CSCE 47503 Computer Networks – Wireshark Introduction

Name: Blake Williams
ID: 010974718

20 points
4 questions (some of them are required screenshots)

Instructions

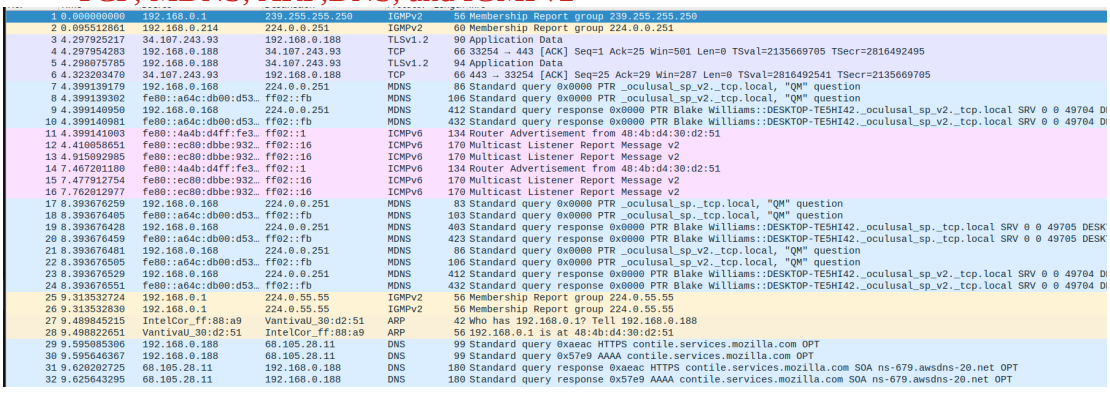
- Type your work, print it to a single PDF, and upload it to Blackboard before the due date and time. It is strongly suggested that you use the given document.
- Show all of your work. Correct answers alone may not carry full credit without proper justification and details of steps.
- -2 points if you do not insert your name and ID at the top of the document.
- -5 points if it is not typed or legible. For this homework, you may scan it with something like the CamScanner app, but just make sure it is a legible PDF.
- -5 points if it is not a PDF file.
- -5 points if it is not a single PDF file. Submit one PDF file. Do not submit zip files containing one or more files.
- -5 points if you present the worked problems out of order. In other words, please show the problems in the order assigned, 1, 2, 3, …

What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running and have explored some of its capabilities. Answer the following questions based on your Wireshark experimentation:

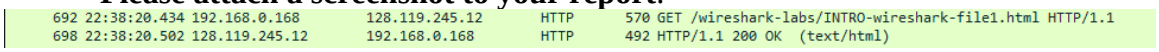
1. (5 pts.) List five protocols appearing in the protocol column in the unfiltered packet-listing window in step 7 above. **Please attach a screenshot to your report**.

