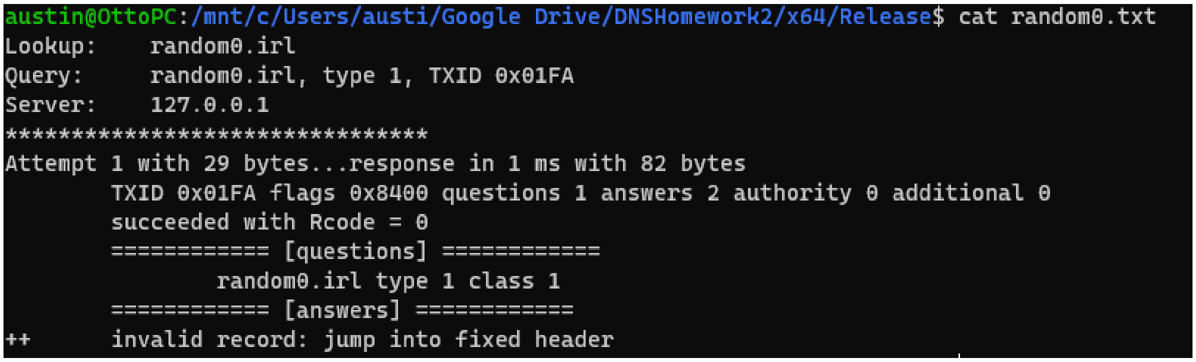
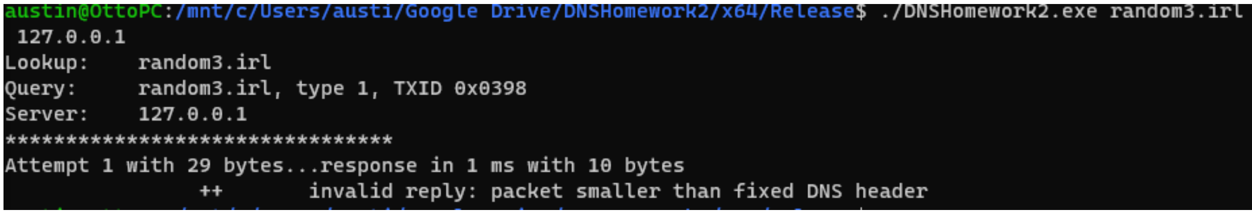
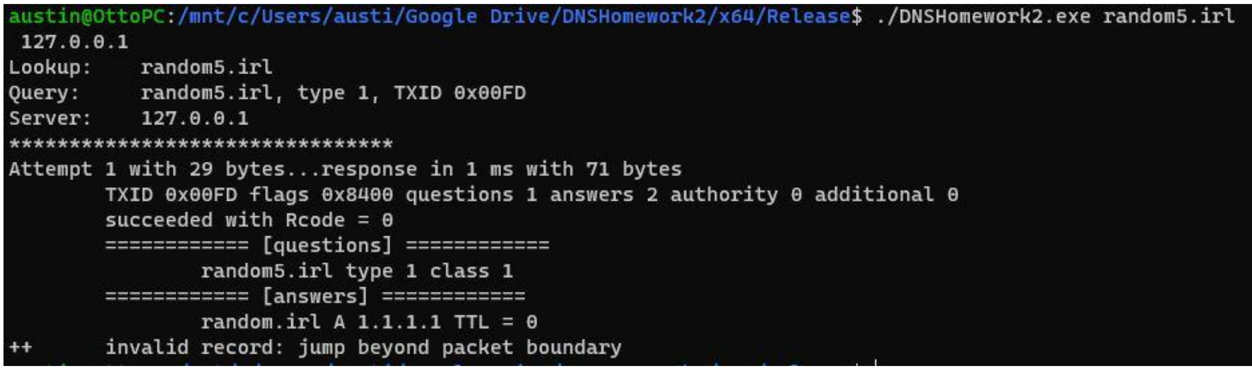
Austin Peterson
926006358

CSCE463: Networks and Distributed Processing
DNS Homework 2 Report

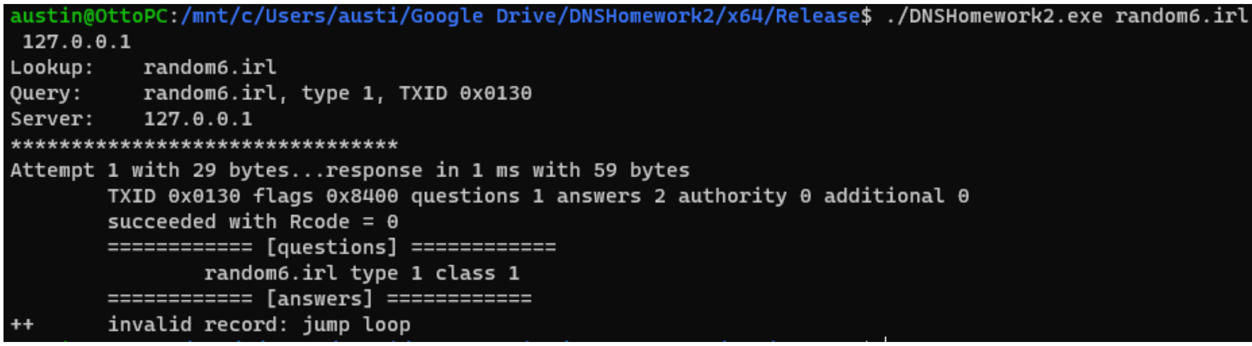
- Random0.irl
  - 

    ```
    austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ cat random0.txt
    Lookup:    random0.irl
    Query:     random0.irl, type 1, TXID 0x01FA
    Server:    127.0.0.1
    ********************************
    Attempt 1 with 29 bytes...response in 1 ms with 82 bytes
            TXID 0x01FA 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 header
    ```
  - As you can see above, random 0 modifies the response packet by making the jump offset such that the tracking pointer jumps into a fixed header, which is checked by seeing if the offset is between 0 and 12, which would make the program try to pull data from a fixed header.
- Random3.irl
  - 

    ```
    austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random3.irl
     127.0.0.1
    Lookup:    random3.irl
    Query:     random3.irl, type 1, TXID 0x0398
    Server:    127.0.0.1
    ********************************
    Attempt 1 with 29 bytes...response in 1 ms with 10 bytes
                    ++      invalid reply: packet smaller than fixed DNS header
    ```
  - Random3’s error is that the packet is smaller than the DNS header, which is easily found by comparing the number of bytes received by recv with the size of FixedDNSheader.
- Random5.irl
  - 

    ```
    austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random5.irl
     127.0.0.1
    Lookup:    random5.irl
    Query:     random5.irl, type 1, TXID 0x00FD
    Server:    127.0.0.1
    ********************************
    Attempt 1 with 29 bytes...response in 1 ms with 71 bytes
            TXID 0x00FD 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 = 0
    ++      invalid record: jump beyond packet boundary
    ```
  - Random5 inserts a jump that would lead the program to look outside of the packet itself, checked by seeing if the offset is larger than the size of the response packet.
