Monitoring and Troubleshooting Without Packet Traces

Leveraging Cyber Tools

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Chris Hull
Distinguished Engineer
Capital One

Background

- Most organizations have a number of different network monitoring tools, designed for different use cases.

- Cybersecurity in general and the related Cyber tools in recent years have been a focus of investment

Network Performance Monitoring

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

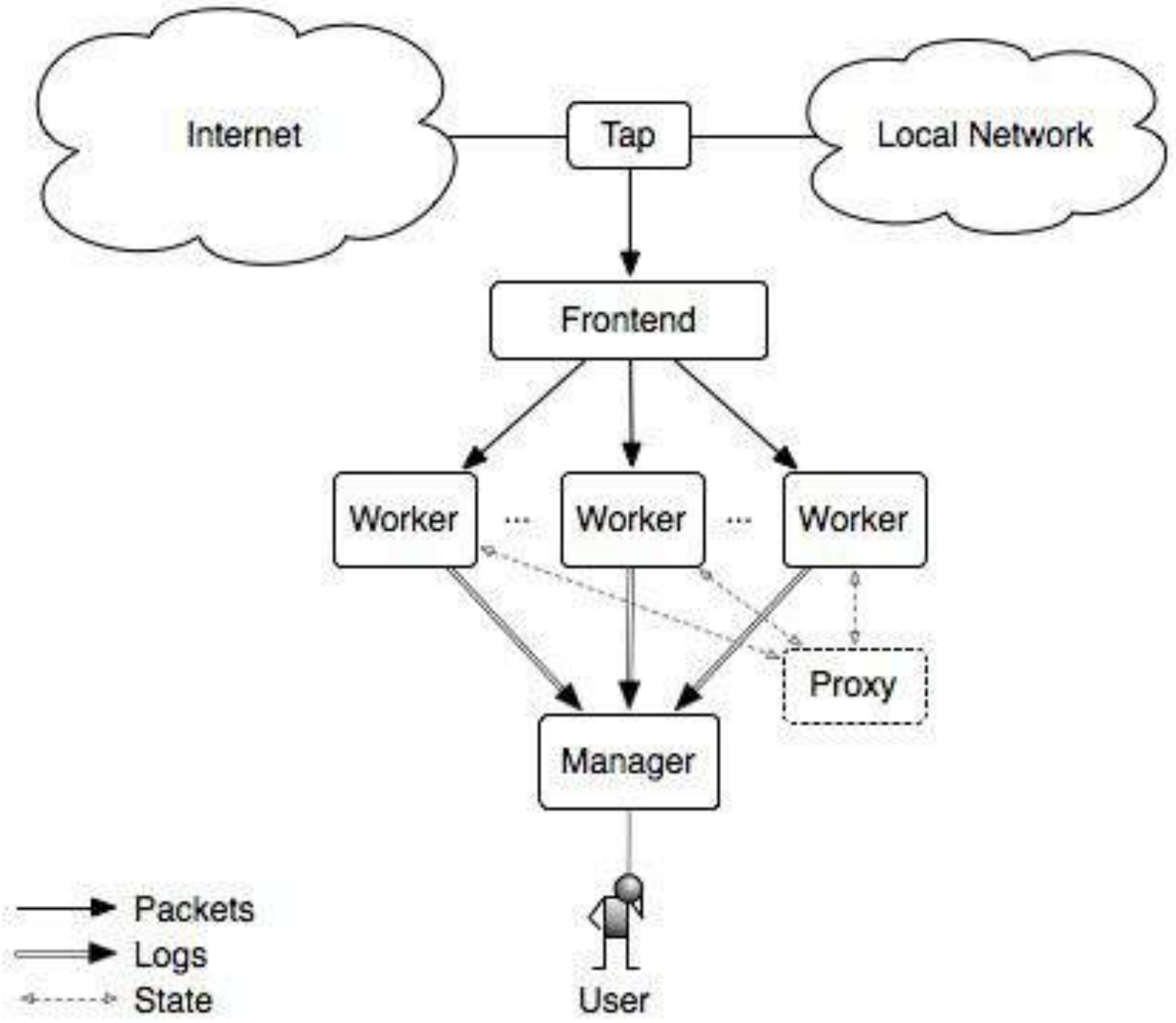
- Netscout
- Riverbed
- ExtraHop
- SolarWinds
- AppNeta
- cPacket
- - *so many others ($$$)*

or

Open Source Cyber Tools

- Wireshark (Packet Analyzer)
- Nagios Core (IDS)
- Snort (IDS/IPS)
- **Zeek (IDS)**
- Various Firewalls

Zeek Architecture

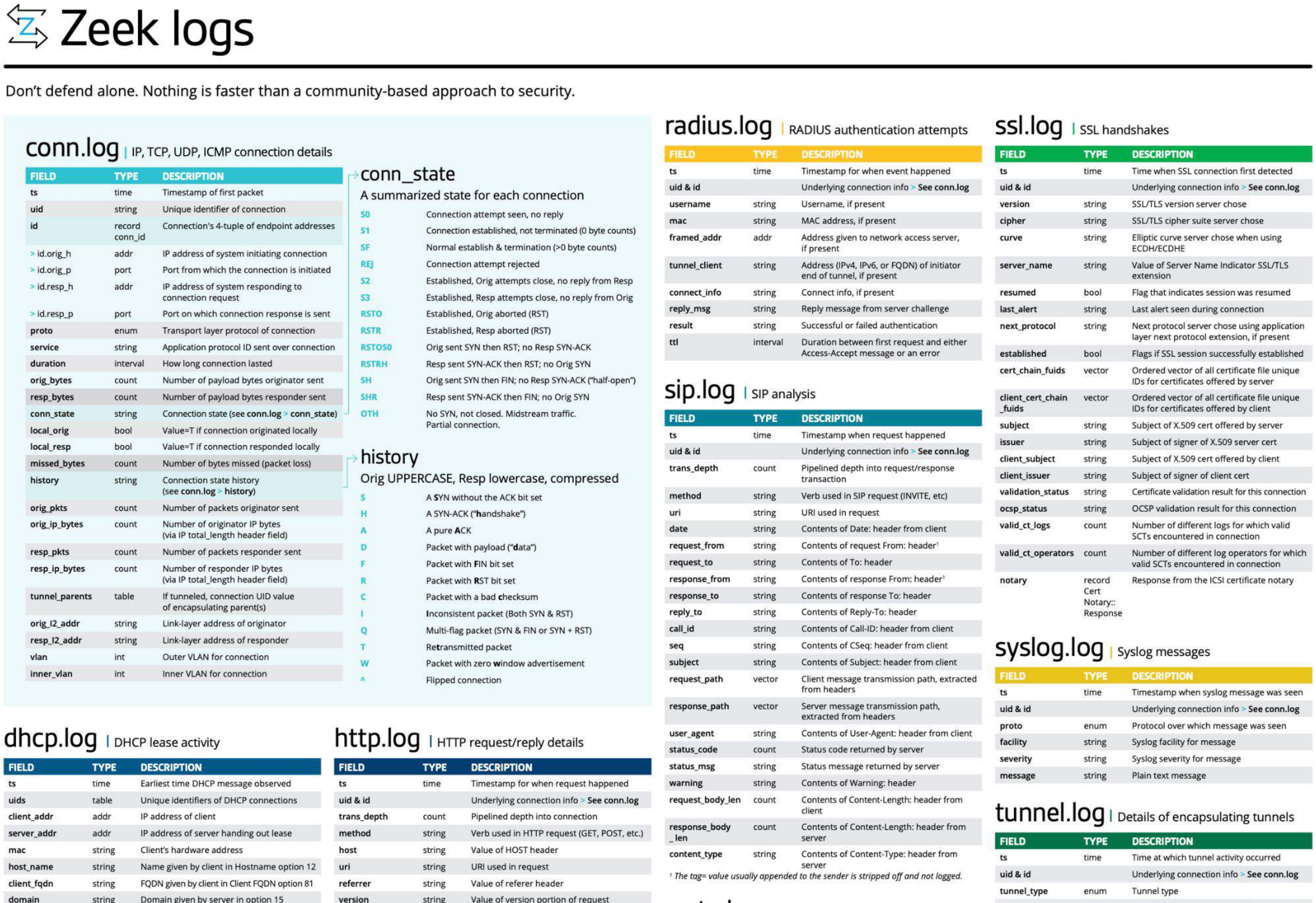


- Runs on Commodity hardware
- Taps from any source
- Scalable architecture
- Frontend is typically packet broker/switch
- Analysis is handled elsewhere

Book of Zeek - https://docs.zeek.org/en/master/cluster-setup.html

Data vs Metadata

- Packets are DATA
- Descriptive information about packet are METADATA
    - 10 packets
    - 23784 bytes
    - 10 connections
    - 4 connection failures
    - HTTP/S Protocol



Zeek logs

Don't defend alone. Nothing is faster than a community-based approach to security.

conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet
uid	string	Unique identifier of connection
id	record conn_id	Connection's 4-tuple of endpoint addresses
> id.orig_h	addr	IP address of system initiating connection
> id.orig_p	port	Port from which the connection is initiated
> id.resp_h	addr	IP address of system responding to connection request
> id.resp_p	port	Port on which connection response is sent
proto	enum	Transport layer protocol of connection
service	string	Application protocol ID sent over connection
duration	interval	How long connection lasted
orig_bytes	count	Number of payload bytes originator sent
resp_bytes	count	Number of payload bytes responder sent
conn_state	string	Connection state (see **conn.log** > **conn_state**)
local_orig	bool	Value=T if connection originated locally
local_resp	bool	Value=T if connection responded locally
missed_bytes	count	Number of bytes missed (packet loss)
history	string	Connection state history (see **conn.log** > **history**)
orig_pkts	count	Number of packets originator sent
orig_ip_bytes	count	Number of originator IP bytes (via IP total_length header field)
resp_pkts	count	Number of packets responder sent
resp_ip_bytes	count	Number of responder IP bytes (via IP total_length header field)
tunnel_parents	table	If tunneled, connection UID value of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of originator
resp_l2_addr	string	Link-layer address of responder
vlan	int	Outer VLAN for connection
inner_vlan	int	Inner VLAN for connection

conn_state

A summarized state for each connection

S0	Connection attempt seen, no reply
S1	Connection established, not terminated (0 byte counts)
SF	Normal establish & termination (>0 byte counts)
REJ	Connection attempt rejected
S2	Established, Orig attempts close, no reply from Resp
S3	Established, Resp attempts close, no reply from Orig
RSTO	Established, Orig aborted (RST)
RSTR	Established, Resp aborted (RST)
RSTOS0	Orig sent SYN then RST; no Resp SYN-ACK
RSTRH	Resp sent SYN-ACK then RST; no Orig SYN
SH	Orig sent SYN then FIN; no Resp SYN-ACK ("half-open")
SHR	Resp sent SYN-ACK then FIN; no Orig SYN
OTH	No SYN, not closed. Midstream traffic. Partial connection.

