

WEEK-4

Implementation of a Local DNS Server and Authoritative Name Server

NAME- T. LOHITH SRINIVAS

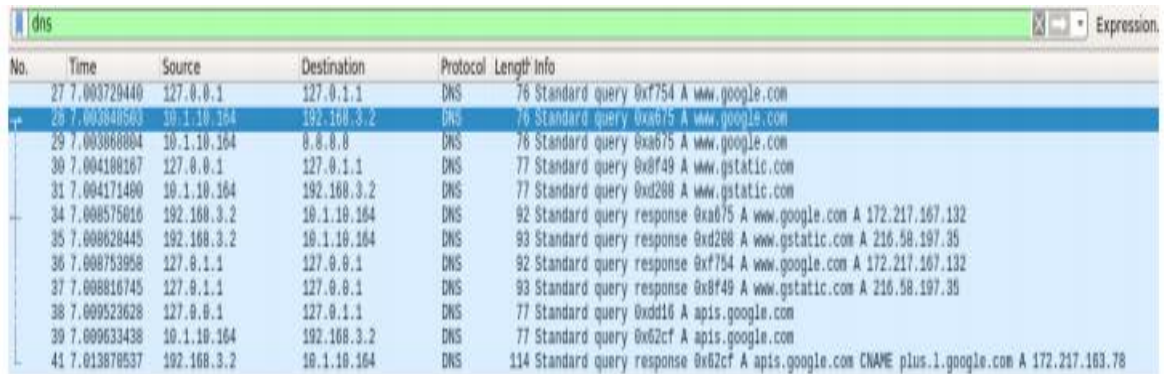
SECTION-D

SRN-PES2UG19CS203

SERVER IP ADDRESS:10.1.10.164

CLIENT IP ADDRESS:10.1.10.111

OBSERVATION 1: Pinging Google.com from Client machine.



The image shows a Wireshark packet capture window titled 'dns'. The packet list pane displays 14 packets. The first packet (No. 27) is a DNS standard query from 127.0.0.1 to 127.0.1.1 for www.google.com. The second packet (No. 28) is a DNS standard query from 10.1.10.164 to 192.168.3.2 for www.google.com. The third packet (No. 29) is a DNS standard query from 10.1.10.164 to 8.8.8.8 for www.google.com. The fourth packet (No. 30) is a DNS standard query from 127.0.0.1 to 127.0.1.1 for www.gstatic.com. The fifth packet (No. 31) is a DNS standard query from 10.1.10.164 to 192.168.3.2 for www.gstatic.com. The sixth packet (No. 34) is a DNS standard query response from 192.168.3.2 to 10.1.10.164 for www.google.com. The seventh packet (No. 35) is a DNS standard query response from 192.168.3.2 to 10.1.10.164 for www.gstatic.com. The eighth packet (No. 36) is a DNS standard query response from 127.0.1.1 to 127.0.0.1 for www.google.com. The ninth packet (No. 37) is a DNS standard query response from 127.0.1.1 to 127.0.0.1 for www.gstatic.com. The tenth packet (No. 38) is a DNS standard query from 127.0.0.1 to 127.0.1.1 for apis.google.com. The eleventh packet (No. 39) is a DNS standard query from 10.1.10.164 to 192.168.3.2 for apis.google.com. The twelfth packet (No. 41) is a DNS standard query response from 192.168.3.2 to 10.1.10.164 for apis.google.com.

