**5 Sub-Project – Written Instruction Development**

**[Hamza Pervaiz]**

In this chapter I will discuss the following topics:

* Introduction
* Overview
* Development
* Aims

**5.1 Introduction**

**5.1.1 Subtitle**

This document is going to outline and detail the written instruction development for Anti-Forensic solutions. It intends to outline the overview, development and aims of the overall sub project.

Computer Forensics is the practice of collecting and analysing digital data in a way which is legally admissible.

Forensics can also be defined as a service provided to a customer for different forensic operations on their devices with their consent- such as data recovery, partition recovery and general PC maintenance.

**5.2 Overview**

**5.2.1 Subtitle**

As part of our project I was assigned the responsibility of working on the sub-project. This was assigned to me by deputy and team leader. I was given the responsibility of creating instructions for the forensic tools we are going to sell.

A list of packages was given to me by deputy and team leader. These are as follows:

Package 1- Password and Encryption

Package 2- Key Recovery and File Recovery

Package 3- Disk Cleanup and Benchmark

Package 4- Hardware monitor, debug hardware , network monitor.

Package 5- Wireshark, Network security assessment tool, Network Monitor, Packet sniffer.

Package 6- All tools.

Forensic software allows forensic investigators to perform a wide variety of operations. The field of computer forensic investigation makes use of tools in order to allow practitioners to carry out their tasks. Its purpose is to enable investigators to examine all types of cyber-crime. As the different types of software can be very complex I decided to create a set of instructions as simple as possible.

Forensic tools allow individuals to gather data from a system without altering the data on the system. This is a fundamental principle of computer forensic examination as it allows evidence to be obtained in different scenarios and also contributes to admissibility of evidence in court.

Many organisations use computer forensics to benefit themselves in a variety of different situations. Some of these are as follows:

* Fraud
* Espionage
* Intellectual Property Theft
* Employment disputes
* Police investigations7

With all forensic investigations with references to law enforcement there are a basic set of principles which must be adhered to in all investigations. These are as follows:

ACPO Principle 1:

“ No action should be taken by an analyst that should change data held on a computer or other media which may subsequently be relied upon in court.”

ACPO Principle 2:

“In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and implications of their actions.”

ACPO Principle 3:

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

ACPO Principle 4:

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

In order for evidence to be presented in court. It is important the above principles are adhered to in order for an investigation to be successful.

(MMU Moodle – Week 3 – Forensic Process)

Our software packages intend to also provide the end user with a “e-document” which notifies them of the different legalities surrounding forensic investigations in order to allow them to obtain wider knowledge on the process.

Upon sale of these products, the overview is to allow customers to effectively conduct forensic examinations and investigations on their own machines and further use the software which they may have thought complex at start with their own ability.

**5.3 Development**

**5.3.1 Subtitle**

I decided to section out the instructions for each software in a tidy way. I did this by separating each software in to different sections and explaining the use of each software.

The overall written responsibility of the software was quite difficult for myself as I had not used these softwares before. As a result, extensive research had to be undertaken in order for a set of written instructions to be created.

After conducting some research it became evident to myself that there are a number of different forensic software available.

This included computer forensics, memory forensics and mobile forensics.

The packages we created contain an array of different software which conduct both computer forensics and mobile forensics.

Example Software 1: Password Unlocking

For this service we provide the software “jPassword”. JPassword is the ultimate recovery tool for Windows and Linux. It is able to crack any password protected archive.

The instructions document outlines on how to install the software and run it with supporting screenshots. I decided screenshots were a crucial part of the document as these allow the end user to visualise and confirm what it is that is required.

