

# Fun with Wireshark

# Intro

This tutorial will give a basic idea on WireShark. It will introduce how to setup filters and how to capture unencrypted traffic and why is it way better to use encrypted websites.

## Learning objectives

- Capture network traffic in our machine
- Analyze the most common used unsecured traffic
- Setting up some basic filters on Wireshark

## Prerequisites

- Windows computer
- Internet connection
- Wireshark
- Connections to nmu network via wifi or lte ( for lesson 3)
- Download these files:

<https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=http.cap>

[https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=http\\_with\\_jpegs.cap.gz](https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=http_with_jpegs.cap.gz)

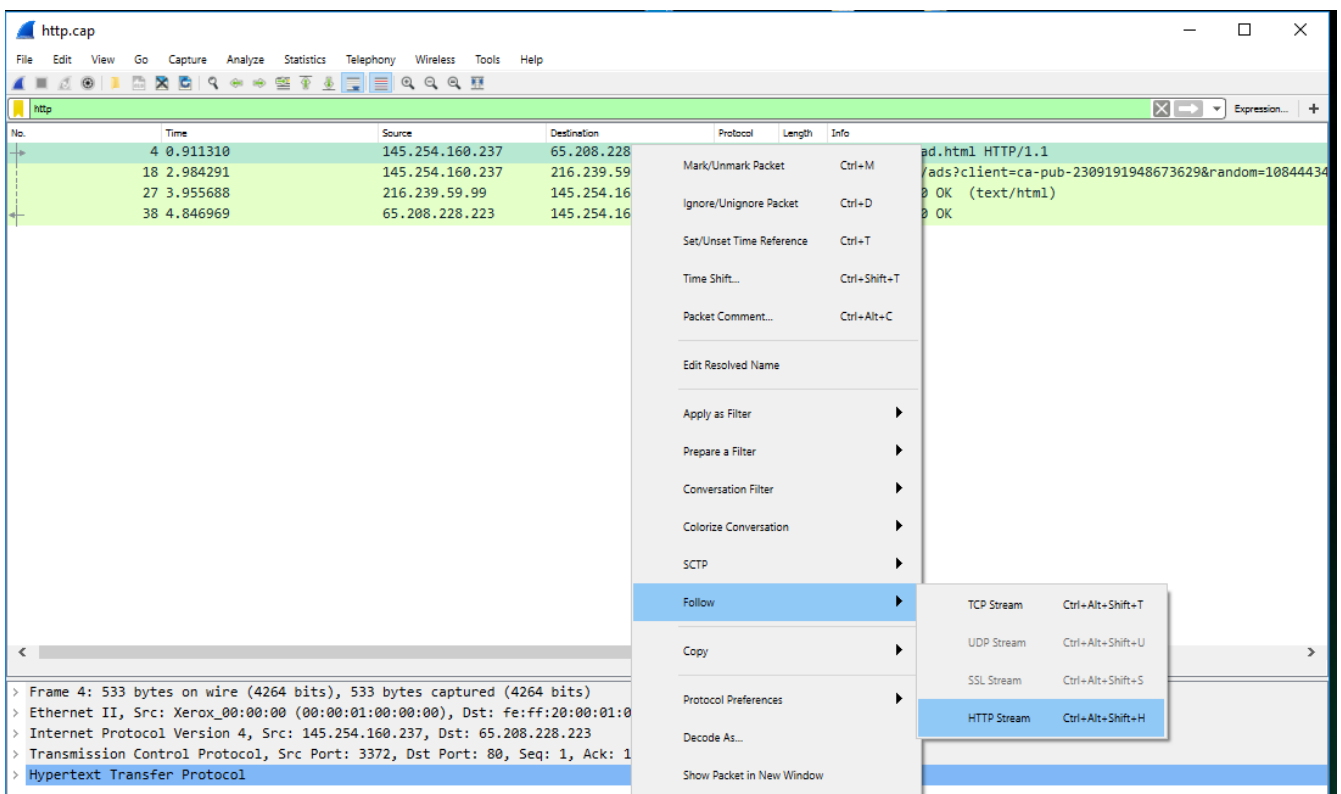
## Instructions

### Lesson one

Lets visit a website where we can reconstruct the website by following the tcp/http stream. \* Open the http.cap file \* Set up the filter to only show http traffic ( this is optional, it just help us to learn the filter)

No.	Time	Source	Destination	Protocol	Length	Info
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-pub-2309191948673629&ra
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html)
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X...	478	HTTP/1.1 200 OK

