



Willkommen zur easybell Webinarserie!

Wireshark: Traces erstellen und auswerten

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



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

The screenshot displays the 3CX web interface. On the left, a navigation menu includes: Dashboard, Telefone, Nebenstellen, Gruppen, SIP-Trunks, Eingehende Regeln, Ausgehende Regeln, Dig. Rezeptionist, and Signalisierungsgruppen. The main content area is titled 'Aktivitätenprotokoll' and contains a search bar, buttons for 'Löschen', 'Filtern', and 'Aktualisieren', and a list of log entries. The entries include: '30.01.2020 13:27:09 - STUN discovery of public IP is', '30.01.2020 13:27:09 - Set log verbosity to MaxLevel', and '30.01.2020 13:27:09 - Loading Contact records from'. A 'Support' dropdown menu is open, showing options like 'Administratorhandbuch', 'Support-Daten erfassen', 'Support-FAQs', '3CX-Blog', '3CX-Foren', 'Handbücher zur Gateway-Konfigurierung', 'Handbücher zur IP-Telefon-Konfigurierung', 'Support-Abo kaufen', 'Fachhändler suchen', and '3CX kontaktieren'. On the right, the 'Aktivitätenprotokoll-Einstellungen' dialog is visible, showing the 'Protokollierungsstufe' (Logging level) set to 'Ausführlich' (Verbose) with a warning: 'Ausführlich - ACHTUNG: Verursacht hohe CPU-Auslastung! Nur für Fehlersuche bis zur Erfassung eines zu untersuchenden Problems verwenden. Anschließend bitte umgehend die Option "Gering" auswählen.' (Verbose - WARNING: Causes high CPU load! Only for troubleshooting until the problem is captured. Then please immediately select the 'Gering' option.) The 'Aufbewahrungsfrist für Protokolldatei-Backups' (Retention period for log file backups) is set to 1 day.

Wireshark: Traces erstellen und auswerten

AVM FRITZ!Box

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

FRITZ! FRITZ!Box 7490 FRITZ!NAS MyFRITZ!

Paketmitschnitt

Die FRITZ!Box kann zur Diagnose alle Datenpakete im Wireshark-Format mitschneiden, wenn die FRITZ!Box als Router eingestellt ist. Es können mehrere Mitschnitte gleichzeitig gestartet werden. Sie helfen dem AVM-Support bei einer genauen Analyse komplexerer Probleme mit dem Internetzugang. Beachten Sie, dass Mitschnitte eventuell Ihre persönlichen Kennwörter enthalten.

Starten Sie den Mitschnitt über die entsprechende Schaltfläche "Start" und speichern Sie die Datei auf der Festplatte. Beenden Sie den Mitschnitt mit der Schaltfläche "Stopp" bzw. "Alle Mitschnitte stoppen".

Wichtig: Brechen Sie nicht das Speichern der Datei auf die Festplatte im Internet Browser ab, wenn Sie den Mitschnitt beenden wollen, sondern drücken Sie die entsprechende "Stopp"-Schaltfläche.

Klicken Sie auf die Schaltfläche "Aktualisieren", wenn die Schaltflächen zum Stoppen des Mitschnitts nicht angezeigt werden.

Internet

1. Internetverbindung	Start	Stopp
Schnittstelle 0 ('internet')	Start	Stopp
	Start	Stopp

FRITZ! FRITZ!Box 7490 FRITZ!NAS MyFRITZ!

Paketmitschnitt

eth0	Start	Stopp
eth1	Start	Stopp
ing0	Start	Stopp
wlan_hotspot	Start	Stopp
ptm_vr9	Start	Stopp
wasp	Start	Stopp
eth0	Start	Stopp
guest	Start	Stopp
ifb1	Start	Stopp
wlan	Start	Stopp

USB

usb2	Start	Stopp
usb1	Start	Stopp

DTrace

zusätzliche Parameter: Start Stopp

neues Ergebnis

Alle stoppen Aktualisieren Zurück

Wireshark: Traces erstellen und auswerten

TCP-Dump

- 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, ...)

```
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
```

Wireshark: Traces erstellen und auswerten

Wireshark vorbereiten

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



Wireshark: Traces erstellen und auswerten

VoIP-Auswertung

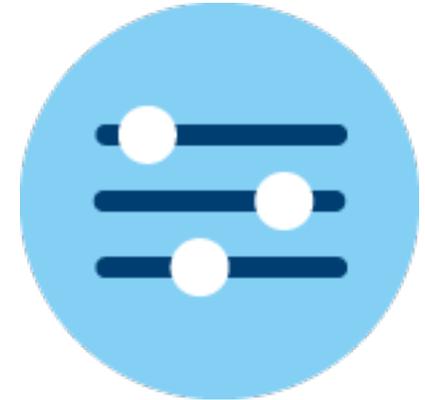
- Interessante Inhalte für SIP
- Interessante Inhalte für RTP



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



Vielen Dank für Ihre Aufmerksamkeit!