**Network Security**

**Part I – Network Security Certifications and Graduate Degree**

1. **Suppose you have determined to pursue a cybersecurity career. List at least three professional certificates that would be most helpful to you for a successful cybersecurity career. List the certificates with links to the corresponding websites. Also, list the year/month when you plan to acquire them and the prerequisites of these certificates. (20 points)**

**CompTIA Security+**

This certification validates core essential skills needed in a cybersecurity role.

<https://www.isc2.org/Certifications/CCSP>

I plan to acquire this certification by 2023 after completion of this class. By the end of this class, my skills in penetration testing and ethical hacking would help in the preparation of the examination. This is an entry-level certification.

**CISSP: Certified Information System Security Professional**

CISSP validates that you’re experienced in IT security and capable of designing, implementing, and monitoring a cybersecurity program.

<https://www.isc2.org/Certifications/CISSP>

I plan to acquire this certification by 2027, because it requires five to seven years of paid work experience in a cybersecurity position.

1. **Based on statistics, a master’s degree in IT or related field ties to higher average salaries when compared to a bachelor’s degree. Georgia Southern University offers the MSIT program https://cec.georgiasouthern.edu/it/degrees/msit/. Go through the information on the page and answer the following questions. (up to 10 bonus points)**
   1. **Would you be interested in this program and the degree? Why or why not? (1 points)**

Yes, I’m currently in the graduate program. It gave me the opportunity to enhance my skills.

* 1. **Would you prefer this program to be face-to-face, 100% online, or hybrid (some content being online while some other content and major milestones such as project/thesis defense being face-to-face)? Why? (3 points)**

Hybrid. Most responsibilities handled by IT professionals can be done remotely from anywhere, but the need to come for face-to-face classes is essential because it’s a requirement by the school.

* 1. **Would you be interested in such a degree without a final master project or a thesis (in other words, completing the program by only completing the required courses without the requirement of completing a master project or thesis toward the end of the program)? Why? (3 points)**

Yes, I would be interested in a thesis program because I’m currently working on my thesis.

* 1. **Any suggestions regarding the MSIT program and courses? (3 points)**

Well, more courses could be added to the program, to encourage options for students who wish to diversify their career path.

**Part II – Kali Linux and Security Tools**

1. **Kali Linux – the #1 platform and tool set for learning and practicing hands-on network security. (40 points + up to 10 bonus points)**

* Go to Kali Linux <https://www.kali.org/> and browse its website.
* **Download Kali Linux and make your bootable USB Kali Linux.**
  + You will need a designated (wipe-clean data before use) USB memory key **at least 8 GB** of storage size (16GB+ is recommended).
  + Follow the instructions at <https://www.kali.org/docs/usb/> to prepare portable Kali on a USB memory key. **Take and attach screenshots/pictures below as proof in your answer that you can successfully boot Kali Linux from your USB memory key to its desktop screen.** Note: you may (or may not) need to go to your computer’s **BIOS** and change boot sequence so that computer will boot from USB memory key. You may (or may not) also need to disable (turn off) SecureBoot in BIOS (where applicable).

Firstly, I went to the Kali website and downloaded the **ISO image for live boot the Apple M1**. Afterward, I downloaded the **balenaEtcher application** which I used in making the flash drive bootable with the ISO image i downloaded and added persistence also.

