# name Investigation of hardware

Task 1: install and Test Netkit Tool

Consult this week’s theory presentation and use the Netkit commands to start and halt a network node as described in the presentation. Netkit and Wireshark are already installed in the preconfigured Linux. If you installed the Linux yourself, then you need to install these tools yourself. (there is a guideline in the Canvas)

Describe the steps you took and provide screenshot of the started node.

1. Download netkit files

Go to <http://wiki.netkit.org/index.php/Download_Official>

* “netkit-2.8.tar.bz2”
* “netkit-filesystem-i386-F5.2.tar.bz2”
* “netkit-kernel-i386-K2.8.tar.bz2”

1. Open terminal and unpack downloaded files using following commands (assuming you’re in the “~$” directory)

* Use this command “tar -xjSf Downloads/netkit-2.8.tar.bz2”
* Use this command “tar -xjSf Downloads/netkit-filesystem-i386-F5.2.tar.bz2”
* Use this command “tar -xjSf Downloads/netkit-kernel-i386-K2.8.tar.bz2”

1. Configuration of variables (assuming you’re still in the “~$” directory)

* The “pwd” command results in current path: /home/<your linux username>
* Use this command “export NETKIT\_HOME=/home/<your username>/netkit”
* Use this command “export MANPATH=:$NETKIT\_HOME/man”
* Use this command “export PATH=$NETKIT\_HOME/bin:$PATH”
* Use this command “. $NETKIT\_HOME/bin/netkit\_bash\_completion”
* Use this command “gedit .bashrc/”. This command opens the bash shell file to save the following variables:
* Insert “export NETKIT\_HOME=/home/<your username>/netkit” at the end of the bashrc file.
* Insert “export MANPATH=:$NETKIT\_HOME/man” at the end of the bashrc file.
* Insert “export PATH=$NETKIT\_HOME/bin:$PATH” at the end of the bashrc file.
* Insert “. $NETKIT\_HOME/bin/netkit\_bash\_completion” at the end of the bashrc file.

1. Check your configuration (assuming you’re still in the “~$” directory)

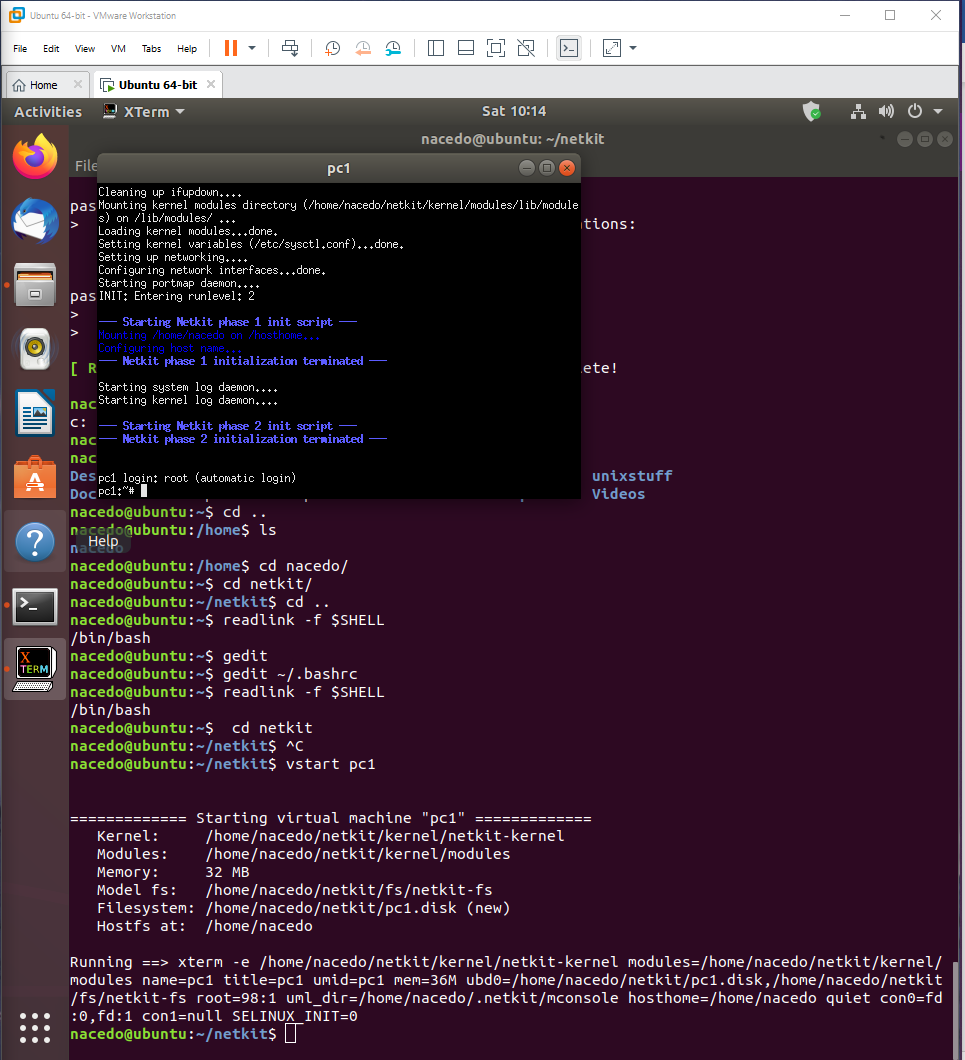
* “cd netkit”
* Use the command “./check\_configuration.sh” in the terminal
* Use the command “sudo apt-get install lib32ncurses5”. Press key “y” on keyboard. If you see this message “Do you want to continue? [Y(es)/n(o)]”.
* Use the command “sudo apt-get install libc6-i386”. Press key “y” on keyboard. If you see this message “Do you want to continue? [Y(es)/n(o)]”
* Use the command “sudo apt-get install xterm”. Press key “y” on keyboard. If you see this message “Do you want to continue? [Y(es)/n(o)]”
* Use the command “./check\_configuration.sh” to check if netkit has install successfully

