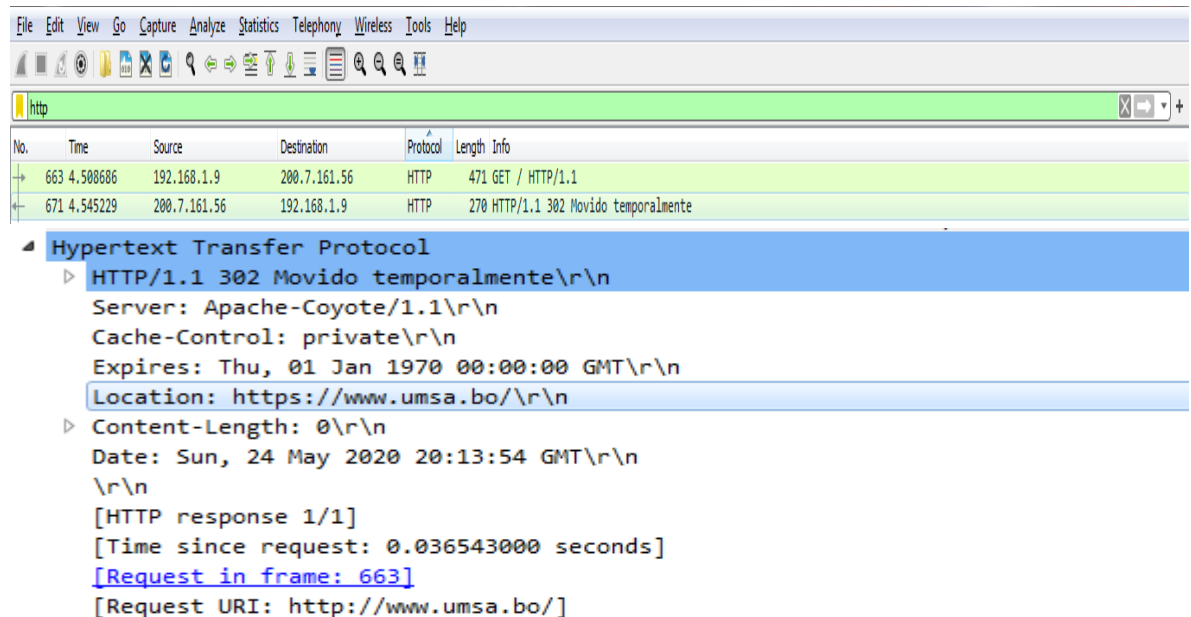


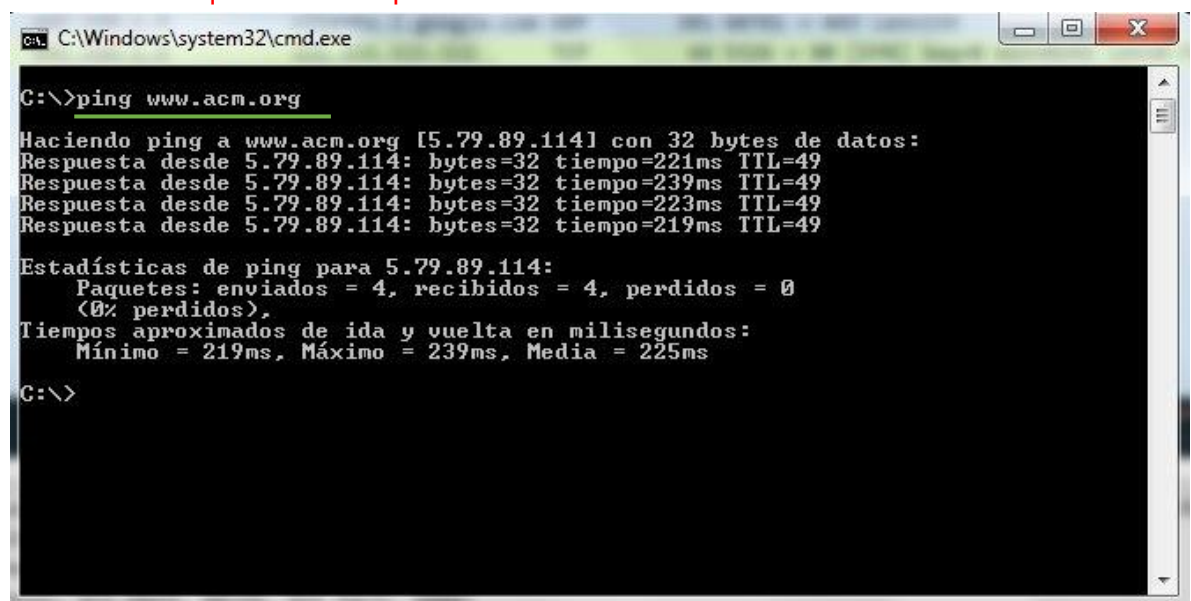
LABORATORIO 5

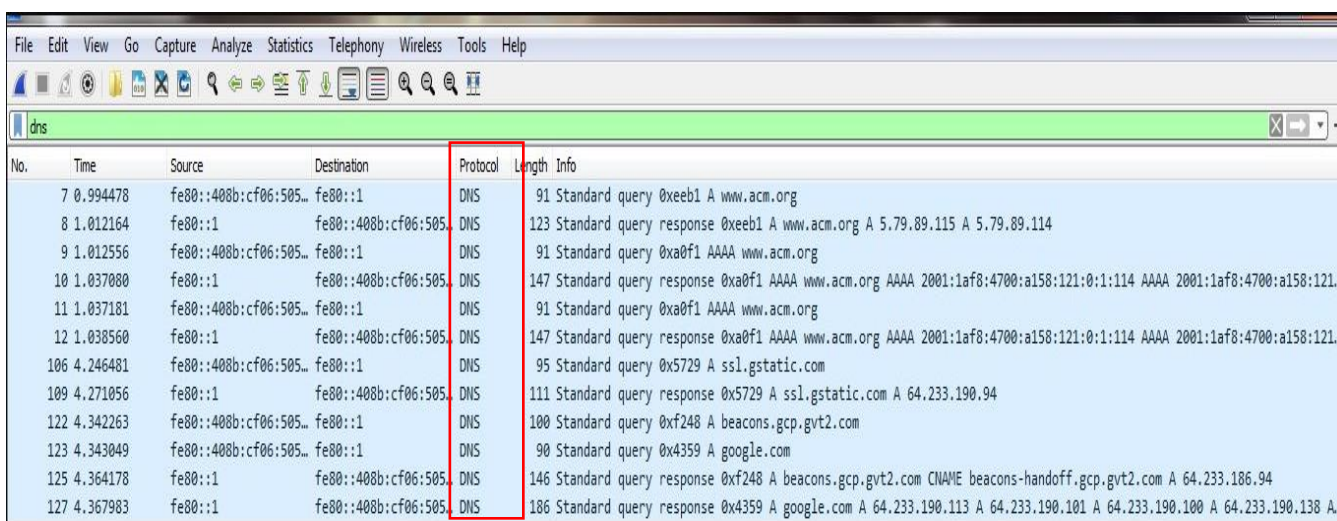
Nombre: Univ. Mamani Chavez Carla Vanesa	CI: 9124602 LP Paralelo: Martes
Docente : Lic. Gallardo Portanda Franz Ramiro	Fecha : 17/05/2020

- 1) Realizar el filtro de captura al acceder a la página de la UMSA www.umsa.bo para obtener en el panel de salida de Wireshark solo un registro con información del servidor web.



- 2) Realizar el filtro de captura de ping www.acm.org Mostrar en el panel de salida la resolución que realiza el protocolo DNS o la tabla DNS.

