
# JW01: *Data Forensics Tool for Investigating Subjects' Suspicious Cloud Activities*

By:

***Ryan O'Connor – 17209382***

Supervised By:

***Jacqueline Walker***

Department of Electronics & Computer Engineering

University of Limerick

**Nov20 2020**

# TABLE OF CONTENTS

# INTRODUCTION AND PROJECT OUTLINE

## PROJECT DESCRIPTION

In the field of data forensics, investigating whether subjects have tried to conceal suspicious data in the cloud can be very difficult for reason of access and lack of information about how the data is stored in the cloud. A necessary first step is establishing that access to the cloud has been made and this is usually done by examining personal devices used to transfer data to and from the cloud. Even this is not as simple as it sounds as the continuous evolution of personal device operating systems combined with knowledge of how to delete such data by culpable users may impede the investigator. Keeping information about this topic up to date is a constant battle for forensic investigators.

In this project, the student will investigate a limited number of example cloud storage systems e.g. Amazon S3, Dropbox and also a limited number of personal device operating systems and fully establish the tell-tale signs of usage that may be left behind. Development of an automated investigative tool may be part of this project. In this project we will naturally have to leave aside legal issues although it would be useful if the student also carried out a brief investigation into the necessary requirements in this jurisdiction.

## PROJECT RATIONALE

As mentioned in the project description, a necessary first step in data forensics is establishing that access to the cloud has been made. This project 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. The data that is found on the image will be available for export where an investigator can further develop their investigation. The investigator can create reports of their findings logging relevant information like; Evidence Found, Time, Date & Location of Evidence, General data from the Image and lastly information about the investigator who took the case. The reports are made available for export to be used in a potential court case situation.

The application aims to seamlessly connect individuals with their teams and superiors. The superiors have access to all information regarding cases and their reports. They can see cases that are in progress and access the reporting list to determine how far the investigator is into the investigation. They can also access all reports that have been created by completed

cases. The superior's main function is to create new investigators as required and monitor the progress of the team.

The application will be Java based integrating the Sleuth Kit using the Java Native Interface (JNI) storing user data and extracted information inside a MYSQL database. The Java aspect to the project will develop user functionality related to accounts and the reporting of the data collected. The disk image that is uploaded will be investigated using the Sleuth Kit and extracted information stored. The application will automate the process of determining whether a suspect has accessed a cloud storage system saving valuable time for an investigator in the investigation of a case. It will investigate remnants left behind on Windows based images. A report on the procedure of investigation of non-windows images such as; Mac, iOS, and Android smartphones will be carried out.

# THEORY

What is cloud computing? Amazon defines cloud computing as the on-demand delivery of IT resources over the internet with pay-as-you-go pricing. They state that instead of buying, owning, and maintaining physical data centres and servers, one can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Service(AWS) [1].

In Cloud Computing there are three main subcategories which include: Public, Private and Hybrid. Public is used to deliver services across the internet, Private is aimed at internal use of an organization and hybrid is a combination of both Public and Private. Inside this there are three types of services offered to users. The first is IaaS (Infrastructure as a Service) it contains the basic building blocks for cloud IT. Typically it provides access to computers, networking features and data storage space. The second is PaaS (Platform as a Service) which removes the need to manage underlying infrastructure and allows focus on the deployment and management of applications. Finally, SaaS (Software as a Service) which provides a complete product that is managed by the service provider. It allows the user to not have to worry about how the service is maintained or how the infrastructure is managed [1]. SaaS is the type of cloud computing in which cloud storage systems such as Google Drive, Dropbox and Evernote fall under.

Gartner, one of the world's leading research and advisory companies, predicts that at the end of 2020, public cloud revenue will grow by up to 6.3% which means it will grow from $242.7 billion (2019) to $257.9 billion. They state that SaaS remains the largest market segment and is forecast to grow to $104.7 billion in 2020. COVID-19 [2] had a major impact on not only the growth of SaaS but the growth of the entire world of cloud computing. A report from the Irish Times [3] has found that at least 40 percent of paid hours worked by employees in Ireland were performed from home at the height of the pandemic. COVID-19 could therefore be regarded as a catalyst for the inevitable change to a cloud-based business model for companies around the world. For this reason, it is important to understand how to conduct forensic based examinations into cloud computing.

With the increased usage of cloud computing, comes a surge in cyber-crime. Cloud computing crime can stem from several approaches; Stealing personal data stored and outsourced in the cloud and attacks that disrupt a company's day to day workflow. Cloud storage services can be used to store and hide incriminating and illegal material or material that

goes against copyright laws. Service providers are attempting to prevent their services from being exploited by these criminals. Companies such as Dropbox have implemented a software that detects data related to child abuse. It searches through the files stored on the service to identify breaches of policies that the perpetrator has agreed to follow. Similarly, Microsoft developed a software called PhotoDNA that is designed to identify similar data [4].

