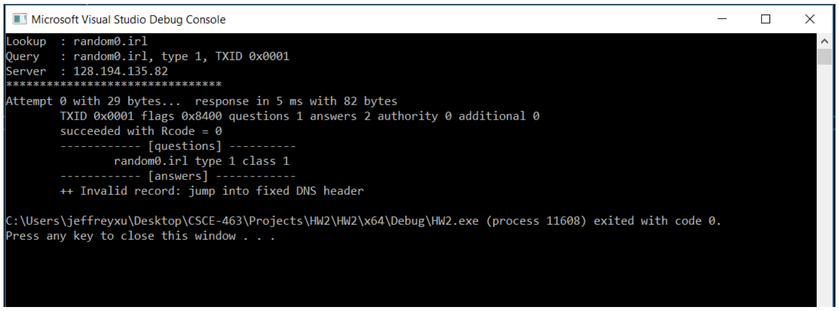
CSCE 463
HW 2 Report
Jeffrey Xu
03/16/21

1 Case 1

1.1 random0.irl

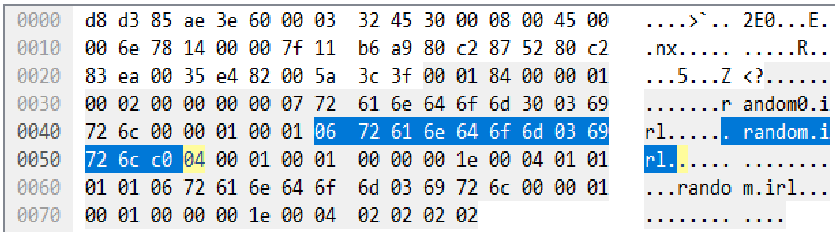
We needed to test *random0.irl* with the provided DNS server. The following output/trace of the program is shown below.



```
Lookup  : random0.irl
Query   : random0.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 5 ms with 82 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 2 authority 0 additional 0
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random0.irl type 1 class 1
        ------------ [answers] ------------
        ++ Invalid record: jump into fixed DNS header

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 11608) exited with code 0.
Press any key to close this window . . .
```

We can see that there apppeared to be a jump into the fixed DNS header. The Wireshark output for the packet is shown below.

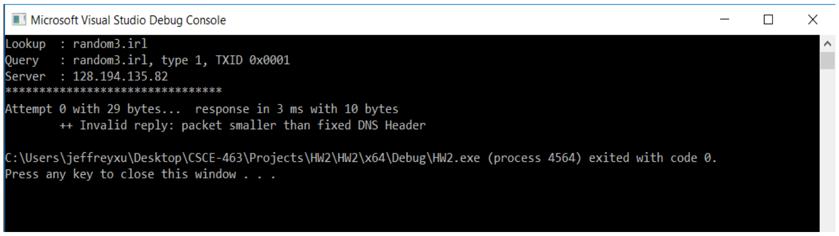


```
0000  d8 d3 85 ae 3e 60 00 03  32 45 30 00 08 00 45 00   ....>`.. 2E0...E.
0010  00 6e 78 14 00 00 7f 11  b6 a9 80 c2 87 52 80 c2   .nx..... .....R..
0020  83 ea 00 35 e4 82 00 5a  3c 3f 00 01 84 00 00 01   ...5...Z <?......
0030  00 02 00 00 00 00 07 72  61 6e 64 6f 6d 30 03 69   .......r andom0.i
0040  72 6c 00 00 01 00 01 06  72 61 6e 64 6f 6d 03 69   rl...... random.i
0050  72 6c c0 04 00 01 00 01  00 00 00 1e 00 04 01 01   rl...... ........
0060  01 01 06 72 61 6e 64 6f  6d 03 69 72 6c 00 00 01   ...rando m.irl...
0070  00 01 00 00 00 1e 00 04  02 02 02 02               ........ ....
```

We can clearly see that after the last *random.irl*, there seems to be a jump but to an offset that is clearly within the fixed DNS header (4 is between 0 and 12 which is the fixed DNS header length). Therefore, the error output is valid.

