Michael Simmons

IT4323 – W01

Project 35 - Individual

Project Wireshark

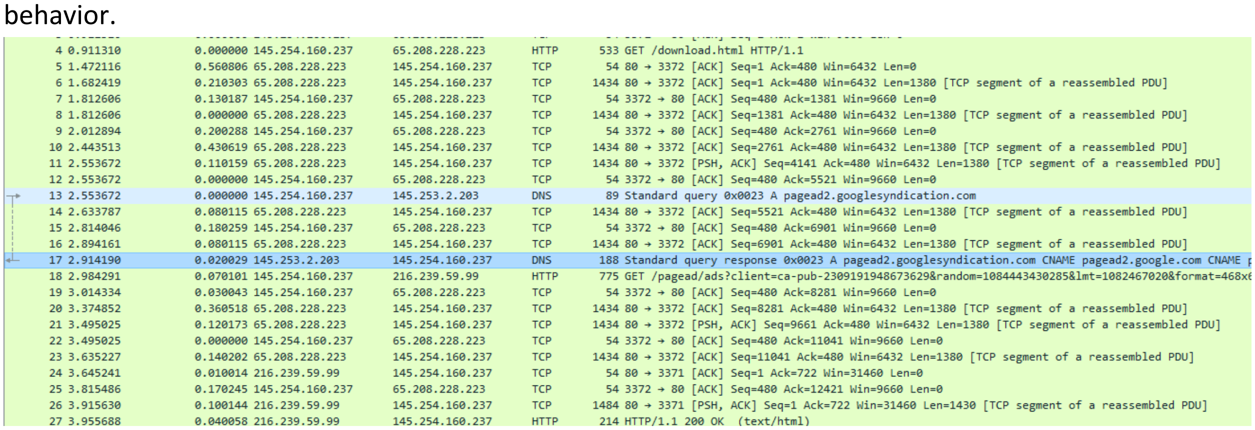
Description: This project requires that you work in a group (or as an individual) to do some research regarding the protocols used in the Wireshark captures provided to try and determine what is happening in the capture. Keep in mind that documentation is a big part of what you will do in the real world in your career. You will have to explain to others your findings and propose solutions. "Hands on" means using your brain, too!

Use the capture files in the Project Work Module in D2L (you will have to unzip the zip files to extract the individual capture files) to answer the following questions:

Part I – HTTP

1. Review the first capture file **(Project Part I-a)** and determine what is happening with the HTTP traffic.
    a. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)
    An HTTP GET request has been made (packet 4) from source 145.254.160.237 to destination 65.208.228.223 on May 13, 2004 at 6:17am. The request took 9ms and is accessing http://www.ethereal.com/development.html\r\n from a Google search. After acknowledgement on port 80, the source IP contacts the DNS once for the Google ad link for Ethereal. The query acknowledgement is (145.253.2.203, packet 13) and the response is (145.254.160.237, packet 17). The source IP then sends a HTTP GET request (216.239.59.99, packet 18), the link contains HTML code driving traffic to the Ethereal page to download the program. HTTP/1.1 200 OK from 216.239.59.99 back to the source 145.254.160.237 (packet 27)

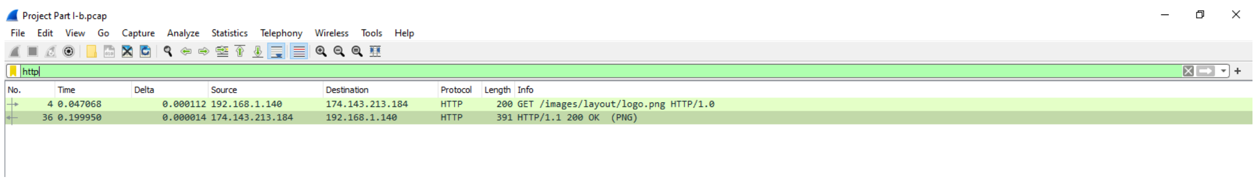
    b. Take a screenshot of the actual packets within the capture file that you observed this behavior.



4	0.911310	0.000000	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472116	0.560806	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.682419	0.210303	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
7	1.812606	0.130187	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	1.812606	0.000000	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
9	2.012894	0.200288	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	2.443513	0.430619	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
11	2.553672	0.110159	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
12	2.553672	0.000000	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13	2.553672	0.000000	145.254.160.237	145.253.2.203	DNS	89	Standard query 0x0023 A pagead2.googlesyndication.com
14	2.633787	0.080115	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
15	2.814046	0.180259	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
16	2.894161	0.080115	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
17	2.914190	0.020029	145.253.2.203	145.254.160.237	DNS	188	Standard query response 0x0023 A pagead2.googlesyndication.com CNAME pagead2.google.com CNAME p
18	2.984291	0.070101	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x6
19	3.014334	0.030043	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
20	3.374852	0.360518	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
21	3.495025	0.120173	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
22	3.495025	0.000000	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0
23	3.635227	0.140202	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=11041 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
24	3.645241	0.010014	216.239.59.99	145.254.160.237	TCP	54	80 → 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
25	3.815486	0.170245	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 Len=0
26	3.915630	0.100144	216.239.59.99	145.254.160.237	TCP	1484	80 → 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=1430 [TCP segment of a reassembled PDU]
27	3.955688	0.040058	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html)

2. Review the second capture file **(Project Part I-b**) and determine what is happening with the HTTP traffic in this capture.
    c. How is the traffic different from the first capture? Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)
    On March 1, 2011 at 3:45pm an HTTP GET request (packet 4) was sent from source 192.168.1.140 to destination 174.143.213.184, http://packetlife.net/images/layout/logo.png. An PNG image was downloaded, File Data 21684 bytes. HTTP/1.1 200 OK from 174.143.213.184 back to the source 192.168.1.140 (packet 36)

    a. Take a screenshot of the actual packets within the capture file that you observed.

