WIRESHARK EDUCATION DAY – OLTEN CH 2026

Network Packet Brokers

Sake Blok

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
  - ... and of the Wireshark Technical Steering Committee
- Started SYN-bit in 2010
  - Application and Network troubleshooting
  - Protocol and packet analysis
  - Training (Wireshark, TCP, TLS)
- Organizer of the Wireshark Users NL meetups
- 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

Challenges in large scale packet capturing

Challenges of packet capturing on a large scale

- Multiple tools need (the same or different) packet data
  - (Application|Network) performance monitoring
  - Intrusion detection
  - Network forensics
  - Troubleshooting
- Limitation on amount of SPAN sessions or TAP ports
- Tools have limited processing power
  - So sending all packets results in bigger more expensive versions
- Legal restrictions and security policy implications
- The interesting data could be encapsulated (VXLAN, GTP, etc)
- The interesting data could be encrypted

Packet capture infrastructure

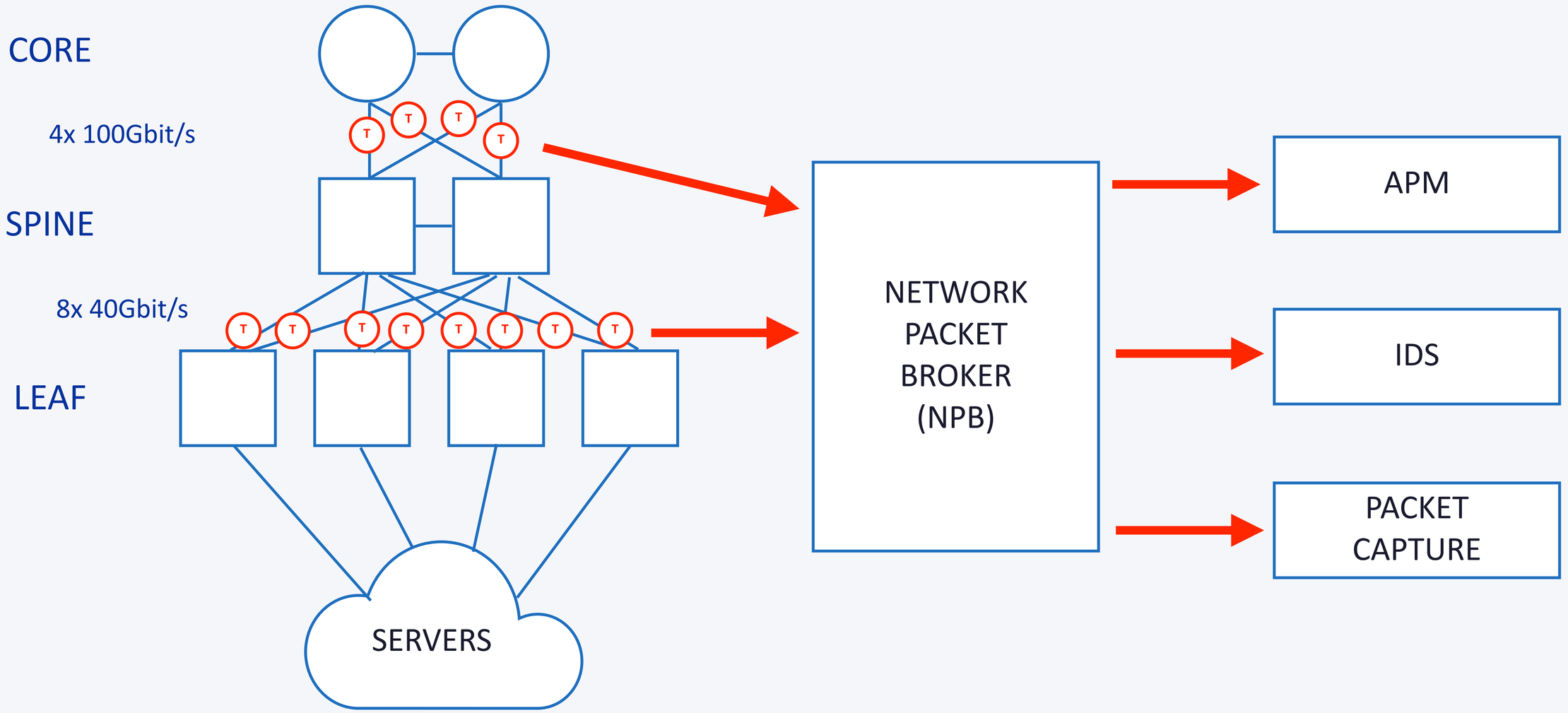
- Secondary network just for packet capturing
- Consists of:
  - capture points
    - SPAN, RSPAN, ERSPAN
    - TAPs
  - Tools needing packet data
    - NPM, APM devices
    - Security tools
    - Troubleshooting tools
  - Network Packet Brokers
    - The magic box that handles all of the packet forwarding to the right tools

