Packet stories

Sake Blok
Relational therapist for computer systems
sake.blok@SYN-bit.nl

SYN-bit
deep traffic analysis

$ whoami

- Relational therapist for computer systems
  - Solve {application,network,performance}-issues by looking at the communication between systems
- Member Wireshark core-team since 2007
- Started SYN-bit in 2010
  - Application and Network troubleshooting
  - Protocol and packet analysis
  - Training (Wireshark, TCP, TLS)
- Wireshark Certified Analyst (WCA) #1 🎉

SYN-bit

deep traffic analysis

Application and network troubleshooting

Protocol and packet analysis

Training (Wireshark, TCP, SSL)

www.SYN-bit.nl

Some stories from real cases

- Cases
  - 1: Can't reach a certain site over a proxy (ask.wireshark.org)
  - 2: Long live (video) streams get interrupted
  - 3: Retransmission on a local area without errors
  - 4: (optional bonus) Hotel WiFi at Sharkfest'25 US
- How to optimize Wireshark for specific tasks
- What information to look for as "proof"

https://www.flickr.com/photos/lexnger/2061061452

Case 01: Question on TCP/RST

- Question about "RST: present, Fin: Absent..."
  - Actually comes from tcp.completeness
- But why is the session reset by the proxy?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.33.192.95	172.16.223.11	TCP	74	42450 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=75
2	0.004341	172.16.223.11	10.33.192.95	TCP	74	8080 → 42450 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PE
3	0.004436	10.33.192.95	172.16.223.11	TCP	66	42450 → 8080 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=750112695 TSecr
4	0.004749	10.33.192.95	172.16.223.11	HTTP	163	CONNECT canara-feedback-api-6aa27f6f44c6.herokuapp.com:443 HTTP/1.1
5	0.005329	172.16.223.11	10.33.192.95	TCP	60	8080 → 42450 [RST] Seq=1 Win=0 Len=0
6	1.032959	10.33.192.95	172.16.223.11	TCP	74	42458 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=75
7	1.036347	172.16.223.11	10.33.192.95	TCP	74	8080 → 42458 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PE
8	1.036451	10.33.192.95	172.16.223.11	TCP	66	42458 → 8080 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=750113727 TSecr
9	1.036786	10.33.192.95	172.16.223.11	HTTP	163	CONNECT canara-feedback-api-6aa27f6f44c6.herokuapp.com:443 HTTP/1.1
10	1.037347	172.16.223.11	10.33.192.95	TCP	60	8080 → 42458 [RST] Seq=1 Win=0 Len=0