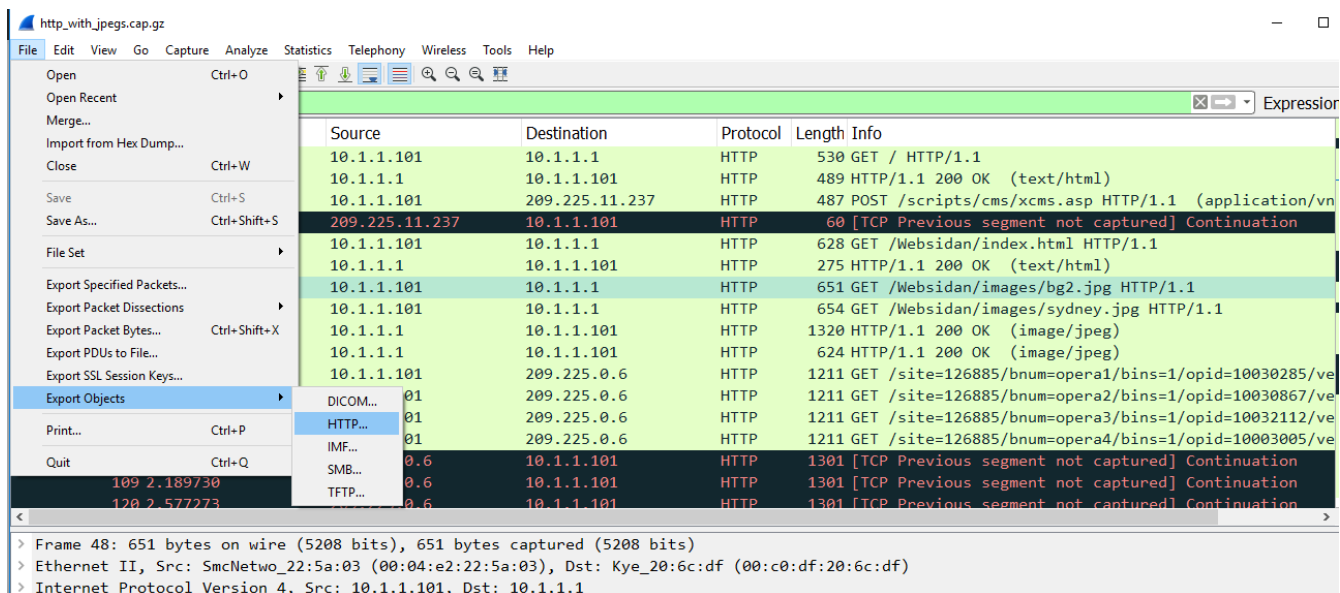
- Now click on the followings



Now we can see the whole html code, with this information we can reconstruct the whole website.

## Lesson two

It is very simple to save pictures from an unencrypted website as well. \* Let sopen the http\_with\_jpegs.cap.gz file \* Open Export Objects, HTTP

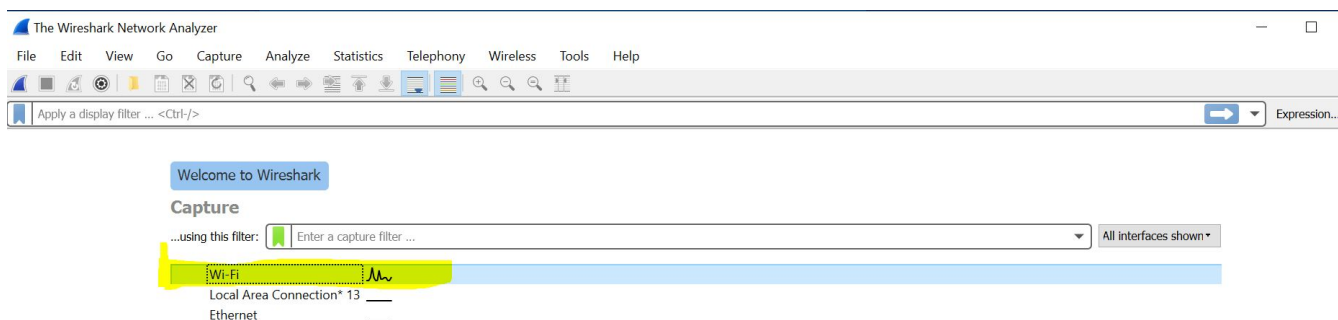


- Find an image file and simply save it.