No.	Time	Source	Destination	Protocol	Length	Info
27	7.003729440	127.0.0.1	127.0.1.1	DNS	76	Standard query 0xf754 A www.google.com
28	7.003840583	10.1.10.164	192.168.3.2	DNS	76	Standard query 0xa675 A www.google.com
29	7.003868804	10.1.10.164	8.8.8.8	DNS	76	Standard query 0xa675 A www.google.com
30	7.004188167	127.0.0.1	127.0.1.1	DNS	77	Standard query 0x8f49 A www.gstatic.com
31	7.004171400	10.1.10.164	192.168.3.2	DNS	77	Standard query 0xd288 A www.gstatic.com
34	7.008575816	192.168.3.2	10.1.10.164	DNS	92	Standard query response 0xa675 A www.google.com A 172.217.167.132
35	7.008628445	192.168.3.2	10.1.10.164	DNS	93	Standard query response 0xd288 A www.gstatic.com A 216.58.197.35
36	7.008753958	127.0.1.1	127.0.0.1	DNS	92	Standard query response 0xf754 A www.google.com A 172.217.167.132
37	7.008816745	127.0.1.1	127.0.0.1	DNS	93	Standard query response 0x8f49 A www.gstatic.com A 216.58.197.35
38	7.009523628	127.0.0.1	127.0.1.1	DNS	77	Standard query 0xdd16 A apis.google.com
39	7.009633438	10.1.10.164	192.168.3.2	DNS	77	Standard query 0x62cf A apis.google.com
41	7.013878537	192.168.3.2	10.1.10.164	DNS	114	Standard query response 0x62cf A apis.google.com CNAME plus-1.google.com A 172.217.163.78

IT DIDN'T CONTACT THE SERVER ,THE FIRST TIME GOOGLE WAS PINGED.

OBSERVATION 2: - Ping google again to observe if Local DNS responds.

dns						Expression...	+
No.	Time	Source	Destination	Protocol	Length	Info	
7	2.910658129	10.1.10.164	10.1.10.111	DNS	77	Standard query 0xc79c A www.example.com	
8	2.911120851	10.1.10.111	10.1.10.164	DNS	126	Standard query response 0xc79c A www.example.com A 172.16.17.1	
10	3.847347224	10.1.10.111	10.1.10.164	DNS	76	Standard query 0xa1c8 A www.google.com	
11	3.847672469	10.1.10.164	10.1.10.111	DNS	340	Standard query response 0xa1c8 A www.google.com A 172.16.17.1	
19	5.971165791	10.1.10.164	10.1.10.111	DNS	86	Standard query 0x47ff PTR 164.10.1.10.in-addr.arpa	

The local DNS doesn't respond.

FOR OBSERVATION 3, ONWARDS DIFFERENT CLIENT AND
SERVER MACHINES WERE USED WHOSE IP ADDRESSES ARE,

SERVER:10.1.180.34

CLIENT:10.1.180.33

OBSERVATION 3:

The image shows a Wireshark network traffic capture window. The top bar indicates the date and time as Feb 23 15:06. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for packet analysis. The main display area is titled 'dns' and shows a list of captured packets. The first packet (No. 23) is a DNS query from 10.18.180.33 to 10.18.180.34, protocol DNS, length 77 bytes, with info 'Standard query 0xa1fc A ssl.gstatic.com'. The subsequent packets (No. 24 to 345) are DNS responses from 10.18.180.34 to 10.18.180.33, protocol DNS, with various info details including 'Standard query response 0xbbf7 AAAA ssl.gstatic.com AAAA 2404..', 'Standard query response 0xa1fc A ssl.gstatic.com A 216.58.196..', 'Standard query response 0xe9cc A www.google.com', 'Standard query response 0xf6cb AAAA www.google.com', 'Standard query response 0xe9cc Server failure A www.google.com', 'Standard query response 0xf6cb Server failure AAAA www.google.com', 'Standard query response 0xe9cc A www.google.com', 'Standard query response 0xf6cb AAAA www.google.com', 'Standard query response 0x81ff A www.google.com OPT', 'Standard query response 0x8062 AAAA www.google.com OPT', 'Standard query response 0x81ff A www.google.com A 172.217.167..', 'Standard query response 0x8062 AAAA www.google.com AAAA 2404:..', 'Standard query response 0xe9cc A www.google.com A 172.217.167..', 'Standard query response 0xf6cb AAAA www.google.com AAAA 2404:..', 'Standard query response 0x1ed5 PTR 132.167.217.172.in-addr.arpa', 'Standard query response 0x1ed5 PTR 132.167.217.172.in-addr.arpa', 'Standard query response 0x15c0 A mail.google.com', 'Standard query response 0x9ec2 AAAA mail.google.com', 'Standard query response 0xad1f A mail.google.com', 'Standard query response 0x15c0 A mail.google.com CNAME google..', 'Standard query response 0xad1f A mail.google.com CNAME google..', 'Standard query response 0x9ec2 AAAA mail.google.com CNAME goo..', 'Standard query response 0xaf00 A play.google.com', 'Standard query response 0x6fea AAAA play.google.com', 'Standard query response 0xafe0 A play.google.com A 216.58.200..', 'Standard query response 0x6fea AAAA play.google.com AAAA 2404..', 'Standard query response 0x9807 A play.google.com', 'Standard query response 0x4c0d AAAA play.google.com', 'Standard query response 0x9807 A play.google.com A 216.58.200..', 'Standard query response 0x4c0d AAAA play.google.com AAAA 2404..', 'Standard query response 0x5076 A play.google.com', 'Standard query response 0x8a7f AAAA play.google.com', 'Standard query response 0x5076 A play.google.com A 216.58.200..', 'Standard query response 0x8a7f AAAA play.google.com AAAA 2404..', 'Standard query response 0xf35e A mail.google.com', 'Standard query response 0xed22 AAAA mail.google.com', 'Standard query response 0xf35e A mail.google.com CNAME google..', 'Standard query response 0xed22 AAAA mail.google.com CNAME goo..'. The bottom status bar shows 'Packets: 401 · Displayed: 40 (10.0%)' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
23	10.161221792	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xa1fc A ssl.gstatic.com
24	10.161237511	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xbbf7 AAAA ssl.gstatic.com
37	10.236498591	10.18.180.34	10.18.180.33	DNS	105	Standard query response 0xbbf7 AAAA ssl.gstatic.com AAAA 2404..
38	10.237548102	10.18.180.34	10.18.180.33	DNS	93	Standard query response 0xa1fc A ssl.gstatic.com A 216.58.196..
57	17.992329253	10.18.180.33	10.18.180.34	DNS	76	Standard query 0xe9cc A www.google.com
58	17.992345270	10.18.180.33	10.18.180.34	DNS	76	Standard query 0xf6cb AAAA www.google.com
