# CST902: DIGITAL FORENSICS & INCIDENT RESPONSE

## AFRICA CENTRE OF EXCELLENCE ON TECHNOLOGY ENHANCED LEARNING (ACETEL)

## NATIONAL OPEN UNIVERSITY OF NIGERIA

# Course Guide for CST902

## Introduction

CST902 – Digital Forensics and Incident Response is a 3-credit unit. The course is a core course in second semester. It will take you 15 weeks to complete the course. You are to spend 91 hours of study for a period of 13 weeks while the first week is for orientation and the last week is for end of semester examination. The credit earned in this course is part of the requirement for graduation.

You will receive the course material which you can read online or download and read off-line. The online course material is integrated in the Learning Management System (LMS). All activities in this course will be held in the LMS. All you need to know in this course is presented in the following sub-headings.

## Course Competencies

By the end of this course, you will gain competency to:

- Perform Forensic Analysis of Data, Systems and Network

## Course Objective

The course objective is to:

- Conduct forensic investigations on digital devices that conform to accepted professional standards and are based on the investigative process.

## Working Through this Course

The course is divided into modules and units. The modules are derived from the course competencies and objectives. The competencies will guide you on the skills you will gain at the end of this course. So, as you work through the course, reflect on the competencies to ensure mastery. The units are components of the modules. Each unit is sub-divided into introduction, intended learning outcome(s), main content, self-assessment exercise(s), conclusion, summary, and further readings. The introduction introduces you to the unit topic. The intended learning outcome(s) is the central point which help to measure your achievement or success in the course. Therefore, study

the intended learning outcome(s) before going to the main content and at the end of the unit, revisit the intended learning outcome(s) to check if you have achieved the learning outcomes. Work through the unit again if you have not attained the stated learning outcomes.

The main content is the body of knowledge in the unit. Self-assessment exercises are embedded in the content which helps you to evaluate your mastery of the competencies. The conclusion gives you the takeaway while the summary is a brief of the knowledge presented in the unit. The final part is the further readings. This takes you to where you can read more on the knowledge or topic presented in the unit. The modules and units are presented as follows:

**Module 1 Fundamentals Digital Forensics**
Unit 1 Overview of digital forensics
Unit 2 Investigative methods and processes

**Module 2 Operating Systems**
Unit 1 Windows OS
Unit 2 Linux OS
Unit 3 Mac OS

**Module 3 Advanced Forensics**
Unit 1 Filesystem Forensics
Unit 2 Network Forensics
Unit 3 Cloud Forensics
Unit 4 Web browser Forensics
Unit 5 Mobile Forensics
Unit 6 Social Media Forensics

**Module 4 Incidence Management**
Unit 1 Incidence Response
Unit 2 Incidence Handling

There are thirteen units in this course. Each unit represent a week of study.

# Presentation Schedule

The weekly activities are presented in Table 1 while the required hours of study and the activities are presented in Table 2. This will guide your study time. You may spend more time in completing each module or unit.

**Table I: Weekly Activities**

| Week | Activity |
|---|---|
| 1 | Orientation and course guide |
| 2 | Module 1 Unit 1 |
| 3 | Module 1 Unit 2 |
| 4 | Module 2 Unit 1 |
| 5 | Module 2 Unit 2 |
| 6 | Module 2 Unit 3 |
| 7 | Module 3 Unit 1 |
| 8 | Module 3 Unit 2 |
| 9 | Module 3 Unit 3 |
| 10 | |
| 11 | Module 3 Unit 1 |
| 12 | Module 3 Unit 2 |
| 13 | Module 3 Unit 3 |
| 14 | Revision and response to questionnaire |
| 15 | Examination |

The activities in Table I include facilitation hours (synchronous and asynchronous), assignments, mini projects, and laboratory practical. How do you know the hours to spend on each? A guide is presented in Table 2.

**Table 2: Required Minimum Hours of Study**

| S/N | Activity | Hour per Week | Hour per Semester |
|---|---|---|---|
| 1 | Synchronous Facilitation (Video Conferencing) | 2 | 26 |
| 2 | Asynchronous Facilitation (Read and respond to posts including facilitator's comment, self-study) | 4 | 52 |
| 3 | Assignments, mini-project, laboratory practical and portfolios | 1 | 13 |
| | Total | 7 | 91 |

# Assessment

Table 3 presents the mode you will be assessed.

**Table 3: Assessment**

| S/N | Method of Assessment | Score (%) |
|---|---|---|
| 1 | Portfolios | 10 |
| 2 | Mini Projects with presentation | 20 |
| 3 | Laboratory Practical | 20 |
| 4 | Assignments | 10 |
| 5 | Final Examination | 40 |
| Total | | 100 |

# Portfolio

A portfolio has been created for you tagged "**My Portfolio**". With the use of Microsoft Word, state the knowledge you gained in every Module and in not more than three sentences explain how you were able to apply the knowledge to solve problems or challenges in your context or how you intend to apply the knowledge. Use this Table format:

# Application of Knowledge Gained

| Module | Topic | Knowledge Gained | Application of Knowledge Gained |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

You may be required to present your portfolio to a constituted panel.

# Mini Projects with presentation

You are to work on the project according to specification. You may be required to defend your project. You will receive feedback on your project defence or after scoring. This project is different from your thesis.

## Laboratory Practical

The laboratory practical may be virtual or face-to-face or both depending on the nature of the activity. You will receive further guidance from your facilitator.

## Assignments

Take the assignment and click on the submission button to submit. The assignment will be scored, and you will receive a feedback.

## Examination

Finally, the examination will help to test the cognitive domain. The test items will be mostly application, and evaluation test items that will lead to creation of new knowledge/idea.

## How to get the Most from the Course

To get the most in this course, you:

- Need a personal laptop. The use of mobile phone only may not give you the desirable environment to work.
- Need regular and stable internet.
- Need to install the recommended software.
- Must work through the course step by step starting with the programme orientation.
- Must not plagiarise or impersonate. These are serious offences that could terminate your studentship. Plagiarism check will be used to run all your submissions.
- Must do all the assessments following given instructions.
- Must create time daily to attend to your study.

## Facilitation

There will be two forms of facilitation – synchronous and asynchronous. The synchronous will be held through video conferencing according to weekly schedule. During the synchronous facilitation:

- There will be two hours of online real time contact per week making a total of 26 hours for thirteen weeks of study time.

- At the end of each video conferencing, the video will be uploaded for view at your pace.
- You are to read the course material and do other assignments as may be given before video conferencing time.
- The facilitator will concentrate on main themes.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.
- Coordinate activities in the platform.
- Score and grade activities when need be.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcasts if need be.

Read all the comments and notes of your facilitator especially on your assignments, participate in forum discussions. This will give you opportunity to socialise with others in the course and build your skill for teamwork. You can raise any challenge encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the synchronous session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help ACETEL to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

# Learner Support

You will receive the following support:

- Technical Support: There will be contact number(s), email address and chatbot on the Learning Management System where you can chat or send message to get assistance and guidance any time during the course.

- 24/7 communication: You can send personal mail to your facilitator and the centre at any time of the day. You will receive answer to you mails within 24 hours. There is also opportunity for personal or group chats at any time of the day with those that are online.

- You will receive guidance and feedback on your assessments, academic progress, and receive help to resolve challenges facing your stuides.

# Course Information

| | |
|---|---|
| Course Code: | CST 902 |
| Course Title: | Digital Forensics and Incident Response |
| Credit Unit: | 3 |
| Course Status: | Compulsory |
| Course Blurb: | This course covers the principles and techniques for digital forensics investigation. Students will learn forensic investigation on both Linux and Windows systems, filesystems and network forensics. |
| Semester: | Second |
| Course Duration: | 13 Weeks |
| Required Hours for Study: | 91 |

# Course Team

| | |
|---|---|
| Course Developer: | ACETEL |
| Course Writers: | Dr Zareefa Mustafa and Dr Imsaila Idris |
| Content Editor: | Dr Ismaila Idris |
| Instructional Designers: | Inegbedion, Juliet O. (PhD) and Dr Lukuman Bello |
| Learning Technologists: | Dr Adewale Adesina and Mr Miracle David |
| Graphic Artist: | Mr Henry Udeh |
| Proofreader: | Mr Awe Olaniyan Joseph |

# Module 1: Fundamentals Digital Forensics

## Module Introduction

Technology has brought about significant improvement in our lives, from online grocery shopping to e-learning, automated farming, remote-controlled surveillance systems and smart homes. All these have one thing in common, which is the Internet. While the low cost of data and the availability of cheap smart devices has created a lot of opportunities, some use this for nefarious purposes. Criminals use technology to commit crimes, crimes committed using digital devices and computer network, such as the internet is called cybercrime. Computers can be used as instruments to commit a crime, can be the target of a crime or can be used to store illegal data (Wall, 2007). Every year, countries lose billions of dollars as a result of cybercrime. In its 2018 report, the Internet Crime Complaint Centre (IC3) reported that victims lost $2.7 billion due to cybercrime and between 2014 to 2018, a total loss of $7.45 billion (IC3, no date). How can such crimes be investigated, the answer is through digital forensics.

This module will introduce students to the concepts of digital forensics, and the module is broken down into the following units:

Unit 1: Overview of Digital Forensics
Unit 2: Investigative Methods and Processes

## Unit 1: Overview of Digital Forensics

### Contents

# 1.0 Introduction

As with any type of crime, the purpose of digital forensics investigation is to know who, what, when, where, why, and how of the crime. Digital forensics is the process of extracting evidence from a digital device using processes and tools that preserve the integrity of the evidence so that such evidence may be used in the court of law. This unit will present various definitions of digital forensics, its classifications and standards.

# 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define digital forensics
- evaluate the concepts of digital forensics
- apply the concepts of digital forensics to an investigation

# 3.0 Main Content

## 3.1 Definition of Digital Forensics

One of the earliest definitions of computer forensics is attributed to McKemmish (1999), who defines it as "the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable". This definition listed the processes involved in conducting a digital investigation.

At the maiden edition of the Digital Forensics Research Workshop titled "A Road Map for Digital Forensic Research," the participants comprising university researchers, computer forensic examiners, and analysts proposed several definitions of digital forensics. They came up with a more encompassing definition as "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources to facilitate or further the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations."(DFRWS, 2001). This definition, while also listing the processes, went further to add the importance of using scientifically validated methods to ensure that such

evidence can be used in the court of law. These definitions show that acquiring admissible evidence is vital to the digital investigation. For evidence to be legally acceptable, it must satisfy the rule of evidence. Therefore evidence should be relevant, authentic and credible, and competent (Graves, 2013).

Evidence acquired from digital devices is referred to as digital evidence. This is defined as data that can be used to

- Establish that a crime has been committed
- Provide a link between a crime to its victim
- Provide a link between a crime and its perpetrator (Casey, 2004).

Digital evidence can be in the form of text, audio, image, or video and binary data. And it can be found in various computing devices such as stand-alone or networked computer systems, mobile devices, host systems, network and peripheral devices. Similarly, it may be applied in criminal investigations, civil investigations, administrative investigations and research.

What are other sources of digital evidence apart from those listed above?

Game consoles, smart TV, washing machines etc

## 3.2 Classification of Digital Forensics

Digital forensics may be classified based on the device type, evidence source. Examples are:

**Computer forensics**: This is a branch of digital forensics that is concerned with investigating a computer system such as a desktop computer and laptop.

**Software forensics**: This examines software code to determine if a crime has been committed. It is usually applied in intellectual property (IP) disputes, copyright infringement or theft.

**Mobile device forensics**: This involves analysing mobile devices such as mobile phones, tablets, smart swatches, game consoles, etc., to acquire evidence.

**Network forensics:** This focuses on analysing data from a computer network. As a network is an interconnection of computers, evidence may be distributed amongst the devices connected to a network, such evidence when analysed could be used to establish that a crime has occurred (Casey, 2011).

**Database forensics:** This involves examining databases to acquire evidence in criminal activities.

**Cloud forensics:** This is the use of digital investigation processes and procedures to extract evidence that can be used to show that crime has occurred.

Others include Internet forensics, Filesystem forensics, video/audio forensics, memory forensics, document forensics etc. are all branches of digital forensics. Internet forensics focuses on investigating user activities on the internet; video/audio forensics focuses on analysing audio and video files, memory forensics involves collecting and analysing memory dump while document forensics investigates documents to acquire evidence.

## 3.3 Standards of Digital Forensics

Currently, there is no universally adopted standard or guidelines for digital forensics investigations, but there are several which digital forensic investigators and law enforcement agencies have adopted. These are:

### 3.3.1 Guideline for Digital Forensics

**Rules of Forensic Computing** (McKemmish, 1999)

- Minimal handling of the original to minimise alteration
- Account for any change by documenting the nature, extent and reason for doing so
- Comply with the rules of evidence
- Do not exceed personal knowledge

**The Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence version 5 (ACPO, 2012)**

Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data, 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 digital 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 has overall responsibility for ensuring that the law and these principles are adhered to

**International Organisation on Computer Evidence (IOCE): Guidelines for Best Practice in the Forensic Examination of Digital Technology** (Adams, 2013)

- The general rules of evidence should be applied to all digital evidence.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When a person must access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken concerning digital evidence while that digital evidence is in their possession.

**Council of Europe (CoE) Electronic Evidence Guide** (Jones *et al.*, 2014)
Principle 1: No action taken should materially change any data, electronic device or media which may subsequently be used as evidence in court.

Principle 2: A record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions but also to achieve the same result.

Principle 3: If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/ external advisers in time and arrange their presence if possible.

Principle 4: First responders must have the necessary and appropriate training to be able to search for and seize electronic evidence if no specialists are available at the scene.

Principle 5: The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter.

These guidelines are similar, and all emphasise on the preservation of evidence to ensure that its integrity is not compromised, the importance of audit trail to check the process followed, and competence of the examiner to ensure that only examiners with the required expertise are used. All these are to ensure that evidence acquired during an investigation is admissible.

### 3.3.2 Standards for Digital Forensics

International Organisation for Standardisation (ISO) has published several standards on digital investigations to ensure that standard processes and methods are maintained during an investigation (ISO, 2015). These standards are:

- ISO/IEC 27041:2015 - Guidance on assuring suitability and adequacy of the incident investigative method.
- ISO/IEC 27043:2015 - Incident investigation principles and processes.
- ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence.
- ISO/IEC 27042:2015 - Guidelines for the analysis and interpretation of digital evidence.

 Discussion

The guidelines on the digital investigation have not changed much over the years; can these be applied to crimes involving emerging technologies? Buttress your position with happenings in your context. Post your response on the forum page.

The guidelines can be applied, with emphasis on preserving evidence and keeping an audit trail.

# 4.0 Self-Assessment Exercise(s)

1. How has digital forensics evolved over time?
   Emerging technologies have changed traditional digital forensics, such as cloud computing, internet of things social media, smart devices etc. Data is no longer saved on computers, but on third party remote servers, access to such servers could be a challenge.

2. Are there guidelines for digital forensic investigations in Nigeria?
   Currently, there are no guidelines for digital investigations in Nigeria. However, a draft Standards for Digital and Computer Forensics in Nigeria was proposed in 2014 by the National Information Technology Development Agency, but it has not been implemented.

3. What are the uses of digital forensics?
   a. Training
   b. Domestic dispute
   c. Civil investigations
   d. All of the above
   e. None of the above

   Answer: *C*

# 5.0 Conclusion

Digital forensics enables investigators to examine digital systems in order to establish that a crime has been committed. Digital forensics has various sub-categories, and each is concerned with extracting and analysing data that can be used as evidence in criminal, civil or administrative investigations. There are guidelines which need to be followed to ensure that evidence is legally acceptable.

# 6.0 Summary

This unit introduced the concepts of digital forensics. The definitions of digital forensics were discussed, selected sub-categories were explained, and some of the guidelines for digital forensics investigations were highlighted to give all-rounded information on the purpose of digital forensics and its importance in today's' society. As shown in the definitions, there are processes of conducting digital forensics investigations. Therefore, the next unit will examine some of these process models.

# 7.0 Further Readings


ACPO (2012). *ACPO Good Practice Guide for Digital Evidence*. Retrieved on 19 January 2016 from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Adams, R. (2013) 'The Emergence of Cloud Storage and the Need for a New Digital Forensic Process Model', in Ruan, K. (ed.). *IGI Global.*

Casey, E. (2004). *Digital Evidence and Computer Crime*. Academic Press.

