OSINT Exercise #1

Fernando D. Parra

Metropolitan State University of Denver

Open-Source Intelligence CYB-3900-001

Alexander Darius Clayton

February 27th, 2025

OSINT Exercise #1

Conducting any serious open-source intelligence requires a thorough review and essential knowledge. Via a concise 3-5 page report, understanding the fundamental principles, creating a functional environment, and having the ability to work within that environment ensures that investigations are not only conducted with an operational approach but produce accurate and reliable results.

Setup

As my primary device, I use a desktop computer I built a few years ago and I've been upgrading it ever since. This is the computer I used the most as it is tailored to all the cybersecurity-related and personal tasks. The antivirus that I'm currently using is *BitDefender*. According to their primary site, the cybersecurity technology company was founded in 2001 in Romania. Bitdefender has two headquarters locations, one evidently in the country of origin and another in the U.S. at Santa Clara, CA. Additionally, they own several offices across the globe and continue to innovate by accomplishing new research alongside partners like the Linux Foundation, Microsoft, and VMware. The current password manager that I'm using is called KeePassXC (the same one shown in the textbook), which can be found as a GitHub Repository along with documentation and a very detailed guide to set up a new password database, this is one of the reasons I use it (it is open-source). It works on different OSs, it has more than three hundred contributors, and it includes effective and essential features of a password manager for free.

Virtual Machines & Linux

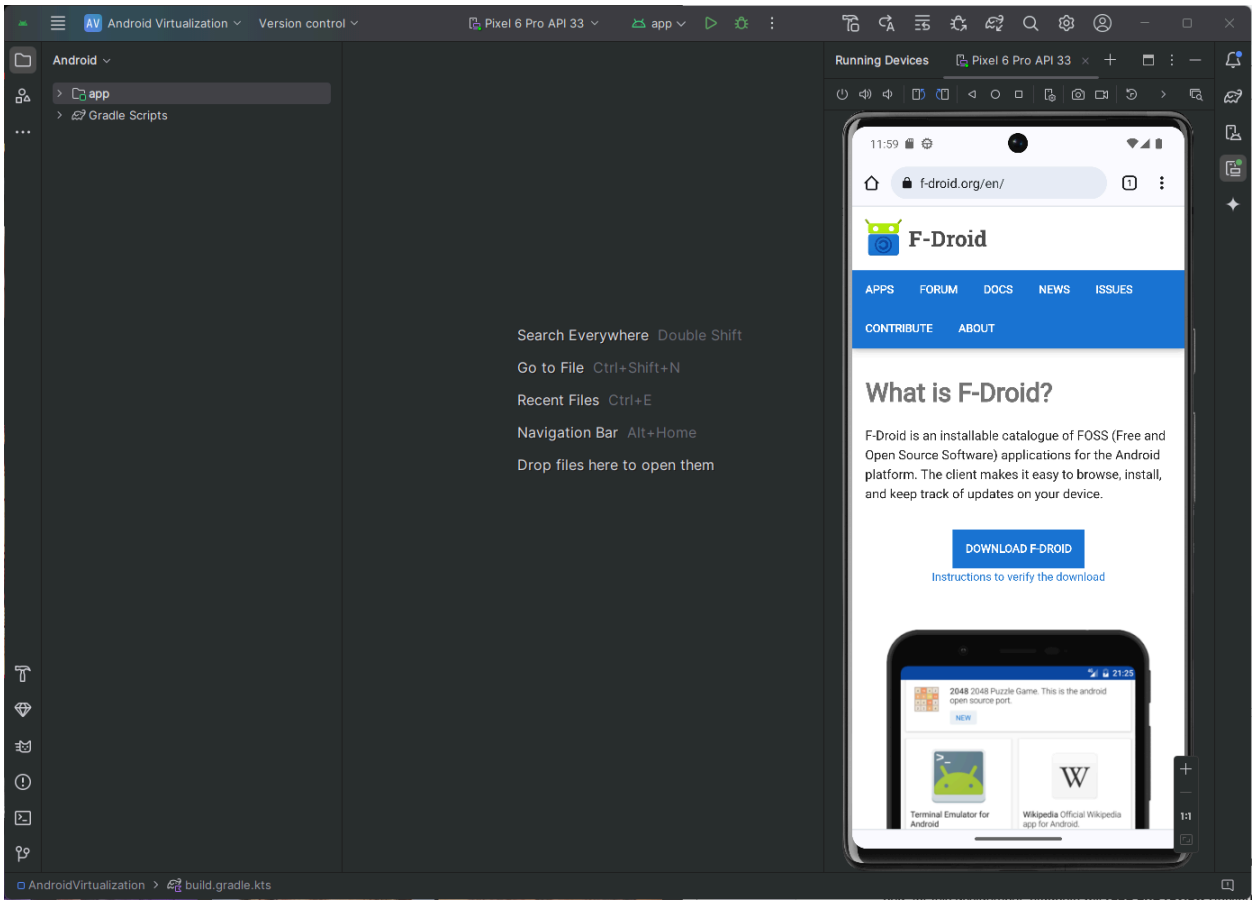
Today, as the textbook shows, VirtualBox is the way to go and it is the one I still use, although I do not go in-depth as the textbook did, Virtualbox sets up a default configuration