- Random6.irl

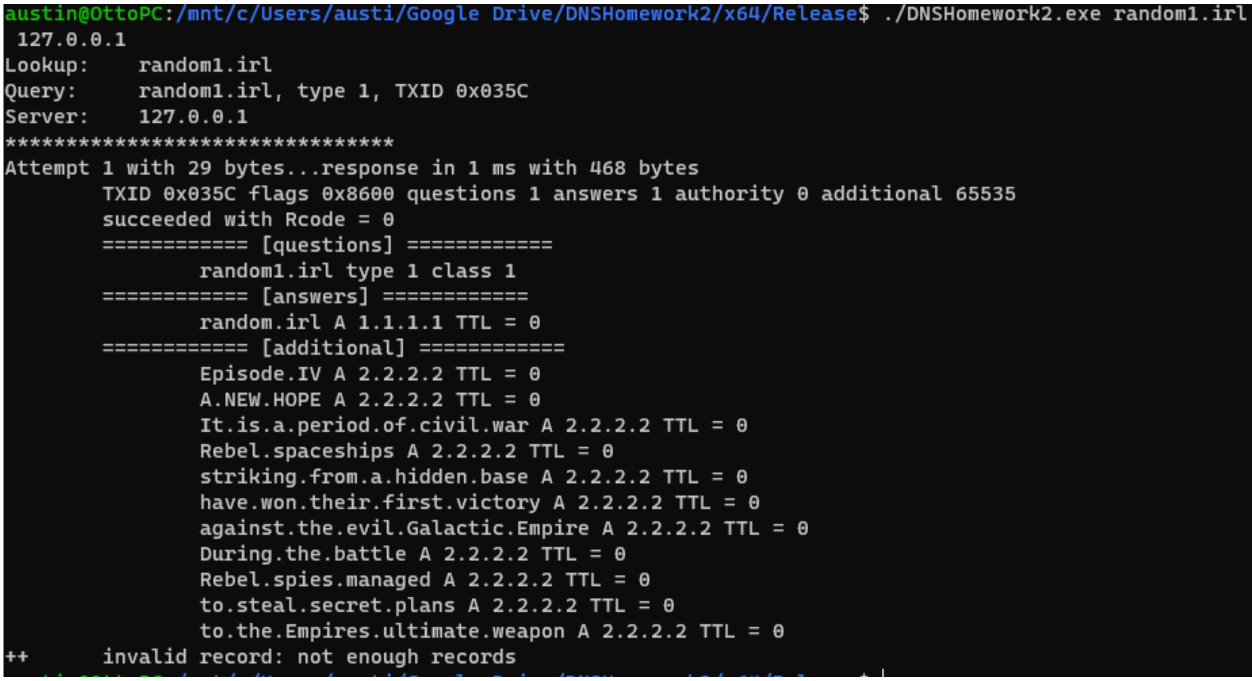
Austin Peterson
926006358



```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random6.irl
 127.0.0.1
Lookup:    random6.irl
Query:     random6.irl, type 1, TXID 0x0130
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 59 bytes
        TXID 0x0130 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
```

  - Random6 results in a jump offset that leads the pointer to another ‘0xC0’ value in the packet, resulting in a jump loop. This is easily checked by looking at the value that is found immediately after the jump, and seeing if it indicates another jump.

- Random1.irl

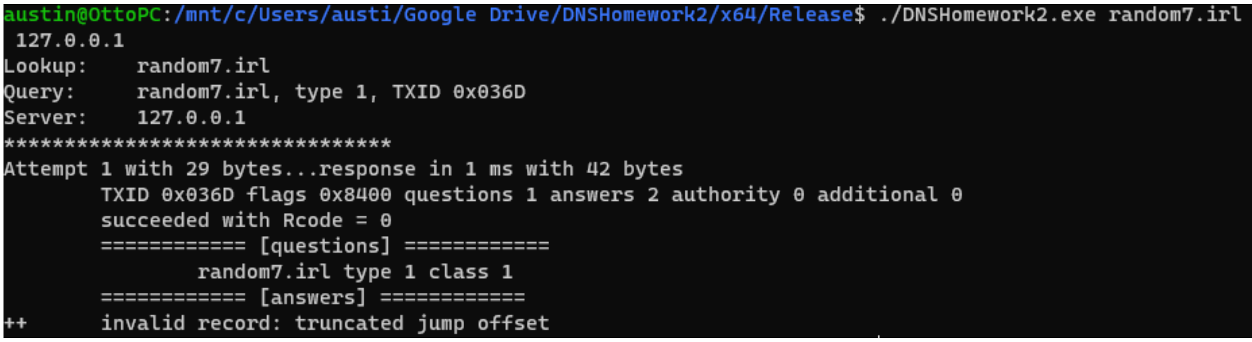


```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random1.irl
 127.0.0.1
Lookup:    random1.irl
Query:     random1.irl, type 1, TXID 0x035C
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 468 bytes
        TXID 0x035C 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 = 0
        ============ [additional] ============
                Episode.IV A 2.2.2.2 TTL = 0
                A.NEW.HOPE A 2.2.2.2 TTL = 0
                It.is.a.period.of.civil.war A 2.2.2.2 TTL = 0
                Rebel.spaceships A 2.2.2.2 TTL = 0
                striking.from.a.hidden.base A 2.2.2.2 TTL = 0
                have.won.their.first.victory A 2.2.2.2 TTL = 0
                against.the.evil.Galactic.Empire A 2.2.2.2 TTL = 0