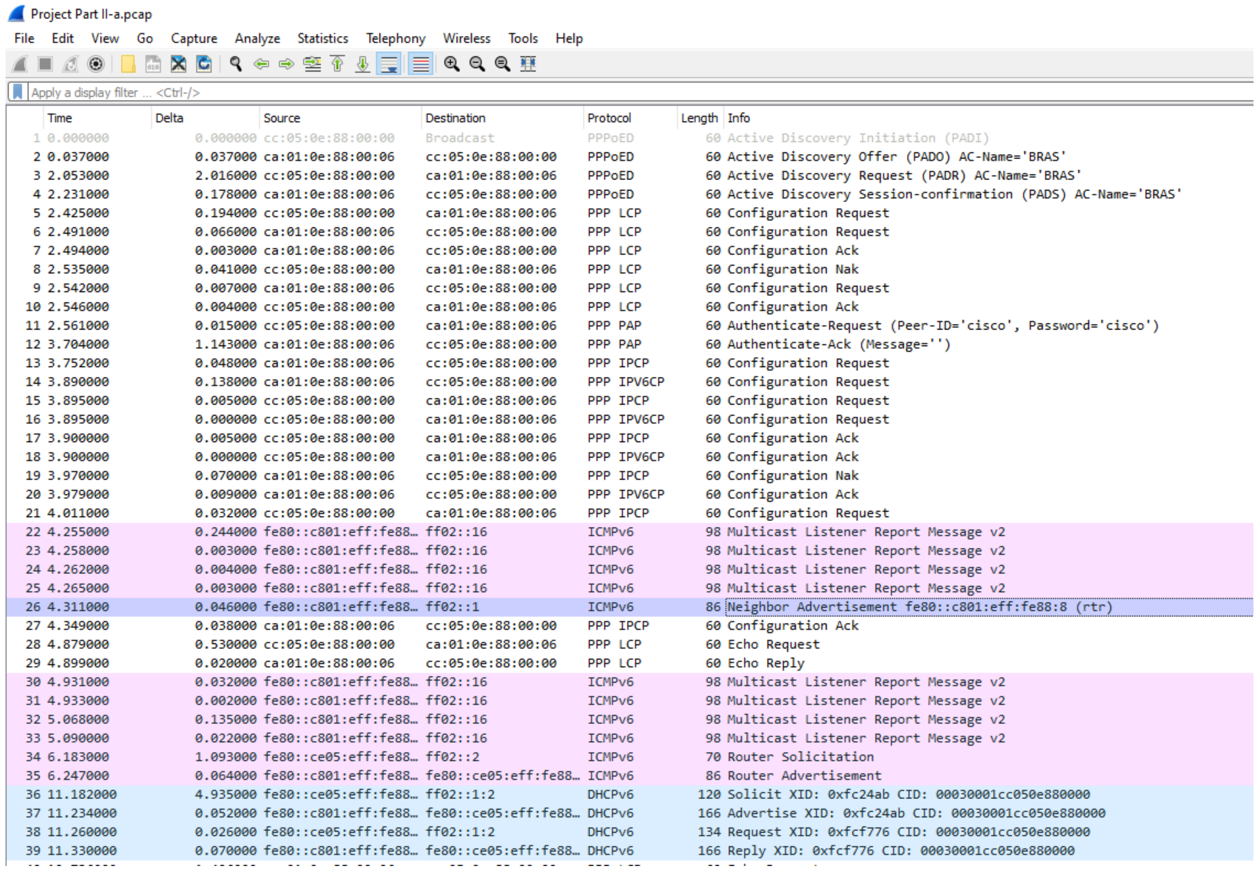


<u>Part II – PPP</u>

3. Review the third capture file **(Project Part II-a)** and determine what is happening with the PPP traffic in this capture.
    a. Research **one** of the protocols relating to PPP and describe it here.
    The PPPoED is attempting to establish a point-to-point connection over ethernet to setup a router. This connection must be confirmed before PPP LCP, PAP, IPCP, or any others can configure, test, or send data.

    b. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)
    The traffic appears to be making a configuration request over the ethernet to setup a new router on Sep 13, 2010 at 9:43am, PPPoED initializes the broadcast router on the ethernet connection (packet 1). The new source router ca:01:0e:88:00:06 makes itself discoverable (packet 2) to the destination broadcast router ca:05:0e:88:00:00. Broadcast ca:05:0e:88:00:00 sends the request to join the network (packet 3). The new router accepts and confirms the session join (packet 4). The broadcast establishes link control with the new router (PPP LCP, packet 5), the two routers begin configuration requests and acknowledgement (though packet 10). Password Authentication Protocol begins asking for an ID and Password (PPP PAP, packet 11), and is acknowledged (packet 12). The Internet Protocol Control Protocol then requests the internet connection but Configure-Nak rejects IPv4, only connecting IPv6 (packet 13-21). ICMPv6 message report configuration (packet 22-35). DHCPv6 configuration (packet 36 – 39).

c. Take a screenshot of the actual packets within the capture file that you observed this behavior.



