

M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

Historie

Dokument erstellt

Rolf Maier Caflisch

16. Februar 2018

Inhalt

1 Wireshark: Netzwerk analysieren - so geht's	2
1.1 Einführung	2
1.2 Möglichkeiten von Wireshark	3
2 Arbeiten mit Wireshark	3
2.1 Installation	3
2.2 Aufzeichnung beginnen	4
2.2.1 Filtern des Datenverkehrs	7
2.2.2 Farben der Datenpakete	8
2.3 Konfiguration von Wireshark	9
2.3.1 Promiscuous Mode	10
2.3.2 pcap-ng format	10
2.3.3 Mitschnittlänge, Limit each packet to	11
2.4 Capture Prozess auch zeitlich begrenzen	12
2.5 Filter für bestimmte Paketsorten einsetzen	13
2.6 Aufzeichnung starten	13
2.7 HTTP-Traffic erzeugen	14
3 Abbildungsverzeichnis	15

M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

1 Wireshark: Netzwerk analysieren - so geht's

1.1 Einführung

Diese Anleitung beschreibt die Fehlersuche im Netzwerk mit Hilfe des Open-Source Netzwerk-Sniffers Wireshark. Ein Netzwerk-Sniffer ist eine Software, die den Datenverkehr im Netzwerk aufzeichnet, dekodiert und diesen dann lesbar darstellt.

Das Packet-Sniffer-Tool Wireshark, setzt sich aus zwei Hauptkomponenten zusammen: einem Capture- und einem Analyse-Modul. Das Capture-Modul (engl. capture = erfassen, mitschneiden) zeichnet über einen gewünschten Zeitraum alle Datenpakete auf, die über einen überwachten Netzwerknoten fließen. Den Mitschnitt der übertragenen Datenpakete packt das Tool in eine sogenannte Capture-Datei, die sich im Anschluss von einem Analyse-Tool genauer untersuchen lässt.

Administratoren setzen Packet Sniffer wie Wireshark ein, um beispielsweise Übertragungsfehlern, Funktionsstörungen oder auch Sicherheitsproblemen im Firmennetz auf die Spur zu kommen. Allerdings lassen sich solche Tools auch missbrauchen, um beispielsweise in ungeschützten Datenverbindungen nach übertragenen Passwörtern zu "schnüffeln".

Für die Fehlersuche muss der Rechner mit der Software Wireshark in dem Netzwerksegment betrieben werden, in dem auch der Fehler auftritt. Es genügt aber nicht, dass diese Station an den entsprechenden Switch angehängt wird, da dieser nur Datenpakete weiterleitet, die für den angeschlossenen Rechner bestimmt sind. Manche Switches haben deshalb einen speziellen Monitoring-Port, der den gesamten Datenverkehr spiegelt.

