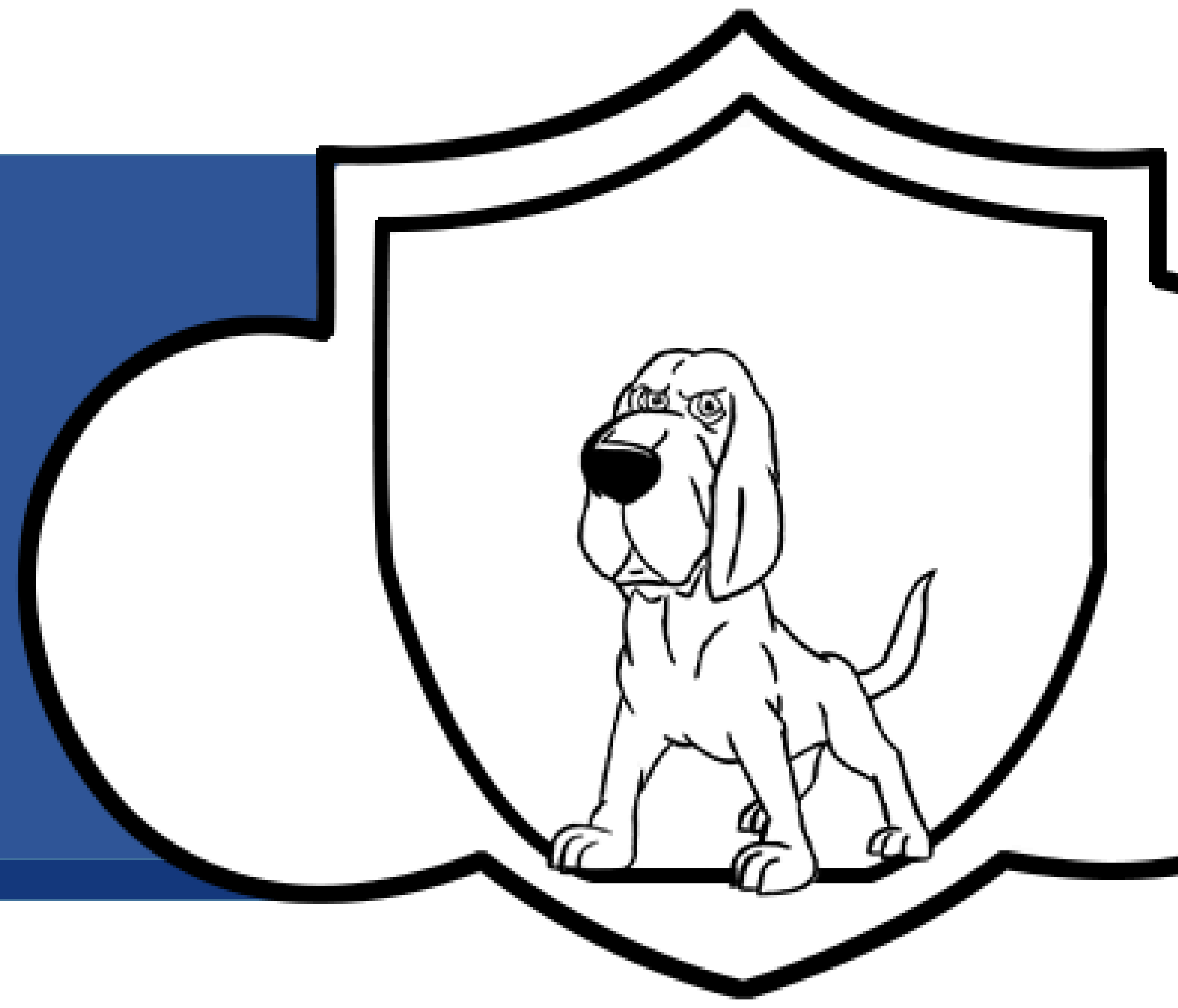
University of Limerick
Ollscoil Luimnigh

E&CE
Department of Electronic and Computer Engineering

CLOUD-TOPSY

JW01: Data Forensics Tool For Investigating Subjects' Suspicious Cloud Activities

Ryan O'Connor - 17209382
Bachelor of Science in
Mobile Communications and Security
(Cyber Security and IT Forensics)



Introduction

A necessary first step in data forensics is **establishing** that **access to the cloud** has been made. ***Cloud-topsy*** aims to create a **platform** for **cyber security individuals** to work alongside their **team** to determine whether suspects have **accessed cloud storage systems**. It aims to investigate supplied **disk images** looking for indications that specific cloud storage platforms have been used.

