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

#sf24us

Three-dimensional display filters with MATE

Chuck Craft

Core Developers

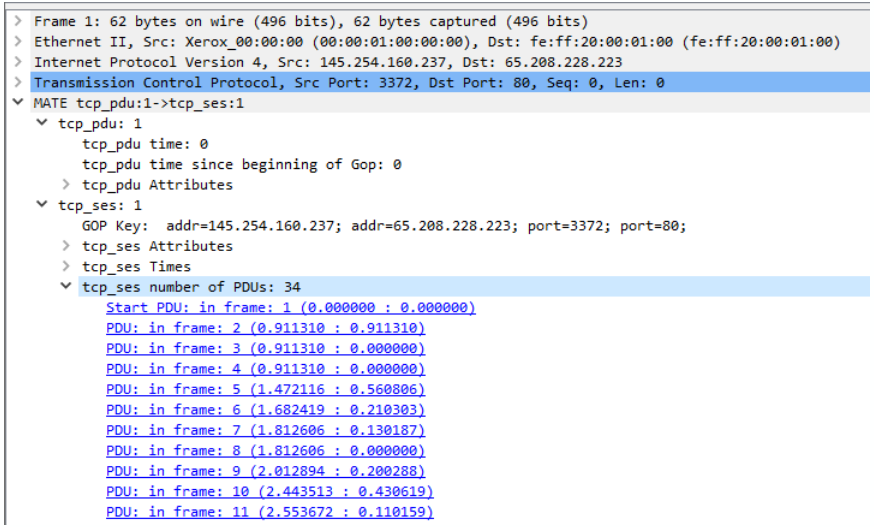
12.2. Getting Started (WSUG)

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

https://www.wireshark.org/docs/wsug_html/#ChMateGettingStarted

These are the steps to try out MATE:

- Run Wireshark and check if the plugin is installed (MATE should appear in Help→About Wireshark:Plugins)
- Get a configuration file e.g., `tcp.mate` (see Mate/Examples for more) and place it somewhere on your harddisk.
- Go to Edit→Preferences…→Protocols→MATE and set the Configuration Filename to the file you want to use and restart Wireshark.
- Load a corresponding capture file (e.g., `http.cap`) and see if MATE has added some new display filter fields, something like: `MATE tcp_pdu:1→tcp_ses:1`
- or, at prompt: `path_to/wireshark -o "mate.config: tcp.mate" -r http.cap`



Spring cleaning (Welcome to 2024)

#sf24us

```
15f90c2dcd MATE: stop config on unknown Proto/Transport/field
12ccb05cf8 MATE: dbg_print - frame line break; print name:id of matching GOG
9ec125e617 MATE (WSUG): update Overview chapter; booleans are now words
71f0456103 MATE (WSUG): update tcp.mate example; code examples formatting
11157e6f74 MATE: new AVPL first added left at end of list
aa0911e709 MATE: Switch times from floats to doubles
bdc66cff21 MATE (WSUG): add images to List of Figures
e179984f0a MATE (WSUG): consistent acronyms; ToC formatting
28e9035eec MATE: Update examples
4ec5c7f78f MATE: Handle fields that are in different data sources
```

OSI Model

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

https://en.wikipedia.org/wiki/OSI_model

Layer			Protocol data unit (PDU)	Function
Host Layers	7	Application	Data	High-level protocols such as for resource sharing or remote file access, e.g. HTTP.
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media Layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Transmission of data frames between two nodes connected by a physical layer
	1	Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

Protocol Data Units (PDUs)

#sf24us

Internet Protocol (IP) PDU

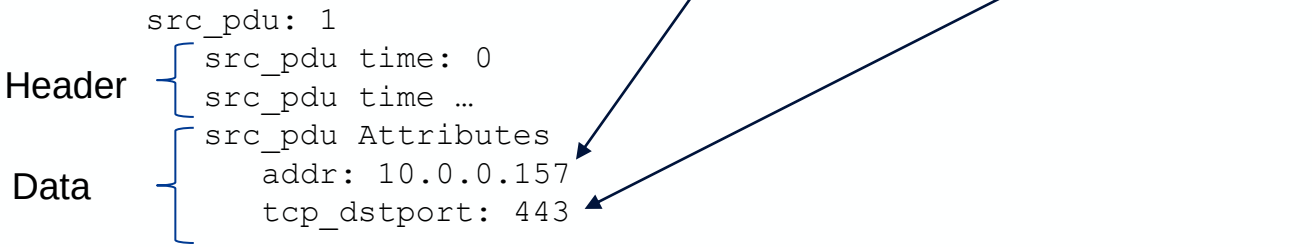
```
Internet Protocol Version 4, Src: 10.0.0.157, Dst: 34.110.207.168
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x4a9d (19101)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.0.157
    Destination Address: 34.110.207.168
    [Stream index: 0]
Data (32 bytes)
```

