Internet Protocols Midterm #3

2016. 5. 23

Student ID _____ Name _____

1. DNS is highly dependent on caching. Thus answers coming back from the DNS system are predominantly non-authoritative. But there is one way you can force an authoritative answer. The following is how you use nslookup to get the authoritative answer for query type "A" on the cnn.com domain. Fill the three empty brackets. **[9pts]**

Step	***Your action***
1	Start nslookup.
	Set query type to [**ns**].
2	Type cnn.com.
3	Use [**server**] command to point your query at <the output of step 2>.
4	Set query type to A.
5	Type [**cnn.com**].

2. If you typed google.co.kr in nslookup *immediately after* Step 5 in Prob. 1, what result would you get? Explain why. **[5pts]**

Error – the authoritative name server for cnn.com domain does not have RRs for google.co.kr domain.

3. In the following IGMPv2 trace that is captured at a set-top box for Korea Telecom's IPTV,

No.	Time	Source	Destination	Info
32173	47.317590	118.48.34.143	233.18.158.62	Membership Report group 233.18.158.62
32177	47.335167	61.72.223.167	233.18.158.52	Membership Query, specific for group 233.18.158.52
32979	48.337557	61.72.223.167	233.18.158.52	Membership Query, specific for group 233.18.158.52
34092	49.696186	118.48.34.143	224.0.0.2	Leave Group 233.18.158.62

A. What is the IP address of the set-top box? _____ **118.48.34.143**_____ **[2pts]**

B. What group did this client leave just before packet #32173? _____ **233.18.158.52**____ **[3pts]**

C. What is the IP address of the multicast router? ____ **61.72.223.167**____ **[2pts]**

D. What is the TTL value of these IGMP messages? _____ **1**_____ **[3pts]**

E. Why do we have identical packets in #32177 and #32979? Explain briefly. __ **To make sure the IGMP query is delivered to any remaining members of 233.18.158.52**_____ **[3pts]**

F. What is the AS number of Korea Telecom (in hexadecimal)? _____ **0x129E**_____ **[3pts]**

G. With the group addressing scheme used in the trace, how many channels can Korea Telecom IPTV create under the ASM model at maximum? ___ 256_____[3pts]

4. The netstat command shows you the TCP connections and their states on your machine. The following figure shows an example of netstat output. For these TCP connections appearing in the example output,

```
TCP    10.16.30.142:13735     203.252.15.181:443     ESTABLISHED
TCP    10.16.30.142:13737     10.16.8.51:7676        TIME_WAIT
TCP    10.16.30.142:13738     211.115.106.78:80      CLOSE_WAIT
TCP    10.16.30.142:13740     89.149.159.203:25793   SYN_SENT
TCP    10.16.30.142:13741     10.16.27.34:7676       TIME_WAIT
TCP    10.16.30.142:13742     211.115.106.78:80      CLOSE_WAIT
TCP    10.16.30.142:13743     89.149.159.214:80      SYN_SENT
TCP    10.16.30.142:13744     163.152.8.53:8443      SYN_SENT
TCP    10.16.30.142:13745     89.149.159.112:80      SYN_SENT
TCP    10.16.30.142:13746     89.149.159.209:80      SYN_SENT
```

A. How many connections are in the 3-way handshake (i.e., connection establishment)? _____ 5_____ [3pts]

B. For how many connections did 10.16.30.142 send the first FIN segment? _____ 2_____ [3pts]

C. How many connections are in normal data exchange? _____ 1_____[3pts]

5. The following TCP trace shows the setup and the termination of a connection (data exchange part is omitted).

No.	Time	Source	Destination	Info
8418	86.346041	10.16.30.142	64.233.189.239	12668 > 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8443	86.409622	64.233.189.239	10.16.30.142	443 > 12668 [SYN, ACK] Seq=0 Ack=1 Win=43152 Len=0 MSS=1380 SACK_PERM=1
8444	86.409688	10.16.30.142	64.233.189.239	12668 > 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0

…

17004	149.083421	10.16.30.142	64.233.189.239	12668 > 443 [FIN, ACK] Seq=789 Ack=5757 Win=16384 Len=0
17028	149.145223	64.233.189.239	10.16.30.142	443 > 12668 [FIN, ACK] Seq=5757 Ack=790 Win=45312 Len=0
17029	149.145277	10.16.30.142	64.233.189.239	12668 > 443 [ACK] Seq=790 Ack=5758 Win=16384 Len=0

