

08.04.2019

## HTTP Monitoring

### 1. HTTP is text-based request-response client-server protocol – why can we say so?

Ans: When we look first at working of web, the client and the server need to be physically connected, means the computer of the client and the web server. That's the job of the internet, using TCP/IP suite of protocols it establishes the connection using a combination of cable media and wireless media. And doing all this it creates all the necessary work to prepare the environment for the two computers to talk via the HTTP protocol. Once connection is established between client and server, client request as HTTP message and being HTTP connectionless protocol client disconnect from server after its request waiting for response. Server other side process the request, prepare the respond, and again establish connection with client and send back respond in form of HTTP message then again disconnect. HTTP messages used in this communication are plain text. This explains HTTP is a text-based request-response client-server protocol.

### 2. How the http connection is usually taking place?

Ans: When client makes request to server via HTTP protocol which is based on TCP/IP protocols, server listen to request made by client using its default port 80, process request and respond in the form of HTTP messages. In both cases, connection is disconnected after making request by client and responding by server as HTTP being connectionless protocol. In this way, HTTP connection is taking place.

### 3. Access the website [www.haaga-helia.fi](http://www.haaga-helia.fi) and monitor the traffic.

#### a) Write in your browser: [http:// www.haaga-helia.fi](http://www.haaga-helia.fi) and capture traffic when the website opens.

The screenshot shows the Wireshark interface with a packet capture on Ethernet 2. The packet list pane displays several HTTP GET requests to various resources on www.haaga-helia.fi. The selected packet (No. 1035) is expanded in the packet details pane, showing the full HTTP request structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The raw packet data pane at the bottom shows the hexadecimal and ASCII representation of the captured data.

No.	Time	Source	Destination	Protocol	Length	Info
1021	7.921302	10.208.0.9	23.42.153.199	HTTP	1058	GET /sync/iframe?mt_uid=ef2d5cab-0eb7-4e00-8601-21d3c49f86d6&no_iframe=1&mt_adid=217439 HTTP/1.1
1023	7.923023	10.208.0.9	37.233.91.219	HTTP	1054	GET /sites/default/files/js/js_CKB1R32EteHCi3hZak7nZfK1re8ZOHusY5V_2MdAPi0.js HTTP/1.1
1024	7.923405	34.251.201.192	10.208.0.9	HTTP	1055	HTTP/1.1 302 Found (text/html)
1026	7.924428	37.233.91.219	10.208.0.9	HTTP	395	HTTP/1.1 304 Not Modified
1028	7.933216	10.208.0.9	37.233.91.219	HTTP	1054	GET /sites/default/files/js/js_El-yLKKd2TFD5odu1093jFyR47LEA0tMf_LKdmDwbpo.js HTTP/1.1
1029	7.934530	10.208.0.9	23.42.153.199	HTTP	1056	GET /sync/img?mt_exid=100858mt_exuid=73f7a064-5e1d-46da-97d2-f86b773d76cd HTTP/1.1
1030	7.934663	37.233.91.219	10.208.0.9	HTTP	395	HTTP/1.1 304 Not Modified
1035	7.952039	10.208.0.9	37.233.91.219	HTTP	1053	GET /sites/default/files/js/js_RSvAPCIk8B_Gf6KBIajsw384yXXYHTK7B03_AfKQmJo.js HTTP/1.1
1038	7.952940	10.208.0.9	104.17.214.204	HTTP	359	GET /4431082.js HTTP/1.1
1041	7.953305	10.208.0.9	104.25.137.118	HTTP	482	GET /js/siteanalyze_6050155.js HTTP/1.1
1042	7.953481	37.233.91.219	10.208.0.9	HTTP	394	HTTP/1.1 304 Not Modified
1050	7.957081	104.17.214.204	10.208.0.9	HTTP	60	HTTP/1.1 200 OK (application/javascript)
1052	7.958037	104.25.137.118	10.208.0.9	HTTP	686	HTTP/1.1 304 Not Modified
1056	7.964798	23.42.153.199	10.208.0.9	HTTP	97	HTTP/1.1 200 OK (GIF89a)
1064	7.981173	23.42.153.199	10.208.0.9	HTTP	88	HTTP/1.1 200 OK (text/html)
1098	8.044958	10.208.0.9	37.233.91.219	HTTP	1037	GET /sites/all/themes/haagahelia/js/hyphenator/patterns/fi.js HTTP/1.1
1099	8.046862	10.208.0.9	37.233.91.219	HTTP	1075	GET /sites/all/themes/haagahelia/js/hyphenator/patterns/fi.js?_t=1554801582813 HTTP/1.1
1100	8.047484	37.233.91.219	10.208.0.9	HTTP	360	HTTP/1.1 304 Not Modified
1104	8.050615	37.233.91.219	10.208.0.9	HTTP	361	HTTP/1.1 200 OK (application/x-javascript)
1128	8.081058	10.208.0.9	104.17.70.176	HTTP	488	GET /analytics/1554801300000/4431082.js HTTP/1.1
1141	8.085158	104.17.70.176	10.208.0.9	HTTP	758	HTTP/1.1 304 Not Modified

Frame 1035: 1053 bytes on wire (8424 bits), 1053 bytes captured (8424 bits) on interface 0  
Ethernet II, Src: 02:00:30:0a:00:02 (02:00:30:0a:00:02), Dst: 02:00:28:83:00:03 (02:00:28:83:00:03)  
Internet Protocol Version 4, Src: 10.208.0.9, Dst: 37.233.91.219  
Transmission Control Protocol, Src Port: 54862, Dst Port: 80, Seq: 19121, Ack: 6840, Len: 999  
Hypertext Transfer Protocol  
GET /sites/default/files/js/js\_RSvAPCIk8B\_Gf6KBIajsw384yXXYHTK7B03\_AfKQmJo.js HTTP/1.1\r\n  
Accept: application/javascript, \*/\*;q=0.8\r\n  
Referer: http://www.haaga-helia.fi/fi/etusivu\r\n  
Accept-Language: en-US\r\n  
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

#### b) How the connection is established?

Ans: When client made request with server then server responds with HTTP message, in this way connection is established.

