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

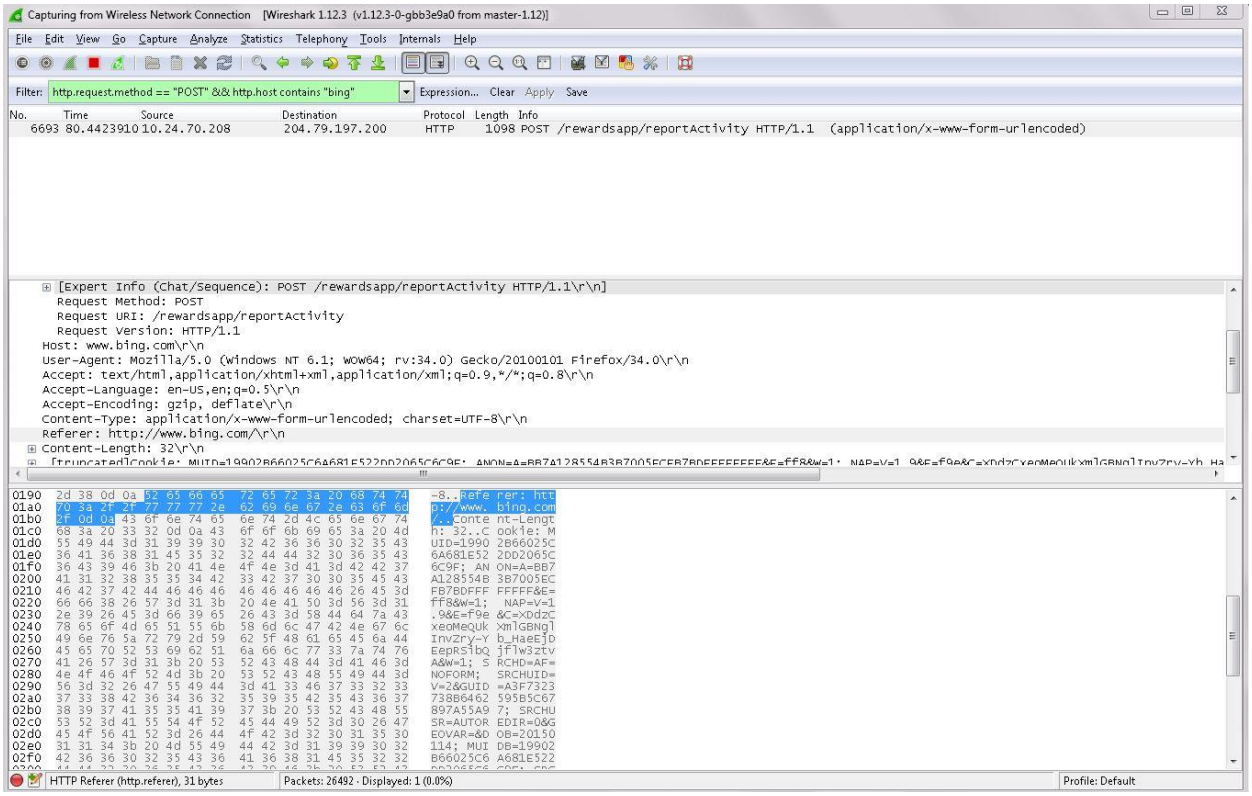
Tools:
- Wireshark
  - Settings - Captures, Filter Toolbar
- Snipping Tool
  - Settings - New
- Web Browsers
  - Opera
  - Firefox
  - Internet Explorer

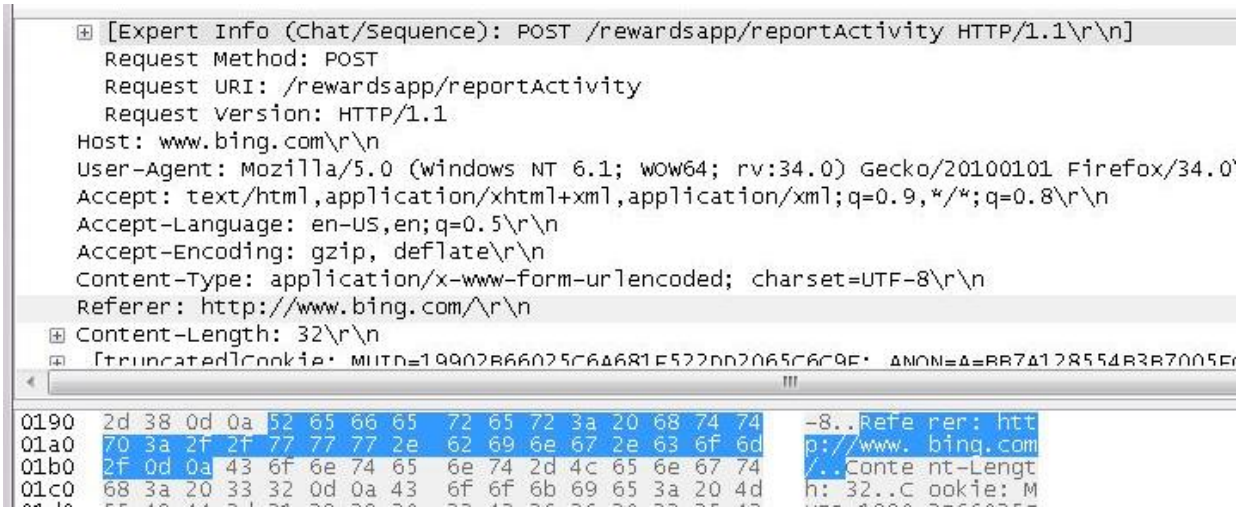
How I Obtained Packets:

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.

