**NORTHEASTERN UNIVERSITY**

**Communication / Network Security**  
**TELE7374 / CSYE7374**  
**Fall 2023**

**LAB ASSIGNMENT 03 (DUE OCT 02)**

**THREATS AND ATTACKS ON ENDPOINTS**

**NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Bhavin Bhatia NUID 002981075\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

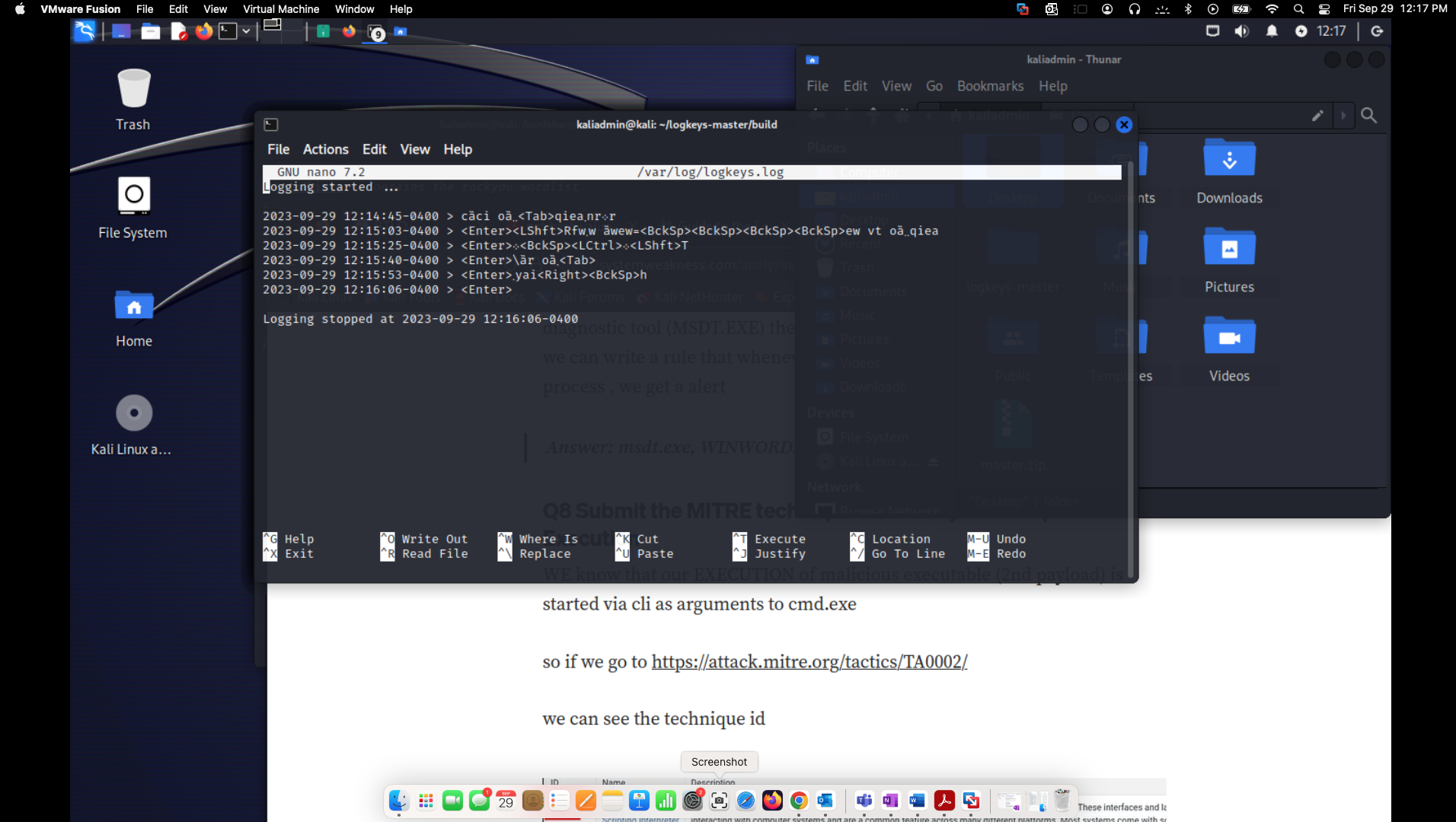
NOTE: The lab assignments follow the Lab Manual for CompTIA Security+ Guide to Network Security Fundamentals. There are some modifications to save time and reinforce class discussions. Please submit screenshots or answers to demonstrate that you have completed the work. You will need a personal computer to complete the task. Good Luck!

**Lab 3.1. Keylogging with Logkeys in Kali**

In this lab, you will set up the Logkeys keylogger locally on the Kali virtual machine and view the results.

