2019 Computer Networks, Ai-Chun Pang

Ai-Chun Pang / Instructor

林偉哲 陳令原 / T.A.s

Assignment I-Packet Analysis

Assignment I Announcement

Assignment 1 – Specification (1/2)

- **Analysis of UDP (User Datagram Protocol) packets**
  - Please find out some 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 (Transmission Control Protocol) packets**
  - 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
```

Assignment 1 – Specification (2/2)

- **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**
  - 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.**

Grading Policy

- **This assignment accounts for 5% of the total score.**
- **Report Only** **(100%)**
  - Analysis of UDP packets (20%)
  - Analysis of TCP packets (20%)
  - Comparing between UDP and TCP packets (30%)
  - Find out a plaintext password (25%)
  - Other observations (5%)
- **Submission**
  - **Your report format must be in "".pdf"" format, or else you will get zero point**.
  - Please submit your report to here. The password is **HappyCoding2019** (it's case-sensitive).
- **Deadline**
  - Due Date : 23:59:59, October 22nd, 2019
  - Penalty for late submission is "20 points per day"

Environment Setup

Environment

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

- 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 3.3.1 (will be also required in later Assignments)

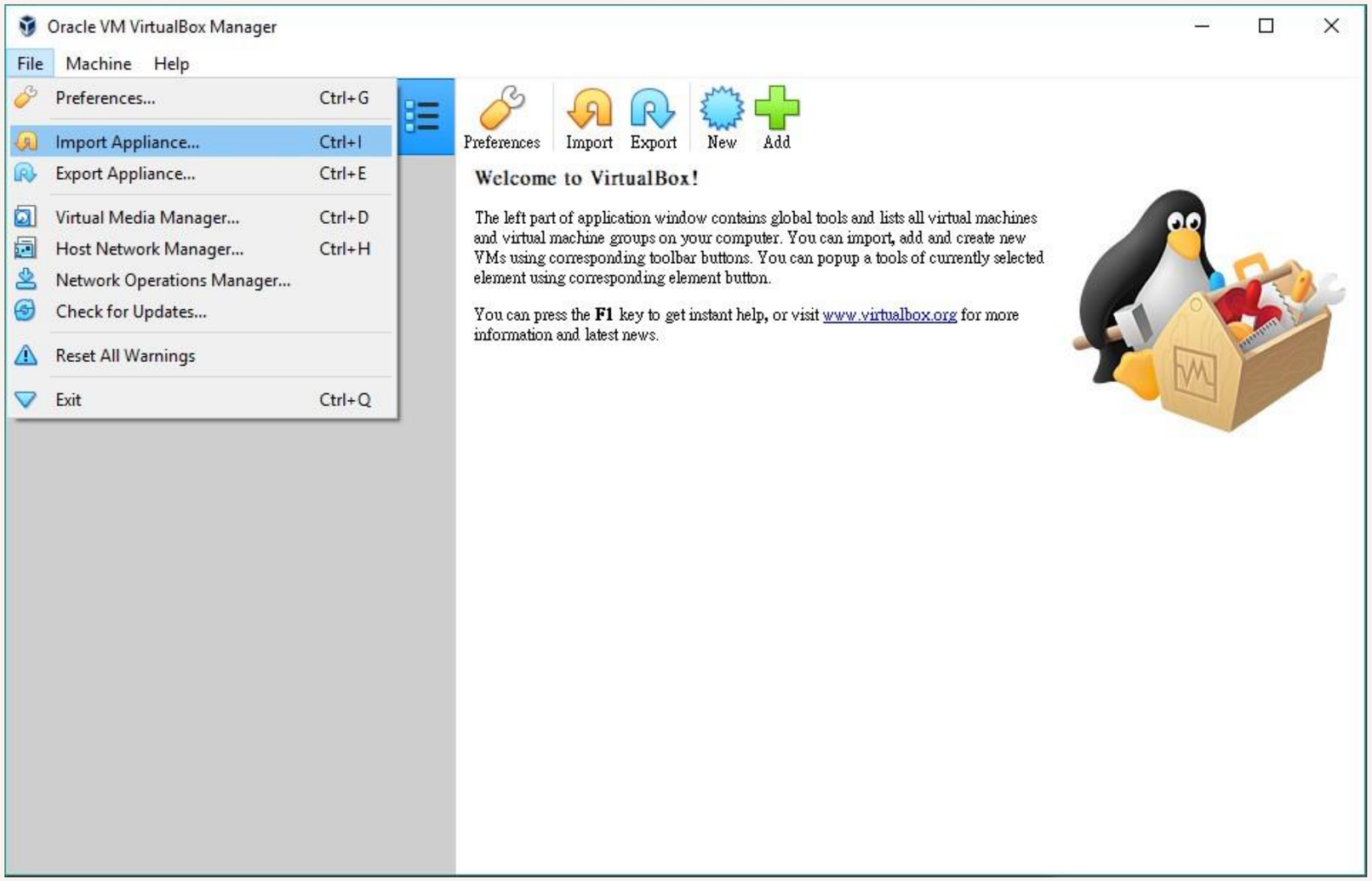
- You can install OpenCV 3.3.1 by following the instruction here.

