Dns Resolver Analysis

Martin Fracker

March 6, 2017

In figure 1 we can see that packet indicates a jump into fixed header. This is essentially an occurence of the byte 0xc0 followed by a byte equal to or less than 0x0b.

In figure 2 the server returned a packet smaller than 12 bytes, the size of the fixed header.

In figure 3 the packet indicated a jump that would result in a location past the end of the packet.

In figure 4 the packet indicates a jump with byte 0xc0 at some position x within the packet, followed by another byte which indicated an offset of x. This results in an infinite jump loop.

In figure 5 the packet indicated a huge amount of additional records. This inevitably results in the program eventually expecting a jump offset past the boundary of the packet.

In figure 6 the packet intends to indicate an answer by jumping. This is indicated by the last byte of the packet, 0xc0. However, because the jump indicator is the last byte of the packet, the packet offset is truncated.

In figure 7 the packet indicates an answer length that is longer than the amount of bytes left in the rest of the packet.

In figure 8 the packet indicates that its one question is x amount of bytes long which is larger than the amount of bytes in the rest of the packet. For this case, since questions are handled differently in code and are displayed differently than answers, authorities, and additional answers, they were special enough to have their own error category.

In figure 9 the packet ends before the next name is finished being specified. That is, not only is there no trailing null byte, but the name length, indicates a name longer than there are bytes left in the rest of the packet.

