National College of Ireland

Project Submission Sheet

Student Name:	Matthew Browne		
Student ID:	x21174415@student.ncirl.ie		
Programme:	MSc/PGD in Cybersecurity	**Year:**	1
Module:	Forensics and eDiscovery		
Lecturer:	Michael Prior MSc/PGD		
Submission Due Date:	28th February 2025		
Project Title:	CA1, Investigating a Social Media Application, MS Teams		
Word Count:	8308		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:	Matthew Browne
Date:	28th February 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Your Name/Student Number	Course	Date
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	27/02/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

- CA Name: CA1, Investigating a Social Media Application Microsoft Team's
- Student Name: Matthew Browne
- Student ID: Student ID: x21174415

Contents

Executive Summary:

Key Descriptor

For my forensic investigation I will be analysing the Microsoft Teams application on Android operating system using a combination of software for forensic analysis. For my investigation I will be using a public android image with content pre-loaded for analysis, the image name is called: Android_14_Public_Image.tar.gz which I will have downloaded from Digital Corpora (Garfinkel, 2025). With this image I will be looking to forensically examine the contents of the device with a particular focus on Microsoft Teams content. The type of communications I will be looking for are, Microsoft teams specific call logs, messages, users and any other viable information related to the investigation. The artifacts I extract from this investigation will be documented a part of both written and image process. This will showcase my abilities to be able to easily extract artifacts and information from any android device.

Key Objective's

To Identify the key objectives I had to understand what is it I needed to accomplish , for me I had to understand the tooling that was being used , I relied heavily on the lecturers that we did for both week 3 and 4 in our classes , as my investigation was on Microsoft Team's I had to remind myself of some of the key things you can do with teams , these were messaging , calling , and configuring user accounts , teams offers many other back end services like sharing files like documents PowerPoints , forms and other artifacts but I decided to identify three key and simple items which I should be able to investigate and find on the device with any forensic tool.

Key Findings of Investigation

To identify the key findings, I needed to recap on my efforts during the investigation which were On the device in question, I was able to use Aleapp extract information like the teams call log for which I could see two calls made on the device from "Liz Dehner" which was detailed in my findings, I was also able to see message such as "They totally did. Just like you said. I should listen to you more often" also sent by Liz

and I was able to see a list of users in the team's app such as "Liz and ThisIs" all showcasing that forensics tools allow us to extract and fine information easily when used with a combination of other toolsets.

Research Conducted

My Strategy

To identify and compute the requirements of finding the information in the course of my investigation I relied primarily on my lecturer's notes I went back over the "Working with Digital Forensic Tools" (Prior, 2025) and the "Mobile Forensic Techniques" (Prior , 2025) PowerPoint which was supplied by Michael to better understand the tooling required for the assessment here I was able to understand better the types of tools required I also went over both week 3 and week 4 lecture recordings located in Moodle alongside the lab tutorial's . (Prior, 2025).

In terms of papers, I decided to go the route of searching google for specific articles one of which I found by Cyber5W, this was related to specific functions within Aleapp , it was here that I got a better grasp on the functionality within Aleapp once I had it installed and working (cyber5w.com, 2025) I also stumbled across another article written by Cellebrite , this went into detail on the level of information which could be attained through Aleapp and then introduced me to some new concepts and applications like , CLEAPP , which is used for chrome specific parsing , RLEAPP which can be used for logs and events and of course WLEAPP which can be used for windows events and log files , my counterpart for Aleapp for android is Ileapp which is what is used in Ios analysis. (Cellbrite, 2022).

In terms of books and or papers , I reviewed the book which was shared by Michael to the class labelled Book 7 - Mobile Forensics here I reviewed some of the chapters and content related to the tools, Autopsy was mentioned so this gave me grounds to use Autopsy as one of my chosen tools. (Anon., Unknown) , Aleapp was mentioned in Michael's "Mobile Forensics_v2.pdf" I used this as my primary source for choosing Aleapp to accompany this I used a really good instructional video to get familiar with the Aleapp install procedure as well. (dfir.science, 2022) alongside this I also used the Dfir science research section on the website to review some papers which helped in understanding Aleapp more. (dfir.science, 2022).

In terms of Industry reports I utilised the San's "The Ultimate Guide (DFIR)" (SANS, 2024) this provided me with some additional background into digital forensics and gave me a flavour for some important considerations while it didn't fully help me with my strategy it still filed in a knowledge gab that I had not thought about.

Forensic Analysis Methodology / Investigation Method's Study

To investigate and find out the tools that would be used in a forensic investigation based on a research paper I read the paper on "Comparative Analysis of Android Mobile Forensics Tools" (Lwin, et al., 202) this was definitely an eye opener, this paper gave insights into four tools which were AFLogical part of the application suite belonging to the FTK imager tool , Via Extract which they ran on a Linux based os and or virtual machine and of course Autopsy as well which I had got hands on experience with through lectures and labs with Michael. The paper went into details on the shortfalls of forensic tools and the drawback to using some of the tools it also highlighted the need for a key chain of evidence when handling tools and evidence which was an interesting peace. The paper highlighted the different steps in the forensic analysis process steps like acquisitions which highlighted that there were three of these, manual, logical and physical they also stipulated that this would vary pending on the acquisition method chosen by the investigator. The key point for a logical acquisition is that only a portion of the data which had not been deleted by a user would be recoverable, they also highlighted that tools for logical acquisition would not service for recovering and sort of data.

The actual analysis and case management of the data was handled using Autopsy which I did cover as part of my investigation and we also covered this in our lecturers so nothing new or additional hear bar the mention the author gave to some paid forensic tools' , they also went back and highlighted the importance of isolating the device from any point of communications weather it was Wi-Fi , Cellular or Data networks. In the article they discussed the context of rooting, and a tool called Odin which could be used to do it. Again, they further discussed tools here which could be used in the different acquisition types. In the article they continued to discuss both Belka soft and Magnet Acquire, showcasing the levels of data these tools could extract from the android device. It's evident from reading the paper that they heavily mentioned Magnet Forensics tooling and toolkits as being a premium standard tooling in the forensics industry (magnetforensics.com, 2025) Based on the finding and conclusions of this study the tooling that came out top was "Magnet Acquire" (Lwin, et al., 202) which is a free tool to members of forensic communities It was highly rated by the authors as atop pic in terms of free tooling. It should be noted though that the authors conclusion was very much inconclusive they deemed multiple tools as the solution, personally I felt this fell short of expectations for the study but still provided a good insight into the investigation methods.

Tools and software used as part of my investigation.

- ALEAPP Version 3.3.0
- Windows PowerShell
- DB Browser for SQLite 3.46.1
- Python 3.13
- Windows 11 Pro version 23h2
- Autopsy Version 4.21.0

Other optional tools I could have used

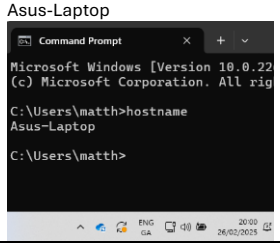
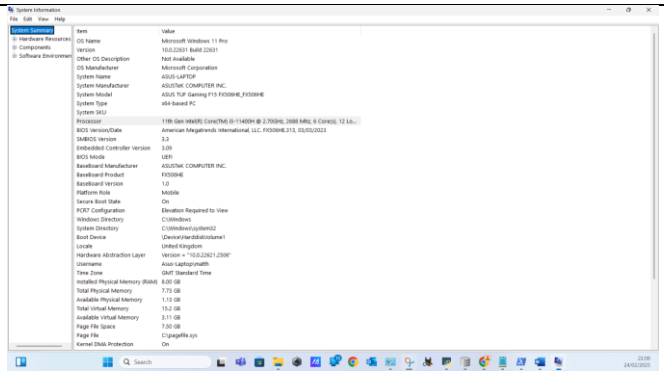
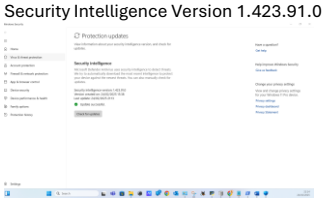
- FTX Imager
- Odin
- Magnet Acquire

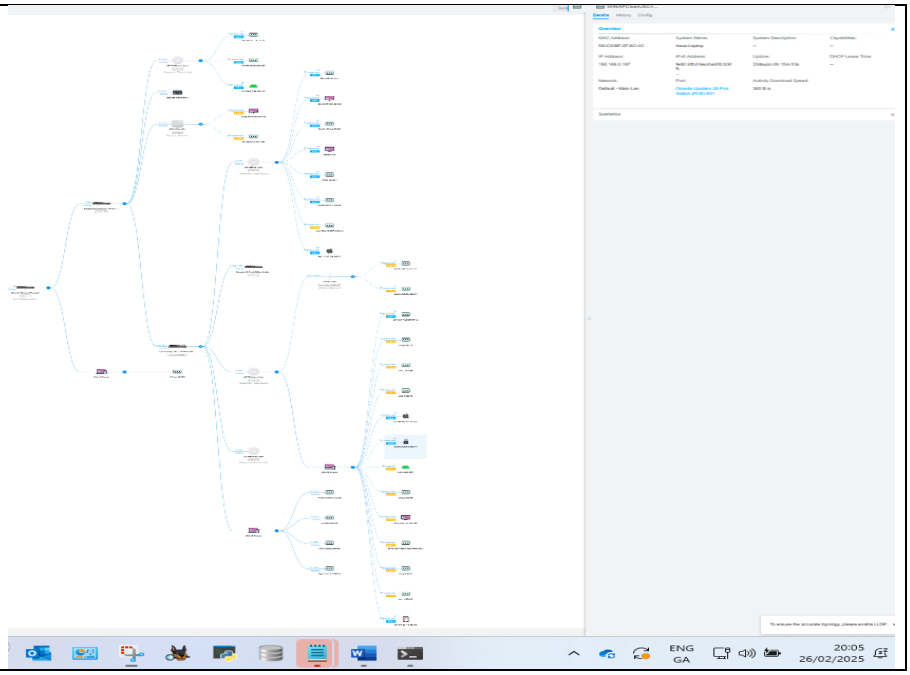
Guiding Principles and or guidelines.

