Buranalyzer Wireshark Manual

Anwenderhandbuch - B&R Analyzer for Wireshark

Version: **x.x (xxxxx)**

Originalbetriebsanleitung

1 Einleitung 4
1.1 BuR Analyzer für Wireshark TM 4
1.1.1 buranalyzer-X.Y.Z_xxxxxx.msi 4
1.1.2 bur_wsX.Y.x_ZZ 4

2 Installation 5
2.1 Systemvoraussetzungen 5
2.2 Setup Tutorial 5
2.3 Konfigurationsprofil 7

3 PLTrace 10
3.1 X20ET8819 Adapter 10
3.1.1 Adapterkonfiguration 10
3.1.2 Aufzeichnung 12
3.1.2.1 Capture Control - (1) 13
3.1.2.2 Liste mit Ethernet Paketen - (2) 13
3.1.2.3 Dekodiertes Ethernet Paket - (3) 14
3.1.2.4 ‚Raw'-(Byte)-Ansicht eines Ethernet Pakets – (4) 14
3.1.2.5 PLTrace Status Bar – (5) 14
3.1.2.6 PLTrace Logger – (6) 14
3.1.2.7 Force Trigger – (7) 15
3.1.2.8 Wireshark Expert Logger – (8) 15

4 Anwendertipps 16
4.1 Welcher Capture Mode soll verwendet werden? 16
4.2 Wie werden Capture Files abgespeichert? 16
4.3 Paketfilter 16
4.3.1 Flags vom X20ET8819 16
4.3.2 Protokollfilter 17
4.4 Paketfilter – Schnellzugriff 18
4.5 Paketsuche 19
4.6 Zeitreferenz innerhalb einer Aufzeichnung 19
4.7 Aufzeichnung mit neuer Konfiguration starten 20
4.8 Performancesteigerung bei großen Capture-Files 21

1 Einleitung

Der „B&R Analyzer für Wireshark“ umfasst div. Erweiterungen für Wireshark. Mit Hilfe dieser Erweiterungen können Aufzeichnungen mit dem X20ET8819 durchgeführt werden, außerdem ermöglicht ein PLK spezifisches Plugin eine detaillierte PLK Analyse.

1.1 BuR Analyzer für Wireshark TM

Das B&R Analyzer Package kann von www.br-automation.com heruntergeladen werden.

Dem Anwender steht jetzt ein .zip Package (buranalyzer-X.Y.Z.zip) zur Verfügung.

Die Versionierung des .zip Package gibt Auskunft, welche Wireshark Versionslinie benötigt wird: buranalyzer-X.Y.Z.zip

X benötigte Wireshark Major Version
Y benötigte Wireshark Minor Version
Z Patch Version des B&R Analyzer Package
(wenn z.B. mehrere Packages mit neuen Features für eine Wireshark Versionslinie gebaut werden)

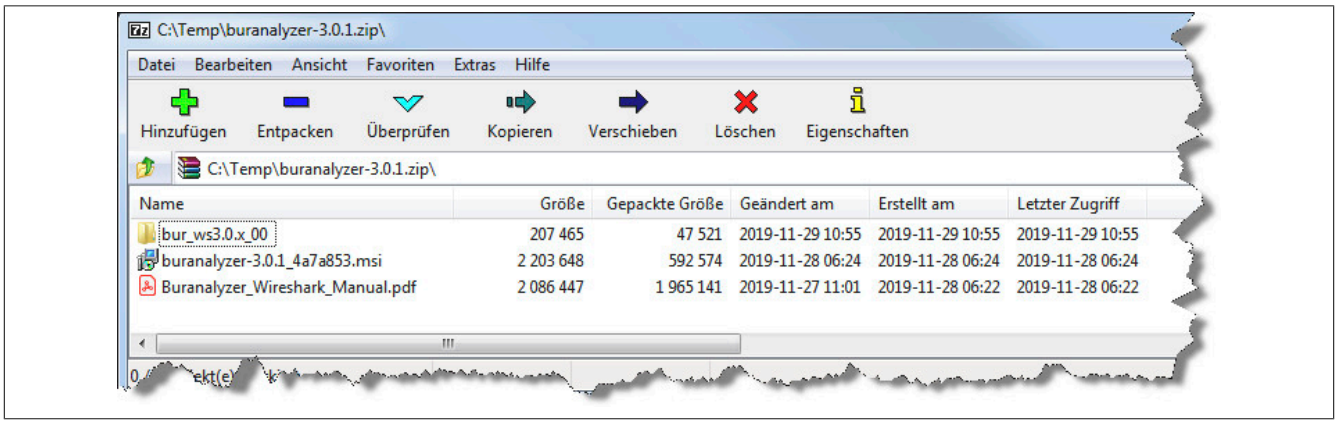


Abbildung 1: Übersicht B&R Analyzer Package (Beispiel für Versionslinie 3.0.x)

1.1.1 buranalyzer-X.Y.Z_xxxxxx.msi

Ausführbare Installationsdatei zum Installieren der B&R Analyzer Komponenten beinhaltet:

- PLTrace (extCap Aufzeichnungstool)
- PLK Plugin (Wireshark Plugin für PLK Analyse)

1.1.2 bur_wsX.Y.x_ZZ

B&R spezifisches Wireshark-Konfigurationsprofil mit div. exportierten Settings (siehe Konfigurationsprofil).

Die Versionierung des Konfigurationsprofils gibt Auskunft für welche Wireshark Versionslinie das Profil geeignet ist.

bur_wsX.Y.*_ZZ

X Wireshark Major Version
Y Wireshark Minor Version
Z Patch Version des B&R spezifischen Profils

2 Installation

2.1 Systemvoraussetzungen

Software	OS Unterstützung	Download
Wireshark VX.X.x	Windows 7, 10	Wireshark
WinPcap V4.1.3 (wird während der Wireshark-Installation mitinstalliert!)	Windows 7	winpcap
Npcap (wird während der Wireshark-Installation mitinstalliert!)	Windows 7, 10	Npcap
B&R Analyzer für Wireshark	Windows 7, 10	B&R Analyzer für Wireshark

Tabelle 1: Software-Übersicht

2.2 Setup Tutorial

Das folgende Tutorial zeigt den Installationsprozess auf einem Windows 7 System. Auf dem System ist keines der oben genannten Tools installiert.

1. Wireshark Setup starten
   a) keine speziellen Einstellungen in den ersten Dialogen nötig
2. Installation von WinPcap bzw. Npcap
   a) Wireshark-Setup erkennt, dass weder WinPcap noch Npcap am System installiert sind

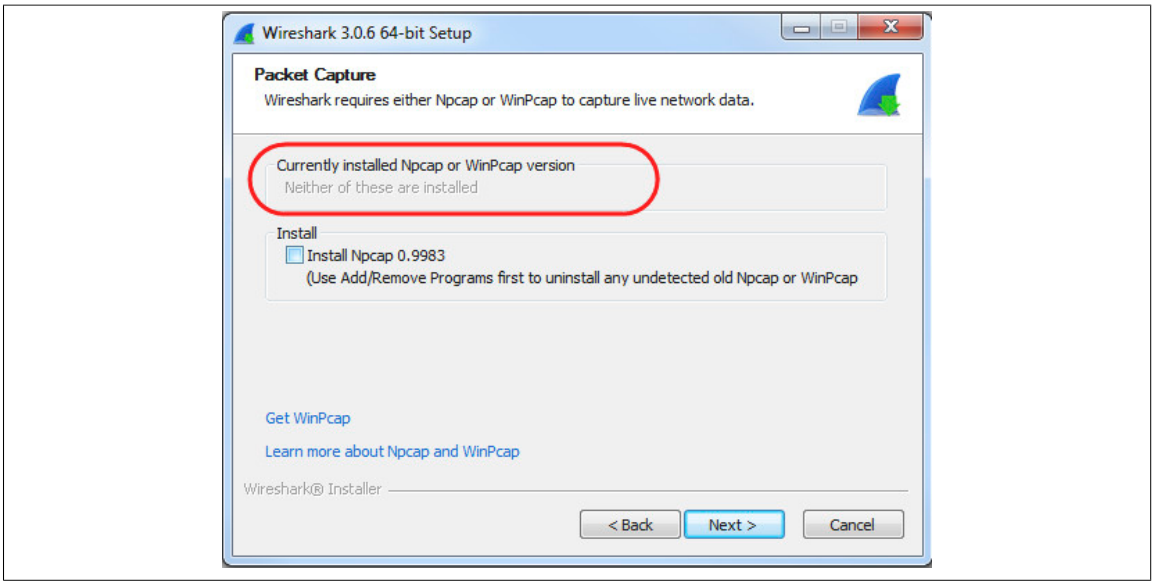


Abbildung 2: Setup sucht nach WinPcap oder Npcap am System

   b) Anwenderentscheidung
   Es muss berücksichtigt werden ob die Installation auf Windows 7 oder Windows 10 System durchgeführt wird (siehe OS Unterstützung).

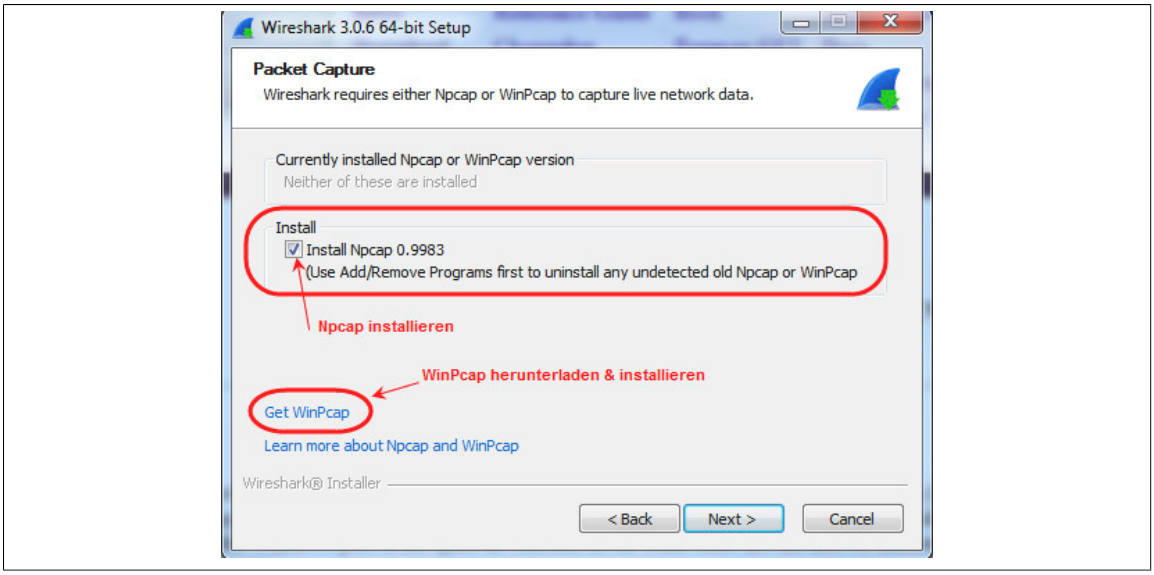


Abbildung 3: Entscheidung für WinPcap oder Npcap

c) der gewählte LowLevel Treiber kann im Anschluss mit Default-Einstellungen installiert werden

3. Wireshark Setup abschließen
4. B&R Analyzer Setup starten
   a) ausführen des im .zip File enthaltenen .msi Installers
   b) es wird geprüft ob eine kompatible Wireshark Version am System installiert ist

