

Put Student Name(s) ↓		Put Student IDs ↓	Due Date	Grade Weight
Ishan Aakash Patel		146151238	As Posted	6%
Name	<a href="#">Lab5: Using TCPDump</a>			
Objective	By the end of this lab, students will be able to use <code>tcpdump</code> to capture and analyze network traffic on their local machine.			
Prerequisites	<ul style="list-style-type: none"> <li>Basic knowledge of command-line interface (CLI).</li> <li>Administrative (root) access to the system.</li> <li><code>tcpdump</code> installed on the system.</li> </ul>			
Instructions	<ul style="list-style-type: none"> <li>It is an Individual assignment. Put your name + Student ID in the empty spaces above.</li> <li>Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.</li> <li>Show your genuine signs of your work is done on your machine. This includes:             <ul style="list-style-type: none"> <li>Screenshots that show your desktop background with Date/Time.</li> <li>Show a pop-up bx that shows "your name + IP".</li> <li>Show your logged account when applicable. Optional: Your photo.</li> </ul> </li> <li>Submit your report name: CYT215-Lab5-Student Name &amp; ID</li> </ul> <p>Steps:</p> <p><b>Step 1: Installing <code>tcpdump</code></b></p> <p>First, ensure that <code>tcpdump</code> is installed on your system.</p> <p><b>For Ubuntu/Debian:</b></p> <pre>sh Copy code sudo apt-get install tcpdump</pre> <p><b>For Red Hat/CentOS:</b></p> <pre>sh Copy code sudo yum install tcpdump</pre>			

## Step 2: Basic Packet Capture

Start by capturing network packets on the default network interface.

1. **Open a terminal.**
2. **Run the following command to capture packets:**

```
sh  
Copy code  
sudo tcpdump
```

**Explanation:** This command starts capturing packets on the default network interface. `sudo` is required because capturing packets usually requires root privileges.

3. **Stop the capture after a few seconds by pressing `Ctrl+C`.**
  - Observe the output. It shows captured packets with details like source and destination IP addresses, ports, and protocols.

## Step 3: Capture Packets on a Specific Interface

Identify the network interfaces available on your system.

1. **List network interfaces:**

```
sh  
Copy code  
sudo tcpdump -D
```

**Explanation:** This command lists all network interfaces that `tcpdump` can capture from.

2. **Capture packets on a specific interface (e.g., `eth0`):**

```
sh  
Copy code
```

```
sudo tcpdump -i eth0
```

3. **Stop the capture after a few seconds by pressing **ctrl+c**.**

- Observe the output. This time, only packets from the specified interface are captured.

#### **Step 4: Save Captured Packets to a File**

Save the captured packets to a file for later analysis.

1. **Capture packets and save to a file:**

```
sh
Copy code
sudo tcpdump -i eth0 -w capture.pcap
```

**Explanation:** The `-w` option writes the captured packets to a file named `capture.pcap`.

2. **Stop the capture after a few seconds by pressing **ctrl+c**.**

#### **Step 5: Read Captured Packets from a File**

Read and analyze the packets from the saved file.

1. **Read packets from the file:**

```
sh
Copy code
sudo tcpdump -r capture.pcap
```

**Explanation:** The `-r` option reads packets from a file instead of capturing live traffic.

2. **Observe the output.** This shows the packets captured previously.

## Step 6: Apply Basic Filters

Filter the captured packets to display only specific types of traffic.

### 1. Capture only TCP packets:

```
sh
Copy code
sudo tcpdump -i eth0 tcp
```

### 2. Capture packets from/to a specific host (e.g., 192.168.1.1):

```
sh
Copy code
sudo tcpdump -i eth0 host 192.168.1.1
```

### 3. Capture packets on a specific port (e.g., HTTP port 80):

```
sh
Copy code
sudo tcpdump -i eth0 port 80
```

## Step 7: Advanced Filtering

Use more advanced filters to capture specific types of traffic.

### 1. Capture only HTTP GET requests:

```
sh
Copy code
sudo tcpdump -i eth0 'tcp port 80 and (((ip[2:2] - ((ip[0] & 0xf) << 2)) - ((tcp[12] & 0xf0) >> 2)) = 0x47455420)'
```

**Explanation:** This filter captures HTTP GET requests by looking for the "GET" method in the packet data.

## 2. Capture DNS queries:

```
sh
Copy code
sudo tcpdump -i eth0 port 53
```

## Step 8: Verbose and Timestamp Options

Enhance the output with more detailed information and human-readable timestamps.

### 1. Capture with verbose output:

```
sh
Copy code
sudo tcpdump -i eth0 -v
```

### 2. Capture with human-readable timestamps:

```
sh
Copy code
sudo tcpdump -i eth0 -ttt
```

## Step 9: Limit the Number of Packets

Capture only a specific number of packets.

### 1. Capture only 10 packets:

```
sh
Copy code
sudo tcpdump -i eth0 -c 10
```

**Explanation:** The `-c` option limits the capture to a specified number of packets.

## Step 10: Analyzing the Captured Data

Use Wireshark to analyze the captured data.

### 1. Install Wireshark if not already installed.

```
sh  
Copy code  
sudo apt-get install wireshark    # For Ubuntu/Debian  
sudo yum install wireshark        # For Red Hat/CentOS
```

### 2. Open the capture file in Wireshark:

- Launch Wireshark.
- Open the `capture.pcap` file created earlier.
- Use Wireshark's GUI to analyze the packets in detail.
- Provide a summary of the packet you generated (example follow the TCP stream and describe what you see)
- You may also choose to open the PCAP in Network Miner, or use AI to generate a script to analyze it as shown in class.

Students Work required for this activity

- For each step above, follow the instructions and provide screenshots of the steps followed.

Grading Alerts

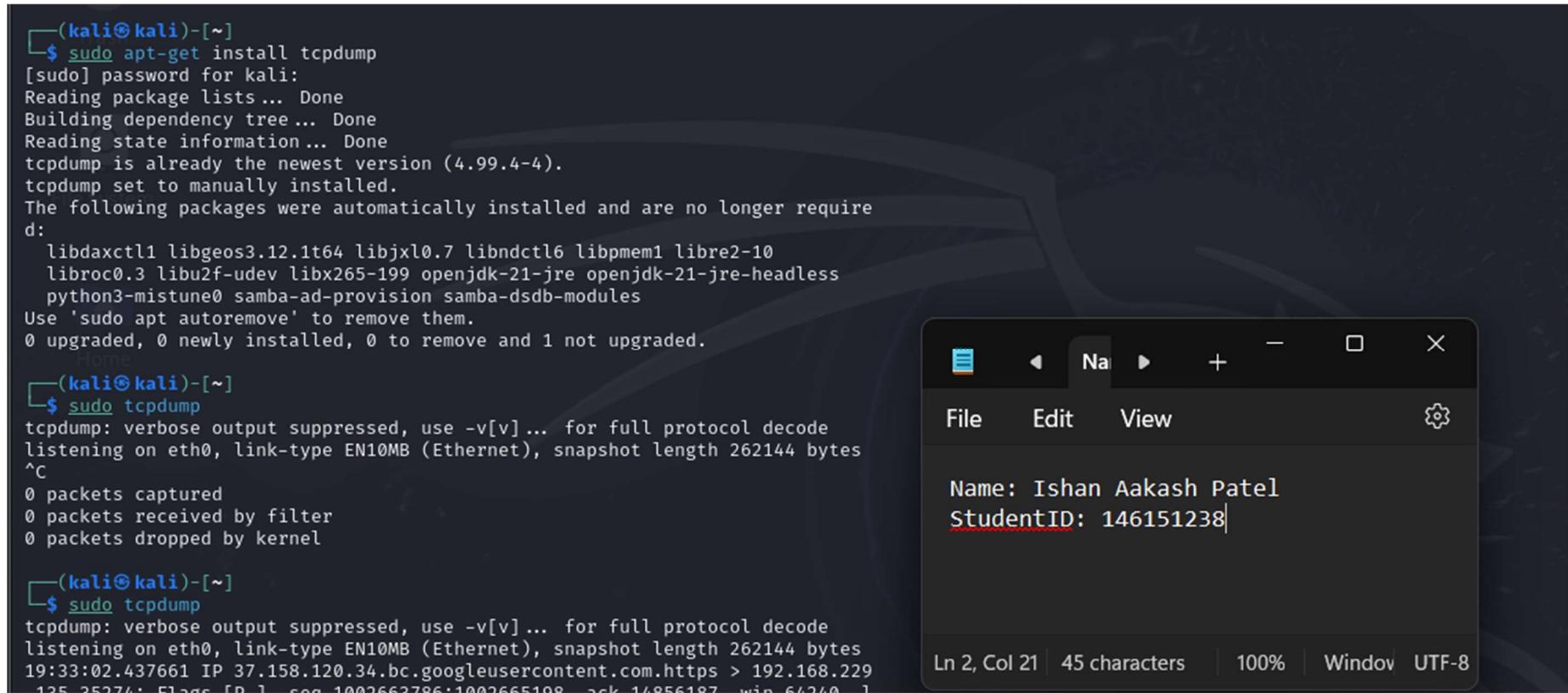
- If you do NOT use this template or delete any part of it or use any other template, you will be degraded.
- If you do NOT follow the file naming convention, you will be degraded.
- If you do NOT submit your file in PDF; you will be degraded.
- If you do NOT show your account real name (when applicable); you will be degraded.
- If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded.
- If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.