No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	cc:05:0e:88:00:00	Broadcast	PPPoED	60	Active Discovery Initiation (PADI)
2	0.037000	0.037000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPPoED	60	Active Discovery Offer (PADO) AC-Name='BRAS'
3	2.053000	2.016000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPPoED	60	Active Discovery Request (PADR) AC-Name='BRAS'
4	2.231000	0.178000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPPoED	60	Active Discovery Session-confirmation (PADS) AC-Name='BRAS'
5	2.425000	0.194000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP LCP	60	Configuration Request
6	2.491000	0.066000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP LCP	60	Configuration Request
7	2.494000	0.003000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP LCP	60	Configuration Ack
8	2.535000	0.041000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP LCP	60	Configuration Nak
9	2.542000	0.007000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP LCP	60	Configuration Request
10	2.546000	0.004000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP LCP	60	Configuration Ack
11	2.561000	0.015000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP PAP	60	Authenticate-Request (Peer-ID='cisco', Password='cisco')
12	3.704000	1.143000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP PAP	60	Authenticate-Ack (Message='')
13	3.752000	0.048000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP IPCP	60	Configuration Request
14	3.890000	0.138000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP IPV6CP	60	Configuration Request
15	3.895000	0.005000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP IPCP	60	Configuration Request
16	3.895000	0.000000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP IPV6CP	60	Configuration Request
17	3.900000	0.005000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP IPCP	60	Configuration Ack
18	3.900000	0.000000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP IPV6CP	60	Configuration Ack
19	3.970000	0.070000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP IPCP	60	Configuration Nak
20	3.979000	0.009000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP IPV6CP	60	Configuration Ack
21	4.011000	0.032000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP IPCP	60	Configuration Request
22	4.255000	0.244000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
23	4.258000	0.003000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
24	4.262000	0.004000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
25	4.265000	0.003000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
26	4.311000	0.046000	fe80::c801:eff:fe88…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::c801:eff:fe88:8 (rtr)
27	4.349000	0.038000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP IPCP	60	Configuration Ack
28	4.879000	0.530000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP LCP	60	Echo Request
29	4.899000	0.020000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP LCP	60	Echo Reply
30	4.931000	0.032000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
31	4.933000	0.002000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
32	5.068000	0.135000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
33	5.090000	0.022000	fe80::c801:eff:fe88…	ff02::16	ICMPv6	98	Multicast Listener Report Message v2
34	6.183000	1.093000	fe80::ce05:eff:fe88…	ff02::2	ICMPv6	70	Router Solicitation
35	6.247000	0.064000	fe80::c801:eff:fe88…	fe80::ce05:eff:fe88…	ICMPv6	86	Router Advertisement
36	11.182000	4.935000	fe80::ce05:eff:fe88…	ff02::1:2	DHCPv6	120	Solicit XID: 0xfc24ab CID: 00030001cc050e880000
37	11.234000	0.052000	fe80::c801:eff:fe88…	fe80::ce05:eff:fe88…	DHCPv6	166	Advertise XID: 0xfc24ab CID: 00030001cc050e880000
38	11.260000	0.026000	fe80::ce05:eff:fe88…	ff02::1:2	DHCPv6	134	Request XID: 0xfcf776 CID: 00030001cc050e880000
39	11.330000	0.070000	fe80::c801:eff:fe88…	fe80::ce05:eff:fe88…	DHCPv6	166	Reply XID: 0xfcf776 CID: 00030001cc050e880000

4. Review the third capture file (**Project Part II-b)** and determine what is happening with the PPP traffic that you are investigating in this capture. What else is involved?

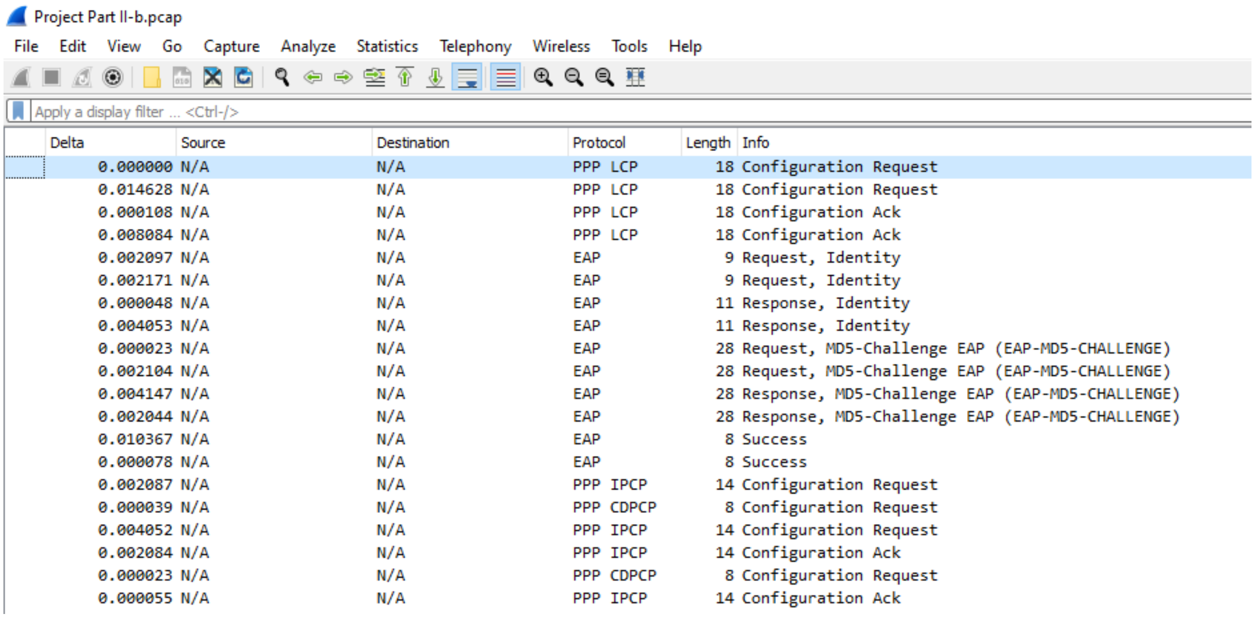
   a. Research **one** of the protocols relating to PPP and describe it here.

