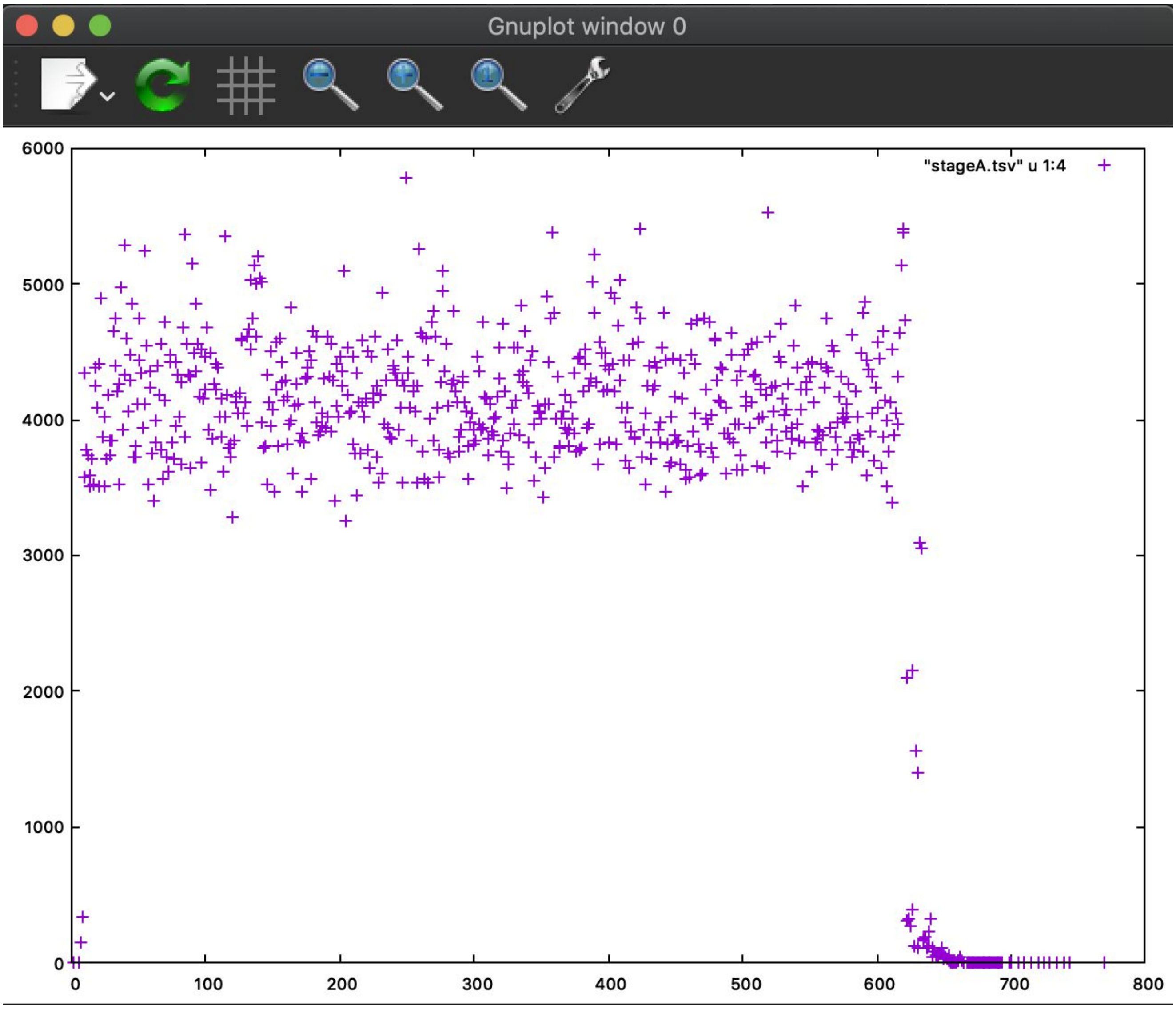
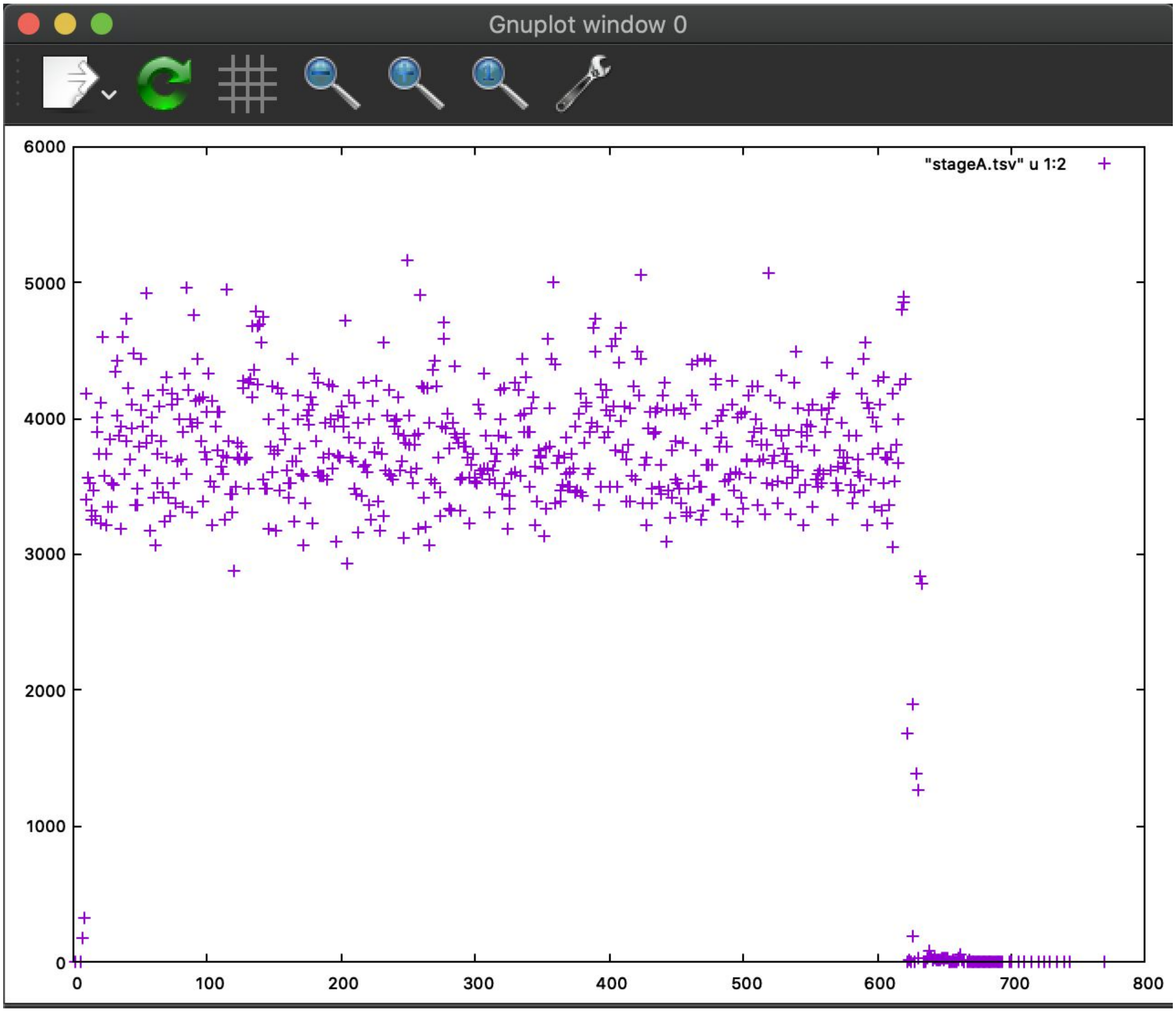
STAGE- 1 : OFFLINE ANALYSIS USING TSHARK