Casey, E. (2011). Digital *Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

DFRWS (2001) 'A Road Map for Digital Forensic Research', Proceedings of the 2001 Digital Forensics Research Workshop (, pp. 1–42. doi: 10.1111/j.1365-2656.2005.01025.x.

Graves, M. W. (2013). *Digital Archaeology: The Art and Science of Digital Forensics*. (1st ed.). Upper Saddle River, N.J: Addison-Wesley.

IC3 (no date) "2018 Internet Crime Report, Internet Crime Complaint Center." Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf.

ISO (2015). ISO - ISO Standards - ISO/IEC JTC 1/SC 27 - IT Security techniques. Retrieved on 21 March 2016 from http://www. iso. org/ iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45 306&published=on&includesc=true

Jones, N. et al. (2014). Electronic Evidence Guide- A Basic Guide for Police Officers, Prosecutors And Judges. Retrieved on 25 February 2016 from https://rm.coe.int/CoERMPublicCommonSearchServices /Display DCTMContent?documentId=0900001680465f73#search =electronic evidence guide

McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.

Mustafa, Z.S. (2017). *Assessing the evidential value of artefacts recovered from the cloud.*

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age. Polity.*

# Unit 2: Investigative Methods and Processes

## Contents



## 1.0 Introduction

Digital forensics employs the use of validated methods and techniques to acquire and analyse evidence that can be to show that a crime has been committed. This unit focuses on the processes involved in digital forensic investigations.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain investigative methods and processes in forensics
- discuss various digital investigative methods for live and dead systems
- describe evidence acquisition.

## 3.0 Main Content

### 3.1 Investigative Methods and Processes

Digital Forensic Investigation Processes (DFIP) are methods and procedures used during a digital forensics investigation. (Ruan, 2013) defines it as a set of procedures and techniques to ensure that any evidence obtained is sufficiently rigorous so that it may be admissible in a court of law. Several models have been proposed over the years. Some of which will be described to give an insight into their significance.

McKemmish (1999) model has four processes, and these are:

- Identification: This involves knowing the type of evidence, its location, how it is stored to determine the best way to extract it.
- Preservation: This is the processes where evidence is acquired in the least intrusive manner to ensure that its integrity is not compromised.
- Analysis: This consists of extracting, processing and interpreting the data identified as evidence.
- Presentation: This is where the evidence is presented in court.

Digital Forensic Research Workshop (DFRWS, 2001) model consists of the following:

- Identification: It involves detecting anomaly on systems, which can lead to detecting crime, systems monitoring and audit analysis.
- Preservation: Focuses on methods of preserving the integrity of evidence, ensuring that the evidence is not compromised.
- Collection: It is the acquisition of evidence, using techniques and tools that protect the evidence.
- Examination: This involves checking acquired evidence to identify and extract hidden data and to conduct pattern matching on the evidence.
- Analysis: The use of techniques to verify the results of the examination process.
- Presentation: Presenting the evidence, including all the steps taken to conclude the evidence. Experts may be called to give input on the process and the conclusion.
- Decision: This is the last processes where a decision is taken based on the findings from the whole process.

Integrated Digital Investigation Process (Carrier and Spafford, 2003)

- Readiness Phase: This phase focuses on ensuring that the investigative team have the necessary infrastructure for the operation. This is broken down into two phases.
    - Operation Readiness Phase – comprises of training and equipment for investigation personnel.
    - Infrastructure Readiness – ensures that there is data for investigation.
- Deployment Phase: This provides the mechanism for an incidence to be detected and confirmed. This is also broken down into two phases:
    - Detection and Notification Phase – this is where an incident is discovered and reported.
    - Confirmation and Authorisation Phase – here, the investigation team receive authorisation to proceed with the investigation.
- Physical crime scene investigation: This is where physical evidence is collected and analysed to reconstruct the events that took place.
    - Preservation Phase: this involves securing the physical crime scene to protect evidence from being tampered.
    - Survey Phase: once the scene is secure, potential physical evidence is identified.

    - Documentation Phase: all evidence identified are documented in this phase.
    - Search and Collection Phase: a thorough search is conducted to gather more evidence. It is in this phase that digital crime scene investigation commences.
    - Reconstruction Phase: all evidence collected are used to reconstruct the events that led to the crime.
    - Presentation Phase: both physical and digital evidence are presented here.
- Digital crime scene investigation: In this phase, digital evidence is collected and analysed. It is further divided into six phases, like the physical crime scene investigation.
    - Preservation Phase: this involves securing the digital crime scene to protect evidence from being tampered.
    - Survey Phase: once the scene is secure, digital evidence is acquired, that is, a replica of the evidence is created, this is called an image.
    - Documentation Phase: all identified evidence are documented in this phase.
    - Search and Collection Phase: this is where the image is analysed for evidence.
    - Reconstruction Phase: all evidence collected are used to reconstruct the events that led to the crime.
    - Presentation Phase: both physical and digital evidence are presented here.
- Review: This involves the review of the whole process to identify areas that need to be improved.

National Institute of Standards and Technology (Kent *et al.*, 2006)

- Data collection: This involves identifying potential sources of data which may be used as evidence and extracting them.
- Examination: After collection, the data is assessed to obtain relevant information.
- Analysis: The information is processed and analysed to draw conclusions.
- Report: The results of the analysis prepared and presented in this phase.

Generic Computer Forensic Investigation Model (GCFIM) (Yusoff *et al.*, 2011)

- Pre-process: These are activities carried out before collecting evidence.
- Acquisition and preservation: This involves the identification, acquisition, storage and preservation of evidence.
- Analysis: This is the phase where evidence is examined to determine if a crime has been committed.
- Presentation: Here, the results of the analysis are presented

- Post-process: This is like the review phase of the Integrated Digital Investigation Process; the whole process is reviewed to identify lapses and finally close the case.

Association of Chief of Police Officers (ACPO) Digital Investigation Strategy (ACPO, 2012)

- Data capture: This consists of steps to be taken to identify and secure relevant evidence.
- Data examination: This step is where the data collected is analysed.
- Data interpretation: After the analysis, the results need to be interpreted in a manner where a non-technical person can understand.
- Data reporting: This is a comprehensive technical report of all the processes undertaken and the results of the examination.
- Interview of witness and suspects: This employs a strategy of extracting information relevant to the investigation.

As can be seen from the above DFIP, the underlying principles of these models are similar. All focus on ensuring that evidence is preserved to ensure that it is admissible in the court of law. Just as with the guidelines, there is no de facto model, investigators can choose the model that suits their investigations as long as it would produce the desired results.

With the dynamic nature of technology, more models would be proposed to accommodate new technologies.

## 3.2 Evidence Acquisition

Evidence acquisition is one of the processes of DFIP, as discussed in Unit 1. It involves collecting data which can be used to show that a crime has been committed, link a crime and its victim or a crime and its perpetrator. This evidence needs to be acquired in a manner that is legally acceptable as it may be used in the court of law. Evidence can be found in various devices and can come in various formats. During an investigation, devices such as desktop computers, laptops, mobile phones may be seized, and these would need to be examined to determine if they contain data that can be used as evidence. This examination cannot be conducted directly on seized devices but on a copy, that is an exact bit-by-bit copy of the device called an image, this is to comply with principles of digital evidence (ACPO, 2012). To create an image of a device, the state of the devices must be considered, that is if powered off or powered on as this will determine how evidence will be acquired.

### 3.2.1 Evidence Acquisition from a Dead System (Data Duplication)

Making a forensic image of a device is an essential aspect of digital forensics as it creates an exact duplicate of the original. There are three types of images; complete disk, partition, and logical images (Luttengs *et al.*, 2014).

**Complete disk image:** This makes a copy of every addressable allocation unit of a storage media. This includes all allocated and unallocated spaces. If the hard disk of a seized computer is 320GB, a complete disk image of the hard disk will be 320GB.
**Partition Image**: This is where an image of a partition or a volume is created. Unlike the complete disk image, this will not have all the data of the source, only the data in the partition or the volume.
**Logical image**: This contains a copy of files and directories that are referenced in the filesystem.

Regardless of the type of imaging method selected, care should be taken to ensure that the original is not changed. Therefore, the write function of the imaging system needs to be disabled. This can be done with hardware or software write blockers. The image can then be created with imaging tools (open source or proprietary).

Still on the evidence preservation, for both original and the image, cryptographic checksums are used as shown in the video. This can be used to verify that the original has not changed and that the image is the exact copy of the original (ACPO, 2012; Luttengs et al., 2014).

Watch the video CST902_Mod1Unit2 for a demo on the dead acquisition.

### 3.2.2 Evidence Acquisition from a Live System

Live evidence refers to evidence acquired from a system that is powered on, for example, a laptop that is running. This enables investigators to access data which would be unavailable if the system is powered off (ACPO, 2012). When acquiring such data, the likelihood of changing the original is high. This is where the application of the guidelines for digital forensics investigations come into play. For example, Rule 2 of McKemmish Rules of Forensic Computing, Principle 2 of the ACPO Guidelines and Principle 3 of IOCE Guidelines take care of this issue.

In acquiring live data, care needs to be taken because such evidence is volatile and can easily be changed. Therefore, there are factors to consider to ensure that it is preserved, these factors include (Luttengs et al. 2014)

- Experience in acquiring data from a similar system
- Can data be acquired with minimal change
- The probability of successful acquisition

- Legal implications of the process
- Tool(s) best suited for the acquisition

During live acquisition, one of the essential sources of evidence is the memory; a memory dump should be taken which may provide the following information (ACPO, 2012)

- listings of running processes
- logged on and registered users
- network information including listening, open and closing network ports
- ARP (address resolution protocol) cache
- registry information

Other information that can be acquired are:
- The system time and date, including the time zone
- Operating system version information
- General system information, such as memory capacity, hard drives, and mounted file systems
- List of services and programs configured to automatically start on boot-up, such as web servers, databases, multimedia applications, and e-mail programs
- List of tasks scheduled to run at given times or intervals automatically
- List of local user accounts and group membership
- Network interface details, including IP and MAC addresses
- The routing table, ARP table, and DNS cache
- Network connections, including associated processes
- Currently loaded drivers or modules
- Files and other open handles
- Running processes, including details such as parent process ID (PID) and runtime
- System configuration data
- User login history, including user name, source, and duration
- Standard system log data
- List of installed software
- Appropriate application log data—web browser history, antivirus logs, and so on
- Full file system listing, including the appropriate timestamps for the file system

Watch video CST902_Mod1Unit2 to learn how to acquire memory.

Assignment: Identify other sources of digital evidence which we encounter in our everyday lives (excluding those listed above).

 Discussion

With reference to Digital Forensic Framework for Cloud Computing, Data Reduction and Data Mining Framework by Quick & Choo 2014, Internet of Things (IoT) Based Digital Forensic Model by Perumal et at 2015 and A Generic Digital Forensic Investigation Framework of Internet of Things (IoT) by Kebande & Ray 2016; interview five practitioners in digital forensic and present your findings on the discussion forum with the inclusion of the sample of your interview questions, and discuss your findings.

## 4.0 Self-Assessment Exercise(s)

**1.** How can investigators determine which DFIP to use?
The types of investigation, the expertise of the investigator and the scene can determine the DFIP to be used. However, the decision lies with the investigator.

2. When you acquire system memory with FTK Imager, what is the
   a. Default file name? *memdump*
   b. File extension? *.mem*

## 5.0 Conclusion

There are several models of DFIP proposed over the years, none of which is adopted as the standard model for digital forensics investigations. The main purpose of using these processes is to ensure that any evidence acquired can stand legal scrutiny. These models give investigators options to choose from, and the nature of the investigation may determine the model to use. In terms of examination/ analysis, this can only be conducted on copies and not original in compliance with principles of electronic evidence. The type of image to be created will depend on the investigator and the circumstances of the investigation.

## 6.0 Summary

Digital forensics investigation processes (DFIP) provide techniques and processes for investigating digital crimes. These processes and techniques are required to protect the integrity of evidence such that the evidence may be admissible in the court of law. There are several models proposed which gives investigators the flexibility to choose the model that best suits their

needs. One of the common processes evidence acquisition, this process is critical to digital forensics as when analysed, can be used to show that a crime was committed. In digital forensics investigation, the state of the device matters as it will determine how the evidence will be acquired and the acquisition type.

The next module will focus on the filesystem. It will examine some of the most common OSes and the corresponding OSes to provide students with requite information on analysing these systems either in an investigation or for research.

# 7.0 References/Further Reading


ACPO (2012). *ACPO Good Practice Guide for Digital Evidence*. Retrieved on19 January 2016 from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Carrier, B. & Spafford, E. H. E. (2003). 'Getting physical with the digital investigation process', *International Journal of Digital Evidence*, 2(2), pp. 1–20.

DFRWS (2001). 'A Road Map for Digital Forensic Research', Proceedings of the 2001 Digital Forensics Research Workshop (, pp. 1–42. doi: 10.1111/j.1365-2656.2005.01025.x.

Kent, K. et al. (2006). *Guide to Integrating Forensic Techniques to Incident Response*, NIST Special Publication.

Luttengs, J. T., Pepe, M. & Mandia, K. (2014). *Incident Response and Computer Forensics.* (3rd ed.). McGraw-Hill Education.

McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.

Mustafa, Z.S. (2017). *Assessing the Evidential Value of Artefacts Recovered from the Cloud.*

*Ruan, K. (ed.) (2013). Cybercrime and Cloud Forensics: Applications for Investigation Processes.* IGI Global.

Yusoff, Y., Ismail, R. & Hassan, Z. (2011). 'Common Phases of Computer Forensics Investigation Models', *International Journal of Computer Science and Information Technology,* 3(3), pp. 17–31. doi: 10.5121/ijcsit.2011.3302.

# Module 2: Operating Systems

## Module Introduction

Windows is the most popular OS for computers which makes it inevitable to be encountered in an investigation. Linux, on the other hand, is not as popular, but it can be used as a forensic workstation. This makes it crucial for investigators to have the knowledge and skills to investigate these OSes. This module will focus on analysing Windows and Linux OS and how to use Linux as a forensic workstation.

Unit 1: Windows OS
Unit 2: Linux OS
Unit 3: Mac OS

## Unit 1: File System Forensics

### Contents



### 1.0 Introduction

In a digital forensic investigation, it is expected that the investigator may come across a computer which runs on a Windows operating system or use a Linux-based forensic station for acquisition and examination. Windows and Linux use different filesystems, the way OS organises files on a disk; therefore, knowledge of the filesystems associated with Windows and Linux is important to digital forensics investigators. For a meaningful analysis of a filesystem, it is important to understand the concepts. Therefore, a

reference model will be used to aid in comparing the various filesystems. This model consists of the following categories; file system, content, metadata, file name, and application. The *file system* consists of general file information; the *content* is the actual data, the *metadata* describes a file, the *filename* is data that assigns names to files and *application* consists of that with special feature (Carrier, 2005). The interaction between these categories is shown in Figure 1.1.

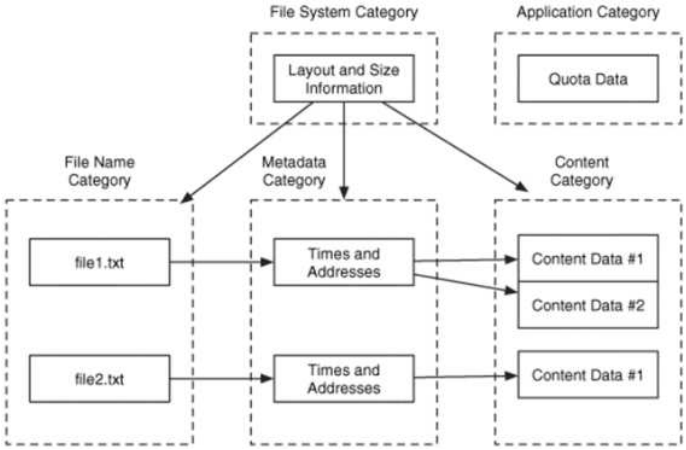


**Fig. 1.1: Interaction between filesystem categories (Carrier, 2005)**

# 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- identify common filesystems used by Windows, Linux and Mac using file signatures
- describe the structures of the common filesystems.