MATE PDU

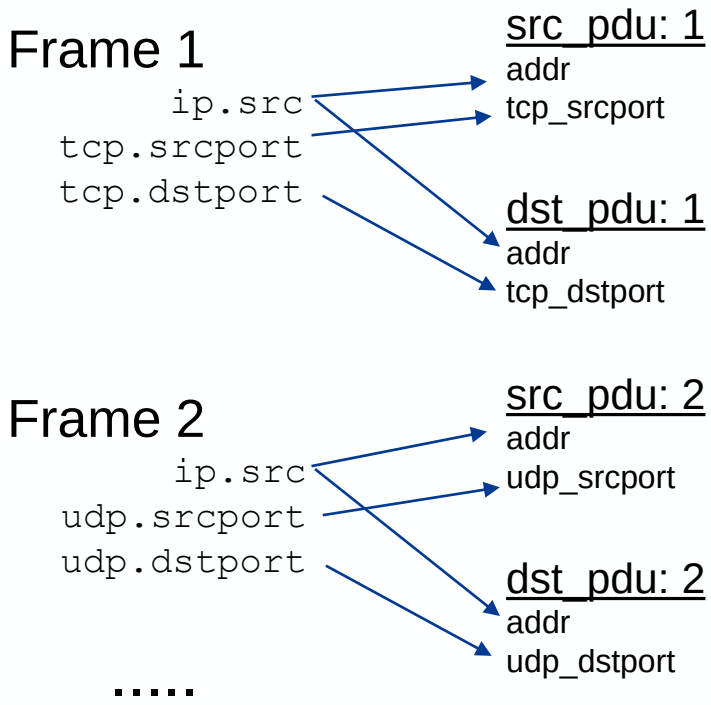
```
src_pdu: 1
  Header
    src_pdu time: 0
    src_pdu time since beginning of Gop: 0
  Data
    src_pdu Attributes
       addr: 10.0.0.157
       tcp_srcport: 14986
```

