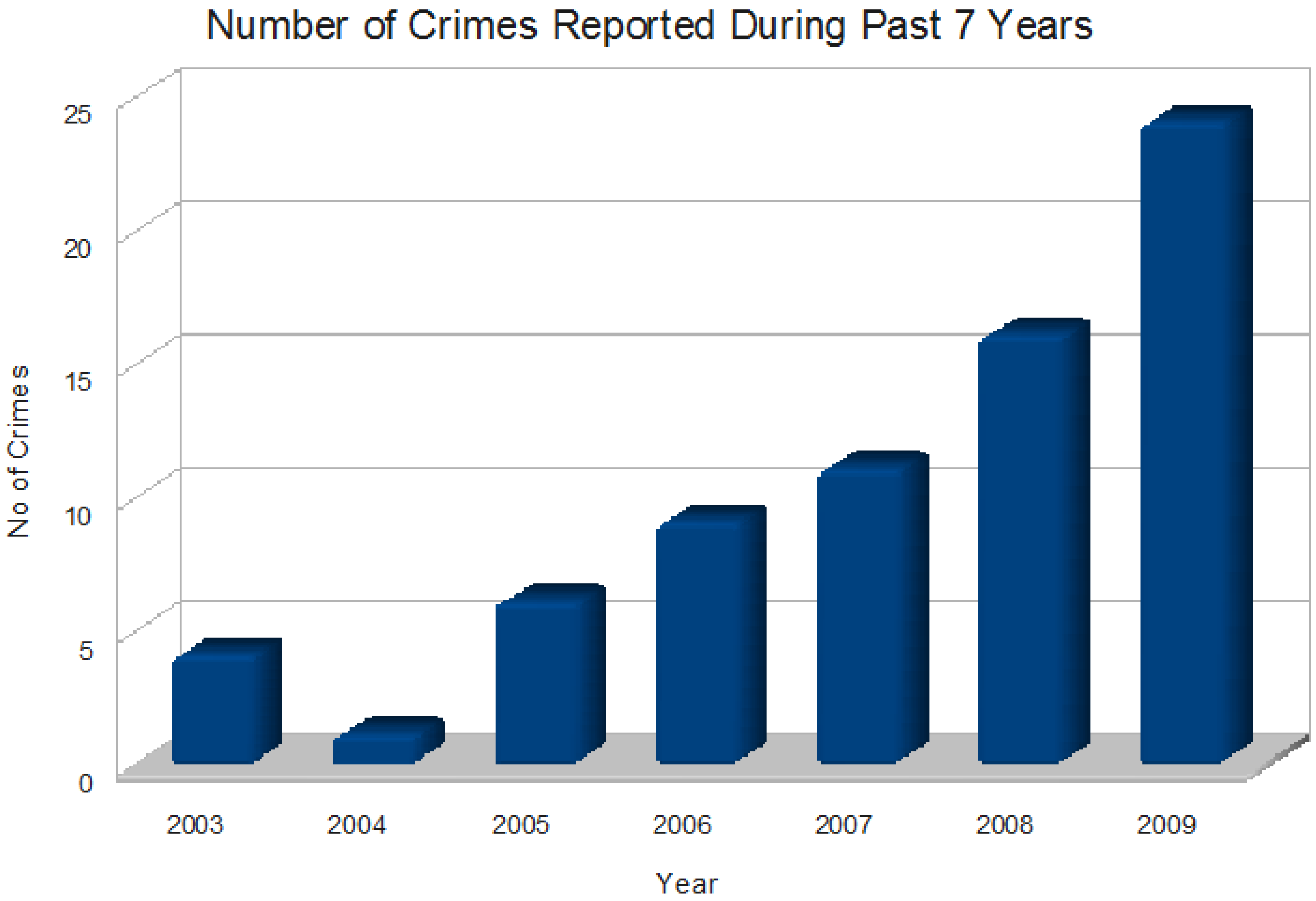
එබැවින් ඉහත සඳහන් කල නඩු භාණ්ඩ ත්‍රස්තවාදී විමර්ශණ කොට්ඨාශයේ පො:සැ: 21321 කුමාරතුංග යන නිලධාරියා බාරයේ ඔබවෙත එවන අතර, මෙම නඩු භාණ්ඩ පරීක්ෂා කර එම භාණ්ඩවල ක්‍රියාකාරීත්වය යහපත් තත්වයේ තිබේද ? එසේනම් එම නඩු භාණ්ඩ තුල තැන්පත්ව ඇති දත්ත මොනවාද ? යන්න සම්බන්ධයෙන් පරීක්ෂා කර ඒ පිලිබඳව වාර්තාවක් ත්‍රස්තවාදී විමර්ශණ කොට්ඨාශයේ පො:සැ: 21221 නිලධාරියා මගින් මෙම අධිකරණය වෙත බාරදීමටද අදාල නඩු භාණ්ඩ පරීක්ෂාවට ලක් කිරීමෙන් පසු නැවත අධිකරණය වෙත බාරදීම සඳහා රැගෙන ඒමට පො:සැ: 21321 කුමාරතුංග නිලධාරියා වෙත බාරදෙන ලෙසටද 1979 අංක 15 දරන අපරාධ නඩු විධාන සංග්‍රහ පනතේ 124 වෙනි වගන්තිය ප්‍රකාරව ඔබට මෙයින් නියෝග කරමි.