VirtualBox Setup

- Download the VM from
  - our server,
  - our Google Drive,
- Install Virtualbox (natively installed on the computers of Lab R204).

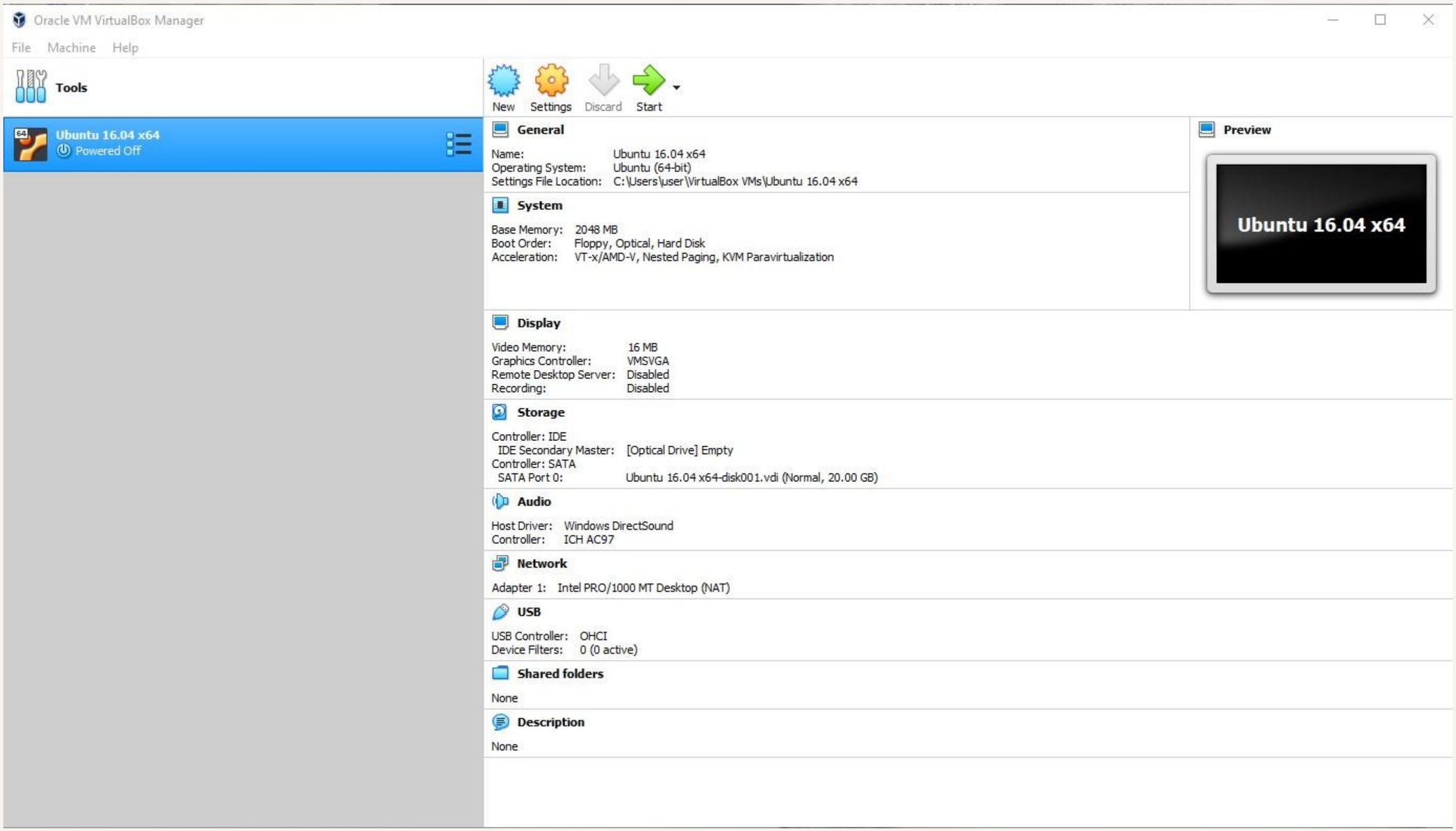
