Overview of Computer (Digital) Forensics

CIS 3003, Introduction to Information Technology
Dr. Sheau-Dong Lang (lang@cs.ucf.edu)
Computer forensics is largely a response to a demand for service from the law enforcement community [Noblett, Pollitt, and Presley]. The term "Computer Forensics" was coined in 1991 in the first training session held by the International Association of Computer Investigative Specialists (IACIS, http://www.cops.org) in Portland, Oregon [Marcella and Greenfield]. Computer forensics is “the application of science and engineering to the legal problem of digital evidence” [Sammes and Jenkinson].

Roles of computer (or digital device) played in digital crime investigations:

- as the instrument used in committing a crime (an intruder or a computer virus writer using computers in illegal activities)
- as the victim (a comprised system, data stolen or deleted)
- as a container or storage warehouse for a crime (a cell phone that has pictures of a stolen car, text messages with suspects)

- The Digital Evidence discipline became part of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board’s (ASCLD/LAB) accreditation program in April 2003, see articles by John J. Barbara, Mark Pollitt, and Carrie Whitcomb discussing the efforts led by the SWGDE (Scientific Working Group on Digital Evidence)
- Formation of the new Digital and Multimedia Sciences Section of the American Academy of Forensic Sciences, 2/20/2008
As personal computers and access to the Internet become more prevalent the modern society is increasingly dependent on the computer and networking technologies for storing, processing, and sharing data, and for email and message communication.

The proliferation of computers has made computer-based systems and computer networks easy targets for criminal activities.

“Computer crimes were originally thought of just in the terms of hackers and virus makers, mainly due to the fact that at first only a few geeks had access to computers, but now anyone can point and click and use a computer to commit just about any crime,” Sgt. Stenger, OCSO Computer Crime Squad
Computer (or digital) forensics involves the following steps in handling of digital evidence:

- preservation (acquiring evidence without tampering, chain of custody, transport and storage, collecting data within legal constraints)
- identification (labeling each item of evidence, bagging and tagging, identifying with case number, descriptions, date/time of collection, signatures of handlers)
- extraction (authenticating evidence using hashes, using tools and established procedures for data analysis, keyword searches, hex and graphics viewer, establishing timeline of events, corroborating evidence, who-what-when-where-why-how)
- documentation (actions taken during investigation, the findings)
- interpretation (testifying and presentation in the court, as an examiner or expert, see a recent news article)
Computer (Digital) forensics tools:

Features provided to aid in forensic examination:
- Recover previously deleted files and folders
- Recognize disk partitions and common file systems (Windows FAT and NTFS, Linux ext2 and ext3, Unix UFS)
- Carve graphics and other files of known signatures from unallocated disk clusters
- Search strings using regular expressions
- Review registry files (on Microsoft Windows systems)
- Recover user passwords
- Recover emails and instant messages (IMs)
- Provide timelines of file access activities based on date/time stamps
- Identify known files based on hash sets
- Identify artifacts specific to the operating system on disk
Host-based computer forensics vs. network forensics:

- host-based forensics deals with personal or desktop devices, small enough to be taken down and imaged for analysis
- network forensics deals with servers, company databases, network devices such as routers, firewalls, intrusion detection

Three issues involved in computer forensics investigations:

- technical (the can-we issue): are there tools to extract the necessary evidence, does the investigator have the expertise
- legal (the may-we issue): is there violation of the 4th amendment of the US Constitution which guards against unreasonable search and seizure, digital wiretapping
- ethical (the should-we issue): ethical concerns relating to the use of computer forensics include proper use of prosecutorial and police discretion (see “Computer forensics: admissibility of evidence in criminal cases” by Jerry Wegman)
Email and IM investigations:

- find email artifacts in client-based email (e.g., Outlook’s PST files, Outlook Express DBX files) and web-based email (Yahoo, Hotmail)
- use FTK or open-source tools libPST (for Outlook), Eindeutig (for Outlook Express), AOL clients (for AOL email) to reconstruct emails
- apply string searches (grep) to filter relevant emails and instant messages (IMs)
- track email origins (reading email header information)
Windows Registry Files:

- identify installed applications (date/time, configurations, deleted applications)
- identify installed malicious code (compromised systems with virus, rootkit, spyware programs)
- identify “most recently used” documents to understand recent activities on a computer
- identify USB devices connected to the computer
- use FTK registry viewer (or regedit) to view registry files
Internet Web-browsing Activity:

- Internet Explorer (IE) uses history, cookies, and temporary Internet Files (i.e. Internet cache) to save web activities.
- Use FTK or open-source tools Pasco and Galleta to view browsing activities (both Pasco and Galleta are available at [http://sourceforge.net/docman/?group_id=78332](http://sourceforge.net/docman/?group_id=78332)).
- Use Paraben’s Netanalysis (commercial tool) for Internet cache, history, cookies, even in unallocated clusters.
- Two articles written by Keith J. Jones and Rohyt Belani about web browser forensics (for IE and Mozilla/Firefox history and cache files) are [http://www.securityfocus.com/infocus/1827](http://www.securityfocus.com/infocus/1827) and [http://www.securityfocus.com/infocus/1832](http://www.securityfocus.com/infocus/1832).
Live system forensics and incident response:

- extract information about running applications (processes), open files, network connections, data contained in RAM
- server machines that cannot be shut down or have too much data requiring filtering from live system
- real time forensic analysis on remote systems (e.g., EnCase Enterprise edition) in corporate environments
- open-source tools Helix and FIRE provide support for live system forensics
- two articles ([1](#), [2](#)) on forensic analysis of live Linux systems
Static and dynamic analysis of unknown executables:

- Malicious codes such as virus, rootkit, spyware are executable (binary) files.