59	17.992848217	10.18.180.34	10.18.180.33	DNS	76	Standard query response 0xe9cc Server failure A www.google.com
60	17.992848683	10.18.180.34	10.18.180.33	DNS	76	Standard query response 0xf6cb Server failure AAAA www.google..
61	17.993093721	127.0.0.1	127.0.0.53	DNS	76	Standard query 0xe9cc A www.google.com
62	17.993124804	127.0.0.1	127.0.0.53	DNS	76	Standard query 0xf6cb AAAA www.google.com
63	17.993658215	10.18.180.33	192.168.3.2	DNS	87	Standard query 0x81ff A www.google.com OPT
64	17.993908963	10.18.180.33	192.168.3.2	DNS	87	Standard query 0x8062 AAAA www.google.com OPT
65	17.994352038	192.168.3.2	10.18.180.33	DNS	103	Standard query response 0x81ff A www.google.com A 172.217.167..
66	17.994352351	192.168.3.2	10.18.180.33	DNS	115	Standard query response 0x8062 AAAA www.google.com AAAA 2404:..
67	17.994626752	127.0.0.53	127.0.0.1	DNS	92	Standard query response 0xe9cc A www.google.com A 172.217.167..
68	17.994822910	127.0.0.53	127.0.0.1	DNS	104	Standard query response 0xf6cb AAAA www.google.com AAAA 2404:..
71	18.037776678	10.18.180.33	10.18.180.34	DNS	90	Standard query 0x1ed5 PTR 132.167.217.172.in-addr.arpa
74	28.456798596	10.18.180.34	10.18.180.33	DNS	128	Standard query response 0x1ed5 PTR 132.167.217.172.in-addr.ar..
87	23.163338966	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x15c0 A mail.google.com
88	23.163344545	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x9ec2 AAAA mail.google.com
89	23.163857543	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xad1f A mail.google.com
90	23.314766025	10.18.180.34	10.18.180.33	DNS	130	Standard query response 0x15c0 A mail.google.com CNAME google..
91	23.314766713	10.18.180.34	10.18.180.33	DNS	130	Standard query response 0xad1f A mail.google.com CNAME google..
95	23.318841103	10.18.180.34	10.18.180.33	DNS	142	Standard query response 0x9ec2 AAAA mail.google.com CNAME goo..
202	39.243474791	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xaf00 A play.google.com
203	39.243490902	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x6fea AAAA play.google.com
204	39.243906089	10.18.180.34	10.18.180.33	DNS	93	Standard query response 0xaf00 A play.google.com A 216.58.200..
205	39.243906402	10.18.180.34	10.18.180.33	DNS	105	Standard query response 0x6fea AAAA play.google.com AAAA 2404..
260	49.350360931	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x9807 A play.google.com
261	49.350377233	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x4c0d AAAA play.google.com
262	49.350876381	10.18.180.34	10.18.180.33	DNS	93	Standard query response 0x9807 A play.google.com A 216.58.200..
263	49.350876741	10.18.180.34	10.18.180.33	DNS	105	Standard query response 0x4c0d AAAA play.google.com AAAA 2404..
290	52.850687799	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x5076 A play.google.com
291	52.850703610	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x8a7f AAAA play.google.com
298	52.925607664	10.18.180.34	10.18.180.33	DNS	93	Standard query response 0x5076 A play.google.com A 216.58.200..
299	52.936348426	10.18.180.34	10.18.180.33	DNS	105	Standard query response 0x8a7f AAAA play.google.com AAAA 2404..
340	63.329455351	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xf35e A mail.google.com
341	63.329460300	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xed22 AAAA mail.google.com
343	63.329894845	10.18.180.34	10.18.180.33	DNS	130	Standard query response 0xf35e A mail.google.com CNAME google..
345	63.330012323	10.18.180.34	10.18.180.33	DNS	142	Standard query response 0xed22 AAAA mail.google.com CNAME goo..