VirtualBox Setup

- 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

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

- To install Wireshark, please run the following command:

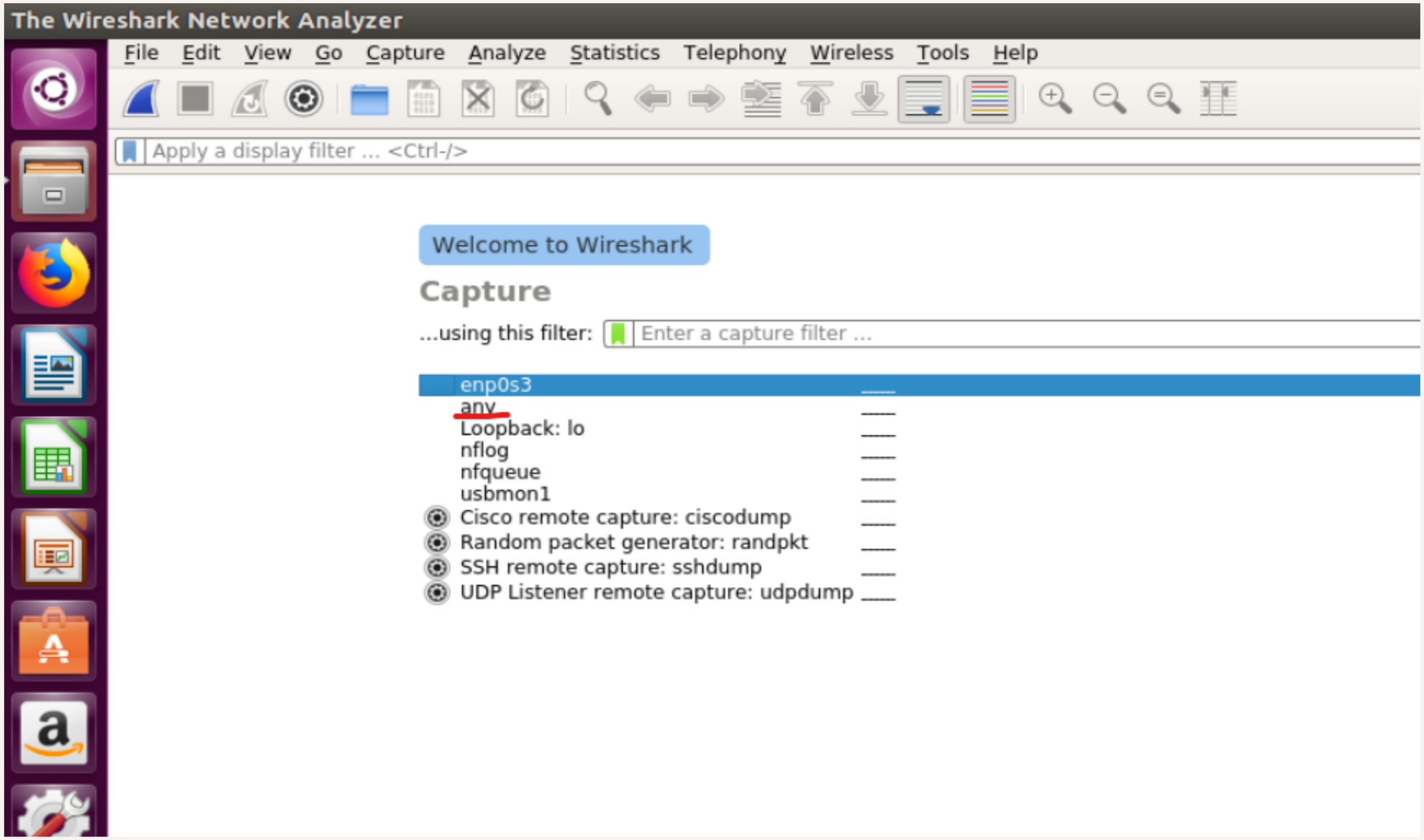
```
$ sudo apt update
$ sudo apt install wireshark
$ sudo usermod -aG wireshark $(whoami)
```