What are NPBs?

Basic features of a network packet broker

- In essence it is an M to N forwarding switch
- Configured with rules on which packets are forwarded to which tools
  - Can aggregate
  - Can replicate
  - Can loadbalance
  - Can filter or L2, L3, L4 and partly on L7
- Usually high port density of high speed ports

Packet Capture Infrastructure

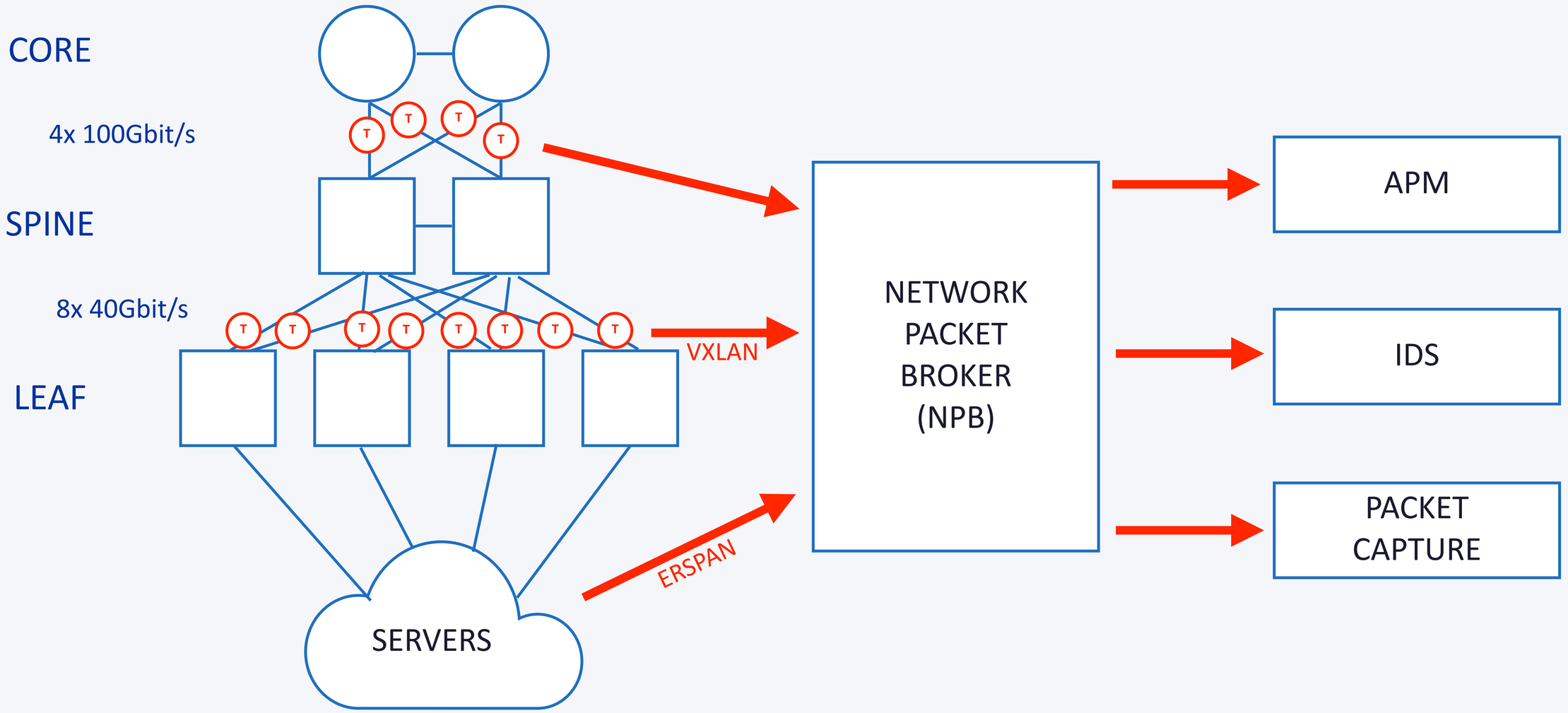


Advanced Features

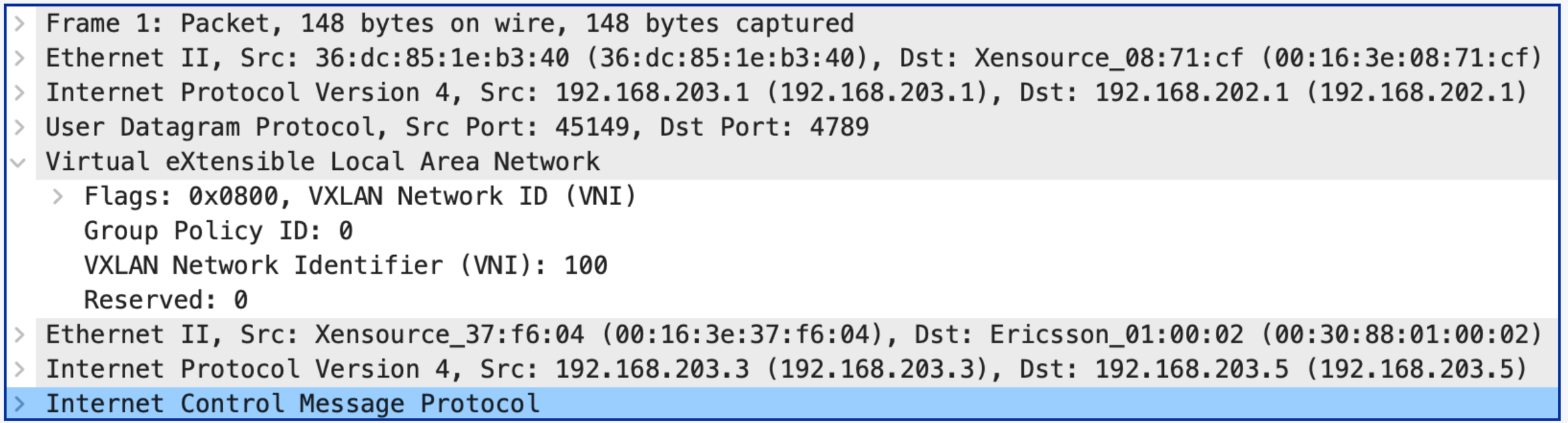
Advanced features of a network packet broker

- Timestamping
- Slicing
- Deduplication
- Decapsulation (VXLAN, GTP, ERSPAN, etc)
  - and being an ERSPAN endpoint
- Decryption (TLS)
- L2-L7 filtering (e.g. mac, vlan, ip, tcp, IMSI)