A little of this, a little of that

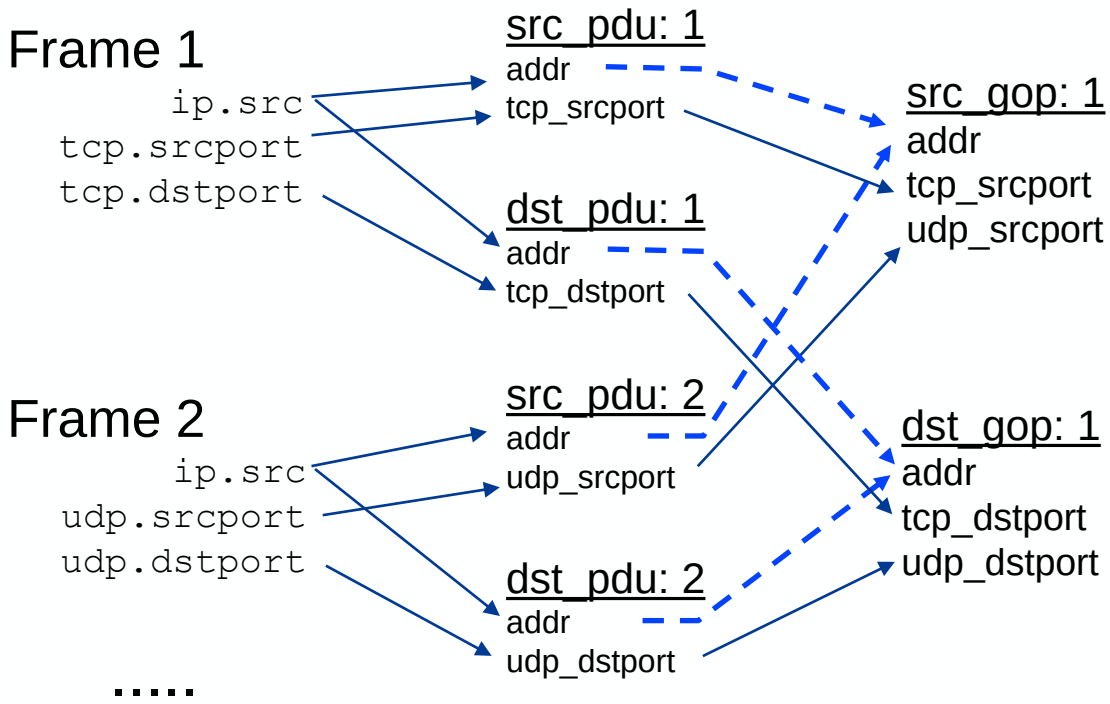

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: d8:bb:c1:56:61:63, Dst: b8:5e:71:f5:e5:87
Internet Protocol Version 4, Src: 10.0.0.157, Dst: 34.110.207.168
Transmission Control Protocol, Src Port: 14986, Dst Port: 443,
```



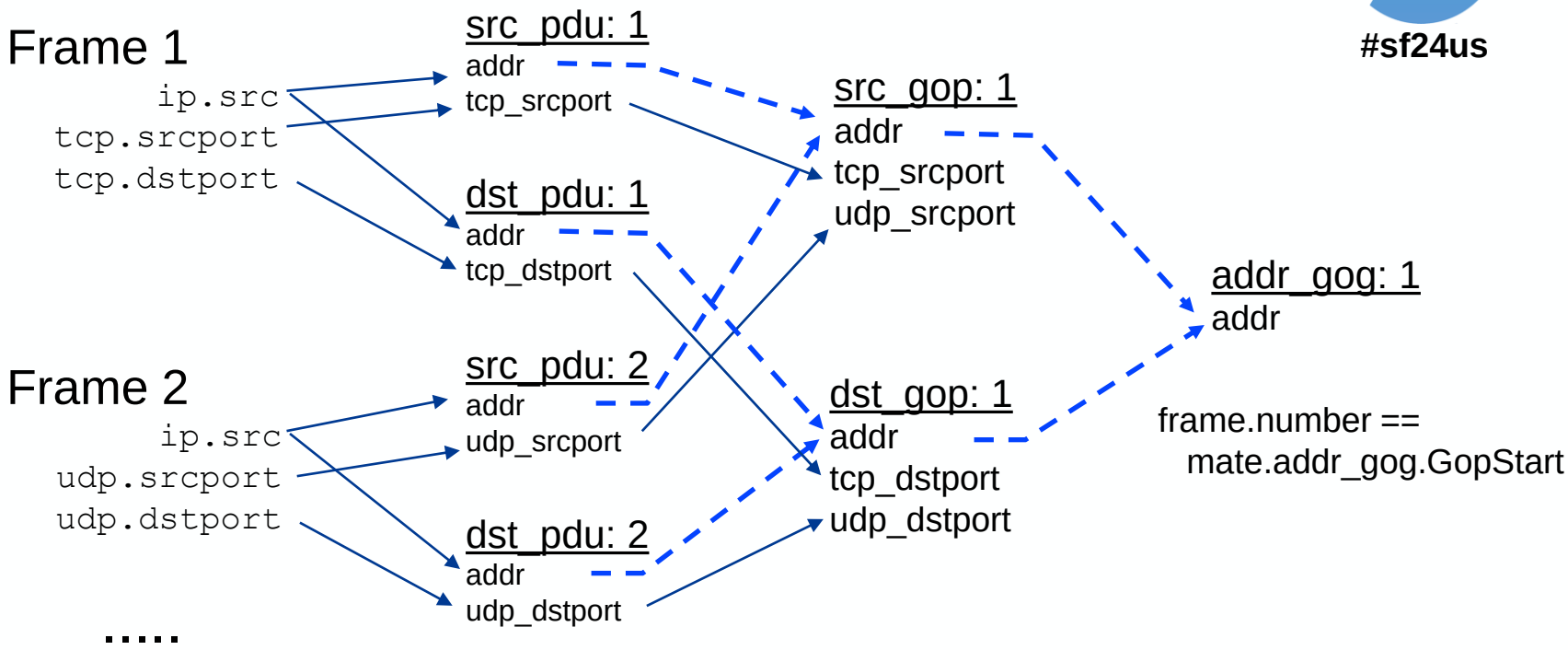
Frames → PDUs



PDUs → GOPs (Group of PDUs)



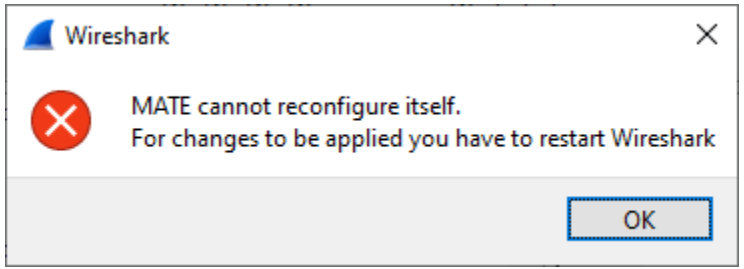
GOPs → GOG (Group of Groups)



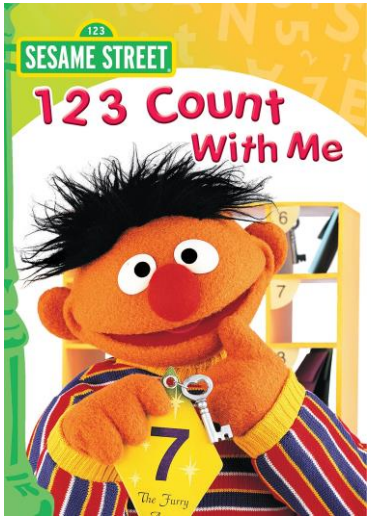
Caveat emptor (Sushi)

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

1. MATE is a plugin. Is the dll loaded?
2. Everything is a string
3. No identical AVPs in a AVPL
3. Time stored as float - precision limited (now doubles !15887)
4. AVP debugging requires a recompile
5. TCP reassembly may cause issues
6. Where to store config files?
7. Restart after config change
8. Check open issues / latest release
9. Post-dissector – run order (epan/epan.c - wslua_init(cb, client_data);)



Counting



frame.time

https://discord.com/channels/889214182837321788/1106444144307613739/1227690365688086588

"Hey Everyone! I'm trying to find the origin of a network loop in a log file and I would like to filter the displayed records so that it only shows the ones that keep repeating. I would like the Time, Header Checksum and Identification columns shown with the values continously matching where the Time column's exact same value repeats at least 10 times."

Frames → PDUs → GOPs

Frame 1
`frame.time=0.000000`

frame_pdu: 1
frame_time

frame_gop: 1
frame_time
`frame_gop number of PDUs: 1`

Frame 2
`frame.time=0.000458`

frame_pdu: 2
frame_time

frame_gop: 2
frame_time
`frame_gop number of PDUs: 1`

Frame 3
`frame.time=0.027285`

frame_pdu: 3
frame_time

frame_gop: 3
frame_time
`frame_gop number of PDUs: 2`

Frame 4
`frame.time=0.027285`

frame_pdu: 4
frame_time

`mate.frame_gop.NumOfPdus > 1`

frame_time.mate


