



**6G6Z0013: Emerging Issues in Security, Privacy and
Forensics (1CWK40)**

IoT Device Investigation Case Study

Meta Quest 2 VR Headset

Group 7

Mohammed Ahmed Khammas

Lok Wing Lavin Wong

Alexander Shore

Assessment Set By: Dr. Tooska Dargahi

Table of Content

Task 1 – Setting up the Environment & Data Collection:	3
Meta Quest 2 VR Headset	3
Data Collection Methodologies	5
Task 2 – Evidence Analysis:	7
Security	7
Privacy	11
Task 3 – Findings Report and Recommendations:	13
Task 4 – Reflection on Group Activities and (individual marks):	14

Task 1 – Setting up the Environment & Data Collection:

Meta Quest 2 VR Headset

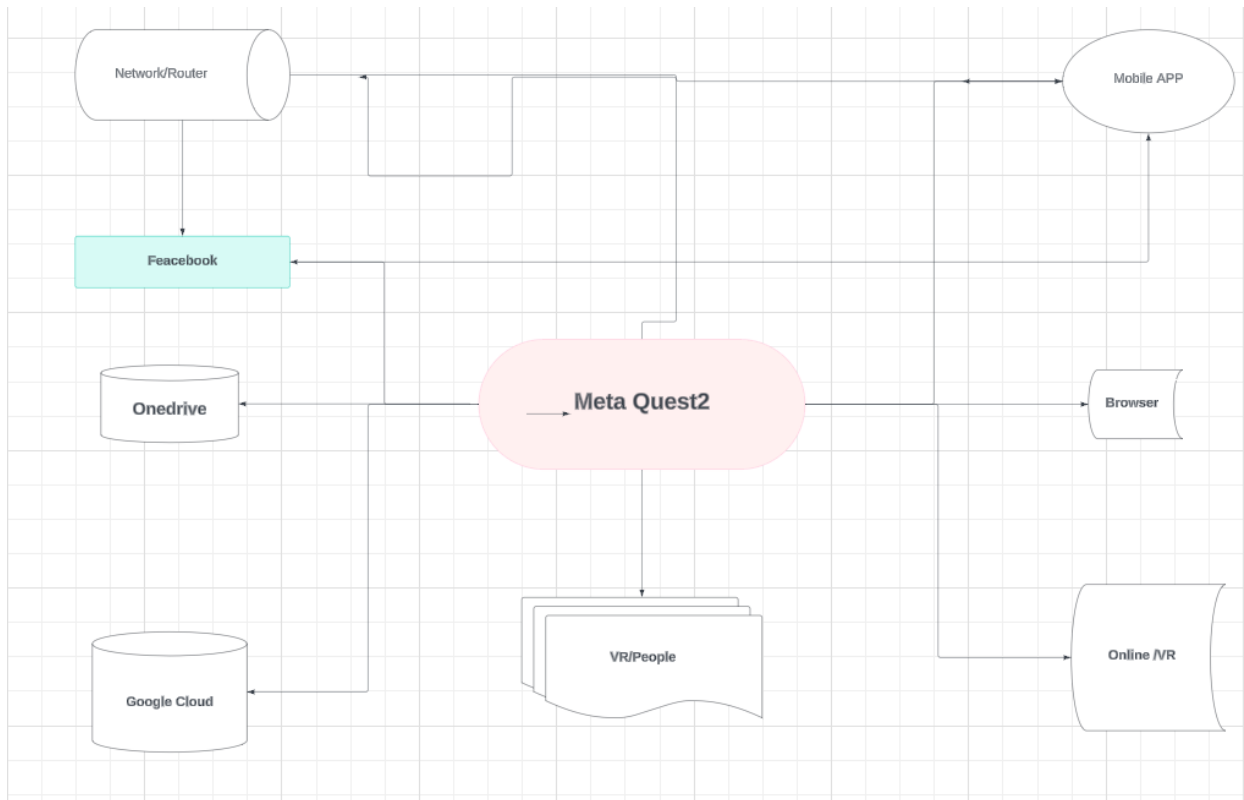


Figure 1: Mind map of how Meta Quest 2 could do and connect

Before we received the IoT device (Meta Quest 2), figure 1 showed our group how Meta Quest 2 may function, including connecting to the internet through a router to access cloud services, online content, and updates. Additionally, it offers a smartphone app for managing applications and watching virtual reality sessions. In addition, the gadget lets users browse the web while in the VR environment, enabling real-time user interaction. The gadget makes avatars for shared experiences and keeps track of the user's movements. Additionally, it syncs user accounts with Facebook, enabling VR activities and sharing material. Lastly, it uses OneDrive to sync and store user data or VR content, enabling accessibility and backup.

Meta Quest 2 VR Headset

Before initiating data collection and testing, we restored the headset to factory default settings and cleared all previous data. We ensured the device ran the latest firmware, including all security and software updates, reflecting the most current user environment. This approach minimises the risk of discovering vulnerabilities that have already been addressed in recent patches and ensures our

findings are relevant to the latest security landscape. By simulating real-world usage conditions, we aimed to identify potential privacy and security issues that could affect users on up-to-date devices (Figure 1), ensuring comprehensive and accurate assessment results.

The Meta Quest 2 pairs with a companion mobile app – Meta Horizon, which is required and functions as the central control hub for the device through the connected mobile phone(s) (Figure 2), Meta account created called ‘gp7tester’. However, data transmitted between the app and the headset may be vulnerable to interception on unsecured networks. To ensure secure communication, it is essential to use encrypted protocols, such as HTTPS, keep the app up to date, and refrain from using the app on public Wi-Fi networks unless a VPN is enabled.