Packet Capture Infrastructure



VXLAN


Frame 1: Packet, 148 bytes on wire, 148 bytes captured
Ethernet II, Src: 36:dc:85:1e:b3:40 (36:dc:85:1e:b3:40), Dst: Xensource_08:71:cf (00:16:3e:08:71:cf)
Internet Protocol Version 4, Src: 192.168.203.1 (192.168.203.1), Dst: 192.168.202.1 (192.168.202.1)
User Datagram Protocol, Src Port: 45149, Dst Port: 4789
Virtual eXtensible Local Area Network
Flags: 0x0800, VXLAN Network ID (VNI)
Group Policy ID: 0
VXLAN Network Identifier (VNI): 100
Reserved: 0
Ethernet II, Src: Xensource_37:f6:04 (00:16:3e:37:f6:04), Dst: Ericsson_01:00:02 (00:30:88:01:00:02)
Internet Protocol Version 4, Src: 192.168.203.3 (192.168.203.3), Dst: 192.168.203.5 (192.168.203.5)
Internet Control Message Protocol

ERSPAN

```
> Frame 49919: Packet, 948 bytes on wire, 948 bytes captured on interface unknown, id 28
> Ethernet II, Src: SuperMicroCo_8b:49:00 (3c:ec:ef:8b:49:00), Dst: EliteGroupCo_0f:cc:5e (1c:69:7a:0f:cc:5e)
> Internet Protocol Version 6, Src: 2a00:6020:ad0b:8300::d061:443 (2a00:6020:ad0b:8300::d061:443), Dst: 2a00:6020:ad0b:8300::c01:22 (2a00:6020:ad0b:8300::c01:22)
v Generic Routing Encapsulation (ERSPAN III)
  > Flags and Version: 0x1000
    Protocol Type: ERSPAN III (0x22eb)
    Sequence Number: 322
v Encapsulated Remote Switch Packet ANalysis Type III
    0010 .... .... .... = Version: Type III (2)
    .... 0000 0000 0000 = Vlan: 0
    000. .... .... .... = COS: 0
    ...0 0... .... .... = Bad/Short/Oversized: Good or unknown integrity (0)
    .... .0.. .... .... = Truncated: Not truncated (0)
    .... ..00 0000 0000 = SpanID: 0
    Timestamp: 445845000
    Security Group Tag: 0
    0... .... .... .... = Has Ethernet PDU: 0
    .000 00.. .... .... = Frame Type: Ethernet (0)
    .... ..00 0000 .... = Hardware ID: 0
    .... .... .... 0... = Direction: Ingress
    .... .... .... .10. = Timestamp granularity: IEEE 1588 (2)
    .... .... .... ...1 = Optional Sub headers: 1
    0001 01.. .... .... .... .... .... .... = Platform ID: 5
    .... ..00 0000 0000 .... .... .... .... = Switch ID: 0
    .... .... .... .... 0000 0000 0000 0000 = Port ID/Index: 0
    Timestamp (seconds): 1772202133
> Ethernet II, Src: 02:00:00:01:03:01 (02:00:00:01:03:01), Dst: PaloAltoNetw_03:12:10 (3c:fa:30:03:12:10)
> Internet Protocol Version 6, Src: 2a01:239:2c2:9900::1 (2a01:239:2c2:9900::1), Dst: 2a00:6020:ad0b:8300::c01:53 (2a00:6020:ad0b:8300::c01:53)
> Transmission Control Protocol, Src Port: 22, Dst Port: 47368, Seq: 109911, Ack: 2483, Len: 780
> SSH Protocol
```

Benefits

Benefits

- Get each tool the packets it needs
  - No more limit on # of SPAN sessions or # of taps
- Get each tool *__only__* the packets it needs
  - Remove duplicates, prevents false analysis
  - Use filters
  - Save on costs for the devices analysing the packets
- Give each tool ***the right*** packets because of decapsulation
- Give each tool ***the same timestamp***
  - Only if the tool understands the custom packet format

Thank you!

WIRESHARK

Sake Blok
sake.blok@SYN-bit.nl

SYN-bit
deep traffic analysis