Edinburgh Napier
UNIVERSITY

CSN08101
Digital Forensics
Lecture 1A: Introduction to Forensics

Module Leader: Dr Gordon Russell

Lecturers: Robert Ludwiniak

Digital Forensics

You will learn in this module:

- The principals of computer and digital forensics a theoretical and practical perspective.
- The skills to apply analytical and evaluative techniques in the use of digital forensic tools within a variety of computer environments.
- The fundamental ethical and professional issues associated with the use of digital forensics, as well as the role of related professional and regulatory bodies.

Practical Work

- You will learn practical skills using some well known forensic tools.
- Mostly the practicals using the Caine environment.
  - This uses The Forensic Sleuth Toolkit (FST), including autopsy.
  - This allows you to perform forensics on a variety of information sources.
- Caine is a Linux environment, based on Ubuntu/Debian.
- The first few weeks of the module includes an introduction to Linux appropriate to get you going with Caine.
- The majority of the remainder of the module focuses on the use of linux-based tools to perform computer forensics.

Recommended Text

- For Linux, any book introducing the linux command line would be fine. We are not going deeply into Linux during this module.
- Recommended book for Forensics:
  - Britz, M. J. (2008) Computer Forensics and Cyber Crime: an introduction. 2nd Edition. New Jersey, USA: Pearson Prentice Hall.
  - Carrier, B., File System Forensic Analysis, March 27 2005, Addison-Wesley Professional
  - Casey, E. (2011) Digital Evidence and Computer Crime. 3rd Edition. London, UK: Academic Press
  - Nelson, B., Phillips, A., Enfinger, F., Steuart, C. (2008) Guide to Computer Forensics and Investigation. 3rd Edition. Boston, USA: Thomson Course Technology.

Online Resources

Digital Forensic Research Workshop (DFRWS)

- http://www.dfrws.org
  - Challenges
  - Projects

National Institute of Standards and Technology (NIST)

- http://www.nist.gov

Journal - Digital Investigation

- http://www.sciencedirect.com

Forensics Wiki

- http://www.forensicswiki.org

Elements Covered

- The module covers some a variety of topics:
- Basic Linux command line and GUI.
- Static Forensics:
  - Introduction to concepts of Computer Forensics and Digital Forensics with respect to digital evidence
  - Introduction to principles involved in Digital Forensic investigations
  - Ethical and professional issues related to Digital Forensics
  - Introduction to forensic techniques used in the examination of end-devices covering boot disks, file systems, system registry, timeline of events, web browsers, email, log files, and network traces.
  - Introduction to open source and commercial forensic tools

Timetable

- You should attend 2 hours of lectures + 2 hours of practicals per week.
- Lectures will be mostly “lecturing”, but will also include group tutorial sessions and deminstrations.
- Attendance will be taken at all events.

Practicals

- These run using any networked PCs.
  - You must have Java installed and allow java applets.
  - Your network must allow direct HTTP (including HTTP Connect), and at least 1 of either Telnet (port 23) or SSH (port 22).
  - You need a good reliable network connection.
- The environment is available online from http://linuxzoo.net
  - We are following the Caine 2.5.1 tutorials. Other tutorials are used in other modules.

Assessment

- There are 2 assessments in this module:
  - A supervised class test in the form of a Short Answer Written Exam.
    - This is worth 40% of the module.
    - This runs in week 7 during your timetabled practical session.
    - The test covers your theoretical understand of Forensics, as well as the initial aspects of practical forensics.
    - This is a closed-book exam.
  - A supervised practical test
    - This is worth 60% of your module marks.
    - This runs in week 13 in your normal practical event.
    - This test asks you to perform various forensic-related tasks within a Caine environment, and you are marked on your ability to produce the data requested.
    - This is an OPEN BOOK exam.

Lectures

- The lectures are 1-2 hours long.
- Lectures are not the source of all knowledge.
- You need to do some reading on your own, and to practice with the Linux machines.
- If you don’t attend the practicals and lectures, and practice what you have learned right from week 1, you will struggle with this module.

Presentation Plan

Module Week	Lecture	Tutorials in Caine 2.5.1 list
1	A: Introduction to Forensics (RL) B: Linux Overview + Caine (GR)	Essentials
2	Essential Linux for Forensics (GR)	Basic
3	Linux Filesystem + Searching (GR)	Search
4	A: Forensic Processes (RL) B: Advanced Search in Linux (GR)	AdvSearch
5	A: PC Boot Process (RL) B: Advanced Linux (GR)	CaineEssentials
6	Forensic Acquisition (RL)	Capture

Module Week	**Lecture**	**Tutorials in Caine 2.5.1 list**
7	Disk Analysis (RL)	store * Short Answer Exam
8	Filesystem Analysis (RL)	files1
9	Data Analysis (RL)	files2
10	A: Registry Forensics (RL) B: Activity/Browser/app/Timeline (RL)	data
11	Encase (RL)	browser
12	Real-World forensic walkthrough (RL)	* Practical Exam

Forensics - Introduction

- Forensic definitions
- Forensic history
- Main forensic concepts

Definitions

Forensic:

> "…a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence)."