   EAP establishes authentication between the source host and destination host. It requests the identity of the source host then confirms with the destination host if it is authorized to connect. (packet 5-14).

   b. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)

   On Jun 7, 2010 at 12:00pm, PPP LCP configures the link to the authenticator (packet 1-4). EAP then requests the identity of the source host, the host will response detailing its identity (packet 5-8). An EAP Challenge request (packet 9-10) is sent to the destination server for authorization response (packet 11-12). If approved the authenticator grants access and configuration is allowed to proceed (packet 13-14). Note: the authenticator sit between the requestor and the server, so source and destination addresses are not displayed.

c. Take a screenshot of the actual packets within the capture file that you observed this behavior.



Delta	Source	Destination	Protocol	Length	Info
0.000000	N/A	N/A	PPP LCP	18	Configuration Request
0.014628	N/A	N/A	PPP LCP	18	Configuration Request
0.000108	N/A	N/A	PPP LCP	18	Configuration Ack
0.008084	N/A	N/A	PPP LCP	18	Configuration Ack
0.002097	N/A	N/A	EAP	9	Request, Identity
0.002171	N/A	N/A	EAP	9	Request, Identity
0.000048	N/A	N/A	EAP	11	Response, Identity
0.004053	N/A	N/A	EAP	11	Response, Identity
0.000023	N/A	N/A	EAP	28	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
0.002104	N/A	N/A	EAP	28	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
0.004147	N/A	N/A	EAP	28	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
0.002044	N/A	N/A	EAP	28	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
0.010367	N/A	N/A	EAP	8	Success
0.000078	N/A	N/A	EAP	8	Success
0.002087	N/A	N/A	PPP IPCP	14	Configuration Request
0.000039	N/A	N/A	PPP CDPCP	8	Configuration Request
0.004052	N/A	N/A	PPP IPCP	14	Configuration Request
0.002084	N/A	N/A	PPP IPCP	14	Configuration Ack
0.000023	N/A	N/A	PPP CDPCP	8	Configuration Request
0.000055	N/A	N/A	PPP IPCP	14	Configuration Ack

5. Review the third capture file **(Project Part II-c**) and determine what is happening with the PPP traffic in this capture. What else is involved?

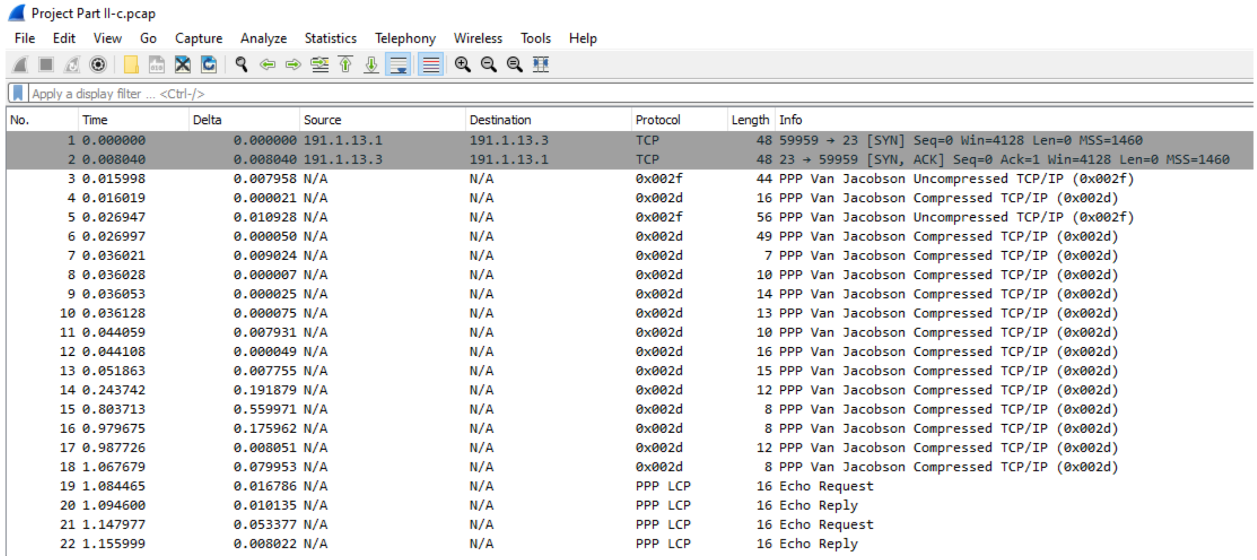
   a. Research **one** of the protocols relating to PPP and describe it here.

   0x002f is the Van Jacobson Uncompressed TCP/IP, it belongs to the PPP Protocol ID. It identifies the type of information encapsulated in packets of information that contain configuration details or data.

   b. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)

   On Aug 4, 2008 at 11:00pm, source 191.1.13.1 requests to sync with destination 191.1.13.3 over TCP (packet 1). The request is acknowledged, and a response is sent by 191.1.13.3 (packet 2). The data to be sent is then compressed using the 0x002d PPP Van Jacobson protocol (packet 6-18). PPP LCP then send an Echo Request/Reply to ensure the connection is still good (packet 19-22).

   c. Take a screenshot of the actual packets within the capture file that you observed this behavior.