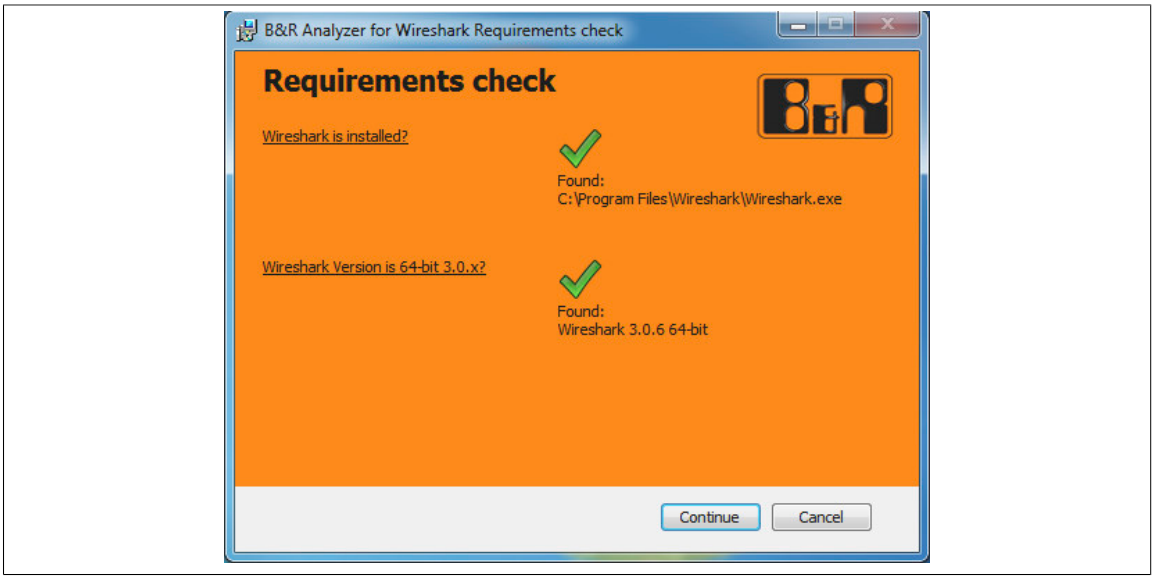


Abbildung 4: Suche nach installiertem Wireshark am System

5. Setup ausführen
   a) keine spezielle Einstellung in den ersten Dialogen nötig
   b) Empfehlung: Setup Type „Complete“ auswählen

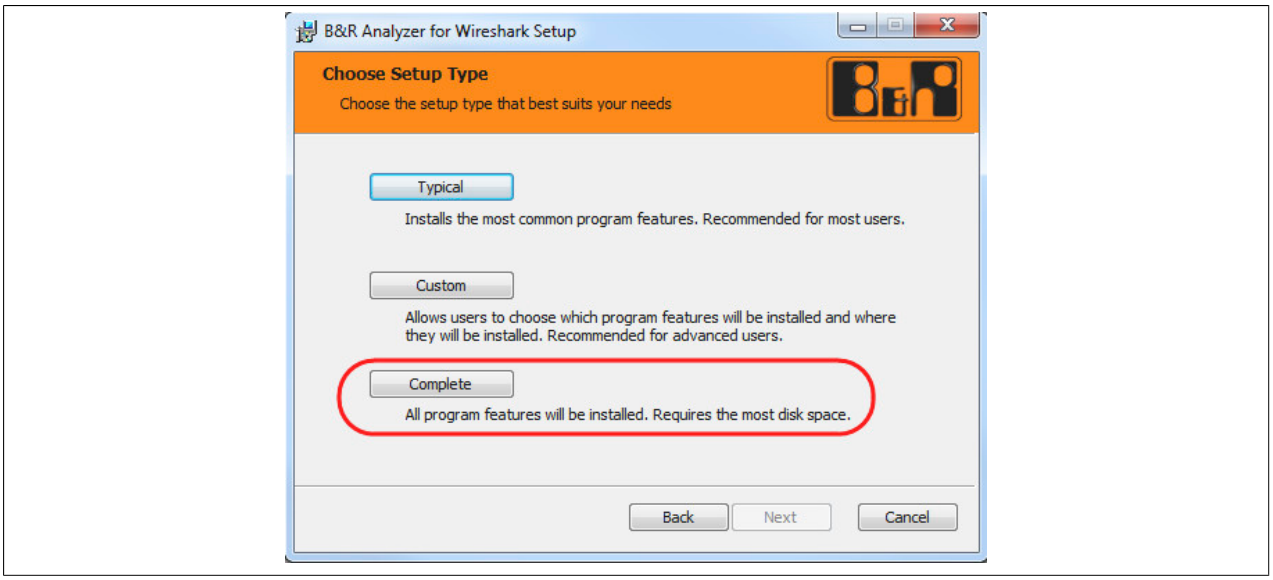


Abbildung 5: Auswahl den Setup-Typs

6. B&R Analyzer Setup abschließen

2.3 Konfigurationsprofil

Für ein einheitliches „Look & Feel“ auf verschiedenen Arbeitsplätzen wurden einige Settings definiert und in ein Profil exportiert. Die Verwendung dieses Profils ist keine zwingende Voraussetzung, unter Umständen wird die Arbeit dadurch allerdings erleichtert.

Das Profil beinhaltet:

- Voreingestellte Schriftart und Schriftgröße
- Vordefinierte Spalten und Spaltennamen im Capture-Fenster
- ‚Coloring-Rules‘ (farbliche darstellung von Paketen mit definierten eigenschaften)

1. Wireshark starten

   a) persönlichen Profilordner öffnen

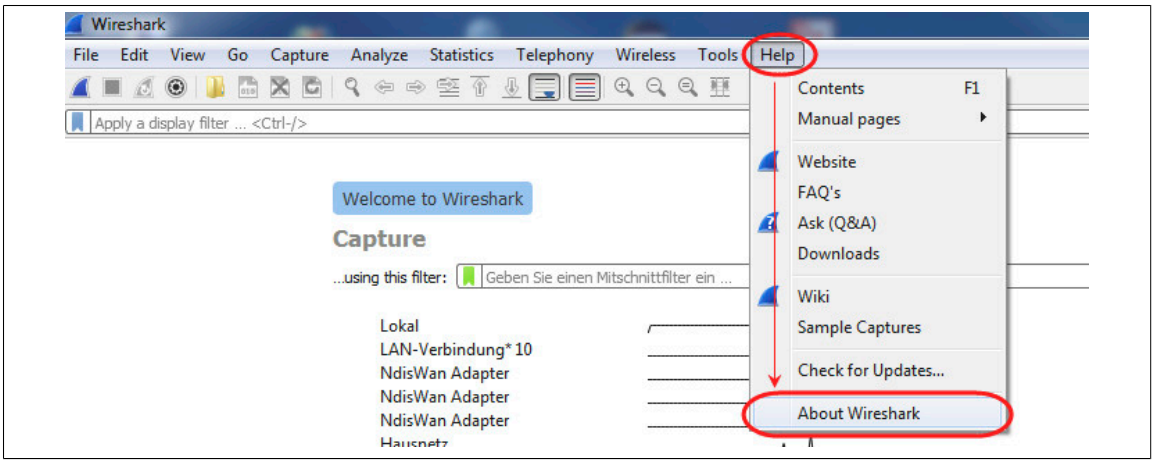


Abbildung 6: Aufrufen des Wireshark About-Dialogs

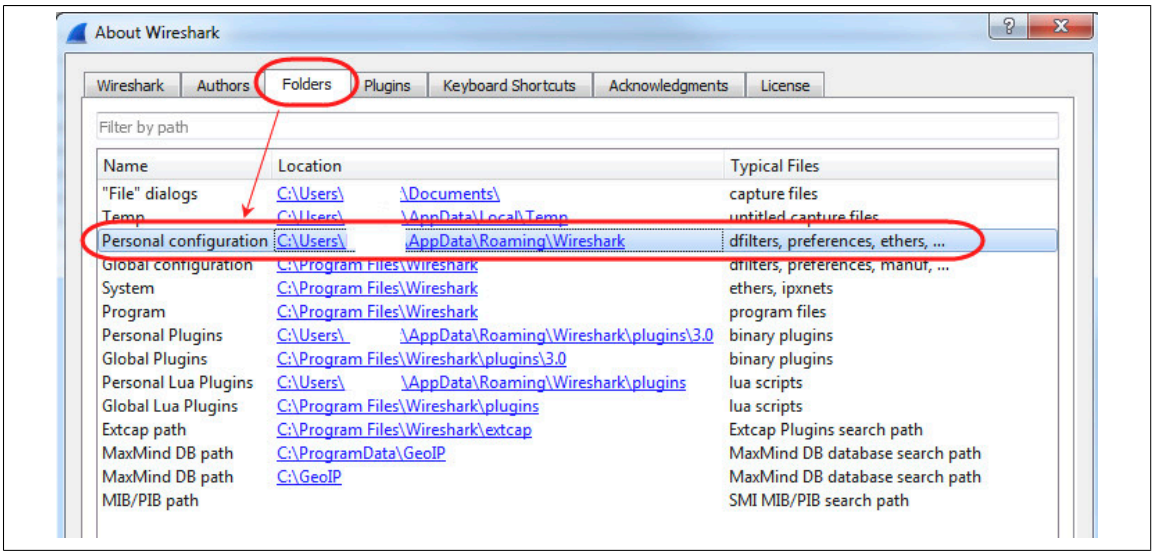


Abbildung 7: Profilordner direkt über den Link öffnen

2. B&R Profil ablegen

a) im geöffneten Ordnerpfad noch eine Ebene tiefer navigieren (..\profiles)

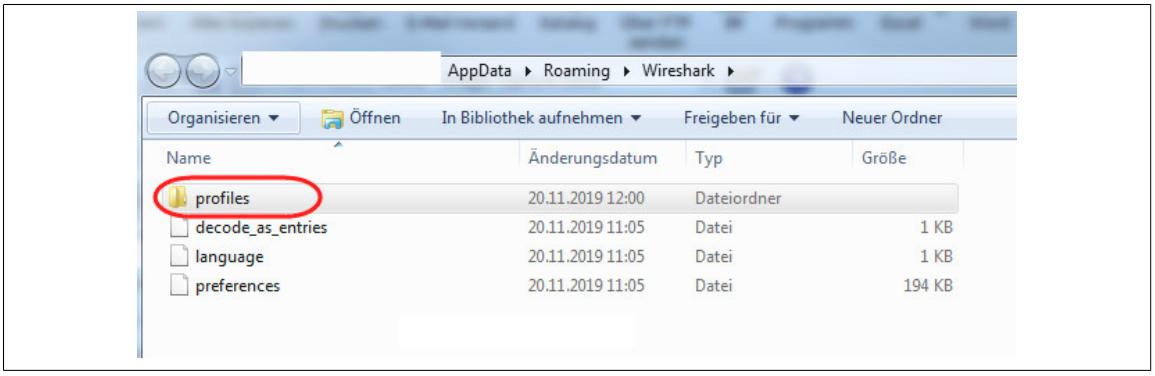


Abbildung 8: Ordner mit allen gesammelten Profilen ('profiles') aufrufen

b) im Pfad (..\profiles) wird der mitgelieferte Profilordner „bur_wsX.X.x_yy“ abgelegt