1.2 random3.irl

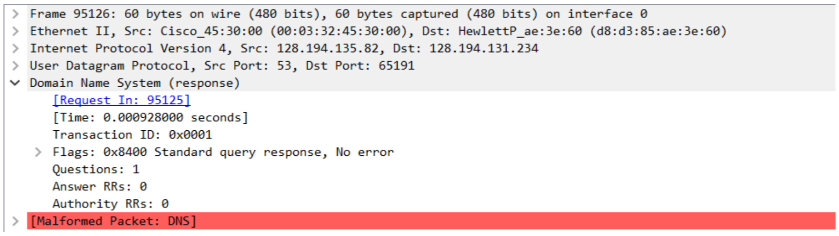
Now we want to test *random3.irl* on the given server. The output is shown below.



```
Lookup  : random3.irl
Query   : random3.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 10 bytes
        ++ Invalid reply: packet smaller than fixed DNS Header

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 4564) exited with code 0.
Press any key to close this window . . .
```

We can clearly see that the response is only 10 bytes making it smaller than the fixed DNS header which is 12 bytes by default. To further prove that this response is incorrect, the Wireshark response is also shown below.

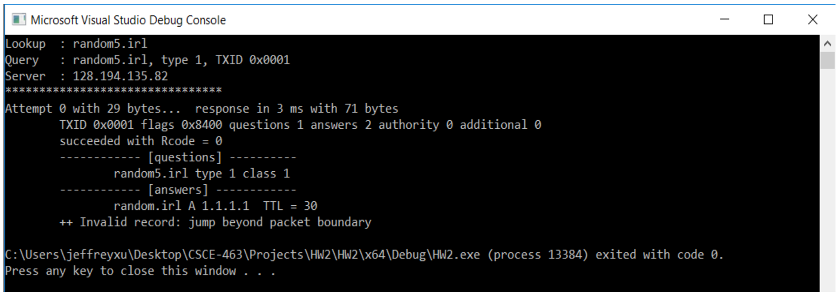


```
> Frame 95126: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Cisco_45:30:00 (00:03:32:45:30:00), Dst: HewlettP_ae:3e:60 (d8:d3:85:ae:3e:60)
> Internet Protocol Version 4, Src: 128.194.135.82, Dst: 128.194.131.234
> User Datagram Protocol, Src Port: 53, Dst Port: 65191
v Domain Name System (response)
     [Request In: 95125]
     [Time: 0.000928000 seconds]
     Transaction ID: 0x0001
   > Flags: 0x8400 Standard query response, No error
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
> [Malformed Packet: DNS]
```

We see that the packet is a malformed DNS packet further proving that the response is incorrectly formatted.

1.3 random5.irl

The trace for *random5.irl* using *128.194.135.82* as the DNS server is shown below.



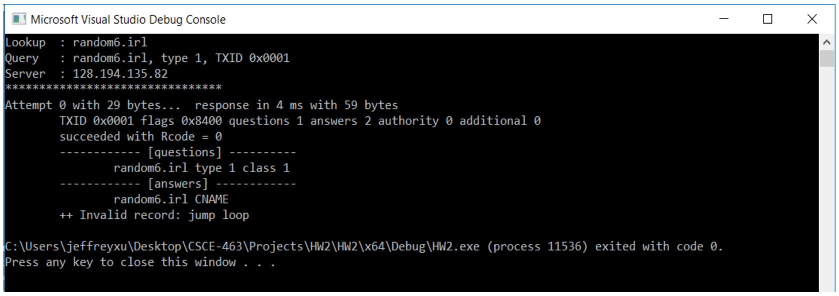
```
Lookup  : random5.irl
Query   : random5.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 71 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 2 authority 0 additional 0
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random5.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A 1.1.1.1  TTL = 30
        ++ Invalid record: jump beyond packet boundary

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 13384) exited with code 0.
Press any key to close this window . . .
```

We can see that on the second answer, there appears to be a jump that went beyond the packet boundary of 71 bytes.