which is just fine for me but when I first started using virtual machines as a beginner, I evidently encountered issues and learned a lot about the process of configuring a new virtual machine. The first time I tried to install the penetration-testing OS, *Kali Linux*, with *VMware*, I followed many YouTube tutorials that showed how it is necessary to share hardware resources; processors, memory, storage, network adapters, or even audio drivers. In another instance, the simple step of enabling virtualization is most likely the first issue a non-experienced user will undergo, as I did myself, many times I also had to troubleshoot network connectivity for long hours, and screen resolutions, but it helped me improve my knowledge and efficiency using CLIs.

I'm currently using Mozilla Firefox for the modifications or extensions available. I have *Ublock Origin*, *Grammarly*, Sponsorblock for YouTube, and *KeePassXC-Browser*. I also started using Firefox due to Google Chrome's tracking and excessive collection of data (telemetry) from users. Installing applications is probably one of my favorite tasks to do and the *Advanced Package Tool* (APT) is the most satisfying way to do it (also used in Chapter 4). Clearly, issues arise depending on the software being installed, for instance, I often have a problem with Python programs that use pip as it requires a virtual environment to install them and even then, if certain requirements are not correctly installed or modules are missing, it is required to troubleshoot. Many software require distinct packet installers and it can become a difficult process very quickly. Programs that I've installed include *spotdl*, *Qbittorrent*, *yt-dlp* (was called YTDL before), *Samba*, *Pi-hole*, *Nmap*, *Aircrack-ng*, *Dvwa* (Damn Vulnerable Web Application), *Nessus* (could not make it work on Raspberry Pi due to the architecture), and many others which include libraries.

Android

The Android simulation was probably the easiest to achieve, there were no issues while downloading and installing due to *Android Studio*'s integration to emulate devices like the Pixel 6 Pro API used on the textbook (the same I tried):