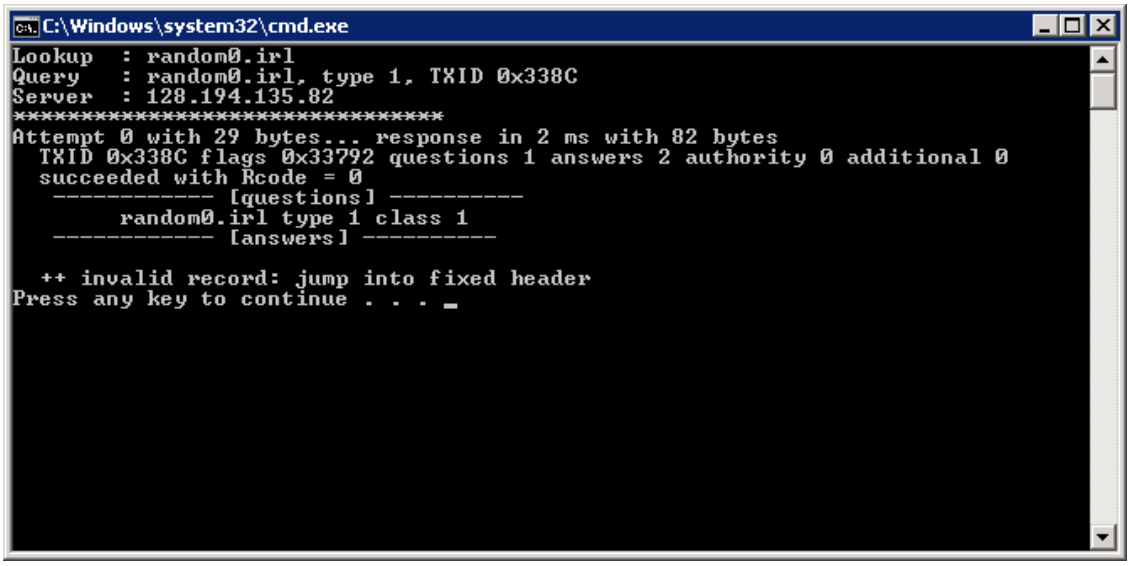

Figure 1: Jump into fixed header

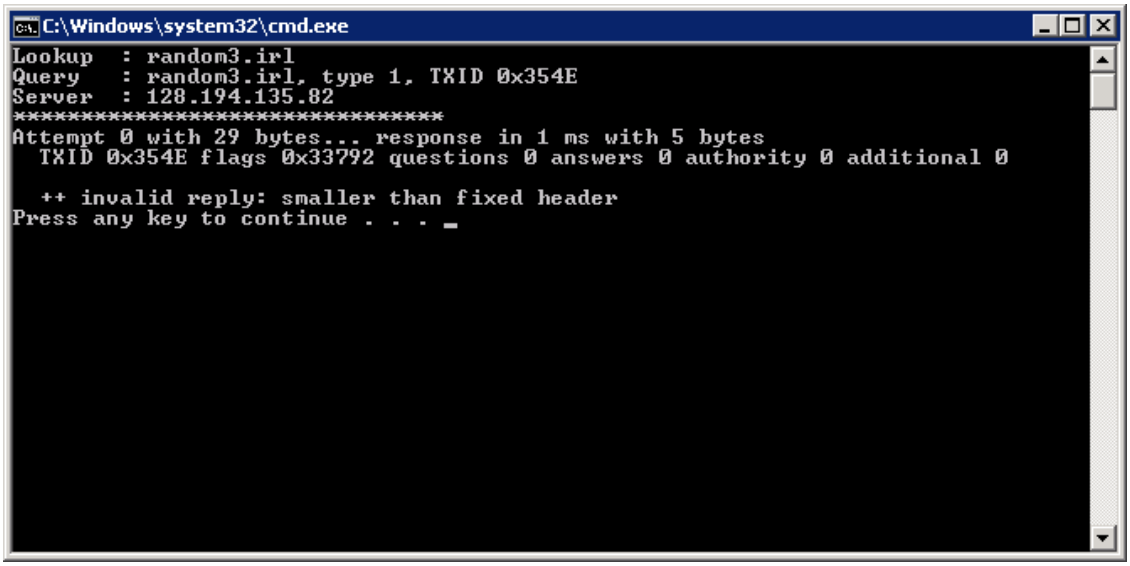

Figure 2: Smaller than fixed header