#### c) Source and Destination Ports?

Source Port: 57464

08.04.2019

Destination Port:

**d) The client/browser first request?**

Client/browser first request GET / HTTP/1.1.\r\n.

**e) Response from the server?**

When request from source 10.208.0.9 is made to Destination 37.233.91.219 with length 834 and info GET / HTTP / 1.1 then its response is 515 HTTP/1.1 302 Moved Temporarily (Text /html).

**f) What HTTP version is used?**

HTTP version is 1.1

**g) What is the web server?**

ECS is the web server.

**h) Find out, how the data is transferred to the browser?**

Ans: When browser sends an HTTP request message to the server for instance asking to send copy of website over internet having TCP/IP protocol, server approves the request and responds the request sending the website's files to browser as a series of small chunks of data packets. When browser receives those packets it assembles the small chunks into a complete website containing text, images, videos and more and displays it to client. In this, the data is transferred to the browser.

**4. Access website [https://..\(your choice\).](https://..(your choice).)**

**a) Find out what TLS version is used?**

Ans: TLS version used is 1.2v.

**b) How Application Data is visible?**

Ans:

The image shows a Wireshark packet capture window titled "Capturing from Ethernet 2". The packet list pane shows several packets, with packet 2187 selected. The packet details pane shows the structure of the selected packet, which is an HTTP GET request. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
2187	30.794860	10.208.0.9	52.49.121.81	HTTP	305	GET / HTTP/1.1
2191	30.842852	52.49.121.81	10.208.0.9	HTTP	437	HTTP/1.1 301 Moved Permanently (text/html)
2225	31.032099	10.208.0.9	54.192.98.109	HTTP	273	GET //MEowSDBGMEQwQjA3BgUrDgMCGGUABBSLwZ6EW5gdYc9UaSEaaljjETWtKAQUv1%2B30c7d4b0M1ws3NcQw6pi0cCCQcndKpN1K3fw%3D%3D HTTP/1.1
2230	31.041309	54.192.98.109	10.208.0.9	OCSP	1016	Response
2242	31.060178	10.208.0.9	52.84.214.78	HTTP	296	GET /MFewTzBNMEswSTA3BgUrDgMCGGUABBRJ9L2KGL92BpfJ3kAtaDtxauTmhgQUPdNQpdagre7z5mAKZdPh1Pj41g8CEAgAQ543siDOVPj1N210sZ8%3D HTTP/1.1
2267	31.281783	52.84.214.78	10.208.0.9	OCSP	525	Response
2865	31.761768	10.208.0.9	93.184.220.29	HTTP	293	GET /MFewTzBNMEswSTA3BgUrDgMCGGUABBRJ9L2KGL92BpfJ3kAtaDtxauTmhgQUPdNQpdagre7z5mAKZdPh1Pj41g8CEAgAQ543siDOVPj1N210sZ8%3D HTTP/1.1
2869	31.763609	93.184.220.29	10.208.0.9	OCSP	842	Response
4606	35.926147	10.208.0.9	93.184.220.29	HTTP	285	GET /MFewTzBNMEswSTA3BgUrDgMCGGUABBRJ9L2KGL92BpfJ3kAtaDtxauTmhgQUPdNQpdagre7z5mAKZdPh1Pj41g8CEAgAQ543siDOVPj1N210sZ8%3D HTTP/1.1
4607	35.928256	93.184.220.29	10.208.0.9	OCSP	842	Response

Internet Protocol Version 4, Src: 10.208.0.9, Dst: 52.49.121.81  
Transmission Control Protocol, Src Port: 55096, Dst Port: 80, Seq: 1, Ack: 1, Len: 251  
Hypertext Transfer Protocol  
GET / HTTP/1.1\r\n  
Accept: text/html, application/xhtml+xml, \*/\*\r\n  
Accept-Language: en-US\r\n  
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n  
Accept-Encoding: gzip, deflate\r\n  
Host: www.studyinfo.fi\r\n  
Connection: Keep-Alive\r\n  
\r\n

0000 02 00 28 83 00 03 02 00 30 0a 00 02 08 00 45 00 ..(-----0-----E:  
0010 01 23 22 7a 40 00 08 06 00 00 0a d0 00 09 34 31 #zg-----41  
0020 79 51 d7 38 00 50 97 a5 3f 4c 20 71 f8 99 50 18 yQ-8-P-2L-q-P  
0030 04 00 b9 70 00 00 47 a5 54 20 2f 20 48 54 54 50 ...p:GE T / HTTP  
0040 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 /1.1:Ac cept: te  
0050 78 74 2f 68 74 6d 6c 2c 20 61 70 70 6c 69 63 61 xt/html, applica

**c) Source and Destination Ports are now?**

Ans: Source Port - 53997, Destination Port - HTTPS (443)