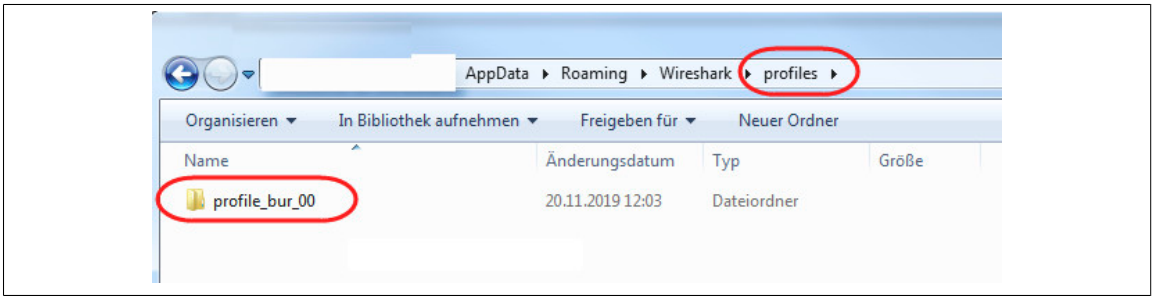


Abbildung 9: B&R spezifisches Profil in der Profilsammlung ablegen

3. B&R Profil aktivieren

a) im Profilmenü von Wireshark wird das B&R Profil zur Auswahl angeboten

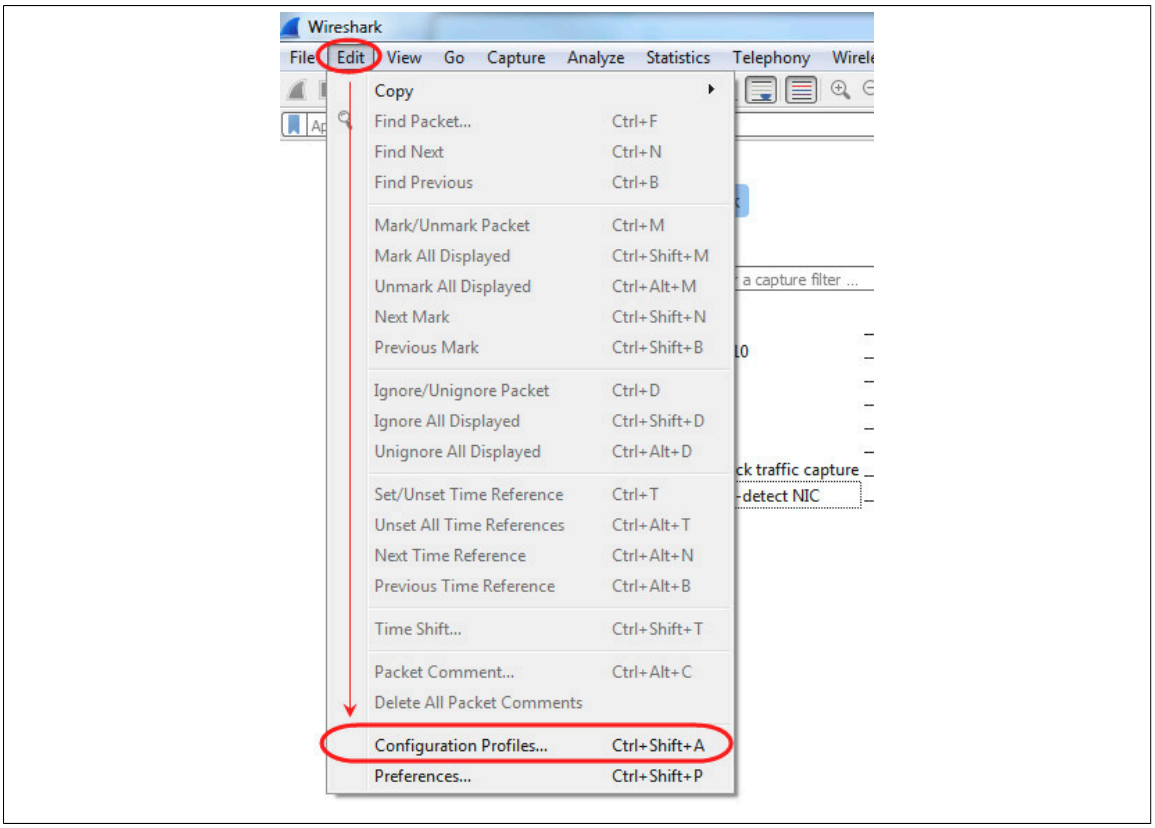


Abbildung 10: Profil-Verwaltungsmenü aufrufen

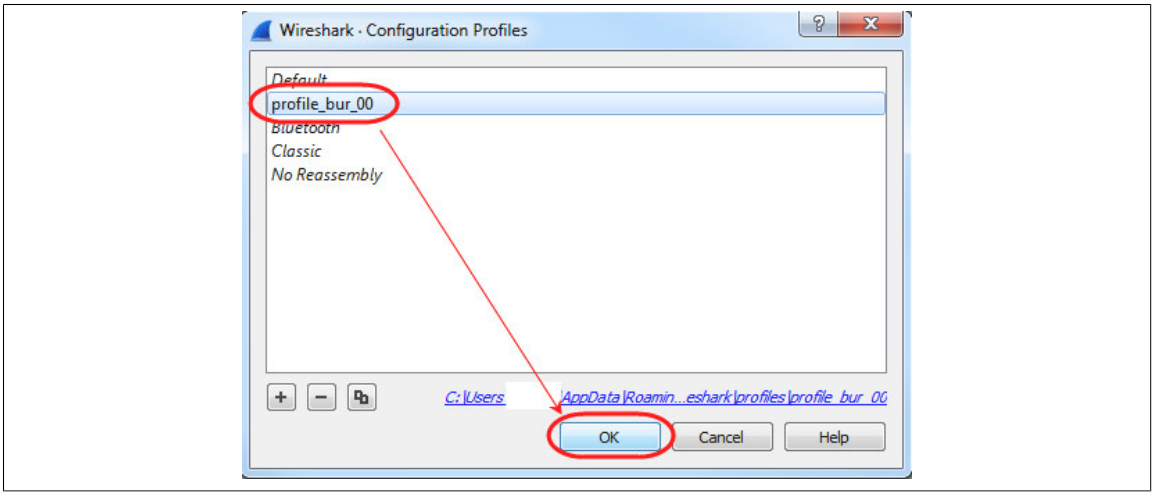


Abbildung 11: B&R Profil aktivieren

3 PLTrace

Das Aufzeichnungstool „PLTrace“ wird über das definierte „extcap-Interface“ in Wireshark eingebunden. Dieses Tool wird benötigt um Aufzeichnungen mit spezieller Zusatzhardwear (z.B X20ET8819, X2X Analyzer) durchzuführen.

3.1 X20ET8819 Adapter

Bevor eine Aufzeichnung mit dem X20ET8819 gemacht wird, sollten (einmalig) die vorhandenen Interface-Toolbars aktiviert werden.

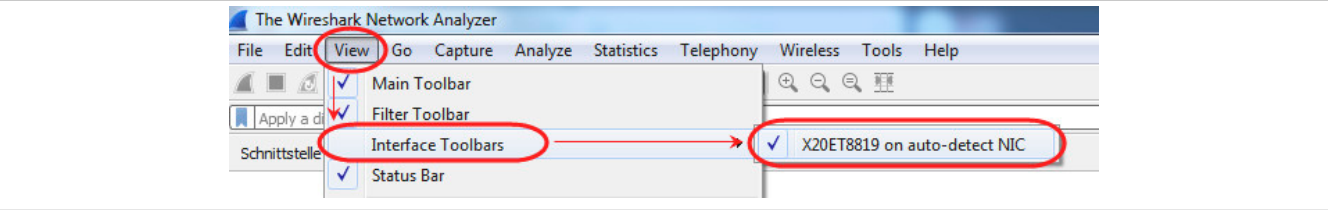


Abbildung 12: Aktivieren der X20ET8819 spezifischen Interface Toolbar

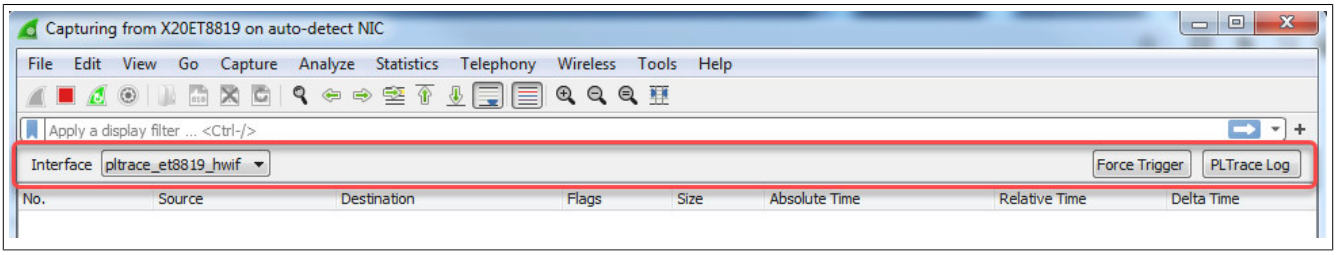


Abbildung 13: Aktive Interface Toolbar

3.1.1 Adapterkonfiguration

Der Adapter für Aufzeichnungen mit dem X20ET8819 wird in Wireshark mit einem „Default-Namen“ dargestellt: *‚X20ET8819 on auto-detect NIC‘*. Dieser Adapter sucht nach dem Starten einer Aufzeichnung auf allen am System verfügbaren Netzwerkkarten nach einem X20ET8819.

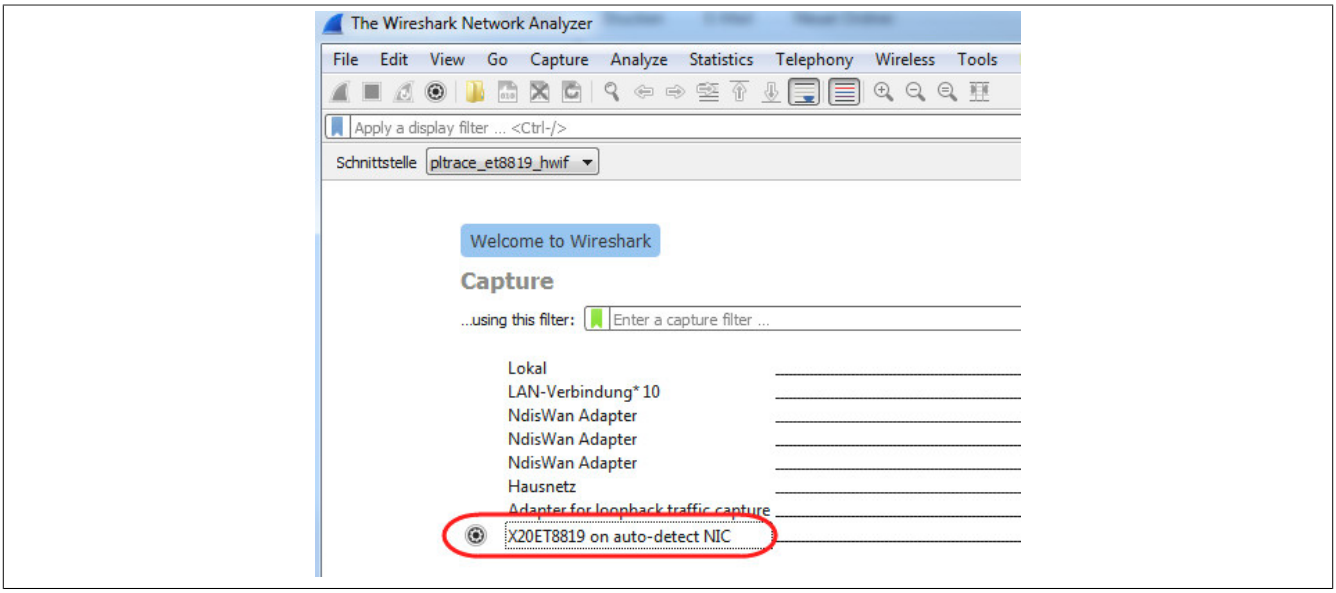


Abbildung 14: PLTrace Adapter für Aufzeichnungen mit dem X20ET8819

Über ein Konfigurationsmenü können div. Einstellungen für den X20ET8819 PLTrace Adapter getätigt werden.