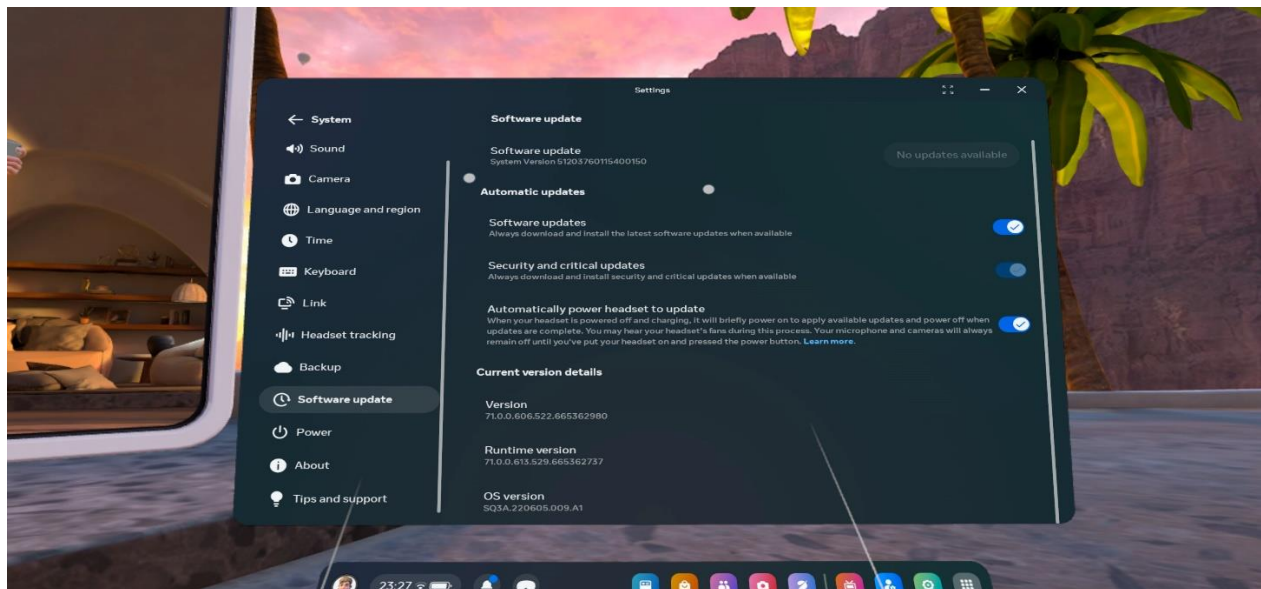


Figure 2: Latest system version of the Meta Quest 2 VR Headset

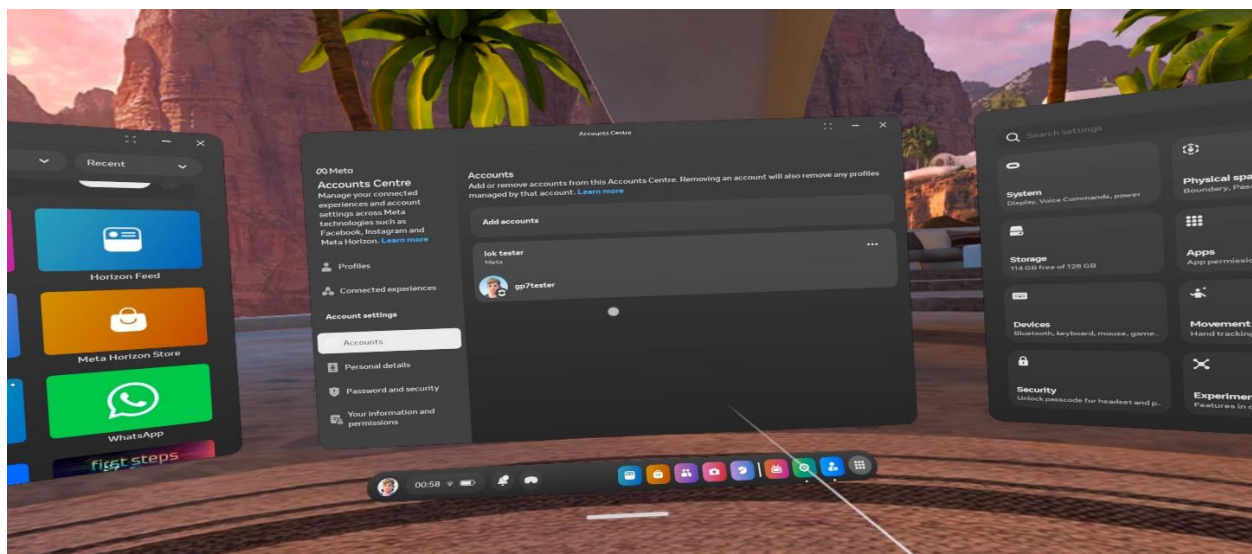


Figure 3: Account setup (with mobile app)

The Meta Quest 2 acts as a central hub for connecting to external systems, which, while enhancing functionality, also expands its potential attack surface. By proactively addressing the security risks associated with each connection, users can substantially mitigate vulnerabilities and ensure a more secure experience.

Data Collection Methodologies

To effectively gather relevant information and network traffic data for the Meta Quest 2 VR headset using a Kali Linux virtual machine, a structured methodology is essential. The process begins with setting up the Kali VM and configuring essential tools such as Wireshark and the Aircrack-ng suite, ensuring proper network configuration and the use of a USB Wi-Fi adapter capable of packet injection. Passive data collection involves monitoring network traffic with Wireshark to capture packets, analyse traffic patterns, and identify potential vulnerabilities or unencrypted data. For active data collection, simulated attacks such as deauthentication (deauth) attacks using Aireplay-ng are conducted to assess network resilience and response. Additionally, enabling Developer Mode on the device provides access to privacy and security settings for further inspection. Finally, the collected data is analysed to identify vulnerabilities, correlate findings with known threats, and document key insights, ensuring that all testing activities remain ethical and compliant. This comprehensive approach ensures a thorough evaluation of the Meta Quest 2's network security and privacy posture.