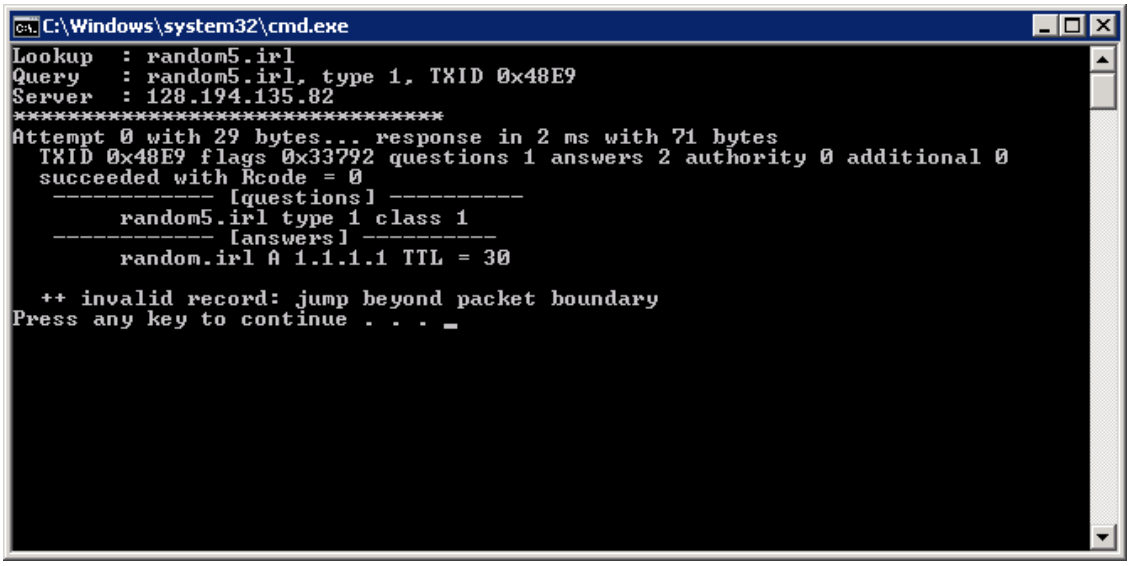

Figure 3: Jump beyond packet boundary

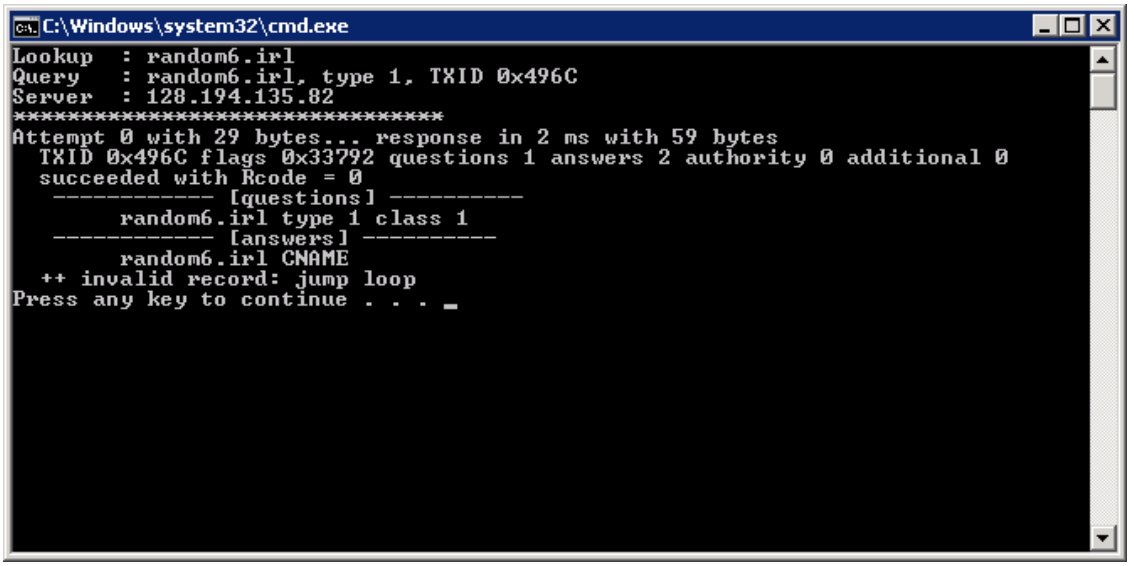

Figure 4: Jump loop

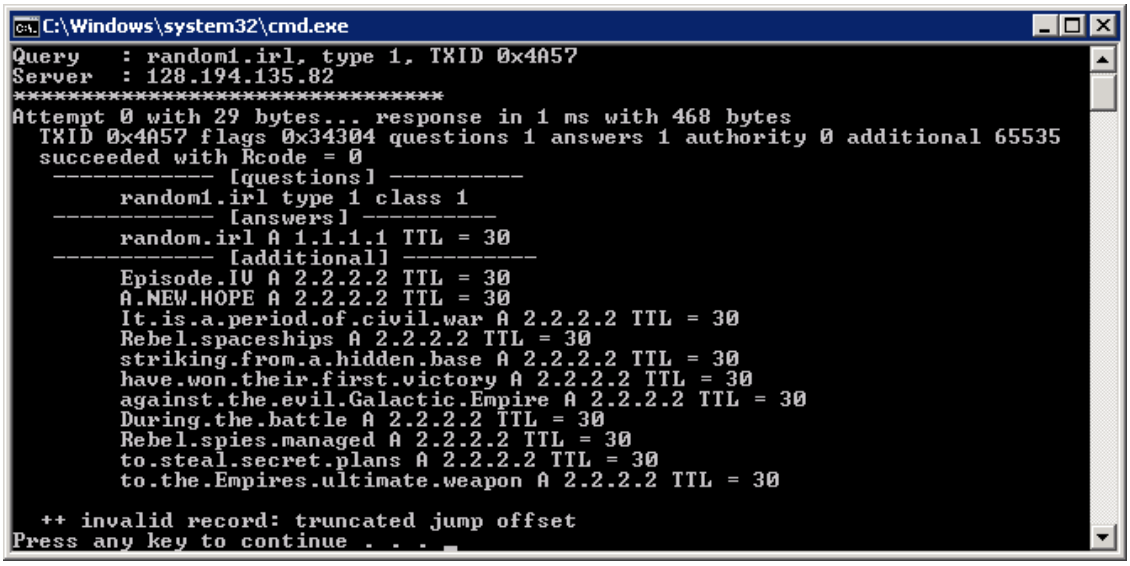