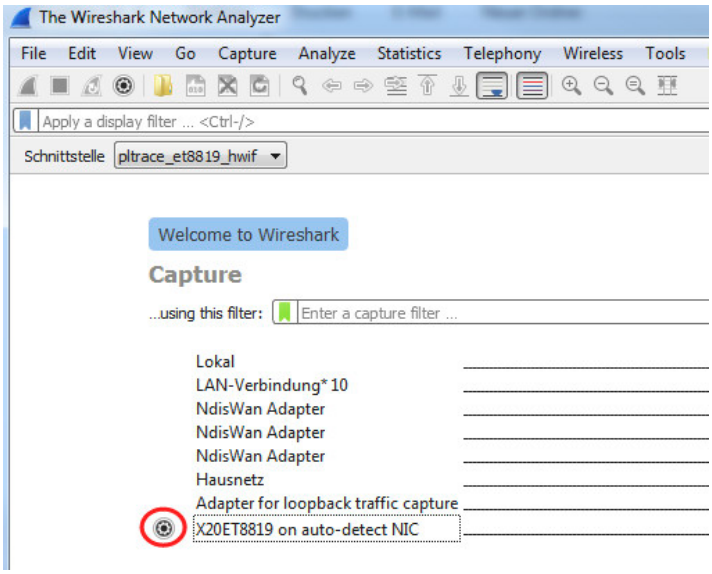


Abbildung 15: Adapterkonfiguration aufrufen

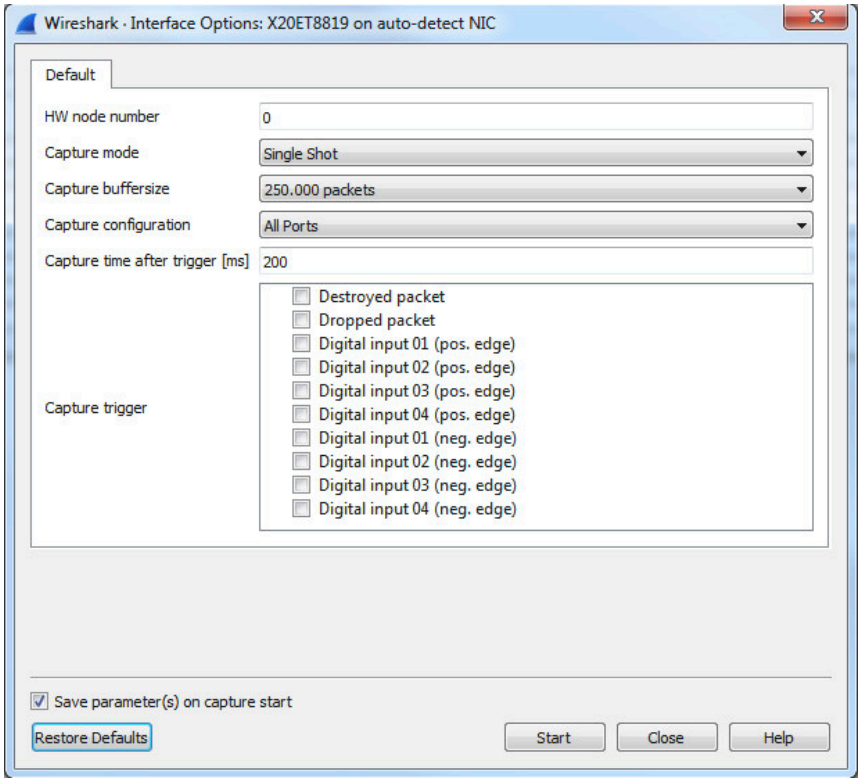


Abbildung 16: Konfigurationsmöglichkeiten des PLTrace X20ET8819 Adapters

Gruppe	Konfiguration
HW node number	**0** • Knotennummer selbstständig erkennen • nur die 1. erkannte Knotennummer wird in weiterer Folge akzeptiert **1-15** • eingestellte Knotennummer muss zum verwndeten X20ET8819 passen
Capture mode	**Live Capture** • alle verfügbaren und dekodierten Frames werden im Wireshark Captur-Fenster dargestellt • Aufzeichnung wird beim auftreten aines Trigger-Ereignis gestoppt **Single Shot** • Pakete werden im Hintergrund aufgezeichnet (Ringbuffer mit konfigurierbarer Größe) • bei auftreten einens Trigger-Ereignis (auch manuell auslösbar), werden die im Ringbuffer verfügberen Pakete im Captur-Fenster von Wireshark dargestellt • danach wird die Aufzeichnung gestoppt
Capture buffersize	• während der Aufzeichnung wird im Hintergrund ein Ringbuffer zur Paketvorbereitung verwendet • beim ‚Live Capture' Modus wird dieser Buffer nur zur Vorsortierung der Pakete benötigt. Die Größe sollte in diesem Fall so klein wie möglich eingestellt werden (die Pakete werden ohnehin sofort an Wireshark weitergeleitet) • beim ‚Single Shot' Modus sollte die Buffer größer, vom Anwender je nach Erfordernissen (geplante Aufzeichnungsdauer,..), gewählt werden. In diesem Fall werden die Pakete nämlich nur im Ringbuffer gespeichert und nur beim Auftreten eines Trigger-Ereignis an Wireshark weitergeleitet.
Capture configuration	**Port01/02** • der X20ET8819 verfügt über 2 Aufzeichnungsports • abhängig vom verwendeten HW-Aufbau werden in der Aufzeichnung Pakete von Port01, 02 oder von beiden Ports benötigt
Capture time after trigger	**100-1000ms** • beim Auftreten eines Trigger-Ereignis werden noch so lange Pakete aufgezeichnet bis die eingestellte Nachtriggerzeit abgelaufen ist.
Capture Trigger	**Destroyed packet** • der X20ET8819 erkennt div. Frame-Fehler, diese Fehler können als Trigger-Ereignis verwendet werden • CRC-, Oversize-, Alignmen-, Preamble-, Nois-Fehler **Dropped packet** • bei Performence-Engpässen am PC oder am Netzwerk können im schlimmsten Fall Pakete vom PC, oder sogar vom X20ET8819 verloren gehen • verlorene Pakete können als Trigger-Ereignis verwendet werden **Digital Input 01-04 (pos. edge)** • eine positive Flanke am digitalen Eingang 01-04 löst ein Trigger-Ereignis aus **Digital Input 01-04 (neg. edge)** • eine negative Flanke am Digitalen Eingang 01-04 löst ein Trigger-Ereignis aus **Manuelles Trigger-Ereignis** • ein Trigger kann manuell vom Anwender ausgelöst werden • in der bereits aktivierten Interface-Toolbar kann ein Trigger vom Anwender durch drücken des ‚Force Trigger' Buttons ausgelöst werden

Tabelle 2: Konfigurationsmöglichkeiten des PLTrace X20ET8819 Adapters

3.1.2 Aufzeichnung

Durch einen Doppelklick auf den Adapter wird die Aufzeichnung mit der zuvor getätigten Adapterkonfiguration gestartet.

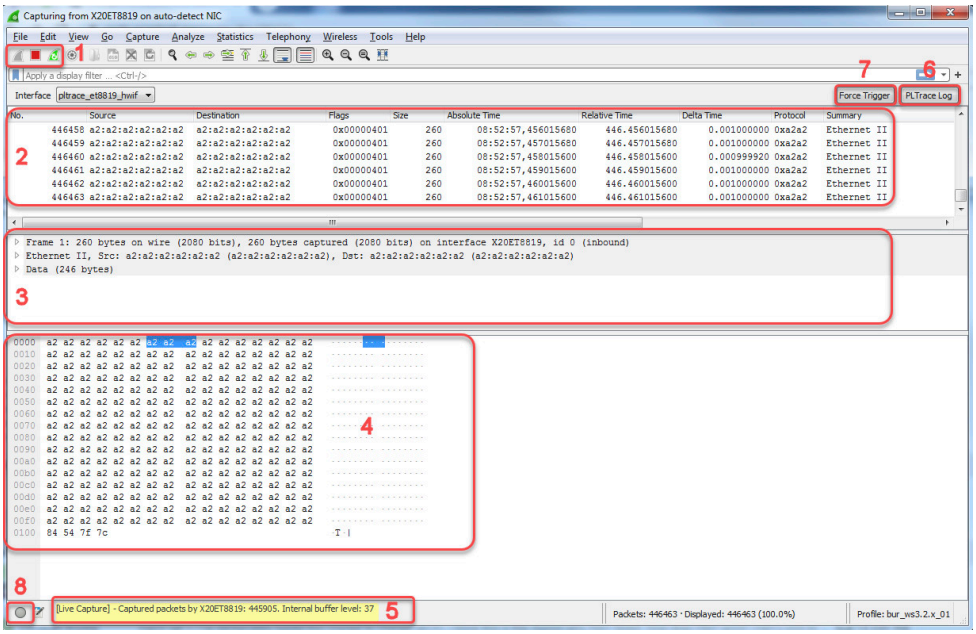


Abbildung 17: Wireshark - Captur Fenster

3.1.2.1 Capture Control - (1)

- Aufzeichnung starten / stoppen / neu-starten

3.1.2.2 Liste mit Ethernet Paketen - (2)

<table>
<tr><th>Spalte</th><th>Beschreibung</th></tr>
<tr><td>No.</td><td>fortlaufende Paketnummer</td></tr>
<tr><td>Source</td><td>• Source MAC Adresse des Ethernet Pakets (ggf. lt. Name-Table dekodiert)
• abhängig vom Pakettype, kann hier z.B. auch die Source IP Adresse dargestellt werden</td></tr>
<tr><td>Destination</td><td>• Destination MAC Adresse des Ethernet Pakets (ggf. lt. Name-Table dekodiert)
• abhängig vom Pakettype, kann hier z.B. auch die Destination IP Adresse dargestellt werden</td></tr>
<tr><td>Flags</td><td>• 32Bit Wert beinhaltet unterschiedlichste Informationen
• die mit (*) markierten Werte werden von Wireshark dekodiert
• die restlichen Werte werden von Wireshark aktuell nicht verwendet
• sollte Wireshark die verwendeten Flags irgendwann doch brauchen, müssen ev. div. Flags entfernt werden

<table>
<tr><th>Wert (jeweils 1Bit)</th><th>Beschreibung</th></tr>
<tr><td>0x00000001*</td><td>X20ET8819 Empfangsport 1</td></tr>
<tr><td>0x00000002*</td><td>X20ET8819 Empfangsport 2</td></tr>
<tr><td>0x00000004-
0x00000100</td><td>nicht verwendet</td></tr>
<tr><td>0x00000200</td><td>X20ET8819 Link Port T0 = OK</td></tr>
<tr><td>0x00000400</td><td>X20ET8819 Link Port T1 = OK</td></tr>
<tr><td>0x00000800</td><td>X20ET8819 Link Port T2 = OK</td></tr>
<tr><td>0x00001000</td><td>X20ET8819 Link Port T3 = OK</td></tr>
<tr><td>0x00002000</td><td>X20ET8819 Link Port T4 = OK</td></tr>
<tr><td>0x00004000</td><td>nicht verwendet</td></tr>
<tr><td>0x00008000</td><td>nicht verwendet</td></tr>
<tr><td>0x00010000</td><td>X20ET8819 Digital Input 01 = 1</td></tr>
<tr><td>0x00020000</td><td>X20ET8819 Digital Input 02 = 1</td></tr>
<tr><td>0x00040000</td><td>X20ET8819 Digital Input 03 = 1</td></tr>
<tr><td>0x00080000</td><td>X20ET8819 Digital Input 04 = 1</td></tr>
<tr><td>0x00100000</td><td>aktuelles Paket wurde nicht mit voller Länge aufgezeichnet (= sliced)</td></tr>
<tr><td>0x00200000</td><td>Trigger Flag – beim aktuellen Paket wurde ein Triggerereignis erkannt</td></tr>
<tr><td>0x00400000</td><td>Dropped Flag – vor dem aktuellen Paket wurden [n] Pakete verloren</td></tr>
<tr><td>0x00800000</td><td>nicht verwendet</td></tr>
<tr><td>0x01000000*</td><td>CRC Fehler</td></tr>
<tr><td>0x02000000*</td><td>Oversize Fehler</td></tr>
<tr><td>0x04000000*</td><td>Undersize Fehler</td></tr>
<tr><td>0x08000000*</td><td>IFG Fehler - nicht verwendet</td></tr>
<tr><td>0x10000000*</td><td>Alignment Fehler</td></tr>
<tr><td>0x20000000*</td><td>SFD Fehler - nicht verwendet</td></tr>
<tr><td>0x40000000*</td><td>Preamble Fehler</td></tr>
<tr><td>0x80000000*</td><td>Noise Fehler</td></tr>
</table></td></tr>
<tr><td>Size</td><td>• Originalgröße des Ethernet Pakets
• aufgezeichnete Länge kann u. U. kürzer sein</td></tr>
</table>

Spalte	Beschreibung
Absolute Time	absolute Tageszeit (gebildet aus dem Zeitstempel des Ethernet Pakets)
Relative Time	relative Zeitdifferenz [ns] zu einem definierten Paket der Aufzeichnung • Default: Relativzeit ggü. dem 1. Paket der Aufzeichnung • beliebiges Paket kann als Referenz-Zeit bestimmt werden
Delta Time	Zeitdifferenz [ns] zum vorigen aufgezeichneten Ethernet Paket
Protocol	erkanntes Ethernet Protokoll (z.B. PLK, IP, …)
Summary	hilfreiche Paketinformationen

3.1.2.3 Dekodiertes Ethernet Paket - (3)

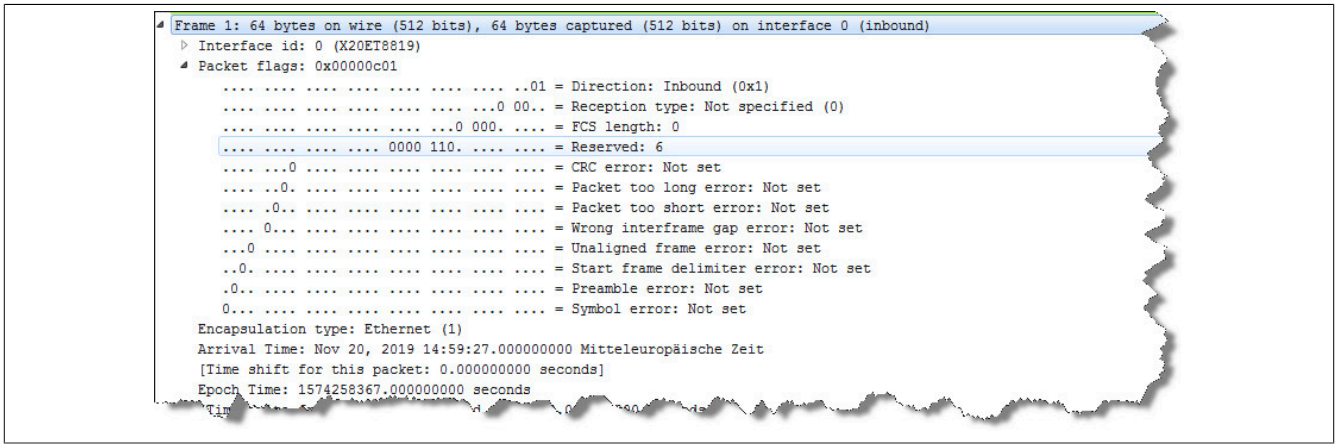


Abbildung 18: Allgemeine Paketinformationen (generiert von Wireshark)

- InterfaceID: 0 = X20ET8819
- (zum Teil) dekodierte Paketflags
- Zeitinformation
- usw...

