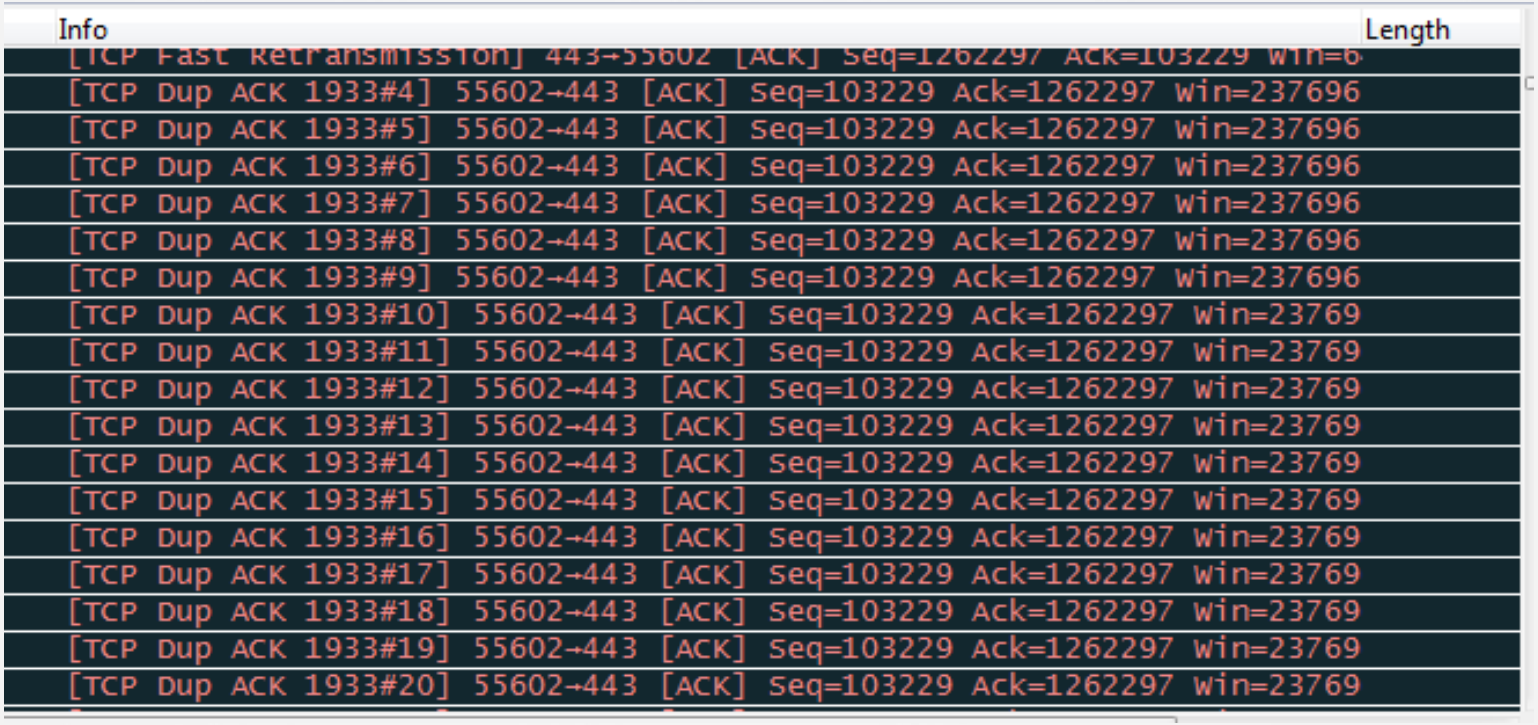
Analysis of the Attack

Analysis of the Attack

- Using Wireshark to solve a security issue
- Buffer 0verflow
  - Odd patterns in the data
  - Retransmissions
  - Resets (RST)
- Denial of Service
  - You can use multiple tools in Wireshark to get answers

