easybell

Willkommen zur easybell Webinarserie!

Wireshark: Traces erstellen und auswerten

easybell

Wireshark: Traces erstellen und auswerten

Heutige Themen

- Wie lassen sich Traces erstellen? (3CX, FRITZ!Box, TCP-Dump)
- Wireshark vorbereiten
- VoIP-Auswertung (SIP und RTP)
- Hilfreiche Filter

easybell

Wireshark: Traces erstellen und auswerten

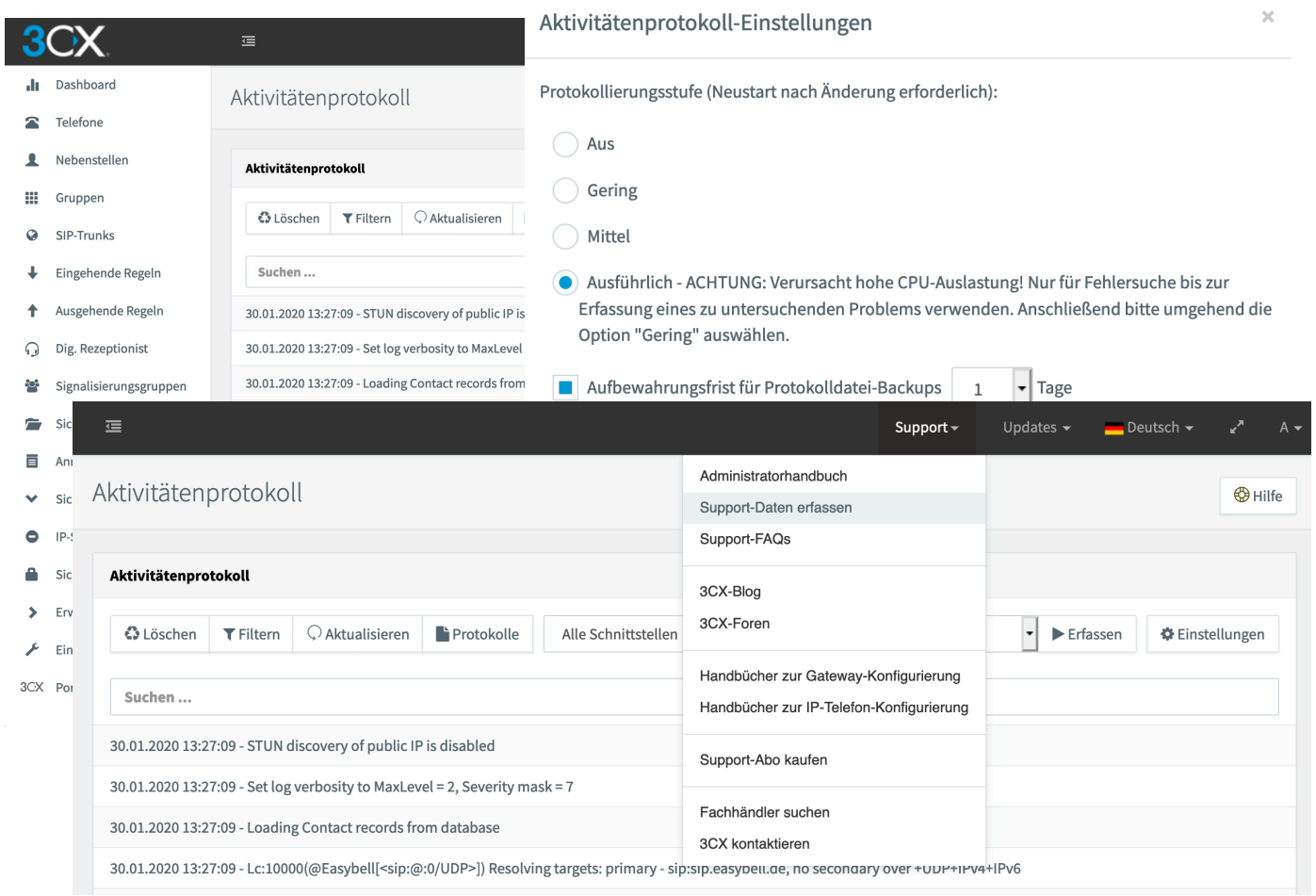
Woher kommen die Traces?

- 3CX: Support-Daten Paket
- AVM FRITZ!Box: .../html/capture.html
- TCP-Dump: SSH Verbindung -> tcpdump

Wireshark: Traces erstellen und auswerten

3CX - Telefonanlage

- Aktivitätenprotokoll
- Debuglevel
- Trace starten/stoppen
- Support-Daten herunterladen

