

Lab 2

AbdelRahman Adel AbdelFattah
17012296

1. nslookup

```
1. nslookup www.asdu.ait.ac.th
   Server:      192.168.1.1
   Address: 192.168.1.1#53
```

```
Non-authoritative answer:
www.asdu.ait.ac.th canonical name = www.misu.ait.ac.th.
Name: www.misu.ait.ac.th
Address: 203.159.12.3
```

```
2. nslookup -type=NS www.can.ac.uk
   Server:      192.168.1.1
   Address: 192.168.1.1#53
```

```
Non-authoritative answer:
*** Can't find www.can.ac.uk: No answer
```

```
Authoritative answers can be found from:
can.ac.uk
  origin = ns0.ulcc.ac.uk
  mail addr = hostmaster.ulcc.ac.uk
  serial = 1999081101
  refresh = 28800
  retry = 7200
  expire = 604800
  minimum = 86400
```

```
3. Request always timeout for some reason, no matter what internet.
```

2. ipconfig/ifconfig

```
→ ~ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 16:cc:4d:cf:a2:4b
    inet6 fe80::14cc:4dff:fecf:a24b%anpi0 prefixlen 64 scopeid 0x4
    nd6 options=201<PERFORMNUD,DAD>
    media: none
    status: inactive
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 16:cc:4d:cf:a2:4c
    inet6 fe80::14cc:4dff:fecf:a24c%anpi1 prefixlen 64 scopeid 0x5
    nd6 options=201<PERFORMNUD,DAD>
    media: none
    status: inactive
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 16:cc:4d:cf:a2:2b
    nd6 options=201<PERFORMNUD,DAD>
    media: none
    status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 16:cc:4d:cf:a2:2c
    nd6 options=201<PERFORMNUD,DAD>
    media: none
    status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TS04,TS06,CHANNEL_IO>
    ether 36:26:3d:b0:c7:c0
    media: autoselect <full-duplex>
    status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TS04,TS06,CHANNEL_IO>
    ether 36:26:3d:b0:c7:c4
    media: autoselect <full-duplex>
    status: inactive
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 72:ed:3c:24:87:4e
    media: autoselect
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 50:ed:3c:24:87:4e
    inet6 fe80::18f9:c5d:c452:d289%en0 prefixlen 64 secured scopeid 0xb
    inet 192.168.1.30 netmask 0xffffffff broadcast 192.168.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM,TXCSUM,TS04,TS06>
```

3. Tracing DNS with Wireshark

- Source Port: 43301 - Destination Port: 53
 - Destination Address: 192.168.1.1 (same as local address)
 - type A, class IN
 - 3 answers containing(Name, Type, Class, TTL, data Length, Address):
 - www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
 - www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
 - www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
 - Yes SYN contains Destination Address: 104.16.45.99
 - Yes multiple queries were sent before the images were retrieved.
-
- Source Port: 52849 - Destination Port: 53
 - Source Address: 192.168.1.19 - Destination Address: 192.168.1.1
 - www.mit.edu: type A, class IN

- 3 answers (Name, Type, Class, TTL, Data Length, CNAME):
www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 92.122.34.235

```

ip.addr == 192.168.1.19 && dns
...
804 17:23:56.476186 192.168.1.1 192.168.1.19 DNS 160 Standard query response 0xf072 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 92.122.34.235
...
> Frame 245: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0
> Ethernet II, Src: zte_39:89:00 (74:b5:7e:39:89:00), Dst: Apple_24:87:4e (50:ed:3c:24:87:4e)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.19
> User Datagram Protocol, Src Port: 53, Dst Port: 52849
> Domain Name System (response)
  Transaction ID: 0xf072
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  Queries
  > www.mit.edu: type A, class IN
  Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type A, class IN, addr 92.122.34.235
  [Request In: 206]
  [Time: 0.157596000 seconds]
  
```

nslookup -type=NS mit.edu is giving me a timeout no matter what is being done.

nslookup www.aitt.or.kr bitsy.mit.edu is giving a timeout no matter what is being done.