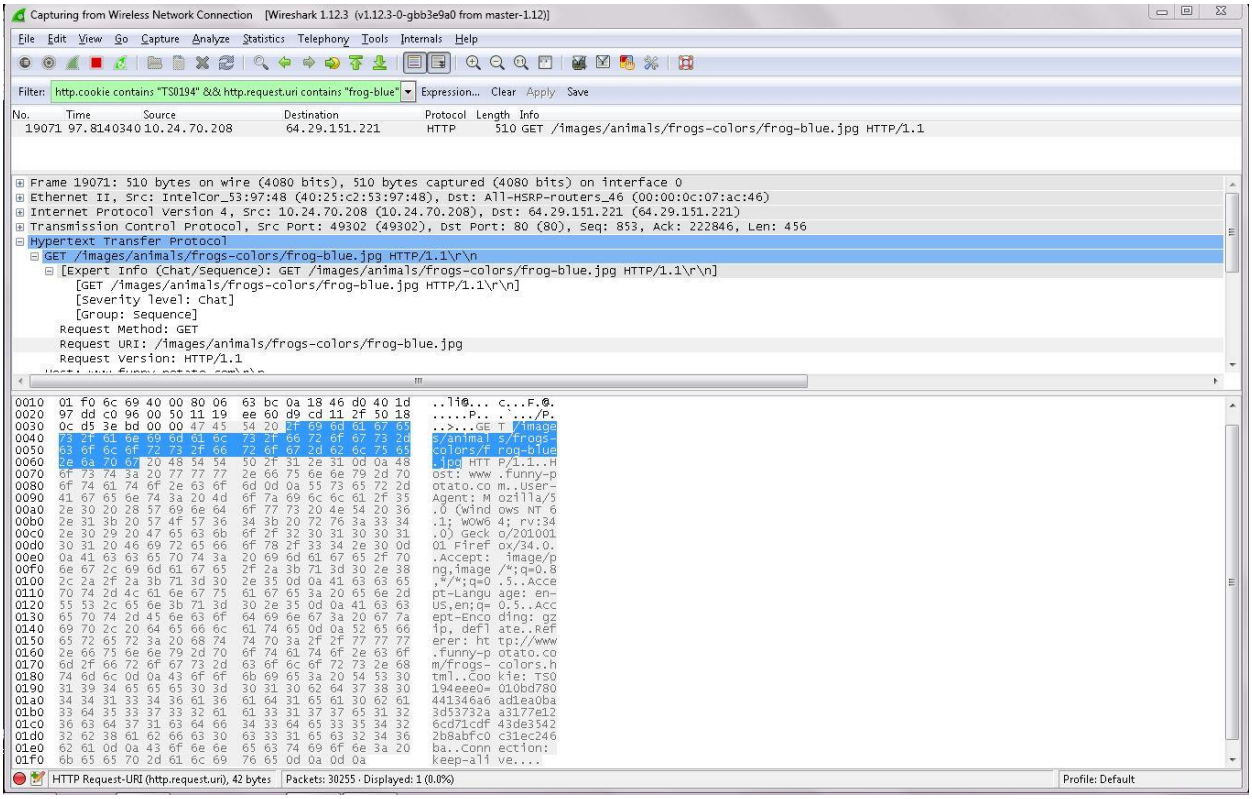
Data

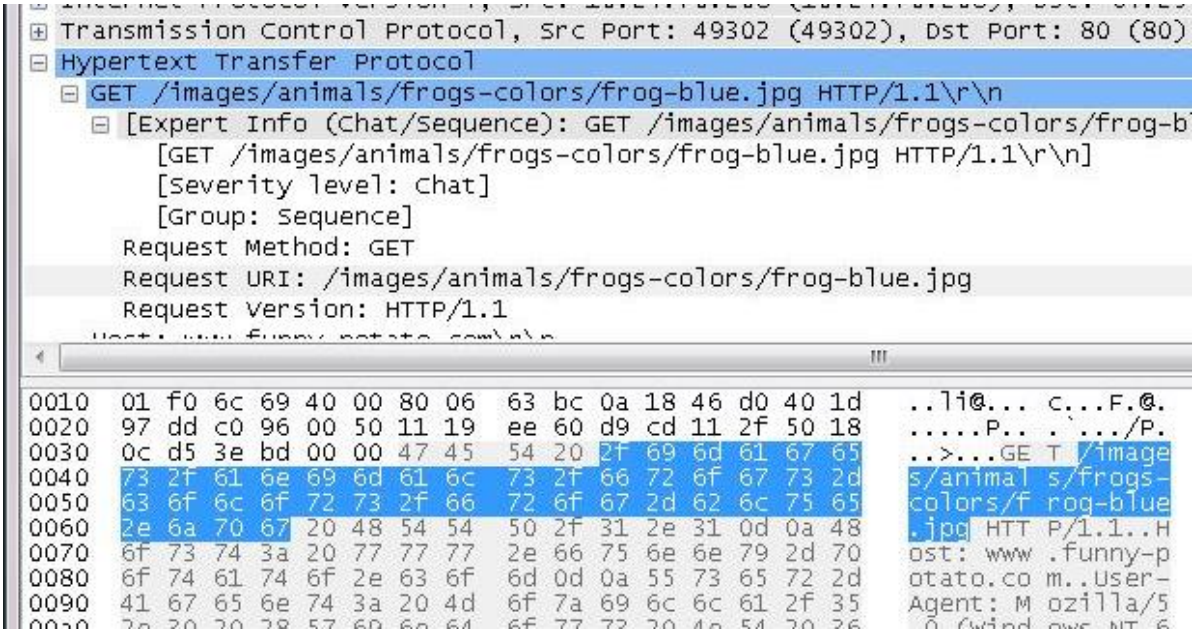
Capture #1



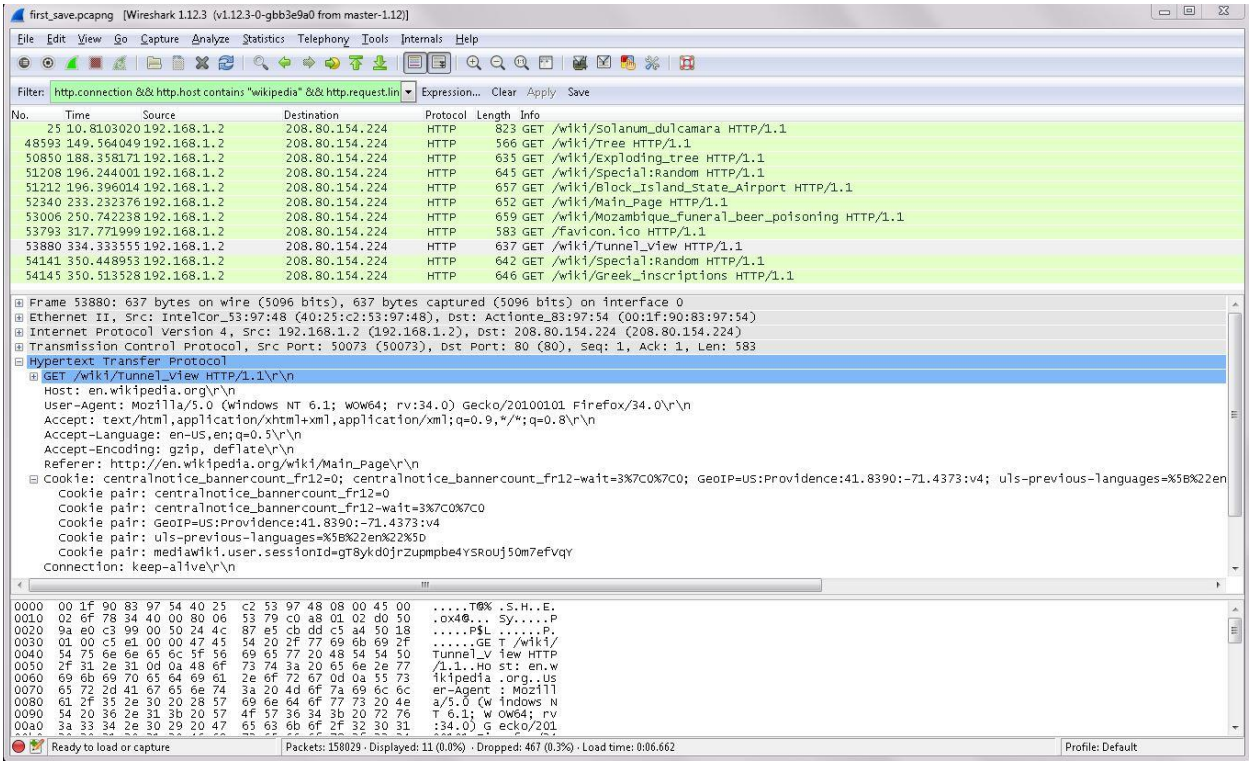


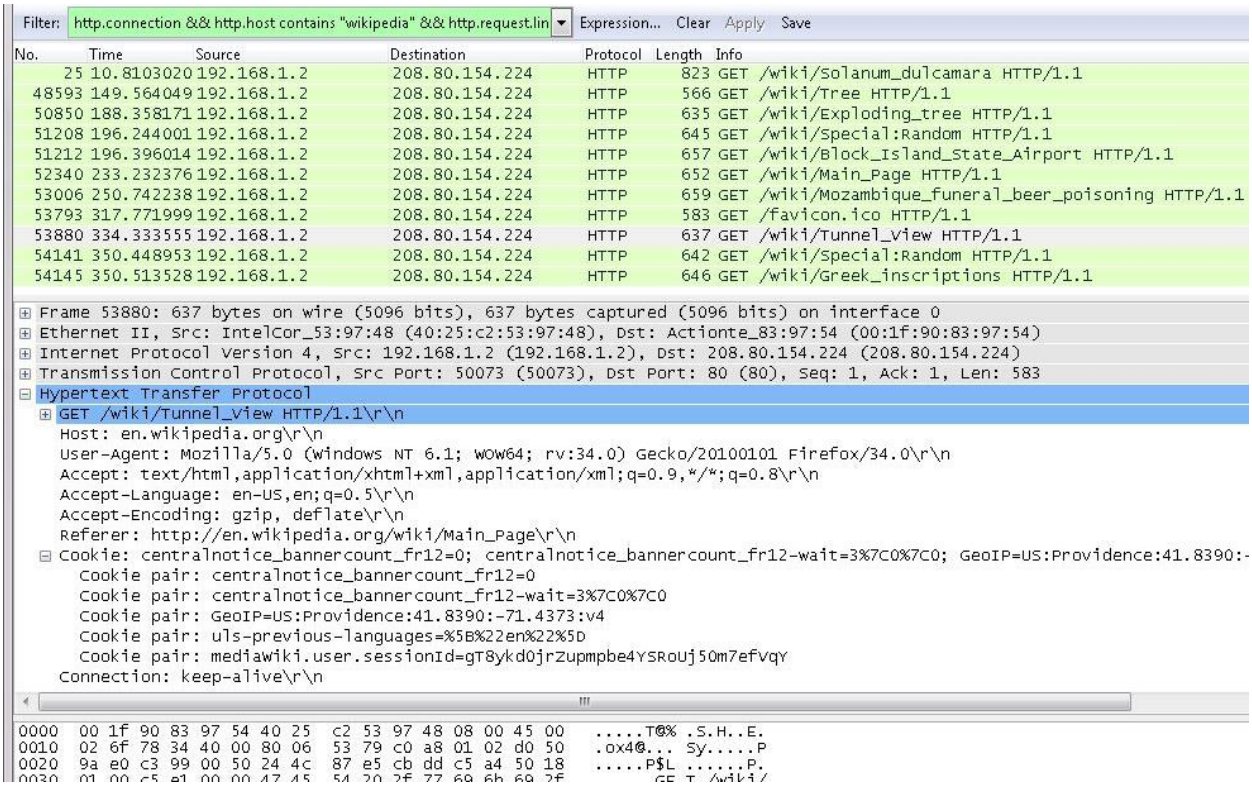
Capture #2


Capturing from Wireless Network Connection [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.cookie contains "TS0194" && http.request.uri contains "frog-blue"
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
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
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 18 .....P.. .`.../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

