WIRE**SHARK Newsletter Januar 2020**

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie regelmässig über Neuerungen im Zusammenhang mit dem Open Source Analyzer Wireshark und weiteren Netzwerkanalyse-Produkten.

Schlagzeilen:

- Neue Funktionen ab **Wireshark Version 3.2x**
- Driver Vergleich: **Npcap** versus **WinPcap**
- **Wireshark für WLAN** unter Windows (mit Npcap)
- Gigabit Capturing mit **Raspberry Pi 4**
- Leistungsmessungen Raspberry Pi 4 mit **Wireshark** oder **TShark**
- Anwendungsbeispiel: **VoIP Fernaufzeichnung** mit Raspberry 4
- Heise-Verlag Raspberry Projekt: **c't-Raspion** für WLAN-Analyse
- **TShark** und **Editcap** Funktionen
- Wireshark's **TCP Expert Meldungen**
- Kurshinweise

Neue Funktionen ab Wireshark Version 3.2x

In der Wireshark Version 3 wurden wieder zahlreiche neue Funktionen implementiert. Zu viele, um diese hier alle erklären zu können.

Diese Vorstellung beschränkt sich deshalb auf die wichtigsten Neuerungen in der GUI Bedienung.

Sämtliche neuen Details finden Sie unter www.wireshark.org/news/ oder in den Release Notes unter www.wireshark.org/docs/relnotes/

Dies ist auch die letzte Version, welche noch Windows 7 und Windows Server 2008 R2 unterstützt.

Komfortablere GUI Bedienung durch folgende neuen Funktionen:

- Drag & Drop für **Display Filter**
- Drag & Drop für zusätzliche **Spalten**

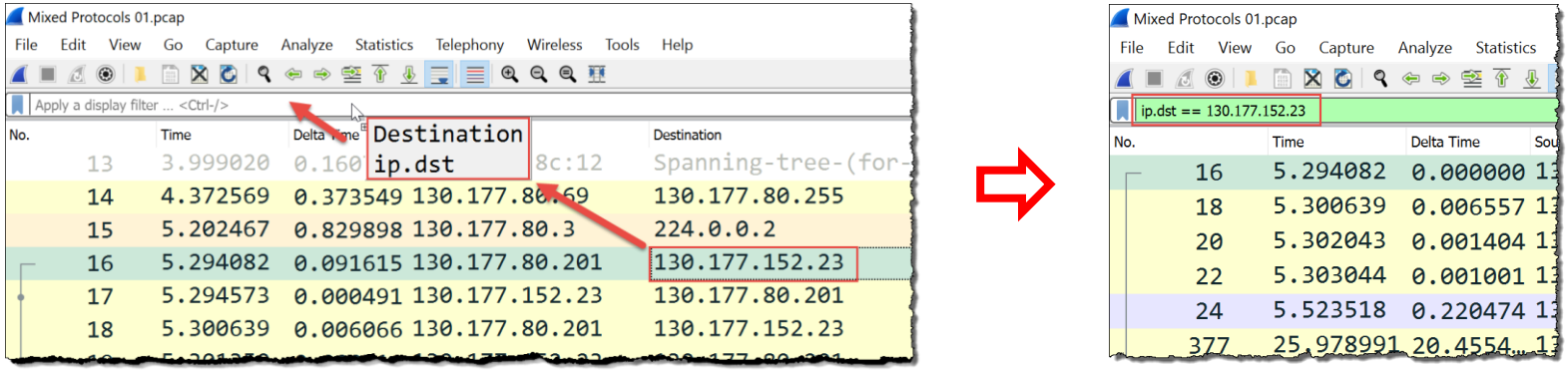
} unbedingt ausprobieren 

- **Mittlere Maustaste** zum Markieren von Paketen
- Anwählen von **mehreren** Paketen
- Export von markierten oder angewählten Paketen

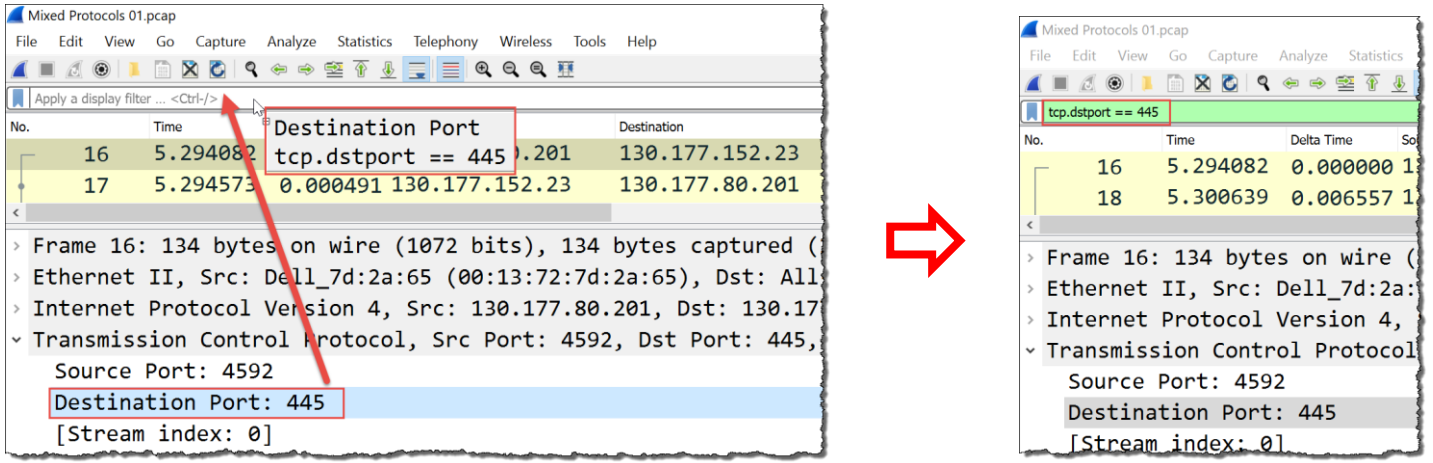
Neue Funktionen ab Wireshark Version 3.2x

Drag & Drop für **Display Filter**

- Felder aus dem **Packet List** Fenster können durch Halten der linken Maustaste in die Display Filter Zeile kopiert werden. Ausnahme: Protocol und Info Spalte (dies sind Zusammenfassungen)



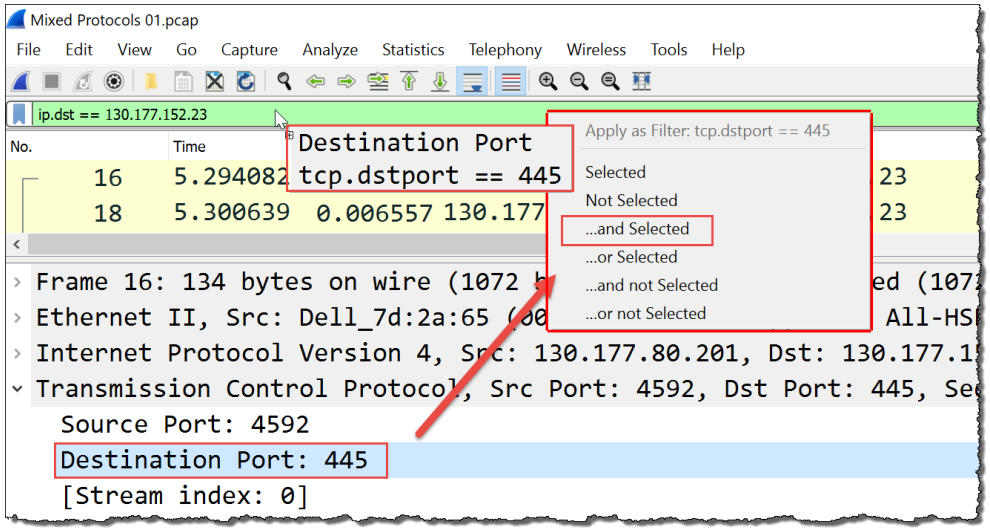
- Auch Felder aus dem **Packet Details** Fenster können in die Display Filter Zeile kopiert werden.