1. Run netkit (assuming you’re still in the “~/netkit$” directory)

Use the command “vstart pc1” (starts virtual machine)

Use the command “vlist” (lists all virtual machines)

Use the command “vhalt -r pc1” (should stop the virtual machine)



Task 2: TCP/IP Layers in Wireshark

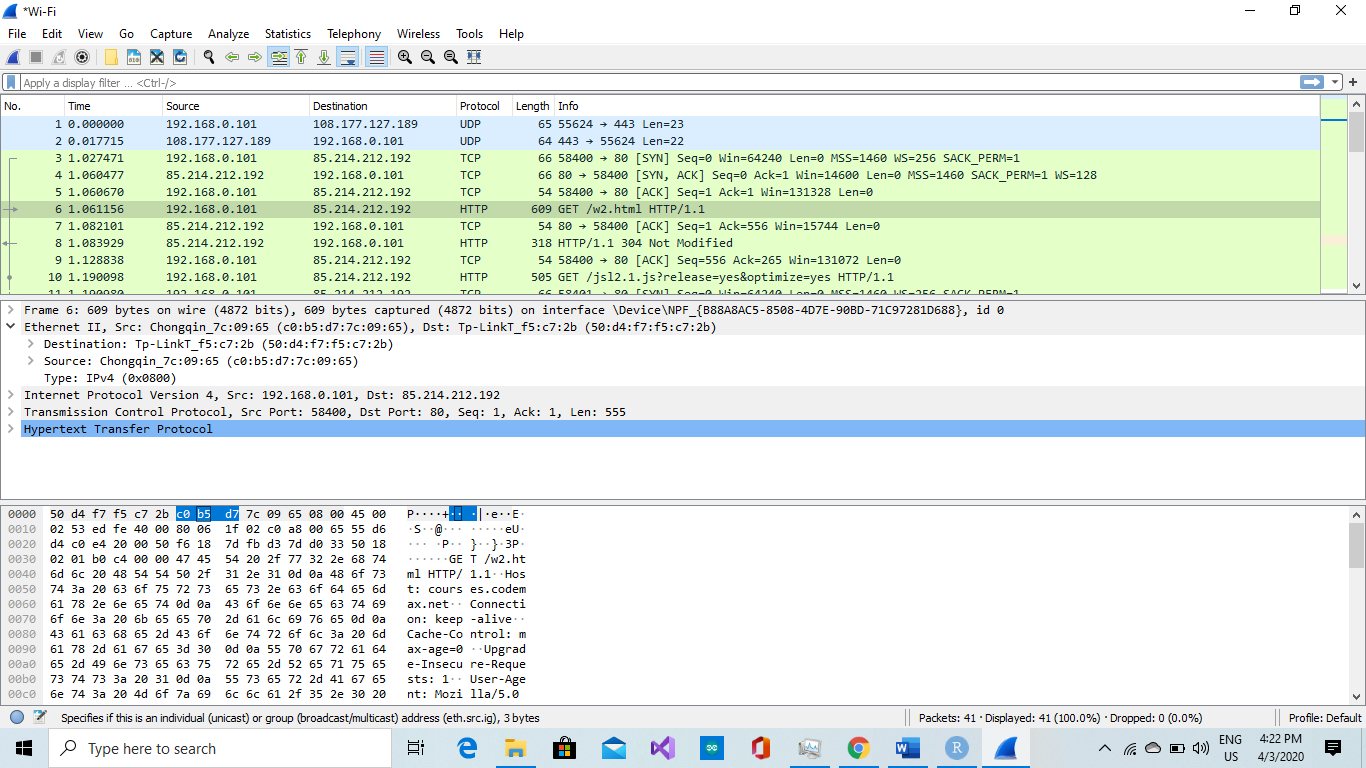
Find a Wireshark Tutorial on the web. Run Wireshark.

