Chapter 1

Preliminary: Introduction to Wireshark, GNS3 and Python

The labs in this course were designed to help the students better understand the concepts that they learn in the course UE21EC351A Computer Communication Networks through hands-on experience. The experiments in this lab cover the important concepts and protocols related to the application layer, transport layer and network layer. Students may explore the link layer functionalities using open ended experiments.

This lab begins with an introduction to the concept of a protocol stack. Students are explained how the process of sending data from host to host across a communication network is parsed into various layers of the protocol stack. Students are also briefed about the role of IPv4 addresses and services provided by each layer.

Introduction to the various software used during the labs are also given.

1.1 Overview

1.1.1 Concept of protocol stack

Application developers have produced a variety of messages (e.g., email, messages containing webpage, etc.), each having its own representation and associated process or program for interpreting the messages and executing the tasks based on contents of the message (e.g., a web browser is a end-user process which runs the HTTP protocol for exchanging messages with a web server which stores webpages). Sending messages from host to host is a complex process as there is a jungle of network components (e.g., routers and switches) which have to be traversed before the message reaches the destination. A host may be running multiple application processes with each communicating with a corresponding process running on a different host on the other side of the internet (sometimes separated by thousands of miles). Further, there are millions of users which are also sending messages to their respective destination hosts via the common network components. Hence, there is a need to execute the above complex process as several subtasks where each subtask has its own functions. These subtasks are referred to as layers which are named as application layer (one which generates and formats the message), transport layer (one which multiplexes and demultiplexes the messages leaving and arriving at the hosts respectively), network layer (one which identifies the path of network components leading to the destination host), link layer (one which pushes the data onto the physical medium connecting the host with the first network component on the path to the destination) and the physical layer (one which carries the data as modulated carrier signals). At the sending host, an application message along with its header is encapsulated into a transport layer segment. The transport layer segment along with its header is encapsulated into an IP datagram. The IP datagram along with its header is encapsulated into a frame. The frame along with its header is converted into bits and the

modulated carrier signal is transmitted at the physical layer. The reverse happens at the receiving host, where each layer starting with the link layer which removes its header after some pre-processing and passes the remaining payload to its upper layer. This process is repeated till the message is retrieved by the corresponding application layer process running at the receiving host.

1.1.2 Software tools

The various software tools used in this lab include Wireshark, GNS3 and Python.

Wireshark is a free network protocol analyzer that runs on Windows, Mac, and Linux /Unix computers. It's an ideal packet analyzer for our labs – it is stable, has a large user base and well documented support that includes a user-guide (available at http://www.wireshark.org/docs/wsug_html_chunked/), man pages (available at http://www.wireshark.org/docs/man-pages/), and a detailed FAQ page (available at http://www.wireshark.org/faq.html), rich functionality that includes the capability to analyze hundreds of protocols, and a well-designed user interface. It operates in computers which use Ethernet, serial (PPP), 802.11 (Wi-Fi) wireless LANs, and many other link-layer technologies.

GNS3 is a very popular network emulator which can be used to virtually design computer networks. GNS3 is used by several companies such as AT&T, CISCO, Intel, etc. The configuration of the network components can also be exported to a real network. GNS3 offers a wide range of configuration commands for the network layer and link layer. A virtual network design in GNS3 can be integrated with a real network and data can be exchanged with destination hosts on the public internet via GNS3 network. Wireshark can be incorporated into GNS3 to analyze the packets exchanged between any pair of devices (e.g., routers and hosts).

Python is a powerful, simple and elegant programming tool. Various open source libraries are available online. Students will use Python 2.7 or above to write socket programs and demonstrate key application layer and transport layer concepts.

1.2 Procedures

1.2.1 Wireshark installation

To download and install the Wireshark go to http://www.wireshark.org/download.html and download and install the Wireshark binary for your computer. In order to run Wireshark, you'll need to have access to a computer that supports both Wireshark and the *libpcap* or *WinPCap* packet capture library. The *libpcap* software will be installed for you, if it is not installed within your operating system, when you install Wireshark. For Linux installation see the end of the chapter.

1.2.2 Familiarizing and running Wireshark

Upon running Wireshark the following window is displayed. The available network adapters can be observed in Fig. 1 under *Interface list*. The network adapter which is connected to the internet is chosen and the start button (displayed as green shark fin) is chosen. A web browser is opened and any url (e.g., http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html) is entered. Wireshark would start displaying various packets exchanged over the network adapter. Three sub-windows appear within the main window (top-down), namely, *packets listing window* which shows the various packets exchanged along with their labels, source and destination IP addresses (or host names), epoch time and size of the packet, *packet headers window* which shows the content of any packet selected in the packets listing window, such as protocol headers arranged according to the protocol stack and the application layer message (if any), and the *packet content window* which shows the raw data corresponding to the packet chosen. The various sub-windows can be observed from Fig. 2.