In order to conduct a successful forensic investigation into cyber-crimes involving digital evidence, the investigator must be able to collect the evidence of the incident or crime that involved both cloud servers and the client device that was used to access the cloud service. It is important for the investigator to be able to locate and report on data remnants that can be located on the suspects' personal machine. This project will focus on the retrieval of these fragments.

# LITERATURE SURVEY

Cloud computing and storage solutions provide companies and private users with the capability to store their data in third part data centres [5]. This data can be targeted by criminals. These attacks can range from stealing personal information from the cloud to disrupting a company's business operations [4].

On the 11th March 2020, the World Health Organization characterized COVID-19 as a pandemic. This upended the worlds business ecosystem as we know it. To maintain business productivity, the enterprise working model turned into one of a working from home model using BYOD (Bring your own device). As a result of the change in working environment cyber-attacks, which previously targeted individuals were now a risk for businesses [6].

Cloud service providers have attempted to prevent exploitation of their services examples include Dropbox child abuse detection software and Microsoft's PhotoDNA. Other security solutions have been proposed, ranging from privacy-preserving to intrusion detection. Despite the existence of these solutions, cybercrimes are still committed. To prosecute cyber criminals, it is necessary to gather digital evidence to prove that the crime has been committed. This process is known as digital forensics [4]. Even though the log of a cloud server can tell the history of a user's action, the hosting companies are not always willing to release information to the investigators to protect clients' privacy. However, traces of user actions are left in the user's device. Webb-Hobson stated that even though user made files such as documents and photos are not stored on local machines, traces or fragments of them which are related to their actions can be found on the machine.[7]

Buyu and Abade [8] analysed artifacts left behind by Dropbox on windows 10 machines. By identifying these remnants, it is possible to get a better understanding of the remaining artifacts to help with forensic investigation. The information sources include client software installation files and browser related artifacts.

Marturana in [9] deduced that on windows 7, browser artefacts, sync logs, timeline of recently opened, modified, deleted files by Dropbox could be obtained.

McClain [10] discovered that for Dropbox, remnants could be found on windows XP that included installation directory, log files, database files and uninstallation data.

The use of a cloud storage service will leave traces in all local devices such as PCs and Smartphones. Therefore, all devices that can access an individual's cloud storage usage must

be examined when undertaking digital forensics on that storage. The Centre for Information Security Technologies (CIST) in Korea proposed a successful process model for investigating artifacts of all accessible devices including Windows, Mac, iPhone, and Android. The process involves identification, collection, analysis and reporting of artifacts related to these machines. Through the use of their model they successfully identified the location of artifacts related to cloud storage services left behind on these machines [11].

The first element for the CIST team was to examine logfiles of web browsers and artifacts of client application that are installed on the machine. The team took two popular web browsers: Internet Explorer and Firefox. Web browser log files are stored in profile directories and the files consist of cache, history, cookies and downloaded files. The history files contain URLs that a user has visited, titles of Web pages, the times of visits, and their number of visits. The cookie files store information about hosts, paths, cookie modification times, cookie expiration times, names, and values; Valuable information in terms of cyber forensics. The team also collected artifacts of client applications installed on the device such as database files and application log files in the form of txt, log and htm files. The database files contained information about credentials, creation time, modification time and files that have been accessed. The log files store general information about authentication information, history of users' behaviours and general user data. [11]

The second element for the CIST team was to analyse the collected data and check if traces of cloud storage services existed in the collected data. If user credentials and any other information were found, a search and seizure warrant should be issued. The user's location in the cloud storage service is a private space. This mean that if an investigator were to login and obtain data without a warrant the evidence would not be admissible in the court of law. The investigator is only allowed to investigate artifacts that remain inside the client's device. [11]

Forensics examiners often use open source software for their investigations according to Altheide and Carvey in [12]. Using freely available software to learn digital forensics has advantages. The software tools allow the investigator to execute, examine options and output, and examine the code that produced the output. This gives the investigator a better understanding of the tool's operations. Aspects of an investigation may be too small to justify spending a significant amount of money on a software to complete it. For these scenarios, an investigator can install and run this software on any hardware that is available to them free of charge [12].

Altheide and Carvey state that the biggest benefit to open source software is that the code is provided. The ability to review and modify the source code that gets compiled into a working program is invaluable. The Sleuth Kit is one such example, describing different ways to review bug fixes in the software. If there is a change to the software, an investigator can look at the freely accessible bug trackers maintained at the Sleuth Kit project site [13]. Proprietary forensic products which develop in a "black box" make the identification software modifications less obvious. Lack of access to the source code acts as an additional layer of abstraction between the investigator and the truth. In this case the layer of abstraction acts as a source of error [12].

Buyu and Abade in their investigation used several software's, some open source, and some closed including Access Data FTK Imager (FTK), and Autopsy. FTK was used for imaging and analysing the virtual machines that they created. They then used Autopsy for the forensic analysis of VM images. Using live forensic installs, artifacts were identified. This was an arduous process to determine what artifacts were created at the installation phase. Had they known what files to look for to begin with, they could have skipped the live forensic investigation and invested more time into the decryption of the artifacts that were eventually collected [8].