## Step 1: Installing `tcpdump`

First, ensure that `tcpdump` is installed on your system.

### For Ubuntu/Debian:

```
sudo apt-get install tcpdump
```



```
(kali㉿kali)-[~]
$ sudo apt-get install tcpdump
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpdump is already the newest version (4.99.4-4).
tcpdump is set to manually installed.
The following packages were automatically installed and are no longer required:
  libdaxctl1 libgeos3.12.1t64 libjxl0.7 libndctl6 libpmem1 libre2-10
  libroc0.3 libu2f-udev libx265-199 openjdk-21-jre openjdk-21-jre-headless
  python3-mistune0 samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.

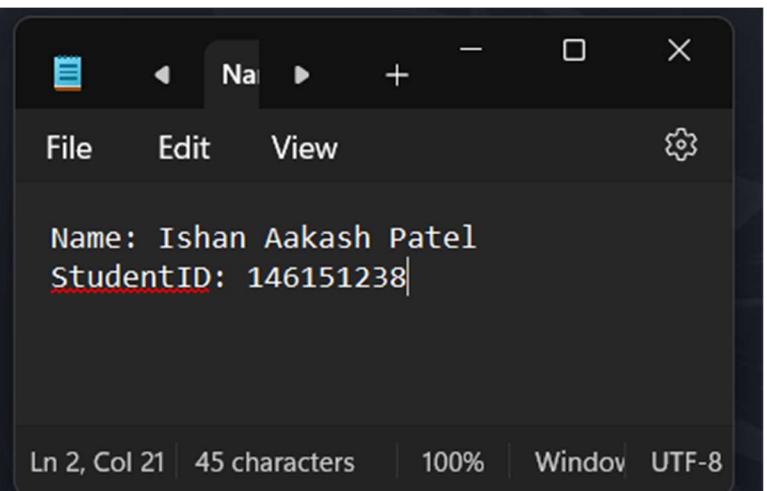
(kali㉿kali)-[~]
$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

(kali㉿kali)-[~]
$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:33:02.437661 IP 37.158.120.34.bc.googleusercontent.com.https > 192.168.229.125.25274: Flags [P.], seq 1002662786:1002665198 ack 14856187 win 64240 [
```

A screenshot of a terminal window titled '(kali㉿kali)-[~]'. It shows the command \$ sudo apt-get install tcpdump being run, followed by the output of the installation process. Then, the command \$ sudo tcpdump is run, and it shows network traffic being captured on interface eth0. To the right of the terminal, there is a small window titled 'Name' containing the text 'Name: Ishan Aakash Patel' and 'StudentID: 146151238'. The window has a dark theme and includes standard window controls like minimize, maximize, and close.

## Step 2: Basic Packet Capture

```
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.  
Home  
└─(kali㉿kali)-[~]  
$ sudo tcpdump  
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
^C  
0 packets captured  
0 packets received by filter  
0 packets dropped by kernel  
  
└─(kali㉿kali)-[~]  
$ sudo tcpdump  
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
19:33:02.437661 IP 37.158.120.34.bc.googleusercontent.com.https > 192.168.229  
.135.35274: Flags [P.], seq 1002663786:1002665198, ack 14856187, win 64240, l  
ength 1412  
19:33:02.437716 IP 192.168.229.135.35274 > 37.158.120.34.bc.googleusercontent  
.com.https: Flags [.], ack 1412, win 65535, length 0  
19:33:02.441387 IP 37.158.120.34.bc.googleusercontent.com.https > 192.168.229  
.135.35274: Flags [P.], seq 1412:2824, ack 1, win 64240, length 1412  
19:33:02.441428 IP 192.168.229.135.35274 > 37.158.120.34.bc.googleusercontent  
.com.https: Flags [.], ack 2824, win 65535, length 0  
19:33:02.447578 IP 37.158.120.34.bc.googleusercontent.com.https > 192.168.229  
.135.35274: Flags [P.], seq 2824:4236, ack 1, win 64240, length 1412  
19:33:02.447633 IP 192.168.229.135.35274 > 37.158.120.34.bc.googleusercontent  
.com.https: Flags [.], ack 4236, win 65535, length 0  
19:33:02.452423 IP 37.158.120.34.bc.googleusercontent.com.https > 192.168.229  
.135.35274: Flags [P.], seq 4236:5648, ack 1, win 64240, length 1412  
19:33:02.452463 IP 192.168.229.135.35274 > 37.158.120.34.bc.googleusercontent  
.com.https: Flags [.], ack 5648, win 65535, length 0  
19:33:02.470790 IP 37.158.120.34.bc.googleusercontent.com.https > 192.168.229
```



### Step 3 : Capture Packets on a Specific Interface

```
(kali㉿kali)-[~]
$ sudo tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7 dbus-system (D-Bus system bus) [none]
8 dbus-session (D-Bus session bus) [none]

(kali㉿kali)-[~]
$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:36:54.547882 IP 192.168.229.135.42041 > 192.168.229.2.domain: 57793+ A? www.google.com. (32)
19:36:54.548135 IP 192.168.229.135.42041 > 192.168.229.2.domain: 26313+ AAAA?
www.google.com. (32)
19:36:54.553209 IP 192.168.229.2.domain > 192.168.229.135.42041: 57793 1/0/0
A 142.251.41.36 (48)
19:36:54.554771 IP 192.168.229.2.domain > 192.168.229.135.42041: 26313 1/0/0
AAAA 2607:f8b0:400b:803::2004 (60)
19:36:54.559001 IP 192.168.229.135.45700 > yyz12s08-in-f4.1e100.net.https: UDP, length 1357
19:36:54.573962 IP 192.168.229.135.33243 > 192.168.229.2.domain: 36294+ PTR?
2.229.168.192.in-addr.arpa. (44)
19:36:54.579868 IP 192.168.229.2.domain > 192.168.229.135.33243: 36294 NXDomain 0/1/0 (121)
19:36:54.580188 IP 192.168.229.135.42604 > 192.168.229.2.domain: 26091+ A? www.facebook.com. (34)
19:36:54.580460 IP 192.168.229.135.57322 > 192.168.229.2.domain: 65316+ PTR?
```

The screenshot shows a terminal window with two main sections. The top section lists network interfaces with their status. The bottom section shows a live capture of network traffic on the 'eth0' interface. The captured traffic includes several DNS queries, notably for 'www.google.com' and 'www.facebook.com', and other standard network communications.

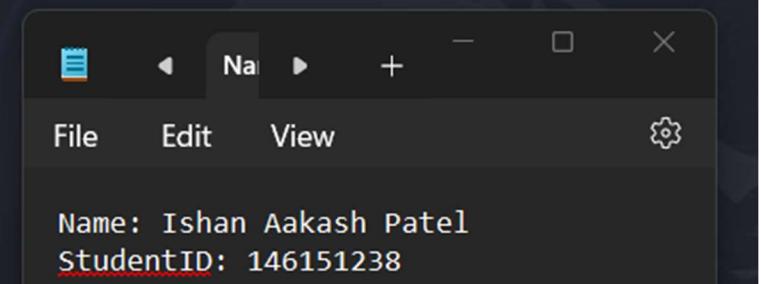
File Edit View

Name: Ishan Aakash Patel  
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

## Step 4: Save Captured Packets to a File

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
^C1964 packets captured
1964 packets received by filter
0 packets dropped by kernel
Home
(kali㉿kali)-[~]
└─$ ls
capture.pcap  Documents  Music      Public      Videos
Desktop       Downloads  Pictures   Templates
(kali㉿kali)-[~]
└─$ sudo tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length
```



## Step 5: Read Captured Packets from a File

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length
262144
19:38:05.886448 IP 192.168.229.135.33573 > 192.168.229.2.domain: 38994+ A? www.facebook.com. (34)
19:38:05.886724 IP 192.168.229.135.33573 > 192.168.229.2.domain: 26718+ AAAA?
www.facebook.com. (34)
19:38:05.893631 IP 192.168.229.2.domain > 192.168.229.135.33573: 38994 2/0/0
CNAME star-mini.c10r.facebook.com., A 31.13.80.36 (79)
19:38:05.903698 IP 192.168.229.2.domain > 192.168.229.135.33573: 26718 2/0/0
CNAME star-mini.c10r.facebook.com., AAAA 2a03:2880:f10e:83:face:b00c:0:25de (91)
19:38:05.907946 IP 192.168.229.135.60559 > edge-star-mini-shv-01-yyz1.facebook.com.https: UDP, length 1357
19:38:05.915394 IP edge-star-mini-shv-01-yyz1.facebook.com.https > 192.168.229.135.60559: UDP, length 1232
19:38:05.915396 IP edge-star-mini-shv-01-yyz1.facebook.com.https > 192.168.229.135.60559: UDP, length 215
19:38:05.915397 IP edge-star-mini-shv-01-yyz1.facebook.com.https > 192.168.229.135.60559: UDP, length 48
19:38:05.916042 IP edge-star-mini-shv-01-yyz1.facebook.com.https > 192.168.229.135.60559: UDP, length 80
19:38:05.918565 IP 192.168.229.135.60559 > edge-star-mini-shv-01-yyz1.facebook.com.https: UDP, length 85
19:38:05.919380 IP 192.168.229.135.60559 > edge-star-mini-shv-01-yyz1.facebook.com.https: UDP, length 85
```