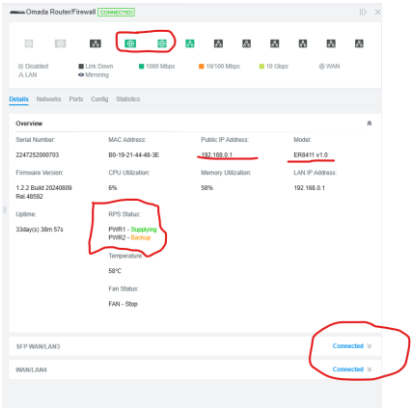
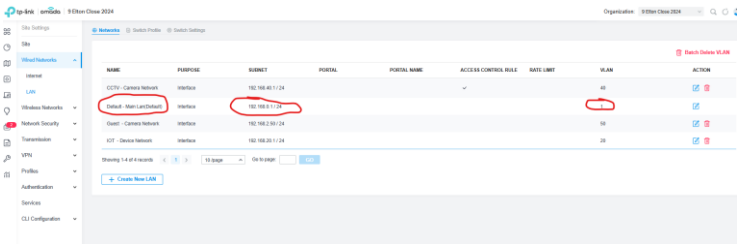
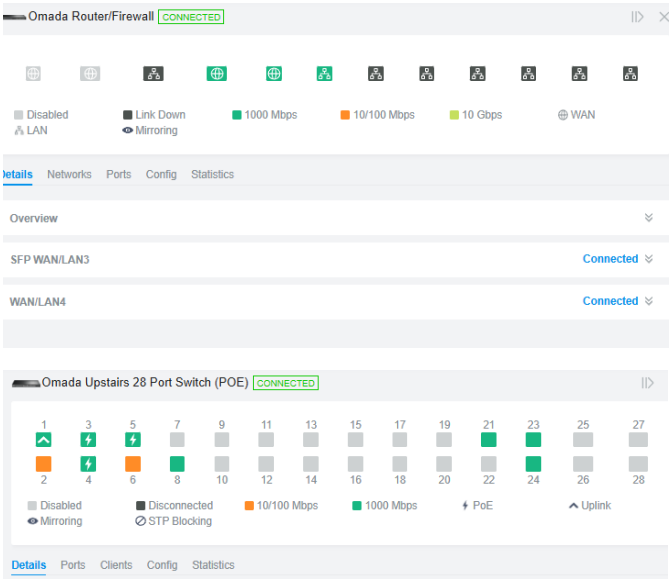
The guiding principles can be described as something an individual sets out in terms of conducting themselves in a professional , ethical and worthy manner such as being legal , morale , honourable and so on or this can also be set out by a common body of knowledge or a member organisation they are a part of , example I am a proud member of ISC2 , ISC2 the International Information System Security Certification Consortium (isc2, 1989) who are a global network of 265,000 member certified across different certifications. Example I hold the SSCP, this stands for "Systems Security Certified Practitioner" From ISC2. (isc2, 1989) within this certification ISC2 sets out guiding principles such as their cannon's this is their form of a code of ethics everyday security professionals try their best live by these codes some examples are of the codes and cannons are , "Protect society" , "Act honourably" , "provide diligent and competent services" , and "advanced and protect the profession", (isc2, 1994) all of which are highly valuable in today's society. While these may be a code of ethics each of us should have our own internal codes which we compute in our brains every day, so for me these were my guiding principles in conducting my forensic analysis and I derived my guidelines from the SSCP CBK under domain 4 number 4.2 "4.2 Understand and support forensic investigations" (isc2, 2024)this provided me with some very well know techniques which I utilised as part of my testing and analysis.

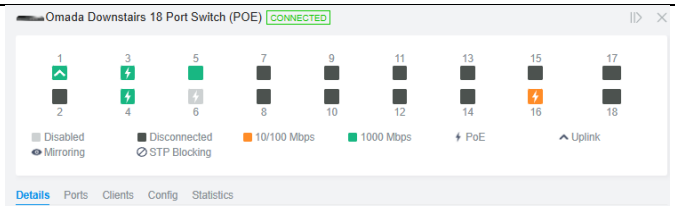
Test Environment OS setup & Configuration

My test environment was rather simple, I conducted all my testing on a physical laptop, my laptop information consists of a System Manufacturer, Model Number, Processor, Base operating system, Base OS version and Build Number, and some private network information, included in my Os environment 4 applications installed with various version number's.

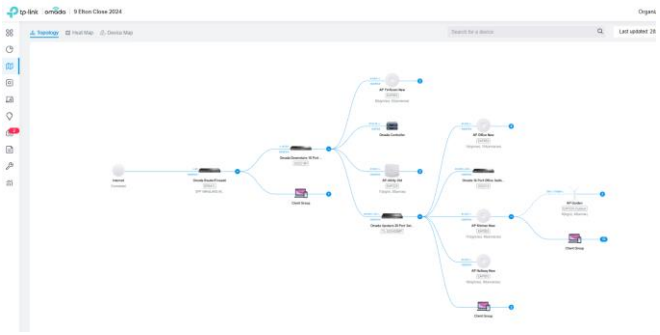
Base OS System Information	
System Manufacturer	ASUSTeK COMPUTER INC.
Model	ASUS TUF Gaming F15 FX506HE_FX506HE
Processor	11th Gen Intel(R) Core (TM) i5-11400H @ 2.70GHz, 2688 Mhz, 6 Core(s), 12 Logical Processor(s)
OS Name	Microsoft Windows 11 Pro
System Hostname	Asus-Laptop 
Version	10.0.22631 Build 22631
Installed Physical Memory (RAM)	8.00 GB
Network information	Locked to a Private segregated network not publicly accessible behind a Firewall. IPv4 Address. . . . . : 192.168.0.187 Subnet Mask . . . . . : 255.255.255.0 Default Gateway . . . . . : 192.168.0.1
System Information Screen Laptop	
Defender Antivirus Information	Security Intelligence Version 1.423.91.0 

System Network Map Location	

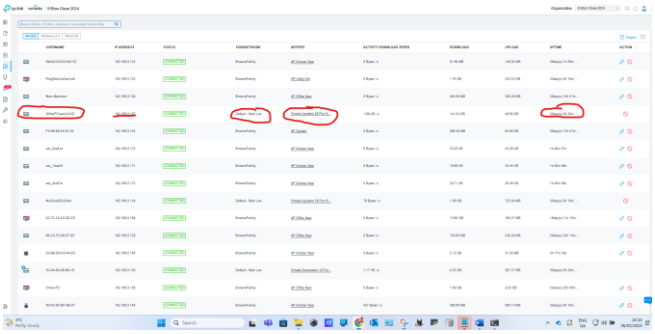
Overall Network Config Infront of Laptop	My Laptop has the following network information as we can see from this pictures and is directly connected into the network via patch point , not on wifi. • Its MacAddress is : D0-C0-BF-2F-6C-4C • Its IP Address is : IP Address is : 192.168.0.187 • Its uptime is : 33 days • Its also connected to the Main VLAN which is 1 in my case • My laptop is connected behind a Firewall Omada ER8411 • We can see that backup and redundency are in place for the firewall and internet connections. Firewall Image  In my network there are 3 Comm's Cabinet each one has a switch 2 of which are POE Switches and my network is controlled by my Omada Cloud solution, which is a typical example of software defined networking ,I also have in place 4 Vlaned networks one for CCTV , One for Guest , One for IOT , And my Main which is Default. For redundency and sandboxing purposes I also have two internet connection's , our Wifi system in seperated across multiple SSID's and Vlan's. (Microsoft , 2024) If we take a look here we see the Default Main Lan.  If we take a look here we see switches , firewall and configs. 



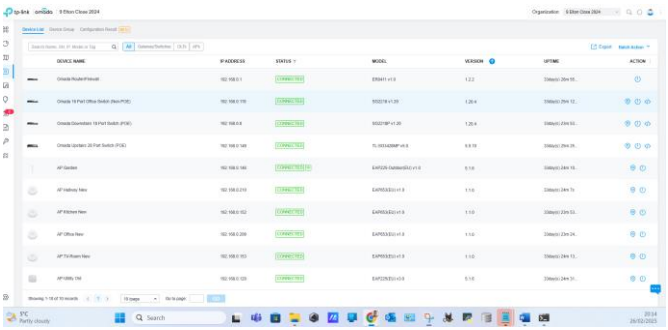
If we take a look here we see the Topology in quick view for my network.



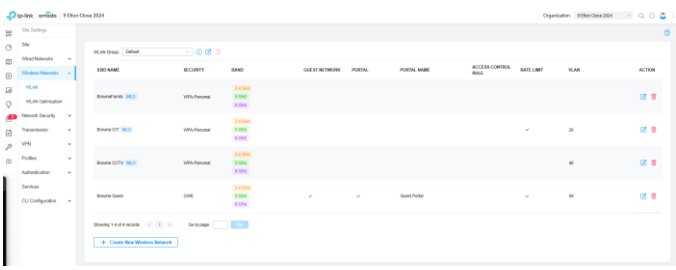
If we take a look here we see the key information of my system on the network.



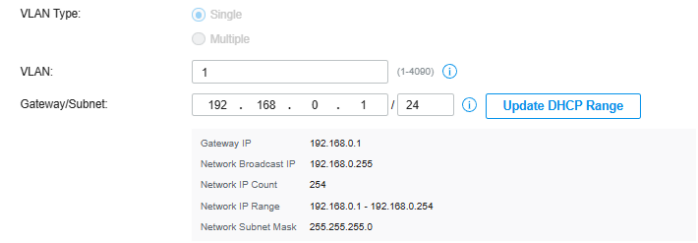
If we take a look here we see all the network hardware which includes switches , accesspoints and firewall and router.



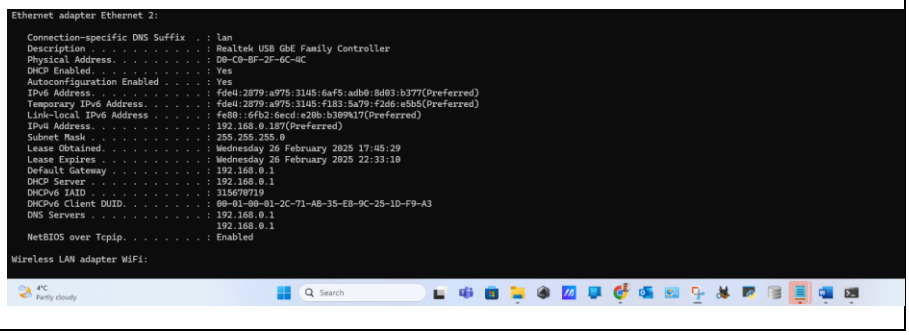
If we take a look here we see all the wifi networks and vlans each one connects to.



Main Vlan laptop is connected to.

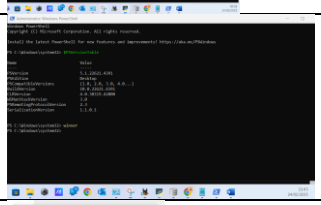
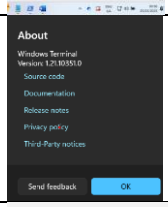


This all further supports the same configuration on my laptop command prompt output.