                During.the.battle A 2.2.2.2 TTL = 0
                Rebel.spies.managed A 2.2.2.2 TTL = 0
                to.steal.secret.plans A 2.2.2.2 TTL = 0
                to.the.Empires.ultimate.weapon A 2.2.2.2 TTL = 0
++      invalid record: not enough records
```

  - Random1, my personal favorite due to the star wars answers, returns the error “not enough records”, which is pretty obvious because the packet suggests that there should be 65535 additional records but the packet itself contains significantly fewer records than that.

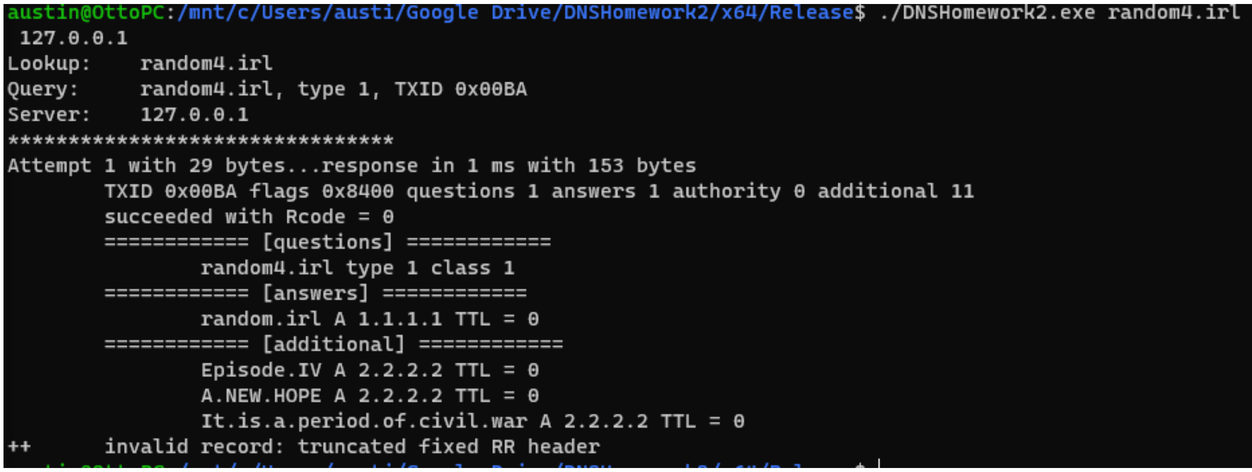
- Random7.irl

Austin Peterson
926006358

- 

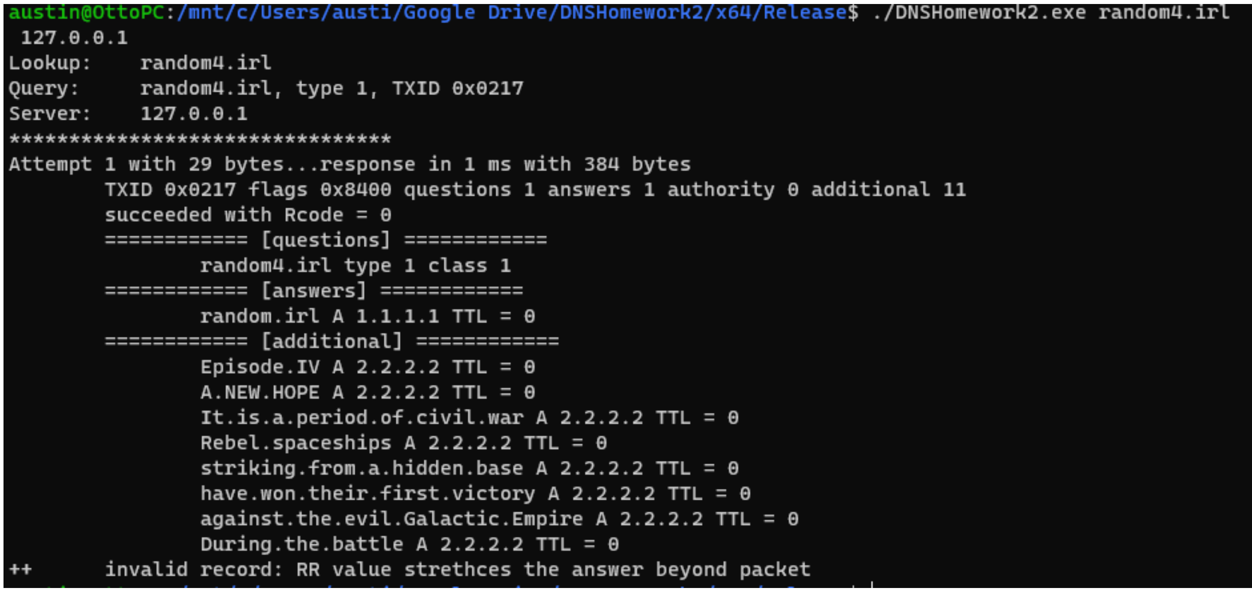
```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random7.irl
 127.0.0.1
Lookup:    random7.irl
Query:     random7.irl, type 1, TXID 0x036D
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 42 bytes
        TXID 0x036D 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
```

- Random7's error is truncated jump offset

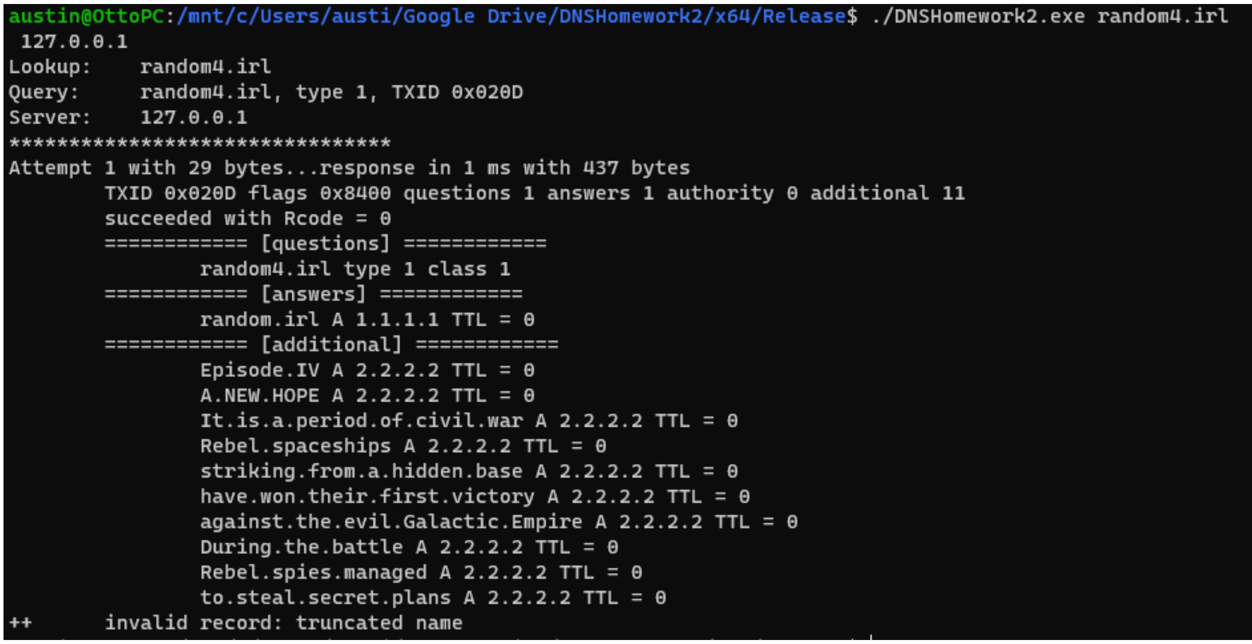
- Random4.irl
  - 

```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random4.irl
 127.0.0.1
Lookup:    random4.irl
Query:     random4.irl, type 1, TXID 0x00BA
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 153 bytes
        TXID 0x00BA 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 = 0