Name: Ishan Aakash Patel  
StudentID: 146151238

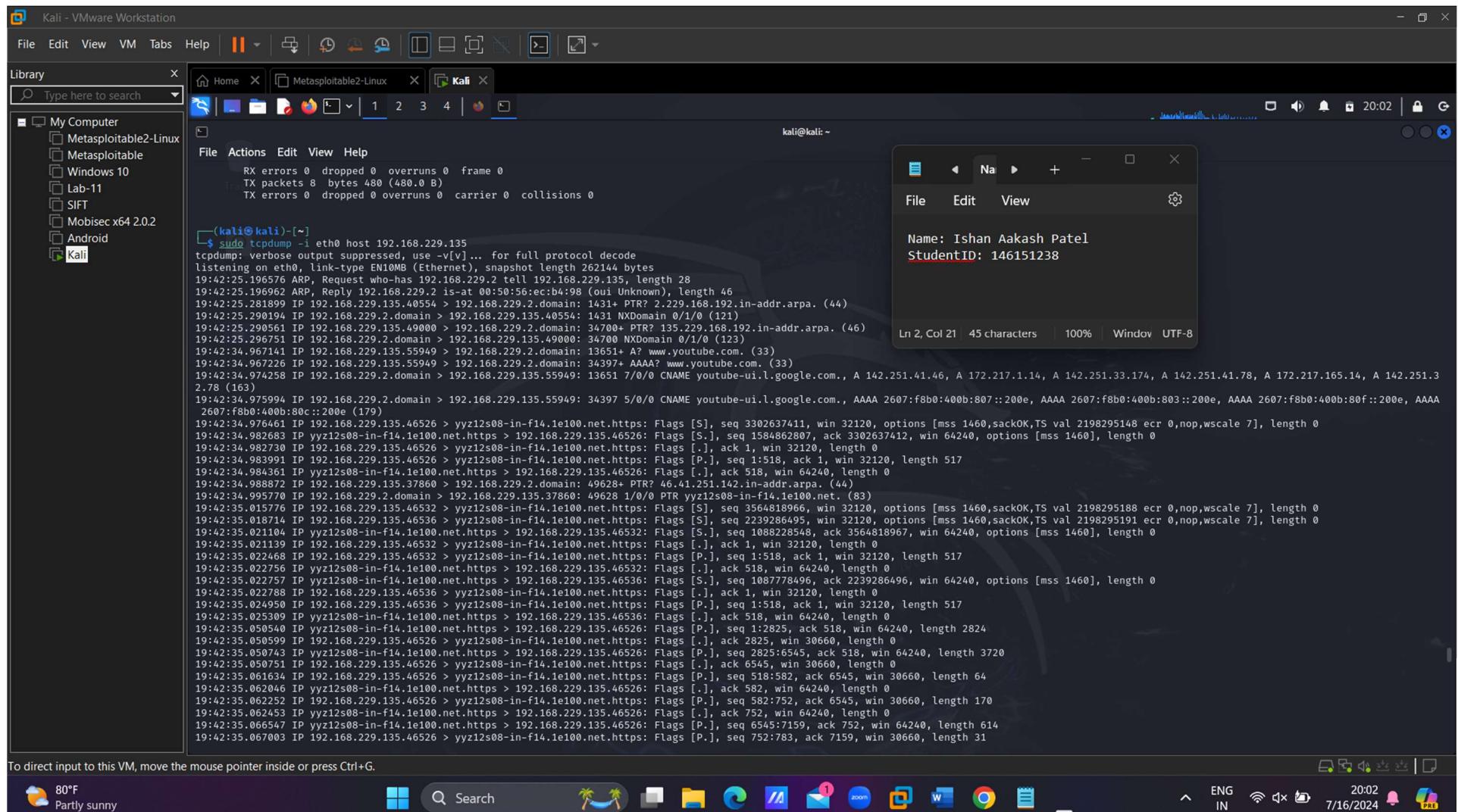
Ln 2, Col 21 | 45 characters | 100%

## Step 6: Apply Basic Filters

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 tcp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:41:15.514860 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [S], seq 2114452386, win 32120, options [mss 1460,sackOK,TS val 442482886 ecr 0,nop,wscale 7], length 0
19:41:15.522356 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [S.], seq 1013469980, ack 2114452387, win 64240, options [mss 1460], length 0
19:41:15.52491 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [.], ack 1, win 32120, length 0
19:41:15.527553 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1:518, ack 1, win 32120, length 517
19:41:15.528300 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 518, win 64240, length 0
19:41:15.582359 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [P.], seq 1:2869, ack 518, win 64240, length 2868
19:41:15.582401 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [.], ack 2869, win 30660, length 0
19:41:15.603553 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 518:582, ack 2869, win 30660, length 64
19:41:15.603893 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 582, win 64240, length 0
19:41:15.616753 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 582:752, ack 2869, win 30660, length 170
19:41:15.617012 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 752, win 64240, length 0
19:41:15.664424 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [P.], seq 2869:3381, ack 752, win 64240, length 512
19:41:15.664487 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 752:783, ack 3381, win 30660, length 31
19:41:15.665181 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 783, win 64240, length 0
19:41:15.669780 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [P.], seq 3381:3412, ack 783, win 64240, length 31
19:41:15.716565 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [.], ack 3412, win 30660, length 0
19:41:16.155329 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 783:1100, ack 3412, win 30660, length 317
19:41:16.156440 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1100, win 64240, length 0
19:41:16.326351 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [P.], seq 3412:19962, ack 1100, win 64240, length 16550
19:41:16.326412 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [.], ack 19962, win 30660, length 0
19:41:16.422652 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1100:1257, ack 19962, win 30660, length 157
19:41:16.423132 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1257, win 64240, length 0
19:41:16.423611 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1257:1357, ack 19962, win 30660, length 100
19:41:16.423945 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1357, win 64240, length 0
19:41:16.424297 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1357:1461, ack 19962, win 30660, length 104
19:41:16.425298 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1461, win 64240, length 0
19:41:16.426253 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1461:1547, ack 19962, win 30660, length 86
19:41:16.426584 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1547, win 64240, length 0
19:41:16.428045 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1547:1634, ack 19962, win 30660, length 87
19:41:16.428433 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1634, win 64240, length 0
19:41:16.429072 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1634:1716, ack 19962, win 30660, length 82
19:41:16.429393 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1716, win 64240, length 0
19:41:16.429897 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1716:1799, ack 19962, win 30660, length 83
19:41:16.430193 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1799, win 64240, length 0
19:41:16.430785 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1799:1881, ack 19962, win 30660, length 82
19:41:16.431095 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1881, win 64240, length 0
19:41:16.431670 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1881:1965, ack 19962, win 30660, length 84
19:41:16.431976 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 1965, win 64240, length 0
19:41:16.432838 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 1965:2050, ack 19962, win 30660, length 85
19:41:16.433129 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 2050, win 64240, length 0
19:41:16.433501 IP 192.168.229.135.52946 > 104.18.4.159.https: Flags [P.], seq 2050:2132, ack 19962, win 30660, length 82
19:41:16.433805 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [.], ack 2132, win 64240, length 0
19:41:16.439308 IP 104.18.4.159.https > 192.168.229.135.52946: Flags [P.], seq 19962:24369, ack 2132, win 64240, length 4407
```

The screenshot shows a Kali Linux VM interface. At the top, there's a toolbar with various icons. Below it is a navigation bar with tabs for Home, Metasploitable2-Linux, and Kali. The main window contains a terminal session where the user has run 'tcpdump -i eth0 tcp' to capture network traffic. The terminal output lists numerous TCP packets being captured between the Kali host and an external IP (104.18.4.159). A small note at the bottom left says 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.' On the right side, there's a small window showing a student profile with the name 'Ishan Akash Patel' and StudentID '146151238'. The bottom of the screen features a dock with various application icons, and the status bar shows the date and time as '7/16/2024 20:01'.