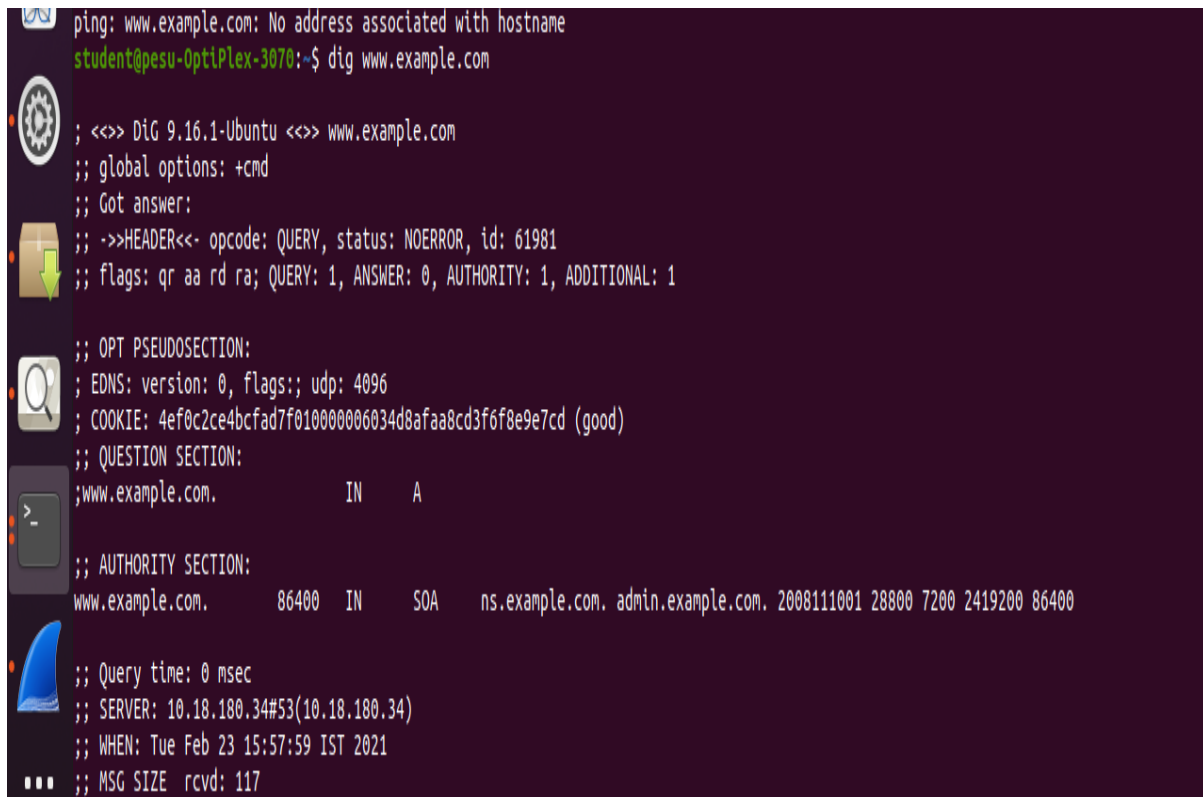
Frame 23: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.18.180.33, Dst: 10.18.180.34
User Datagram Protocol, Src Port: 42851, Dst Port: 53
Domain Name System (query)