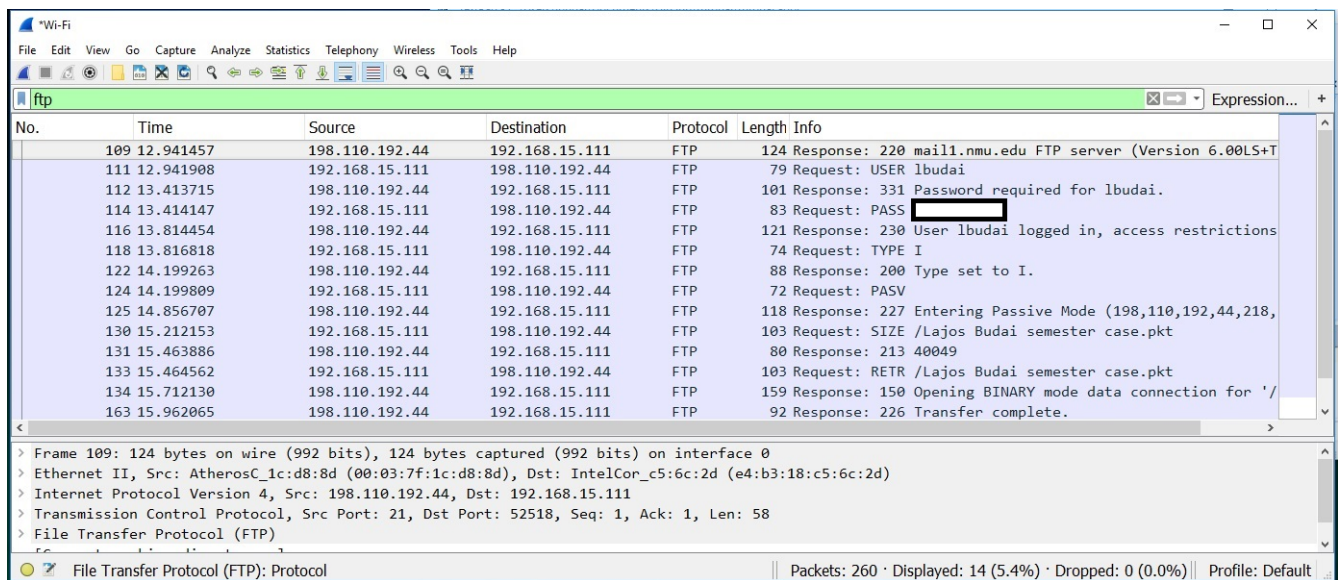
## Lesson three

Now let's connect to the NMU FTP server

- Go to File Explorer and find [lbudai] on myweb.nmu.edu [this should be your nmuid]
- If it asks your username and password you are all set and you can skip the next bulletpoint
- Create a random txt file, and upload it in here. Now delete the file from your computer, and try to open the file from your nmu server.
- Start capturing the traffic on the interface where we see traffic.



- Now we will have way more traffic, so lets make sure to type ftp to the filter bar.
- The following packets should be in front of us.



No.	Time	Source	Destination	Protocol	Length	Info
109	12.941457	198.110.192.44	192.168.15.111	FTP	124	Response: 220 mail1.nmu.edu FTP server (Version 6.00LS+T
111	12.941908	192.168.15.111	198.110.192.44	FTP	79	Request: USER lbudai
112	13.413715	198.110.192.44	192.168.15.111	FTP	101	Response: 331 Password required for lbudai.
114	13.414147	192.168.15.111	198.110.192.44	FTP	83	Request: PASS [REDACTED]
116	13.814454	198.110.192.44	192.168.15.111	FTP	121	Response: 230 User lbudai logged in, access restrictions
118	13.816818	192.168.15.111	198.110.192.44	FTP	74	Request: TYPE I
122	14.199263	198.110.192.44	192.168.15.111	FTP	88	Response: 200 Type set to I.
124	14.199809	192.168.15.111	198.110.192.44	FTP	72	Request: PASV
125	14.856707	198.110.192.44	192.168.15.111	FTP	118	Response: 227 Entering Passive Mode (198,110,192,44,218,
130	15.212153	192.168.15.111	198.110.192.44	FTP	103	Request: SIZE /Lajos Budai semester case.pkt
131	15.463886	198.110.192.44	192.168.15.111	FTP	80	Response: 213 40049
133	15.464562	192.168.15.111	198.110.192.44	FTP	103	Request: RETR /Lajos Budai semester case.pkt
134	15.712130	198.110.192.44	192.168.15.111	FTP	159	Response: 150 Opening BINARY mode data connection for '/'
163	15.962065	198.110.192.44	192.168.15.111	FTP	92	Response: 226 Transfer complete.

> Frame 109: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0 > Ethernet II, Src: AtherosC_1c:d8:8d (00:03:7f:1c:d8:8d), Dst: IntelCor_c5:6c:2d (e4:b3:18:c5:6c:2d) > Internet Protocol Version 4, Src: 198.110.192.44, Dst: 192.168.15.111 > Transmission Control Protocol, Src Port: 21, Dst Port: 52518, Seq: 1, Ack: 1, Len: 58 > File Transfer Protocol (FTP)	
--	--

Now behind the white-black rectangle my password for nmuh is hiding. Anyone who could capture this data, can see my very sensitive password. Using FTP without encryption is a bad practice.

## Challenge

- Lets capture some real traffic. Go and visit some comonly used websites. Can you find any useful information?
- Try to find a website with unencrypted traffic, and try to figure out the context by using wireshark, and try to save down some images.

## Reflection

- What do you think about unencrypted wireless traffic? Can someone capture these kind of traffics from the "air"?