

The background features a series of overlapping, wavy lines in shades of purple, green, blue, yellow, and pink. Scattered throughout are small grey 'x' marks and several colored diamond shapes (orange, blue, green, pink, red). A white L-shaped line is positioned in the top-left corner, and another white L-shaped line is in the bottom-right corner.

Assignment 1

Packet Analysis

Al-Chun Pang / Instructor
Wei-Chun Dai & Sheng Chen / TAs

The background features a series of overlapping, wavy lines in shades of purple, green, blue, yellow, and pink. A white rectangular frame is positioned in the center-left. Inside the frame, there are several small, colored diamond shapes (red, orange, pink) and a cluster of small 'x' marks. Outside the frame, there are more colored diamond shapes (green, blue) and another cluster of small 'x' marks.

Assignment 1 Announcement



Assignment 1

Specification (1/2)

01 Analysis of UDP packets

- Please find out a UDP packet on Wireshark.
- Taking a screenshot of the UDP packet.
- Write down which website or webserver it is, and what kind of service this packet provides.

Analysis of TCP packets

02

- Run the video streaming client App of Assignment 2.
- Taking a screenshot of the TCP packet.
- Write down which port does the server uses for this application.
- TCP executable code is here. Please download and execute it on our environment. To execute the code, please enter command below on terminal,

```
$ chmod 777 ./client  
$ ./client
```


03

Compare the headers of transport layer between TCP and UDP

- Write down the different fields between these 2 protocols based on your observation.

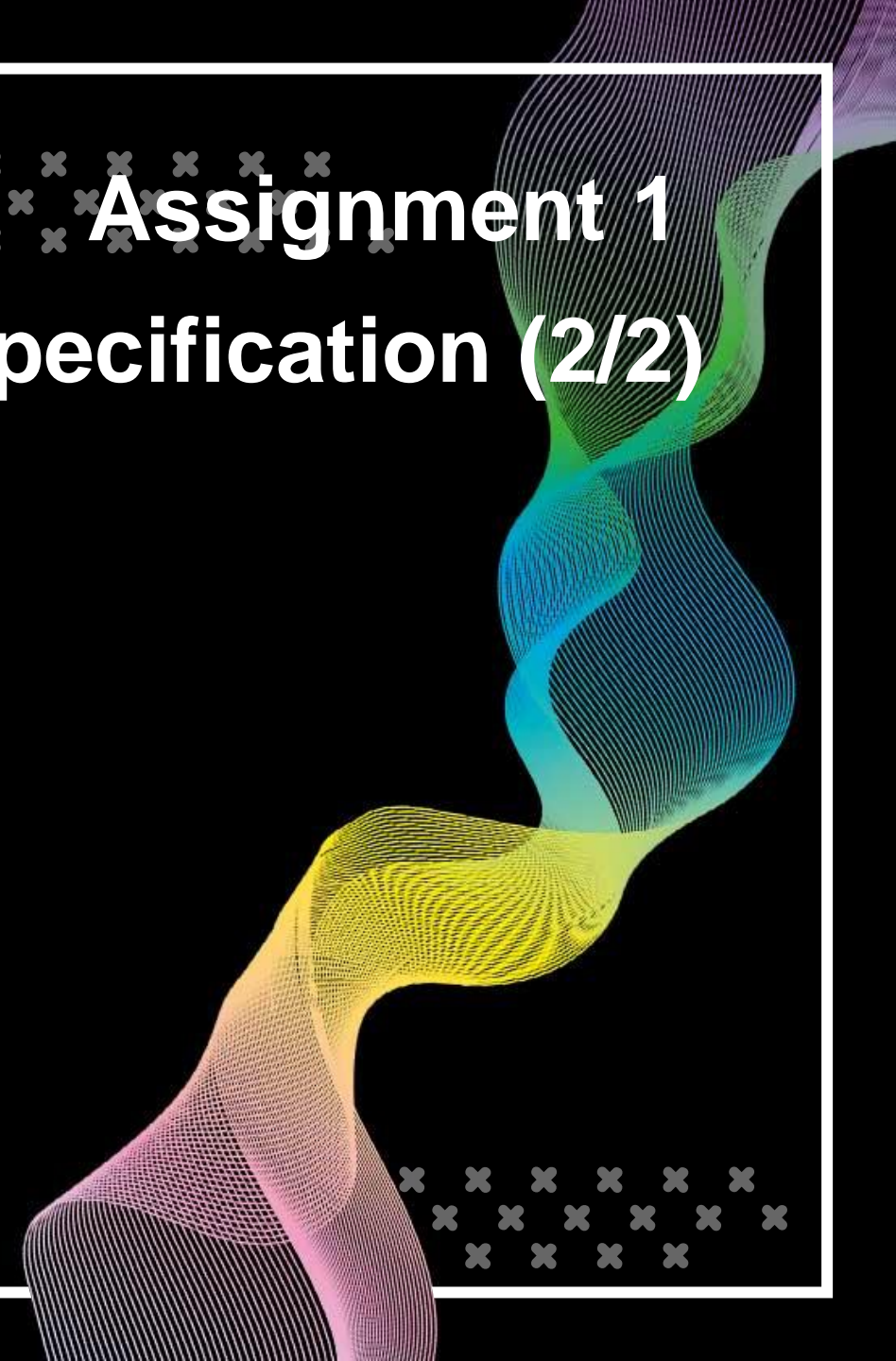
Find out a plaintext password

04

- Taking a screenshot of a packet with your password in plaintext. (You can put a black bar or do pixelate on your password)
- Write down which website it is.
- Why is it not safe to send passwords in plaintext?