```
Pdu frame_pdu Proto frame Transport mate {
    Extract frame_time From frame.time;
};

Gop frame_gop On frame_pdu Match (frame_time) {
    Start (frame_time);
    Stop (frame_time="FOO");
};

Done;
```

Gitlab issue #18827


```
frame_gop: 8
    GOP Key:  frame_time=Jun 10, 2024 16:35:19.986071000
Central Daylight Time;
    frame_gop Attributes
    frame_gop Times
    frame_gop number of PDUs: 5
        Start PDU: in frame: 9 (0.000000 : 0.000000)
        PDU: in frame: 10 (0.000000 : 0.000000)
        PDU: in frame: 11 (0.000000 : 0.000000)
        PDU: in frame: 12 (0.000000 : 0.000000)
        PDU: in frame: 13 (0.000000 : 0.000000)
```

mate.frame_gop.Pdu

Ability to filter on occurrences of a field
https://gitlab.com/wireshark/wireshark/-/issues/18827

lua detour (GOP Start/last)


```
...
MATE frame_pdu:9->frame_gop:8->frame_gog:8
MATE extra_pdu:9->extra_gop:8->frame_gog:8
Important EASYPOST Protocol
    EASYPOST gopstart: 9
    EASYPOST gopend: 13
```

```
(mate.frame_gop.NumOfPdus > 1) and
   frame.number==easypost.gopstart
```

```
pf = { gopstart = ProtoField.int32("easypost.gopstart", "EASYPOST gopstart"),
       gopend = ProtoField.int32("easypost.gopend", "EASYPOST gopend") }

easypost_payload_f = Field.new("mate.frame_gop.Pdu")

finfo = { easypost_payload_f() }
subtree:add(pf.gopstart, finfo[1].value)
subtree:add(pf.gopend, finfo[#finfo].value)
```

frame_time_rollup.mate


```
<snip> *** See frame_time.mate ***


Pdu extra_pdu Proto frame Transport mate {
    Extract frame_time From frame.time;
};

Gop extra_gop On extra_pdu Match (frame_time) {
    Start (frame_time);
    Stop (frame_time="FOO");
};

Gog frame_gog {
    Member frame_gop(frame_time);
    Member extra_gop(frame_time);
};

