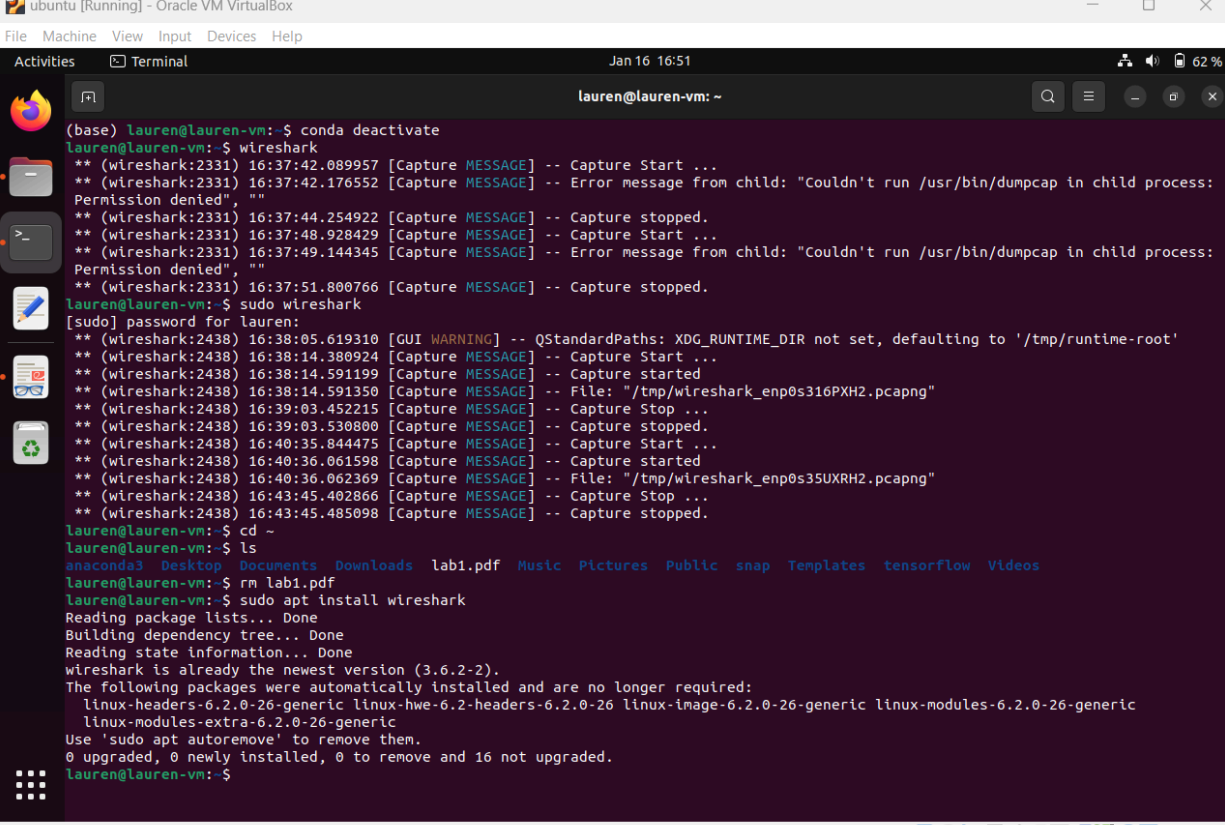


Lab 1 - Advanced Computer Networks

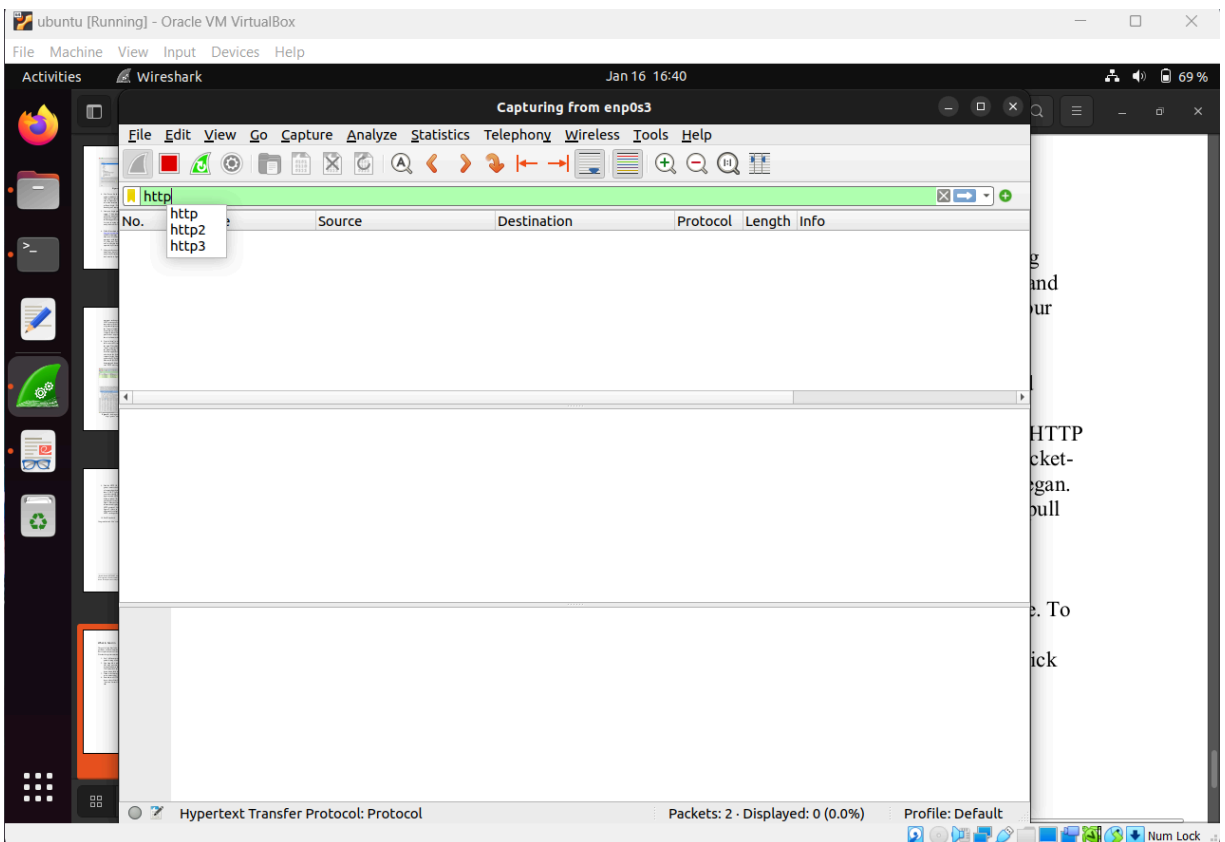
1. The first thing I did was install Wireshark on my Ubuntu 22.04 virtual machine. In this case I do not have the screenshot of the installation so below is a screenshot showing that I have the most updated version.