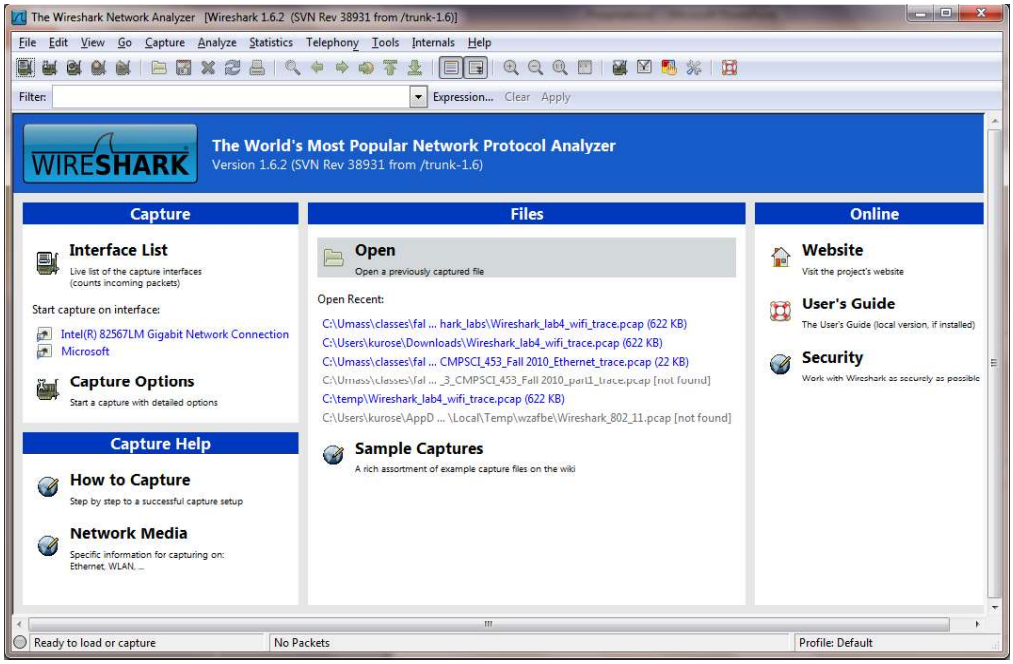

Fig. 1: Initial Wireshark Screen

Packets can also be chosen according to the protocol type by entering the packet type in the search bar. For example, enter *http* into the search bar and only packets containing HTTP messages are displayed in the packets listing window. Selecting the HTTP GET message will display the HTTP message along with the HTTP header. Besides, even the transport layer header, datagram header (i.e., network layer header), link layer header can be observed as in Fig. 3.