Project Part II-c.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

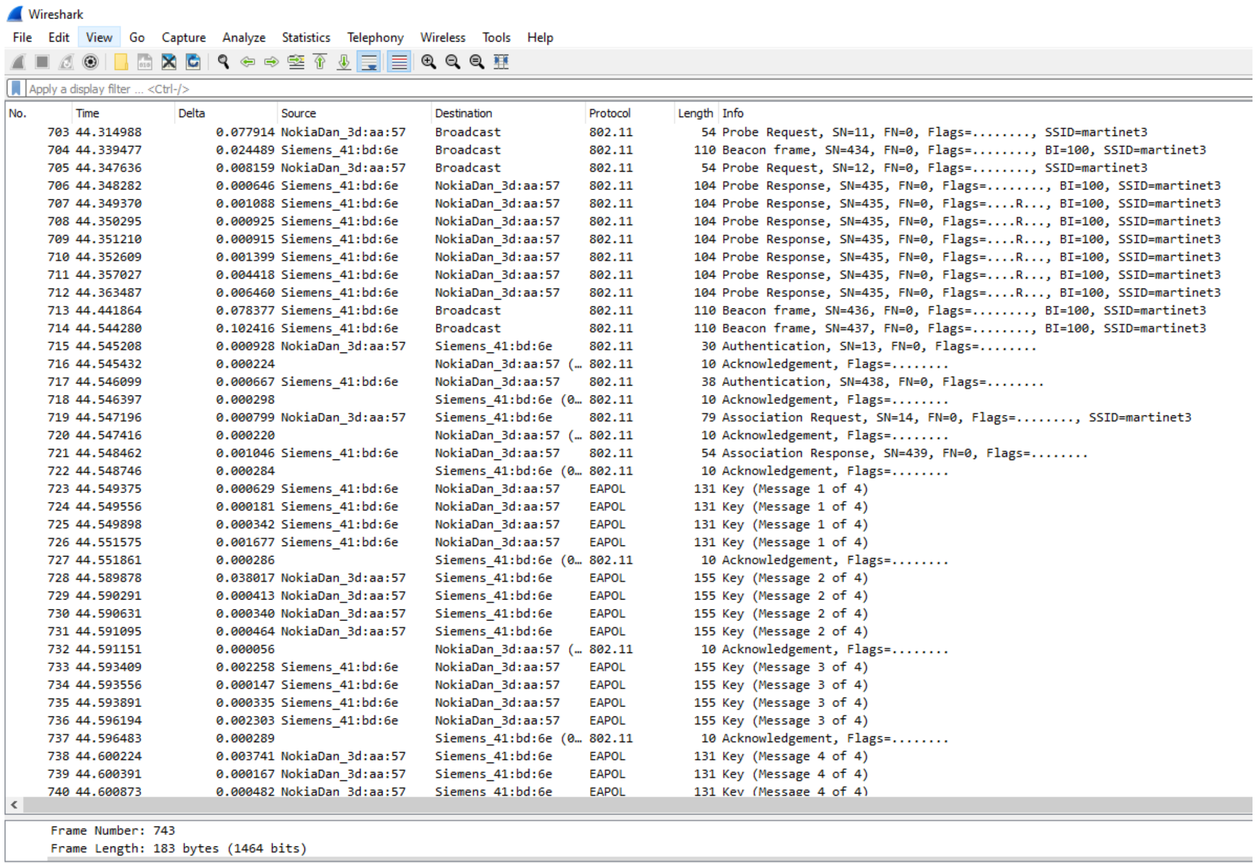
No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	191.1.13.1	191.1.13.3	TCP	48	59959 → 23 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
2	0.008040	0.008040	191.1.13.3	191.1.13.1	TCP	48	23 → 59959 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
3	0.015998	0.007958	N/A	N/A	0x002f	44	PPP Van Jacobson Uncompressed TCP/IP (0x002f)
4	0.016019	0.000021	N/A	N/A	0x002d	16	PPP Van Jacobson Compressed TCP/IP (0x002d)
5	0.026947	0.010928	N/A	N/A	0x002f	56	PPP Van Jacobson Uncompressed TCP/IP (0x002f)
6	0.026997	0.000050	N/A	N/A	0x002d	49	PPP Van Jacobson Compressed TCP/IP (0x002d)
7	0.036021	0.009024	N/A	N/A	0x002d	7	PPP Van Jacobson Compressed TCP/IP (0x002d)
8	0.036028	0.000007	N/A	N/A	0x002d	10	PPP Van Jacobson Compressed TCP/IP (0x002d)
9	0.036053	0.000025	N/A	N/A	0x002d	14	PPP Van Jacobson Compressed TCP/IP (0x002d)
10	0.036128	0.000075	N/A	N/A	0x002d	13	PPP Van Jacobson Compressed TCP/IP (0x002d)
11	0.044059	0.007931	N/A	N/A	0x002d	10	PPP Van Jacobson Compressed TCP/IP (0x002d)
12	0.044108	0.000049	N/A	N/A	0x002d	16	PPP Van Jacobson Compressed TCP/IP (0x002d)
13	0.051863	0.007755	N/A	N/A	0x002d	15	PPP Van Jacobson Compressed TCP/IP (0x002d)
14	0.243742	0.191879	N/A	N/A	0x002d	12	PPP Van Jacobson Compressed TCP/IP (0x002d)
15	0.803713	0.559971	N/A	N/A	0x002d	8	PPP Van Jacobson Compressed TCP/IP (0x002d)
16	0.979675	0.175962	N/A	N/A	0x002d	8	PPP Van Jacobson Compressed TCP/IP (0x002d)
17	0.987726	0.008051	N/A	N/A	0x002d	12	PPP Van Jacobson Compressed TCP/IP (0x002d)
18	1.067679	0.079953	N/A	N/A	0x002d	8	PPP Van Jacobson Compressed TCP/IP (0x002d)
19	1.084465	0.016786	N/A	N/A	PPP LCP	16	Echo Request
20	1.094600	0.010135	N/A	N/A	PPP LCP	16	Echo Reply
21	1.147977	0.053377	N/A	N/A	PPP LCP	16	Echo Request
22	1.155999	0.008022	N/A	N/A	PPP LCP	16	Echo Reply

