

# Data Remanence: Storage & Processing Tool

## Project Scope & Objective :~\$

Due to the conceptual nature of the project the expectations and scope for its development were loosely defined and relatively broad, however it relates back to Dr Roberts' thesis and work from Dr Laurenson's thesis that Dr Roberts recommended we include. The overall goal was the development of an automated system with the ability to image, analyze and store information from used digital devices.

## Project Team :~\$

**Blake Larson** = Security, Dev/Design, Linux, Project Manager  
**Dalvir Singh** = Programming, Testing  
**Vrajesh Choksi** = DBA, Project Coordinator  
**Yousuf Hassen** = App Dev, Testing

**Client** = Dr Dax Roberts && **Advisor** = Dr Scott Morton

## Historical background :~\$

This project is a proof of concept developed to compliment a thesis by our client, Dr Dax Roberts. Dr Roberts completed a PhD thesis in 2013 "Data Remanence in New Zealand" that identifies the amount of data remanence on used storage devices after disposal. As discussed by Dr Roberts, this oversight can expose the previous owners to a range of risks (blackmail, fraud) through the access of the personal data that remains on the device.

As a part of that thesis, used hard drives were analyzed to inspect the content and determine the baseline of data remanence in New Zealand, those results were then compared with international statistics to see how New Zealand compares and what further action (if any) needs to be taken.

The genesis for this project was the challenge of storing large volumes of data, easily adding new forensic data to the system and ensuring the tools used were up to date.

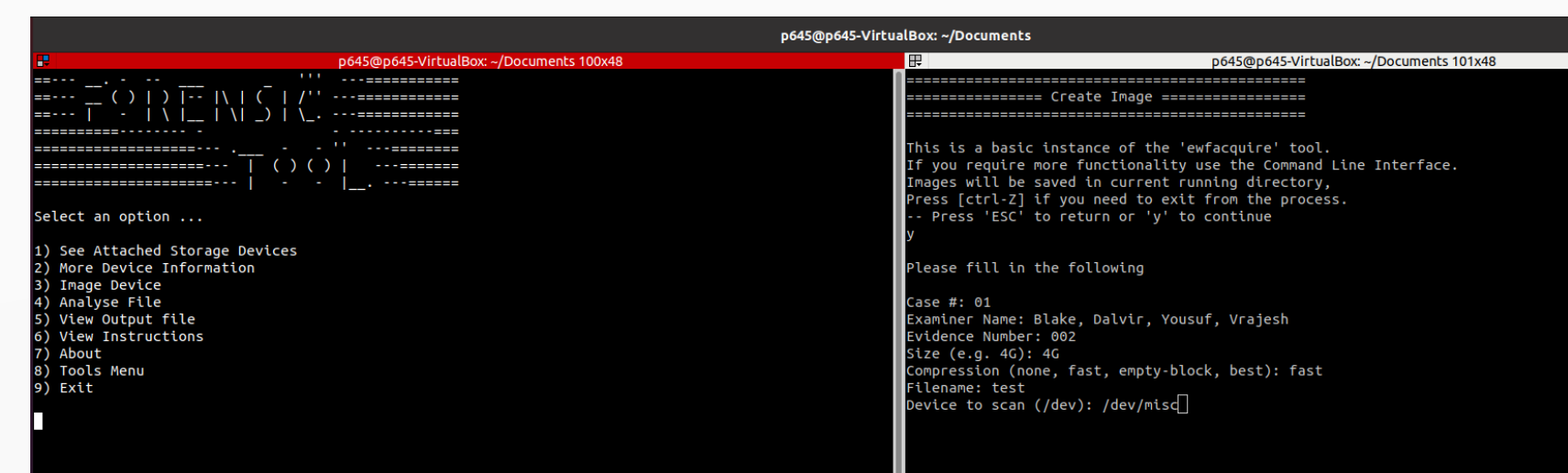
## Development :~\$

Linux was chosen as the operating environment for development because of its availability of open source forensic tools and scripting benefits (especially from within the CLI). Debian was initially chosen, and although in the first instance this was Kali, it was found that although the range of preloaded tools were impressive for the purpose of starting it was unnecessary – due to this and other reasons discussed the operating environment was ultimately changed to a customized version of Ubuntu 20.04.1 LTS. The process of development started with a shell script containing simple functions and Linux commands, this was designed to loop back to a command

