# **3 Sub-Project – Packages 1, 2 and 3**

# **[Andrew Slater]**

In this chapter I will discuss the following topics:

* Product aim
* Research
* Software
* Job role
* Product overview

## **3.1 Product aim**

The overall aim of the product is to create multiple sets of tools designed to give the average, less tech savvy user, a means to get the most out of their system without needing to do their own research and be readily available from the get go. Fundamentally, our product is purely plug in and play.

## **3.2 Research**

For this section of the report, I will be discussing the research I conducted to attain the software which would make up the bulk of our product. This is arguably the most important aspect of the task I was set as without a suitable investigation of the tools, then we could potentially be selling a defunct creation to our user-base. This would be harmful to the company, and its employee’s, reputation, both short and long-term.

To be sure that I attained the best possible software tools to fit their labelled needs, I had to conduct a proper and thorough research. To do this I scoured the internet for numerous articles about the section of anti-forensics they come under and managed to obtain the best possible tools based on the recommendation of established technology writers and experts.

When performing the research for package 1, I came across an article on the reputable site known as TechRepublic (I have included a link too said article below). From this article I have been able to extrapolate what are deemed the best and most trustworthy password recovery tools, they even provided images which gives you a clearer idea of how each program works. Once I had chosen the programs for this package, I then set out to downloading each program and inserting them all into a compressed .zip file name “Package1” so it could be ready to place onto a pen-drive and prepared for sale.

[*http://www.techrepublic.com/blog/five-apps/five-trustworthy-password-recovery-tools/*](http://www.techrepublic.com/blog/five-apps/five-trustworthy-password-recovery-tools/)

As with package 1, carrying out research for package 2 underwent a similar process; searching the internet for viable and reputable tech news outlets, however, I did have some slight trouble collecting information for this part of the product as there was not much in the way of easily available, easy to read information discussing open source lost data-recovery tools so I decided to use a different approach to gather my research data. I asked on a vastly populated discussion forum for a popular technology website, known as Tom’s Hardware, what they would deem to be the best open-source software for this particular area. They delivered many responses and helped in my search a great deal.

Package 3 (optimisation) did not garner as much trouble for me as package 2 did as open source optimisation tools are more plentiful than product key recovery software. The research I did here involve looking at the more well-known optimisation tools that the more tech savvy person will already know about, and search for the best open source alternatives which would be feasible for us to use within our product.

## **3.3 Software**

This section of the report is about the software tools themselves. This will be about what the tools actually accomplish plus an explanation about of some of the technicalities about what they are intended to carry out.

**3.3.1 Package 1 (Password Recovery)**

**jPassword Recovery Tool**

Jpassword is an incredibly lightweight tool designed to help the user recover the password for any password protected archive file. This tool may also require additional archiving software such as “WinRar” or “7zip”.

**OPHCrack Live- Windows Account Password Recovery**

OPHcrack is an application designed to crack Windows passwords. It does this via a method called LM hash cracking.

LM hash cracking is an encryption function intended to store away password hashes in windows. It is somewhat outdated but is still seen in use on local and domain hashes. LM hash will split the password into two segments and each individual segment can go up to seven characters, if the password is not seven characters long then the second section will just simply be a blank hash. The LM hashing method used by OPHcrack is known as “rainbow tables”. The program creates a table consisting of passwords and hash combinations. It then looks up the halves of all the hashes and once it has examined them all, brute forces its way through the password.

**Hash Suite**

Hash Suite is a program intended to assess the safety and security of password hashes. Hash Suite creates many different passwords and as they are inputted into the program, hashes them and matches the hashes with hashes which have been stored. This method seemingly works as people tend to create passwords for themselves which are simple to break. Additionally, Windows operates in a way that its hash function are extremely quick to compute, particularly if your password is attacked.

**3.3.2 Package 2 (Data Recovery)**

**Lazesoft Windows Key Finder**

This is a very basic and lightweight program. The intention of this program is to assist you should you misplace the product key for your version of Windows or Microsoft Office. It will reacquire said product key for you and copy it to your clipboard, allowing you to simply paste it in giving you full access to your copy of Windows or Microsoft Office again.

**Recuva Undelete Software**

Recuva is a software application created to restore files which have been erased, whether accidentally or maliciously. It is able to bring back files from an emptied recycle bin, or even files from external devices like music or photos which were initially saved on a digital camera.