history

Orig UPPERCASE, Resp lowercase, compressed

S	A **S**YN without the ACK bit set
H	A SYN-ACK ("**h**andshake")
A	A pure **A**CK
D	Packet with payload ("**d**ata")
F	Packet with **F**IN bit set
R	Packet with **R**ST bit set
C	Packet with a bad **c**hecksum
I	**I**nconsistent packet (Both SYN & RST)
Q	Multi-flag packet (SYN & FIN or SYN + RST)
T	Re**t**ransmitted packet
W	Packet with zero **w**indow advertisement
^	Flipped connection

dhcp.log | DHCP lease activity

FIELD	TYPE	DESCRIPTION
ts	time	Earliest time DHCP message observed
uids	table	Unique identifiers of DHCP connections
client_addr	addr	IP address of client
server_addr	addr	IP address of server handing out lease
mac	string	Client's hardware address
host_name	string	Name given by client in Hostname option 12
client_fqdn	string	FQDN given by client in Client FQDN option 81
domain	string	Domain given by server in option 15

http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when request happened
uid & id		Underlying connection info > **See conn.log**
trans_depth	count	Pipelined depth into connection
method	string	Verb used in HTTP request (GET, POST, etc.)
host	string	Value of HOST header
uri	string	URI used in request
referrer	string	Value of referer header
version	string	Value of version portion of request

radius.log | RADIUS authentication attempts

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid & id		Underlying connection info > **See conn.log**
username	string	Username, if present
mac	string	MAC address, if present
framed_addr	addr	Address given to network access server, if present
tunnel_client	string	Address (IPv4, IPv6, or FQDN) of initiator end of tunnel, if present
connect_info	string	Connect info, if present
reply_msg	string	Reply message from server challenge
result	string	Successful or failed authentication
ttl	interval	Duration between first request and either Access-Accept message or an error

sip.log | SIP analysis

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when request happened
uid & id		Underlying connection info > **See conn.log**
trans_depth	count	Pipelined depth into request/response transaction
method	string	Verb used in SIP request (INVITE, etc)
uri	string	URI used in request
date	string	Contents of Date: header from client
request_from	string	Contents of request From: header[1]
request_to	string	Contents of To: header
response_from	string	Contents of response From: header[1]
response_to	string	Contents of response To: header
reply_to	string	Contents of Reply-To: header
call_id	string	Contents of Call-ID: header from client
seq	string	Contents of CSeq: header from client
subject	string	Contents of Subject: header from client
request_path	vector	Client message transmission path, extracted from headers
response_path	vector	Server message transmission path, extracted from headers
user_agent	string	Contents of User-Agent: header from client
status_code	count	Status code returned by server
status_msg	string	Status message returned by server
warning	string	Contents of Warning: header
request_body_len	count	Contents of Content-Length: header from client
response_body _len	count	Contents of Content-Length: header from server
content_type	string	Contents of Content-Type: header from server

[1] *The tag= value usually appended to the sender is stripped off and not logged.*

ssl.log | SSL handshakes

FIELD	TYPE	DESCRIPTION
ts	time	Time when SSL connection first detected
uid & id		Underlying connection info > **See conn.log**
version	string	SSL/TLS version server chose
cipher	string	SSL/TLS cipher suite server chose
curve	string	Elliptic curve server chose when using ECDH/ECDHE
server_name	string	Value of Server Name Indicator SSL/TLS extension
resumed	bool	Flag that indicates session was resumed
last_alert	string	Last alert seen during connection
next_protocol	string	Next protocol server chose using application layer next protocol extension, if present
established	bool	Flags if SSL session successfully established
cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by server
client_cert_chain _fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by client
subject	string	Subject of X.509 cert offered by server
issuer	string	Subject of signer of X.509 server cert
client_subject	string	Subject of X.509 cert offered by client
client_issuer	string	Subject of signer of client cert
validation_status	string	Certificate validation result for this connection
ocsp_status	string	OCSP validation result for this connection
valid_ct_logs	count	Number of different logs for which valid SCTs encountered in connection
valid_ct_operators	count	Number of different log operators for which valid SCTs encountered in connection
notary	record Cert Notary:: Response	Response from the ICSI certificate notary

syslog.log | Syslog messages

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when syslog message was seen
uid & id		Underlying connection info > **See conn.log**
proto	enum	Protocol over which message was seen
facility	string	Syslog facility for message
severity	string	Syslog severity for message
message	string	Plain text message

tunnel.log | Details of encapsulating tunnels

FIELD	TYPE	DESCRIPTION
ts	time	Time at which tunnel activity occurred
uid & id		Underlying connection info > **See conn.log**
tunnel_type	enum	Tunnel type

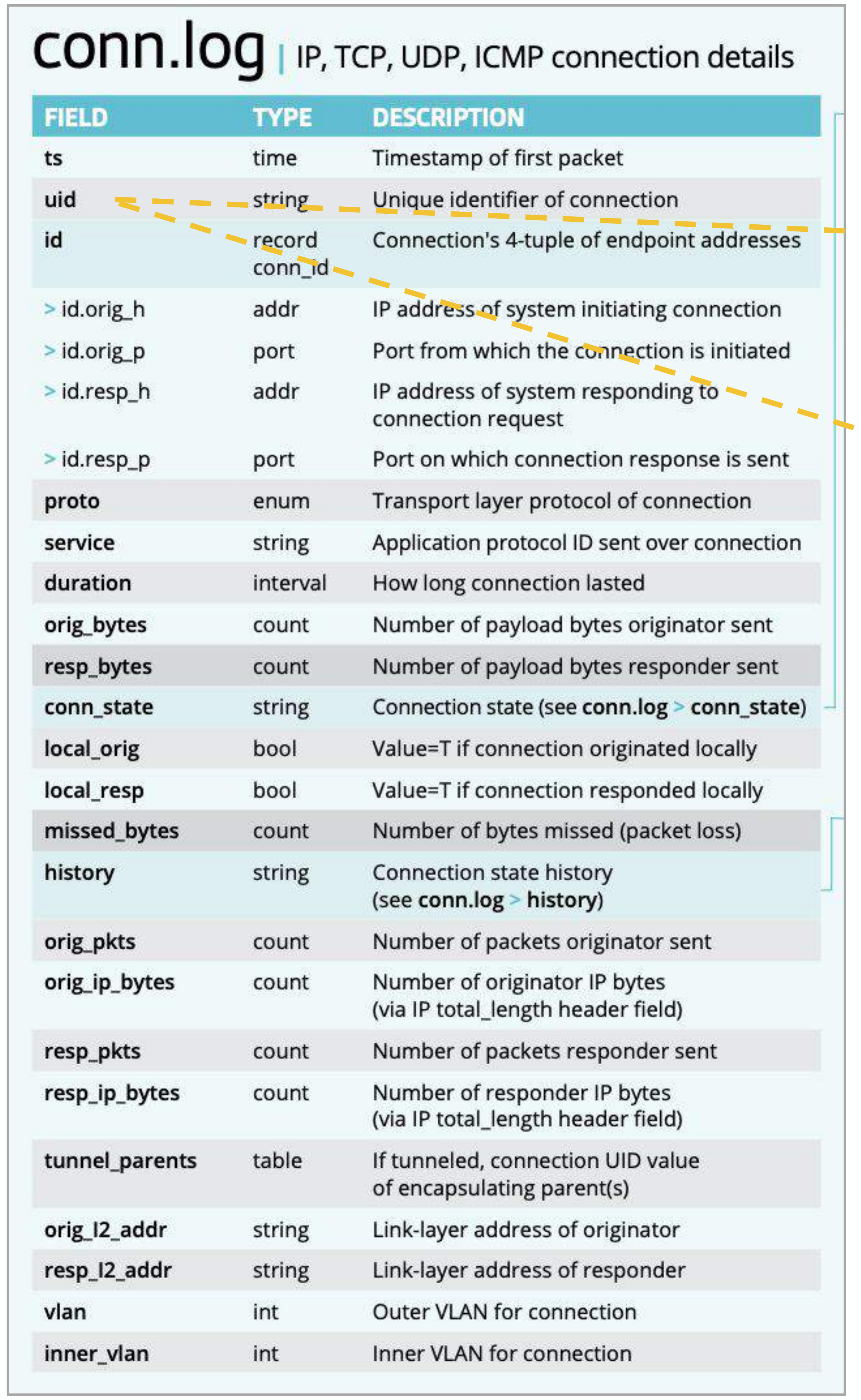
rkFest'24 US
15-20 · Fairfax, VA

#sf24us

Log Analytics

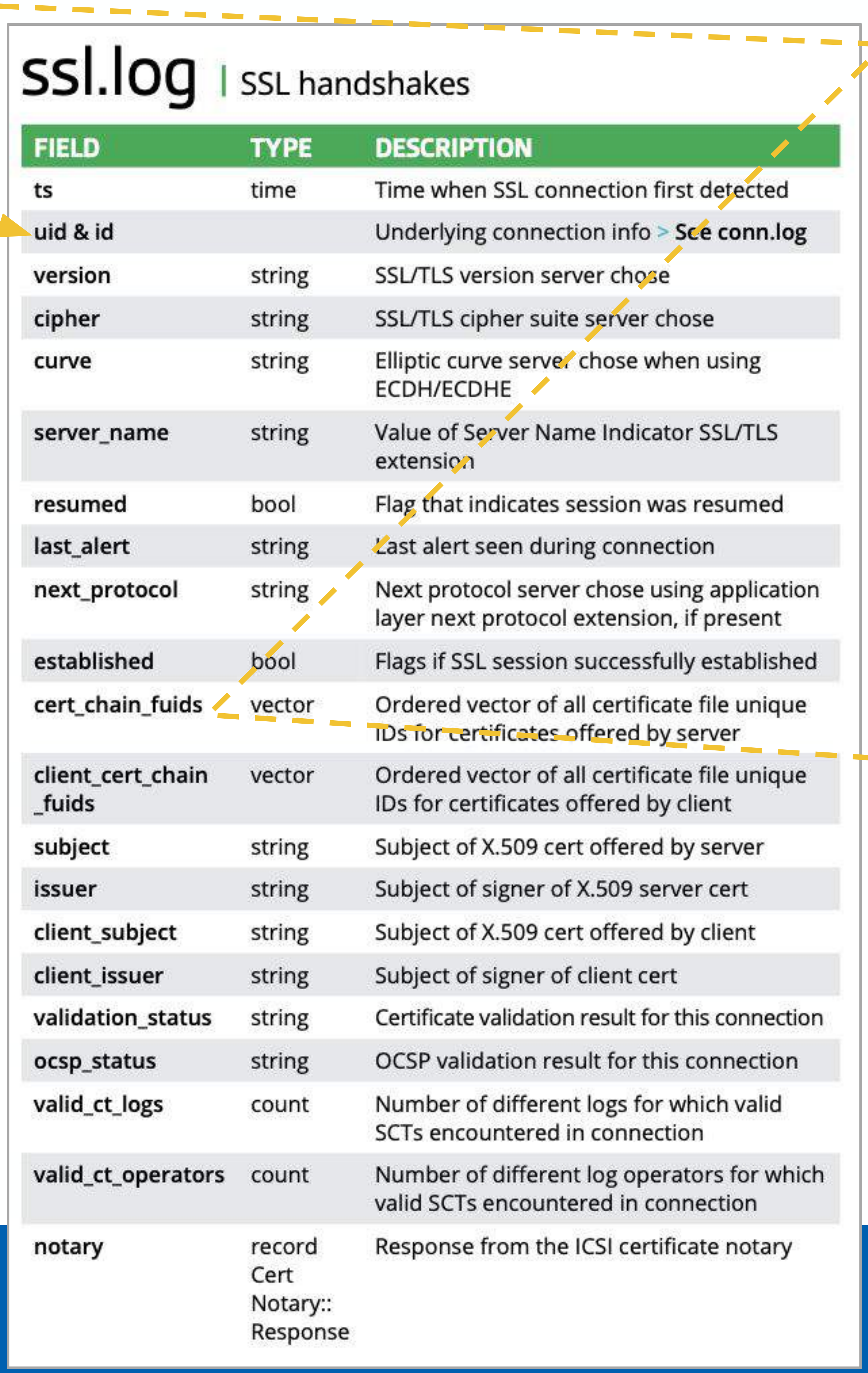
- May need to correlate across multiple logs
  - conn > ssl > files > x509 (investigate certs)
  - conn > dns (lookup hostnames)
- Log written at end of connection
  - No intermediate data available *without customization*

