



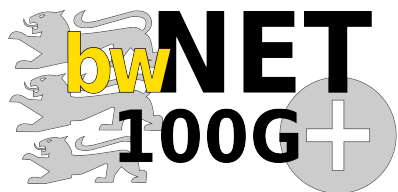
ZDV / bwNET 2.0 - Verteilte Netflow/IPFIX Sensorplattform im Kommunikationsnetz der Universität Tübingen

Benjamin Steinert, Gabriel Paradzik, Heinrich Abele
Zentrum für Datenverarbeitung
Universität Tübingen





- bwNET seit 2013, seit April 2024 aktuelles Projekt: bwNET 2.0



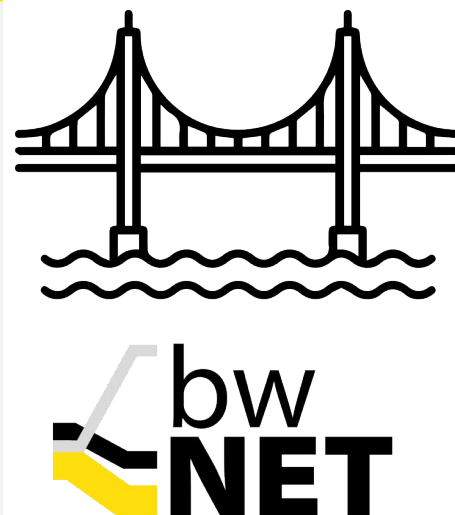
- Forschungsgruppen und Rechenzentren arbeiten eng zusammen:



Was will man mit bwNET erreichen?

Betrieb

- ▶ Fokus: Verlässlicher Betrieb
- ▶ Weiterentwicklung eher inkrementell oder evolutionär
- ▶ Geringes Zeitbudget für neue Ideen
- ▶ Neueste Ansätze aus Forschung /Industrie nicht immer bekannt



Forschung

- ▶ Fokus: Innovation
- ▶ Frühe Nutzung oder gar Entwicklung neuer Technologien
- ▶ Hohes Zeitbudget für neue Ideen
- ▶ Probleme des realen Netzbetriebs sind oft weit weg

Betrieb und Forschung sollen voneinander profitieren !



Monitoring




Angriffserkennung und
Mitigation



Network Softwarization



Technology Scouting

- ▶ Aufbau einer verteilten IPFIX Sensorplattform
- ▶ Datenschutzkonforme Bereitstellung von Betriebsdaten zur Forschung mit **LSDF**
- ▶ Sammlung, Nutzung und Teilen von Threat Intelligence Daten
- ▶ Technology Scouting: Streaming Telemetry (u.a. Stichwort  **OPENCONFIG**)



Ausschnitt weiterer Projektthemen



Monitoring



Angriffserkennung und
Mitigation



Intelligente
Verkehrssteuerung



Technology Scouting

- ML-basierte Staukontrolle & DDoS Erkennung @ KIT
- Network Digital Twin @ HKA
- Zero Trust, Zugriffskontrolle, Kontinuierliche Authentisierung @ UULM
- Speedtests & Segment Routing @ BelWü