The determination and detection of artifacts using live forensic investigation, is a lengthy process that can impair the investigator. If the latter had access to software that could locate the artifacts and allow access to the relevant data, it would accelerate the advancement of the criminal case. Had the investigator known that there were no artifacts to be restored on the image, they could have saved valuable time. They would not have had to carry out a live forensic investigation process. Using research in [8] and [11], a software could have been developed that accelerates the location of artifacts for the investigator.

# OUTLINE DESIGN

## SOFTWARE LIFECYCLE MODEL

Software development lifecycle (SDLC) is a framework that defines the steps involved in the development of software at each phase. It is the process used by the software industry to design, develop and test high quality software. The aim is to produce a software that is high in quality, meets the needs of the customer and is completed within the specified timeframe and cost estimates. It was one of the first aspects that came to mind when developing a concept for my project brief. Several approaches were investigated, two of which are discussed below.

### *WATERFALL MODEL*

The first of the software lifecycle models which was researched for this project was the Waterfall model. It breaks down the project activities into linear sequential phases. Each phase is dependent on the completion of the previous phase and corresponds to a specialization of tasks. It uses a clear structure when compared with other methodologies. Each step must be completed in full before moving onto the next. If any problems are encountered, they are addressed right away, stopping the project progression in its tracks, leaving the developer with a complete and polished product as a result. This model permitted me to start right away without any steep learning curve to slow down my process. The model determines the end goals early and transfers information well as it is a highly methodical approach.

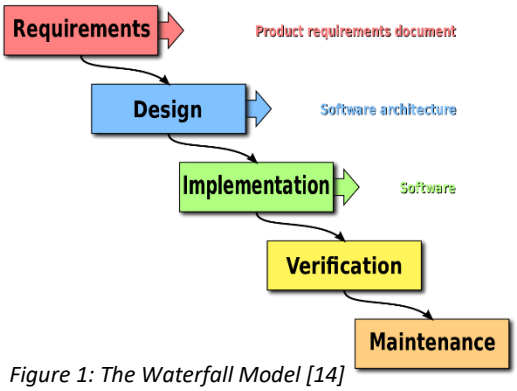

*Figure 1: The Waterfall Model [14]*

When investigating further into the waterfall model, it was found that any project changes that were required, would be difficult to implement. It left no room for unexpected changes or revisions. It was also found that its delayed testing until after completion of the project. This would not be a good solution due to the time constraints for this project. For these reasons it was decided to look further into other approaches that could possibly use.

### *AGILE APPROACH*

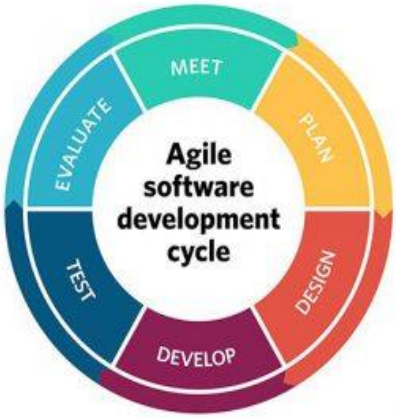


*Figure 2: The Agile Approach [15]*

The next software lifecycle that was decided on was the Agile Approach. It was found that the Agile method promotes a disciplined project management approach that encourages frequent inspection and adaptation. The approach corresponds with the Agile Manifesto which has several principles including Delivering working software frequently, getting tasks done in assigned amounts of time and allowing changes in the project at any stage in the development. It was found that the short timeframe for project development made this an ideal approach. This model would allow the testing of each of the software elements as they are being delivered. It would permit late project changes such as extra implementations at any developmental stage. This would be advantageous since many of the concepts are new.