Cloud-topsy is written in the **Java** programming language and integrates **the Sleuth Kit (TSK)** through the use of the **Java Native Interface (JNI)**. TSK stores information related to the suspect's personal machine inside a **SQLite** database. Collected data related to cases are stored inside a **MYSQL** database.

Cloud-topsy **automates** the process of **investigating** the **remnants** left behind on the **suspect's physical machine** saving valuable **time** for an investigator in the investigation of a case.

Aims

Specific

To develop a computer forensics tool to aid in the process of cloud investigations.

Measurable

Success measured in the functions achieved throughout the development.

Achievable

To understand the workings of TSK and it's implementation in the project.

Relevant

Develop adequate number of functions to provide poof of concept in given timeframe.

Time-Bound

Working proof of concept produced by submission date.

Method

The method for the development of this project can be broken down into a several key categories; Research, Software, Testing and Results.

- **Research**: Before commencing any development of the software, it was necessary to further my **knowledge** in the field of data forensics. It was necessary to find suitable **programming languages**, **libraries** and **software** capable of carrying out forensic investigations. It was also necessary to understand how forensic investigations are carried out.
- **Software: *Cloud-topsy*** consists of a java interface which integrates the Sleuth Kit though the use of a Java Native Interface. To access the Sleuth Kit, data model JAR files had to be compiled along with the **building of an associated dynamic library** from the **'C' code**. This was completed through the use of **Apache Ant**. A number of software design models and patterns were used such as; **Data Factory**, **Data Broker**, **Singleton** and **Model-View-Controler**.