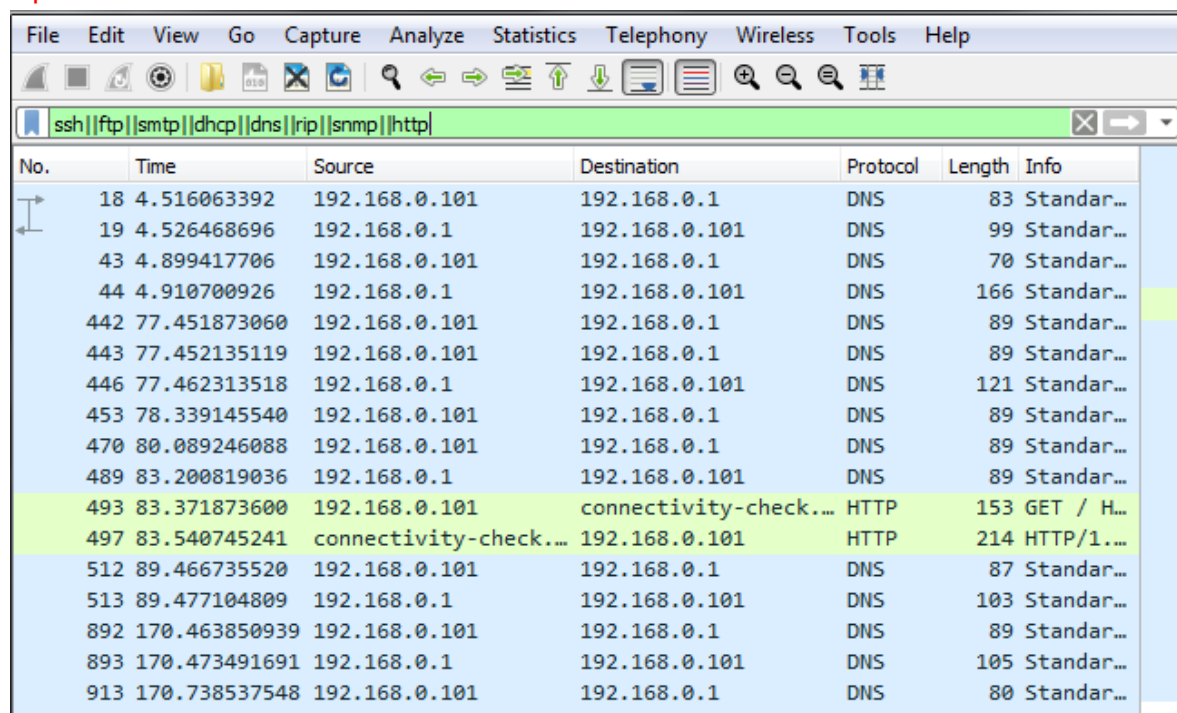




No.	Time	Source	Destination	Protocol	Length	Info
7	0.994478	fe80::408b:cf06:505...	fe80::1	DNS	91	Standard query 0xeeb1 A www.acm.org
8	1.012164	fe80::1	fe80::408b:cf06:505...	DNS	123	Standard query response 0xeeb1 A www.acm.org A 5.79.89.115 A 5.79.89.114
9	1.012556	fe80::408b:cf06:505...	fe80::1	DNS	91	Standard query 0xa0f1 AAAA www.acm.org
10	1.037080	fe80::1	fe80::408b:cf06:505...	DNS	147	Standard query response 0xa0f1 AAAA www.acm.org AAAA 2001:1af8:4700:a158:121:0:1:114 AAAA 2001:1af8:4700:a158:121...
11	1.037181	fe80::408b:cf06:505...	fe80::1	DNS	91	Standard query 0xa0f1 AAAA www.acm.org
12	1.038560	fe80::1	fe80::408b:cf06:505...	DNS	147	Standard query response 0xa0f1 AAAA www.acm.org AAAA 2001:1af8:4700:a158:121:0:1:114 AAAA 2001:1af8:4700:a158:121...
106	4.246481	fe80::408b:cf06:505...	fe80::1	DNS	95	Standard query 0x5729 A ssl.gstatic.com
109	4.271056	fe80::1	fe80::408b:cf06:505...	DNS	111	Standard query response 0x5729 A ssl.gstatic.com A 64.233.190.94
122	4.342263	fe80::408b:cf06:505...	fe80::1	DNS	100	Standard query 0xf248 A beacons.gcp.gvt2.com
123	4.343049	fe80::408b:cf06:505...	fe80::1	DNS	90	Standard query 0x4359 A google.com
125	4.364178	fe80::1	fe80::408b:cf06:505...	DNS	146	Standard query response 0xf248 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 64.233.186.94
127	4.367983	fe80::1	fe80::408b:cf06:505...	DNS	186	Standard query response 0x4359 A google.com A 64.233.190.113 A 64.233.190.101 A 64.233.190.100 A 64.233.190.138 A...