## USE CASE DIAGRAM

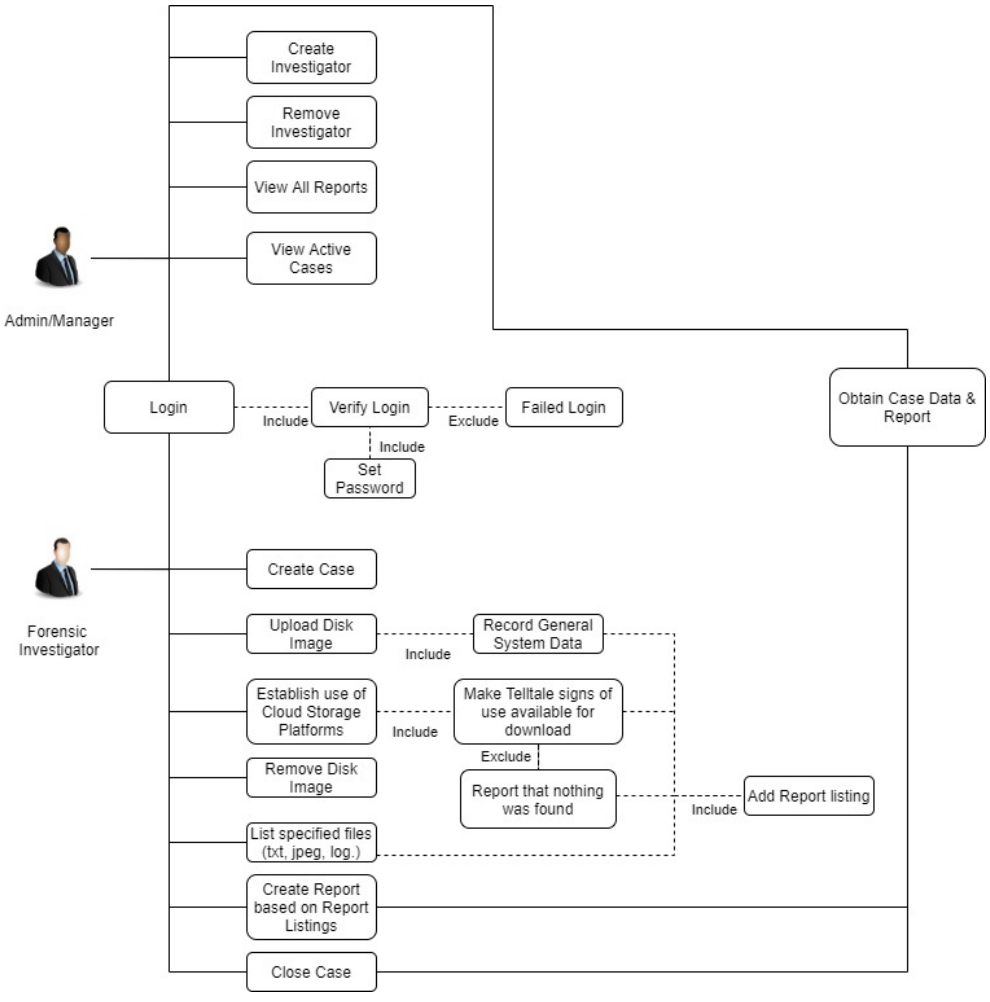


*Figure 3: Use Case Diagram*

# USE CASE DESCRIPTION

## LOGIN

| **Use Case 1** | ***Login*** | |
|---|---|---|
| **Goal in Context** | Actors can login to the system to use actions that are related to their status. | |
| **Precondition** | Account must be made and knowledge of credentials. | |
| **Success End Conditions** | Actor successfully able to login and access features. | |
| **Failed End Condition** | Actor login is unsuccessful. | |
| **Trigger** | The application is launched. | |
| **Actors** | All Actors. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor launches the application. |
| | 2 | Window asking for login credentials is presented. |
| | 3 | Login information is passed in. |
| | 4 | System checks first if the account exists and then if the password is correct. |
| **Extensions** | **Step** | **Branching Action** |
| | 4 | If the credentials are incorrect, the system will display a message indication it. |

## CREATE INVESTIGATOR

| **Use Case 2** | ***Create Investigator*** | |
|---|---|---|
| **Goal in Context** | Actor creates an Investigator user who can perform investigations on images. | |
| **Precondition** | Knowing basic information about the person who is going to be set up. | |
| **Success End Conditions** | Actor successfully creates an account. | |
| **Failed End Condition** | Actor is unable to create an account. | |
| **Trigger** | Actor presses button named ‘Create New Investigator’. | |
| **Actors** | Admin/ Manager. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor clicks create button. |
| | 2 | Actor collects and enters required personal information about the new investigator. |
| | 3 | System checks that the new user’s email is unique. |
| | 4 | System saves the data and creates an account. |
| **Extensions** | **Step** | **Branching Action** |

| | | |
|---|---|---|
| | 3 | If the email already exists in the system, then the system will show "Please use unique email" and will not allow the new user to be created. |
| | 4 | The account is saved. Upon initial login the user will be asked to set a password. |

REMOVE INVESTIGATOR

| **Use Case 3** | ***Remove Investigator*** | |
|---|---|---|
| **Goal in Context** | Actor removes an Investigator user from the database. | |
| **Precondition** | Knowing basic information about the person who is going to be removed. | |
| **Success End Conditions** | Actor successfully removes an account. | |
| **Failed End Condition** | Actor is unable to remove an account. | |
| **Trigger** | Actor presses button named 'Remove an Investigator'. | |
| **Actors** | Admin/ Manager. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor clicks remove button. |
| | 2 | Actor selects the investigator user which is going to be removed. |
| | 3 | System checks that the user exists in the database. |
| | 4 | System removes all information related to the user from the database. |
| **Extensions** | **Step** | **Branching Action** |
| | 4 | The system will not remove any case information related to the user. It will also store the name of the user to use for case referencing. |