The aim of forensic science is:

> "…to demonstrate how digital evidence can be used to reconstruct a crime or incident, identify suspects, apprehend the guilty, defend the innocent, and understand criminal motivations."

Ref: Casey, "Digital Evidence and Computer Crime"

Computer Forensics vs Digital Forensics

“Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud.”

Robbins, Judd , PC Software Forensics

The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from the digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Digital Forensics Research Workshop

Locard's Exchange Principle

It is impossible for the criminal to act, especially considering the intensity of a crime, without leaving traces of his presence

With contact between two items, there will be an exchange

History of Computer/Digital Forensics

1970s

Electronic crimes were increasing, especially in the financial sector.

Most law enforcement officers didn’t know enough about computers to ask the right questions or to preserve evidence for trial.

1980s

PCs gained popularity and different OSs emerged.

Disk Operating System (DOS) was available.

Forensics tools were simple, and most were generated by government agencies.

Mid-1980s

Xtree Gold appeared on the market able to recognize file types and retrieve lost or deleted files.

Norton DiskEdit soon followed and became the best tool for finding deleted files.

History of Computer/Digital Forensics

- 1984
  - Scotland Yard: Computer Crime Unit
  - FBI computer forensics departments

- Early 1990s
  - Tools for computer forensics were available
  - **International Association of Computer Investigative Specialists (IACIS)**
    - Training on software for forensics investigations
  - IRS created search-warrant programs
  - ExpertWitness for the Macintosh
    - First commercial GUI software for computer forensics Created by ASR Data. Recovers deleted files and fragments of deleted files

- 1990
  - Computer Misuse Act (CMA)

Investigative Context

	Primary Objectives	Secondary Objectives	Environment
Law Enforcement	Prosecution		Post-Mortem
Military IW Ops	Continuity of Operations	Prosecution	Real-Time/Post-Mortem
Business and Industry	Continuity of Service	Prosecution	Real-Time/Post-Mortem

Digital Investigation

A *digital investigation* is a process where we develop and test hypotheses that answer questions about digital events. This is done using the scientific method where we develop a hypothesis using evidence that we find and then test the hypothesis by looking for additional evidence that shows the hypothesis is impossible.

Digital Evidence is a digital object that contains reliable information that supports or refutes a hypothesis.

- B. Carrier, 2006
File System Forensic Analysis,

Characteristics of Evidence

1. Data can be viewed at different levels of abstraction
2. Data requires interpretation
3. Data is Fragile
4. Data is Voluminous
5. Data is difficult to associate with reality

Characteristics of Evidence

1. Data can be viewed at different levels of abstraction
2. Data requires interpretation
3. Data is Fragile
4. Data is Voluminous
5. Data is difficult to associate with reality

Characteristics of Evidence

1. Data can be viewed at different levels of abstraction
2. Data requires interpretation
3. Data is Fragile
4. Data is Voluminous
5. Data is difficult to associate with reality

Characteristics of Evidence

1. Data can be viewed at different levels of abstraction
2. Data requires interpretation
3. Data is Fragile
4. Data is Voluminous
5. Data is difficult to associate with reality

Characteristics of Evidence

1. Data can be viewed at different levels of abstraction
2. Data requires interpretation
3. Data is Fragile
4. Data is Voluminous
5. Data is difficult to associate with reality

Investigation Process

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

Investigation Process

According to many professionals, Computer Forensics is a four (4) step process:

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

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 United States and internal laws

Tool Requirements

Usability - Present data at a layer of abstraction that is useful to an investigator

Comprehensive - Present all data to investigator so that both inculpatory and exculpatory evidence can be identified

Accuracy - Tool output must be able to be verified and a margin of error must be given

Deterministic - A tool must produce the same output when given the same rule set and input data.

Verifiable - To ensure accuracy, one must be able to verify the output by having access to the layer inputs and outputs. Verification can be done by hand or a second tool set.

Brian Carrier, 2003, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers

Challenges

- Size of storage devices
- Embedded flash devices
- Proliferation of operating systems and file formats
- Multi-device analysis
- Pervasive Encryption
- Cloud computing
- RAM-only Malware
- Legal Challenges decreasing the scope of forensic investigations

Research Challenges facing the investigation community

- S.L. Garfinkel, ***Digital forensics research: The next 10 years***, Digital Investigation, vol. 1, no. 7, pp. 64-73, 2010
- “The coming Digital Forensics Crisis”

ANY QUESTIONS …

Assessment: Short-Answer Examples

Question:

Describe a role of Acquisition process in Computer Forensic Investigation.

Assessment: Short-Answer Examples

Question:

Describe a role of Acquisition process in Computer Forensic Investigation.

Answer:

Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices

Assessment: Short-Answer Examples

Question:

List and describe minimum two challenges facing Digital Forensics in the next 10 years.

Assessment: Short-Answer Examples

Question:

List and describe minimum two challenges facing Digital Forensics in the next 10 years.

Answer:

Size of storage devices – due to technical advances the size of the storage devices increases with every year. The bigger the storage the more time is required to acquire the storage device and to analyse the data on it.

RAM-only Malware – this type of code is executed in the RAM and it is not written to any storage devices. To be able to trace/analyse the malware live forensic examination is required while the computer device is switched on. It is not possible to analyse the malware using post-mortem forensics.