NT21 Assignment 1

TCP/IP Layers in Wireshark, Linux

Task 1: Install Linux Environment

If you don’t have Linux environment yet, follow these steps:

1. Make sure you have 20 GB of free disk space
2. If you’ve already installed image for semester 2, you can skip the steps up to step 4. Otherwise, download the virtual guest OS image from:

<https://www.fhict.nl/docent/downloads/TI/S2/>

Move the image to a suitable folder.

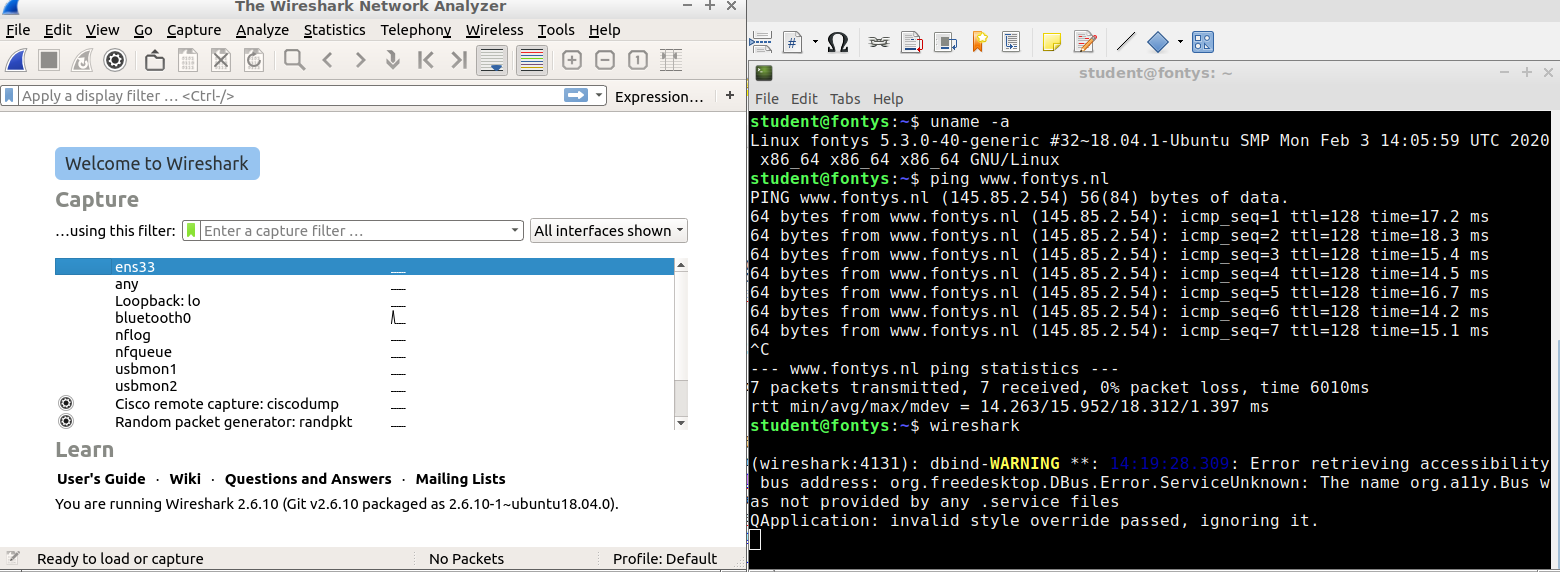
1. Install VMWare from the VMWare Store (<https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain_child_child=6130e417-ad1a-e511-940d-b8ca3a5db7a1&cmi_mnuMain_child=aafc5891-884f-e511-940f-b8ca3a5db7a1&ws=857bd84b-368b-de11-a28c-003048c1b605&vsro=8>)

Use VMWare Workstation software for Windows PC and VMWare Fusion software for MACs.

1. Unzip the downloaded file and start the Linux guest OS. Your password is “student”. If VMWare asks you whether you moved or copied the image, choose “I copied it”.
2. Check if you can open a terminal (e.g. by issuing CTRL+ALT+T command) and use one of available terminals.
3. Try a few commands like

* uname –a
* ping [www.fontys.nl](http://www.fontys.nl/)
* wireshark

Note: sudo will ask for your password: *student.*

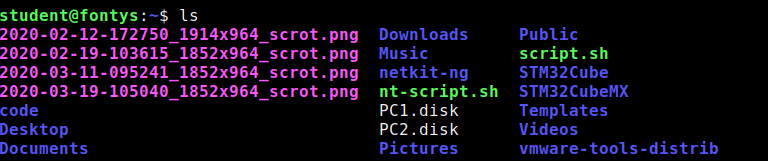
**

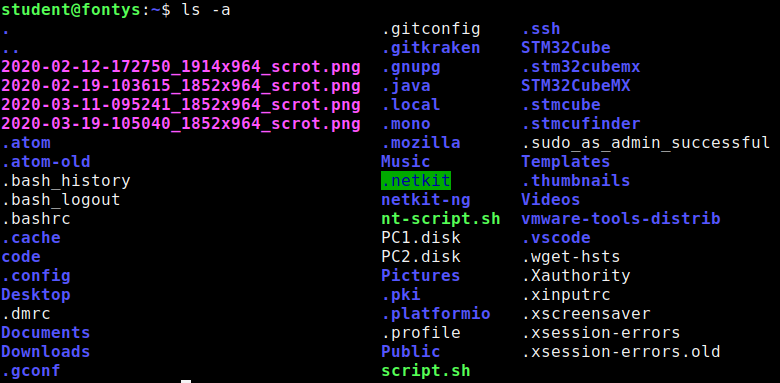
Task 2: Do Linux Tutorial

Go to <http://www.ee.surrey.ac.uk/Teaching/Unix/unix1.html> and do the 1st basic Unix tutorial. Do this tutorial individually.