CREATE CASE

| **Use Case 4** | ***Create Case*** | |
|---|---|---|
| **Goal in Context** | Actor creates a case and assigns information to identify what the case is about. | |
| **Precondition** | Must have some basic information about case. E.G. Suspect name etc. | |
| **Success End Conditions** | Actor successfully creates case. | |
| **Failed End Condition** | Actor does not create the case. | |
| **Trigger** | Create new case button is selected by actor. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor presses button to create a new case. |
| | 2 | Actor enters information related to the case into the system. |
| | 3 | System verifies that the case title has not been used before. |

| | | |
|---|---|---|
| | 4 | The system produces an identification number for the case. |
| **Extensions** | **Step** | **Branching Action** |
| | 3 | The case identification number and the case title will be used to identify each of the cases. |

UPLOAD DISK IMAGE

| **Use Case 5** | ***Upload Disk Image*** | |
|---|---|---|
| **Goal in Context** | Actor can upload the image they want to examine. | |
| **Precondition** | Must have image in correct format. | |
| **Success End Conditions** | Image is uploaded successfully. | |
| **Failed End Condition** | Image is not uploaded. | |
| **Trigger** | Actor selects button to upload image. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor presses button to upload an image of a disk. |
| | 2 | System preforms basic analysis on the disk image. |
| | 3 | System functions are enabled to work on the image passed in. |
| **Extensions** | **Step** | **Branching Action** |
| | 2 | The basic information about the disk is read and displayed for the investigator to see. This will let the Investigator know that the image is ready to be analysed. |

REMOVE DISK IMAGE

| **Use Case 6** | ***Remove Disk Image*** | |
|---|---|---|
| **Goal in Context** | Actor can remove an image if they have another image they want to work on inside the case. | |
| **Precondition** | Must have image in correct format. | |
| **Success End Conditions** | Image is removed successfully. | |
| **Failed End Condition** | Image is not removed. | |
| **Trigger** | Actor selects button to remove image. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor presses button to remove image of a disk. |
| | 2 | System removes the relation to the case. |
| **Extensions** | **Step** | **Branching Action** |

| | | |
|---|---|---|
| | 2 | Any reports that have been established with the image that is being removed will still reference the name of the image that they are based on. |

ESTABLISH TELLTALE SIGNS OF CLOUD STORAGE USE

| **Use Case 7** | ***Establish Tell-tale Signs of Cloud Storage Usage*** | |
|---|---|---|
| **Goal in Context** | Actor determines what cloud storage systems have been used on the image. | |
| **Precondition** | Image of a disk must have been uploaded and case been created. | |
| **Success End Conditions** | Actor successfully identifies what cloud storage systems. | |
| **Failed End Condition** | Actor not able to identify cloud storage systems. | |
| **Trigger** | Establish Cloud Storage button pressed by Actor. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor presses button to establish the cloud storage usage signs. |
| | 2 | System performs checks looking for use of different cloud storage systems. |
| | 3 | System returns a list of the cloud storage systems found on the image. |
| **Extensions** | **Step** | **Branching Action** |
| | 3 | A predefined list of storage systems will be checked. |
| | 3 | User can obtain the relevant data found. |

LIST SPECIFIED FILES

| **Use Case 8** | ***List Specified Files*** | |
|---|---|---|
| **Goal in Context** | Actor determines what files they would like to look from in the image. E.G. JPEG, log & txt. | |
| **Precondition** | Image of a disk must have been uploaded and case been created. | |
| **Success End Conditions** | Actor successfully identifies a list of files that have been found inside the image. | |
| **Failed End Condition** | Actor not able to identify cloud storage systems. | |
| **Trigger** | Establish Cloud Storage button pressed by Actor. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor presses button to establish list of specified files. |
| | 2 | System performs checks looking for the files specified within the image. |
| | 3 | System returns a list of the files found on the image. |
| **Extensions** | **Step** | **Branching Action** |
| | 3 | User can obtain the relevant data found. |

ADD REPORT LISTING

| **Use Case 9** | ***Add Report Listing*** | |
|---|---|---|
| **Goal in Context** | Actor adds a finding to the report list. | |
| **Precondition** | Case has been created, image uploaded, and an investigation function started. | |
| **Success End Conditions** | A report is successfully added to the list. | |
| **Failed End Condition** | A report is not added to the list. | |
| **Trigger** | Add report listing button pressed by Actor. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor completes an investigative step and button becomes available. |
| | 2 | Actor presses button to add listing. |
| | 3 | The listing is added to a list associated with the case. |

CREATE REPORT

| **Use Case 10** | ***Create Report based on Report Listing*** | |
|---|---|---|
| **Goal in Context** | System creates a report that becomes available to be downloaded and used in a case. | |
| **Precondition** | At least one Report listing must be added. | |
| **Success End Conditions** | A report is successfully available for export for the investigator. | |
| **Failed End Condition** | A report is not available for export. | |
| **Trigger** | Button for creating a report is pressed / The case is closed. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | The Actor clicks button to create a report or the Actor closes the case. |
| | 2 | System creates a report using report listings that is available for export. |

