



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



Network Security (NS)

Lab -

Introduction to Digital Forensics

Faculty of Architecture, Computing & Engineering

School of Applied Computing

Mount Pleasant Campus

Swansea

SA1 6ED

1. INTRODUCTION

1.1 Background

Today, virtually every business and personal document is prepared on a computer and mobile, hand-held devices. E-mail records and pages visited on the Internet yield even more critical information about our daily lives. More importantly, the information stored on a computer can make or break a business or a person or a group of people or a court case.

Computer and digital forensics is the science of retrieving and chronicling evidence located on a computer's hard drives and other sources of Electronically Stored Information (ESI) such as floppies, CDs and DVDs, external drives, thumb drives and voice mail servers, so that it can be presented as evidence in a court of law. It is the use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage.

Computer and digital forensics is useful for the detection and investigation of crime committed on computers, computer networks, the internet and other digital devices with the intent of giving digital evidence in law courts and tribunals. It is also the professional extraction and handling of potential electronic evidence from any digital device or digital storage media to assist investigators, prosecutors, and the trier of fact (Judges, magistrates and members of tribunals) in a criminal justice system in arriving at the right judgment in litigation.

Definition: The practice of computer and digital forensics includes the use of formal, accepted techniques for collecting, analyzing, and presenting suspect data in court, concentrating on rules of evidence, the legal processes, the integrity and perpetuity of evidence, reporting of facts, and the preparation and presentation of expert testimony.

It requires the use of specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.

Similar to all forms of forensic science, computer and digital forensics comprises of the application of the law to computer technology. Computer and digital forensics deals with the preservation, identification, extraction, and documentation of computer evidence. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.

Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. The applications of computer forensics require specialized training and techniques and state of the art forensics tools and software to evaluate the potential usefulness of computer data, to retrieve and interpret "hidden" data from computer media, and to provide chain of custody and data accuracy with court-accepted techniques.

Law-enforcement agencies worldwide have successfully used computer forensics experts to investigate crimes such as fraud, murder, terrorism, hacking, cyber-warfare, money laundering and other cases for many years. But the advent of PCs (personal computers) used by businesses and individuals in recent years has dramatically increased the volume of criminal acts committed with the use of computers.

Hence, digital and computer forensics can be used to investigate the following crimes amongst others:

1. Espionage
2. Terrorism and Treason
3. attacks against National Critical Infrastructure
4. Cyber Terrorism
5. Cyber Warfare
6. Identity Theft
7. Hacking
8. Financial Fraud e.g. e-Payment fraud, ATM fraud etc.
9. Human resource/Payroll Fraud
10. Fraudulent Websites and mails
11. Blackmails
12. Theft
13. Narcotics
14. Homicide
15. Forgery
16. Electoral Fraud
17. Kidnapping
18. Threats and malicious calls
19. Extortion
20. Recovering evidence after formatting hard drive or after evidence deletion
21. Corporate or Governmental internal investigation
22. Law-enforcement investigation
23. Computer Security violations
24. Child Pornography;
25. Corporate or Governmental Policy Violation;
26. Perjury etc.
27. Digital and Computer Forensics can also be used proactively as a preventive tool against cyber-attacks.

Digital or electronic evidence, therefore, is any data stored or transmitted using a computer or similar electronic devices (including phones, hand-held devices) that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent and alibi. It is estimated that over 85 percent of all criminal cases today have one form of digital, electronic or forensic evidence or the other.

2. DIGITAL AND COMPUTER FORENSIC INVESTIGATION

According to the British Association of Chief Police Officers' (ACPO), as information technology is ever developing and as each new development finds a greater role in our lives, the recovery of evidence from electronic devices has now become firmly part of investigative activity in both public and private sector domains.

According to the ACPO, in its Good Practice Guide for Computer-Based Electronic Evidence (www.acpo.police.uk):

“Electronic evidence is valuable evidence and it should be treated in the same manner as traditional forensic evidence - with respect and care. The methods of recovering electronic evidence, whilst maintaining evidential continuity and integrity may seem complex and costly, but experience has shown that, if dealt with correctly, it will produce evidence that is both compelling and cost effective.”

ACPO went further to give four Principles of Computer-Based Electronic Evidence. These are listed and explained below:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Explanation of the ACPO'S principles:

Computer-based electronic evidence is subject to the same rules and laws that apply to documentary evidence. The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of police.

Operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed. In order to comply with the principles of computer-based electronic evidence, wherever practicable, an image should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this impracticable. However, investigators should be careful to ensure that all relevant evidence is captured if this approach is adopted.

In a minority of cases, it may not be possible to obtain an image using a recognized imaging device. In these circumstances, it may become necessary for the original machine to be accessed to recover the evidence. With this in mind, it is essential that a witness, who is competent to give evidence to a court of law makes any such access.

It is essential to display objectivity in a court, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

2.1 The Nature of Computer-Based Electronic Evidence

Digital and Computer Forensics is the application of science and technology to law in the search for truth in civil, criminal, and social behavioural matters to the end that injustice shall not be done to any member of society.

It can also be defined as the acquisition, preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis using well-defined and approved methodologies and procedures.

It is also the study of network traffic to search for truth in civil, criminal, and administrative matters to protect users and resources from exploitation, invasion of privacy, and any other crime fostered by the continual expansion of network connectivity.

2.2 To determine the evidential value of crime scene and related evidence.

Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer. As such, this evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence is latent.

In its natural state, we cannot see what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence available. Testimony may be required to explain the examination and any process limitations. Computer-based electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

2.3 Functions of the Digital and Computer Forensic Examiner

The functions of digital forensic examiner are:

(a) Analysis of Physical / Electronic Evidence

- (b) Provision of Expert Opinion/ Testimony
- (c) Furnishes training in the proper Recognition, Collection, Analysis and Preservation of physical / electronic evidence.