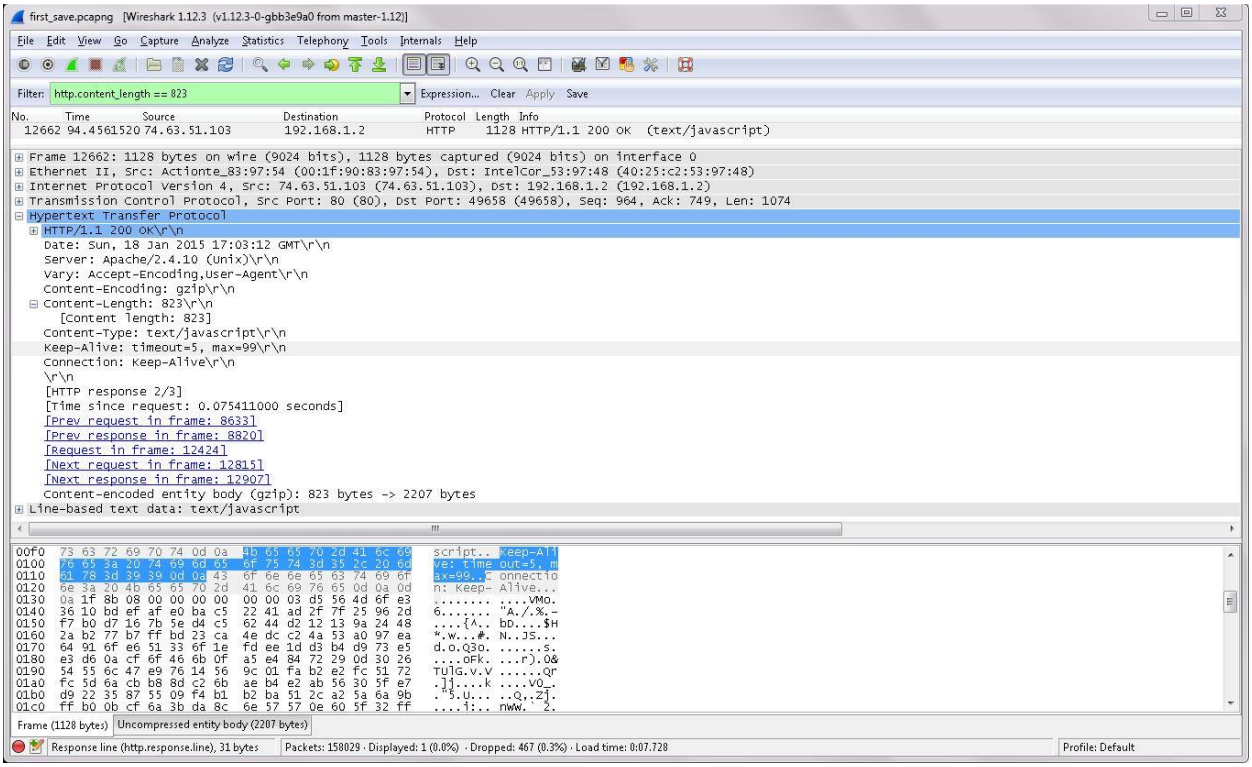
Capture #3

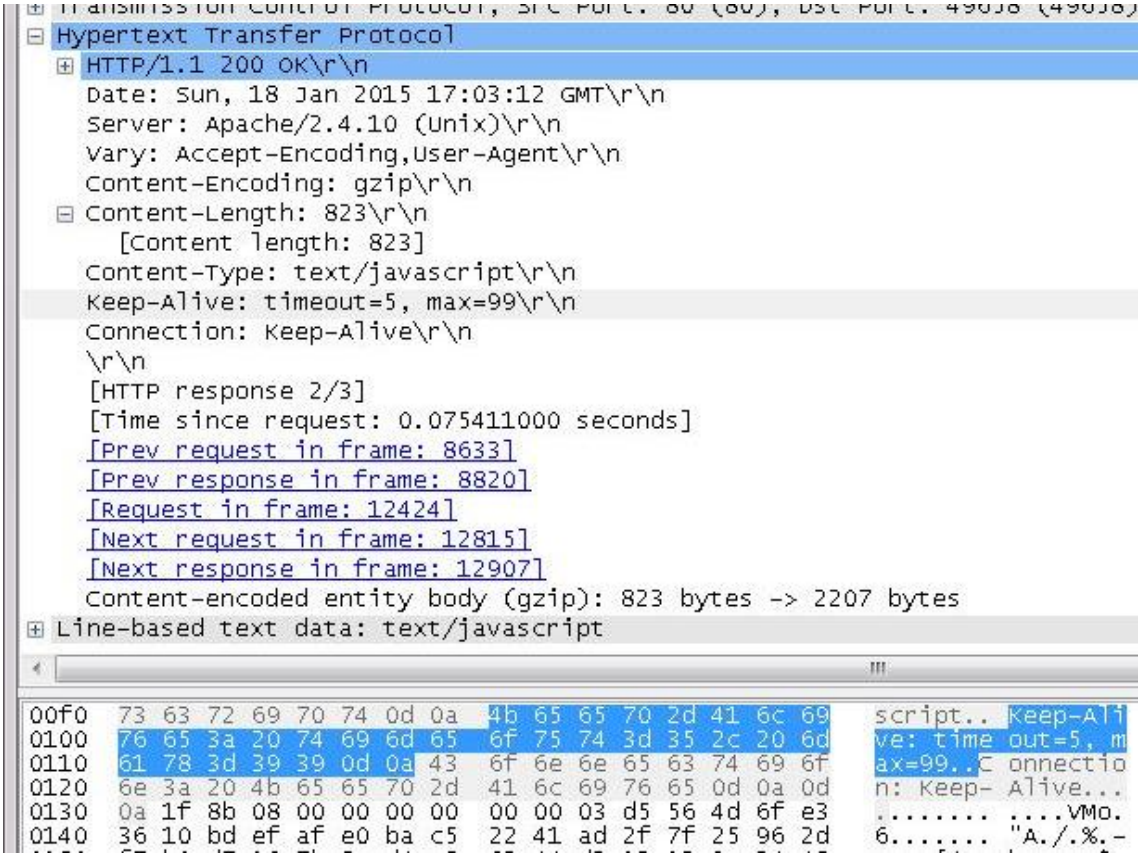




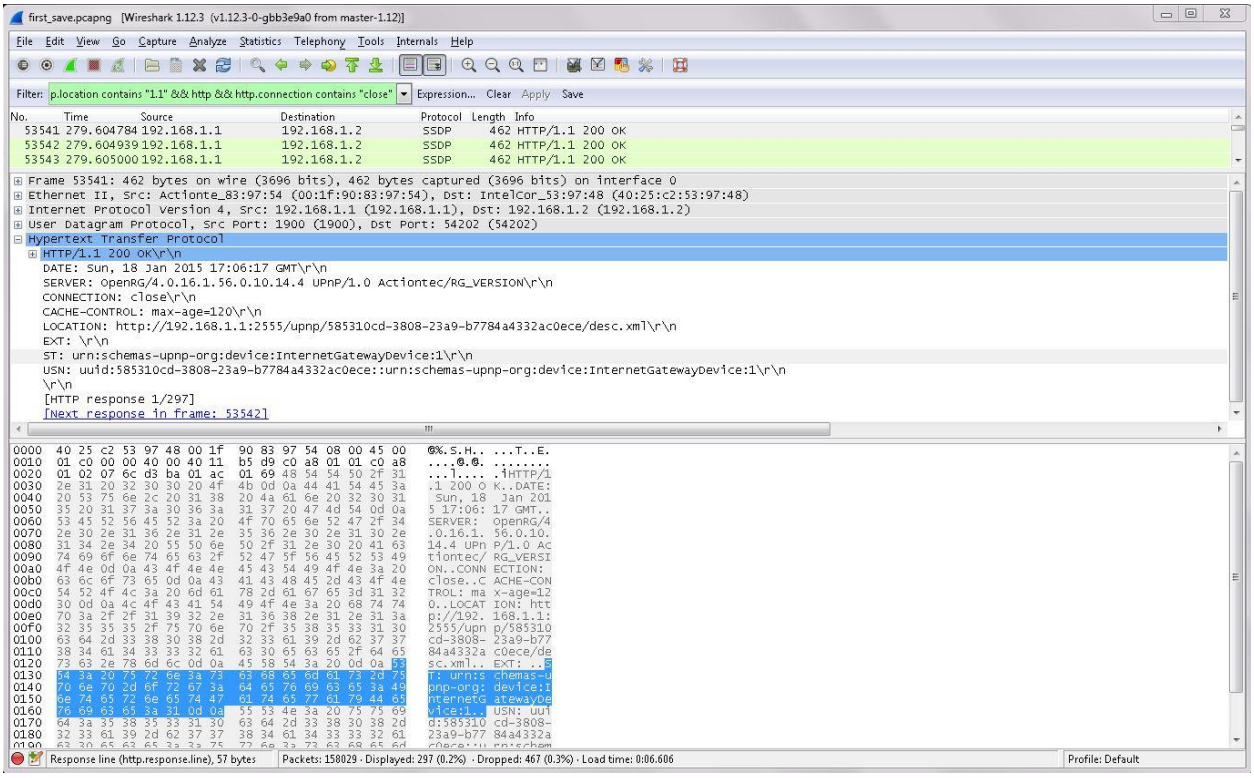
*I was unable to filter this down to one packet, and no text seemed to be highlighted along the bottom for this selection.