# 3.0 Main Content

## 3.1 Windows Filesystem

Windows remains the most common OS for both laptop and desktop computers. It supports two primary filesystems, file allocation table (FAT) and New Technology File System (NTFS). FAT was the first filesystem developed by Microsoft for PCs, but NTFS has replaced it for PCs while it is still being used for flash drives and memory cards. Therefore, digital forensics investigators/ researchers need to have a thorough understanding of the structure of these file systems to be able to analyse them.

### 3.1.1 FAT

File Allocation Table (FAT) was the default filesystem for Microsoft DOS and Windows 3.x, 95 and 98 before it was replaced by Microsoft New Technology File System (NTFS) for subsequent versions of Windows. It is also used in removable storage media such as compact flash drives used in digital cameras and flash drives (Carrier, 2005; Altheide and Carvey, 2011). While investigators may not come across Microsoft DOS and Windows, it is useful to understand the structure of FAT and how to analyse it as it is still used by flash drives and compact flash drives used in digital cameras which are quite common.

**FAT Structure**

FAT is a basic filesystem with few data structures, in FAT, disks and volumes are broken down into clusters of specific sizes which are determined by the version (Altheide and Carvey, 2011). This means that identifying the FAT version in an investigation is vital to ensure that the proper analysis techniques are used.

FAT has two basic structure, the File Allocation Table which is the primary and backup structures of FAT and directory entries which are data structures for every file and directory stored in the system (Carrier, 2005). In terms of layout, FAT is divided into three sections, the reserved area, this contains the boot sector, the FAT area which contains the primary and backup structures and Data area which contain the directory entries (Carrier, 2005). The differences in layout between FAT12/16 and FAT32 are as follows:

- The reserved area for FAT12/16 is only one sector while that of FAT32 is more than one.
- The data area for FAT12/16 starts with the root directory while for FAT32, the root directory can be anywhere.

**FAT Analysis**

File System Category – as mentioned earlier, contains data that describes the filesystem. For FAT analysis, the physical layout needs to be known and the information contained in the layout. This includes the boot sector data, which provides data on the size of the reserved area, the number of FAT structures and the size of each FAT structure for the FAT area and the number of clusters per sector for the data area. This information can be used to calculate sizes of the reserved area, FAT area and data area.

Content Category: In FAT, data is stored in clusters and the maximum cluster size 32KB, each cluster is allocated an address which starts from cluster 2, which is the first cluster of the data area (Carrier, 2005). For FAT12/16, the first sector is reserved for the root directory. Therefore cluster 2 starts at the sector after the root directory while for FAT32, cluster

2 starts at the first sector of the data area (Carrier, 2005). This information is vital in finding data that can be used as evidence in an investigation.

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT
OEM Name: MSDOS5.0
Volume ID: 0x4c194603
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FAT DISK
File System Type Label: FAT32
Backup Boot Sector Location: 6
FS Info Sector Location: 1

Next Free Sector (FS Info): 1778
Free Sector Count (FS Info): 203836
Sectors before file system: 100800

