Incourse Exam (Special)
3rd year 1st Semester 2020
CSE3102: Computer Networks

Time: 1 Hour

Q1. Fig.1-3 show 2 packets (DNS) captured and analyzed by Wireshark. Answer the following questions: (10)

a) What is the IP of the DNS server?
b) What does the client want to know from the DNS server?
c) Can you say whether the answers which the client gets was directly from DNS server's cache or not?
d) You can see that there are multiple answers. Write down the significance of each answer.
e) How can you tell whether the DNS response packet (Fig. 2, 3) is associated with the DNS query (Fig. 1) or not?

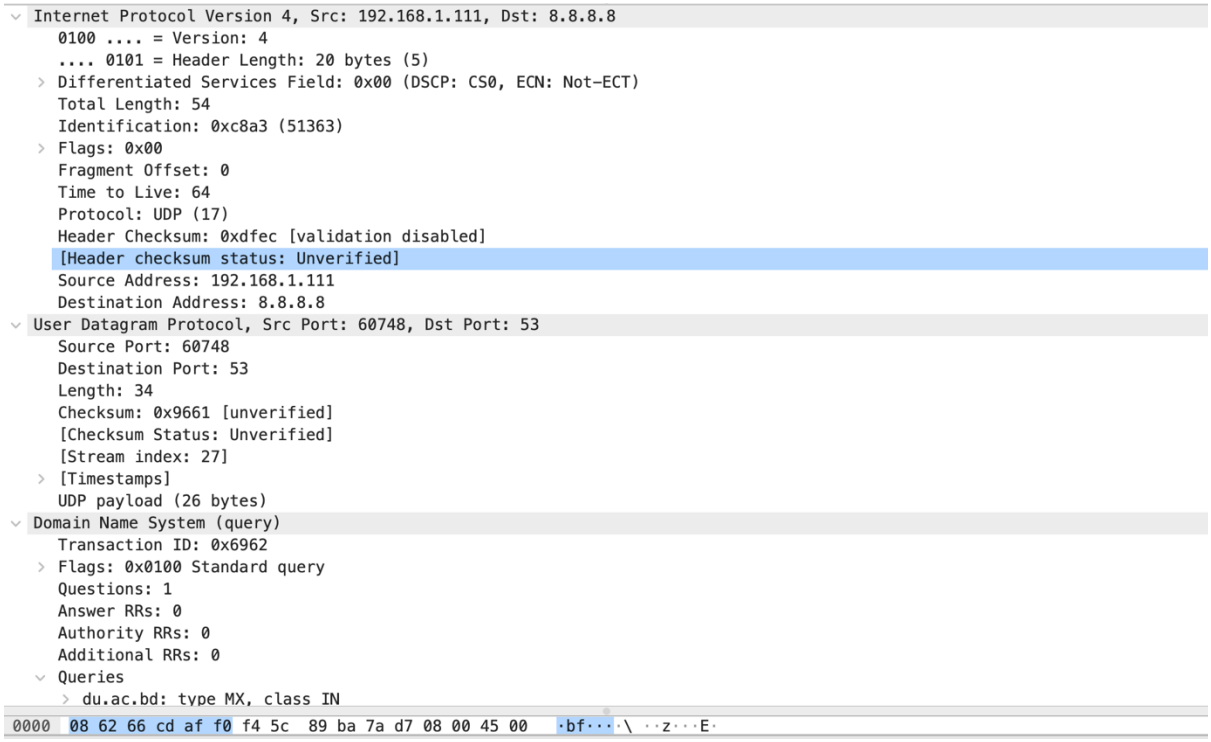

Fig. 1: Packet 1

```
> Frame 235: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface en0, id 0
> Ethernet II, Src: ASUSTekC_cd:af:f0 (08:62:66:cd:af:f0), Dst: Apple_ba:7a:d7 (f4:5c:89:ba:7a:d7)
v Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.111
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 233
      Identification: 0xab39 (43833)
    > Flags: 0x00
      Fragment Offset: 0
      Time to Live: 55
      Protocol: UDP (17)
      Header Checksum: 0x05a4 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 8.8.8.8
      Destination Address: 192.168.1.111
v User Datagram Protocol, Src Port: 53, Dst Port: 60748
      Source Port: 53
      Destination Port: 60748
      Length: 213
      Checksum: 0x1fb7 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 27]
    > [Timestamps]
      UDP payload (205 bytes)
v Domain Name System (response)
      Transaction ID: 0x6962
    > Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 7
      Authority RRs: 0
      Additional RRs: 0
    v Queries
      > du.ac.bd: type MX, class IN
    v Answers
      v du.ac.bd: type MX, class IN, preference 30, mx aspmx2.googlemail.com
            Name: du.ac.bd
            Type: MX (Mail eXchange) (15)
            Class: IN (0x0001)
            Time to live: 1079 (17 minutes, 59 seconds)
            Data length: 25
            Preference: 30
            Mail Exchange: aspmx2.googlemail.com
      v du.ac.bd: type MX, class IN, preference 10, mx aspmx.l.google.com
            Name: du.ac.bd
            Type: MX (Mail eXchange) (15)
            Class: IN (0x0001)
            Time to live: 1079 (17 minutes, 59 seconds)
```