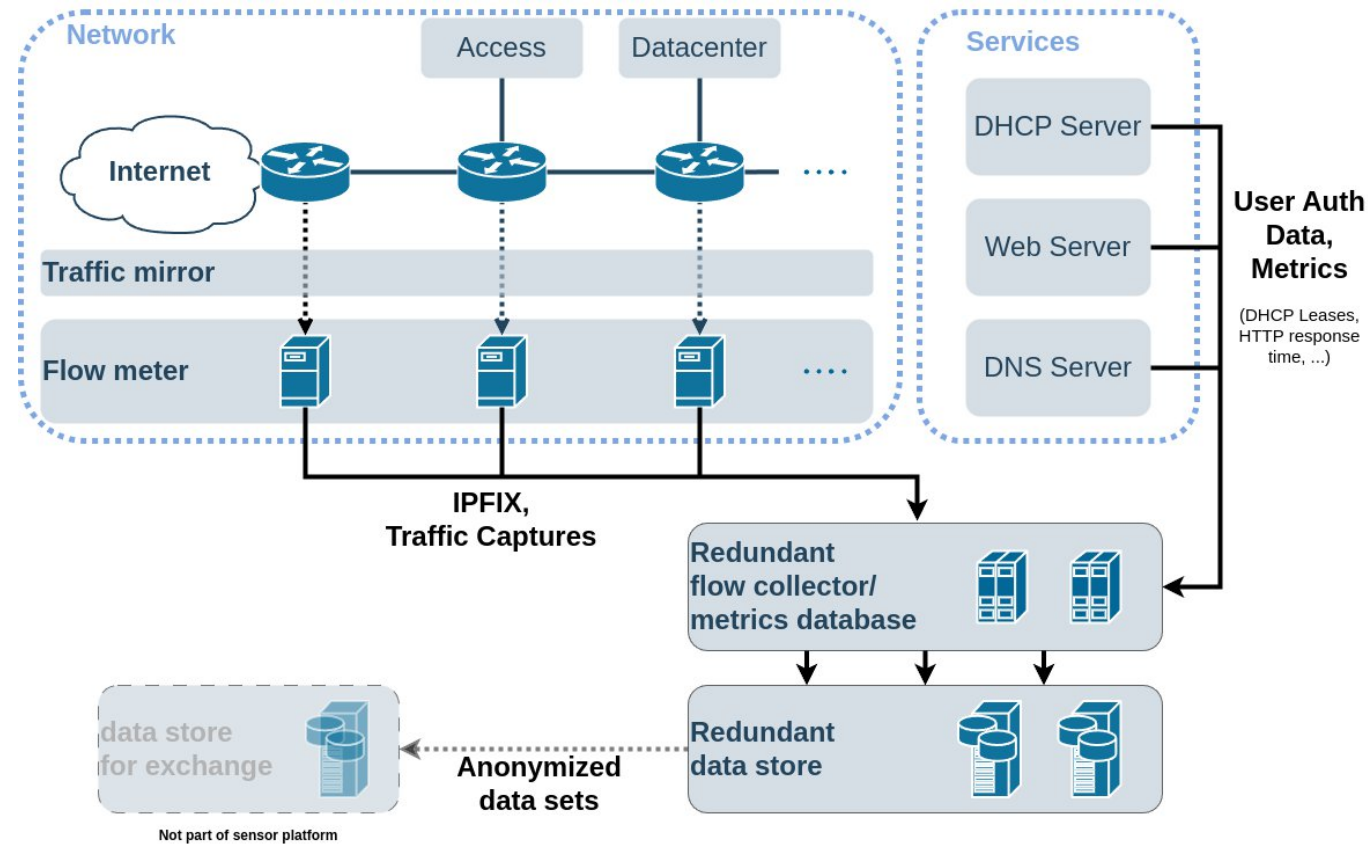
BelWü Speedtest Site
Landeshochschulnetz Baden-Württemberg

- Dualstack
- IPv4-only
- IPv6-only

Speedtest	Anforderungen
Browser-Speedtest	<ul style="list-style-type: none">• Browser• Abhängig von der Performance des Browsers
HTTP Download	<ul style="list-style-type: none">• HTTP Client
PerfSonar Speedtest	<ul style="list-style-type: none">• Testserver: testpoint.perfsonar.belwue.de• Öffentliches Dashboard• Wenn Sie Interesse haben, unserem öffentlichen Dashboard beizutreten, können Sie uns gerne per Mail kontaktieren.

