National College of Ireland

Configuration Manual

MSc Research Project
Academic Internship

Eduards Samuls
21244545

School of Computing
National College of Ireland

Supervisor: Evgeniia Jayasekera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Eduards Samuls.....

Student ID: 21244545.....

Programme: MSc Cybersecurity..... Year: 1.....

Module: Academic Internship.....

Lecturer: Evgeniia Jayasekera.....

Submission Due Date: 18 September 2023.....

Project Title: Configuration Manual.....

Word Count: 1,180..... Page Count: 6.....

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 bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Eduards Samuls

Date: 16 September 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

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

Configuration Manual

Eduards Samuls
21244545

1 Tools

Table 1 shows the tools and their version used in the report.

Tool Name	Description	Version
Chrome	Browser used for examination	114.0.5735.196-573519627
Brave	Browser used for examination	1.52.129-415212927
Firefox	Browser used for examination	115.0-2015958819
Tor Browser	Browser used for examination	102.2.1-Release_(12.5)-2015960783
Hardware	Hardware Device	Galaxy S20 5G SM-G981x
Frida	Toolkit used for RAM dump	16.0.19
Fridump	Performs RAM dump	0.1
Android	Android version	13 (API 33)
ADB	For communication with android	1.0.41
MITMProxy	MITM Service	9.0
Strings	Finds readable strings in files	2.54 (SysInternals version)
Android Studio	Used for emulating an android device	Flamingo — 2022.2.1 Patch 2
Windows	Operating system used.	10.0.19045
Odin	Used to flash Samsung phone	3.13.1
Magisk	Used to root the Samsung device.	d390ca2f (26104)
uBlock Origin	Addon used to test private browsing	1.51.0
Dark Reader	Addon used to test private browsing	4.9.64

Figure 1: Tools and version used in the report.

2 Rooting Samsung

In order to dump RAM, it is necessary to root the samsung s20 5g android device. To do this:

1. Go to settings on the device → about phone → software information → click 5 times on build number.
2. Go back to settings → developer tools → enable OEM unlocking.
3. Turn off the phone.
4. Keep the up and down volume buttons pressed and insert a USB C cable into the device which is plugged into the Windows 10 host machine to enter download mode.
5. Press volume up button to continue to unlock bootloader screen.
6. Press volume up button again to unlock bootloader. This deletes all files on the phone and unlocks the bootloader.
7. Download Magisk Manager (2023).
8. Download Samsung Firmware from SamFw (2023) using the query ‘SM-G981B’. Download version ‘G981BXXUGHWCG’ as seen in figure 2. Extract the

Figure 2: The correct Samsung Firmware needed.

downloaded zip file → extract the ‘AP_G981BXXUGHWCG_G981BXXUGHWCG_MQB63657841_REV01_user_low_ship_MULTI_CERT_meta_OS13.tar’ file → convert the ‘boot.img.lz4’ file to a tar file using 7zip.

9. Transfer the ‘boot.img.tar’ file and magiskmanager apk to the Samsung device using the USB C cable.
10. Install MagiskManager apk on Samsung.
11. Select Install and click the ‘Select and Patch a File’ method which prompts to select the ‘boot.img.tar’ file.
12. Magisk creates a ‘magisk_patched.tar’ file which is then sent to the Windows host machine.
13. Repeat step 4.
14. Download Odin (2023), open it and place the patched magisk file in the AP slot as shown in figure 3. Make sure to unselect auto reboot in the options and start flashing.