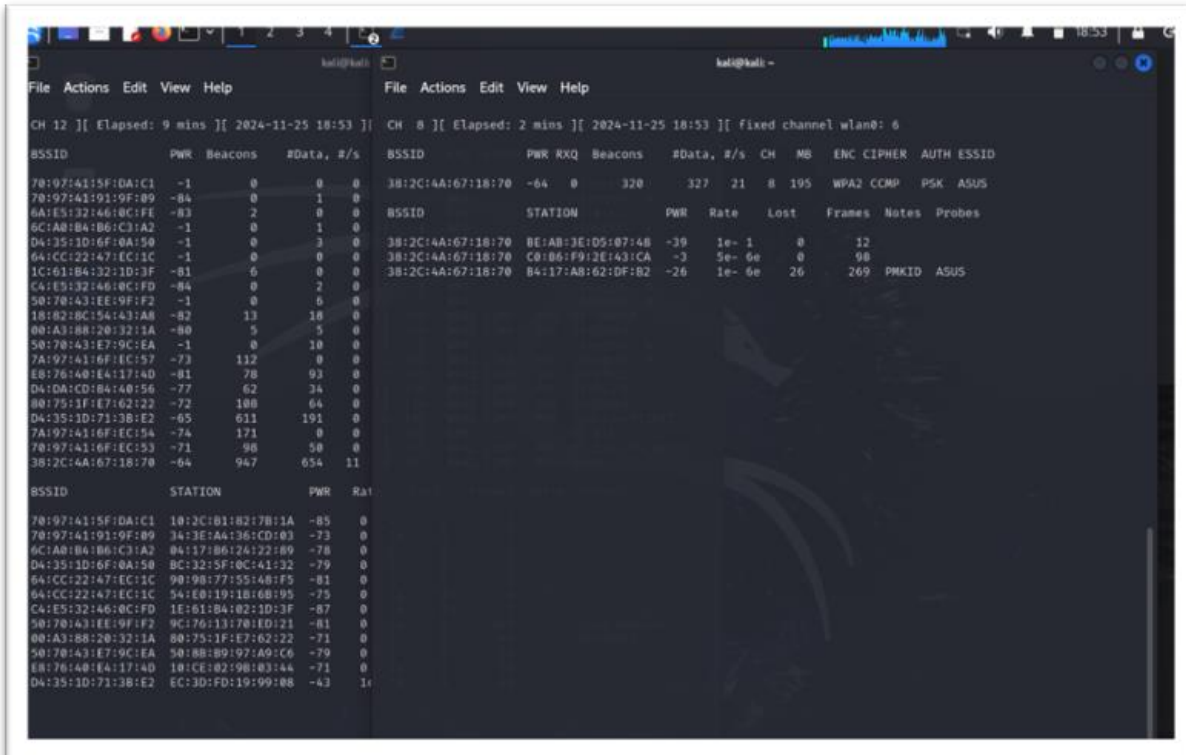
```
kali@kali: ~  
File Actions Edit View Help  
$ sudo airmon-ng check kill  
Killing these processes:  
PID Name  
4713 wpa_supplicant  
  
(kali@kali)-[~]  
$ sudo ifconfig wlan0 up  
  
(kali@kali)-[~]  
$ iwconfig  
lo      no wireless extensions.  
eth0    no wireless extensions.  
wlan0    IEEE 802.11  ESSID:off/any  
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm  
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off  
          Power Management:off  
  
(kali@kali)-[~]  
$ sudo ifconfig wlan0 down  
  
(kali@kali)-[~]  
$ sudo iwconfig wlan0 mode monitor  
  
(kali@kali)-[~]  
$ sudo ifconfig wlan0 up  
  
(kali@kali)-[~]  
$ iwconfig  
lo      no wireless extensions.  
eth0    no wireless extensions.  
wlan0    IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm  
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off  
          Power Management:off
```

Figure 4: Configuration and setup for the wireless adapter for wireless network attack

Task 2 – Evidence Analysis:

Security

According to impact analysis, security and privacy risks have the potential to compromise user data's Confidentiality, Integrity, and Availability (CIA). Information disclosure exposes personal information, harming confidentiality. Local storage manipulation may compromise data integrity, and a successful denial-of-service attack could impact availability, making the headset unusable or reducing the quality of virtual reality experiences.



BSSID	PWR	Beacons	#Data, #/s
78:97:41:5F:DA:C1	-1	0	0 0
78:97:41:5F:DA:C1	-84	0	1 0
6A:1E:52:46:0C:FE	-83	2	0 0
6C:1A:84:B6:C3:A2	-1	0	1 0
DA:35:1D:6F:0A:50	-1	0	3 0
6A:1E:52:46:0C:FE	-1	0	0 0
1C:61:84:32:1D:3F	-81	6	0 0
CA:1E:52:46:0C:FE	-84	0	2 0
50:70:43:EE:9F:F2	-1	0	6 0
18:82:8C:54:43:A8	-82	13	18 0
80:A3:88:20:32:1A	-80	5	5 0
50:70:43:E7:9C:EA	-1	0	10 0
7A:97:41:6F:EC:57	-73	112	0 0
E8:76:40:E4:17:4D	-81	78	93 0
DA:10A:CD:84:A8:56	-77	62	34 0
80:75:1F:E7:62:22	-72	188	64 0
DA:35:1D:71:3B:E2	-65	611	191 0
7A:97:41:6F:EC:54	-74	171	0 0
78:97:41:6F:EC:53	-71	98	58 0
38:12C:4A:67:18:70	-64	947	654 11

BSSID	STATION	PWR	Rate
78:97:41:5F:DA:C1	10:2C:81:82:7B:1A	-85	0
78:97:41:5F:DA:C1	34:3E:AA:36:CD:03	-73	0
6C:1A:84:B6:C3:A2	04:17:B6:26:12:89	-78	0
DA:35:1D:6F:0A:50	BC:32:5F:0C:41:32	-79	0
6A:1E:52:46:0C:FE	90:98:77:55:48:F9	-81	0
6A:1E:52:46:0C:FE	5A:E0:19:1B:68:95	-75	0
CA:1E:52:46:0C:FE	1E:61:BA:02:1D:3F	-87	0
50:70:43:EE:9F:F2	9C:76:13:70:1E:21	-81	0
80:A3:88:20:32:1A	80:75:1F:E7:62:22	-71	0
50:70:43:E7:9C:EA	50:88:B9:97:A9:C6	-79	0
E8:76:40:E4:17:4D	10:CE:02:9B:03:44	-71	0
DA:35:1D:71:3B:E2	EC:3D:FD:19:99:08	-43	1e

Figure 5: Network Active Reconnaissance

According to figure 4, the airodump-ng tool as part of the Aircrack-ng suite, is used for wireless reconnaissance and provides real-time data on nearby wireless networks. It displays essential details such as the access point (AP) BSSID (namely ASUS), signal strength (PWR), encryption type, and the number of connected clients. This information is valuable for identifying networks that may be vulnerable due to weak configurations or insufficient security measures. The screenshot illustrates a network operating on Channel 8 with WPA2-PSK encryption, which is selected for further testing. Additionally, airodump-ng highlights connected stations, enabling targeted attacks on specific clients or access points. The scanning process is efficient and provides a comprehensive view of the wireless environment, facilitating the selection of a network for testing, such as the one using WPA2 encryption on Channel 8.