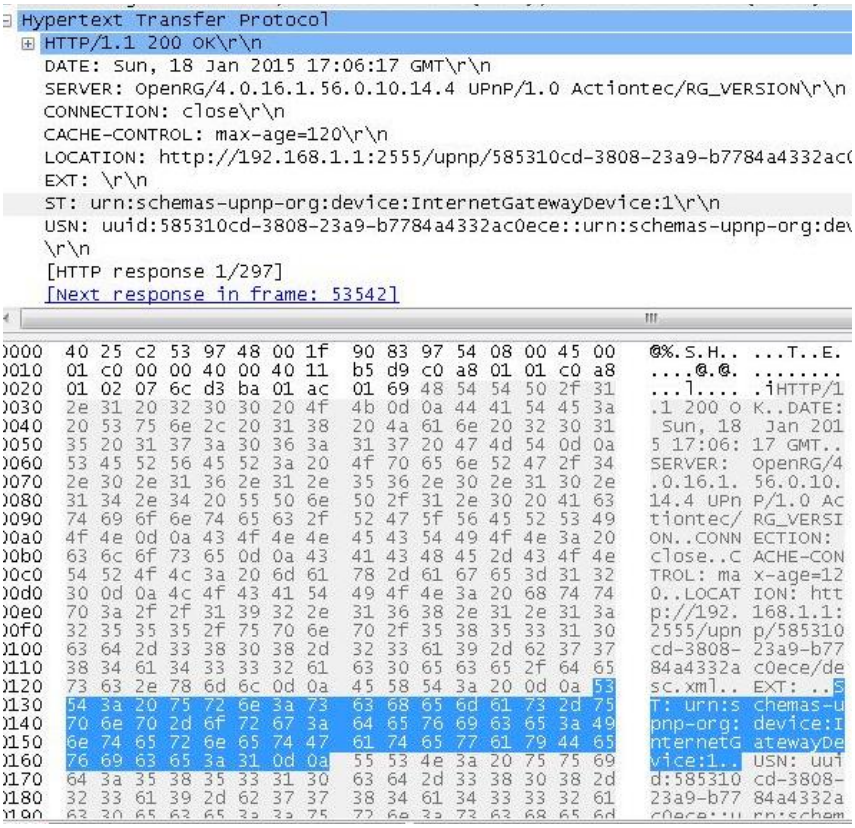
Capture #4


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-Ali
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./.%.-
0150 f7 b0 d7 16 7b 5e d4 c5 62 44 d2 12 13 9a 24 48 ....{^.. bD....$H
0160 2a b2 77 b7 ff bd 23 ca 4e dc c2 4a 53 a0 97 ea *.w...#. N..JS...
0170 64 91 6f e6 51 33 6f 1e fd ee 1d d3 b4 d9 73 e5 d.o.Q3o. ......s.
0180 e3 d6 0a cf 6f 46 6b 0f a5 e4 84 72 29 0d 30 26 ....oFk. ...r).0&
0190 54 55 6c 47 e9 76 14 56 9c 01 fa b2 e2 fc 51 72 TUlG.v.V ......Qr
01a0 fc 5d 6a cb b8 8d c2 6b ae b4 e2 ab 56 30 5f e7 .]j....k ....V0_.
01b0 d9 22 35 87 55 09 f4 b1 b2 ba 51 2c a2 5a 6a 9b .^5.U... ..Q,.Zj.
01c0 ff b0 0b cf 6a 3b da 8c 6e 57 57 0e 60 5f 32 ff ....j;.. nWW.`_2.
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

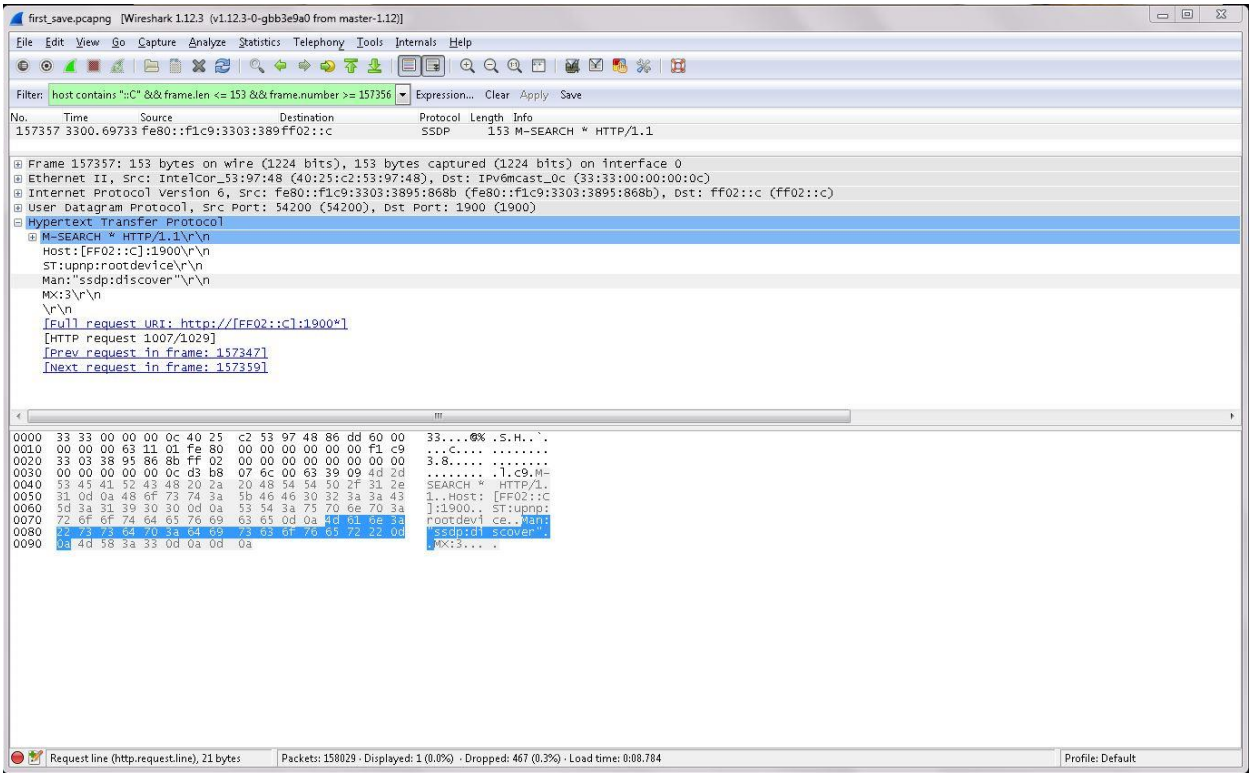

Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 18 Jan 2015 17:03:12 GMT\r\n
Server: Apache/2.4.10 (Unix)\r\n
Vary: Accept-Encoding,User-Agent\r\n
Content-Encoding: gzip\r\n
Content-Length: 823\r\n
[Content length: 823]
Content-Type: text/javascript\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: 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-Ali
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./.%.-

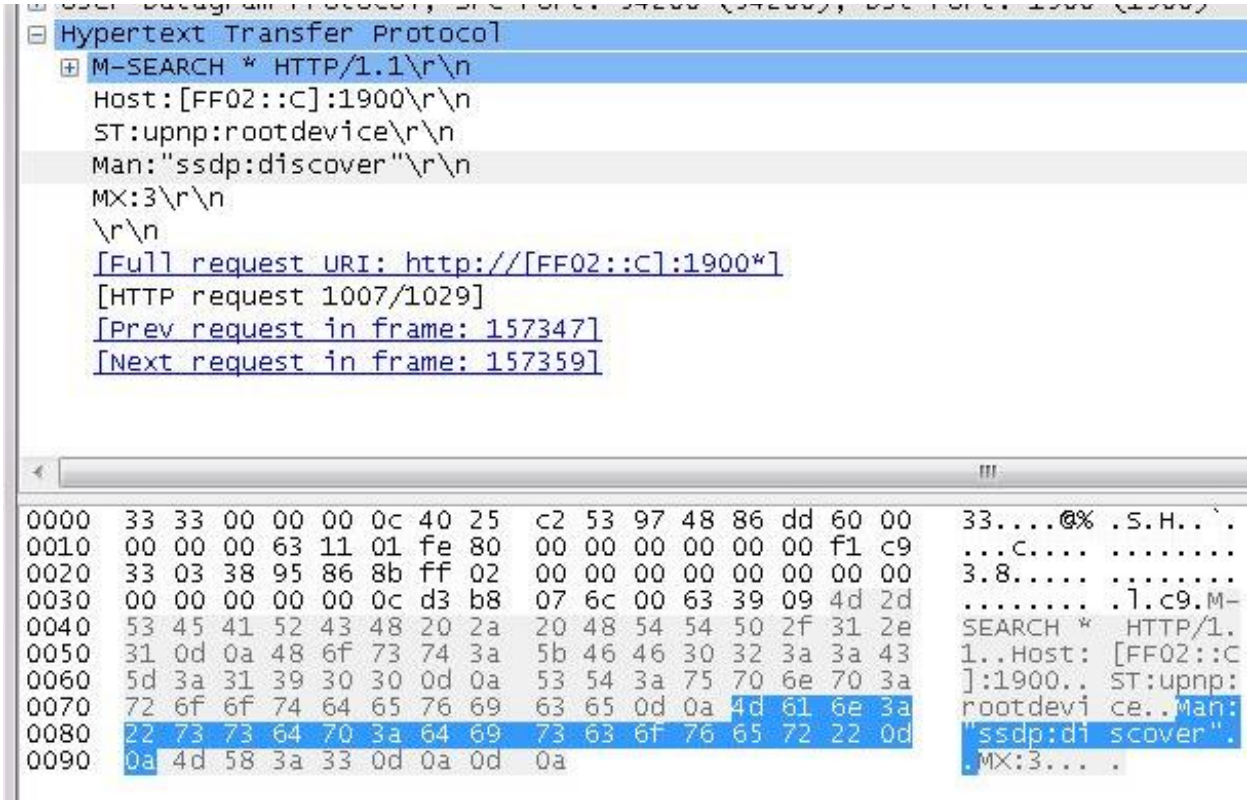
Capture #5


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: p.location contains "1.1" && http && http.connection contains "close"
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: 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: 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
DATE: Sun, 18 Jan 2015 17:06:17 GMT\r\n
SERVER: OpenRG/4.0.16.1.56.0.10.14.4 UPnP/1.0 Actiontec/RG_VERSION\r\n
CONNECTION: close\r\n
CACHE-CONTROL: max-age=120\r\n
LOCATION: http://192.168.1.1:2555/upnp/585310cd-3808-23a9-b7784a4332ac0ece/desc.xml\r\n
EXT: \r\n
ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
USN: 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: 0:06.606
Profile: Default