Figure 5: Truncated jump offset

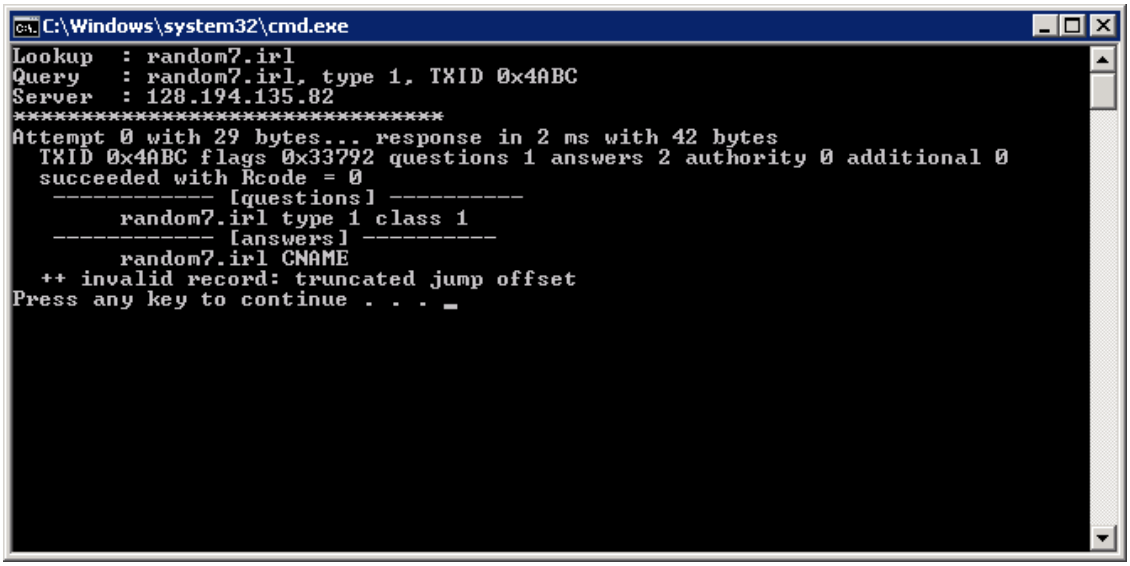

Figure 6: Truncated jump offset

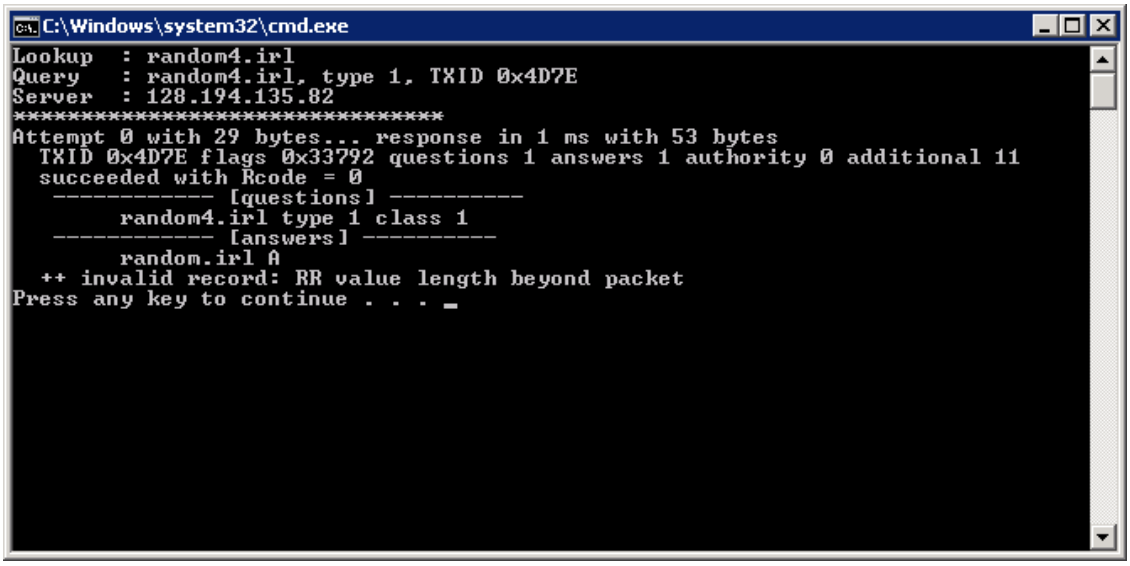

