

Jessica Spinney/Swanson
Dr. Calabrese
January 25-February 11, 2015
Lab #1 - Wireshark
ITEC 2081 T/TH

Abstract

In this lab, I used WireShark to capture packets. I filtered the captured packets so that only HTTP packets would appear. I isolated individual packets using various filters. I found that I needed to research how to utilize several of the search options, but was able to succeed in most attempts.

Method

Lab Information:

This lab is about the exploration of protocols using Wireshark. Here, Wireshark is used to capture packets from an active interface (one that is communicating with the Internet) whether it is wireless or wired. The Wireshark color coding is used to help differentiate between packet types.

As the user navigates various web pages on the Internet, Wireshark captures the packets that are generated in real time. AutoScroll can be used to keep up with the latest incoming packets, or to be able to hover over specific areas of interest without losing the location.

Filtering this quickly accumulating pile of data can be accomplished using the Filter Toolbar near the top of the screen. In this lab, only the HTTP traffic is examined. This can be accomplished by typing “http” into the toolbar, or by clicking the Expression... button to its immediate right and looking for the desired term and style of use. Multiple expressions can be combined using the “&&” operator. The filters can be removed by clicking the nearby Clear button.

There are many types of packets, including GET requests, Host, User-Agent, Accepts, and cookies. These have different parts and data viewable beneath the list of packets.

Lab Environment:

- IP Address (unknown)
- MAC address: 40-25-C2-53-97-48
- Hardware type: HP Pavilion dv7-6135dx Entertainment PC
- Internet Source: Johnson & Wales University’s Academic Center Computer Lab, Room 403

Tools:

- Wireshark
 - Settings - Captures, Filter Toolbar
- Snipping Tool
 - Settings - New
- Web Browsers
 - Opera
 - Firefox
 - Internet Explorer

How I Obtained Packets:

I obtained packets by surfing the Internet. I used three browsers, Opera, Mozilla Firefox, and Internet Explorer. The pages I visited included my home pages (including a Wikipedia article), several search engines (including Bing and a search for frog pictures), and several sites I visit frequently (including Etsy). I did various searches and clicked around within all of them.

Data

Capture #1

Capturing from Wireless Network Connection [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: `http.request.method == "POST" && http.host contains "bing"` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6693	80.442391010.24.70.208	204.79.197.200		HTTP	1098	POST /rewardsapp/reportActivity HTTP/1.1 (application/x-www-form-urlencoded)

[Expert Info (Chat/Sequence): POST /rewardsapp/reportActivity HTTP/1.1\r\n]

Request Method: POST
Request URI: /rewardsapp/reportActivity
Request version: HTTP/1.1
Host: www.bing.com\r\nUser-Agent: Mozilla/5.0 (windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded; charset=UTF-8\r\nReferer: http://www.bing.com/\r\nContent-Length: 32\r\n

[Truncated] cookie: MUID=19902B66025C6A681E522DD2065C6C9E; ANON=4=BB7A128554B3B7005E

0190 2d 38 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 -8...Referer: htt
01a0 70 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d p://www.bing.com
01b0 2f 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 /.Content-Lengt
01c0 68 3a 20 33 32 0d 0a 43 6f 6f 6b 69 65 3a 20 4d h: 32..Cookie: M
01d0 55 49 44 3d 31 39 39 30 32 42 36 36 30 32 35 43 UID=1990 2B66025C
01e0 36 41 36 38 31 45 35 32 32 44 44 32 30 36 35 43 6A681E52 2002065C
01f0 36 43 39 46 3b 20 41 4e 4f 4e 3d 41 3d 42 42 37 6C9F; AN ON=A=BB7
0200 41 31 32 38 35 35 34 42 33 42 37 30 30 35 45 43 A128554B 3B7005EC
0210 46 42 37 42 44 46 46 46 46 46 46 46 46 26 45 3d FB7B0FFF FFFFFE=1
0220 66 66 38 26 3d 31 3b 20 4e 41 50 3d 56 3d 31 FF8d=1; NAP=v=1
0230 2e 39 26 45 3d 66 39 65 26 43 3d 58 44 64 7a 43 .98e=F9e 8C-xdd2C
0240 78 65 6f 4d 65 51 55 6b 58 6d 6c 47 42 4e 67 6c xeoMeQuk xmlGBNq1
0250 49 6e 76 5a 72 79 2d 59 62 5f 48 61 65 45 6a 44 Inv2ry-Y b.HaeEJD
0260 45 65 70 52 53 69 62 51 6a 66 6c 77 33 7a 74 76 Eepr51bq jFlw3ztv
0270 41 26 57 3d 31 3b 20 53 52 43 48 44 3d 41 46 3d A8w=1; S RCHIDAF=1
0280 46 4f 46 4f 52 4d 3b 20 53 52 43 48 55 49 44 3d NOFORM; SRCHUID=1
0290 56 3d 32 26 47 55 49 44 3d 41 33 46 37 33 32 33 V=2&GUID =A3F7323
02a0 37 33 38 42 36 34 36 32 35 39 35 42 35 43 36 37 739B6462 595B5C67
02b0 38 39 37 41 35 41 39 37 3b 20 53 52 43 48 55 897A55A9 7; SRCHU
02c0 53 52 3d 41 55 54 4f 52 45 44 49 52 3d 30 26 47 SR=AUTOR EDIR=0&G
02d0 45 4f 56 41 52 3d 26 44 4f 42 3d 32 30 31 35 30 EOVAR=60 OB=20150
02e0 31 31 34 3b 20 4d 55 49 44 42 3d 31 39 39 30 32 114; MUI DB=19902
02f0 42 36 30 32 35 43 36 41 36 38 31 45 35 32 32 B66025C6 A681E522
0300 45 44 23 20 26 32 43 32 43 30 48 2b 2a 63 43 63 6025C6 A681E522

HTTP Referer (http.referer), 31 bytes Packets: 26492 - Displayed: 1 (0.0%) Profile: Default

[Expert Info (Chat/Sequence): POST /rewardsapp/reportActivity HTTP/1.1\r\n]

Request Method: POST
Request URI: /rewardsapp/reportActivity
Request version: HTTP/1.1
Host: www.bing.com\r\nUser-Agent: Mozilla/5.0 (windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded; charset=UTF-8\r\nReferer: http://www.bing.com/\r\nContent-Length: 32\r\n

[Truncated] cookie: MUID=19902B66025C6A681E522DD2065C6C9E; ANON=4=BB7A128554B3B7005E

0190 2d 38 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 -8...Referer: htt
01a0 70 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d p://www.bing.com
01b0 2f 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 /.Content-Lengt
01c0 68 3a 20 33 32 0d 0a 43 6f 6f 6b 69 65 3a 20 4d h: 32..Cookie: M

Capture #2

Capturing from Wireless Network Connection [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: http.cookie contains "TS0194" && http.request.uri contains "frog-blue" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
19071	97.8140340	10.24.70.208	64.29.151.221	HTTP	510	GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1

Frame 19071: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface 0

Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: All-HSRP-routers_46 (00:00:0c:07:ac:46)

Internet Protocol version 4, Src: 10.24.70.208 (10.24.70.208), Dst: 64.29.151.221 (64.29.151.221)

Transmission Control Protocol, Src Port: 49302 (49302), Dst Port: 80 (80), Seq: 853, Ack: 222846, Len: 456

Hypertext Transfer Protocol

- GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1\r\n]
 - [GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /images/animals/frogs-colors/frog-blue.jpg
 - Request Version: HTTP/1.1