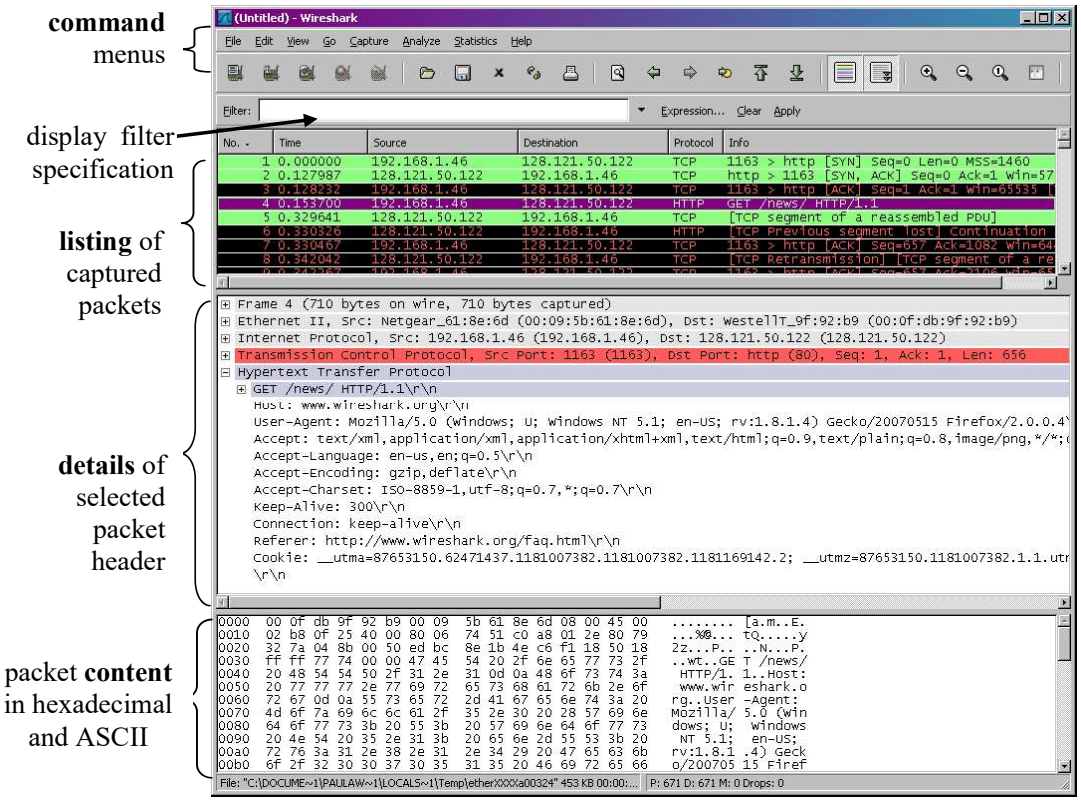

Fig. 2: Wireshark Graphical User Interface, during packet capture and analysis

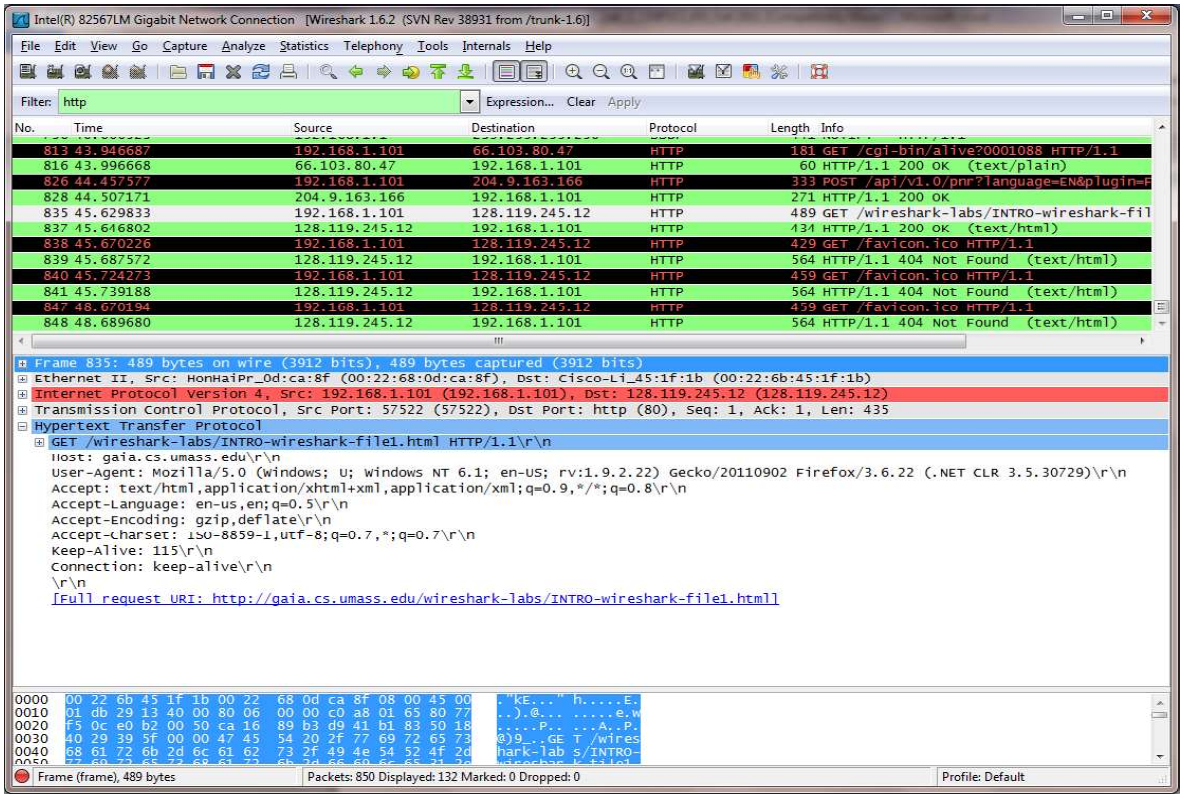

Fig. 3: Wireshark window upon entering http in search bar

1.2.3 GNS3 installation

GNS3 1.1.3 is downloaded from www.gns3.com and installed by selecting the exe file. Select GNS3, WinPCAP, Wireshark, Dynamips, VPCS during the installation (in the choose components window) and follow the instructions.

Download the ios images for CISCO routers c7200 and c3725 from the internet by searching in google **or** in the link https://mega.nz/folder/nJR3BTjJ#N5wZsncqDkdKyFQLELU1wQ or from the google drive link https://drive.google.com/drive/folders/18Aqx2n6XlNTc-ajxp7ThigRCMc1ac4u5?usp=sharing.