2007.02.23

ප්‍රධාන මහේස්ත්‍රාත්,
ප්‍රධාන මහේස්ත්‍රාත් අධිකරණය,

[illegible]
අතිරේක මහේස්ත්‍රාත්
ප්‍රධාන මහේස්ත්‍රාත් අධිකරණය
කොළඹ - 12.

Year *vs.* Number of Crimes



Problems Faced

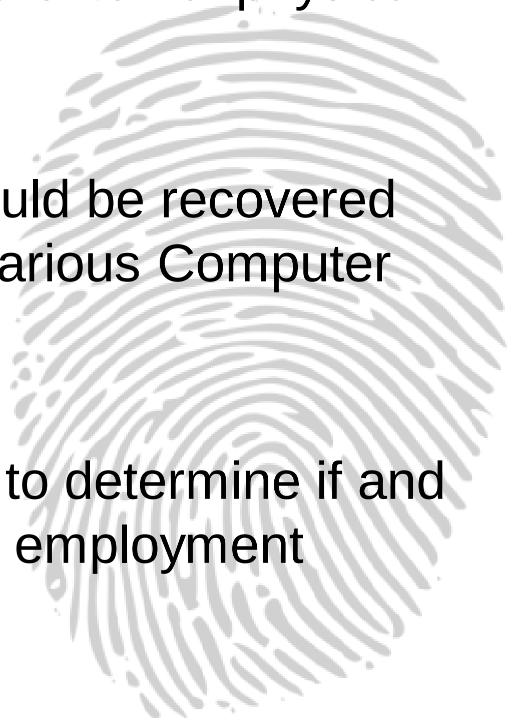
- Evidence not being collected in an acceptable manner.
- Evidence being damaged due to time and environmental factors.
- Evidence being damaged (wiped/formatted) before collection.

Why?

- Equipments are not available.
- Software are not available.
- Procedures and policies are not in place.
- Lack of IT knowledge in the Law Enforcement Sector.

Steps Of Computer Forensics

- According to many professionals, Computer Forensics is a four (4) step process.
  - **Acquisition**
    - Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices.
  - **Identification**
    - This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites.
  - **Evaluation**
    - Evaluating the information/data recovered to determine if and how it could be used again the suspect for employment termination or prosecution in court.

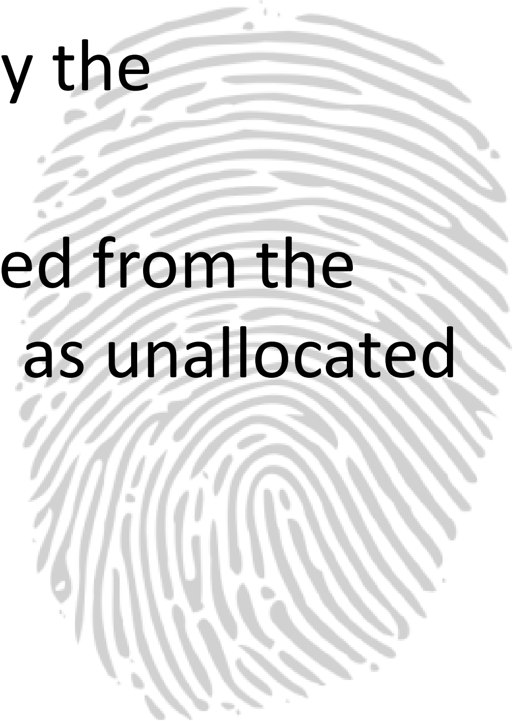


Steps Of Computer Forensics cont.

- **Presentation**
  - This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by laws.

Where is the evidence?