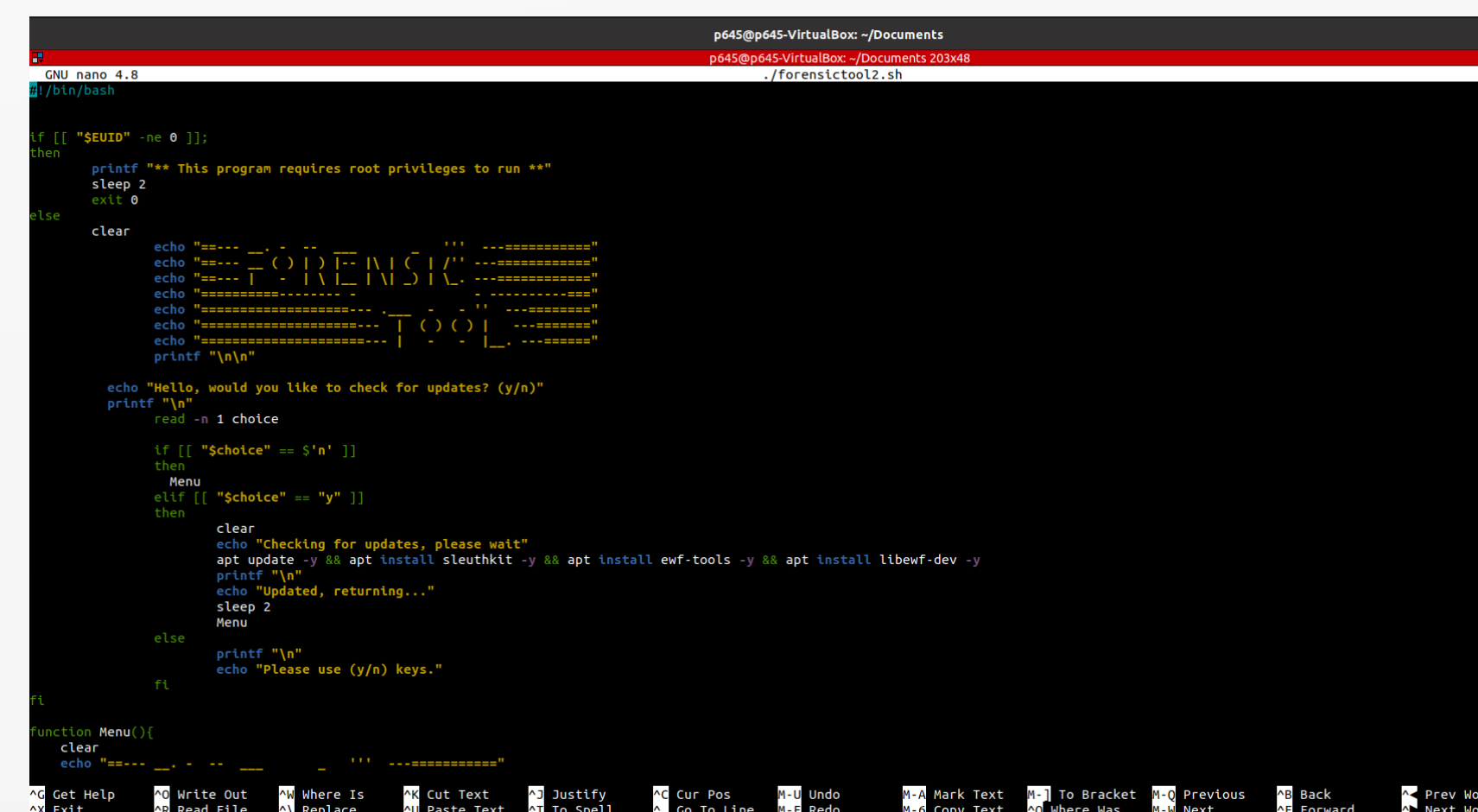
menu and automate the process of obtaining and analyzing a forensic image, this was used as a dynamically updated and working script that was developed and tested simultaneously.

The group met weekly for SCRUM and catch up sessions, although most of the work was completed remotely via a .ssh or RDP session on a blade server on the individuals' local machine. The benefit of creating a bash script that was designed to be portable make it interchangeable between machines without issue. The front-end and Database were developed to a limited level of functionality but to a stage where it can be reasonably determined that both will be possible. The Web-app was developed using ASP.NET Core to take advantage of its Cross-Platform capabilities and PHP was trialed using PHPmyadmin to connect to MySQL.

The focus of the project gradually switched from a holistic approach to a singular focus on application development, this was done so in communication with the client as we discovered what the needs and priorities for this system were throughout the development process.



CLI menu in terminal emulator



Script in GNU nano text editor

## Project Scope & Objective :~\$

The major difficulties faced were around the process of integration of the three aspects that were identified in the development of the project scope, we found that working on an automated script and dynamically changing the other aspects was impractical, it was therefore decided to focus on developing a working system using the CLI exclusively throughout the process with the intention of passing these recommendations on to future iterations.

As a team, our competencies and areas of expertise did not align ideally with the project, being a proof of concept with the broad scope however there was a certain freedom to work within this constraint. Having recognized this, an observation would be that there was a significant amount of time that could have been utilized more effectively by spending more time on creating well defined deliverables. The Kali blade crashed and remained in a tty state with limited use, however we also discovered that a blade server was unable to recognize the physical media over the network (without major tinkering) which led to the use of a physical machine running Ubuntu. This however was not a major problem as the program allows the user to specify a file path to preexisting images or these images can simply be uploaded into the directory.

## Recommendations :~\$

The major changes and realizations that presented were as relating to the integration of the three aspects that were identified in the development of the project scope. It was discovered that working on an automated script and dynamically changing the other aspects was impractical, it was therefore decided to focus on developing a working system using the CLI exclusively throughout the process with the intention of passing these recommendations on to future iterations.

This process itself created a thorough and tested list of recommendations that will be passed on to the client for future consideration. For future development, the addition of members with more specialized skillsets in the areas of database administration and OS/Cross platform integration would benefit the project significantly to extend its UI/UX depending on its requirement. As this has been created in Debian, the commands are all Debian based and therefore another recommendation would be to modify the script for use in other Linux distributions.

## References:

- <https://github.com/thomaslaurenson/IRDNumberScanner>
- <https://manpages.debian.org/unstable/sleuthkit/fiwalk.1.en.html>
- Roberts, D. (2013). Data Remanence In New Zealand
- Laurenson, T. (2017). Automated Digital Forensic Triage: Rapid Detection of Anti-Forensic Tools