- To launch the wireshark, run the following command:

```
$ sudo wireshark
```

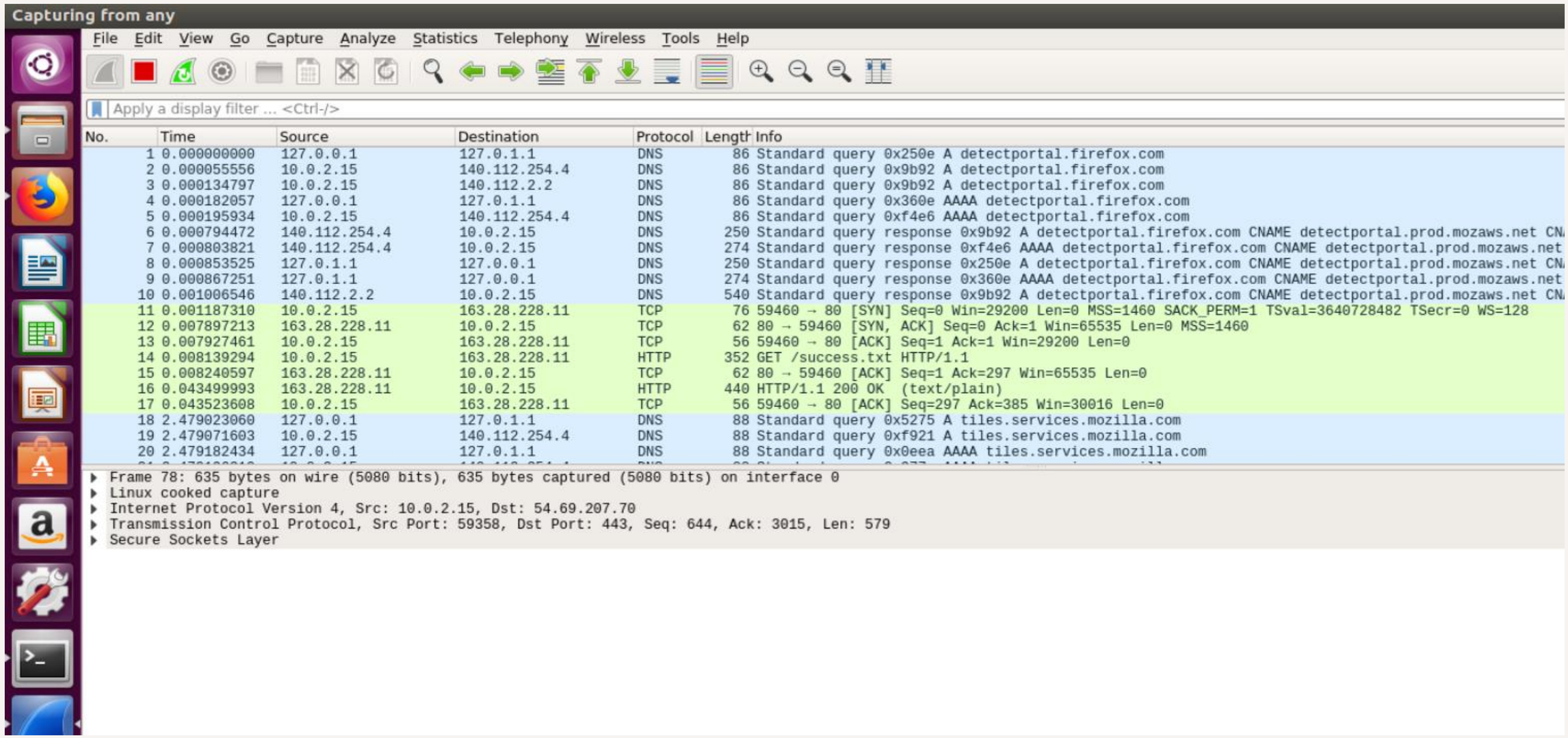
Wireshark Instruction

- Double click on “any”



