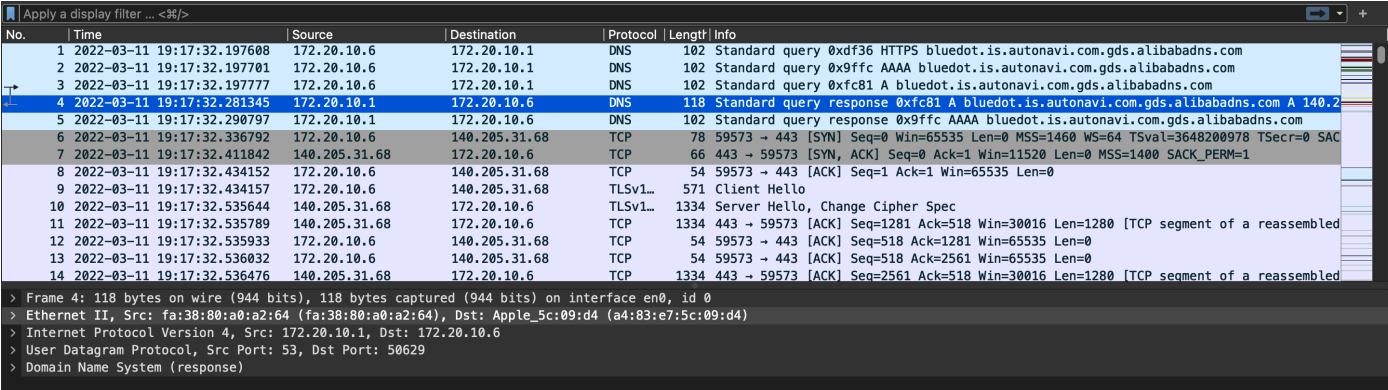


练习：用Wireshark分析HTTP

1. TCP/IP协议的5层结构

五层协议（5层）：物理层、数据链路层、网络层、运输层、应用层。

如图所示：



从上往下依次是：

- Frame 4：数据链路层
- Ethernet II：数据链路层
- Internet Protocol Version 4：网络层
- User Datagram Protocol：传输层
- Domain Name System：应用层

2. 分析哪些协议以及协议所占百分比

协议如下：

物理层：RJ45、CLOCK、IEEE802.3

数据链路：PPP、FR、VLAN、MAC

网络层：IP、ICMP、ARP、OSP、IPX、RIP、IGRP

传输层：TCP、UDP、SPX

应用层：FTP、DNS、Telnet、SMTP、HTTP

物理层和数据链路层没有接受到协议。

网络层接受到了IP：

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-11 19:17:32.197608	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xdf36 HTTPS blue dot.is.autonavi.com.gds.alibabadns.com
2	2022-03-11 19:17:32.197701	172.20.10.6	172.20.10.1	DNS	102	Standard query 0x9ffc AAAA blue dot.is.autonavi.com.gds.alibabadns.com
3	2022-03-11 19:17:32.197777	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xfc81 A blue dot.is.autonavi.com.gds.alibabadns.com
4	2022-03-11 19:17:32.281345	172.20.10.1	172.20.10.6	DNS	118	Standard query response 0xfc81 A blue dot.is.autonavi.com.gds.alibabadns.com A 140.2
5	2022-03-11 19:17:32.290797	172.20.10.1	172.20.10.6	DNS	102	Standard query response 0x9ffc AAAA blue dot.is.autonavi.com.gds.alibabadns.com
6	2022-03-11 19:17:32.336792	172.20.10.6	140.205.31.68	TCP	78	59573 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3648200978 TSecr=0 SAC
7	2022-03-11 19:17:32.411842	140.205.31.68	172.20.10.6	TCP	66	443 → 59573 [SYN, ACK] Seq=0 Ack=1 Win=11520 Len=0 MSS=1400 SACK_PERM=1
8	2022-03-11 19:17:32.434152	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9	2022-03-11 19:17:32.434157	172.20.10.6	140.205.31.68	TLSv1...	571	Client Hello
10	2022-03-11 19:17:32.535644	140.205.31.68	172.20.10.6	TLSv1...	1334	Server Hello, Change Cipher Spec
11	2022-03-11 19:17:32.535789	140.205.31.68	172.20.10.6	TCP	1334	443 → 59573 [ACK] Seq=1281 Ack=518 Win=30016 Len=1280 [TCP segment of a reassembled
12	2022-03-11 19:17:32.535933	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=518 Ack=1281 Win=65535 Len=0
13	2022-03-11 19:17:32.536032	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=518 Ack=2561 Win=65535 Len=0
14	2022-03-11 19:17:32.536476	140.205.31.68	172.20.10.6	TCP	1334	443 → 59573 [ACK] Seq=2561 Ack=518 Win=30016 Len=1280 [TCP segment of a reassembled