4) Abrir el archivo de captura Reporte.pcapng y mostrar en el panel de salida de Wireshark protocolos TCP/IP a nivel de la capa de:

Aplicación



No.	Time	Source	Destination	Protocol	Length	Info
18	4.516063392	192.168.0.101	192.168.0.1	DNS	83	Standar...
19	4.526468696	192.168.0.1	192.168.0.101	DNS	99	Standar...
43	4.899417706	192.168.0.101	192.168.0.1	DNS	70	Standar...
44	4.910700926	192.168.0.1	192.168.0.101	DNS	166	Standar...
442	77.451873060	192.168.0.101	192.168.0.1	DNS	89	Standar...
443	77.452135119	192.168.0.101	192.168.0.1	DNS	89	Standar...
446	77.462313518	192.168.0.1	192.168.0.101	DNS	121	Standar...
453	78.339145540	192.168.0.101	192.168.0.1	DNS	89	Standar...
470	80.089246088	192.168.0.101	192.168.0.1	DNS	89	Standar...
489	83.200819036	192.168.0.1	192.168.0.101	DNS	89	Standar...
493	83.371873600	192.168.0.101	connectivity-check...	HTTP	153	GET / H...
497	83.540745241	connectivity-check...	192.168.0.101	HTTP	214	HTTP/1...
512	89.466735520	192.168.0.101	192.168.0.1	DNS	87	Standar...
513	89.477104809	192.168.0.1	192.168.0.101	DNS	103	Standar...
892	170.463850939	192.168.0.101	192.168.0.1	DNS	89	Standar...
893	170.473491691	192.168.0.1	192.168.0.101	DNS	105	Standar...
913	170.738537548	192.168.0.101	192.168.0.1	DNS	80	Standar...

The image shows a Wireshark packet capture analysis. The top pane displays the packet list, and the bottom pane shows the packet details. The selected packet is a UDP packet from 192.168.0.101 to 192.168.0.1.

Packet 18: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlan0, id 0

- Interface id: 0 (wlan0)
- Encapsulation type: Ethernet (1)
- Arrival Time: May 22, 2020 10:42:42.893294161 Hora estándar de Venezuela
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1590158562.893294161 seconds
- [Time delta from previous captured frame: 0.000462866 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 4.516063392 seconds]
- Frame Number: 18
- Frame Length: 83 bytes (664 bits)
- Capture Length: 83 bytes (664 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- Protocols in frame: ethertype:ip:udp:dns
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]

Ethernet II, Src: ChiconyE_9d:f1:74 (4c:bb:58:9d:f1:74), Dst: Tp-LinkT_4c:ec:f6 (f8:1a:67:4c:ec:f6)

- Destination: Tp-LinkT_4c:ec:f6 (f8:1a:67:4c:ec:f6)
- Source: ChiconyE_9d:f1:74 (4c:bb:58:9d:f1:74)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 69
- Identification: 0xe276 (57974)
- Flags: 0x4000, Don't fragment
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0xd67a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.101
- Destination: 192.168.0.1

User Datagram Protocol, Src Port: 39001, Dst Port: 53

- Source Port: 39001
- Destination Port: 53
- Length: 49
- Checksum: 0xbd29 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 2]
- [Timestamps]

Domain Name System (query)

- Transaction ID: 0x19d1
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- [Response In: 19]