Part III – 802.11

6. Review the first capture file **(Nokia)** and determine what is happening with the 802.11 traffic. Hint: use the Analyze/Conversation Filter

   d. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)
   On Dec. 31, 1999 at 7:04pm Beacon frames are captured establishing connectivity from a wireless access point, Siemens_41:bd:6e, to anything in range (packet 1-151). Some data is made visible on the network (packet 152-431). NokiaDan_3d:aa:57 sends a probe request to the broadcast network (packet 689). Siemens_41:bd:6e responds to NokiaDan_3d:aa:57, acknowledging communication (packet 690-701). NokiaDan_3d:aa:57 then send authentication/acknowledgment to Siemens_41:bd:6e (packet 715-716), Siemens_41:bd:6e returns the same (packet 717-718). The association request/response is acknowledged (719-722) and Siemens_41:bd:6e sends the WPA key packets to NokiaDan_3d:aa:57 for access using EAPOL protocol (723-742). Data begins to flow (packet 743-776).

   e. Take a screenshot of the actual packets within the capture file that you observed this behavior.



No.	Time	Delta	Source	Destination	Protocol	Length	Info
703	44.314988	0.077914	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=11, FN=0, Flags=........, SSID=martinet3
704	44.339477	0.024489	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=434, FN=0, Flags=........, BI=100, SSID=martinet3
705	44.347636	0.008159	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=12, FN=0, Flags=........, SSID=martinet3
706	44.348282	0.000646	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=........, BI=100, SSID=martinet3
707	44.349370	0.001088	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....R..., BI=100, SSID=martinet3
708	44.350295	0.000925	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....R..., BI=100, SSID=martinet3
709	44.351210	0.000915	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....R..., BI=100, SSID=martinet3
710	44.352609	0.001399	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....R..., BI=100, SSID=martinet3
711	44.357027	0.004418	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....R..., BI=100, SSID=martinet3
712	44.363487	0.006460	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....R..., BI=100, SSID=martinet3
713	44.441864	0.078377	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=436, FN=0, Flags=........, BI=100, SSID=martinet3
714	44.544280	0.102416	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=437, FN=0, Flags=........, BI=100, SSID=martinet3
715	44.545208	0.000928	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	30	Authentication, SN=13, FN=0, Flags=........
716	44.545432	0.000224		NokiaDan_3d:aa:57 (…	802.11	10	Acknowledgement, Flags=........
717	44.546099	0.000667	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	38	Authentication, SN=438, FN=0, Flags=........
718	44.546397	0.000298		Siemens_41:bd:6e (0…	802.11	10	Acknowledgement, Flags=........
719	44.547196	0.000799	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	79	Association Request, SN=14, FN=0, Flags=........, SSID=martinet3
720	44.547416	0.000220		NokiaDan_3d:aa:57 (…	802.11	10	Acknowledgement, Flags=........
721	44.548462	0.001046	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	54	Association Response, SN=439, FN=0, Flags=........
722	44.548746	0.000284		Siemens_41:bd:6e (0…	802.11	10	Acknowledgement, Flags=........
723	44.549375	0.000629	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
724	44.549556	0.000181	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
725	44.549898	0.000342	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
726	44.551575	0.001677	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
727	44.551861	0.000286		Siemens_41:bd:6e (0…	802.11	10	Acknowledgement, Flags=........
728	44.589878	0.038017	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
729	44.590291	0.000413	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
730	44.590631	0.000340	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
731	44.591095	0.000464	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
732	44.591151	0.000056		NokiaDan_3d:aa:57 (…	802.11	10	Acknowledgement, Flags=........
733	44.593409	0.002258	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
734	44.593556	0.000147	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
735	44.593891	0.000335	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
736	44.596194	0.002303	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
737	44.596483	0.000289		Siemens_41:bd:6e (0…	802.11	10	Acknowledgement, Flags=........
738	44.600224	0.003741	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	131	Key (Message 4 of 4)
739	44.600391	0.000167	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	131	Key (Message 4 of 4)
740	44.600873	0.000482	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	131	Key (Message 4 of 4)

Frame Number: 743
Frame Length: 183 bytes (1464 bits)