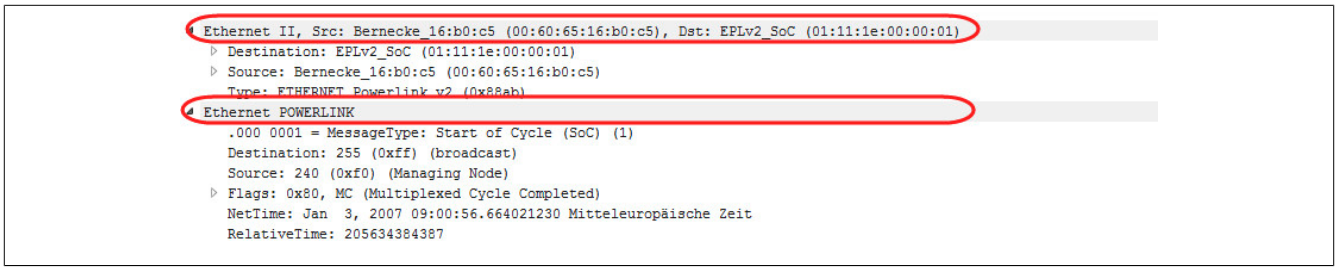


Abbildung 19: gefundene Protokolle innerhalb des Paketes

- bei einem PLK Paket wird die Wireshark Heuristik „nur“ Ethernet und PLK erkennen
- wenn aber z.B. TCP Pakete aufgezeichnet werden, können u. U. noch mehrere Protokolle im Paket enthalten sein

3.1.2.4 ‚Raw‘-(Byte)-Ansicht eines Ethernet Pakets – (4)

- aufgezeichnete Rohdaten (Hex-(Byte-) Ansicht des Ethernet Pakets

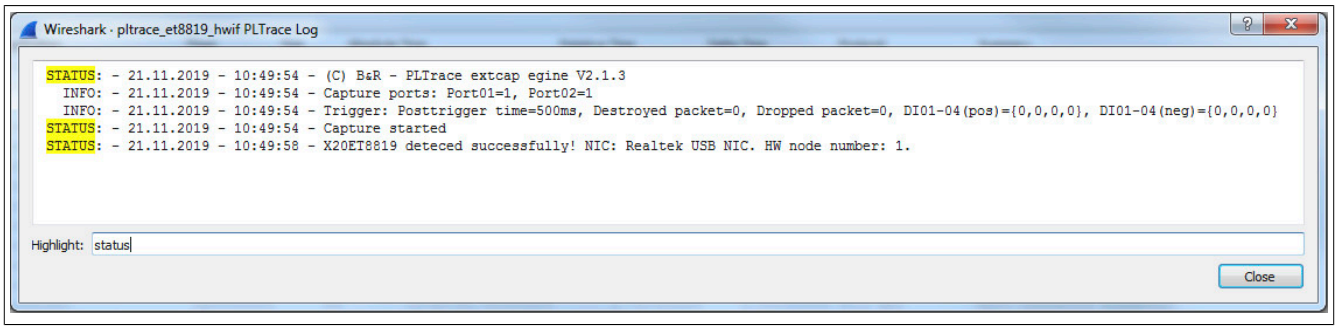
3.1.2.5 PLTrace Status Bar – (5)

- in der Statusbar werden vom PLTrace-Aufzeichnungstool laufend Updates eingetragen
- der Anwender wird so über den aktuellen Stand informiert

3.1.2.6 PLTrace Logger – (6)

- Loggerfenster mit div. Informationen vom PLTrace Aufzeichnungstool
- jede Meldung ist mit Severity, Datum & Uhrzeit versehen
- mögliche Severities:
  - ⇨ STATUS
  - ⇨ INFO

⇨ WARNING
⇨ ERROR



3.1.2.7 Force Trigger – (7)

- Auslösen eines manuellen Trigger-Ereignis durch den Anwender (Verhalten ist ident zum Auftreten eines konfigurierten Trigger-Ereignis)
- alle Pakete die aktuell im Ringbuffer vorhanden sind werden an Wireshark weitergeleitet
- die Aufzeichnung wird danach beendet

3.1.2.8 Wireshark Expert Logger – (8)

- Einträge vom registrierten Dissector-Plugin (z.B B&R PLK Plugin)

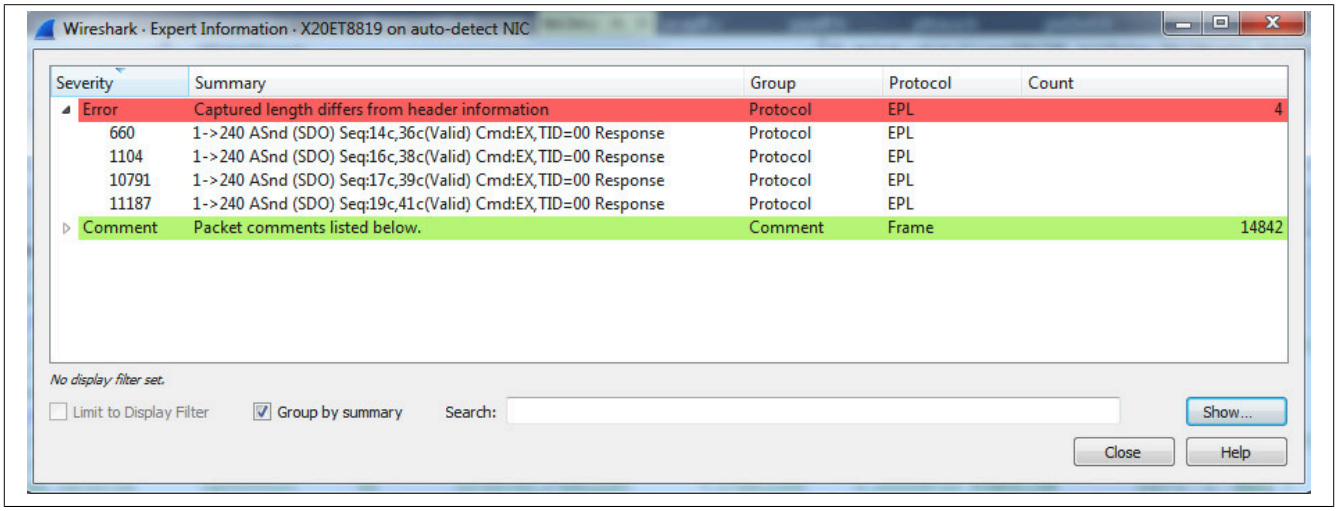


Abbildung 20: Expert Log

4 Anwendertipps

4.1 Welcher Capture Mode soll verwendet werden?

Generell gilt:

- kurze Aufzeichnung um einen Überblick über das Netzwerk zu gewinnen => Live Capture
- Langzeitaufzeichnungen mit definiertem (oder manuell ausgelöstem) Trigger-Ereignis => Single Shot

Wenn Pakete live aufgezeichnet werden, werden die Pakete von Wireshark im Capture Fenster dargestellt. Gleichzeitig werden im Hintergrund Files generiert. Je nach Aufzeichnungslänge werden diese Files immer größer und die Performane von Wireshark leidet.

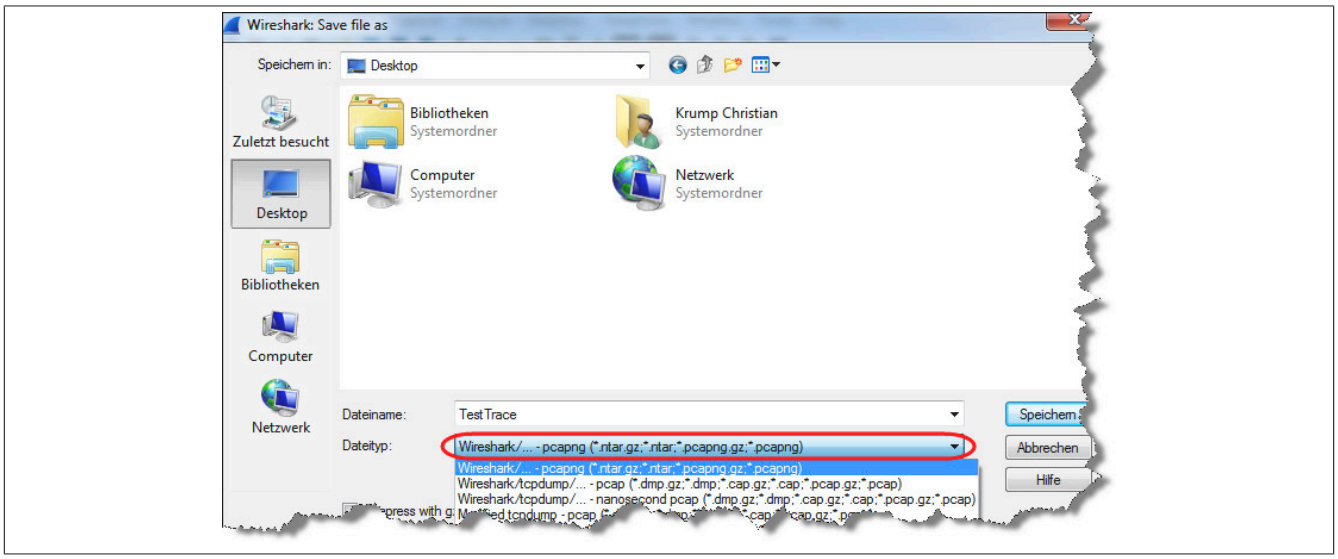
Der große Vorteil der Single Shot Aufzeichnung ist, dass man einen kompakten Trace (konfigurierbare Anzahl an Paketen) erhält. Aus Erfahrung sind bei einer Fehlersuche maximal einige wenige Netzwerkzyklen vor dem Trigger-Ereignis und einige wenige Netzwerkzyklen nach dem Trigger-Ereignis zum Auffinden der Fehlersuche relevant. Bei einer Live-Aufzeichnung die nach der Zeit (x), nach einem Trigger-Ereignis angehalten wird, werden oft unnötig viele Daten mitgeschleppt, die auch die Weiterverarbeitung z.B. Versenden von E-Mail erschweren.

Sollte die Performance für ein „Live Capture“ nicht ausreichen, laufen die Verwaltungsbuffer im Hintergrund über, folglich wird die Aufzeichnung beendet und der Anwender mit einer Warnung informiert.

4.2 Wie werden Capture Files abgespeichert?

Wenn Aufzeichnungen mit dem PLTrace X20ET8819 Adapter gemacht werden, stehen viele interessante Paket-Informationen (z.B. die Flags, oder die Paket-Kommentare) zur Verfügung. Es sollte darauf geachtet werden, dass diese Information beim Speichern der Aufzeichnung nicht verloren gehen.

Eine Datei sollte (zwingend) im ‚pcapng‘ Format gespeichert werden. Dieses Format ist das Default-Format, das von Wireshark beim Speichern angeboten wird.



4.3 Paketfilter

In Wireshark kann einfach auf bestimmte Daten innerhalb eines Pakets gefiltert werden. Prinzipiell kann in Wireshark auf jedes dekodierte Element über das Kontextmenü ein entsprechender Filter definiert werden.

4.3.1 Flags vom X20ET8819

Werden die Flags von Wireshark dekodiert, können die dekodierten Flags einfach (über das Kontextmenü) als Filterbedingung übernommen werden.

