

Abdullah Alrfeedi

Lab #1

## 1) What is the Internet address of your computer?

The IP Address is 10.8.21.29.

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows a packet from 10.8.21.29 to 128.119.245.12. The packet details pane shows the following information:

- Frame 2699: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
- Interface id: 0 (\Device\NPF\_{3178888F-E42D-487E-9735-DC81D5A65808})
- Encapsulation type: Ethernet (1)
- Arrival Time: Mar 6, 2019 19:27:05.471757000 Eastern Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1551918425.471757000 seconds
- [Time delta from previous captured frame: 0.000288000 seconds]
- [Time delta from previous displayed frame: 0.015508000 seconds]
- [Time since reference or first frame: 0.634926000 seconds]
- Frame Number: 2699
- Frame Length: 492 bytes (3936 bits)
- Capture Length: 492 bytes (3936 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: ethertype:ip:tcp:data-text-lines]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: Cisco 59:ec:bf:00:2c:c8:59:ec:bf, Dst: Dell 17:44:3d:14:b3:1f:17:44:3d

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and HTTP GET request.

2) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

The three different protocols that appear in the packet listing are ARP, SSDP, AND TCP.

The screenshot displays the Wireshark interface for a 'Local Area Connection'. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
3117	16.794711	10.8.21.29	34.214.20.242	TCP	55	[TCP Keep-Alive] 50702 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1
3118	16.794730	10.8.21.29	34.214.20.242	TCP	55	[TCP Keep-Alive] 50701 → 443 [ACK] Seq=1 Ack=1 Win=64140 Len=1
3119	16.890656	34.214.20.242	10.8.21.29	TCP	66	[TCP Keep-Alive ACK] 443 → 50702 [ACK] Seq=1 Ack=2 Win=116 Len=0 SLE=1 SRE=2
3120	16.891767	Cisco:82:d2:a7	PVST+	STP	64	Conf. Root = 32768/808/00:2c:c8:59:ec:00 Cost = 0 Port = 0x8100
3121	16.893221	34.214.20.242	10.8.21.29	TCP	60	[TCP Keep-Alive ACK] 443 → 50701 [ACK] Seq=1 Ack=2 Win=20710 Len=0
3122	16.903113	Cisco:82:d2:a7	PVST+	STP	64	Conf. Root = 32768/820/00:2c:c8:59:ec:00 Cost = 0 Port = 0x8100
3123	16.915568	SamsungE_81:ab:77	Broadcast	ARP	60	Who has 10.8.20.1? Tell 10.8.21.18
3124	16.918147	SamsungE_81:ab:85	Broadcast	ARP	60	Who has 10.8.20.1? Tell 10.8.21.193
3125	16.931804	SamsungE_38:09:32	Broadcast	ARP	60	Who has 10.8.20.1? Tell 10.8.21.175
3126	16.996340	10.8.20.128	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3127	17.274835	Dell_16:3f:81	Broadcast	ARP	60	Who has 10.8.20.243? Tell 10.8.20.162
3128	17.440897	fe80::947b:3c4f:494...	ff02::1:ffae:e214	ICMPv6	86	Neighbor Solicitation for fe80::26be:5fff:feae:e214 from 44:8a:5b:55:0d:17
3129	17.727923	172.217.7.132	10.8.21.29	TCP	60	443 → 50738 [FIN, ACK] Seq=2855 Ack=611 Win=81952 Len=0
3130	17.728032	10.8.21.29	172.217.7.132	TCP	54	50738 → 443 [ACK] Seq=611 Ack=2856 Win=65792 Len=0
3131	18.000360	10.8.20.128	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3132	18.440230	fe80::947b:3c4f:494...	ff02::1:ffae:e214	ICMPv6	86	Neighbor Solicitation for fe80::26be:5fff:feae:e214 from 44:8a:5b:55:0d:17

The packet details pane for the selected packet (3132) shows the following structure:

- Frame 2682: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
- Ethernet II, Src: Dell\_17:44:3d (14:b3:1f:17:44:3d), Dst: Cisco\_59:ec:b (00:2c:c8:59:ec:b)
- Internet Protocol Version 4, Src: 10.8.21.29, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 50751, Dst Port: 80, Seq: 1, Ack: 426
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 2c 08 59 ec bf 14 b3 1f 17 44 3d 08 00 45 00  ,Y.....De:E-
0010 01 02 31 c1 40 00 00 06 00 00 0a 08 15 1d 80 77  -1@.....w
0020 5f 0c c6 3f 00 50 06 9f e4 d6 cf 12 71 7a 50 18  -?P.....qSP
0030 01 02 06 6d 00 00 47 45 54 20 2f 77 69 72 65 73  -m-GE T/wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d  hark-lab s/DNTR0
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e  vireshar k-file1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48  html HT P/1.1-H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61  ost: gai a.cs.uma
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69  ss.edu- Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a  on: keep -alive-
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65  Upgrade- Insecure
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a b5 73  -Request s: 1..0
00c0 65 72 20 41 67 65 6e 74 3a 20 40 67 7a 69 6c 6c  er-Agent: Mozilla
00d0 31 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4a  2f.5.0 (Windows N
00e0 54 20 36 2e 31 3b 20 57 69 6e 36 34 30 20 70 36  T.6.1; Win64; w
00f0 34 29 20 41 70 70 6c 65 57 65 62 40 69 74 2f 35  AppleWebKit/5
0100 33 37 2e 33 36 20 28 40 48 54 4d 4c 2c 20 6c 69  37.36 (KHTML, li
0110 6b 65 20 47 65 63 0b 6f 29 20 43 68 72 6f 6d 65  ke Gecko ) Chrome
0120 2f 37 32 2e 30 2e 33 36 32 36 2e 31 32 31 20 53  /72.0.36.26.121 S
0130 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 afari/53.7.36-Ac
```

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

The screenshot shows the Wireshark interface with a packet capture of an HTTP transaction. The packet list at the top shows two packets: a GET request (No. 2682) and a 200 OK response (No. 2699). The packet details pane for the response (No. 2699) is expanded, showing the arrival time as Mar 6, 2019 19:27:05.471757000 Eastern Standard Time. The packet bytes pane at the bottom shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
2682	8.619418	10.8.21.29	128.119.245.12	HTTP	480	GET /wireshark-labs/INTRO-wireshark-file.html HTTP/1.1
2699	8.634926	128.119.245.12	10.8.21.29	HTTP	492	HTTP/1.1 200 OK (text/html)

Arrival Time: Mar 6, 2019 19:27:05.471757000 Eastern Standard Time

Frame 2699: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0  
Interface id: 0 (Device\NPF\_{3178888F-E420-487E-9755-DCB1D5A65808})  
Ethernet II, Src: Cisco 59:ec:bf:00:2c:c8:59:ec, Dst: Dell 17:44:3d:14:b3:1f:17:44:3d

The GET request was arrived at Mar 6,2019 19:27:05.471757000

Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2682	8.619418	10.8.21.29	128.119.245.12	HTTP	480	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2699	8.634926	128.119.245.12	10.8.21.29	HTTP	492	HTTP/1.1 200 OK (text/html)
2774	9.431779	10.8.21.29	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
2775	9.447018	128.119.245.12	10.8.21.29	HTTP	538	HTTP/1.1 404 Not Found (text/html)