DEMO: case-01.pcapng

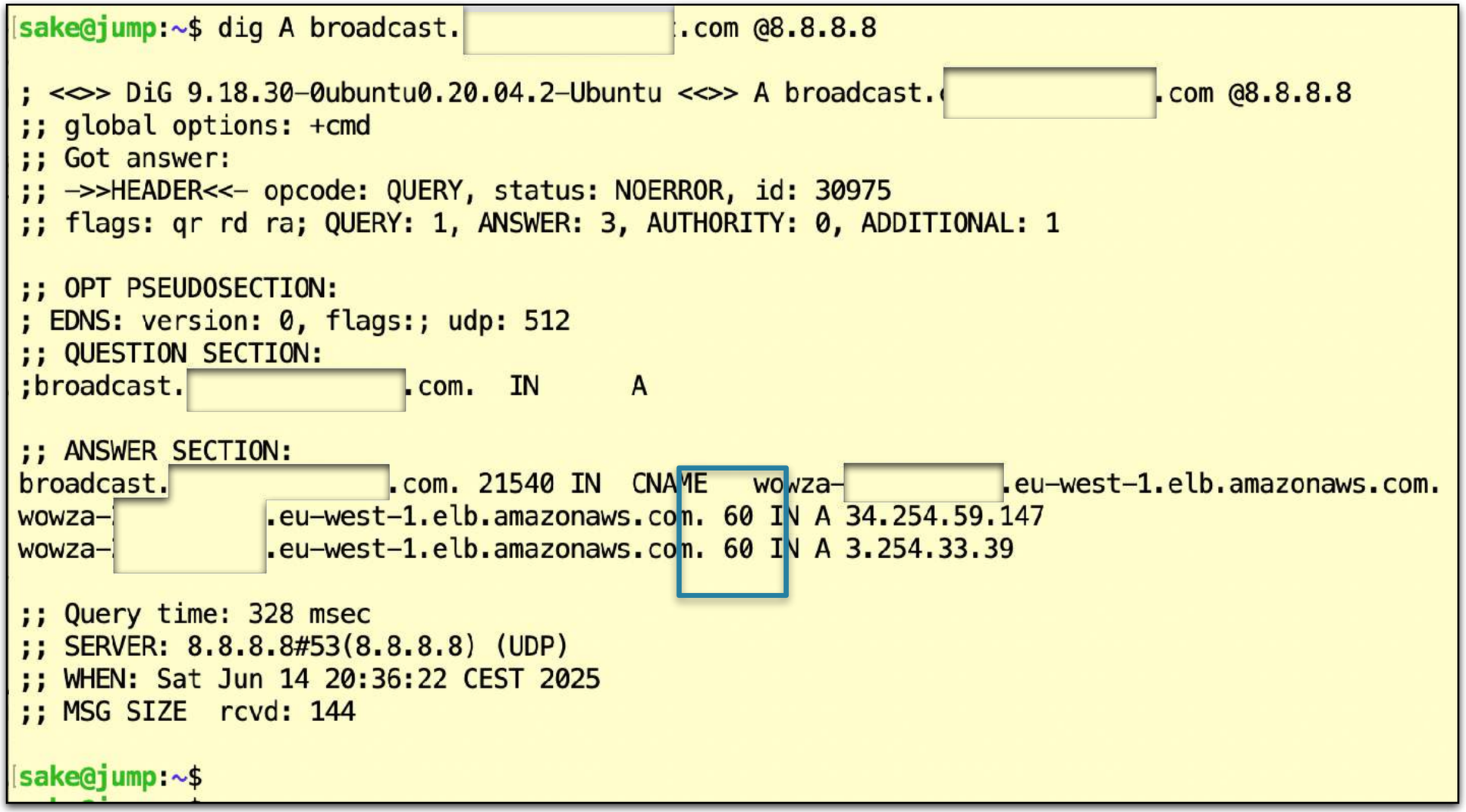
Case 01: Resolution & tips

- Firewall has URL filtering enabled and blocked the website
- Add columns of interest, makes life a lot easier
- Timing of packets is important
  - Can things happen at the time shown in Wireshark?

Case 02: Broken video streams

- Live streaming of city council hearings
- Streams break
  - Usually in long hearings
  - Mostly at ten to the hour (like ~22:50)
- Cause of issue not clear
  - client blames streaming provider
  - streaming provider blames clients network
  - Suspicion of DNS involvement
- TCP sessions of up to 14 hours long
  - 10-30 GB each! A total of 800 GB was captured
  - 10-100 million packets each

Case 02: DNS TTL of 60 seconds



```
sake@jump:~$ dig A broadcast.[redacted].com @8.8.8.8

; <<>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <<>> A broadcast.[redacted].com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30975
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;broadcast.[redacted].com.  IN      A

;; ANSWER SECTION:
broadcast.[redacted].com. 21540 IN  CNAME   wowza-[redacted].eu-west-1.elb.amazonaws.com.
wowza-[redacted].eu-west-1.elb.amazonaws.com. 60 IN A 34.254.59.147
wowza-[redacted].eu-west-1.elb.amazonaws.com. 60 IN A 3.254.33.39

;; Query time: 328 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sat Jun 14 20:36:22 CEST 2025
;; MSG SIZE  rcvd: 144

sake@jump:~$
```