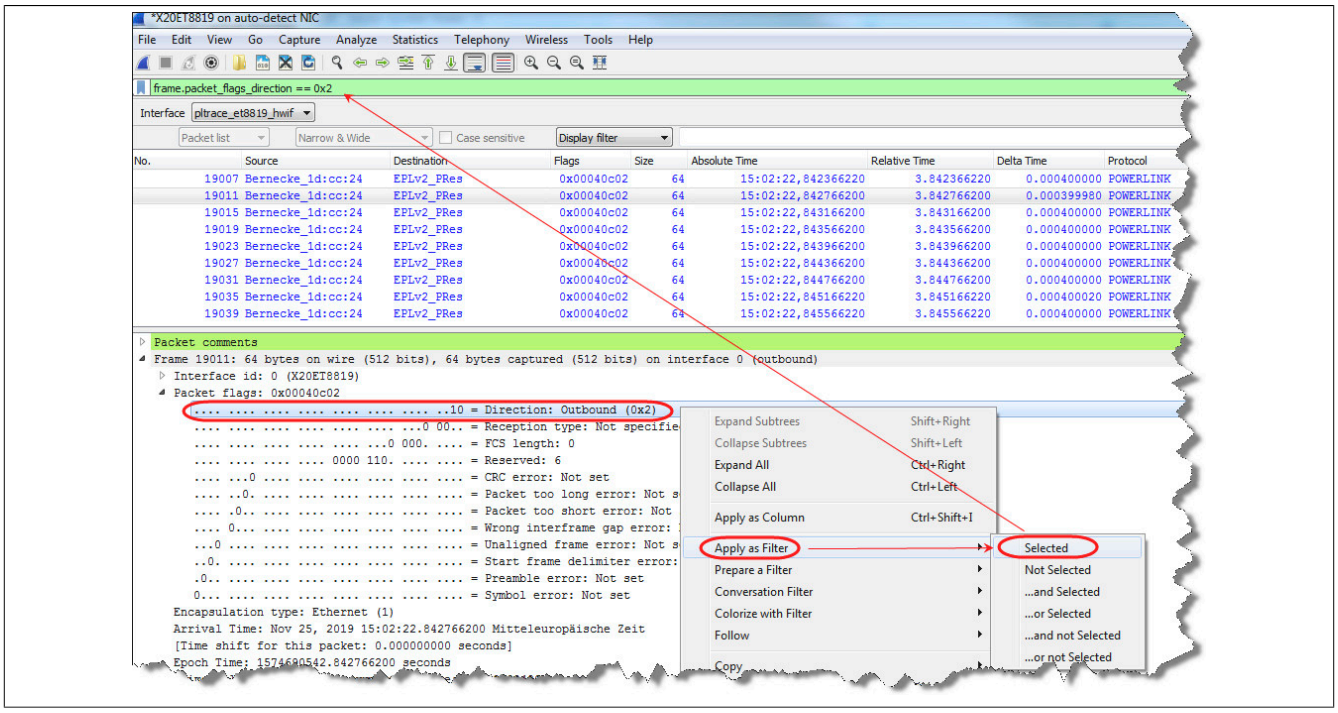


Abbildung 21: Pakete vom X20ET8819 Port 2 herausfiltern

Wenn div. Flags von Wireshark nicht dekodiert werden (z.B. das „Dropped-Flag“) kann man diese Pakete aber immer noch herausfiltern. Die Filterbedingung wird dabei über eine einfache Maskierung definiert.

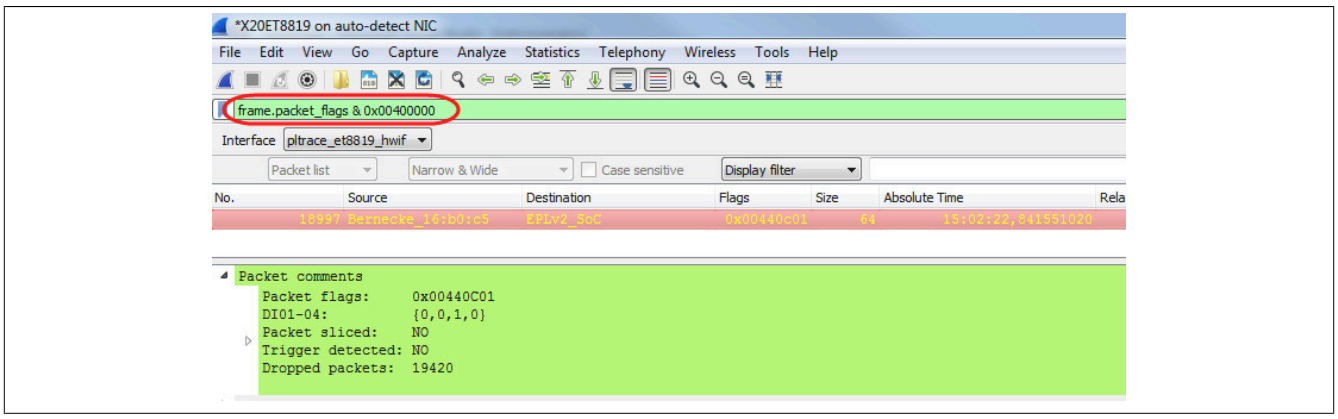


Abbildung 22: alle Pakete mit gesetztem "Dropped Flag" herausfiltern

Achtung!

Eine „ungleich“ Filterbedingung wird in Wireshark wie folgt formuliert:

- **gleich-Bedingung: (frame.packet_flags & 0x00400000)**
- **ungleich-Bedingung: !(frame.packet_flags & 0x00400000)**

4.3.2 Protokollfilter

Eine Übersicht über alle verfügbaren Protokollfilter ist direkt in Wireshark abrufbar. Die Protokollfilter werden von den unterschiedlichen Plugin-Herstellern definiert, im Normalfall werden ausreichend viele Filter angeboten. Über ein GUI-Interface können so auch einfach Filter zusammengebaut und verknüpft werden.

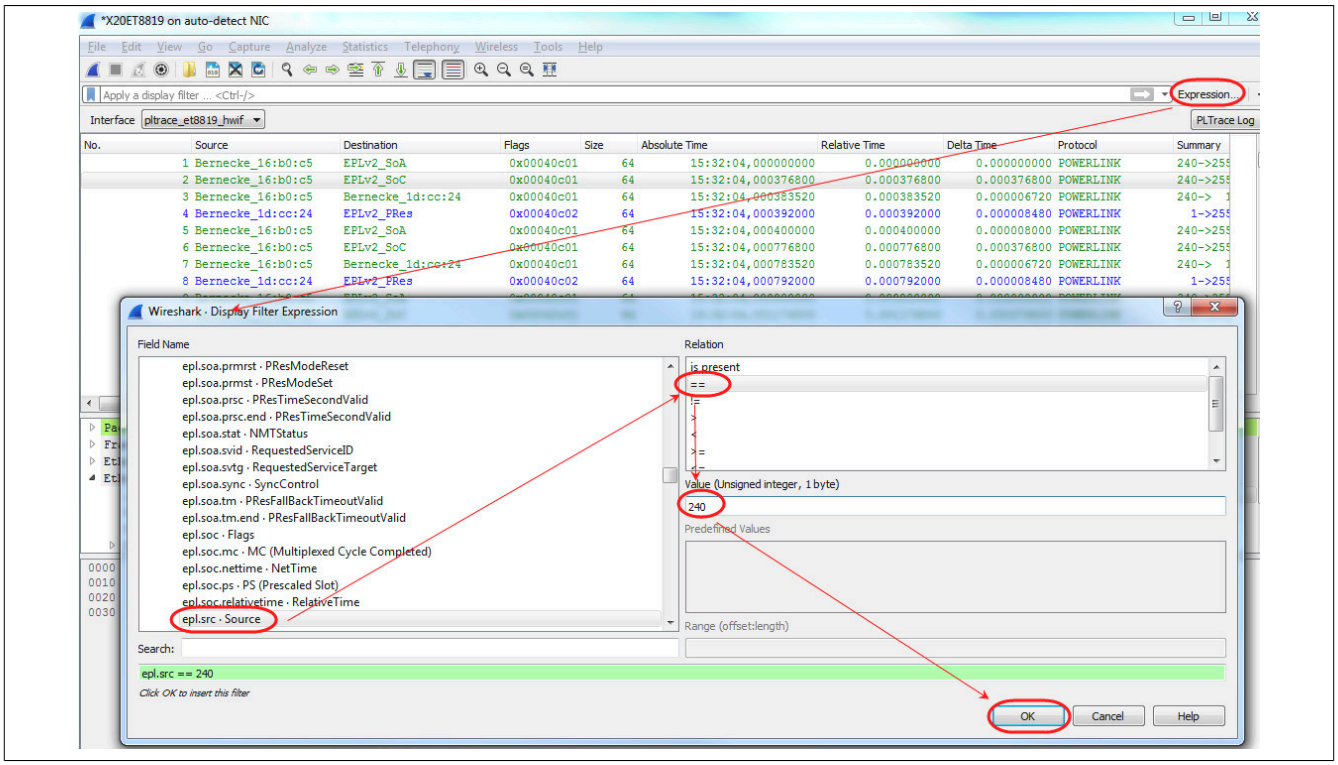


Abbildung 23: EPL V2 Filter - Beispiel: alle Pakete vom MN

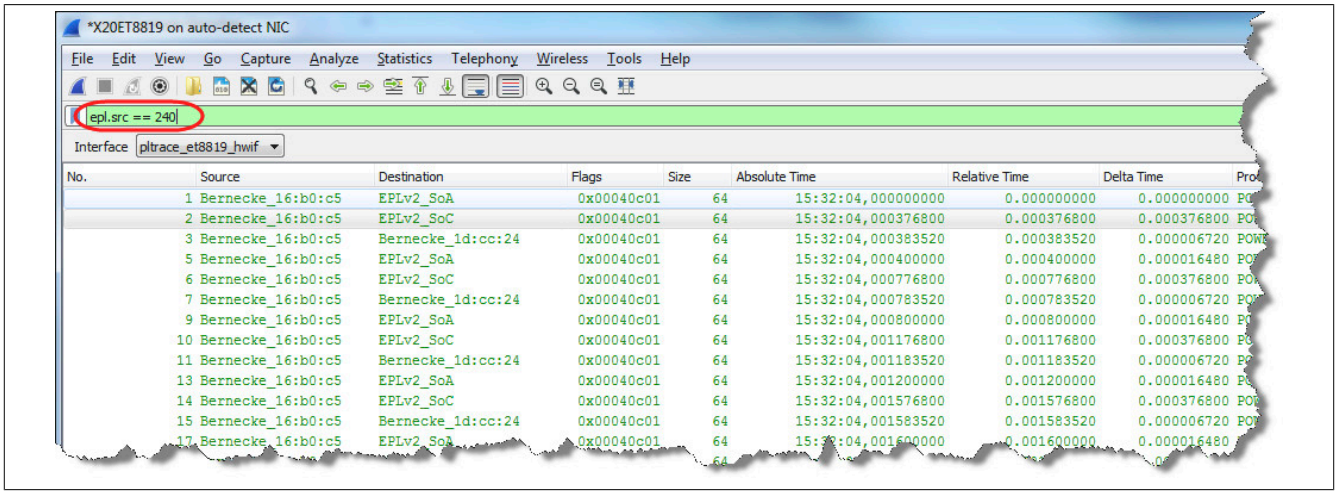


Abbildung 24: resultierende Filterbedingung

4.4 Paketfilter – Schnellzugriff

Wenn div. Filter sehr oft benötigt werden, können diese als Schnellzugriff-Button abgelegt werden.