**Test Disk - Partition Recovery**

Similar to Recuva, test disk is designed to recover lost data. However, its method is somewhat different. Test disks purpose is to reinstate previously lost partitions. It also contains many other useful features such as repairing a previously defunct boot-up disk or something more complex like rebuilding an NTFS boot sector.

**AIRCRACK**

AIRCRACK is a very useful suite of tools dedicated to evaluating your WiFi network’s security. Its array of tools concentrates on four different areas of network security.

* Monitoring: Watches all packets apprehended and observes any data that is exported in a text format for further evaluation.
* Attacks: The software will replicate an attack allowing you to see how your network was penetrated. Prevents any de-authentication (which is when a legitimate user has been removed from the network).
* Testing: This is essentially just a benchmark test for your WiFi cards and the capabilities of your drivers.
* Cracking: Again if you have misplaced or simply forgotten your WiFi key (WPA/WPA2) this program has the ability to recover them so you can regain access to your network.

**3.3.3 Package 3 (PC Optimisation)**

**Little Disk Cleaner**

Little Disk Cleaner is a simplistic and lightweight tool created to rid your system of any unwanted files, deemed “junk”. Removing junk will help optimise the performance of your computer allowing for a smoother user experience.

**BleachBit**

Bleachbit takes things a step further than Little Disk Cleaner as on top of deleting junk and unnecessary files, it does a good job clearing out other clutter on your system. It will also clean the cache, cookies, old logs and temporary files which are no longer needed and broken shortcuts. As well as clearing unneeded browser data it will keep other programs tidy, like Photoshop and OpenOffice enabling for a smoother experience all round.

**Mem Reduct**

Mem Reduct is a lightweight program which permits you to observe and reduce the usage of your computer’s memory (RAM). It does this through eliminating obsolete system cache data and modified and idle processes, because of this RAM usage is significantly decreased allowing more memory available for other tasks.

## **3.4 Job role**

My role as a sub-project team member is to conduct any operation which has been delegated to me. In this instance I have been given the task of creating three alternative, unique packages which cater to specific areas of anti-forensics. For further, in-depth details of my work please read the previous sections.

Another part of my role was to attend group discussions and meetings. During these, we initially brainstormed multiple ideas before deciding acquiring open source tools, packaging them and vending them to a previously untouched place in the market was the best course of action.

I felt I contributed well in these meetings as I would spit-ball ideas at whatever point I could and I feel I was designated a task that I could accomplish successfully.

## **3.5 Product overview**

This section will be a more simplistic overview of what I have gone over in the previous sections; reciting the overall aim of each package and how the final product should ideally function in the hands of a user of the product.

The first package is a collection of password recovery tools. The objective of a password recovery tool is to help you recuperate any lost passwords be it you have forgotten them or somebody else has tampered with your password and changed it themselves, or if somebody accessed your password protected material with malicious intent.

The second package is directed at product key recovery, which means that should a product key for, for instance, an operating system is lost by the user they can simply use the tool I have procured, follow the simple instructions created by one of my fellow team members and they should have their key again, ready to be inserted and used. This does not just apply to operating systems, there are also tools we have made available which also allow you to re-acquire the product key of various other programs and key items such as your Wi-Fi password or Windows account passwords.

The third and final package for which I obtained various tools for (there are other packages) is slightly more varied than the previous two packages. Package three is about optimising your PC to achieve the best and most efficient performance possible from your hardware specifications. In order to accomplish this I devised a plan of collecting tools which function and target separate areas of the system’s memory. For example, one program is a disk cleaner which wipes away anything the program considers “junk” leaving your hard-drive with more space available and your computer running smoother. However, a separate program I used may do multiple things like defragmenting the hard-drive or clearing your browser’s history.

**3.6 Summary**

In conclusion I have discussed the aim of our product and how it targets a previously unexplored gap in the market (one of my fellow group members will have discussed this in further detail), the research which needed to be done in order for us to have a functioning product of the highest calibre so we can establish a loyal customer-base, the end-results of the research I conducted as well as a thorough explanation of each piece of software, what my specific role in the company entailed and an overview of the product which provides a more simplistic explanation of each package.