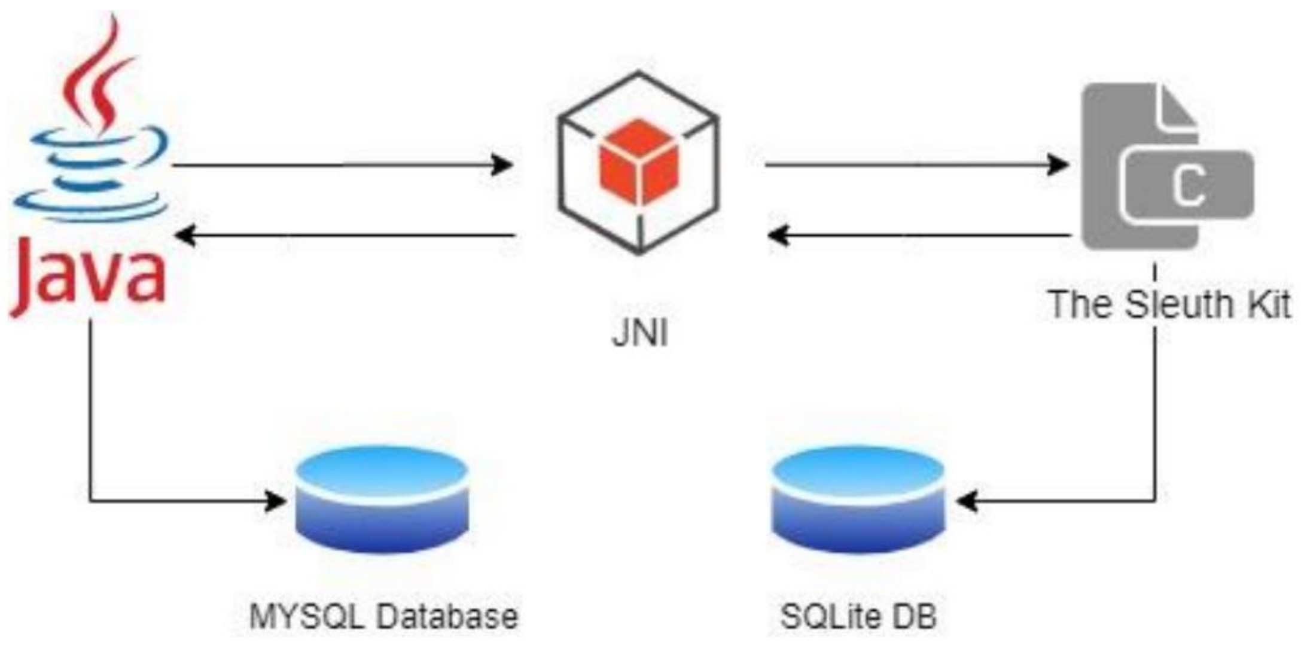
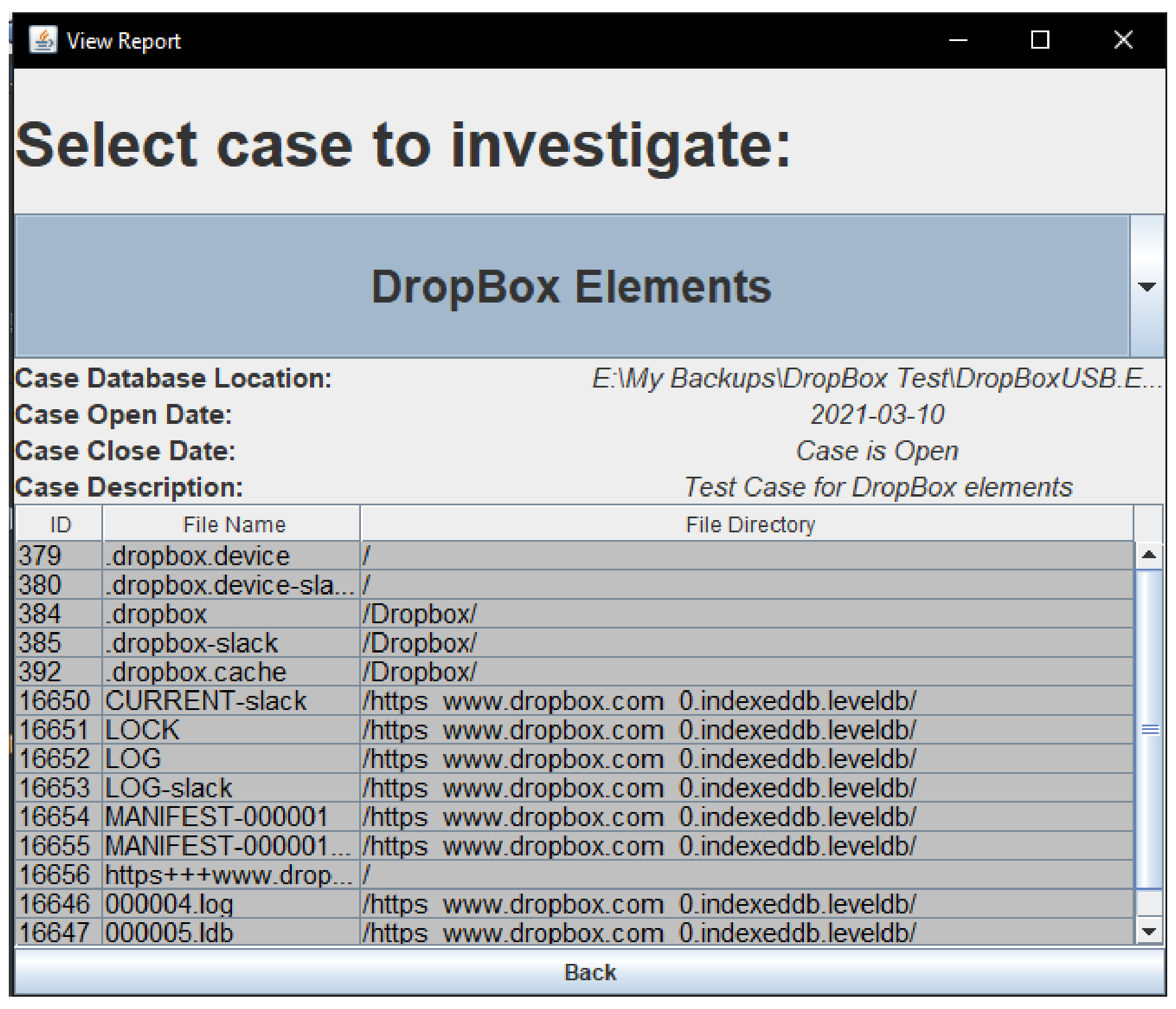


