

IS 504 – Lab #1

Due: March 1, 2020 – 23:30

Submission and Grading Policy

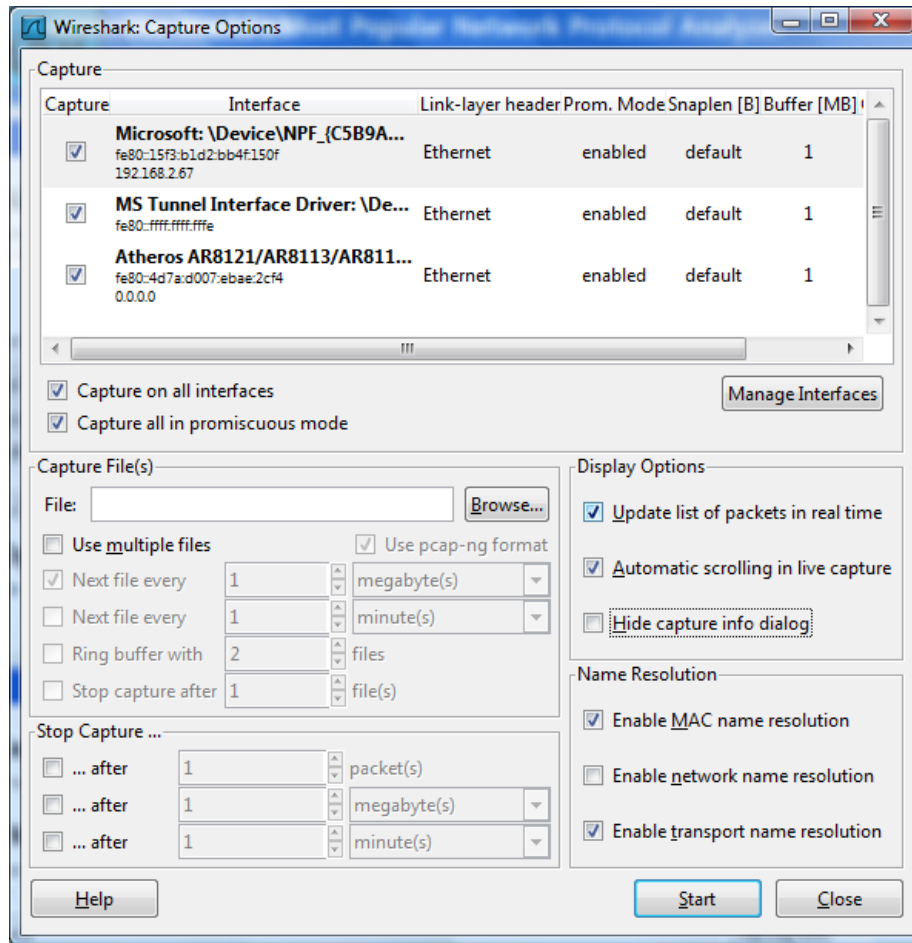
- This is an individual assignment. Please don't collaborate.
- You have to adhere to academic integrity principles.
- Submit your assignments to the corresponding assignment link in <https://odtuclass.metu.edu.tr>.
- Solutions should be submitted in a single doc, docx or pdf file named: <metuusername>_LAB_1.<extension> (e.g., "e123456_LAB_1.pdf").
- In lab assignments, you must also upload the captured data file (.pcapng file). You should zip your assignment report and captured the data file into a zip format. Do not upload any other files.
- Late submissions can be accepted by March 4, 2020, 23:30 with a 15% per day penalty.
- Do not hesitate to write your questions about the assignments to the related assignment topic under the Discussions - Q&A forum on ODTUClass.

Lab Homework Instructions

The goal of this first assignment is primarily to introduce you to Wireshark. Download "Wireshark" and based on the Wireshark experimentation in "Wireshark_Intro" document answer the questions under "What to hand in" section. Prepare **a report** covering the answers of these questions. Save the captured packet data in the extension of **.pcapng** used to obtain your solutions for the questions and **submit it along with your report**.

Notes:

- In case your computer has more than one active network interface (e.g., if you have both a wireless and a wired Ethernet connection), you will need to select an interface that is being used to send and receive packets (mostly likely the wired interface). Select **"Capture on all interfaces"** option as shown below figure.