Case 02: Let's monitor DNS changes

```
#!/bin/bash

OLDFILE=/home/sake/.dns-current
LOGFILE=/home/sake/.dns.log
DATETIME=$(date "+%Y%m%d-%H:%M")

OLD=$(cat $OLDFILE)
NEW=$(dig A broadcast.xxx.com +short | grep -v "communications error" | sort | paste -s -d, -)

if [ "$NEW" = "$OLD" ]; then
        echo "$DATETIME : no change" >> $LOGFILE
else
        echo "$DATETIME : $NEW" >> $LOGFILE
        echo $NEW > $OLDFILE
        curl --request POST \
             --url https://api.pushover.net/1/messages.json \
             --header 'Accept: application/json' \
             --header 'Content-Type: application/json' \
             --data "{
               \"token\": \"auyi5.........................\",
               \"user\": \"uorg3.........................\",
               \"title\": \"DNS changed for broadcast.xxx.com\",
               \"message\": \"New A records: $NEW\nOld A records: $OLD\",
               \"priority\": 0
             }"
fi
```

Case 02: Some stats on 1 stream

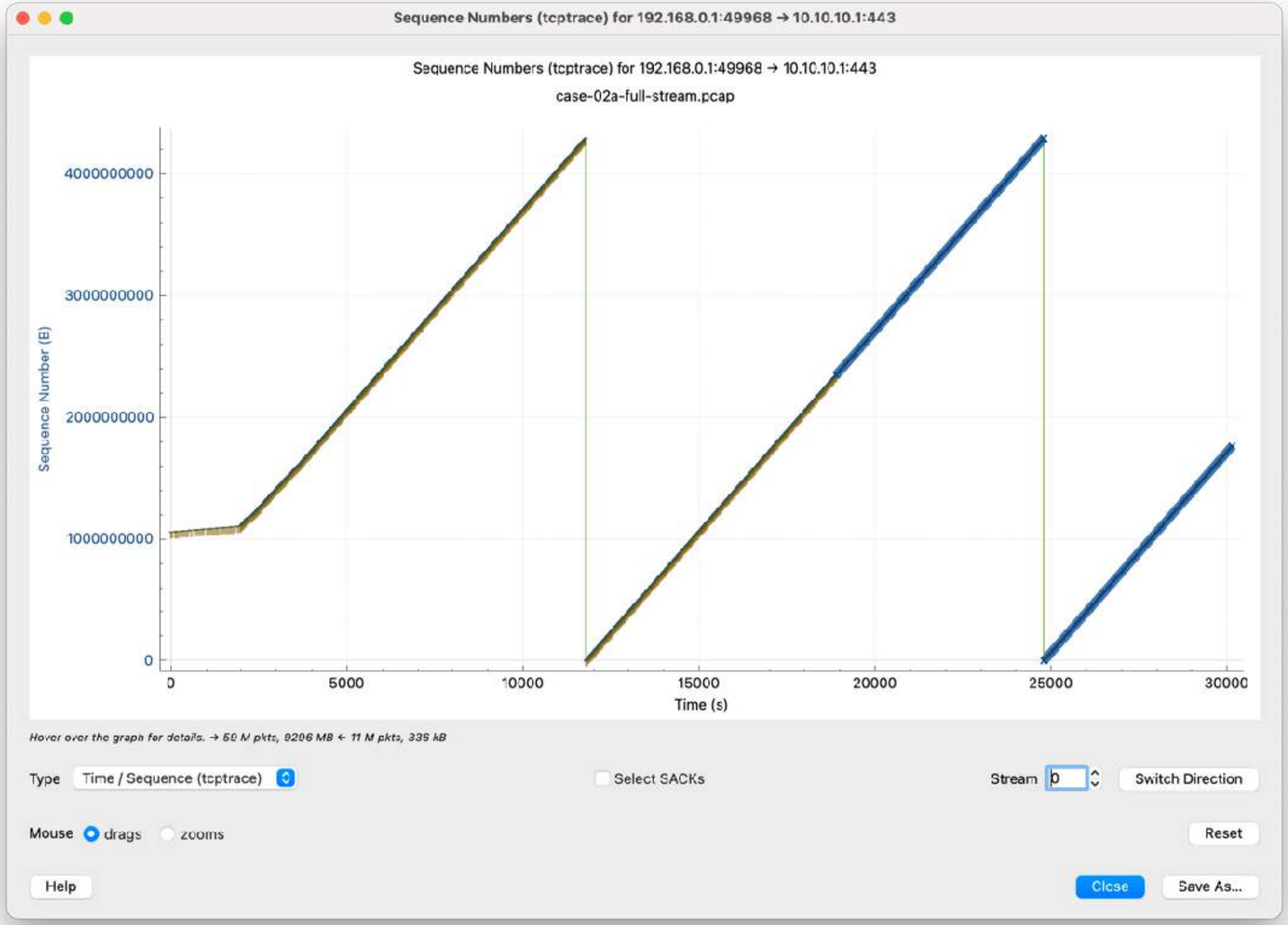
Time

First packet:	2024-11-22 08:30:32
Last packet:	2024-11-22 16:53:08
Elapsed:	08:22:36

Statistics

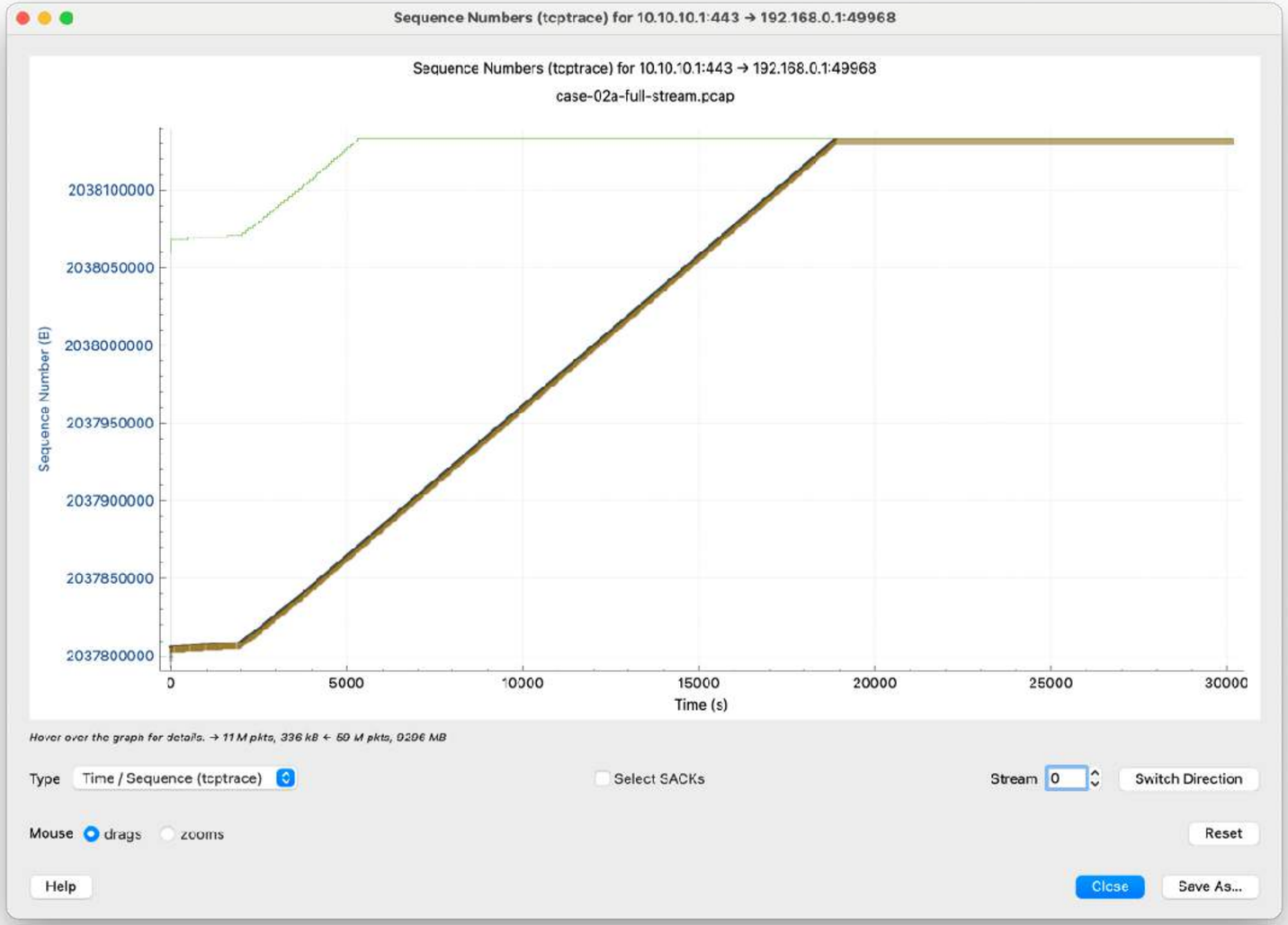
Measurement	Captured
Packets	70616773
Time span, s	30156.019
Average pps	2341.7
Average packet size, B	191
Bytes	13459875259
Average bytes/s	446 k
Average bits/s	3570 k