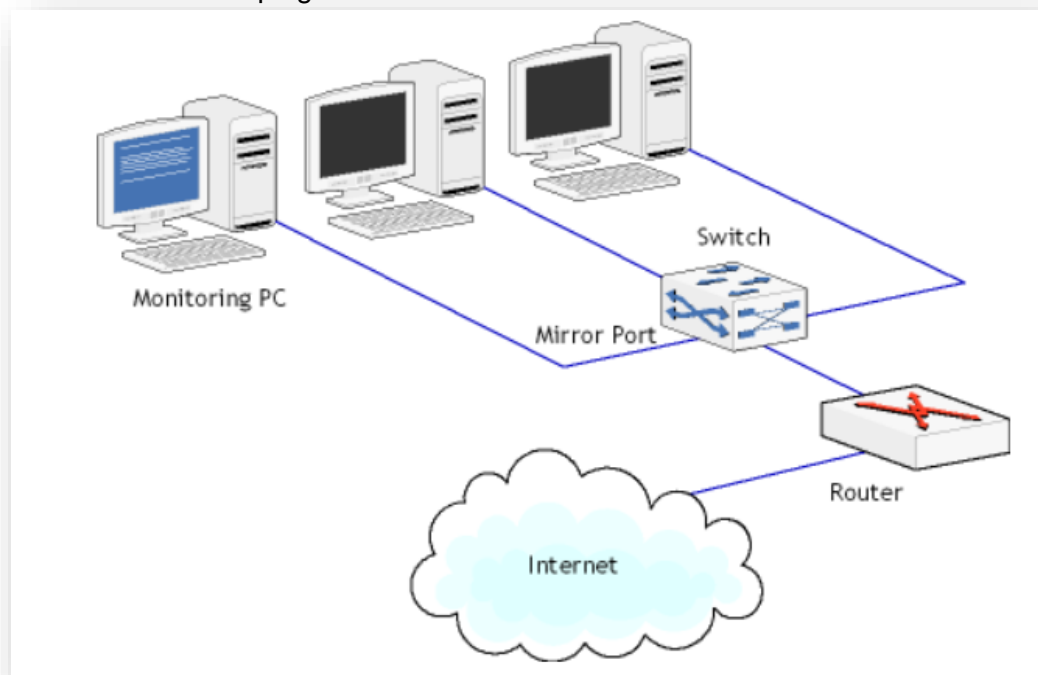


Abbildung 1: Bei einem Switch mit Monitoring-Port: Wireshark auf Monitoring PC

M129	LAN-Komponenten in Betrieb nehmen	Theorie
Wireshark Anleitung		

Falls der Switch keinen Monitoring-Port bietet, dann können Sie diesen auch mit einem einfachen Hub ersetzen, der ebenfalls den Datenverkehr aller Ports erfasst.

Für diese Fälle könnte Wireshark für Sie von Nutzen sein:

- Ihr Netzwerk funktioniert nicht oder ist langsam
- fehlerhaft konfigurierte Clients (DNS, Subnetzmask, IP Adressen)

Ausserdem kann mit Wireshark deutlich gemacht werden, wie leicht Passwörter in verschiedenen Zusammenhängen über das Netzwerk ausgelesen werden können.

1.2 Möglichkeiten von Wireshark

- Fehler finden
- Übertragung optimieren
- Datenstrom überwachen - mit Tools und Apps wie Wireshark behalten Sie den Überblick im Netzwerk.
- Wireshark wird nichts im Netzwerk manipulieren. Das „Messen“ ist die eigentliche Aktivität. Wireshark sendet selber keine Pakete ins Netzwerk ausser, es geht um die Namensauflösungen. Das kann aber deaktiviert werden.

Der Funktionsumfang des Analysetools Wireshark ist gewaltig, weshalb wir dessen umfassende Analysemöglichkeiten im Folgenden nur anreissen werden. Dabei soll zunächst ein Mitschnitt aller Datenverbindungen zwischen Ihrem Windows-Client und dem Internet erstellt werden, indem eine Browser-Verbindung zu einem Webserver im Internet aufgebaut wird. Im Anschluss filtern Sie mit Wireshark nützliche Informationen zu dieser Verbindung aus dem Mitschnitt heraus.

2 Arbeiten mit Wireshark

Die nachfolgenden Übungen können Sie in der Vmware-Umgebung durchführen.

2.1 Installation

1. Melden Sie sich als Administrator am PC1 an.
2. Laden Sie Wireshark für Windows 32-bit von der Internet-Seite <http://www.wireshark.org/> herunter.
3. Installieren Sie Wireshark mit den Standardeinstellungen.

M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

- 2.2 Aufzeichnung beginnen**
- So zeichnen Sie Netzwerkaktivitäten auf:
1. Starten Sie Wireshark am PC1 über "Start | Programme | Wireshark"

