ECE435: Embedded Systems – Homework 8

TCP, DNS

Due: Wednesday, 16 November 2016, 3pm

For this homework short answers will suffice.

To submit, create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 8" and be sure your name is included in the document.

1. In HW#3 we looked at a mystery Ethernet frame, and then in HW#5 we decoded the Ethernet/IPv4 parts. Now it is time to decode the rest.

   As a reminder, the frame looked like this:

```
0x0000:  0013 3b10 667f b827 ebaf 3711 0800 4500  ..;.f..'..7...E.
0x0010:  0038 572a 4000 4006 69cc c0a8 0833 826f  .8W*@.@.i....3.o
0x0020:  2e7f bda5 0050 cdc4 6a49 3c7b 6ca5 8018  .....P..jI<{l...
0x0030:  00e5 79f4 0000 0101 080a 0104 3e58 34a8  ..y.........>X4.
0x0040:  7bc3 4745 540a                           {.GET.
```

   Fill in the field types and values:

```
BEGIN TCP HEADER

0x0022:  bda5 ____________________
0x0024:  0050 ____________________
0x0026:  cdc4 6a49 _______________
0x002a:  3c7b 6ca5 _______________
0x002e:  80 ______________________
0x003f:  18 ______________________
0x0030:  00e5 ____________________
0x0032:  79f4 ____________________
0x0034:  0000 ____________________
0x0036:  01    _______________
0x0037:  01        _______________
0x0038:  080a      _______________
0x003a:  0104 3e58 _______________
0x003e:  34a8 7bc3 _______________

END TCP_HEADER

BEGIN DATA:

0x0042:  4745 540a _______________

END DATA:
```

2. In the frame from the previous question:

   (a) What type of server was being connected to (based on the port number)?

   (b) What percent of the frame was useful data? (as opposed to header overhead)

3. You use tcpdump to monitor our sockets program from HW#3. You may answer at a high level (don't feel the need to explain each TCP header value, just describe at a high level what is happening in the protocol).

   (a) You start the server, then connect with the client and you see the following:

```
16:38:55.451412 IP macbook-air.52658 > pi3.31337:
Flags [S], seq 3649305635, win 29200,
options [mss 1460,sackOK,TS val 23595005 ecr 0,nop,wscale 7], length 0

16:38:55.451762 IP pi3.31337 > macbook-air.52658:
Flags [S.], seq 2280757527, ack 3649305636, win 28960,
options [mss 1460,sackOK,TS val 122287507 ecr 23595005,nop,wscale 7], length 0

16:38:55.451829 IP macbook-air.52658 > pi3.31337:
Flags [.], ack 1, win 229,
options [nop,nop,TS val 23595005 ecr 122287507], length 0
```

   What just happened?

   (b) You type "Hi" on the client and press enter and the following happens:

```
16:39:01.056250 IP macbook-air.52658 > pi3.31337:
Flags [P.], seq 1:4, ack 1, win 229,
options [nop,nop,TS val 23596406 ecr 122287507], length 3

16:39:01.056551 IP pi3.31337 > macbook-air.52658:
Flags [.], ack 4, win 227,
options [nop,nop,TS val 122288067 ecr 23596406], length 0

16:39:01.057167 IP pi3.31337 > macbook-air.52658:
Flags [P.], seq 1:4, ack 4, win 227,
options [nop,nop,TS val 122288067 ecr 23596406], length 3

16:39:01.057265 IP macbook-air.52658 > pi3.31337:
Flags [.], ack 4, win 229,
options [nop,nop,TS val 23596406 ecr 122288067], length 0
```

   Describe what is going on in each packet.

(c) After typing Bye and receiving the result BYE you see the following set of packets:

```
16:39:16.168569 IP macbook-air.52658 > pi3.31337:
Flags [F.], seq 18, ack 18, win 229,
options [nop,nop,TS val 23600184 ecr 122289578], length 0

16:39:16.168921 IP pi3.31337 > macbook-air.52658:
Flags [F.], seq 18, ack 19, win 227,
options [nop,nop,TS val 122289578 ecr 23600184], length 0

16:39:16.168974 IP macbook-air.52658 > pi3.31337:
Flags [.], ack 19, win 229,
options [nop,nop,TS val 23600184 ecr 122289578], length 0
```

What is going on with these packets?

4. On a Linux / Raspberry Pi machine run the whois utility for the umaine.edu domain:
`whois umaine.edu`
(you might need to install it first, `apt-get install whois`)

   (a) When was the umaine.edu domain set up?

   (b) What is the name of the registrar that umaine.edu uses?

5. On a Linux / Raspberry Pi machine use dig to look at DNS records. You might need to install the dnsutils package `apt-get install dnsutils`

   (a) What is the IP address of weaver.eece.maine.edu?
   `dig weaver.eece.maine.edu A`

   (b) What is the IPv6 address of maine.edu?
   `dig weaver.eece.maine.edu AAAA`

   (c) What is the name of the UMaine nameservers?
   `dig maine.edu NS`

   (d) What is the name of the UMaine mailservers?
   `dig maine.edu MX`