2893	13.412895	10.8.21.29	10.8.21.34	HTTP	997	GET /secars/secars.dll?h=519E007C1D7197EABEC0DFAF8A5608A38042EC88330762F9FA184ED349A431C76C0FAF83BCESB2CC6DEF0482D2FAB4F3F1C4765B910A1ABF9CDE25AB46C730FBF38574F476786833AFDF1568A58CB98749EE2...
2988	13.414585	10.2.1.34	10.8.21.29	HTTP	1042	HTTP/1.1 200 OK (text/html)
2989	13.414585	10.8.21.29	10.2.1.34	HTTP	953	HEAD /secars/secars.dll?h=9030171967CC0880C43FD5051EDE895738042EC88330762F9FA184ED349A431C76C0FAF83BCESB2CC6DEF0482D2FAB4F3F1C4765B910A1ABF9CDE25AB46C730FBF38574F476786833AFDF1568A58CB98749EE2...
2993	13.567867	10.2.1.34	10.8.21.29	HTTP	242	HTTP/1.1 400 Bad Request
2915	13.044277	10.8.21.29	10.2.1.34	HTTP	394	POST /secars/secars.dll?h=7A7D48823E3395E77D242E488194870D5C0DCA4D10290C907158132931379F43964CAE928D00E63C41B92828D850FFD083E8F9C1ABCE59907270B541F98C41B84AC62D73D68390FCACD68C11C06D81238C5...
2917	13.050747	10.2.1.34	10.8.21.29	HTTP	255	HTTP/1.1 200 OK
2923	13.938423	10.8.21.29	10.2.1.34	HTTP	729	POST /secars/secars.dll?h=4971A0ABE32F83C58D1698279928157452C8CA4D18290C907158132931379F43964CAE928D00E63C41B92828D850FFD083E8F9C1ABCE59907270B541F98C41B84AC62D73D68390FCACD68C11C06D81238C5...
2925	13.945234	10.2.1.34	10.8.21.29	HTTP	255	HTTP/1.1 200 OK

Frame 2682: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0  
 Interface id: 0 (Device\NPF\_{3378888F-482E-487E-9355-0C81D5A658D8})  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 6, 2019 19:27:05.456249000 Eastern Standard Time  
 Epoch Time: 1551918425.456249000 seconds  
 Time delta from previous captured frame: 0.000018000 seconds  
 Time delta from previous displayed frame: 0.000000000 seconds  
 Time since reference or first frame: 8.619418000 seconds  
 Frame Number: 2682  
 Frame Length: 480 bytes (3840 bits)  
 Capture Length: 480 bytes (3840 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: ethertype:ip:tcp:http]  
 [Coloring Rule Name: HTTP]  
 [Coloring Rule String: http || tcp.port == 80 || http2]  
 Ethernet II, Src: Dell 17:44:3d (14:b3:1f:17:44:3d), Dst: Cisco 59:ec:b3 (00:21:c1:59:ec:b3)

0000 00 2c 59 ec bf 14 b3 1f 17 44 3d 00 00 45 00 .Y.....D...E-  
 0010 01 d2 31 c1 40 00 00 06 00 00 0a 08 15 1d 80 77 ..1@.....w  
 0020 f5 0c c6 3f 00 50 80 9f a4 06 cf 12 71 7a 50 18 ...?P....qsp  
 0030 01 02 96 6d 00 00 47 45 54 20 2f 7f 69 72 65 73 ...m GE T /wires  
 0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-  
 0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.  
 0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HT P/1.1 H  
 0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.una  
 0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu+ Connecti  
 0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive-  
 00a0 55 70 67 72 61 64 65 10 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
 00b0 10 49 6e 73 65 63 75 72 65 10 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
 00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill  
 00d0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N  
 00e0 54 20 36 2e 31 3b 20 57 69 6e 36 34 3b 20 78 36 T 6.1; W in64; x6  
 00f0 34 20 20 41 70 70 6c 65 57 65 62 40 69 74 2f 35 4) Apple WebKit/S  
 0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37 36 (K HTML, 11  