```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:43:58.384623 IP 192.168.229.135.60344 > yyz12s07-in-f3.1e100.net.http: Flags [.], ack 1072840992, win 31545, length 0
19:43:58.384706 IP 192.168.229.135.60344 > yyz12s07-in-f3.1e100.net.http: Flags [.], ack 73242109, win 31545, length 0
19:43:58.384804 IP yyz12s07-in-f3.1e100.net.http > 192.168.229.135.60344: Flags [.], ack 1, win 64240, length 0
19:43:58.384805 IP yyz12s07-in-f3.1e100.net.http > 192.168.229.135.60344: Flags [.], ack 1, win 64240, length 0
19:43:58.636625 IP 192.168.229.135.54478 > yyz12s07-in-f3.1e100.net.http: Flags [.], ack 987241028, win 31545, length 0
19:43:58.636884 IP yyz12s07-in-f3.1e100.net.http > 192.168.229.135.54478: Flags [.], ack 1, win 64240, length 0
19:43:59.916595 IP 192.168.229.135.37614 > server-18-67-33-215.yt050.r.cloudfront.net.http: Flags [.], ack 1118835498, win 31177, length 0
19:43:59.917000 IP server-18-67-33-215.yt050.r.cloudfront.net.http > 192.168.229.135.37614: Flags [.], ack 1, win 64240, length 0
19:44:00.428664 IP 192.168.229.135.33786 > server-18-67-33-215.yt050.r.cloudfront.net.http: Flags [.], ack 73287235, win 31176, length 0
19:44:00.429492 IP server-18-67-33-215.yt050.r.cloudfront.net.http > 192.168.229.135.33786: Flags [.], ack 1, win 64240, length 0
19:44:01.200058 IP 192.168.229.135.42224 > cloudproxy10041.sucuri.net.http: Flags [.], ack 354226527, win 30660, length 0
19:44:01.200708 IP cloudproxy10041.sucuri.net.http > 192.168.229.135.42224: Flags [.], ack 1, win 64240, length 0
19:44:03.923917 IP cloudproxy10041.sucuri.net.http > 192.168.229.135.42224: Flags [FP.], seq 1, ack 1, win 64240, length 0
19:44:03.924211 IP 192.168.229.135.42224 > cloudproxy10041.sucuri.net.http: Flags [F.], seq 1, ack 2, win 30660, length 0
19:44:03.924787 IP cloudproxy10041.sucuri.net.http > 192.168.229.135.42224: Flags [.], ack 2, win 64239, length 0
^C
15 packets captured
15 packets received by filter
0 packets dropped by kernel

(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 'tcp port 80 and (((ip[2:2] - ((ip[0] & 0xf) << 2)) - ((tcp[12] & 0xf0) >> 2)) = 0x47455420)'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode

```

Name: Ishan Aakash Patel  
StudentID: 146151238

## Step 7: Advanced Filtering

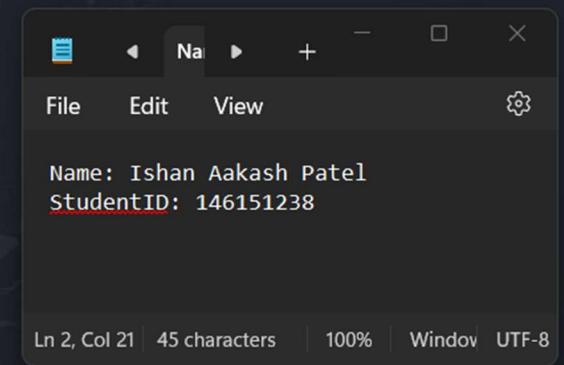
```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 'tcp port 80 and (((ip[2:2] - ((ip[0] & 0xf) << 2)) - ((tcp[12] & 0xf0) >> 2)) = 0x47455420)'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 'tcp port 80 and (((ip[2:2] - ((ip[0] & 0xf) << 2)) - ((tcp[12] & 0xf0) >> 2)) = 0x47455420)'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
```

Name: Ishan Aakash Patel  
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100%

```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 port 53
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:52:07.857835 IP 192.168.229.135.57708 > 192.168.229.2.domain: 62414+ A? forums.kali.org. (33)
19:52:07.858351 IP 192.168.229.135.57708 > 192.168.229.2.domain: 48820+ AAAA? forums.kali.org. (33)
19:52:07.909590 IP 192.168.229.135.49772 > 192.168.229.2.domain: 56224+ PTR? 2.229.168.192.in-addr.arpa. (44)
19:52:07.922956 IP 192.168.229.2.domain > 192.168.229.135.57708: 62414 2/0/0 A 104.18.5.159, A 104.18.4.159 (65)
19:52:07.924184 IP 192.168.229.2.domain > 192.168.229.135.57708: 48820 2/0/0 AAAA 2606:4700::6812:49f, AAAA 2606:4700::6812:59f (89)
19:52:07.940958 IP 192.168.229.2.domain > 192.168.229.135.49772: 56224 NXDomain 0/1/0 (121)
19:52:07.942248 IP 192.168.229.135.54971 > 192.168.229.2.domain: 4045+ PTR? 135.229.168.192.in-addr.arpa. (46)
19:52:08.066441 IP 192.168.229.2.domain > 192.168.229.135.54971: 4045 NXDomain 0/1/0 (123)
19:52:12.329629 IP 192.168.229.135.41062 > 192.168.229.2.domain: 47943+ A? www.facebook.com. (34)
19:52:12.614761 IP 192.168.229.135.40902 > 192.168.229.2.domain: 40966+ A? static.xx.fbcdn.net. (37)
19:52:12.671984 IP 192.168.229.135.50839 > 192.168.229.2.domain: 51836+ A? scontent-yyz1-1.xx.fbcdn.net. (46)
19:52:12.672231 IP 192.168.229.135.50839 > 192.168.229.2.domain: 19783+ AAAA? scontent-yyz1-1.xx.fbcdn.net. (46)
19:52:13.435725 IP 192.168.229.2.domain > 192.168.229.135.41062: 47943 2/0/0 CNAME star-mini.c10r.facebook.com., A 31.13.80.36 (79)
19:52:13.436215 IP 192.168.229.135.51845 > 192.168.229.2.domain: 24920+ A? www.facebook.com. (34)
19:52:13.436346 IP 192.168.229.135.51845 > 192.168.229.2.domain: 36698+ AAAA? www.facebook.com. (34)
19:52:13.534848 IP 192.168.229.2.domain > 192.168.229.135.40902: 40966 2/0/0 CNAME scontent.xx.fbcdn.net., A 31.13.80.12 (76)
19:52:13.534848 IP 192.168.229.2.domain > 192.168.229.135.50839: 51836 1/0/0 A 31.13.80.12 (62)
19:52:13.534848 IP 192.168.229.2.domain > 192.168.229.135.50839: 19783 1/0/0 AAAA 2a03:2880:f00e:13:face:b00c:0:3 (74)
19:52:13.536872 IP 192.168.229.2.domain > 192.168.229.135.51845: 24920 2/0/0 CNAME star-mini.c10r.facebook.com., A 31.13.80.36 (79)
19:52:13.536873 IP 192.168.229.2.domain > 192.168.229.135.51845: 36698 2/0/0 CNAME star-mini.c10r.facebook.com., AAAA 2a03:2880:f10e:83:face:b00c:0:25de (91)
19:52:14.072209 IP 192.168.229.135.51771 > 192.168.229.2.domain: 37831+ A? static.xx.fbcdn.net. (37)
19:52:14.072290 IP 192.168.229.135.51771 > 192.168.229.2.domain: 43713+ AAAA? static.xx.fbcdn.net. (37)
19:52:14.319119 IP 192.168.229.2.domain > 192.168.229.135.51771: 37831 2/0/0 CNAME scontent.xx.fbcdn.net., A 31.13.80.12 (76)
19:52:14.319120 IP 192.168.229.2.domain > 192.168.229.135.51771: 43713 2/0/0 CNAME scontent.xx.fbcdn.net., AAAA 2a03:2880:f00e:13:face:b00c:0:3 (88)
^C
24 packets captured
24 packets received by filter
0 packets dropped by kernel
```



A screenshot of a terminal window showing student information. The window has a dark theme with light-colored text. At the top, there are standard window controls (minimize, maximize, close) and a menu bar with 'File', 'Edit', and 'View'. Below the menu, the text 'Name: Ishan Aakash Patel' and 'StudentID: 146151238' is displayed in a monospaced font. At the bottom of the window, there is status information: 'Ln 2, Col 21 | 45 characters | 100% | Window UTF-8'.