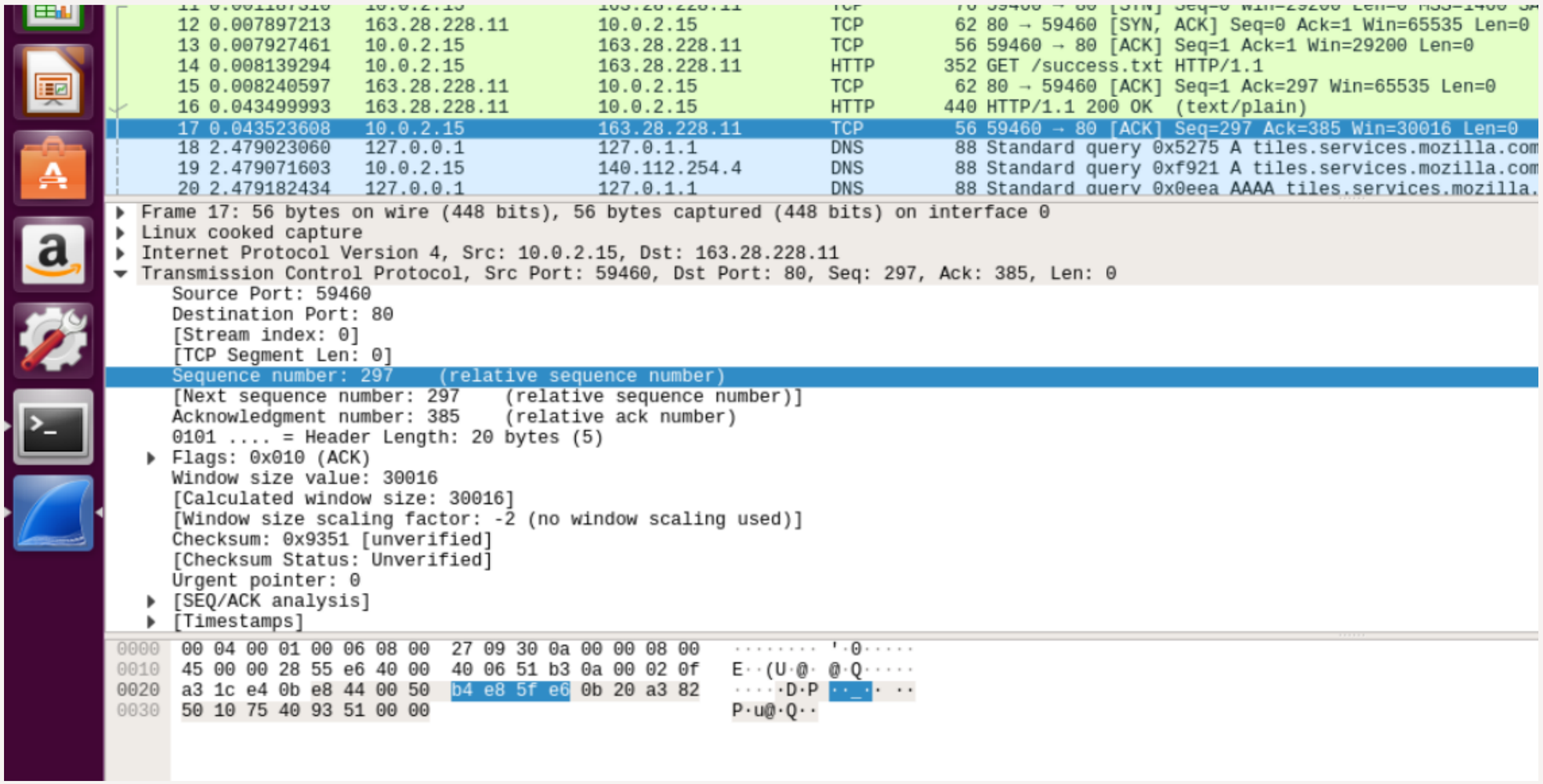
Wireshark Instruction

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



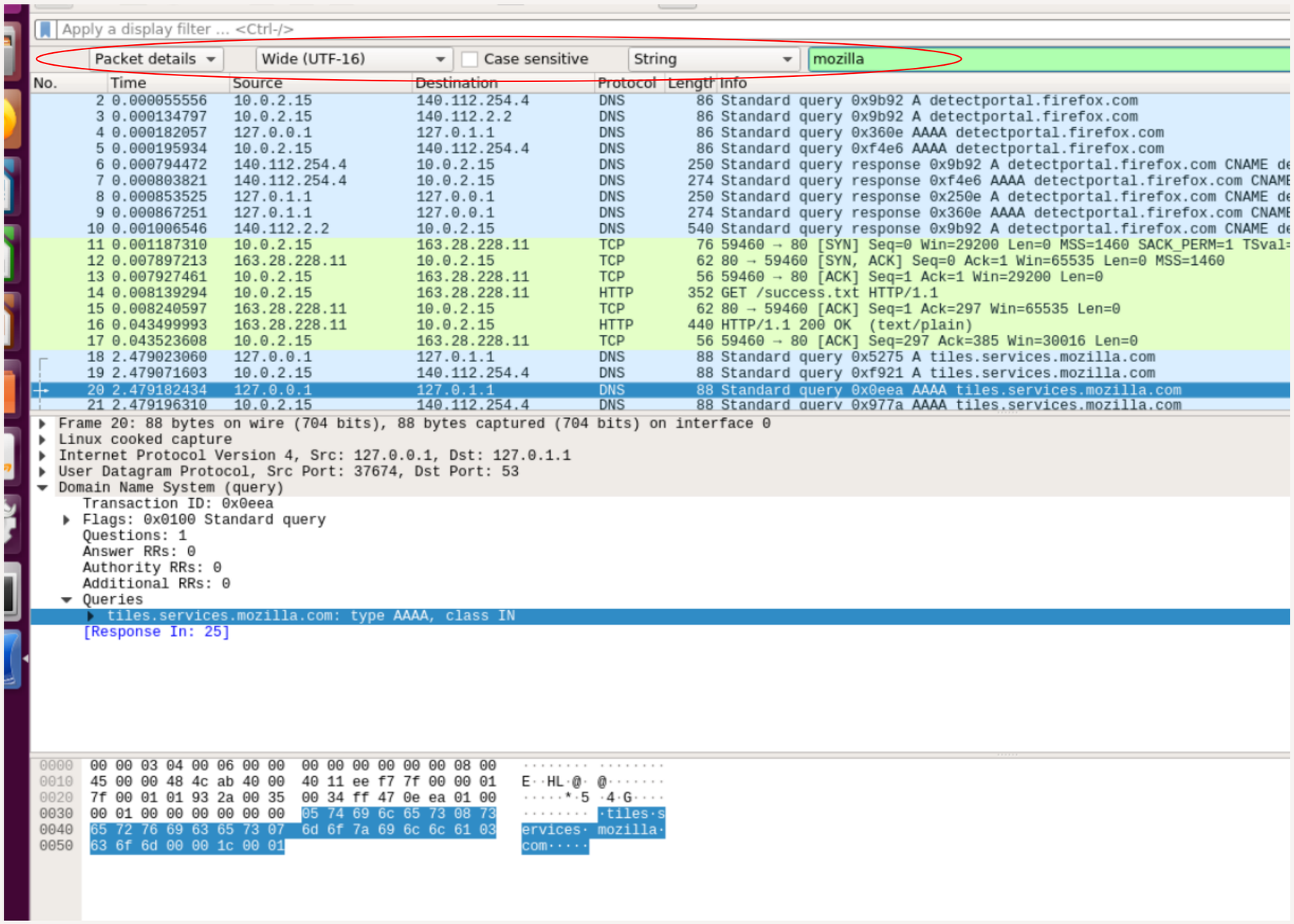
Wireshark Instruction