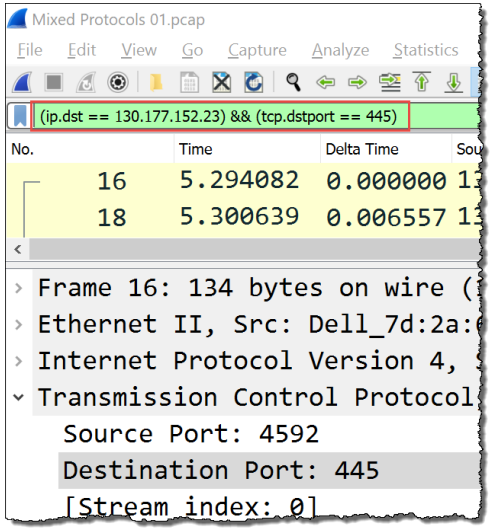


Neue Funktionen ab Wireshark Version 3.2x

Drag & Drop für **Display Filter**

- Ist bereits ein Filter aktiv, kann dieser nach Wahl entweder ergänzt oder ersetzt werden



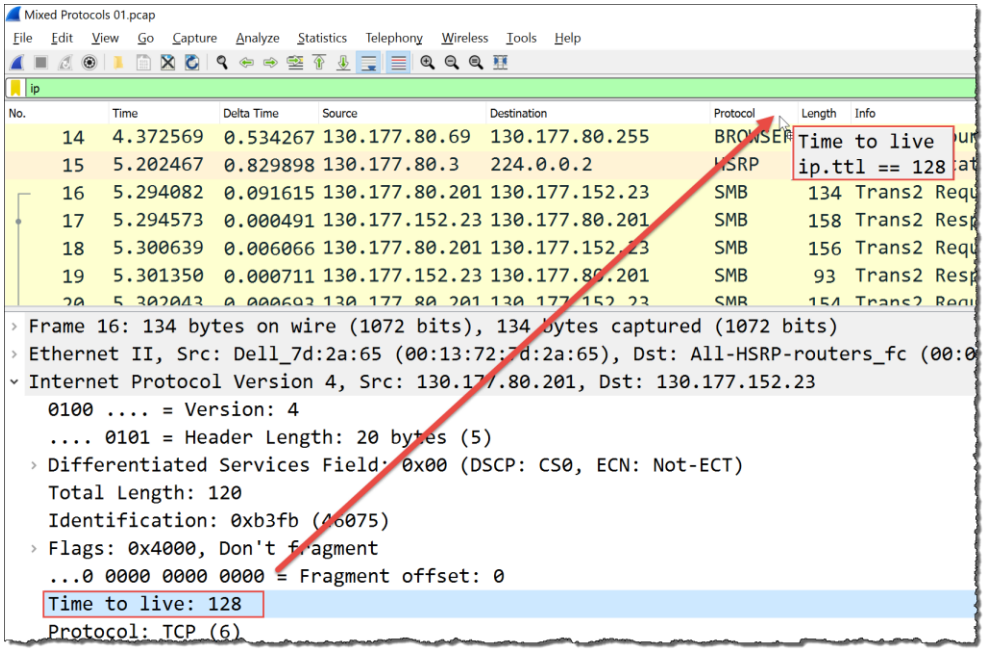


Anmerkung: Leider enthält die Version 3.2 noch einige Bugs; z.B. die in unseren TCP/IP Kursen häufig verwendete grafische Darstellung einer TCP Session unter → Statistics → TCP Stream Graphs → Time Sequence (tcptrace) zeigt keine Datenpakete! 🙁 Den Fehler habe ich in der Wireshark Bug Database unter Bug 16281 bereits gemeldet.

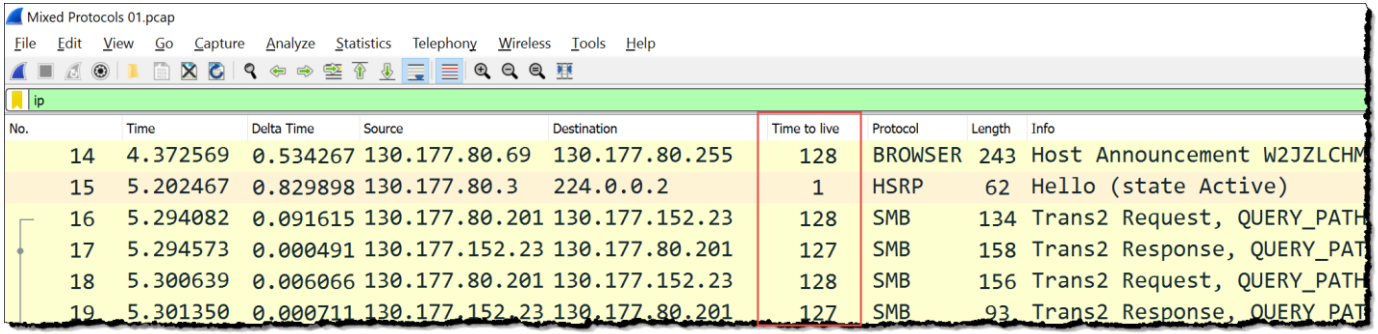
Neue Funktionen ab Wireshark Version 3.2x

Drag & Drop für **zusätzliche Spalten**

- Zusätzlich Spalten (Columns) können neu auch mit Drag & Drop eingefügt werden



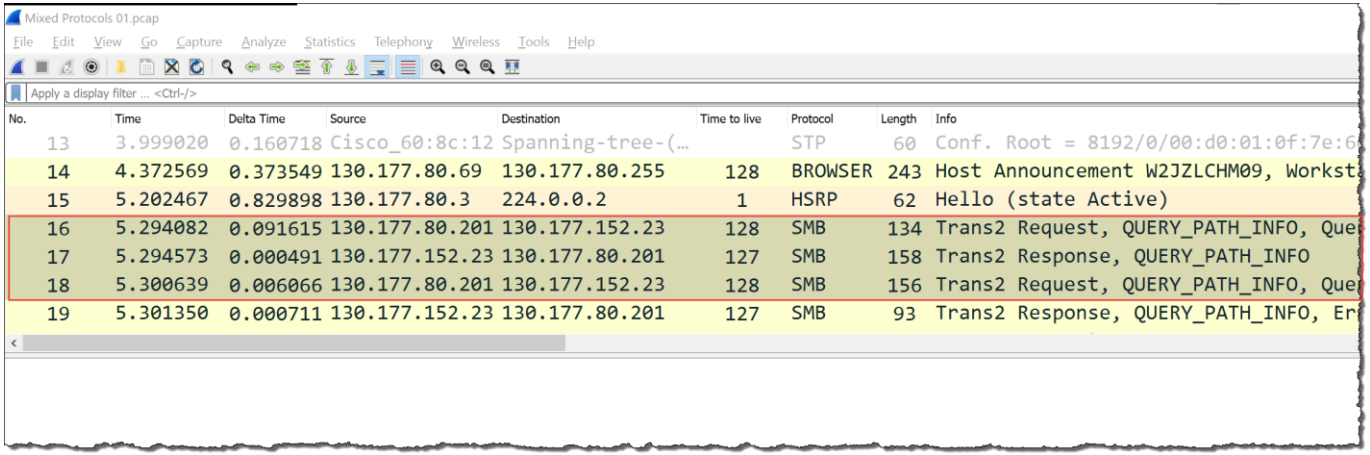
- Das neu als Spalte gewünschte Feld mit gehaltener linken Maustaste auf eine bestehende Spaltenüberschrift ziehen und loslassen.
- Die neue Spalte wird links von der angewählten Spalte eingefügt.



