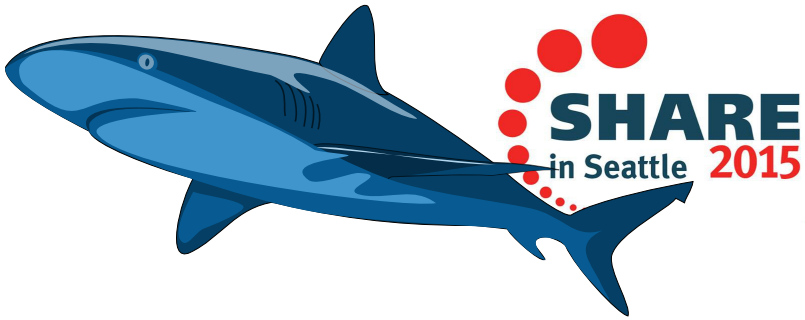
SHARK@SHARE



wireshark Hands-On Lab

Thursday, March 5, 2015
01:45 PM – 02:45 PM
Sheraton Seattle, Redwood
Session 16752
https://ibm.biz/SHARKatSHARE

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

Wireshark Lab Part I. General Questions

- How long was the trace running?
  - The trace captured a timeframe of _____ seconds
- What is the average packet rate?
  - The average packet rate is ____ packets/s
- What are the 3 top talker IP addresses in the trace?
  - IP address 1: __.__.__.__ - ____ packets
  - IP address 2: __.__.__.__ - ____ packets
  - IP address 3: __.__.__.__ - ____ packets
- Save number_1's traffic under a new filename
  - Filter: ip.addr eq aa.bb.cc.dd
  - File → Export specified packets → wireshark pcapng format!
  - Filename: SHARE16752.TopTalker.pcapng

Wireshark Lab Part II. TCP Questions

- How many TCP sessions start in this trace
  - The trace contains _____ new TCP connections
- How many TCP sessions terminate in this trace
  - The trace contains _____ terminating TCP connections
- What are the top 3 clients connecting in the trace?
  - IP address 1: __.__.__.__ - ____ new sessions
  - IP address 2: __.__.__.__ - ____ new sessions
  - IP address 3: __.__.__.__ - ____ new sessions
- Save number_1's traffic under a new filename
  - Filter: ip.addr eq aa.bb.cc.dd - File → Export specified packets
  - Filename: SHARE16752.TopTalker.client1.pcapng
- Save number_2's and number_3's traffic also
  - File → Export …

Wireshark Lab Part III. TN3270 Questions

- How many TN3270 sessions are started in the trace?
  - There are ___ new TN3270 sessions starting in the trace
- How many TCP ports is the TN3270 Server listening on?
  - The TN3270 Server listens on ports ___ ___ ___ ___ ___
- What are the top 3 clients connecting to the TN3270 server?
  - IP address 1: __.__.__.__ - ____ new sessions
  - IP address 2: __.__.__.__ - ____ new sessions
  - IP address 3: __.__.__.__ - ____ new sessions
- What is the percentage of all TN3270 traffic in the trace?
  - Filter: tcp.port==23 or tcp.port==nnnn || tcp.port= nnnn ...
  - Filename: SHARE16752.TopTalker.client1.pcapng
- Save all TN3270 traffic under a new file
  - File → Export … SHARE16752.TN3270.pcapng

Wireshark Lab Part III. TLS Questions

- How many active TLS sessions are in the trace?
  - There are ____ sessions that carry TLS application data.
- What other server ports besides TN3270 support TLS?
  - Following servers sent a ServerHello: Ports ___ ___ ___ ___
- What are the top clients connecting via SSL to the TN3270?
  - IP address 1: __.__.__.__ - ____ ClientHello packets
  - IP address 2: __.__.__.__ - ____ ClientHello packets
  - IP address 3: __.__.__.__ - ____ ClientHello packets
  - IP address 4: __.__.__.__ - ____ ClientHello packets
  - IP address 5: __.__.__.__ - ____ ClientHello packets
- Save all traffic of the IP subnet of #4 and #5 under a new file
  - File → Export … SHARE16752.IPSubnet.pcapng