Host: www.funny-potato.com

0010 01 f0 6c 69 40 00 80 06 63 bc 0a 18 46 d0 40 1d ...li@... c...F.@.
0020 97 dd c0 96 00 50 11 19 ee 60 d9 cd 11 2f 50 18P.P.
0030 0c d5 3e bd 00 00 47 45 54 20 2f 69 6d 61 67 65 ...>...GE T /image
0040 73 2f 61 6e 69 6d 61 6c 73 2f 66 72 6f 67 73 2d s/animal s/frogs-
0050 63 6f 6c 6f 72 73 2f 66 72 6f 67 2d 62 6c 75 65 colors/f rog-blue
0060 2e 6a 70 67 20 48 54 54 50 2f 31 2e 31 0d 0a 48 .jpg] HTT P/1.1..H
0070 6f 73 74 3a 20 77 77 77 2e 66 75 6e 6e 79 2d 70 ost: www .funny-p
0080 6f 74 61 74 6f 2e 63 6f 6d 0d 0a 55 73 65 72 2d otato.co m..User-
0090 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5
0100 2e 30 20 28 57 69 6e 6a 6f 77 73 20 4e 54 20 36 .0 Cwind ows NT 6
0110 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 33 34 .!; w0w6 4; rv:34
0120 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 .0) geck o/201001
0130 30 31 20 46 6f 67 75 61 67 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-
0140 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 70 .Accept: image/p
0150 6e 67 2c 69 6d 61 67 65 2f 2a 3b 71 3d 30 2e 38 ng,image /*;q=0.8
0160 2c 2a 2f 2a 3b 71 3d 30 2e 38 2e 35 0d 0a 41 63 63 65 ,/*;q=0 .5..Acce
0170 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-
0180 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 us,en;q= 0.5..Acc
0190 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-enCo ding: gz
01a0 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 52 65 66 lp, defl ate, Ref
01b0 65 72 63 74 2f 6f 77 77 77 6f 74 61 74 6f 2e 63 6f .funny-p otato.co
01c0 2e 66 75 6e 6e 79 2d 70 6f 74 61 74 6f 2e 63 6f m/frogs- colors.h
01d0 6d 2f 66 72 6f 67 73 2d 63 6f 6c 6f 72 73 2e 68 tml,.coo kie: TS0
01e0 74 6d 6c 0d 0a 43 6f 6f 6b 69 65 3a 20 54 53 30 194eee0= 010b0780
01f0 31 39 34 65 65 30 3d 30 31 30 62 64 37 38 30 2b9abfc0 c31ec246
0200 34 34 31 33 34 36 61 36 61 64 31 65 61 30 62 61 441346a6 ad1ea0ba
0210 33 64 35 33 37 33 32 61 61 33 31 37 37 65 31 32 3d53732a a3177e12
0220 36 63 64 37 31 63 64 66 34 33 64 65 33 35 34 32 6cd7LcdF 43de3542
0230 32 62 38 61 62 66 63 30 63 33 31 65 63 32 34 36 2b9abfc0 c31ec246
0240 62 61 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 ba..conn ection:
0250 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 0d 0a keep-al1 ve....

HTTP Request-URI (http.request.uri), 42 bytes Packets: 30255 · Displayed: 1 (0.0%) Profile: Default

Transmission Control Protocol, Src Port: 49302 (49302), Dst Port: 80 (80)

Hypertext Transfer Protocol

- GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /images/animals/frogs-colors/frog-b
 - [GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: sequence]
 - Request Method: GET
 - Request URI: /images/animals/frogs-colors/frog-blue.jpg
 - Request version: HTTP/1.1

Host: www.funny-potato.com

0010 01 f0 6c 69 40 00 80 06 63 bc 0a 18 46 d0 40 1d ...li@... c...F.@.
0020 97 dd c0 96 00 50 11 19 ee 60 d9 cd 11 2f 50 18P.P.
0030 0c d5 3e bd 00 00 47 45 54 20 2f 69 6d 61 67 65 ...>...GE T /image
0040 73 2f 61 6e 69 6d 61 6c 73 2f 66 72 6f 67 73 2d s/animal s/frogs-
0050 63 6f 6c 6f 72 73 2f 66 72 6f 67 2d 62 6c 75 65 colors/f rog-blue
0060 2e 6a 70 67 20 48 54 54 50 2f 31 2e 31 0d 0a 48 .jpg] HTT P/1.1..H
0070 6f 73 74 3a 20 77 77 77 2e 66 75 6e 6e 79 2d 70 ost: www .funny-p
0080 6f 74 61 74 6f 2e 63 6f 6d 0d 0a 55 73 65 72 2d otato.co m..User-
0090 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5
0100 2e 30 20 28 57 69 6e 6a 6f 77 73 20 4e 54 20 36 .0 Cwind ows NT 6

Capture #3

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.connection && http.host contains "wikipedia" && http.request.lin Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
25	10.8103020	192.168.1.2	208.80.154.224	HTTP	823	GET /wiki/solanumdulcamara HTTP/1.1
48593	149.564049	192.168.1.2	208.80.154.224	HTTP	566	GET /wiki/Tree HTTP/1.1
50850	188.358171	192.168.1.2	208.80.154.224	HTTP	635	GET /wiki/exploding_tree HTTP/1.1
51208	196.244001	192.168.1.2	208.80.154.224	HTTP	645	GET /wiki/Special:Random HTTP/1.1
51212	196.396014	192.168.1.2	208.80.154.224	HTTP	657	GET /wiki/Block_Island_State_Airport HTTP/1.1
52340	233.232376	192.168.1.2	208.80.154.224	HTTP	652	GET /wiki/Main_Page HTTP/1.1
53006	250.742238	192.168.1.2	208.80.154.224	HTTP	659	GET /wiki/Mozambique_funeral_beer_poisoning HTTP/1.1
53793	317.771999	192.168.1.2	208.80.154.224	HTTP	583	GET /favicon.ico HTTP/1.1
53880	334.333555	192.168.1.2	208.80.154.224	HTTP	637	GET /wiki/Tunnel_View HTTP/1.1
54141	350.448953	192.168.1.2	208.80.154.224	HTTP	642	GET /wiki/Special:Random HTTP/1.1
54145	350.513528	192.168.1.2	208.80.154.224	HTTP	646	GET /wiki/Greek_inscriptions HTTP/1.1

Frame 53880: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface 0

Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: Actionte_83:97:54 (00:1f:90:83:97:54)

Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 208.80.154.224 (208.80.154.224)

Transmission Control Protocol, Src Port: 50073 (50073), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 583

Hypertext Transfer Protocol

GET /wiki/Tunnel_View HTTP/1.1\r\n

Host: en.wikipedia.org\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0\r\n

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

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://en.wikipedia.org/wiki/Main_Page\r\n

Cookie: centralnotice_bannercount_fr12=0; centralnotice_bannercount_fr12=wait=3%7C0%7C0; GeoIP=US:Providence:41.8390:-71.4373:v4; uls-previous-languages=%5B%22en%22%5D; Cookie pair: centralnotice_bannercount_fr12=0; Cookie pair: centralnotice_bannercount_fr12=wait=3%7C0%7C0; Cookie pair: GeoIP=US:Providence:41.8390:-71.4373:v4; Cookie pair: uls-previous-languages=%5B%22en%22%5D; Cookie pair: mediawiki.user.sessionid=gT8ykdojrZupmpbe4YSrouj50m7efvqy

Connection: keep-alive\r\n

0000 00 1f 90 83 97 54 40 25 c2 53 97 48 08 00 45 00T@% .S.H..E.
0010 02 6f 78 34 40 00 80 06 53 79 c0 a8 01 02 d0 50 ..ox4@... Sy....P
0020 9a e0 c3 99 00 50 24 4c 87 e5 cb dd c5 a4 50 18P\$LP
0030 01 00 c5 e1 00 60 47 45 54 20 2f 77 69 6b 69 2fGE /wiki/
0040 54 75 6e 6e 65 6c 5f 56 69 65 77 20 48 54 50 Tunnel_View HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 6e 2e 77 /1.1..Ho st: en.w
0060 69 6b 69 70 65 64 69 61 2e 6f 72 67 0d 0a 53 73 ikipedia .org.us
0070 65 72 20 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0080 61 2f 31 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N
0090 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 T 6.1; W OW64; rv
00a0 3a 33 34 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :34.0) G ecko/201

Packets: 158029 - Displayed: 11 (0.0%) - Dropped: 467 (0.3%) - Load time: 0:06.662

Profile: Default

Filter: http.connection && http.host contains "wikipedia" && http.request.lin Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
25	10.8103020	192.168.1.2	208.80.154.224	HTTP	823	GET /wiki/solanumdulcamara HTTP/1.1
48593	149.564049	192.168.1.2	208.80.154.224	HTTP	566	GET /wiki/Tree HTTP/1.1
50850	188.358171	192.168.1.2	208.80.154.224	HTTP	635	GET /wiki/Exploding_tree HTTP/1.1
51208	196.244001	192.168.1.2	208.80.154.224	HTTP	645	GET /wiki/Special:Random HTTP/1.1
51212	196.396014	192.168.1.2	208.80.154.224	HTTP	657	GET /wiki/Block_Island_State_Airport HTTP/1.1
52340	233.232376	192.168.1.2	208.80.154.224	HTTP	652	GET /wiki/Main_Page HTTP/1.1
53006	250.742238	192.168.1.2	208.80.154.224	HTTP	659	GET /wiki/Mozambique_funeral_beer_poisoning HTTP/1.1
53793	317.771999	192.168.1.2	208.80.154.224	HTTP	583	GET /favicon.ico HTTP/1.1
53880	334.333555	192.168.1.2	208.80.154.224	HTTP	637	GET /wiki/Tunnel_View HTTP/1.1
54141	350.448953	192.168.1.2	208.80.154.224	HTTP	642	GET /wiki/Special:Random HTTP/1.1
54145	350.513528	192.168.1.2	208.80.154.224	HTTP	646	GET /wiki/Greek_inscriptions HTTP/1.1