Case 02: The video upload



DEMO: case-02b-rollover.pcapng

Case 02: Zero window?



DEMO: case-02c-ws-decline.pcapng

DEMO: case-02d-zerowindow.pcapng

Case 02: Collected info (I)

Real time	Source	Info
09:30:03,999	CwcEncodingManager.log	INFO CWCEncodingManager.WebcastManager - Time: server = 11/22/2024 08:30:04, encoder = 11/22/2024 09:30:00, difference = 00:59:56.6088423 (0.99905801175h)
09:30:10,492	H264EncodingService.log	INFO Cwc.H264EncodingService.Models.Writer - Writer starting C:\Program Files\xxx\CwcEncodingService\archive\xxx_20241122_1-part0.ts
09:30:11,147	H264EncodingService.log	INFO Cwc.H264EncodingService.Models.Writer - Writer starting rtmps://broadcast.xxx.com:443/live/CWCENCODER-xxx/<UUID>
09:30:12,182	PCAP	DNS: broadcast.xxx.com => 34.241.39.86, 54.155.185.97
09:30:12,185	PCAP	TCP: SYN 10.x.x.x:57525 -> 34.241.39.86:443, MSS=1460/1460, WS=256/256
09:30:13,259	H264EncodingService.log	INFO Cwc.H264EncodingService.Models.Writer - Starttime 2024-11-22T08:30:12.2880000Z
10:57:06,351	PCAP	Last window-size increase (1020 -> 1026, ie 261120 -> 262656)
10:57:20,912	PCAP	Start final window-size decline to 0 (1026 -> 1025, ie 262656 -> 262400)
15:45:00,000	DNS-check	DNS changed to 52.212.68.153,63.34.179.176

Case 02: Collected info (II)

Real time	Source	Info
16:01:57,402	PCAP	Last data from server
16:01:57,419	PCAP	Start zero-window condition in client
18:18:12,486	H264EncodingService.log	WARN Cwc.H264EncodingService.Models.Writer - @Gap 500ms.
18:18:13,126	H264EncodingService.log	INFO Cwc.H264EncodingService.Models.Writer - NewTotalReportedOffset: 1000