Fig 2. Packet 2 (1/2)

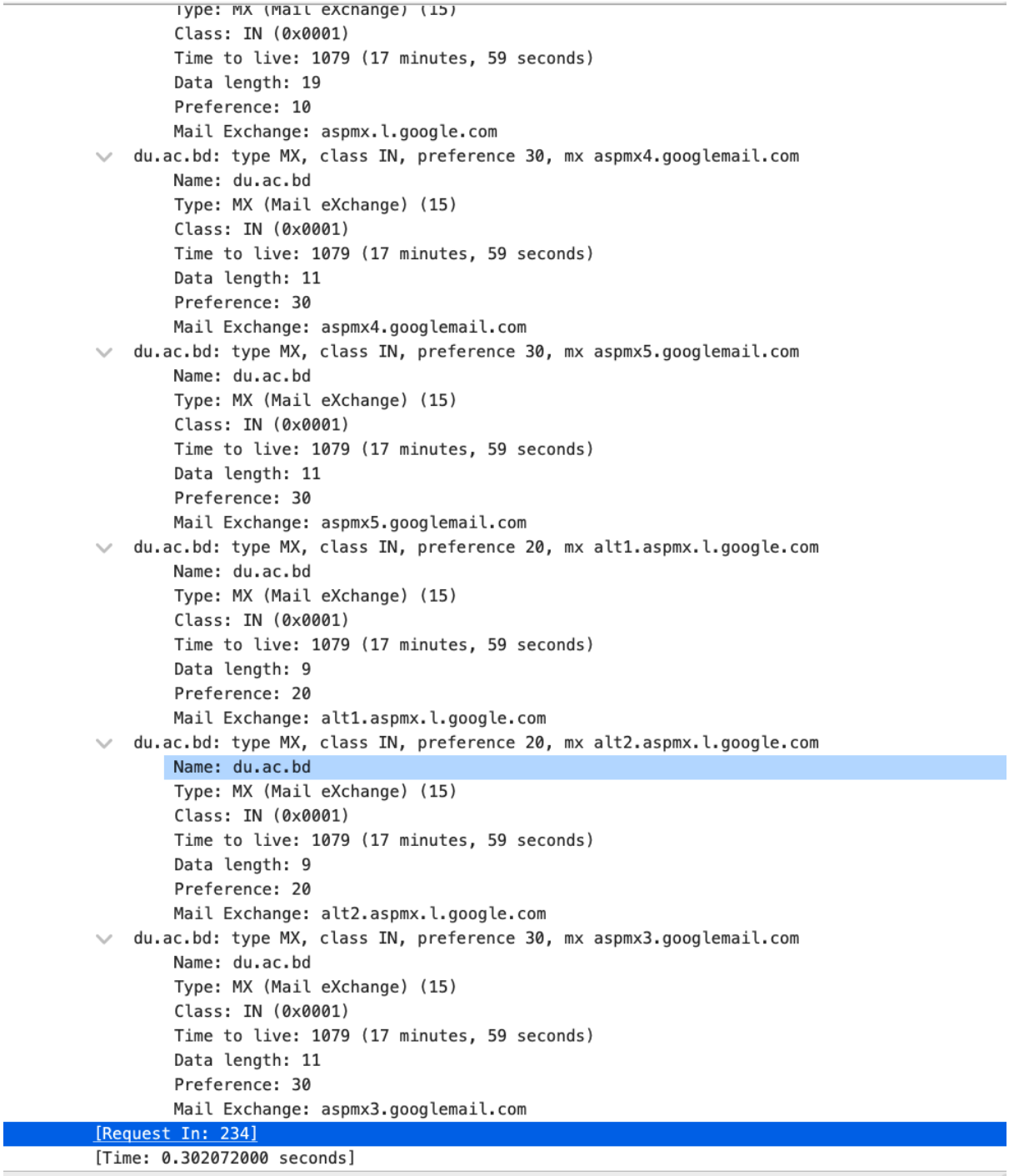

Fig. 3: Packet 2 (2/2)

Q2. In order to prevent content piracy, some companies tend to disrupt P2P services by deploying decoys (i.e. misbehaving peers meant to disrupt downloads by other peers). Company A deployed a peer which advertises all chunks and sends fake content to others. On the other hand, company B deployed a peer which advertises all chunks but never sends any (fake or original) to others but repeatedly connects to other peers. Which method is more effective in disrupting P2P services and why? (10)

Q3. Consider the delay introduced by the TCP slow-start phase. Consider a client and a Web server directly connected by one link of rate *R*. Suppose the client wants to retrieve an object whose size is exactly equal to 11 *S*, where *S* is the maximum segment size (MSS). The round-trip time between client and server is RTT (assumed to be constant). Ignoring protocol headers, determine the time to retrieve the object (including TCP connection establishment) when $S/R > RTT$. Show the packet exchange timing diagram. (10)