Frame 53880: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface 0

Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: Actionte_83:97:54 (00:1f:90:83:97:54)

Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 208.80.154.224 (208.80.154.224)

Transmission Control Protocol, Src Port: 50073 (50073), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 583

Hypertext Transfer Protocol

GET /wiki/Tunnel_View HTTP/1.1\r\n

Host: en.wikipedia.org\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0\r\n

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

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://en.wikipedia.org/wiki/Main_Page\r\n

Cookie: centralnotice_bannercount_fr12=0; centralnotice_bannercount_fr12=wait=3%7C0%7C0; GeoIP=US:Providence:41.8390:-71.4373:v4; uls-previous-languages=%5B%22en%22%5D; Cookie pair: centralnotice_bannercount_fr12=0; Cookie pair: centralnotice_bannercount_fr12=wait=3%7C0%7C0; Cookie pair: GeoIP=US:Providence:41.8390:-71.4373:v4; Cookie pair: uls-previous-languages=%5B%22en%22%5D; Cookie pair: mediawiki.user.sessionid=gT8ykdojrZupmpbe4YSrouj50m7efvqy

Connection: keep-alive\r\n

0000 00 1f 90 83 97 54 40 25 c2 53 97 48 08 00 45 00T@% .S.H..E.
0010 02 6f 78 34 40 00 80 06 53 79 c0 a8 01 02 d0 50 ..ox4@... Sy....P
0020 9a e0 c3 99 00 50 24 4c 87 e5 cb dd c5 a4 50 18P\$LP
0030 01 00 c5 e1 00 60 47 45 54 20 2f 77 69 6b 69 2fGE /wiki/
0040 54 75 6e 6e 65 6c 5f 56 69 65 77 20 48 54 50 Tunnel_View HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 6e 2e 77 /1.1..Ho st: en.w
0060 69 6b 69 70 65 64 69 61 2e 6f 72 67 0d 0a 53 73 ikipedia .org.us
0070 65 72 20 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0080 61 2f 31 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N
0090 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 T 6.1; W OW64; rv
00a0 3a 33 34 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :34.0) G ecko/201

*I was unable to filter this down to one packet, and no text seemed to be highlighted along the bottom for this selection.

Capture #4

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.content_length == 823 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
12662	94.4561520	74.63.51.103	192.168.1.2	HTTP	1128	HTTP/1.1 200 OK (text/javascript)

Frame 12662: 1128 bytes on wire (9024 bits), 1128 bytes captured (9024 bits) on interface 0

Ethernet II, Src: Actionte_83:97:54 (00:1f:90:83:97:54), Dst: IntelCor_53:97:48 (40:25:c2:53:97:48)

Internet Protocol Version 4, Src: 74.63.51.103 (74.63.51.103), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49658 (49658), Seq: 964, Ack: 749, Len: 1074

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 18 Jan 2015 17:03:12 GMT\r\n

Server: Apache/2.4.10 (Unix)\r\n

Vary: Accept-Encoding,User-Agent\r\n

Content-Encoding: gzip\r\n

Content-Length: 823\r\n

[Content length: 823]

Content-Type: text/javascript\r\n

Keep-Alive: timeout=5, max=99\r\n

Connection: Keep-Alive\r\n

\r\n

[HTTP response 2/3]

[Time since request: 0.075411000 seconds]

[Prev request in frame: 8633]

[Prev response in frame: 8820]

[Request in frame: 12424]

[Next request in frame: 12815]

[Next response in frame: 12907]

Content-encoded entity body (gzip): 823 bytes -> 2207 bytes

Line-based text data: text/javascript

00f0 73 63 72 69 70 74 0d 0a 4b 65 65 70 2d 41 6c 69 script.. Keep-Alive
0100 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d ve: time out=5, m
0110 61 78 3d 39 39 0d 0a 43 6f 6e 6e 65 63 74 69 6f ax=99..C onnectio
0120 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d n: Keep- Alive...
0130 0a 1f 8b 08 00 00 00 00 00 00 03 d5 56 4d 6f e3 VMo.
0140 36 10 bd ef af e0 ba c5 22 41 ad 2f 7f 25 96 2d 6..... "A./.%.-

Frame (1128 bytes) Uncompressed entity body (2207 bytes)

Response line (http.response.line), 31 bytes Packets: 158029 - Displayed: 1 (0.0%) - Dropped: 467 (0.3%) - Load time: 0:07.728 Profile: Default

TRANSMISSION CONTROL PROTOCOL, Src Port: 80 (80), Dst Port: 49658 (49658)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 18 Jan 2015 17:03:12 GMT\r\n

Server: Apache/2.4.10 (Unix)\r\n

Vary: Accept-Encoding,User-Agent\r\n

Content-Encoding: gzip\r\n

Content-Length: 823\r\n

[Content length: 823]

Content-Type: text/javascript\r\n

Keep-Alive: timeout=5, max=99\r\n

Connection: Keep-Alive\r\n

\r\n

[HTTP response 2/3]

[Time since request: 0.075411000 seconds]

[Prev request in frame: 8633]

[Prev response in frame: 8820]

[Request in frame: 12424]

[Next request in frame: 12815]

[Next response in frame: 12907]

Content-encoded entity body (gzip): 823 bytes -> 2207 bytes

Line-based text data: text/javascript

00f0 73 63 72 69 70 74 0d 0a 4b 65 65 70 2d 41 6c 69 script.. Keep-Alive
0100 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d ve: time out=5, m
0110 61 78 3d 39 39 0d 0a 43 6f 6e 6e 65 63 74 69 6f ax=99..C onnectio
0120 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d n: Keep- Alive...
0130 0a 1f 8b 08 00 00 00 00 00 00 03 d5 56 4d 6f e3 VMo.
0140 36 10 bd ef af e0 ba c5 22 41 ad 2f 7f 25 96 2d 6..... "A./.%.-

Capture #5

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes. The top pane shows a list of captured packets, with a filter expression 'p.location contains "11" && http && http.connection contains "close"'. The middle pane displays the details of the selected packet (No. 53542), showing the Hypertext Transfer Protocol section expanded. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates 'Response line (http.response.line), 57 bytes', 'Packets: 158029 - Displayed: 297 (0.2%) - Dropped: 467 (0.3%) - Load time: 0.006', and 'Profile: Default'.

Filter: p.location contains "11" && http && http.connection contains "close" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
53541	279.604784	192.168.1.1	192.168.1.2	SSDP	462	HTTP/1.1 200 OK
53542	279.604939	192.168.1.1	192.168.1.2	SSDP	462	HTTP/1.1 200 OK
53543	279.605000	192.168.1.1	192.168.1.2	SSDP	462	HTTP/1.1 200 OK

Frame 53541: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface 0
Ethernet II, Src: Actiontec_83:97:54 (00:1f:90:83:97:54), Dst: Intelcor_53:97:48 (40:25:c2:53:97:48)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 54202 (54202)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n\r\nDATE: Sun, 18 Jan 2015 17:06:17 GMT\r\nSERVER: OpenRG/4.0.16.1.56.0.10.14.4 UPnP/1.0 Actiontec/RG_VERSION\r\nCONNECTION: close\r\nCACHE-CONTROL: max-age=120\r\nLOCATION: http://192.168.1.1:2555/upnp/585310cd-3808-23a9-b7784a4332ac0ece/desc.xml\r\nEXT: \r\n\r\nST: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n\r\nUSN: uuid:585310cd-3808-23a9-b7784a4332ac0ece::urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n\r\n[HTTP response 1/297]
[Next response in frame: 53542]

Response line (http.response.line), 57 bytes Packets: 158029 - Displayed: 297 (0.2%) - Dropped: 467 (0.3%) - Load time: 0.006 Profile: Default

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n\r\nDATE: Sun, 18 Jan 2015 17:06:17 GMT\r\nSERVER: OpenRG/4.0.16.1.56.0.10.14.4 UPnP/1.0 Actiontec/RG_VERSION\r\nCONNECTION: close\r\nCACHE-CONTROL: max-age=120\r\nLOCATION: http://192.168.1.1:2555/upnp/585310cd-3808-23a9-b7784a4332ac0ece/desc.xml\r\nEXT: \r\n\r\nST: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n\r\nUSN: uuid:585310cd-3808-23a9-b7784a4332ac0ece::urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n\r\n[HTTP response 1/297]
[Next response in frame: 53542]