**If you got some other observations,
please write them down in your report.**

Assignment 1 Specification (2/2)



Grading Policy



Analysis of UDP packets



Analysis of TCP packets



Compare UDP and TCP
packets



Find out a plaintext
password

Submission

- Your report format must be in “.pdf” format, or else you will get **0 point**.
- Please submit your report on NTU Cool.

Deadline

- Due Date : 23:59:59, October 27th, 2020
- Penalty for late submission is “**20 points** per day”

BONUS

Other observations (**5 points**)

An abstract graphic on a black background. It features several overlapping, wavy bands of color: purple on the left, transitioning through green, blue, yellow, and pink towards the right. These bands are composed of many fine, parallel lines. A white rectangular frame is positioned in the center-left, enclosing a portion of the blue and green waves. Inside this frame, there are two clusters of small grey 'x' marks: one at the bottom left and one at the top left. Outside the frame, there are five colored diamond shapes: a red one at the top left, a yellow one on the left, a pink one at the bottom left, a green one at the bottom right, and a blue one at the bottom right. The text 'Environment Setup' is written in white, bold, sans-serif font, positioned to the right of the white frame.

Environment Setup

Environment

Solution 1



We provide a VirtualBox environment for you to run our binary code and you can run Wireshark on this environment.

Download the VM from

- [our server](#)

Install [Virtualbox](#) (natively installed on the computers of Lab R204).