Following Zeek Logs



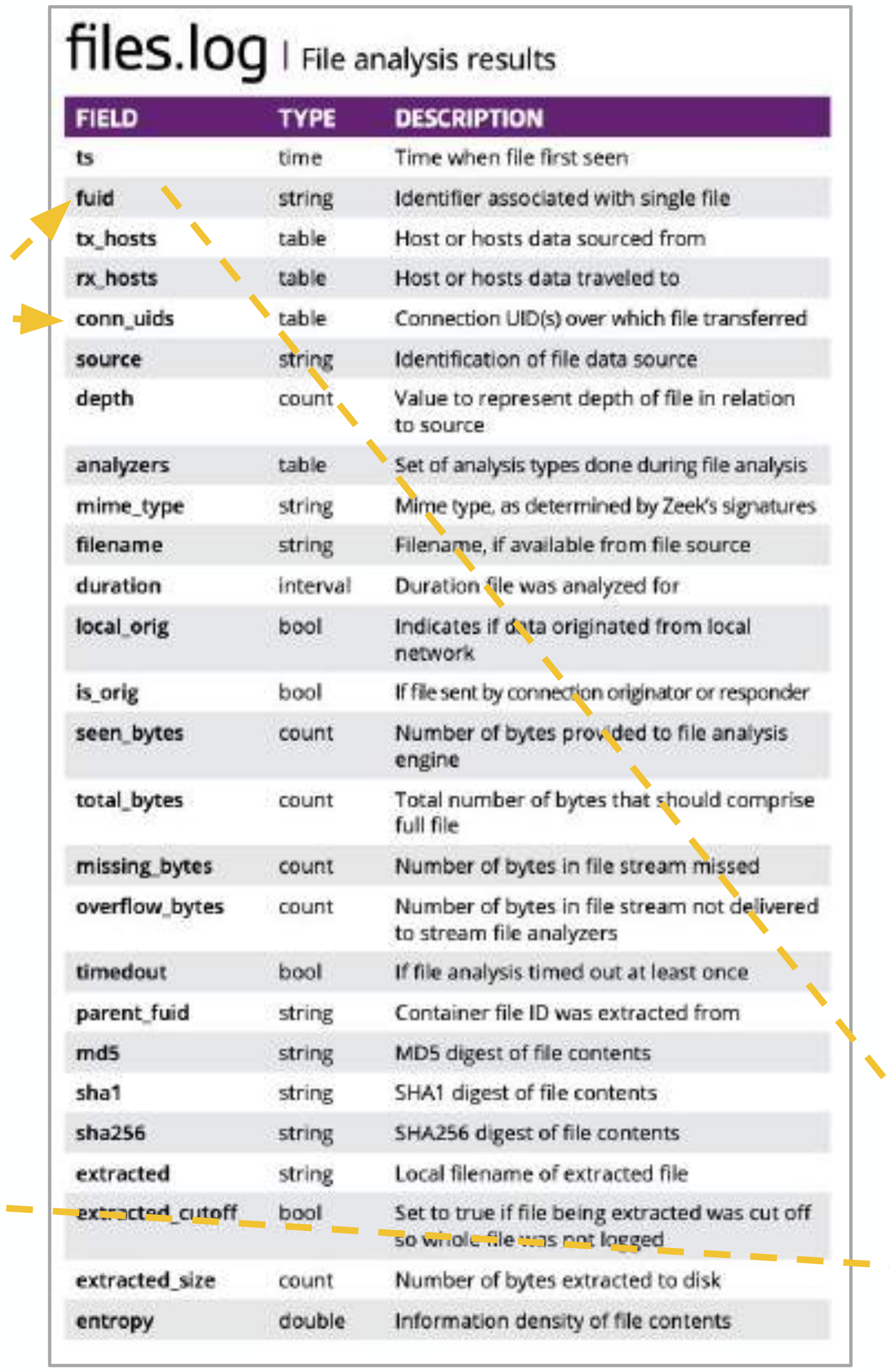
conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet
uid	string	Unique identifier of connection
id	record conn_id	Connection's 4-tuple of endpoint addresses
> id.orig_h	addr	IP address of system initiating connection
> id.orig_p	port	Port from which the connection is initiated
> id.resp_h	addr	IP address of system responding to connection request
> id.resp_p	port	Port on which connection response is sent
proto	enum	Transport layer protocol of connection
service	string	Application protocol ID sent over connection
duration	interval	How long connection lasted
orig_bytes	count	Number of payload bytes originator sent
resp_bytes	count	Number of payload bytes responder sent
conn_state	string	Connection state (see **conn.log** > **conn_state**)
local_orig	bool	Value=T if connection originated locally
local_resp	bool	Value=T if connection responded locally
missed_bytes	count	Number of bytes missed (packet loss)
history	string	Connection state history (see **conn.log** > **history**)
orig_pkts	count	Number of packets originator sent
orig_ip_bytes	count	Number of originator IP bytes (via IP total_length header field)
resp_pkts	count	Number of packets responder sent
resp_ip_bytes	count	Number of responder IP bytes (via IP total_length header field)
tunnel_parents	table	If tunneled, connection UID value of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of originator
resp_l2_addr	string	Link-layer address of responder
vlan	int	Outer VLAN for connection
inner_vlan	int	Inner VLAN for connection



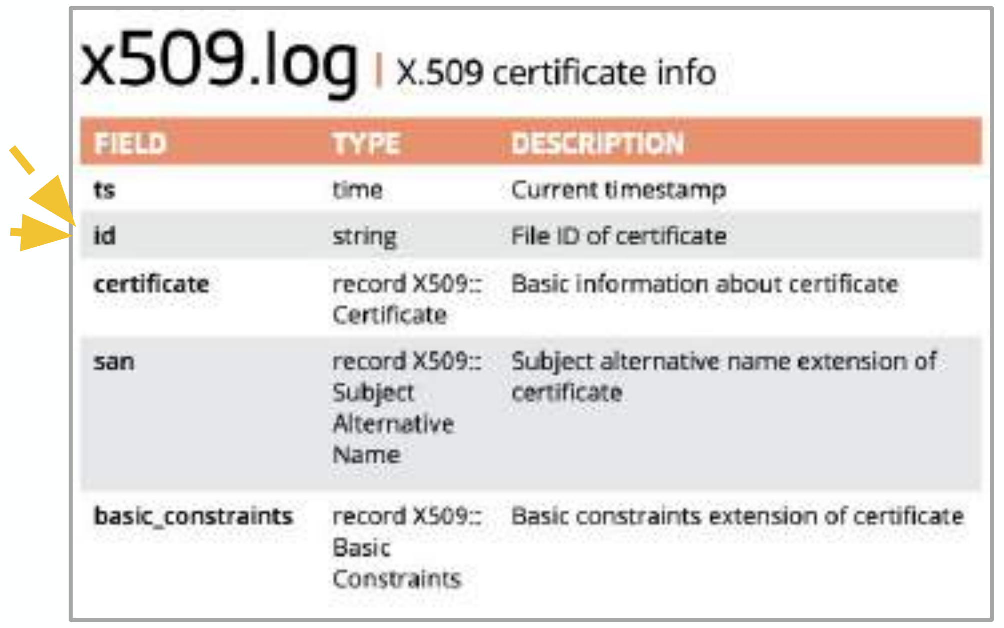
ssl.log | SSL handshakes

FIELD	TYPE	DESCRIPTION
ts	time	Time when SSL connection first detected
uid & id		Underlying connection info > **See conn.log**
version	string	SSL/TLS version server chose
cipher	string	SSL/TLS cipher suite server chose
curve	string	Elliptic curve server chose when using ECDH/ECDHE
server_name	string	Value of Server Name Indicator SSL/TLS extension
resumed	bool	Flag that indicates session was resumed
last_alert	string	Last alert seen during connection
next_protocol	string	Next protocol server chose using application layer next protocol extension, if present
established	bool	Flags if SSL session successfully established
cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by server
client_cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by client
subject	string	Subject of X.509 cert offered by server
issuer	string	Subject of signer of X.509 server cert
client_subject	string	Subject of X.509 cert offered by client
client_issuer	string	Subject of signer of client cert
validation_status	string	Certificate validation result for this connection
ocsp_status	string	OCSP validation result for this connection
valid_ct_logs	count	Number of different logs for which valid SCTs encountered in connection
valid_ct_operators	count	Number of different log operators for which valid SCTs encountered in connection
notary	record Cert Notary:: Response	Response from the ICSI certificate notary



files.log | File analysis results

FIELD	TYPE	DESCRIPTION
ts	time	Time when file first seen
fuid	string	Identifier associated with single file
tx_hosts	table	Host or hosts data sourced from
rx_hosts	table	Host or hosts data traveled to
conn_uids	table	Connection UID(s) over which file transferred
source	string	Identification of file data source
depth	count	Value to represent depth of file in relation to source
analyzers	table	Set of analysis types done during file analysis
mime_type	string	Mime type, as determined by Zeek's signatures
filename	string	Filename, if available from file source
duration	interval	Duration file was analyzed for
local_orig	bool	Indicates if data originated from local network
is_orig	bool	If file sent by connection originator or responder
seen_bytes	count	Number of bytes provided to file analysis engine
total_bytes	count	Total number of bytes that should comprise full file
missing_bytes	count	Number of bytes in file stream missed
overflow_bytes	count	Number of bytes in file stream not delivered to stream file analyzers
timedout	bool	If file analysis timed out at least once
parent_fuid	string	Container file ID was extracted from
md5	string	MD5 digest of file contents
sha1	string	SHA1 digest of file contents
sha256	string	SHA256 digest of file contents
extracted	string	Local filename of extracted file
extracted_cutoff	bool	Set to true if file being extracted was cut off so whole file was not logged
extracted_size	count	Number of bytes extracted to disk
entropy	double	Information density of file contents