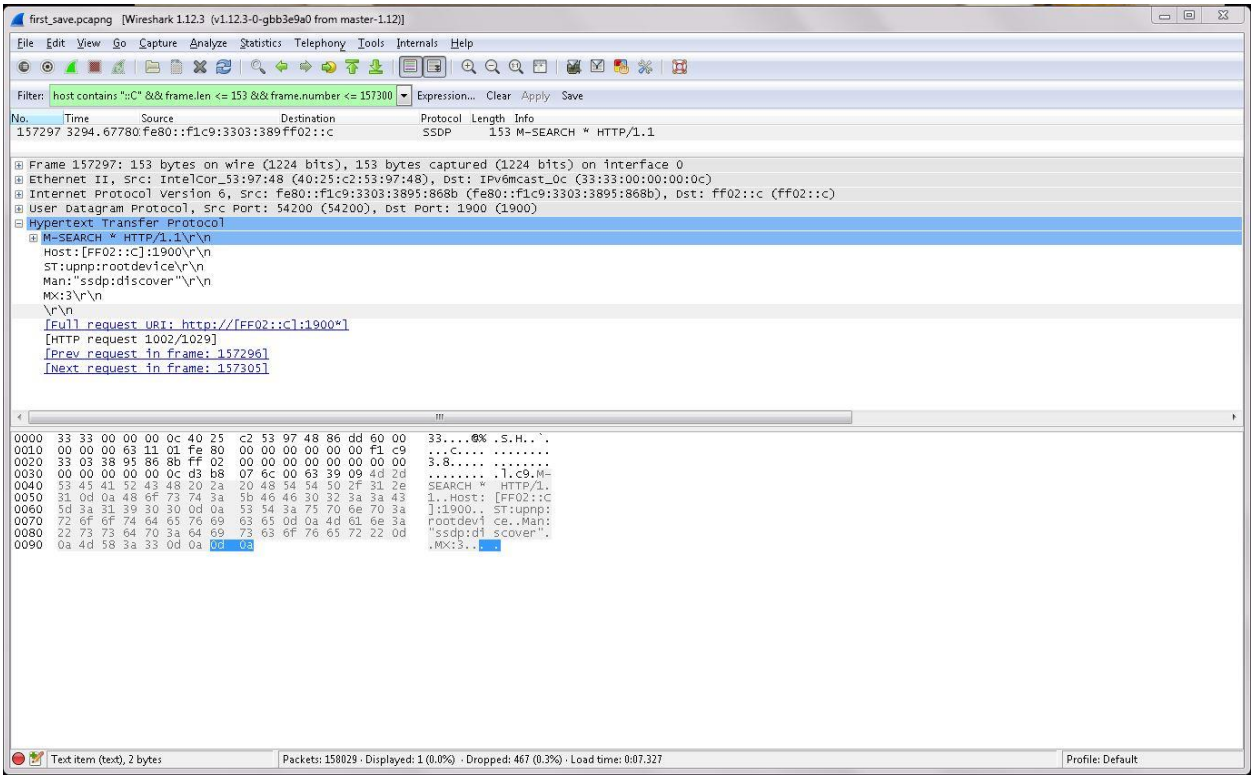

Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
DATE: Sun, 18 Jan 2015 17:06:17 GMT\r\n
SERVER: OpenRG/4.0.16.1.56.0.10.14.4 UPnP/1.0 Actiontec/RG_VERSION\r\n
CONNECTION: close\r\n
CACHE-CONTROL: max-age=120\r\n
LOCATION: http://192.168.1.1:2555/upnp/585310cd-3808-23a9-b7784a4332ac0
EXT: \r\n
ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
USN: uuid:585310cd-3808-23a9-b7784a4332ac0ece::urn:schemas-upnp-org:dev
\r\n
[HTTP response 1/297]
[Next response in frame: 53542]

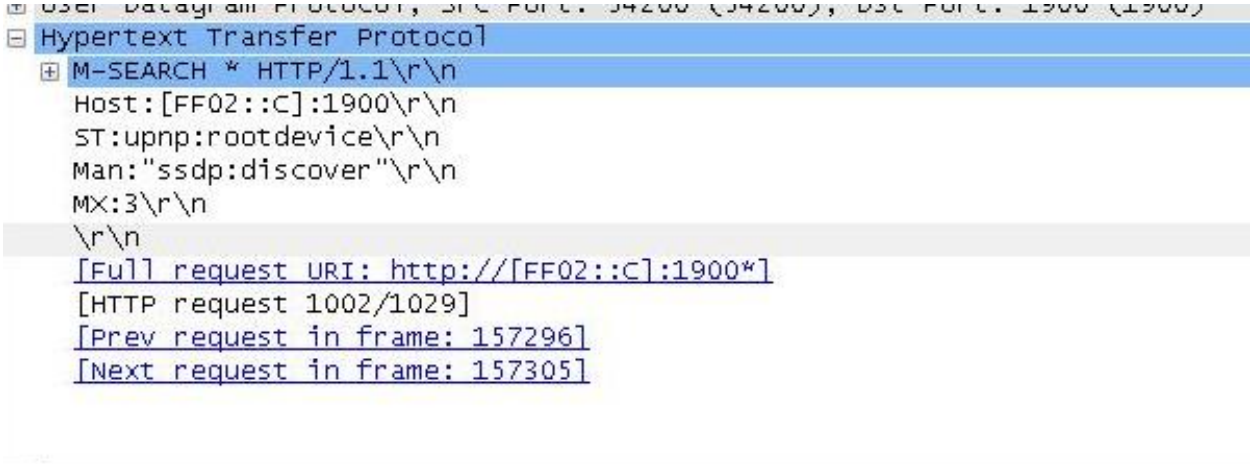
Capture #6

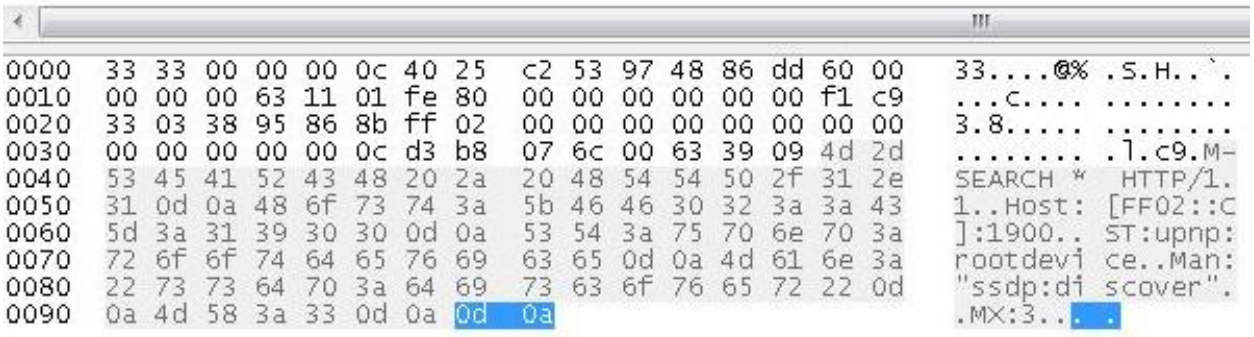

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: host contains "::C" && frame.len <= 153 && frame.number >= 157356
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
157357 3300.69733 fe80::f1c9:3303:389 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 f1 c9 ...c.... ....
0020 33 03 38 95 86 8b ff 02 00 00 00 00 00 00 00 0c 3.8..... ....
0030 00 00 00 00 00 0c d3 b8 07 6c 00 63 39 09 4d 2d l.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.request.line), 21 bytes
Packets: 158029 · Displayed: 1 (0.0%) · Dropped: 467 (0.3%) · Load time: 0:08.784
Profile: Default


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 f1 c9 ...c.... ....
0020 33 03 38 95 86 8b ff 02 00 00 00 00 00 00 00 0c 3.8..... ....
0030 00 00 00 00 00 0c d3 b8 07 6c 00 63 39 09 4d 2d l.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... .