The MAC address B4:17:AB:62:DF:B2 associated with the Meta Quest 2 VR Headset, and it is the targeted client to perform wireless network attack. (Shown in Figure 5)

```

kali@kali:~$ sudo aireplay-ng --deauth 1666 -a 38:2C:4A:67:18:70 -c B4:17:AB:62:DF:B2 wlan0
18:59:16 Waiting for beacon frame (BSSID: 38:2C:4A:67:18:70) on channel 12
18:59:17 wlan0 is on channel 12, but the AP uses channel 8
18:59:20 Waiting for beacon frame (BSSID: 38:2C:4A:67:18:70) on channel 12
18:59:20 wlan0 is on channel 12, but the AP uses channel 8
18:59:22 Waiting for beacon frame (BSSID: 38:2C:4A:67:18:70) on channel 3
18:59:22 wlan0 is on channel 3, but the AP uses channel 8
18:59:23 Waiting for beacon frame (BSSID: 38:2C:4A:67:18:70) on channel 11
18:59:24 wlan0 is on channel 11, but the AP uses channel 8
18:59:25 Waiting for beacon frame (BSSID: 38:2C:4A:67:18:70) on channel 8
18:59:26 Sending 64 directed DeAuth (code 7). STMAC: [B4:17:AB:62:DF:B2] [ 0] 0 ACKs
18:59:26 Sending 64 directed DeAuth (code 7). STMAC: [B4:17:AB:62:DF:B2] [ 0] 0 ACKs
18:59:27 Sending 64 directed DeAuth (code 7). STMAC: [B4:17:AB:62:DF:B2] [ 0] 1 ACKs
18:59:27 Sending 64 directed DeAuth (code 7). STMAC: [B4:17:AB:62:DF:B2] [14] 19 ACKs
19:01:10 Sending 64 directed DeAuth (code 7). STMAC: [B4:17:AB:62:DF:B2] [40] 63 ACKs
19:01:58 Sending 64 directed DeAuth (code 7). STMAC: [B4:17:AB:62:DF:B2] [24] 30 ACKs

```

Figure 6: Deauthentication attack via Kali Linux

According to figure 5, a deauthentication (deauth) attack is demonstrated to disconnect the network between the Meta Quest 2 and the AP (ASUS). In Kali Linux, the attack is executed using the aireplay-ng tool to disconnect clients from a wireless network. It exploits a Wi-Fi standard flaw, allowing attackers to force users onto rogue networks or interrupt their connections. The process involves a wireless adapter's channel mismatch with the target AP's channel, and the tool provides feedback to align the adapter to Channel 8. After switching to Channel 8, the tool successfully sends deauth frames, causing the client to disconnect from the AP.

Deauth attack is a form of denial-of-service (DoS) attack that targets the communication between a client device and an access point. By sending forged deauthentication frames, the attacker can force the client to disconnect from the network, thereby disrupting the connection and temporarily interrupting access to the network service. This type of attack can lead to significant service disruptions and impact the availability and reliability of wireless networks (Aggrawal et al, 2023). Deauth attacks can have various malicious purposes, such as intercepting traffic, denying service to legitimate users, or gaining access to a pre-shared key. This process demonstrates how easily a

device can be kicked off a network and how attackers can exploit this type of attack. Deauth attack result is shown as below with figure 6 and 7:



Figure 7: Meta Quest 2 is still connecting to internet (before deauth attack)

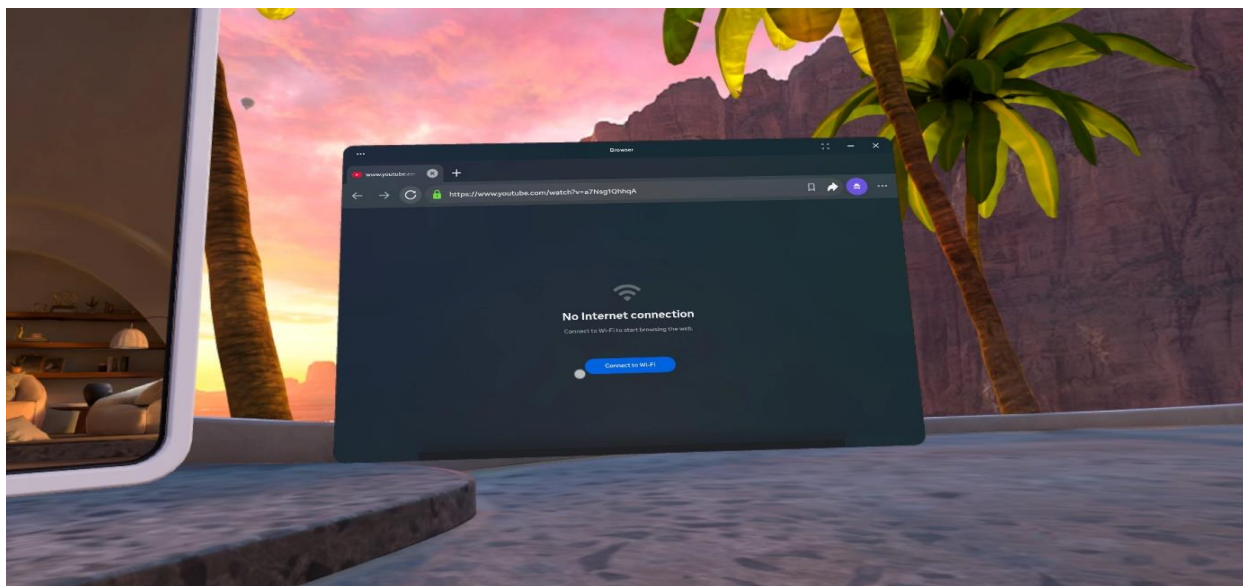


Figure 8: Meta Quest 2 is disconnected from internet (DoS occurred after deauth attack)

The Meta Quest 2 without a passcode introduces significant security vulnerabilities that can compromise user safety and privacy. First and foremost, the absence of a passcode facilitates unauthorised access; anyone with physical possession of the device can operate it without restriction, posing a risk of disruption or misuse. Additionally, there is an increased risk of potential

exploitation, where an individual could engage in activities such as playing games or using applications in ways that may result in unauthorised purchases or violations of terms of service. Finally, the security of the user's account and payment details is jeopardised. Without a passcode, an attacker who gains access to the device could log into the associated Meta account, make changes to account settings, and potentially initiate financial transactions.

Figures 9 and 10 illustrate the security configurations both without and with a passcode, highlighting the difference in protection levels for the headset.

