Project Document

Course Title: CE 340 Cryptography & Network Security
Project Title: Wireshark Usage
Project Member: Emre Övünç

CONTENTS

PART I

1. Wireshark

1.1 What is Wireshark

1.2 Purposes

PART II

2. How to Use Wireshark

2.1 Wireshark Interface

2.2 Capturing Data

2.3 Filters

PART III

3. Packets

3.1 EAPOL Handshake

3.2 Domain Name Server (DNS)

3.3 D.o.S SYN Flood

3.4 HTTP

3.5 IP&Port Scanning

PART I

1.1 What is Wireshark?

Wireshark is a free and open-source protocol&packet analyzer which will try to capture network packets and tries to display that packet data as detailed as possible. Also, it is a tool for seeing the bits and bytes flowing through a network in human readable form.

Note !

Wireshark isn’t an intrusion detection system.

Wireshark will not manipulate things on the network.

1.2 Purposes

Some people like Network Administrators, Security Engineers, developers use it for learn network protocol, troubleshoot network problems or examine security problems

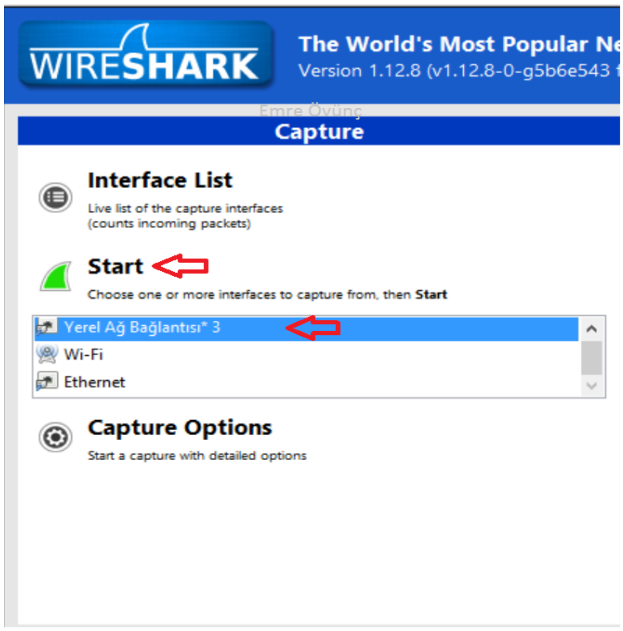
PART II

2.1 Wireshark Interface

After installing Wireshark, you can start it and you should interface list of your devices on the Wireshark GUI. If you don't, your wireless adapter may not install correctly or your computer has another problems.

2.2 Capture

You can select a device and press Start to see receiving and sending packet on your network.



2.3 Filters

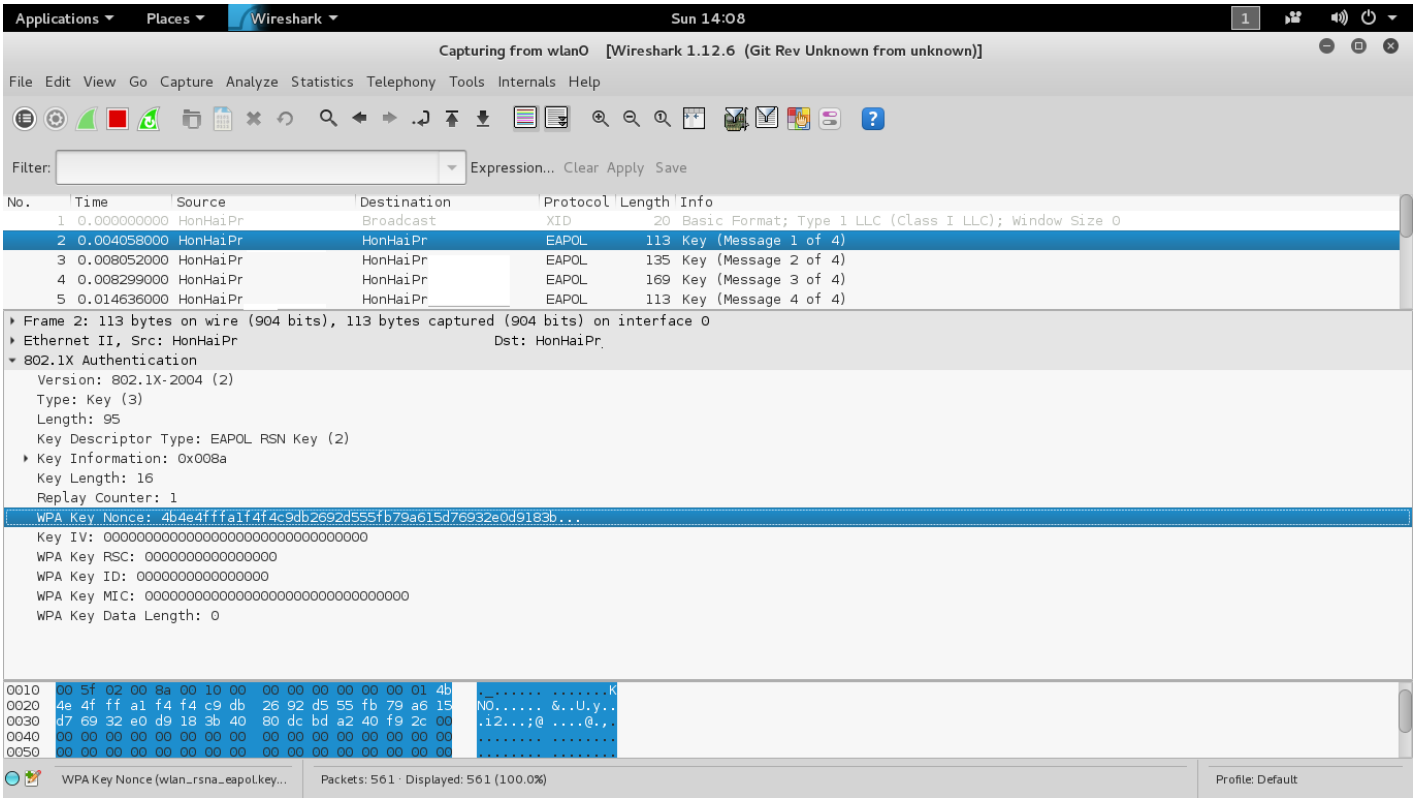
You can filter captured data by using Wireshark Filters. It provides us to analyse specific data on the network and see what is going in there. The best filters which people generally use are ;