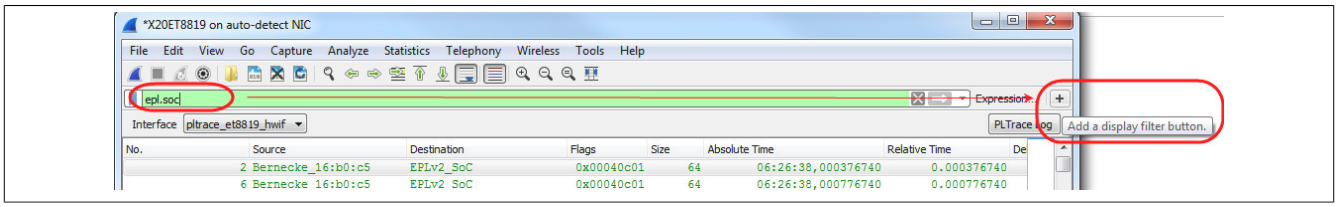


Abbildung 25: beliebigen Filter (z.B. EPL SOCs) auswählen

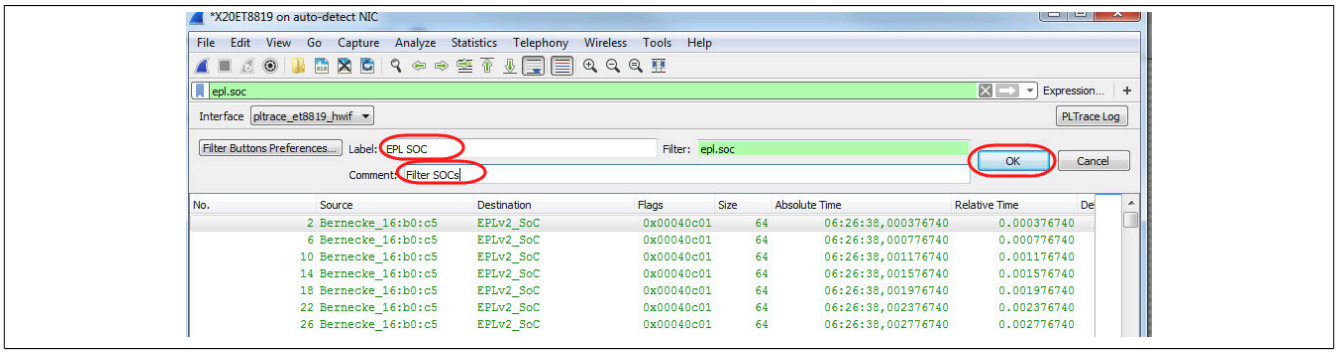


Abbildung 26: Namen & Beschreibungen des neuen Filterbuttons definieren

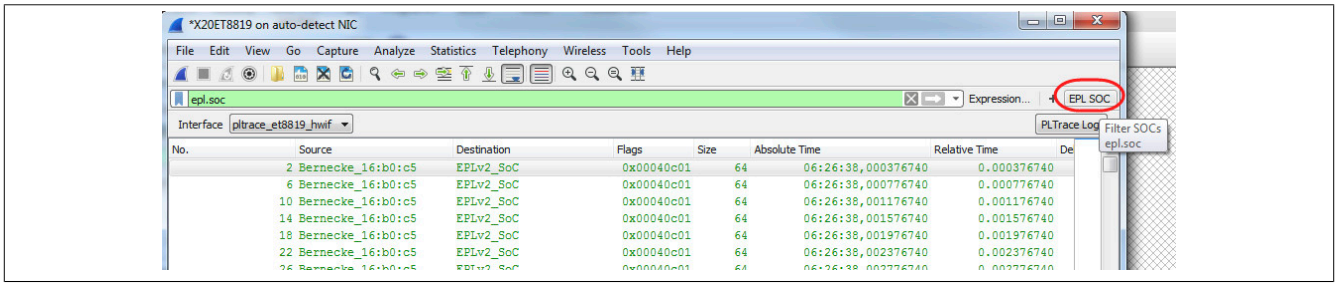


Abbildung 27: neu erstellter Filter-Button ist verfügbar

4.5 Paketsuche

Ähnlich wie das Filtern der Pakete funktioniert auch die Suche. Es können Pakete nach beliebigen Bedingungen gesucht werden, der Unterschied zum Filtern: Pakete die nicht zum Filter passen werden nicht (wie beim Filtern) ausgeblendet, das heißt, man sieht auch die Vorgeschichte zum entsprechenden Paket.

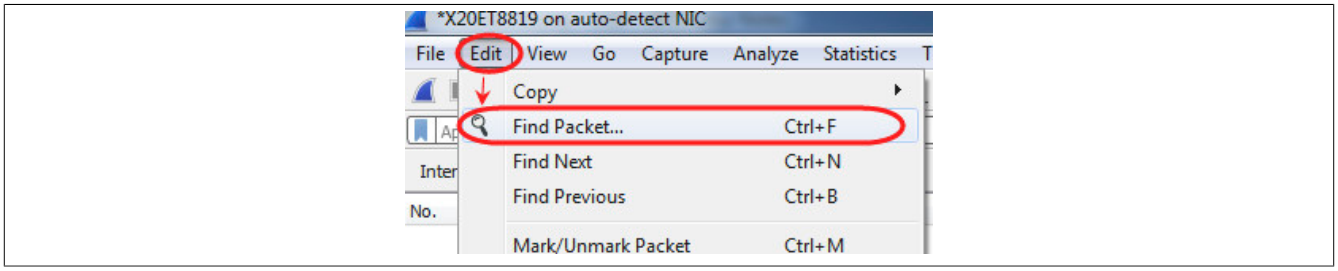


Abbildung 28: Paketsuche öffnen

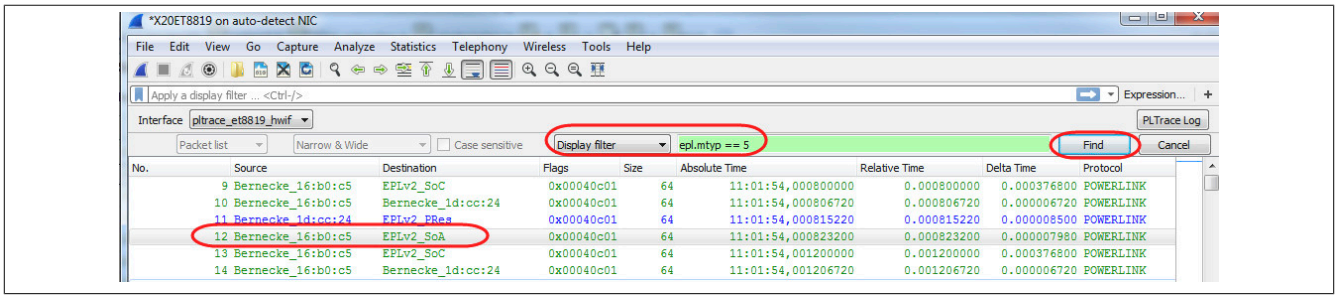


Abbildung 29: SOAs suchen (mit Klick auf "Find" kommt man zum nächsten passenden Paket)

4.6 Zeitreferenz innerhalb einer Aufzeichnung

Die Relativzeit eines Pakets gibt die Zeitdifferenz [ns] zum definierten Referenzpaket an. Stanardmäßig verwendet Wireshark das 1. Paket innerhalb der Aufzeichnung als Referenzpaket, das heißt, die Relativzeit eines Pakets stellt im Endeffekt auch die Aufzeichnungsdauer dar (= Differenz zwischen 1. und aktuellen Paket).

Beispiel:

Zeitmessung zwischen 2 PLK SOCs, die 3 Zyklen auseinander liegen

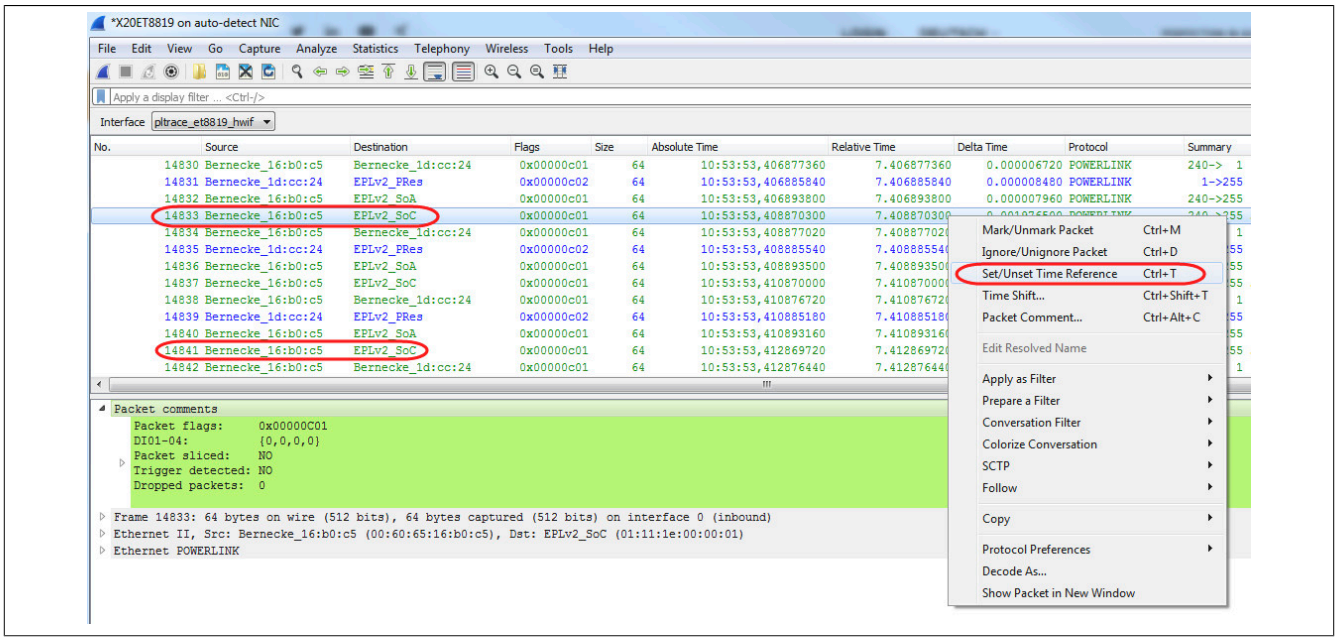


Abbildung 30: Paket als Referenzpaket bestimmen

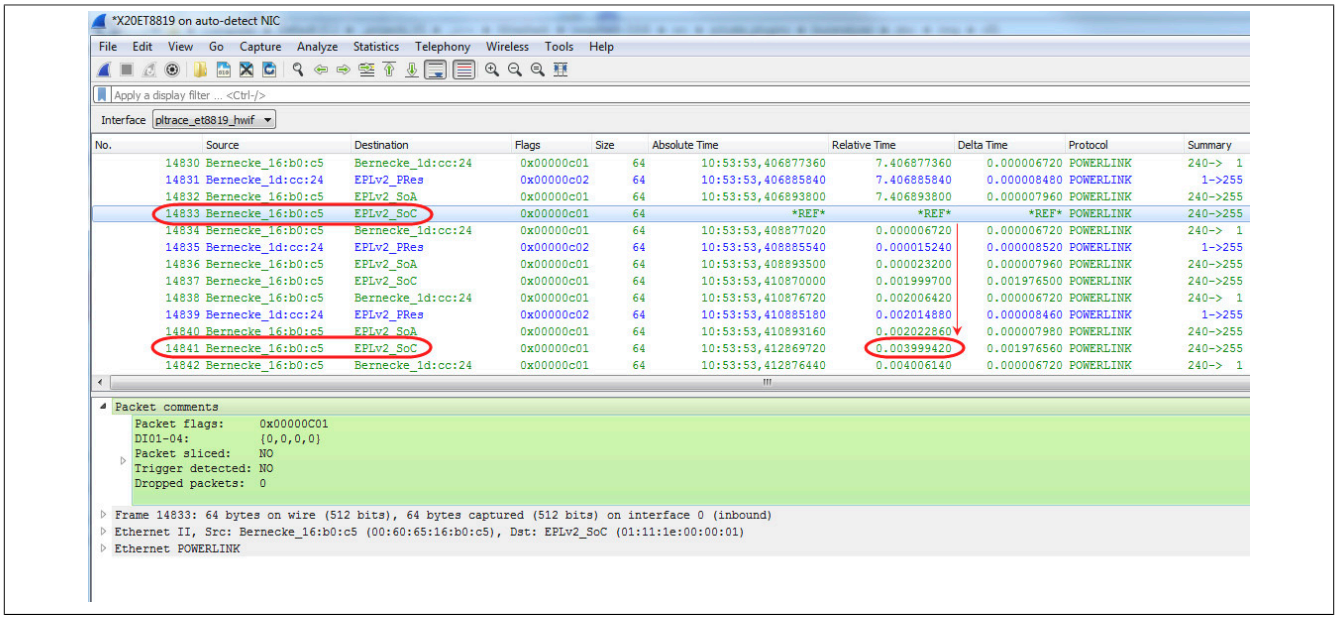


Abbildung 31: Relativzeit wird relativ zum definierten Referenzpaket bestimmt

4.7 Aufzeichnung mit neuer Konfiguration starten

Wenn eine laufende Aufzeichnung gestoppt und eine neue Aufzeichnung mit neuer Konfiguration gestartet wird, muss der Adapter neu gestartet werden.