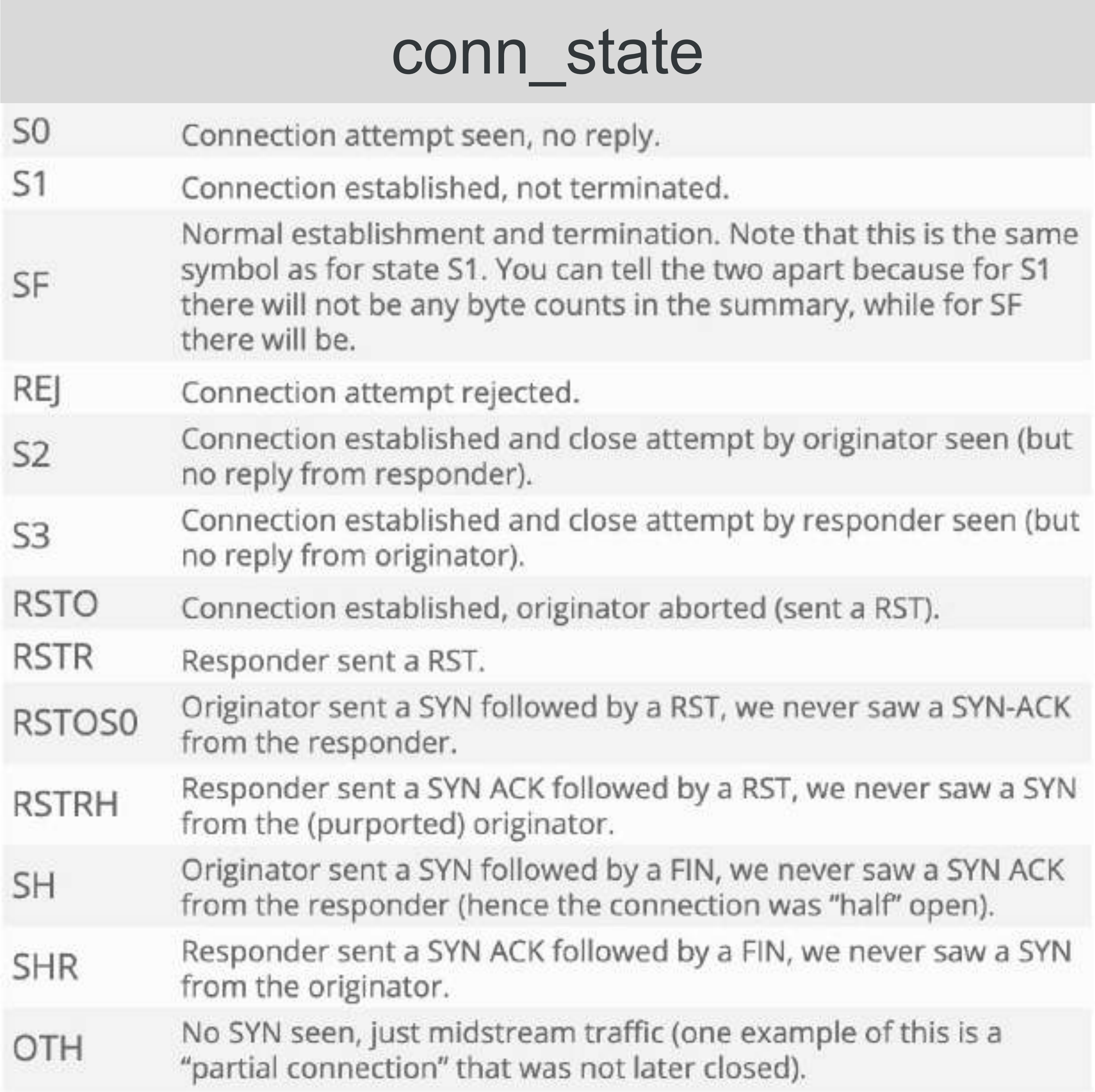


x509.log | X.509 certificate info

FIELD	TYPE	DESCRIPTION
ts	time	Current timestamp
id	string	File ID of certificate
certificate	record X509:: Certificate	Basic information about certificate
san	record X509:: Subject Alternative Name	Subject alternative name extension of certificate
basic_constraints	record X509:: Basic Constraints	Basic constraints extension of certificate

TCP Connection State

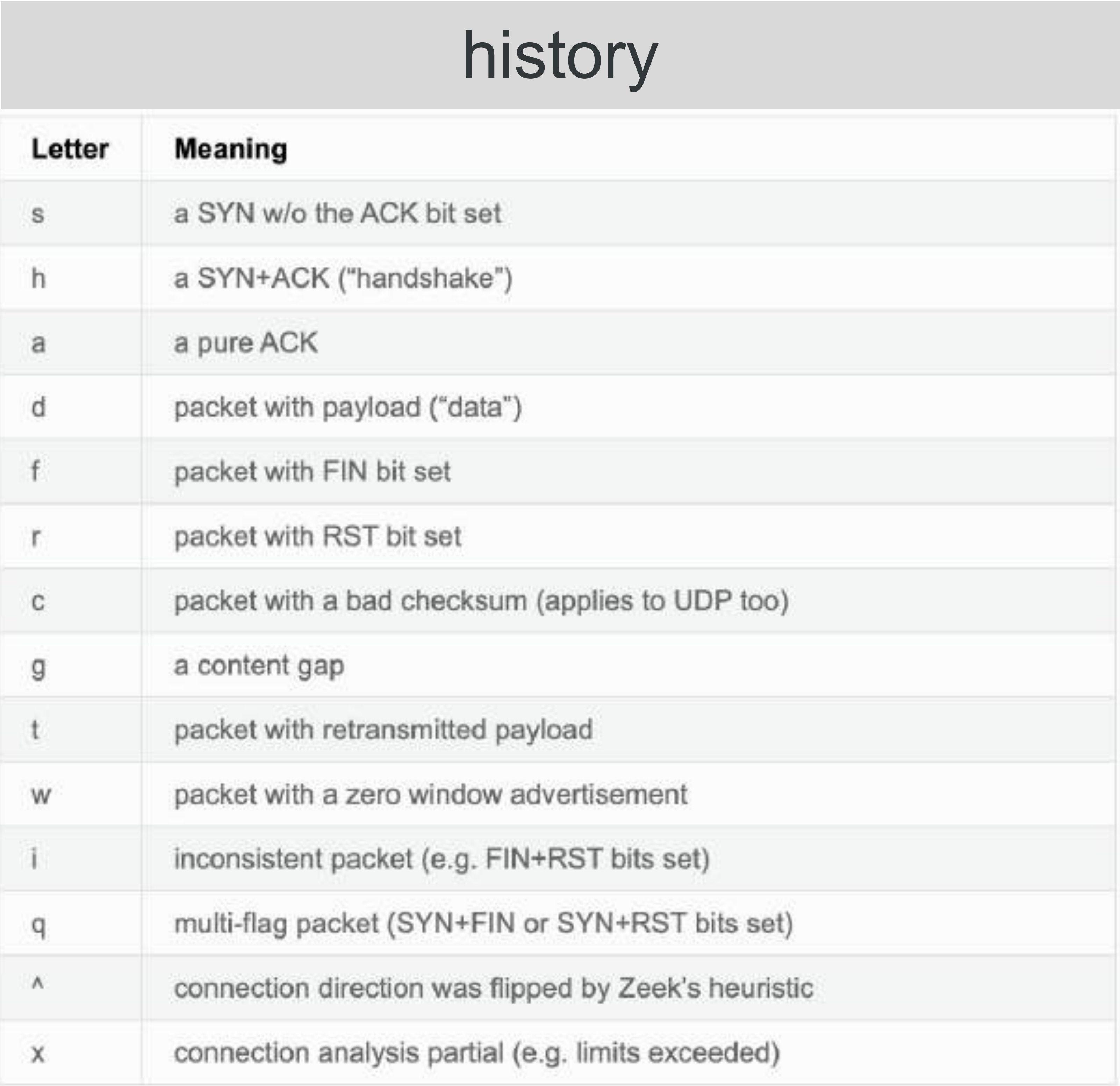
- Zeek Data Analytics
  - TCP Connection State Metadata



conn_state	
S0	Connection attempt seen, no reply.
S1	Connection established, not terminated.
SF	Normal establishment and termination. Note that this is the same symbol as for state S1. You can tell the two apart because for S1 there will not be any byte counts in the summary, while for SF there will be.
REJ	Connection attempt rejected.
S2	Connection established and close attempt by originator seen (but no reply from responder).
S3	Connection established and close attempt by responder seen (but no reply from originator).
RSTO	Connection established, originator aborted (sent a RST).
RSTR	Responder sent a RST.
RSTOS0	Originator sent a SYN followed by a RST, we never saw a SYN-ACK from the responder.
RSTRH	Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.
SH	Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder (hence the connection was "half" open).
SHR	Responder sent a SYN ACK followed by a FIN, we never saw a SYN from the originator.
OTH	No SYN seen, just midstream traffic (one example of this is a "partial connection" that was not later closed).

TCP Connection State

- Zeek Data Analytics
  - Retransmissions (T/t)
    - Uses logarithmic scale



history

Letter	Meaning
s	a SYN w/o the ACK bit set
h	a SYN+ACK ("handshake")
a	a pure ACK
d	packet with payload ("data")
f	packet with FIN bit set
r	packet with RST bit set
c	packet with a bad checksum (applies to UDP too)
g	a content gap
t	packet with retransmitted payload
w	packet with a zero window advertisement
i	inconsistent packet (e.g. FIN+RST bits set)
q	multi-flag packet (SYN+FIN or SYN+RST bits set)
^	connection direction was flipped by Zeek's heuristic
x	connection analysis partial (e.g. limits exceeded)

Examples

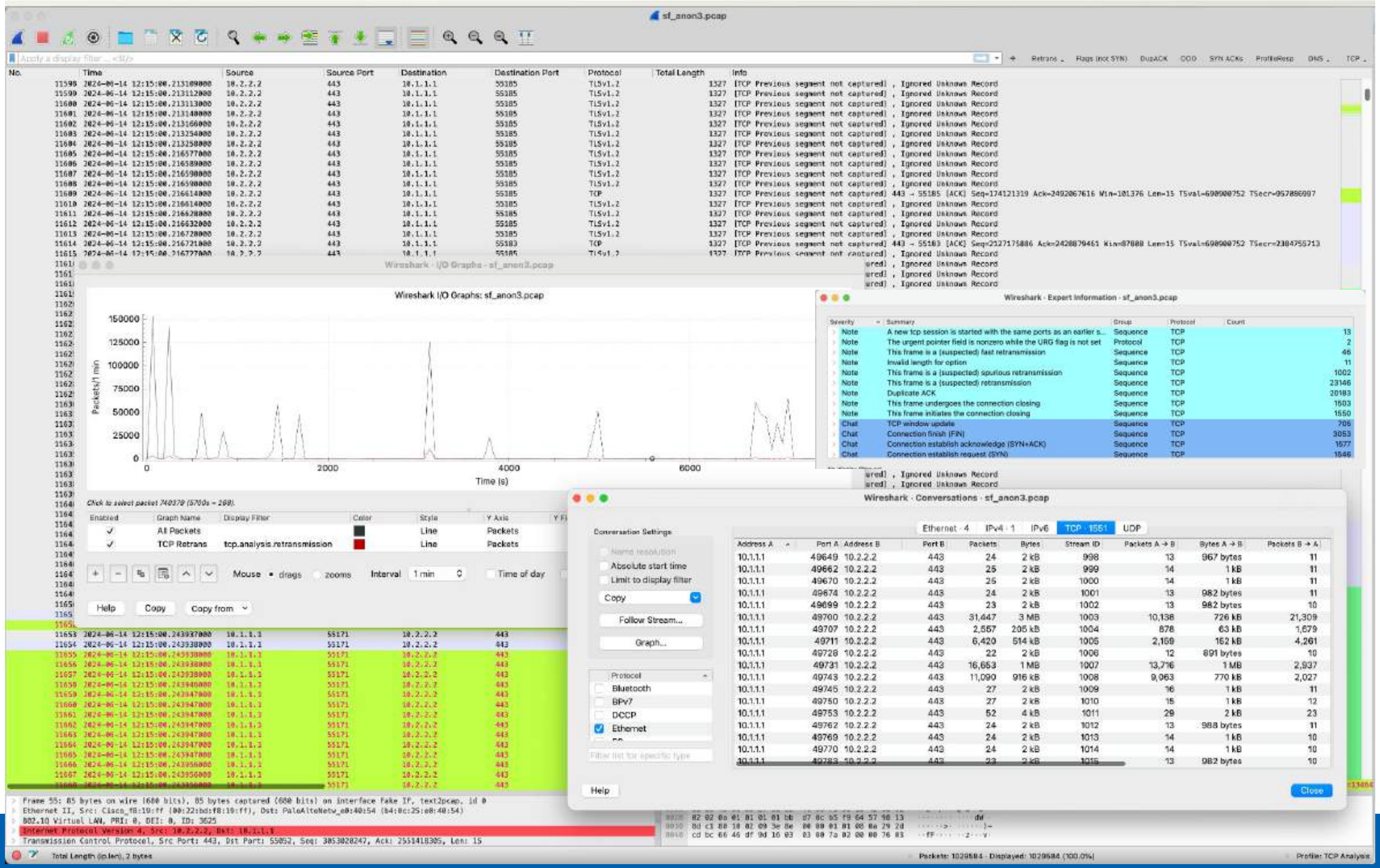
- Testing for 2.5 Hours with Variable WiFi
- SaaS Incident