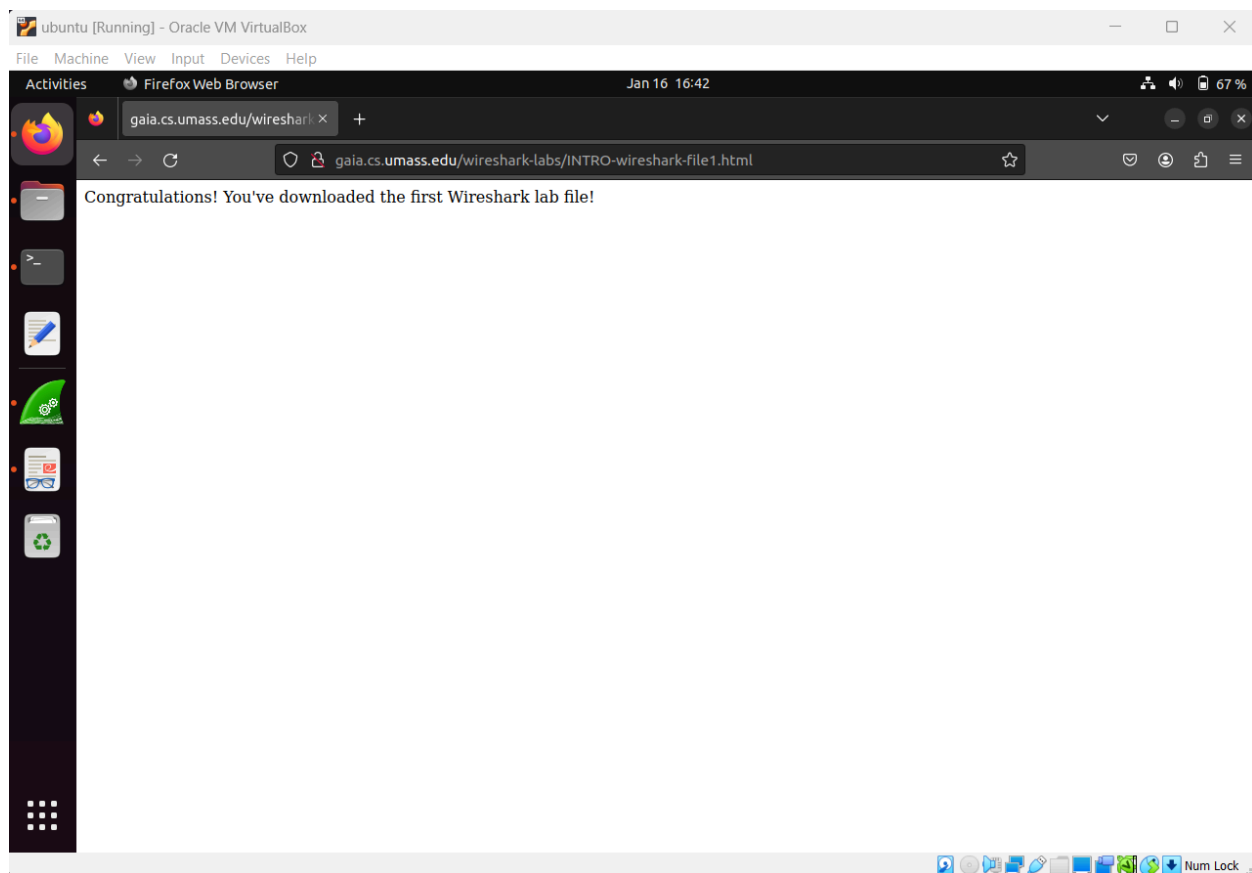
The screenshot shows a terminal window in an Oracle VM VirtualBox environment. The user is logged in as 'lauren' on a machine named 'lauren-vm'. The terminal output shows the following commands and their results:

```
(base) lauren@lauren-vm:~$ conda deactivate
lauren@lauren-vm:~$ wireshark
** (Wireshark:2331) 16:37:42.089957 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:2331) 16:37:42.176552 [Capture MESSAGE] -- Error message from child: "Couldn't run /usr/bin/dumpcap in child process: Permission denied", ""
** (Wireshark:2331) 16:37:44.254922 [Capture MESSAGE] -- Capture stopped.
** (Wireshark:2331) 16:37:48.928429 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:2331) 16:37:49.144345 [Capture MESSAGE] -- Error message from child: "Couldn't run /usr/bin/dumpcap in child process: Permission denied", ""
** (Wireshark:2331) 16:37:51.800766 [Capture MESSAGE] -- Capture stopped.
lauren@lauren-vm:~$ sudo wireshark
[sudo] password for lauren:
** (Wireshark:2438) 16:38:05.619310 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (Wireshark:2438) 16:38:14.380924 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:2438) 16:38:14.591199 [Capture MESSAGE] -- Capture started
** (Wireshark:2438) 16:38:14.591350 [Capture MESSAGE] -- File: "/tmp/wireshark_enp0s316PXH2.pcapng"
** (Wireshark:2438) 16:39:03.452215 [Capture MESSAGE] -- Capture Stop ...
** (Wireshark:2438) 16:39:03.530800 [Capture MESSAGE] -- Capture started
** (Wireshark:2438) 16:40:35.844475 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:2438) 16:40:36.061598 [Capture MESSAGE] -- Capture started
** (Wireshark:2438) 16:40:36.062369 [Capture MESSAGE] -- File: "/tmp/wireshark_enp0s35UXRH2.pcapng"
** (Wireshark:2438) 16:43:45.402866 [Capture MESSAGE] -- Capture Stop ...
** (Wireshark:2438) 16:43:45.485098 [Capture MESSAGE] -- Capture stopped.
lauren@lauren-vm:~$ cd ~
lauren@lauren-vm:~$ ls
anaconda3 Desktop Documents Downloads lab1.pdf Music Pictures Public snap Templates tensorflow Videos
lauren@lauren-vm:~$ rm lab1.pdf
lauren@lauren-vm:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (3.6.2-2).
The following packages were automatically installed and are no longer required:
  linux-headers-6.2.0-26-generic linux-hwe-6.2-headers-6.2.0-26 linux-image-6.2.0-26-generic linux-modules-6.2.0-26-generic
  linux-modules-extra-6.2.0-26-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
lauren@lauren-vm:~$
```