VIEW ALL REPORTS

| **Use Case 11** | ***View All Reports*** |
|---|---|
| **Goal in Context** | View all the reports that have been created. |
| **Precondition** | At least one report must be created. |
| **Success End Conditions** | The reports are available to view and download. |
| **Failed End Condition** | The reports are not available. |
| **Trigger** | Actor selects button to view all reports. |

| **Actors** | Admin/Manager | |
|---|---|---|
| **Description** | **Step** | **Action** |
| | 1 | Actor clicks button to view all reports. |
| | 2 | System displays all reports that have been created. |
| **Extensions** | **Step** | **Branching Action** |
| | 2 | Actor can also individually view all reports and export them. |

OBTAIN CASE DATA & REPORT

| **Use Case 12** | ***Obtain Case Data & Report*** | |
|---|---|---|
| **Goal in Context** | Case reports and data exported by the actors. | |
| **Precondition** | Case reports must be created. | |
| **Success End Conditions** | Case report and data successfully exported. | |
| **Failed End Condition** | Case report and data not exported. | |
| **Trigger** | Actor selects the case to be exported. | |
| **Actors** | All Actors. | |
| **Description** | **Step** | **Action** |
| | 1 | Actor selects the case report they wish to export. |
| | 2 | Case report and data is exported and available to the actor. |

CLOSE CASE

| **Use Case 13** | ***Close Case*** | |
|---|---|---|
| **Goal in Context** | Close a case and create a report based on the findings. | |
| **Precondition** | Case has been created. | |
| **Success End Conditions** | Case successfully close and report created. | |
| **Failed End Condition** | Case is not closed. | |
| **Trigger** | Button to close case is clicked by Actor. | |
| **Actors** | Investigator. | |
| **Description** | **Step** | **Action** |
| | 1 | Button to close case selected by actor. |
| | 2 | System performs functions to close the case and generates a report based on findings. |
| | 3 | Report is made available for export to the actor. |

## DESCRIBING HARDWARE

Due to the recent COVID-19 pandemic, access to any of the University of Limerick's (UL) facilities are restricted. This means that the project will be developed and ran on personal hardware. Access to the laboratories in UL is not possible due to COVID restrictions; so, the project will be undertaken from home.

The system which will develop the software is running an Intel(R) Core (TM) i5-4460 central processing unit (CPU) with 3.20GHz. It has 8GB of random-access memory (RAM) installed and a Nvidia 960 graphical processing unit (GPU).

For the purposes of testing and deployment, VMWare Workstation 15 Pro will be used it was purchased earlier this year. This software was chosen because it allows simultaneously running of virtual machines which will be used to create different scenarios that will be described in the final report of this project.

## DESCRIBING SOFTWARE

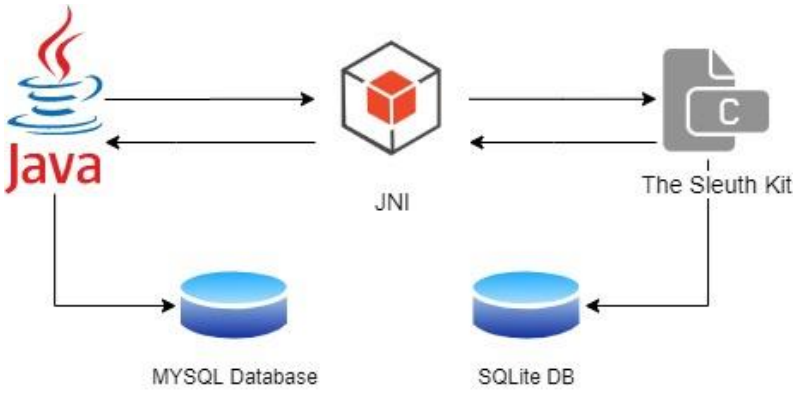


*Figure 4: Software Outline*

The Software will consist of a java interface which integrates the Sleuth Kit (TSK) using a Java Native Interface (JNI). TSK will use an SQLite database to store basic information regarding cases and sources of data. Java will use a MYSQL database that will contain user specific data and information related to case reports. The SQLite database is self-contained meaning that it is an embedded database that runs as part of the app. On the other hand, the MYSQL database is a relational database management system (RDBMS) used to store, retrieve, modify, and administrate a database.

### *JAVA*

The shell of the application will be written using the Java programming language. Java is object-oriented, meaning that a modular program can be created and increasing the amount of reusable code. It is platform independent meaning that it does not need any software to be installed to be executed but JVM must be present on the machine.

Java has features that focus on the graphical user interface (GUI) development. Previously in project development, Swing was implemented to aid the development of GUIs, but for the purpose of this project alternative options will be considered. These options include Abstract Windowing Toolkit and JavaFX. The decision will then be made as to which is the most suitable implementation to use.