Base Sandboxing Measures	
What is Sandboxing (Check Point , 1994)	Sandboxing is a form of safeguarding your system against unexpected threats from testing out applications, software and code. Usually, a system administrator implements sandboxing measure where they are looking to examine the output of specific commands , often a sandbox environment will replicate a real environment where the system administrator is looking to replicate the changes in the desired environment , example a system administrator may have a locked down windows laptop or desktop or virtual machine to perform actions such as installing software , analysing code , or analysing malware. Sandboxing is essentially a method of ensuring you do not leave your system or any system open to known vulnerabilities should the worst happen. It allows a system administrator to play with and experiment with software, code, environments without any repercussions. Sandboxing comes in many forms • An isolated network (In the form of a lab subnet) • A Restricted Virtual local area network (in the form of a guest or lan subnet) • An isolated workstation or server (workstation not connected to any network) • A restricted workstation or server (server located on a devops platform, Azure) • A Proxy server on premise or in the cloud (Controlling routes in and out of lan) • A Firewall on premise or in the cloud (behind or in front of server or workstation) • A Virtual Private Network Connection
Why do we implement Sandboxing (Check Point , 1994)	Some of the key benefits to sandboxing are • Less exposure to any potential known indicators of compromise which are published publicly through forms and websites. • A method to be able to test new vendors where you as the administrator do not know how, what or why a particular piece of code of software works and enables you to install and test this in an isolated space without any security concerns. • It is also a method for testing items or pieces of code which are in development to ensure there are no known vulnerabilities or indicators of compromise. • With sandboxing you can analyse forms of malware, spyware and ransomware without the implications of something bad happening to your system. • Sandboxing is a common process and is usually used in enterprise environments for different stages of a Cab process.
Sandboxing Measures in place (My Environment)	Some of the key Sandboxing measures in my environment My Network & Firewall Access Secured Custom design and configuration built by me, I have built my network from the ground up , it all starts with my own personal domain , accompanied by a software defined cloud network management solution and on premise and cloud based Azure domain controller's , this is interlinked by a Virtual Private Network and a custom Virtual Desktop Infrastructure environment hosting multiple vm's for testing , in this case I decided to opt for my test laptop so I could use something local. My Network & File Access Secured Custom allow/block and filtering through my Omada firewall handles all access in and out of my on-premises network with a VPN (Microsoft , 2025) to Azure AD Domain controllers which support backup and redundancy options for site recovery with a hot side ready to go should a failover need to happen , my access is also tightly controlled via group policy management in active directory and Intune configuration profiles for laptops and workstations. My Endpoint Detection & Response Custom Defender Edr & Av capabilities in active mode which include but are not limited to filtering of websites from gateway and proxy server level redirection across azure vnet and vpn , privileged identity and access management tied in with Entra id against both on-premises and cloud assets and hardened windows operating system image from CIS which has further lockdown from Microsoft Intune and windows server active directory environments in azure and on premise. My Encryption Standards Proprietary Microsoft BitLocker encryption enabled on my test laptop with backup recovery keys stored offsite for recovery purposes integrated with a cloud Laps Microsoft solution and rotating key.

Test Environment OS Installed Applications

Application's	Version number	Image Evidence
ALEAPP	Version 3.3.0	
Windows PowerShell	Version 5.1.22621.4391	
DB Browser for SQLite	Version 3.46.1	
Python	Version 3.13 or 1.21	
Windows 11 Pro Version	Version 23H2	
Windows 11 Pro Build Number	Version 22631.4602	
Autopsy Version	Version 4.21.0	

Test Environment OS Installed Applications Descriptor's

Tool	Descriptor	Justification for using tool.

ALEAPP	Aleapp allows not just any individual's but forensic specialists to forensically examine an android devices operating system root folder and contents which would be stored on the device, this can be then accessed from a windows operating system using the Aleapp gui. It allows an individual to forensically examine the contents of the android device and parse through the different components which make up the android operating system. (ycsc.org.uk, 2024) Alongside this it allows the forensic specialist or the individual using the program to easily recover lost and deleted data by any user, it also primarily serves as a way for an individual or forensic specialist to identify key components of data at rest, data in use and data in transit on the device. With Aleapp an individual or forensic specialist can download the application through the windows PowerShell command line which is also freely available on windows and once installed correctly can use, Aleapp's graphical user interface to generate a report for the device for various components of data stored on the device. Aleapp is an open-source community project which means anybody can use the software free of charge they would only need to understand how you could perform actions within the report it provides and how to use the gui once installed.	• I chose Aleapp as it was extensively covered in the google scholar comparison study, I covered during my research stage. • Our lecturer Michael also covered this on our teams' sessions and in his notes and lecturer videos in week 3 and 4 with additional guides and labs. • It was also provided as an open-source solution which made it a primary choice alongside plenty of documentation being available for diagnosing any issues I had with it.
Windows PowerShell (https://learn.microsoft.com, 2024)	Windows PowerShell allows an individual to avail of and use the command line utility known as cmd available openly in the windows operating system. Windows PowerShell while openly available in the Microsoft operating system still requires a valid licence key where the operating system should be deemed genuine once the os itself is activated with a licence key. In contrast to Aleapp which starts at the command line and then progress to gui, windows PowerShell is exclusively a command line tool and is compatible with applications around the world both paid and open source. Because windows PowerShell works as a command line tool many applications are compatible with it making it a primary tool for forensic analysis.	• I chose to use windows PowerShell as it was natively available in my operating system edition windows 11 pro without any additional cost, • It was also featured in many of the videos and articles I watched alongside being compatible with the other applications I chose to use. • It was also provided as an open-source solution freely available on Microsoft os which made it a primary choice alongside plenty of documentation being available for it Aswell • I have extensive hands-on skills and certification with using PowerShell for the last 20+ years.
DB Browser for SQLite (sqlitebrowser.org, 2023)	DB Browser for SQLite allows an individual to analyse and open database files and content. It allows an individual to edit the databases themselves which can be imported into the program for viewing and analysis. One of its most important functions it that an individual can search through the database they import and complete discovery on the files and structures themselves.	• While I have chosen to list DB browser in terms of tools, I only did a very small amount with it. • While DB browser is open source easy to download and install on windows and had also been mentioned a few times in our lectures, so I felt it was a good tool to test out on a small database. • It allowed me to parse through a database file and export additional information during my testing.
Python (python.org, 2025)	Python is a popular programming language used across industries such as website development, graphical user interface development, software and systems development. It's a common programming language which is taught in schools at leaving certificate level QQI level 5 (Qualifax, 2023) and then taught as part of multiple higher level QQI courses such as BSc, PgD , MSc and PhD which are level 8 (National College Of Ireland , 2019) , 9 (National College Of Ireland , 2019) , 10 (UCD.ie, 2025) across various universities. The Python programming language is usually required where users need to learn to code in python or where other programs rely on its features for usability.	• Python is an open-source programming language very popular among many web developers, in terms of compatibility across other programs its widely known to work within a range of industries • It was a primary prerequisite requirement if I wanted to run and use Aleapp.

Windows 11 Pro Version (wikipedia , 2021)	An operating system which was created by Microsoft out of the original NT Product. (wikipedia, 2001) (Microsoft, 1991) Windows 11 is the next version of windows after windows 10 and is commonly found across personal, business and enterprise level computing. It is one of most famous operating systems worldwide.	• I chose to use windows 11 pro as its my daily driver for both work and personal computing needs. • Its ease of functionality and the fact that I have 35 Certifications in Microsoft technologies made it an obvious choice for forming part of my investigative toolkit. • I have also worked on windows platform for 20 plus years.
Autopsy (autopsy.com, 2024)	Autopsy is an open-source forensic investigation tool which allows both individuals and forensic specialists to install it on their chose operating system. Autopsy is compatible with all major operating systems such as Windows, Linux, Mac, and various flavours of Linux such as red hat, Ubuntu. Autopsy is used by forensic specialists to create case files, store artifacts in a systematic and logical way while providing the individual with ways of managing source and destination of their choosing for artifacts and report findings. Autopsy is like Aleapp in that it offers a gui, graphical user interface to be able to perform analysis of many types of devices such as phones, laptops, workstations, servers and more. It provides an easy to use but dated gui to be able to store, investigate and log evidence in a case file. It creates a structured manageable format to generate a forensic report for investigators, Autopsy do offer a paid version with additional capabilities for enterprises and law enforcement, but the free version will provide a solid capability for any individual.	• Autopsy came up quiet a few times around forensics and tool kits, its widely accepted as a standard free open-source toolkit but is quite dated. • I chose to include Autopsy as we had studied it as part of our lecturers and courseware alongside it appearing in my education papers comparison. • I also wanted to get some hands-on level functional user testing with the software and case management system.

App Investigation & Findings

Aleapp Prerequisite's

To begin my investigation, I grabbed my test laptop running windows 11 professional Version 23H2, my build number for this laptop was Version 22631.4602. I began to install the relevant applications I would need for carrying out my investigations these applications were Python Version 3.13, DB Browser for SQLite Version 3.46.1, Autopsy Version 4.21.0 and ALEAPP Version 3.3.0.

Within my downloads folder I created the following folders

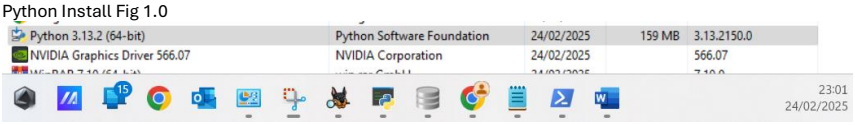
Root folder of "C:\Users\matth\Downloads\MSC Testing"

Followed this with three other folders one for autopsy, one for test results, one for the public android file I would download.

"C:\Users\matth\Downloads\MSC Testing\Autopsy"
"C:\Users\matth\Downloads\MSC Testing\Test Results"
"C:\Users\matth\Downloads\MSC Testing\Test Android File"

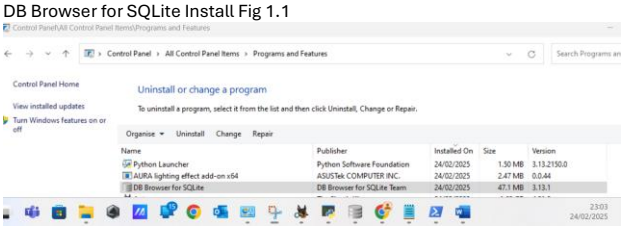
I Then installed the Python application

Python Install Fig 1.0



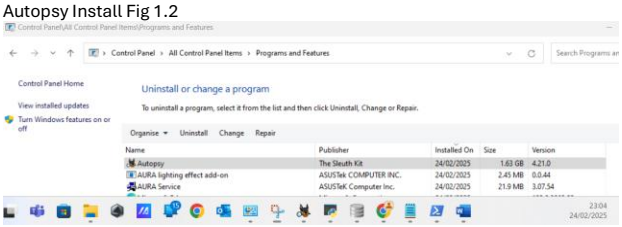
Following this I installed the DB Browser for SQLite

DB Browser for SQLite Install Fig 1.1



Next, I began to install the Autopsy

Autopsy Install Fig 1.2



There was not requirement to install PowerShell as this comes with windows, I did however check the version I was running by using the "$PSVersion Table" Command confirming I had version 5.1 installed.

Next, I moved onto the install of ALEAPP

Aleapp Install

I did this by going to the following within PowerShell
"PS C:\> cd C:\Users\matth\Downloads\ALEAPP-main"

I input the command "PS C:\Users\matth\Downloads\ALEAPP-main> pip install -r requirements.txt" which I had taken from the GitHub page. (Abrignoni, 2023)

I received a notice to update the Python version which I did.
"[notice] A new release of pip is available: 24.3.1 -> 25.0.1
[notice] to update, run: python.exe -m pip install --upgrade pip"

I did this by running "python.exe -m pip install --upgrade pip" this began the process of updating the python application and installing the updates as evident in the screenshots.