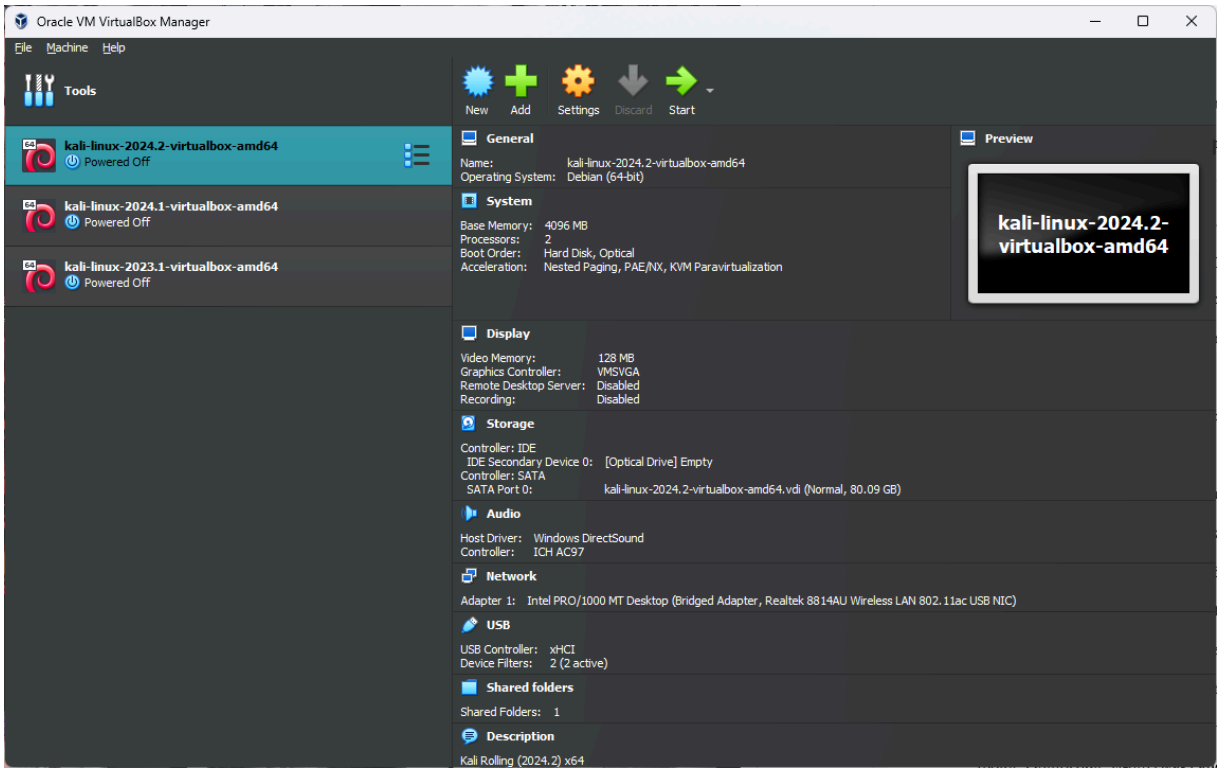
This is the Windows *Android Studio* version, I had previously used it to learn Android code using my Pixel Watch, and the only step I needed to complete was setting up the API and Tiramisu.