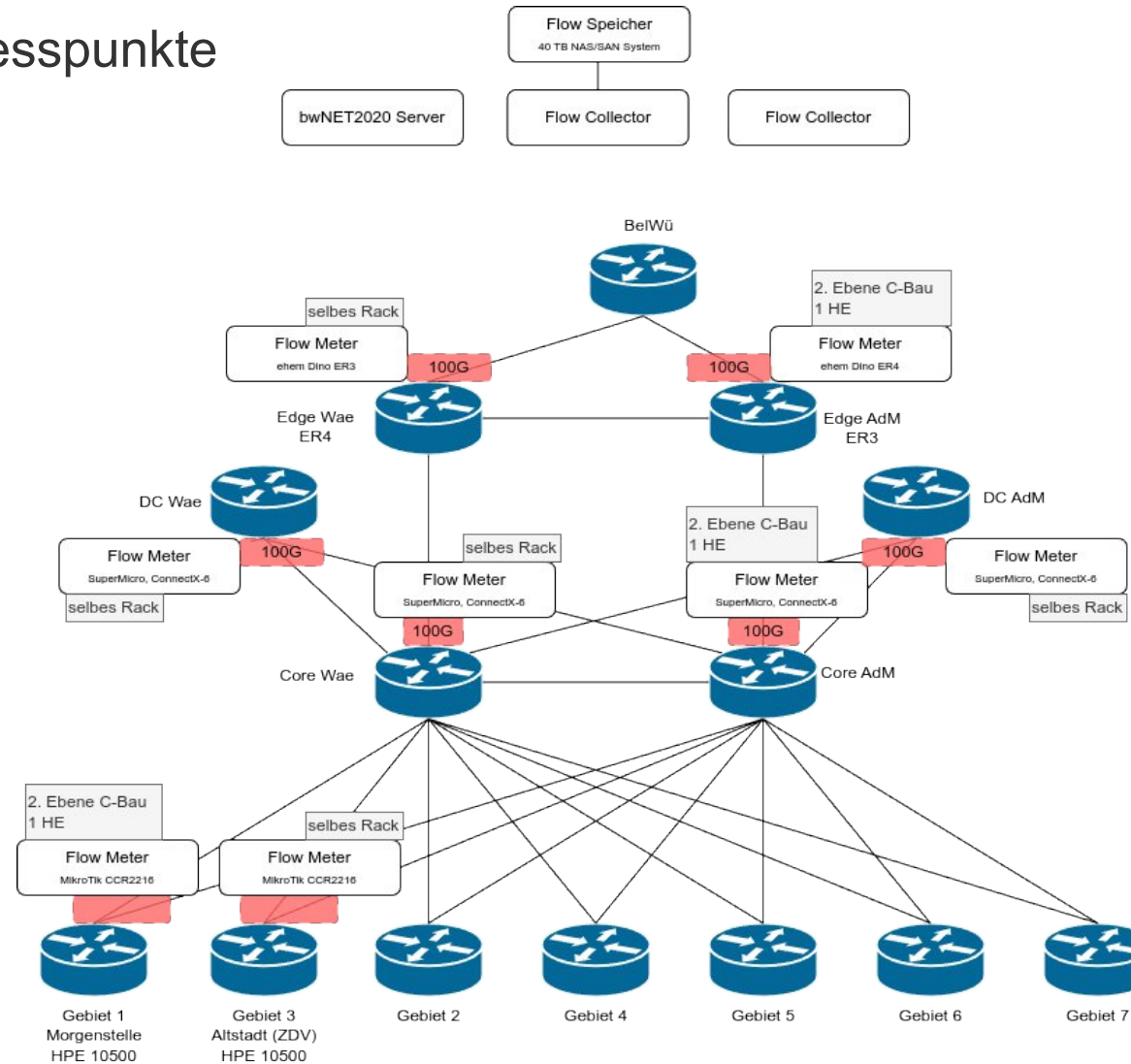
[Impressum und Datenschutzerklärung](#)

- Ziel: Aufbau einer verteilten IPFIX Sensorplattform zur Erfassung von unsampled Flow-Daten bei 100+ Gbit/s





► Konkrete Architektur & Messpunkte





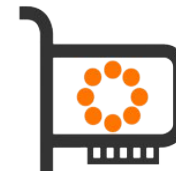
- ▶ Nutzung von Server-basierten Flow-Sensoren mit effizienten Software-basierten Bausteinen, oder kleinen Appliance-basierten Flow-Sensoren
 - z.B. Yet Another Flowmeter (YAF) [1] mit ConnectX-6 und RYZEN 9 [2]
- ▶ Von klein bis groß, von 1 Gbit/s - 100+ Gbit/s
- ▶ Verschiedene Capture Technologien verfügbar, umfangreicher Vergleich geplant:
 - libpcap [3]
 - PF_RING™ (ntop) [4]
 - PF_RING ZC (Zero Copy) (ntop) [4]
 - NIC Treiber (z.B. mlx5)
 - AF_PACKET, AF_XDP
 - DPDK



[1] <https://tools.netsa.cert.org/yaf/>



[3] <https://www.tcpdump.org/>



PF_RING™

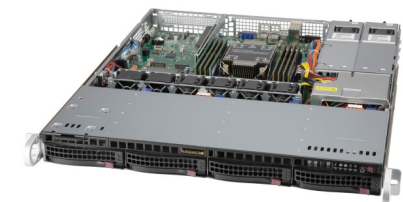
[3] https://www.ntop.org/products/packet-capture/pf_ring/



https://mikrotik.com/product/ccr2004_1g_2xs_pcie



https://mikrotik.com/product/ccr2216_1g_12xs_2xq

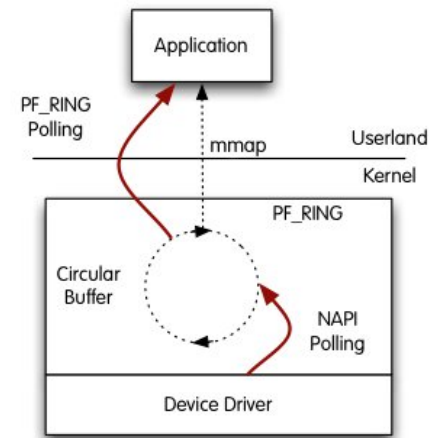


[2] <https://www.primeline-solutions.com/de/supermicro-server-egino-13041s-b650-amd-epycm-4004/>