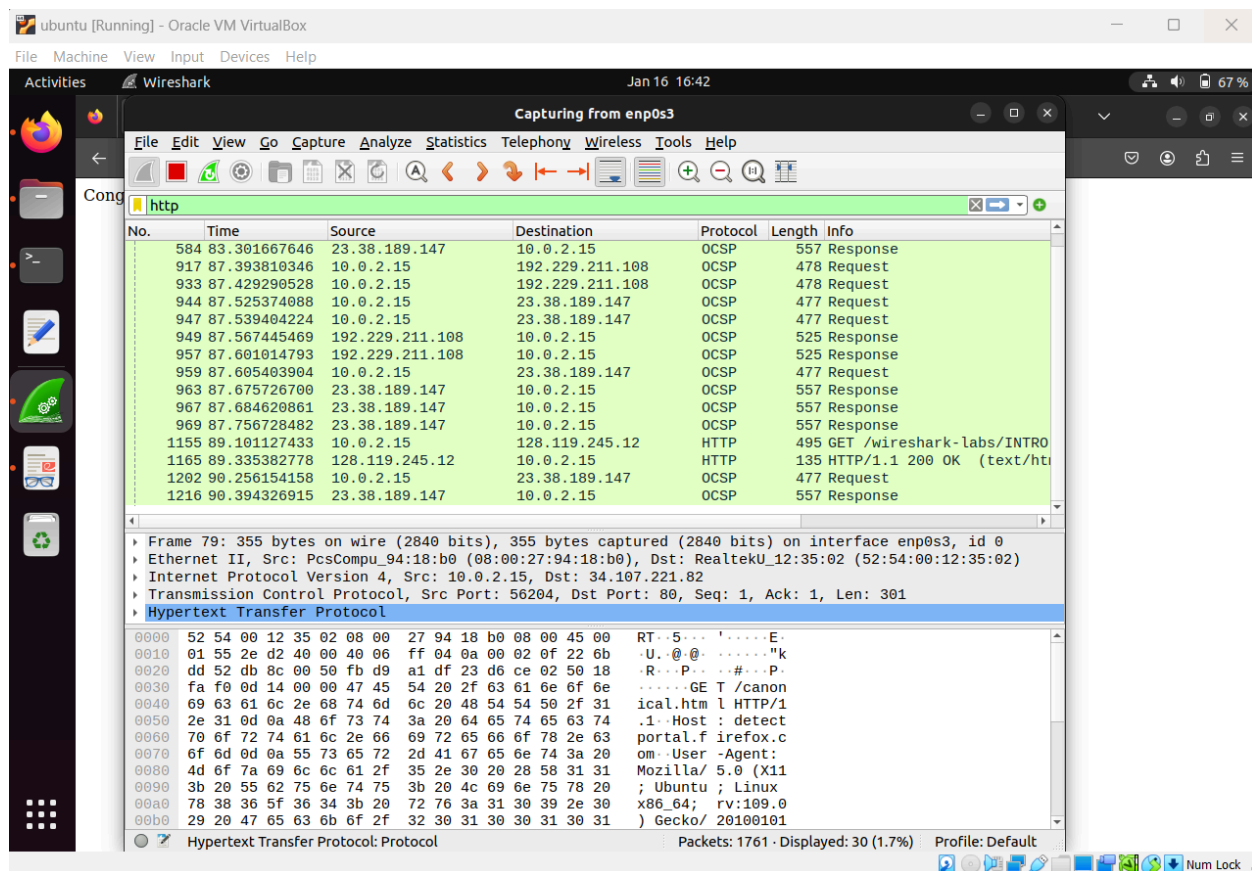
2. Next I opened Wireshark and investigated the UI as the lab suggested. I then initiated a packet capturing session.



3. Next I navigated to the URL provided in the lab to generate the appropriate packets.



4. I then filtered Wireshark by "http" and located the correct packets.



Lab Questions:

- 1. OCSP, HTTP, UDP
- 2. < 1 second
- 3. 128.119.245.12, 10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1155	89.101128	10.0.2.15	128.119.245.12	HTTP	495	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 1155: 495 bytes on wire (3960 bits), 495 bytes captured (3960 bits)						
Ethernet II, Src: PcsCompu_94:18:b0 (08:00:27:94:18:b0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)						
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12						
Transmission Control Protocol, Src Port: 33924, Dst Port: 80, Seq: 1, Ack: 1, Len: 441						
Hypertext Transfer Protocol						
No.	Time	Source	Destination	Protocol	Length	Info
1165	89.335383	128.119.245.12	10.0.2.15	HTTP	135	HTTP/1.1 200 OK (text/html)
Frame 1165: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)						
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_94:18:b0 (08:00:27:94:18:b0)						
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15						
Transmission Control Protocol, Src Port: 80, Dst Port: 33924, Seq: 302, Ack: 442, Len: 81						
[2 Reassembled TCP Segments (382 bytes): #1163(301), #1165(81)]						
Hypertext Transfer Protocol						
4.	Line-based text data: text/html (3 lines)					