# Netzwork Security Monitoring

Martin Scheu

26. Februar 2022

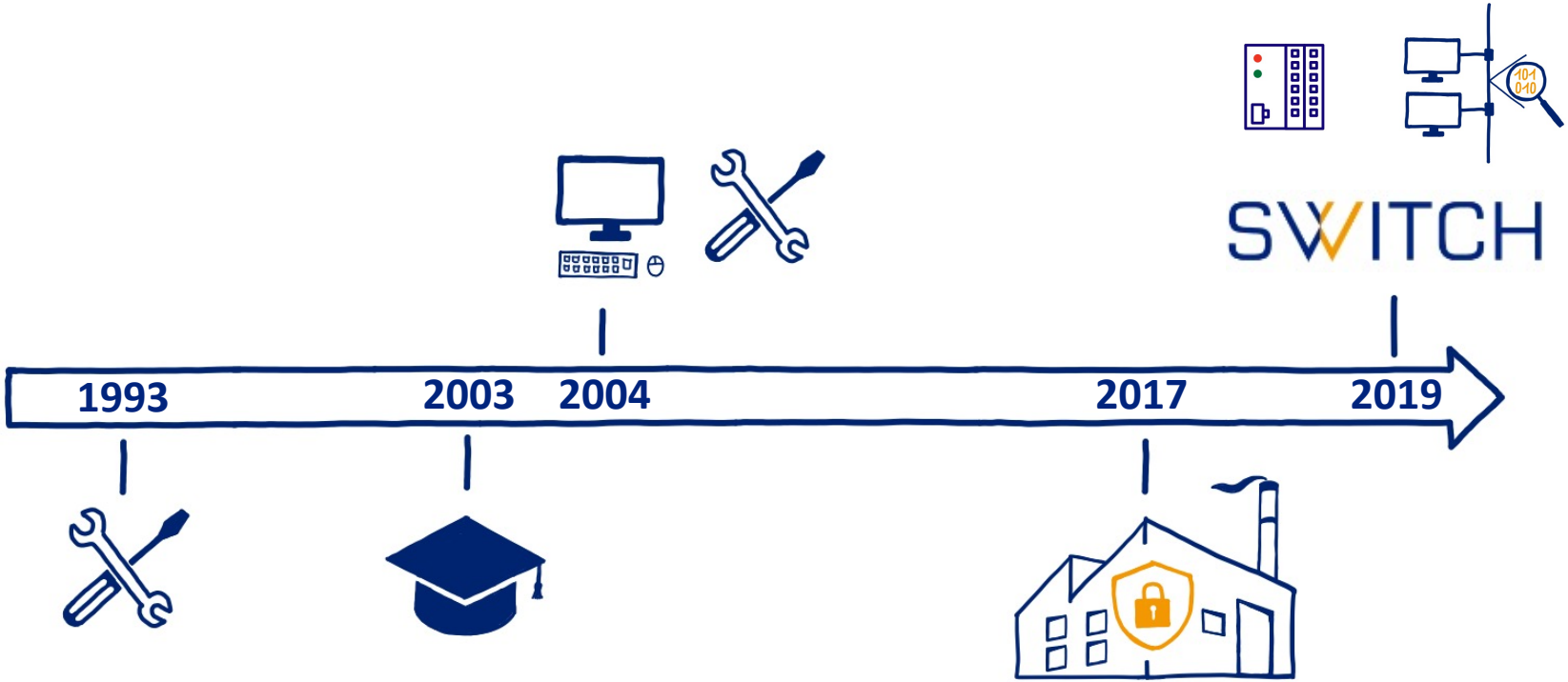
# Agenda

Kommunikation und Pakete

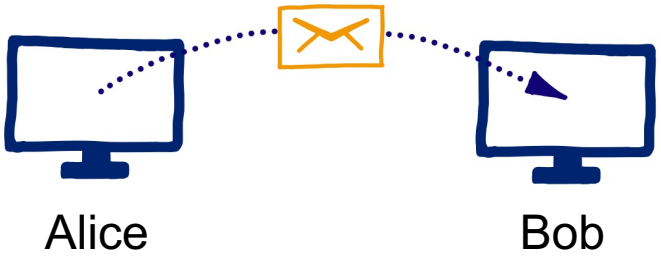
Umsetzung

Beispiele / Demo

# #whoami



# Kommunikation



# Kommunikation

Alice Bob

Router
Internetbox
Modem


ISP: Internet Service Provider