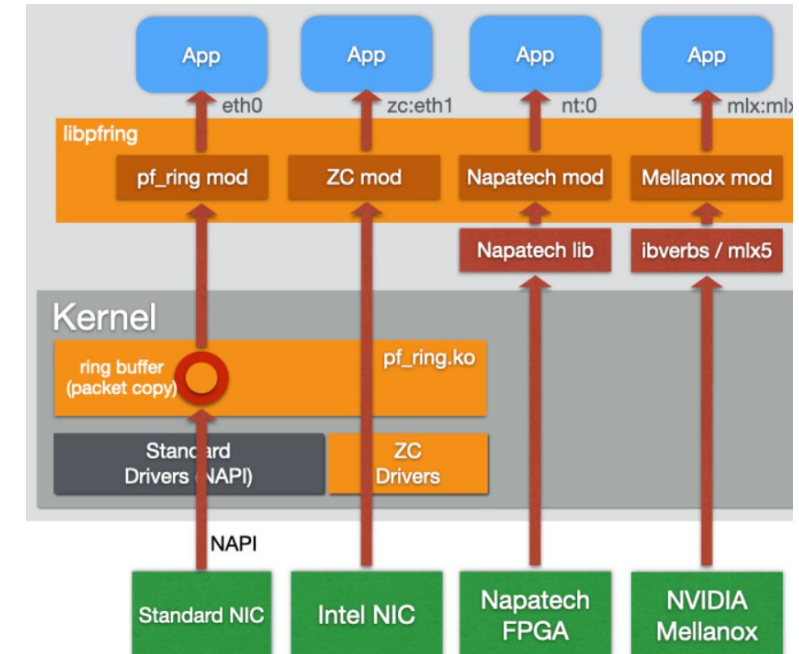
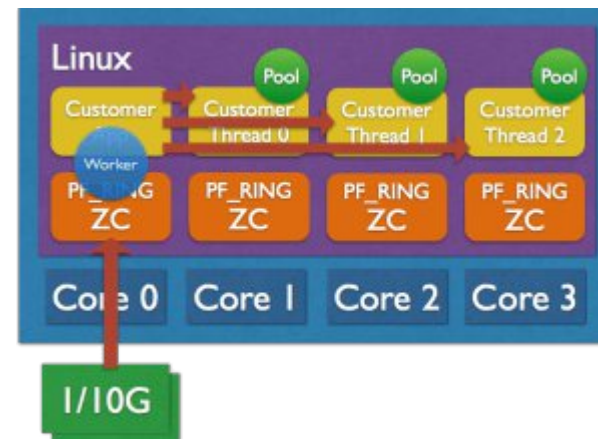
Capture Technologie: PF_RING (ZC)

► PF_RING™ (ntop)



Vanilla PF_RING

► PF_RING ZC (Zero Copy) (ntop)



https://www.ntop.org/products/packet-capture/pf_ring/



- ▶ Strukturierte Sammlung & Speicherung der Flowdaten
 - z.B. mit nfcapd [1], rflowpack [2], GoFlow2 [3]
- ▶ Nutzung von Analysewerkzeugen zur Erkennung von Störungen oder Angriffen
 - z.B. nfdump [1], SiLK analysis suite [2], flowpipeline [4]
- ▶ Aufbau automatisierter Analyse-Pipelines
 - Zeitserienvorhersage und -Dekomposition
 - Anomalieerkennung
 - ML-basierte automatische Analyse und Korrelation
 - Nutzung von SIEM, SOAR, XDR, ... (?)
 - Nutzung von Open Source Threat Intelligence Quellen