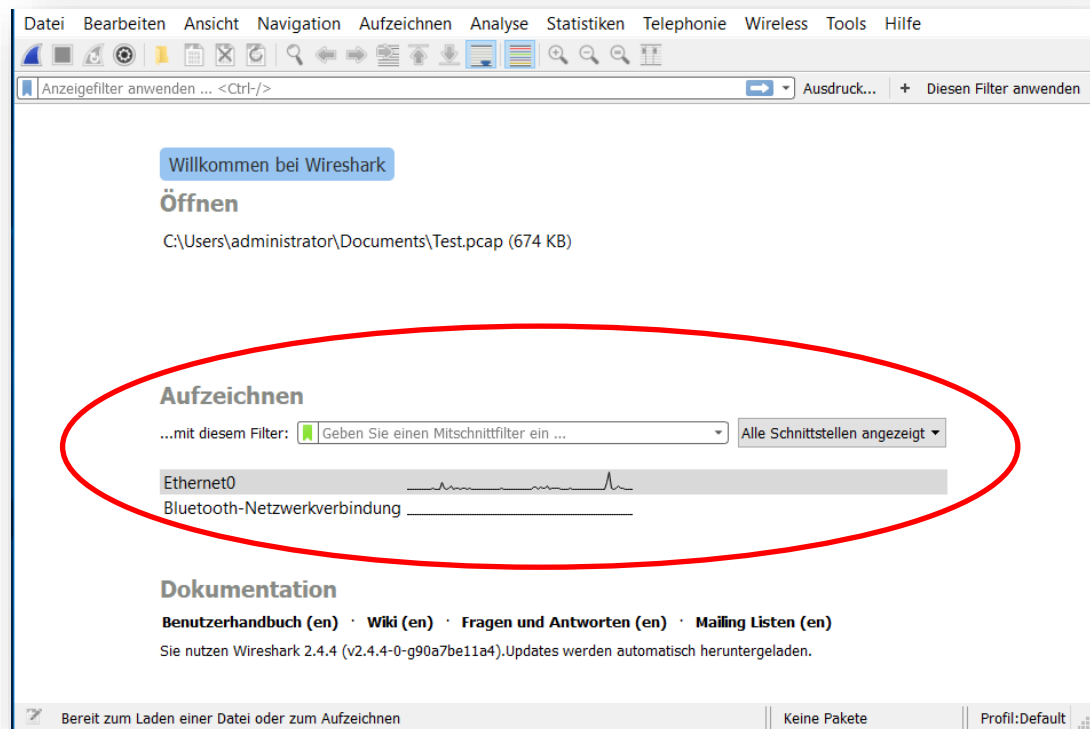


Abbildung 2: Startbildschirm mit Schnittstellen, bei denen der Datenverkehr aufgezeichnet werden kann.

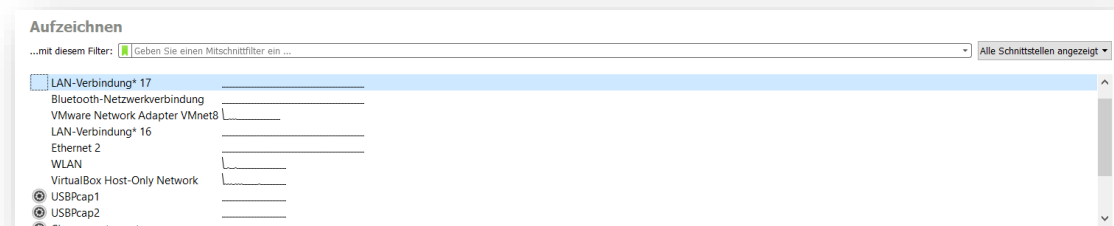


Abbildung 3: Mögliche Netzwerkadapter für die die Aufzeichnung gemacht werden kann.

oder im Legacy-Mode

Start | Programme | Wireshark Legacy

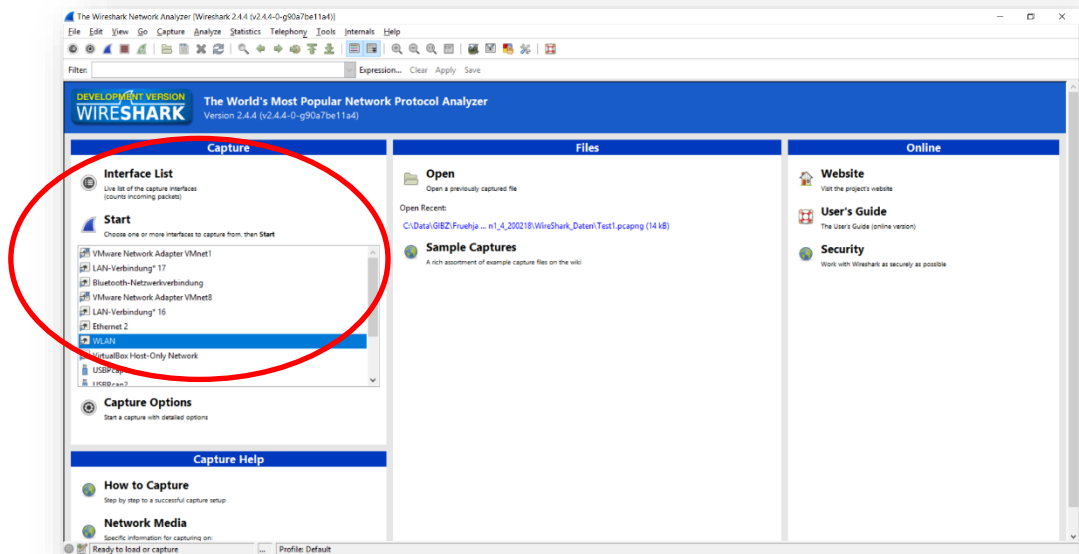
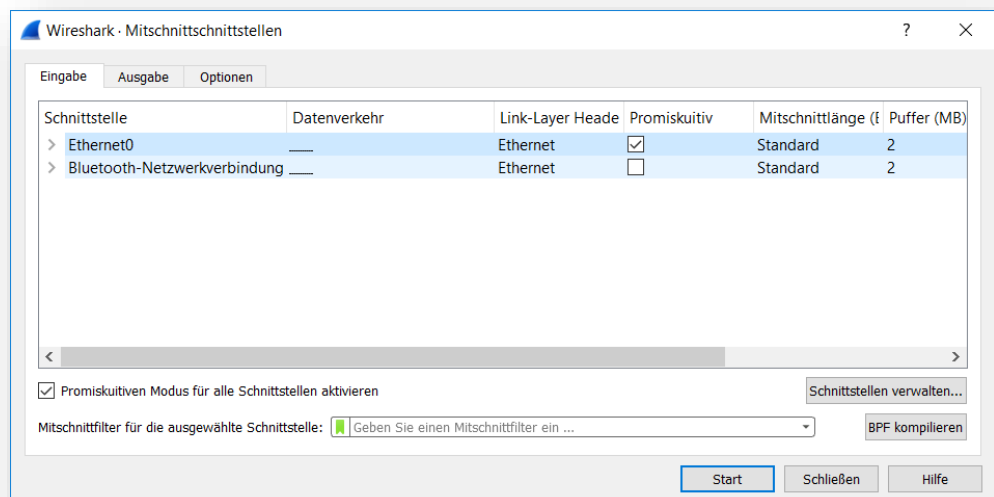