# Kommunikation

Geräteadressierung

MAC Adresse : 00-80-41-ae-fd-7e

Hersteller: 00-80-41 https://maclookup.app/

IP Adresse : v4 192.168.1.1

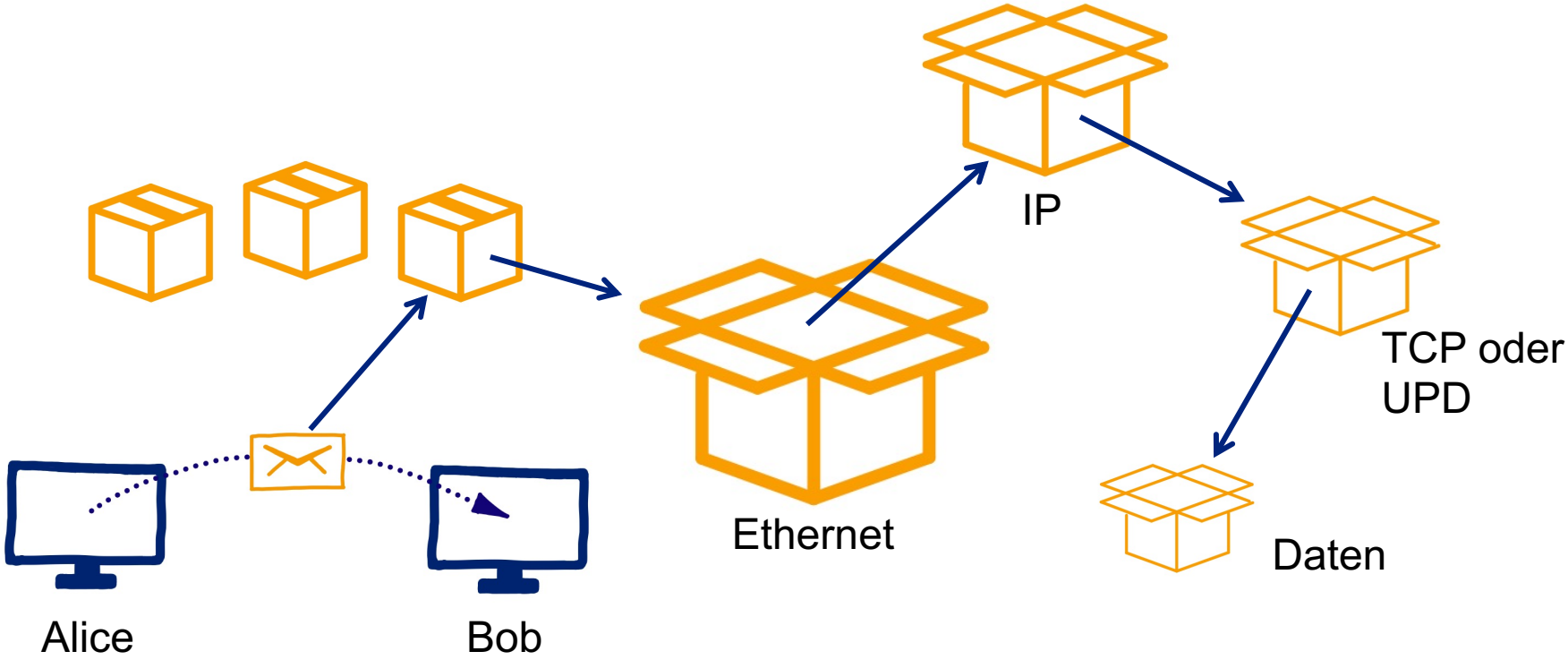
v6 fe80::1ff:fe23:4567:890a

Dienste rund ums Netzwerk

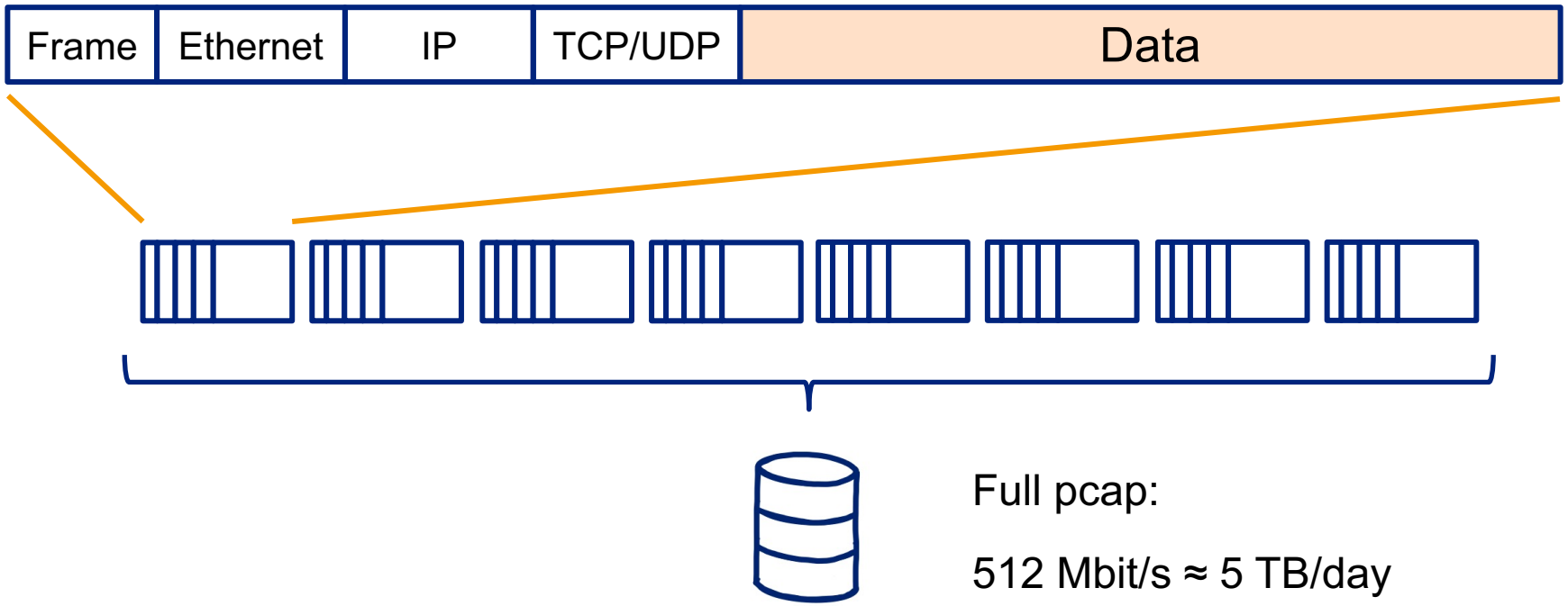
DNS : digiges.ch

DHCP, NTP, HTTP(S), SMB, SMPT, ...