Demonstration

Testing - Wireshark View

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



```
No.    Time                           Source    Source Port  Destination  Destination Port  Protocol  Total Length  Info
11598  2024-06-14 12:15:00.213109000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11599  2024-06-14 12:15:00.213112000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11600  2024-06-14 12:15:00.213113000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11601  2024-06-14 12:15:00.213140000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11602  2024-06-14 12:15:00.213166000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11603  2024-06-14 12:15:00.213254000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11604  2024-06-14 12:15:00.213258000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11605  2024-06-14 12:15:00.216577000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11606  2024-06-14 12:15:00.216589000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11607  2024-06-14 12:15:00.216590000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11608  2024-06-14 12:15:00.216590000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11609  2024-06-14 12:15:00.216614000  10.2.2.2  443          10.1.1.1     55185             TCP       1327  [TCP Previous segment not captured] 443 → 55185 [ACK] Seq=174121319 Ack=2492067616 Win=101376 Len=15 TSval=690900752 TSecr=957886097
11610  2024-06-14 12:15:00.216614000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11611  2024-06-14 12:15:00.216628000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11612  2024-06-14 12:15:00.216632000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11613  2024-06-14 12:15:00.216720000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
11614  2024-06-14 12:15:00.216721000  10.2.2.2  443          10.1.1.1     55183             TCP       1327  [TCP Previous segment not captured] 443 → 55183 [ACK] Seq=2127175886 Ack=2428879461 Win=87808 Len=15 TSval=690900752 TSecr=2384755713
11615  2024-06-14 12:15:00.216727000  10.2.2.2  443          10.1.1.1     55185             TLSv1.2   1327  [TCP Previous segment not captured] , Ignored Unknown Record
                                                                                                              ured] , Ignored Unknown Record
                                                                                                              ured] , Ignored Unknown Record
                                                                                                              ured] , Ignored Unknown Record
```

Click to select packet 740379 (5700s = 269).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis
✓	All Packets		■	Line	Packets
✓	TCP Retrans	tcp.analysis.retransmission	🟥	Line	Packets

Mouse ● drags ○ zooms Interval 1 min □ Time of day

Help Copy Copy from

Wireshark · Expert Information · sf_anon3.pcap

Severity	Summary	Group	Protocol	Count
Note	A new tcp session is started with the same ports as an earlier s...	Sequence	TCP	13
Note	The urgent pointer field is nonzero while the URG flag is not set	Protocol	TCP	2
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	46
Note	Invalid length for option	Sequence	TCP	11
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1002
Note	This frame is a (suspected) retransmission	Sequence	TCP	23146
Note	Duplicate ACK	Sequence	TCP	20183
Note	This frame undergoes the connection closing	Sequence	TCP	1503
Note	This frame initiates the connection closing	Sequence	TCP	1550
Chat	TCP window update	Sequence	TCP	706
Chat	Connection finish (FIN)	Sequence	TCP	3053
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	1577
Chat	Connection establish request (SYN)	Sequence	TCP	1546

```
                                                                                                              ured] , Ignored Unknown Record
                                                                                                              ured] , Ignored Unknown Record
```

Wireshark · Conversations · sf_anon3.pcap

Conversation Settings
□ Name resolution
□ Absolute start time
□ Limit to display filter
Copy
Follow Stream...
Graph...

Protocol
□ Bluetooth
□ BPv7
□ DCCP
☑ Ethernet

Filter list for specific type

Ethernet · 4 IPv4 · 1 IPv6 **TCP · 1561** UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A
10.1.1.1	49649	10.2.2.2	443	24	2 kB	998	13	967 bytes	11
10.1.1.1	49662	10.2.2.2	443	25	2 kB	999	14	1 kB	11
10.1.1.1	49670	10.2.2.2	443	25	2 kB	1000	14	1 kB	11
10.1.1.1	49674	10.2.2.2	443	24	2 kB	1001	13	982 bytes	11
10.1.1.1	49699	10.2.2.2	443	23	2 kB	1002	13	982 bytes	10
10.1.1.1	49700	10.2.2.2	443	31,447	3 MB	1003	10,138	726 kB	21,309
10.1.1.1	49707	10.2.2.2	443	2,557	205 kB	1004	878	63 kB	1,679
10.1.1.1	49711	10.2.2.2	443	6,420	514 kB	1005	2,159	162 kB	4,261
10.1.1.1	49728	10.2.2.2	443	22	2 kB	1006	12	891 bytes	10
10.1.1.1	49731	10.2.2.2	443	16,653	1 MB	1007	13,716	1 MB	2,937
10.1.1.1	49743	10.2.2.2	443	11,090	916 kB	1008	9,063	770 kB	2,027
10.1.1.1	49745	10.2.2.2	443	27	2 kB	1009	16	1 kB	11
10.1.1.1	49750	10.2.2.2	443	27	2 kB	1010	15	1 kB	12
10.1.1.1	49753	10.2.2.2	443	52	4 kB	1011	29	2 kB	23
10.1.1.1	49762	10.2.2.2	443	24	2 kB	1012	13	988 bytes	11
10.1.1.1	49769	10.2.2.2	443	24	2 kB	1013	14	1 kB	10
10.1.1.1	49770	10.2.2.2	443	24	2 kB	1014	14	1 kB	10
10.1.1.1	49783	10.2.2.2	443	23	2 kB	1015	13	982 bytes	10

Help Close

```
11653  2024-06-14 12:15:00.243937000  10.1.1.1  55171  10.2.2.2  443
11654  2024-06-14 12:15:00.243938000  10.1.1.1  55171  10.2.2.2  443
11655  2024-06-14 12:15:00.243938000  10.1.1.1  55171  10.2.2.2  443
11656  2024-06-14 12:15:00.243938000  10.1.1.1  55171  10.2.2.2  443
11657  2024-06-14 12:15:00.243938000  10.1.1.1  55171  10.2.2.2  443
11658  2024-06-14 12:15:00.243946000  10.1.1.1  55171  10.2.2.2  443
11659  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11660  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11661  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11662  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11663  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11664  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11665  2024-06-14 12:15:00.243947000  10.1.1.1  55171  10.2.2.2  443
11666  2024-06-14 12:15:00.243956000  10.1.1.1  55171  10.2.2.2  443
11667  2024-06-14 12:15:00.243956000  10.1.1.1  55171  10.2.2.2  443

> Frame 55: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Cisco_f8:19:ff (00:22:bd:f8:19:ff), Dst: PaloAltoNetw_e0:40:54 (b4:0c:25:e0:40:54)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3625
> Internet Protocol Version 4, Src: 10.2.2.2, Dst: 10.1.1.1
> Transmission Control Protocol, Src Port: 443, Dst Port: 55052, Seq: 3853028247, Ack: 2551418305, Len: 15

0020  02 02 0a 01 01 01 01 bb  d7 8c b5 f9 64 57 98 13   ············dW··
0030  8d c1 80 10 02 09 3e 8e  00 00 01 01 08 0a 29 2d   ······>·······)-
0040  cd bc 66 46 df 9d 16 03  03 00 7a 02 00 00 76 03   ··fF······z···v·
```

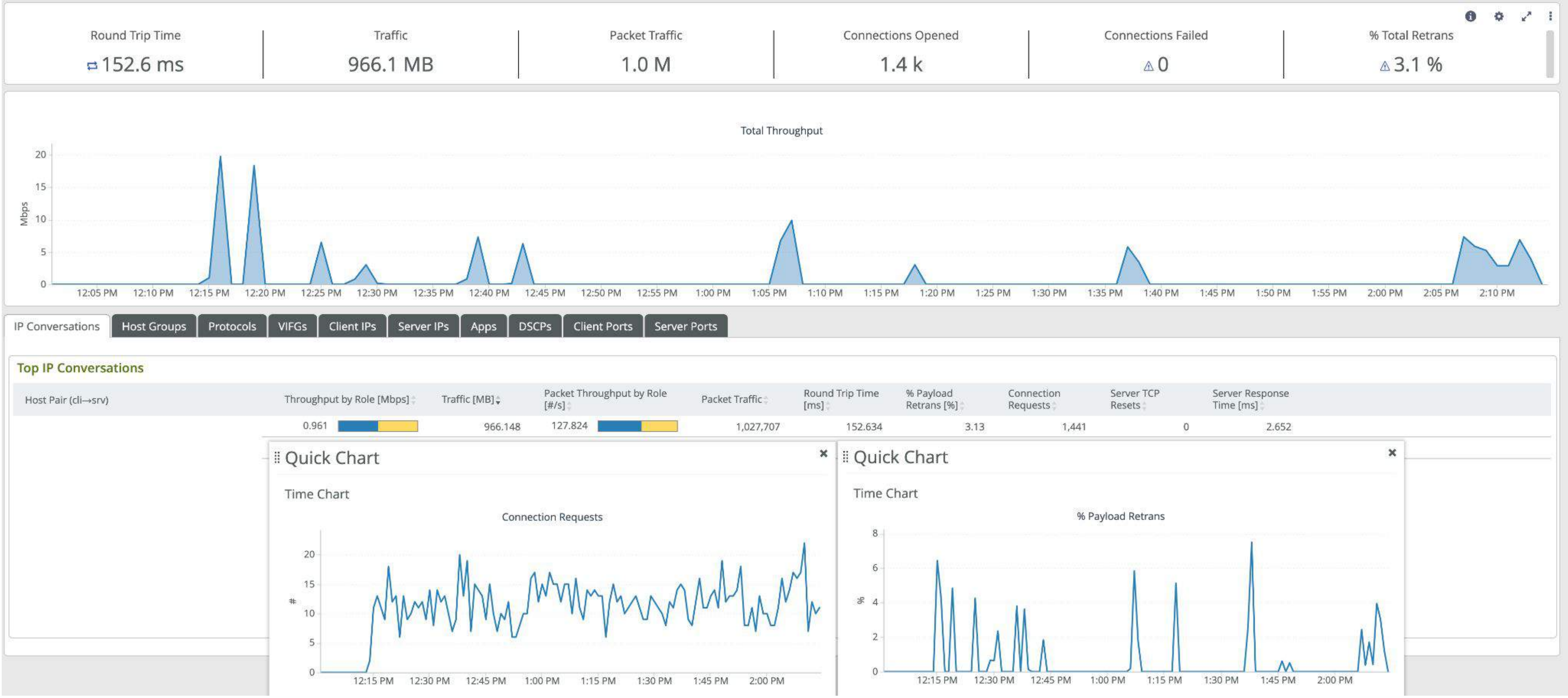
Total Length (ip.len), 2 bytes

Packets: 1029684 · Displayed: 1029684 (100.0%)