eeth.addr==aa:bb:cc:11:22:33
ip.src==192.168.1.2
arp.dst.proto_ipv4==192.168.1.100
ip.addr==192.168.1.2
ip.addr==192.168.1.2 && ip.addr==192.168.1.3
ipv6.addr==2001::4
tcp.port==444
http and arp
http or dns

PART III

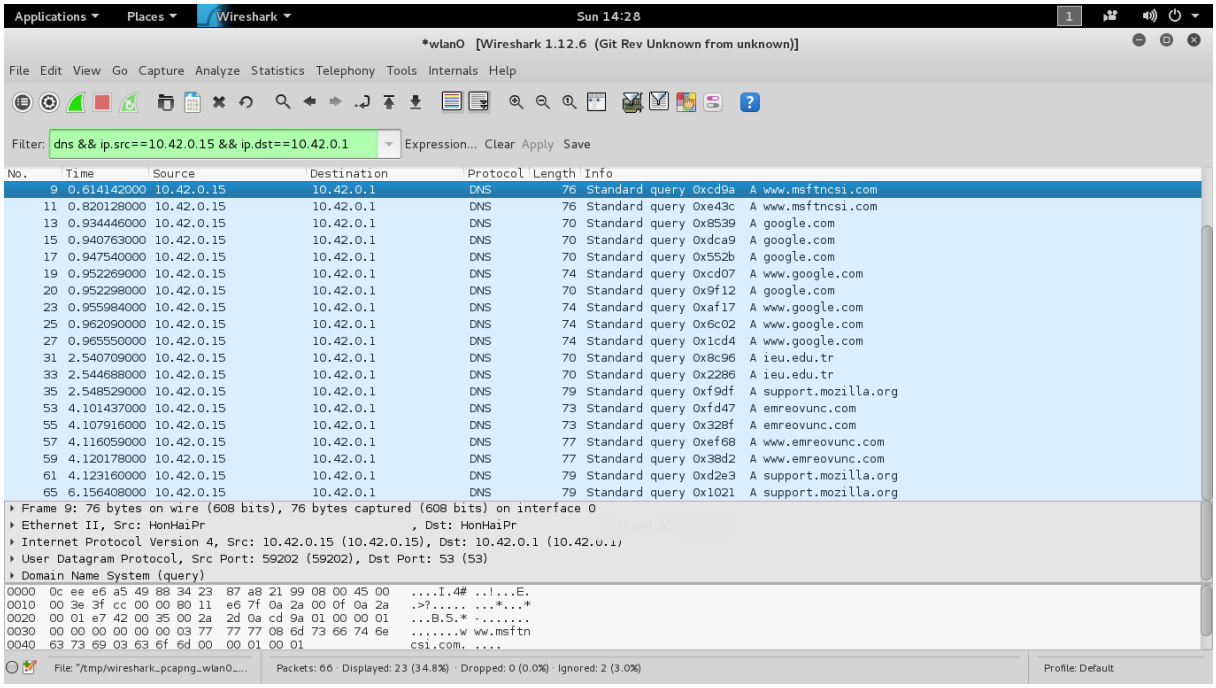
3.1 EAPOL Handshake

WPA and WPA2 use keys derived from an EAPOL handshake to encrypt traffic. Unless all four handshake packets are present for the session you are trying to decrypt.