Abbildung 4: Startbildschirm im Legacy-Mode mit Schnittstellen, bei denen der Datenverkehr aufgezeichnet werden kann.

Der Packet Sniffer Wireshark bietet einen Bereich für die eigenen Mitschnitte (Capture) und einen Bereich (Files), um Capture-Dateien (Mitschnitte) zu analysieren.

- Wählen bei "**Aufzeichnen**" (oder im linken Bereich unter dem Menü; Legacy Mode) oder beim Menü "**Aufzeichnen | Optionen**" (Capture | Optionen) das aktive Netzwerk-Interface aus und klicken auf **Start**. Klicken Sie im Menü Capture auf Interfaces...



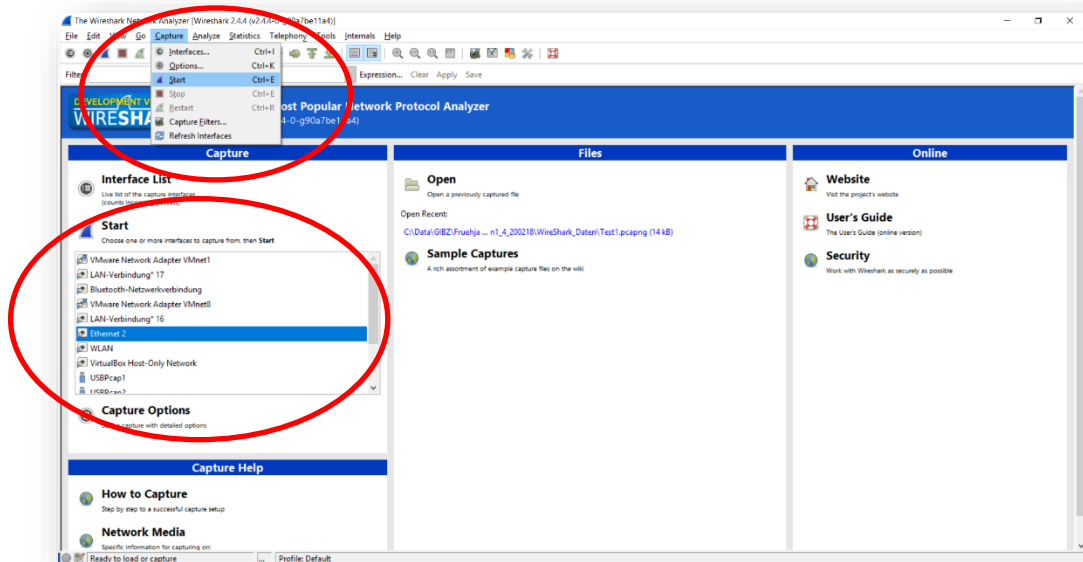
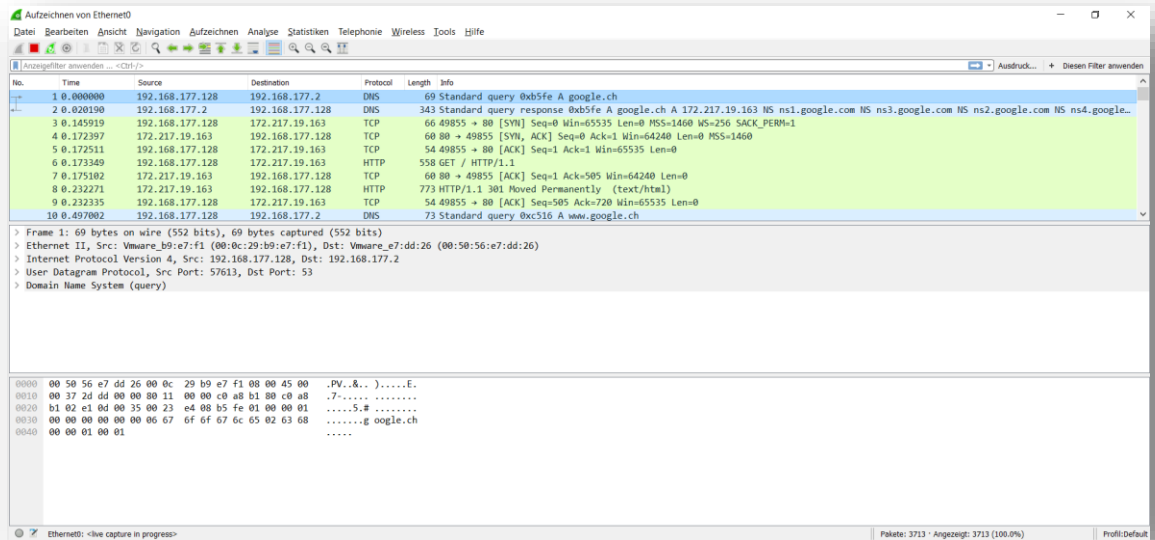