- **You should put all the screenshots of the captured data related to the answers. Add each screenshot below the related answer in your assignment report (not put them into a zip file). You should also mark the parts pointing the answers on the screenshots as shown below figure.**

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
6	0.296821	192.168.2.21	128.119.245.12	HTTP	GET /wireshark-labs/INTRO-wireshark-file.html HTTP/1.1
8	0.582848	128.119.245.12	192.168.2.21	HTTP	HTTP/1.1 200 OK (text/html)
24	6.643998	192.168.2.21	209.85.229.104	HTTP	GET / HTTP/1.1
29	6.826418	209.85.229.104	192.168.2.21	HTTP	HTTP/1.1 302 Found (text/html)
35	6.861186	192.168.2.21	69.147.112.160	HTTP	GET / HTTP/1.1
38	6.884654	192.168.2.21	64.4.20.184	HTTP	GET /mail/logout.aspx HTTP/1.1
46	7.016622	192.168.2.21	209.85.229.147	HTTP	GET / HTTP/1.1
50	7.173088	69.147.112.160	192.168.2.21	HTTP	HTTP/1.1 302 Found (text/html)
63	7.207525	209.85.229.147	192.168.2.21	HTTP	HTTP/1.1 200 OK (text/html)
68	7.210218	64.4.20.184	192.168.2.21	HTTP	HTTP/1.1 200 OK (text/html)
69	7.256829	192.168.2.21	64.4.20.184	HTTP	GET / HTTP/1.1
72	7.275463	192.168.2.21	63.111.24.129	HTTP	GET /weather/local/TUXX0002?cc=%&unit=m HTTP/1.1
75	7.276209	192.168.2.21	65.212.118.26	HTTP	GET /1?1?id=1166158504&nd=41853683 HTTP/1.1
79	7.440431	192.168.2.21	199.7.50.72	OCSP	Request
84	7.531431	63.111.24.129	192.168.2.21	HTTP/XML	HTTP/1.1 200 OK
85	7.532553	65.212.118.26	192.168.2.21	HTTP	HTTP/1.1 200 OK (GIF89a)
86	7.532569	192.168.2.21	63.111.24.129	HTTP	GET /weather/local/TUXX0002?dayf=2&unit=m HTTP/1.1
88	7.578006	64.4.20.184	192.168.2.21	HTTP	HTTP/1.1 302 Found (text/html)
89	7.581519	192.168.2.21	209.85.229.147	HTTP	GET /csi?v=3&s=webhp&action=&e=17259,24029,24035&ei=POGbs8Vkk6qT4gbN9ez2Pag&exp1=...
92	7.700362	199.7.50.72	192.168.2.21	OCSP	Response
98	7.713853	192.168.2.21	209.85.229.101	HTTP	GET /generate_204 HTTP/1.1
102	7.749190	209.85.229.147	192.168.2.21	HTTP	HTTP/1.1 204 No Content
107	7.783141	63.111.24.129	192.168.2.21	HTTP/XML	HTTP/1.1 200 OK
109	7.852287	209.85.229.101	192.168.2.21	HTTP	HTTP/1.1 204 No Content

Frame 109 (200 bytes on wire, 200 bytes captured)

Ethernet II, Src: Airtiesw_76:3e:7d (00:1c:a8:76:3e:7d), Dst: IntelCor_64:1f:48 (00:21:5d:64:1f:48)

Internet Protocol, Src: 209.85.229.101 (209.85.229.101), Dst: 192.168.2.21 (192.168.2.21)

Transmission Control Protocol, Src Port: http (80), Dst Port: 60355 (60355), Seq: 1, Ack: 676, Len: 146

Source port: http (80)

Destination port: 60355 (60355)

[Stream index: 14]

Sequence number: 1 (relative sequence number)

[Next sequence number: 147 (relative sequence number)]

0000 00 21 5d 64 1f 48 00 1c a8 76 3e 7d 08 00 45 40 ...!dH...>}.E8

0010 00 ba 00 9d 00 36 06 09 e9 d1 55 e5 65 c0 a86...U.e..

0020 02 15 00 50 eb c3 1d 80 06 e2 04 9d fe b4 50 18 ...P....P.

