Sean Poston
Wireshark DNS & Python DNS

nslookup

1. www.aiit.or.kr – 58.229.6.225
2. (Trinity College Dublin) tcd.ie

```
Non-authoritative answer:
tcd.ie  nameserver = auth-ns3.tcd.ie
tcd.ie  nameserver = auth-ns2.tcd.ie
tcd.ie  nameserver = auth-ns2.ucd.ie
tcd.ie  nameserver = auth-ns1.tcd.ie
```

3. nslookup mail.yahoo.com auth-ns3.tcd.ie
   Address: 193.1.193.161

ipconfig

1. ipconfig /displaydns

```
Windows IP Configuration

    1.0.0.127.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 1.0.0.127.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 505127
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : localhost


    fcmconnection.googleapis.com
    ----------------------------------------
    Record Name . . . . . : fcmconnection.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 51
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 172.217.5.10


    aka.ms
```
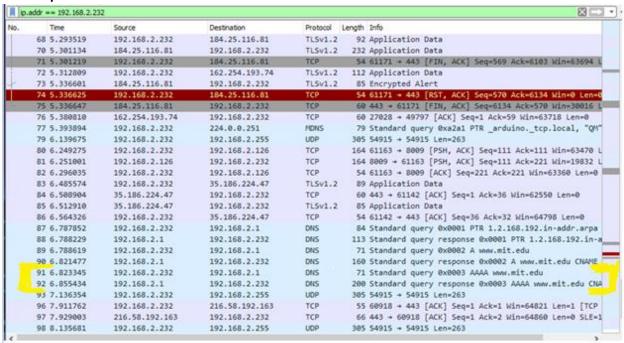
Sean Poston
Wireshark DNS & Python DNS

Tracing DNS with Wireshark

www.ietf.org

		ip.addr == 192.168.2.232				

No.	Time	Source	Destination	Protocol	Length	Info
1170	26.434242	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=606104 Ack=2564 Win=65535 Len
1171	26.434385	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=607564 Ack=2564 Win=65535 Len
1172	26.434393	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=609024 Win=64400 Len
1173	26.434508	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=609024 Ack=2564 Win=65535 Len
1174	26.434720	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=610484 Ack=2564 Win=65535 Len
1175	26.434728	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=611944 Win=64400 Len
1176	26.434843	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [PSH, ACK] Seq=611944 Ack=2564 Win=6553
1177	26.436278	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=613404 Ack=2564 Win=65535 Len
1178	26.436286	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=614864 Win=64400 Len
1179	26.436415	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=614864 Ack=2564 Win=65535 Len
1180	26.436625	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=616324 Ack=2564 Win=65535 Len
1181	26.436633	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=617784 Win=64400 Len
1182	26.436748	172.67.33.249	192.168.2.232	TLSv1.3	1514	Application Data [TCP segment of a reassembled PDU]
1183	26.436965	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=619244 Ack=2564 Win=65535 Len
1184	26.436973	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=620704 Win=64400 Len
1185	26.437087	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [PSH, ACK] Seq=620704 Ack=2564 Win=6553
1186	26.438221	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=622164 Ack=2564 Win=65535 Len
1187	26.438229	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=623624 Win=64400 Len
1188	26.438345	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=623624 Ack=2564 Win=65535 Len
1189	26.438558	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=625084 Ack=2564 Win=65535 Len
1190	26.438566	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=626544 Win=64400 Len
1191	26.438680	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=626544 Ack=2564 Win=65535 Len
1192	26.438920	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [ACK] Seq=628004 Ack=2564 Win=65535 Len
1193	26.438925	192.168.2.232	172.67.33.249	TCP	54	60841 → 443 [ACK] Seq=2564 Ack=629464 Win=64400 Len
1194	26.439004	172.67.33.249	192.168.2.232	TCP	1514	443 → 60841 [PSH, ACK] Seq=629464 Ack=2564 Win=6553
1195	26.439829	4.31.198.44	192.168.2.232	TCP	60	443 → 60842 [ACK] Seq=1 Ack=518 Win=30016 Len=0
1196	26.440984	4.31.198.44	192.168.2.232	TLSv1.2	1514	Server Hello