Once either .image or .bin file is downloaded, install them by following the instructions as given in https://www.computernetworkingnotes.com/ccna-study-guide/how-to-add-install-or-import-ios-in-gns3.html **or** Start GNS3 and select the Edit from the Menu and then select Preferences. Choose IOS routers. Add a new router IOS by locating it in the PC.

After adding the router, click on the Ok button. For Linux installation see the end of the chapter.

1.2.4 Simple network configuration using GNS3

Draw the following simple network by dragging and dropping the components from the left pane as shown in Fig. 4. Right click on the router and select configure. Select slots, choose slot 2 and add NM-4T to add 4 serial ports to the router (will be used in later experiments).

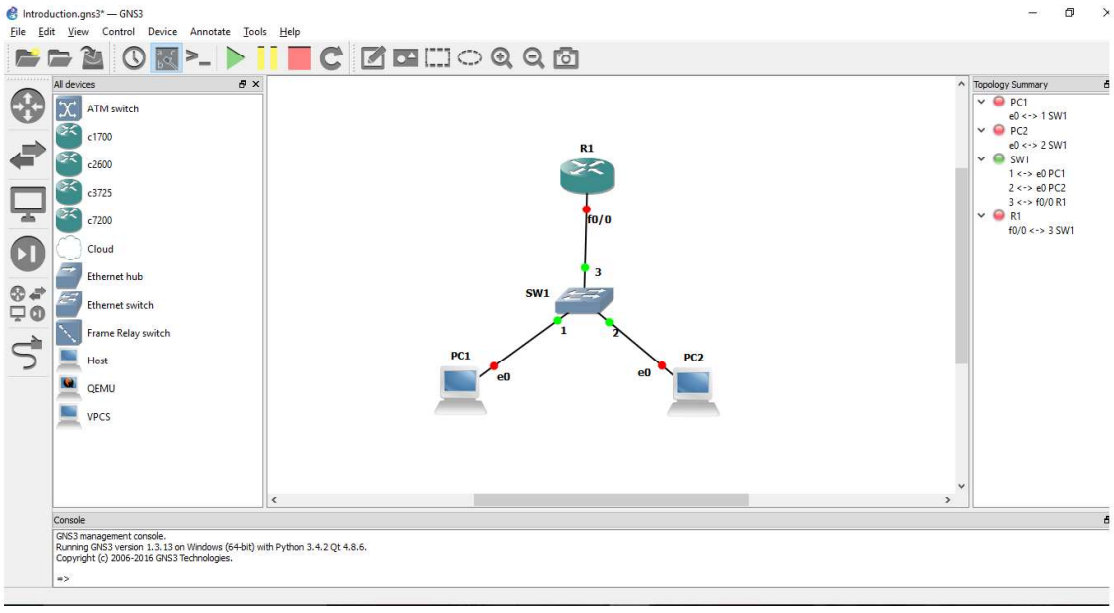

Fig. 4: Simple network in GNS3

Turn on all devices by clicking on the play button. Right click on the router and select Idle_PC, thereafter, choose any value with an asterisk to set the resources for the virtual router. Type the following commands for configuring the router (c3725 router).

```
R1#configure terminal
R1(config)#interface f0/1
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

Type the command PC1> ip 10.0.0.2/24 10.0.0.1 in PC1 by double clicking it. Similarly, type PC1> ip 10.0.0.3/24 10.0.0.1 in PC2 by double clicking it. Next, type the following command in PC1 to display the ping statistics. Observe whether ping was successful. Ping is used to check if a destination device (clients/router) are available.

```
PC1> ping 10.0.0.3
```

Right click on any port and select Start capture. Repeat ping operation and observe the packets exchanged.

1.2.5 Python installation

Python installation can be done by downloading Python 2.7 or above from www.python.org. After installing python, open Python IDLE from which you can choose the editor for writing python programs with the .py.

Alternatively, you can install Sypder 3 or above from https://www.anaconda.com/download/

Linux installation

1. Open Ubuntu software center and install Spyder 3
2. To install GNS 3:
    a. Open terminal and type the following
    b. sudo add-apt-repository ppa:gns3/ppa
    c. sudo apt-get update
    d. sudo apt-get install dynamips gns3
3. To import router C3725 open https://www.sysnettechsolutions.com/en/gns3/gns3-supported-ios-images-download/. Download c3725-adventerprisek 9-mz.124-15.T14. After extracting the file, open GNS3 and add ios image by right clicking on the router images.
4. To enable Wireshark capture type the following in the terminal
    a. sudo dpkg-reconfiugure wireshark-common
    b. select yes
    c. sudo chmod 777 /usr/bin/dumpcap