- String searches of executables may reveal minimum information regarding the code’s functionality.

- A disassembler such as OllyDbg features an intuitive user interface, advanced code analysis capable of recognizing procedures, loops, API calls, switches, tables, constants and strings, an ability to attach to a running program, and good multi-thread support.

- A disassembler and debugger such as IDA Pro provides controlled execution and debugging of executables allowing user interactions and analysis of runtime behaviors.
Data Analysis:

- Forensic examiners typically are given some background information from the investigator (case agent) – things like names, addresses, time window, types of files (spreadsheets, pictures, movies), installed applications -- that will aid the examination phase.

- Experienced examiners know where (files, folders, Windows registry) to look for relevant evidence, how to corroborate evidences, and how to get the most out of forensic tools.
AccessData’s FTK:

The initial screen (Overview tab selected) for an open case in FTK
AccessData’s FTK (cont’d):

Graphics tab selected for an open case in FTK
AccessData’s FTK (cont’d):

Search results in FTK

**Enter search term**

**Search Results**

**Viewer of the search hits**

**File List**
AccessData’s FTK (cont’d):

FTK Email Viewer
AccessData’s FTK (cont’d):

FTK Cookie Viewer
Other Forensics Tools:

Guidance Software’s EnCase
Other Forensics Tools (cont’d):

![TSK/Autopsy’s Interface for File Analysis](image)

- File List
- Viewer for selected file
Helix live system analysis:

Helix initial screen
Helix live system analysis (cont’d):

Built-in tools on Helix CD
Using Helix to image disk:

Helix uses dd (data dump) to duplicate disks (see explanation of the command syntax and options at http://www.softpanorama.org/Tools/dd.shtml)
Using helix to image a floppy disk (cont’d):
Audit.log file after dd is complete:
Forensics Software Tools:

- Guidance Software's EnCase (commercial, requires license dongle)
- Access Data Forensic Toolkit (commercial, runs in demo mode without license dongle)
- Penguin Sleuth (knock-off of Knoppix with extra forensic tools)
- Helix (another knock-off): booting from Penguin Sleuth or Helix will boot all drives Read-Only, boots into Linux in RAM (with more than 128MB of RAM)
- The Sleuth Kit consists of command-line tools and a browser-like front-end Autopsy
- Spada (Law Enforcement only, also a knock-off)
- AccessData’s FTK Imager (does not require license dongle)
Forensics Software Tools (cont’d):

- **Norton Utilities/SystemWorks** (DiskEdit is the primary one)
  * Unerase - in 2003 and earlier
  * Unformat - in 2003 and earlier
  * gDisk - in 2003 and earlier
- **WhatFormat, FileAlyzer**: tools to analyze files
- **Quick View Plus**: views many different file types (read-only)
- **WinHex**: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor

Forensic Report:

FTK’s Case Report
Careers in Computer Forensics:

- An article on computer forensics careers available at http://About.com under careers > tech careers > computer jobs
- Monster.com’s career advices on computer forensics
- Search http://www.careerbuilder.com/ entering keywords “computer forensics”

It is a tough job to be a computer forensics expert: “In view of the above I find that the defendants have not met their burden of showing by a preponderance of the evidence that Moshlak's methodologies are reliable under Federal Rule of Evidence 702, or would otherwise assist the jury to understand the evidence or to determine a fact in issue. Therefore, it is my recommendation that plaintiff's motion to exclude Moshlak as an expert witness at trial be GRANTED.” in United States District Court, D. Puerto Rico, Nilda RIVERA-CRUZ, Plaintiff, v. LATIMER, BIAGGI, RACHID & GODREAU, LLP, et al., Defendants,.Civil No. 04-2377 (ADC). June 16, 2008.
The Defendants' expert witness Mr. Steven Moshlak contacted me via email on 11/29/2008 and gave the following response to the ruling of the Daubert Hearing:

"After reading Chief Magistrate-Judge's R&R (Report and Recommendation), it was quite contrary to the testimony and exhibits that were presented at the Daubert Hearing. Although the US District Judge assigned to this case relied upon the Magistrate's R&R, she never saw the testimony and the attorneys for the defense should have aggressively pursued the misinformation. No mention of the alteration of the data contained on the hard drive, while in the custody of the Plaintiff's Counsel's Expert, was noted in the R&R, which can impact the credibility of the Plaintiff's case, nor was the testimony cited that the basis for the CF methodology employed is based upon US Department of Justice computer forensics methodologies.

In essence the attorney is responsible for being an advocate of the client and the interface with the court, not the CF person. Thus, the CF person was essentially left "hung-out to dry," due to the systems and circumstances beyond the control of the CF person in this case."