File System Layout (in sectors)
Total Range: 0 - 205631
* Reserved: 0 - 37
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 38 - 834
* FAT 1: 835 - 1631
* Data Area: 1632 - 205631
** Cluster Area: 1632 - 205631
*** Root Directory: 1632 - 1635
CONTENT-DATA INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 1024
Total Cluster Range: 2 - 102001
```

**Fig. 1. 2: Example of FAT32 File System Category Data**

Metadata Category: Contains a description of files and directories, and this includes their locations, permissions, dates and times. In FAT, directory entry handles this function; it is 32 bytes in size and stores file information, including the attributes and starting cluster for the file (Carrier, 2005). The file attributes are divided into seven; three essential and four non-essential attributes. The essential attributes are directory, long filename, volume label and the non-essential are read-only, hidden, system and archive. Each directory entry has three-time stamps, date created, last accessed and date modified (Carrier, 2005). When using these dates in an investigation, it is important to note that the created and last accessed are optional and accurate to a certain degree while the modified is accurate to two seconds.

File Name Category: This is where files and directories are assigned names. It enables investigators to map names with their corresponding metadata. If the file name exceeds eight characters or it has special characters, a long file name (LFN) type is added to the directory entry. This means the file will have both LFN and short file name (SFN) in the directory entry (Carrier,

2005). This is because the LFN does not contain time, size and starting cluster of the file (Carrier, 2005). During analysis, once a file is found, then its metadata will also be found as it is stored in the directory entry, and when a file is deleted, its file name is deleted, but metadata remains in the directory entry until it is overwritten. This means that it can be recovered which may provide useful information in an investigation.

### 3.1.2 NTFS

NTFS is a filesystem designed by Microsoft, and it is the most widely used on Windows systems from Windows 2000. It has several advantages over FAT such as reliability, security, networking and storage efficiency.

**NTFS Structure**
It consists of system files which manage the volume, these are summarised below.

**Table 1: Summary of NTFS System Files**

**(Carrier, 2005; Altheide and Carvey, 2011)**

| Entry | Name | Description |
|---|---|---|
| 0 | $MFT | Master File Table contains one record for each folder and file on the system |
| 1 | $MFTMirr | Stores the first four records of the $MFT, which are the $MFT, $MFTMirr, $LogFile and $Volume |
| 2 | $LogFile | A relational database of transactional logs for the volume that can be used for system recovery |
| 3 | $Volume | Contains information on the volume like the volume label and version information |
| 4 | $AttrDef | A table that stores attribute name, descriptors and numbers |
| 5 | $. | Root of the volume |
| 6 | $Bitmap | Contains a record of clusters in use and those that are not in use in a volume |
| 7 | $Boot | contains the boot record for the volume |
| 8 | $BadClus | Keeps track of bad clusters in a volume |
| 9 | $Secure | Stores unique security descriptors for all the files in a volume |
| 10 | $UpCase | Converts Unicode lowercase to Unicode uppercase characters |
| 11 | $Extend | A directory where extended system files are located |

The structure is shown in Video CST902_Mod3Unit1_3.1.

**NTFS Analysis**
File System Category: The MFT is an important system file as it stores the records of every file and directory on the system; its location is stored in

the boot sector. Once this is identified, the first entry $MFT can then be used to locate the rest of the MFT, and if any data is corrupt, the $MFTMirr can be used to access the backup of $MFT (Carrier, 2005). Once this is done, the $Volume and $AttrDef can be used to determine the volume label, filesystem version, and information for each attribute of the system.

Content Category: Files in NTFS consists of attributes some of which are resident, these store content in the MFT and others which are non-resident, these store content in clusters (Carrier, 2005). Regarding analysis, once a cluster is located, its allocation status can be determined by $Bitmap, and the content examined. This may yield data that can be used as evidence in an investigation.

Metadata Category: The metadata of a file in NTFS are stored in $STANDARD_INFORMATION attribute. This stores date and time (creation, modified, MFT modified and accessed time), ownership, security and quota information; $FILE_NAME attribute, which stores name for each file encoded in UTF-16 Unicode; and $DATA attribute, which stores data (Carrier, 2005). This information, when analysed, can provide more information on a specific file or directory.

File Name Category: NTFS uses indexes to organise contents of a directory; an index is a collection of data structures sorted by some key (Carrier, 2005). The $INDEX_ROOT which is the root of the index and $INDEX_ALLOCATION which contains index records of other nodes. The allocation of these attributes is managed by $Bitmap (Carrier, 2005). For the analysis of a file name, the contents of $INDEX_ROOT and $INDEX_ALLOCATION need to be examined as allocated files may have unallocated entries as well as allocated entries due to file addition and deletion. Also, when files are deleted, the index tree is sorted, and entries are moved to other nodes or other locations within a node, but that file will continue to remain in an unallocated space of a node until it is overwritten. This means using a file name, and it may be possible to recover a deleted file in an unallocated space before it is overwritten.
How does FAT differ from NTFS in terms of deleted file recovery?

Both can be recovered before they are overwritten as the file remains on disk after deletion. But as more data is written to the disk, deleted files at some point may be overwritten making their recovery difficult.

## 3.2 Linux File System

Ext3 is the default filesystem for many Linux distributions. It is a newer version of ext2 but with journaling support. Ext4 is gradually replacing ext3. There are other filesystems used by Linux such as ReiserFS, XFS and Journaled File System (JFS). This section will only focus on ext3.

### 3.2.1 Ext3 Structure

Ext3 filesystem is divided into block groups; it has an optional reserved area for administrative purposes. Each block group contains the same number of blocks, and these are used to store file names, content and metadata. This ext3 filesystem structure is summarised in Table 2.

**Table 2: Ext3 Block Group Summary**

**(Carrier, 2005; Altheide and Carvey, 2011)**

| Field | Description |
|---|---|
| Superblock | Stores information about the layout of the file system, block and inode information, volume name, last write time, last mount time |
| Group Descriptor Table | Contains information on every block group in the filesystem |
| Block Bitmap | Manages allocation information of the blocks in the block group |
| Inode Bitmap | Manages allocation information of inodes in the block group |
| Inode Table | Stores inodes, inodes store metadata information for files and directories |
| Data Blocks | Store contents of a file |

The structure is shown in Video CST902_Mod3Unit1_3.2

**Ext3 Analysis**
File System Category: In ext3, the superblock contains information related to the filesystem. It is located at 1,024 bytes from the start of the filesystem, and it is 1,024 bytes in size (Carrier, 2005). For the analysis of an ext3 system, it is important to locate the superblock, and as its location is fixed, this is straightforward. Once it is located, it can then be used to locate the group descriptor table, and these two combined will provide information on the data structure of the files and directories stored on the system.

Content Category: Ext3 uses blocks as its data unit, and each block is a group of consecutive sectors. A can be 1,024, 2,048 or 4,096 bytes in size

and the size is specified in the superblock(Carrier, 2005). In terms of analysis, the location of a block, it's content and allocation status can easily be determined by using the information in the superblock, group descriptor table and block bitmap.
Metadata Category: The metadata for a file in ext3 is stored in the inode table. To locate the inode of a specific file, firstly, the block group of the inode needs to be determined. The group descriptor table for that group can be examined to identify its inode table, then locate the entry for that inode. Once this is done, the information can then be used for investigation.

File Name Category: Ext3 uses various methods to assign names to files and directories such as directory entries, links and mount points, and hash trees (Carrier, 2005). In finding a file name, the root directory needs to be located, and this is always in inode 2, then the directory content can then be examined to get the file name.

Application Category: Filesystem journaling which is a feature of ext3 records updates to the filesystem for faster recovery after a crash (Carrier, 2005). During an investigation, information relating to updates can be found using the journal superblock and its associated descriptor block.

## 3.3 HFS+ Filesystem

HFS+ is the filesystem used by Apple devices. This is a replacement for HFS. The key features of HFS Plus include efficient use of disk space, internationally friendly file names, future support for named forks and ease of booting on other operating systems (Hoog and Strzempka, 2011). HFS Plus consists of volumes; each of these is divided into equal-sized allocation blocks. The structure of the HFS Plus volume consists of volume header or alternate volume header and five special files. The HFS Plus filesystem is summarised in Table 3.

**Table 3: Summary of HFS+ Structure**

**(Burghardt and Feldman, 2008; Hoog and Strzempka, 2011)**

| Filename | Description |
|---|---|
| Volume Header | Stores information about the volume such as creation date and time, number of files on the volume and location of five special files of the volume. |
| Alternate Volume Header | This is a copy of the volume header stored at the end of the volume, and it is intended to be used by disk repair utilities |
| Startup File | This keeps a record on information on booting non-Mac computers from the HFS volume |
| Allocation File | This file keeps track of which allocation blocks are free and which are in use |
| Catalog File | This stores information on all the folders and files in a volume |
| Extents Overflow File | This stores additional extents for fragmented files that is, file with more than eight extents |
| Attributes File | This stores additional data for a folder or file |

HFS+ uses B-trees for catalog, extents overflow and attributes files. B-tree is a data structure that stores data in a manner that allows efficient searches, modifications and deletion. HFS+ uses journaling to keep a log of related changes before their implementation on the filesystem. New logs are added to the journal file until the end is reached, then it starts at the beginning of the file, thereby overwriting old data. When data is deleted in HFS+, the catalog and allocation files are updated, but the deleted data remains on the disk until it is overwritten. This means like in filesystems discussed in earlier sections; it can be recovered and used in an investigation.

Discussion
Discuss the importance of deleted files in a digital forensics investigation.

# 4.0 Self-Assessment Exercise(s)

1. Create a Windows 7 Virtual Machine and view the system files in FTK Imager. Identify the location of $. List the directories in the root.

   $. is the root and is located in the NTFS partition. The directories are $Extend, $Recycle.Bin, Boot, Documents and Settings, Perflogs, Program Files, Program Files (x86), Program Data, Recovery, System Volume Information, Users and Windows.

2. Create a Linux VM and
   a. Identify the filesystem and version (ext version 4 but it could be 3 depending on the Linux distro).
   b. List the files and directories in the partition.

   Files - Superblock, group descriptor table, block bitmap, inode bitmap, inode table, boot record, bad blocks and journal
   Directory – root and unallocated space
3. Which of the files in (b) is responsible for keeping track of changes not yet made to the filesystem?

   Journaling simply means keeping a record of all changes being made to a disk for ease of recovery in the case of an outage or system crash.

# 5.0 Conclusion

FAT and NTFS are Windows filesystems. Nowadays, FAT is mostly found on a flash drive and compact flash drive used in digital cameras, therefore, it is vital for investigations to have the skills of analysing this filesystem. NTFS has replaced FAT as the primary filesystem for Microsoft Windows, and Windows is the most popular OS, which makes it inevitable to be encountered in a digital forensics investigation. In both filesystems, deleted files remain on disk until they are overwritten which make recovery possible.

ExtX is the most common filesystem used by Linux distributions. This means that a digital forensics investigator may be required to analyse extX

filesystem at a point in his or her career. Even though this unit focused on ext3, the structure has remained more or less the same in the versions; therefore, it is expected that the analysis techniques and methods will be similar.

HFS Plus, a replacement of HFS is a filesystem used by Apple devices. Like FAT, NTFS and extX, when data is deleted, all pointers to the data are deleted, but the data itself remains on the disk until it is overwritten, this makes it recoverable and useful in an investigation.

# 6.0 Summary

FAT is a filesystem with a simple structure. It comes in various versions, FAT12, 16, 32 and exFAT. In this unit, the focus was on FAT12/16 and FAT32 because of the differences in their structures. The analysis of FAT was discussed in terms of the filesystem categories by Carrier (2005). NTFS, unlike FAT, is a more complex filesystem, it consists of crucial 12 system files which were summarised in Table 1. As with FAT, the analysis of NTFS was also discussed based on the filesystem categories. The two filesystems are similar for recovery of deleted files, as deleted files remain on disk until they are overwritten.

Various filesystems can be used with a Linux system, but the most common is extX.

ExtX has different versions, each an upgrade of the preceding one, they are ext2, ext3 and ext4, but the structure remains the same. Like Fat and NTFS, deleted files can be recovered because they remain in a disk until overwritten.

HFS Plus is a filesystem used by Apple devices, while the structure differs from those of FAT, NTFS and ExtX, it is similar in terms of data deletion.

# 7.0 References/Further Reading


Altheide, C. & Carvey, H. A. (2011). *Digital Forensics with Open Source Tools*. Syngress Media Incorporated.

Burghardt, A., & Feldman, A. J. (2008). "Using the HFS+ Journal for Deleted File Recovery." *Digital Investigation* 5, S76–S82. doi:10.1016/j.diin.2008.05.013

Carrier, B. (2005). *File system forensic analysis*, *Computer*. Addison-Wesley. doi: 10.1016/B978-1-59749-472-4.00002-0.

Charles, B., Rowe, N.C. & McCarrin, M.R. (2018). "Memory Forensics and the Macintosh OS X Operating System. In Digital Forensics and Cyber Crime." 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings (Vol. 216, p. 175). Springer.

Fairbanks, K. D. (2012) 'An analysis of Ext4 for digital forensics', *Digital Investigation*. (The Proceedings of the Twelfth Annual DFRWS Conference12th Annual Digital Forensics Research Conference), 9(.), pp. S118–S130. doi: 10.1016/j.diin.2012.05.010.

Hoog, A., & Strzempka, K. (2011). *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*. Syngress.

Luttengs, J. T., Pepe, M. & Mandia, K. (2014). *Incident Response and Computer Forensics*. (3rd ed.). McGraw-Hill Education.

Maddu, B. & Roa, P. (2019). "OS X Artifact Analysis." *International Journal of Recent Technology and Engineering* (IJRTE)(pp. 26-32).

Matoušek, P. & Schmiedecker, M. (Eds). (2018). "Digital Forensics and Cyber Crime." 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings (Vol. 216). Springer.

Messier, R. (2015). *Operating system forensics.* Syngress.

Prasad, E., Dija, S. & Lakshmi, M.D. (2018). "Towards Live Forensic Acquisition and Analysis of Mac OS Systems." In 2018 International CET Conference on Control, Communication, and Computing (IC4) (pp. 415-418). IEEE.

Reddy, N. (2019). *Mac OS Forensics. In Practical Cyber Forensics* Berkeley, CA: Apress. (pp. 101-132).

Skulkin, O. & de Courcier, S. (2017). *Windows Forensics Cookbook*. Packt Publishing Ltd.

# Unit 2: Windows OS

## Contents



## 1.0 Introduction

Windows is an operating system developed by Microsoft. It has evolved over the years from Windows 1.0 released in 1985 to Windows 10, released in 2015 (Ward, 2019). As the most popular OS, investigators are bound to come across it during an investigation. This section discusses the types of evidence that can be found on a Windows system, with a focus on Windows 7.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- investigate Windows system to identify,
- acquire and analyse evidence that can be used in the court of law.

## 3.0 Main Content

### 3.1 Sources of Evidence on a Windows OS

Windows, as discussed in Module 2, Unit 1 supports two primary filesystems, FAT and NTFS, whose structure and analysis was covered in the unit. Other sources of evidence are as follows:

**Registry:** This contains OS and application configuration settings of a system. It is located at *C:\Windows\System32\config*, the files of interest are Software, Security and System hives; these require a registry viewer to access the information stored in

them. For specific user information, the USRCLASS.DAT located at *C:\Users\User_Name\AppData\Local\Microsoft\Windows*. Some of the information that can be retrieved the registry hives using a registry editor such as regedit shown at Figure 1.3 (this is available on Windows, to access it, search regedit) are summarised at Table 3.

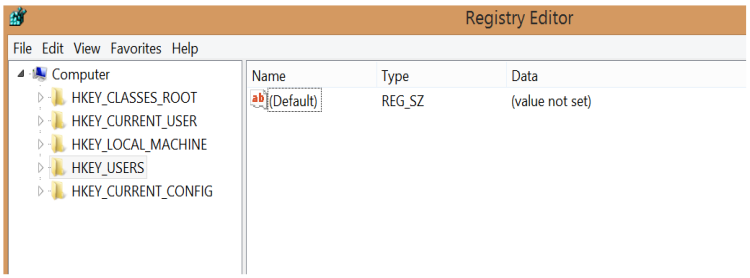


**Fig. 1 3: Regedit View**

See Video CST902_Mod2_Unit2

**Table 4: Information from Registry Hive**

| Registry Key | Description |
|---|---|
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName | Computer name |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion | OS version |
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation | Time Zone |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\ | Networks connected, including dates and times |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | Programs that load at boot |
| HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs | Shows a list of recently opened files |
| HKEY_USERS\{SID}\Software \Microsoft\Windows\CurrentVersion \Explorer\RunMRU | Lists applications executed with Run |
| HKEY_USERS\{SID}\Software\Microsoft\Terminal Server Client | Shows remote connection and configuration |
| HKEY_USERS\{SID}\Software\Microsoft\Internet Explorer\TypedURLs | Lists the URLs typed in Internet Explorer |

**Event Log**: Event logs keep a record of user and system activities. Windows has three event logs; System, Application and Security, these are located at *C:\Windows\System32\winevt\Logs* and have a .evt extension. System.evt records system related activities such as Windows service events, changes to the system time, driver loads and unloads, and network configuration issues; Application.evt keeps a record of user's applications and programs; and Security.evt record Windows authentication and security processes (Luttengs et al. 2014). Event logs require tools to be analysed and can be used to do the following (Luttengs et al. 2014):

- Identify a successful and failed login attempts and determine their origin
- Track the creation, start, and stop of system services
- Track usage of specific applications
- Track alterations to the audit policy
- Track changes to user permissions
- Monitor events generated by installed applications

**Prefetch**: This was introduced in Windows XP to reduce boot and application load times. It enables programs that are frequently used to be loaded faster by keeping part of the code in a specific location (Altheide and Carvey, 2011). Prefetch files are stored at *C:\Windows\Prefetch* directory and the files have a .pf extension. For example, if a user uses Google Chrome as a browser, its prefetch file will look like "CHROME.EXE-A64F19A4.pf".

Prefetch files can be used in an investigation to determine the programs frequently used by a suspect. The metadata of prefetch files can be used to determine when the program was last used.

How can information in prefetch files and event logs be used in an investigation?

Event logs keep a record of user activities, used with prefetch file. They can be used for event reconstruction and provide corroborative evidence.

**Shortcut Files**: In Windows, shortcut files are created during program installation, or when a user double clicks a file, they have the .lnk extension and are stored in *C:\Users\User_Name\Links* or *C:\Users\User_Name\Recent* (depending on Windows version) and C:*Users\User_Name\AppData\Roaming\Microsoft\Office\Recent.* These files once analysed paint a picture of user activities. They can also be used as corroborative evidence.

**Memory (RAM):** Information in RAM is volatile and can only be acquired while a system is powered on (discussed in Module 1, Unit 3). One of the most important sources of evidence are the processes running on the

system. Other information from a memory analysis includes network connections, both opened and recently closed, loaded drivers and the console command history (Luttengs et al. 2014). All these can be used to build up a case in an investigation.

Video CST902_Mod2_Unit2 shows how to access information on the Windows system, which can be used as evidence in an investigation.

Discussion

Discuss the impact of information stored in the registry in digital forensics investigation.

# 4.0 Self-Assessment Exercise(s)

1. Using the VM created in Module 2 Unit 1, use the registry to identify
   a. Typed URLs
   b. Computer Name
   c. OS version

   *This is user-dependent*
2. List the items in prefetch directory

   *This is also user-dependent*

# 5.0 Conclusion

There are various sources of evidence on a Windows system and the registry when analysed properly will provide useful information. The other sources of information may be used as corroborative evidence to information in the registry. In an investigation, all activities carried out need to be documented as a report would be required after the investigation.