1.4 random6.irl

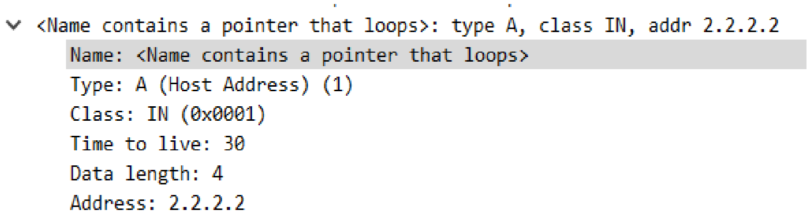
The trace for *random6.irl* using *128.194.135.82* as the DNS server is shown below.



```
Lookup  : random6.irl
Query   : random6.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 4 ms with 59 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 2 authority 0 additional 0
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random6.irl type 1 class 1
        ------------ [answers] ------------
                random6.irl CNAME
        ++ Invalid record: jump loop

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 11536) exited with code 0.
Press any key to close this window . . .
```

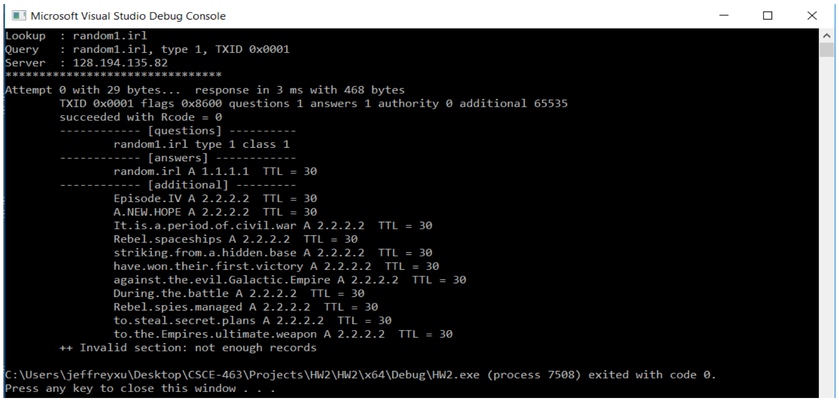
We see that a jump loop seems to be present within the first answer. This is corroborated with the hex dump from Wireshark.



```
<Name contains a pointer that loops>: type A, class IN, addr 2.2.2.2
    Name: <Name contains a pointer that loops>
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 30
    Data length: 4
    Address: 2.2.2.2
```

2 Case 2

Now we want to see what outputs result from *random1.irl* using the same DNS server. The output from the program is shown below.



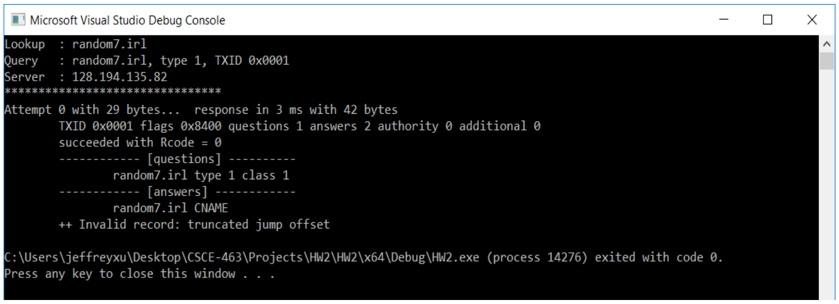
```
Lookup  : random1.irl
Query   : random1.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 468 bytes
        TXID 0x0001 flags 0x8600 questions 1 answers 1 authority 0 additional 65535
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random1.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A 1.1.1.1  TTL = 30
        ------------ [additional] ---------
                Episode.IV A 2.2.2.2  TTL = 30
                A.NEW.HOPE A 2.2.2.2  TTL = 30
                It.is.a.period.of.civil.war A 2.2.2.2  TTL = 30
                Rebel.spaceships A 2.2.2.2  TTL = 30
                striking.from.a.hidden.base A 2.2.2.2  TTL = 30
                have.won.their.first.victory A 2.2.2.2  TTL = 30
                against.the.evil.Galactic.Empire A 2.2.2.2  TTL = 30
                During.the.battle A 2.2.2.2  TTL = 30
                Rebel.spies.managed A 2.2.2.2  TTL = 30
                to.steal.secret.plans A 2.2.2.2  TTL = 30
                to.the.Empires.ultimate.weapon A 2.2.2.2  TTL = 30
        ++ Invalid section: not enough records

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 7508) exited with code 0.
Press any key to close this window . . .
```

We can clearly see that the *additional* section does not contain enough records as there are 65536 additional records and the packet size doesn't even come close to containing that many records.