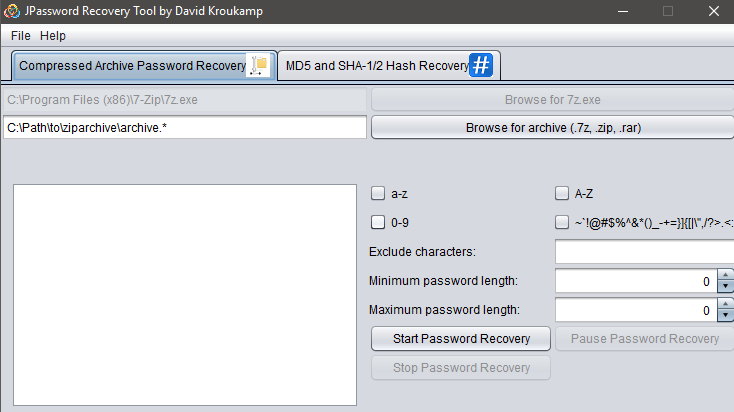


Figure 1: “jPassword”

Upon detailing the instructions and use of the software we decided to include a “sample file” of which the end user is able to “trial” the software. This is to ensure they do not lose any personal data on their files which they are using in the software for the first time.

Example software 2: WirelessKeyView

For this service we provided the software WirelessKeyView. WirelessKeyView allows the user to view the network keys stored on their device. This is beneficial to the end user as it allows them to obtain any wifi passwords they may have lost.

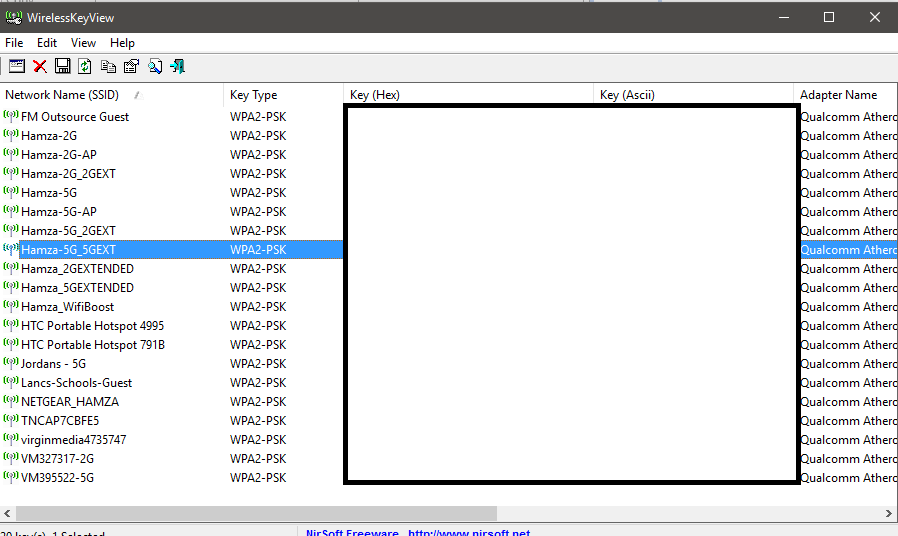
I detailed the instructions on how to run and install the software in the instructions document. I then also provided a screenshot of what the result should look like:

Figure 2: “WirelessKeyView”

The above shows the result of WirelessKeyView. The keys are displayed in the “key” field.

Example software 3: Lazesoft Windows KeyFinder

Lazesoft Windows KeyFinder is a tool which allows the end user to obtain their product key in the event it is misplaced or unobtainable. In most scenarios the product key is printed physically on the back of a device. However in some scenarios this can be an issue.

The instructions document details and outlines the installation and execution of the software. Once installed it displays the result straight away. Below is a screenshot of what is displayed to the end user:

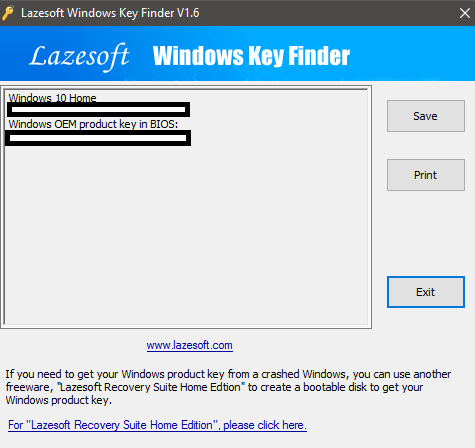


Figure 3: “Lazesoft Windows Key Finder”

As you can see above, the program has displayed the product keys for both the Windows installation and Windows product key

Example Software 4: Hardware Monitor

Hardware monitor is a software which reads the PC’s main system health sensors and provides detailed information all devices connected to the computer.