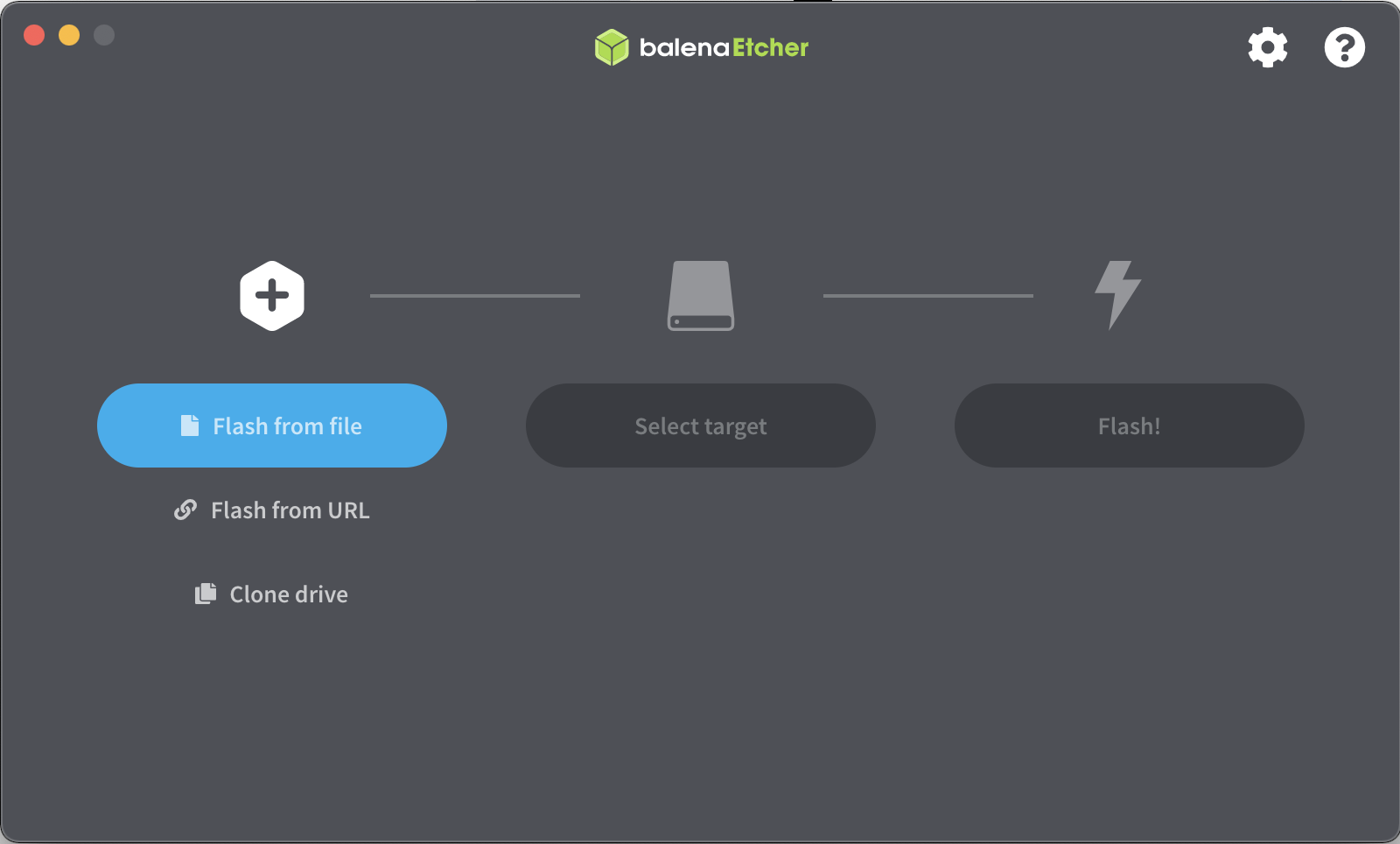


Figure 1: Making the flash drive bootable using balenaEtcher.