Abbildung 5: Legacy-Mode: Schnittstelle auswählen und Aufzeichnung starten.

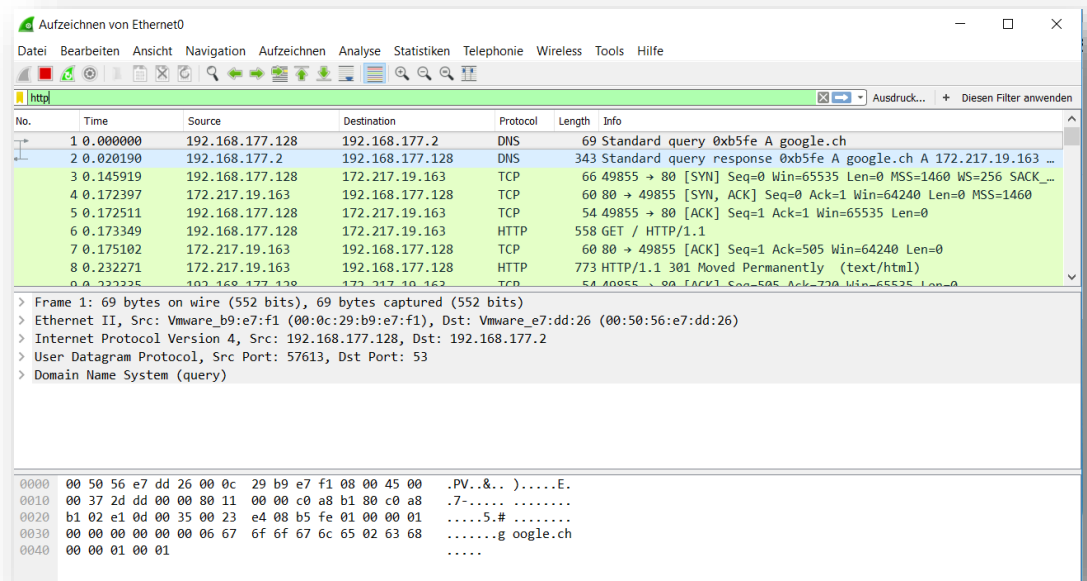
3. Starten Sie den Webbrowser (Edge, Firefox) und rufen Sie eine Internet-Seite auf. Anschliessend sehen Sie den Datenverkehr im Fenster.



