CNT 4704: Computer Networking
Mid-Term Exam

Oct. 28, 2015

Instructions:

- The exam is open everything, including books, notes, and computers.
- The total number of points for each question is given in parenthesis. There are 100 points total.
- Show all your work. Partial credit is possible for an incorrect answer, but only if you show some correct intermediate steps in obtaining the answer.

Affidavit:

I certify that I have finished this exam solely by myself without any discussion or help from any other persons.

Student Name:

PID:

Question 1: Knowledge questions (20points)

Answer each of the following questions *briefly, i.e., in at most a few sentences.*

a). What is the major differences between TCP and UDP? Why DNS usually uses UDP instead of TCP for its service?

b). According to the course's textbook, how many layers are included in the Internet (give their names too)? Give one example of application, or protocol, or device, that corresponding to each layer.

c). What does "TTL" mean? What is the usage of TTL in DNS resource record? What is the usage of TTL in packet IP header?

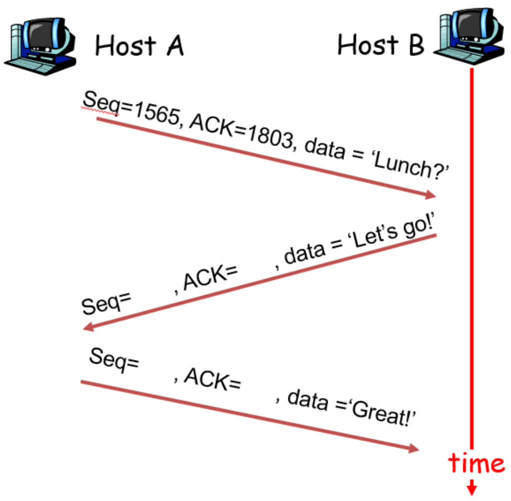
d). Suppose a web server has 2 ongoing TCP connections. How many server-side sockets are used? How many server-side port numbers are used? (Hint: remember the server implements fork() as introduced in lectures)

e). What is the standard size of a TCP header? What is the standard size of a UDP header? What fields exist in both TCP header and UDP header?

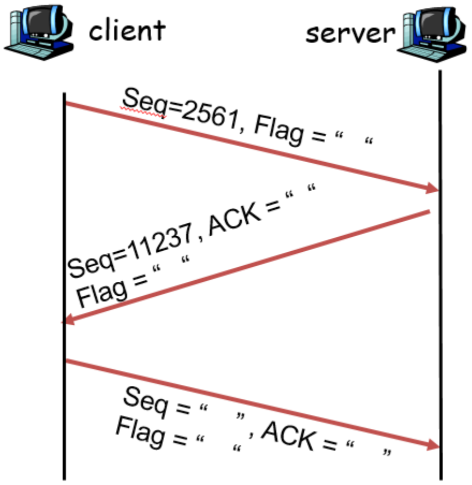
f). Comparing the transmission efficiency of the three MAC protocol, slotted ALOHA, pure ALOHA, CSMA/CD, which one has the highest efficiency? Which one has the lowest efficiency?

Question 2: TCP protocol (20 points)

Suppose the TCP packet transmission between host A and host B (or a client and a server) follow the following scenarios, fill in the missing sequence number and ack number (for the TCP connection setup scenario, fill in the TCP packet flag value as well).


Host A
Host B
Seq=1565, ACK=1803, data = 'Lunch?'
Seq= , ACK= , data = 'Let's go!'
Seq= , ACK= , data ='Great!'
time

TCP seq/ack number



TCP connection setup (Flag
are the values used in TCP packet header flag field)

Question 3: Packet checksum and CRC calculation (20 points)

1). Suppose a packet contains four 16-bit data, which are represented by hexadecimal format as 0xFF35, 0xDB4D, 0x951C, 0xA999. Compute the checksum for this packet. Show all your work.

2). For the data D = “01100110”, the divisor G = “10011”, what is the CRC code R?

Question 4: DNS service (20 points)

Suppose you want to email a reporter called ‘Alice’ in National Public Radio. Her email address is alice@npr.org. Now you are curious how NPR’s email works. You can log in to Eustis or Eustis2 Linux machines in our department (or use your own Linux machine), then run “dig” command. Please try to find answers to the following questions:

(1). What is the domain name of the email server used by @npr.org? please show the dig command line you are using.

(2). What are the IP addresses of the NPR’s email server? (it has more than one IP address) please show the dig command line you are using.