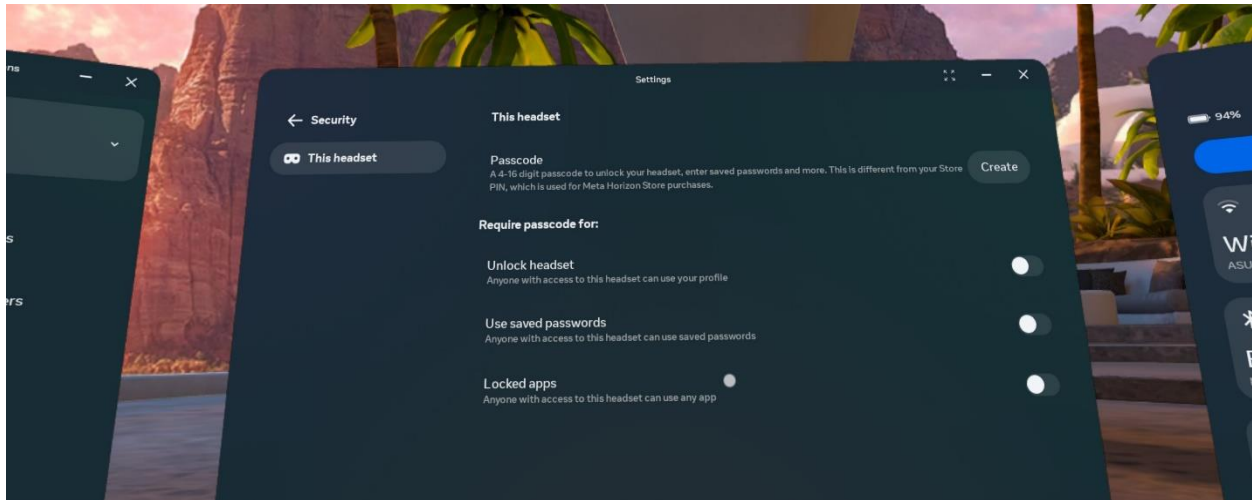


Figure 9: Passcode setting of the Meta Quest 2 headset (no passcode when set up)



Figure 10: Passcode setting of the Meta Quest 2 headset (passcode created for security)

Privacy

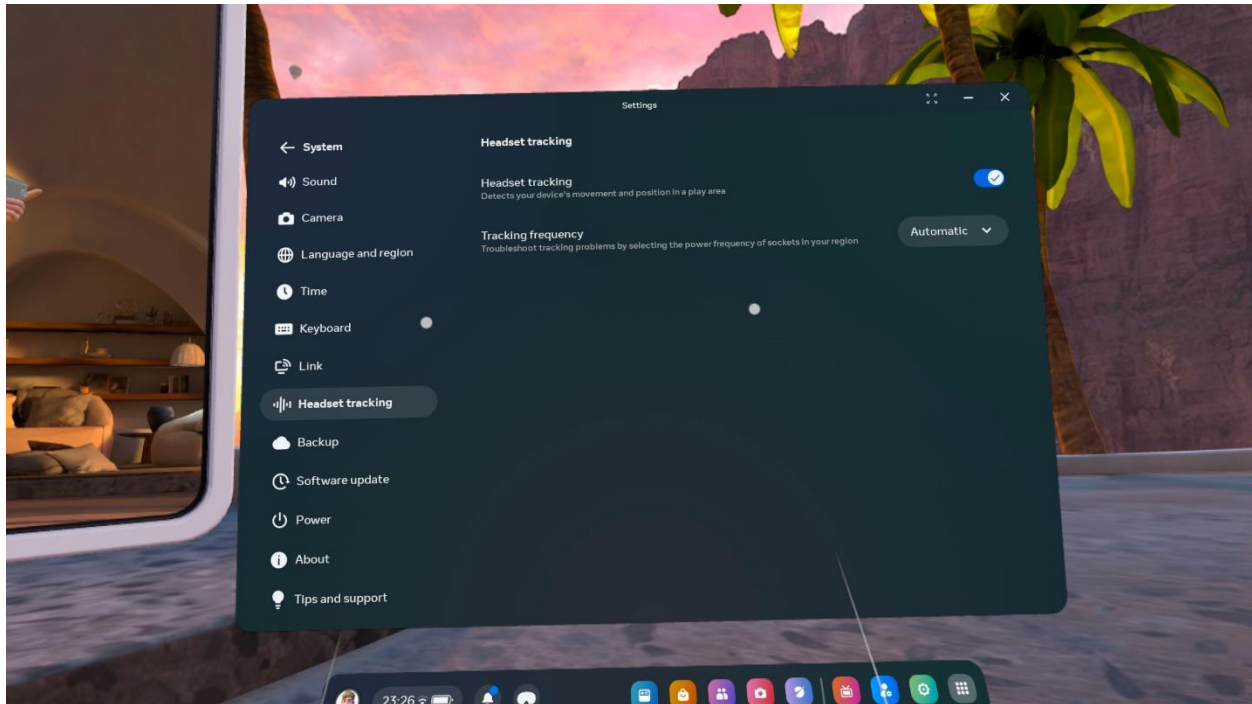


Figure 11: Headset tracking settings



Figure 12: Hands (Controllers) tracking settings

From figure 11 and 12, the VR headset's tracking capabilities introduce considerable privacy concerns. The continuous collection of biometric data such as body movements, hand gestures, and spatial positioning, poses a significant risk if not adequately secured. Compromised access to this sensitive information could facilitate unauthorised profiling or behavioural surveillance, particularly following a data breach or if the data is improperly shared with unverified third parties. Additionally, persistent monitoring of physical interactions increases the attack surface, potentially exposing personal information without explicit user consent. The absence of transparency regarding data retention policies, encryption standards, and third-party access raises further concerns about data governance and long-term security.

Researchers at the University of California found that artificial intelligence can accurately infer personal information such as height, weight, age, and marital status based on user movements during virtual reality (VR) experiences. This data can be collected without users explicitly providing these details, raising concerns about privacy risks. The study demonstrated that AI achieved over 94% accuracy in identifying individuals from a group of 50,000 VR users, using just 200 seconds of motion data. (Henry, 2023)

The findings underscore the need for enhanced privacy measures in VR platforms to prevent the misuse of sensitive information such as maintain transparent data handling practices. AI technology can also determine more detailed characteristics, such as ethnicity, country of origin, and other personal attributes, by tracking hand, eye, and body movements. Therefore, it is essential to provide users with clear mechanisms to manage or delete their data is critical to maintaining privacy and safeguarding against potential exploitation.

Task 3 – Findings Report and Recommendations:

The Meta Quest 2 like any wireless device that uses Wi-Fi can be vulnerable to man in the middle attacks and fake Wi-Fi networks which can be used to intercept data from the device. This means the interceptor can gain access to network traffic such as what packets are being sent which are being requested this information can be used to see what web browsing is going on removing all privacy from the user who may be inputting private data such as usernames passwords, names, addresses and other sensitive information. Which can be exploited in a variety of ways such as identity theft, bank fraud, selling data to third parties and allows a profile to be constructed of the user and could combine a variety of data from different sources.