A. What MSS would this connection use for the data exchange? 1380 (bytes) [3pts]

B. In packet #17004, what would be the *actual* value written in the window size field in the TCP header? (Hint: Window Scale option) ___ 64_____[4pts]

C. How many data bytes did this connection transport from 10.16.30.142 to 64.233.189.239? _____ 788_____[4pts]

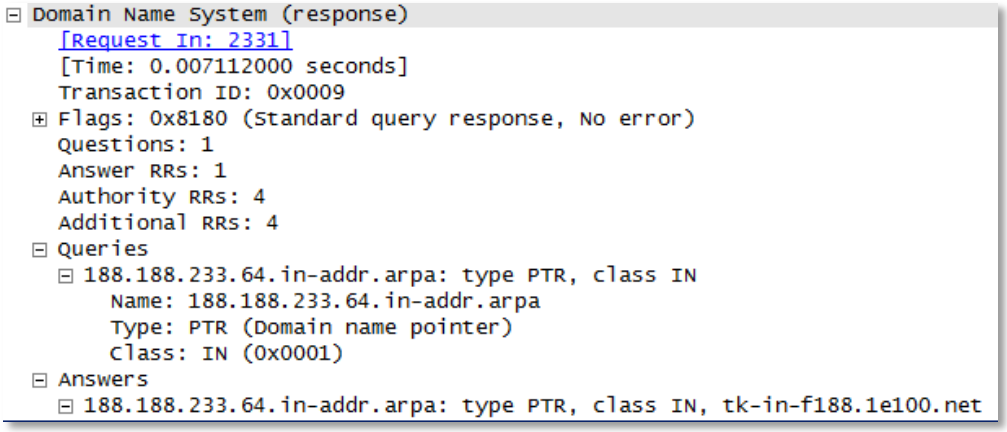
D. How many data bytes did this connection transport from 64.233.189.239 to 10.16.30.142? _____ 5756_____[4pts]

E. Which value tells you that these are all signaling packets (i.e., carrying no data)? _____ Len=0_____[2pts]

6. In the following DNS response packet,

   A. How many bytes would the first domain name (188.188.233.64.in-addr.arpa) in the *Answers* section take for its representation in the DNS packet? _____ **2** _____ **[4pts]**

   B. What is the IP address that is being queried about? _____ **64.233.188.188** _____ **[3pts]**



7. The following output is a result of a DNS query.

   A. What was the query type? _____ **SOA** _____ **[2pts]**

   B. If you have any question about the administration of the domain, where can you send an email? ___ **root@kuccgx.korea.ac.kr** _____ **[2pts]**

   C. How many times a day does the secondary name server check if a zone transfer is necessary? _____ **4** _____ **[3pts]**

   D. Why would Korea University Computing Center place the two authoritative name servers on different subnets? Provide a brief explanation. **[5pts]**

Putting both servers on the same subnet would jeopardize the entire service in case the subnet fails.

```
korea.ac.kr
        primary name server = kuccgx.korea.ac.kr
        responsible mail addr = root.kuccgx.korea.ac.kr
        serial  = 2016052004
        refresh = 21600 (6 hours)
        retry   = 600 (10 mins)
        expire  = 604800 (7 days)
        default TTL = 21600 (6 hours)
korea.ac.kr     nameserver = kucc.korea.ac.kr
korea.ac.kr     nameserver = kuccgx.korea.ac.kr
kucc.korea.ac.kr        internet address = 163.152.11.6
kuccgx.korea.ac.kr      internet address = 163.152.1.1
```

8. The following trace is obtained for the output in Prob. 7.

   A. Why the first two queries that lead to the NXDOMAIN error? Answer by explaining how the nslookup is thought to be configured. **[5pts]**

Nslookup is configured to try the two suffixes (korea.ac.kr. & ac.kr.) in case the input domain name is not FQDN.