nslookup

		ip.addr == 192.168.2.232				

No.	Time	Source	Destination	Protocol	Length	Info
68	5.293519	192.168.2.232	184.25.116.81	TLSv1.2	92	Application Data
70	5.301134	184.25.116.81	192.168.2.232	TLSv1.2	232	Application Data
71	5.301219	192.168.2.232	184.25.116.81	TCP	54	61171 → 443 [FIN, ACK] Seq=569 Ack=6103 Win=63694 L
72	5.312809	192.168.2.232	162.254.193.74	TLSv1.2	112	Application Data
73	5.336601	184.25.116.81	192.168.2.232	TLSv1.2	85	Encrypted Alert
74	5.336625	192.168.2.232	184.25.116.81	TCP	54	61171 → 443 [RST, ACK] Seq=570 Ack=6134 Win=0 Len=0
75	5.336647	184.25.116.81	192.168.2.232	TCP	60	443 → 61171 [FIN, ACK] Seq=6134 Ack=570 Win=30016 L
76	5.380810	162.254.193.74	192.168.2.232	TCP	60	27028 → 49797 [ACK] Seq=1 Ack=59 Win=63718 Len=0
77	5.393894	192.168.2.232	224.0.0.251	MDNS	79	Standard query 0xa2a1 PTR _arduino._tcp.local, "QM"
79	6.139675	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
80	6.249275	192.168.2.232	192.168.2.126	TCP	164	61163 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=63470 L
81	6.251001	192.168.2.126	192.168.2.232	TCP	164	8009 → 61163 [PSH, ACK] Seq=111 Ack=221 Win=19832 L
82	6.296035	192.168.2.232	192.168.2.126	TCP	54	61163 → 8009 [ACK] Seq=221 Ack=221 Win=63360 Len=0
83	6.485574	192.168.2.232	35.186.224.47	TLSv1.2	89	Application Data
84	6.508904	35.186.224.47	192.168.2.232	TCP	60	443 → 61142 [ACK] Seq=1 Ack=36 Win=62550 Len=0
85	6.512910	35.186.224.47	192.168.2.232	TLSv1.2	85	Application Data
86	6.564326	192.168.2.232	35.186.224.47	TCP	54	61142 → 443 [ACK] Seq=36 Ack=32 Win=64798 Len=0
87	6.787852	192.168.2.232	192.168.2.1	DNS	84	Standard query 0x0001 PTR 1.2.168.192.in-addr.arpa
88	6.788229	192.168.2.1	192.168.2.232	DNS	113	Standard query response 0x0001 PTR 1.2.168.192.in-a
89	6.788619	192.168.2.232	192.168.2.1	DNS	71	Standard query 0x0002 A www.mit.edu
90	6.821477	192.168.2.1	192.168.2.232	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME
91	6.823345	192.168.2.232	192.168.2.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
92	6.855434	192.168.2.1	192.168.2.232	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNA
93	7.136354	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
96	7.911762	192.168.2.232	216.58.192.163	TCP	55	60918 → 443 [ACK] Seq=1 Ack=1 Win=64821 Len=1 [TCP
97	7.929003	216.58.192.163	192.168.2.232	TCP	66	443 → 60918 [ACK] Seq=1 Ack=2 Win=64860 Len=0 SLE=1
98	8.135681	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263