# Pakete - OSI Modell



# Pakete aufzeichnen - full pcap

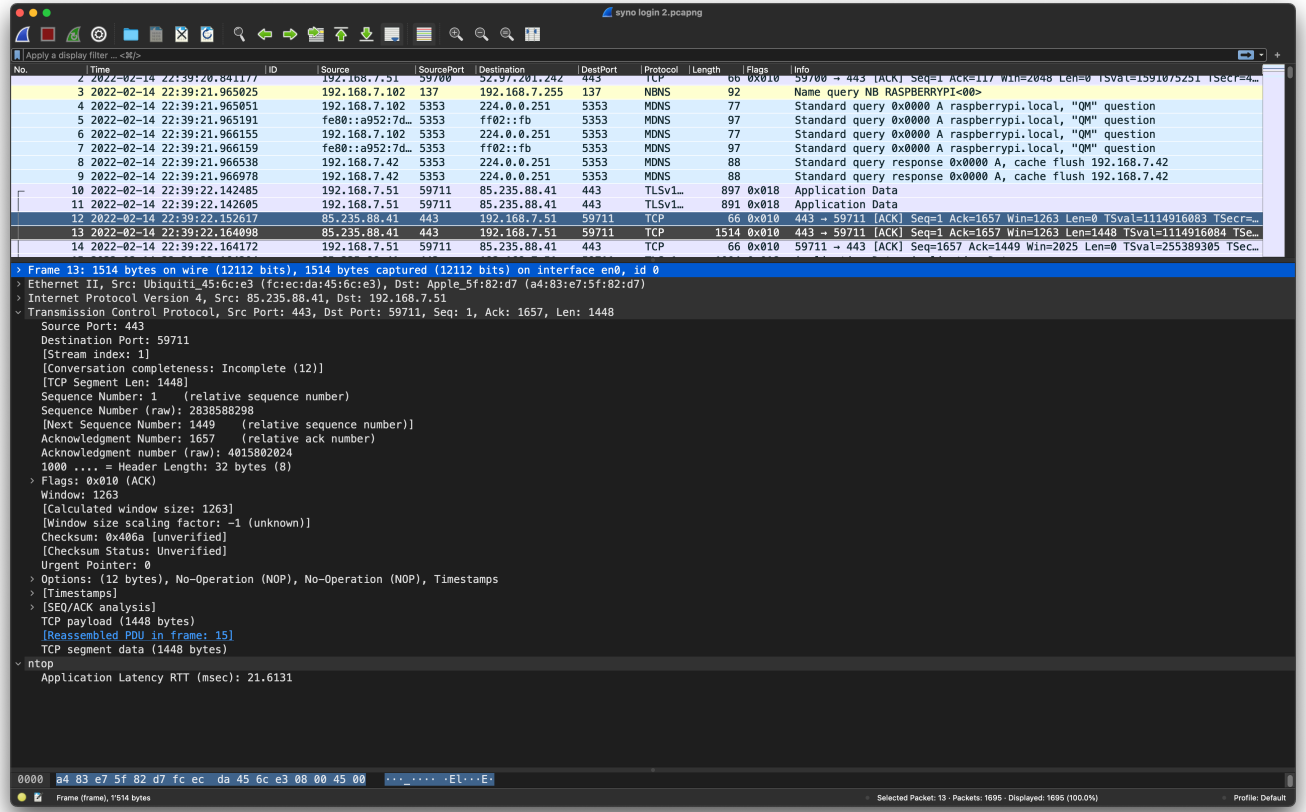


# Pakete aufzeichnen - Flow

| IP.Src | Src.Port | IP.Dst | Dst.Port | Proto |
|---|---|---|---|---|
| 172.16.2.11 | 58336 | 172.16.2.1 | 53 | DNS |
| 172.16.2.1 | 45771 | 9.9.9.9 | 53 | DNS |