Vorgehensweise wie folgt:

1. die laufende Aufzeichnung stoppen

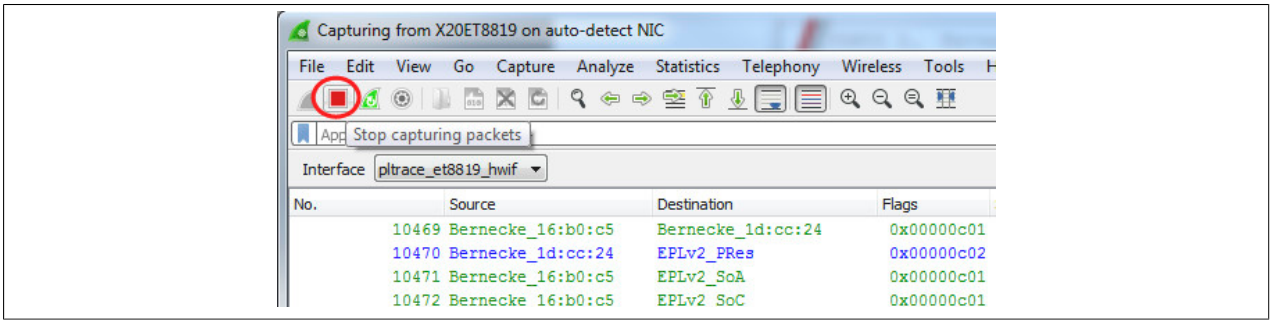


Abbildung 32: laufende Aufzeichnung stoppen

2. aktuelles Capture schließen

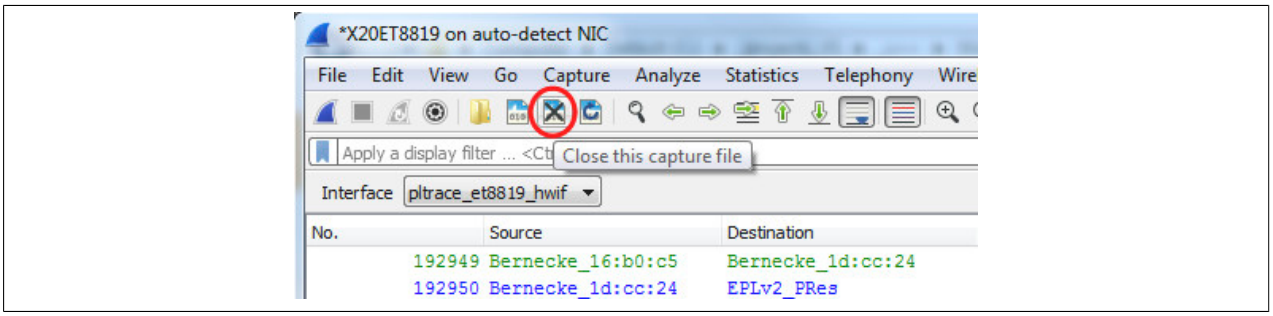


Abbildung 33: aktuelle Aufzeichnung schließen

3. Adapterkonfiguration modifizieren und neue Aufzeichnung starten

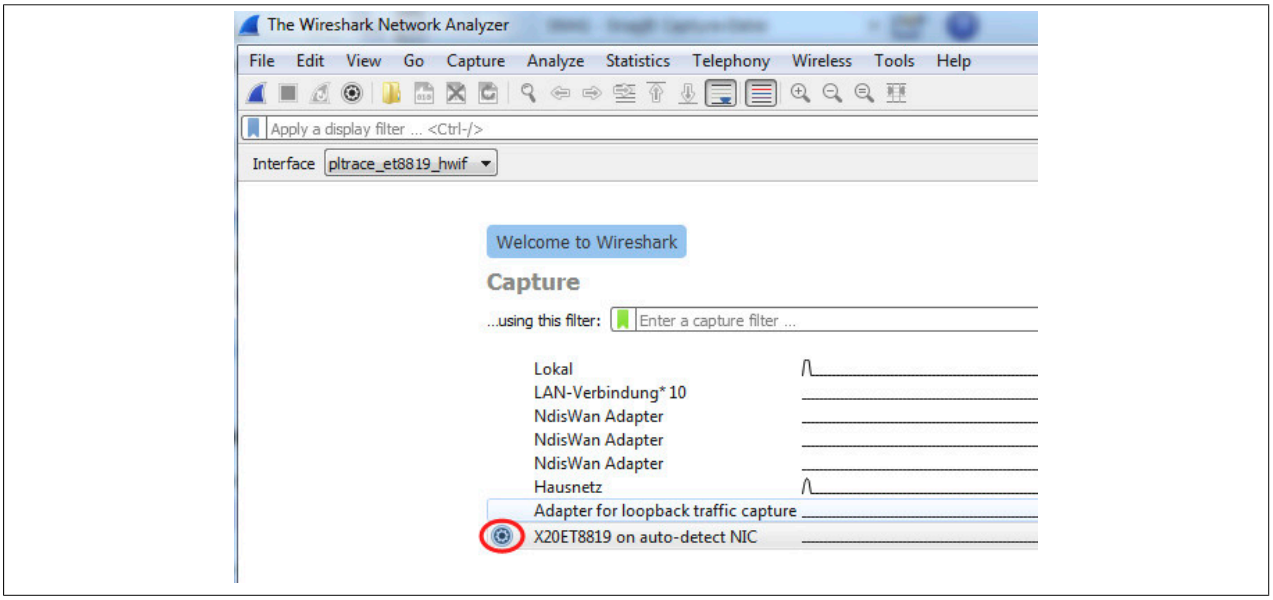


Abbildung 34: Adapterkonfiguration anpassen

4.8 Performancesteigerung bei großen Capture-Files

Wireshark schreibt im Hintergrund alle Daten in ein Temporäres File und stellt diese im Captur Fenster dar. Um die (trotz SSD-Festplatten) relativ performance-intensiven Festplatten-Zugriffe zu reduzieren, könnte man sich z.B. eine RAM-Disk am System anlegen und Wireshark so konfigurieren, dass die temporären Files auf dieser RAM-Disk angelegt werden. Dies führt zu einer erheblichen Performence-Steigerung beim Arbeiten mit großen Captur-Files.

Zum Anlegen einer RAM-Disk am System eignen sich Rools wie z.B. „ImDisk Toolkit“.

Damit die Temporären Files automatisch auf der RAM-Disk ausgelagert werden, können einfach die Systempfade „TEMP“ & „TMP“ explizit für Wireshark auf die RAM-Disk verlegt werden. Dafür kann z.B. einfach ein .bat File erstellt werden über dieses Wireshark in Zukunft gestartet wird.

```
@echo off
SET TEMP=W:\Temp
SET TMP=W:\Temp
start "" "C:\Program Files\Wireshark\Wireshark.exe"
exit
```

Tabelle 3: Batch File zum Starten von Wireshark mit angepasstem TEMP / TMP Pfad

Alternativ kann auch für jede Aufzeichnung bei Bedarf der Pfad manuell adjustiert werden.

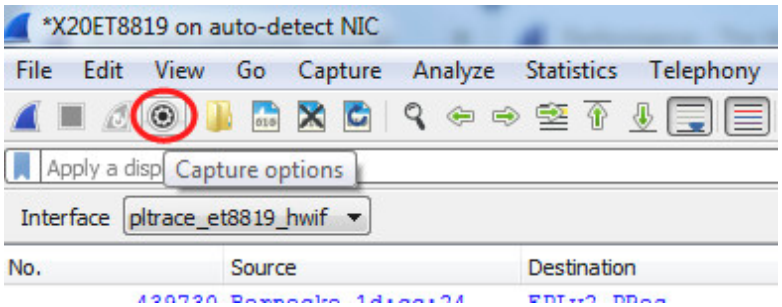


Abbildung 35: Capture Options bearbeiten

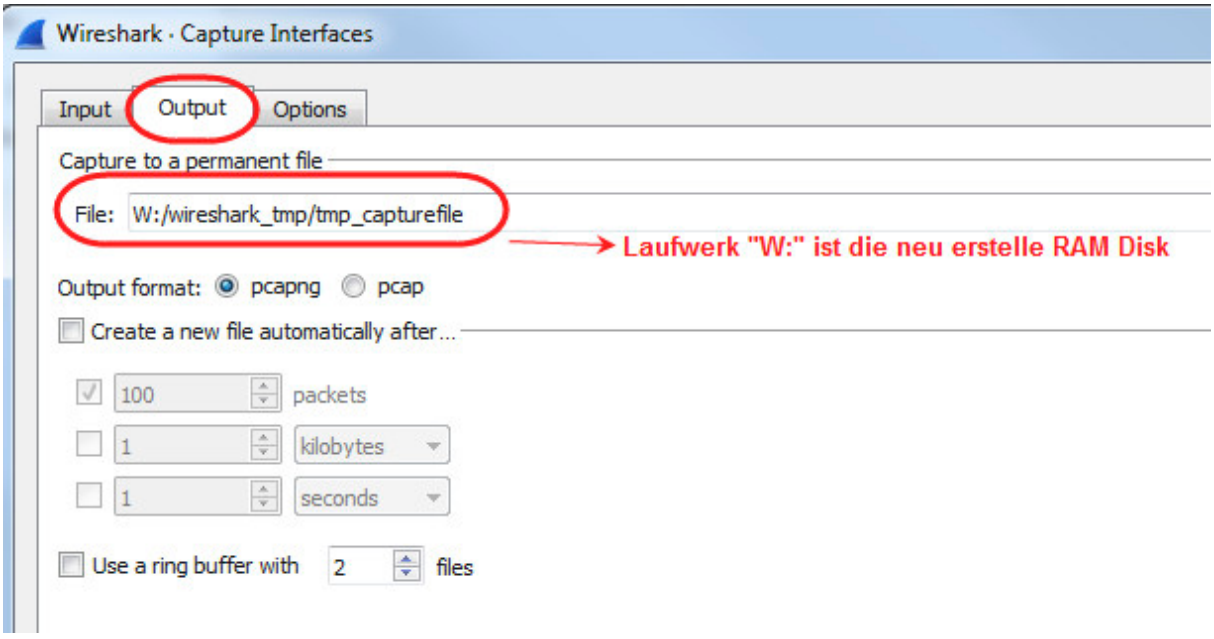


Abbildung 36: Output File auf die RAM-Disk legen

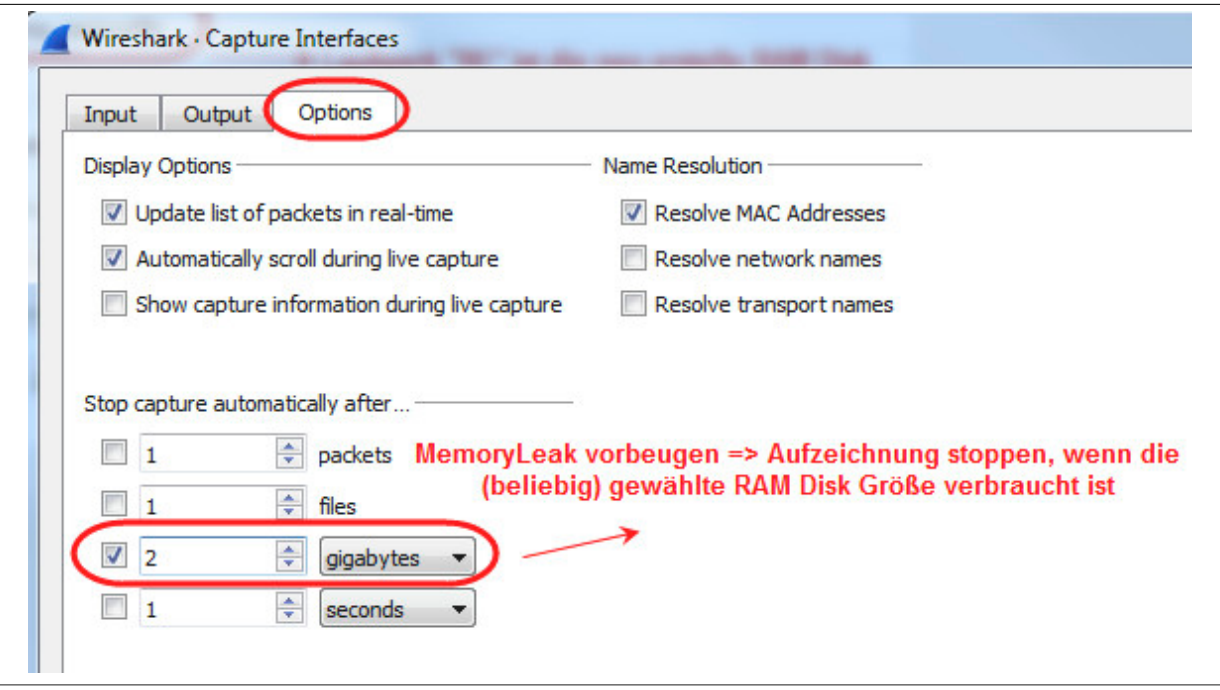


Abbildung 37: MemoryLeak vorbeugen