Python Updates Fig 1.3

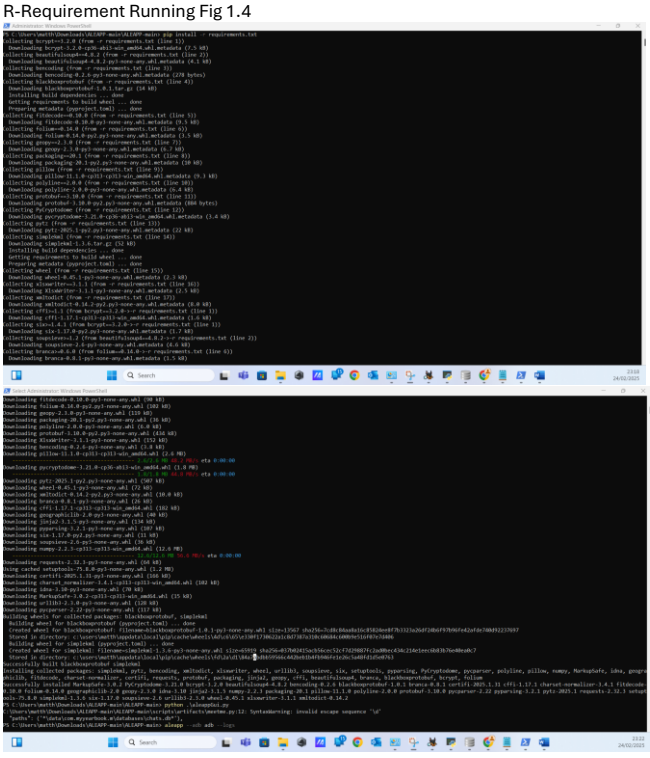
```
PS C:\Users\matth\Downloads\ALEAPP-main> pip install -r requirements.txt

[notice] A new release of pip is available: 24.3.1 -> 25.0.1
[notice] To update, run: python.exe -m pip install --upgrade pip
ERROR: Could not open requirements file: [Errno 2] No such file or directory: 'requirements.txt'
PS C:\Users\matth\Downloads\ALEAPP-main> python.exe -m pip install --upgrade pip
Requirement already satisfied: pip in c:\users\matth\appdata\local\programs\python\python313\lib\site-packages (24.3.1)
Collecting pip
  Downloading pip-25.0.1-py3-none-any.whl.metadata (3.7 kB)
Downloading pip-25.0.1-py3-none-any.whl (1.8 MB)
   ---------------------------------------- 1.8/1.8 MB 34.7 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 24.3.1
    Uninstalling pip-24.3.1:
      Successfully uninstalled pip-24.3.1
Successfully installed pip-25.0.1
```

Next, I went back to the requirements install and re-ran it using the following

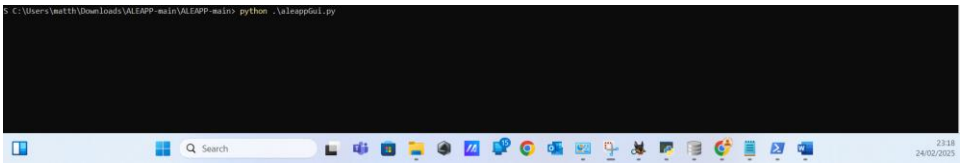
"PS C:\Users\matth\Downloads\ALEAPP-main\ALEAPP-main> pip install -r requirements.txt"

R-Requirement Running Fig 1.4



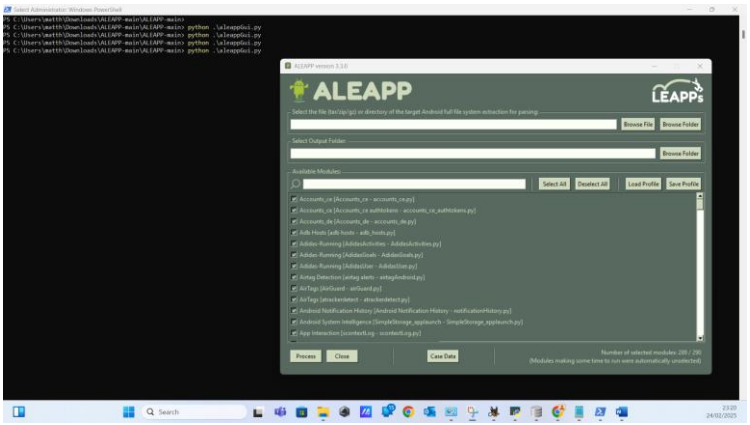
Once the process completed, I launched the Aleapp Graphical user interface console.

Ready to launch Aleapp Running Fig 1.5



What I got was the ALEAPP Version 3.3.0 Gui next

Aleapp Running Fig 1.6



Once I got to this point, I was able to continue onto the Artifacts analysis.

Sources of Forensic Artifacts

The First Report I ran was solely based on Microsoft Teams

This report allowed me to collect the following information

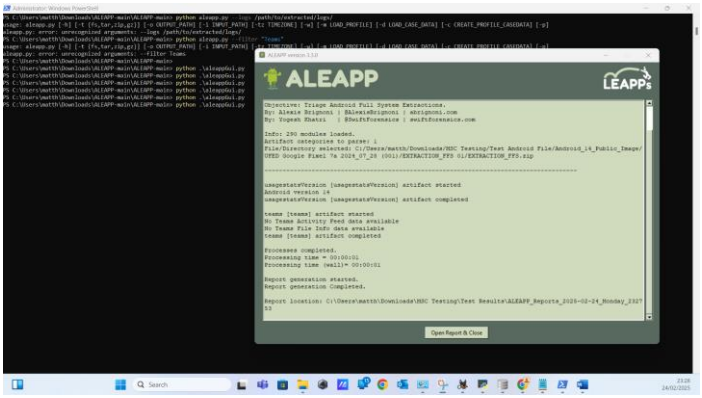
Extraction location which was: C:/Users/matth/Downloads/MSC Testing/Test Android File/Android_14_Public_Image/UFED Google Pixel 7a 2024_07_28 (001)/EXTRACTION_FFS 01/EXTRACTION_FFS.zip

Report Directory which was: C:\Users\matth\Downloads\MSC Testing\Test Results\ALEAPP_Reports_2025-02-24_Monday_232753

Device Details such as the

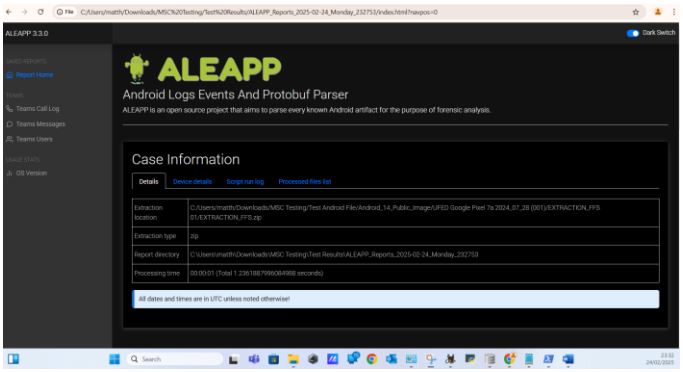
- Android version per Usagestats: 14
- Codename per Usagestats: REL
- Build version per Usagestats: 11206848

Aleap running Teams only Module Fig 1.7

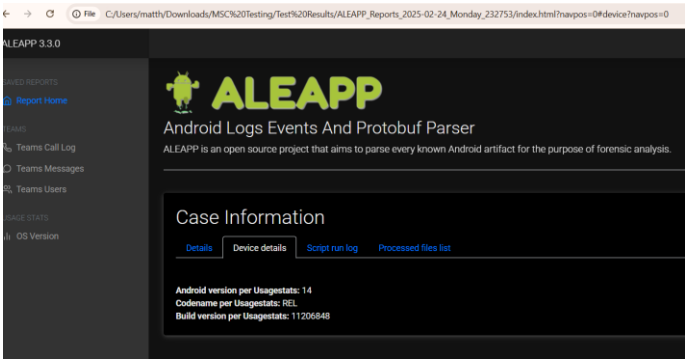


Aleapp Finding's

Case Details Fig 1.8



Device Details Fig 1.9



Artifact -1 Microsoft Teams Call Log's

From here I moved onto looking at the artifacts the first one I looked at was.

1: Microsoft Teams Call Log's

For the teams call logs I was able to see the following

- Start and End times e.g. dates and time stamps of the calls.
- The call states e.g. accepted or declined; in my case both were accepted.
- Type of call, e.g. single or two party.
- The person who made the call, e.g. in both of my cases it was "Liz Dehner"
- The direction on which the call was, outgoing or incoming, e.g. in my case they were both outgoing.

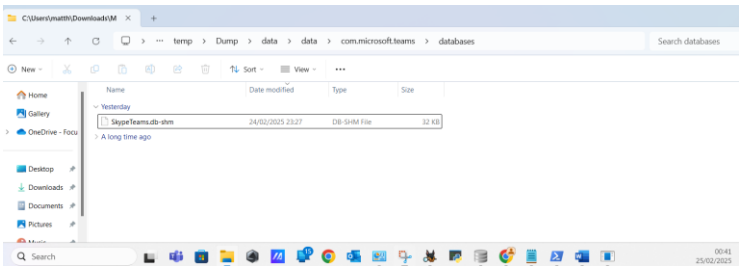
From the teams call log report I was also able to identify the database for further analysis which was located at

C:\Users\matth\Downloads\MSC Testing\Test Results\ALEAPP_Reports_2025-02-24_Monday_232753\temp\Dump\data\data\com.microsoft.teams\databases\SkypeTeams.db

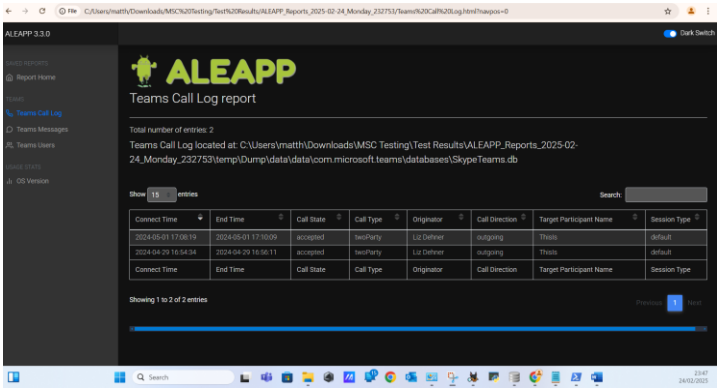
Main location being: Dump\data\data\com.microsoft.teams\databases\SkypeTeams.db

Knowing this location, I will be able to analyse this further with "DB Browser for SQLite Version 3.13.1"

Microsoft Teams Call Logs DB Location



Teams Call Log Report Fig 2.0



Artifact -2 Microsoft Teams Call Messages

For the team's message logs I was able to see the following.