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



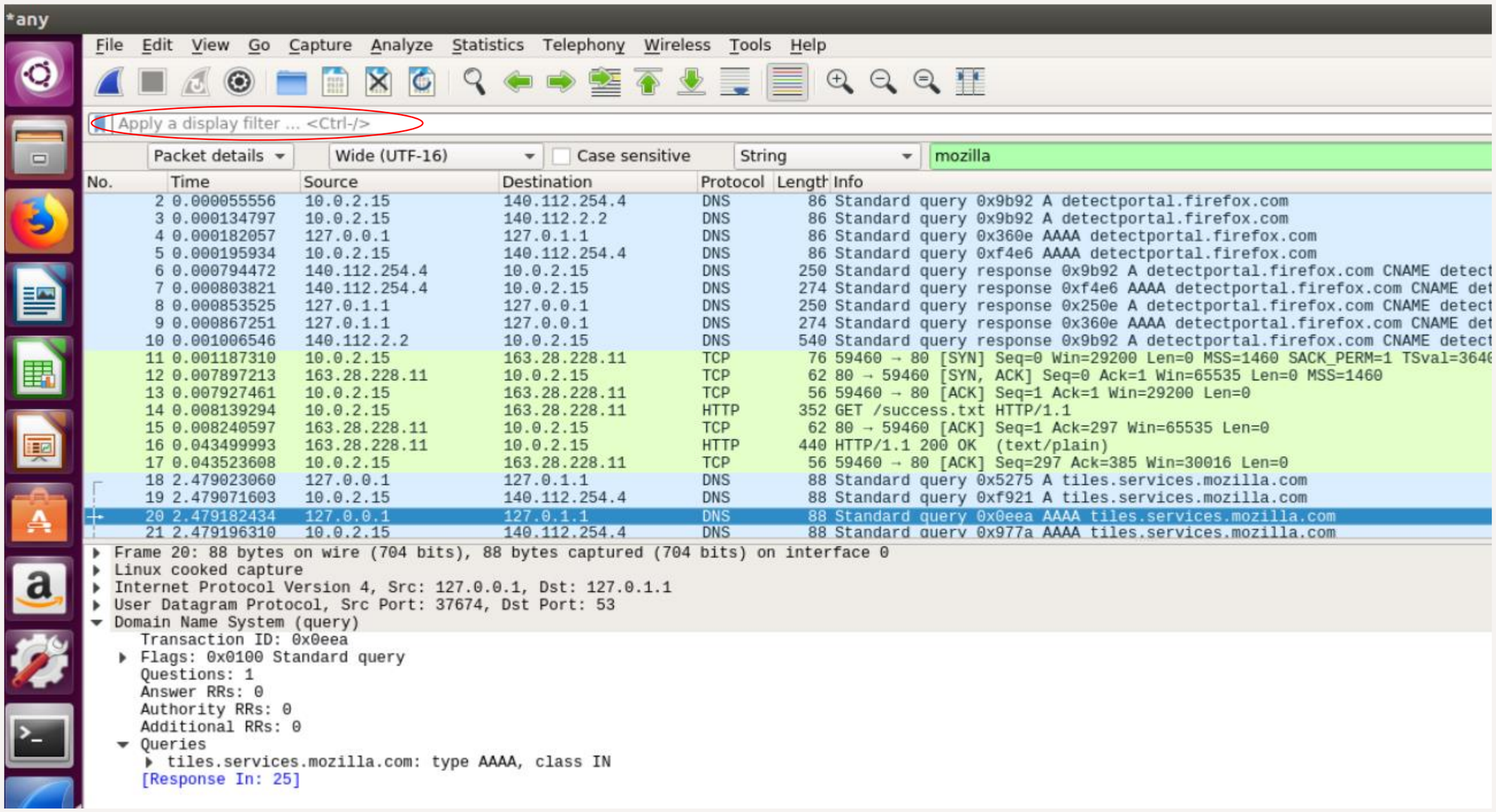
Wireshark Instruction

- 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).