# 6.0 Summary

Knowledge and skills for conducting digital forensics investigation on Windows systems are essential to investigators as it is the most common OS, and therefore likely to be encountered. This unit covered sources of evidence on a Windows system, this is by no means exhaustive, but they are quite crucial.

# 7.0 References/Further Reading


Altheide, C. & Carvey, H. A. (2011). *Digital Forensics with Open Source Tools*. Syngress Media Incorporated.

Carrier, B. (2005). *File system forensic analysis, Computer*. Addison-Wesley. doi: 10.1016/B978-1-59749-472-4.00002-0.

Luttengs, J. T., Pepe, M. & Mandia, K. (2014). *Incident Response and Computer Forensics*. (3rd ed.). McGraw-Hill Education.

Messier, R. (2015). *Operating system forensics*. Syngress.

Mustafa, Z.S. (2017). *Assessing the evidential value of artefacts recovered from the cloud.*

Skulkin, O. & de Courcier, S. (2017). *Windows Forensics Cookbook*. Packt Publishing Ltd.

Ward, K. (2019). *A Brief History of Microsoft Windows, Lifewire*. Retrieved on 26 August 2019 from https://www.lifewire.com/brief-history-of-microsoft-windows-3507078 (Accessed:).

# Unit 3: Linux OS

## Contents



## 1.0 Introduction

Linux is an open-source operating system with many distributions such as Ubuntu, Red Hat, Fedora, Debian etc. It is frequently used as a forensic workstation, but it can also be the focus of an investigation. This unit will explore the sources of evidence on a Linux OS and how it can be used as a forensic workstation to analyse evidence.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- investigate a Linux system to identify, acquire and analyse evidence that can be used in the court of law
- create a Linux forensic workstation for acquisition and analysis of evidence.

## 3.0 Main Content

### 3.1 Sources of Evidence on Linux

Linux has a standard directory structure based on Filesystem Hierarchy Standard (FHS). It is made up of the following directories shown in Table 4.

**Table 5: Linux Standard Directories**

**(Altheide and Carvey, 2011)**

| Directory | Description |
|---|---|
| /bin | Contains essential command binaries for users |
| /boot | Files for system startup |
| /dev | Device files |
| /etc | Configuration files for the system |
| /home | Home directories for users |
| /lib | Shared libraries files used by programs |
| /media | Mount point for removable devices |
| /mnt | Mount points for filesystem |
| /opt | Optional files and programs for third party applications |
| /root | Home directory for superuser |
| /sbin | System commands |
| /tmp | Hold temporary files |

This is shown in Video CST902_Mod2_Unit3

Sources of evidence include (Altheide and Carvey, 2011)

User Accounts: Information on users is stored in */etc/passwd* file. This records username, user ID, primary group ID, user's full name or name of the service account, the path of user's home directory and programs that run on login. Another file, */etc/shadow* stores password related details like username, encrypted password, number of days since the password was changed in Unix epoch and minimum days between password change, maximum validity for the password, number of days to password expiry and expiry date.

Home Directories: This contains sub-directories where users store data. They are Desktop, Documents, Downloads, Music, Pictures, Public, Templates and Videos.

Logs: Logs in Linux are usually in plaintext. This makes the analysis straight forward. The logs can either be generated by user activities or system activities. User activity logs are located in */var/run/utmp*, this stores active logons; */var/log/wtmp*, this stores longtime logon; and */var/log/lastlog* which stores last long time for each user. These files are in binary format and can be viewed in the command line. System activity logs, Syslog are stored in /var/log. They contain the date of message creation and deletion, the hostname of the system that created the log entry, a process that created the entry and text of the log entry.
All these need to be analysed to extract information that can be used as evidence.

## 3.2 Linux as a Forensic Workstations

Linux can be used as a forensics workstation to acquire and analyse evidence. In acquiring evidence, a Linux command-line tool dd may be used, other variants of the tool like dcfldd and dc3dd can also be used, though these need to be installed. The syntax for creating an image using dd is dd if=”source” of=”destination”

Example

dd if=/dev/sda of=/dev/sdb1/image.img

This means copy drive on sda and save it as image.img in partition 1 of drive sdb. Images created using dd and its variants can be analysed with other forensic tools. Another way around this is to use a Linux live CD and boot the system of interest directly to the CD; the dd can be used to create an image.

In analysing an image, open-source digital forensic tools can be installed on a Linux system. Man and info commands can be used to get information on how to use the tools. Image to be analysed needs to be mounted as *read-only* to prevent the system from making changes to the image file. Note that most of these tools are command-line tools, but GUI tools are also available.

See Video CST902_Mod2_Unit3.

Discussion

Discuss scenarios where a Linux Live CD is best suited for acquiring and analysing evidence.

## 4.0 Self-Assessment Exercise(s)

1. Create a Caine Live CD view system information on the Windows VM created in Module 2 Unit 1.
   *This is user-dependent*
2. Use the Linux VM to create an image of a 2GB flash drive and save it in the Documents directory of the VM. Attach a screenshot of the image.
   *This is also user-dependent*

# 5.0 Conclusion

Evidence in Linux can be extracted from various sources, and these provide information on system and users and their activities. Tools need to be installed to use Linux as a forensic workstation. However, a live CD comes with tools pre-installed. The investigator can choose the method that best suits the investigation.

# 6.0 Summary

Linux systems as a focus of the forensic investigation are not as complicated as the Windows system. Most evidence in Linux can be accessed straightforwardly. Linux can also be used for evidence acquisition and analysis.

# 7.0 References/Further Reading


Altheide, C. & Carvey, H. A. (2011). *Digital Forensics with Open Source Tools*. Syngress Media Incorporated.

Carrier, B. (2005). *File System Forensic Analysis, Computer*. Addison-Wesley. doi: 10.1016/B978-1-59749-472-4.00002-0.

Fairbanks, K. D. (2012). 'An analysis of Ext4 for digital forensics', Digital Investigation. (The Proceedings of the Twelfth Annual DFRWS Conference12th Annual Digital Forensics Research Conference), 9(.), pp. S118–S130. doi: 10.1016/j.diin.2012.05.010.

Messier, R. (2015). *Operating System Forensic*s. Syngress.

Mustafa, Z.S. (2017). *Assessing the Evidential Value of Artefacts Recovered from The Cloud.*

# Unit 4: Mac OS

## Contents



## 1.0 Introduction

Macintosh (Mac) OS is the operating system used by Apple systems. It was developed in 1984 as the first GUI based OS. This OS was redesigned, and Mac OS X was released in 2001. Over the years, Apple systems have become quite popular both for personal, and business use and incidences on these systems are rising. Therefore, the skills required to examine a Mac OS is critical for digital forensics investigators. The focus of this unit is sources and types of evidence that can be found on a device that uses Mac OS.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- investigate a Mac OS X
- identify, acquire and analyse evidence that can be used in the court of law.

## 3.0 Main Content

### 3.1 Mac OS X

Mac OS X uses HFS Plus filesystem; this was discussed in Unit 1 of this Module. There are four domains for data classification in Mac OS X; the local, system, network and user domains (Luttengs et al. 2014). The local

domain contains applications and configurations. These are available to all the users of the system; only users with administrative privileges can modify the data in this domain. The local domain has three directories. These are:

- Application directory: This contains all applications installed in the system
- Developer directory: It is the path used by Apple's development environment
- The Library directory: This stores application setting for three levels, the OS */System/Library*, shared by users */Library* and user-specific settings */Users/User_Name/Library*.

The system domain contains data installed by Apple and other specialised utilities. Data in this domain can only be modified by a user with administrative privileges—the network domain stores applications and data that will be shared amongst systems and users on a network. And finally, the user domain which contains user-specific content. The */User* directory of this domain contains individual directories for all the user accounts on the system. Each user directory has the following sub-directories

- Applications
- Desktop
- Document
- Library
- Music
- Movies
- Pictures
- Public
- Sites
- Trash

These domains contain data that may be used as evidence. There are other sources of evidence such as (Maddu, B and Rao, P 2019):

**System logs**: These contain logs related to user activities; the main log is located at */var/logs*. Other logs are audit log which stores security information and records of user log in and log off, and user creation and deletion. These logs are located in */var/audit*. Software Installation records are stored in */Library/receipts/installhistory.plist*. This file contains the history of software installation and update information.

**Preference files:** Contain preference settings for various levels of a system, and they have a .plist extension. The system preferences files store preference settings for all the uses on a system. They are stored in */library/preferences*. Global preferences store information such as time zones and location coordinates; these are located in */Library/preferences/.globalpreferences.plist*. Login window info records

user-related activities like user name and login information including dates and times the user logged in, this can be found in */Library/preferences/com.apple.loginwindow.plist*. Bluetooth preferences located in */Library/preferences/com.apple.bluetooth.plist* store information on devices connected to the system via Bluetooth, it keeps records of details such as device name and last updated time. These are shown in Video CST902_Mod2_Unit4

**Network Artefacts:** The network plist records information related to networks connected to the system. The information includes the last connection date, Wi-Fi ID, and security type. This file is located in */Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist*.

**User Artefacts:** This records information related to user activities such as login details, user directories and files, attached devices and the system time. All these are shown in Video CST902_Mod2_Unit4.

Other sources of evidence are summarised in Table 6.

**Table 6: Source of Evidence on Mac OS X (Luttengs et al. 2014)**

| Artefact | Location |
|---|---|
| System host name | /Library/Preferences/SystemConfiguration/preferences.plist. |
| OS version information | /System/Library/CoreService/SystemVersion.plist. |
| IP addresses | If defined in the Network Preferences, /Library/Preferences/ SystemConfiguration/preferences.plist. If configured for DHCP, /private/var/db/dhcpclient/leases/. |
| Date of OS install | File creation date of /private/var/db/.AppleSetupDone or the InstallDate value in /private/var/db/receipts/com.apple.pkg.InstallMacOSX.plist. |
| System time zone, connected printers (via colour profiles) | /Library/Preferences/.GlobalPreferences.plist. Note that if the user allows Location Services to set the time zone, this file contains the latitude and longitude of the recent locations. |
| The 10 most recently run applications, connected server | /Users/User_Name/Library/Preferences/com.apple.recentitems.plist |

| | |
|---|---|
| information, and documents recently accessed by the user | |
| Items moved to Trash | Items moved to Trash |
| Agents started by the system or per user | /Library/LaunchAgents /System/Library/LaunchAgents ~/Library/LaunchAgents |
| Daemons started by the system or per user | /Library/LaunchDaemons /System/Library/LaunchDaemons ~/Library/LaunchDaemons |
| Legacy system startup items | /Library/StartupItems /System/Library/StartupItems |

 Discussion

What is the importance of preference files in an investigation?

# 4.0 Self-Assessment Exercise(s)

Create a Mac VM and connect it to 2-3 Wi-Fi networks. Use the appropriate .plist file to identify the following */Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist*.

a. SSID of the network
   *User-specific*
b. Last connection date
*c. User-specific*
d. Wi-Fi ID
   *User-specific*

# 5.0 Conclusion

Mac OS X is the default OS for Apple systems from 2001, a redesigned version of Mac OS. It has four domains for data classification: the local, system, network and user domains. The system and the user domains are the major domains to be examined in an investigation. This is due to the information stored in them. There are several sources of evidence; all these were discussed, including their locations.

# 6.0 Summary

Mac is becoming more popular, while it is not as popular as Windows; digital forensics investigators need to acquire knowledge and skills to examine Mac systems. Evidence that relates to a system and network configurations and user activities can easily be identified and extracted for analysis, once analysed, such evidence may be used in the court of law.

This module has covered the three main OSes, each identifying where potential evidence may be found. The next module will focus on some of the sub-categories of digital forensics, the first being network forensics.

# 7.0 References/Further Reading


Burghardt, A., & Feldman, A.J. (2008). "Using the HFS+ journal for deleted file recovery." *Digital Investigation* 5, S76–S82. doi:10.1016 /j.diin. 2008.05.013

Charles, B., Rowe, N.C. & McCarrin, M.R. (2018). "Memory Forensics and the Macintosh OS X Operating System." In Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings (Vol. 216, p. 175). Springer.

Hoog, A., & Strzempka, K. (2011*). iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices.* Syngress.

Luttengs, J. T., Pepe, M. & Mandia, K. (2014). *Incident Response and Computer Forensics*. (3rd ed.). McGraw-Hill Education.

Maddu, B. & Roa, P. (2019). "OS X Artifact Analysis." *International Journal of Recent Technology and Engineering (IJRTE)(*pp. 26-32).

Matoušek, P. & Schmiedecker, M. (Eds.), (2018). "Digital Forensics and Cyber Crime." 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings (Vol. 216). Springer.

Messier, R. (2015). *Operating system forensics*. Syngress.

Prasad, E., Dija, S. & Lakshmi, M.D. (2018). "Towards Live Forensic Acquisition and Analysis of Mac OS Systems." In 2018 International CET Conference on Control, Communication, and Computing (IC4) (pp. 415-418). IEEE.

Reddy, N. (2019). *Mac OS Forensics. In Practical Cyber Forensics* Apress, Berkeley, CA. (pp. 101-132).

# Module 3: Advanced Forensics

## Module Introduction

The prevalence of online products and services used in homes and offices has made computer networks a source of digital forensics. Digital forensics investigators need to be equipped with knowledge and skill to conduct investigations in a network environment. This module covers sources of evidence on a network and how to analyse evidence acquired in a networked environment.

Unit 1: Filesystem Forensics
Unit 2: Network Forensics
Unit 3: Cloud Forensics
Unit 4: Web browser Forensics
Unit 5: Mobile Forensics
Unit 6: Social Media Forensics

## Unit 1: Network Forensics

### Contents



### 1.0 Introduction

Network forensics is a branch of digital forensics that analyses data from a network to determine if a crime has been committed. DFRWS (2001) defines network forensics as "*The use of scientifically proven techniques to*

*collect, fuse, identify, examine, correlate, analyse, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorised activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities*." In network forensics, all devices in a network need to be analysed as evidence may be distributed across any number of these devices.

# 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the sources of evidence in computer networks
- analyse data from network devices
- analyse data packets in an investigation.

# 3.0 Main Content

## 3.1 Sources of Evidence in Computer Networks

Computer networks have become common in homes and corporate environments, and these need to be examined to extract evidence in investigations. Source of evidence on a network include Dynamic Host Configuration Protocol (DHCP), logs, event logs, application logs, anti-virus logs, proxy and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) logs, Internet Service Provider (ISP) notices (network logs) and devices such as computers, routers, switches and servers (Lilliard *et al.*, 2010; Davidoff and Ham, 2012). Davidoff and Ham (2012) and ENISA (2019) identified four types of network-based evidence. These are:

- full-content data
- user data and metadata contained in a packet; session data, summaries of communication between a source and destination such as source and destination addresses, timestamp, port and protocol used;
- alert data, anomaly notifications based on defined rules and signatures;
- statistical data, analysis of network traffic detect certain patterns or behaviours that might be associated with illegal activities.

In terms of the investigation processes, those outlined in Module 1, Unit 2 can be applied. However, Davidoff and Ham (2012) proposed a methodology for network forensics which has five processes;

- Obtain information,
- Strategise,
- Collect evidence,
- Analyse, and
- Report.

This methodology is referred to as OSCAR. One fundamental difference between traditional digital forensics (computers) and network forensics is network traffic is by its nature highly dynamic, making it volatile and it can easily be changed, this makes it difficult to preserve. Therefore, investigators need to ensure that necessary measures are taken when acquiring such data. Davidoff and Ham (2012) suggested a strategy for collecting network evidence, these are

- Do not power down devices – any device that is powered on during an investigation should not be powered down as doing so will result in the loss of evidence in the memory of the device. Therefore, such evidence needs to be acquired before the device is switched off.
- Connect via a console – this option enables an investigator to preserve evidence unlike connecting via a network which will modify the network configuration.
- Keep a record of time – document both the device time and the actual time and note the difference; this plays a key role in correlating evidence.
- Collect evidence based on volatility level – volatile evidence can easily be modified or lost. Therefore, such evidence should be acquired first, from the most volatile to the least volatile to ensure completeness of evidence.
- Document the processes – all actions taken during evidence acquisition should be documented

Evidence from a network can be acquired in an active manner; this involves interacting with the system by sending requests, logging users out or accessing management console or in a passive manner, where the system is not interacted with (ENISA, 2019).

Video CST902_Mod3_Unit1 demonstrates passive acquisition.

Evidence in networks is classified into two, network-based and host-based. Network-based evidence can be found in the following (Davidoff and Ham, 2012; ENISA, 2019):

Cables: These enable point-to-point communication between devices. Traffic from cables is a good source of evidence as investigators can tap into the cabling to acquire network traffic while it is being transmitted.

In the air: Wireless access points broadcast signals and messages within a specific range and devices within that range can connect to the network. Investigators can capture traffic traversing across a wireless network.

Hubs: These connect systems physically on a local subnet. It does not have information on the ports each device is connected to; rather, it broadcasts any message to all the ports.

Switches: These are like hubs with additional capability. Unlike hubs, switches keep a record of devices and the ports they are connected to in a content addressable memory (CAM) table. A switch does not broadcast messages. Instead, it sends the message to the destination port. The information in the CAM is a good source of evidence.
Routers: Connect subnets or networks and transmit data between different network segments. Routers have a routing table where ports are mapped to the network they connect. The data in a routing table can be used as evidence.

DHCP servers: DHCP server logs keep records of IP address and hosts assigned to them, the MAC address of the host and connection time. All these can be used to build a case in an investigation.

Name Server: When DNS servers are configured to queries for IP address and hostname resolutions, the queries will provide information on connection attempts, websites, external mail server etc.

Authentication Servers: Organisation use authentication servers to manage user accounts in a centralised location. Such servers keep a log of successful and unsuccessful login attempts.

Host-based evidence was discussed in earlier modules.

## 3.2 Network Traffic Analysis

Network traffic is by its nature highly dynamic, making it volatile. Therefore it needs to be acquired early in an investigation as stated in the evidence collection strategy proposed by Davidoff and Ham (2012), which suggested that evidence should be collected based on the level of volatility. Once network traffic is captured, the next step is to analyse data that can be used as evidence. There are various analyses methods, such as:

### 3.2.1 Protocol Analysis

Protocol analysis enables investigators to examine the fields in the data structure of the protocol. Protocol analysis comprises of the following:

- Protocol identification: captured network traffic can be analysed to identify the protocol used. Watch Video CST902_Mod3_Unit1 to learn how to identify a protocol.
- Protocol decoding: this involves interpreting the data in a frame. This is shown in Video CST902_Mod3_Unit1
- Exporting fields – after identifying and decoding, the next action is to extract fields of interest and analyse it. This is also shown in the video.

### 3.2.2 Packet Analysis

Packet analysis is a process of examining contents of a data packet or the metadata of a packet to extract evidence. Packet analysis can be done in the following ways:

- Pattern matching: this is the process of identifying packets based on a specific value.
- Parsing protocol fields: this enables investigators to extract the contents of protocol fields for further analysis
- Packet filtering: here, packets are separated based on specific of a protocol.

### 3.2.3 Flow Analysis

Flow analysis examines the sequence of packets to identify patterns in network traffic, to isolate suspicious activity or extract data. This can be done in the following ways

- List conversations and flows: this lists all conversations and flows, and specific conversations or flows of interest are then further analysed.
- Export a flow: here, a single flow or multiple flows are isolated and extracted for further analysis.
- File and data carving: this involves extracting data from reassembled flows to use in event reconstruction in an investigation.

### 3.2.4 Wireless Traffic Analysis

Wireless network data can either be captured in monitor mode or promiscuous mode (ENISA, 2019). Traffic capture in monitor mode captures all traffic within a range, and it is not associated with a specific access point. In contrast, traffic capture in promiscuous mode captures all traffic associated with a particular access point. During analysis, traffic captured in monitor mode provides more information than that of promiscuous mode. Some of the information that can be used as evidence from wireless traffic includes the following (ENISA, 2019):

- Broadcast Service Set Identifier (SSID)
- Wireless Access Point (WAP) MAC address
- Supported encryption/authentication algorithms.
- Associated client MAC addresses

Also, other useful information from network traffic includes
- Time of capture: This can be used to correlate the activities of a suspect
- Name resolution: This enables IP addresses to be resolved to hostnames.
- Host identification: This allows information related to a localhost to be identified.

Video CST902_Mod3_Unit1 shows all these in more details.

Discussion

Discuss the differences between passive acquisition, active acquisition and live acquisition.

# 4.0 Self-Assessment Exercise(s)

1. How does the OSCAR methodology differ from the models in Module 2, Unit 2?
   There is no difference; the OSCAR methodology applies to traditional digital forensics.

2. Install Wireshark on the Windows VM and connect the VM to the internet. Start the capture and observe the process, identify the IP address assigned to the VM. Capture the traffic for 10 minutes and save the file.

   This is user-dependent

# 5.0 Conclusion

There are several sources of evidence in a networked environment, both home and corporate, some of which are highly volatile. Such evidence needs to be acquired in a manner that will preserve the integrity of the evidence. Evidence from a network may be used as standalone or corroborative, and it can aid in event reconstruction.

# 6.0 Summary

In today's world, people are connected to some sort of network; this, coupled with the rise of cybercrime, made it imperative that investigators are equipped with knowledge and skills to conduct network-related investigations. This unit discussed the sources of network-based evidence as host-based evidence was covered in Modules 2 and 3. One of the critical sources of evidence in network forensics is network traffic, once captured, it needs to be analysed; this is the focus of the next unit.

# 7.0 References/Further Reading


ACPO (2012). *ACPO Good Practice Guide for Digital Evidence*. Retrieved on 19 January 2016 from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed:).

Carrier, B. (2005). *File system forensic analysis, Computer*. Addison-Wesley. doi: 10.1016/B978-1-59749-472-4.00002-0.

Casey, E. (2004). *Digital Evidence And Computer Crime*. Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

Davidoff, S. & Ham, J. (2012). *Network Forensics: Tracking Hackers through Cyberspace*. Prentice-Hall. doi: 10.1017/ CBO978 110741 5324.004.

DFRWS (2001). 'A Road Map for Digital Forensic Research', Proceedings of the 2001 Digital Forensics Research Workshop (, pp. 1–42. doi: 10.1111/j.1365-2656.2005.01025.x.

ENISA (2019). *Introduction to Network Forensics.*

Lilliard, T. V et al. (2010). *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*. Syngress Media Incorporated. doi: 10.1016/B978-1-59749-537-0.00012-0.

Luttengs, J. T., Pepe, M. & Mandia, K. (2014). *Incident Response and Computer Forensics.* (3rd ed.). McGraw-Hill Education.

*Mustafa, Z.S. (2017). Assessing the Evidential Value of Artefacts Recovered from The Cloud*.

# Unit 2: Cloud Forensics

## Contents



## 1.0 Introduction

Cloud computing is a technology that offers low cost, high power computing, along with large amounts of storage space to users. It grants users pay=per- use access to a range of resources, such as computing infrastructure, application development environments, software and storage, all of which are available real-time over the network on which the cloud sits and can be accessed using a wide range of devices. Cloud computing has three common service model; Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), and three deployment models: private, public, community and hybrid clouds.

While it offers a lot of benefits, these same benefits can be used for criminal activities, and this is where cloud forensics come in. Cloud forensics is a branch of digital forensics where digital investigation processes are applied in cloud computing to extract evidence that can be used in a court of law. Ruan et al. (2011) define cloud forensics as a subset of network forensics, the application of digital forensics in the cloud to generate digital evidence while (NIST, n.d.) defines cloud forensics as,

"*Cloud Computing forensic science is the application of scientific principles, technological practices and derived and proven methods to process past Cloud computing events through identification, collection, preservation, examination and reporting of digital data for the purpose of facilitating the reconstruction of these events.*"

# 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the concept of cloud forensics
- apply investigative techniques to acquire and analyse evidence from the cloud
- write an investigative note which can be used by a third party to obtain the same results.

# 3.0 Main Content

## 3.1 Protocol Analysis

Cloud forensics differs from traditional digital forensics as the processes that are applied in conventional computer forensics may not work in the Cloud due to the nature of the technology (Lillard et al., 2010). For example, data may be stored on servers hosted either on or offsite, which can span multiple jurisdictions, therefore complicating access to evidence, including those that can be found on network devices, multiple users share the same resources which can affect privacy and so on. Therefore, aspects of both traditional digital forensics and network forensics need to be combined with other digital forensics and investigative techniques that are specific to cloud computing to provide a model or guidelines for cloud forensics.

On the flip side, cloud computing can be used in digital investigations acquire, process, analyse and store evidence (Barrett and Kipper, 2010).

In terms of the investigation models, the following were proposed for cloud forensics

Cloud Forensic Framework by Martini and Choo (2012)

- Evidence source identification and preservation
- Collection,
- Examination and Analysis, and
- Reporting and Presentation

This model is slightly different from other models as it has an iteration phase. If evidence of cloud usage is discovered in the examination and analysis phase, a new iteration of the framework commences ensuring all relevant information is collected. There can be more than one iteration when this model is used.

Guoa et al. Model

- Determine the purpose of the forensic requirement
- Identify service type
- Determine Cloud technology
- Identify the source of evidence

Meera et al. (2015) propose a Cloud forensics investigation model with four phases:

- Identification,
- Acquisition and Preservation,
- Analysis and
- Presentation.

Open Cloud Forensics (OCF) by Zawoad et al. (2015)

- Preservation,
- Identification,
- Collection,
- Organisation,
- Presentation, and
- Verification.

As mentioned previously, cloud computing has three main service types: IaaS, PaaS and StaaS. Still, over the years, many more have been proposed such as Storage-as-a-Service (StaaS), Desktop-as-a-Service, Security-as-a-Service and Recovery-as-a-Service. This section will focus on the investigation of StaaS, the provision of block storage space to users on a pay-per-use basis, as cloud-based storage services, are becoming more prevalent both for personal and official use. Examples of cloud storage services include Dropbox, OneDrive, iCloud, GoogleDrive and ownCloud.

**Dropbox** is one of the early cloud storage services made available to users. It is free up to 2GB after that; the user needs to pay for additional space. It can be used as a desktop application, as a web application or as a mobile application. Either way, its usage leave remnants of user activities. For the desktop application, artefacts and their location are summarised in Table 7.

### Table 7: Dropbox Desktop Application Artefacts

| **Artefact** | **Location (Windows 7)** |
|---|---|
| User profile | C:\Users\User_Name\Local\Dropbox |
| Sync folder | C:\Users\ User_Name \Dropbox |
| Prefetch files | C:\Windows\Prefetch\DROPBOX.EXE-XXXXXXXX.pf<br>C:\Windows\Prefetch\DROPBOXUPDATE.EXE-XXXXXXXX.pf |
| Link files | C:\Users\User_Name\Links |

Where the application is accessed via a web browser, deleted files can be recovered within 30 days of deletion in the free version, while in the paid version, there is no time limit for the recovery. Also, web browser and memory analysis can provide more information such as username, filenames, devices connected to the Dropbox account, version history of files (Quick et al. 2013). These are shown in Video CST902_Mod3_Unit2.

**Google Drive** is a file storage service developed by Google. Like Dropbox, it has a desktop application, web application and mobile application. It is associated with a Gmail account and offers 15GB free storage. For the desktop application, the artefacts and their location are summarised in Table 8.

**Table 8: Google Drive Desktop Artefacts**

| **Artefact** | **Location (Windows 7)** |
|---|---|
| Program file | C:\Program Files (x86)\Google |
| User profile | C:\Users\User_Name\AppData\Local\Google\Drive |
| Sync folder | C:\Users\User_Name \GoogleDrive |
| Prefetch file | C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-XXXXXXXX.pf<br>C:\Windows\Prefetch\GOOGLEUPDATE.EXE-XXXXXXXX.pf |
| Link file | C:\Users\User_Name\Desktop\Google Drive.lnk (default location) |

When Google Drive is accessed online, deleted items can be recovered, and analysis of the web browser and memory can provide information on file version history, recent activities, username and local sync path. These are shown in Video CST902_Mod3_Unit2.

## 3.2 Investigation Notes

In Module 1, Unit 1, the guidelines and standards for digital forensics have shown the importance of audit trail and Module 1; Unit 2 has shown that a report is an essential part of an investigation. The report should be clear, focused, timely and reproducible. An analysis report should include the following (Luttengs et al. 2014)

- Title page and table of contents
- Background
- Findings
- Evidence examined
- Timeline
- Conclusion and summary.

Investigation notes should be detailed enough such that a third party can use it for the same analysis and get the same result. It is also important to show that all actions taken by an investigator did not compromise the integrity of evidence, especially when such evidence may be used in the court of law.

 Discussion

What is the impact of analysing only the client's side of cloud storage services in an investigation?

# 4.0 Self-Assessment Exercise(s)

Using the Windows VM created in Module 2, create a Gmail account and install Google Drive. Add and modify five files to Google Drive, using both the desktop application and via the web application over five days. Delete three of the files and add two new ones. Create the image of the VM and extract the following:

a. The sync folder path
b. Last browser session
c. Previous versions of the edited files

*Answers are user-dependent*

# 5.0 Conclusion

Cloud forensics is still relatively new in comparison with traditional digital forensics. It requires the combination of traditional digital forensics, network forensics with the multi-tenant and cross-jurisdictional approach. Several models of DFIP were proposed for cloud forensics to ensure that evidence recovered are legally acceptable. Usage of cloud services such as storage leave remnants of data that can be used as evidence in an investigation.

# 6.0 Summary

The use of cloud services for both personal and organisational are becoming more and more prevalent. This comes with its challenges, especially when investigating a crime. This module has shown that while it is possible to recover information on the use of cloud storage that can be used as

evidence, the investigator may not have access to information that is not resident on the local system. Web browser analysis can be used to extract more information on the use of such services. This is the focus of the next Unit.

# 7.0 References/Further Reading


ACPO (2012). *ACPO Good Practice Guide for Digital Evidence*. Retrieved on19 January 2016 from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Adams, R. (2013). 'The Emergence of Cloud Storage and the Need for a New Digital Forensic Process Model', in Ruan, K. (ed.*). IGI Global.* https://digital-forensics.sans.org/summit-

Eppifani, M. (2013). *Cloud Storage Forensics*. Retrieved from https://digital-forensics.sans.org/summit-archives/Prague_Summit/Cloud_Storage_Forensics_Mattia_Eppifani.pdf

ENISA (2019). *Introduction to Network Forensics*.

Guo, H., Jin, B. & Shang, T. (2012). "Forensic investigations in Cloud environments." In: 2012 International Conference on Computer Science and Information Processing (CSIP). Presented at the 2012 International Conference on Computer Science and Information Processing (CSIP), pp. 248–251. doi:10.1109/CSIP.2012.6308841

Jones, N. et al. (2014). Electronic Evidence Guide- A Basic Guide for Police Officers, Prosecutors and Judges. Retrieved on 25 February 2016 from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680465f73#search=electronic evidence guide

Lilliard, T. V et al. (2010). *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data.* Syngress Media Incorporated. doi: 10.1016/B978-1-59749-537-0.00012-0.

Luttengs, J. T., Pepe, M. & Mandia, K. (2014). *Incident Response and Computer Forensics.* (3rd ed.). McGraw-Hill Education.

# Unit 3: Web Browser Forensics

## Contents



## 1.0 Introduction

A web browser is a software that is used to display contents of web pages. There are several types of web browsers, both open source and proprietary and the most common ones are Internet Explorer, Mozilla Firefox, Google Chrome, Microsoft Edge and Opera. The use of web browsers on the Internet create artefacts relating to user activities which can be used in a digital forensics investigation. This Unit will describe the different types of web browsers and artefacts that can be recovered from their usage.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- discuss common web browsers (Edge, Chrome, Safari and Firefox)
- state the types of evidence that can be acquired from these web browsers.

## 3.0 Main Content

In an investigation, the examination and analysis of internet usage via a web browser are critical as it can be used to support other evidence found or as stand-alone evidence. Information that can be extracted includes the following

- History
- Cache
- Cookies
- Typed URLs
- Form values (Searches, Autofill)
- Downloaded files (Downloads)
- Favourites

These will further be explored in relation to the four web browsers selected for this Unit.

## 3.1 Internet Explorer

Internet Explorer was the default web browser for Windows OS from 1995, but it was replaced by Microsoft Edge with Windows 10. It was a popular web browser due to the popularity of Windows OS, and it is still being used today. Earlier versions of Internet Explorer record data related to websites visited by a user in Index.dat file, while from Internet Explorer 10, this file was replaced by WebCacheV01.dat. The locations of these files are shown in Table 9.

**Table 9: Summary of Internet Explorer Artefacts**

| Artefact | Location |
|---|---|
| History | C:\Users\User_Name\AppData\Local\Microsoft\Windows\History |
| Cache | C:\Users\User_Name\AppData\Local\Microsoft\Windows\INetCache<br><br>C:\Users\User_Name\AppData\Local\Microsoft\Windows\Temporary Internet Files (Win 7) |
| Cookies | C:\Users\User_Name\AppData\Local\Microsoft\Windows\INetCookies<br><br>C:\Users\User_Name\AppData\Roaming\Microsoft\Windows\Cookies |
| Typed URLs | HKEY_USERS\{SID}\Software\Microsoft\Internet Explorer\TypedURLs |
| Favourites | C:\Users\User_Name\Favorites |
| Downloads | C:\Users\User_Name\Downloads |
| Session Data | C:\Users\User_Name\AppData\Local\Microsoft\Internet Explorer\Recovery |

These are shown in Video CST902_Mod3_Unit3.

## 3.2 Microsoft Edge

Microsoft Edge is the default web browser from Windows 10. It is a replacement of Internet Explorer. Evidence that can be recovered from Microsoft Edge is summarised in the table below.

**Table 10: Summary of Microsoft Edge Artefacts**

| Artefact | Location |
|---|---|
| Settings | C:\Users\User_Name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxx\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\xxxxx\DBStore\spartan.edb |
| History | C:\Users\User_Name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat |
| Cache | C:\Users\User_Name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\ |
| Cookies | C:\Users\User_Name\AppData\Local\Packages\microsof.microsofedge_xxxxx\AC\MicrosofEdge\Cookies\ |
| URLs | C:\Users\User_Name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat |
| Favourites | C:\Users\User_Name\AppData\Local\Packages\Microsoft.MicrosoftEdge_8xxxxx\AC\MicrosoftEdge\User\Default\DataStore\Data\ nouser1\120712-0049\BDStore |
| Downloads | C:\Users\User_Name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat |
| Session Data | C:\Users\User_Name\AppData\Local\Microsoft\Internet Explorer\Recovery\Active |

These are shown in Video CST902_Mod3_Unit3.

What is the difference between Typed URLs and History URLs in Internet Explorer?

## 3.3. Mozilla Firefox

Mozilla Firefox is a free and open-source web browser developed by Mozilla. It is one of the popular web browser and according to W3Counter (2019), the fourth most popular web browser. It stores user data in SQLite RDMS, which can be viewed using SQLite viewers. The summary of data that can be used as evidence and where they can be found are summarised in Table 11

**Table 11: Mozilla Firefox Artefacts**

| Artefact | Location |
|---|---|
| History/ Typed URLs/ Favorites/ Downloads | C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite |
| Cache | C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries |
| Cookies | C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite |
| Session Data | C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\sessionstore.js |
| Form Data | C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\formhistory.sqlite |

These are shown in Video CST902_Mod3_Unit3.

## 3.4 Google Chrome

Google Chrome is a web browser developed by Google. It is the most popular web browser, according to W3Counter (2019), which means that the probability of coming across it in an investigation is high. The summary of the artefacts and their location is shown in Table 12.

**Table 12: Google Chrome Artefacts**

| Artefact | Location |
|---|---|
| History/ Typed URLs/ Downloads | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\History |
| Cache | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Cache\<br><br>C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\GPUCache\<br><br>C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Media Cache\ |
| Cookies | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Cookies.db |
| Favourites | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Bookmarks |
| Session Data | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Current Session |

| | |
|---|---|
| | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Last Session<br><br>C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Current Session |
| Form Data | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Web Data |
| Tabs | C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Current Tabs<br><br>C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Last Tabs |

These are shown in Video CST902_Mod3_Unit3.

 Discussion

What is the significance of browser history in digital forensics?

# 4.0 Self-Assessment Exercise(s)

Using the Windows VM, install Google Chrome and Mozilla Firefox, use the two browsers to visit some sites and fill some information over a period of 1 week. Do not disable Auto-fill. Use the tool and extract the following for both browsers

1. Usernames
   *C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Web Data*
   *C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\formhistory.sqlite*
2. Cookies
   *C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Cookies.db*
   *C:\Users\User_Name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite*
3. Last Tab in Google Chrome
   *C:\Users\User_Name\AppData\Local\Google\Chrome\User Data\Default\Last Tabs*

# 5.0 Conclusion

There are many web browsers available, both open-source and proprietary. Regardless of the licence type, they store information that can be used as evidence. Web browsers discussed in this unit are Internet Explorer and Edge by Microsoft, Firefox by Mozilla (Open Source) and Chrome by Google. These are the five most popular browsers, including Safari by Apple.

# 6.0 Summary

Digital forensics enables investigators to examine and analyse data from various sources to have complete information and for event reconstruction. Web browsers are important in an investigation as they provide information on user activities while surfing the Internet. Such information can either be used as stand-alone evidence or as corroborative evidence.

# 7.0 References/Further Reading


Muir, B. (2015). *Windows 10 - Microsoft Edge Browser Forensics*. Retrieved from https://bsmuir.kinja.com/windows-10-microsoft-edge-browser-forensics-1733533818

Muniz, J. & Lakhani, A. (2018). *Investigating the cyber breach: the digital forensics guide for the network engineer.* Cisco Press.