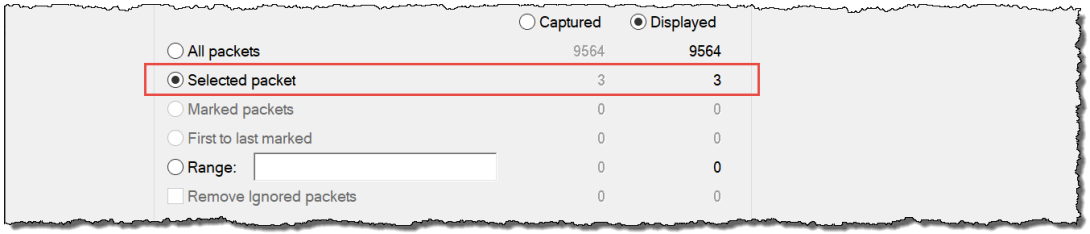
Neue Funktionen ab Wireshark Version 3.2x

Markieren oder Auswählen von Paketen

- Nicht neu ist, dass Pakete schwarz **markiert** und wieder **unmarkiert** werden können; bisher durch rechten Mausklick auf ein Paket. Neu kann dies direkt mit der mittleren Maustaste erfolgen.
- Bisher konnte nur ein Paket **angewählt** werden (mit der linken Maustaste), neu können durch zusätzliches Halten der Shift- oder Ctrl-Taste beliebig viele Pakete angewählt werden.
- Sobald mehr als ein Paket angewählt wird, bleiben Packet Details und Packet Bytes Fenster leer.



- Speichern der angewählten (oder markierten) Pakete unter → File → Export Specified Packets…

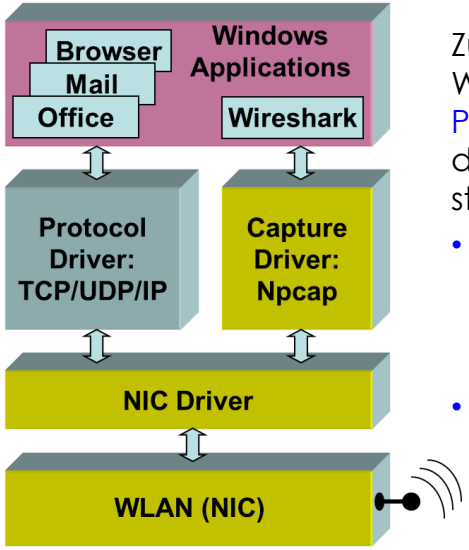


Vergleich Npcap (neu) gegen WinPcap (alt)

Zur Aufzeichnung im Promiscuous Mode braucht Wireshark einen speziellen Driver. Seit Beginn wurde der Open Source Driver WinPcap verwendet. Da dieser nicht mehr unterstützt wurde, wird ab Wireshark Version 3 der Open Source Driver Npcap mitgeliefert.

Dies hat auf die Funktion von Wireshark mit Ethernet keinen Einfluss, es werden jedoch **neu auch einige interne WLAN Adapter** unter Windows unterstützt.

Auf den nächsten Seiten wird erklärt, welche Adapter unterstützt sind und wie die Installation funktioniert.



Zur Aufzeichnung muss ein WLAN Adapter sowohl den Promiscuous Mode als auch den Monitor Mode unterstützen.

- Promiscuous Mode zeigt auch die Datenpakete von anderen Mobile Clients in derselben Funkzelle
- Monitor Mode zeigt auch die Management- und Control-Pakete (wichtig für die WLAN Analyse)

Feature	Npcap	WinPcap
Info		
Actively maintained and supported	Yes	No (WinPcap development was terminated)
Last release date	July 30, 2019	March 8, 2013
libpcap version	1.9.0 (2019)	1.0.0 (2008)
License	Free for personal use	BSD-style
Supported commercial/redistributable version	Yes (Npcap OEM)	No (WinPcap Professional product terminated)
Security		
EV SHA-256 code signing	Yes	No
Limit access to administrators (optional)	Yes	No
Basic features		
Packet capture with the cross-platform libpcap API	Yes	Yes
Link-layer packet injection	Yes	Yes
Source code available	Yes (Link)	Yes (Link)
Advanced Features		
Capture raw 802.11 frames	Yes, with many widely-available adapters	Yes, with specialized AirPcap hardware
Capture Loopback traffic	Yes	No
Inject Loopback traffic	Yes	No

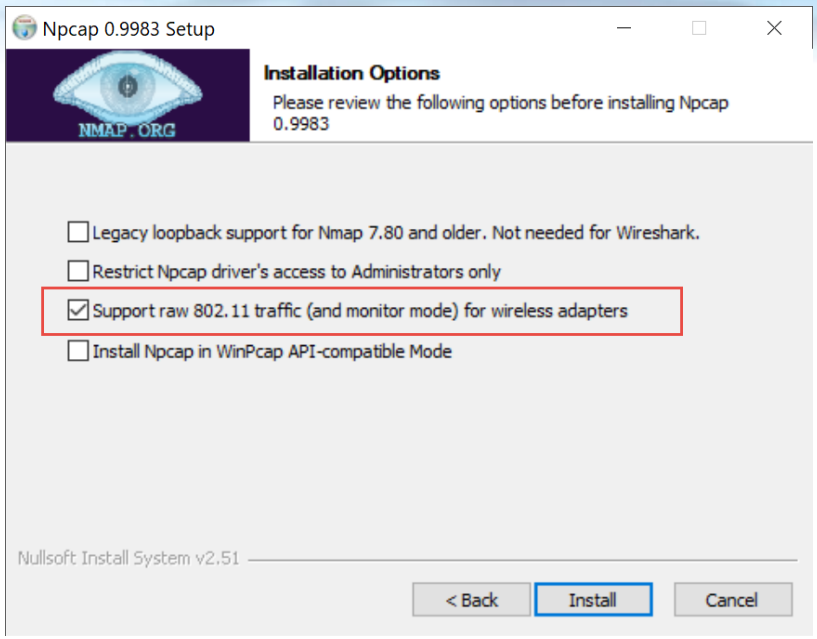
Quelle: https://nmap.org/npcap/vs-winpcap.html

Wireshark für WLAN unter Windows (mit Npcap)

Npcap Installation und Erkennung des WLAN Interfaces

Installation von Npcap

- Die aktuellste Version von Npcap runterladen von https://nmap.org/npcap/ (aktuell 0.9986)
- Neue Npcap Version über die alte installieren (Wireshark muss nicht neu installiert werden)
- Beim Installieren von Npcap muss die Option 802.11 (WLAN) aktiviert werden →



Version des eingebauten WLAN herausfinden:

- Im CMD Window in die Npcap Directory wechseln und den unten genannten Befehl eingeben
- Den Schnittstellennamen merken (z.B. "WLAN")
- Weitere Schritte auf nächster Seite…

```
C:\WINDOWS\System32\Npcap>netsh interface show interface

Verw.-status    Status          Typ             Schnittstellenname
-------------------------------------------------------------------------
Aktiviert       Getrennt        Dediziert       WLAN
Deaktiviert     Getrennt        Dediziert       Ethernet 6
Deaktiviert     Getrennt        Dediziert       Ethernet 7
Aktiviert       Verbunden       Dediziert       VirtualBox Host-Only Network
Aktiviert       Verbunden       Dediziert       Ethernet 3
```

Wireshark für WLAN unter Windows (mit Npcap)

WLAN Adapter Typ auf Monitor Mode Unterstützung prüfen

```
C:\WINDOWS\System32\Npcap>netsh WLAN show interface

Es ist 1 Schnittstelle auf dem System vorhanden:

    Name                   : WLAN
    Beschreibung           : Intel(R) Dual Band Wireless-AC 7260
    GUID                   : 3bb55b86-3518-4db3-9d54-[illegible]891bbb147b
    Physische Adresse      : 7c:7a:91:79:46:04
    Status                 : Verbunden
    SSID                   : LNS WLAN
    BSSID                  : 20:c9:d0:a9:3b:31
    Netzwerktyp            : Infrastruktur
    Funktyp                : 802.11n
    Authentifizierung      : WPA2-Personal
    Verschlüsselung        : CCMP
    Verbindungsmodus       : Profil
    Kanal                  : 36
    Empfangsrate (MBit/s)  : 300
    Übertragungsrate (MBit/s) : 300
    Signal                 : 90%
    Profil                 : LNS WLAN
```

Ev. “WLAN” durch den Namen ihres Wireless Adapters ersetzen

Adapter Typ mit untenstehendem Link auf Monitor Mode Unterstützung prüfen

Resultat: dieser Adapter unterstützt **kein** Monitor Mode!