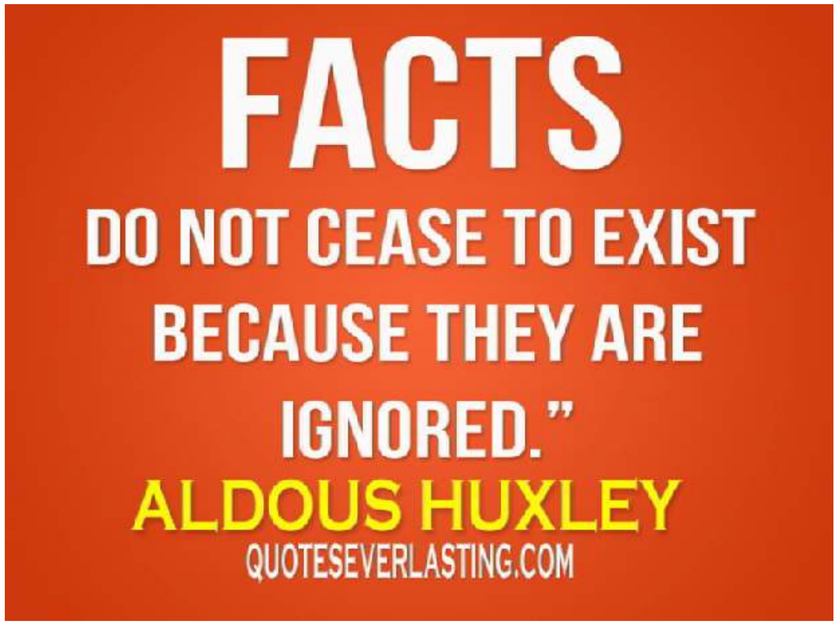
DEMO: case-02e-rst.pcapng

Case 02: Collected info (II)

Real time	Source	Info
16:01:57,402	PCAP	Last data from server
16:01:57,419	PCAP	Start zero-window condition in client
18:18:12,486	H264EncodingService.log	WARN Cwc.H264EncodingService.Models.Writer - @Gap 500ms.
18:18:13,126	H264EncodingService.log	INFO Cwc.H264EncodingService.Models.Writer - NewTotalReportedOffset: 1000
22:52:50,136	PCAP	Last ACK from the server
22:52:50,386	PCAP	First retransmissions from the client
22:52:51,134	H264EncodingService.log	WARN Cwc.H264EncodingService.Models.Writer - @Gap 1083ms.
22:52:52,635	H264EncodingService.log	INFO Cwc.H264EncodingService.Models.Writer - NewTotalReportedOffset: 2000
22:52:59,687	PCAP	Last retransmission from the client
22:53:07,640	H264EncodingService.log	WARN Cwc.H264EncodingService.Models.Writer - @Stream interrupted, restarting. Possible causes: bad connection or invalid api key.
22:53:09,287	PCAP	TCP/RST from the client

Case 02: facts so far...

- Analysed 16 full video streams
- Only broken when DNS change during stream
  - But DNS change not always breaks the stream
  - The stream breaks a long time after DNS change
- Failing retransmissions -> RST
- Firewall (Fortigate) rules based on FQDN
  - temporarily changing 1 test encoder to "ALL"
  - problem does not occur for that encoder
- Still puzzled by the "ten to the hour" timing
- Is this a BUG or a FEATURE (config issue!)?



https://www.flickr.com/photos/quoteseverlasting/8740641703

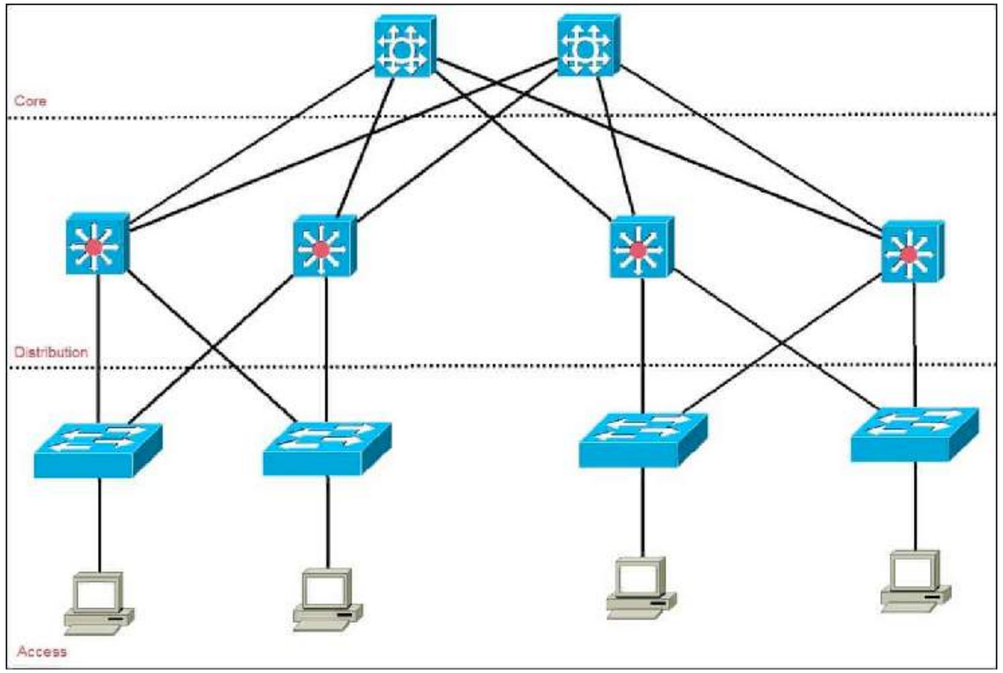
Case 02: ... the resolution!