Transporte

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	138.197.56.216	192.168.0.101	TLSv1.2	91	Applica...
2	0.000076050	192.168.0.101	138.197.56.216	TCP	66	43664 →...
3	0.001324486	192.168.0.101	138.197.56.216	TLSv1.2	95	Applica...
4	0.082773151	192.168.0.1	255.255.255.255	UDP	215	33782 →...
5	0.121942589	138.197.56.216	192.168.0.101	TLSv1.2	91	Applica...
6	0.162866988	192.168.0.101	138.197.56.216	TCP	66	43664 →...
7	0.547827269	192.168.0.101	beacons.gvt2.com	UDP	104	51231 →...
9	1.898871393	192.168.0.101	cb-in-f188.1e100.net	TCP	66	56112 →...
10	1.943516448	cb-in-f188.1e100.net	192.168.0.101	TCP	66	[TCP AC...
12	3.050665788	192.168.0.1	255.255.255.255	UDP	215	33782 →...
13	3.827409675	192.168.0.101	cb-in-f103.1e100.net	ICMP	98	Echo (p...
14	3.874573920	cb-in-f103.1e100.net	192.168.0.101	ICMP	98	Echo (p...
15	3.946877719	192.168.0.101	104.27.170.247	TCP	54	44798 →...
16	3.991535482	104.27.170.247	192.168.0.101	TCP	54	[TCP AC...
17	4.515600526	192.168.0.101	23.111.228.228	TCP	66	36896 →...
18	4.516063392	192.168.0.101	192.168.0.1	DNS	83	Standar...
19	4.526468696	192.168.0.1	192.168.0.101	DNS	99	Standar...

The image shows two screenshots of the Wireshark network protocol analyzer. The top screenshot displays the packet list and packet details for a TCP connection. The bottom screenshot shows the packet details for a DNS query and response.

Top Screenshot: Packet List and Details

No.	Time	Source	Destination	Protocol	Length	Info
18	4.516063392	192.168.0.101	192.168.0.1	DNS	83	Standard query 0x19d1 A mmx-ds.cdn.whatsapp.net
19	4.526468696	192.168.0.1	192.168.0.101	DNS	99	Standard query response 0x19d1 A mmx-ds.cdn.whatsapp.net A 157.240.204.60
20	4.526737347	192.168.0.101	157.240.204.60	TCP	74	36058 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=152675764 TSecr=0 WS=128
21	4.574308770	157.240.204.60	192.168.0.101	TCP	74	443 → 36058 [SYN, ACK] Seq=0 Ack=1 Win=27760 Len=0 MSS=1400 SACK_PERM=1 TSval=3956840429 TSecr=152675764 WS=128

Packet Details (Frame 18):

- Interface: 0 (wlan0)
- Encapsulation type: Ethernet (1)
- Arrival Time: May 22, 2020 10:42:42.893294161 Hora estándar de Venezuela
- Time shift for this packet: 0.000000000 seconds
- Epoch Time: 1590158562.893294161 seconds
- Time delta from previous captured frame: 0.000462866 seconds
- Time delta from previous displayed frame: 0.000462866 seconds
- Time since reference or first frame: 4.516063392 seconds
- Frame Number: 18
- Frame Length: 83 bytes (664 bits)
- Capture Length: 83 bytes (664 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- Protocols in frame: ethertype:ip:udp:dns
- Coloring Rule Name: UDP
- [Coloring Rule String: udp]
- Ethernet II, Src: ChiconyE_9d:f1:74 (4c:bb:58:9d:f1:74), Dst: Tp-LinkT_4c:ec:f6 (f8:1a:67:4c:ec:f6)
- Destination: Tp-LinkT_4c:ec:f6 (f8:1a:67:4c:ec:f6)
- Source: ChiconyE_9d:f1:74 (4c:bb:58:9d:f1:74)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 69
- Identification: 0xe276 (57974)
- Flags: 0x4000, Don't fragment
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0xd67a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.101
- Destination: 192.168.0.1
- User Datagram Protocol, Src Port: 39001, Dst Port: 53
- Source Port: 39001
- Destination Port: 53
- Length: 49
- Checksum: 0xbd29 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 2]
- [Timestamps]
- Domain Name System (query)
- Transaction ID: 0x19d1
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- [Response In: 19]