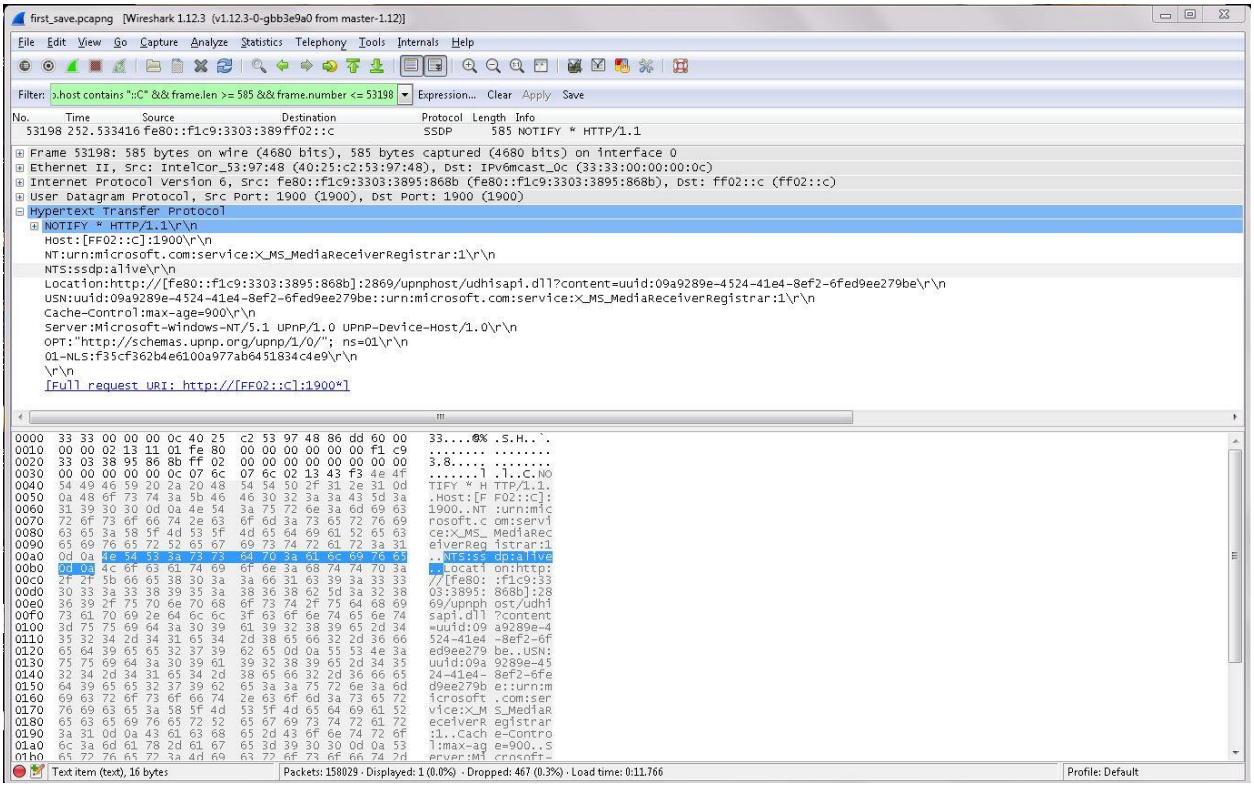
Capture #7

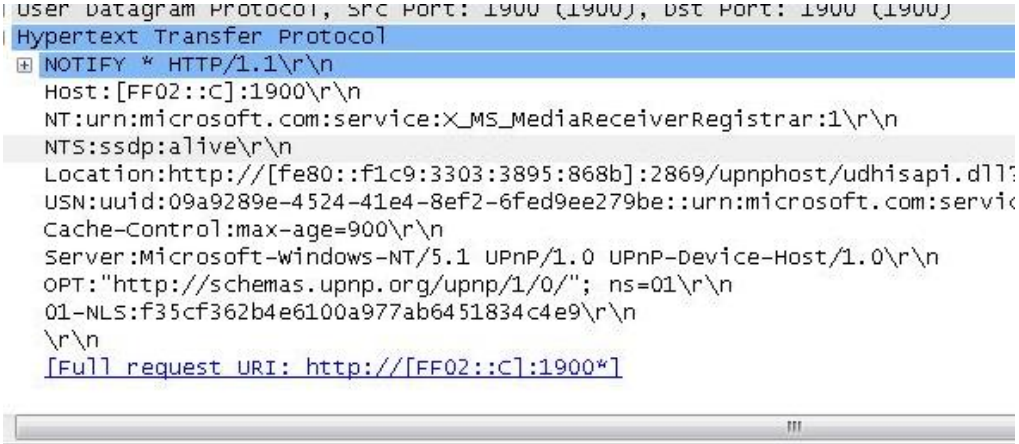

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: host contains "::C" && frame.len <= 153 && frame.number <= 157300
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
157297 3294.67780 fe80::f1c9:3303:389 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 2d l.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

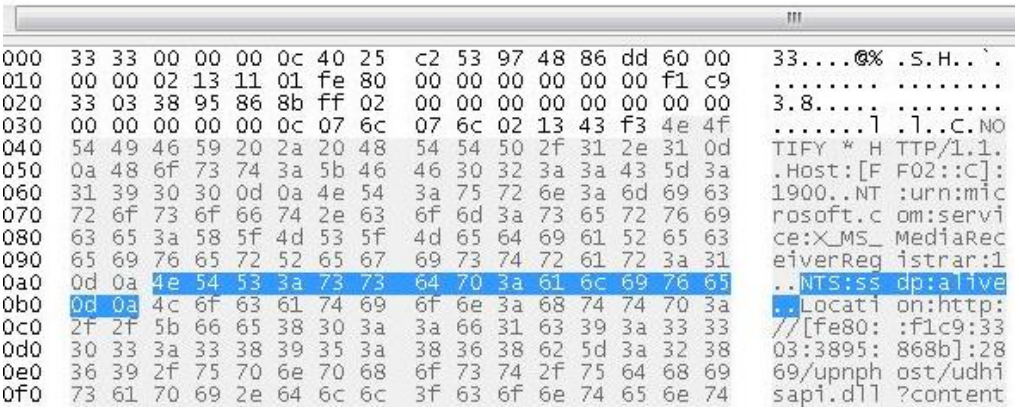

Hypertext Transfer Protocol
M-SEARCH * HTTP/1.1\r\n
Host:[FF02::C]:1900\r\n
ST:upnp:rootdevice\r\n
Man:"ssdp:discover"\r\n
MX:3\r\n
\r\n
[Full request URI: http://[FF02::C]:1900*]
[HTTP request 1002/1029]
[Prev request in frame: 157296]
[Next request in frame: 157305]


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 2d l.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.. .