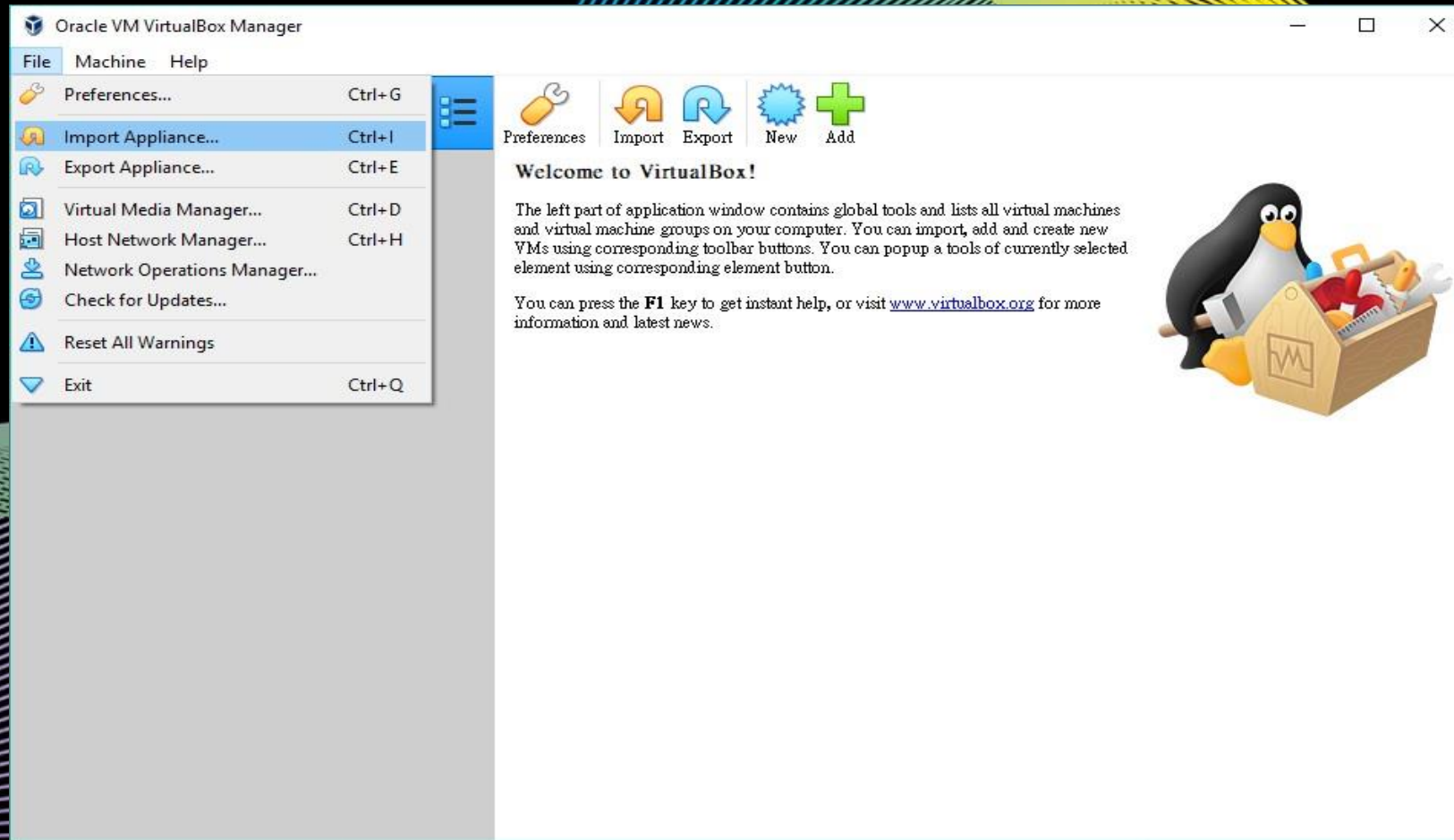
Solution 2

If you would like to setup the environment on your OS rather than our virtual machine, here is information of our environment.

- Ubuntu 16.04 x64
- OpenCV 3.4.4

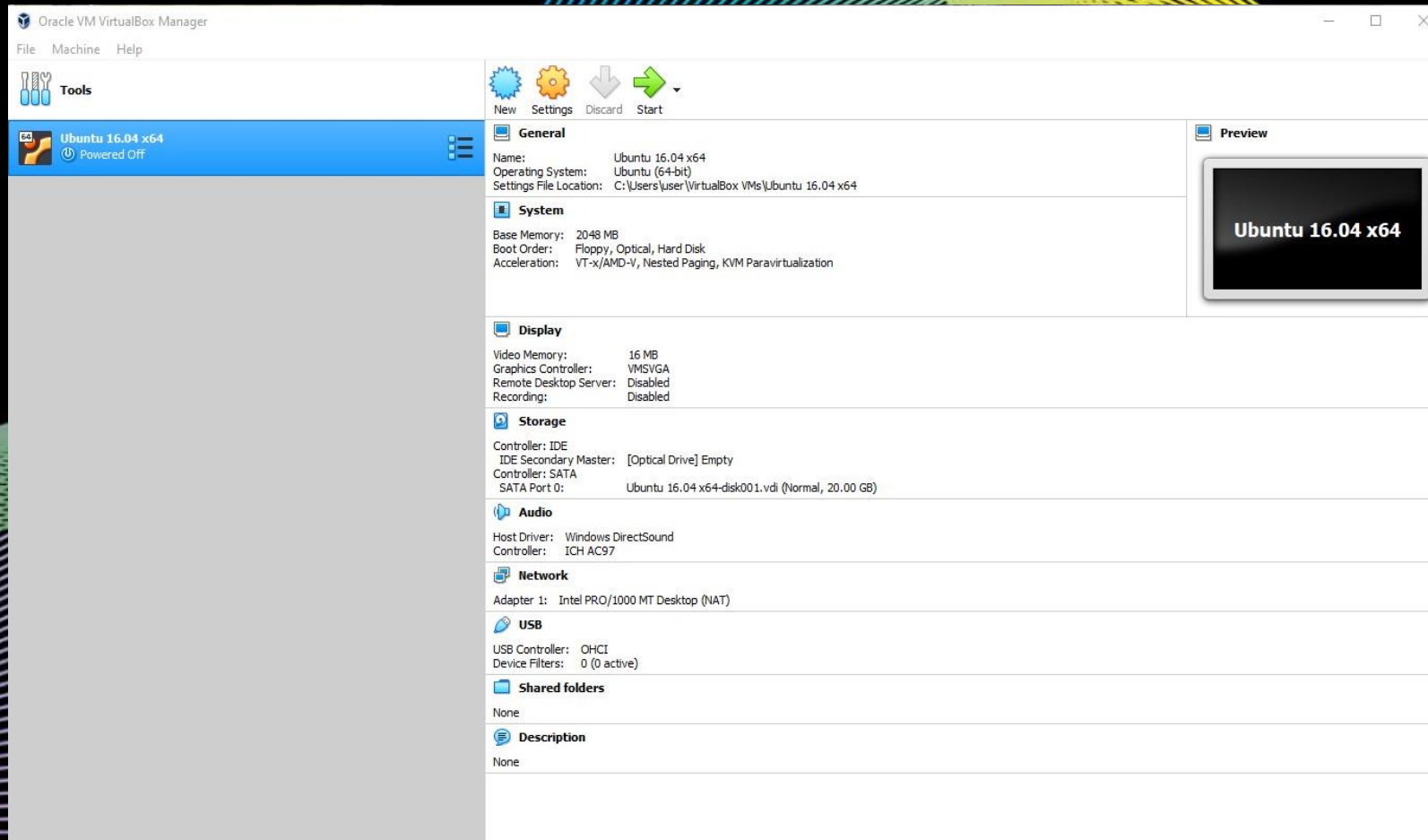
You can install OpenCV 3.4.4 by following the instruction [here](#).