Src = Source / Ursprung
Dst = Destination / Ziel
Proto = Protokoll

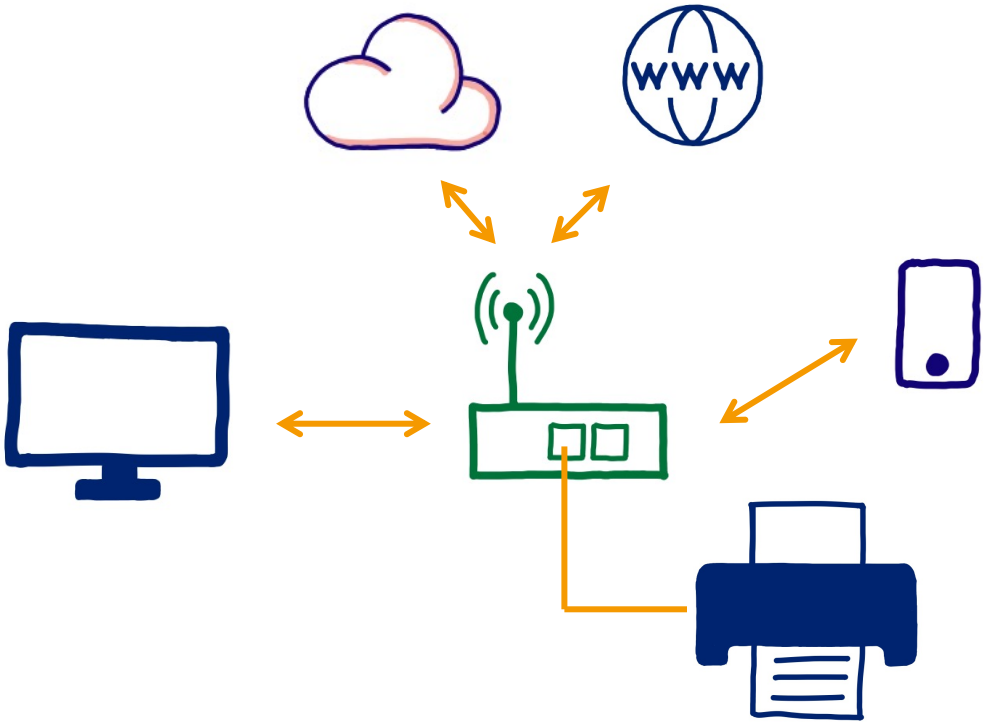
# Wireshark



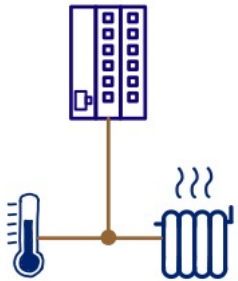


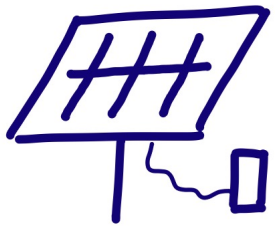

Get Wireshark: https://www.wireshark.org/

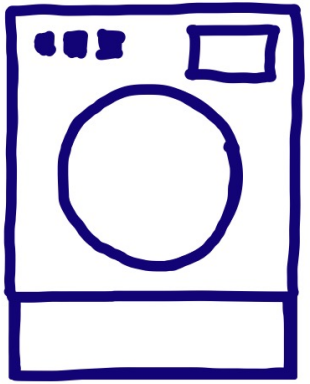
# Geräte im Netzwerk



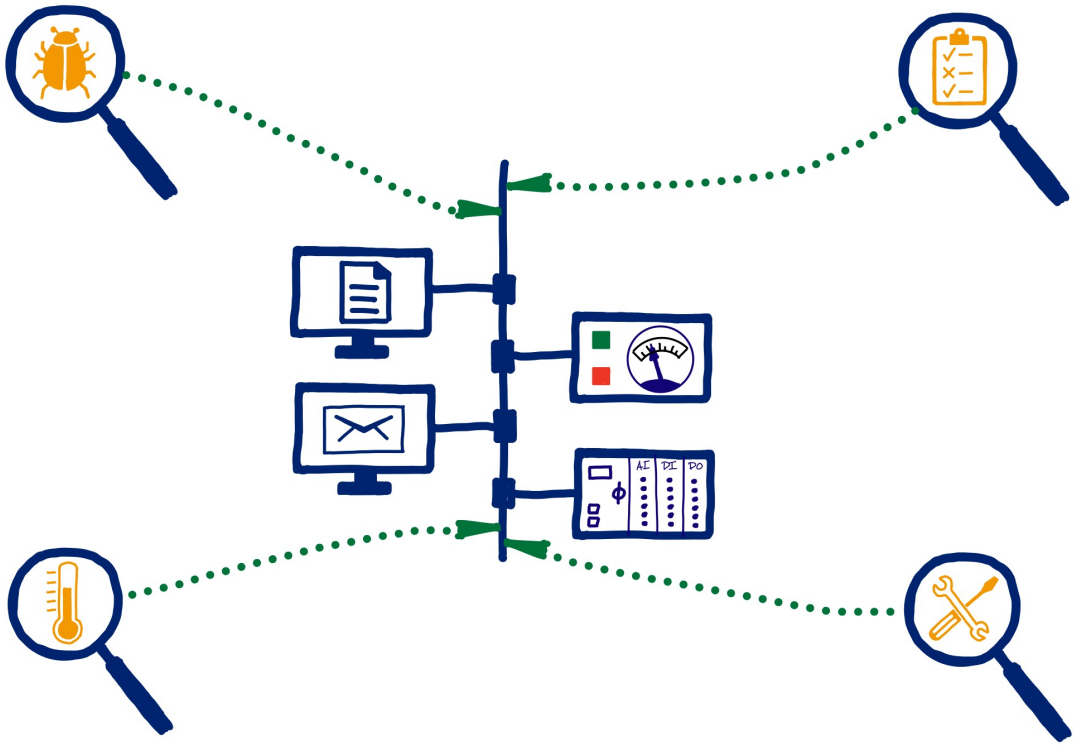