Liste von Wireless Adaptern: https://secwiki.org/w/Npcap/WiFi_adapters

Wireshark für WLAN unter Windows (mit Npcap)

Konfiguration für Wireless Adapter, welche den Monitor Mode unterstützen

```
C:\WINDOWS\System32\Npcap>wlanhelper WLAN mode monitor
Success

C:\WINDOWS\System32\Npcap>wlanhelper WLAN channel 11
Success

→ Nach der Aufzeichnung nicht vergessen:
C:\WINDOWS\System32\Npcap>wlanhelper WLAN mode managed
Success

→ Zeigt alle verfügbaren Optionen
C:\WINDOWS\System32\Npcap>wlanhelper -h
```

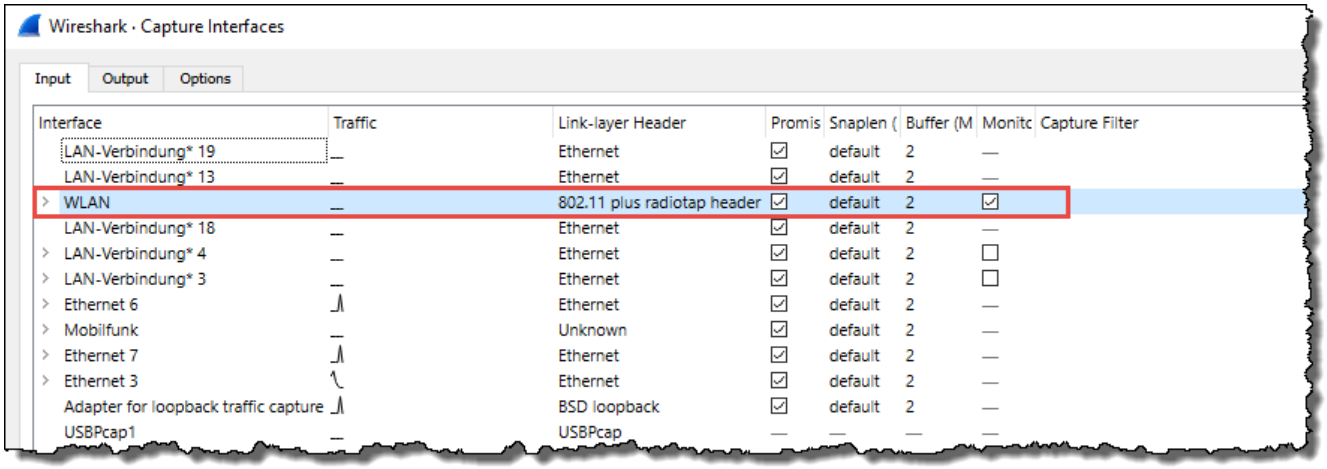
Setze Adapter in **Monitor Mode***

Wähle WLAN **Kanal Nummer**

Setze Adapter **zurück in Operation**

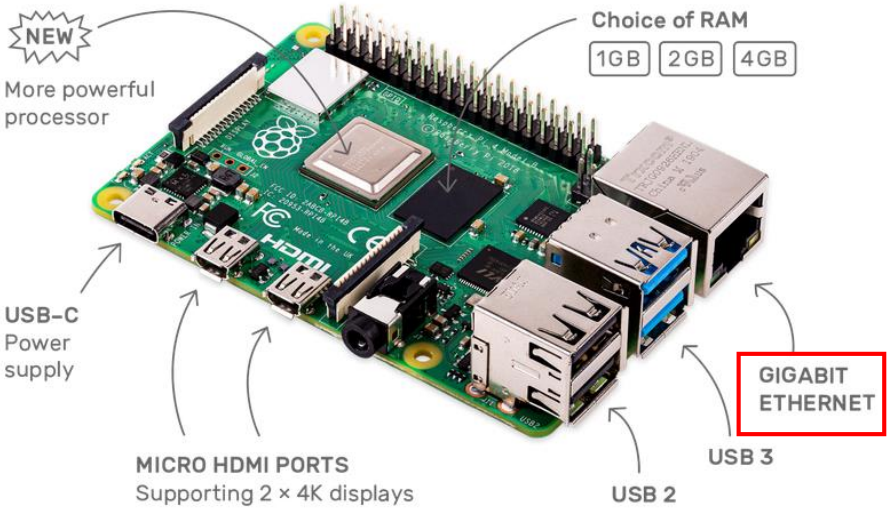
* Ein WLAN in Monitor Mode ist passiv und vom Access-Point getrennt.

- Wireshark aufstarten und Monitor Mode verifizieren
- Wireshark Aufzeichnung starten
- Es sollten z.B. Beacon Pakete sichtbar sein



Gigabit Capturing mit Raspberry Pi 4

Neue Spezifikationen



Quelle: www.raspberrypi.org

- System-on-a-Chip (SOC) BCM211 von Broadcom
- Speicher-Grössen: 1, 2 oder 4 GB RAM
- 2 Micro-HDMI-Ausgänge zur Verfügung (neu HDMI 2.0 statt HDMI 1.4)
- Auflösung bis 4K bei 60 Hz unterstützt (4K bei 60 Hz plus 1080p oder zweimal 4K bei 30 Hz möglich)
- 4 Kerne vom Typ Cortex A-72 getaktet mit 1.5 GHz
- GPU vom Typ VideoCore VI (VC6, 500 MHz), die 4K-Wiedergabe ermöglicht
- Stromanschluss neu via USB-C (3A, 5V)
- 2 × USB 2.0 Typ A
- 2 × USB 3.0 Typ A (Raspi 3 B+ hatte nur 4 × USB 2.0)
- 2.4 GHz und 5.0 GHz IEEE 802.11ac WLAN
- 1 × Gigabit Ethernet RJ45
- Bluetooth 5.0, BLE (Raspi 3 B+: Bluetooth 4.2)
- die GPIO-Pins sind abwärtskompatibel

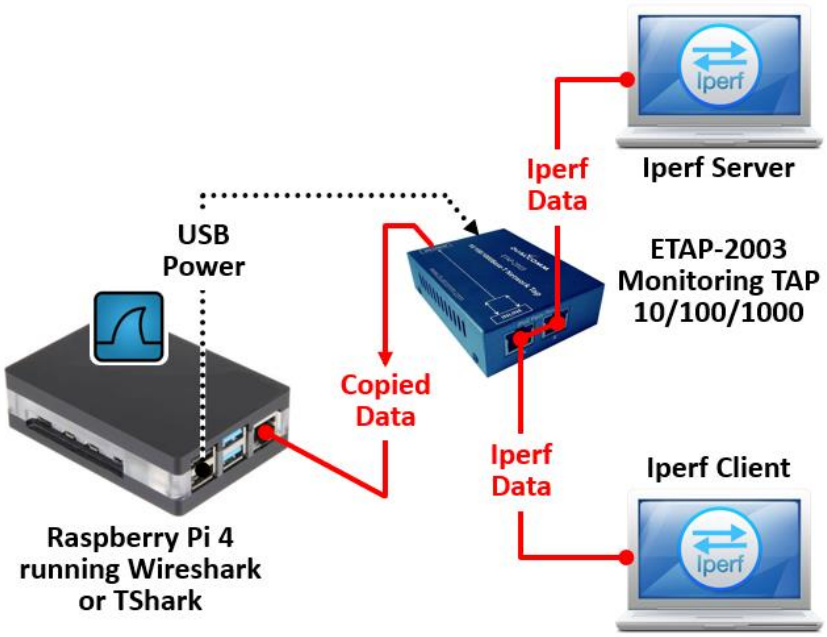
Anmerkungen:

- Die gesteigerte Leistung bewirkt auch einen höheren Strombedarf. Abhängig von den angeschlossenen Peripheriegeräten ist ev. ein neues Netzgerät erforderlich (rote LED blinkt, wenn zu wenig Power!)
- Bedingt durch die neuen Anschlüsse ist das Gehäuse nicht mit älteren Raspberry Gehäusen kompatibel.