Done;
```

```
(mate.frame_gop.NumOfPdus > 1) &&
 (frame.number == mate.frame_gog.GopStart)
```

frame.md5_hash

#sf24us

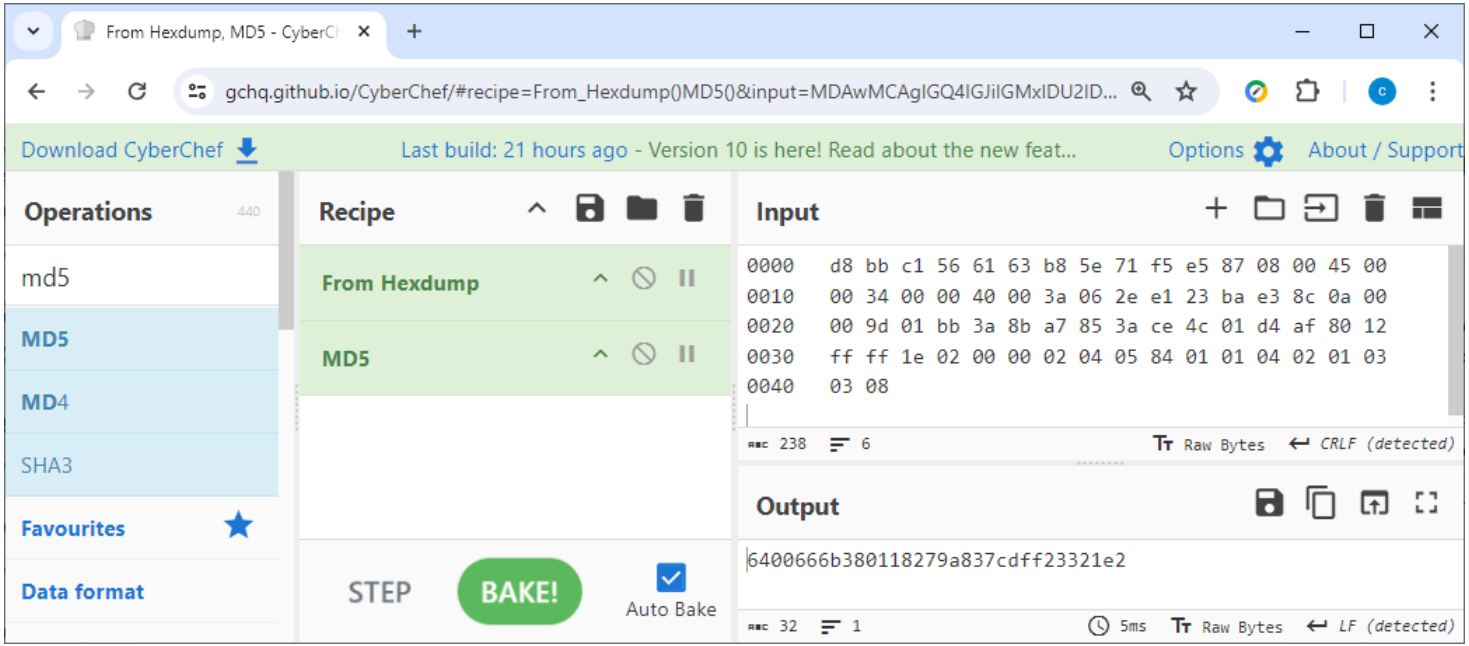
```
Preference:
frame.generate_md5_hash     "Generate an MD5 hash of each frame"

"Whether or not MD5 hashes should be generated for each frame,
useful for finding duplicate frames."(bd9ac163)
```