B. How can you prevent the problem? __ **Use FQDN by putting a dot at the end of the input domain name, i.e., "korea.ac.kr." not "korea.ac.kr"** **[3pts]**

No.	Time	Source	Destination	Info
1575	10.883499	10.16.30.142	163.152.1.1	Standard query SOA korea.ac.kr.korea.ac.kr
1576	10.886751	163.152.1.1	10.16.30.142	Standard query response, No such name
1577	10.887499	10.16.30.142	163.152.1.1	Standard query SOA korea.ac.kr.ac.kr
1581	10.901172	163.152.1.1	10.16.30.142	Standard query response, No such name
1582	10.901927	10.16.30.142	163.152.1.1	Standard query SOA korea.ac.kr
1584	10.905783	163.152.1.1	10.16.30.142	Standard query response SOA kuccgx.korea.ac.kr

9. In Prob. 3, if we observe other traffic from the set-top box, we can see SNMP traps being generated and sent to somewhere every time we change the channel (see below). Provide a plausible explanation. (Hint: `whois` shows that `218.144.152.143` is an address that belongs to Korea Telecom.) **[3pts]**

KT is monitoring subscriber's channel selection (for various reasons such as charging and rating).

No.	Time	Source	Destination	Info
6701	7.540178	118.48.34.143	224.0.0.251	V2 Membership Report / Join group 224.0.0.251
7521	8.491038	118.48.34.143	233.18.158.113	V2 Membership Report / Join group 233.18.158.113
7529	8.508187	118.48.34.143	224.0.0.2	V2 Leave Group 233.18.158.113
7530	8.508192	118.48.34.143	233.18.158.68	V2 Membership Report / Join group 233.18.158.68
7541	8.548014	118.48.34.143	218.144.152.143	sNMPv2-Trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.
9644	11.138496	118.48.34.143	233.18.158.68	V2 Membership Report / Join group 233.18.158.68
9904	11.455507	118.48.34.143	224.0.0.2	V2 Leave Group 233.18.158.68
9905	11.455723	118.48.34.143	233.18.158.104	V2 Membership Report / Join group 233.18.158.104
9922	11.495011	118.48.34.143	218.144.152.143	sNMPv2-Trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.
10682	13.221827	118.48.34.143	233.18.158.104	V2 Membership Report / Join group 233.18.158.104
10972	13.867681	118.48.34.143	224.0.0.2	V2 Leave Group 233.18.158.104
10992	13.967882	118.48.34.143	218.144.152.143	sNMPv2-Trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.

10. The following is the trace we obtain when we try `telnet spam.korea.ac.kr 25` on a command window, after which we immediately push the Close ("X") button.

No.	Source	Destination	Info
1596	10.16.30.142	163.152.6.23	2075 > 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1599	163.152.6.23	10.16.30.142	25 > 2075 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1380 SACK_PERM=1 WS=128
1600	10.16.30.142	163.152.6.23	2075 > 25 [ACK] Seq=1 Ack=1 Win=16384 Len=0
1610	163.152.6.23	10.16.30.142	S: 220 smtp1.korea.ac.kr ESMTP imoxion SensMail SmtpServer 8.0; Fri, 20 May 2016
1639	10.16.30.142	163.152.6.23	2075 > 25 [ACK] Seq=1 Ack=95 Win=16384 Len=0
1640	163.152.6.23	10.16.30.142	[TCP Retransmission] S: 220 smtp1.korea.ac.kr ESMTP imoxion SensMail SmtpServer 8
1641	10.16.30.142	163.152.6.23	[TCP Dup ACK 1639#1] 2075 > 25 [ACK] Seq=1 Ack=95 Win=16384 Len=0 SLE=1 SRE=95
1839	10.16.30.142	163.152.6.23	2075 > 25 [FIN, ACK] Seq=1 Ack=95 Win=16384 Len=0
1840	163.152.6.23	10.16.30.142	S: 221 Bye
1841	10.16.30.142	163.152.6.23	2075 > 25 [RST, ACK] Seq=2 Ack=104 Win=0 Len=0
1842	163.152.6.23	10.16.30.142	25 > 2075 [FIN, ACK] Seq=104 Ack=2 Win=14720 Len=0

A. What do you think caused the retransmission at packet #1640? _____
Loss of ACK (#1639)_____ **[3pts]**

B. Which is the first packet that pressing the Close ("X") button trigger? _
#1839_____**[2pts]**

C. What event caused the client (10.16.30.142) to send a RST in #1841? __
Server sends data (#1840) after the client's FIN (#1839) instead of a FIN **[3pts]**

D. How many characters does the welcome message from the mail server (packet #1610) contain? _____ **94**_____**[3pts]**