Start capturing the network traffic. To generate HTTP traffic, go to <http://courses.codemax.net/w2.html> web browser. 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 and Answer the following questions and provide the screenshots:

* What is the source and destination MAC address of this HTTP packet?

Source MAC address: c0:b5:d7:7c:09:65  
Destination MAC address: 50:d4:f7:f5:c7:2b

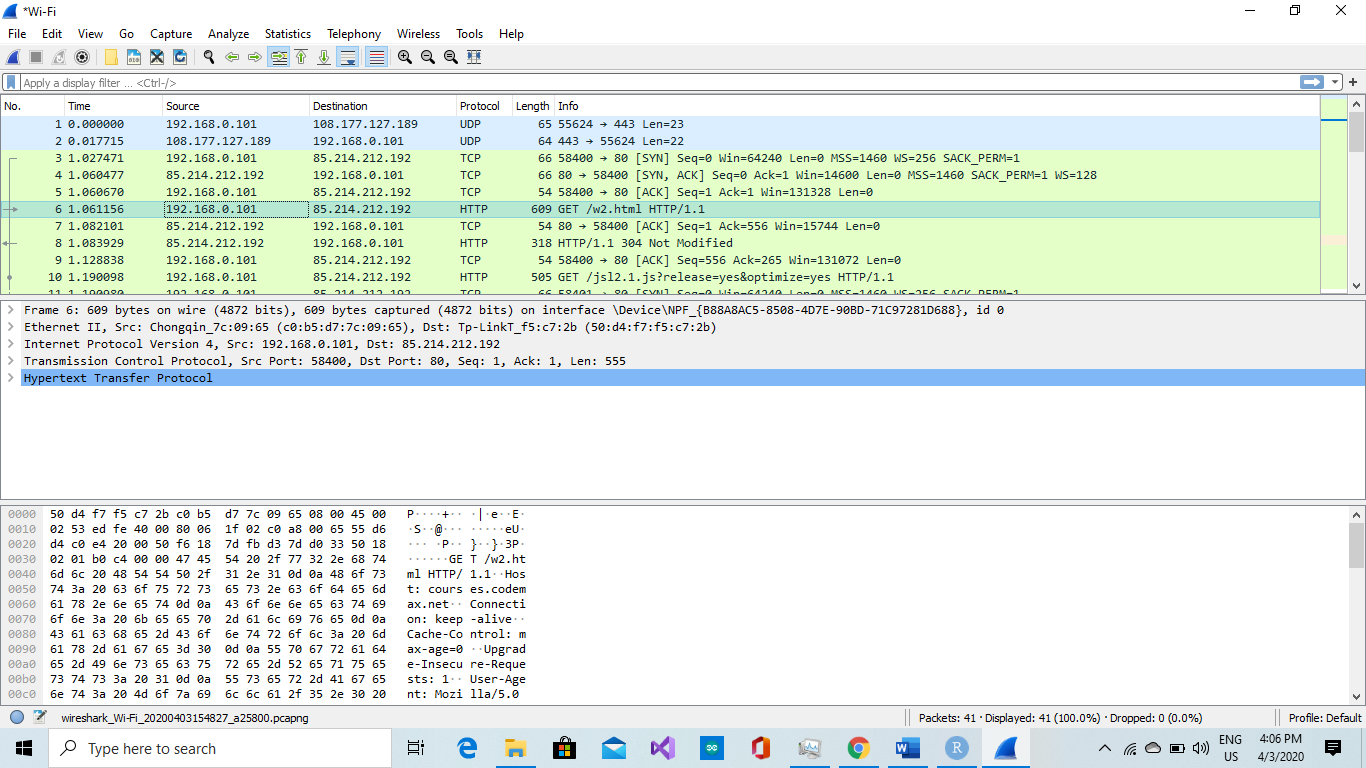
Provide a screenshot below with the Wireshark snapshot and highlight these addresses:



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

Source IP address : 192.168.0.101  
Destination IP address : 85.214.212.192

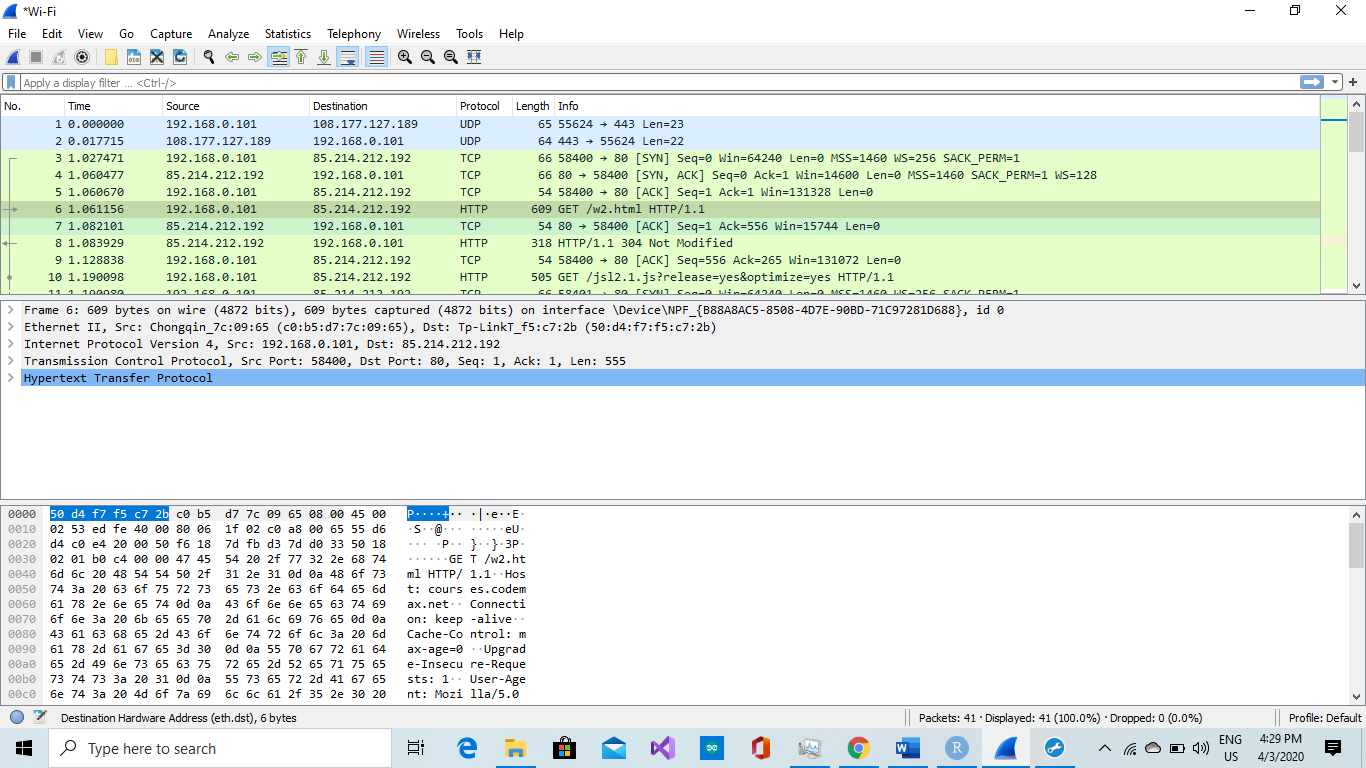
Provide a screenshot below with the Wireshark snapshot and highlight these addresses:



* What is the source and destination port of this HTTP packet? Provide a screenshot to prove it

Source port : 58400  
Destination port: 80

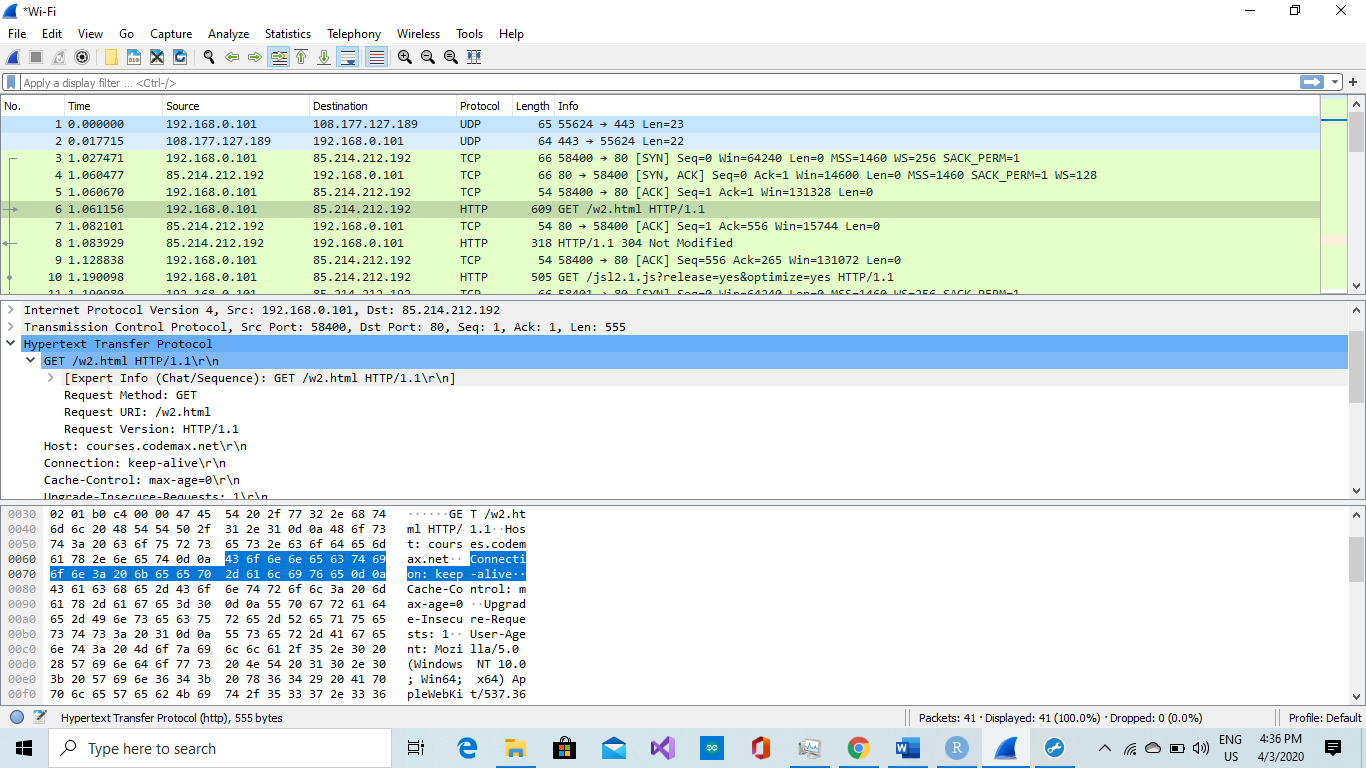
Provide a screenshot below with the Wireshark snapshot and highlight these addresses:



* What is the host name of this HTTP Get packet?

