HW 2 Report

Case 1:

Random0 - Jump into fixed DNS header

```
Lookup  : random0.irl
Query   : random0.irl, type 1, TXID 0x00EA
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 82 bytes
  TXID 0x00EA, flags 0x8400, questions 1, answers 2, authority 0, additional 0
  succeeded with Rcode = 0
  ------------ [questions] ----------
        random0.irl type 1 class 1
  ------------ [answers] ----------
        random.irl.♦ type  1.1.1.6 TTL = 7680
         type  114.97.110.100 TTL = 67174657
```

random3 - Packet size < FixedDNSHeader

```
Lookup  : random3.irl
Query   : random3.irl, type 1, TXID 0x00ED
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 4 bytes
  TXID 0x00ED, flags 0x8400, questions 52685, answers 52685, authority 52685, additional 52685
  ++    invalid reply: packet smaller than fixed DNS header
```

random5 - RR value length stretches the answer beyond packet

```
Lookup  : random5.irl
Query   : random5.irl, type 1, TXID 0x00C6
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 71 bytes
  TXID 0x00C6, flags 0x8400, questions 1, answers 2, authority 0, additional 0
  succeeded with Rcode = 0
  ------------ [questions] ----------
        random5.irl type 1 class 1
  ------------ [answers] ----------
        random.irl type A 1.1.1.1 TTL = 30
  ++    invalid record: RR value length stretches the answer beyond packet
```

random6 - Packet has infinite jumps in CNAME and query name (jump loop)

```
Lookup  : random6.irl
Query   : random6.irl, type 1, TXID 0x0180
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 59 bytes
  TXID 0x0180, flags 0x8400, questions 1, answers 2, authority 0, additional 0
  succeeded with Rcode = 0
  ------------ [questions] ----------
        random6.irl type 1 class 1
  ------------ [answers] ----------
  ++    invalid record: jump loop
```

Case 2:

random1 – Count for additional records greater than the amount of data received

```
Lookup  : random1.irl
Query   : random1.irl, type 1, TXID 0x00ED
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 1 ms with 468 bytes
  TXID 0x00ED, flags 0x8600, questions 1, answers 1, authority 0, additional 65535
  succeeded with Rcode = 0
  ++    invalid record: RR value length stretches the answer beyond packet
```

Case 3:

random7 - Truncated jump offset

```
Lookup  : random7.irl
Query   : random7.irl, type 1, TXID 0x00D3
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 42 bytes
  TXID 0x00D3, flags 0x8400, questions 1, answers 2, authority 0, additional 0
  succeeded with Rcode = 0
  ------------ [questions] ----------
        random7.irl type 1 class 1
  ------------ [answers] ----------
  ++    invalid record: truncated jump offset
```

Case 4:

random4 – Packet is incomplete/missing data (variable length. Simulated packet loss?)

- Packet has incomplete DNSAnswerHeader for the last additional record. Number of additional records is also less than the header says.

```
Lookup  : random4.irl
Query   : random4.irl, type 1, TXID 0x00DD
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 100 bytes
  TXID 0x00DD, flags 0x8400, questions 1, answers 1, authority 0, additional 11
  succeeded with Rcode = 0
  ------------ [questions] ----------
       random4.irl type 1 class 1
  ------------ [answers] ----------
       random.irl type A 1.1.1.1 TTL = 30
  ------------ [additional] ----------
       Episode.IV type  0.1.0.1 TTL = 1684352585
     ++ Error: malformed packet
```

- Address is truncated at end of packet for the last additional record. Number of additional records is also less than the header says.

```
Lookup  : random4.irl
Query   : random4.irl, type 1, TXID 0x00DA
Server  : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 1 ms with 147 bytes
  TXID 0x00DA, flags 0x8400, questions 1, answers 1, authority 0, additional 11
  succeeded with Rcode = 0
  ------------ [questions] ----------
       random4.irl type 1 class 1
  ------------ [answers] ----------
       random.irl type A 1.1.1.1 TTL = 30
  ------------ [additional] ----------
       Episode.IV type  0.1.0.1 TTL = 1684352585
     ++ Error: malformed packet
```

- Character length shows as being 8, but only 3 characters found (at end of packet)

```
Lookup   : random4.irl
Query    : random4.irl, type 1, TXID 0x00D3
Server   : 127.0.0.1
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 290 bytes
  TXID 0x00D3, flags 0x8400, questions 1, answers 1, authority 0, additional 11
  succeeded with Rcode = 0
  ------------ [questions] ----------
       random4.irl type 1 class 1
  ------------ [answers] ----------
       random.irl type A 1.1.1.1 TTL = 30
  ------------ [additional] ----------
       Episode.IV type  0.1.0.1 TTL = 1684352585
     ++ Error: malformed packet
```

All these errors are caught by this section for Questions, Answers, Auth, and Additional records

```
// parse Additional
printf("  ------------ [additional] ----------\n");
char* addSection;
if (numAuthority <= 0) {
    addSection = ansSections[numAnswers - 1] + strlen(ansSections[numAnswers - 1]) + sizeof(DNSAnswerHeader) + 5;
}
else {
    addSection = authSections[numAuthority - 1] + strlen(authSections[numAuthority - 1]) + 5;
}

char* additional = addSection;
for (int i = 0; i < numAdditional; i++) {
    int length = strlen(additional);

    if ((additional[0] & 0xC0) == 0xC0) { // compression detected. Jump!
        int offset = ntohs(*(USHORT*)additional) & 0x3FFF;
        char* label = (*recvBuf) + offset + 1;

        int labelLength = strlen(label);
        length = labelLength + 2;
        addSections[i] = label;
        //printf("Jumped to %X\n", label);
    }
    else {
        addSections[i] = additional + 1;

        if (length == 0) {
            printf("     ++ Error: malformed packet\n");
            quit();
        }

        //convert char lengths to dots
        for (u_int j = 0; j < length - 1; j++) {
            if (additional[j] < '0') {
                additional[j] = '.';
            }
        }

        currentHeader = ((DNSAnswerHeader*)(additional + strlen(additional) + 1));
    }


    // print header and name info
    DNSAnswerHeader* currentHeader = (DNSAnswerHeader*)(additional + 2);
    int type = ntohs(currentHeader->aType);
    DWORD* ip = (DWORD*)(currentHeader + 1);
    struct in_addr pAddress;
    pAddress.S_un.S_addr = *ip;
    char* address = inet_ntoa(pAddress);
```

Extra Credit:

Random8 – the server is placing a random number of consecutive instances of ‘lol’ (0x6c 0x6f 0x6c) into a seemingly random spot in the packet. There is no correlation between the position/number of instances of ‘lol’ and the number of answers, questions, txid, etc. The rest of the packet remains constant between different responses.