VirtualBox Setup

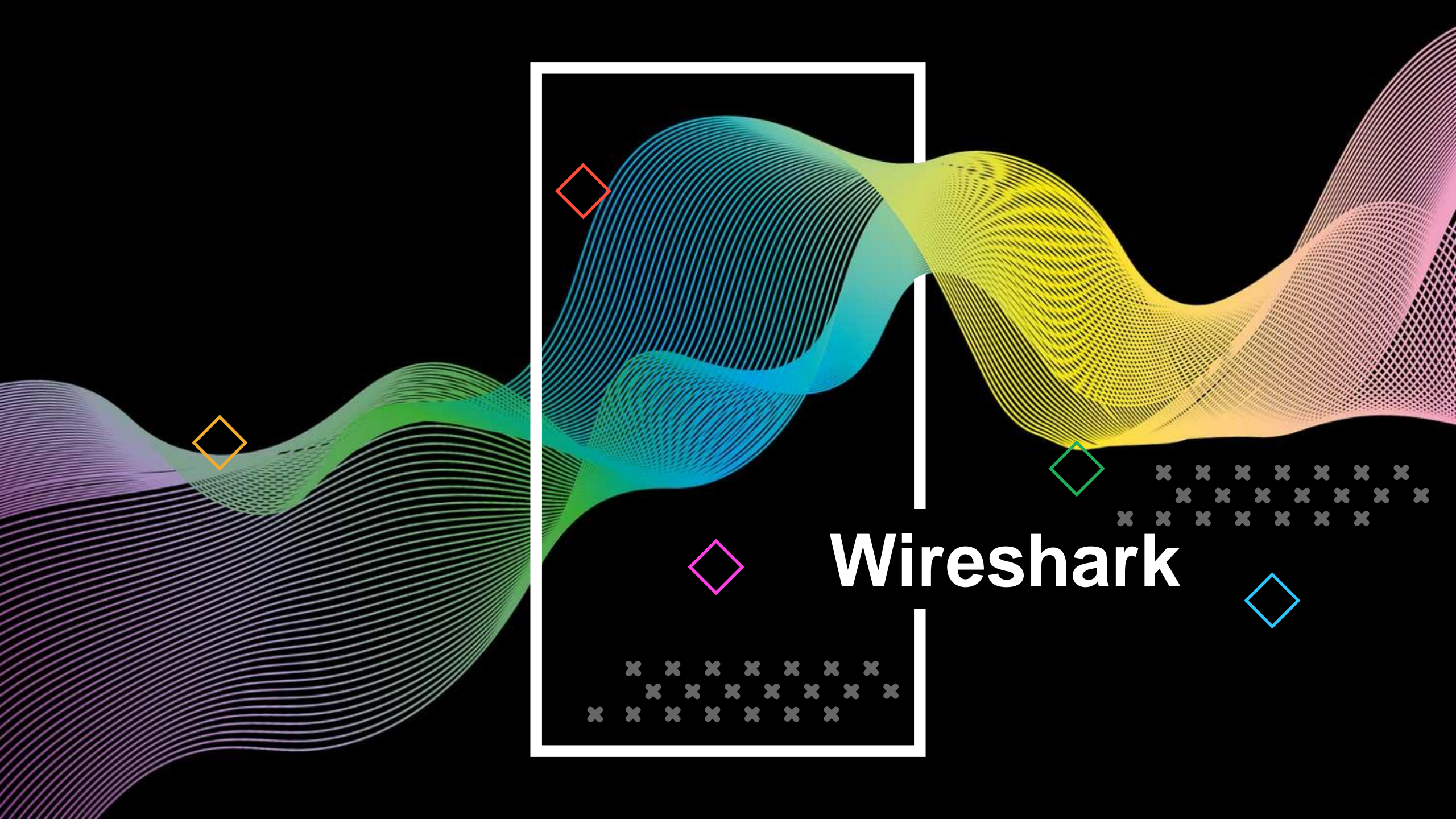


Go to “File” and click “Import Appliance” to import the “CN-Ubuntu_16.04_x64.ova”

VirtualBox Setup



Choose “Ubuntu 16.04 x64” and then start the machine.



Wireshark



Wireshark Installation

01

Superuser permission

Superuser permission is necessary to install the Wireshark. Our password is **ZACKISHANDSOME**.