ICMP:

No.	Time	Source	Destination	Protocol	Length	Info
2161	2022-03-11 19:17:40.264750	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
2162	2022-03-11 19:17:40.264779	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
2163	2022-03-11 19:17:40.264796	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
4062	2022-03-11 19:17:49.834477	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
4085	2022-03-11 19:17:53.533401	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
4114	2022-03-11 19:17:53.649262	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8112	2022-03-11 19:18:02.219800	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8386	2022-03-11 19:18:04.401079	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8406	2022-03-11 19:18:06.245656	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8409	2022-03-11 19:18:06.673334	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8412	2022-03-11 19:18:06.707663	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8413	2022-03-11 19:18:06.707738	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8415	2022-03-11 19:18:06.709059	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)
8417	2022-03-11 19:18:06.712670	172.20.10.6	172.20.10.1	ICMP	70	Destination unreachable (Port unreachable)

占比来说IP占绝大部分，ICMP较少。

传输层接受到了TCP:

No.	Time	Source	Destination	Protocol	Length	Info
6	2022-03-11 19:17:32.336792	172.20.10.6	140.205.31.68	TCP	78	59573 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3648200978 TSecr=0 SAC
7	2022-03-11 19:17:32.411842	140.205.31.68	172.20.10.6	TCP	66	443 → 59573 [SYN, ACK] Seq=0 Ack=1 Win=11520 Len=0 MSS=1400 SACK_PERM=1
8	2022-03-11 19:17:32.434152	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9	2022-03-11 19:17:32.434157	172.20.10.6	140.205.31.68	TLSv1...	571	Client Hello
10	2022-03-11 19:17:32.535644	140.205.31.68	172.20.10.6	TLSv1...	1334	Server Hello, Change Cipher Spec
11	2022-03-11 19:17:32.535789	140.205.31.68	172.20.10.6	TCP	1334	443 → 59573 [ACK] Seq=1281 Ack=518 Win=30016 Len=1280 [TCP segment of a reassembled
12	2022-03-11 19:17:32.535933	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=518 Ack=1281 Win=65535 Len=0
13	2022-03-11 19:17:32.536032	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=518 Ack=2561 Win=65535 Len=0
14	2022-03-11 19:17:32.536476	140.205.31.68	172.20.10.6	TCP	1334	443 → 59573 [ACK] Seq=2561 Ack=518 Win=30016 Len=1280 [TCP segment of a reassembled
15	2022-03-11 19:17:32.536476	140.205.31.68	172.20.10.6	TLSv1...	175	Application Data
16	2022-03-11 19:17:32.536477	140.205.31.68	172.20.10.6	TCP	54	443 → 59573 [ACK] Seq=1 Ack=518 Win=30016 Len=0
17	2022-03-11 19:17:32.536477	140.205.31.68	172.20.10.6	TCP	175	[TCP Retransmission] 443 → 59573 [PSH, ACK] Seq=3841 Ack=518 Win=30016 Len=121
18	2022-03-11 19:17:32.536813	172.20.10.6	140.205.31.68	TCP	54	59573 → 443 [ACK] Seq=518 Ack=3962 Win=65535 Len=0
19	2022-03-11 19:17:32.536815	172.20.10.6	140.205.31.68	TCP	54	[TCP Dup ACK 18#1] 59573 → 443 [ACK] Seq=518 Ack=3962 Win=65535 Len=0

UDP:

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-11 19:17:32.197608	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xdf36 HTTPS blue dot.is.autonavi.com.gds.alibabadns.com
2	2022-03-11 19:17:32.197701	172.20.10.6	172.20.10.1	DNS	102	Standard query 0x9ffc AAAA blue dot.is.autonavi.com.gds.alibabadns.com
3	2022-03-11 19:17:32.197777	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xfc81 A blue dot.is.autonavi.com.gds.alibabadns.com
4	2022-03-11 19:17:32.281345	172.20.10.1	172.20.10.6	DNS	118	Standard query response 0xfc81 A blue dot.is.autonavi.com.gds.alibabadns.com A 140.2
5	2022-03-11 19:17:32.290797	172.20.10.1	172.20.10.6	DNS	102	Standard query response 0x9ffc AAAA blue dot.is.autonavi.com.gds.alibabadns.com
40	2022-03-11 19:17:33.197528	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xdf36 HTTPS blue dot.is.autonavi.com.gds.alibabadns.com
41	2022-03-11 19:17:34.398032	172.20.10.6	172.20.10.1	DNS	78	Standard query 0x78d5 HTTPS api.smoot.apple.cn
42	2022-03-11 19:17:34.398106	172.20.10.6	172.20.10.1	DNS	78	Standard query 0xe4c7 AAAA api.smoot.apple.cn
43	2022-03-11 19:17:34.398181	172.20.10.6	172.20.10.1	DNS	78	Standard query 0x9c82 A api.smoot.apple.cn
44	2022-03-11 19:17:34.536359	172.20.10.1	172.20.10.6	DNS	161	Standard query response 0x9c82 A api.smoot.apple.cn CNAME api.smoot.apple.com CNAME
45	2022-03-11 19:17:34.536361	172.20.10.1	172.20.10.6	DNS	145	Standard query response 0xe4c7 AAAA api.smoot.apple.cn CNAME api.smoot.apple.com CN
46	2022-03-11 19:17:34.537129	172.20.10.6	172.20.10.1	DNS	83	Standard query 0xa5ff AAAA bag-smoot.v.aaplimg.com
47	2022-03-11 19:17:34.544761	172.20.10.1	172.20.10.6	DNS	83	Standard query response 0xa5ff AAAA bag-smoot.v.aaplimg.com
62	2022-03-11 19:17:34.916273	172.20.10.6	172.20.10.1	DNS	75	Standard query 0xd9e9 A locintco.wos.cn

占比来说TCP占绝大部分，UDP较少。

应用层接受到了DNS:

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-03-11 19:17:32.197608	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xdf36 HTTPS blue-dot.is.autonavi.com.gds.alibabadns.com
2	2022-03-11 19:17:32.197701	172.20.10.6	172.20.10.1	DNS	102	Standard query 0x9ffc AAAA blue-dot.is.autonavi.com.gds.alibabadns.com
3	2022-03-11 19:17:32.197777	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xfc81 A blue-dot.is.autonavi.com.gds.alibabadns.com
4	2022-03-11 19:17:32.281345	172.20.10.1	172.20.10.6	DNS	118	Standard query response 0xfc81 A blue-dot.is.autonavi.com.gds.alibabadns.com A 140.2
5	2022-03-11 19:17:32.290797	172.20.10.1	172.20.10.6	DNS	102	Standard query response 0x9ffc AAAA blue-dot.is.autonavi.com.gds.alibabadns.com
40	2022-03-11 19:17:33.197528	172.20.10.6	172.20.10.1	DNS	102	Standard query 0xdf36 HTTPS blue-dot.is.autonavi.com.gds.alibabadns.com
41	2022-03-11 19:17:34.398032	172.20.10.6	172.20.10.1	DNS	78	Standard query 0x78d5 HTTPS api.smoot.apple.cn
42	2022-03-11 19:17:34.398106	172.20.10.6	172.20.10.1	DNS	78	Standard query 0xe4c7 AAAA api.smoot.apple.cn
43	2022-03-11 19:17:34.398181	172.20.10.6	172.20.10.1	DNS	78	Standard query 0x9c82 A api.smoot.apple.cn
44	2022-03-11 19:17:34.536359	172.20.10.1	172.20.10.6	DNS	161	Standard query response 0x9c82 A api.smoot.apple.cn CNAME api.smoot.apple.com CNAME
45	2022-03-11 19:17:34.536361	172.20.10.1	172.20.10.6	DNS	145	Standard query response 0xe4c7 AAAA api.smoot.apple.cn CNAME api.smoot.apple.com CN
46	2022-03-11 19:17:34.537129	172.20.10.6	172.20.10.1	DNS	83	Standard query 0xa5ff AAAA bag-smoot.v.aaplimg.com
47	2022-03-11 19:17:34.544761	172.20.10.1	172.20.10.6	DNS	83	Standard query response 0xa5ff AAAA bag-smoot.v.aaplimg.com
62	2022-03-11 19:17:34.916273	172.20.10.6	172.20.10.1	DNS	75	Standard query 0xd9e9 A logintcp.wps.cn

HTTP:

No.	Time	Source	Destination	Protocol	Length	Info
48	2022-03-11 19:17:34.619301	172.20.10.6	222.35.78.41	HTTP	233	GET /params/login_params_tcp.json HTTP/1.1
54	2022-03-11 19:17:34.914469	222.35.78.41	172.20.10.6	HTTP	661	HTTP/1.1 200 OK
110	2022-03-11 19:17:35.271292	172.20.10.6	120.92.106.21	HTTP	704	GET /api/v1/connectors?protocol=tcp&usertype=40 HTTP/1.1
117	2022-03-11 19:17:35.338638	120.92.106.21	172.20.10.6	HTTP/...	557	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
3894	2022-03-11 19:17:44.200991	172.20.10.6	112.53.36.112	HTTP	888	POST /mmtls/01524042 HTTP/1.1
3961	2022-03-11 19:17:47.145405	172.20.10.6	112.53.36.112	HTTP	1021	POST /mmtls/01530537 HTTP/1.1
8437	2022-03-11 19:18:07.453498	172.20.10.6	112.53.36.112	HTTP	1021	POST /mmtls/01582643 HTTP/1.1
8446	2022-03-11 19:18:07.593215	112.53.36.112	172.20.10.6	HTTP	457	HTTP/1.1 200 OK

占比来说DNS占绝大部分，HTTP较少。

3. 指出Web服务器的IP地址

本机的IP地址：172.20.10.6

```
wangxinhao@wangxinhaodeMacBook-Pro My_Personal_Blog % ifconfig | grep "inet " |
grep -v 127.0.0.1
    inet 172.20.10.6 netmask 0xfffffff0 broadcast 172.20.10.15
```

对端的：39.156.66.10

```
wangxinhao@wangxinhaodeMacBook-Pro My_Personal_Blog % ping baidu.cn
PING baidu.cn (39.156.66.10): 56 data bytes
```

4. 应用显示过滤器，分析你的主机与Web服务器之间HTTP协议

如图：

No.	Time	Source	Destination	Protocol	Length	Info
48	2022-03-11 19:17:34.619301	172.20.10.6	222.35.78.41	HTTP	233	GET /params/login_params_tcp.json HTTP/1.1
54	2022-03-11 19:17:34.914469	222.35.78.41	172.20.10.6	HTTP	661	HTTP/1.1 200 OK
110	2022-03-11 19:17:35.271292	172.20.10.6	120.92.106.21	HTTP	704	GET /api/v1/connectors?protocol=tcp&usertype=40 HTTP/1.1
117	2022-03-11 19:17:35.338638	120.92.106.21	172.20.10.6	HTTP/...	557	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
3894	2022-03-11 19:17:44.200991	172.20.10.6	112.53.36.112	HTTP	888	POST /mmtls/01524042 HTTP/1.1
3961	2022-03-11 19:17:47.145405	172.20.10.6	112.53.36.112	HTTP	1021	POST /mmtls/01530537 HTTP/1.1
8437	2022-03-11 19:18:07.453498	172.20.10.6	112.53.36.112	HTTP	1021	POST /mmtls/01582643 HTTP/1.1
8446	2022-03-11 19:18:07.593215	112.53.36.112	172.20.10.6	HTTP	457	HTTP/1.1 200 OK