Gigabit Capturing mit Raspberry Pi 4

Leistungsmessungen

- Ziel ist die max. Aufzeichnungsrate vom Raspi 4 zu testen, d.h. ab welcher Durchsatzrate Pakete verloren gehen.
- Dazu wird das anerkannte Tool **Iperf 3** verwendet, welches wir im letzten Newsletter Feb. 19 vorgestellt haben.



Anmerkungen:

- Der TAP ETAP-2003 ist ein Aggregation TAP, d.h. die Summe der Daten in beide Richtungen darf total 1 Gigabit/sec nicht überschreiten.
- Dies hat keinen Einfluss auf die Raspi 4 Messung, da dessen Aufzeichnungsrate weit unter 1 Gbit/s liegt.
- Gemessen wurde mit Wireshark Buffer von 100 MB und Paketgrössen von 1500 Bytes.
- Der Raspi 4 wird durch die gesteigerte CPU-Leistung relativ warm, als Alternative wurde auch mit aktiver Kühlung (Gehäuse mit Lüfter) gemessen.

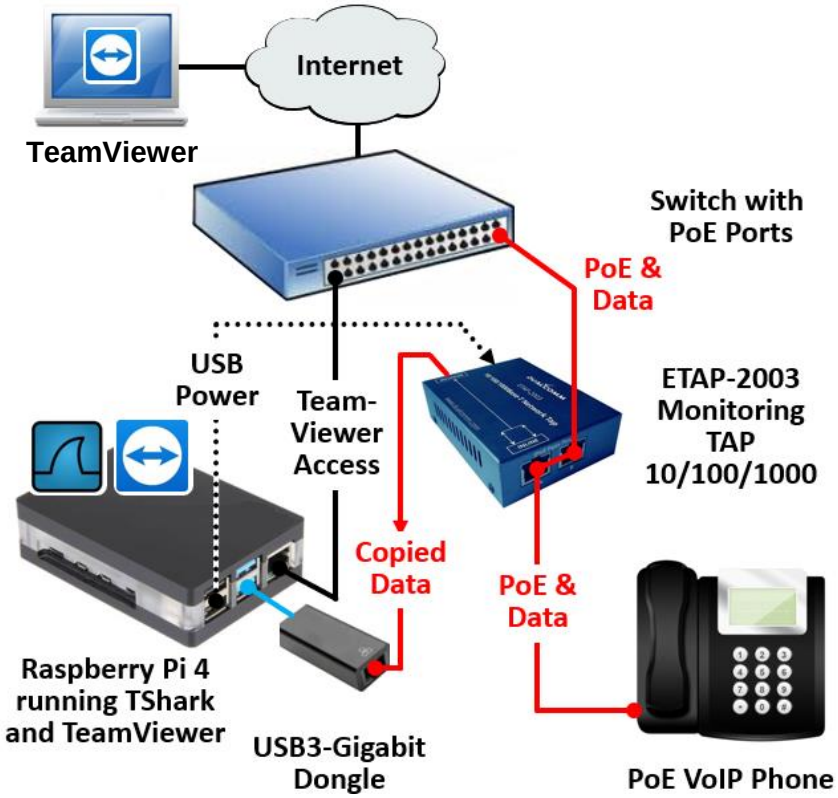
Messresultate:

- Der Raspi 4 (mit 4GB RAM) vermag Datenraten bis zu **80Mbit/s ohne Paketverlust** aufzuzeichnen.
- Derselbe Wert gilt sowohl bei der Aufzeichnung mit Wireshark als auch TShark.
- CPU Belastung mit Wireshark: ca. 15%
- Temperatur mit passiver Kühlung: bis 70° C
- Temperatur mit aktiver Kühlung: bis 40° C
- CPU Belastung mit TShark: ca. 3%

Gigabit Capturing mit Raspberry Pi 4

Anwendungsbeispiel: VoIP Aufzeichnungen

Die Firma Dreikom AG setzt Raspberry Pi 4 erfolgreich für die Fernaufzeichnung bei VoIP-Problemen ein. Erich Roth, Mitinhaber und Leiter Technik hat mehrere Raspi 4 beschafft und installiert diese zusammen mit unserem Monitoring TAP ETAP-2003 bei Bedarf in Kundennetzwerken. Der Fernzugriff über TeamViewer ermöglicht das Konfigurieren sowie das Abgreifen von Capture Files.



Raspberry Pi 4 mit USB3-Ethernet Dongle (oder über WLAN) als zweites Interface: eines für Capturing, das zweite für TeamViewer Zugriff

Vorteile

- Kostengünstig, mehrere Raspi können dadurch an verschiedenen Messpunkten installiert werden
- Remote Konfiguration und pcap File Abgriff
- Long Term Capturing (für die Aufzeichnung von nur sporadisch auftretenden Problemen)
- NTP für Zeitsynchronisation
- TShark empfohlen (geringe CPU Last, d.h. weniger Abwärme)

Voraussetzung

- Braucht Internet Zugriff für TeamViewer Zugriff.

Heise-Verlag Raspberry Projekt

Anwendungsbeispiel: c't-Raspion für WLAN Analyse

Im Heise c't Magazin 1/2020 wird beschrieben, wie mit einem Raspi 3 oder 4 auch WLAN Verkehr aufgezeichnet werden kann.

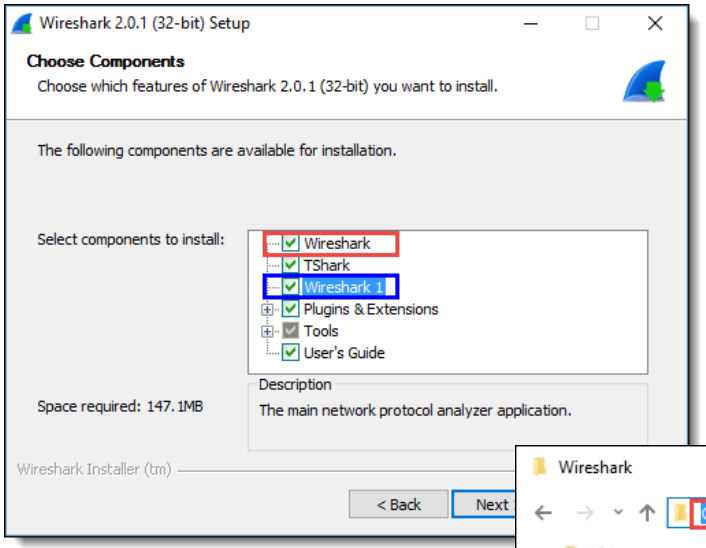
Der c't-Raspion bildet dazu ein eigenes WLAN, in dem die zu beobachteten Geräte "eingebucht" sein müssen. Mit einem zusätzlichen USB-Ethernet-Dongle lassen sich auch kabelgebundene Geräte in Augenschein nehmen.

Damit der c't-Raspion diesen Adapter erkennen und korrekt einbinden kann, muss er beim Einschalten des Raspberry Pi bereits angeschlossen und aktiv sein. Mehr Informationen unter obigem Link.