Mitigation strategies include using robust authentication, such as WPA3 for Wi-Fi and secure pairing protocols for Bluetooth, to increase the security of both Wi-Fi and Bluetooth, ensuring that any data that is intercepted wirelessly cannot be read by anyone other than the sender and intended recipient. The user can also help mitigate this issue by only using the device on trusted networks such as their home network and avoiding public networks that are often unsecure or completely fake. For example, we used the aircrack-ng suite to carry out a deauthentication attack which could then be used to disconnect the device and force it onto another network which an attacker would use to steal information and gain access to sensitive data. (Rymar et al, 2023)

The Meta Quest 2 allows any user to put their quest into developer mode which allows data to be accessed from the device that can't be accessed by default this means anyone who gets a hold of the device can set it to developer mode and gain access to more information. Tighter Access limits can be implemented on the quest 2 to ensure that only developers can set the device to developer mode or at least require the user to enter a pin to prevent unauthorised users from exploiting it and guarantees that only authorised users can change important settings. (Revo4n6, 2023)

The Supplemental Meta Platforms Technologies Privacy Policy outlines the types of data collected from Meta Quest 2 headsets and the associated policies governing their use. To operate the device, users are required to create a Meta Horizon profile, which collects personal information such as profile name, picture, username, avatar, and details of interactions within games or apps. This process creates a user-specific profile to associate various data points with the individual. Additionally, the device collects a range of sensitive environmental and physiological data, including hand and body tracking, audio data, eye tracking, and camera footage. This information enables Meta to construct detailed user profiles and track device usage patterns, which can be cross-referenced with data from other Meta devices and services. While users can limit some data collection by disabling specific features, many data collection practices are mandatory and non-negotiable. If users wish to use the device, they must consent to the collection of certain data, which raises significant privacy and security concerns. The potential for abuse of this data underscores the importance of strong safeguards and transparency in data handling practices. (Meta, 2024)

The meta quest has a built-in browser in which allows users to surf the web directly from the VR environment, but it also introduces traditional web-based risks such as phishing, malware, trojan horses, ddos(denial of service) and many more. Users should avoid entering sensitive information through the VR browser, use ad blockers and browser security settings, and enable features that warn users about suspicious websites or insecure connections. Online VR experiences rely on the Meta Quest 2's connection to remote servers, which exposes the device to risks from unverified servers or interactions with malicious users. To mitigate these risks, users should only connect to trusted servers or VR platforms with robust security measures, use a VPN, and regularly update VR applications to patch security vulnerabilities.

Task 4 – Reflection on Group Activities and (individual marks):

As for the work distribution (Figure 13), my group leader, Khammas, was responsible for Task 1, while I handled Task 2, and Shore took on Task 3. The collaboration allowed for a balanced division of work, ensuring that each member contributed effectively to the project's overall success.

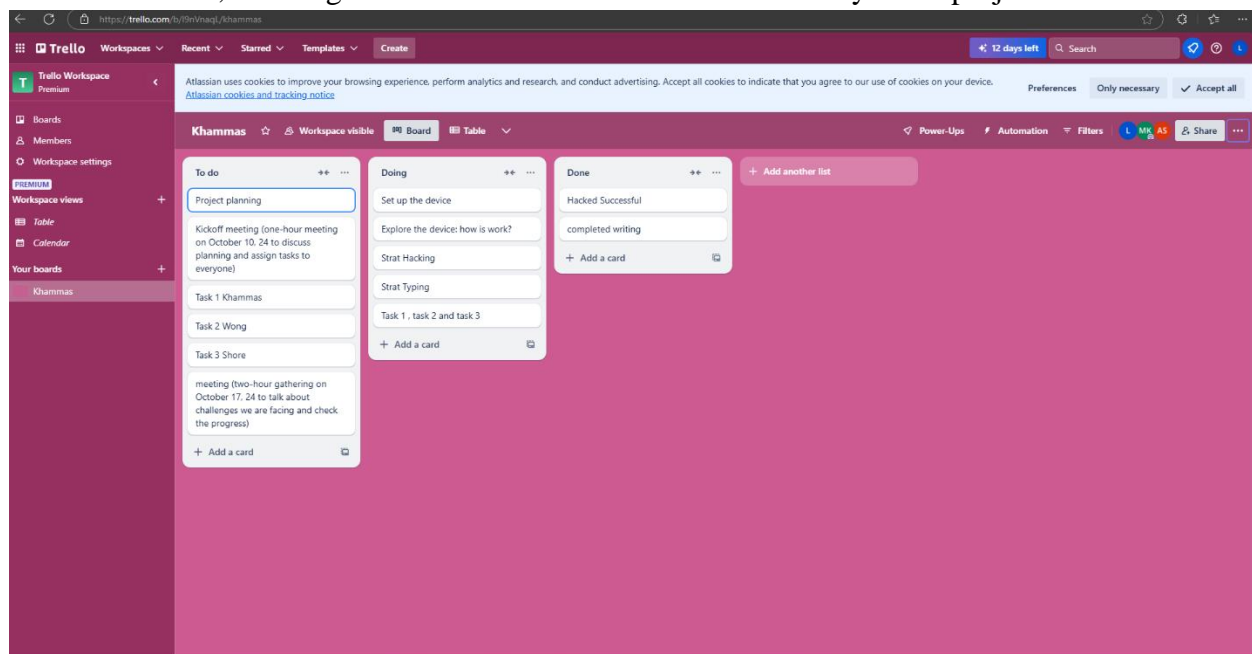


Figure 13: Trello record

In this group project, my primary responsibility was to assess the security and privacy aspects of the Meta Quest 2 VR Headset, focusing on identifying vulnerabilities and attack vectors within the device's settings. My work involved evaluating the device's configuration to uncover potential security weaknesses and privacy concerns that could affect users. Additionally, I reviewed and edited the group's report for clarity and grammar, making reviews as proofreading where necessary (Figure 14).