- May-dirty?
  - https://community.fortinet.com/t5/FortiGate/Technical-Tip-Dirty-session/ta-p/197748
  - https://community.fortinet.com/t5/FortiGate/Technical-Tip-Explanation-of-the-FQDN-nbsp-default-nbsp-cache/ta-p/213280
  - https://community.fortinet.com/t5/FortiGate/Technical-Tip-Information-about-firewall-session-dirty/ta-p/195802
- Feature to re-evaluate the policy rules under certain conditions
  - FortiGuard update being one of them
  - Configured hourly update interval at...
    - ... "ten to the hour" !!!
- So when...
  - There was a DNS change during the video stream...
  - ... and an update to the FortigGuard files...
  - ... the session is marked "dirty" and the policy rule gets re-evaluated...
  - ... and because the IP address does not match the ones in DNS...
  - ... the packets are dropped, causing retransmissions... and finally a TCP/RST

Case 03: TCP retransmissions

- Two servers are connected to different server switches (L2)
- The two server switches use the same distribution switch (L2)
- The distribution switch is connected to the core switch that provides the routing function in this network (L3)

- ***Many retransmissions are detected on the servers (TCP stats) and the source of the retransmissions needs to be found***



Case 03: Packet Hero Quiz Time

- Which of the following statements is true (choose one):

A. The packet with sequence number 49 (frame 4) was received out of order by host 10.0.0.1

B. Frame 14 is a retransmission of frames 4, 5, 6, 7, 8 and 11 because these frames were not received by host 10.0.0.1

C. Frame 4 was dropped by an intermediate network device, therefor frames 5, 6 and 7 generated 3 duplicate ACKs that triggered the fast-retransmission in frame 14

D. The ICMP redirect in frame 16 was caused by a wrongly configured subnet-mask on host 10.0.0.2

DEMO: case-03.pcapng

Case 03: True or False

- Which of the following statements is true (choose one):

A. ✅The packet with sequence number 49 (frame 4) was received out of order by host 10.0.0.1

B. ✅Frame 14 is a retransmission of frames 4, 5, 6, 7, 8 and 11
❌because these frames were not received by host 10.0.0.1

C. ❌Frame 4 was dropped by an intermediate network device, therefor
✅frames 5, 6 and 7 generated 3 duplicate ACKs that triggered the fast-retransmission in frame 14

D. ❌The ICMP redirect in frame 16 was caused by a wrongly configured subnet-mask on host 10.0.0.2

Case 03: Resolution & tips

- Static (host) routes on all systems, even though in the same subnet
  - Lazy standardised deployment scenario
- Each second, 1 ICMP redirect message
  - packet is routed over the CPU to generate the ICMP message
  - Process switched packets are slower (1 ms!)
- Use the right columns
- Use (temporary) coloring
- ICMP is your friend
- Using the ip.id field in troubleshooting can help
  - But beware of the different ip.id numbering strategies