3 Case 3

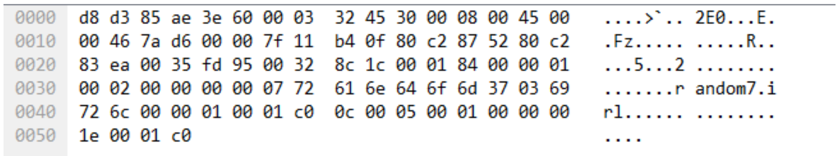
Now we need to check what *random7.irl* gives us. The output from the program is shown below.



```
Lookup  : random7.irl
Query   : random7.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 42 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 2 authority 0 additional 0
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random7.irl type 1 class 1
        ------------ [answers] ------------
                random7.irl CNAME
        ++ Invalid record: truncated jump offset

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 14276) exited with code 0.
Press any key to close this window . . .
```

We see that there appears to be a truncated jump offset which means that a jump was present but the packet ended before any offset information was provided. The Wireshark trace below shows more information.

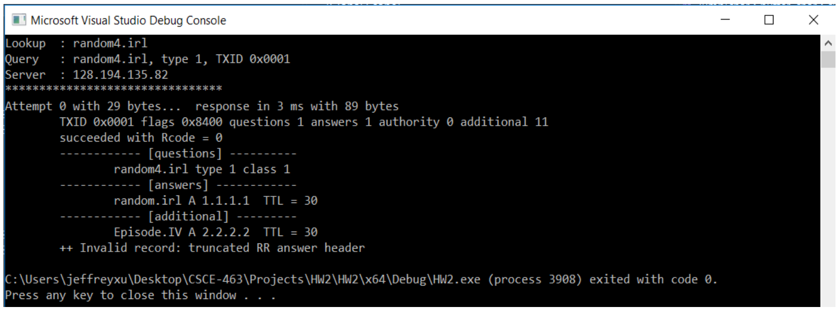


```
0000  d8 d3 85 ae 3e 60 00 03  32 45 30 00 08 00 45 00   ....>`.. 2E0...E.
0010  00 46 7a d6 00 00 7f 11  b4 0f 80 c2 87 52 80 c2   .Fz..... .....R..
0020  83 ea 00 35 fd 95 00 32  8c 1c 00 01 84 00 00 01   ...5...2 ........
0030  00 02 00 00 00 00 07 72  61 6e 64 6f 6d 37 03 69   .......r andom7.i
0040  72 6c 00 00 01 00 01 c0  0c 00 05 00 01 00 00 00   rl...... ........
0050  1e 00 01 c0                                        ....
```

We can see that the last byte of the packet is *0XC0* but there's no jump information provided.

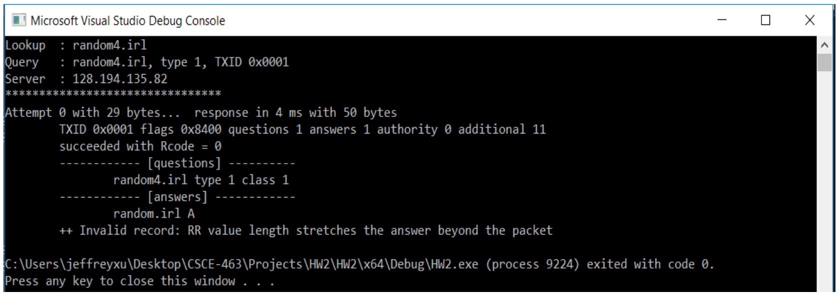
4 Case 4

Now we want to test the different outputs that come from *random4.irl*. Some of the outputs are shown below.