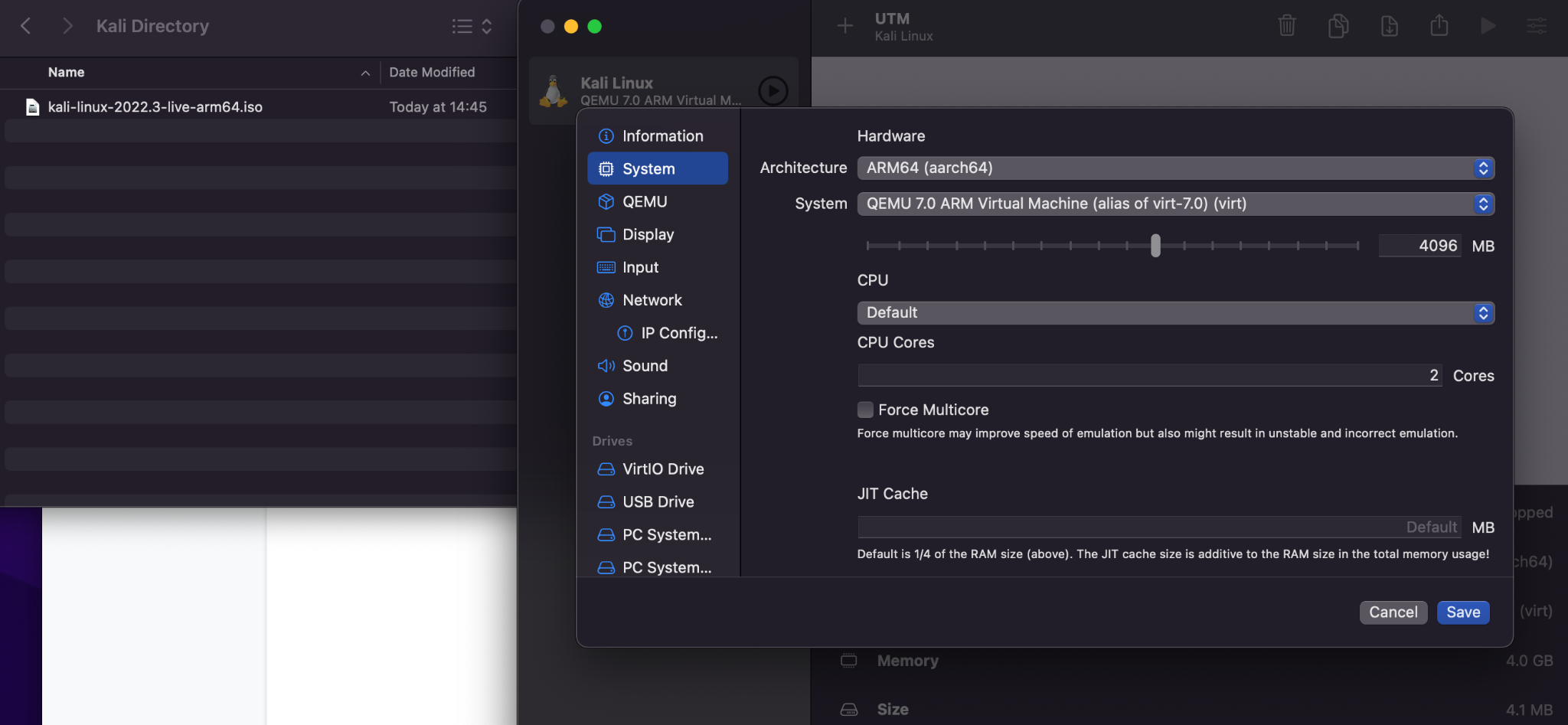


Figure 2:Setting up the Kali linux on UTM (VirtualMachine)



Figure 3: Complete installation of Kali Linux

* Here is a **list of security tools** available on Kali Linux <https://www.kali.org/tools/> with brief instructions and examples. There are many videos on YouTube that may be very useful for learning how to use Kali and its tools.
* **You can only run/test security tools or conduct ethical attacks or penetration testing within your own computer with your own accounts without impacting any other unauthorized systems or networks or accounts. THIS IS VERY IMPORTANT!!!**
* **Attach screenshots/photos** to show that you can launch **Denial of Service (DoS) attack to your own machine using the hping3 tool in Kali** (example shown in module slides). Also **attach screenshots/photos** to show your CPU load and memory usage (find commands/tools) during the attack.