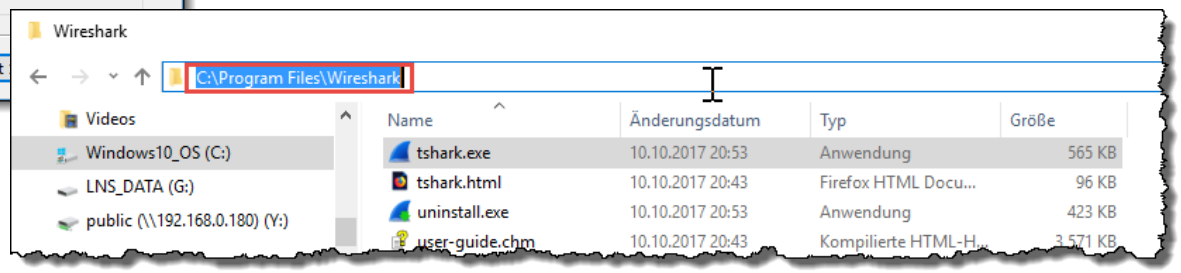
Quelle:
https://www.heise.de

TShark Installation und Konfiguration

- TShark, Terminal basierende Version von Wireshark zum Aufzeichnen von Netzwerkdaten
- Kommt zum Einsatz, wenn eine grafische Oberfläche (GUI) nicht nötig oder nicht verfügbar ist
- Lässt sich mit weiteren Shell-Tools verknüpfen - ermöglicht es, die Ausgabe weiterzuverarbeiten.
- TShark kann grosse Files vorfiltern, bevor diese mit Wireshark geöffnet werden
- Detaillierte Infos www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html



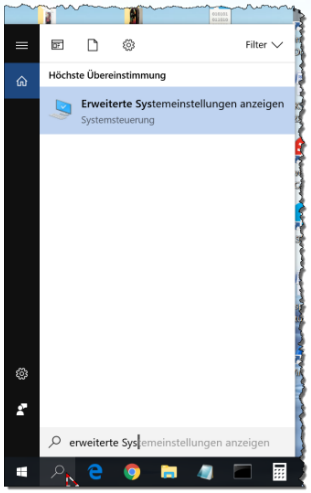
TShark wird nach entsprechender Auswahl im Startmenu zusammen mit Wireshark installiert ←



- Weitere Tools wie Editcap.exe, Mergecap.exe usw. befinden sich im selben Ordner

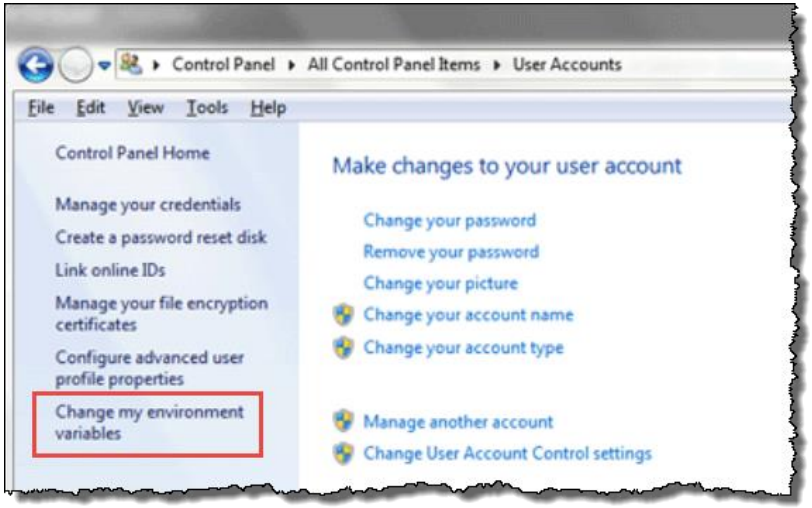
TShark Installation und Konfiguration

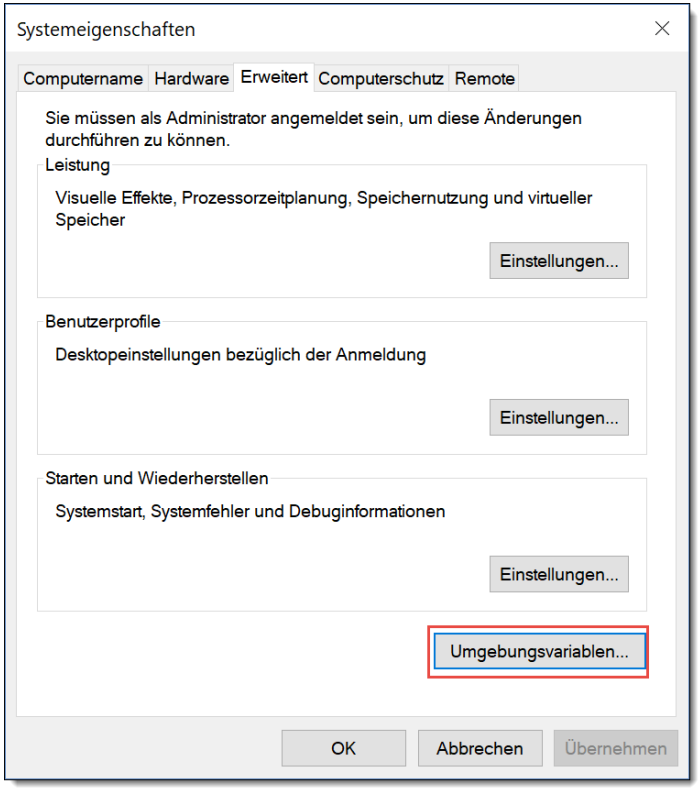
- Zum direkten Start von TShark, Editcap, Mergecap etc. können die Umgebungs-variablen des Betriebssystems ergänzt werden.