0000 40 25 c2 53 97 48 00 1f 90 83 97 54 08 00 45 00 00 S.H. ...T..E.
0010 01 c0 00 00 40 00 40 11 b5 d9 c0 a8 01 01 c0 a8 ...@.
0020 01 02 07 6c d3 ba 01 ac 01 69 48 54 54 50 2f 31 ...1....iHTTP/1
0030 2e 31 20 32 30 30 20 4f 4b 0d 0a 44 41 54 45 3a .1 200 O K..DATE:
0040 20 53 75 6e 2c 20 31 38 20 4a 61 6e 20 32 30 31 Sun, 18 Jan 201
0050 35 20 31 37 3a 30 36 3a 31 37 20 47 4d 54 0d 0a 5 17:06: 17 GMT..
0060 53 45 52 56 45 52 3a 20 4f 70 65 6e 52 47 2f 34 SERVER: OpenRG/4
0070 2e 30 2e 31 36 2e 31 2e 35 36 2e 30 2e 31 30 2e .0.16.1. 56.0.10.
0080 31 34 2e 34 20 55 50 6e 50 2f 31 2e 30 20 41 63 14.4 UPn P/1.0 Ac
0090 74 69 6f 6e 74 65 63 2f 52 47 5f 56 45 52 53 49 tiontec/ RG_VERSI
00a0 4f 4e 0d 0a 43 4f 4e 4e 45 43 54 49 4f 4e 3a 20 ON..CONN ECTION:
00b0 63 6c 6f 73 65 0d 0a 43 41 43 48 45 2d 43 4f 4e close..C ACHE-CON
00c0 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d 31 32 TROL: ma x-age=12
00d0 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 74 74 0..LOCAT ION: htt
00e0 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 31 2e 31 3a p://192. 168.1.1:
00f0 32 35 35 35 2f 75 70 6e 70 2f 35 38 35 33 31 30 2555/upn p/585310
0100 63 64 2d 33 38 30 38 2d 32 33 61 39 2d 62 37 37 cd-3808- 23a9-b77
0110 38 34 61 34 33 33 32 61 63 30 65 63 65 2f 64 65 84a4332a c0ece/de
0120 73 63 2e 78 6d 6c 0d 0a 45 58 54 3a 20 0d 0a 53 sc.xml.. EXT: ..
0130 54 3a 20 75 72 6e 3a 73 63 68 65 6d 61 73 2d 75 T: urn:s chemas-u
0140 70 6e 70 2d 6f 72 67 3a 64 65 76 69 63 65 3a 49 npn-org: device:I
0150 6e 74 65 72 6e 65 74 47 61 74 65 77 61 79 44 65 nternetG atewayDe
0160 76 69 63 65 3a 31 0d 0a 55 53 4e 3a 20 75 75 69 vice:1.. USN: uui
0170 64 3a 35 38 35 33 31 30 63 64 2d 33 38 30 38 2d d:585310 cd-3808-
0180 32 33 61 39 2d 62 37 37 38 34 61 34 33 33 32 61 23a9-b77 84a4332a
0190 63 30 65 63 65 3a 3a 75 72 6e 3a 73 63 68 65 6d c0ece::u rn:schem

Capture #6

Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)

Filter: host contains "C" && frame.len <= 153 && frame.number >= 157356

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
157357	3300.69733	fe80::f1c9:3303:3895:ff02::c	ff02::c	SSDP	153	M-SEARCH * HTTP/1.1

Frame 157357: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0

Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::f1c9:3303:3895:868b (fe80::f1c9:3303:3895:868b), Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 54200 (54200), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

M-SEARCH * HTTP/1.1\r\n

Host:[ff02::c]:1900\r\n

ST:upnp:rootdevice\r\n

Man:"ssdp:discover"\r\n

MX:3\r\n

\r\n

[Full request URI: http://[ff02::c]:1900*]

[HTTP request 1007/1029]

[Prev request in frame: 157347]

[Next request in frame: 157359]

0000 33 33 00 00 00 0c 40 25 c2 53 97 48 86 dd 60 00 33...@% .S.H..`.

0010 00 00 00 63 11 01 fe 80 00 00 00 00 00 00 00 f1 c9 ...C....

0020 33 03 38 95 86 ff 02 00 00 00 00 00 00 00 00 00 3.8.....

0030 00 00 00 00 00 0c d3 b8 07 6c 00 63 39 09 4d 2d1.c9.M-

0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.

0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [ff02::c

0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 70 6e 70 3a]:1900.. ST:upnp:

0070 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 61 6e 3a rootdevi ce..Man:

0080 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".

0090 0a 4d 58 3a 33 0d 0a 0d 0a .MX:3....

Request line (http.requestline), 21 bytes

Packets: 158029 · Displayed: 1 (0.0%) · Dropped: 467 (0.3%) · Load time: 0:08.784

Profile: Default

Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)

Filter: host contains "C" && frame.len <= 153 && frame.number >= 157356

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
157357	3300.69733	fe80::f1c9:3303:3895:ff02::c	ff02::c	SSDP	153	M-SEARCH * HTTP/1.1

Frame 157357: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0

Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::f1c9:3303:3895:868b (fe80::f1c9:3303:3895:868b), Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 54200 (54200), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

M-SEARCH * HTTP/1.1\r\n

Host:[ff02::c]:1900\r\n

ST:upnp:rootdevice\r\n

Man:"ssdp:discover"\r\n

MX:3\r\n

\r\n

[Full request URI: http://[ff02::c]:1900*]

[HTTP request 1007/1029]

[Prev request in frame: 157347]

[Next request in frame: 157359]

0000 33 33 00 00 00 0c 40 25 c2 53 97 48 86 dd 60 00 33...@% .S.H..`.

0010 00 00 00 63 11 01 fe 80 00 00 00 00 00 00 00 00 f1 c9 ...C....

0020 33 03 38 95 86 ff 02 00 00 00 00 00 00 00 00 00 3.8.....

0030 00 00 00 00 00 0c d3 b8 07 6c 00 63 39 09 4d 2d1.c9.M-

0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.

0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [ff02::c

0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 70 6e 70 3a]:1900.. ST:upnp:

0070 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 61 6e 3a rootdevi ce..Man:

0080 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".

0090 0a 4d 58 3a 33 0d 0a 0d 0a .MX:3....

Request line (http.requestline), 21 bytes

Packets: 158029 · Displayed: 1 (0.0%) · Dropped: 467 (0.3%) · Load time: 0:08.784

Profile: Default

Capture #7

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9e0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: host contains "c" && frame.len <= 153 && frame.number <= 157300 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
157297	3294.67780	fe80::f1c9:3303:3895:868b	ff02::c	SSDP	153	M-SEARCH * HTTP/1.1

Frame 157297: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0

Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::f1c9:3303:3895:868b (fe80::f1c9:3303:3895:868b), Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 54200 (54200), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

M-SEARCH * HTTP/1.1\r\n

Host:[FF02::C]:1900\r\n

ST:upnp:rootdevice\r\n

Man:"ssdp:discover"\r\n

MX:3\r\n

\r\n

[Full request URI: http://[FF02::C]:1900*]

[HTTP request 1002/1029]

[Prev request in frame: 157296]

[Next request in frame: 157305]

0000 33 33 00 00 00 0c 40 25 c2 53 97 48 86 dd 60 00 33....@% .S.H...
 0010 00 00 00 63 11 01 fe 80 00 00 00 00 00 00 f1 c9 ...C....
 0020 33 03 38 95 86 8b ff 02 00 00 00 00 00 00 00 00 3.8....
 0030 00 00 00 00 00 0c d3 b8 07 6c 00 63 39 09 4d 2dl.c9.M-
 0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
 0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [FF02::C
 0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 70 6e 70 3a]:1900.. ST:upnp:
 0070 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 61 6e 3a rootdevi ce..Man:
 0080 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".
 0090 0a 4d 58 3a 33 0d 0a 0d 0a .MX:3...