1. Start your Kali VM (from lab 1.3) and log in.
2. Open a terminal window.
3. Type **sudo apt-get install autotools-dev -y** and press **Enter** to install the software you need to set up Logkeys.
4. Type **sudo apt-get install automake -y** and press **Enter** to install additional software needed for setup. Ignore any error message.
5. Type **wget https://github.com/kernc/logkeys/archive/master.zip** and press **Enter** to download the files for Logkeys.
6. Type **unzip master.zip** and press **Enter** to extract the files.
7. Type **cd logkeys-master/** and press **Enter** to change directories to the newly extracted one.
8. Type **sudo ./autogen.sh** and press **Enter** to run the installation script.
9. Type **cd build** and press **Enter** to change directories to the build directory.
10. Type **sudo ../configure** and press **Enter** to run the configuration script.
11. Type **sudo make** and press **Enter**. Type **sudo make install,** and press **Enter** to complete the base installation.
12. Type **sudo locale-gen** and press **Enter** to generate locales for the program.
13. Type **sudo logkeys -s** and press **Enter** to start logging keystrokes.
14. Type **nano passwords.txt** and press Enter to create a new file called passwords.txt and open it in the Nano text editor.
15. Type **These are my passwords.** into the Nano editor.
16. Press **Ctrl+X** to exit the editor and then press **Y** to save the text file. Press **Enter** to accept the default filename.
17. Type **cat passwords.txt** and press **Enter** to confirm that you entered the sentence and saved the file.
18. Type **sudo logkeys -k** and press **Enter** to stop logging keystrokes.
19. Type **sudo nano /var/log/logkeys.log** and press **Enter** to view the keystroke log from Logkeys. Take a screenshot and paste it below to show your work.
20. Exit Nano (CTRL+X) and shut down your Kali virtual machine.

Answer: Enter the screenshot here:

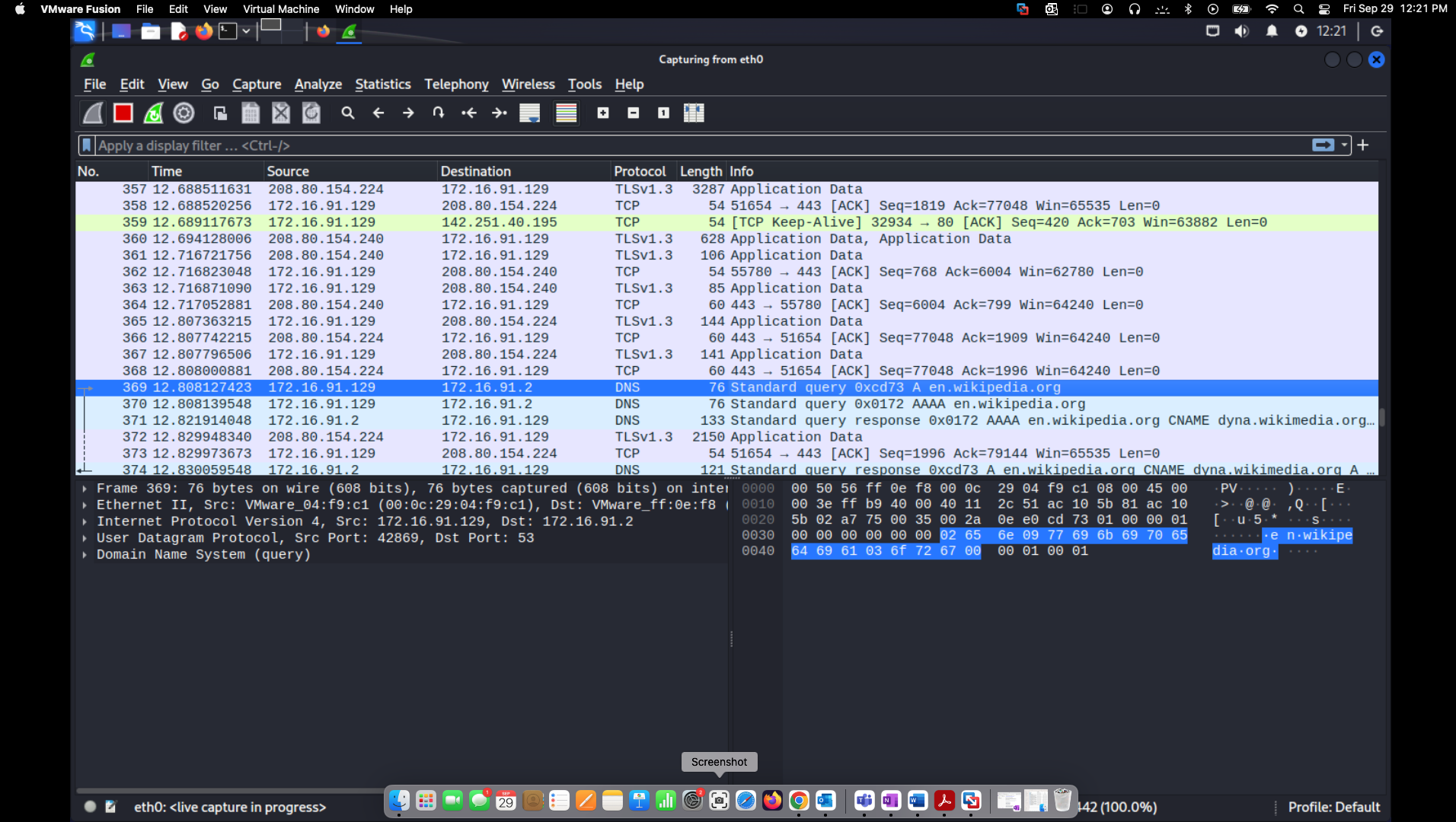
****

**Lab 3.2. Capturing packets using Wireshark**

In this lab, you will use Wireshark to capture network traffic in Kali.

1. Start and log in to your Kali VMs (this was created in the previous lab).
2. Open the main Kali menu.
3. Point to **Sniffing & Spoofing**, and then click **Wireshark**. If you are asked for the Kali password, enter **kali**.
4. Double-click the **eth0** interface to start capturing packets on that interface.
5. Open a browser window in your Kali VM. Navigate to **https://www.wikipedia.org/**
6. Return to Wireshark and note the different connections that are being opened. Take a screenshot of the window.
7. Close all windows and shut down your virtual machines.

Answer: Enter the screenshot here:

****