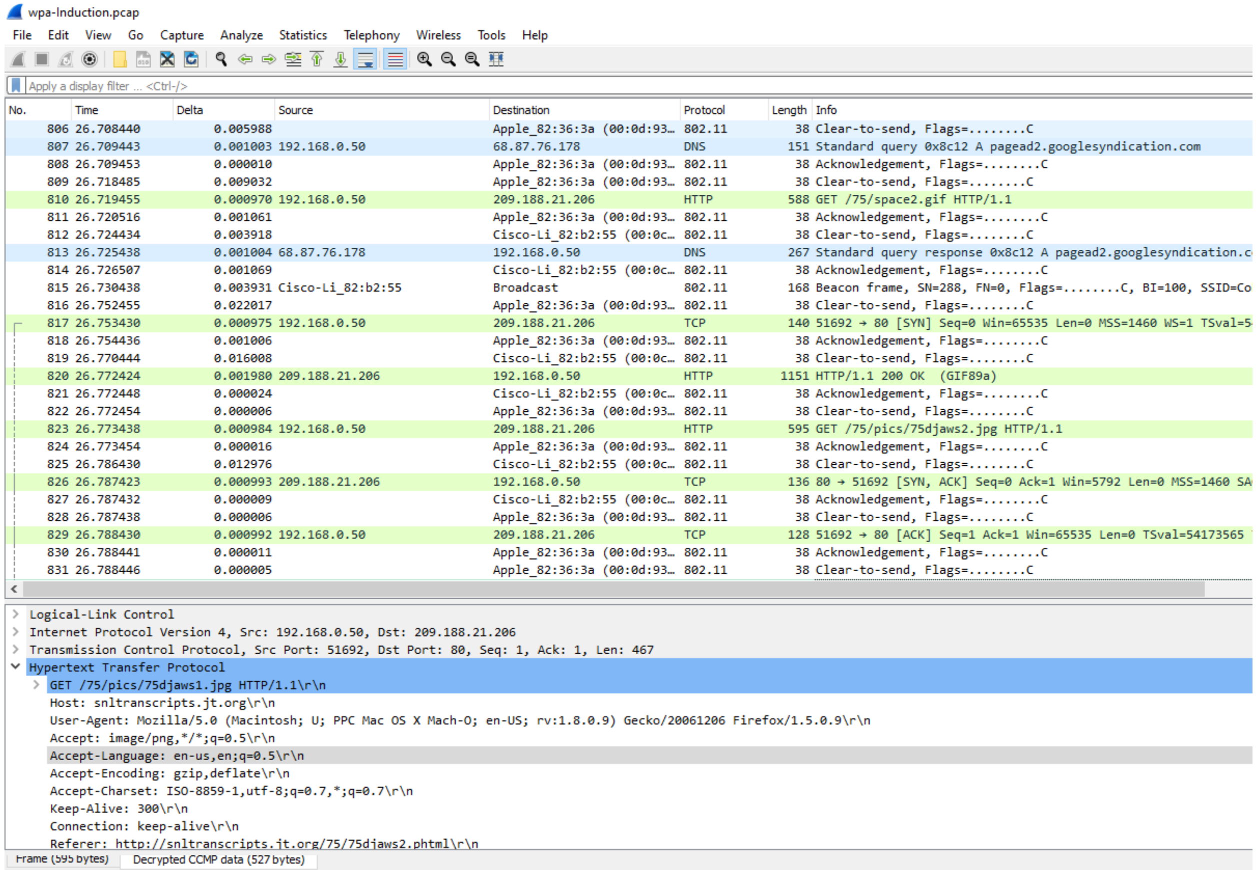
7. Review the second capture file **(wpa)** and determine what is happening with the WPA traffic in this capture. (password is “Induction”). Hint: Use Edit->preferences, Protocol IEEE 802.11, decryption with “Induction”); Look at the packets prior to and after decryption. Use this https://wiki.wireshark.org/HowToDecrypt802.11 . You are STILL required to answer the following questions in your own words and provide a screenshot!

   f. What do you different once you have decrypted the packets?
   The decrypted packets are now displayed below the encrypted packets.

   What is decrypted and what is happening? (include source, destination, time of capture)

   On Jan 4, 2007 at 1:15am, multiple HTTP GET request have been sent to download pictures. The request from Source 192.168.0.50 to destination 209.188.21.206 to download space2.gif (packet 810). The DNS has been queried (packet 813) and HTTP 200 OK (packet 820). The request from Source 192.168.0.50 to destination 209.188.21.206 to download jaws2.gif (packet 823). The request from Source 192.168.0.50 to destination 209.188.21.206 to download jaws1.gif (packet 832).

   d. Take a screenshot of the actual packets within the capture file that you observed.

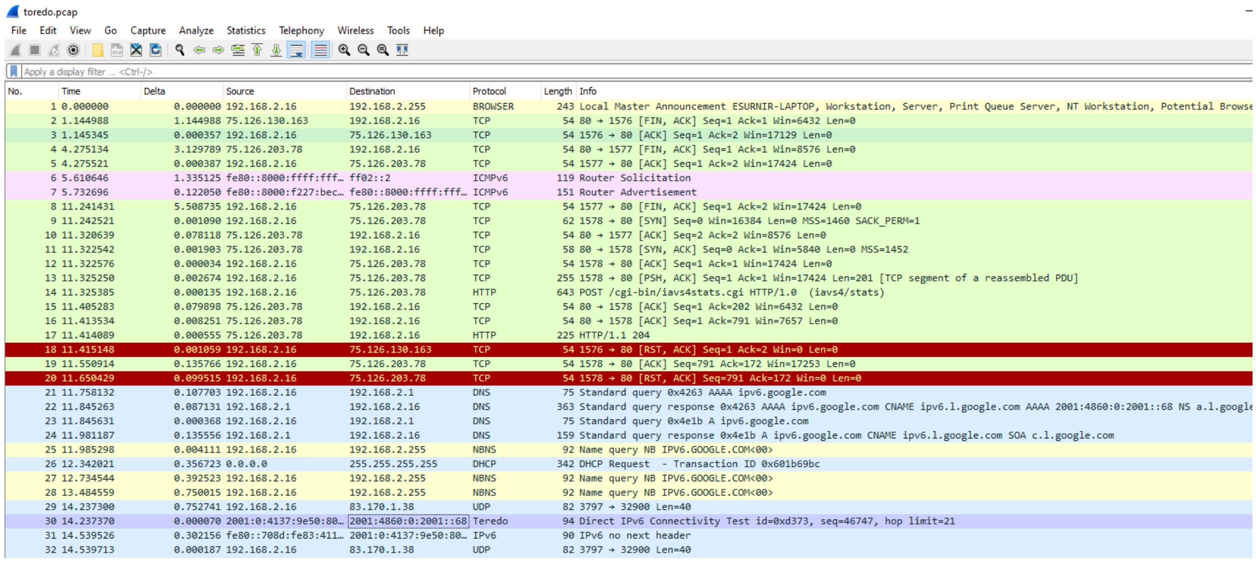


<u>Part IV – Ipv6 – Ipv4</u>

8. Review the third capture file **(teredo)** and determine what is happening with the Ipv4-IPv6 traffic in this capture.
    a. Research Teredo for encapsulation relating to Ipv6 using the content links in the course and describe it here.
    Teredo allows an IPv4 host full connection to an IPv6 host. It uses a tunneling protocol to provide IPv6 connectivity by encapsulating IPv6 data packets into IPv4 UDP packets. Used as a temporary connection until IPv6 can be fully implemented.