- In our dealings we have found that we have to categorize the types of data we work with.
  - Archival: Data stored on backup tapes.
  - Active: Data that is currently seen by the operating system.
  - Forensic: Data that has been removed from the operating systems view, also known as unallocated space.

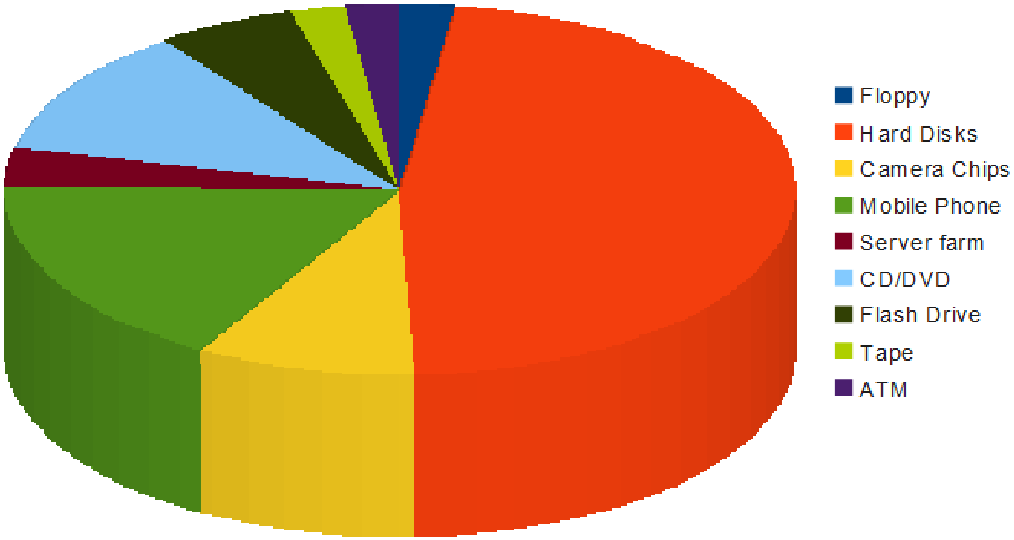


Types of recoverable media

- What all can we recover forensic data from?
  - CD-RWs
  - DVD-RWs
  - Floppies
  - Hard drives
  - Flash ram (smart media, SONY memory stick, mmc, secure digital)
  - and more!

Media

Storage Medium Analysed for Different Crimes



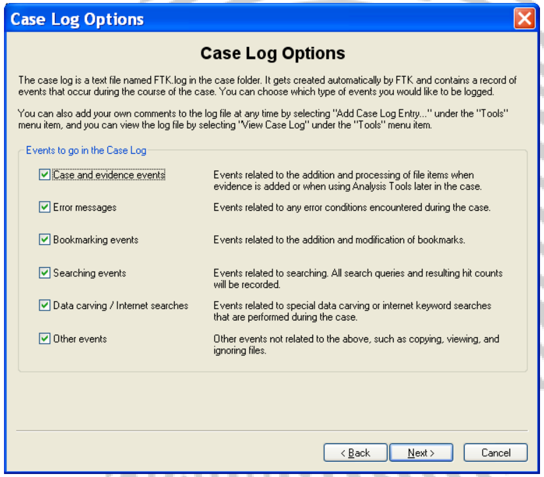
Available Tools

Tools

FTK

- Advanced Code Breaking and Password Recover.
- Full Unicode and Code Page Support.
- Advanced Email Support.
- Powerful Search Functionality.
- Registry Supplemental Reports.
- Easy to use interface.

NOT FREE



Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

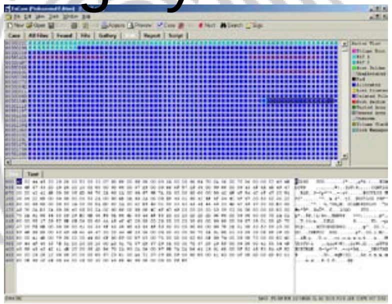
☑ Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
☑ Error messages	Events related to any error conditions encountered during the case.
☑ Bookmarking events	Events related to the addition and modification of bookmarks.
☑ Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
☑ Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
☑ Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

Tools

Encase

- Securely investigate/analyze many machines simultaneously.
- Limit incident impact and eliminate system downtime with immediate response capabilities.
- Investigate and analyze multiple platforms.
- Efficiently collect only potentially relevant data.
- Audit large groups of machines for sensitive or classified information.
- Identify fraud, security events and employee integrity issues.

NOT FREE



Tools

Seluthkit

- Collection of UNIX-based command line file and volume system forensic analysis tools
- Analyzes raw (i.e. *dd*), Expert Witness (i.e. EnCase) and AFF file system and disk images.
- Various analysis Techniques- meta-data structure analysis, time line generation, sort files based on their types etc.