 0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko ) Chrome  
 0120 2f 37 32 2e 30 2e 33 36 32 36 2e 31 32 31 20 53 /72.0.36.26.121.5  
 0130 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 afari/53 7.36 -Ac

Packets: 3170 · Displayed: 12 (0.4%) · Dropped: 0 (0.0%) Profile: Default

The HTTP OK is arrived at Mar 6, 2019 19:27:05.456249000

So the time took from HTTP GET TO HTTP OK is .456249000 - .471757000 = 0.015508

#### 4) What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?

The Internet Address of gaia.cs.umass.edu is 128.119.245.12

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows a packet from 10.8.21.29 to 128.119.245.12. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the packet.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
2682	8.619418	10.8.21.29	128.119.245.12	HTTP	480	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2699	8.634826	128.119.245.12	10.8.21.29	HTTP	492	HTTP/1.1 200 OK (text/html)
2774	9.431779	10.8.21.29	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
2775	9.447018	128.119.245.12	10.8.21.29	HTTP	538	HTTP/1.1 404 Not Found (text/html)
2893	13.412895	10.8.21.29	10.2.1.34	HTTP	997	GET /secars/secars.dll?h=519E0807C1D7197EAECD01DFA8A5680A3B042EC88330762F9FA184ED349A431C76C8FAF838CE582CC6DEF048202FA94F3F1C47658918A18B9CDE25A846C730FBF38574F476786833AFDF1568A58CB98749EE2...
2898	13.414595	10.2.1.34	10.8.21.29	HTTP	1042	HTTP/1.1 200 OK (text/html)
2902	13.566817	10.8.21.29	10.2.1.34	HTTP	953	HEAD /secars/secars.dll?h=903D17967CC088DC43FD05E1EDE895738042EC88330762F9FA184ED349A431C76C8FAF838CE582CC6DEF048202FA94F520E207955EF9736E7914B11214059C44F648FD3647354CDFA5227C6685206A68968CF...
2903	13.567867	10.2.1.34	10.8.21.29	HTTP	242	HTTP/1.1 400 Bad Request
2915	13.844277	10.8.21.29	10.2.1.34	HTTP	394	POST /secars/secars.dll?h=7A7D48823E3395E7F0242E480194B7D052C85CA4D1029C90715B132931379F43964CAE928D00E63C41B9282B0850FFD083E8F9CB1ABCE5990727D8541F98C41884AC62D73D68390FCACD68C11C06D81238C5...
2917	13.858747	10.2.1.34	10.8.21.29	HTTP	255	HTTP/1.1 200 OK
2923	13.938423	10.8.21.29	10.2.1.34	HTTP	729	POST /secars/secars.dll?h=4971A848E32F83C8D1698279928157452C85CA4D1029C90715B132931379F43964CAE928D00E63C41B9282B0850FFD083E8F9CB1ABCE5990727D8541F98C41884AC62D73D68390FCACD68C11C06D81238C5...
2925	13.945234	10.2.1.34	10.8.21.29	HTTP	255	HTTP/1.1 200 OK

**Packet Details:**

- Frame 2699: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
- Interface id: 0 (Device\NPF\_{3178886F-E42D-407E-9735-DC81D5465808})
- Encapsulation type: Ethernet (1)
- Arrival Time: Mar 6, 2019 19:27:05.471757000 Eastern Standard Time
- Time shift for this packet: 0.000000000 seconds
- Epoch Time: 1551918425.471757000 seconds
- Time delta from previous captured frame: 0.000288000 seconds
- Time delta from previous displayed frame: 0.015508000 seconds
- Time since reference or first frame: 8.634926000 seconds
- Frame Number: 2699
- Frame Length: 492 bytes (3936 bits)
- Capture Length: 492 bytes (3936 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: ethertype:ip:tcp:http:data-text-lines]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: Cisco 59:ec:bf:00:2c:c8:59:ec:bf, Dst: Dell 17:44:3d:14:b3:1f:17:44:3d

**Packet Bytes:**