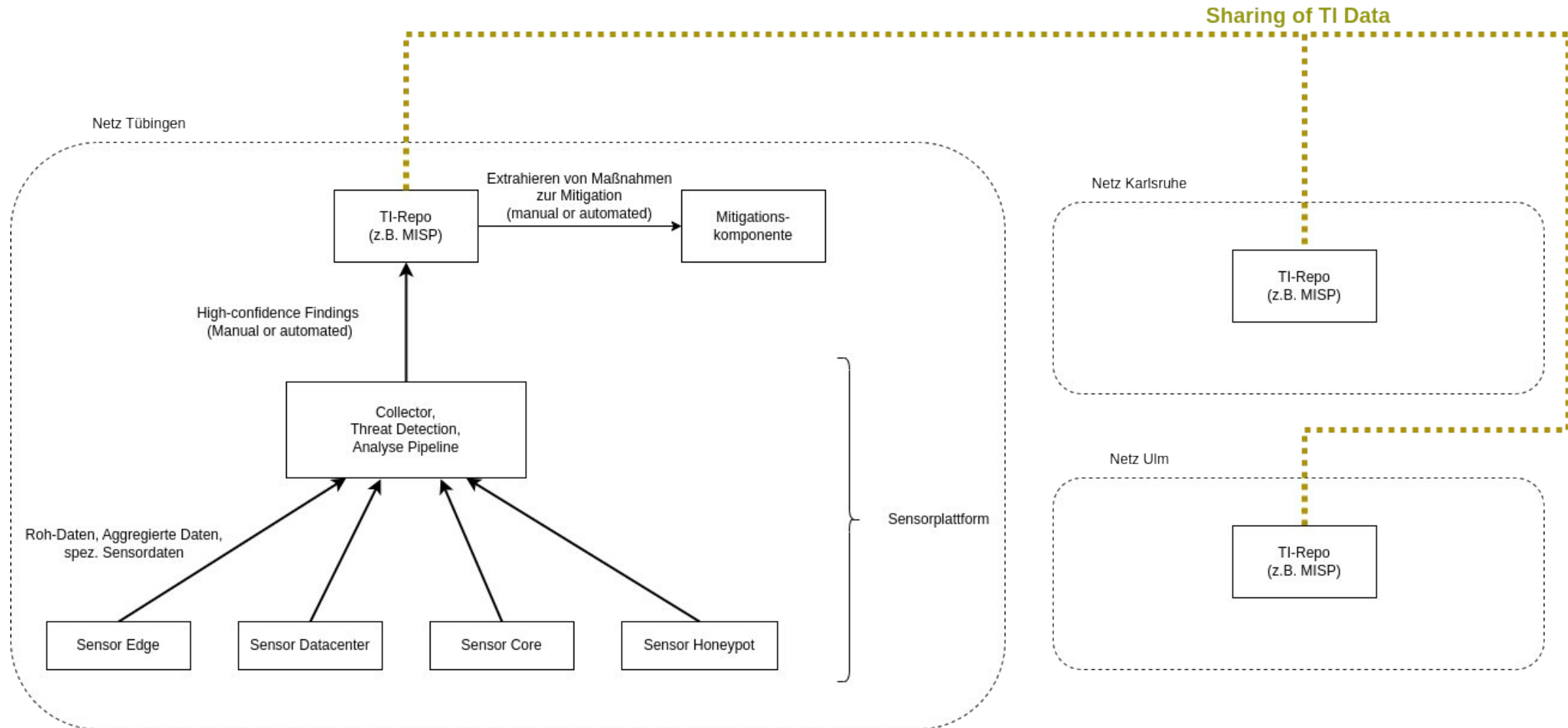


Generated by ChatGPT

- [1] <https://github.com/phaag/nfdump>
- [2] <https://tools.netsa.cert.org/silk/docs.html>
- [3] <https://github.com/netsampler/goflow2>
- [4] <https://github.com/BelWue/flowpipeline>



► Sammeln/Nutzen/Bereitstellen von Threat Intelligence Feeds zwischen Standorten





- ▶ Sensorplattform weiter aufbauen
- ▶ (Automatisierte) Analyse-, Detektions- & Visualisierungs- & Sharing- Pipelines aufbauen
- ▶ Flowmeter Benchmarking inkl. Vergleich verschiedener Capture Technologien
- ▶ bwNET Umfrage – bitte ausfüllen



Benjamin Steinert, Gabriel Paradzik, Heinrich Abele
Zentrum für Datenverarbeitung
Universität Tübingen

{vorname.nachname}@uni-tuebingen.de

VIELEN DANK!

FRAGEN?





WERBUNG



- ▶ Was?
 - Linuxtag mit Vorträgen, Workshops, Messeständen, Bewirtung
- ▶ Wann?
 - 05. Juli 2025 ab 9:30 Uhr
- ▶ Wo?
 - Sand 14, 72076 Tübingen, Web: tuebix.org