```
Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window UTF-8
```

## Step 8: Verbose and Timestamp Options

The screenshot shows a Kali Linux terminal window titled "Kali - VMware Workstation". The terminal is running a command to capture network traffic on interface eth0:

```
sudo tcpdump -i eth0 -v
```

The output of the command is displayed in the terminal window, showing numerous network packets with detailed timestamp and verbose information. A small window titled "Nautilus" is open in the background, showing a file browser with the path "Metasploitable2-Linux". The status bar at the bottom of the screen shows system information like weather (80°F, Partly sunny), date (7/16/2024), and time (20:04).

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:52:48.812633 IP (tos 0x0, ttl 64, id 48652, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55366 > 146.190.62.39.http: Flags [.], cksum 0x7730 (incorrect → 0xad70), ack 1891904769, win 30660, length 0
19:52:48.812737 IP (tos 0x0, ttl 64, id 58456, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55373 > 146.190.62.39.http: Flags [.], cksum 0x7730 (incorrect → 0x170d), ack 3791473777, win 31675, length 0
19:52:48.812741 IP (tos 0x0, ttl 64, id 33559, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55362 > 146.190.62.39.http: Flags [.], cksum 0x7730 (incorrect → 0x5631), ack 1294888190, win 30660, length 0
19:52:48.812780 IP (tos 0x0, ttl 64, id 57556, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55374 > 146.190.62.39.http: Flags [.], cksum 0x7730 (incorrect → 0x83da), ack 1354988102, win 31136, length 0
19:52:48.812891 IP (tos 0x0, ttl 128, id 15425, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55366: Flags [.], cksum 0x2a43 (correct), ack 1, win 64240, length 0
19:52:48.812998 IP (tos 0x0, ttl 128, id 15426, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55378: Flags [.], cksum 0x97d6 (correct), ack 1, win 64240, length 0
19:52:48.812999 IP (tos 0x0, ttl 128, id 15427, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55362: Flags [.], cksum 0xd303 (correct), ack 1, win 64240, length 0
19:52:48.812999 IP (tos 0x0, ttl 128, id 15428, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55374: Flags [.], cksum 0x0289 (correct), ack 1, win 64240, length 0
19:52:48.901805 IP (tos 0x0, ttl 64, id 62150, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.229.135.39257 > 192.168.229.2.domain: 60664+ PTR? 39.62.190.146.in-addr.arpa. (44)
19:52:48.928068 IP (tos 0x0, ttl 128, id 15429, offset 0, flags [none], proto UDP (17), length 139)
    192.168.229.2.domain > 192.168.229.135.39257: 60664 NXDomain 0/1/0 (111)
19:52:48.929037 IP (tos 0x0, ttl 64, id 19440, offset 0, flags [DF], proto UDP (17), length 74)
    192.168.229.135.52136 > 192.168.229.2.domain: 10439+ PTR? 135.229.168.192.in-addr.arpa. (46)
19:52:49.012656 IP (tos 0x0, ttl 128, id 15430, offset 0, flags [none], proto UDP (17), length 151)
    192.168.229.2.domain > 192.168.229.135.52136: 10439 NXDomain 0/1/0 (123)
19:52:49.013115 IP (tos 0x0, ttl 64, id 35840, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.229.135.48522 > 192.168.229.2.domain: 34048+ PTR? 2.229.168.192.in-addr.arpa. (44)
19:52:49.047892 IP (tos 0x0, ttl 128, id 15431, offset 0, flags [none], proto UDP (17), length 149)
    192.168.229.2.domain > 192.168.229.135.48522: 34048 NXDomain 0/1/0 (121)
19:52:51.333801 IP (tos 0x0, ttl 128, id 15432, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55362: Flags [FP.], cksum 0xd2fa (correct), seq 1, ack 1, win 64240, length 0
19:52:51.333803 IP (tos 0x0, ttl 128, id 15433, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55374: Flags [FP.], cksum 0x0280 (correct), seq 1, ack 1, win 64240, length 0
19:52:51.333804 IP (tos 0x0, ttl 128, id 15434, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55366: Flags [FP.], cksum 0x2a3a (correct), seq 1, ack 1, win 64240, length 0
19:52:51.334275 IP (tos 0x0, ttl 64, id 48653, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55366 > 146.190.62.39.http: Flags [F.], cksum 0x7730 (incorrect → 0xad6d), seq 1, ack 2, win 30660, length 0
19:52:51.334735 IP (tos 0x0, ttl 64, id 57557, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55374 > 146.190.62.39.http: Flags [F.], cksum 0x7730 (incorrect → 0x83d7), seq 1, ack 2, win 31136, length 0
19:52:51.335190 IP (tos 0x0, ttl 128, id 15435, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55366: Flags [.], cksum 0x2a42 (correct), ack 2, win 64239, length 0
19:52:51.335554 IP (tos 0x0, ttl 128, id 15436, offset 0, flags [none], proto TCP (6), length 40)
    146.190.62.39.http > 192.168.229.135.55374: Flags [.], cksum 0x0288 (correct), ack 2, win 64239, length 0
19:52:51.335695 IP (tos 0x0, ttl 64, id 33560, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.229.135.55362 > 146.190.62.39.http: Flags [F.], cksum 0x7730 (incorrect → 0x562e), seq 1, ack 2, win 30660, length 0
```

## Step 9: Limit the Number of Packets

```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 -c 10
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:53:49.996702 IP 192.168.229.135.49504 > 93.184.215.14.http: Flags [.], ack 758794819, win 31217, length 0
19:53:49.997382 IP 93.184.215.14.http > 192.168.229.135.49504: Flags [.], ack 1, win 64240, length 0
19:53:50.062007 IP 192.168.229.135.34122 > 192.168.229.2.domain: 16301+ PTR? 14.215.184.93.in-addr.arpa. (44)
19:53:50.088859 IP 192.168.229.2.domain > 192.168.229.135.34122: 16301 NXDomain 0/1/0 (115)
19:53:50.089498 IP 192.168.229.135.56869 > 192.168.229.2.domain: 9014+ PTR? 135.229.168.192.in-addr.arpa. (46)
19:53:50.096608 IP 192.168.229.2.domain > 192.168.229.135.56869: 9014 NXDomain 0/1/0 (123)
19:53:50.165068 IP 192.168.229.135.45470 > 192.168.229.2.domain: 41035+ PTR? 2.229.168.192.in-addr.arpa. (44)
19:53:50.170180 IP 192.168.229.2.domain > 192.168.229.135.45470: 41035 NXDomain 0/1/0 (121)
19:53:57.580673 IP 192.168.229.135.51212 > 166.188.117.34.bc.googleusercontent.com.https: Flags [P.], seq 3042551947:3042551986, ack 104877257, win 31064, length 39
19:53:57.581900 IP 166.188.117.34.bc.googleusercontent.com.https > 192.168.229.135.51212: Flags [.], ack 39, win 64240, length 0
10 packets captured
14 packets received by filter
0 packets dropped by kernel

(kali㉿kali)-[~]
$
```

Name: Ishan Aakash Patel  
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

## Step 10: Analyzing the Captured Data

The screenshot shows the Wireshark interface running on a Kali Linux VM. The main window displays a list of network packets captured from the 'capture.pcap' file. The first few packets show a DNS query from 192.168.229.135 to 192.168.229.2 for the domain www.facebook.com. The packet details and bytes panes provide a detailed view of the captured data, including DNS records and HTTP headers. A small terminal window is visible at the bottom, showing the user's name and student ID. The system tray at the bottom right shows the date and time as 7/16/2024, 20:17.

capture.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.229.135	192.168.229.2	DNS	76	Standard query 0x9852 A www.facebook.com
2	0.000276	192.168.229.135	192.168.229.2	DNS	76	Standard query 0x685e AAAA www.facebook.com
3	0.007183	192.168.229.2	192.168.229.135	DNS	121	Standard query response 0x9852 A www.facebook.com CNAME star-mini.c10r.facebook.com A 31.13.80.36
4	0.017250	192.168.229.2	192.168.229.135	DNS	133	Standard query response 0x685e AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:28...
5	0.021498	192.168.229.135	31.13.80.36	QUIC	1399	0-RTT, DCID=16062db20977de51d, SCID=72c02d
6	0.028946	31.13.80.36	192.168.229.135	QUIC	1274	Initial, DCID=72c02d, SCID=9421009115ad6af4, PKN: 9040302, CRYPTO, ACK, PADDING
7	0.028948	31.13.80.36	192.168.229.135	QUIC	257	Handshake, DCID=72c02d, SCID=9421009115ad6af4
8	0.028949	31.13.80.36	192.168.229.135	QUIC	90	Protected Payload (KPO), DCID=72c02d
9	0.029594	31.13.80.36	192.168.229.135	QUIC	122	Protected Payload (KPO), DCID=72c02d
10	0.032117	192.168.229.135	31.13.80.36	QUIC	127	Handshake, DCID=9421009115ad6af4, SCID=72c02d
11	0.032932	192.168.229.135	31.13.80.36	QUIC	999	Protected Payload (KPO), DCID=9421009115ad6af4
12	0.037149	31.13.80.36	192.168.229.135	QUIC	84	Handshake, DCID=72c02d, SCID=9421009115ad6af4
13	0.037151	31.13.80.36	192.168.229.135	QUIC	154	Protected Payload (KPO), DCID=72c02d
14	0.037152	31.13.80.36	192.168.229.135	QUIC	314	Protected Payload (KPO), DCID=72c02d
15	0.037152	31.13.80.36	192.168.229.135	QUIC	90	Protected Payload (KPO), DCID=72c02d
16	0.038712	192.168.229.135	31.13.80.36	QUIC	76	Protected Payload (KPO), DCID=9421009115ad6af4
17	0.082481	31.13.80.36	192.168.229.135	QUIC	1274	Protected Payload (KPO), DCID=72c02d
18	0.082483	31.13.80.36	192.168.229.135	QUIC	1146	Protected Payload (KPO), DCID=72c02d
19	0.084471	192.168.229.135	31.13.80.36	QUIC	83	Protected Payload (KPO), DCID=9421009115ad6af4

Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)  
Ethernet II, Src: VMware\_a6:42:47 (00:0c:29:a6:42:47), Dst: VMware\_ec:b4:98 (00:50:56:ec:b4:98)  
Internet Protocol Version 4, Src: 192.168.229.135, Dst: 192.168.229.2  
User Datagram Protocol, Src Port: 33573, Dst Port: 53  
Domain Name System (query)

Name: Ishan Aakash Patel  
StudentID: 146151238

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

File Edit View File Edit View Name: Ishan Aakash Patel StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window UTF-8 | Packets: 1964 · Displayed: 1964 (100.0%) | Profile: Default

77°F Mostly sunny

Search

2017 IN 7/16/2024 ENG

Kali - VMware Workstation

File Edit View VM Help || Library Metasploitable2-Linux Kali

Type here to search

My Computer Metasploitable2-Linux Metasploitable Windows 10 Lab-1 SIFT Mobisec x64 2.0.2 Android Kali

capture.pcap

tcp

No.	Time	Source	Destination	Protocol	Length	Info
21	1.262277	192.168.229.135	192.229.211.108	TCP	54	41452 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
22	1.262857	192.229.211.108	192.168.229.135	TCP	60	[TCP ACKed unseen segment] 80 → 41452 [ACK] Seq=1 Ack=2 Win=64240 Len=0
25	6.554558	192.168.229.135	142.251.41.36	TCP	74	33230 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=743695465 TSecr=0 WS=128
29	6.559529	142.251.41.36	192.168.229.135	TCP	60	443 → 33230 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
31	6.559618	192.168.229.135	142.251.41.36	TCP	54	33230 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
34	6.562557	192.168.229.135	142.251.41.36	TLSv1.3	713	Client Hello (SNI=www.google.com)
35	6.563039	142.251.41.36	192.168.229.135	TCP	60	443 → 33230 [ACK] Seq=1 Ack=660 Win=64240 Len=0
36	6.563095	192.168.229.135	142.251.41.36	TLSv1.3	6	Change Cipher Spec
37	6.563219	192.168.229.135	142.251.41.36	TLSv1.3	224	Application Data
38	6.563379	142.251.41.36	192.168.229.135	TCP	60	443 → 33230 [ACK] Seq=1 Ack=666 Win=64240 Len=0
39	6.563557	142.251.41.36	192.168.229.135	TCP	60	443 → 33230 [ACK] Seq=1 Ack=836 Win=64240 Len=0
40	6.563731	192.168.229.135	172.217.165.3	TCP	74	37274 → 443 [SYN] Seq=0 Win=32120 MSS=1460 SACK_PERM TStamp=2094559960 TSecr=0 WS=128
43	6.570915	192.168.229.135	172.217.1.3	TCP	74	59432 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=3716755095 TSecr=0 WS=128
47	6.594539	172.217.1.3	192.168.229.135	TCP	60	443 → 59432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
49	6.594540	172.217.165.3	192.168.229.135	TCP	60	443 → 37274 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
51	6.594573	192.168.229.135	172.217.1.3	TCP	54	59432 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
52	6.594630	192.168.229.135	172.217.165.3	TCP	54	37274 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
53	6.598797	192.168.229.135	172.217.1.3	TLSv1.3	571	Client Hello (SNI=www.gstatic.com)
54	6.599187	172.217.1.3	192.168.229.135	TCP	60	443 → 59432 [ACK] Seq=1 Ack=518 Win=64240 Len=0

Frame 21: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)  
Ethernet II, Src: VMware\_a6:42:47 (00:0c:29:a6:42:47), Dst: VMware\_ec:b4:98 (00:50:56:ec:b4:98)  
Internet Protocol Version 4, Src: 192.168.229.135, Dst: 192.229.211.108  
Transmission Control Protocol, Src Port: 41452, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000 00 50 56 ec b4 98 00 0c 29 a6 42 47 08 00 45 00 .PV..... BG.E.  
0010 00 28 64 65 40 00 40 06 9b e8 c0 a8 e5 87 c0 e5 .(de@. ....  
0020 d3 6c a1 ec 00 50 0d d7 23 d2 5c 47 59 49 50 10 l..P. # \GYIP.  
0030 7b cb 3a 9d 00 00 { :...  
File Edit View Name: Ishan Aakash Patel  
StudentID: 146151238  
Ln 2, Col 21 45 characters 100% Window UTF-8 Packets: 1964 - Displayed: 626 (31.9%) Profile: Default  
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.  
Upcoming Earnings Search Zoom Mail WPS Office Google Chrome Microsoft Word Microsoft Excel ENG IN 20:18 7/16/2024 PRE

## Installing NetworkMiner

```
kali@kali: /opt/NetworkMiner_2-9
File Actions Edit View Help
inflating: /opt/NetworkMiner_2-9/NetworkMiner.exe
inflating: /opt/NetworkMiner_2-9/NetworkWrapper.dll
inflating: /opt/NetworkMiner_2-9/PacketHandlerFramework.dll
inflating: /opt/NetworkMiner_2-9/PacketParser.dll
inflating: /opt/NetworkMiner_2-9/SharedUtils.dll

└─(kali㉿kali)-[~]
$ cd /opt/
└─(kali㉿kali)-[/opt]
$ ls
microsoft NetworkMiner_2-9

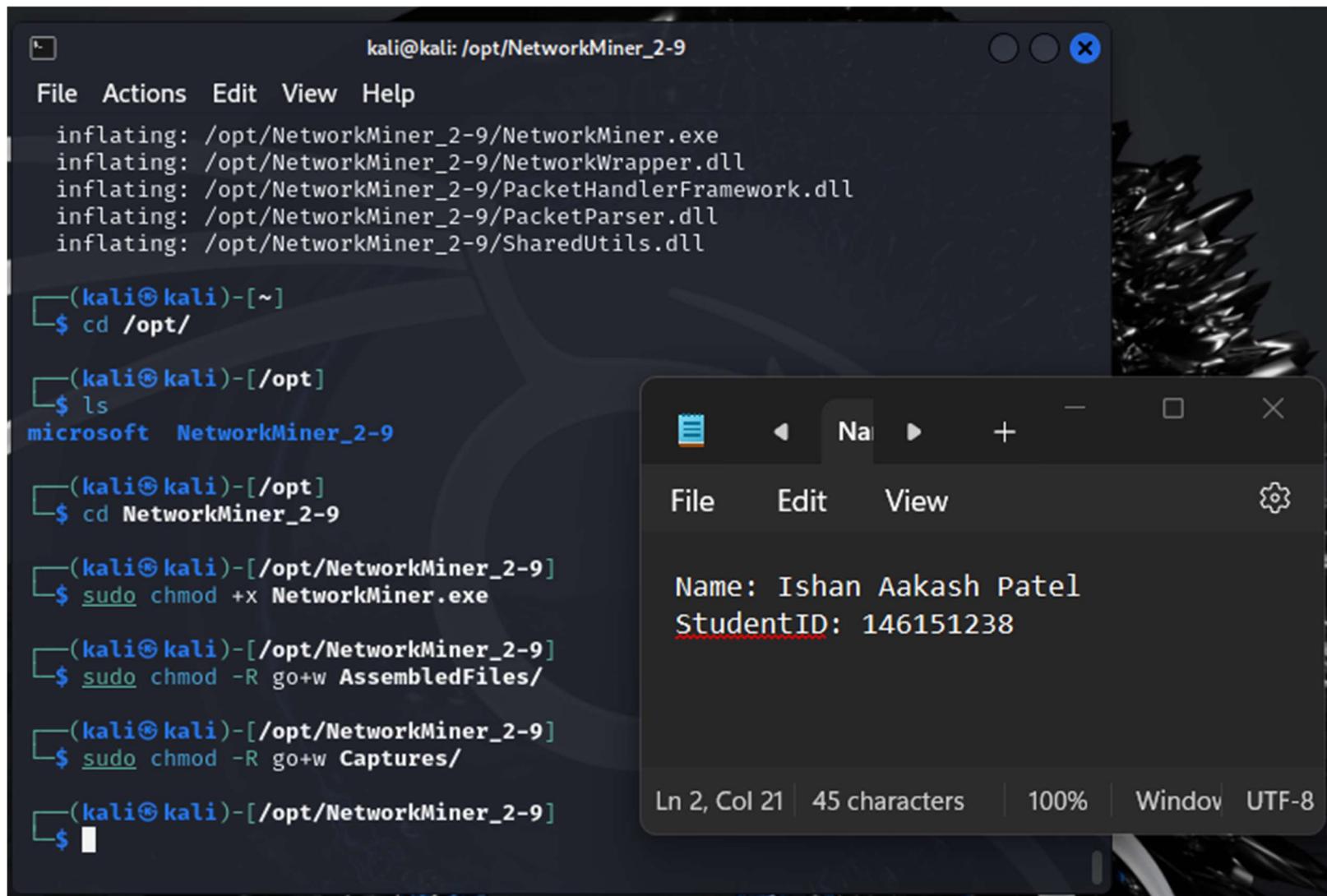
└─(kali㉿kali)-[/opt]
$ cd NetworkMiner_2-9

└─(kali㉿kali)-[/opt/NetworkMiner_2-9]
$ sudo chmod +x NetworkMiner.exe

└─(kali㉿kali)-[/opt/NetworkMiner_2-9]
$ sudo chmod -R go+w AssembledFiles/

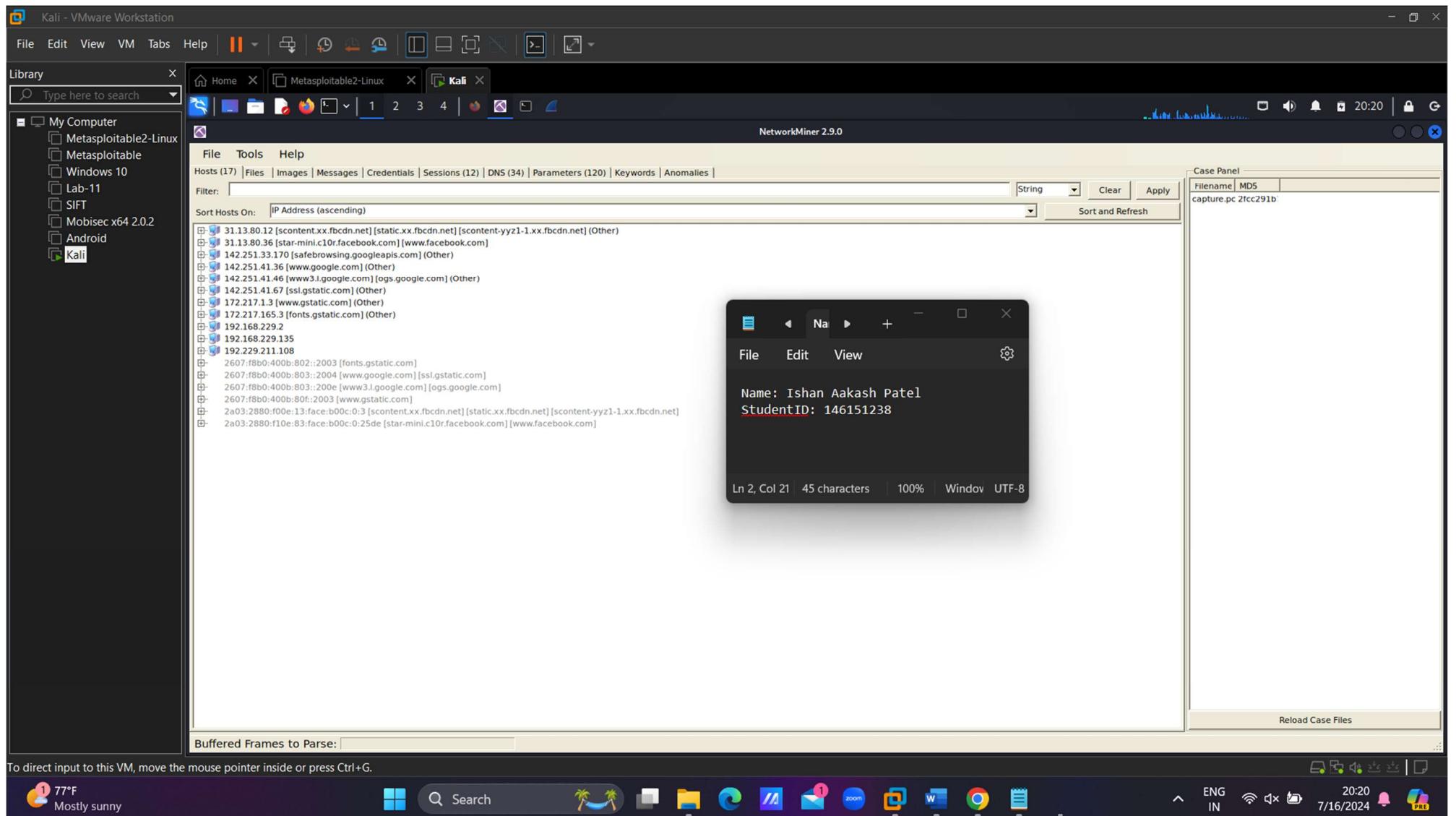
└─(kali㉿kali)-[/opt/NetworkMiner_2-9]
$ sudo chmod -R go+w Captures/

└─(kali㉿kali)-[/opt/NetworkMiner_2-9]
$ ┌───┐
```