Analysis of the Attack



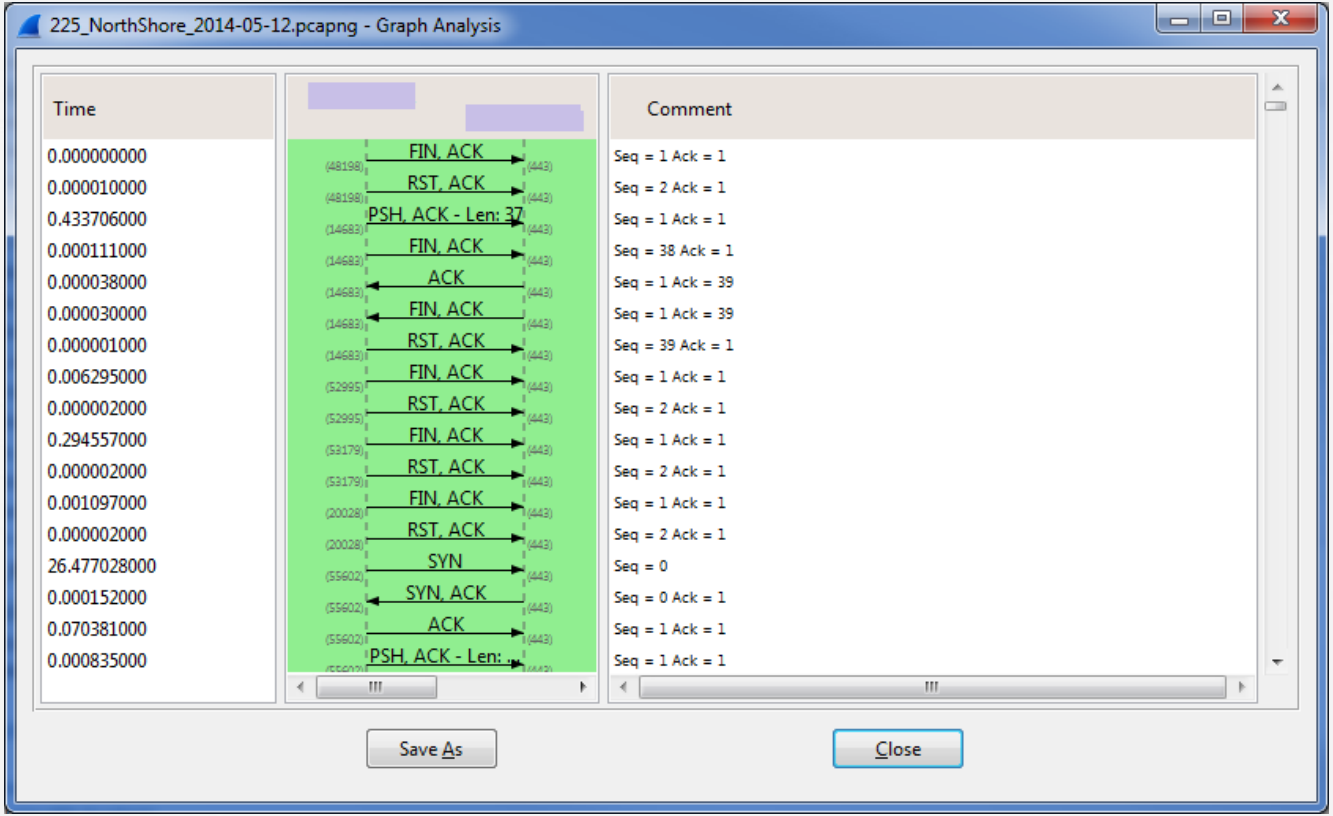
Analysis of the Attack

```
[redacted]#show buffers

Buffer elements:
     500 in free list (500 max allowed)
     2370 hits, 0 misses, 0 created

Public buffer pools:
Small buffers, 104 bytes (total 16, permanent 10):
     11 in free list (0 min, 10 max allowed)
     1770 hits, 33 misses, 22 trims, 28 created
     9 failures (0 no memory)
Middle buffers, 600 bytes (total 90, permanent 90):
     89 in free list (10 min, 200 max allowed)
     590 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Big buffers, 1524 bytes (total 90, permanent 90):
     90 in free list (5 min, 300 max allowed)
     126 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
VeryBig buffers, 4520 bytes (total 10, permanent 10):
     10 in free list (0 min, 300 max allowed)
     50 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Large buffers, 5024 bytes (total 10, permanent 10):
     10 in free list (0 min, 30 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Huge buffers, 18024 bytes (total 2, permanent 0):
     0 in free list (0 min, 13 max allowed)
```

Analysis of the Attack



Questions?