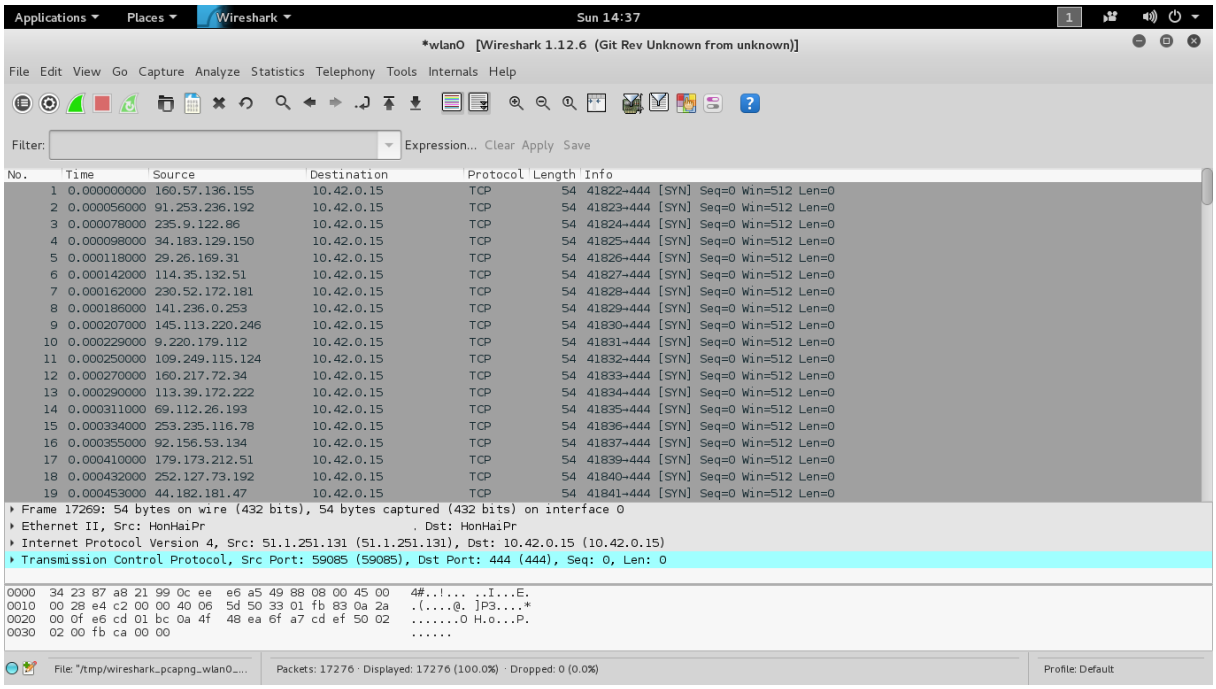
3.2 Domain Name Server (DNS)

DNS is the system used to resolve store information about domain names including IP addresses, mail servers, and other information.