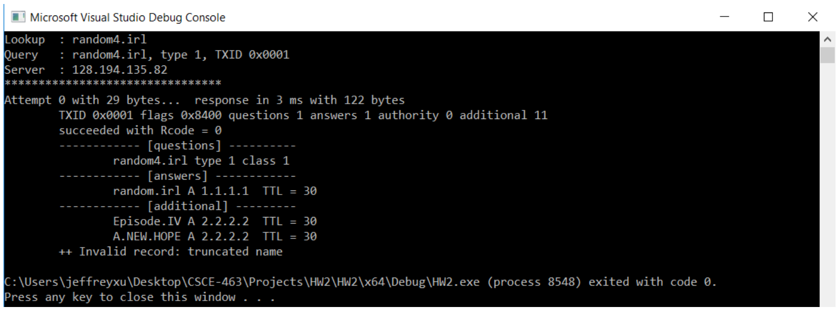
```
Lookup  : random4.irl
Query   : random4.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 89 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 1 authority 0 additional 11
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random4.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A 1.1.1.1  TTL = 30
        ------------ [additional] ---------
                Episode.IV A 2.2.2.2  TTL = 30
        ++ Invalid record: truncated RR answer header

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 3908) exited with code 0.
Press any key to close this window . . .
```



```
Lookup  : random4.irl
Query   : random4.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 4 ms with 50 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 1 authority 0 additional 11
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random4.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A
        ++ Invalid record: RR value length stretches the answer beyond the packet

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 9224) exited with code 0.
Press any key to close this window . . .
```



```
Lookup  : random4.irl
Query   : random4.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 122 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 1 authority 0 additional 11
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random4.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A 1.1.1.1  TTL = 30
        ------------ [additional] ---------
                Episode.IV A 2.2.2.2  TTL = 30
                A.NEW.HOPE A 2.2.2.2  TTL = 30
        ++ Invalid record: truncated name

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 8548) exited with code 0.
Press any key to close this window . . .
```

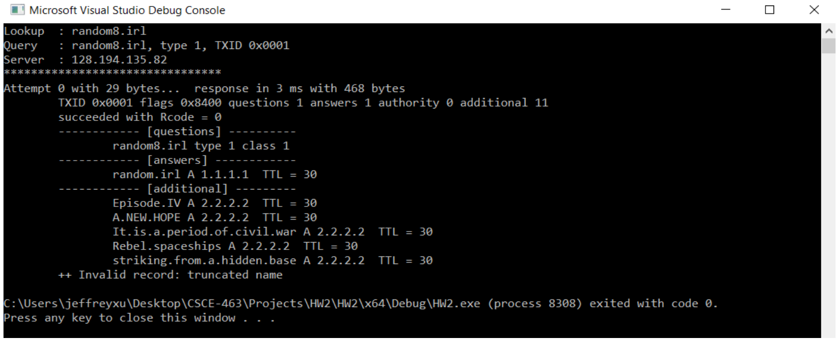
We see that there is an output with a truncated RR answer header. To check for this case, I simply put an if-statement that checks if the current point plus the size of the RR answer header is greater than the total number of bytes. If so, then the program outputs the error message and quits the program.

Another possible error message is that the RR value length stretches the answer beyond the packet. To check for this, I simply check if the length of the fixed RR header (length field of the RR header) goes beyond the packet, if so then we output the error and quit the program.

Finally, we have the truncated name error message. To check for this error, I simply put another if-statement within the jump function that checks if the current block will go beyond the packet length. If so, then we output the error and quit the program.

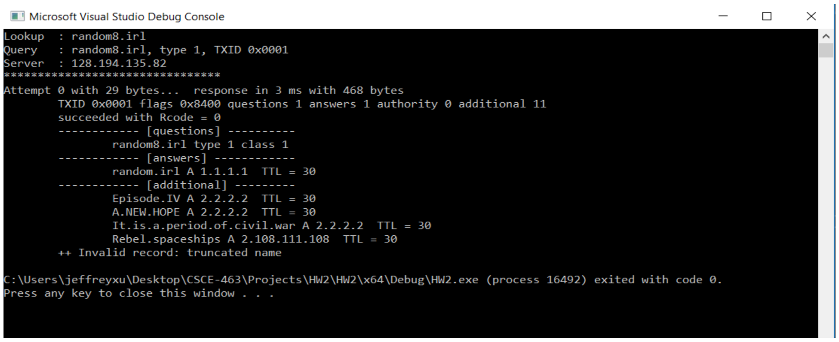
5 Case 5

Now we want to explore what *random8.irl* is sending back and what algorithm is behind it that is creating the errors. From an initial testing of the host, it seems that the server is generating the same response packet each time, but truncating the packet at a random location within the packet. Some outputs from the host are shown below.