Case 04: Hotel WiFi

- Internet access is really slow...
- Independent of time of day...

```
sake@Mac16:~$ scp 10MB.bin proton:
10MB.bin                                      100%   10MB 641.7KB/s   00:15
sake@Mac16:~$ scp  proton:10MB.bin .
10MB.bin                                      100%   10MB  36.9KB/s   04:37
sake@Mac16:~$ scp 10MB.bin proton:
10MB.bin                                      100%   10MB 574.4KB/s   00:17
sake@Mac16:~$ scp  proton:10MB.bin .
10MB.bin                                      100%   10MB  74.0KB/s   02:18
sake@Mac16:~$
```

Case 04: traceroute packet loss...

```
Start: 2025-06-18T00:13:47-0400
HOST: Mac16.local                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 172.20.0.1                                           0.0%   100    2.9  11.0   2.3 127.3  23.0
  2.|-- 50.219.234.33                                        9.0%   100  128.7  66.1  14.1 276.2  52.5
  3.|-- eg-1-1-18-3986-soag07.valley.va.richmond.comcast.net  6.0%   100   77.3  74.3  11.8 314.3  60.9
  4.|-- lg-107-ceg02.valley.va.richmond.comcast.net           3.0%   100   49.1  64.4   4.1 261.9  48.9
  5.|-- ae-286-ar02.staplesmllrd.va.richmond.comcast.net      7.0%   100   55.0  64.2   4.6 214.2  45.7
  6.|-- 68.86.172.249                                         6.0%   100   36.6  54.1   3.9 173.0  37.9
  7.|-- be-31512-cs01.doraville.ga.ibone.comcast.net          4.0%   100  186.1  59.9  15.7 186.1  30.8
  8.|-- be-2311-pe11.56marietta.ga.ibone.comcast.net          3.0%   100  137.7  56.6  15.0 169.0  23.9
  9.|-- ???                                                 100.0   100    0.0   0.0   0.0   0.0   0.0
 10.|-- be2847.ccr41.atl01.atlas.cogentco.com                 7.0%   100   74.1  73.5  15.7 305.3  59.9
 11.|-- be2112.ccr41.dca01.atlas.cogentco.com                 6.0%   100  160.5  85.8  23.3 291.4  59.3
 12.|-- port-channel8247.ccr91.dca04.atlas.cogentco.com       3.0%   100  181.0  96.4  20.9 301.1  66.0
 13.|-- be8073.ccr41.jfk02.atlas.cogentco.com                 8.0%   100  212.5 174.3 111.2 321.0  55.0
 14.|-- be3471.ccr31.bos01.atlas.cogentco.com                 6.0%   100  162.7 171.0 112.3 288.3  44.3
 15.|-- port-channel8668.ccr91.lhr01.atlas.cogentco.com       7.0%   100  153.1 159.8 107.1 319.0  43.3
 16.|-- be8669.ccr41.lon13.atlas.cogentco.com                 7.0%   100  251.6 170.6 120.5 347.8  45.7
 17.|-- be12194.ccr41.ams03.atlas.cogentco.com                9.0%   100  199.0 171.4 120.6 386.3  49.2
 18.|-- be2434.agr21.ams03.atlas.cogentco.com                 5.0%   100  152.6 166.6 120.0 334.4  37.0
 19.|-- 149.11.65.174                                        1.0%   100  282.2 166.8 119.1 360.3  53.5
 20.|-- 87.255.32.130                                        8.0%   100  231.8 172.6 124.4 308.6  48.4
 21.|-- proton.soleus.nu                                     6.0%   100  182.9 174.1 120.4 298.7  40.9
```

DEMO: case-04-{laptop|server}.pcapng

Case 04: Resolution & tips

- Deterministic or random packet loss?
- Packet loss in both directions?
- It helps to have captures on both sides, but...
  - SACK and DSACK can really help too
- TCP streamgraph (tcptrace) is your friend

Feedback:

(or through the online conference agenda)

Thank you!

If you still have questions?

sake.blok@SYN-bit.nl

SYN-bit
deep traffic analysis