        ============ [additional] ============
                Episode.IV A 2.2.2.2 TTL = 0
                A.NEW.HOPE A 2.2.2.2 TTL = 0
                It.is.a.period.of.civil.war A 2.2.2.2 TTL = 0
++      invalid record: truncated fixed RR header
```

  - Random4's first error is truncated fixed header, calculated by checking if the current position plus the DNSanswerHdr size is greater than the number of bytes received, indicating a truncated buffer.



```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random4.irl
 127.0.0.1
Lookup:    random4.irl
Query:     random4.irl, type 1, TXID 0x0217
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 384 bytes
        TXID 0x0217 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 = 0
        ============ [additional] ============
                Episode.IV A 2.2.2.2 TTL = 0
                A.NEW.HOPE A 2.2.2.2 TTL = 0
                It.is.a.period.of.civil.war A 2.2.2.2 TTL = 0
                Rebel.spaceships A 2.2.2.2 TTL = 0
                striking.from.a.hidden.base A 2.2.2.2 TTL = 0
                have.won.their.first.victory A 2.2.2.2 TTL = 0
                against.the.evil.Galactic.Empire A 2.2.2.2 TTL = 0
                During.the.battle A 2.2.2.2 TTL = 0
++      invalid record: RR value strethces the answer beyond packet
```

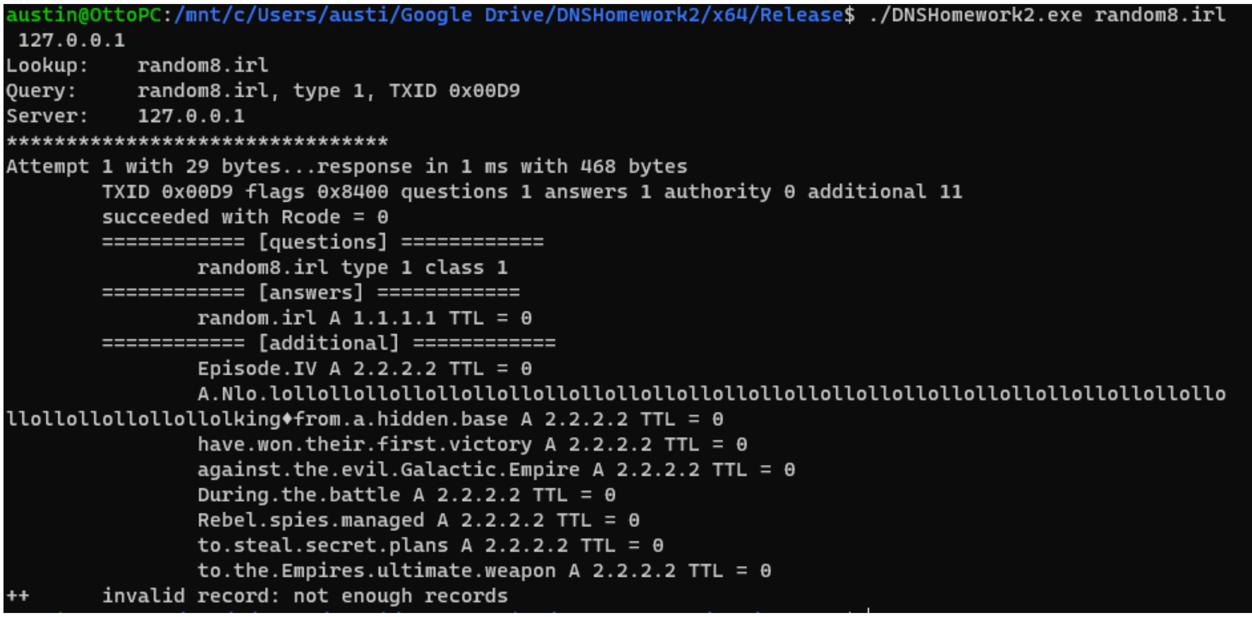
