Computer Networks Project

(100 Points or more)

For: CSE and CEES

Aly Osama

Prof. Ayman Bahaa

1 Project Description:

1.1 Introduction

- Wireshark is the best packet analyzer program. Many network engineers used it in order to solve communication issues.
- You can find many jobs require Wireshark for a network engineer with average salary $88000 in US. Check this link for more details.
- Now, you are familiar with Wireshark so we can move the next step which is implementing a program similar to Wireshark.

1.2 Goals (What will you gain from this project?)

- Be familiar with low level network programming and get experience with different packet protocols.
- Improve your programming and software engineering skills.
- Learn more about GUI applications
- Use multithreading in your applications.
- Be familiar with git for version control and how you use it with a team.
- You can add this project to your C.V. which will prove your coding skills for the companies' interviews.
- It will help you to get more points and adjust your computer network course work

2. Project Logistics:

2.1 Team members:

- **3-4 members** in each team.
- If you don't find any team, you can coordinate with your class representative.
- Select a cool name for your team (les miserable) ;)

2.2 Deliverables:

- **SourceCode:** You have to push your code on **github.com** repository.
- **Document:** You have to write a brief (very brief) a report with your project description, source code link (github), project features and screenshots.

2.3 Time:

- You have to send the document before **12:00AM on Friday 22th Dec 2017**
  - To: cse-networks-2016@googlegroups.com
  - Subject: **TeamLeaderID_Class_PROJECT**
    - As example: 11P6006_CESS_PROJECT
- Discuss the project details with the TA on **Saturday 23th Dec 2017**
  - **To be announced**
- Note:
  - No excuses or delay for the deadline even if (لو سمحت يا باشمهندس ممكن تأخره عشان عندنا عيد ميلاد)… Congratulations by the way.

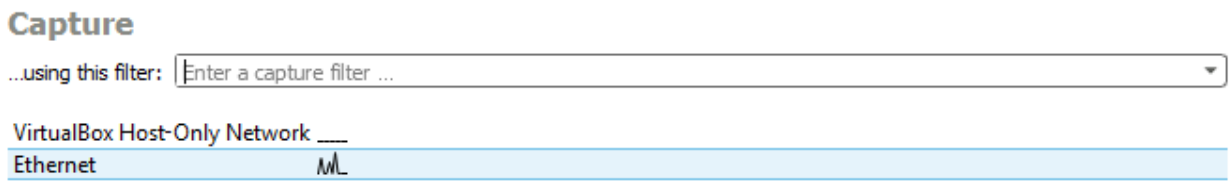
2.4 Grading:

- 50% on implementing required project features. (Team grading)
- 10% on the document (Team grading)
- 10% on the repository (Team grading)
  - Everyone in the project should commit his own code
- 30% on individual discussion (Individual grading)
- 20% Bonus on the best team (only one team)

3. Project Requirements:

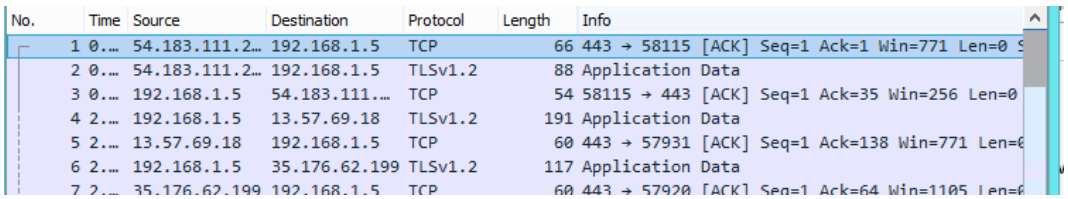
3.1 Project main features:

1. Select Capture Network (Ethernet, WIFI, ..etc)



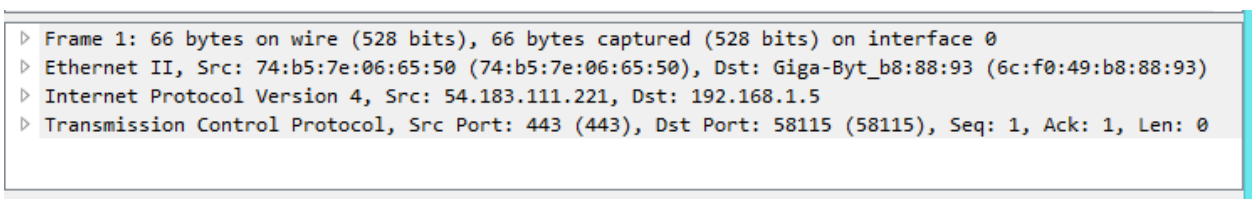
2. Control the Start and Stop sniffing

3. Show main details of the packets in a table

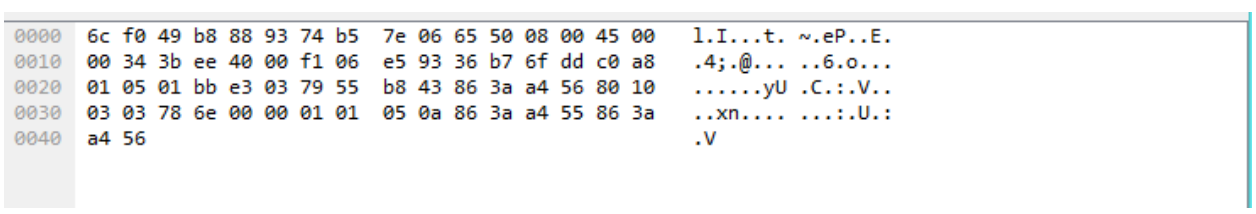


No.	Time	Source	Destination	Protocol	Length	Info
1	0.…	54.183.111.2…	192.168.1.5	TCP	66	443 → 58115 [ACK] Seq=1 Ack=1 Win=771 Len=0 S
2	0.…	54.183.111.2…	192.168.1.5	TLSv1.2	88	Application Data
3	0.…	192.168.1.5	54.183.111.…	TCP	54	58115 → 443 [ACK] Seq=1 Ack=35 Win=256 Len=0
4	2.…	192.168.1.5	13.57.69.18	TLSv1.2	191	Application Data
5	2.…	13.57.69.18	192.168.1.5	TCP	60	443 → 57931 [ACK] Seq=1 Ack=138 Win=771 Len=0
6	2.…	192.168.1.5	35.176.62.199	TLSv1.2	117	Application Data
7	2.…	35.176.62.199	192.168.1.5	TCP	60	443 → 57920 [ACK] Seq=1 Ack=64 Win=1105 Len=0

4. If you click on a packet, it will show you detailed view for HTTP or TCP protocols at least. For the another protocols it will be bonus



5. If you click on a packet, it will show you hex view



6. You can save and load the captured packets in pcap format.
7. You can filter the captured packets based on the main columns of the table

8. The program should be multithreaded with graphical user interface.

3.2 Tools and programming languages:

- You can use C++, Java, C# or Python. (I wrote all of them so I can understand your code)
- For the GUI applications, use QT or JavaFX
- For the network libraries, use **Pcap** or **libpcap** library
    - Pcap library is used in Wireshark too. It is a c library.
    - Fortunately, many did a wrapper for this library for C++,Java, Python and .Net
        - The only one I know is C++ library **PcapPlusPlus**.
        - Use **Google** to find other wrappers for different languages in case you use language rather than C++
- For Source Control use **git**.
- You can use any other library but you have to include a clarification in the document (why you use that)

Good Luck

Computer Networks with Machine Learning

(Bonus Project)

Bonus Project Description:

Description

- In case your passion is machine learning, I have a project for you which will learn you a lot about the machine learning cycle.
- You can work on a creating a model for classify the packets into (normal and up normal). Or classify packets into different applications or protocols (based on a statistical features In your data)

Data Selection:

- You can use Wireshark program for creating your dataset manually.
- Or you can download any available dataset. Check "towards generating real-life data sets for network intrusion detection" paper
- Or you can check this dataset

Feature extraction:

- Unfortunately, network packets is not same as image. You have to extract different features from the packet. Check this paper paper

Model Selection

- Split your data with 80% 20% rule.
- You can try different algorithms like SVM, Bayes classifier, NN, CNN and LSTM.

Deliverable:

- **Document:** Write a document in latex format including your work in the same format as scientific papers. (**In case your document is awesome which means you get a significant accuracy, we can work on it in the vacation and publish it in a conference**)
- **Code:** on a private repository in "Gitlab.com"

Time and Grading is same as the pervious project