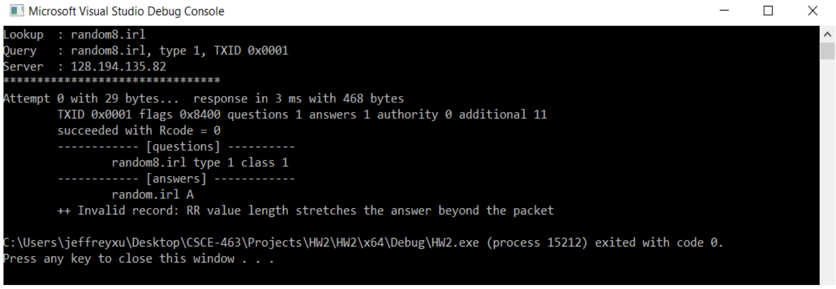
```
Lookup  : random8.irl
Query   : random8.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 468 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 1 authority 0 additional 11
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random8.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A 1.1.1.1  TTL = 30
        ------------ [additional] ---------
                Episode.IV A 2.2.2.2  TTL = 30
                A.NEW.HOPE A 2.2.2.2  TTL = 30
                It.is.a.period.of.civil.war A 2.2.2.2  TTL = 30
                Rebel.spaceships A 2.2.2.2  TTL = 30
                striking.from.a.hidden.base A 2.2.2.2  TTL = 30
        ++ Invalid record: truncated name

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 8308) exited with code 0.
Press any key to close this window . . .
```



```
Lookup  : random8.irl
Query   : random8.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 468 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 1 authority 0 additional 11
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random8.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A 1.1.1.1  TTL = 30
        ------------ [additional] ---------
                Episode.IV A 2.2.2.2  TTL = 30
                A.NEW.HOPE A 2.2.2.2  TTL = 30
                It.is.a.period.of.civil.war A 2.2.2.2  TTL = 30
                Rebel.spaceships A 2.108.111.108  TTL = 30
        ++ Invalid record: truncated name

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 16492) exited with code 0.
Press any key to close this window . . .
```



```
Lookup  : random8.irl
Query   : random8.irl, type 1, TXID 0x0001
Server  : 128.194.135.82
********************************
Attempt 0 with 29 bytes...  response in 3 ms with 468 bytes
        TXID 0x0001 flags 0x8400 questions 1 answers 1 authority 0 additional 11
        succeeded with Rcode = 0
        ------------ [questions] ----------
                random8.irl type 1 class 1
        ------------ [answers] ------------
                random.irl A
        ++ Invalid record: RR value length stretches the answer beyond the packet

C:\Users\jeffreyxu\Desktop\CSCE-463\Projects\HW2\HW2\x64\Debug\HW2.exe (process 15212) exited with code 0.
Press any key to close this window . . .
```

We see each time that there is always 1 question, 1 answer, and 11 additional records for the response. The order in which the response come are also in the same order with *random.irl* as the answer, *Episode.IV* as the first additional record, *A.NEW.HOPE* as the next additional record and so on. As it occurs, the packet seems to be writing out the intro for Star Wars Episode IV but using the additional record names to output the words.

I think that the server is probably putting illegitimate jumps and block sizes which would cause the issues of having truncated names, having the RR value go beyond the packet, having the issue of not having enough records (or what it seems based on the information in the packet), etc.

If someone were to write a parser to parse these packets, they would most likely have to check all jump values and block size values when perform jumps to make sure that values are legit and don't cause an error. This only really needs to be done during the jump function since it seems that all issues occur when the program is jumping to read a name from another offset in the packet.