Profile: TCP Analysis

Testing - NPM Monitoring

#sf24us



Round Trip Time	Traffic	Packet Traffic	Connections Opened	Connections Failed	% Total Retrans
⇄ 152.6 ms	966.1 MB	1.0 M	1.4 k	⚠ 0	⚠ 3.1 %

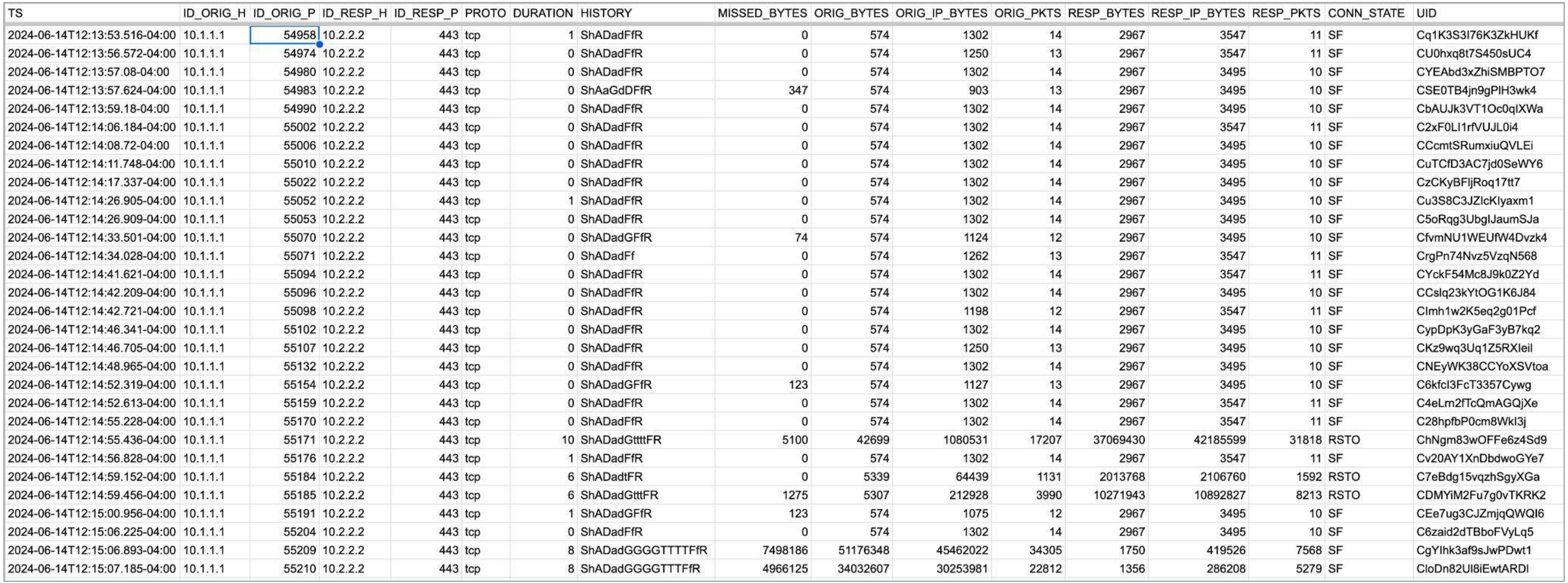
Top IP Conversations

Host Pair (cli→srv)	Throughput by Role [Mbps]	Traffic [MB]	Packet Throughput by Role [#/s]	Packet Traffic	Round Trip Time [ms]	% Payload Retrans [%]	Connection Requests	Server TCP Resets	Server Response Time [ms]
	0.961	966.148	127.824	1,027,707	152.634	3.13	1,441	0	2.652

Testing - Zeek View

SharkFest'24 US
June 15-20 · Fairfax, VA

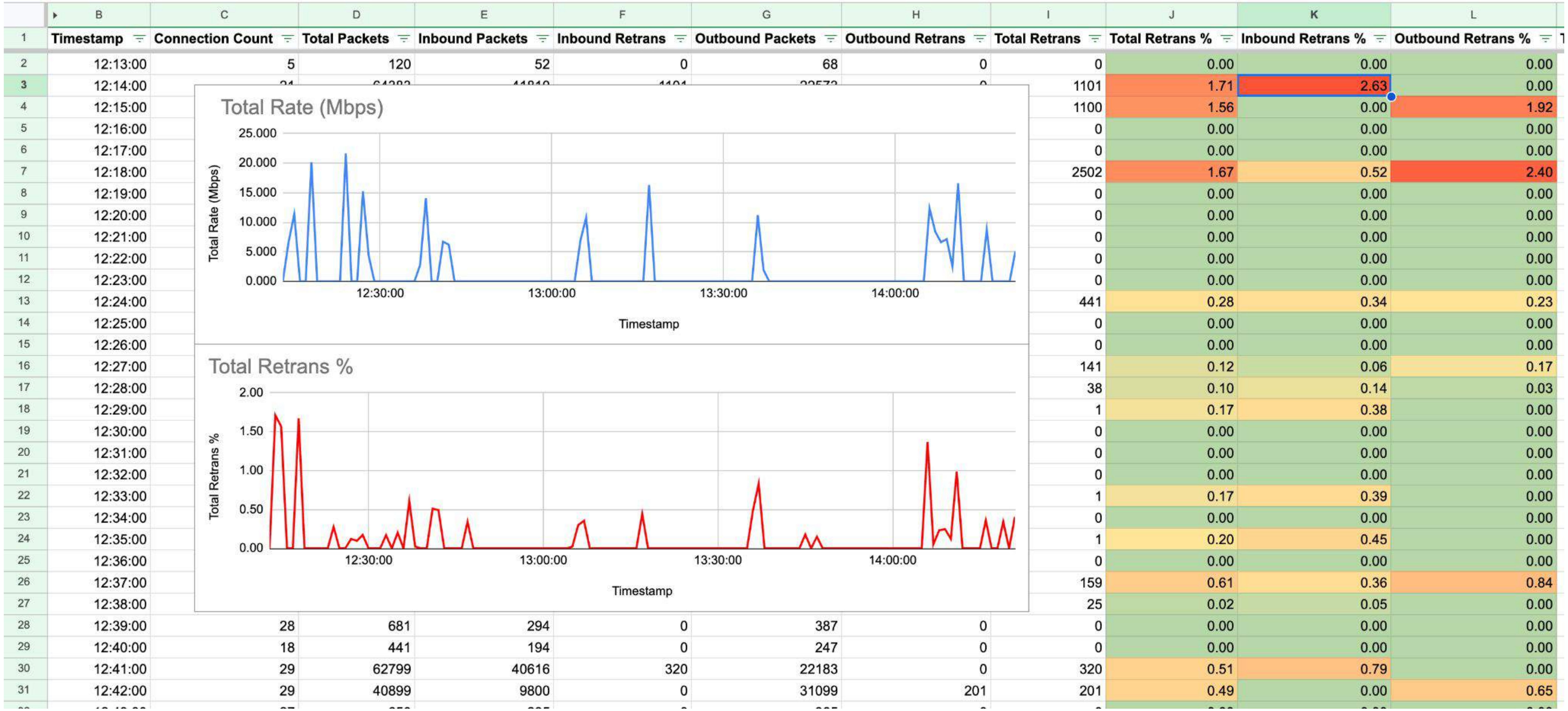
#sf24us



TS	ID_ORIG_H	ID_ORIG_P	ID_RESP_H	ID_RESP_P	PROTO	DURATION	HISTORY	MISSED_BYTES	ORIG_BYTES	ORIG_IP_BYTES	ORIG_PKTS	RESP_BYTES	RESP_IP_BYTES	RESP_PKTS	CONN_STATE	UID
2024-06-14T12:13:53.516-04:00	10.1.1.1	54958	10.2.2.2	443	tcp	1	ShADadFfR	0	574	1302	14	2967	3547	11	SF	Cq1K3S3I76K3ZkHUKf
2024-06-14T12:13:56.572-04:00	10.1.1.1	54974	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1250	13	2967	3547	11	SF	CU0hxq8t7S450sUC4
2024-06-14T12:13:57.08-04:00	10.1.1.1	54980	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CYEAbd3xZhiSMBPTO7
2024-06-14T12:13:57.624-04:00	10.1.1.1	54983	10.2.2.2	443	tcp	0	ShAaGdDFfR	347	574	903	13	2967	3495	10	SF	CSE0TB4jn9gPIH3wk4
2024-06-14T12:13:59.18-04:00	10.1.1.1	54990	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CbAUJk3VT1Oc0qIXWa
2024-06-14T12:14:06.184-04:00	10.1.1.1	55002	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3547	11	SF	C2xF0LI1rfVUJL0i4
2024-06-14T12:14:08.72-04:00	10.1.1.1	55006	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CCcmtSRumxiuQVLEi
2024-06-14T12:14:11.748-04:00	10.1.1.1	55010	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CuTCfD3AC7jd0SeWY6
2024-06-14T12:14:17.337-04:00	10.1.1.1	55022	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CzCKyBFljRoq17tt7
2024-06-14T12:14:26.905-04:00	10.1.1.1	55052	10.2.2.2	443	tcp	1	ShADadFfR	0	574	1302	14	2967	3495	10	SF	Cu3S8C3JZlcKlyaxm1
2024-06-14T12:14:26.909-04:00	10.1.1.1	55053	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	C5oRqg3UbglJaumSJa
2024-06-14T12:14:33.501-04:00	10.1.1.1	55070	10.2.2.2	443	tcp	0	ShADadGFfR	74	574	1124	12	2967	3495	10	SF	CfvmNU1WEUfW4Dvzk4
2024-06-14T12:14:34.028-04:00	10.1.1.1	55071	10.2.2.2	443	tcp	0	ShADadFf	0	574	1262	13	2967	3547	11	SF	CrgPn74Nvz5VzqN568
2024-06-14T12:14:41.621-04:00	10.1.1.1	55094	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3547	11	SF	CYckF54Mc8J9k0Z2Yd
2024-06-14T12:14:42.209-04:00	10.1.1.1	55096	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CCslq23kYtOG1K6J84
2024-06-14T12:14:42.721-04:00	10.1.1.1	55098	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1198	12	2967	3547	11	SF	CImh1w2K5eq2g01Pcf
2024-06-14T12:14:46.341-04:00	10.1.1.1	55102	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CypDpK3yGaF3yB7kq2
2024-06-14T12:14:46.705-04:00	10.1.1.1	55107	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1250	13	2967	3495	10	SF	CKz9wq3Uq1Z5RXIeil
2024-06-14T12:14:48.965-04:00	10.1.1.1	55132	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	CNEyWK38CCYoXSVtoa
2024-06-14T12:14:52.319-04:00	10.1.1.1	55154	10.2.2.2	443	tcp	0	ShADadGFfR	123	574	1127	13	2967	3495	10	SF	C6kfcl3FcT3357Cywg
2024-06-14T12:14:52.613-04:00	10.1.1.1	55159	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3547	11	SF	C4eLm2fTcQmAGQjXe
2024-06-14T12:14:55.228-04:00	10.1.1.1	55170	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3547	11	SF	C28hpfbP0cm8Wkl3j
2024-06-14T12:14:55.436-04:00	10.1.1.1	55171	10.2.2.2	443	tcp	10	ShADadGttttFR	5100	42699	1080531	17207	37069430	42185599	31818	RSTO	ChNgm83wOFFe6z4Sd9
2024-06-14T12:14:56.828-04:00	10.1.1.1	55176	10.2.2.2	443	tcp	1	ShADadFfR	0	574	1302	14	2967	3547	11	SF	Cv20AY1XnDbdwoGYe7
2024-06-14T12:14:59.152-04:00	10.1.1.1	55184	10.2.2.2	443	tcp	6	ShADadtFR	0	5339	64439	1131	2013768	2106760	1592	RSTO	C7eBdg15vqzhSgyXGa
2024-06-14T12:14:59.456-04:00	10.1.1.1	55185	10.2.2.2	443	tcp	6	ShADadGtttFR	1275	5307	212928	3990	10271943	10892827	8213	RSTO	CDMYiM2Fu7g0vTKRK2
2024-06-14T12:15:00.956-04:00	10.1.1.1	55191	10.2.2.2	443	tcp	1	ShADadGFfR	123	574	1075	12	2967	3495	10	SF	CEe7ug3CJZmjqQWQI6
2024-06-14T12:15:06.225-04:00	10.1.1.1	55204	10.2.2.2	443	tcp	0	ShADadFfR	0	574	1302	14	2967	3495	10	SF	C6zaid2dTBboFVyLq5
2024-06-14T12:15:06.893-04:00	10.1.1.1	55209	10.2.2.2	443	tcp	8	ShADadGGGGTTTTFfR	7498186	51176348	45462022	34305	1750	419526	7568	SF	CgYIhk3af9sJwPDwt1
2024-06-14T12:15:07.185-04:00	10.1.1.1	55210	10.2.2.2	443	tcp	8	ShADadGGGGTTTFfR	4966125	34032607	30253981	22812	1356	286208	5279	SF	CloDn82Ul8iEwtARDl