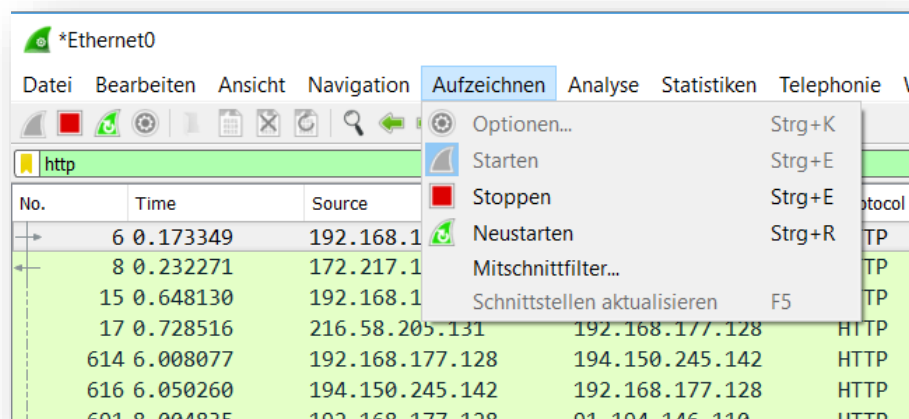
2.2.1 Filtern des Datenverkehrs

Den Datenverkehr können Sie nach verschiedenen Gesichtspunkten filtern. Sie können sich z.B. den Datenverkehr mit dem Protokoll HTTP anzeigen lassen.

1. Geben Sie im Textfeld Filter den Text **http** ein und klicken Sie auf den blauen Pfeil  (Anwenden resp. Apply).



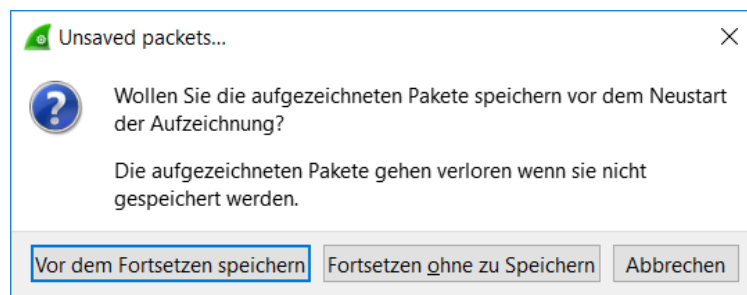
2. Beenden Sie die Aufzeichnung mit "Aufzeichnen | Stoppen" resp. "Capture | Stop".



M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

In den folgenden Beispielen lernen Sie, wie Sie die angezeigten Angaben auswerten können.

Wenn Sie, ohne das Programm zu beenden, eine erneute Aufzeichnung beginnen wollen, wählen Sie die Schaltfläche "**Aufzeichnen | Starten**" und dann **Fortsetzen ohne zu Speichern** resp. **Continue without Saving**:



2.2.2

Farben der Datenpakete

Bereits in der Standardeinstellung färbt Wireshark die Datenpakete anhand von vorgegeben Regeln ein.

"Ansicht | Einfärbungsregeln"

