Forensic Report

|  |  |
| --- | --- |
| Client: |  |
| Client’s Case ref: |  |
| Case name: |  |
|  |  |
| CF Case ref: |  |
| Report number: |  |
| Report Author: |  |
| Report date: |  |

Forensic Report

# Introduction

## For the purposes of this report, technical explanations of the various procedures and terms used will be found in the **Descriptions** Section 5. Items covered in this way will be underlined thus **EnCase®**.

# Case Background

## 

# The Material

## All analysis was carried out using a **Forensic Workstation** (**FWS**) and software known as **EnCase®**

## A forensic image copy, using EnCase® version 6.71, was made of the hard drive prior to any analysis being undertaken.

## All analysis was then carried out using the forensic copy in the form of an .E01 file.

# Descriptions

## **EnCase**®

Software produced by Guidance Software which provides investigators with the tools to conduct complex investigations with accuracy and efficiency. It allows completely non-invasive computer forensic investigations while allowing examiners to easily manage large volumes of computer evidence and view computer drive contents including files, operating system artefacts, file system artefacts, and deleted files or file fragments located in file slack or unallocated space.

## **Internet Evidence Finder (IEF)**

## Software produced by Magnet Forensics which provides investigators with tools to conduct complex investigations with accuracy and efficiency. IEF allows investigators a complete non-invasive full computer search for all common files and evidence possibly relevant to the forensic investigation. IEF comes with many search features such as to search for a certain type of document, including PDF files, Text files, Word Documents, Excel Documents, and much more.

## **Internet Browser**

## Software on a computing device which allows you to visit and browse webpages on the internet. The most common 3 web browsers are Internet explorer, Firefox & Google Chrome. These are created and compiled under different variants of computer code however relate with the same principles of visiting web pages and recording them in browser history.

## **Internet Browsing History**

## A data collection of webpage names, sources and times, created by an Internet Browser. Internet browsing history shows exactly what the Internet Browser has been used for and where it has visited on the web.

## **Google Search Engine**

## A search engine created by Google ™ which allows you to quickly search through the internet to find websites and information about what it is that you are looking for. It is the most common internet search engine and can find and search through millions and millions of websites located on the internet.

## **Internet Search Tabs**

## During usage of an Internet Browser, each website you visit is stored and presented in what is called a tab. Users of the Internet browser can have multiple tabs open at one time in order to effectively and efficiently search through multiple pages of the internet at the same time.

## **Central Processing Unit (CPU)**

## The Central Processing Unit (CPU), is the heart of a computing device, it is the internal hardware component which processes every bit of data necessary to compute the mathematical and electrical circuitry equations and actions required to fulfil tasks and functions in an everyday computing device.

## **Random Access Memory (RAM)**

## The Random Access Memory (RAM), is the internal component of a computing device which stores execution instructions for the CPU to retrieve and initiate; in the form of machine code. The CPU retrieves the instructions from the RAM and translates them into a binary representation of the value in order to execute the instructions in the form of sending voltage (1) and not sending the voltage (0) to millions of transistors; a series of electrical circuits.

## **E01 Image File**

## An .E01 image file is a copy of a hard drive created by EnCase®. All files are copied from the hard drive whilst preventing write access to the hard drive in order preserve evidential integrity. The files are then compressed into what we call an image of the drive.

## 

## **Compression**

## Compression is a method of reducing the representation of a value usually required to store data. For example in ASCII code, a type of machine code, values are usually represented by a 7 digit code however can be shortened to a 3 digit. Compressing a file or multiple files dramatically decreases the size required to store the data, and as such further dramatically increases the speed of transferring the required data from one location to another.

## **7-zip & .zip files**

## 7-zip is software created for the purpose of compressing files into one single file which it can then later access and un-compress/extract if desired. This software has its own file type in the name of .7zip, however it can also use much more file types, for example .zip. This software provides the capability of different compression methods among other features, such as setting a password on your compressed file. A zip is a compressed file.

## **ExifTool**

## Software created by Phil Harvey for the forensic viewing of metadata information attached to a file. On every file on a computer is contained metadata, metadata is a bundle of information about a file on a computer. This information can include such examples as creation date and time, modified date and time, last accessed date and time, creation author, file size, file type and much more. ExifTool provides a tool outside of EnCase which allows forensic practitioners the ability to securely and certifiably retrieve all information available within a file.

## **Registry**

The registry is the central hierarchical database used in all versions of the operating system Microsoft Windows. The registry is used to store information necessary to configure and as such run the operating system. The registry contains crucial information that Windows continually collocates with during operation. Examples of information contained inside the registry can include the profiles for each user account on the system, applications installed on the computer, types of documents that each user can create, what hardware exists on the system, and much, much more.

# Section 1 – PC Information

# Section 2 - Evidence

# Appendices