1. Graphs for incoming and outgoing traffic from server obtained from the pacp dump are as follows:

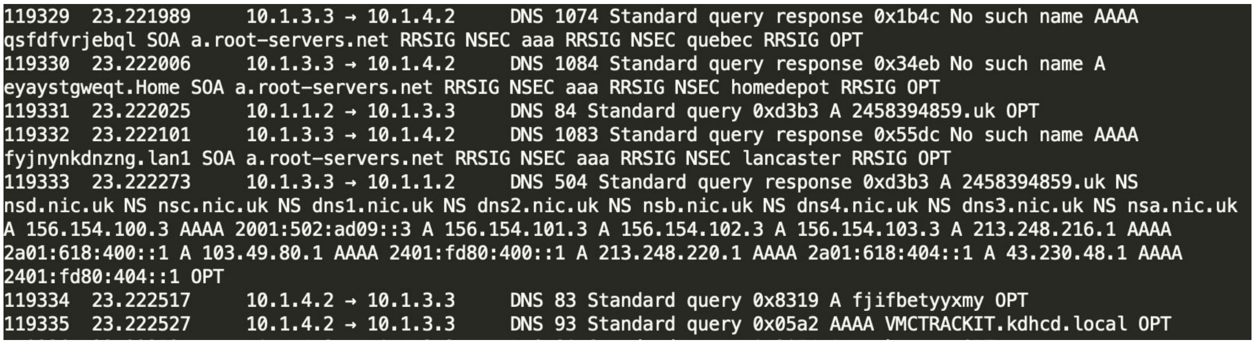
    ❑ Incoming traffic graph:



- ❏ Outgoing traffic graph:

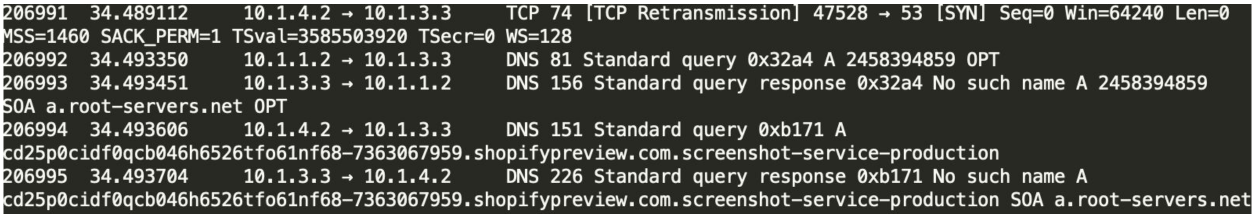


2. Analyse UDP and TCP queries using tshark and pcap dump
    a) Output for the UDP query : dig a \2458394859.uk



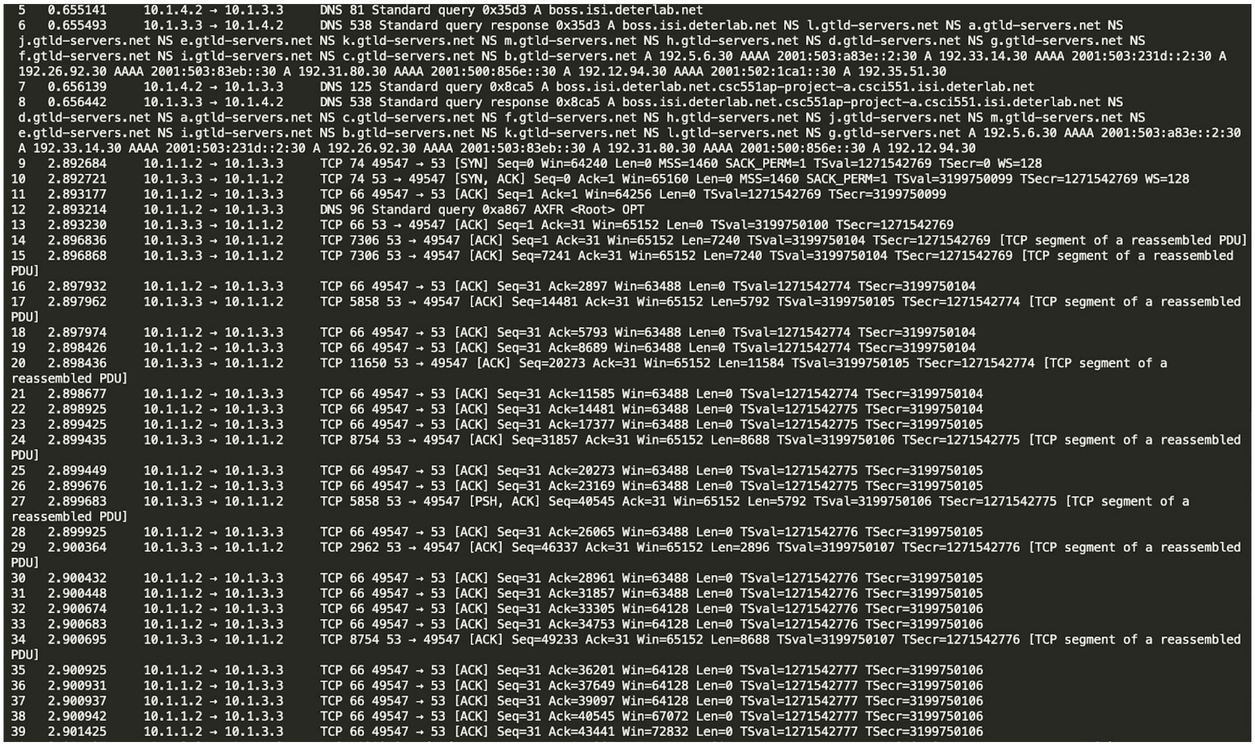
```
119329  23.221989     10.1.3.3 → 10.1.4.2     DNS 1074 Standard query response 0x1b4c No such name AAAA
qsfdfvrjebql SOA a.root-servers.net RRSIG NSEC aaa RRSIG NSEC quebec RRSIG OPT
119330  23.222006     10.1.3.3 → 10.1.4.2     DNS 1084 Standard query response 0x34eb No such name A
eyaystgweqt.Home SOA a.root-servers.net RRSIG NSEC aaa RRSIG NSEC homedepot RRSIG OPT
119331  23.222025     10.1.1.2 → 10.1.3.3     DNS 84 Standard query 0xd3b3 A 2458394859.uk OPT
119332  23.222101     10.1.3.3 → 10.1.4.2     DNS 1083 Standard query response 0x55dc No such name AAAA
fyjnynkdnzng.lan1 SOA a.root-servers.net RRSIG NSEC aaa RRSIG NSEC lancaster RRSIG OPT
119333  23.222273     10.1.3.3 → 10.1.1.2     DNS 504 Standard query response 0xd3b3 A 2458394859.uk NS
nsd.nic.uk NS nsc.nic.uk NS dns1.nic.uk NS dns2.nic.uk NS nsb.nic.uk NS dns4.nic.uk NS dns3.nic.uk NS nsa.nic.uk
A 156.154.100.3 AAAA 2001:502:ad09::3 A 156.154.101.3 A 156.154.102.3 A 156.154.103.3 A 213.248.216.1 AAAA
2a01:618:400::1 A 103.49.80.1 AAAA 2401:fd80:400::1 A 213.248.220.1 AAAA 2a01:618:404::1 A 43.230.48.1 AAAA
2401:fd80:404::1 OPT
119334  23.222517     10.1.4.2 → 10.1.3.3     DNS 83 Standard query 0x8319 A fjifbetyyxmy OPT
119335  23.222527     10.1.4.2 → 10.1.3.3     DNS 93 Standard query 0x05a2 AAAA VMCTRACKIT.kdhcd.local OPT
```