HTTP协议报文详细信息：

```

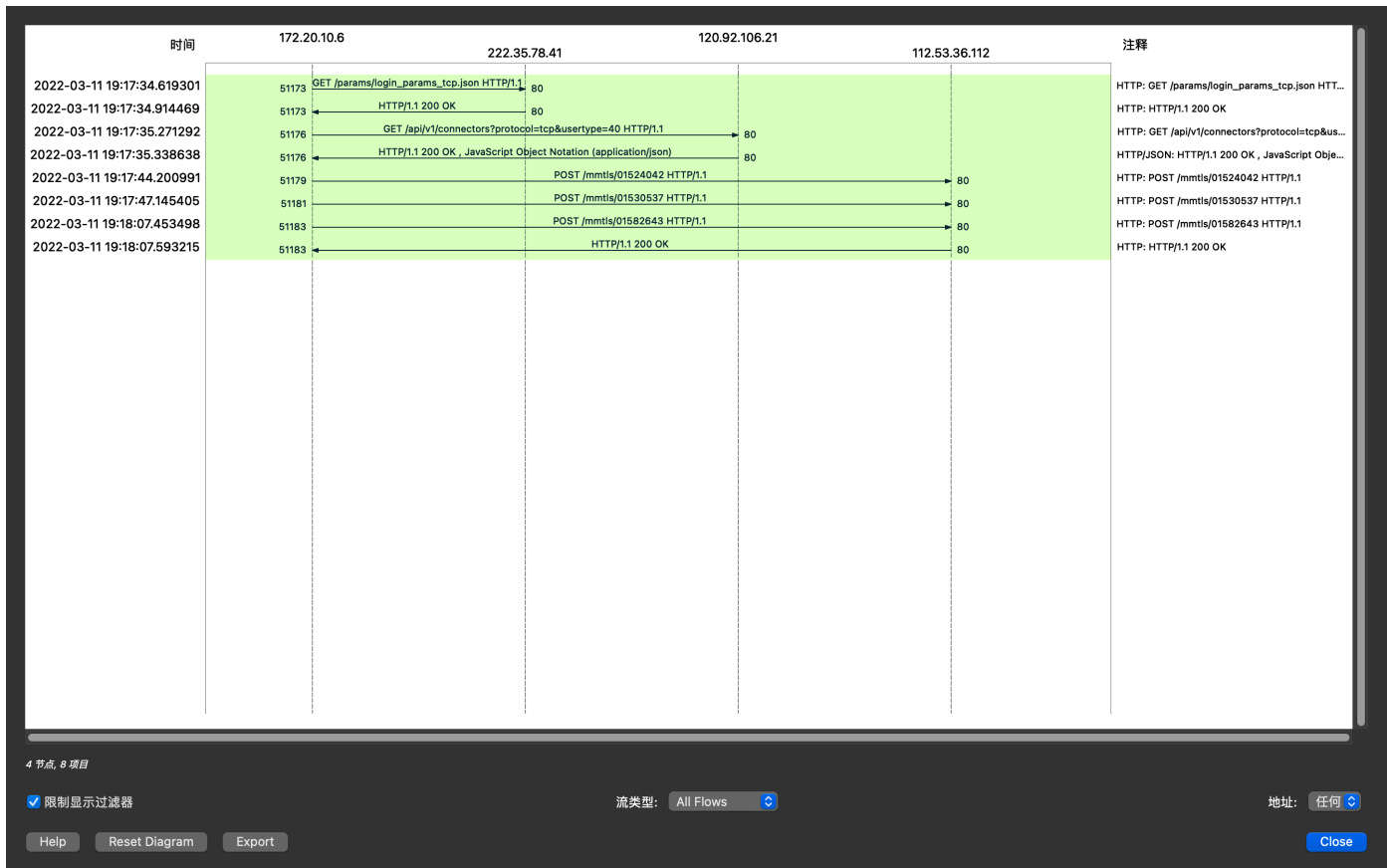
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Connection: close\r\n
  Content-Type: application/octet-stream\r\n
> Content-Length: 1703\r\n
  \r\n
[HTTP response 1/1]
[Time since request: 0.139717000 seconds]
[Request in frame: 8437]
[Request URI: http://szextshort.weixin.qq.com/mmtls/01582643]
File Data: 1703 bytes

```

以下是 HTTP 请求/响应的步骤：

1. 客户端连接到Web服务器 一个HTTP客户端，通常是浏览器，与Web服务器的HTTP端口（默认为80）建立一个TCP套接字连接。例如， <http://www.baidu.com>。
2. 发送HTTP请求 通过TCP套接字，客户端向Web服务器发送一个文本的请求报文，一个请求报文由请求行、请求头部、空行和请求数据4部分组成。
3. 服务器接受请求并返回HTTP响应 Web服务器解析请求，定位请求资源。服务器将资源复本写到TCP套接字，由客户端读取。一个响应由状态行、响应头部、空行和响应数据4部分组成。
4. 释放连接TCP连接 若connection 模式为close，则服务器主动关闭TCP连接，客户端被动关闭连接，释放TCP连接;若connection 模式为keepalive，则该连接会保持一段时间，在该时间内可以继续接收请求;
5. 客户端浏览器解析HTML内容 客户端浏览器首先解析状态行，查看表明请求是否成功的状态代码。然后解析每一个响应头，响应头告知以下为若干字节的HTML文档和文档的字符集。客户端浏览器读取响应数据HTML，根据HTML的语法对其进行格式化，并在浏览器窗口中显示。

5. 执行 统计—>流量图，显示浏览器与HTTP服务器之间的HTTP协议过程



6. 执行 统计—>HTTP，显示浏览器与HTTP服务器之间请求与响应分组总数及占比

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Total HTTP Packets	8				0.0002	100%	0.0200	3.074
Other HTTP Packets	0				0.0000	0.00%	-	-
▼ HTTP Response Packets	3				0.0001	37.50%	0.0100	2.717
??? broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
▼ 2xx: Success	3				0.0001	100.00%	0.0100	2.717
200 OK	3				0.0001	100.00%	0.0100	2.717
1xx: Informational	0				0.0000	0.00%	-	-
▼ HTTP Request Packets	5				0.0002	62.50%	0.0100	2.422
POST	3				0.0001	60.00%	0.0100	12.003
GET	2				0.0001	40.00%	0.0100	2.422

显示过滤器:

应用

复制 另存为...

Close

7. 其他问题及发现

我发现我捕获的信号中代表http协议的信号非常少，反而大部分是DNS协议的信号，不知道是什么原因。