# Geräte im Netzwerk



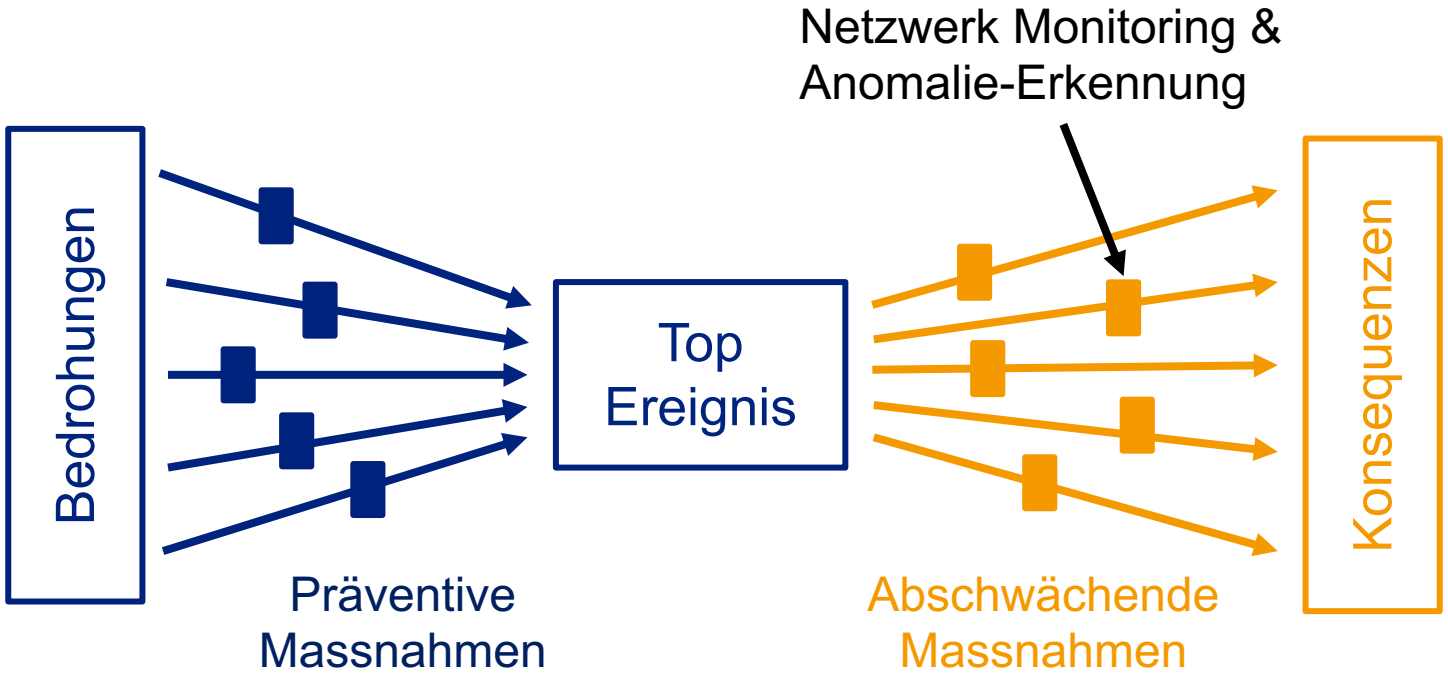




# Netzwerk Security Monitoring



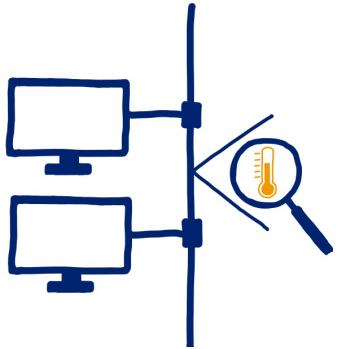
# Ingenieurs -

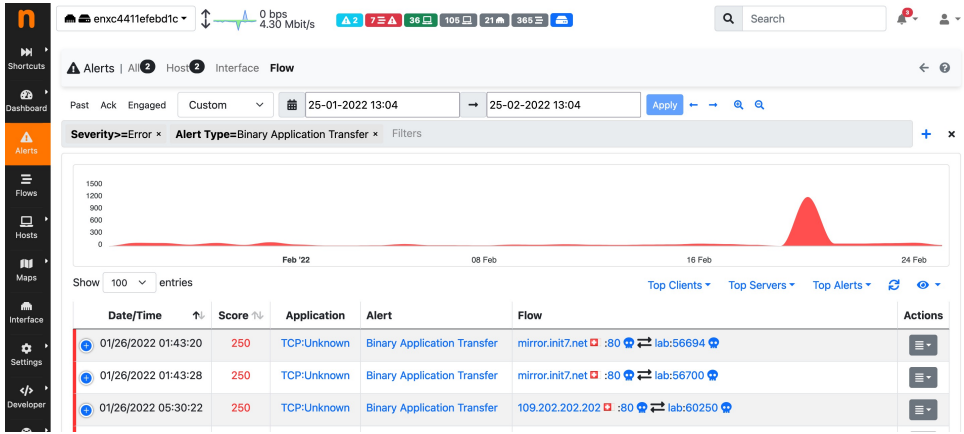





Source: #S4x20, Shiny Object Syndrome, Rebekah Mohr

# Netzwerk Security Monitoring






Sensor

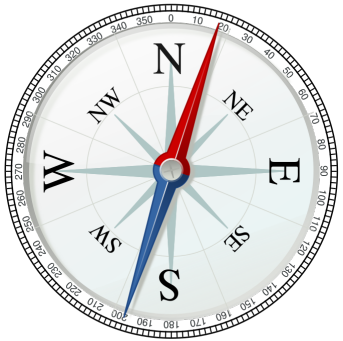
Anzeige und Administration
über Webbrowser