2.4 Methodology of Digital Forensics

- (a) Acquire the evidence without altering or damaging the original.
- (b) Authenticate that the recovered evidence is the same as the original seized.
- (c) Analyze the data without modifying it.

2.5 Categories of Digital Evidence

- 1. Hardware
- 2. Software
 - a. Data
 - b. Programs

2.6 Digital Evidence

Digital data that can establish that:

- 1. A crime has been committed or
- 2. Can provide a link between a crime and its victim or
- 3. Provide a link between a crime and its perpetrator.

2.7 Categories of Digital Evidence

Digital evidence can be categorised into the following:

- 1. Text
- 2. Audio
- 3. Image
- 4. Video

2.8 Where Digital Forensic Evidence Resides

Digital Forensics evidence resides in Computer systems, Laptops, Phone and Mobile devices, etc. They are found in the following areas:

- 1. Logical file system
- 2. File system
- 3. Files, directories and folders, FAT, Clusters, Partitions, Sectors, Random Access memory,
- 4. Physical storage media such as HDD, CD, Flash-Drives, etc.
- 5. Slack space: space allocated to file but not actually used due internal fragmentation

6. Unallocated space

4. DIGITAL FORENSICS TOOLS

Over the last decade, several digital forensics tools have surfaced in the market. Some of these tools are proprietary technologies, while others are free open source. Most of the forensics tools, especially the proprietary ones, are widely accepted in courts of law around the globe. Different forensics tools do different things. There are many digital forensics tools, too numerous to mention here. Some of the popular forensics tools are outlined below.

Digital Forensics Tool	Usage	Licence
1. Encase	This is a general purpose forensics tool. It is the most comprehensive and widely accepted global standard tool for digital forensics examination.	Not Free.
2. Access Data FTK Forensics Tools	The FTK is the second most popular proprietary digital forensics tool in the market. It is also a general purpose tool capable of performing several forensics analysis tasks.	Not Free (But the FTK Imager is free).
3. Belkasoft	This is a relatively new entrant to the proprietary forensics tool market. The Russian product tries to compete with Encase and	Not Free
4. CAINE	The CAINE Live Forensic Tool is a bootable DVD in Linux. It can also be run from windows as a stand alone application.	Free Open Source.

DIGITAL FORENSICS TOOL: CAINE

Switch your PC on without the CAINE DVD in the drive. After a successful boot-up, insert the CAINE DVD. It should auto-run and load a program called Win-UFO.exe. If your DVD fails to auto-run, use the Windows explorer to browse the CAINE DVD and double click on the Win-UFO.exe file. If it asks you for administrator's password, this will be furnished to you by your Module Leader. Type the admin password and click on 'Ye'. The CAINE application will load as shown in Figure 1 below.

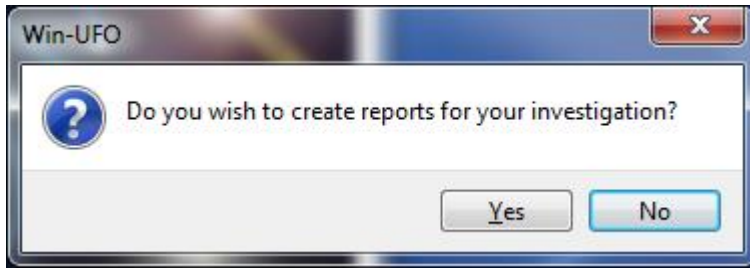


Figure 1: Creating Reports option.

Click on the 'Yes' button to close the window in Figure 1. Under normal circumstance, you would like to click on the 'Yes' button, so that CAINE automatically generates for you a report of your forensics investigation. License agreement window will pop up. Accept the agreement. Select a destination on your computer to create a folder where your forensics reports will be saved as shown in Figure 2 below.

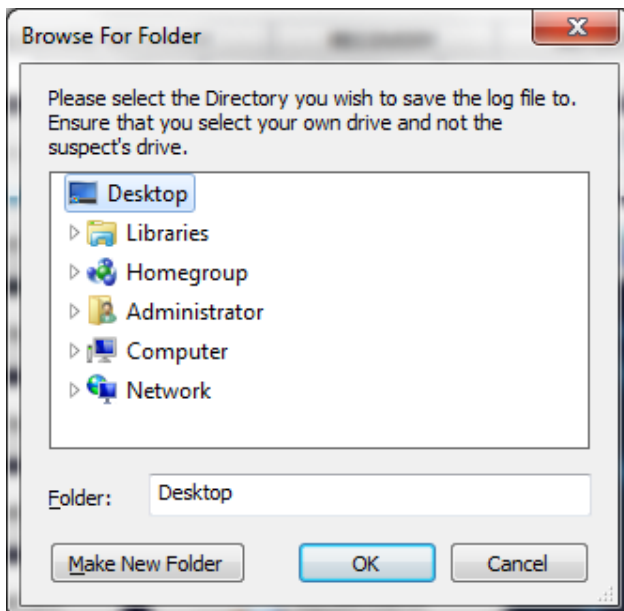


Figure 2: Creating folder for saving reports.

Select the 'Make New Folder' button and create a folder on your desktop called 'Forensics Reports'. Click on 'OK' button and close the window. You are now ready to use the array of forensics tools available in the CAINE DVD. This is called Ultimate Forensics Outflow.



Figure 3: Win-UFO programs.

In the next lab session, you will learn how to conduct real life forensics investigation using some of the applications in Win-UFO.