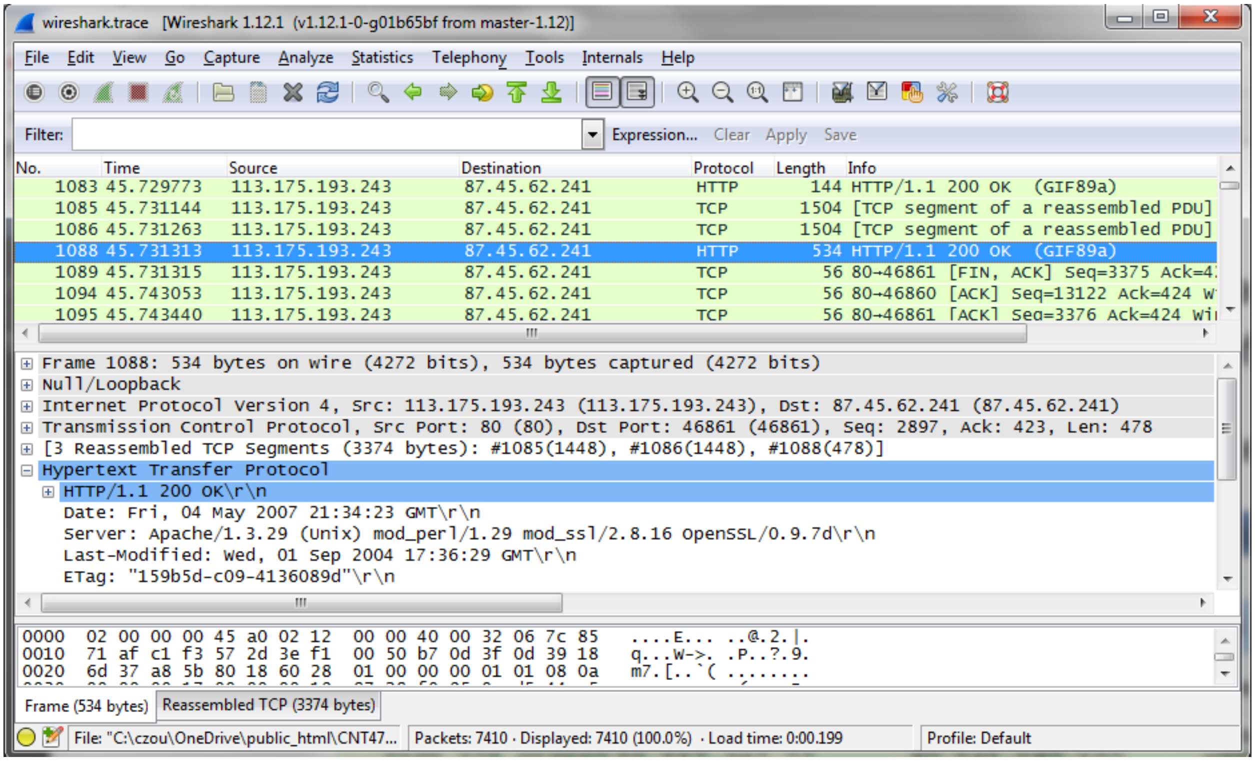
Question 5: Wireshark Packet Monitoring (20 points)

This question tests your ability to analyze Wireshark packet capturing file. On Webcourse the midterm assignment tab, it provides a Wireshark trace file “wireshar.trace”. It is one trace file provided by Drs. Paxson/Wagner in UC Berkeley in their course “CS161: computer security” in Spring 2010: http://www-inst.eecs.berkeley.edu/~cs161/sp10/projects/proj2.pdf

Please download it and open it by Wireshark by using Wireshark menu “File”→”Open…”. Then answer the following questions.

(1). There are several DNS servers that have been queried by various clients in this packet capturing file. Please show the IP addresses of these DNS servers.

(2). find the web server running the oldest version of Apache. (Apache is the most widely used web server program on the Internet.) Don’t count “Apache-Coyote” as “Apache”; also, ignore any servers that don’t specify their version. Show the server’s IP address, and then show the SCREENSHOT image of the wireshark window when you select a particular packet showing this server’s HTTP packet that contains the Apache’s version information, like the following example shows one packet that contains HTTP information of “Server: Apache/1.3.29”:


wireshark.trace [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Frame (534 bytes)
Reassembled TCP (3374 bytes)
Profile: Default

```
No.     Time       Source            Destination    Protocol  Length  Info
   1083 45.729773  113.175.193.243   87.45.62.241   HTTP       144 HTTP/1.1 200 OK  (GIF89a)
   1085 45.731144  113.175.193.243   87.45.62.241   TCP       1504 [TCP segment of a reassembled PDU]
   1086 45.731263  113.175.193.243   87.45.62.241   TCP       1504 [TCP segment of a reassembled PDU]
   1088 45.731313  113.175.193.243   87.45.62.241   HTTP       534 HTTP/1.1 200 OK  (GIF89a)
   1089 45.731315  113.175.193.243   87.45.62.241   TCP         56 80→46861 [FIN, ACK] Seq=3375 Ack=4
   1094 45.743053  113.175.193.243   87.45.62.241   TCP         56 80→46860 [ACK] Seq=13122 Ack=424 W
   1095 45.743440  113.175.193.243   87.45.62.241   TCP         56 80→46861 [ACK] Seq=3376 Ack=424 Wi
```

```
⊞ Frame 1088: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
⊞ Null/Loopback
⊞ Internet Protocol Version 4, Src: 113.175.193.243 (113.175.193.243), Dst: 87.45.62.241 (87.45.62.241)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 46861 (46861), Seq: 2897, Ack: 423, Len: 478
⊞ [3 Reassembled TCP Segments (3374 bytes): #1085(1448), #1086(1448), #1088(478)]
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Fri, 04 May 2007 21:34:23 GMT\r\n
    Server: Apache/1.3.29 (Unix) mod_perl/1.29 mod_ssl/2.8.16 OpenSSL/0.9.7d\r\n
    Last-Modified: Wed, 01 Sep 2004 17:36:29 GMT\r\n
    ETag: "159b5d-c09-4136089d"\r\n
```

```
0000  02 00 00 00 45 a0 02 12  00 00 40 00 32 06 7c 85   ....E... ..@.2.|.
0010  71 af c1 f3 57 2d 3e f1  00 50 b7 0d 3f 0d 39 18   q...W->. .P..?.9.
0020  6d 37 a8 5b 80 18 60 28  01 00 00 00 01 01 08 0a   m7.[..`( ........
```

File: "C:\czou\OneDrive\public_html\CNT47... Packets: 7410 · Displayed: 7410 (100.0%) · Load time: 0:00.199