Text item (text), 2 bytes Packets: 158029 · Displayed: 1 (0.0%) · Dropped: 467 (0.3%) · Load time: 0:07.327 Profile: Default

User Datagram Protocol, Src Port: 54200 (54200), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

M-SEARCH * HTTP/1.1\r\n

Host:[FF02::C]:1900\r\n

ST:upnp:rootdevice\r\n

Man:"ssdp:discover"\r\n

MX:3\r\n

\r\n

[Full request URI: http://[FF02::C]:1900*]

[HTTP request 1002/1029]

[Prev request in frame: 157296]

[Next request in frame: 157305]

0000 33 33 00 00 00 0c 40 25 c2 53 97 48 86 dd 60 00 33....@% .S.H...
 0010 00 00 00 63 11 01 fe 80 00 00 00 00 00 00 f1 c9 ...C....
 0020 33 03 38 95 86 8b ff 02 00 00 00 00 00 00 00 00 3.8....
 0030 00 00 00 00 00 0c d3 b8 07 6c 00 63 39 09 4d 2dl.c9.M-
 0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
 0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [FF02::C
 0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 70 6e 70 3a]:1900.. ST:upnp:
 0070 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 61 6e 3a rootdevi ce..Man:
 0080 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".
 0090 0a 4d 58 3a 33 0d 0a 0d 0a .MX:3...

Capture #8

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The filter bar shows a filter: `host contains "C" && frame.len >= 585 && frame.number <= 53198`. The packet list shows a single packet, 53198, at time 252.533416, from source `fe80::f1c9:3303:3895:ff02::c` to destination `SSDP`, with protocol `NOTIFY * HTTP/1.1`. The packet details pane shows the structure of the NOTIFY message, including Host, NT, NTS, Location, USN, Cache-Control, Server, OPT, and NLS fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Filter: `host contains "C" && frame.len >= 585 && frame.number <= 53198`

No. 53198 Time 252.533416 Source `fe80::f1c9:3303:3895:ff02::c` Destination `SSDP` Protocol Length Info `NOTIFY * HTTP/1.1`

Frame 53198: 585 bytes on wire (4680 bits), 585 bytes captured (4680 bits) on interface 0
Ethernet II, Src: IntelCor_53:97:48 (40:25:c2:53:97:48), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
Internet Protocol Version 6, Src: `fe80::f1c9:3303:3895:868b` (fe80::f1c9:3303:3895:868b), Dst: `ff02::c` (ff02::c)
User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1900 (1900)
Hypertext Transfer Protocol
NOTIFY * HTTP/1.1\r\n
Host:[FF02::C]:1900\r\n
NT:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n
NTS:ssdp:alive\r\n
Location:http://[fe80::f1c9:3303:3895:868b]:2869/upnphost/udhisapi.dll?content=uuid:09a9289e-4524-41e4-8ef2-6fed9ee279be\r\n
USN:uuid:09a9289e-4524-41e4-8ef2-6fed9ee279be:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n
Cache-Control:max-age=900\r\n
Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n
01-NLS:f35cf362b4e6100a977ab6451834c4e9\r\n
Full request URI: [http://\[FF02::C\]:1900/](http://[FF02::C]:1900/)

Text item (text), 16 bytes

Packets: 158029 - Displayed: 1 (0.0%) - Dropped: 467 (0.3%) - Load time: 0:11:766

Profile: Default

```
User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1900 (1900)
Hypertext Transfer Protocol
+ NOTIFY * HTTP/1.1\r\n
  Host:[FF02::C]:1900\r\n
  NT:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n
  NTS:ssdp:alive\r\n
  Location:http://[fe80::f1c9:3303:3895:868b]:2869/upnphost/udhisapi.dll?
  USN:uuid:09a9289e-4524-41e4-8ef2-6fed9ee279be:urn:microsoft.com:servi
  Cache-Control:max-age=900\r\n
  Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
  OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n
  01-NLS:f35cf362b4e6100a977ab6451834c4e9\r\n
  \r\n
  Full request URI: http://[FF02::C]:1900/
```

```
000 33 33 00 00 0c 40 25 c2 53 97 48 86 dd 60 00 33....@% .S.H..
010 00 00 02 13 11 01 fe 80 00 00 00 00 00 00 f1 c9 .....
020 33 03 38 95 86 8b ff 02 00 00 00 00 00 00 00 00 3.8....
030 00 00 00 00 00 0c 07 6c 07 6c 02 13 43 f3 4e 4f .....l .l..C.NO
040 54 49 46 59 20 2a 20 48 54 54 50 2f 31 2e 31 0d TIFY * H TTP/1.1.
050 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 5d 3a .Host:[F F02::C]:
060 31 39 30 30 0d 0a 4e 54 3a 75 72 6e 3a 6d 69 63 1900..NT :urn:mic
070 72 6f 73 6f 66 74 2e 63 6f 6d 3a 73 65 72 76 69 rosoft.c om:servi
080 63 65 3a 58 5f 4d 53 5f 4d 65 64 69 61 52 65 63 ce:X_MS_ MediaRec
090 65 69 76 65 72 52 65 67 69 73 74 72 61 72 3a 31 eiverReg istrar:1
0a0 0d 0a 4e 54 53 3a 73 73 64 70 3a 61 6c 69 76 65 ..NTS:ss dp:alive
0b0 0d 0a 4c 6f 63 61 74 69 6f 6e 3a 68 74 74 70 3a ..Locati on:http:
0c0 2f 2f 5b 66 65 38 30 3a 3a 66 31 63 39 3a 33 33 //[fe80::f1c9:33
0d0 30 33 3a 33 38 39 35 3a 38 36 38 62 5d 3a 32 38 03:3895: 868b]:28
0e0 36 39 2f 75 70 6e 70 68 6f 73 74 2f 75 64 68 69 69/upnph ost/udhi
0f0 73 61 70 69 2e 64 6c 6c 3f 63 6f 6e 74 65 6e 74 sapi.dll ?content
```


Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12.3)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `in >= 1484 && frame.number <= 53198 && tcp.analysis.fast_retransmit` Expression... Clear Apply Save

No. Time Source Destination Protocol Length Info

46102 134.578282 23.67.244.146 192.168.1.2 HTTP 1484 [TCP Fast Retransmission] HTTP/1.1 200 OK (JPEG JFIF image)

Frame 46102: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface 0

Ethernet II, Src: Actiontec_83:97:54 (00:1f:00:83:97:54), Dst: IntelCor_53:97:48 (40:25:c2:53:97:48)

Internet Protocol Version 4, Src: 23.67.244.146 (23.67.244.146), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49817 (49817), Seq: 94035, Ack: 5025, Len: 1430