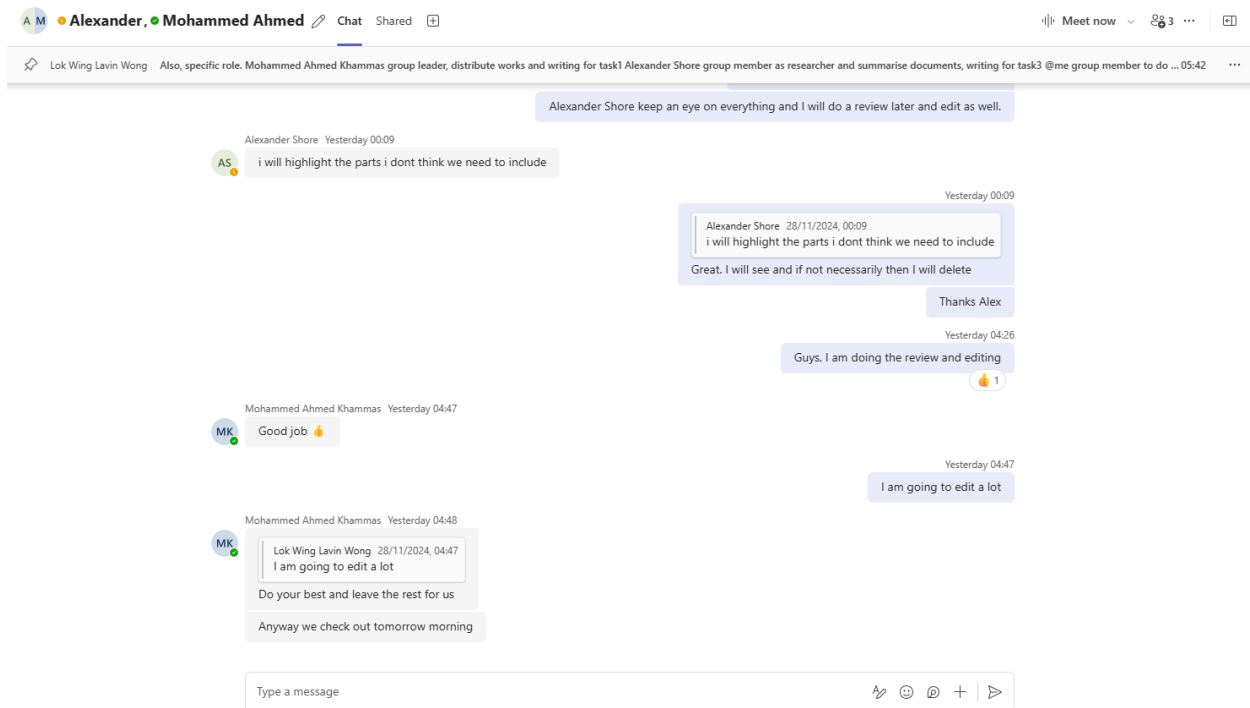


Figure 14: Conversations in Teams (I do review and editing of report)

I conducted a Deauthentication Attack to simulate a Denial of Service (DoS) scenario, effectively demonstrating wireless network vulnerabilities. Additionally, I examined various security and privacy settings, highlighting issues related to permissions for headset and hand tracking, location access, and passcode configurations. (Figure 15-17)

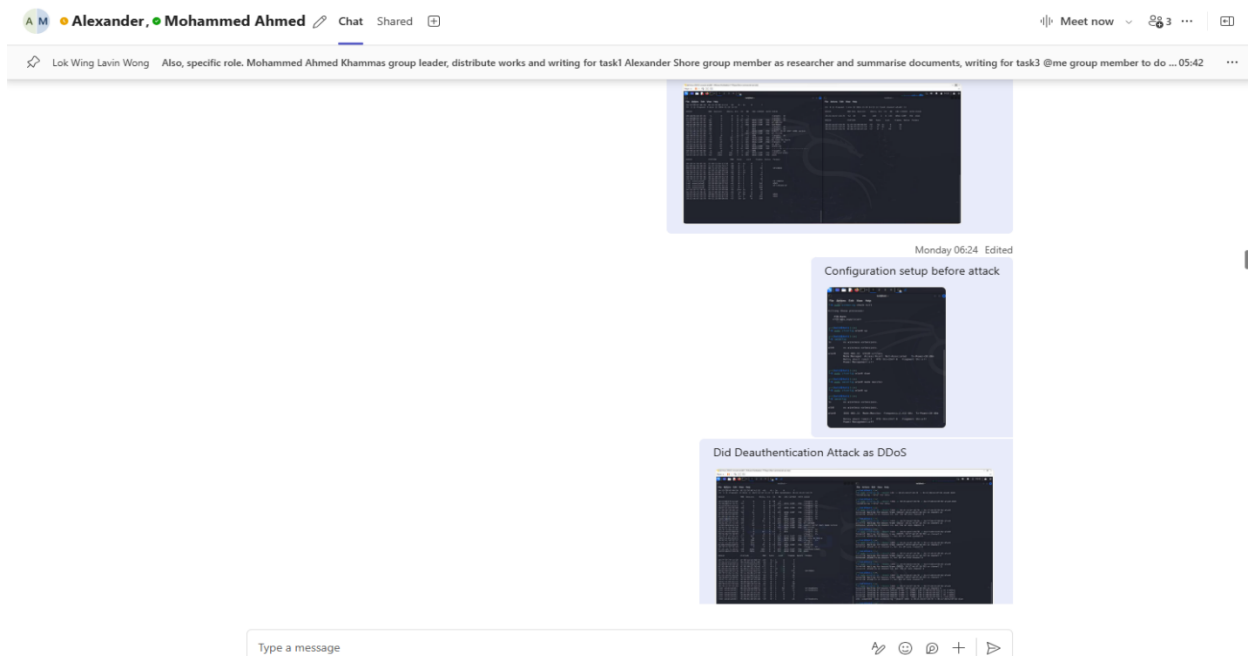


Figure 15: Teams record (screenshots of the attack sent to the group)