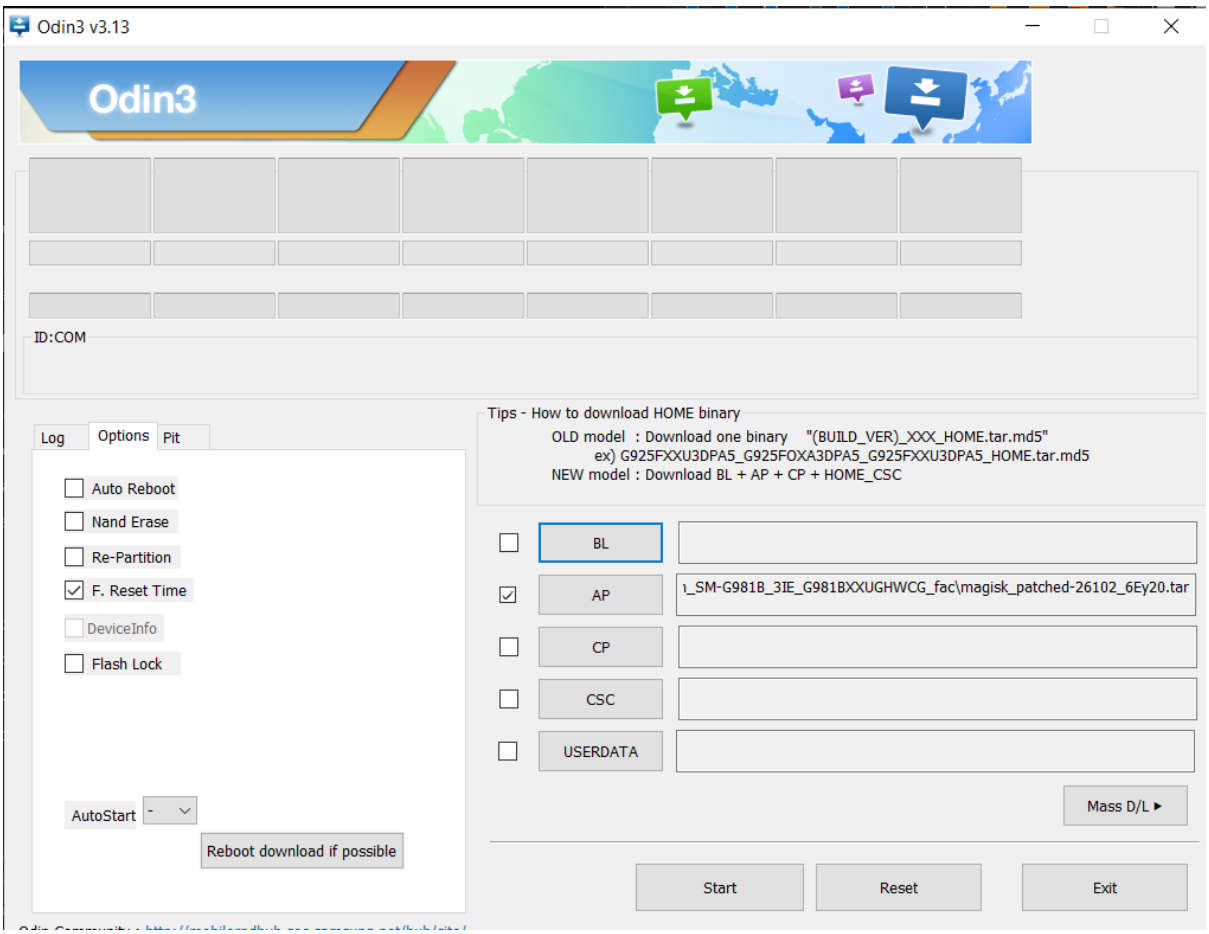

Figure 3: Flashing Samsung Device

15. Boot the device into recovery mode by pressing the down volume button and power button. Press volume up when the device turns on and select ‘Wipe Data/Factory Reset’ option.
16. Reboot the system. Transfer the magisk manager apk and install it if it does not appear automatically, otherwise the device is fully rooted.

3 Setting up Android Studio Emulation

To setup Android Studio for emulation experiments:

1. Download and install Android Studio (2023) Flamingo 2022.2.1 Patch 2.
2. In Android Studio, go to device manager and create a new virtual device.
3. Select the Pixel 6 Pro screen.
4. Select the Tiramisu API Level 33 system image.
5. Click advanced settings on the verify configuration screen.
6. Select Cold Boot, 6GB RAM, 6GB VM heap, 20GB internal storage and no SD Card as seen in figure 4.