Name: Ishan Aakash Patel  
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8



Kali - VMware Workstation

File Edit View VM Help | Library | Metasploitable2-Linux | Kali | Home | 1 2 3 4 | NetworkMiner 2.9.0 | 20:21 | 2021 | 7/16/2024 | PRE

**Library**

Type here to search

- My Computer
  - Metasploitable2-Linux
  - Metasploitable
  - Windows 10
  - Lab-11
  - SIFT
  - Mobisec x64 2.0.2
  - Android
  - Kali

**NetworkMiner 2.9.0**

File Tools Help

Hosts (17) | Files | Images | Messages | Credentials | Sessions (12) | DNS (34) | Parameters (120) | Keywords | Anomalies | Filter keyword:

Frame nr.	Timestamp	client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer
3	2024-07-16 23:38:05 UTC	192.168.229.135	33573	192.168.229.2	53	128	0:00:05	0x9852	0x0005 (CNAME)	www.facebook.com	star-mini.c10r.facebook.com
3	2024-07-16 23:38:05 UTC	192.168.229.135	33573	192.168.229.2	53	128	0:00:05	0x9852	0x0001 (HostAddress)	star-mini.c10r.facebook.com	31.13.80.36
4	2024-07-16 23:38:05 UTC	192.168.229.135	33573	192.168.229.2	53	128	0:00:05	0x685E	0x0005 (CNAME)	www.facebook.com	star-mini.c10r.facebook.com
4	2024-07-16 23:38:05 UTC	192.168.229.135	33573	192.168.229.2	53	128	0:00:05	0x685E	0x001C (AAAA)	star-mini.c10r.facebook.com	2a03:2880:f10e:83:face:b00c:0:25de
27	2024-07-16 23:38:12 UTC	192.168.229.135	38214	192.168.229.2	53	128	0:00:05	0x161A	0x0001 (HostAddress)	www.google.com	142.251.41.36
28	2024-07-16 23:38:12 UTC	192.168.229.135	60518	192.168.229.2	53	128	0:00:05	0x0363	0x0001 (HostAddress)	fonts.gstatic.com	172.217.165.3
30	2024-07-16 23:38:12 UTC	192.168.229.135	60518	192.168.229.2	53	128	0:00:05	0x236F	0x001C (AAAA)	fonts.gstatic.com	2607:f8b0:400b:802::2003
41	2024-07-16 23:38:12 UTC	192.168.229.135	39641	192.168.229.2	53	128	0:00:05	0x1F73	0x0001 (HostAddress)	www.gstatic.com	172.217.1.3
42	2024-07-16 23:38:12 UTC	192.168.229.135	39641	192.168.229.2	53	128	0:00:05	0x7B6F	0x001C (AAAA)	www.gstatic.com	2607:f8b0:400b:80f::2003
48	2024-07-16 23:38:12 UTC	192.168.229.135	54178	192.168.229.2	53	128	0:00:05	0x0420	0x0001 (HostAddress)	www.google.com	142.251.41.36
50	2024-07-16 23:38:12 UTC	192.168.229.135	54178	192.168.229.2	53	128	0:00:05	0xA31E	0x001C (AAAA)	www.google.com	2607:f8b0:400b:803::2004
101	2024-07-16 23:38:12 UTC	192.168.229.135	55928	192.168.229.2	53	128	0:00:05	0x5314	0x0001 (HostAddress)	www.gstatic.com	172.217.1.3
102	2024-07-16 23:38:12 UTC	192.168.229.135	36683	192.168.229.2	53	128	0:00:05	0x17C4	0x0001 (HostAddress)	fonts.gstatic.com	172.217.165.3
103	2024-07-16 23:38:12 UTC	192.168.229.135	36683	192.168.229.2	53	128	0:00:05	0xAF56	0x001C (AAAA)	fonts.gstatic.com	2607:f8b0:400b:802::2003
104	2024-07-16 23:38:12 UTC	192.168.229.135	55928	192.168.229.2	53	128	0:00:05	0xB817	0x001C (AAAA)	www.gstatic.com	2607:f8b0:400b:80f::2003
355	2024-07-16 23:38:14 UTC	192.168.229.135	50902	192.168.229.2	53	128	0:00:05	0xD908	0x0005 (CNAME)	static.xx.fbcdn.net	scontent.xx.fbcdn.net
355	2024-07-16 23:38:14 UTC	192.168.229.135	50902	192.168.229.2	53	128	0:00:05	0x9D08	0x0001 (HostAddress)	scontent.xx.fbcdn.net	31.13.80.12
356	2024-07-16 23:38:14 UTC	192.168.229.135	50902	192.168.229.2	53	128	0:00:05	0xAC0C	0x0005 (CNAME)	static.xx.fbcdn.net	scontent.xx.fbcdn.net
356	2024-07-16 23:38:14 UTC	192.168.229.135	50902	192.168.229.2	53	128	0:00:05	0x0AC0C	0x001C (AAAA)	scontent.xx.fbcdn.net	2a03:2880:f00e:13:face:b00c:0:3
551	2024-07-16 23:38:14 UTC	192.168.229.135	36260	192.168.229.2	53	128	0:00:05	0x6A23	0x0001 (HostAddress)	scontent.xx.fbcdn.net	31.13.80.12
552	2024-07-16 23:38:14 UTC	192.168.229.135	36260	192.168.229.2	53	128	0:00:05	0x8521	0x001C (AAAA)	scontent.xx.fbcdn.net	2a03:2880:f00e:13:face:b00c:0:3
613	2024-07-16 23:38:14 UTC	192.168.229.135	48905	192.168.229.2	53	128	0:00:05	0x93C3	0x0005 (CNAME)	static.xx.fbcdn.net	scontent.xx.fbcdn.net
613	2024-07-16 23:38:14 UTC	192.168.229.135	48905	192.168.229.2	53	128	0:00:05	0x93C3	0x0001 (HostAddress)	scontent.xx.fbcdn.net	31.13.80.12
616	2024-07-16 23:38:14 UTC	192.168.229.135	48905	192.168.229.2	53	128	0:00:05	0xA6C1	0x0005 (CNAME)	static.xx.fbcdn.net	scontent.xx.fbcdn.net
616	2024-07-16 23:38:14 UTC	192.168.229.135	48905	192.168.229.2	53	128	0:00:05	0xA6C1	0x001C (AAAA)	scontent.xx.fbcdn.net	2a03:2880:f00e:13:face:b00c:0:3
1105	2024-07-16 23:38:16 UTC	192.168.229.135	36388	192.168.229.2	53	128	0:00:05	0x1EE2	0x0001 (HostAddress)	scontent-yz1-1.xx.fbcdn.net	31.13.80.12
1106	2024-07-16 23:38:16 UTC	192.168.229.135	36388	192.168.229.2	53	128	0:00:05	0xA6FF	0x001C (AAAA)	scontent-yz1-1.xx.fbcdn.net	2a03:2880:f00e:13:face:b00c:0:3
1328	2024-07-16 23:38:16 UTC	192.168.229.135	49174	192.168.229.2	53	128	0:00:05	0x164F	0x0001 (HostAddress)	safebrowsing.googleapis.com	142.251.33.170
1515	2024-07-16 23:38:18 UTC	192.168.229.135	37428	192.168.229.2	53	128	0:00:05	0x5850	0x0005 (CNAME)	ogs.google.com	www.3i.google.com
1515	2024-07-16 23:38:18 UTC	192.168.229.135	37428	192.168.229.2	53	128	0:00:05	0x5850	0x0001 (HostAddress)	www.3i.google.com	142.251.41.46
1516	2024-07-16 23:38:18 UTC	192.168.229.135	37428	192.168.229.2	53	128	0:00:05	0x9F4D	0x0005 (CNAME)	ogs.google.com	www.3i.google.com
1516	2024-07-16 23:38:18 UTC	192.168.229.135	37428	192.168.229.2	53	128	0:00:05	0x9F4D	0x001C (AAAA)	www.3i.google.com	2607:f8b0:400b:803::200e
1653	2024-07-16 23:38:18 UTC	192.168.229.135	48173	192.168.229.2	53	128	0:00:05	0x1C73	0x0001 (HostAddress)	ssl.gstatic.com	142.251.41.67
1654	2024-07-16 23:38:18 UTC	192.168.229.135	48173	192.168.229.2	53	128	0:00:05	0xF972	0x001C (AAAA)	ssl.gstatic.com	2607:f8b0:400b:804::2003