0030 00 6f e3 6f 00 00 48 54 54 50 2f 31 2e 31 20 32 ...o.o..HT TP/1.1 2

0040 00 34 20 4e 6f 20 43 6f 6e 74 65 6e 74 0d 0a 43 04 No Co ntent..c

File: C:\Users\acer\AppData\Local\Temp\... Packets: 1426 Displayed: 255 Marked: 0 Dropped: 0

Profile: Default

- Your screenshots related to **HTTP protocol** includes the **details of the selected packet header and packet content**, as shown below figure.

Atheros L1C PCI-E Ethernet Controller \Device\NPF_{20105473-2956-4E11-A4FD-B12637583F70} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
357	12.0813130	199.7.51.72	144.122.98.231	OCSP	789	Response
370	12.1874970	144.122.98.231	199.7.55.72	OCSP	620	Request
372	12.2661880	199.7.55.72	144.122.98.231	OCSP	1491	Response
382	12.3331890	144.122.98.194	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
514	15.3715580	144.122.98.194	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
541	18.3714580	144.122.98.194	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
555	21.3715130	144.122.98.194	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
614	31.0947690	144.122.98.231	144.122.98.14	HTTP	517	GET / HTTP/1.1
635	31.6625800	144.122.98.14	144.122.98.231	HTTP	643	HTTP/1.1 200 OK (text/html)

Frame 614: 517 bytes on wire (4136 bits), 517 bytes captured (4136 bits) on interface 0

Ethernet II, Src: Giga-Byt_b4:67:3b (00:24:1d:b4:67:3b), Dst: Fujitsu_68:d2:79 (00:19:99:68:d2:79)

Internet Protocol Version 4, Src: 144.122.98.231 (144.122.98.231), Dst: 144.122.98.14 (144.122.98.14)

Transmission Control Protocol, Src Port: 49264 (49264), Dst Port: http (80), Seq: 1, Ack: 1, Len: 463

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: www.fi.metu.edu.tr\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; tr; rv:1.9.2.24) Gecko/20111013 Firefox/3.6.24\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: tr-tr;tr;q=0.8,en-us;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-9,utf-8;q=0.7,*;q=0.7\r\n

Keep-Alive: 115\r\n

Connection: keep-alive\r\n

Cookie: __utma=182427199.956471360.1294902253.1296545753.1321530107.4\r\n

\r\n

[Full request URI: http://www.fi.metu.edu.tr/]

0000 00 19 99 68 d2 79 00 24 1d b4 67 3b 08 00 45 00 ...h.y.\$..g;..E.

0010 01 f7 14 90 40 00 80 06 00 00 90 7a 62 e7 90 7a ...8...ab..2.

0020 62 0e c0 70 00 50 8e 8c 19 4c d9 07 71 86 50 18 b..p.p...L..q.p.

0030 40 29 e7 d3 00 00 47 45 54 20 2f 20 48 54 54 50 0)...GE T / HTTP

0040 2f 31 2d 21 67 74 3a 20 77 77 2d 2e /1..HO st: www.

0050 69 69 2e 6d 65 74 75 2e 65 64 75 2e 74 72 0d 0a fi.metu. edu.tr..

0060 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi

0070 6c 6c 61 2f 2e 30 28 57 69 6e 64 6f 77 73 lla/5.0 (windows

0080 3b 20 53 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 : U; win dows NT

0090 36 2e 31 3b 20 74 72 3b 20 72 76 3a 31 2e 39 2e 6.1; tr; rv:1.9.

00a0 32 2e 32 34 29 20 47 65 63 6b 6f 2f 32 30 31 32 2.24) Ge cko/2011

00b0 31 31 30 33 20 46 69 72 65 66 6f 78 2f 32 2e 36 1103 Fir efox/3.6

00c0 2e 32 34 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 .24..Acc ept: tex

00d0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,a pplicati

00e0 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 61 70 70 on/xhtml +xml app

00f0 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication /xml;q=0

0100 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 .9,*/*;q =0.8..Ac

0110 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 74 cept-Lan guage: t

HTTP Accept Encoding (http.accept-encodi... Packets: 1789 Displayed: 213 Marked: 0 Dropped: 0

Profile: Default

- If the question says "**print**", use the print option "**print the output to file**". Then, open this file in notepad, take the screenshot of it as below figure and also put this screenshot to your assignment report.