Bei Windows 10 unter:
Erweiterte Systemeinstellungen

Bei Windows 7 unter:
Benutzerkonten

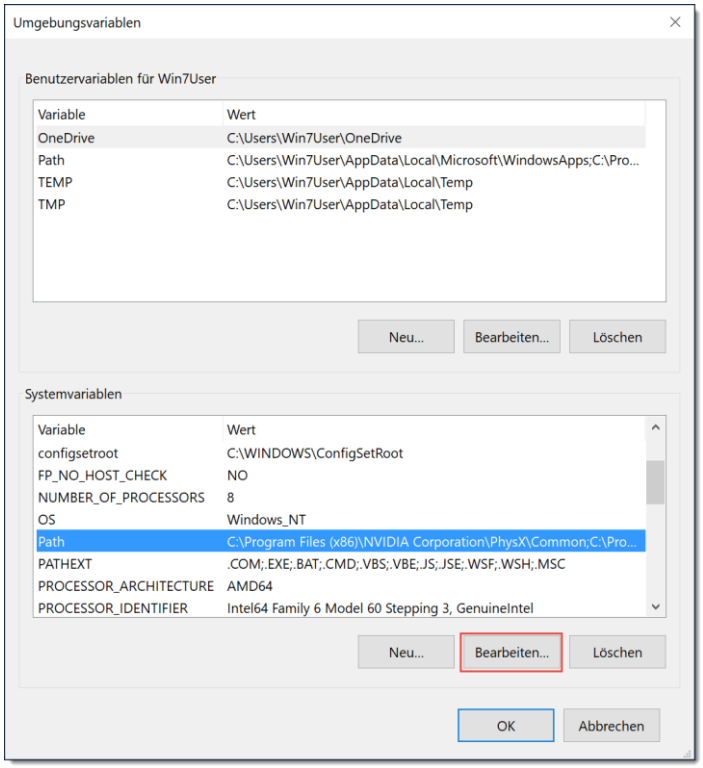




Umgebungsvariablen hier ändern

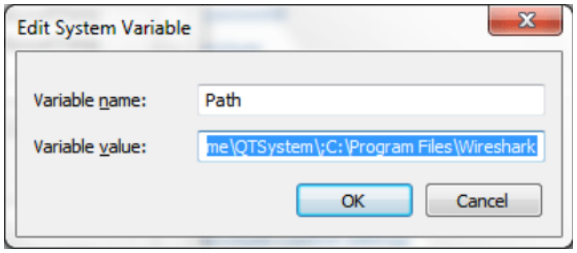
TShark Installation und Konfiguration

- Zum direkten Start von TShark können die Umgebungsvariablen ergänzt werden



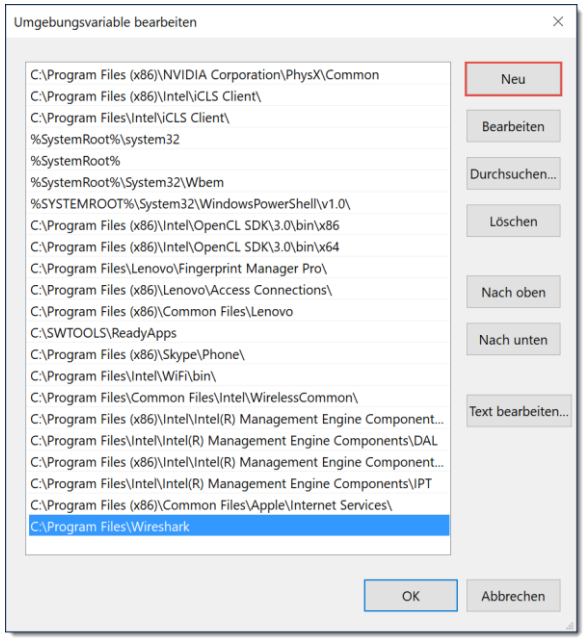
Bearbeiten der Path Einstellungen

Windows 7



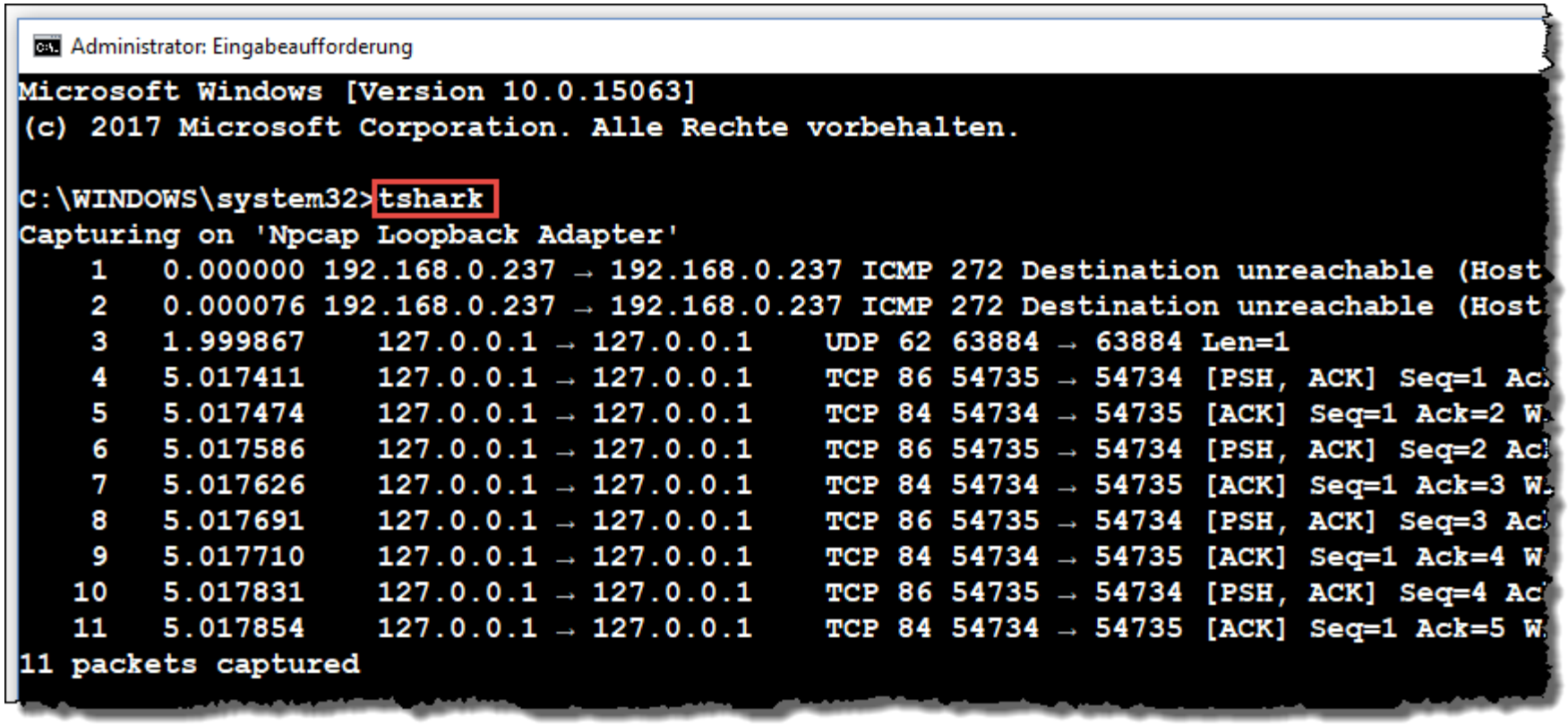
Eintragen der Path Information für den Wireshark Ordner

Windows 10



TShark Bedienung und Optionen

- Eingabe von tshark startet die Aufzeichnung, Ctrl C beendet die Aufzeichnung
- Ohne Befehlsoptionen zeigt TShark im CMD-Fenster eine Zeile pro Paket vom ersten internen Interface. Die Daten werden nur angezeigt, nicht abgespeichert.



TShark Bedienung und Optionen

- Die Option tshark -D listet die vorhanden Interfaces mit Nummer und Beschreibung

```
C:\WINDOWS\system32>tshark -D
1. \Device\NPF_{1325071B-18CB-4758-800B-EAFFD4BADED0} (Npcap Loopback Adapter)
2. \Device\NPF_{A03331E1-952B-464E-8874-FF47FDE7378E} (LAN-Verbindung* 11)
3. \Device\NPF_{3BB55B86-3518-4DB3-9D54-65891BBB147B} (WLAN)
4. \Device\NPF_{6B6D9894-C04A-4542-929C-E58813EAF5E2} (LAN-Verbindung* 12)
5. \Device\NPF_{D1685201-8506-4019-809D-418AFC8A1416} (Mobilfunk)
6. \Device\NPF_{7D916E10-B400-4051-9741-B0336F901267} (Ethernet 3)
7. \\.\USBPcap1 (USBPcap1)
8. \\.\USBPcap2 (USBPcap2)
9. \\.\USBPcap3 (USBPcap3)
```

- Mit Option tshark -i 6 werden Daten vom Interface Nr. 6 (Ethernet 3) angezeigt

```
C:\WINDOWS\system32>tshark -i 6
Capturing on 'Ethernet 3'
    1   0.000000 192.168.0.237 → 239.255.255.250 SSDP 484 NOTIFY * HTTP/1.1
    2   0.031464 192.168.0.237 → 239.255.255.250 SSDP 493 NOTIFY * HTTP/1.1
    3   0.115519 192.168.0.237 → 239.255.255.250 SSDP 540 NOTIFY * HTTP/1.1
    4   0.162414 192.168.0.237 → 239.255.255.250 SSDP 544 NOTIFY * HTTP/1.1
    5   0.268518 SamsungE_10:f9:28 → Broadcast    ARP 60 Who has 192.168.0.1? Tell 192.168.0.212
    6   0.299970 WistronI_62:53:65 → Broadcast    ARP 42 Who has 192.168.0.30? Tell 192.168.0.237
    7   0.300017 WistronI_62:53:65 → Broadcast    ARP 42 Who has 192.168.0.62? Tell 192.168.0.237
7 packets captured
```

TShark Bedienung und Optionen

```
tshark -i 6 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-w speichert die Daten von I/F 6 gemäss dem Pfad und dem angegeben File Namen

```
tshark -i 6 -c 100 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-c xxx stoppt die Aufzeichnung nach Erreichen der angegebenen Anzahl Pakete

```
tshark -i 6 -a duration:100 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-a duration xxx stoppt die Aufzeichnung nach der angegebenen Anzahl Sekunden