0000 00 04 00 01 00 06 00 4e 01 a2 81 40 00 00 00 00N...@....
wireshark_any_20210223150505_2VrmX1.pcapng Packets: 401 · Displayed: 40 (10.0%) Profile: Default

CLIENT OBTAINS DNS RECORD FROM SERVER SUCCESSFULLY.

dig www.example.com

(terminal SCREENSHOT)



```
ping: www.example.com: No address associated with hostname
student@pesu-OptiPlex-3070:~$ dig www.example.com

; <<> DiG 9.16.1-Ubuntu <<> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61981
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

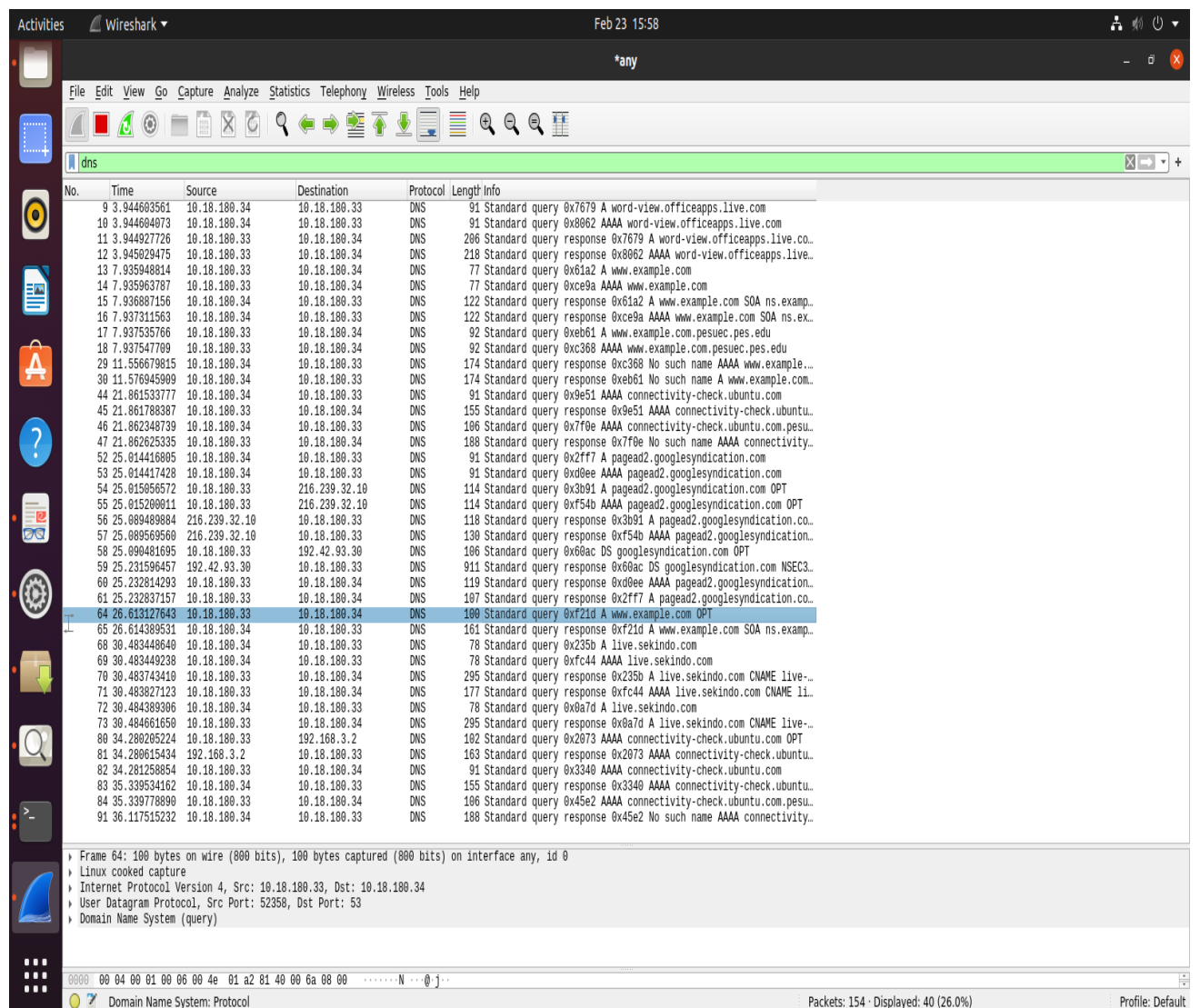
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4ef0c2ce4bcfad7f010000006034d8afaa8cd3f6f8e9e7cd (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

;; AUTHORITY SECTION:
www.example.com.                86400   IN      SOA     ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400

;; Query time: 0 msec
;; SERVER: 10.18.180.34#53(10.18.180.34)
;; WHEN: Tue Feb 23 15:57:59 IST 2021
;; MSG SIZE  rcvd: 117
```