    e. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture) (Hint: look at all Ipv6 packets that have Toredo in their details)
    On May 16, 2008 at 11:50am, laptop source 192.168.2.16 is attempting to connect to the internet using an IPv4 host. It is rejected over TCP. The request is reset and acknowledged (packet 18); the DNS query reports the connection requested is IPv6 (21-24). Teredo spins up and runs a connectivity test over UDP (packet 30). Converts IPv4 toIPv6 temporarily (packet 31-57). The DNS IPv6 runs again (packet 58) allowing access to the HTTP page (packet 73).

f. Take a screenshot of the actual packets within the capture file that you observed this behavior.



9. Review the fourth capture file **(6to4)** and determine what is happening with the Ipv4- IPv6 traffic in this capture. What else is involved?

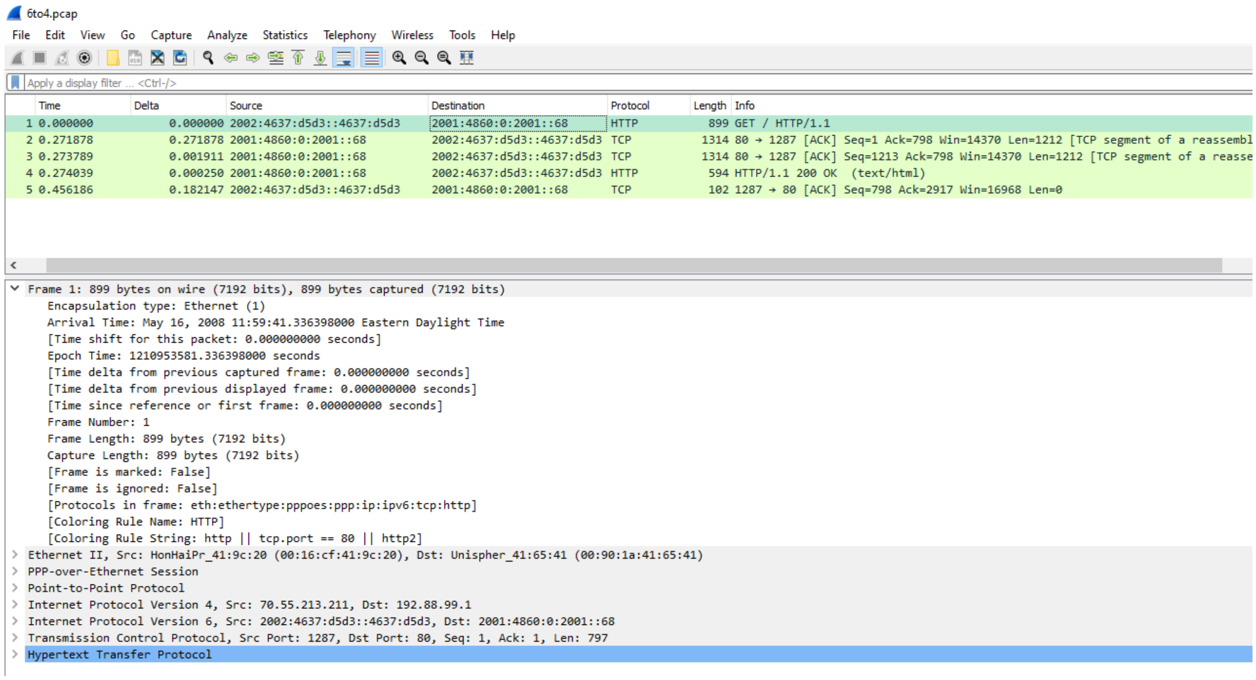
a. Research 6to4 protocol using the content links in the course relating to 6to4 and describe it here.

6to4 protocol is a way to gain IPv6 connection via an IPv4 host. It is mainly used for static addresses. Unlike Teredo, it does not use tunneling to complete this. Instead it uses its own gateway that unencapsulates data through the network interface.

g. Describe the traffic: what packets are involved and what is happening? (include source, destination, time of capture)

On May 16, 2008 at 11:59am, source 2002:4637:d5d3::4637:d5d3 initiates an HTTP GET request to 2001:4860:0:2001::68 (packet 1). The 6to4 protocol has converted the IPv4 to IPv6 connection with the first packet. The IPv6 connection is the carried over to all subsequent packet, completing the request (packet 4) without rejection over TCP.

h. Take a screenshot of the actual packets within the capture file that you observed this behavior.



10. How do the two different methods differ?
    6to4 is completed within the first packet through an independent gateway. The TCP protocol is completed without being rejected or converting to UDP.
    Teredo will convert to IPv6 after IPv4 has been rejected, it then must encapsulate the data over UDP for transport.

11. Are there any other transitioning methods for IPv6 that you came across in your research that are noteworthy?
    The AYIYA protocol can also support UDP encapsulation for transport over NAT connection.

<u>**Group Members: (List your group Members Here if you worked in a group)**</u>

Task List: (List the tasks that were performed in this project and which team members were involved in this task, plus the % of their contribution to the project)

<u>**Submission**</u>

After you have finished answering all the questions, please submit this part of the project to the drop box for this submission as a group.