02

Install Wireshark

To install Wireshark, please run the following command:

```
$ sudo apt update  
$ sudo apt install wireshark  
$ sudo usermod -aG wireshark $(whoami)
```

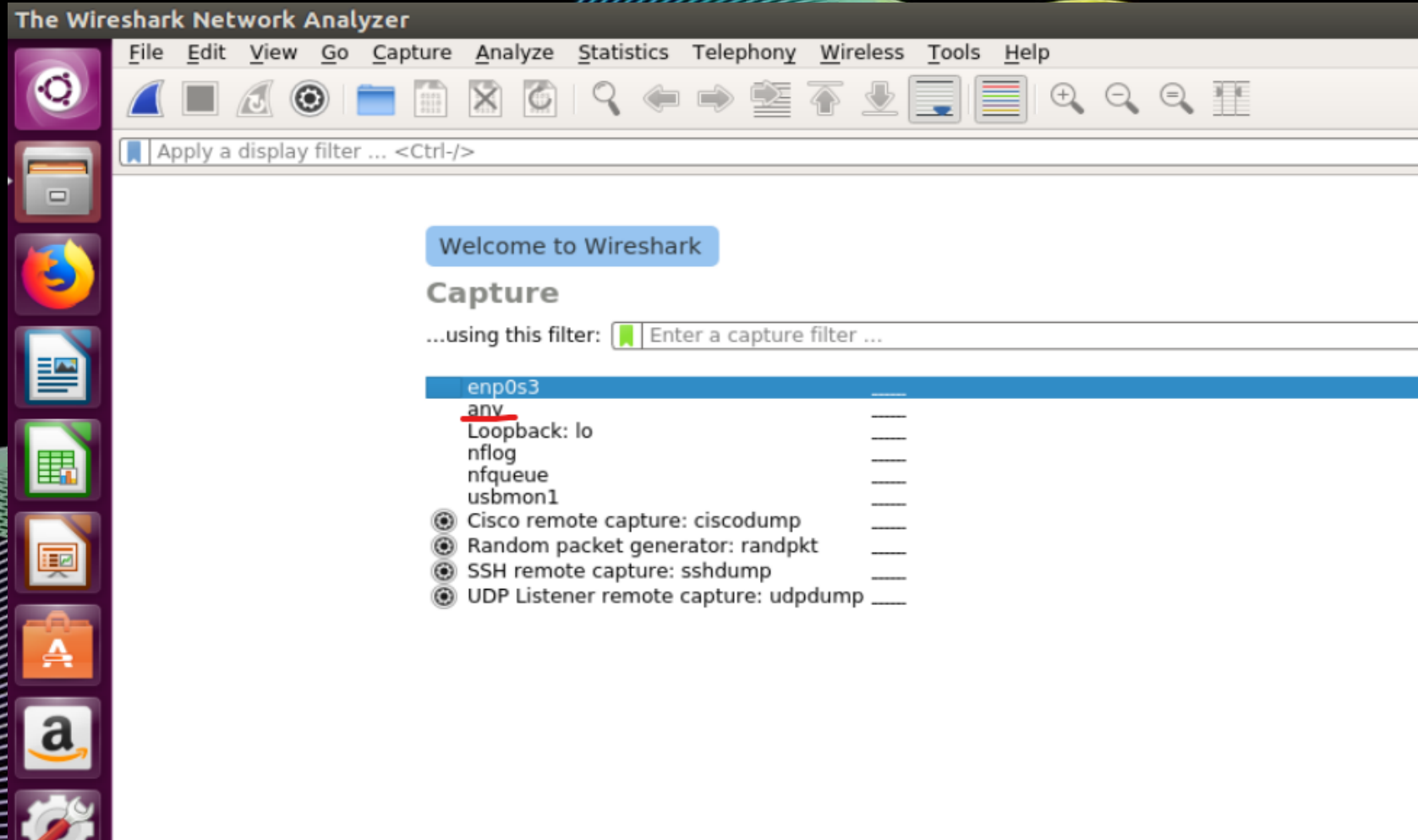
03

Launch Wireshark

To launch Wireshark, run the following command:

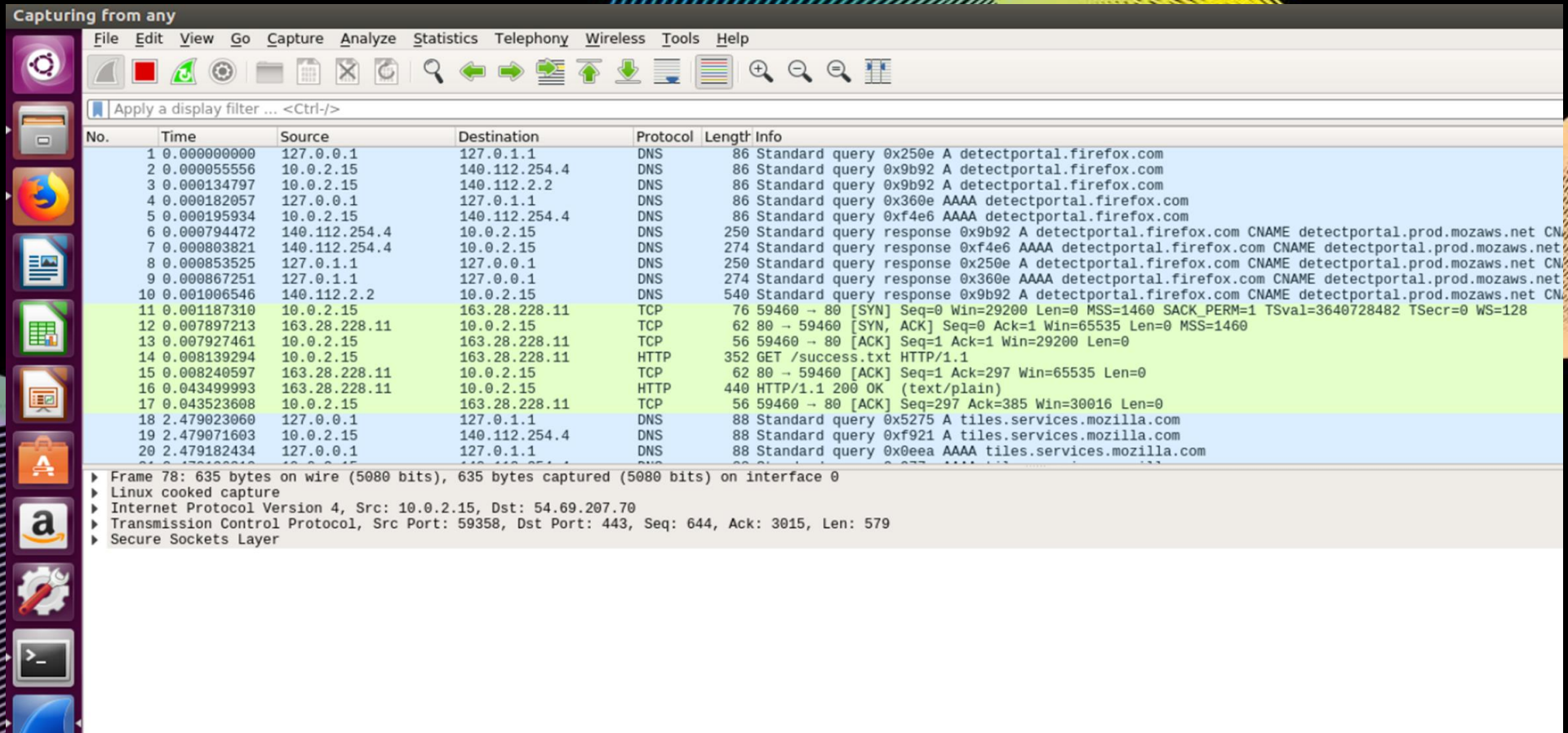
```
$ sudo wireshark
```

Wireshark Instruction



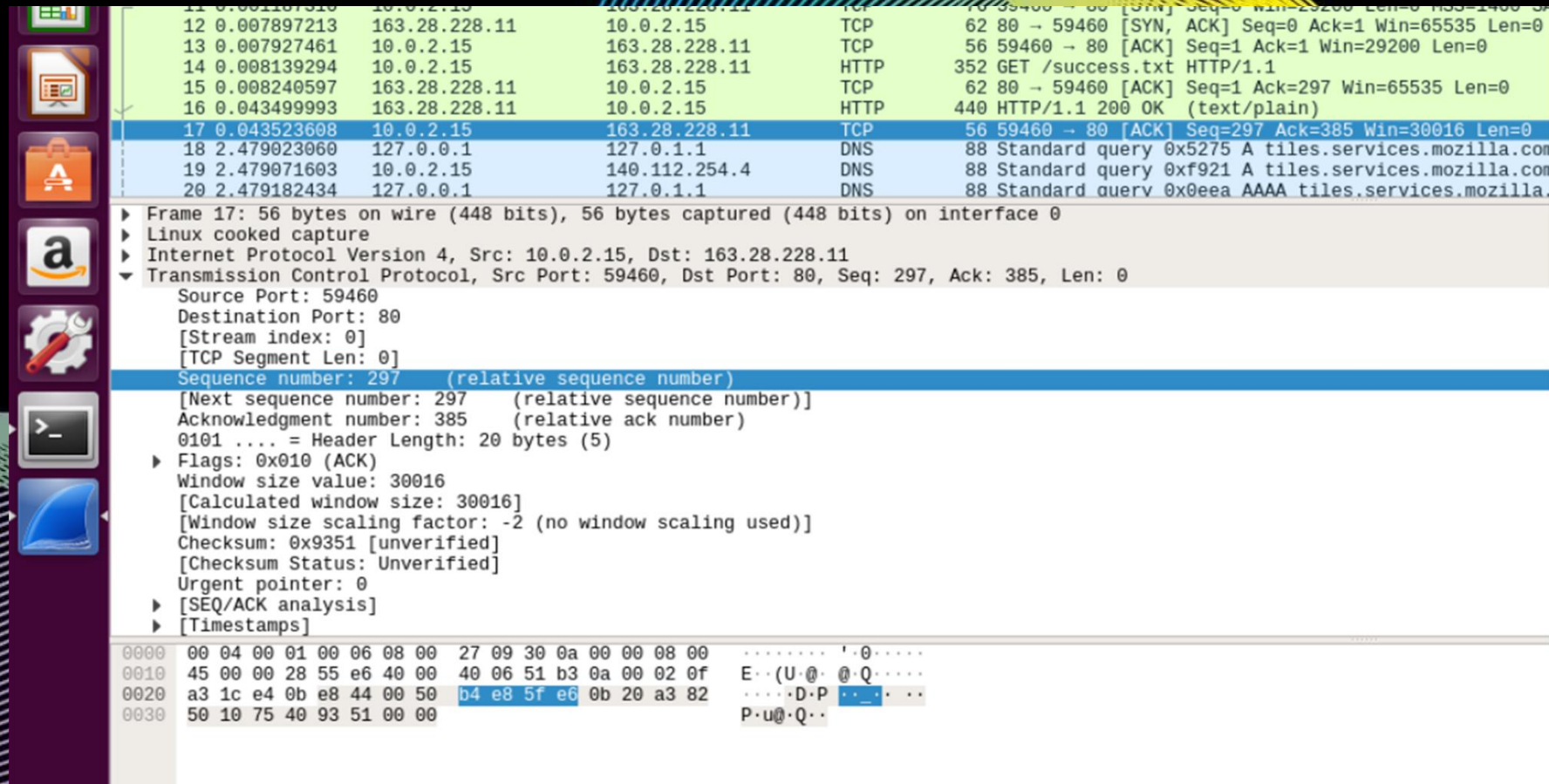
Double click on "any"

