Report Homework 2
Mian Qin (UIN:725006574)

1. Case 1: random0.irl, random3.irl, random5.irl, and random6.irl.

random0.ril trace:

```
Lookup: random0.irl
Query : random0.irl, type 1, TXID 0000
Server : 128.194.135.82
*********************************
Attempt 0 with 29 bytes... response in 0 ms with 82 bytes
  TXID 0000 flags 8400 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
```

random3.ril trace:

```
Lookup: random3.irl
Query : random3.irl, type 1, TXID 0000
Server : 128.194.135.82
*********************************
Attempt 0 with 29 bytes...
  ++    invalid reply: smaller than fixed header
```

random5.ril trace:

```
Lookup: random5.irl
Query : random5.irl, type 1, TXID 0000
Server : 128.194.135.82
*********************************
Attempt 0 with 29 bytes... response in 0 ms with 71 bytes
  TXID 0000 flags 8400 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: jump beyond packet boundary
```

random6.ril trace:

```
Lookup: random6.irl
Query : random6.irl, type 1, TXID 0000
Server : 128.194.135.82
*********************************
Attempt 0 with 29 bytes... response in 1 ms with 59 bytes
  TXID 0000 flags 8400 questions 1 answers 2 authority 0 additional 0
  succeeded with Rcode = 0
```

```
------------ [questions] ----------
     random6.irl type 1 class 1
------------ [answers] ------------
++   invalid record: jump loop
```

2. Case 2: random1.irl.

random1.ril trace:

```
Lookup: random1.irl
Query : random1.irl, type 1, TXID 0000
Server : 128.194.135.82
*******************************
Attempt 0 with 29 bytes... response in 1 ms with 468 bytes
  TXID 0000 flags 8600 questions 1 answers 1 authority 0 additional 65535
  succeeded with Rcode = 0
  ------------ [questions] ----------
       random1.irl type 1 class 1
  ------------ [answers] ------------
       random.irl type A 1.1.1.1 TTL = 30
  ------------ [additional] ------------
       Episode.IV type A 2.2.2.2 TTL = 30
       A.NEW.HOPE type A 2.2.2.2 TTL = 30
       It.is.a.period.of.civil.war type A 2.2.2.2 TTL = 30
       Rebel.spaceships type A 2.2.2.2 TTL = 30
       striking.from.a.hidden.base type A 2.2.2.2 TTL = 30
       have.won.their.first.victory type A 2.2.2.2 TTL = 30
       against.the.evil.Galactic.Empire type A 2.2.2.2 TTL = 30
       During.the.battle type A 2.2.2.2 TTL = 30
       Rebel.spies.managed type A 2.2.2.2 TTL = 30
       to.steal.secret.plans type A 2.2.2.2 TTL = 30
       to.the.Empires.ultimate.weapon type A 2.2.2.2 TTL = 30
  ++   invalid section: not enough records
```

3. Case 3: random7.irl.

random7.ril trace:

```
Lookup: random7.irl
Query : random7.irl, type 1, TXID 0000
Server : 128.194.135.82
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 42 bytes
  TXID 0000 flags 8400 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
```

4. Case 4: random4.irl.

random4.ril trace:

```
Lookup: random4.irl
Query : random4.irl, type 1, TXID 0000
Server : 128.194.135.82
*******************************
Attempt 0 with 29 bytes... response in 1 ms with 180 bytes
  TXID 0000 flags 8400 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 A 2.2.2.2 TTL = 30
       A.NEW.HOPE type A 2.2.2.2 TTL = 30
       It.is.a.period.of.civil.war type A 2.2.2.2 TTL = 30
  ++    invalid record: RR value length beyond packet
```

RR value length beyond packet error indicates that the answer in a record (length: FixedRR->length) is beyond the packet size. The way to handle this error is to check after get the FixedRR structure data. Compare the answer length (FixedRR->length) plus the current offset and the received packet size. If current offset plus answer length is greater than the total packet size, then it is a RR value length beyond packet error. Below is the related code:

```
FixedRR *frr = (FixedRR *)(recvBuf + *curPos);
       *curPos += sizeof(FixedRR);
       // check RR value length beyond packet error
       if (*curPos + ntohs(frr->dataLen) > recvBytes)
       {
              printf("  ++\tinvalid record: RR value length beyond packet\n");
              return false;
       }
```

```
Lookup: random4.irl
Query : random4.irl, type 1, TXID 0000
Server : 128.194.135.82
*******************************
Attempt 0 with 29 bytes... response in 0 ms with 35 bytes
  TXID 0000 flags 8400 questions 1 answers 1 authority 0 additional 11
  succeeded with Rcode = 0
  ------------ [questions] ----------
       random4.irl type 1 class 1
  ------------ [answers] ------------
```

++ invalid record: truncated name

Truncated name error indicates that the name of a record (whether in the beginning of a record or at the end) is truncated by the packet. This error can be detected by keep checking the current offset and the packet total size when parsing the name.
When a truncated name occurs, it must happens in the uncompressed part, so in my implementation, at the beginning of the uncompressed part parsing (There is a while loop parsing every name to handle multiple jumps). The related code is as below:

```
// check Truncated name error
	if (ans + *ans + 1 > (UBYTE *)(recvBuf + recvBytes - 1))
	{
		printf("  ++\tinvalid record: truncated name\n");
		return false;
	}
```