### *JNI AND THE SLEUTH KIT (C/C++)*

The Sleuth Kit (TSK) Java bindings allow the java program to access data extracted by TSK. TSK is an open source digital forensic tool kit developed by Brian Carrier. The project will use his library and collection of command line tools to allow the investigation of disk images. It enables analysis of volumes and file system data to determine the use of cloud storage solutions on the disk. One of the main advantages of its use is that it is open source. Full access to the code is included and can modify such code if required.

There are three types of classes in TSK package. The first contains all of the code that deals with the backend SQLite database. The second deals with the bindings to the C/C++ code, allowing population of the database or allowing file content to be read. The third stores information about specific files or volumes. Integrating this into the Java shell will result in a software that can prove useful to forensic investigators.

### *MULTI-THREADING*

For the software to achieve multitasking it will use a process known as multi-threading. It enables multiple operations to be performed at once. For example, it will be able to run several background tasks, such as logging file data, updating the GUI, and processing requests at the same time. It also will make the software more stable, if one of the threads has an error, it will not cause the entire program to crash.

# DETAILED ACTION PLAN

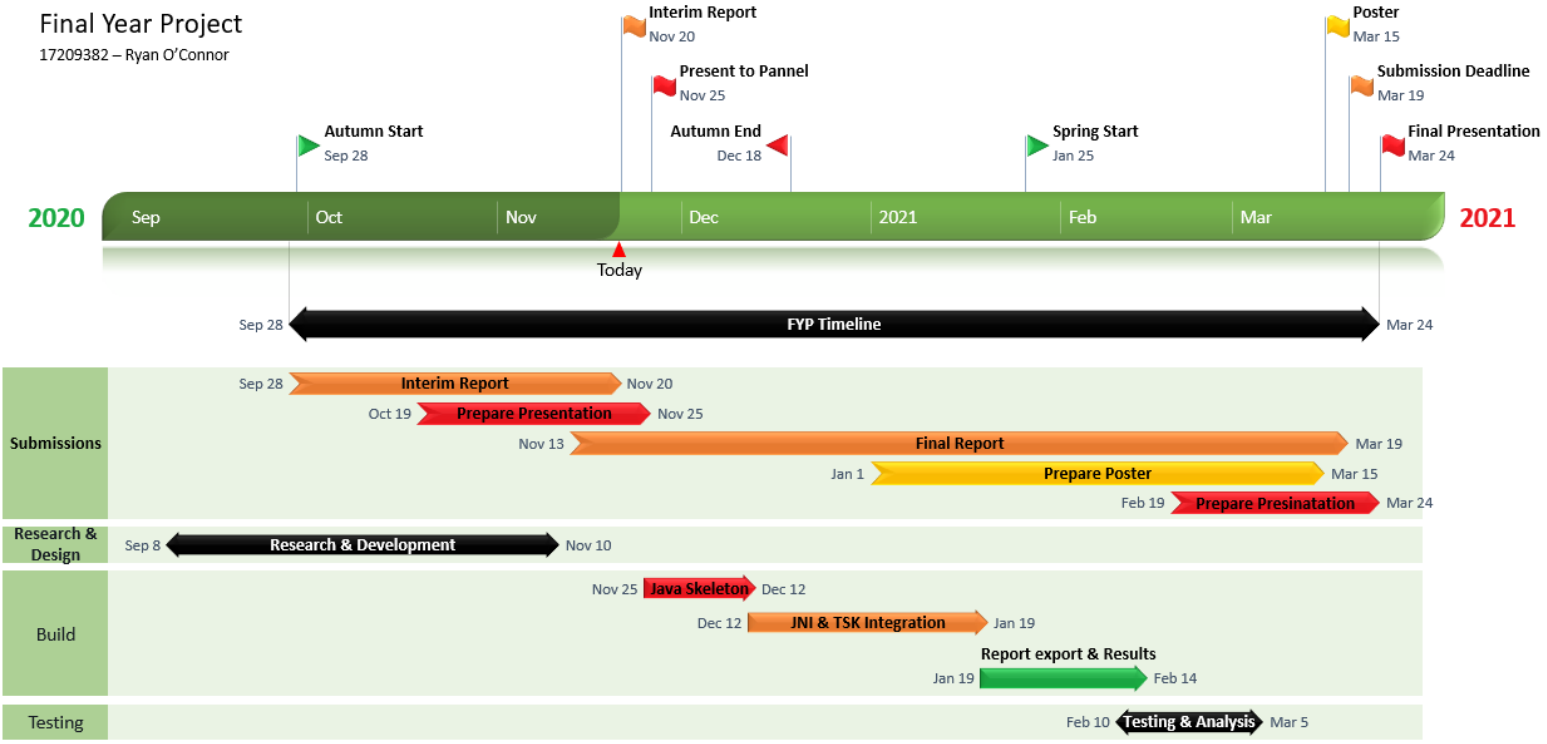


*Figure 5: Detailed Action Plan*

| Deliverable | Description | Due Date |
|---|---|---|
| Java Skeleton | The java Skeleton consist of the base java application including:<br>• The GUI (User Interface)<br>• Connection with the database<br>• User functionality inside the Java | 12th December |
| JNI & TSK integration | Integrating the JNI to allow use of TSK (The Sleuth Kit) including:<br>• Having the Sleuth Kit read an uploaded image.<br>• Process that image and gather data related to the image.<br>• Passing & Storing the collected data. | 19th January |
| Report export & Result | Formulating the exportable report from the data collected. Exportation of forensic data for further investigation | 14th February |
| Testing & Analysis | Testing will be completed by this date, but most of the testing will be done prior as development advances. | 5th March |