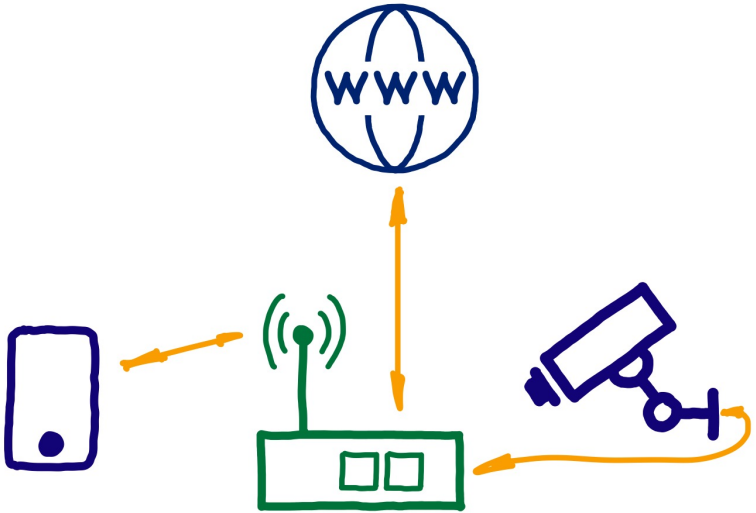
Alarmierung

# Open-source Netzwerk Security Monitoring

| | Com-munity | Benutzer-freundlich | Resourcen Anforderung | Installation und Einrichten |
|---|---|---|---|---|
| Malcolm | klein | nein | gross | kompliziert |
| ntop | klein | ja | klein | einfach |
| Suricata Open Source IDS / IPS / | gross | nein | klein | kompliziert |
| SNORT | gross | nein | klein | kompliziert |
| SOS | mittel | ja | mittel - viel | einfach - mittel |
| zeek | gross | nein | klein | kompliziert |