Case Panel  
Filename | MDS  
Capture.pc 2tcc291b

Name: Ishan Aakash Patel  
StudentID: 146151238

Ln 2, Col 21 45 characters | 100% | Window U

Reload Case Files

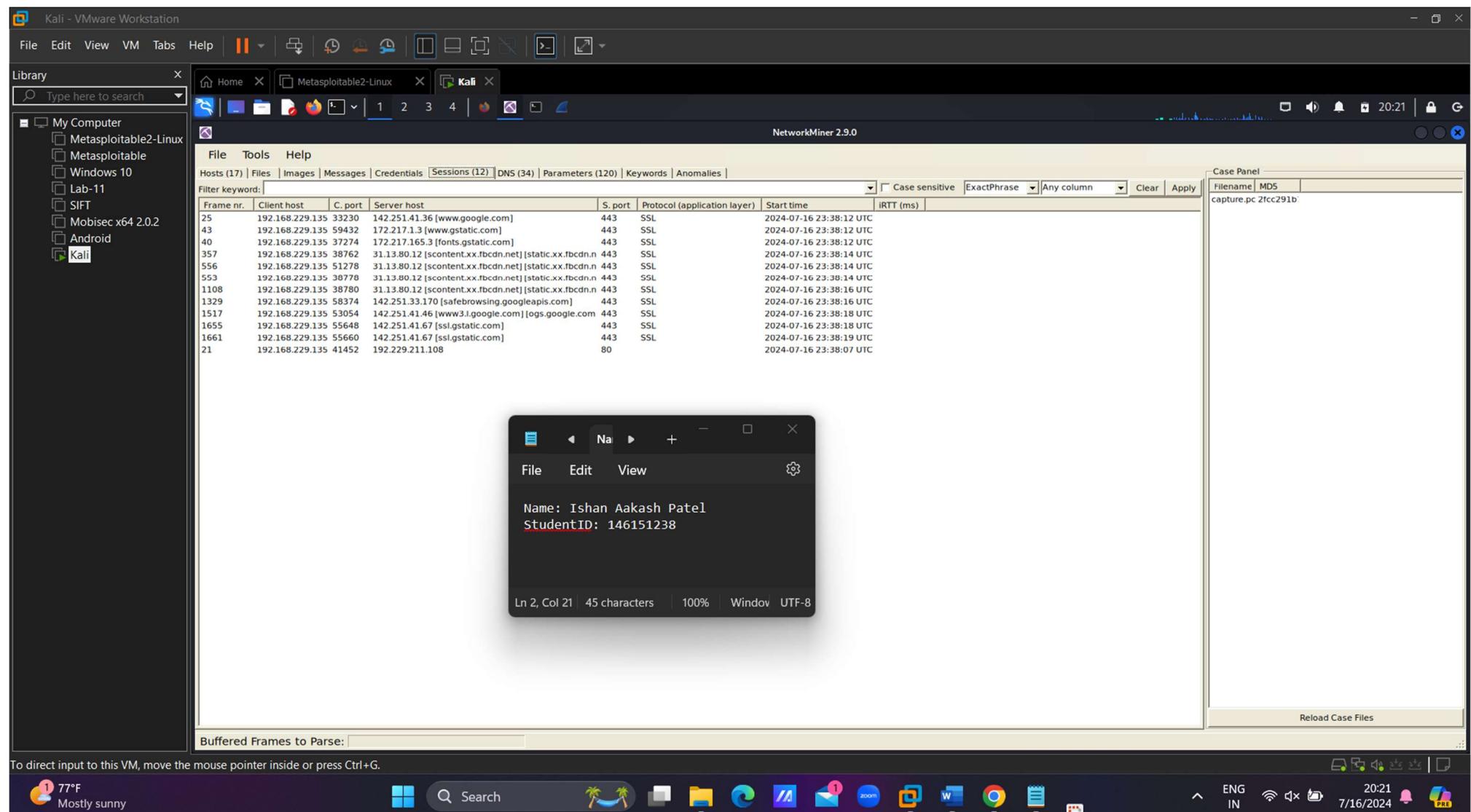
Buffered Frames to Parse:

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

77°F Mostly sunny

Search

File Edit View VM Help | Library | Metasploitable2-Linux | Kali | Home | 1 2 3 4 | NetworkMiner 2.9.0 | 20:21 | 2021 | 7/16/2024 | PRE



## **Learning Experience**

This lab was an enriching experience that allowed me to dive deep into the world of network traffic analysis using tcpdump. Initially, I was somewhat apprehensive about using a command-line tool for such a technical task. However, the step-by-step instructions provided a clear path to follow, which made the process manageable and even enjoyable. From installing tcpdump to capturing and analyzing packets, each step built on the previous one, reinforcing my understanding of network interfaces and packet structures. By the end of the lab, I felt much more confident in my ability to monitor and troubleshoot network issues using tcpdump.

One of the most valuable aspects of this lab was the hands-on practice with different filtering options. Learning how to capture only specific types of traffic, such as HTTP GET requests or DNS queries, provided practical skills that I can apply in real-world scenarios. Additionally, saving captured packets to a file and analyzing them later with Wireshark opened my eyes to the power of combining different tools for comprehensive network analysis. Overall, this lab not only enhanced my technical skills but also boosted my confidence in using command-line tools to perform detailed network diagnostics.