Wireshark Instruction



Then, you can see all the packet sent to this machine (that is, virtual machine if you use our VirtualBox).

Wireshark Instruction



You can see packet information on the center area and the binary raw data of the packets.

Wireshark Instruction

Apply a display filter ... <Ctrl-/>

Packet details ▾ Wide (UTF-16) ▾ Case sensitive String mozilla

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000055556	10.0.2.15	140.112.254.4	DNS	86	Standard query 0x9b92 A detectportal.firefox.com
3	0.000134797	10.0.2.15	140.112.2.2	DNS	86	Standard query 0x9b92 A detectportal.firefox.com
4	0.000182057	127.0.0.1	127.0.1.1	DNS	86	Standard query 0x360e AAAA detectportal.firefox.com
5	0.000195934	10.0.2.15	140.112.254.4	DNS	86	Standard query 0xf4e6 AAAA detectportal.firefox.com
6	0.000794472	140.112.254.4	10.0.2.15	DNS	250	Standard query response 0x9b92 A detectportal.firefox.com CNAME de
7	0.000803821	140.112.254.4	10.0.2.15	DNS	274	Standard query response 0xf4e6 AAAA detectportal.firefox.com CNAME de
8	0.000853525	127.0.1.1	127.0.0.1	DNS	250	Standard query response 0x250e A detectportal.firefox.com CNAME de
9	0.000867251	127.0.1.1	127.0.0.1	DNS	274	Standard query response 0x360e AAAA detectportal.firefox.com CNAME de
10	0.001006546	140.112.2.2	10.0.2.15	DNS	540	Standard query response 0x9b92 A detectportal.firefox.com CNAME de
11	0.001187310	10.0.2.15	163.28.228.11	TCP	76	59460 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
12	0.007897213	163.28.228.11	10.0.2.15	TCP	62	80 → 59460 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
13	0.007927461	10.0.2.15	163.28.228.11	TCP	56	59460 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
14	0.008139294	10.0.2.15	163.28.228.11	HTTP	352	GET /success.txt HTTP/1.1
15	0.008240597	163.28.228.11	10.0.2.15	TCP	62	80 → 59460 [ACK] Seq=1 Ack=297 Win=65535 Len=0
16	0.043499993	163.28.228.11	10.0.2.15	HTTP	440	HTTP/1.1 200 OK (text/plain)
17	0.043523608	10.0.2.15	163.28.228.11	TCP	56	59460 → 80 [ACK] Seq=297 Ack=385 Win=30016 Len=0
18	2.479023060	127.0.0.1	127.0.1.1	DNS	88	Standard query 0x5275 A tiles.services.mozilla.com
19	2.479071603	10.0.2.15	140.112.254.4	DNS	88	Standard query 0xf921 A tiles.services.mozilla.com
20	2.479182434	127.0.0.1	127.0.1.1	DNS	88	Standard query 0x0eea AAAA tiles.services.mozilla.com
21	2.479196310	10.0.2.15	140.112.254.4	DNS	88	Standard query 0x977a AAAA tiles.services.mozilla.com