Sean Poston
Wireshark DNS & Python DNS

nslookup -type=NS mit.edu

ip.addr == 192.168.2.232

No.	Time	Source	Destination	Protocol	Length	Info
29	3.766375	192.168.2.232	192.168.2.126	TCP	54	61163 → 8009 [ACK] Seq=111 Ack=111 Win=63250 Len=0
31	4.006736	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
34	5.007695	192.168.2.232	172.217.0.4	TCP	62	61205 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
35	5.008816	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
36	5.026694	172.217.0.4	192.168.2.232	TCP	62	443 → 61205 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
37	5.026738	192.168.2.232	172.217.0.4	TCP	54	61205 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
38	5.026890	192.168.2.232	172.217.0.4	TLSv1	571	Client Hello
39	5.045712	172.217.0.4	192.168.2.232	TCP	60	443 → 61205 [ACK] Seq=1 Ack=518 Win=65535 Len=0
40	5.055491	172.217.0.4	192.168.2.232	TLSv1.3	1484	Server Hello, Change Cipher Spec
41	5.055735	172.217.0.4	192.168.2.232	TLSv1.3	1259	Application Data
42	5.055747	192.168.2.232	172.217.0.4	TCP	54	61205 → 443 [ACK] Seq=518 Ack=2636 Win=64350 Len=0
43	5.056313	192.168.2.232	172.217.0.4	TLSv1.3	118	Change Cipher Spec, Application Data
44	5.079549	172.217.0.4	192.168.2.232	TCP	60	443 → 61205 [ACK] Seq=2636 Ack=582 Win=65535 Len=0
46	5.621055	192.168.2.232	192.168.2.1	DNS	84	Standard query 0x0001 PTR 1.2.168.192.in-addr.arpa
47	5.621436	192.168.2.1	192.168.2.232	DNS	113	Standard query response 0x0001 PTR 1.2.168.192.in-a
48	5.621816	192.168.2.232	192.168.2.1	DNS	67	Standard query 0x0002 NS mit.edu
49	5.643685	192.168.2.1	192.168.2.232	DNS	234	Standard query response 0x0002 NS mit.edu NS usw2.a
50	5.772139	192.168.2.232	224.0.0.251	MDNS	79	Standard query 0x6c08 PTR _arduino._tcp.local, "QM"
53	6.009916	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
54	6.500627	192.168.2.232	239.255.255.250	UDP	698	61278 → 3702 Len=656
55	6.642298	192.168.2.232	192.168.2.126	TCP	164	55871 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=63140 L
56	6.644881	192.168.2.126	192.168.2.232	TCP	164	8009 → 55871 [PSH, ACK] Seq=111 Ack=221 Win=19832 L
57	6.689115	192.168.2.232	192.168.2.126	TCP	54	55871 → 8009 [ACK] Seq=221 Ack=221 Win=63030 Len=0
58	6.689240	192.168.2.232	239.255.255.250	UDP	698	61278 → 3702 Len=656
60	7.007923	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
61	7.069689	192.168.2.232	239.255.255.250	UDP	698	61278 → 3702 Len=656

nslookup www.google.com asia1.akam.net (aiit.or.kr doesn't seem to exist anymore)

ip.addr == 192.168.2.232

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.232	192.168.2.126	TCP	164	55871 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=63030 Len=110 [TC
2	0.006624	192.168.2.126	192.168.2.232	TCP	164	8009 → 55871 [PSH, ACK] Seq=1 Ack=111 Win=19832 Len=110 [
3	0.046786	192.168.2.232	192.168.2.126	TCP	54	55871 → 8009 [ACK] Seq=111 Ack=111 Win=62920 Len=0
4	0.056535	192.168.2.232	224.0.0.251	MDNS	79	Standard query 0x1823 PTR _arduino._tcp.local, "QM" quest
6	0.911406	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
8	1.918437	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
9	2.093199	192.168.2.232	95.100.175.64	DNS	86	Standard query 0x0001 PTR 64.175.100.95.in-addr.arpa
10	2.150044	95.100.175.64	192.168.2.232	DNS	86	Standard query response 0x0001 Refused PTR 64.175.100.95.
11	2.150923	192.168.2.232	95.100.175.64	DNS	74	Standard query 0x0002 A www.google.com
12	2.185219	192.168.2.232	192.168.2.126	TCP	164	61163 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=63140 Len=110 [T
13	2.186669	192.168.2.126	192.168.2.232	TCP	164	8009 → 61163 [PSH, ACK] Seq=1 Ack=111 Win=19832 Len=110
14	2.207504	95.100.175.64	192.168.2.232	DNS	90	Standard query response 0x0002 A www.google.com A 8.8.8.8
15	2.207738	192.168.2.232	95.100.175.64	DNS	74	Standard query 0x0003 AAAA www.google.com
16	2.232967	192.168.2.232	192.168.2.126	TCP	54	61163 → 8009 [ACK] Seq=111 Ack=111 Win=63030 Len=0
17	2.264242	95.100.175.64	192.168.2.232	DNS	143	Standard query response 0x0003 AAAA www.google.com SOA a1
18	2.917688	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263
20	3.913420	192.168.2.232	192.168.2.255	UDP	305	54915 → 54915 Len=263

Sean Poston
Wireshark DNS & Python DNS

Python DNS

seanpocs480@gmail.com
to to_email ▾

We are sending an email using Python and Gmail, how fun! We can fill this with html, and gmail supports a decent range of css style attributes too - https://developers.google.com/gmail/design/css#example.

Mail Delivery Subsystem <mailer-daemon@googlemail.com>
to me ▾

Address not found

Your message wasn't delivered to **to_email@gmail.com** because the address couldn't be found, or is unable to receive mail.

LEARN MORE

The response was:

550 5.1.1 The email account that you tried to reach does not exist. Please try double-checking the recipient's email address for typos or unnecessary spaces. Learn more at https://su