Custom Tools

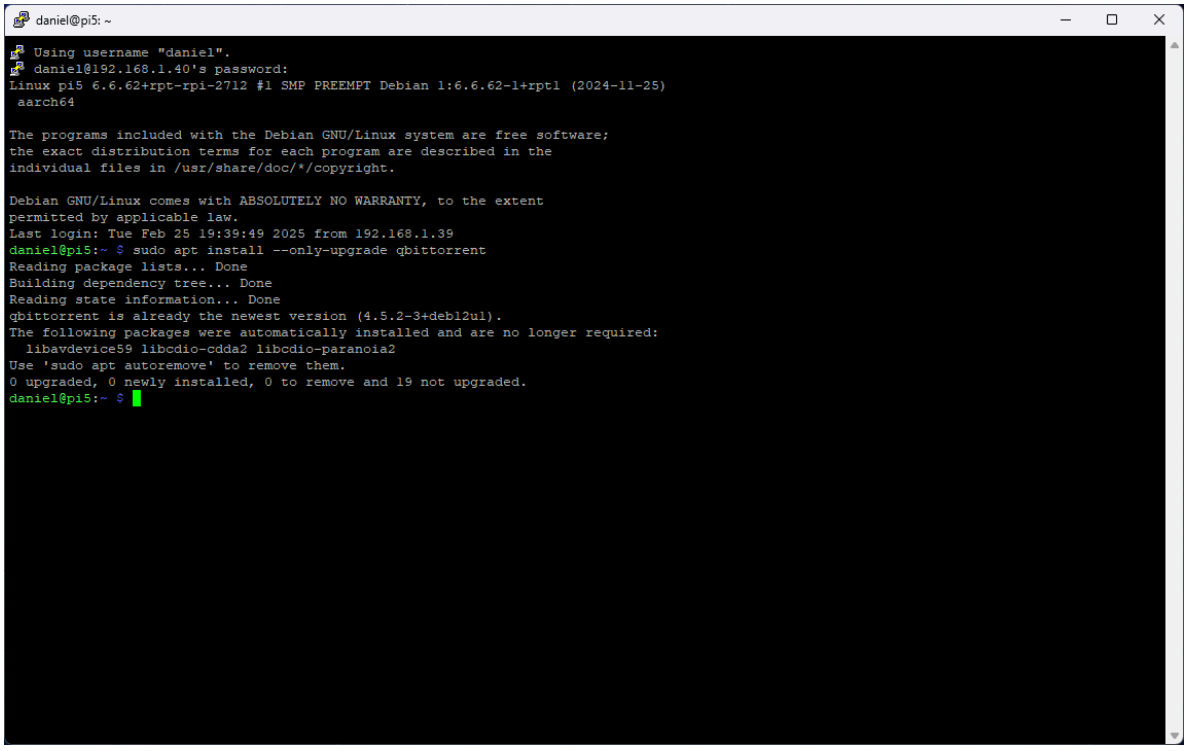
Although I do not use any specific tools other than making tailored Google Dorks, threads, and forums, I did start using some of the tools from IntelTechniques such as the Documents Search Tool or the LinkedIn Search Tool when I try to find precise information from

an employer or recruiter. The textbook illustrates the use of the site's (IntelTechniques.com) tools.zip to add and modify the current search tools through the use of *VSCodium,* the author explains the HTML code of the email search tool, to try this myself, I downloaded the zip file and dove deep into the LinkedIn Search Tool HTML. As a resolution, all the resources are outstanding and a prominent strategy to designate a baseline for anybody looking to do an Open Source Intelligence Investigation or even just to have some fun traversing the internet.