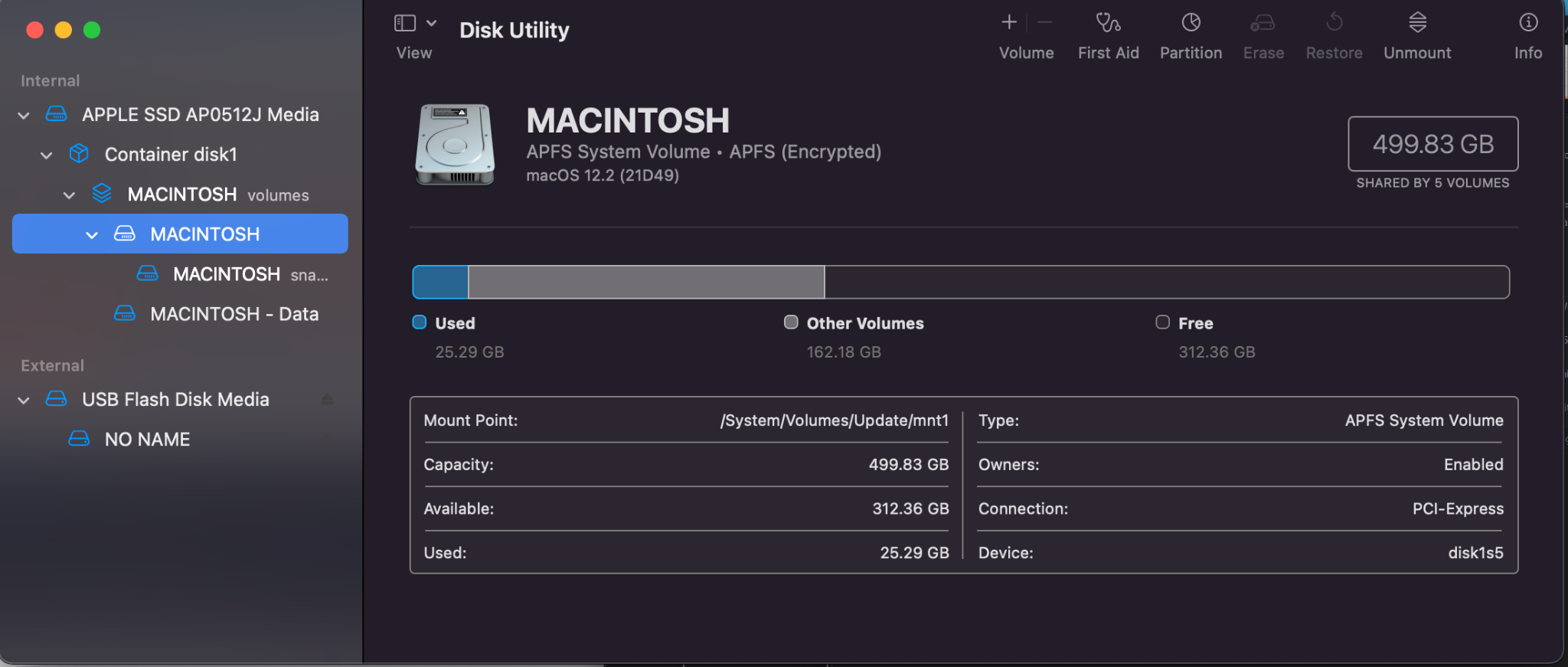


Figure 4: Disk Utilization”(CPU load) before running the Hping3 on the system.(Look at the used memory)