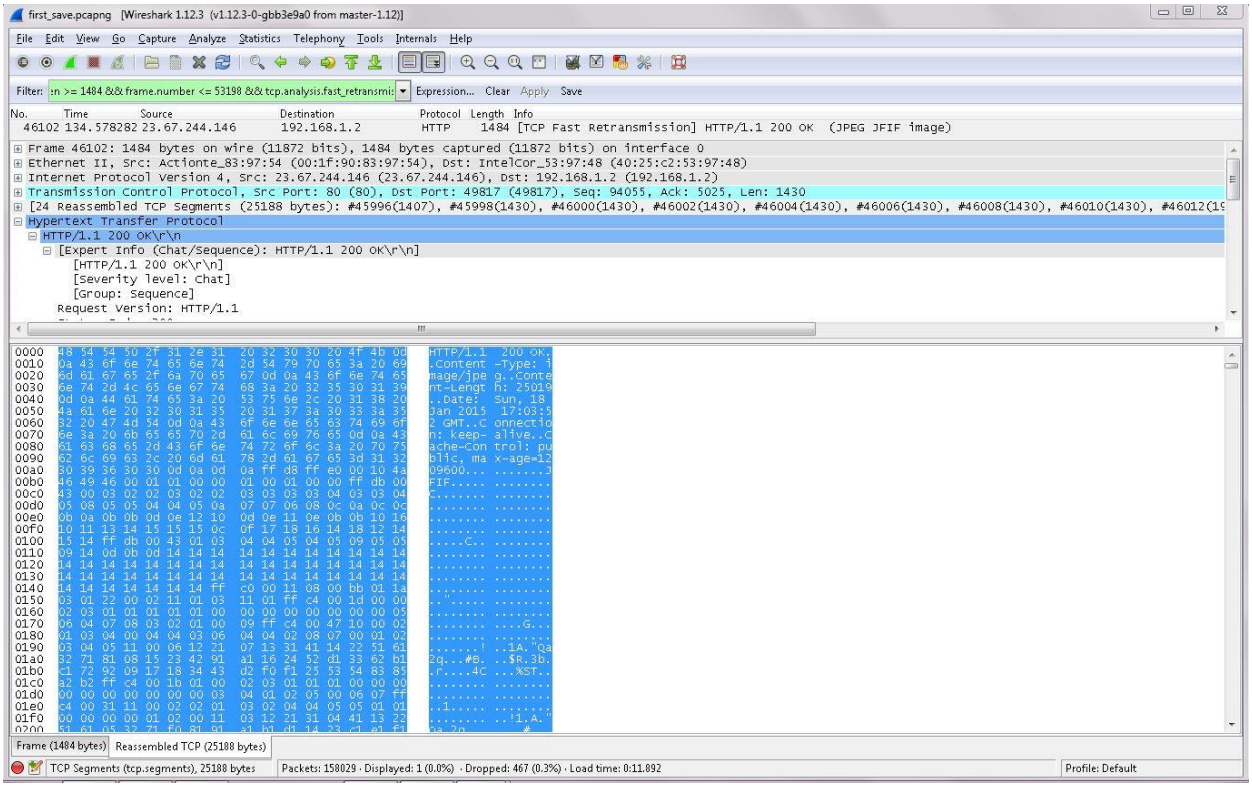
Capture #8

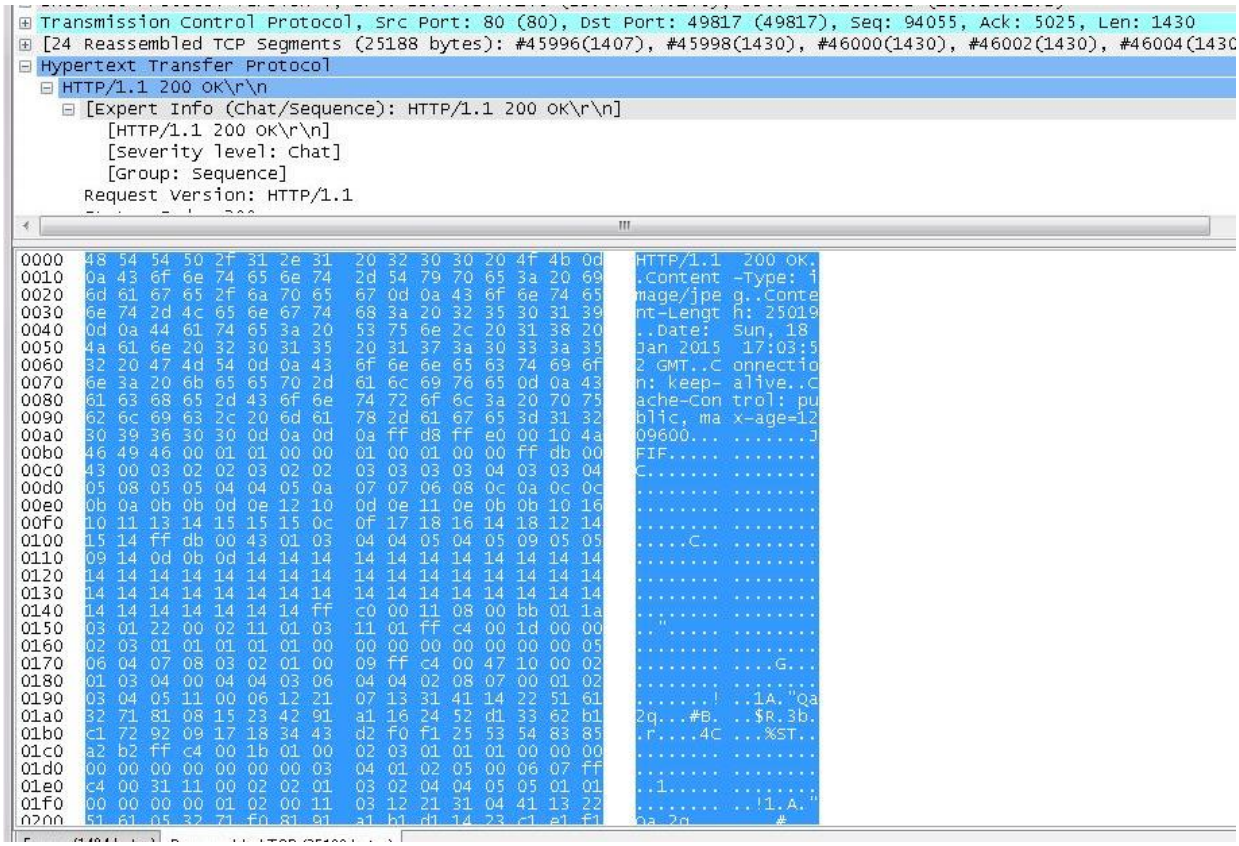

first_save.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:).host contains "::C" && frame.len >= 585 && frame.number <= 53198 Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
53198 252.533416 fe80::f1c9:3303:389 ff02::c SSDP 585 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
\r\n
[Full request URI: 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:servic
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*]

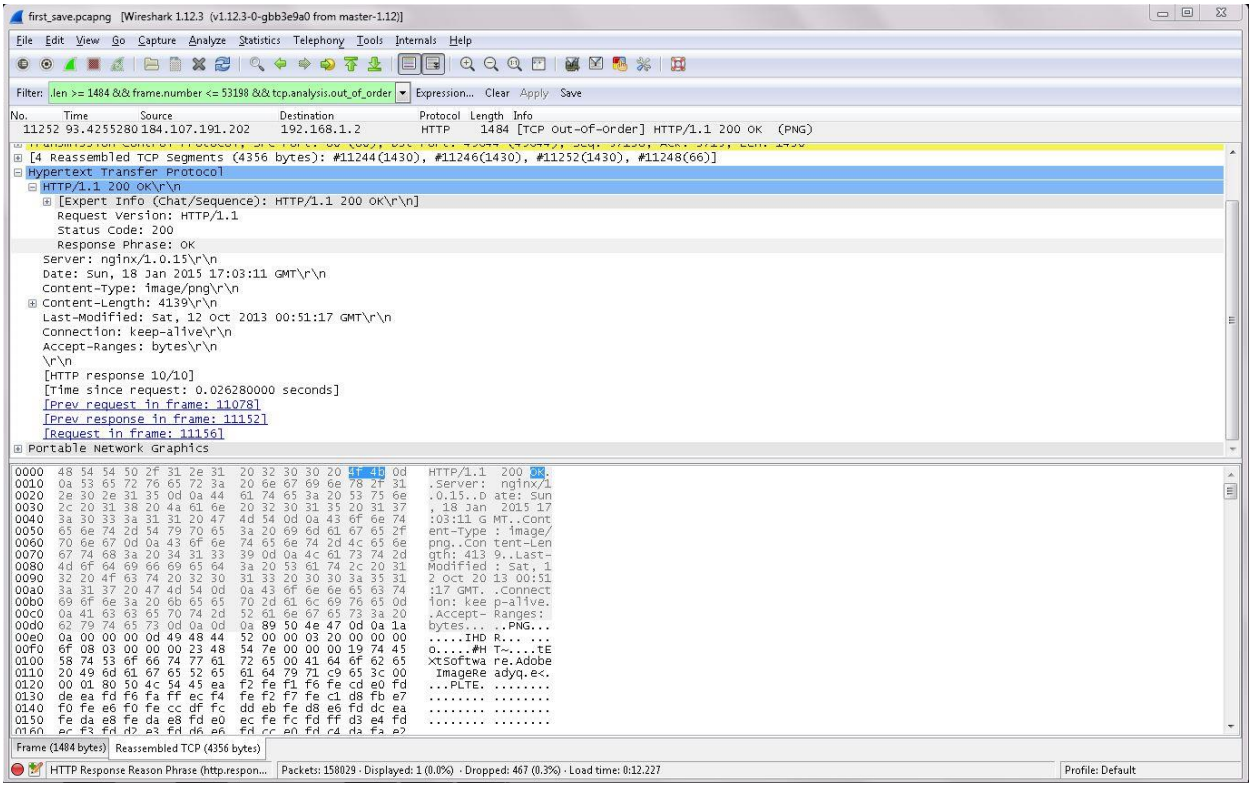

000 33 33 00 00 00 0c 40 25 c2 53 97 48 86 dd 60 00 33....@% .S.H..`.
010 00 00 02 13 11 01 fe 80 00 00 00 00 00 00 f1 c9 ....
020 33 03 38 95 86 8b ff 02 00 00 00 00 00 00 00 0c 3.8..... ....
030 00 00 00 00 00 00 0c 07 6c 07 6c 02 13 43 f3 4e 4f .... l.l..C.NO
040 54 49 46 59 20 2a 20 48 54 54 50 2f 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