- Random4’s second error is that the RR value stretches the answer beyond the packet, which is checked by adding the RRheader’s len variable to the current position and seeing if that is larger than the size of the packet itself.
- 

```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random4.irl
 127.0.0.1
Lookup:    random4.irl
Query:     random4.irl, type 1, TXID 0x020D
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 437 bytes
        TXID 0x020D 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 = 0
        ============ [additional] ============
                Episode.IV A 2.2.2.2 TTL = 0
                A.NEW.HOPE A 2.2.2.2 TTL = 0
                It.is.a.period.of.civil.war A 2.2.2.2 TTL = 0
                Rebel.spaceships A 2.2.2.2 TTL = 0
                striking.from.a.hidden.base A 2.2.2.2 TTL = 0
                have.won.their.first.victory A 2.2.2.2 TTL = 0
                against.the.evil.Galactic.Empire A 2.2.2.2 TTL = 0
                During.the.battle A 2.2.2.2 TTL = 0
                Rebel.spies.managed A 2.2.2.2 TTL = 0
                to.steal.secret.plans A 2.2.2.2 TTL = 0
++      invalid record: truncated name
```

- The last error of random4 is truncated name, which is found while parsing a given RR. If the current position minus the response buffer plus the size of the next string found in the buffer is more than the number of bytes received, then the name has been truncated.

Austin Peterson