[24 Reassembled TCP Segments (25188 bytes): #45996(1407), #45998(1430), #46000(1430), #46002(1430), #46004(1430), #46006(1430), #46008(1430), #46010(1430), #46012(1430), #46014(1430), #46016(1430), #46018(1430), #46020(1430), #46022(1430), #46024(1430), #46026(1430), #46028(1430), #46030(1430), #46032(1430), #46034(1430), #46036(1430), #46038(1430), #46040(1430), #46042(1430), #46044(1430), #46046(1430), #46048(1430), #46050(1430), #46052(1430), #46054(1430), #46056(1430), #46058(1430), #46060(1430), #46062(1430), #46064(1430), #46066(1430), #46068(1430), #46070(1430), #46072(1430), #46074(1430), #46076(1430), #46078(1430), #46080(1430), #46082(1430), #46084(1430), #46086(1430), #46088(1430), #46090(1430), #46092(1430), #46094(1430), #46096(1430), #46098(1430), #46100(1430), #46102(1430), #46104(1430), #46106(1430), #46108(1430), #46110(1430), #46112(1430), #46114(1430), #46116(1430), #46118(1430), #46120(1430), #46122(1430), #46124(1430), #46126(1430), #46128(1430), #46130(1430), #46132(1430), #46134(1430), #46136(1430), #46138(1430), #46140(1430), #46142(1430), #46144(1430), #46146(1430), #46148(1430), #46150(1430), #46152(1430), #46154(1430), #46156(1430), #46158(1430), #46160(1430), #46162(1430), #46164(1430), #46166(1430), #46168(1430), #46170(1430), #46172(1430), #46174(1430), #46176(1430), #46178(1430), #46180(1430), #46182(1430), #46184(1430), #46186(1430), #46188(1430), #46190(1430), #46192(1430), #46194(1430), #46196(1430), #46198(1430), #46200(1430), #46202(1430), #46204(1430), #46206(1430), #46208(1430), #46210(1430), #46212(1430), #46214(1430), #46216(1430), #46218(1430), #46220(1430), #46222(1430), #46224(1430), #46226(1430), #46228(1430), #46230(1430), #46232(1430), #46234(1430), #46236(1430), #46238(1430), #46240(1430), #46242(1430), #46244(1430), #46246(1430), #46248(1430), #46250(1430), #46252(1430), #46254(1430), #46256(1430), #46258(1430), #46260(1430), #46262(1430), #46264(1430), #46266(1430), #46268(1430), #46270(1430), #46272(1430), #46274(1430), #46276(1430), #46278(1430), #46280(1430), #46282(1430), #46284(1430), #46286(1430), #46288(1430), #46290(1430), #46292(1430), #46294(1430), #46296(1430), #46298(1430), #46300(1430), #46302(1430), #46304(1430), #46306(1430), #46308(1430), #46310(1430), #46312(1430), #46314(1430), #46316(1430), #46318(1430), #46320(1430), #46322(1430), #46324(1430), #46326(1430), #46328(1430), #46330(1430), #46332(1430), #46334(1430), #46336(1430), #46338(1430), #46340(1430), #46342(1430), #46344(1430), #46346(1430), #46348(1430), #46350(1430), #46352(1430), #46354(1430), #46356(1430), #46358(1430), #46360(1430), #46362(1430), #46364(1430), #46366(1430), #46368(1430), #46370(1430), #46372(1430), #46374(1430), #46376(1430), #46378(1430), #46380(1430), #46382(1430), #46384(1430), #46386(1430), #46388(1430), #46390(1430), #46392(1430), #46394(1430), #46396(1430), #46398(1430), #46400(1430), #46402(1430), #46404(1430), #46406(1430), #46408(1430), #46410(1430), #46412(1430), #46414(1430), #46416(1430), #46418(1430), #46420(1430), #46422(1430), #46424(1430), #46426(1430), #46428(1430), #46430(1430), #46432(1430), #46434(1430), #46436(1430), #46438(1430), #46440(1430), #46442(1430), #46444(1430), #46446(1430), #46448(1430), #46450(1430), #46452(1430), #46454(1430), #46456(1430), #46458(1430), #46460(1430), #46462(1430), #46464(1430), #46466(1430), #46468(1430), #46470(1430), #46472(1430), #46474(1430), #46476(1430), #46478(1430), #46480(1430), #46482(1430), #46484(1430), #46486(1430), #46488(1430), #46490(1430), #46492(1430), #46494(1430), #46496(1430), #46498(1430), #46500(1430), #46502(1430), #46504(1430), #46506(1430), #46508(1430), #46510(1430), #46512(1430), #46514(1430), #46516(1430), #46518(1430), #46520(1430), #46522(1430), #46524(1430), #46526(1430), #46528(1430), #46530(1430), #46532(1430), #46534(1430), #46536(1430), #46538(1430), #46540(1430), #46542(1430), #46544(1430), #46546(1430), #46548(1430), #46550(1430), #46552(1430), #46554(1430), #46556(1430), #46558(1430), #46560(1430), #46562(1430), #46564(1430), #46566(1430), #46568(1430), #465

```

# Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49817 (49817), Seq: 94055, Ack: 5025, Len: 1430
# [24 Reassembled TCP Segments (25188 bytes): #45996(1407), #45998(1430), #46000(1430), #46002(1430), #46004(1430)
# Hypertext Transfer Protocol
#   HTTP/1.1 200 OK\r\n
#     [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
#       [HTTP/1.1 200 OK\r\n]
#       [Severity level: Chat]
#       [Group: Sequence]
#     Request Version: HTTP/1.1
#     ...
0000  48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d  HTTP/1.1 200 OK.
0010  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 69  .Content -Type: i
0020  6d 61 67 65 2f 6a 70 65 67 0d 0a 43 6f 6e 74 65  mage/jpeg .Conte
0030  6e 74 2d 4c 65 6e 67 74 68 3a 20 32 35 30 31 39  nt-Length: 25019
0040  0d 0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 38 20  .Date: Sun, 18
0050  4a 61 6e 20 32 30 31 35 20 31 37 3a 30 33 3a 35  Jan 2015 17:03:5
0060  32 20 47 4d 54 0d 0a 43 6f 6e 6e 65 63 74 69 6f  2 GMT..C onnectio
0070  6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43  n: keep-alive..C
0080  61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 70 75  ache-Control: pu
0090  62 6c 69 63 2c 20 6d 61 78 2d 61 67 65 3d 31 32  blic, max-age=12
00a0  30 39 36 30 30 0d 0a 0d 0a ff d8 ff e0 00 10 4a  09600...J
00b0  46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00  FIF.....
00c0  43 00 03 02 02 03 02 02 03 03 03 04 03 03 04  .C.....
00d0  05 08 05 05 04 0a 05 0a 07 07 06 08 0c 0a 0c 0c  .....
00e0  0b 0a 0b 0b 0d 0e 12 10 0d 0e 11 0e 0b 0b 10 16  .....
00f0  10 11 13 14 15 15 15 0c 0f 17 18 16 14 18 12 14  .....
0100  15 14 ff db 00 43 01 03 04 04 05 04 05 09 05 05  ....C.....
0110  09 14 0d 0b 0d 14 14 14 14 14 14 14 14 14 14  .Content-Dispo
0120  14 14 14 14 14 14 14 14 14 14 14 14 14 14 14  .Content-Dispo
0130  14 14 14 14 14 14 14 14 14 14 14 14 14 14 14  .Content-Dispo
0140  14 14 14 14 14 14 14 14 ff c0 00 11 08 00 bb 01 1a  .Content-Dispo
0150  03 01 22 00 02 11 01 03 11 01 ff c4 00 1d 00 00  .Content-Dispo
0160  02 03 01 01 01 01 00 00 00 00 00 00 00 00 05  .Content-Dispo
0170  06 04 07 08 03 02 01 00 09 ff c4 00 47 10 00 02  .Content-Dispo
0180  01 03 04 00 04 03 06 04 04 02 08 07 00 01 02  .Content-Dispo
0190  03 04 05 11 00 06 12 21 07 13 31 41 14 22 51 61  .Content-Dispo
01a0  32 71 81 08 15 23 42 91 a1 16 24 52 d1 33 62 b1  2q...#B...$R.3b.
01b0  c1 72 92 09 17 18 34 43 d2 f0 f1 25 53 54 83 85  .r...4C...%ST...
01c0  a2 b2 ff c4 00 1b 01 00 02 03 01 01 01 00 00 00  .r...4C...%ST...
01d0  00 00 00 00 00 00 00 03 04 01 02 05 00 06 07 ff  .r...4C...%ST...
01e0  c4 00 31 11 00 02 02 01 03 02 04 04 05 05 01 01  .r...4C...%ST...
01f0  00 00 00 00 01 02 00 11 03 12 21 31 04 41 13 22  .r...4C...%ST...
0200  51 61 05 32 71 f0 81 91 a1 b1 d1 14 23 c1 e1 f1  .r...4C...%ST...

```


Capture #10

The screenshot shows the Wireshark interface with a packet capture of an HTTP response. The filter is set to 'len >= 1484 && frame.number <= 53198 && tcp.analysis.out_of_order'. The selected packet is #11252, an HTTP 200 OK response from 192.168.1.2 to 93.4255280184.107.101.202. The packet details show the response structure: HTTP/1.1 200 OK, with various headers including Server: nginx/1.0.15, Date: Sun, 18 Jan 2015 17:03:11 GMT, Content-Type: image/png, Content-Length: 4139, Last-Modified: Sat, 12 Oct 2013 00:51:17 GMT, Connection: keep-alive, and Accept-Ranges: bytes. The packet bytes pane shows the raw data, with the first few bytes being 0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d.

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: len >= 1484 && frame.number <= 53198 && tcp.analysis.out_of_order

No. Time Source Destination Protocol Length Info

11252 93.4255280184.107.101.202 192.168.1.2 HTTP 1484 [TCP Out-Of-Order] HTTP/1.1 200 OK (PNG)

[4 Reassembled TCP Segments (4356 bytes): #11244(1430), #11246(1430), #11252(1430), #11248(66)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n\r\n]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Server: nginx/1.0.15\r\n

Date: Sun, 18 Jan 2015 17:03:11 GMT\r\n

Content-Type: image/png\r\n

Content-Length: 4139\r\n

Last-Modified: Sat, 12 Oct 2013 00:51:17 GMT\r\n

Connection: keep-alive\r\n

Accept-Ranges: bytes\r\n

\r\n

[HTTP response 10/10]

[Time since request: 0.026280000 seconds]

[Prev request in frame: 11078]

[Prev response in frame: 11152]

[Request in frame: 11156]

Portable Network Graphics

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.