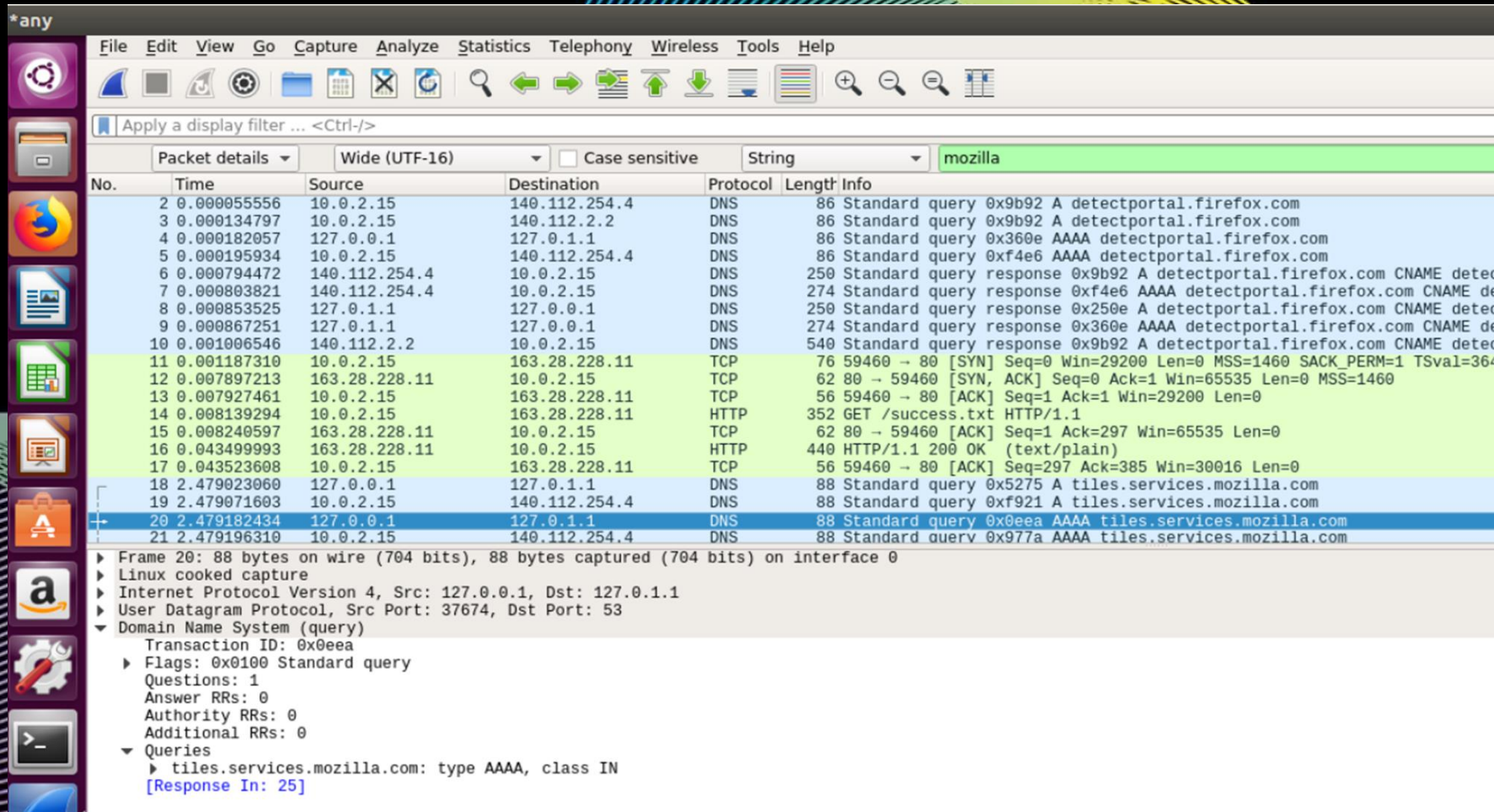
Frame 20: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
- User Datagram Protocol, Src Port: 37674, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0eea
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - tiles.services.mozilla.com: type AAAA, class IN [Response in: 25]

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 08 00
0010 45 00 00 48 4c ab 40 00 40 11 ee f7 7f 00 00 01 E..HL..@.....
0020 7f 00 01 01 93 2a 00 35 00 34 ff 47 0e ea 01 00*.5..4.G..
0030 00 01 00 00 00 00 00 00 05 74 69 6c 65 73 08 73tiles.s
0040 65 72 76 69 63 65 73 07 6d 6f 7a 69 6c 6c 61 03 services..mozilla.
0050 63 6f 6d 00 00 1c 00 01 com.....

Press “Ctrl + F”, then you can search some terms on the packets your machine heard.

Wireshark Instruction



If you want to display only some packets of given statements, enter some statement on “Apply a display filter ...”

Wireshark Instruction

Here are some common fields.

Object	Field
ip.addr	IP of all hosts
ip.src	IP of all source hosts
ip.dst	IP of all destination hosts
ip.proto	Protocol of all packets

For example, if you enter “`ip.addr == 127.0.0.1`”, it will retain all packet sent from or to `localhost (127.0.0.1)`.