Host name: courses.codemax.net

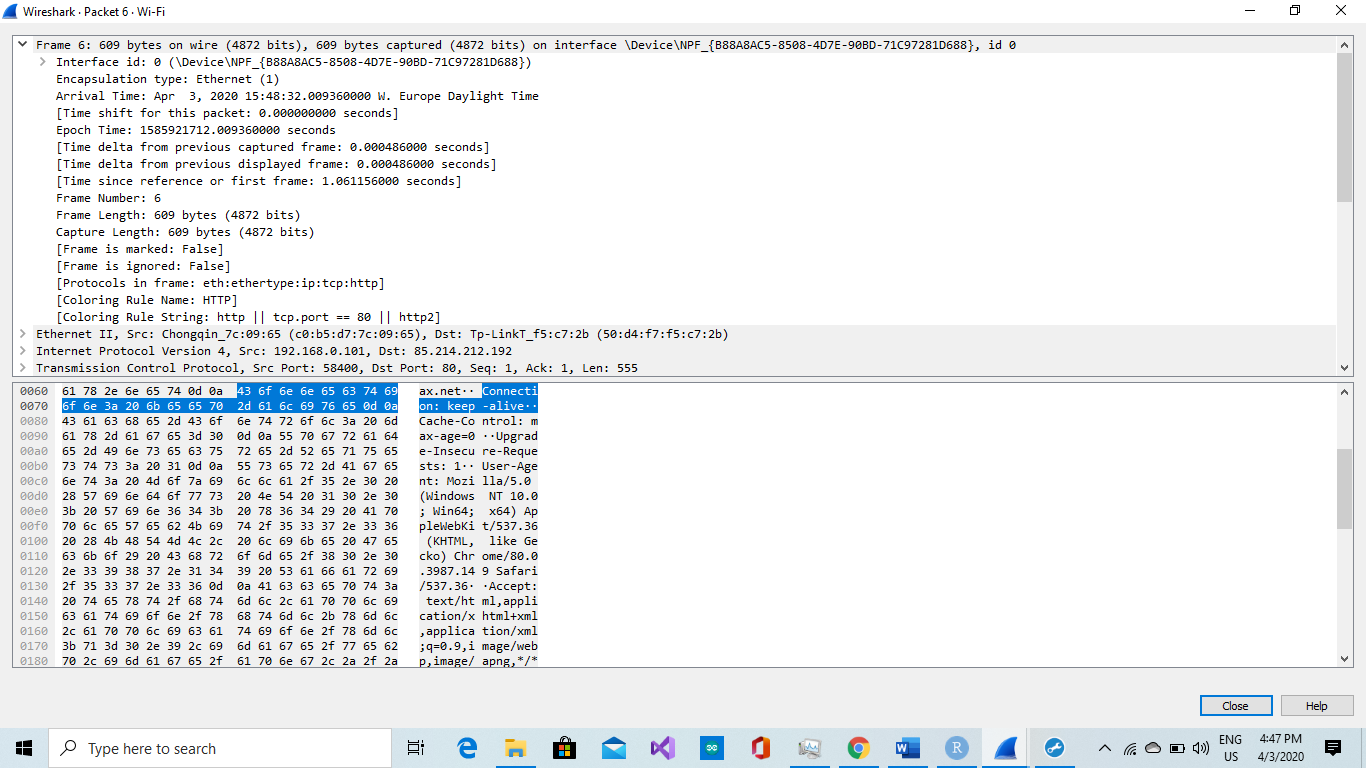
Provide a screenshot below with the Wireshark snapshot and highlight the host name:



* Find the HTTP Response belonging to the HTTP Get packet. How much time elapsed between the HTTP Get and HTTP response?

Time elapsed: 1.061156000 seconds

Provide a screenshot below with the Wireshark snapshot and highlight the elapsed time:



Task 3: Do Linux Tutorial

Go to <http://www.ee.surrey.ac.uk/Teaching/Unix/index.html> and do the tutorial three.

Provide screenshots of all exercises in section 3.4



Exercise 3b