- Timestamp of the message, e.g. one message was sent on "2024-04-29 15:53:15"
- User Display Name, e.g. one name that came up was "Liz Dehner"
- Conversation ID, e.g. one conversation id was "19:uni01_fy5nd3xuvhdzadouocl5s5pgds52e2hc6pxlnyculliwgleofljq@thread.v2"
- Message ID, e.g. "1714405995913"

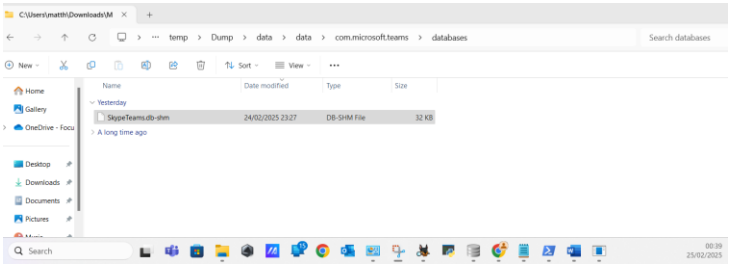
From the teams Messages log report, I was also able to identify the database for further analysis which was located at

C:\Users\matth\Downloads\MSC Testing\Test Results\ALEAPP_Reports_2025-02-24_Monday_232753\temp\Dump\data\data\com.microsoft.teams\databases\SkypeTeams.db

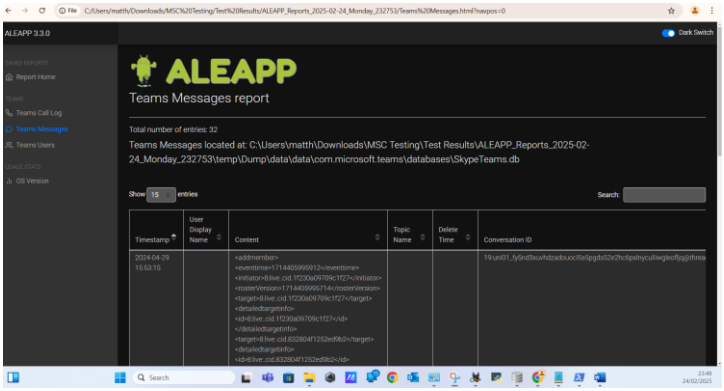
Main location being: temp\Dump\data\data\com.microsoft.teams\databases\SkypeTeams.db

Knowing this location, I will be able to analyse this further with "DB Browser for SQLite Version 3.13.1"

Microsoft Teams Messages DB Location



Teams Messages Log report Fig 2.1



Artifact -3 Microsoft Teams User's

For the team's users logs I was able to see the following.

- Last Sync Date and Time
- First name of user e.g. one first name was "ThisIs"
- Last name of user e.g. one last name was "DfirTwo"
- Display Name e.g. one name was "Liz Dehner"

- Email Address e.g. one of the email addresses were ldehner505@gmail.com
- User Type, e.g. in our case all users were TFL User types.
- Private Chat Functionality enabled, e.g. knowing if this functioning was enabled for user.

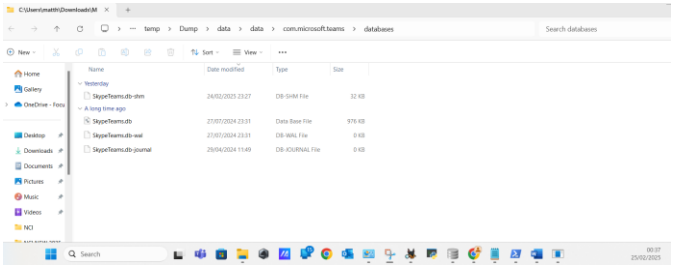
From the teams User log report, I was also able to identify the database for further analysis which was located at:

C:\Users\matth\Downloads\MSC Testing\Test Results\ALEAPP_Reports_2025-02-24_Monday_232753\temp\Dump\data\data\com.microsoft.teams\databases\SkypeTeams.db

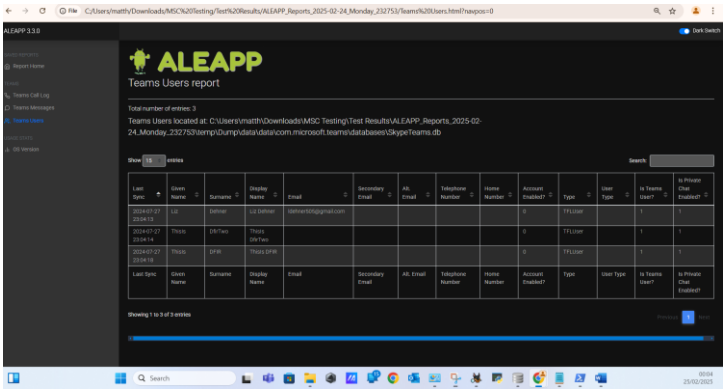
Main location being: temp\Dump\data\data\com.microsoft.teams\databases\SkypeTeams.db

Knowing this location, I will be able to analyse this further with the tool “DB Browser for SQLite Version 3.13.1”

Microsoft Teams Users DB Location

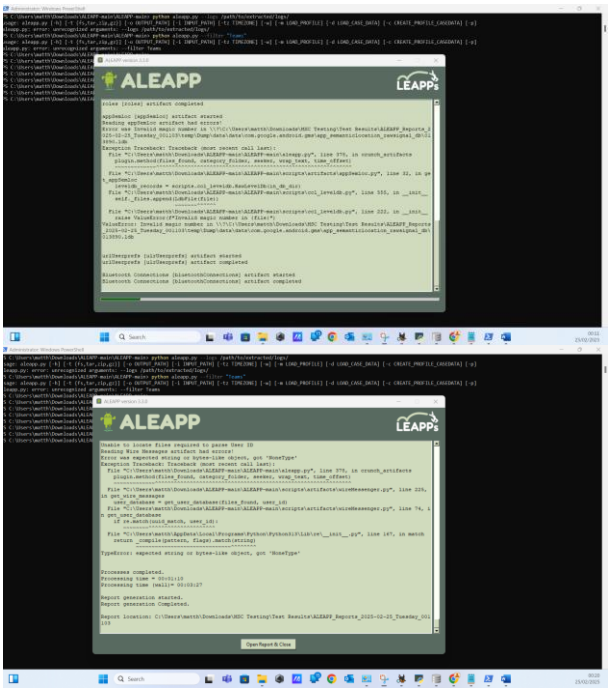


Teams Messages Users report Fig 2.2

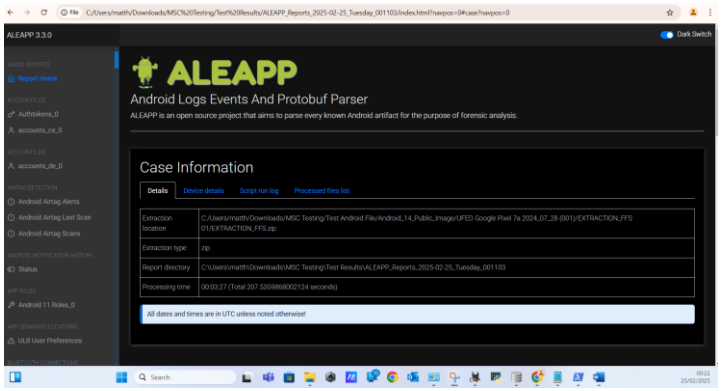


Next, I decided to run the full export against everything just to examine, analyse , and review anything else I may have missed , This did take considerably longer here is the start and finish screenshot of when I did it.

All module report Fig 2.3



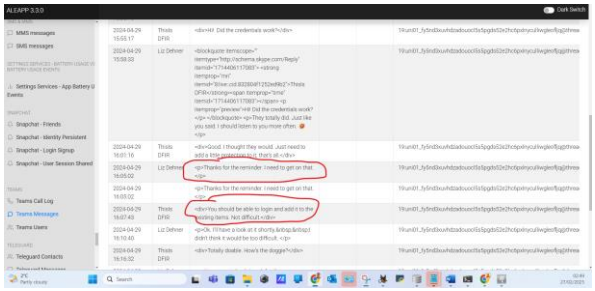
With the more detailed report I was able to delve into the analysis further with Aleapp



Some other examples within Aleapp in general for Artifacts finds were outside of Teams.

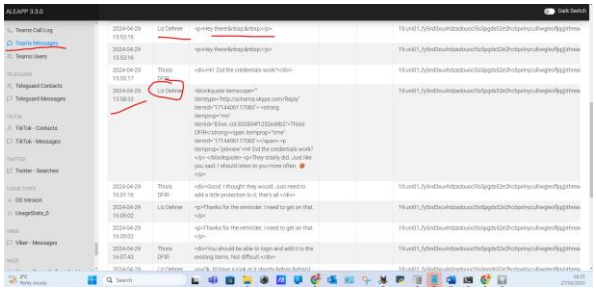
Aleapp Sample 01 Analysis

Teams Messages extracted using Aleapp 01.



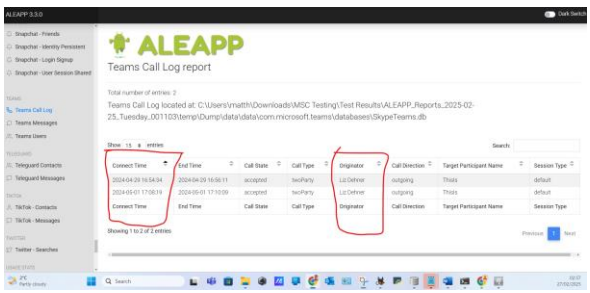
Aleapp Sample 02 Analysis

Teams Messages extracted using Aleapp 02.



Aleapp Sample 03 Analysis

Teams Calls extracted using Aleapp 03.

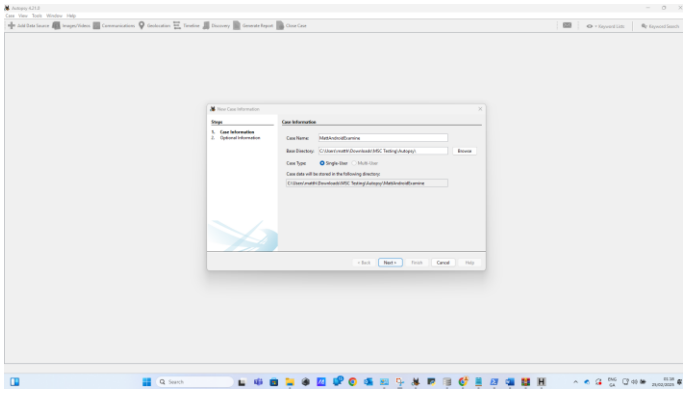


The next thing I wanted to do was to also test out the features using Autopsy

I installed Autopsy, set a default data location e.g. below.