Figure 1: Software Outline

- **Testing:** In order to test the functionality of the software, a number of **sample disk images** needed to be created. Three USB devices were set up to contain remnants of cloud storage platforms and images were taken using **FTK Imager**. A control USB was also used. **JUnit testing** was carried out on a number of the **core functions**.

Results

Cloud-topsy produces two forms of outputs for the investigation of a case; An **on-screen view** of elements found within the disk image, and a **CSV file** containing generic case information and the case findings.


View Report

Select case to investigate:

DropBox Elements

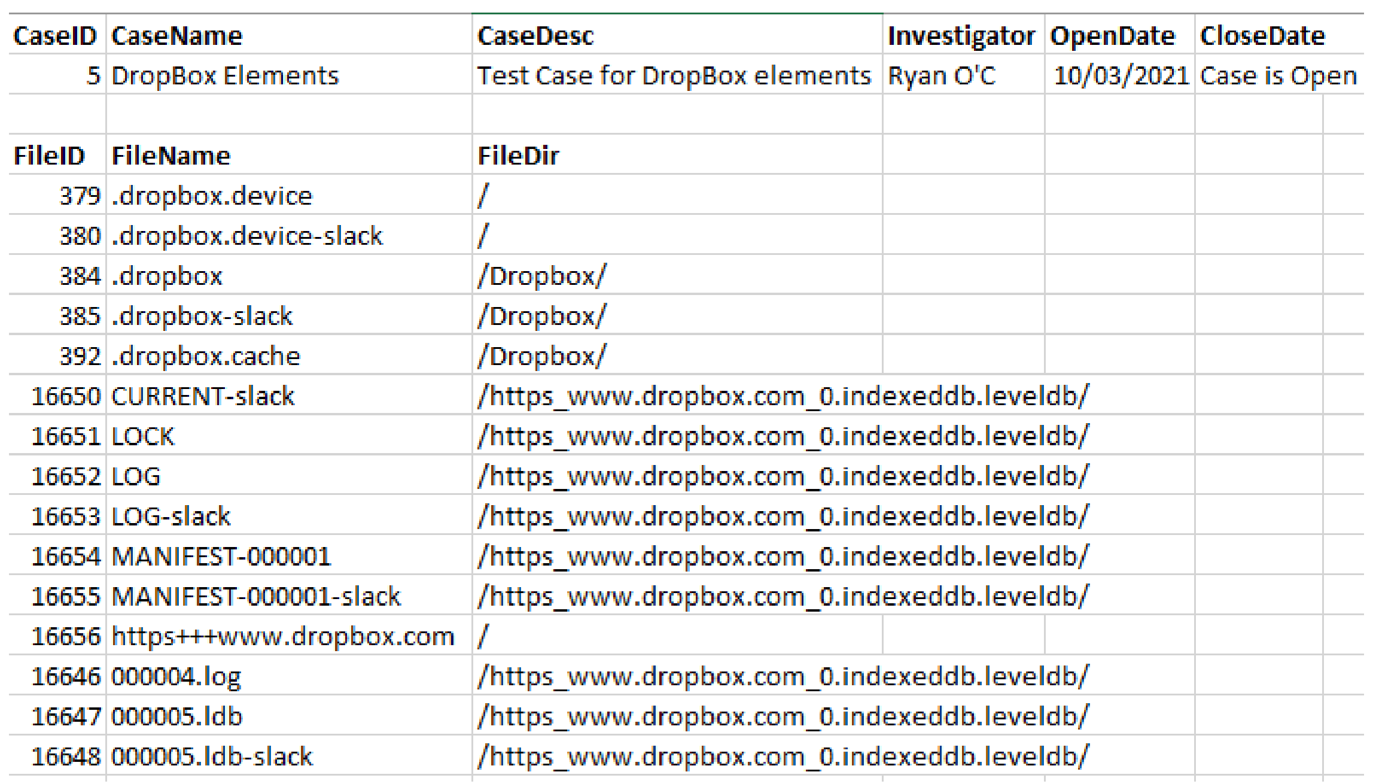
Case Database Location: E:\My Backups\DropBox Test\DropBoxUSB.E...
Case Open Date: 2021-03-10
Case Close Date: Case is Open
Case Description: Test Case for DropBox elements