```
tshark -i 6 -a filesize:100 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-a filesize xxx stoppt die Aufzeichnung beim Erreichen der File Grösse xxx in KB

```
tshark -i 6 -b duration:100 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-b duration xxx generiert ein neues File nach der angegebenen Anzahl Sekunden

```
tshark -i 6 -b filesize:100 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-b filesize xxx generiert ein neues File nach der angegebenen Anzahl in KB

```
tshark -i 6 -b files:10 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-b files xxx Generiert einen Ringbuffer mit der angegeben Anzahl Files

```
tshark -i 6 -a files:10 -w C:\Users\Win7User\Desktop\capture01.pcapng
```

-a files xxx stoppt die Aufzeichnung beim Erreichen der angegeben Anzahl Files

Editcap Funktionen

- Editcap.exe kann aufgezeichnete pcap & pcapng Trace File verändern und bearbeiten
- Grosse Files können aufgeteilt, Pakete können gekürzt, Zeitstempel verändert werden usw.
- Detaillierte Infos unter https://www.wireshark.org/docs/man-pages/editcap.html

```
editcap -c 100000 capture_in.pcapng capture_out.pcapng
```

-c xxx teilt ein bestehendes File auf in Zielfiles mit der angegeben Anzahl Pakete

```
editcap -s 200 capture_in.pcapng capture_out.pcapng
```

-s xxx kürzt alle Pakete auf die angegeben Länge in Bytes und speichert diese im Zielfile

```
editcap -C 38 -L capture_GRE.pcapng capture_No_GRE.pcapng
```

-C xxx entfernt die angegebene Anzahl Bytes am Anfang jedes Paketes & passt die Länge an

```
editcap -C 12:4 -L capture_vlan.pcap capture_no_vlan.pcap
```

-C 12:4 -L entfernt Anzahl Bytes an einer bestimmten Position und passt die Paketlänge neu an

```
editcap -d capture_in.pcapng capture_out.pcapng
```

-d entfernt Duplikate von Paketen aufgrund übereinstimmender Länge und des MD5 Wertes

```
editcap -F snoop capture_in.pcap capture_out.snoop
```

-F xxx konvertiert das Format des Input Files in das gewählte Output Format

TCP Analyse mit dem Wireshark Expert

Wireshark Expert Meldungen

Expert Meldungen variieren je nach Messposition zwischen dem Sender und Empfänger.

Nahe beim Sender sollten folgende Meldungen nicht erscheinen: Previous segment not captured oder TCP Out-Of-Order. Wenn diese trotzdem erscheinen, besteht ev. ein TCP-Driver Problem auf dem Sender oder (viel wahrscheinlicher) beim Aufzeichnen gingen Pakete verloren.

- Previous segment not captured

Ein Daten-Paket wird mit dieser Meldung markiert, wenn dieses eine höhere Sequenznummer enthält als die als nächstes erwartete. Deutet auf Verlust von einem oder mehreren Paketen hin.

- TCP Retransmission

Dieses Paket hat eine Sequenznummer, die von Wireshark bereits aufgezeichnet wurde; die Bestätigung zu diesem Paket ist jedoch noch ausstehend.

- TCP Fast Retransmission

Ein fehlendes Paket, das nachgeliefert wurde bevor der Retransmission-Timer des Senders abgelaufen ist. Der Vorgang heisst Fast Recovery und wird vom Sender ausgelöst beim Empfang von mehreren (default 3) Duplicate ACKs. Wireshark markiert ein Paket mit TCP Fast Retransmission, wenn das letzte ACK vor weniger als 20ms erkannt wurde.

- TCP Out-Of-Order

Ein Paket mit einer Sequenznummer, welches bereits vom Empfänger bestätigt wurde.

TCP Analyse mit dem Wireshark Expert

Wireshark Expert Meldungen (Fortsetzung)

- TCP Spurious Retransmissions

Ein Paket wird als Spurious (falsch, unberechtigt, unnötig) bezeichnet, wenn dieses bereits bestätigt wurde und das SYN oder FIN Bit gesetzt ist.

- TCP Dup ACK

Ein Acknowledgement, welches von Wireshark bereits aufgezeichnet wurde, d.h. die ACK Nr. ist dieselbe wie in vorherigen ACKs. Z.B. die Meldung TCP Dup ACK 787#17 zeigt die Nummer des originalen ACKs (787) und zum wievielten Mal dasselbe ACK schon übertragen wurde (17).

TCP Dup ACKs werden vom Empfänger jedes Mal gesendet, wenn ein Paket empfangen wird, welches eine höhere Sequenznummer als die als nächstes erwartete enthält. Dies ist ein Anzeichen, dass ein oder mehrere Paket verloren gingen (siehe TCP Fast Retransmission)

- TCP ACKed unseen segment

Wireshark hat ein ACK, jedoch nicht das entsprechende Daten-Packet aufgezeichnet.

Bei der Aufzeichnung gingen ev. Pakete verloren oder sie fand an einer Multi-Link Strecke statt.

- TCP ZeroWindow

Ein Empfänger sendet diese Meldung, wenn der Eingangs-Buffer komplett voll ist und keine Daten mehr empfangen werden können. Damit wird die Übertragung blockiert (Fluss-Kontrolle).

Die wahrscheinlichste Ursache ist, dass die Daten auf dem Empfänger nicht verarbeitet werden. Um die Datenübertragung wieder zu aktivieren, muss ein TCP Window Update gesendet werden.

TCP Analyse mit dem Wireshark Expert

Wireshark Expert Meldungen (Fortsetzung)

- TCP Window Full

Wireshark markiert ein Daten-Paket mit dieser Meldung, wenn dieses den Eingangs-Buffer des Empfängers füllt. Der Empfänger wird mit einer TCP ZeroWindow Meldung antworten.

Die Gründe sind meistens, dass die Daten auf dem Empfänger nicht verarbeitet werden oder ein fehlendes Paket die Weiterleitung an die Applikation blockiert.

- TCP Keep-Alive

Der Sender dieses Paketes verifiziert, ob die TCP-Session noch aktiv ist; die Sequenznummer dieses Paketes ist normalerweise 1 tiefer als die aktuelle Sequenznummer. Der Empfänger sollte mit einem ACK oder einem TCP Keep-Alive ACK antworten.

Oft zu sehen bei blockierten Verbindungen durch TCP ZeroWindow oder wenn längere Zeit auf einer Session keine Daten ausgetauscht werden.

- TCP Keep-Alive ACK

Antwort auf eine TCP Keep-Alive Anfrage (siehe oben), wenn die Session noch aktiv ist.

- TCP Port numbers reused

Das Duplikat eines SYN Paketes mit denselben IP-Adressen und denselben TCP Port Nummern, jedoch mit unterschiedlicher Sequenznummer, wird von Wireshark mit dieser Meldung markiert.

Unsere Wireshark & Protokoll Kurse

- **WLAN Netzwerkanalyse mit Wireshark**, WaveXpert und WiSpy
  27./28 April 2020, HSR Hochschule für Technik Rapperswil → Zur Anmeldung bei HSR
- **VoIP Analyse mit Wireshark**
  24. März 2020, HSR Hochschule für Technik Rapperswil → Zur Anmeldung bei HSR
- **TCP/IP Analyse mit Wireshark**
  8. - 10. Juni 2020, HSR Hochschule für Technik Rapperswil → Zur Anmeldung bei HSR

Unser Spezialität sind **Firmenkurse** oder **Tech-Sessions** nach ihren Wünschen zu den Themen:

- Einführung Netzwerkanalyse, Wireshark Tipps & Tricks, TCP/IP, WLAN, VoIP und IPv6

Die komplette Liste aller unserer öffentlichen Kurse in der Schweiz, Österreich und Deutschland finden Sie auf unserer Webseite https://www.netsniffing.ch/de/wireshark-kurse/oeffentliche-kurse

Unser Newsletter Archiv finden sie unter: https://www.netsniffing.ch/de/wireshark-infos/newsletter

Es würde uns freuen, Sie in einem unserer Kurse begrüssen zu können.

Mit freundlichen Grüssen Rolf Leutert