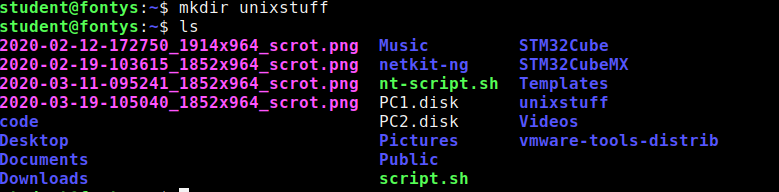
Provide screenshots of all exercises in section 1.6.

1.1



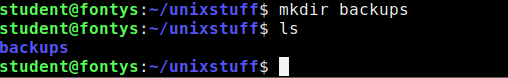


1.2



1.3





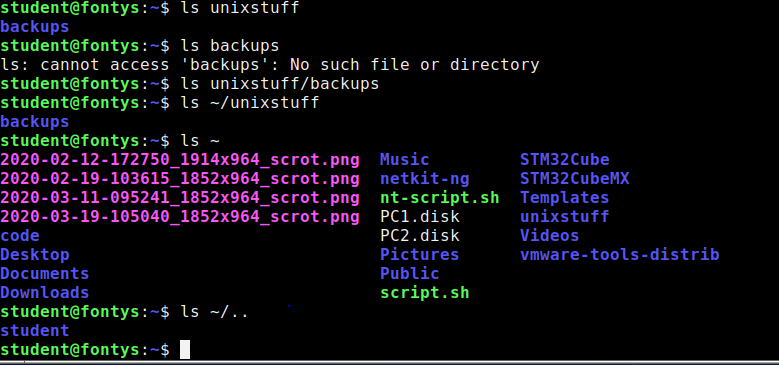
1.4



1.5



1.6



Task 3: TCP/IP Layers in Wireshark

Find a Wireshark Tutorial on the web and study how it works. Install and run Wireshark.

Start capturing network traffic. To generate HTTP traffic, go to some web page with your web browser (watch out that you go to an HTTP page and not HTTPS page; HTTPS traffic is encrypted and not completely readable in Wireshark; example HTTP page : [http://www.apache.org](http://www.apache.org/). You can find more sites via <https://www.androidauthority.com/sites-still-on-http-889265/> ). Don’t forget to stop capturing as you can get a lot of traffic in your capture.

Look at your captured packets and find an HTTP GET packet.

Answer the following questions and provide the screenshots:

1. What is the source and destination MAC address of this HTTP packet? Provide a screenshot to prove it

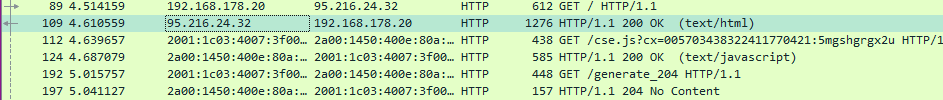


Source: 74:70:fd:b8:19:c4

Destination: 18:35:d1:03:68:00

1. What is the source and destination IP address of this HTTP packet?

Provide a screenshot to prove it



Source: 192.168.178.20

Destination: 95.216.24.32

1. What is the source and destination port of this HTTP packet?

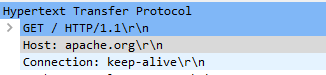
Provide a screenshot to prove it



Source: 50369

Destination: 80

1. What is the host name of this HTTP Get packet?



Host: apache.org\r\n

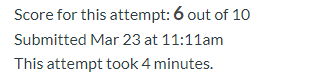
5. Find the HTTP Response belonging to the HTTP Get packet. How much

time elapsed between the HTTP Get and HTTP response ?



0.1 seconde

Task 4: Fill in Canvas Quiz Week 1



Task 5 (Optional challenge): Analyze a Wireshark Trace

Open provided Wireshark trace (ch1.pcap) in Wireshark.

Do investigation of the trace and answer the following questions:

1. Which 2 application layer protocols are being used in the trace? Give a short description of what these protocols do.
2. Both of these protocols use client/server architecture and their server has a “well-known” or standard TCP port. Which well-known ports do the servers of the found application protocols use?
3. How many packets per application protocol are there in the trace?
4. What are the client’s IP address, MAC address and TCP Port for both protocols?
5. Both application protocols are pretty old, from the time when security was not so important yet. They are now mostly replaced by other, more secure protocols. Find out which protocols have the same functionality with security features.
6. One of the 2 protocols is so insecure, that you can actually find the login password in the trace. What password is being used?