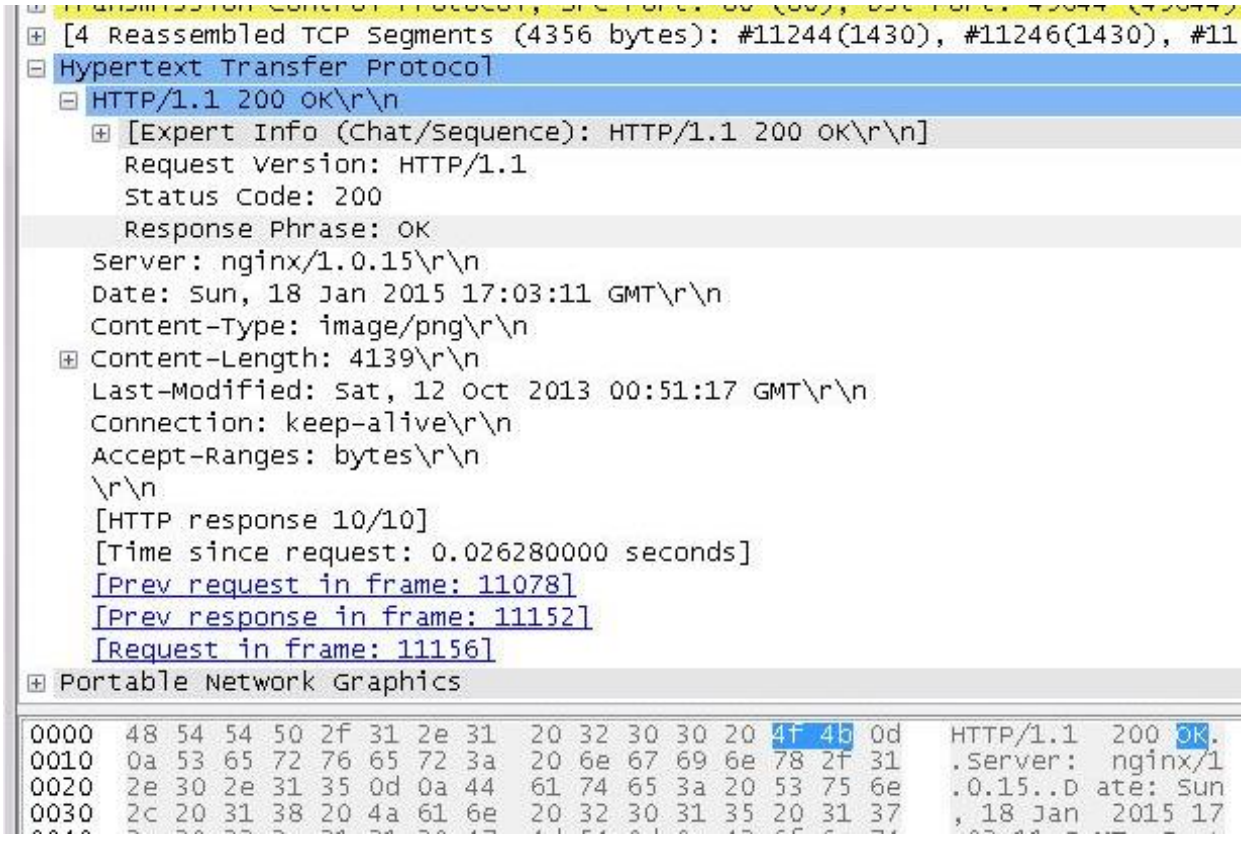
Capture #9


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: :n >= 1484 && frame.number <= 53198 && tcp.analysis.fast_retransmi: 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: 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: 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: 94055, 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(1
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
Frame (1484 bytes)
Reassembled TCP (25188 bytes)
TCP Segments (tcp.segments), 25188 bytes
Packets: 158029 · Displayed: 1 (0.0%) · Dropped: 467 (0.3%) · Load time: 0:11.892
Profile: Default


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

Capture #10


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: .len >= 1484 && frame.number <= 53198 && tcp.analysis.out_of_order
Expression... Clear Apply Save
No. 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)]
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 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 2d 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 30 31 33 20 30 30 3a 35 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 65 73 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 00 .....IHD 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 ImageRe adyq.e<.
0120 00 01 80 50 4c 54 45 ea f2 fe f1 f6 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 e6 fd dc ea ....
0150 fe da e8 fe da e8 fd e0 ec fe fc fd ff d3 e4 fd ....
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: 0:12.227
Profile: Default


[4 Reassembled TCP Segments (4356 bytes): #11244(1430), #11246(1430), #11
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 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

Analysis

Filtering:

Capture #1

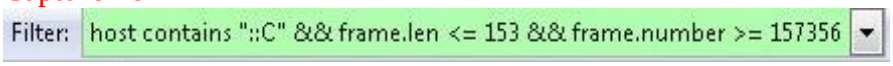
This was an attempt to filter by the name of a website I had visited. I reduced it by filtering for 'POST,' which appeared in the info section.

This resulted in this one packet.

Capture #3

This was an attempt to filer 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.

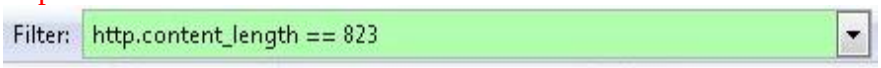
Capture #6



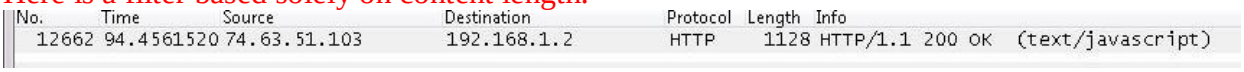
This is another search based upon the host site, this time also filtered by frame length. This was not specific enough, so an exact frame number was chosen and filtered for, as well.

This one packet resulted.

Capture #4



Here is a filter based solely on content length.



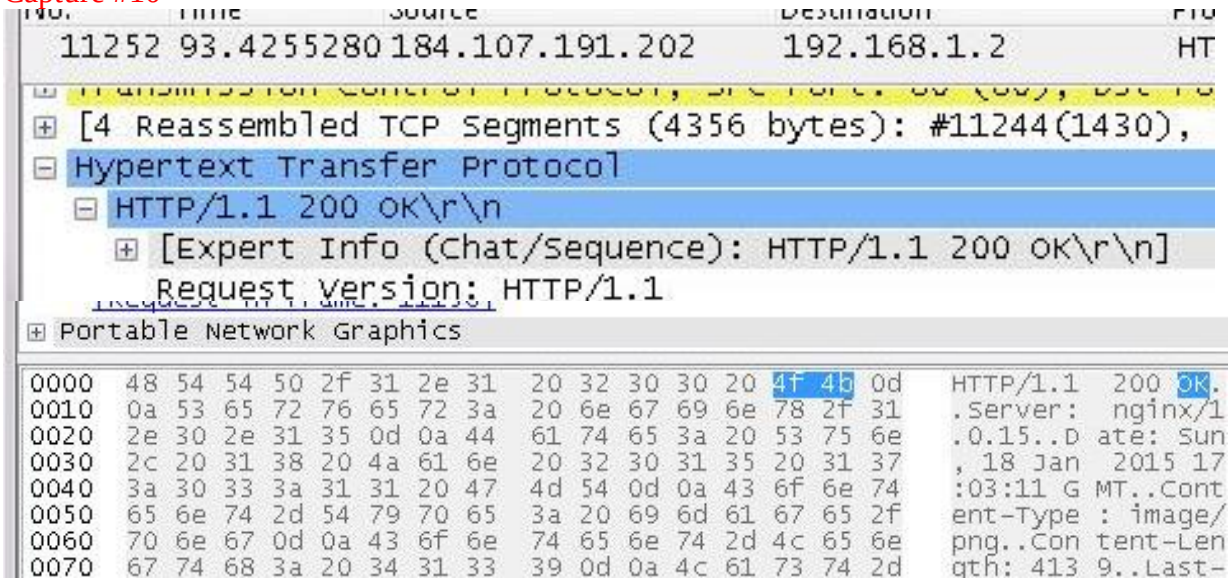
This is the packet that resulted from the filtering.

Data Correlations:

Capture #9

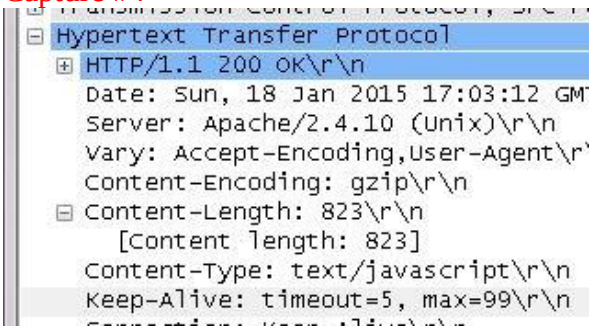
This is a large packet that has been reassembled from 24 TCP segments. Selecting 'HTTP/1.1 200 OK\r\n' under 'Hypertext Transfer Protocol' has highlighted all of the data. This means that HTTP/1.1 200 OK \r\n must reference the entire packet.

Capture #10

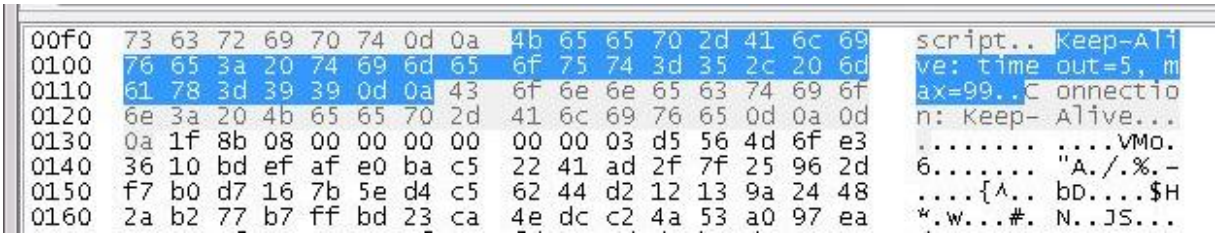


Selecting '[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]' under the two headings listed for Capture #9 resulted in a very short segment of data being highlighted. Only 'OK' and the matching hexadecimal code, '4f 4B' were a part of this data.

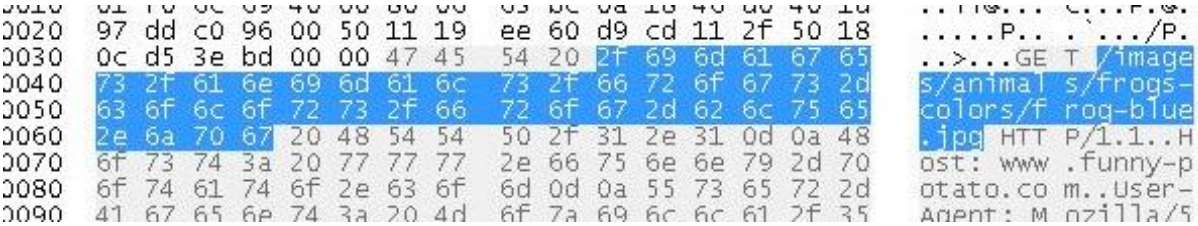
Capture #4



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.

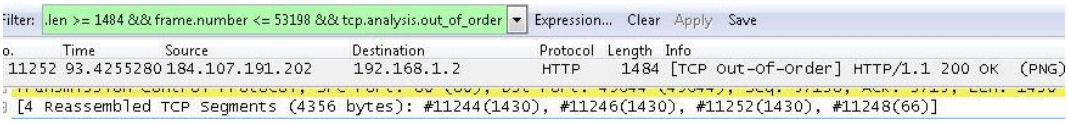
Discussion & Questions

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.



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.