# Sensor platzieren

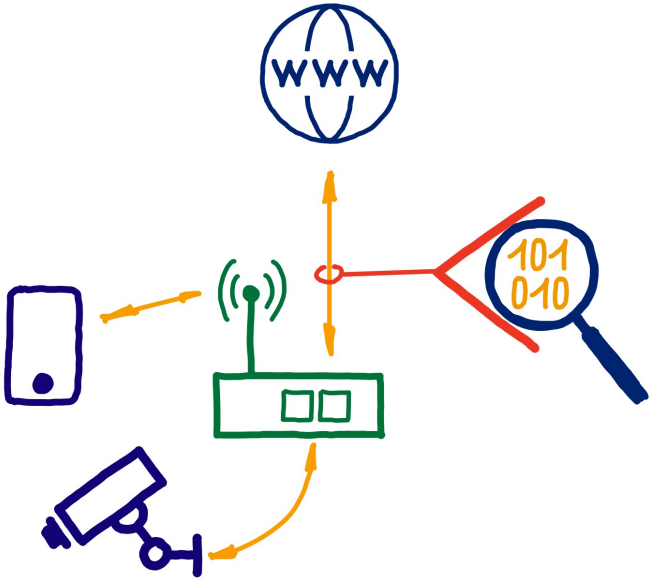


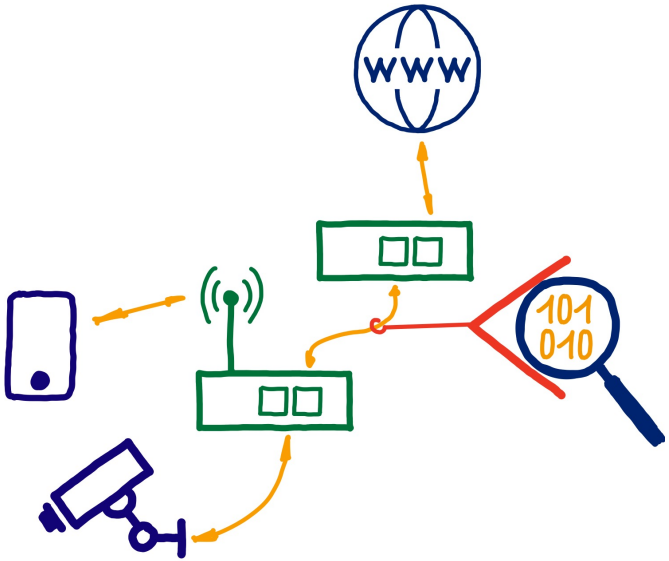






Quelle Symbol: https://openclipart.org/

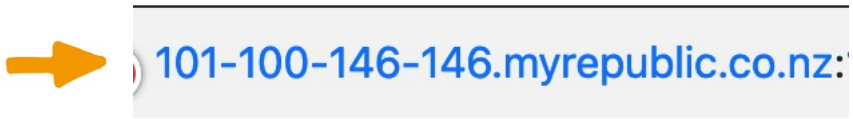
# Sensor platzieren



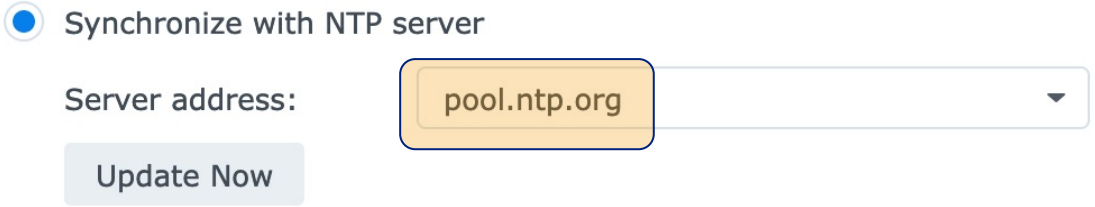
# Beispiele / Demo

# Beispiel I - komische Verbindung

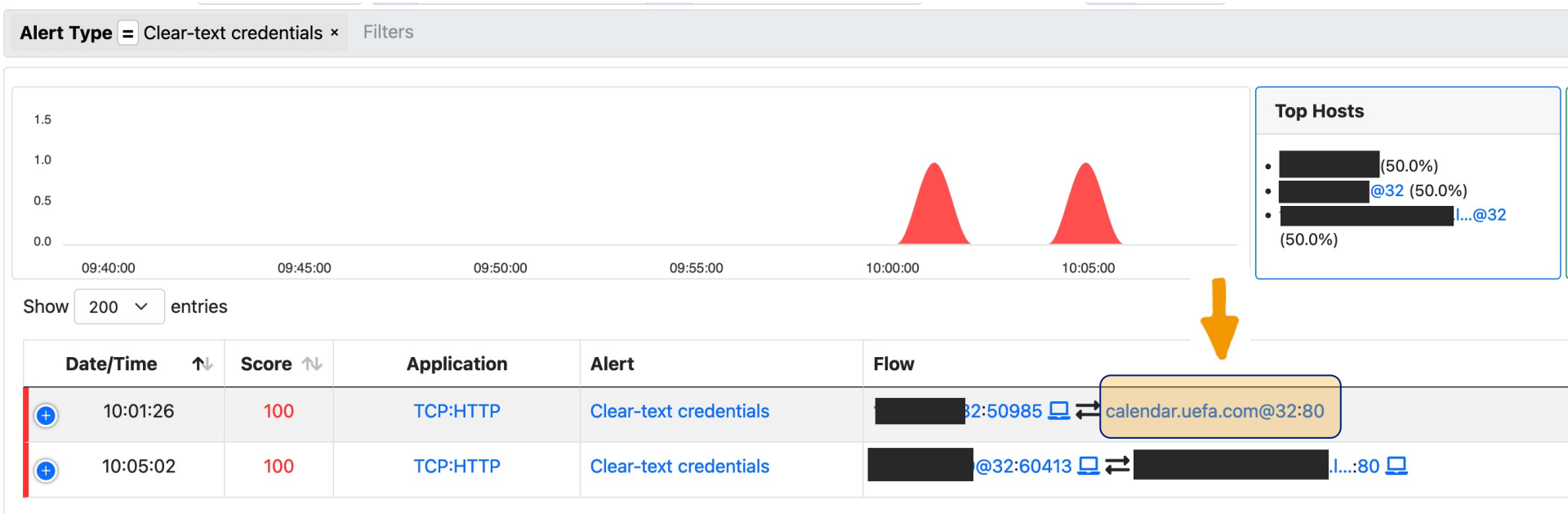



| Flow | Protocol | Application | Score | Pkts | Bytes | Thpt | Begin | End |
|---|---|---|---|---|---|---|---|---|
| 101-100-146-146.myrepublic.co.nz:123 ⇄ valdivia.mscheu.ch:123 | UDP | NTP | 10 | 2 Pkts | 110 Bytes | 880 bit/s | 12/29/21 23:13:08 | 12/29/21 23:13:08 |

| Application | Score | Pkts | Bytes |
|---|---|---|---|
| NTP | 10 | 2 Pkts | 110 Bytes |