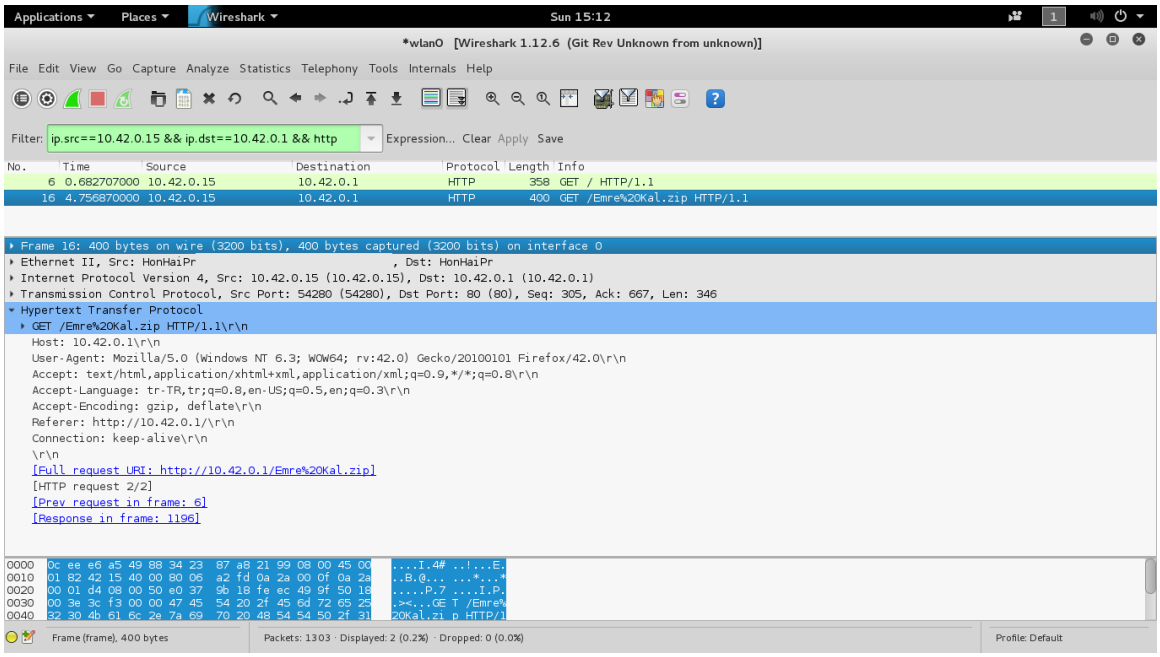
3.3 D.o.S SYN Flood

On the network , I simulate the DoS attack by using SYN Flood and capture the all traffics. This results show us about attack type which is generated random source and SYN Flood attack.



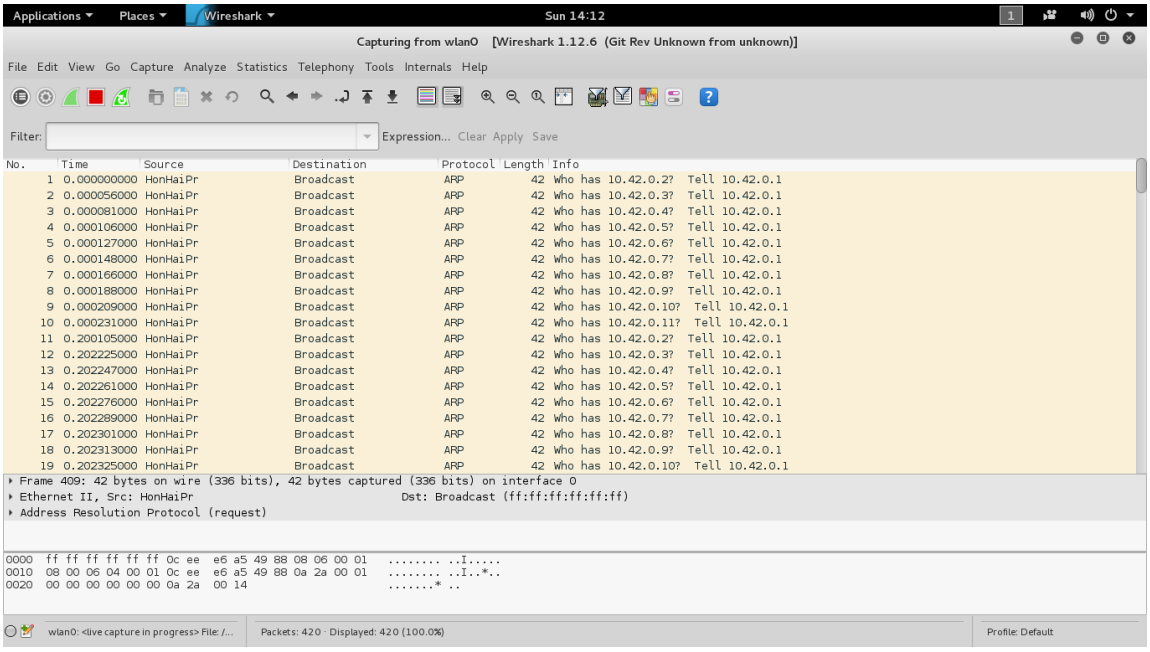
3.4 HTTP

When you visit a web site, you request something from the web server. If you run Wireshark on your system and go to a web site, you will see packets about the web site. In addition, in this picture I download a zip file from the server.



3.5 IP&Port Scanning

Ip and Port Scanning is one of the most popular techniques attackers use to discover services on your computer. Well Known Ports (0 – 1023) & Registered Ports (1024 – 49151)



References:

https://en.wikipedia.org/wiki/Wireshark

https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html