```
Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
on ...
    Section number: 1
...
    Frame Number: 3
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame MD5 Hash: 6400666b380118279a837cdff23321e2]
...
```

CyberChef detour

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

https://gchq.github.io/CyberChef/

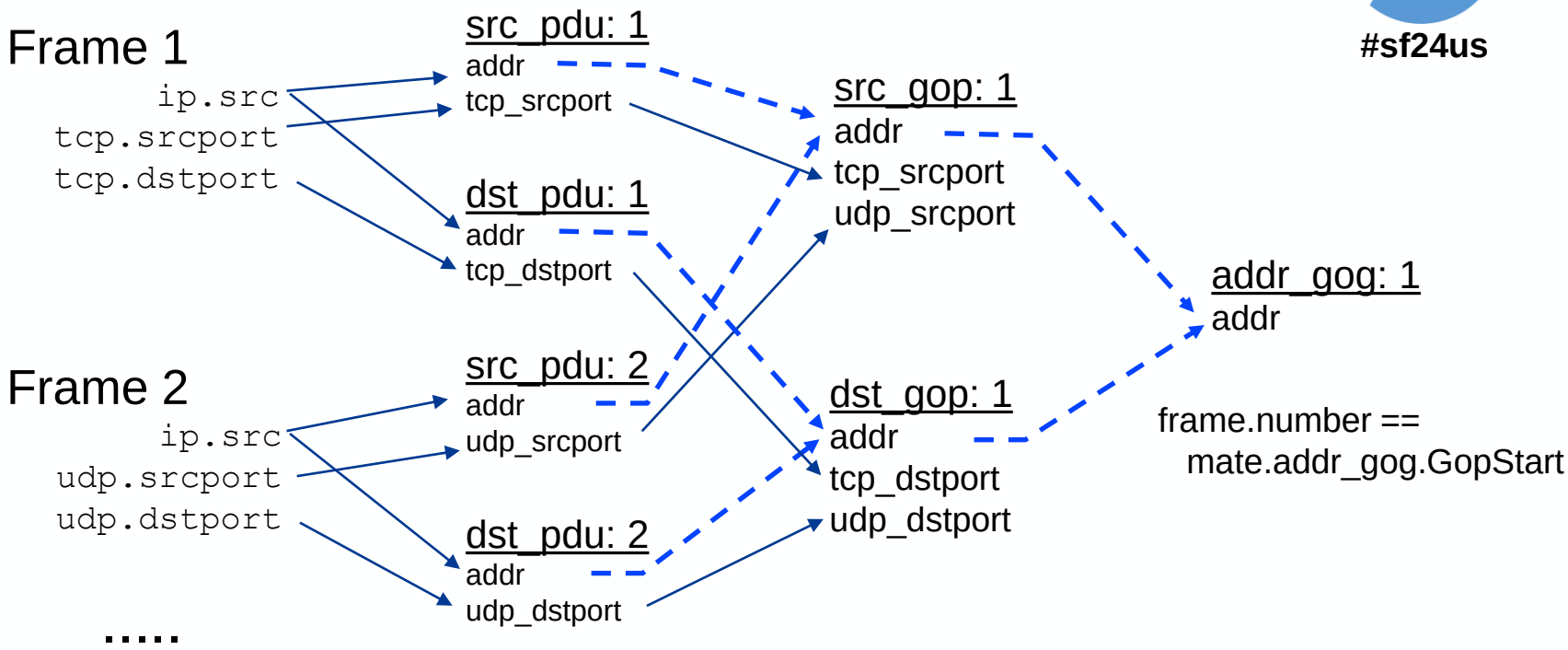


frame_md5_hash.mate

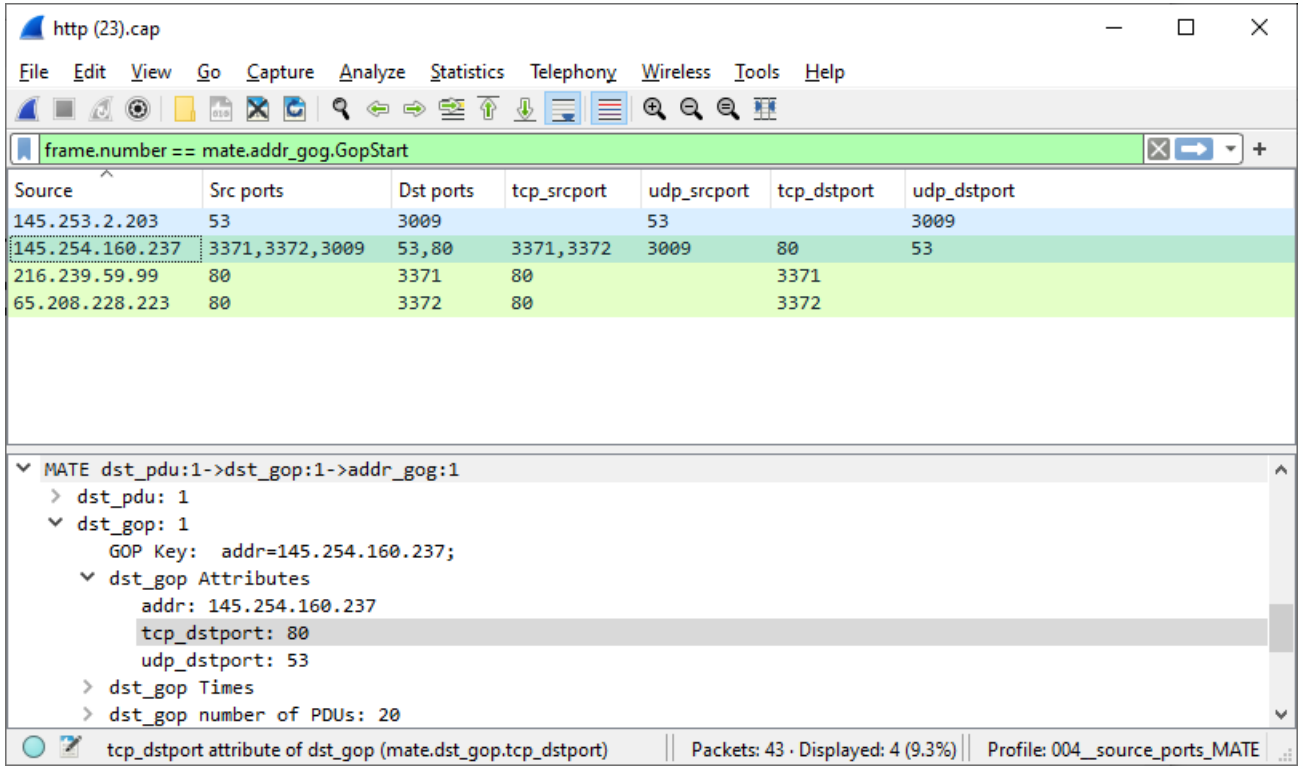

```
Pdu frame_pdu Proto frame Transport mate {
    Extract frame_hash From frame.md5_hash;
};

Gop frame_gop On frame_pdu Match (frame_hash) {
    Start (frame_hash);
    Stop (frame_hash="FOO");
};