dig www.example.com

(WIRESHARK CAPTURE)



The image shows a Wireshark network traffic capture. The top bar indicates the date and time as Feb 23 15:58. The main window displays a list of captured packets, with the 'dns' filter applied. The packet list shows various DNS queries and responses, including standard queries, responses, and queries for specific domains like 'www.example.com' and 'connectivity-check.ubuntu.com'. The packet details pane on the right shows the structure of the selected packet (Frame 64), including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (query) header. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	3.944663561	10.18.180.34	10.18.180.33	DNS	91	Standard query 0x7679 A word-view.officeapps.live.com
10	3.944664073	10.18.180.34	10.18.180.33	DNS	91	Standard query 0x8062 AAAA word-view.officeapps.live.com
11	3.944927726	10.18.180.33	10.18.180.34	DNS	206	Standard query response 0x7679 A word-view.officeapps.live.co.
12	3.945029475	10.18.180.33	10.18.180.34	DNS	218	Standard query response 0x8062 AAAA word-view.officeapps.live..
13	7.935948814	10.18.180.33	10.18.180.34	DNS	77	Standard query 0x61a2 A www.example.com
14	7.935963787	10.18.180.33	10.18.180.34	DNS	77	Standard query 0xc9a AAAA www.example.com
15	7.936887156	10.18.180.34	10.18.180.33	DNS	122	Standard query response 0x61a2 A www.example.com SOA ns.examp.
16	7.937311563	10.18.180.34	10.18.180.33	DNS	122	Standard query response 0xc9a AAAA www.example.com SOA ns.ex.
17	7.937535766	10.18.180.33	10.18.180.34	DNS	92	Standard query 0xeb61 A www.example.com.pesuec.pes.edu
18	7.937547709	10.18.180.33	10.18.180.34	DNS	92	Standard query 0xc368 AAAA www.example.com.pesuec.pes.edu
29	11.556679815	10.18.180.34	10.18.180.33	DNS	174	Standard query response 0xc368 No such name AAAA www.example...
30	11.576945909	10.18.180.34	10.18.180.33	DNS	174	Standard query response 0xeb61 No such name A www.example.com.
44	21.861533777	10.18.180.34	10.18.180.33	DNS	91	Standard query 0x9e51 AAAA connectivity-check.ubuntu.com
45	21.861788387	10.18.180.33	10.18.180.34	DNS	155	Standard query response 0x9e51 AAAA connectivity-check.ubuntu..
46	21.862340739	10.18.180.34	10.18.180.33	DNS	106	Standard query 0x7f0e AAAA connectivity-check.ubuntu.com.pesu.
47	21.862625335	10.18.180.33	10.18.180.34	DNS	188	Standard query response 0x7f0e No such name AAAA connectivity..
52	25.014416805	10.18.180.34	10.18.180.33	DNS	91	Standard query 0x2ff7 A pagead2.googlesyndication.com
53	25.014417428	10.18.180.34	10.18.180.33	DNS	91	Standard query 0xd0ee AAAA pagead2.googlesyndication.com
54	25.015056572	10.18.180.33	216.239.32.10	DNS	114	Standard query 0x3b91 A pagead2.googlesyndication.com OPT
55	25.015200011	10.18.180.33	216.239.32.10	DNS	114	Standard query 0xf54b AAAA pagead2.googlesyndication.com OPT
56	25.089489884	216.239.32.10	10.18.180.33	DNS	118	Standard query response 0x3b91 A pagead2.googlesyndication.co.
57	25.089569560	216.239.32.10	10.18.180.33	DNS	130	Standard query response 0xf54b AAAA pagead2.googlesyndication..
58	25.089481695	10.18.180.33	192.42.93.30	DNS	106	Standard query 0x60ac DS googlesyndication.com OPT
59	25.231596457	192.42.93.30	10.18.180.33	DNS	911	Standard query response 0x60ac DS googlesyndication.com NSEC3.
60	25.232814293	10.18.180.33	10.18.180.34	DNS	119	Standard query response 0xd0ee AAAA pagead2.googlesyndication..
61	25.232837157	10.18.180.33	10.18.180.34	DNS	107	Standard query response 0x2ff7 A pagead2.googlesyndication.co.
64	26.613127643	10.18.180.33	10.18.180.34	DNS	100	Standard query 0xf21d A www.example.com OPT
65	26.614389531	10.18.180.34	10.18.180.33	DNS	161	Standard query response 0xf21d A www.example.com SOA ns.examp.
68	30.483448640	10.18.180.34	10.18.180.33	DNS	78	Standard query 0x235b A live.sekindo.com
69	30.483449238	10.18.180.34	10.18.180.33	DNS	78	Standard query 0xfc44 AAAA live.sekindo.com
70	30.483743410	10.18.180.33	10.18.180.34	DNS	295	Standard query response 0x235b A live.sekindo.com CNAME live..
71	30.483827123	10.18.180.33	10.18.180.34	DNS	177	Standard query response 0xfc44 AAAA live.sekindo.com CNAME li.
72	30.484389306	10.18.180.34	10.18.180.33	DNS	78	Standard query 0x0a7d A live.sekindo.com
73	30.484661650	10.18.180.33	10.18.180.34	DNS	295	Standard query response 0x0a7d A live.sekindo.com CNAME live..
80	34.280295224	10.18.180.33	192.168.3.2	DNS	102	Standard query 0x2073 AAAA connectivity-check.ubuntu.com OPT
81	34.280615434	192.168.3.2	10.18.180.33	DNS	163	Standard query response 0x2073 AAAA connectivity-check.ubuntu..
82	34.281258854	10.18.180.33	10.18.180.34	DNS	91	Standard query 0x3340 AAAA connectivity-check.ubuntu.com
83	35.339534162	10.18.180.34	10.18.180.33	DNS	155	Standard query response 0x3340 AAAA connectivity-check.ubuntu..
84	35.339778890	10.18.180.33	10.18.180.34	DNS	106	Standard query 0x45e2 AAAA connectivity-check.ubuntu.com.pesu.
91	36.117515232	10.18.180.34	10.18.180.33	DNS	188	Standard query response 0x45e2 No such name AAAA connectivity..

Frame 64: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.18.180.33, Dst: 10.18.180.34
User Datagram Protocol, Src Port: 52358, Dst Port: 53
Domain Name System (query)

0000 00 04 00 01 00 06 00 4e 01 a2 81 40 00 6a 00 00N...@j..

Domain Name System: Protocol

Packets: 154 · Displayed: 40 (26.0%)

Profile: Default