Lookup: random4.irl
Query : random4.irl, type 1, TXID 0000
Server : 128.194.135.82
****
Attempt 0 with 29 bytes... response in 1 ms with 259 bytes
 TXID 0000 flags 8400 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 A 2.2.2.2 TTL = 30
    A.NEW.HOPE type A 2.2.2.2 TTL = 30
    It.is.a.period.of.civil.war type A 2.2.2.2 TTL = 30
    Rebel.spaceships type A 2.2.2.2 TTL = 30
    striking.from.a.hidden.base type A 2.2.2.2 TTL = 30
 ++ invalid record: truncated fixed RR header

Truncated fixed RR header error indicates that the FixedRR is not completed (beyond the packet size). The way to handle this error is to check after successfully parsing the name, before get the FixedRR structure data. Compare the FixedRR header length (sizeof(FixedRR)) plus the current offset and the received packet size. If current offset

plus FixedRR header length is greater than the total packet size, then it is a fixed RR header error. Below is the related code:

```
// check Truncated fixedRR error
	if ((*curPos + sizeof(FixedRR)) > recvBytes - 1)
	{
		printf("  ++\tinvalid record: truncated fixed RR header\n");
		return false;
	}
```

5 Extra credit: random8.irl.

After a few probe of the random8.irl with my program. I figured out how the sender end works. The reply packet is a 486-bytes fixed packet. It is a constant content legal packet polluted by random number (range from 10 to 40) of continuous “lol” blocks in random position (after offset 0x60 before 0x1e0).

Below is the original packet content.

The random parameters are speculated after a huge number of trying. I changed the program a little bit to capture the beginning of the “lol” pollution and the number of “lol’ blocks, but didn’t found any fixed pattern. But the number of “lol” blocks are always from 10 to 40 (so I guess it generated by 10 + rand(30) something with linear distribution) Also, the starting offset of “lol” blocks are always greater than 0x60 and smaller or equal 0x1e0 also linear distribution.

```
0000   9c 8e 99 25 91 ea 00 03 32 45 30 00 08 00 45 00  ...%....2E0...E.
0010   01 f0 03 c4 00 00 7f 11 29 77 80 c2 87 52 80 c2  ........)w...R..
0020   83 eb 00 35 eb 9a 01 dc f3 25 00 01 84 00 00 01  ...5.....%......
0030   00 01 00 00 00 0b 07 72 61 6e 64 6f 6d 38 03 69  .......random8.i
0040   72 6c 00 00 01 00 01 06 72 61 6e 64 6f 6d 03 69  rl......random.i
0050   72 6c 00 00 01 00 01 00 00 00 1e 00 04 01 01 01  rl..............
0060   01 07 45 70 69 73 6f 64 65 02 49 56 00 00 01 00  ..Episode.IV....
0070   03 00 00 00 1e 00 04 02 02 02 02 01 41 03 4e 45  ............A.NE
0080   57 04 48 4f 50 45 00 00 01 00 03 00 00 00 1e 00  W.HOPE..........
0090   04 02 02 02 02 02 49 74 02 69 73 01 61 06 70 65  ......It.is.a.pe
00a0   72 69 6f 64 02 6f 66 05 63 69 76 69 6c 03 77 61  riod.of.civil.wa
00b0   72 00 00 01 00 03 00 00 00 1e 00 04 02 02 02 02  r...............
00c0   05 52 65 62 65 6c 0a 73 70 61 63 65 73 68 69 70  .Rebel.spaceship
00d0   73 00 00 01 00 03 00 00 00 1e 00 04 02 02 02 02  s...............
00e0   08 73 74 72 69 6b 69 6e 67 04 66 72 6f 6d 01 61  .striking.from.a
00f0   06 68 69 64 64 65 6e 04 62 61 73 65 00 00 01 00  .hidden.base....
0100   03 00 00 00 1e 00 04 02 02 02 02 04 68 61 76 65  ............have
0110   03 77 6f 6e 05 74 68 65 69 72 05 66 69 72 73 74  .won.their.first
0120   07 76 69 63 74 6f 72 79 00 00 01 00 03 00 00 00  .victory........
0130   1e 00 04 02 02 02 02 07 61 67 61 69 6e 73 74 03  ........against.
0140   74 68 65 04 65 76 69 6c 08 47 61 6c 61 63 74 69  the.evil.Galacti
0150   63 06 45 6d 70 69 72 65 00 00 01 00 03 00 00 00  c.Empire........
0160   1e 00 04 02 02 02 02 06 44 75 72 69 6e 67 03 74  ........During.t
0170   68 65 06 62 61 74 74 6c 65 00 00 01 00 03 00 00  he.battle.......
```

```
0180   00 1e 00 04 02 02 02 02 05 52 65 62 65 6c 05 73  .........Rebel.s
0190   70 69 65 73 07 6d 61 6e 61 67 65 64 00 00 01 00  pies.managed....
01a0   03 00 00 00 1e 00 04 02 02 02 02 02 74 6f 05 73  ............to.s
01b0   74 65 61 6c 06 73 65 63 72 65 74 05 70 6c 61 6e  teal.secret.plan
01c0   73 00 00 01 00 03 00 00 00 1e 00 04 02 02 02 02  s...............
01d0   02 74 6f 03 74 68 65 07 45 6d 70 69 72 65 73 08  .to.the.Empires.
01e0   75 6c 74 69 6d 61 74 65 06 77 65 61 70 6f 6e 00  ultimate.weapon.
01f0   00 01 00 03 00 00 00 1e 00 04 02 02 02 02        ..............
```