Testing - Zeek View

#sf24us



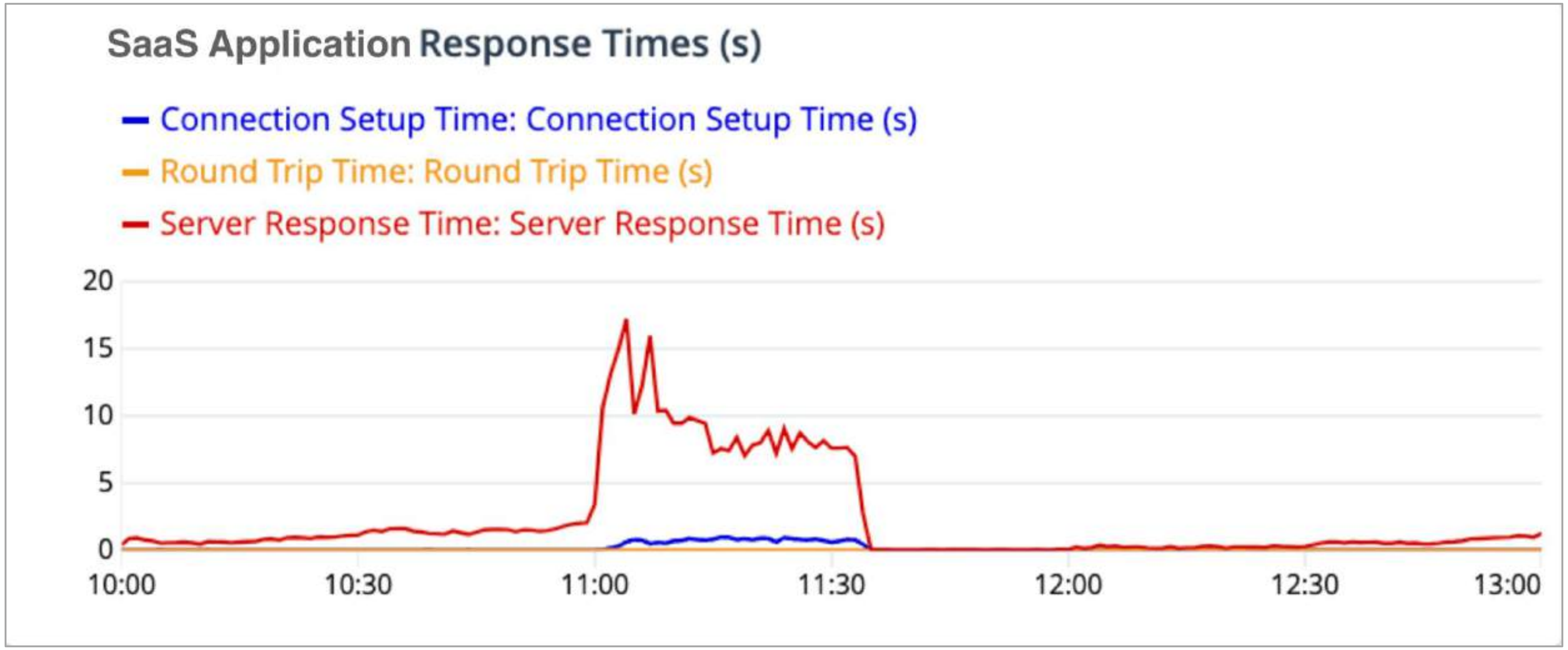
	B	C	D	E	F	G	H	I	J	K	L
1	Timestamp	Connection Count	Total Packets	Inbound Packets	Inbound Retrans	Outbound Packets	Outbound Retrans	Total Retrans	Total Retrans %	Inbound Retrans %	Outbound Retrans %
2	12:13:00	5	120	52	0	68	0	0	0.00	0.00	0.00
3	12:14:00	21	64383	41810	1101	22573	0	1101	1.71	2.63	0.00
4	12:15:00							1100	1.56	0.00	1.92
5	12:16:00							0	0.00	0.00	0.00
6	12:17:00							0	0.00	0.00	0.00
7	12:18:00							2502	1.67	0.52	2.40
8	12:19:00							0	0.00	0.00	0.00
9	12:20:00							0	0.00	0.00	0.00
10	12:21:00							0	0.00	0.00	0.00
11	12:22:00							0	0.00	0.00	0.00
12	12:23:00							0	0.00	0.00	0.00
13	12:24:00							441	0.28	0.34	0.23
14	12:25:00							0	0.00	0.00	0.00
15	12:26:00							0	0.00	0.00	0.00
16	12:27:00							141	0.12	0.06	0.17
17	12:28:00							38	0.10	0.14	0.03
18	12:29:00							1	0.17	0.38	0.00
19	12:30:00							0	0.00	0.00	0.00
20	12:31:00							0	0.00	0.00	0.00
21	12:32:00							0	0.00	0.00	0.00
22	12:33:00							1	0.17	0.39	0.00
23	12:34:00							0	0.00	0.00	0.00
24	12:35:00							1	0.20	0.45	0.00
25	12:36:00							0	0.00	0.00	0.00
26	12:37:00							159	0.61	0.36	0.84
27	12:38:00							25	0.02	0.05	0.00
28	12:39:00	28	681	294	0	387	0	0	0.00	0.00	0.00
29	12:40:00	18	441	194	0	247	0	0	0.00	0.00	0.00
30	12:41:00	29	62799	40616	320	22183	0	320	0.51	0.79	0.00
31	12:42:00	29	40899	9800	0	31099	201	201	0.49	0.00	0.65