b) Output for the UDP query : dig a \2458394859.



```
206991  34.489112     10.1.4.2 → 10.1.3.3     TCP 74 [TCP Retransmission] 47528 → 53 [SYN] Seq=0 Win=64240 Len=0
MSS=1460 SACK_PERM=1 TSval=3585503920 TSecr=0 WS=128
206992  34.493350     10.1.1.2 → 10.1.3.3     DNS 81 Standard query 0x32a4 A 2458394859 OPT
206993  34.493451     10.1.3.3 → 10.1.1.2     DNS 156 Standard query response 0x32a4 No such name A 2458394859
SOA a.root-servers.net OPT
206994  34.493606     10.1.4.2 → 10.1.3.3     DNS 151 Standard query 0xb171 A
cd25p0cidf0qcb046h6526tfo61nf68-7363067959.shopifypreview.com.screenshot-service-production
206995  34.493704     10.1.3.3 → 10.1.4.2     DNS 226 Standard query response 0xb171 No such name A
cd25p0cidf0qcb046h6526tfo61nf68-7363067959.shopifypreview.com.screenshot-service-production SOA a.root-servers.net
```

c) Output for the TCP query : dig axfr . 10.1.3.3 (IP Address of the server)



```
 5   0.655141     10.1.4.2 → 10.1.3.3     DNS 81 Standard query 0x35d3 A boss.isi.deterlab.net
 6   0.655493     10.1.3.3 → 10.1.4.2     DNS 538 Standard query response 0x35d3 A boss.isi.deterlab.net NS l.gtld-servers.net NS a.gtld-servers.net NS
 j.gtld-servers.net NS e.gtld-servers.net NS k.gtld-servers.net NS m.gtld-servers.net NS h.gtld-servers.net NS d.gtld-servers.net NS g.gtld-servers.net NS
 f.gtld-servers.net NS i.gtld-servers.net NS c.gtld-servers.net NS b.gtld-servers.net A 192.5.6.30 AAAA 2001:503:a83e::2:30 A 192.33.14.30 AAAA 2001:503:231d::2:30 A
 192.26.92.30 AAAA 2001:503:83eb::30 A 192.31.80.30 AAAA 2001:500:856e::30 A 192.12.94.30 AAAA 2001:502:1ca1::30 A 192.35.51.30
 7   0.656139     10.1.4.2 → 10.1.3.3     DNS 125 Standard query 0x8ca5 A boss.isi.deterlab.net.csc551ap-project-a.csci551.isi.deterlab.net
 8   0.656442     10.1.3.3 → 10.1.4.2     DNS 538 Standard query response 0x8ca5 A boss.isi.deterlab.net.csc551ap-project-a.csci551.isi.deterlab.net NS
 d.gtld-servers.net NS a.gtld-servers.net NS c.gtld-servers.net NS f.gtld-servers.net NS h.gtld-servers.net NS j.gtld-servers.net NS m.gtld-servers.net NS
 e.gtld-servers.net NS i.gtld-servers.net NS b.gtld-servers.net NS k.gtld-servers.net NS l.gtld-servers.net NS g.gtld-servers.net A 192.5.6.30 AAAA 2001:503:a83e::2:30
 A 192.33.14.30 AAAA 2001:503:231d::2:30 A 192.26.92.30 AAAA 2001:503:83eb::30 A 192.31.80.30 AAAA 2001:500:856e::30 A 192.12.94.30
 9   2.892684     10.1.1.2 → 10.1.3.3     TCP 74 49547 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1271542769 TSecr=0 WS=128
10   2.892721     10.1.3.3 → 10.1.1.2     TCP 74 53 → 49547 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3199750099 TSecr=1271542769 WS=128
11   2.893177     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1271542769 TSecr=3199750099
12   2.893214     10.1.1.2 → 10.1.3.3     DNS 96 Standard query 0xa867 AXFR <Root> OPT
13   2.893230     10.1.3.3 → 10.1.1.2     TCP 66 53 → 49547 [ACK] Seq=1 Ack=31 Win=65152 Len=0 TSval=3199750100 TSecr=1271542769
14   2.896836     10.1.3.3 → 10.1.1.2     TCP 7306 53 → 49547 [ACK] Seq=1 Ack=31 Win=65152 Len=7240 TSval=3199750104 TSecr=1271542769 [TCP segment of a reassembled PDU]
15   2.896868     10.1.3.3 → 10.1.1.2     TCP 7306 53 → 49547 [ACK] Seq=7241 Ack=31 Win=65152 Len=7240 TSval=3199750104 TSecr=1271542769 [TCP segment of a reassembled
PDU]
16   2.897932     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=2897 Win=63488 Len=0 TSval=1271542774 TSecr=3199750104
17   2.897962     10.1.3.3 → 10.1.1.2     TCP 5858 53 → 49547 [ACK] Seq=14481 Ack=31 Win=65152 Len=5792 TSval=3199750105 TSecr=1271542774 [TCP segment of a reassembled