```
0000  14 b3 1f 17 44 3d 00 2c c8 59 ec bf 00 00 45 00  ....Dm.,Y....E-
0010  01 de 52 d0 40 00 33 06 5e a1 00 77 f5 0c 0a 00  ..R@3:~....
0020  15 1d 00 50 c6 3f cf 12 71 7a 86 9f e6 80 50 18  ..P?..qz...P-
0030  00 ed 27 f0 00 48 54 54 50 2f 31 2e 31 20 32  ..-..HTTP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75  00 OK-D ate: Thu
0050  2c 20 30 37 20 4d 61 72 20 32 30 31 39 20 30 30  , 07 Mar 2019 00
0060  3a 32 37 3a 30 35 20 47 4d 54 0d 0a 53 65 72 76  :27:05 G MT- Serv
0070  65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36  err: Apac he/2.4.6
0080  20 20 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53  (CentOS) OpenS
0090  4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48  L/1.0.2k -flps PH
00a0  50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72  P/5.4.16 mod_per
00b0  6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 76 35  1/2.0.10 Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69  .16.3-L ast-Modl
00d0  66 69 65 64 3a 20 57 65 64 2c 20 30 36 20 4d 61  Filed: he d, 06 Ma
00e0  72 20 32 30 31 39 20 30 36 3a 35 39 3a 30 31 20  r 2019 0 6:59:01
00f0  47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 35  GMT-ETa g: "51-5
0100  30 33 37 30 36 34 63 62 61 64 66 22 0d 0a 41 8367864c badf"-A
0110  63 65 70 74 2d 52 61 66 67 65 73 3a 20 62 79 ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6a 74 65 6a 74 2d 4c 65 6e tes:Con Tent-Len
0130  67 74 68 3a 20 38 31 0d 0a 4b 65 65 70 2d 41 6c gth: 81-Keep-Al
```

## HTTP MESSAGE GET

C:\Users\Saints\AppData\Local\Temp\wireshark\_Local Area Connection\_20190306192656\_a07180.pcapng 3170 total packets, 12 shown

No.	Time	Source	Destination	Protocol	Length	Info
2682	8.619418	10.8.21.29	128.119.245.12	HTTP	480	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 2682: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0

Interface id: 0 (\Device\NPF\_{3178B88F-E42D-487E-9735-DC81D5A65BD8})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2019 19:27:05.456249000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1551918425.456249000 seconds

[Time delta from previous captured frame: 0.000681000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 8.619418000 seconds]

Frame Number: 2682

Frame Length: 480 bytes (3840 bits)

Capture Length: 480 bytes (3840 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: Dell\_17:44:3d (14:b3:1f:17:44:3d), Dst: Cisco\_59:ec:bf (00:2c:c8:59:ec:bf)

Internet Protocol Version 4, Src: 10.8.21.29, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50751, Dst Port: 80, Seq: 1, Ack: 1, Len: 426 Hypertext Transfer Protocol

## HTTP MESSAGE OK

C:\Users\Saints\AppData\Local\Temp\wireshark\_Local Area Connection\_20190306192656\_a07180.pcapng 3170 total packets, 12 shown

No.	Time	Source	Destination	Protocol	Length	Info
2699	8.634926	128.119.245.12	10.8.21.29	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 2699: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0

Interface id: 0 (\Device\NPF\_{3178B88F-E42D-487E-9735-DC81D5A65BD8})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2019 19:27:05.471757000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1551918425.471757000 seconds

[Time delta from previous captured frame: 0.000288000 seconds]

[Time delta from previous displayed frame: 0.015508000 seconds]

[Time since reference or first frame: 8.634926000 seconds]

Frame Number: 2699

Frame Length: 492 bytes (3936 bits)

Capture Length: 492 bytes (3936 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: Cisco\_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell\_17:44:3d (14:b3:1f:17:44:3d)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.21.29

Transmission Control Protocol, Src Port: 80, Dst Port: 50751, Seq: 1, Ack: 427, Len: 438

Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)