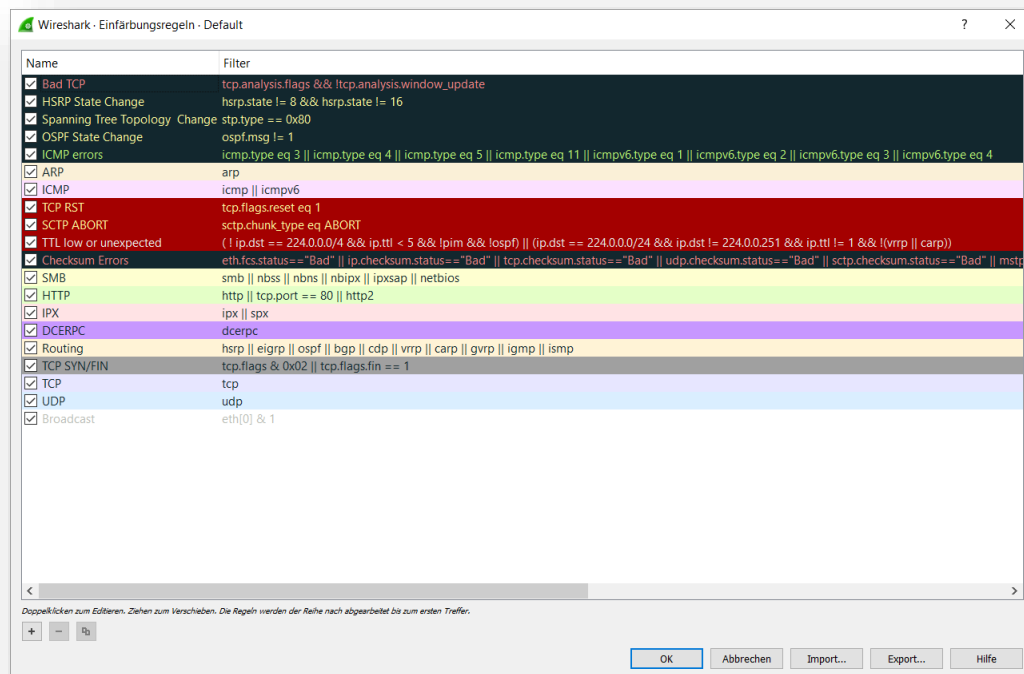


Abbildung 6: Standard-Farbschema für Datenpakete.

In unserem Fall wird ein Mitschnitt über ein paar Sekunden bereits ein recht buntes Werk: Hellblaue Farbe für DNS-Anfragen, leichtes Grün für Standard-TCP-Transfer

M129	LAN-Komponenten in Betrieb nehmen	Theorie
Wireshark Anleitung		

oder hellgelb für Broadcast. Schon nach kurzer Zeit, wenn man Wireshark öfters benutzt, geht das Farbschema in Fleisch und Blut über und der Administrator erkennt schon anhand der Farbe, um was für einen Pakettypen es sich handelt.

Mit eingeschaltetem **Filter** für **http** wird das Farbspektrum deutlich kleiner.

2.3 Konfiguration von Wireshark

Wenn Sie Wireshark zum ersten Mal starten, müssen Sie das Netzwerk Interface auswählen, dessen Netzwerkverkehr Sie analysieren wollen:

"**Aufzeichnen | Optionen ...**" resp. "**Capture | Options ...**", **Register Eingabe**.