TCP, MDNS, ARP,DNS, and IGMPv2



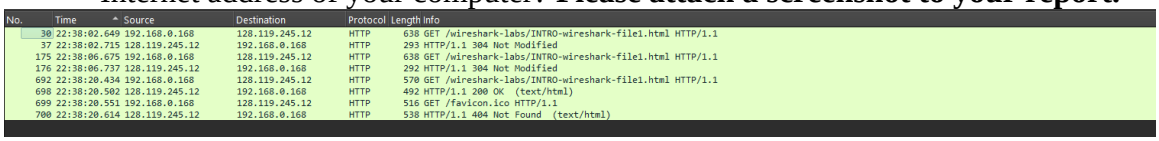
1	0.000000000	192.168.0.1	239.255.255.250	IGMPv2	56	Membership Report group 239.255.255.250
2	0.095512861	192.168.0.214	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
3	4.297925217	34.107.243.93	192.168.0.188	TLSv1.2	90	Application Data
4	4.297954283	192.168.0.188	34.107.243.93	TCP	66	33254 → 443 [ACK] Seq=1 Ack=25 Win=501 Len=0 TSval=2135669705 TSecr=2816492495
5	4.298075785	192.168.0.188	34.107.243.93	TLSv1.2	94	Application Data
6	4.323203470	34.107.243.93	192.168.0.188	TCP	66	443 → 33254 [ACK] Seq=25 Ack=29 Win=287 Len=0 TSval=2816492541 TSecr=2135669705
7	4.399139179	192.168.0.168	224.0.0.251	MDNS	86	Standard query 0x0000 PTR _oculusal_sp_v2._tcp.local, "QM" question
8	4.399139302	fe80::a64c:db00:d53…	ff02::fb	MDNS	106	Standard query 0x0000 PTR _oculusal_sp_v2._tcp.local, "QM" question
9	4.399140950	192.168.0.168	224.0.0.251	MDNS	412	Standard query response 0x0000 PTR Blake Williams::DESKTOP-TE5HI42._oculusal_sp_v2._tcp.local SRV 0 0 49704 D
10	4.399140981	fe80::a64c:db00:d53…	ff02::fb	MDNS	432	Standard query response 0x0000 PTR Blake Williams::DESKTOP-TE5HI42._oculusal_sp_v2._tcp.local SRV 0 0 49704 D
11	4.399141003	fe80::4a4b:d4ff:fe3…	ff02::1	ICMPv6	134	Router Advertisement from 48:4b:d4:30:d2:51
12	4.410058651	fe80::ec80:dbbe:932…	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
13	4.915092985	fe80::ec80:dbbe:932…	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
14	7.467201180	fe80::4a4b:d4ff:fe3…	ff02::1	ICMPv6	134	Router Advertisement from 48:4b:d4:30:d2:51
15	7.477912754	fe80::ec80:dbbe:932…	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
16	7.762012977	fe80::ec80:dbbe:932…	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
17	8.393676259	192.168.0.168	224.0.0.251	MDNS	83	Standard query 0x0000 PTR _oculusal_sp._tcp.local, "QM" question
18	8.393676405	fe80::a64c:db00:d53…	ff02::fb	MDNS	103	Standard query 0x0000 PTR _oculusal_sp._tcp.local, "QM" question
19	8.393676428	192.168.0.168	224.0.0.251	MDNS	403	Standard query response 0x0000 PTR Blake Williams::DESKTOP-TE5HI42._oculusal_sp._tcp.local SRV 0 0 49705 DESK
20	8.393676459	fe80::a64c:db00:d53…	ff02::fb	MDNS	423	Standard query response 0x0000 PTR Blake Williams::DESKTOP-TE5HI42._oculusal_sp._tcp.local SRV 0 0 49705 DESK
21	8.393676481	192.168.0.168	224.0.0.251	MDNS	86	Standard query 0x0000 PTR _oculusal_sp_v2._tcp.local, "QM" question
22	8.393676505	fe80::a64c:db00:d53…	ff02::fb	MDNS	106	Standard query 0x0000 PTR _oculusal_sp_v2._tcp.local, "QM" question
23	8.393676529	192.168.0.168	224.0.0.251	MDNS	412	Standard query response 0x0000 PTR Blake Williams::DESKTOP-TE5HI42._oculusal_sp_v2._tcp.local SRV 0 0 49704 D
24	8.393676551	fe80::a64c:db00:d53…	ff02::fb	MDNS	432	Standard query response 0x0000 PTR Blake Williams::DESKTOP-TE5HI42._oculusal_sp_v2._tcp.local SRV 0 0 49704 D
25	9.313532724	192.168.0.1	224.0.55.55	IGMPv2	56	Membership Report group 224.0.55.55
26	9.313532830	192.168.0.1	224.0.55.55	IGMPv2	56	Membership Report group 224.0.55.55
27	9.489845215	IntelCor_ff:88:a9	VantivaU_30:d2:51	ARP	42	Who has 192.168.0.1? Tell 192.168.0.188
28	9.498822651	VantivaU_30:d2:51	IntelCor_ff:88:a9	ARP	56	192.168.0.1 is at 48:4b:d4:30:d2:51
29	9.595085306	192.168.0.188	68.105.28.11	DNS	99	Standard query 0xaeac HTTPS contile.services.mozilla.com OPT
30	9.595646367	192.168.0.188	68.105.28.11	DNS	99	Standard query 0x57e9 AAAA contile.services.mozilla.com OPT
31	9.620202725	68.105.28.11	192.168.0.188	DNS	180	Standard query response 0xaeac HTTPS contile.services.mozilla.com SOA ns-679.awsdns-20.net OPT
32	9.625643295	68.105.28.11	192.168.0.188	DNS	180	Standard query response 0x57e9 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net OPT

2. (5 pts.) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the Time column value in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull-down menu, select Time *Display Format*, then choose *Time-of-day*.) **Please attach a screenshot to your report**.



According to the image it took 0.068 seconds for the HTTP OK was received.

3. (5 pts.) What is the Internet address of the ***gaia.cs.umass.edu***? What is the Internet address of your computer? **Please attach a screenshot to your report.**



According to the screenshot the address of gaia.cs.unmass.edu was 128.119.245.12 while my computers address is 192.168.0.168

4. (5 pts.) Print the two HTTP messages (GET and OK) in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, select the "*Selected Packet Only*" and "*Print as displayed*" radial buttons, and then click OK.

```
No.     Time         Source               Destination          Protocol Length Info
    692 22:38:20.434 192.168.0.168        128.119.245.12       HTTP     570    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 692: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface \Device\NPF_{182947D6-8450-4126-
A771-0F72F8156D47}, id 0
Ethernet II, Src: MicroStarINT_58:99:10 (00:d8:61:58:99:10), Dst: VantivaUSA_30:d2:51 (48:4b:d4:30:d2:51)
Internet Protocol Version 4, Src: 192.168.0.168, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57543, Dst Port: 80, Seq: 2, Ack: 1, Len: 516
Hypertext Transfer Protocol
No.     Time         Source               Destination          Protocol Length Info
    698 22:38:20.502 128.119.245.12       192.168.0.168        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 698: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{182947D6-8450-4126-
A771-0F72F8156D47}, id 0
Ethernet II, Src: VantivaUSA_30:d2:51 (48:4b:d4:30:d2:51), Dst: MicroStarINT_58:99:10 (00:d8:61:58:99:10)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.168
Transmission Control Protocol, Src Port: 80, Dst Port: 57543, Seq: 1, Ack: 518, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```