Rathod, D. (2017). "Web Browser Forensics: Google Chrome." *International Journal of Advanced Research in Computer Science.* 8. 896. 10.26483/ijarcs.v8i7.4433.

Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. McGraw-Hill Education Group.

Shipley, T.G. & Bowker, A. (2013). *Investigating internet crimes: an introduction to solving crimes in cyberspace.* Newnes.

Skulkin, O. & Mikhaylov, I. (n.d.). *An Overview of Web Browser Forensics*. Retrieved from https://www.digitalforensics.com/blog/an-overview-of-web-browser-forensics/#content-anchor

W3Counter (2019). *Browser and Platform Market Share*. Retrieved from https://www.w3counter.com/globalstats.php

# Unit 4: Mobile Forensics

## Contents



## 1.0 Introduction

Smart devices have become prevalent in our society. The abilities and functionalities of these devices have become integral parts of our lives. They enable users to connect to the internet and access their emails, applications and browse. While the capabilities of these devices are advantageous, the same capabilities can also be used for criminal activities. Therefore, there is a need for digital forensics to be equipped with knowledge and skills to examine mobile devices as they may contain data that can be used as evidence in an investigation.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- create an image of a mobile device (Android, Windows and Apple) and analyse them
- plan the procedure of acquiring evidence from these devices.

## 3.0 Main Content

### 3.1 Android

Android is an open-source mobile device platform based on the Linux kernel (Hoog, 2011). It is the most popular mobile platform, according to StatCounter (2019) with 76.24% of the global market share. Android devices store huge amounts of data, and the primary source of these data

are apps, these include apps that ship with the device, apps installed by the manufacturer and apps installed by the user. Other sources of data are

- Text messages
- Contacts
- Call logs
- E-mail messages
- Instant Messenger/Chat
- GPS coordinates
- Photos/Videos
- Web history
- Search history
- Social media clients
- Files stored on the device
- Music collection

Android devices store data in two main locations, internal and external storage. The Android API controls internal data storage, while that of external storage is user and application dependent. In terms of memory, it can either be volatile (RAM) or non-volatile. Data in RAM can easily be lost as it is not saved during system reboot. That said, it can still contain data that can be used as evidence such as passwords, encryption keys, usernames, App data and data from system processes and services. The non-volatile data, on the other hand, can easily be preserved as they remain in the memory after reboot or shut down. These include system files and user data. Mobile devices use NAND flash, which is being replaced by eMMC and SD cards for the storage of non-volatile data.

Android supports various filesystems; these are summarised in Table 13.

**Table 13: Android Filesystem Categories**

**(Tamma et al., 2019)**

| Filesystem Category | Examples |
|---|---|
| Flash memory filesystems | exFAT, F2FS, JFFS2, YAFFS2, RFS |
| Media-based filesystems | ExtX, FAT, VFAT |
| Pseudo filesystems | cgroup, rootfs, Procfs, sysfs, tmpfs |

Android devices have six main partitions; /boot, /system, /recovery, /data, /cache and /misc. The /data directory contains user data such as e-mail, contacts, call logs, SMS, and MMS, third party apps, Android apps and some Android settings files. This directory is of great significance as it holds valuable data in terms of digital forensics. Summary of data stored in this directory, most in SQLite databases are shown in Table 14.

**Table 14: Android Device Artefacts and their Locations (Reiber, 2018)**

| Artefact | Location |
|---|---|
| Bluetooth devices | /data/com.android.bluetooth/btopp.db |
| Browser history/ bookmarks/ searches | /data/com.android.browser.db<br>/dbdata/databases/com.android.browser/browser.db (if dbdata exists)<br>/com.android.browser.providers/browser.db |
| Call history/ Contacts | /data.com.android.providers.contacts/contacts2.db<br>/data.com.android.providers.contacts/databases/contacts2.db<br>/dbdata/databases/com.android.providers.contacts/contacts.db (if dbdata exists) |
| Media (images, audio & videos) | /data/com.android.providers.media/external.db<br>/dbdata/databases/com.android.providers.media/external.db (if dbdata exixts) |
| SMS | /data/com.android.providers.telephony/mmssms.db<br>/data.com.android.providers.telephony/app_parts (associated media to message<br>/dbdata/database/com.android.providers.telephony/mmssms.db |
| Autofill data | /data/com.android.browser/databases/autofill.db |
| Geolocation data | /data/com.android.browser/app-geolocation/CachedGeoposition.db |
| Downloads | /data/com.android.providers.download/databases/downloads.db<br>dbdata/databases/com.android.providers.download/downloads.db (if dbdata exists) |
| Apps search | /data/com.android.vending/databases/suggestions.db |
| Email data | /data/com.android.email/cache/<br>/data/com.android.email/db/EmailProvider.db |

These are shown in Video CST902_Mod3_Unit4_1. Other important sources of evidence, also shown in Video CST902_Mod3_Unit4_1 are summarised in Table 15.

### Table 15: Other sources of evidence

| Artefact | Location |
|---|---|
| Installed apps | /system/packages.list – text file with no permissions<br>/system/packages.xml – xml file with permissions |
| Wi-Fi hotspots | /misc/wifi/wpa_supplicant.conf<br>/wifi/bcm_supp.conf<br>/wifi/networkHistory.txt |
| Google artefacts | /data/com.google.android.xxxx |
| Dropped calls | /log/CallDropInfoLog.txt |
| Calls attempted while there was no service | /log/CallNosvcInfoLog.txt |
| Accounts | data/system/accounts.db |
| SIM card data | /system/SimCard.dat |

Where can an investigator find the password in an investigation of Android devices?

## 3.2 iOS

iOS is an operating system used by Apple devices such as iPhone, iPad, iPad mini, and iPod touch, while Apple TV and Apple watch use a hybrid iOS, tvOS and watch OS respectively (Epifani and Stirparo, 2016). iOS uses HFS+; this was discussed in Module 2: Unit 1. Apple devices use NAND memory which is divided into two partitions, system partition and data partition. The system partition contains the OS and all pre-installed applications while the data partition contains user data and user-installed applications. iOS, like Android, stores most of its data in the SQLite database. Artefacts and their locations are summarised in Table 16.

### Table 16: Apple Device Artefacts

### (Epifani and Stirparo, 2016; Reiber 2018)

| Artefacts | Location |
|---|---|
| User password | /private/etc/passwd |
| Saved password | /private/var/Keychains/ |
| Wi-Fi Information | /private/var/preferences/SystemConfiguration/com.apple.wifi.plist |
| SIM card data | /private/var/wireless/Library/Preferences/com.apple.commcenter.plist |
| Account information | /private/var/mobile/Library/DataAccess/AccountInformation.plist<br>/private/var/mobile/Library/Accounts/Accounts3.sqlite<br>/private/var/root/Library/Lockdown/data_ark.plist |
| Contacts | /private/var/mobile/Library/AddressBook/Addressbook.sqlitedb |

| | |
|---|---|
| Audio recording | /private/var/mobile/Media/Recordings/ |
| Call history | /private/var/wireless/Library/CallHistoryDB/CallHistory.storedata<br>/private/var/wireless/Library/CallHistory/call_history.db<br>/private/var/wireless/Library/CallHistoryDB/CallHistory.storedata (iOS 8)<br>/private/var/mobile/Library/Preferences/com.apple.mobile phone.plist<br>/private/var/mobile/Library/Preferences/com.apple.mobilephone.speeddial.plist |
| Email data | /private/var/mobile/Library/Mail/ |
| Images | /private/var/mobile/Media/<br>/private/var/mobile/Media/PhotoData/Thumbnails/<br>/private/var/mobile/Media/PhotoData/Photos.sqlite |
| Maps | /private/var/mobile/Containers/Data/Application/2EA1D4AC-1C04-4CA5-8A77-349D47468457/<br>/private/var/mobile/Library/Preferences/com.apple.Maps.plist |
| Bluetooth devices | /private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.paired.db (from iOS 8)<br>/private/var/mobile/Applications/systemgroup.com.apple.bluetooth/Library/Database (iOS 11x) |
| Safari browser data | /private/var/mobile/Library/Safari/<br>/private/var/mobile/Library/Safari/Bookmarks.db<br>/private/var/mobile/Library/Cookies/Cookies.binarycookies |
| SMS/ iMessage | /private/var/mobile/Library/SMS/sms.db<br>/private/var/mobile/Library/SMS/Attachments<br>/private/var/mobile/Library/SMS/Drafts |
| Social Media and Instant message | /private/var/mobile/Library/Preferences/com.skype.skype.plist<br>/private/var/mobile/Library/Preferences/net.whatsapp.WhatsApp.plist<br>/private/var/mobile/Containers/Shared/AppGroup/<br>/private/var/mobile/Library/Preferences/com.facebook.Facebook.plist |

These are shown in Video CST902_Mod3_Unit4_2.

Discussion

Does the acquisition of mobile devices differ from that of computers?

# 4.0 Self-Assessment Exercise(s)

You are called as a digital forensics examiner in a criminal investigation, and two mobile phones, an Android and an iPhone were given to you to examine to extract the following information (use the image provided for this):

1. Names associated with the devices
2. Networks the device were connected to
3. The last number dialled
4. The last website visited
5. First SMS on received

These are user-dependent.

# 5.0 Conclusion

Android and Apple devices are the most popular smart devices in the world today; this makes them likely to be encountered during an investigation. This unit discussed the types of information on Android and Apple devices that use iOS, which may be of evidential value and their locations.

# 6.0 Summary

Smart devices have become an integral part of our lives. Their capabilities enable us to access the Internet, use various apps, make and receive audio and video calls, send and receive multimedia messages etc. for both personal and business use. However, these capabilities are being exploited by criminals to commit crimes. Thus, digital forensics experts need skills to examine, analyse and interpret these devices either for investigation or for research purpose. A source of evidence from mobile forensics which was not covered in this unit is social media applications; this will be discussed in the next unit.

# 7.0 References/Further Reading


Abalenkovs, D., Bondarenko, P., Pathapati, V.K., Nordbø, A., Piatkivskyi, D., Rekdal, J.E. & Ruthven, P.B. (2012). *Mobile Forensics: Comparison of Extraction and Analyzing Methods of iOS and Android*. Gjovik, Norway: Gjovik University College.

Al-Hadadi, M. & AlShidhani, A. (2013). "Smartphone forensics analysis: A case study." *International Journal of Computer and Electrical Engineering,* 5(6), p.576.

Aouad, L.M. & Kechadi, T.M. (2012). "Android Forensics: A Physical Approach." In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Birani, B. & Birani, M. (2016). *iOS Forensics Cookbook.* Packt Publishing Ltd.

*Curran, K., Robinson, A., Peacocke, S. & Cassidy, S. (2012). Mobile Phone Forensic Analysis. In Crime Prevention Technologies and Applications for Advancing Criminal Investigation* (pp. 250-262). IGI Global.

Epifani, M. & Stirparo, P. (2016). *Learning iOS Forensics*. Packt Publishing Ltd.

Hoog, A. & Strzempka, K. (2011). *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS devices*. Elsevier.

*Hoog, A., 2011. Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Elsevier.

Jovanovic, Z. & Redd, I.D.D. (2012). *Android Forensics Techniques*.

# Unit 5: Social Media Forensics

## Contents



## 1.0 Introduction

Social media are social networking sites that allow individuals to build up their profiles, interact with their contacts and access information based on their preferences. There are several categories of social media-based such as collaboration platforms, blogs, location-based, content communities, virtual platforms etc. (Brunty & Helenek, 2014). Social media applications include Facebook, Twitter, LinkedIn, YouTube and so on. Most of these applications have both mobile, and web applications and they come bundled on smartphones.

Social media applications have become very popular where media outlets quote tweets, and Facebook posts and most organisations have social media handles for disseminating information. While social media have numerous advantages, they also have their disadvantages as criminals use them for nefarious activities such as harassment, identity theft and bullying. The use of social media applications leaves data remnants which can be used as evidence in an investigation and therefore, investigators must have the skills and knowledge required to conduct investigations on social media applications in a legally acceptable manner.

This unit will focus on two popular social media applications, Facebook and Twitter, and the evidence that that can be retrieved from their use.

# 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- identify the types of evidence that can be acquired from social media applications
- analyse evidence from social media applications.

# 3.0 Main Content

## 3.1 Facebook

Facebook is the most popular social networking applications, with more than 1 billion active users. Users can add friends, send messages, post texts, images, audios, videos and locations on their timelines, comment and like posts etc. It has both web and mobile app, which means that during an investigation, both need to be considered to ensure that all data related to Facebook use which may be used as evidence is recovered.

Facebook App stores data related to user activities in several SQLite databases from Window 10 in C:\Users\User_ Name\ AppData\ Local\ Packages\Facebook.Facebook_xxxxx\LocalState\FacebookUserID\DB. These are summarised in Table 17.

**Table 17: Facebook Artefacts (Choudhary et al., 2016)**

| Artefact | Description |
|---|---|
| Analytics.sqlite | Stores user activities for feedback. |
| Friends.sqlite | Stores information on friends including names, emails and phone numbers |
| FriendsRequest.sqlite | Stores pending friend request with timestamp |
| Messages.sqlite | Stores message information with sender and receiver details, timestamps, attachments etc |
| Notifications.sqlite | Stores user notifications such as events, comments, likes etc |
| StickerPacks.sqlite | Stores information on stickers used in chats with timestamps |
| Stories.sqlite | Stores news feeds on the user timeline |

These are shown in Video *CST902_Mod3_Unit4_1*. In the case where the web application is used, then the web browser analysis, discussed in Unit 3 of this Module, will provide information on user activities which can be used as evidence.

## 3.2 Twitter

Twitter is another popular social media application where users can send and read short messages with a character limit of 280. Users can also like, retweet and reply messages and post images, audios, videos and location. It also has both web and mobile applications.

In terms of analysis, the Twitter app from Windows 10 store user activities also in SQLite database at C:\Users\User_Name\ AppData\Local\ Packages\xxxx.Twitter_xxxxx\LocalState\xxxxx\Twitter_ID\twitter.sqlite. Unlike Facebook, Twitter only has one SQLite database, but this stores a wealth of information that are of evidentiary value such as tweets, followers, retweets, etc. The Tables of interest are summarised in Table 18.

**Table 18: Twitter Artefacts (Majeed & Saleem, 2017)**

| Table | Description |
|---|---|
| Messages | Stores tweets and direct messages |
| Search_queries | Stores searches by the user |
| Users | Stores information of the user's followers |
| Statuses | Stores previous and current statuses of the user |
| Activities2 | Stores activities related to the user such as mentions, tweets, followers etc |

These are shown in Video *CST902_Mod3_Unit4_2.* Also, the application settings for Twitter are located at C:\Users\User_ Name\App Data\ Local\Packages\xxxx.Twitter_xxxxx\Settings\settingsd.dat, this stores user name, profile picture and Twitter ID. As with Facebook, if the web application was used, then web browser forensics should be used to obtain evidence.

Other sources of evidence for both Facebook and Twitter include link files, prefetch files, registry hives, event logs and memory analysis. All these were discussed in Module 2; Unit 2.

As previously mentioned, these applications can be accessed via a mobile app. In such a case, mobile forensics, discussed in the previous Unit, may be used to extract and analyse evidence.

 Discussion

How can the information stored in the databases of Facebook and Twitter account be retrieved without compromising the integrity of these databases?

# 4.0 Self-Assessment Exercise(s)

Create a Windows 10 VM and install both Facebook and Twitter Apps. Use fictional IDs to create a user and interact with the applications for a week, add and delete files and message. Create the image of the disk and extract the SQLite databases for both apps. Take a screenshot of the following and attach

1. Tweets
   C:\Users\User_Name\AppData\Local\Packages\xxxx.Twitter_xxxxx\LocalState\xxxxx\Twitter_ID\twitter.sqlite - Messages
2. Friends
   C:\Users\User_Name\AppData\Local\Packages\Facebook.Facebook_xxxxx\LocalState\FacebookUserID\DB\friends.sqlite
3. Activities
   C:\Users\User_Name\AppData\Local\Packages\xxxx.Twitter_xxxxx\LocalState\xxxxx\Twitter_ID\twitter.sqlite - Activities
4. Notifications
   C:\Users\User_Name\AppData\Local\Packages\Facebook.Facebook_xxxxx\LocalState\FacebookUserID\DB\Nnotifiations.sqlite

# 5.0 Conclusion

User activities on social media applications have been shown to provide detailed information which can be used to create a timeline of user activities in an investigation. Apart from the databases, there are other sources of evidence which were discussed in earlier parts of this course. All these need to be taken into account during an investigation to ensure completeness of evidence.

# 6.0 Summary

The advent of social media has made interactions between communication among people faster and easier with a wider reach of audience. This has made it attractive to individuals with criminal intentions to use it to commit crimes. The application of digital forensics processes and guidelines to investigate such crime to show that a crime has been committed in the use of social media applications can be termed as social media forensics. And unlike traditional digital forensics, this encompasses various types of digital forensics; traditional, web browser, network and mobile forensics. Therefore, all these components of digital forensics need to be employed to ensure that comprehensive evidence is acquired.

# 7.0 Further Readings


Al Mutawa, N., Baggili, I. & Marrington, A. (2012). "Forensic analysis of social networking applications on mobile devices." *Digital Investigation*, 9, pp.S24-S33.

Awan, F.A. (December 2015). "Forensic Examination of Social Networking Applications on Smartphones." In 2015 conference on information assurance and cybersecurity (pp. 36-43). IEEE.

Muniz, J. & Lakhani, A. (2018). *Investigating the Cyber Breach: The Digital Forensics Guide for the Network Enginee*r. Cisco Press.

Powell, A. & Haynes, C. (2020). *Social Media Data in Digital Forensics Investigations. In Digital Forensic Education* Springer, Cham. (pp. 281-303).

Shipley, T.G. & Bowker, A. (2013). *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace.* Newnes.

Yusoff, M.N., Dehghantanha, A. & Mahmod, R. (2017). "Forensic Investigation Of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as Case Studies." *In Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications* (pp. 41-62). Syngress.

Zampoglou, M., Papadopoulos, S., Kompatsiaris, Y., Bouwmeester, R. & Spangenberg, J. (April 2016).. "Web and social media image forensics for news professionals." In Tenth International AAAI Conference on Web and Social Media.

# Module 4: Incidence Management

## Module Introduction

Module 4 is on incidence management. It contains types and process of incidence response and policies based on best practices and incidence handling action plan that will counteract the different attack types. It consists of two units.

Unit 1: Incidence Response
Unit 2: Incidence Handling

## Unit 1: Incidence Response

### Contents



### 1.0 Introduction

In this unit, you will learn the types and process of incidence response, phases which an incidence response most address and polices of incidence response. It is a recipe for disaster if you have to wait for an incident to occur before figuring out what you will do. Adequate incident response planning and implementation allow responds by an organisation in a systematic manner to an incident that will be effective and on time. Not planning for cybersecurity incident by an organisation will cause huge losses for a long duration of time. An increase in incident occurrence is shown in the current trend. The attacks are now getting more sophisticated, resulting in escalating losses.

# 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the incidence response
- describe the types of incidence
- develop incidence response policies based on best practice.

# 3.0 Main Content

## 3.1 Incidence Response

An incident is an imminent threat of violation of computer security policies, standard security practices or acceptable use policies. Some other definition is an attempted use or unauthorised access that is successful, disclosure, modification, use, or loss of information or interference with network operations. Organisations do define an incident as human threat activities. It could include any disruptive thing, including an order from the court for the discovery of disruption from natural or electronic disaster information.

## 3.2 Types of Incidence

An incident in cybersecurity is an event that impacts in a negatively way the integrity, confidentiality and data availability. An incident in Cybersecurity may be unintentional, e,g someone forgets the activation of access list in a router or intentional, like a targeted attack by a hacker. Classification of this event could be technical or physical. Technical incidents include malware, viruses, denial-of-service (DoS) and system failure. Physical incidents include lost or stolen laptops or social engineering and mobile devices.

There are various type of related incidents of Cybersecurity, and the emergence of new types of incidents frequently. US-CERT provides categories of reporting time frames used by federal agencies and security incidents, as shown in **figure 4.1**.

| Figure 4.1: Security Incidents and Reporting Time Frames | | | |
|---|---|---|---|
| **Category** | **Name** | **Description** | **Reporting Time Frame** |
| CAT 1 | Unauthorised Access | Logical or physical access is gained by individual without been permitted to the system, network, data, application or other sources | Within 1 hour of discovery/ detection |