Done;
```

```
(mate.frame_gop.NumOfPdus > 100) &&
      (frame.number == easypost.gopstart)
```

Ports per source (address)



Ports per source (address)



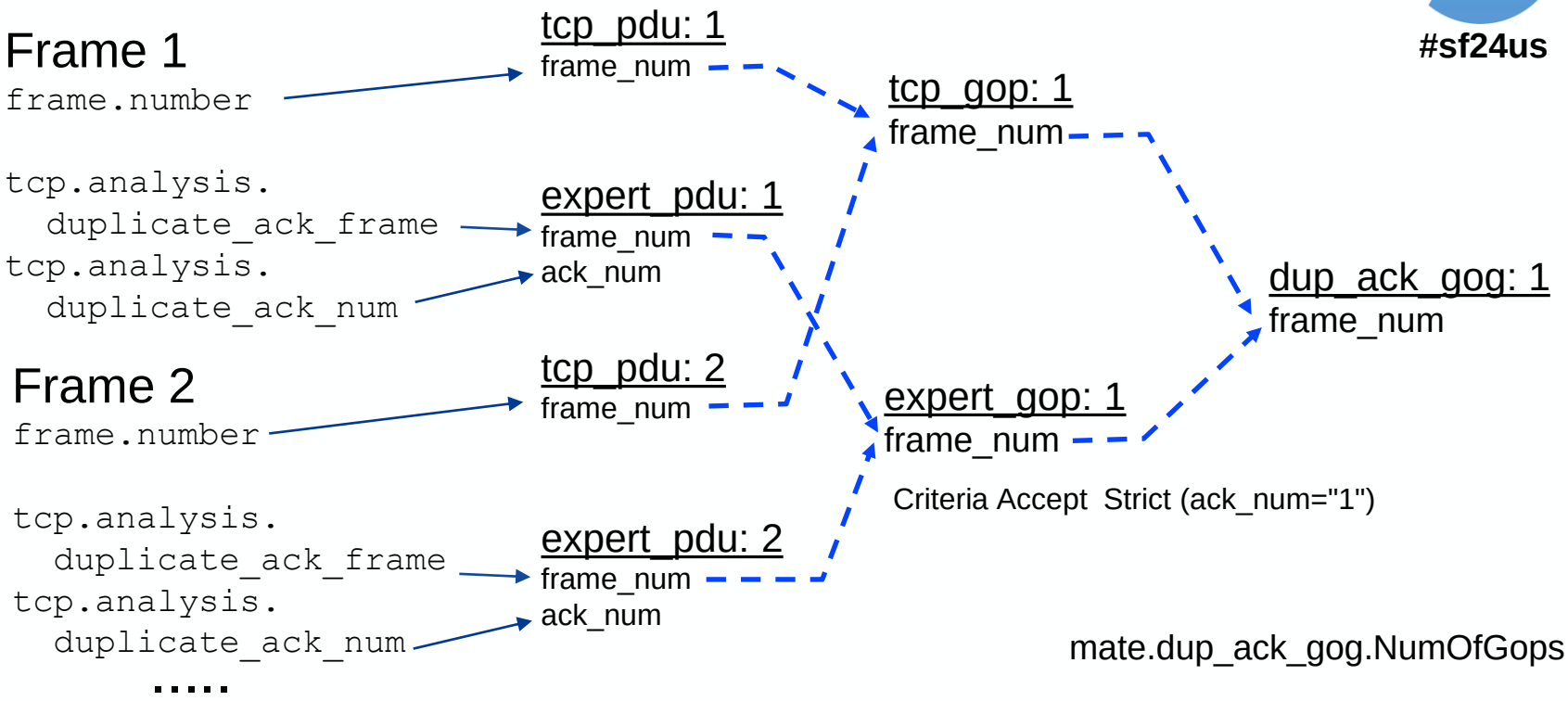
How are we related?

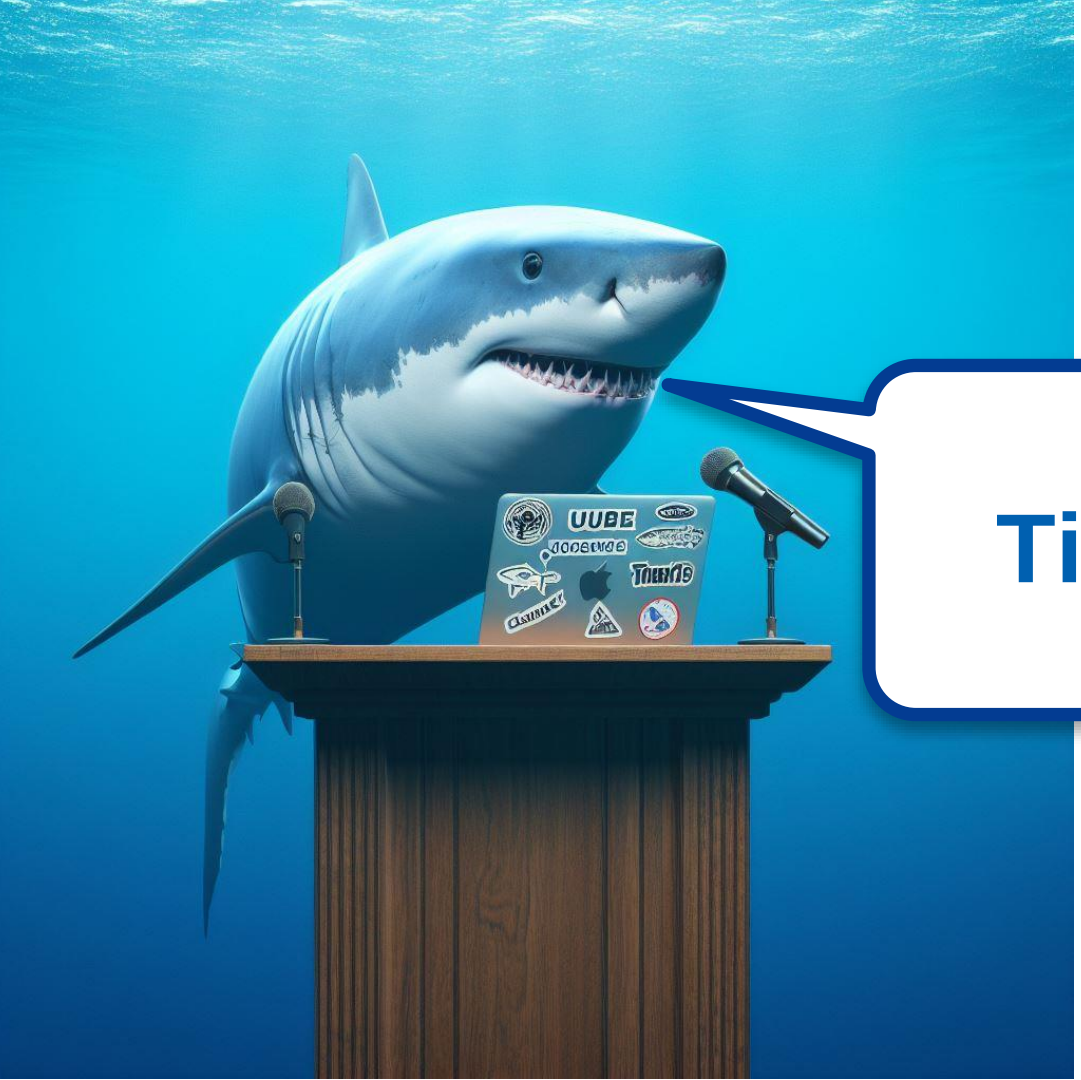