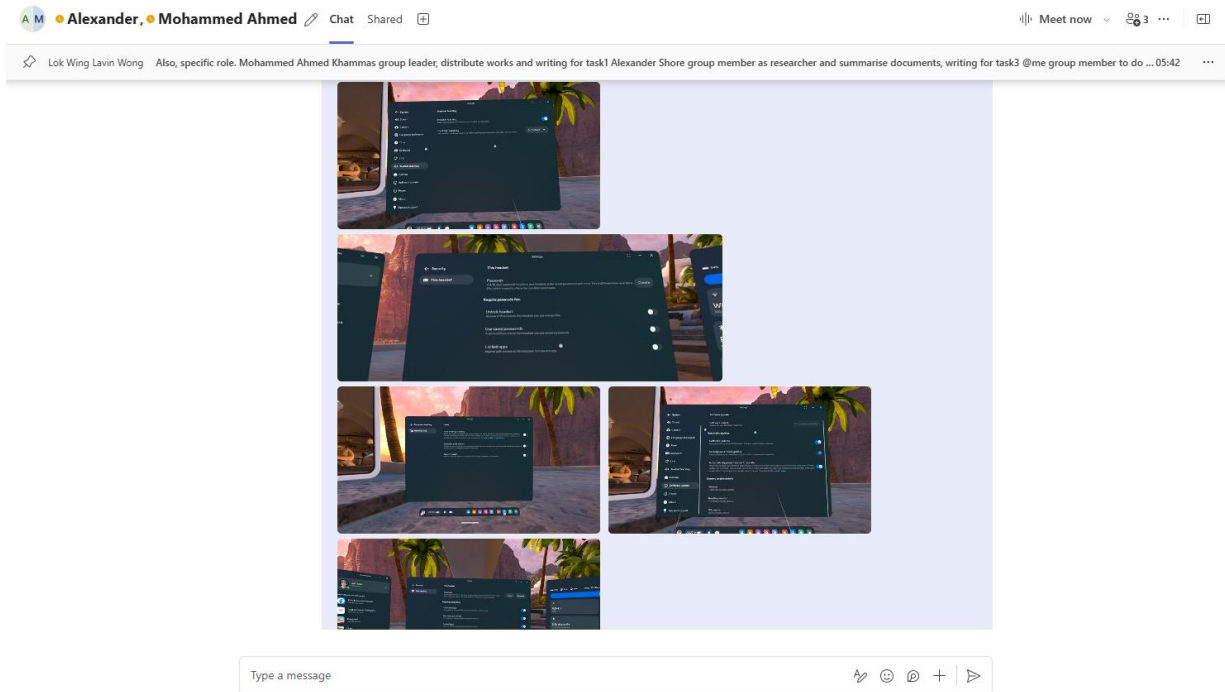


Figure 16: Teams record (screenshots of the findings of the headset settings)

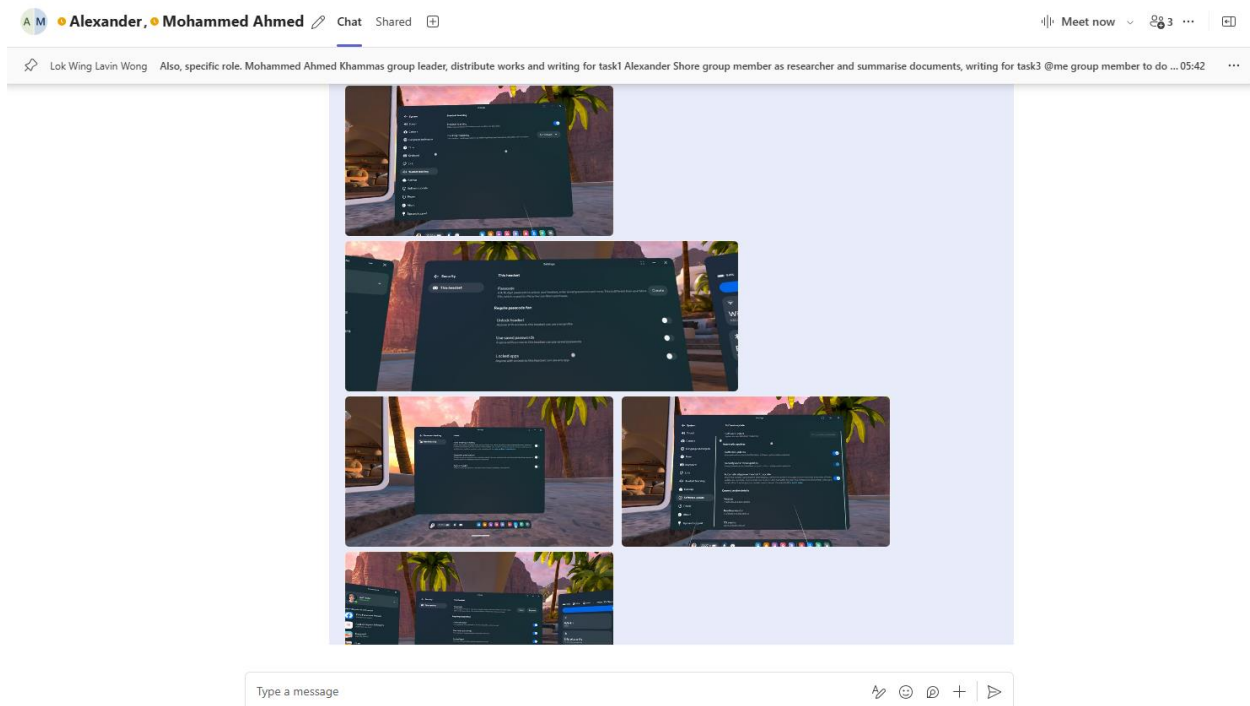


Figure 17: Teams record (screenshots of the findings of the headset settings)

A key strength of my contribution was the methodical and thorough approach I applied to the technical assessment. This ensured our findings were comprehensive, well-documented and evidence-based, likewise adding significant value to the group's overall analysis. My review and editing of the group report further preserve its clarity, contributing to a polished final deliverable.

However, I have recognised areas for improvement. While I effectively conducted technical assessments, I could have facilitated better knowledge sharing to ensure all team members fully understood the technical details. Additionally, improving time management of our group would allow for a more balanced focus on both in-depth analysis and collaborative tasks. Although our group has a problem for organising meetings, we sorted it out when we met in the lab sessions and emphasised the importance of using Teams to work. To move forward, enhancing communication and providing regular updates are important to our group which can strengthen team cohesion and contribute to more effective collaborative outcomes.

References

1. Meta (4/11/2024) Supplemental Meta Platforms Technologies Privacy Policy Available at: https://www.meta.com/gb/legal/privacy-policy/?utm_source=srt.facebook.com&utm_medium=dollyredirect
2. Revo4n6 (12/6/23) Meta Quest 2 Forensic Extraction (Testing) Available at: <https://revo4n6.com/blog-posts/f/meta-quest-2-forensic-extraction-testing>
3. Aggrawal, A., Arora, I. and Giri, A., 2023, February. Analysis and Rendering of Deauthentication Attack Using IoT Technology. In *Proceedings of 3rd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2022* (pp. 41-51). Singapore: Springer Nature Singapore.
4. Virtual reality forensics: Forensic analysis of Meta Quest 2(Emma Raymer, Aine MacDermott , Alex Akinbi(2023) Available at: [Virtual reality forensics: Forensic analysis of Meta Quest 2](#)
5. A Survey on Metaverse: Fundamentals, Security, and Privacy, Yuntao Wang, Zhou Su, Ning Zhang, Rui Xing, Dongxiao Liu, Tom H. Luan (2023) Available at:[IEEE Xplore Full-Text PDF:](#)
6. Joseph Henry (2023) Meta's VR Headset Quest 2 Sparks Privacy Concerns When Combined With AI <https://www.techtimes.com/articles/294957/20230810/metasp-vr-headset-quest-2-sparks-privacy-concerns-when-combined.htm>