I created a case named: MatthewAndroidExamine

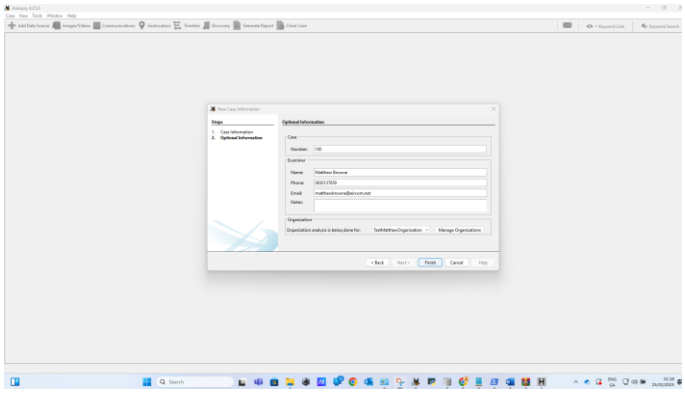
This case had a base directory of C:\Users\matth\Downloads\MSC Testing



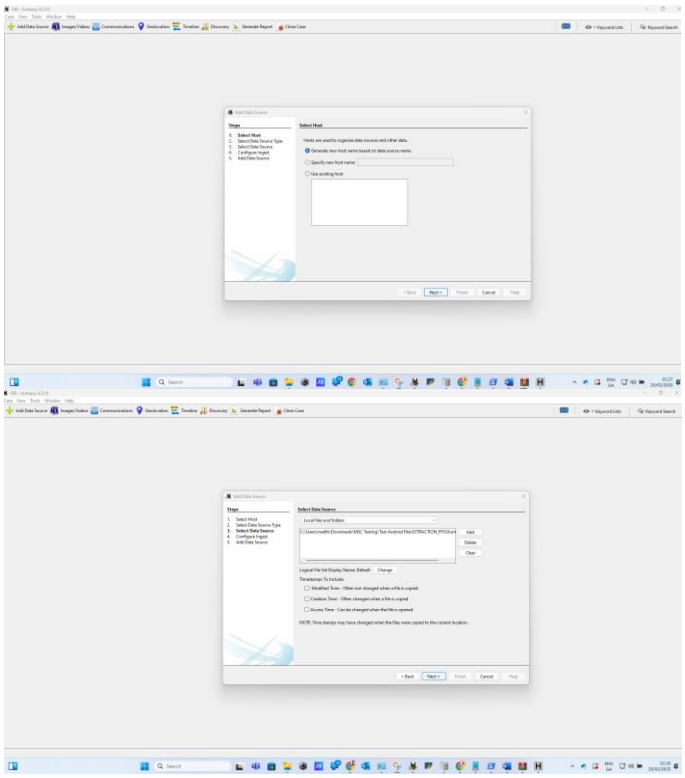
Next, I created the following Case details

Provide a Case Number of 100
Examiner Information was

- Name: Matthew Browne
- Phone: 0830137659
- Email: matthewbrowne@eircom.net
- Organisation analysis is being done for: Test Matthew Organisation



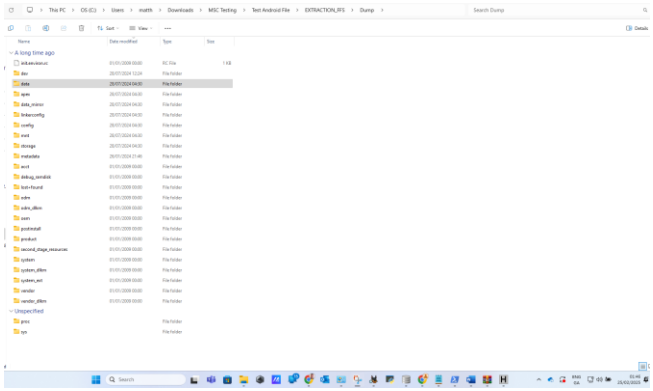
I went through the process of generating a new hostname then I chose logical files as my data source.



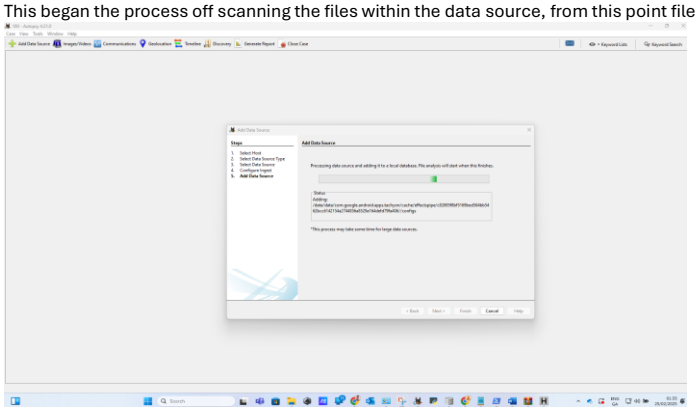
I pointed my data source to the. Tar image which I had extracted into:

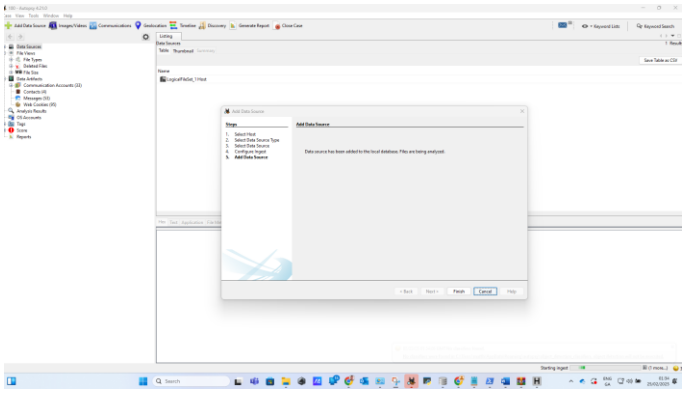
C:\Users\matth\Downloads\MSC Testing\Test Android File\EXTRACTION_FFS\Dump

I ensured it was pointing at the Data folder, as this is the folder It needs to read for Autopsy to parse through all files.

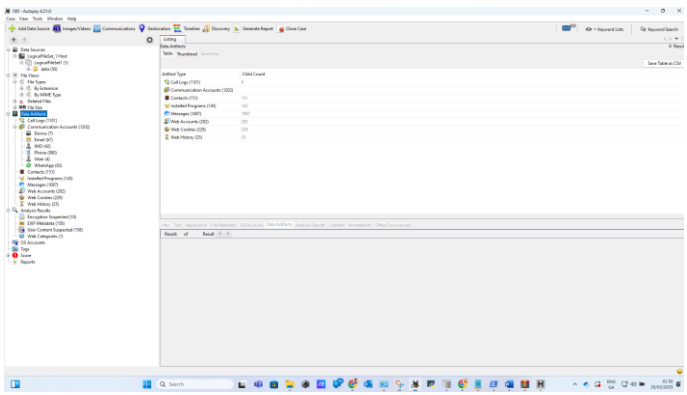


This began the process off scanning the files within the data source, from this point file analysis began.





Once file analysis completed, I ended up with the below in Autopsy



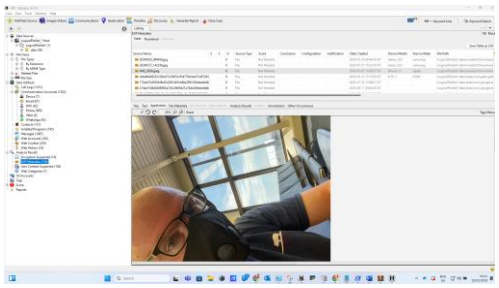
From here I was able to explore in even more detail what was on the android device.

In general, e.g. I was able to pull this image from the data and many more just like it.

Some Examples.

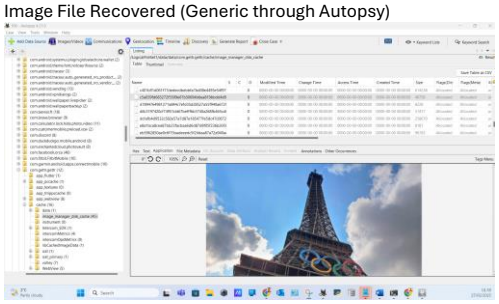
Sample – A Analysis

Image File Recovered (Generic through Autopsy)



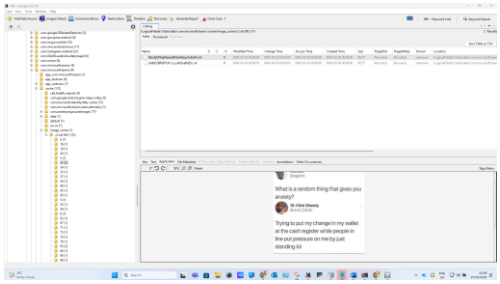
Sample – B Analysis

Image File Recovered (Generic through Autopsy)



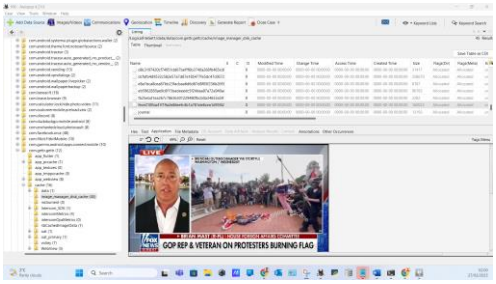
Sample – C Analysis

Image File Recovered (Generic through Autopsy)



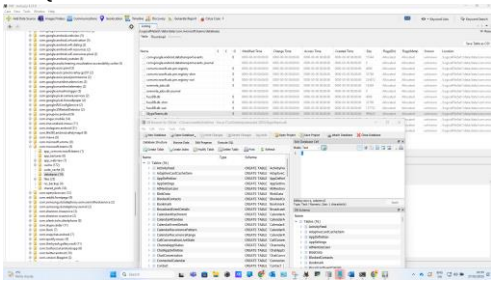
Sample – D Analysis (Team's Specific through Autopsy)

Extraction of SkypeTeams.db through autopsy into DB Browser for SQL Lite.



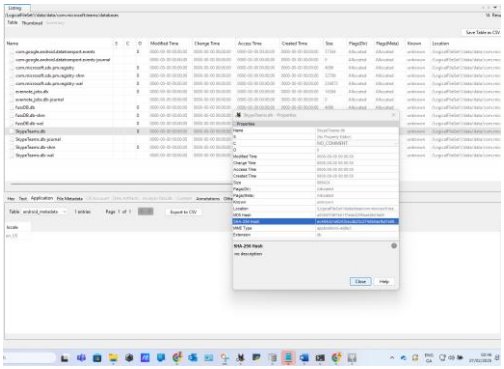
Sample – E Analysis (Team's Specific through Autopsy)

Extraction of image from Teams cache through autopsy



Sample – F Analysis (Team's Specific through Autopsy)

Extraction of SHA 256 Hash Teams through autopsy

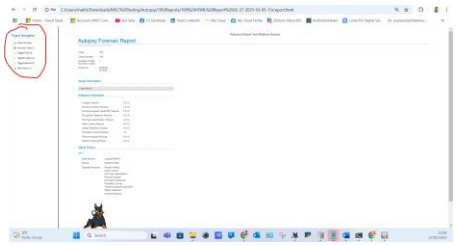


In general, the Overall Main Artifacts I found were located in different sections of the android operating system and users data folder .