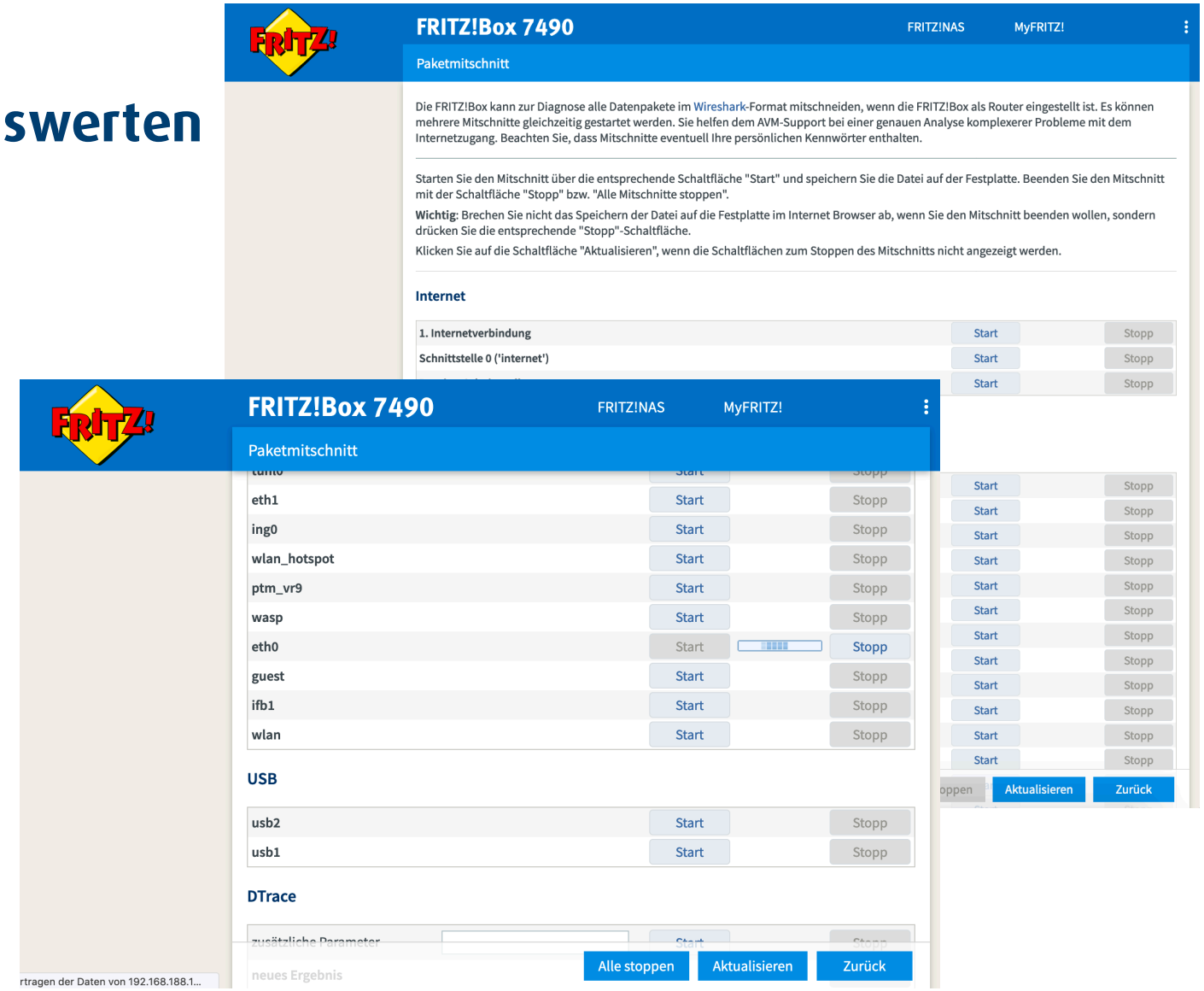


easybell

Wireshark: Traces erstellen und auswerten

AVM FRITZ!Box

- [IP.der.FRITZ.Box]/html/capture.html
- Schnittstelle auswählen
- Trace starten/stoppen
- Trace herunterladen



easybell

Wireshark: Traces erstellen und auswerten

TCP-Dump

```
Linux ce3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64
System information as of: Thu Jan 30 13:15:30 CET 2020

System load:    0.16    Memory usage:   51.4%
Usage on /:     18%     Swap usage:     0.0%
Local users:    0


The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 29 17:43:00 2020 from 192.168.251.2
root@ce3:~# tcpdump -i any host 212.123.123.123 -w meintrace.pcap
```

- Zugriff auf Zielsystem
- SSH-Verbindung (Putty/Terminal)
- tcpdump -w /tmp/**meintrace.pcap** -i **[gewünschte Schnittstelle]**

  tcpdump -i any host **[IP.des.gewünschten.Host]** -w **meintrace.pcap**

  strg + c
- Trace herunterladen (direkter Download, scp, ...)

easybell

Wireshark: Traces erstellen und auswerten

Wireshark vorbereiten

- Wireshark herunterladen: www.wireshark.org
- Installation
- Anpassung der Ansicht

easybell

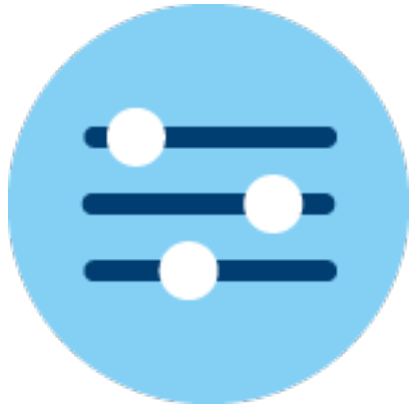
Wireshark: Traces erstellen und auswerten

VoIP-Auswertung

- Interessante Inhalte für SIP
- Interessante Inhalte für RTP

easybell

Wireshark: Traces erstellen und auswerten



Filter

- sip > Anzeige aller SIP-Pakete
- rtp > Anzeige aller RTP-Pakete
- ip.addr==192.123.123.123 > Zeigt alle Pakete von und zu 192.123.123.123 an
- sip.CSeq.method==REGISTER > Zeigt alle REGISTER Pakete an (INVITE, SUBSCRIBE,...)

Wie geht es weiter?

Nächster Webinartermin

- Voraussichtlich am Donnerstag, dem 5. März ab 14:00
- Infos folgen unter easybell.de/business/webinare und im Newsletter

Bei Fragen und Anregungen

Kontaktieren Sie uns!

webinare@easybell.de

easybell

Vielen Dank für Ihre Aufmerksamkeit!