Again I included all the installation and running instructions to the end user.

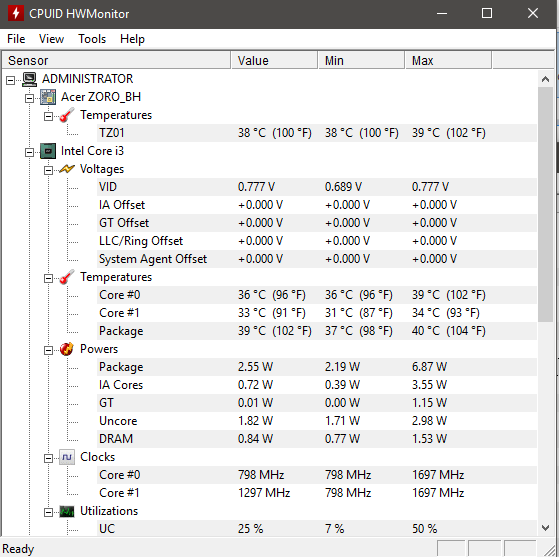
Upon opening the software it provides a detailed breakdown on an all elements of the PC. For example:

Figure 4: CPU HW Monitor

Example software 5: Process Hacker

Process hacker is a great tool which allows you to monitor, debug and suspend all running processes on your system. The application displays data in a graphical GUI with different outputs in order to allow the user to monitor and manage their processes.

Again I included all the installation and running instructions to the end user.

I then provided the end user with a sample screenshot of what the application will look like. I did this in order to ensure the end user does not get confused and everything matches on their screen.

Below is a screenshot of process hacker:

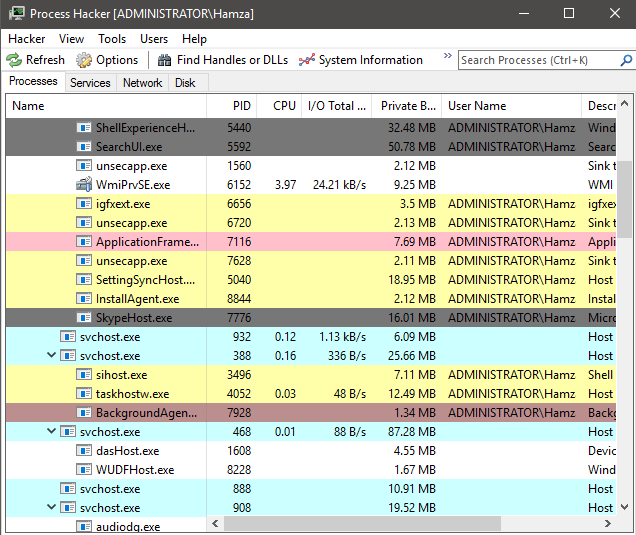


Figure 5: “Process Hacker”

As you can see, the software has listed all running processes using “colours” to show most memory consuming processes. The tabs at the top allow the user to run different commands such as find handles or DLL’s, terminate processes and much more.

**5.4 Aims**

**5.4.1 Subtitle**

As a lot of computer forensic software is very complex to use and expensive, we decided to create an alternative which is creating manually defined packages with specific software that could be sold to potential customers.

As there are many organisations out there which charge extortionate prices for data recovery and various forensic processes, our aim is to create these packages with detailed instructions , providing a cheap and efficient service for the customer also allowing them to obtain an insight on how the forensic process goes.

Main aims:

* To provide efficient software.
* To provide supporting documentation.
* Providing a service to the end user of which completes all their requirements to the highest of standards.
* Providing support to the end user where required.
* Generating profit and sales by marketing of the software (as outlined in other subprojects)

These are the main aims which we have set out to be achieved. To provide a service that completely fulfils the customers requirements. These softwares are to be sold to individual customers, or also businesses with business licences.