- User Chat information and log files these were located in
  TeamsChat.database, File Type Database, Database Table Name
- User Call information log and log files, these were located in:
  Call History.database, File Type Database, Database Table Name
- Android os teams' storage (Default location), these were located in:
  /data/data/com.microsoft.teams/, File Type Database, Database Table Name

- MS Team Application logs, these were located in:
  Log-cat, File Type Database

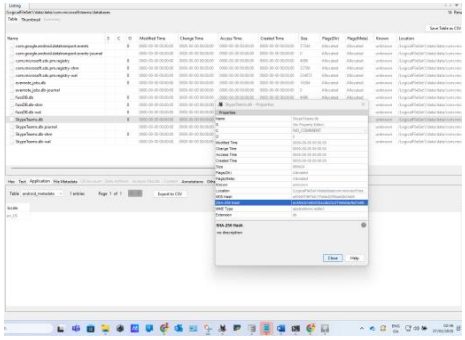
As a Plus one After testing out Autopsy I also tested the Reporting feature in Autopsy which turned out like below adding in some notable artifacts like, images, links and messages.



Computing Hash Files of Data

A sample of a computing hash would be the one I've extracted from the team's database located on my android phone. With this hash you could then use a tool like "Hashab" from boi to verify the hash value and do a comparison, this is very much common practice for companies uploading payroll files to banks for running payments on pay day. (BankOfIreland, 2025)

Teams Hash for chat database.

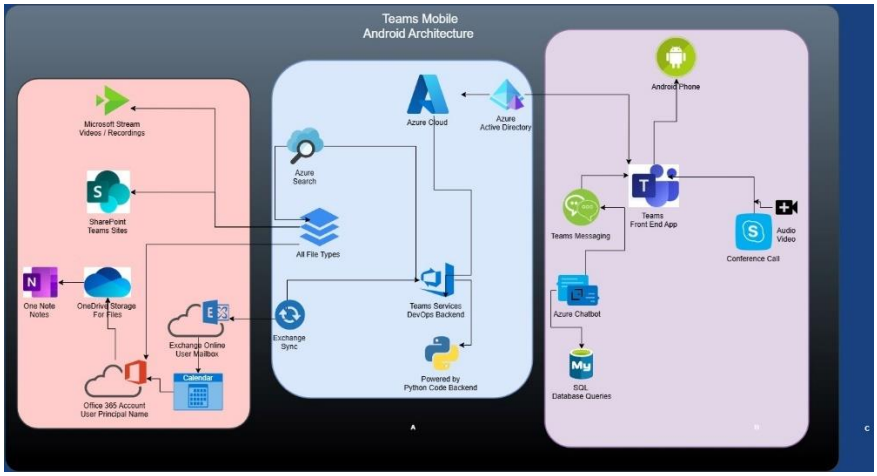


Team's Architecture

Diagram Of Teams Mobile Application.

My Take on the Architecture Diagram of the Team's application, based of research from the article

"Ignite–Get an overview of Microsoft Teams architecture Session Summary" (Boam's, 2017)



Team's App Behaviour

1. Behaviour of the application and detail.

   (interaction with os, files, network, main purpose of app (what its used for)

Team App Recommendations

Use for Teams in an organisation / enterprise environment (Microsoft , 2025)	Microsoft teams is used in small and medium sized organisations alongside enterprise organisations. The business use case is it allow an organisation and its employees to communicate on a single platform that's tied in with there office 365 and active directory account or what's known as their identity in the organisation. Teams can be centrally managed through office 365 admin centre and allows for a unified experience of communication across the organisations office 365, azure and SharePoint backend systems.
Types of use for Teams in an organisation / enterprise environment (Microsoft, 2025)	Employees can • Instant chat. • Setup meetings. • Share documents, presentations, forms. • Send calendar invites for webinars and meetings. • Collaborate across there different teams.
Team's Forensic Specific Use Cases	Where teams is rolled out in an organisation while it enriches the employee's life it also adds additional artifacts for discovery should a forensic investigation need to be conducted. Some of the specific use cases to include would be • Forensically analysing chat messages. • Forensically analysing content shared across the platform. • Forensically analysing timelines for messages and calls. • Forensically analysing data leakage probabilities and score. • Essentially adding significant content analysis across the platform for the forensic examiner.

Conclusion

Overall discussion of finding's

Overall, the finding's for the exercise and key outputs I took were that there's no single application which provided a best in bread practice , or a golden bullet that states you must use x software to get y result , ultimately forensics is game of utilising your skills set and solving problems that have had no solution before , your experience around IT and the multifaceted disciplines will determine your level of understanding , having hands on training and certification will be advantageous when seeking roles as a forensic examiner , I found there were many paid and free applications which can be helpful when conducting the analysis , guiding principals are a must when conducting forensics and chain of evidence is key , this was well drilled in with Autopsy and Aleapp I was also able to acknowledge that the ISC2 SSCP certification and CompTIA SecurityX And CySA+ domains crossed paths allot with the tooling and techniques covered , already having exposure helped a bit more in configuration of my lab testing and analysis , ultimately forensics is changing rapidly and the art of the possible is growing so continued professional development is key in conducting forensics analysis alongside ensuring integrity across evidence collected is maintained.

limitations and implications

Overall, the limitations on toolsets,

I did find that after drilling into both Aleapp and Autopsy that they didn't fully provide some of the functionality I was expecting a unified solution with a visual representation of the device being examined would have been a plus. I also found that due to the different states of forensic acquisition one would need to understand or have a list of toolsets which are aligned closer to the job tasks and analysis. Some of the limitations of the applications included a nice Gui while Aleapp opted for a simpler gui checklist once running and Autopsy looked dated I felt there was functionality missing out of both even after running reports and more , easily viewing content as the user would see it would have been a nice touch in the reports example my android phone should have been virtualised where to the point I could see as I was performing the forensic analysis what it looked like on the phone rather than lines of folders and nested folders etc. other functionality like making comments highlighting content was either not easy in autopsy or non-existent in Aleapp , so again two other functions which lacked intuitive dashboards and reporting.

Overall, the implications on the forensic examiner

Based on the findings and the research from what I could see is, there allot of tooling's available for both open-source software and paid forensic software. Analysis of the documentation and video's in our Moodle made it abundantly clear we should be aware that a specialist image exists for Linux with the tools pre-installed ready to go but not every tool will be required sometimes you need to match up the job task analysis based the requirements to be achieved for the role or analysis of artifacts , I also learned that each operating system may

require its own tool example Ileap is used in windows operating system for windows logs and more so again different tools for different purposes and roles.

Next steps If I had additional Time

If I had additional time, I would have liked to explore autopsy more and understand how its timeline option works alongside notable items selections and creation process , additional time understanding how to do this would have been nice , I would have also liked to spend some time with the Linux specific images which had the tools preloaded and get to know them , I have a keen interest in parsing through encrypted files and stenography and would have also loved to explore that avenue. Getting some hands-on intense sessions with our lecturer on forensics would have been nice for example exams like oscp from offensive security test you on pen testing and forensics analysis and capture the flag, getting hands on and doing some of those labs in call would have provided a variety of learning outcomes and skilling opportunities alongside a breadth of exposure to real world forensics and pen testing. Ultimately just having more time with doing this discovery and analysis would have been nice as I felt ultimately the given time frame was shorter then expected.

References

Abrignoni, B., 2023. https://github.com/abrignoni/ALEAPP. [Online]
Available at: https://github.com/abrignoni/ALEAPP
[Accessed 24th February 2025].
Anon., Unknown. 9d82c6b2-d28c-441a-b165-e73b1a87736f/FORC%20Book%207.pdf. [Online]
Available at: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/9d82c6b2-d28c-441a-b165-e73b1a87736f/FORC%20Book%207.pdf
[Accessed 25th February 2025].
autopsy.com, 2024. https://www.autopsy.com/about/. [Online]
Available at: https://www.autopsy.com/about/
[Accessed 24th February 2025].
BankOfIreland, 2025. https://businessbanking.bankofireland.com/business-online-payments/hashtab/. [Online]
Available at: https://businessbanking.bankofireland.com/business-online-payments/hashtab/
[Accessed 27th February 2025].
Boam's, M., 2017. Ignite–Get an overview of Microsoft Teams architecture Session Summary. [Online]
Available at: https://ucmart.uk/2017/09/28/ignite-get-an-overview-of-microsoft-teams-architecture-session-summary/
[Accessed 27th February 2025].
Cellbrite, 2022. aleapp-for-android-devices-parsing-even-more-data. [Online]
Available at: https://cellebrite.com/en/aleapp-for-android-devices-parsing-even-more-data/
[Accessed 25th February 2025].
Check Point , 1994. cyber-hub/threat-prevention/what-is-sandboxing. [Online]
Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/#:~:text=Sandboxing%20is%20a%20cybersecurity%20practice,inspect%20untested%20or%20untrusted%20code.
[Accessed 26th February 2025].
cyber5w.com, 2025. Guide to Mobile Forensics with ALEAPP. [Online]
Available at: https://blog.cyber5w.com/a-guide-to-mobile-forensics-with-aleapp
[Accessed 25th February 2025].
dfir.science, 2022. Fast Android forensic triage with ALEAPP. [Online]
Available at: https://www.youtube.com/watch?v=_cm1n0stVrA
[Accessed 25th February 2025].
dfir.science, 2022. https://dfir.science/research. [Online]
Available at: https://dfir.science/research
[Accessed 25th February 2025].
Garfinkel, S., 2025. https://corp.digitalcorpora.org/corpora/mobile/android_14/. [Online]
Available at: https://corp.digitalcorpora.org/corpora/mobile/android_14/
https://learn.microsoft.com, 2024. What is PowerShell?. [Online]
Available at: https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.5
[Accessed 24th February 2025].
isc2, 1989. https://www.isc2.org/about. [Online]
Available at: https://www.isc2.org/about
[Accessed 27th February 2025].
isc2, 1989. https://www.isc2.org/certifications/sscp. [Online]
Available at: https://www.isc2.org/certifications/sscp
[Accessed 27th February 2025].
isc2, 1994. https://www.isc2.org/ethics. [Online]
Available at: https://www.isc2.org/ethics
[Accessed 27th February 2025].
isc2, 2024. https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-English.pdf. [Online]
Available at: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-English.pdf
[Accessed 27th February 2025].
Lwin, H. H., Aung, W. P. & Lin, K. K., 202. Comparative Analysis of Android Mobile Forensics Tools. [Online]
Available at: https://ieeexplore.ieee.org/abstract/document/9022838/authors#authors
[Accessed 26th February 2025].
magnetforensics.com, 2025. https://www.magnetforensics.com/. [Online]
Available at: https://www.magnetforensics.com/
[Accessed 26th February 2025].
Microsoft , 2024. Understand the usage of virtual networks and VLANs. [Online]
Available at: https://learn.microsoft.com/en-us/windows-server/networking/sdn/manage/understanding-usage-of-virtual-networks-and-vlans
[Accessed 27th February 2025].
Microsoft , 2025. Microsoft Teams for enterprise. [Online]
Available at: https://www.microsoft.com/en-ie/microsoft-teams/enterprise#:~:text=Empower%20your%20team%20to%20connect,closer%20to%20what%20matters%20most.&text=Manage%20your%20email%2C%20calendar%2C%20tasks,contacts%20together%20in%20one%20place.&text=Work%20smarter%20
[Accessed 27th February 2025].