0010 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 .Server: nginx/1

0020 2e 30 2e 31 35 0d 0a 44 61 74 65 3a 20 53 75 6e .0.15..D ate: Sun

0030 2c 20 31 38 20 4a 61 6e 20 32 30 31 35 20 31 37 , 18 Jan 2015 17

0040 3a 30 33 3a 31 31 20 47 4d 54 0d 0a 43 6f 6e 74 :03:11 G MT,.Cont

0050 65 6e 74 d 54 79 70 65 3a 20 69 6d 61 67 65 2f ent-Type : image/

0060 70 6e 67 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e png..con tent-Len

0070 67 74 68 3a 20 34 31 33 39 0d 0a 4c 61 73 74 2d gth: 413 9..Last-

0080 4d 6f 64 69 66 69 65 64 3a 20 53 61 74 2c 20 31 Modified : Sat, 1

0090 32 20 4f 63 74 20 32 31 33 20 30 30 3a 43 31 2 Oct 20 13 00:51

00a0 3a 31 37 20 47 4d 54 0d 0a 43 6f 6e 6e 65 63 74 :17 GMT, -Connect

00b0 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee p-alive.

00c0 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 ,Accept- Ranges:

00d0 62 79 74 0d 0a 0d 0a 89 50 4e 47 0d 0a 1a bytes...PNG...

00e0 0a 00 00 00 0d 49 48 44 52 00 00 03 20 00 00 00IHD R....

00f0 6f 08 03 00 00 00 23 48 54 7e 00 00 00 19 74 45 o.....#H T.....TE

0100 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 Xtsoftwa re,Adobe

0110 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 ImageR eadyq.e.c.

0120 00 01 80 50 4c 54 45 ea f2 fe f1 fe fe cd e0 fd ...PLTE:

0130 de ea fd f6 fa ff ec f4 fe f2 f7 fe c1 d8 fb e7

0140 f0 fe e6 f0 fe cc df fc dd eb fe d8 e9 fd dc ea

0150 fe da e8 fe da e9 fd e0 ec fe fc fd ff d3 e4 fd

0160 ec f3 fd d2 e3 fd d6 e6 fd cc e0 fd cd da fa e2

Frame (1484 bytes) Reassembled TCP (4356 bytes)

HTTP Response Reason Phrase (http.respon... Packets: 158029 - Displayed: 1 (0.0%) - Dropped: 467 (0.3%) - Load time: 0:12:22 Profile: Default

The screenshot shows the Wireshark interface with a packet capture of an HTTP response. The filter is set to 'len >= 1484 && frame.number <= 53198 && tcp.analysis.out_of_order'. The selected packet is #11252, an HTTP 200 OK response from 192.168.1.2 to 93.4255280184.107.101.202. The packet details show the response structure: HTTP/1.1 200 OK, with various headers including Server: nginx/1.0.15, Date: Sun, 18 Jan 2015 17:03:11 GMT, Content-Type: image/png, Content-Length: 4139, Last-Modified: Sat, 12 Oct 2013 00:51:17 GMT, Connection: keep-alive, and Accept-Ranges: bytes. The packet bytes pane shows the raw data, with the first few bytes being 0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d.

[4 Reassembled TCP Segments (4356 bytes): #11244(1430), #11246(1430), #11252(1430), #11248(66)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n\r\n]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Server: nginx/1.0.15\r\n

Date: Sun, 18 Jan 2015 17:03:11 GMT\r\n

Content-Type: image/png\r\n

Content-Length: 4139\r\n

Last-Modified: sat, 12 Oct 2013 00:51:17 GMT\r\n

Connection: keep-alive\r\n

Accept-Ranges: bytes\r\n

\r\n

[HTTP response 10/10]

[Time since request: 0.026280000 seconds]

[Prev request in frame: 11078]

[Prev response in frame: 11152]

[Request in frame: 11156]

Portable Network Graphics

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.

0010 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 .Server: nginx/1

0020 2e 30 2e 31 35 0d 0a 44 61 74 65 3a 20 53 75 6e .0.15..D ate: Sun

0030 2c 20 31 38 20 4a 61 6e 20 32 30 31 35 20 31 37 , 18 Jan 2015 17

0040 3a 30 33 3a 31 31 20 47 4d 54 0d 0a 43 6f 6e 74 :03:11 G MT,.Cont

0050 65 6e 74 d 54 79 70 65 3a 20 69 6d 61 67 65 2f ent-Type : image/

0060 70 6e 67 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e png..con tent-Len

0070 67 74 68 3a 20 34 31 33 39 0d 0a 4c 61 73 74 2d gth: 413 9..Last-

0080 4d 6f 64 69 66 69 65 64 3a 20 53 61 74 2c 20 31 Modified : Sat, 1

0090 32 20 4f 63 74 20 32 31 33 20 30 30 3a 43 31 2 Oct 20 13 00:51

00a0 3a 31 37 20 47 4d 54 0d 0a 43 6f 6e 6e 65 63 74 :17 GMT, -Connect

00b0 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee p-alive.

00c0 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 ,Accept- Ranges:

00d0 62 79 74 0d 0a 0d 0a 89 50 4e 47 0d 0a 1a bytes...PNG...

00e0 0a 00 00 00 0d 49 48 44 52 00 00 03 20 00 00 00IHD R....

00f0 6f 08 03 00 00 00 23 48 54 7e 00 00 00 19 74 45 o.....#H T.....TE

0100 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 Xtsoftwa re,Adobe

0110 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 ImageR eadyq.e.c.

0120 00 01 80 50 4c 54 45 ea f2 fe f1 fe fe cd e0 fd ...PLTE:

0130 de ea fd f6 fa ff ec f4 fe f2 f7 fe c1 d8 fb e7

0140 f0 fe e6 f0 fe cc df fc dd eb fe d8 e9 fd dc ea

0150 fe da e8 fe da e9 fd e0 ec fe fc fd ff d3 e4 fd

0160 ec f3 fd d2 e3 fd d6 e6 fd cc e0 fd cd da fa e2

Frame (1484 bytes) Reassembled TCP (4356 bytes)

HTTP Response Reason Phrase (http.respon... Packets: 158029 - Displayed: 1 (0.0%) - Dropped: 467 (0.3%) - Load time: 0:12:22 Profile: Default

Analysis

Filtering:

Capture #1

Filter: `http.request.method == "POST" && http.host contains "bing"`

This was an attempt to filter by the name of a website I had visited. I reduced it by filtering for 'POST,' which appeared in the info section.

No.	Time	Source	Destination	Protocol	Length	Info
6693	80.4423910	10.24.70.208	204.79.197.200	HTTP	1098	POST /rewardsapp/reportActivity HTTP/1.1 (application/x-www-form-urlencoded)

This resulted in this one packet.

Capture #3

Filter: `http.connection && http.host contains "wikipedia" && http.request.lin`

This was an attempt to filter based upon a different website I had visited. I managed to filter the list until only 'GET' packets were remaining, but as shown directly below, I could not figure out how to reduce the list to only one packet. There were 11 packets at the end of this filtering process.

No.	Time	Source	Destination	Protocol	Length	Info
25	10.8103020	192.168.1.2	208.80.154.224	HTTP	823	GET /wiki/solanum_dulcamara HTTP/1.1
48593	149.564049	192.168.1.2	208.80.154.224	HTTP	566	GET /wiki/Tree HTTP/1.1
50850	188.358171	192.168.1.2	208.80.154.224	HTTP	635	GET /wiki/Exploding_tree HTTP/1.1
51208	196.244001	192.168.1.2	208.80.154.224	HTTP	645	GET /wiki/Special:Random HTTP/1.1
51212	196.396014	192.168.1.2	208.80.154.224	HTTP	657	GET /wiki/Block_Island_State_Airport HTTP/1.1
52340	233.232376	192.168.1.2	208.80.154.224	HTTP	652	GET /wiki/Main_Page HTTP/1.1
53006	250.742238	192.168.1.2	208.80.154.224	HTTP	659	GET /wiki/Mozambique_funeral_beer_poisoning HTTP/1.1
53793	317.771999	192.168.1.2	208.80.154.224	HTTP	583	GET /favicon.ico HTTP/1.1
53880	334.333555	192.168.1.2	208.80.154.224	HTTP	637	GET /wiki/Tunnel_View HTTP/1.1
54141	350.448953	192.168.1.2	208.80.154.224	HTTP	642	GET /wiki/Special:Random HTTP/1.1
54145	350.513528	192.168.1.2	208.80.154.224	HTTP	646	GET /wiki/Greek_inscriptions HTTP/1.1

Capture #6

Filter: `host contains "::C" && frame.len <= 153 && frame.number >= 157356`

This is another search based upon the host site, this time also filtered by frame length. This was not specific enough, so an exact frame number was chosen and filtered for, as well.

No.	Time	Source	Destination	Protocol	Length	Info
157357	3300.69733	fe80::f1c9:3303:389ff02::c		SSDP	153	M-SEARCH * HTTP/1.1

This one packet resulted.