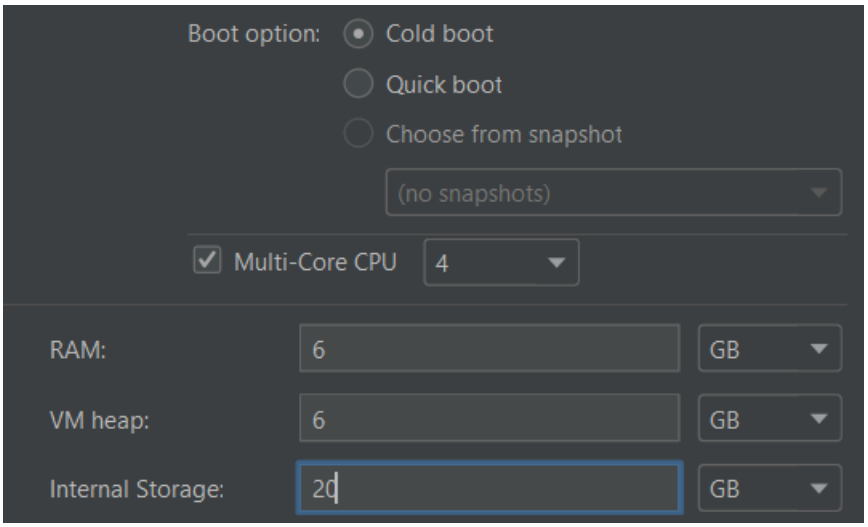

Figure 4: Emulation configuration options.

7. Click finish which creates the android emulated environment used for the report.

4 Connecting Samsung Phone to Android Studio

To connect the Samsung device to the Windows host for the hardware experiments:

1. On the Samsung device go to developer tools → Wireless Debugging → Pair Device with QR code
2. On Android Studio go to Device Manager → Physical → Pair using Wifi. Make sure both the Windows host machine and Samsung are connected to the same LAN.
3. Scan the given QR code from Android Studio using Samsung.

5 Private Browsing Modes Experiments

For collecting disk and ram for private browsing modes:

1. Install correct browser versions from table 1 from APKMirror (2023). (This is also the step to install addons for the addon experiments from in the browser)
2. Before starting each experiment, a downloaded Frida (2023) server 16.0.19 is placed inside the /data/local/tmp directory in Android using the ADB push command - “adb push frida-server /data/local/tmp/” → then chmod is applied to be able to run it ‘adb shell "chmod 755 /data/local/tmp/frida-server"’. The server is then run using ‘adb shell "/data/local/tmp/frida-server &"’.
3. The steps to conduct browser experiments are run from the report.

4. After the steps were completed, the host windows machine runs the downloaded Fridump (2019) using the command “python fridump.py -U -s Firefox”, changing the command to the name of the browser tested. Fridump will create a strings file with all legible strings found in RAM – use the notepad search function to search for keywords the same as step 5.
5. To acquire disk storage of the browser, the windows host uses “adb pull /data/data/org.mozilla.firefox .” to pull browser contents to the windows host for analysis. The folder name changes depending on the browser used. Use powershell command “ Get-ChildItem -Recurse | Select-String -Pattern ”ncirl” -List ../../brave normal 1 ncirl.txt” to search for keywords. I use “NCIRL”, “EFF”, “21244545”, “Signal” and “Tutanota” in the report.

6 Setting up Android for MITMProxy

For the experiment to see what HTTP requests are sent back to the developer do:

1. Turn on the android Samsung device / emulator.
2. Download and install MITMProxy (2023) and turn on MITMWeb on the windows host machine.
3. On Windows, go to Powershell and type ‘ipconfig’ to find out the local LAN IP of the PC.
4. On Android go to settings → Network & Internet → Select the network you are connected to and go to its settings → Go to Advanced Options and enter Manual Proxy settings of the Windows host IP on port 8080 as seen in figure 5.