SaaS Incident

SharkFest'24 US
June 15-20 · Fairfax, VA

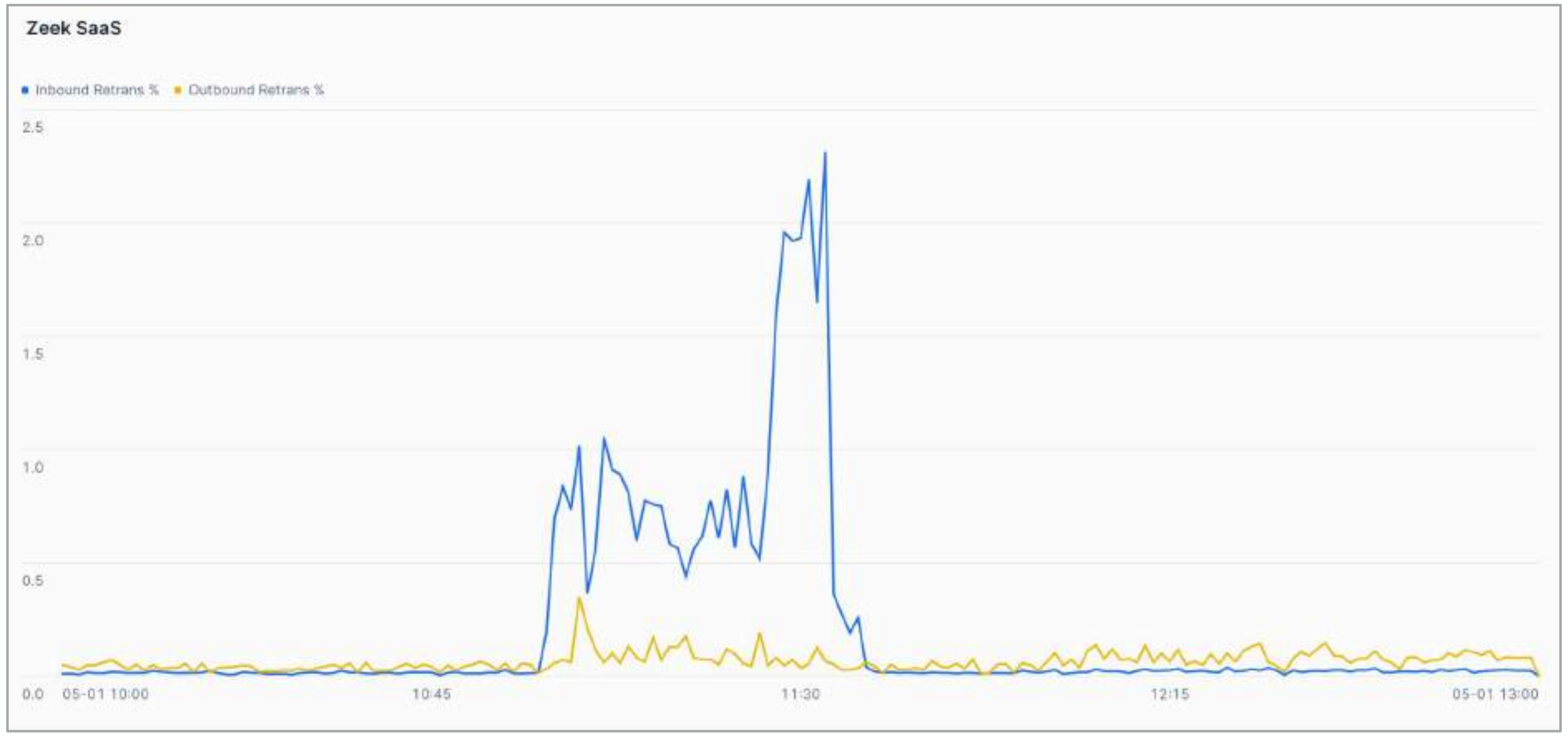
#sf24us

- Network Performance Monitoring
  - Alerted on Response Times



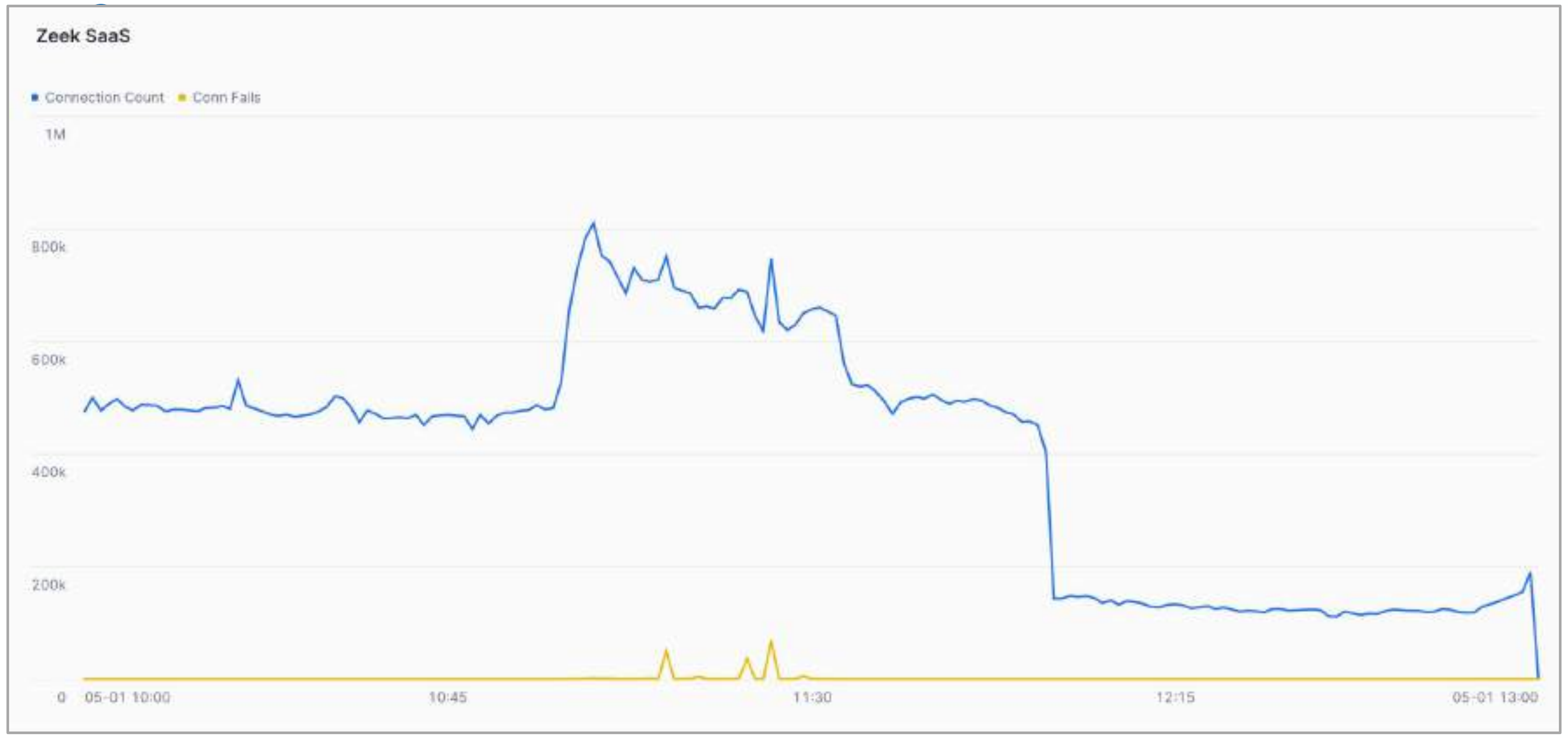
SaaS Incident

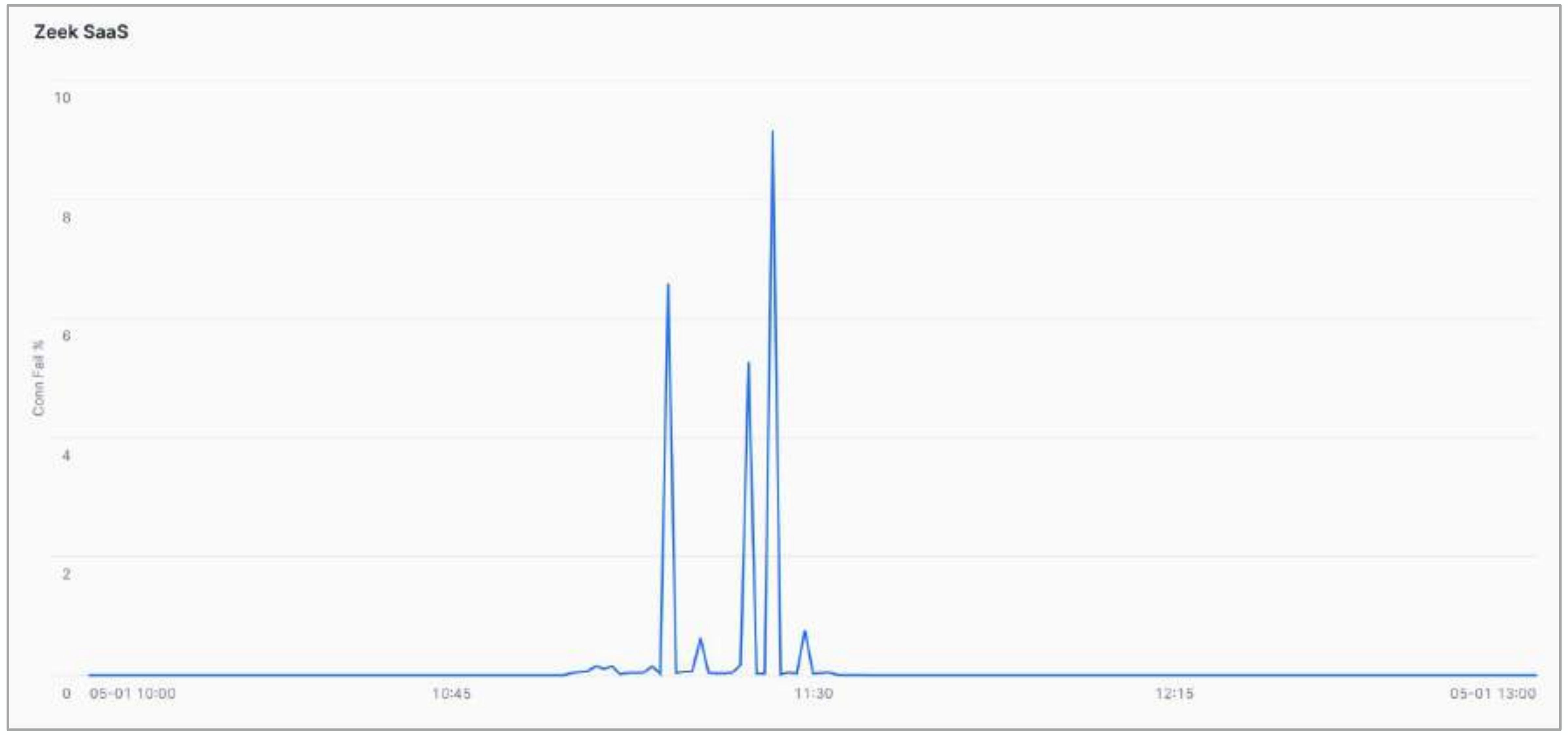
- Zeek Data Analytics
    - No Response Times
    - Caught Retransmissions (another symptom)



Internal Service Degradation

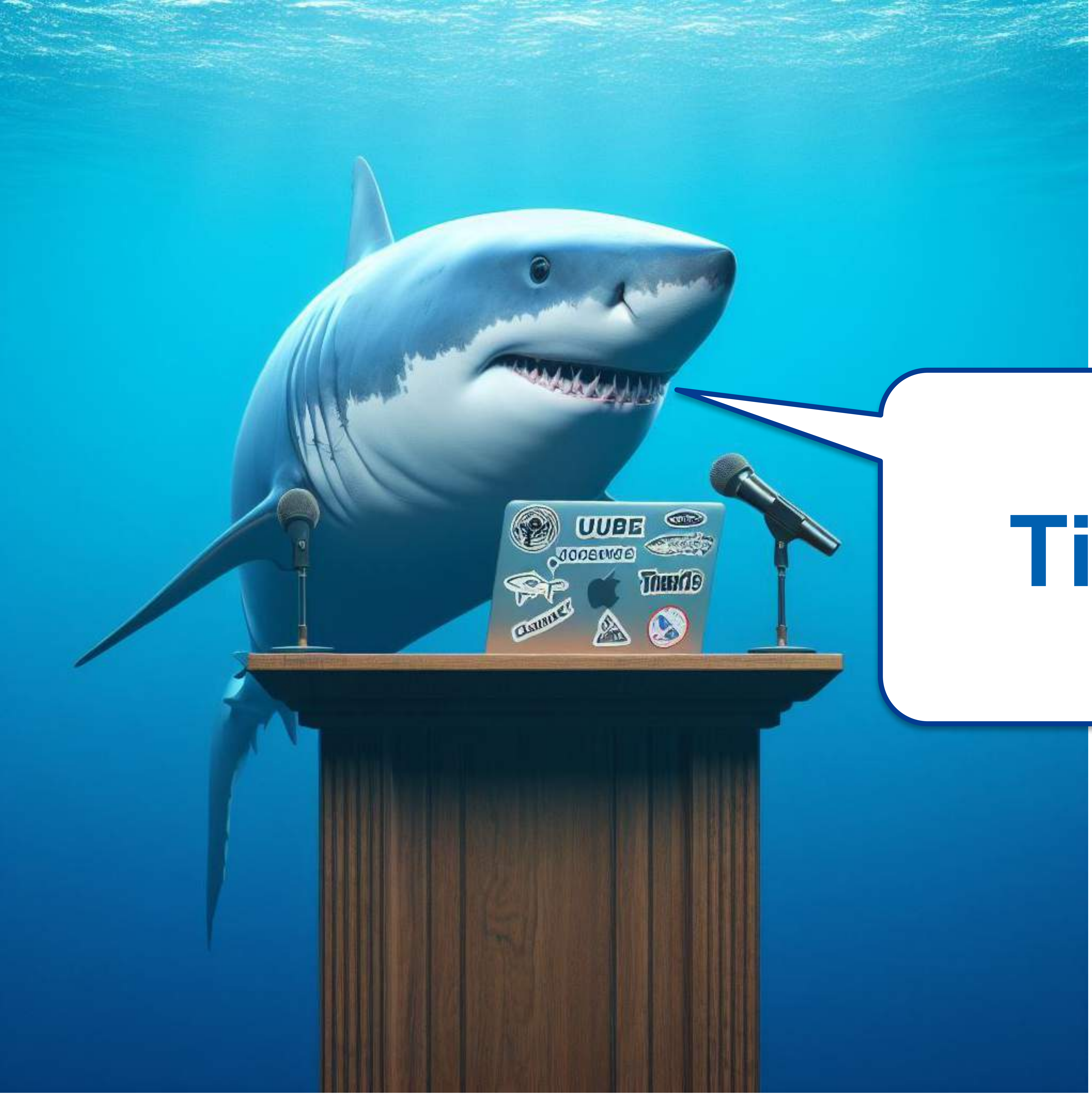
- Zeek Data Analytics
  - Connection Rate Spike
  - Connection Failures





Takeaways

- Cyber tooling can be used for network monitoring in lieu of dedicated NPM tools
  - Leverage focus on Cyber Security
  - Open Source options
- Network Troubleshooting
  - Leverage extensive metadata



SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Time for Q & A