# REQUIREMENTS OF FACILITIES AND MATERIAL

1. Computer and peripherals
2. VMWare Workstation 15
3. Windows 10 installation image
4. Windows 7 installation image
5. Ubuntu Linux installation image
6. The Sleuth Kit tool kit
7. Java SE Development Kit
8. Installation files for cloud storage solutions
    a. Dropbox
    b. Google Drive/ Google Docs
    c. Evernote
    d. Amazon S3

# REFERENCES AND SOURCES OF INFORMATION

[1] Amazon, "What is Cloud Computing", Amazon Web Services, Inc., 2020. [Online]. Available: https://aws.amazon.com/what-is-cloud-computing/. [Accessed: 05- Oct- 2020].

[2] HSE Ireland, "Coronavirus", HSE, 2020. [Online]. Available: https://www2.hse.ie/coronavirus/. [Accessed: 05- Oct- 2020].

[3] E. Burke-Kennedy, "Ireland had one of highest rates of home-working during Covid-19 crisis", The Irish Times, 2020. [Online]. Available: https://www.irishtimes.com/business/work/ireland-had-one-of-highest-rates-of-home-working-during-covid-19-crisis-1.4369346. [Accessed: 08- Oct- 2020].

[4] K. R. Choo, C. Esposito and A. Castiglione, "Evidence and Forensics in the Cloud: Challenges and Future Research Directions", *IEEE Cloud Computing*, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7962121. [Accessed: 10-Oct-2020].

[5] M. Sang Chang, "Forensic investigation of Amazon Cloud Drive on Windows 10", Ijiset.com, 2016. [Online]. Available: http://ijiset.com/vol3/v3s6/IJISET_V3_I6_69.pdf. [Accessed: 15- Oct- 2020].

[6] M. I. Ali *et al*., "Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment", IEEE *Access*, 2020. Available: https://ieeexplore.ieee.org/document/9199866. [Accessed: 15- Oct- 2020].

[7] E. Webb-Hobson, "Digital Investigations in the Cloud", *Docuri.com*, 2017. [Online]. Available: https://docuri.com/download/digital-investigations-in-the-cloud_59c1e21af581710b286a47a1_pdf. [Accessed: 15- Oct- 2020].

[8] W. Buyu and E. Odira Abade, "Forensic Analysis of Dropbox Data Remnants on Windows 10", ResearchGate, 2020. [Online]. Available: https://www.researchgate.net/publication/342991973_Forensic_Analysis_of_Dropbox_Data_Remnants_on_Windows_10. [Accessed: 21- Oct- 2020].

[9] F. Marturana, G. Me and S. Tacconi, "A case study on digital forensics in the cloud", ResearchGate, 2012. [Online]. Available: https://www.researchgate.net/publication/234063077_A_Case_Study_on_Digital_Forensics_in_the_Cloud. [Accessed: 21- Oct- 2020].

[10] F. McClain, "Dropbox Forensics - Forensic Focus", Forensic Focus, 2020. [Online]. Available: https://www.forensicfocus.com/articles/dropbox-forensics/. [Accessed: 21- Oct- 2020].

[11] H. Chung, J. Park, S. Lee, and C. Kang, "Digital Forensic Investigation of Cloud Storage Services", ResearchGate, 2012. [Online]. Available: https://www.researchgate.net/publication/257687927_Digital_Forensic_Investigation_of_Cloud_Storage_Services. [Accessed: 21- Oct- 2020].

[12] C. Altheide and H. Carvey, Digital forensics with open source tools. Burlington, MA: Syngress, 2011.

[13] B. Carrier, "Trackers - SleuthKitWiki", Wiki.sleuthkit.org, 2020. [Online]. Available: http://wiki.sleuthkit.org/index.php?title=Trackers. [Accessed: 04- Nov- 2020].

[14] P. Smith, "Waterfall model", En.wikipedia.org, 2010. [Online]. Available: https://en.wikipedia.org/wiki/Waterfall_model. [Accessed: 11- Nov- 2020].

[15] J. Denman, "Get started with these Agile basics", SearchSoftwareQuality, 2020. [Online]. Available: https://searchsoftwarequality.techtarget.com/feature/Agile-basics-FAQ-Getting-started-with-Agile. [Accessed: 11- Nov- 2020].