PDU]
18   2.897974     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=5793 Win=63488 Len=0 TSval=1271542774 TSecr=3199750104
19   2.898426     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=8689 Win=63488 Len=0 TSval=1271542774 TSecr=3199750104
20   2.898436     10.1.3.3 → 10.1.1.2     TCP 11650 53 → 49547 [ACK] Seq=20273 Ack=31 Win=65152 Len=11584 TSval=3199750105 TSecr=1271542774 [TCP segment of a
reassembled PDU]
21   2.898677     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=11585 Win=63488 Len=0 TSval=1271542774 TSecr=3199750104
22   2.898925     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=14481 Win=63488 Len=0 TSval=1271542775 TSecr=3199750104
23   2.899425     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=17377 Win=63488 Len=0 TSval=1271542775 TSecr=3199750105
24   2.899435     10.1.3.3 → 10.1.1.2     TCP 8754 53 → 49547 [ACK] Seq=31857 Ack=31 Win=65152 Len=8688 TSval=3199750106 TSecr=1271542775 [TCP segment of a reassembled
PDU]
25   2.899449     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=20273 Win=63488 Len=0 TSval=1271542775 TSecr=3199750105
26   2.899676     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=23169 Win=63488 Len=0 TSval=1271542775 TSecr=3199750105
27   2.899683     10.1.3.3 → 10.1.1.2     TCP 5858 53 → 49547 [PSH, ACK] Seq=40545 Ack=31 Win=65152 Len=5792 TSval=3199750106 TSecr=1271542775 [TCP segment of a
reassembled PDU]
28   2.899925     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=26065 Win=63488 Len=0 TSval=1271542776 TSecr=3199750105
29   2.900364     10.1.3.3 → 10.1.1.2     TCP 2962 53 → 49547 [ACK] Seq=46337 Ack=31 Win=65152 Len=2896 TSval=3199750107 TSecr=1271542776 [TCP segment of a reassembled
PDU]
30   2.900432     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=28961 Win=63488 Len=0 TSval=1271542776 TSecr=3199750105
31   2.900448     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=31857 Win=63488 Len=0 TSval=1271542776 TSecr=3199750105
32   2.900674     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=33305 Win=64128 Len=0 TSval=1271542776 TSecr=3199750106
33   2.900683     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=34753 Win=64128 Len=0 TSval=1271542776 TSecr=3199750106
34   2.900695     10.1.3.3 → 10.1.1.2     TCP 8754 53 → 49547 [ACK] Seq=49233 Ack=31 Win=65152 Len=8688 TSval=3199750107 TSecr=1271542776 [TCP segment of a reassembled
PDU]
35   2.900925     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=36201 Win=64128 Len=0 TSval=1271542777 TSecr=3199750106
36   2.900931     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=37649 Win=64128 Len=0 TSval=1271542777 TSecr=3199750106
37   2.900937     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=39097 Win=64128 Len=0 TSval=1271542777 TSecr=3199750106
38   2.900942     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=40545 Win=67072 Len=0 TSval=1271542777 TSecr=3199750106
39   2.901425     10.1.1.2 → 10.1.3.3     TCP 66 49547 → 53 [ACK] Seq=31 Ack=43441 Win=72832 Len=0 TSval=1271542777 TSecr=3199750106
```

3. Following are the responses of the 2 UDP queries:

a) dig a \2458394859.uk : 0 (NOERROR)

b) dig a \2458394859. : 3 (NXDOMAIN)

The response codes for both the queries **are different**. As the domain name is invalid for the second query, it returned with the response code of 3 stating the same. On the contrary, for the first query as the domain name is valid, it returned a no error response code of 0.