Figure 7: RR value length beyond packet

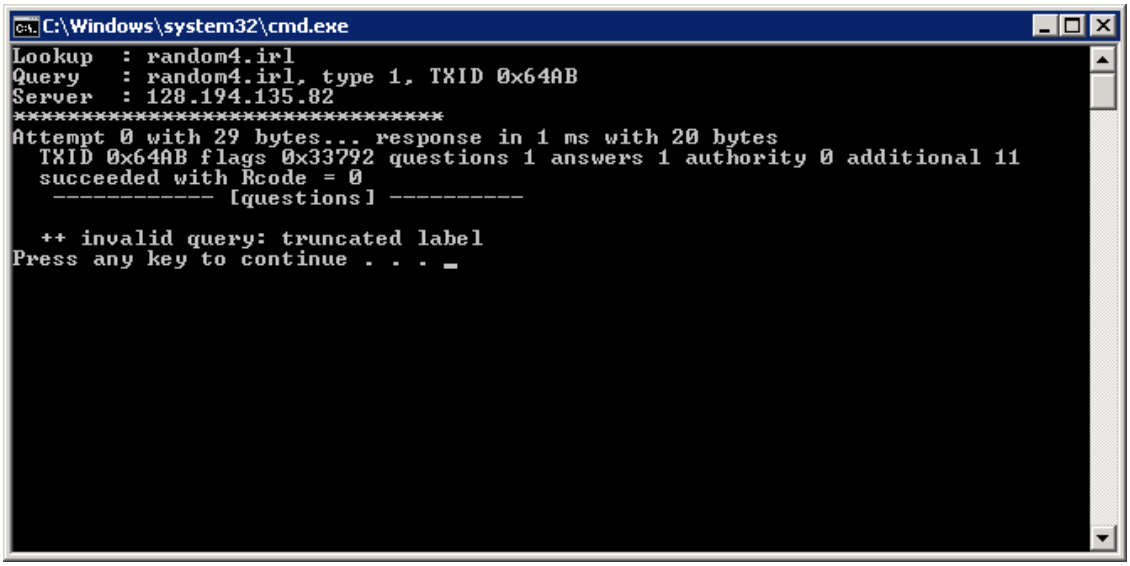

Figure 8: Truncated label

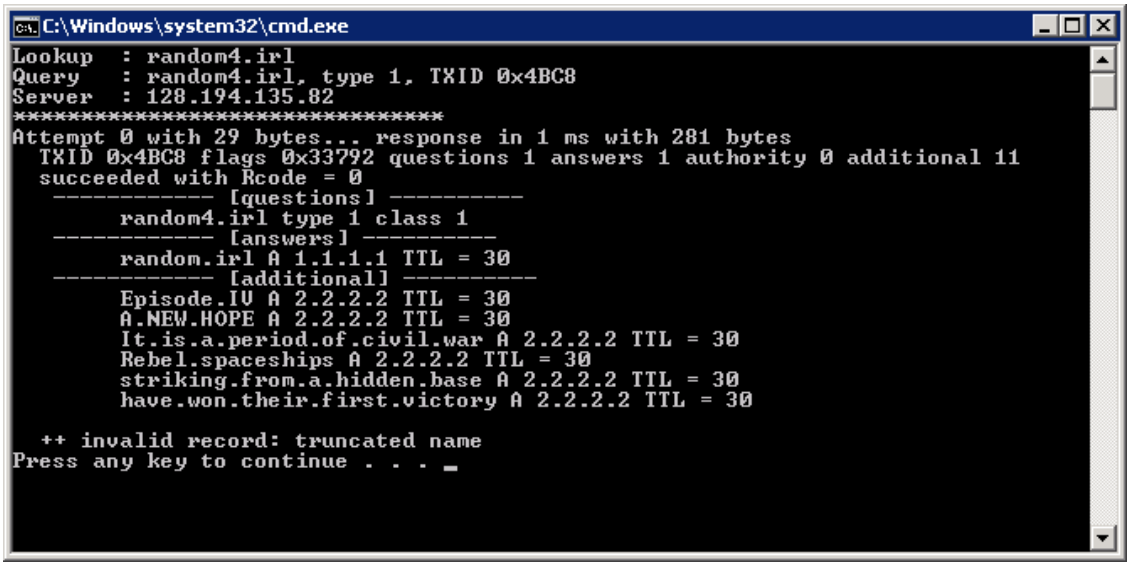

Figure 9: Truncated name