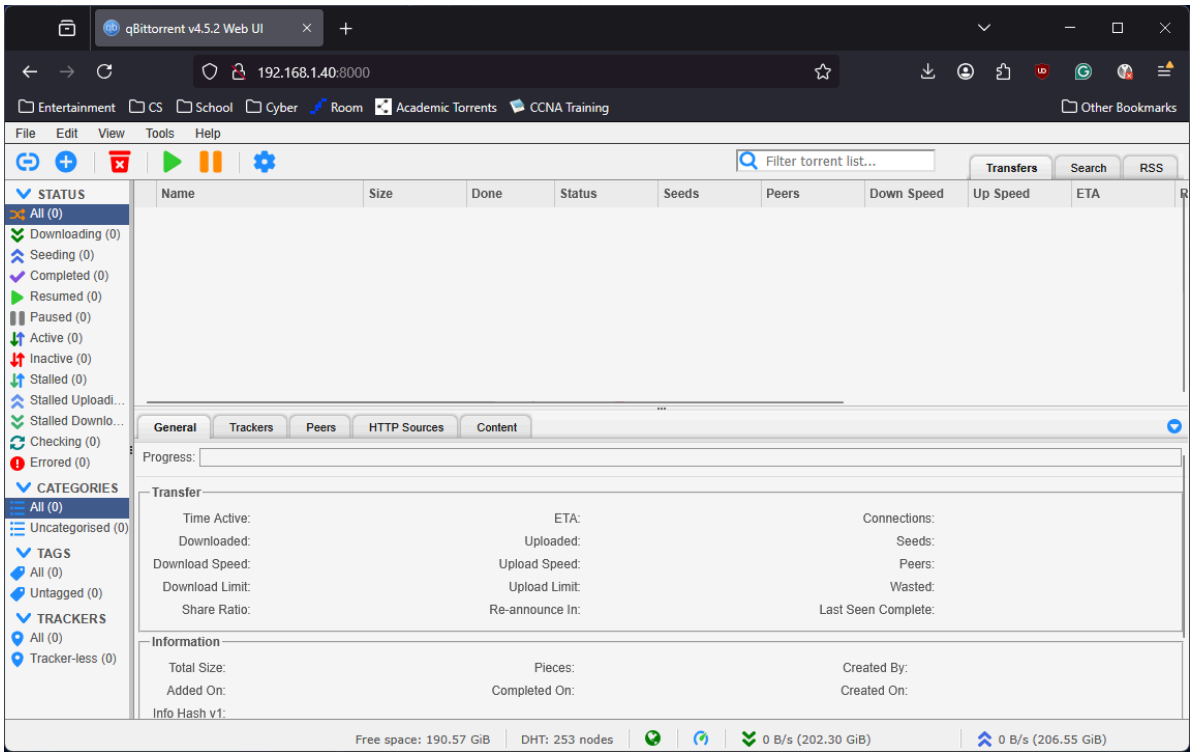
VirtualBox in My Computer



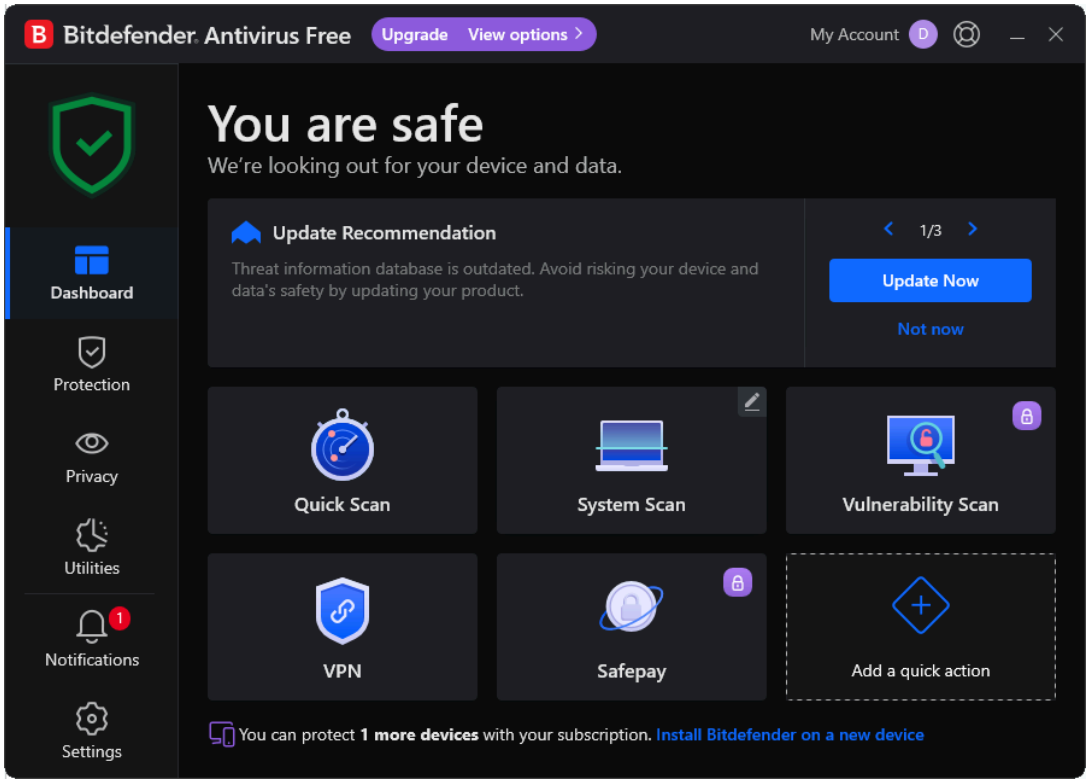
Installing Qbittorrent Upgrade With APT (none were available)



Web User Interface of Qbittorrent



Bitdefender Antivirus in My Computer



LinkedIn Search Tool Using NeoVim