OPEN SOURCE

Tools

Autopsy

- GUI for *Sleuthkit*
- Dead analysis and live analysis
- Case management using client server model
- Various analysis Techniques- meta-data structure analysis, keyword search, time line generation, sort files based on their types etc.

OPEN SOURCE

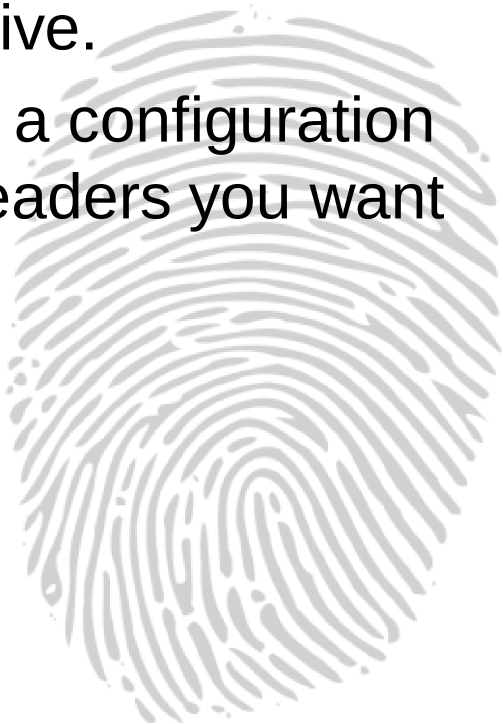
Tools

Foremost and scalpel

- Linux program to recover files based on their headers and footers.
- Can work on image files, such as those generated by *dd*, Safeback, Encase, etc, or directly on a drive.
- The headers and footers are specified by a configuration file, so you can pick and choose which headers you want to look for.

OPEN SOURCE

Not much user friendly



Tools

PyFlag

- PyFlag is a forensic and log analysis GUI and computer forensics framework written in python.
- Basically it provides features for log analysis, disk forensic and network forensic.
- Disk forensic - extracting forensic information from hard disk images, keyword search , MD5 hash comparison.
- log analysis.
- network forensic.

OPEN SOURCE

Not much user friendly

Tools

PTK

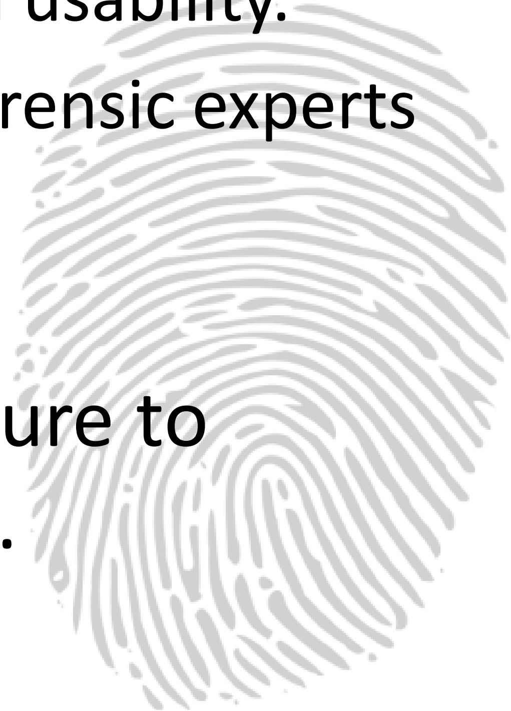
- Enhanced GUI for *Sleuthkit*- extended version of autopsy
- Indexing Engine
- Disk image integrity.
- Various analysis Techniques- meta-data structure analysis, keyword search, time line generation, gallery, file filtering etc.

NOW FULL VERSION IS NOT OPEN SOURCE

Tools

FIT4D

- A software toolkit utilizes the limited resources in developing countries.
  - Improves the efficiency, privacy and usability.
  - Addresses the problem of lack of forensic experts in developing countries.
- A low-cost, distributed infrastructure to deploy the FIT4D software toolkit.



Comparison Between PTK and FIT4D Features

Feature	PTK	FIT4D
Creating disk images		√
Searching /filtering the disk image.	√	√
Analysis and searching disk image piece wise		√
Report generation	√	√
Graphics processing tools		√
Compare file content within the image		√
Attach legal documents such as court orders to the case		√
Evidence not stored in a central server		√
Dynamic Timeline	√	√
Multiple investigators and case lock	√	√

Demonstration