Wireshark Lab Part Background

- What the TCP payload looks like

Telnet Negotiation

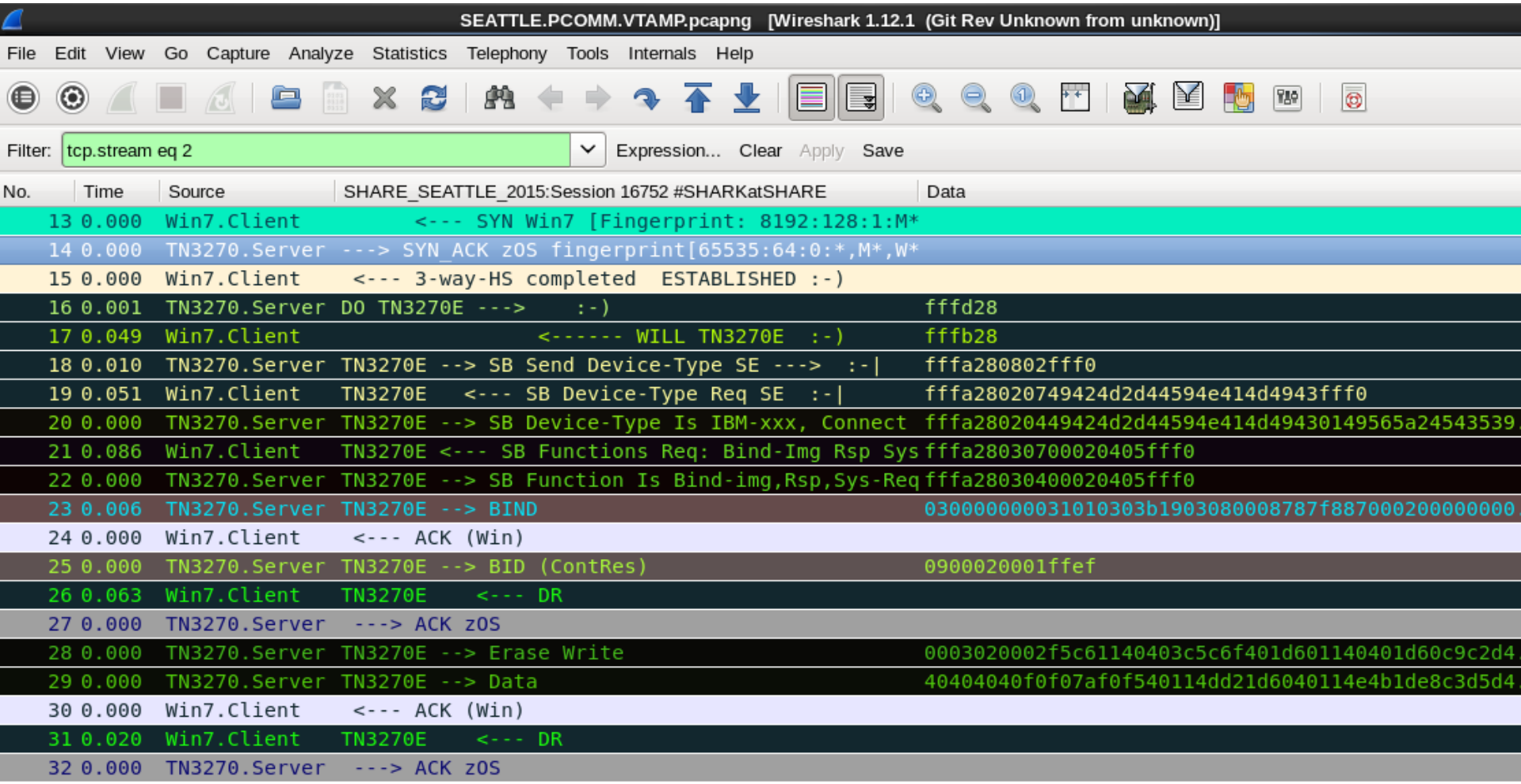
```
FFFD2E DO   TLS
FFFC2E WONT TLS
FFFD28 DO   TN3270E
FFFB28 WILL TN3270E
FFFA28 SB TN3270E
          00 Associate
          01 Connect
          02 Dev-Type
          03 Functions
          04 Is
          05 Reason
          06 Reject
          07 Request
          08 Send
```

Keepalive Probes

```
FFFB06 WILL TIMEMARK
FFFC06 WONT TIMEMARK
FFFD06 DO TIMEMARK
```

```
8055010301 SSLV2 ClientHello V31
14 --- Change Cipher Spec ---
1403vv 0001 01 ChangeCipherSpec
15 --- Alert ---------------
1603vv xxxx yy
    00  SSL3.0
16 --- Handshake Protocol ---
1603vv xxxx yy
    00  SSL3.0
    01  TLS1.0
    02  TLS1.1
    03  TLS1.2
          01 ClientHello
          02 ServerHello
          0B Certificate
          0E ServerHelloDone
          10 ClientKeyExchange
17 --- Application Data ---
1703vv xxxx yy Encrypted ApplData
```

Successful TN3270 Negotiation



Successful TLS Negotiation