ID	File Name	File Directory
379	.dropbox.device	/
380	.dropbox.device-sla...	/
384	.dropbox	/Dropbox/
385	.dropbox-slack	/Dropbox/
392	.dropbox.cache	/Dropbox/
16650	CURRENT-slack	/https www.dropbox.com 0.indexeddb.leveldb/
16651	LOCK	/https www.dropbox.com 0.indexeddb.leveldb/
16652	LOG	/https www.dropbox.com 0.indexeddb.leveldb/
16653	LOG-slack	/https www.dropbox.com 0.indexeddb.leveldb/
16654	MANIFEST-000001	/https www.dropbox.com 0.indexeddb.leveldb/
16655	MANIFEST-000001...	/https www.dropbox.com 0.indexeddb.leveldb/
16656	https+++www.drop...	/
16646	000004.log	/https www.dropbox.com 0.indexeddb.leveldb/
16647	000005.ldb	/https www.dropbox.com 0.indexeddb.leveldb/

Figure 2: On-Screen Output

- **On-Screen Output**

The on-screen output displays data that was found to contain any **remnants** of the **cloud storage system**, in this case 'Dropbox'. It is in table format, displaying each element's file number, file name and the path to the file's directory. Location of the database, case open & close date and the case description are displayed above the remnants table.



CaseID	CaseName	CaseDesc	Investigator	OpenDate	CloseDate
5	DropBox Elements	Test Case for DropBox elements	Ryan O'C	10/03/2021	Case is Open

FileID	FileName	FileDir
379	.dropbox.device	/
380	.dropbox.device-slack	/
384	.dropbox	/Dropbox/
385	.dropbox-slack	/Dropbox/
392	.dropbox.cache	/Dropbox/
16650	CURRENT-slack	/https_www.dropbox.com_0.indexeddb.leveldb/
16651	LOCK	/https_www.dropbox.com_0.indexeddb.leveldb/
16652	LOG	/https_www.dropbox.com_0.indexeddb.leveldb/
16653	LOG-slack	/https_www.dropbox.com_0.indexeddb.leveldb/
16654	MANIFEST-000001	/https_www.dropbox.com_0.indexeddb.leveldb/
16655	MANIFEST-000001-slack	/https_www.dropbox.com_0.indexeddb.leveldb/
16656	https+++www.dropbox.com	/
16646	000004.log	/https_www.dropbox.com_0.indexeddb.leveldb/
16647	000005.ldb	/https_www.dropbox.com_0.indexeddb.leveldb/
16648	000005.ldb-slack	/https_www.dropbox.com_0.indexeddb.leveldb/

Figure 3: CSV Output

- **CSV Output**

The outputted CSV file contains the elements chosen from the onscreen results. These are files chosen by the **investigator** that are deemed to be **suspicious** on the **suspect's machine**. This file contains information related to the case such as; case identification, case name, case description, investigator name and dates related to the case. It also contains file information similar to that found in the **on-screen view**.

Conclusion & Reflection

In conclusion, this integration of **The Sleuth Kit** resulted in an easy-to-use software, to identify remnants of cloud storage solutions left behind on suspects' machines.

The software contains **good practice models** and **patterns**. It also contains **cryptographic functions** inside the database, to ensure that user data is encrypted.

I would like to further develop this software while undertaking my Masters degree in cyber security. I see great potential in the future of ***Cloud-topsy***.

Acknowledgements

Brian Carrier
The Sleuth Kit (TSK)

Jacqueline Walker
University of Limerick