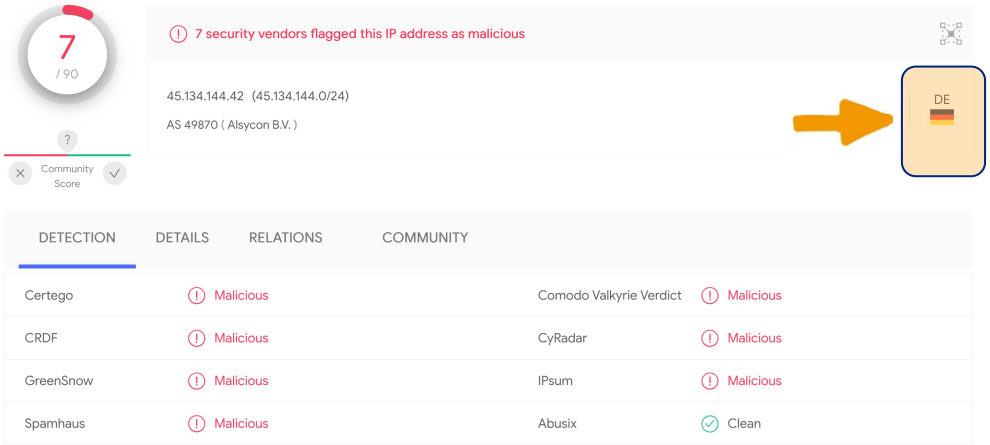
# Beispiel II - Klartext Passwörter

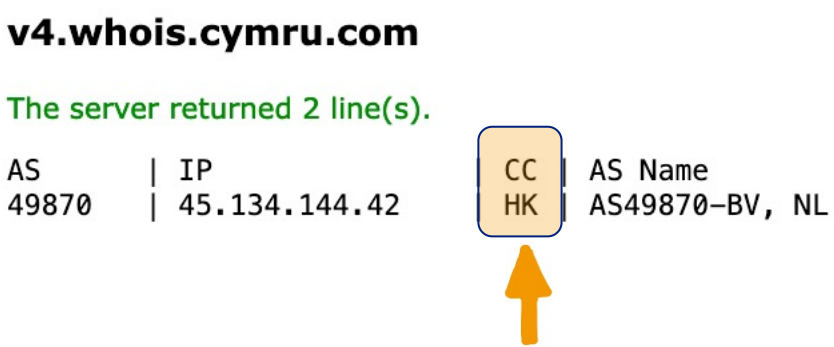


# Beispiel III - GEO Fence in Firewalls

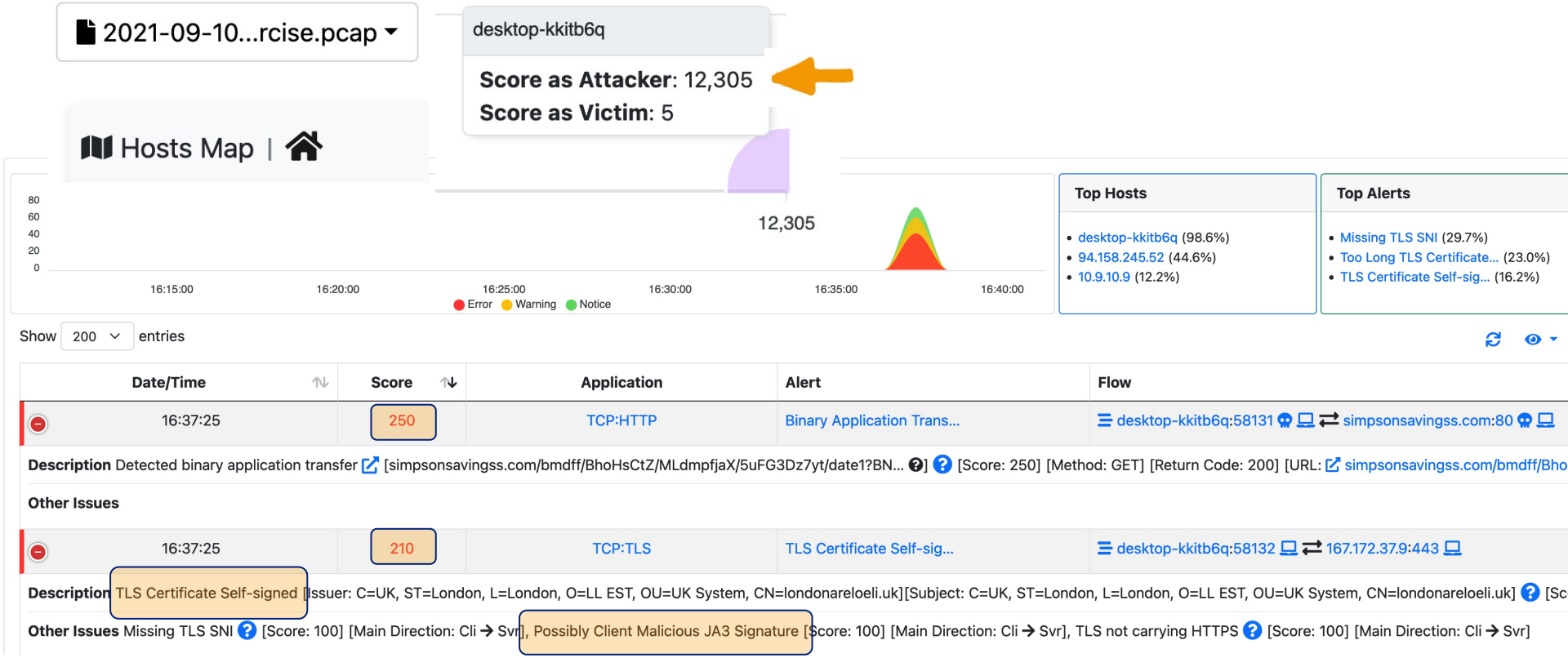
| Date/Time | Score | Application | Alert | Flow | Des |
|---|---|---|---|---|---|
| 09/11/2021 10:13:26 | 200 | TCP:HTTP | Blacklisted Flow | 45.134.144.42@3654:44588 [redacted]l...:80 | Bla |

**Other Issues** Remote to Local Insecure Protocol [Score: 100] [Predominant Traffic: Srv → Cli]



# Example IV - Schadsoftware






Source sample: https://www.malware-traffic-analysis.net/2021/09/10/index.html

# Demo

# Werkzeuge


Desktop pcap Analyse

https://www.brimdata.io/download/

Pcaps mit Schadsoftware,
Anleitungen und Tutorials

https://malware-traffic-analysis.net/

NetworkMiner, Desktop pcap Analyse

https://www.netresec.com/?page=NetworkMiner

TraceWrangler - Packet Capture Toolkit

https://www.tracewrangler.com/


Pcap aufzeichnen
und analysieren

https://www.wireshark.org/

# Dankeschön!



martin.scheu@switch.ch


martin-scheu


@martin_scheu