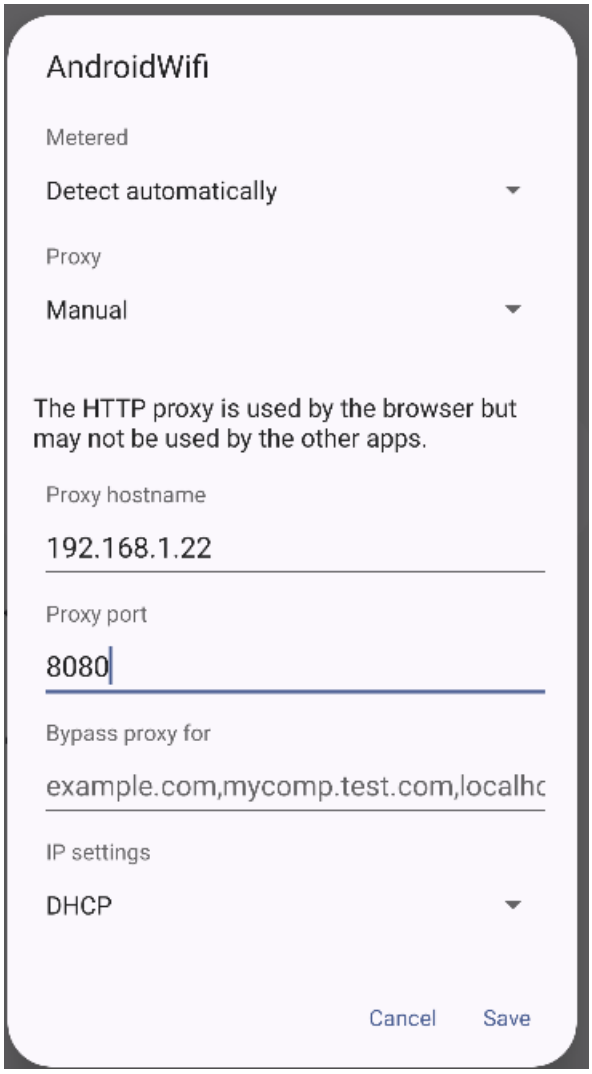

Figure 5: Proxy settings on Android

5. On Android, go to a browser and type ‘mitm.it’. If output from figure 6 is visible it means the proxy was configured successfully. If not, the host IP is not reachable and you need to try again.

Figure 6: Certificates are visible in Android.

6. Download the Android certificate.
7. Go to settings → security → More security settings → encryption & credentials → Install a certificate → CA certificate → Select and upload the downloaded certificate.
8. Browser HTTP traffic will now be intercepted by the Windows Host. Firefox and Tor additionally require you to go to their browser → go to settings → select “About Firefox” or “About Tor” → click the logo 5 times to enter debug mode → go back to settings and find ‘Secret Settings’ → In there select “Use third party CA certificates”.
9. Once each experiment is complete, go to File → Save. On the saved file, apply filters to filter uninteresting traffic and analyse what was transmitted.

References

Magisk Manager (2023) *Download Magisk Manager Latest Version 26.1 For Android 2023*. Available at: https://magiskmanager.com/ [Accessed 13 August 2023].

SamFw (2023) *Download Samsung Firmware max speed and Free. Official update.* Available at: https://samfw.com/ [Accessed 13 August 2023].

Android Studio (2023) *Android Studio download archives.* Available at: https://developer.android.com/studio/archive [Accessed 13 August 2023].

APKMirror (2023) *Free and safe Android APK downloads.* Available at: https://www.apkmirror.com/ [Accessed 13 August 2023].

Frida (2023) *See https://frida.re/news/ for details.* Available at: https://github.com/frida/frida/releases [Accessed 13 August 2023].

Fridump (2019) *A universal memory dumper using Frida.* Available at: https://github.com/Nightbringer21/fridump [Accessed 13 August 2023].

MITMProxy (2023) *mitmproxy is a free and open source interactive HTTPS proxy.* Available at: https://mitmproxy.org/ [Accessed 13 August 2023].

Odin (2023) *Samsung Odin - Root Android download page.* Available at: https://odindownload.com/download/ [Accessed 13 August 2023].