Bottom Screenshot: Packet List and Details

No.	Time	Source	Destination	Protocol	Length	Info
18	4.516063392	192.168.0.101	192.168.0.1	DNS	83	Standard query 0x19d1 A mmx-ds.cdn.whatsapp.net
19	4.526468696	192.168.0.1	192.168.0.101	DNS	99	Standard query response 0x19d1 A mmx-ds.cdn.whatsapp.net A 157.240.204.60
20	4.526737347	192.168.0.101	157.240.204.60	TCP	74	36058 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=152675764 TSecr=0 WS=128
21	4.574308770	157.240.204.60	192.168.0.101	TCP	74	443 → 36058 [SYN, ACK] Seq=0 Ack=1 Win=27760 Len=0 MSS=1400 SACK_PERM=1 TSval=3956840429 TSecr=152675764 WS=128

Packet Details (Frame 19):

- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 69
- Identification: 0xe276 (57974)
- Flags: 0x4000, Don't fragment
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0xd67a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.101
- Destination: 192.168.0.1
- User Datagram Protocol, Src Port: 39001, Dst Port: 53
- Source Port: 39001
- Destination Port: 53
- Length: 49
- Checksum: 0xbd29 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 2]
- [Timestamps]
- Domain Name System (query)
- Transaction ID: 0x19d1
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- [Response In: 19]

Red

arp ndp l2tp eth						
No.	Time	Source	Destination	Protocol	Length	Info
18	4.516063392	192.168.0.101	192.168.0.1	DNS	83	Standard query 0x19d1 A mmx-ds.cdn.whatsapp.net
19	4.526468696	192.168.0.1	192.168.0.101	DNS	99	Standard query response 0x19d1 A mmx-ds.cdn.whatsapp.net A 157.240.204.60
43	4.899417706	192.168.0.101	192.168.0.1	DNS	70	Standard query 0xd125 A google.com
44	4.910700926	192.168.0.1	192.168.0.101	DNS	166	Standard query response 0xd125 A google.com A 64.61.254.226
442	77.451873060	192.168.0.101	192.168.0.1	DNS	89	Standard query 0xf277 A connectivity-check.ubuntu.com
443	77.452135119	192.168.0.101	192.168.0.1	DNS	89	Standard query 0x3441 AAAA connectivity-check.ubuntu.com
446	77.462313518	192.168.0.1	192.168.0.101	DNS	121	Standard query response 0xf277 A connectivity-check.ubuntu.com
453	78.339145540	192.168.0.101	192.168.0.1	DNS	89	Standard query 0x3441 AAAA connectivity-check.ubuntu.com
470	80.089246088	192.168.0.101	192.168.0.1	DNS	89	Standard query 0x3441 AAAA connectivity-check.ubuntu.com
489	83.200819036	192.168.0.1	192.168.0.101	DNS	89	Standard query response 0x3441 AAAA connectivity-check.ubuntu.com
512	89.466735520	192.168.0.101	192.168.0.1	DNS	87	Standard query 0xacea A chat-pa.clients6.google.com
513	89.477104809	192.168.0.1	192.168.0.101	DNS	103	Standard query response 0xacea A chat-pa.clients6.google.com
892	170.463850939	192.168.0.101	192.168.0.1	DNS	89	Standard query 0x50f2 A addons-pa.clients6.google.com
893	170.473491691	192.168.0.1	192.168.0.101	DNS	105	Standard query response 0x50f2 A addons-pa.clients6.google.com
913	170.738537548	192.168.0.101	192.168.0.1	DNS	80	Standard query 0x26c5 A beacons.gcp.gvt2.com
914	170.748134027	192.168.0.1	192.168.0.101	DNS	126	Standard query response 0x26c5 A beacons.gcp.gvt2.com
1199	225.609490863	192.168.0.101	192.168.0.1	DNS	79	Standard query 0x1084 A clients4.google.com
1200	225.619971640	192.168.0.1	192.168.0.101	DNS	199	Standard query response 0x1084 A clients4.google.com