Capture #4

Filter: `http.content_length == 823`

Here is a filter based solely on content length.

No.	Time	Source	Destination	Protocol	Length	Info
12662	94.4561520	74.63.51.103	192.168.1.2	HTTP	1128	HTTP/1.1 200 OK (text/javascript)

This is the packet that resulted from the filtering.

Data Correlations:

Capture #9

```

[+] Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49817 (49817), Seq: 94055, Ack: 5025, Len: 1430
[+] [24 Reassembled TCP Segments (25188 bytes): #45996(1407), #45998(1430), #46000(1430), #46002(1430), #46004(1430)]
[+] Hypertext Transfer Protocol
    [+] HTTP/1.1 200 OK\r\n
        Content-Type: image/jpeg
        Content-Length: 25019
        Date: Sun, 18 Jan 2015 17:03:52 GMT
        Connection: keep-alive
        Cache-Control: public, max-age=1209600
        FIF...
        C...
        ....C..
        .....
        ..".
        .....G...
        .....! ..1A."Qa
        2q...#B. ...$R.3b.
        .r....4C ...%ST..
        .....
        ..1.....
        .....!1.A."
        Qa2q...#

```

This is a large packet that has been reassembled from 24 TCP segments. Selecting 'HTTP/1.1 200 OK\r\n' under 'Hypertext Transfer Protocol' has highlighted all of the data. This means that HTTP/1.1 200 OK \r\n must reference the entire packet.

Capture #10

The image shows a Wireshark packet capture of an HTTP 200 OK response. The packet list on the left shows a single packet (No. 11252) from 193.42.55.280 to 192.168.1.2 on port 80. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The status bar at the bottom shows the selected packet details: 0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK. The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header.

No.	Time	Source	Destination	Port
11252	93.4255280	193.42.55.280	192.168.1.2	80

Packet Details:

- Ethernet II, Src: Realtek (08:00:00:00:00:00), Dst: Realtek (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 193.42.55.280, Dst: 192.168.1.2
- Transmission Control Protocol, Src Port: 80, Dst Port: 80
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Request Version: HTTP/1.1

Status Bar: 0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK

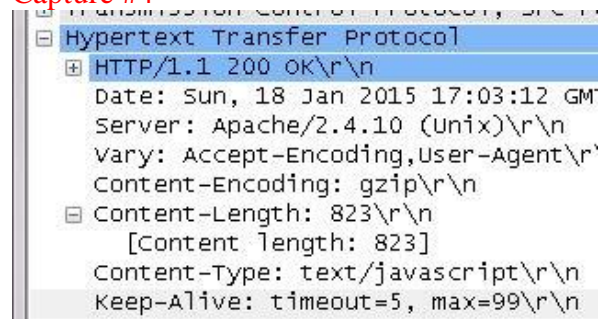
Packet Bytes:

```

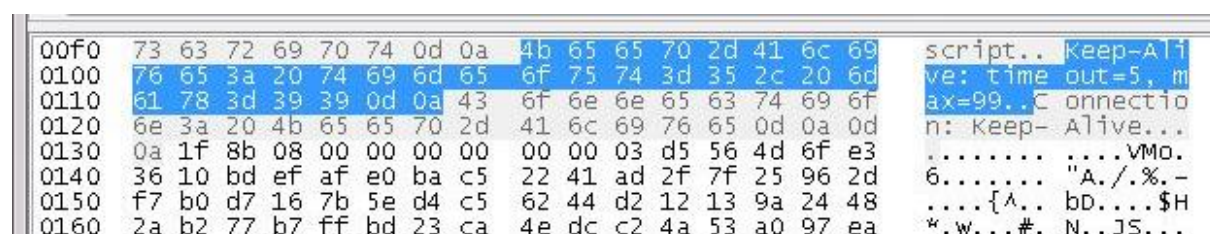
0000  48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d  HTTP/1.1 200 OK
0010  0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31  .Server: nginx/1
0020  2e 30 2e 31 35 0d 0a 44 61 74 65 3a 20 53 75 6e  .0.15..Date: Sun
0030  2c 20 31 38 20 4a 61 6e 20 32 30 31 35 20 31 37  , 18 Jan 2015 17
0040  3a 30 33 3a 31 31 20 47 4d 54 0d 0a 43 6f 6e 74  :03:11 GMT..Cont
0050  65 6e 74 2d 54 79 70 65 3a 20 69 6d 61 6f 6e 2f  ent-Type : image/
0060  70 6e 67 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e  png..Content-Len
0070  67 74 68 3a 20 34 31 33 39 0d 0a 4c 61 73 74 2d  gth: 413 9..Last
  
```

Selecting '[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]' under the two headings listed for Capture #9 resulted in a very short segment of data being highlighted. Only 'OK' and the matching hexadecimal code, '4f4B' were a part of this data.

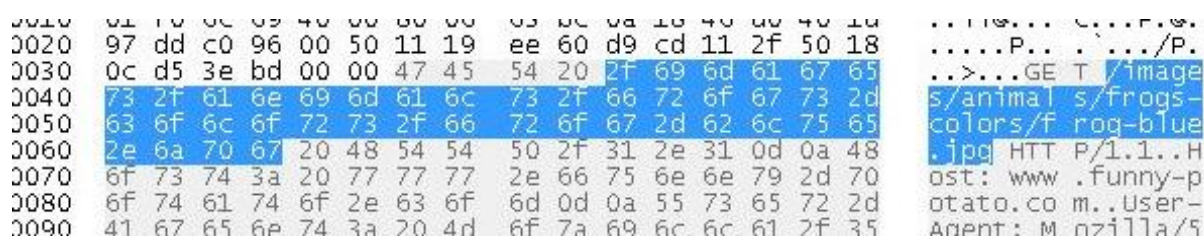
Capture #4



Selecting 'Keep-Alive: timeout=5, max=99\r\n' under the same headings as Capture #9 resulted in essentially the same data appearing in the ASCII window, with matching code in the hexadecimal window.



Capture #2



Under 'Hypertext Transfer Protocol,' selecting '[Expert Info (Chat/Sequence): GET /images/animals/frogs-colors/frog-blue.jpg HTTP/1.1\r\n]' and then 'Request URI: /images/animals/frogs-colors/frog-blue.jpg' highlighted again, a nearly identical segment of data at the bottom and the corresponding hexadecimal code.

Discussion & Questions

Beginner's Issues:

- I failed to record the IP address of the device used at the time.
- In Capture #3, I failed to discover how to further narrow down the results list before moving ahead to attempt more filters. I now know that I could have filtered for many things, including packet length, packet number, and possibly the time.

Dr. Calabrese's Questions:

- a. What is the importance of a tool such as Wireshark to students learning network protocols? How would you think this tool could be used to isolate a network protocol problem?

- i. I think Wireshark is a very important tool for students who are learning network protocols. It allows them to practice using the various parts of a packet to glean real results, instead of memorizing the information from a table. It also allows them to view a wide variety of formats that packets may take, and personalize the experience by being able to identify elements from their own web browsing sessions.
- ii. I think this tool could be used to isolate a network protocol problem because it can be used for specific errors within very specific ranges. It is also able to isolate a specific time frame if the details of the error are uncertain. Here is a minor error (out of order) I found in Capture #10 that the network seems to have corrected on its own.

Filter:		.len >= 1484 && frame.number <= 53198 && tcp.analysis.out_of_order		Expression...	Clear	Apply	Save
o.	Time	Source	Destination	Protocol	Length	Info	
11252	93.4255280	184.107.191.202	192.168.1.2	HTTP	1484	[TCP out-of-order] HTTP/1.1 200 OK (PNG)	
[4 Reassembled TCP Segments (4356 bytes): #11244(1430), #11246(1430), #11252(1430), #11248(66)]							

- b. What is the correlation between the hexadecimal numbers at the bottom of the Wireshark display and the rest of the Wireshark display? Why is seeing these numbers important - give an example of how they are used in connection with 802.3 (specifically the type codes)? Give me a list of the top type codes used in industry.
- i. The hexadecimal numbers at the bottom of the screen give the same data as the rest of the screen does. Computers communicate in binary. Hexadecimal is a way to condense binary into more manageable chunks. The ASCII characters to the right of the hexadecimal characters either are, or may as well be the translation of the hexadecimal code. The information along the top of the screen has all been extracted or inferred from the same binary that the hexadecimal code is from.
 - ii. Seeing these numbers is important because it can be used to garner specific details, such as whether a packet is an ARP packet or an IP packet, simply by looking at the correct chunk of code without having to know much about Wireshark's layout.
 - iii. The top type codes used in the industry are IP 0800 and ARP 0806.