Tracing DNS with Wireshark

Now that we are familiar with *nslookup* and *ipconfig*, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web-surfing activity.

- Use *ipconfig* to empty the DNS cache in your host.
- Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
- Open Wireshark and enter "ip.addr == your_IP_address" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: http://www.ietf.org
- Stop packet capture.

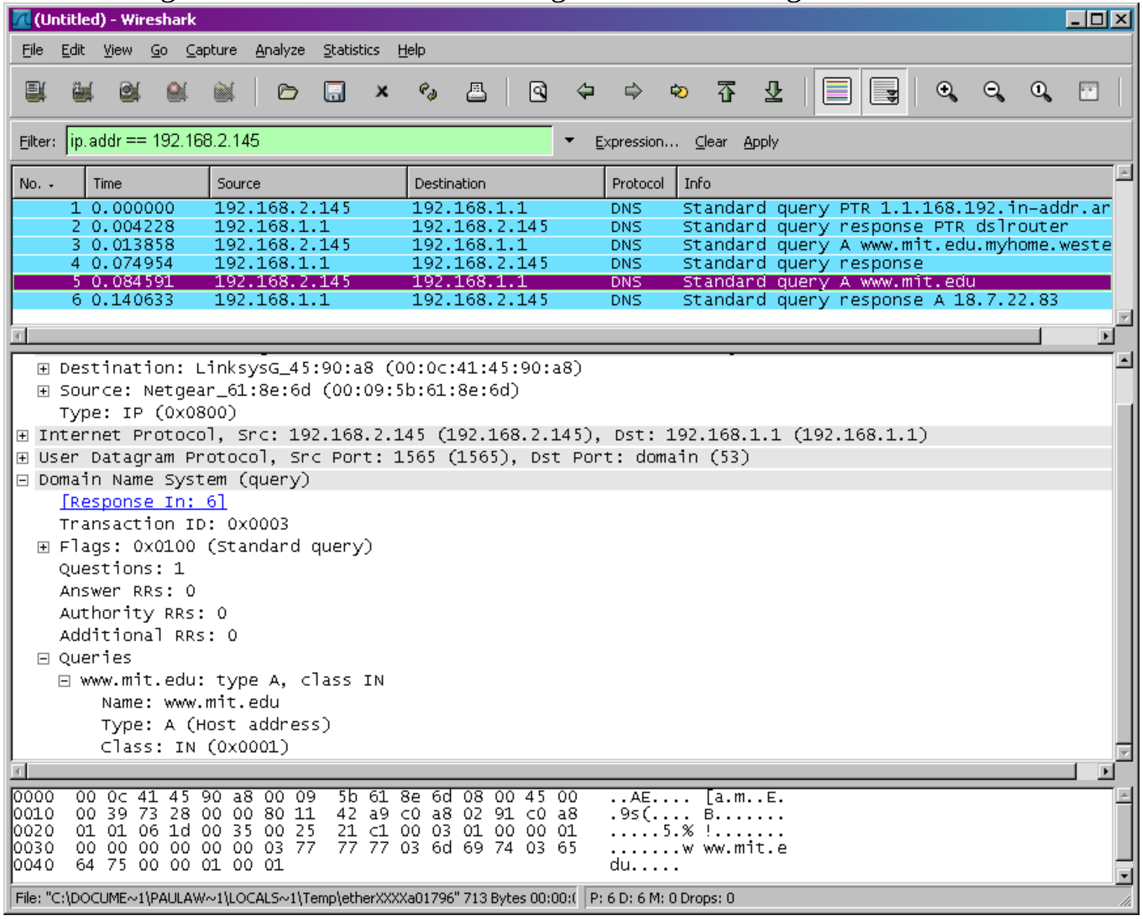
Answer the following questions.

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Now let's play with *nslookup*.

- Start packet capture.
- Do an *nslookup* on www.mit.edu
- Stop packet capture.

You should get a trace that looks something like the following:



(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: ip.addr == 192.168.2.145

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.145	192.168.1.1	DNS	Standard query PTR 1.1.168.192.in-addr.ar
2	0.004228	192.168.1.1	192.168.2.145	DNS	Standard query response PTR dslrouter
3	0.013858	192.168.2.145	192.168.1.1	DNS	Standard query A www.mit.edu.myhome.weste
4	0.074954	192.168.1.1	192.168.2.145	DNS	Standard query response
5	0.084591	192.168.2.145	192.168.1.1	DNS	Standard query A www.mit.edu
6	0.140633	192.168.1.1	192.168.2.145	DNS	Standard query response A 18.7.22.83

```
  ⊞ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
  ⊞ Source: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: 1565 (1565), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 6]
    Transaction ID: 0x0003
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.mit.edu: type A, class IN
        Name: www.mit.edu
        Type: A (Host address)
        Class: IN (0x0001)
```

```
0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  00 39 73 28 00 00 80 11  42 a9 c0 a8 02 91 c0 a8   .9s(.... B.......
0020  01 01 06 1d 00 35 00 25  21 c1 00 03 01 00 00 01   .....5.% !.......
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 00 00 01 00 01                               du.....
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa01796" 713 Bytes 00:00:(P: 6 D: 6 M: 0 Drops: 0

We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

8. What is the destination port for the DNS query message? What is the source port of DNS response message?
9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Now repeat the previous experiment, but instead issue the command:

```
nslookup –type=NS mit.edu
```

Answer the following questions:

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
14. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

Now repeat the previous experiment, but instead issue the command:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Answer the following questions:

15. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
16. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
17. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?