926006358

- Random8



```
austin@OttoPC:/mnt/c/Users/austi/Google Drive/DNSHomework2/x64/Release$ ./DNSHomework2.exe random8.irl
 127.0.0.1
Lookup:    random8.irl
Query:     random8.irl, type 1, TXID 0x00D9
Server:    127.0.0.1
********************************
Attempt 1 with 29 bytes...response in 1 ms with 468 bytes
        TXID 0x00D9 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 = 0
        ============ [additional] ============
                Episode.IV A 2.2.2.2 TTL = 0
                A.Nlo.lollollollollollollollollollollollollollollollollollollollollollollollollollollollo
llollollollollollolking♦from.a.hidden.base A 2.2.2.2 TTL = 0
                have.won.their.first.victory A 2.2.2.2 TTL = 0
                against.the.evil.Galactic.Empire A 2.2.2.2 TTL = 0
                During.the.battle A 2.2.2.2 TTL = 0
                Rebel.spies.managed A 2.2.2.2 TTL = 0
                to.steal.secret.plans A 2.2.2.2 TTL = 0
                to.the.Empires.ultimate.weapon A 2.2.2.2 TTL = 0
++      invalid record: not enough records
```

  - As far as I can tell random 8 just inserts a bunch of lols into the answer to throw off the program. My guess is that the server is trying to insert as much text as possible to attempt to cause a buffer overflow with the buffer used to read text when parsing the buffer, resulting in overwritten data and invalid records