```
tcp.analysis.duplicate_ack_num == 1

No.       Time       Source        Destination     Info
10420     0.000000   10.10.10.10   10.9.9.9        [TCP Dup ACK 10418#1] 1479 → 30000 [ACK] ...
12039     0.466165   10.10.10.10   10.9.9.9        [TCP Dup ACK 12037#1] 1479 → 30000 [ACK] ...
15700     2.234908   10.10.10.10   10.9.9.9        [TCP Dup ACK 15698#1] 1479 → 30000 [ACK] ...
15845     0.079956   10.10.10.10   10.9.9.9        [TCP Dup ACK 15843#1] 1479 → 30000 [ACK] ...
32017     89.478746  10.10.10.10   10.9.9.9        [TCP Dup ACK 32015#1] 1479 → 30000 [ACK] ...

[SEQ/ACK analysis]
    [TCP Analysis Flags]
        [This is a TCP duplicate ack]
    [Duplicate ACK #: 1]
    [Duplicate to the ACK in frame: 10418]
        [Expert Info (Note/Sequence): Duplicate ACK (#1)]
            [Duplicate ACK (#1)]
            [Severity level: Note]
            [Group: Sequence]
```

“Betty Approved“ - ACK (#0)


```
mate.dup_ack_gog.NumOfGops > 1
Time="Seconds Since Previous Displayed Packet"

No.       Time       Source        Destination     Info
10418     0.000000   10.10.10.10   10.9.9.9        1479 → 30000 [ACK] ...
10420     0.000038   10.10.10.10   10.9.9.9        [TCP Dup ACK 10418#1] 1479 → 30000 [ACK] ...

12037     0.466137   10.10.10.10   10.9.9.9        1479 → 30000 [ACK] ...
12039     0.000028   10.10.10.10   10.9.9.9        [TCP Dup ACK 12037#1] 1479 → 30000 [ACK] ...

15698     2.166349   10.10.10.10   10.9.9.9        1479 → 30000 [ACK] ...
15700     0.068559   10.10.10.10   10.9.9.9        [TCP Dup ACK 15698#1] 1479 → 30000 [ACK] ...

15843     0.067816   10.10.10.10   10.9.9.9        1479 → 30000 [ACK] ...
15845     0.012140   10.10.10.10   10.9.9.9        [TCP Dup ACK 15843#1] 1479 → 30000 [ACK] ...

32015     89.478505  10.10.10.10   10.9.9.9        1479 → 30000 [ACK] ...
32017     0.000241   10.10.10.10   10.9.9.9        [TCP Dup ACK 32015#1] 1479 → 30000 [ACK] ...
```

[Duplicate ACK (#0)]





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

#sf2
4us

Time for Q & A

Generated with Microsoft Designer AI