| CAT 2 | Denial-of-service (DoS) | The success of this attack impairs or prevent a normal authorized functionality of application, systems or network by exhausting the resources | Within 2 hours of discovery/ detection if the successful attack is still ongoing |
| CAT 3 | Malicious Code | Malicious software installation successfully (e.g., Trojan horse, virus, worm, or other code-based malicious entity) which infects the operating system. Application | Daily; within 1 hour of discovery/detection if widespread |
| CAT 4 | Improper Usage | Acceptable computing use policies are violated by persons | Weekly |
| CAT 5 | Scans/Probes/ Attempted Access | Seeking to identify a computer or access by any activities. protocols, service open ports or whatever combination | Monthly |
| CAT 6 | Investigation | Unconfirmed incidents that are anomalous activity or potentially malicious | N/A |

## 3.3 Process of Incidence Response

When a formal program can prepare an entity for an incident is known as incident response. It generally includes:

- **Preparation** to establish roles, responsibilities, and plans for how an incident will be handled
- **Detection and Analysis** capabilities to identify incidents as early as possible and effectively assess the nature of the incident
- **Investigation** capability of recognizing an adversary is required
- **Mitigation and Recovery** procedures to contain the incident, reduce losses and return operations to normal
- **Post-incident Analysis** to determine corrective actions to prevent similar incidents in the future.

### 3.3.1 Incidents phases which an incident response policy must address

The proposed model presented by Schultz, Brown, and Longstaff demonstrate the six-phase model of incident response which including preparation, identification, containment, eradication, restoration and follow-up:

**Preparation**: This phase prepares the organisation into developing an incident response plan before an incident occur. Proper preparation enhances smooth execution. This phase activity includes:

- Setting up of an approach for incident handling
- Setting up policy and warning banners in information systems to deter intruders and allow information collection
- Setting up a stakeholders communication plan
- Building up criteria on when reporting of the incident to the authorities is done.
- Building up a process that will activate the incident management team
- Setting up a location that is secured to execute the incident response plan
- Ensuring the equipment needed is available

**Identification**: This phase aims to verify if an incident has already happened, and more detail found out about the incident. Reports may come from information systems on the possible incident, other organisations or end-users. Not all reports are valid incidents, as they may be false alarms or may not qualify as an incident. Activities in this phase include:

- Assigning ownership of a potential incident or an accident to an incident handler
- confirm that event or reports qualify as an incident
- Set up a chain of custody during identification when handling potential evidence
- Determining the severity of an incident and escalating it as necessary

**Containment**: After the identification and confirmation of an incident, the IMT is activated, and incident handler information is shared. A detailed assessment will be conducted by the team and contact the business manager or system owner of the affected assets/information systems to coordinate further action. Action that was taken in this phase is to limit the exposure. Activities in this phase include:

- Activate the incident response/management team to contain the incident
- Notify the stakeholders that are appropriately affected by the incident

- Securing agreement on actions that are taken which may affect service availability of risk or service of the containment process
- Getting the IT representative and relevant virtual team members involved to implement containment procedures
- Obtaining and preserving evidence
- Documenting and taking backups of actions from this phase onward
- Controlling and managing communication to the public by the public relations team

**Eradication**: When containment measures have been deployed, it is time to determine the root cause of the incident and eradicate it. Eradication can be done in several ways: restoring backups to achieve a clean state of the system, removing the root cause, improving defences and performing vulnerability analysis to find further potential damage from the same root cause. Activities in this phase include:

- Determining the signs and cause of incidents
- Locating the most recent version of backups or alternative solutions
- Removing the root cause. In the event of worm or virus infection, it can be removed by deploying appropriate patches and updated antivirus software.
- Improving defences by implementing protection techniques
- Performing vulnerability analysis to find new vulnerabilities introduced by the root cause

**Recovery**: This phase ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDO) or business continuity plan (BCP). The time constraint up to this phase is documented in the RTO. Activities in this phase include:

- Restoring operations to normal
- Validating that actions taken on restored systems were successful
- Getting involvement of system owners to test the system
- Facilitating system owners to declare a normal operation

**Lessons learned**: At the end of the incident response process, a report should always be developed to share what occurred, what measures were taken, and the results after the plan were executed. Part of the report should contain lessons learned that provide the IMT and other stakeholders valuable learning points of what could have been done

better. These lessons should be developed into a plan to enhance the incident management capability and the documentation of the incident response plan. Activities in this phase include:

- Writing the incident report
- Analysing issues encountered during incident response efforts
- Proposing improvement based on issues encountered
- Presenting the report to relevant stakeholders.

### 3.3.2 Policies of Incidence Response

Policy governing incident response is highly individualized to the organisation. However, most policies include the same key elements: Example of these policies are:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms

The definition of roles and Organisational structure, levels of authority and responsibilities; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process

- Prioritisation or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

## 4.0 Self-Assessment Exercise(s)

1) List the process of incidence response.
2) Explain two activities in the preparation phase of incidence response policy.

# 5.0 Conclusion

The Unit present the process and phases of incidence response policies based on best practices. Several organisations are required to put effort significantly into cyberattack protection and prevention from causing disruption or harm. However, there are no perfect security controls, and all this cannot be eliminated; therefore, it is important organisations make preparation for, and are capable of managing and detecting potential problems of cybersecurity. Incidence response policies and processes through planning make it easy to prepare against the attack and reduce the risk of attack to an organisation.

# 6.0 Summary

The Unit took us through the basic definition of incidence response. Security incidents and the reporting time frame was discussed in section 3.2. Section 3.3 discussed the process of incidence response and incident phases which an incident response policy must address, and lastly policies of incidence response.

# 7.0 References/Further Reading


MITRE (February 2014). *Common Attack Pattern Enumeration and Classification* (CAPEC) Retrieved from http://capec.mitre.org/

Moody, R. (2001). "Ports and Port Scanning: An Introduction", *ISACA Journal*, Volume 4,
www.isaca.org/Journal/Past-Issues/2001/Volume-5/Pages/Ports-and-Port-Scanning-An-Introduction.aspx

National Institute of Standards and Technology (NIST), (September 2012). Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, USA,

Open Web Application Security Project (OWASP). OWASP Top 10, 2013, www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Schultz, E.E., Brown, D.S., & Longstaff, T.A.; (1990). *Responding to Computer Security Incidents: Guidelines for Incident Handling, Lawrence Livermore National Lab.,* USA,

The 2013 Global Information Security Workforce Study, 2014, www.isc2cares.org/Workforcestudy

https://searchsecurity.techtarget.com/definition/incident-response

# Unit 2: Incidence Handling

## Contents



## 1.0 Introduction

In this unit, you will learn about the requirement and facilities for the incident handler, steps to follow in handling incident and recommendation for incident handling. This study will guide you in the prevention of computer or network attack while eliminating incident and minimise loss through proper handling of incidents.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain incidence handling
- develop incidence handling action plan to counteract attacks.

## 3.0 Main Content

### 3.1 Incidence Handling

Incidence handling capabilities are required to be able to detect incidents rapidly and minimises loss. It makes the computer more secure and capable enough to withstand any type of attack. Incidence handling requires tools and resources for effective handling of the incident. These lists are supposed to be a starting point for discussions on which resources and tools an organisation's incident handlers need. For example, smartphones are one of the ways to have a coordination mechanism and resilient emergency

communication. An organisation should have multiple (separate and different) coordination mechanisms and communication in case of failure of one mechanism.

## 3.2 Incident Handler Communications and Facilities

There is need the incident handler communicates and also have facilities for prompt organisation response. The types of communication and facilities are discussed below:

- **Contact information:** For team members and others within and outside the organisation (primary and backup contacts), such as other incident response teams and law enforcement; information might be an email address, phone numbers, instructions for verifying the contact's identity and public encryption.
- **On-call information:** For teams that are within the organisation, including escalation information.
- **Incident reporting mechanisms:** Such as online forms, email address, phone numbers and secure instant messaging systems that users could use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously.
- **Issue tracking system:** For incident information tracking, status, etc.
- **Smartphones:** To be carried by members of the team for off-hour support and onsite communications.
- **Encryption software:** To be used among team members for communication, within the organisation and with external parties; for Federal agencies, the software must use a FIPS-validated encryption algorithm.
- **War room:** For central communication and coordination; if a permanent war room is not necessary or practical, the team should create a procedure for procuring a temporary war room when needed.
- **Secure storage facility:** For securing evidence and other sensitive materials.

**Incident Analysis Hardware and Software**

- **Digital forensic workstations and backup devices** to create disk images, preserve log files, and save other relevant incident data
- **Laptops** for activities such as analysing data, sniffing packets, and writing reports.
- **Spare workstations, servers, and networking equipment, or the virtualized equivalents**, which may be used for many purposes, such as restoring backups and trying out malware.
- **Blank removable media**

- **Portable printer** to print copies of log files and other evidence from non-networked systems.
- **Packet sniffers and protocol analysers** to capture and analyse network traffic.
- **Digital forensic software** to analyse disk images
- **Removable media** with trusted versions of programs to be used to gather evidence from systems.
- **Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions future.

## 3.3 Steps to Take in Handling Incident

Table 3-1 checklist shows the most important steps to undergo during incident handling. There may be a variation of the steps based on the incident and the nature of the different incidents. For example, If what has happened is known by the handler due to analysis of indicators (Step 1.1), there may be no need for performing step 1.2 or 1.3 which is to research the activity further. The checklist provides guidelines to handlers on the major steps that should be performed; The exact sequence of the steps to be followed is not dictated.

**Table 19: Incident Handling Checklist**

| Action | | Completed |
|---|---|---|
| **Detection and Analysis** | | |
| 1. | Confirm if an incident has occurred | |
| 1.1 | Analyse the indicators and precursors | |
| 1.2 | Look for correlating information | |
| 1.3 | Perform research (e.g., search engines, knowledge base) | |
| 1.4 | As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence | |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) | |
| 3. | Report the incident to the appropriate internal personnel and external organizations | |
| **Containment, Eradication, and Recovery** | | |
| 4. | Acquire, preserve, secure, and document evidence | |
| 5. | Contain the incident | |
| 6. | Eradicate the incident | |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited | |
| 6.2 | Remove malware, inappropriate materials, and other components | |
| 6.3 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them | |

| | | |
|---|---|---|
| 7. | Recover from the incident | |
| 7.1 | Return affected systems to an operationally ready state | |
| 7.2 | Confirm that the affected systems are functioning normally | |
| 7.3 | If necessary, implement additional monitoring to look for future related activity | |
| **Post-Incident Activity** | | |
| 8. | Create a follow-up report | |
| 9. | Hold lessons learned meeting (mandatory for major incidents, optional otherwise) | |

### 3.3.1 Recommendations for Incidence Handling

Below is a summary of key recommendations for handling incident:

- **Acquire tools and resources that may be of value during incident handling:** For efficient handling of incidence by the team, several tools and resources must be made available to them. E.g. port list, contact lists, encryption software.
- **Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secured.** It is beneficial to the organisation preventing incidents and also reduces the workload of the incident response team. Performing periodic risk assessments and reducing the identified risks to an acceptable level is effective in reducing the number of incidents. Awareness of security policies and procedures by users, IT staff, and management is also very important.
- **Identify precursors and indicators through alerts generated by several types of security software:** Intrusion detection and prevention systems, antivirus software, and file integrity checking software are valuable for detecting signs of incidents. Each type of software may detect incidents that the other types of software cannot, so the use of several types of computer security software is highly recommended. Third-party monitoring services can also be helpful.
- **Establish mechanisms for outside parties to report incidents:** Outside parties may want to report incidents to the organization—for example, they may believe that one of the organization's users is attacking them. Organizations should publish a phone number and email address that outside parties can use to report such incidents.
- **Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems.** Logs from operating systems, services, and applications frequently provide value during incident analysis, particularly if auditing was enabled. The logs can provide information such as which accounts were accessed and what actions were performed.

- **Profile networks and systems:** Profiling measures the characteristics of expected activity levels so that changes in patterns can be easily identified. If the profiling process is automated, deviations from expected activity levels can be detected and reported to administrators quickly, leading to faster detection of incidents and operational issues.
- **Understand the normal behaviours of networks, systems, and applications:** Team members who understand normal behaviour should be able to recognize abnormal behaviour more easily. This knowledge can best be gained by reviewing log entries and security alerts; the handlers should become familiar with the typical data and can investigate the unusual entries to gain more knowledge.
- **Create a log retention policy:** Information regarding an incident may be recorded in several places. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks.
- **Perform event correlation:** Evidence of an incident may be captured in several logs. Correlating events among multiple sources can be invaluable in collecting all the available information for an incident and validating whether the incident occurred.
- **Keep all host clocks synchronised:** If the devices reporting events have inconsistent clock settings, event correlation will be more complicated. Clock discrepancies may also cause issues from an evidentiary standpoint.
- **Maintain and use a knowledge base of information:** Handlers need to reference information quickly during incident analysis; a centralized knowledge base provides a consistent, maintainable source of information. The knowledge base should include general information, such as data on precursors and indicators of previous incidents.
- **Start recording all information as soon as the team suspects that an incident has occurred:** Every step took, from the time the incident was detected to its final resolution, should be documented and timestamped. Information of this nature can serve as evidence in a court of law if legal prosecution is pursued. Recording the steps performed can also lead to a more efficient, systematic, and less error-prone handling of the problem.
- **Safeguard incident data:** It often contains sensitive information regarding such things as vulnerabilities, security breaches, and users that may have performed inappropriate actions. The team should ensure that access to incident data is restricted properly, both logically and physically.

- **PrioritiSe handling of the incidents based on the relevant factors;** This is because of resource limitations, incidents should not be handled on a first-come, first-served basis. Instead, organisations should establish written guidelines that outline how quickly the team must respond to the incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident. This saves time for the incident handlers and justifies management and system owners for their actions. Organisations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.
- **Include provisions regarding incident reporting in the organisation's incident response policy:** Organisations should specify which incidents must be reported when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organisation, and system owners.
- **Establish strategies and procedures for containing incidents;** It is important to contain incidents quickly and effectively to limit its business impact. Organisations should define acceptable risks in containing incidents and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.
- **Follow established procedures for evidence gathering and handling:** The team should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss evidence handling, then develop procedures based on those discussions.
- **Capture volatile data from systems as evidence:** This includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system's evidence.
- **Obtain system snapshots through full forensic disk images, not file system backups:** Disk images should be made to sanitised write-protectable or write-once media. This process is superior to a file system backup for investigatory and evidentiary purposes. Imaging is also valuable in that it is much safer to analyze an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.

- **Hold lessons learned meetings after major incidents:** Lessons-learned meetings are extremely helpful in improving security measures and the incident handling process itself.

## 4.0 Self-Assessment Exercise(s)

1) Explain incidence handling.

Incidence handling capabilities are required to be able to detect incidents rapidly and minimise loss. It makes the computer more secure and capable enough to withstand any type of attack. Incidence handling requires tools and resources for effective handling of the incident.

## 5.0 Conclusion

This Unit presented incident handling with an emphasis on communication facilities for incidence handlers. It examined steps required in the performing of incident handling and recommendation for effective handling of incidence. The ability of an incident handler in following all discussed procedure will help for the development of action plans of incident handling, therefore, making it easy for prompt incident detection and loss reduction. It will also help our network and computer security in case of an attack.

## 6.0 Summary

The Unit took us through the basics of incident handling. Incident handler communication facilities were presented in 3.2. Section 3.3 explains the steps required for effective performance during incident handling and also recommendation on best practices during incident handling.

## 7.0 References/Further Reading

FIPS 199, *Standards for Security Categorisation of Federal Information and Information Systems*. Retrieved from http://csrc.nist.gov/publications/PubsFIPS.html

FIPS 140-2, *Security Requirements for Cryptographic Modules*, Retrieved from http://csrc.nist.gov/publications/PubsFIPS.html.

*Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.2.* Retrieved from http://csrc.nist.gov/ publications/ PubsSPs.html#800-117.

NIST_Operating System And Application Security Baselines Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-30. *Guide for Conducting Risk Assessments*. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html#800-30-Rev1.

NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organisations. Retrieved from* http://csrc.nist.gov/publications/PubsSPs.html#800-137

NIST hosts a security checklists repository Retrieved from http://checklists.nist.gov/.

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* Retrieved from http://csrc.nist.gov/publications/PubsSPs.html#800-83).