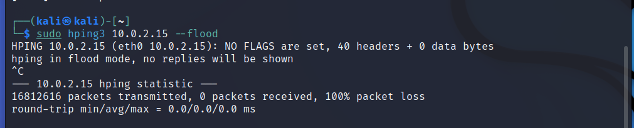


Figure5: Hping3 flood command

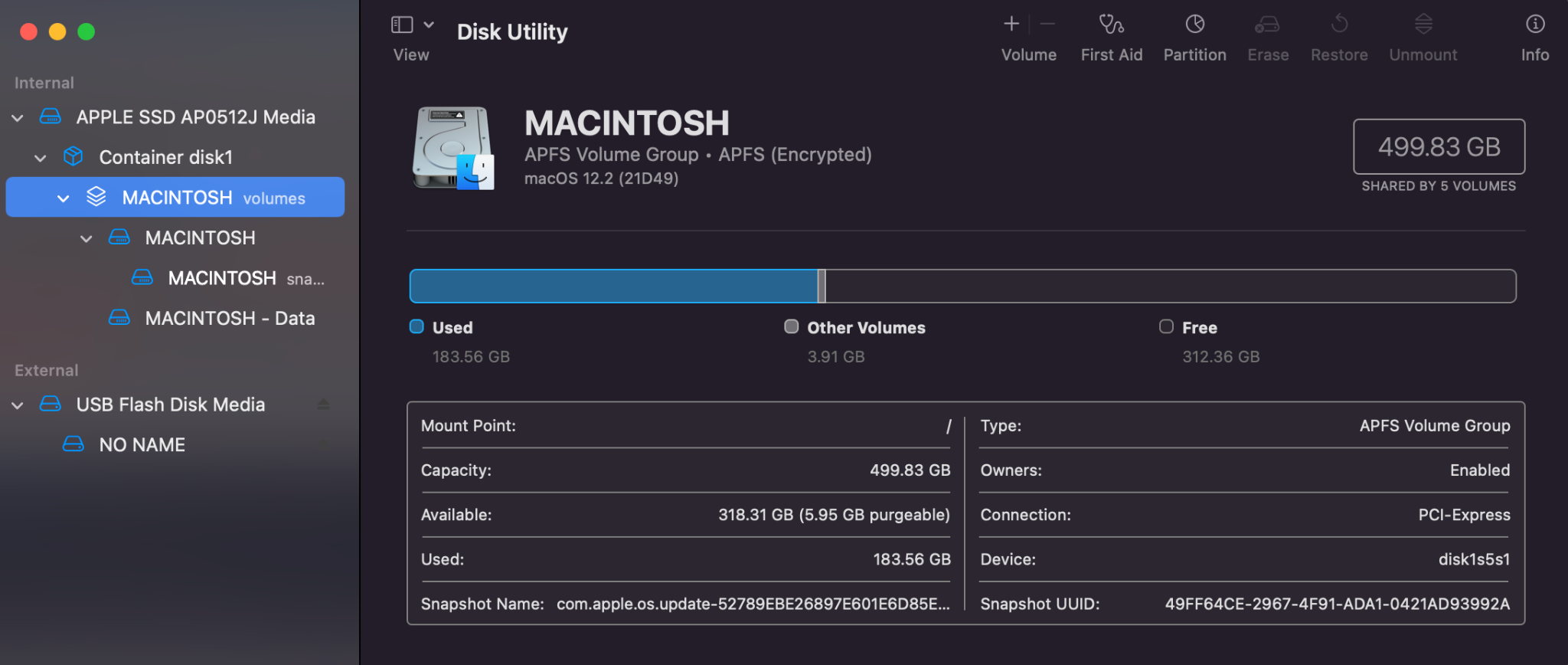


Figure 6: Disk Utilization after the hping3 command. (Look at the used memory)

* **Bonus up to 10 points**: **show using screenshots/photos** that you can use **at least one** additional Kali tool to launch attack to your own machine; **explain** the tool/command and how the attack works; **provide** **suggestions** and **recommendations** for defending against such attacks. Google and YouTube could be helpful for finding tools.

The second tool I will be using is called Macchanger tool. This tool is used to change or fake the Media Access Control Address (MAC) Address of any computer on the same network port as the host computer.

I used the command **“sudo apt install macchanger”** to install the tool on my kali linux.

Then I initialize the network port “eth0” using the command “ macchanger -s eth0”. This is my home network port connected to my computer. This command displays my current MAC address and my Permanent MAC address.

Using the command **“sudo ifconfig eth0 down”**. I was able to switch off my home ethernet network. Then I changed the current MAC address using the command **“sudo macchanger -r eth0”.**

Then I switched on the network after changing the MAC address when the network was down.