Microsoft , 2025. VPN connection types. [Online]
Available at: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/vpn/vpn-connection-type
[Accessed 27th February 2025].
Microsoft, 1991. https://www.microsoft.com/en-ie/windows/windows-11?r=1. [Online]
Available at: https://www.microsoft.com/en-ie/windows/windows-11?r=1
[Accessed 26th February 2025].
Microsoft, 2025. Microsoft Teams Enterprise. [Online]
Available at: https://www.microsoft.com/en-us/microsoft-teams/enterprise/teams-enterprise?activetab=pivot:overviewtab
[Accessed 27th February 2025].
National College Of Ireland , 2019. Higher Diploma in Science in Data Analytics. [Online]
Available at: https://www.ncirl.ie/Courses/NCI-Course-Details/course/HDSDA
[Accessed 26 February 2025].
National College Of Ireland , 2019. Postgraduate Diploma in Science in Cybersecurity. [Online]
Available at: https://www.ncirl.ie/Courses/NCI-Course-Details/course/PGDCYBE
[Accessed 26th February 2025].
Prior , M., 2025. Week 4: Mobile Forensics.. [Online]
Available at: https://moodle2024.ncirl.ie/course/section.php?id=37018
[Accessed 25th February 2025].
Prior, M., 2025. Forensics and eDiscovery (PGDCYB_JAN25). [Online]
Available at: https://moodle2024.ncirl.ie/course/view.php?id=1894
[Accessed 25th February 2025].
Prior, M., 2025. Week 3: Forensics Tools. [Online]
Available at: https://moodle2024.ncirl.ie/course/section.php?id=37017
[Accessed 25th February 2025].
python.org, 2025. python.org. [Online]
Available at: https://www.python.org/
[Accessed 24th February 2025].
Qualifax, 2023. Programming & Software Development - Pre University. [Online]
Available at: https://www.qualifax.ie/course/39
[Accessed 26th February 2025].
SANS, 2024. Getting Started in Digital Forensics. [Online]
Available at: https://sansorg.egnyte.com/dl/jp9c9WRyNe
[Accessed 26th February 2025].
sqlitebrowser.org, 2023. https://sqlitebrowser.org/. [Online]
Available at: https://sqlitebrowser.org/
[Accessed 24th February 2025].
UCD.ie, 2025. PhD Computer Science NFQ Level 10. [Online]
Available at: https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=COURSE&MAJR=T113&KEYWORD=t113
[Accessed 26th February 2025].
wikipedia , 2021. Windows 11. [Online]
Available at: https://en.wikipedia.org/wiki/Windows_11
[Accessed 27th February 2025].
wikipedia, 2001. wikipedia.org/wiki/Windows_11. [Online]
Available at: https://en.wikipedia.org/wiki/Windows_11
[Accessed 26th February 2025].
ycsc.org.uk, 2024. Mobile Forensics. [Online]
Available at: https://ycsc.org.uk/mobile-forensics/#:~:text=ALEAPP%20and%20iLEAPP%20is%20an,use%20it%20on%20Kali%20Linux.
[Accessed 27th February 2025].

Appendix

Bibliography

Abrignoni, B., 2023. https://github.com/abrignoni/ALEAPP. [Online]
Available at: https://github.com/abrignoni/ALEAPP
[Accessed 24th February 2025].
Anon., Unknown. 9d82c6b2-d28c-441a-b165-e73b1a87736f/FORC%20Book%207.pdf. [Online]
Available at: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/9d82c6b2-d28c-441a-b165-e73b1a87736f/FORC%20Book%207.pdf
[Accessed 25th February 2025].
autopsy.com, 2024. https://www.autopsy.com/about/. [Online]
Available at: https://www.autopsy.com/about/
[Accessed 24th February 2025].
BankOfIreland, 2025. https://businessbanking.bankofireland.com/business-online-payments/hashtab/. [Online]
Available at: https://businessbanking.bankofireland.com/business-online-payments/hashtab/
[Accessed 27th February 2025].
Boam's, M., 2017. Ignite–Get an overview of Microsoft Teams architecture Session Summary. [Online]
Available at: https://ucmart.uk/2017/09/28/ignite-get-an-overview-of-microsoft-teams-architecture-session-summary/
[Accessed 27th February 2025].
Cellbrite, 2022. aleapp-for-android-devices-parsing-even-more-data. [Online]
Available at: https://cellebrite.com/en/aleapp-for-android-devices-parsing-even-more-data/
[Accessed 25th February 2025].
Check Point , 1994. cyber-hub/threat-prevention/what-is-sandboxing. [Online]
Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/#:~:text=Sandboxing%20is%20a%20cybersecurity%20practice,inspect%20untested%20or%20untrusted%20code.
[Accessed 26th February 2025].
cyber5w.com, 2025. Guide to Mobile Forensics with ALEAPP. [Online]
Available at: https://blog.cyber5w.com/a-guide-to-mobile-forensics-with-aleapp
[Accessed 25th February 2025].
dfir.science, 2022. Fast Android forensic triage with ALEAPP. [Online]
Available at: https://www.youtube.com/watch?v=_cm1n0stVrA
[Accessed 25th February 2025].

dfir.science, 2022. https://dfir.science/research. [Online]
Available at: https://dfir.science/research
[Accessed 25th February 2025].
Garfinkel, S., 2025. https://corp.digitalcorpora.org/corpora/mobile/android_14/. [Online]
Available at: https://corp.digitalcorpora.org/corpora/mobile/android_14/
https://learn.microsoft.com, 2024. What is PowerShell?. [Online]
Available at: https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.5
[Accessed 24th February 2025].
isc2, 1989. https://www.isc2.org/about. [Online]
Available at: https://www.isc2.org/about
[Accessed 27th February 2025].
isc2, 1989. https://www.isc2.org/certifications/sscp. [Online]
Available at: https://www.isc2.org/certifications/sscp
[Accessed 27th February 2025].
isc2, 1994. https://www.isc2.org/ethics. [Online]
Available at: https://www.isc2.org/ethics
[Accessed 27th February 2025].
isc2, 2024. https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-English.pdf. [Online]
Available at: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-English.pdf
[Accessed 27th February 2025].
Lwin, H. H., Aung, W. P. & Lin, K. K., 202. Comparative Analysis of Android Mobile Forensics Tools. [Online]
Available at: https://ieeexplore.ieee.org/abstract/document/9022838/authors#authors
[Accessed 26th February 2025].
magnetforensics.com, 2025. https://www.magnetforensics.com/. [Online]
Available at: https://www.magnetforensics.com/
[Accessed 26th February 2025].
Microsoft , 2024. Understand the usage of virtual networks and VLANs. [Online]
Available at: https://learn.microsoft.com/en-us/windows-server/networking/sdn/manage/understanding-usage-of-virtual-networks-and-vlans
[Accessed 27th February 2025].
Microsoft , 2025. Microsoft Teams for enterprise. [Online]
Available at: https://www.microsoft.com/en-ie/microsoft-teams/enterprise#:~:text=Empower%20your%20team%20to%20connect,closer%20to%20what%20matters%20most.&text=Manage%20your%20email%2C%20calendar%2C%20tasks,contacts%20together%20in%20one%20place.&text=Work%20smarter%20
[Accessed 27th February 2025].
Microsoft , 2025. VPN connection types. [Online]
Available at: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/vpn/vpn-connection-type
[Accessed 27th February 2025].
Microsoft, 1991. https://www.microsoft.com/en-ie/windows/windows-11?r=1. [Online]
Available at: https://www.microsoft.com/en-ie/windows/windows-11?r=1
[Accessed 26th February 2025].
Microsoft, 2025. Microsoft Teams Enterprise. [Online]
Available at: https://www.microsoft.com/en-us/microsoft-teams/enterprise/teams-enterprise?activetab=pivot:overviewtab
[Accessed 27th February 2025].
National College Of Ireland , 2019. Higher Diploma in Science in Data Analytics. [Online]
Available at: https://www.ncirl.ie/Courses/NCI-Course-Details/course/HDSDA
[Accessed 26 February 2025].
National College Of Ireland , 2019. Postgraduate Diploma in Science in Cybersecurity. [Online]
Available at: https://www.ncirl.ie/Courses/NCI-Course-Details/course/PGDCYBE
[Accessed 26th February 2025].
Prior , M., 2025. Week 4: Mobile Forensics.. [Online]
Available at: https://moodle2024.ncirl.ie/course/section.php?id=37018
[Accessed 25th February 2025].
Prior, M., 2025. Forensics and eDiscovery (PGDCYB_JAN25). [Online]
Available at: https://moodle2024.ncirl.ie/course/view.php?id=1894
[Accessed 25th February 2025].
Prior, M., 2025. Week 3: Forensics Tools. [Online]
Available at: https://moodle2024.ncirl.ie/course/section.php?id=37017
[Accessed 25th February 2025].
python.org, 2025. python.org. [Online]
Available at: https://www.python.org/
[Accessed 24th February 2025].
Qualifax, 2023. Programming & Software Development - Pre University. [Online]
Available at: https://www.qualifax.ie/course/39
[Accessed 26th February 2025].
SANS, 2024. Getting Started in Digital Forensics. [Online]
Available at: https://sansorg.egnyte.com/dl/jp9c9WRyNe
[Accessed 26th February 2025].
sqlitebrowser.org, 2023. https://sqlitebrowser.org/. [Online]
Available at: https://sqlitebrowser.org/
[Accessed 24th February 2025].
UCD.ie, 2025. PhD Computer Science NFQ Level 10. [Online]
Available at: https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=COURSE&MAJR=T113&KEYWORD=t113
[Accessed 26th February 2025].
wikipedia , 2021. Windows 11. [Online]
Available at: https://en.wikipedia.org/wiki/Windows_11
[Accessed 27th February 2025].
wikipedia, 2001. wikipedia.org/wiki/Windows_11. [Online]
Available at: https://en.wikipedia.org/wiki/Windows_11
[Accessed 26th February 2025].
ycsc.org.uk, 2024. Mobile Forensics. [Online]
Available at: https://ycsc.org.uk/mobile-forensics/#:~:text=ALEAPP%20and%20iLEAPP%20is%20an,use%20it%20on%20Kali%20Linux.
[Accessed 27th February 2025].