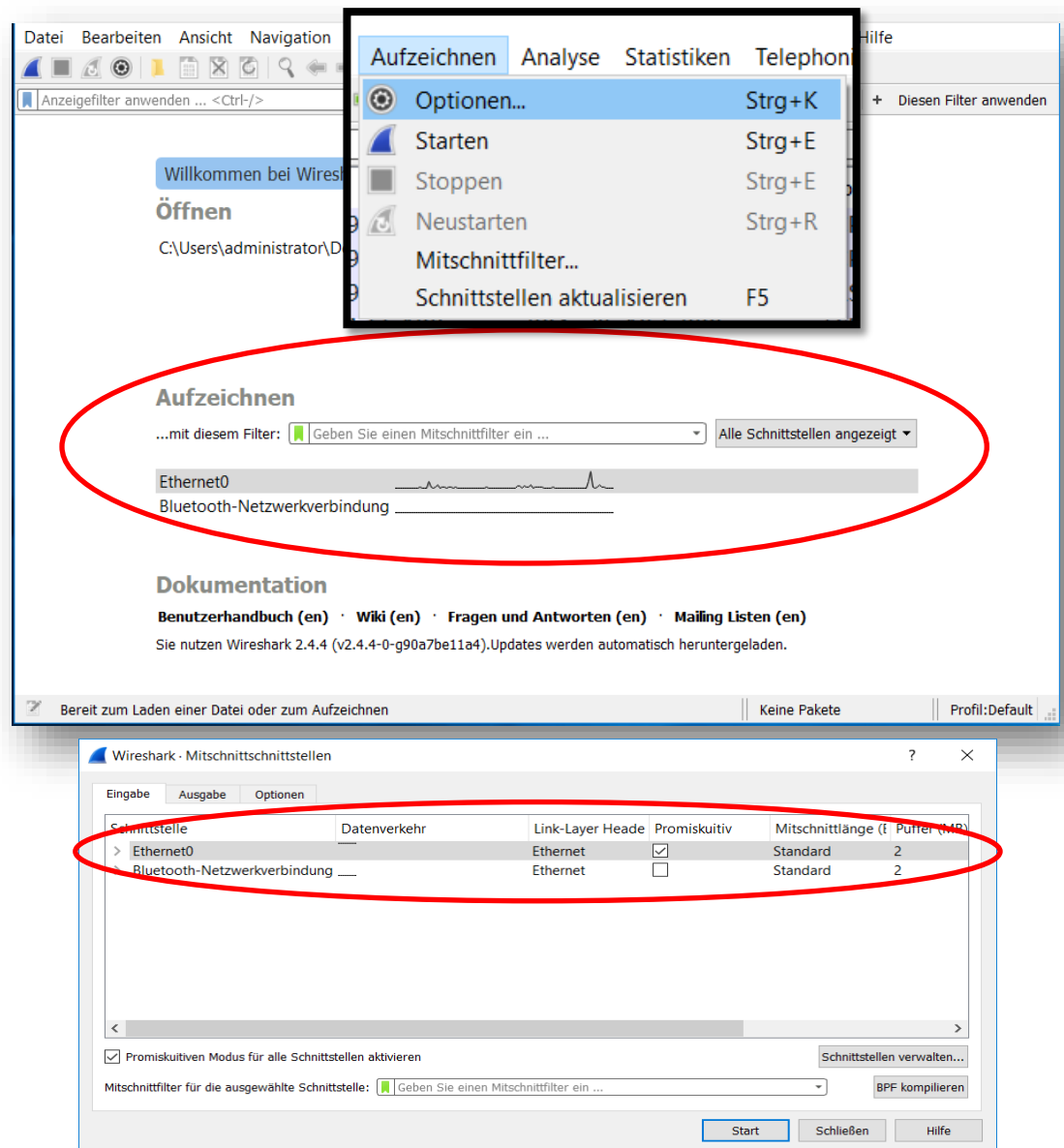


Abbildung 7: Zuerst prüfen wir das ausgewählte Netzwerk Interface.

M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

2.3.1 Promiscuous Mode

Anschliessend müssen die weiteren Aufzeichnungs-Optionen (Capture- Optionen) definiert werden.

Wir sind immer noch bei Wireshark auf **"Aufzeichnen | Optionen ..."** Register Eingabe. Hier legen Sie weitere Kriterien fest, nach welchen Mustern Sie den Datenverkehr scannen möchten.

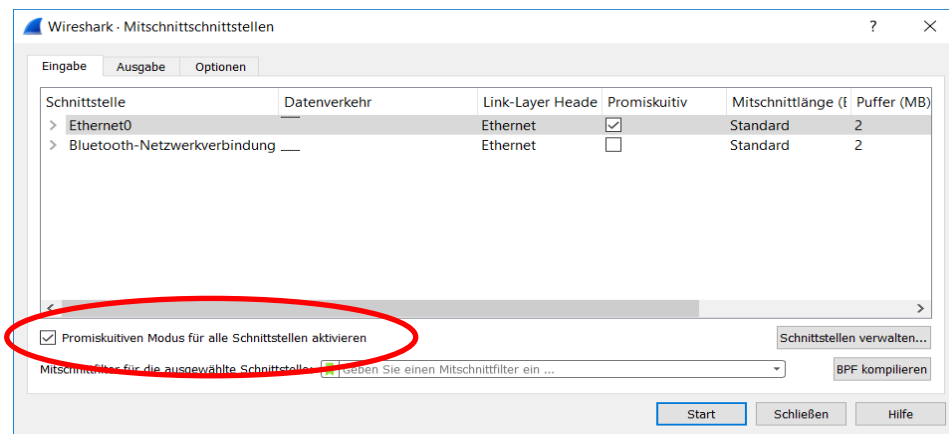


Abbildung 8: Den Promiscuous Mode ein- oder abschalten.

Wenn der Promiscuous Mode aktiviert wird, schneidet Wireshark den ganzen Traffic im Netzwerk mit, den es erkennen kann. Wird der Promiscuous Mode nicht aktiviert, wird nur der Traffic einbezogen, der direkt an unsere oben ausgewählte Netzwerkkarte geschickt wird.

2.3.2 pcap-ng format

Wird der Punkt "pcap-ng" Ausgabeformat aktiviert, werden die Pakete im "next-generation Format" gecaptured. Der Unterschied zwischen den Formaten liegt im Umfang der gesammelten Daten. pcap-ng verwendet z.B. einen erweiterten Zeitstempel, speichert zusätzliche Informationen über die NIC u.v.m.

Der Übersichtlichkeit halber sollte zu Beginn darauf verzichtet werden.

M129	LAN-Komponenten in Betrieb nehmen	Theorie
Wireshark Anleitung		

Wir sind immer noch bei Wireshark auf **"Aufzeichnen | Optionen ..."** Register **Ausgabe**. Hier legen Sie die Kriterien fest, nach welchen Mustern Sie scannen möchten.

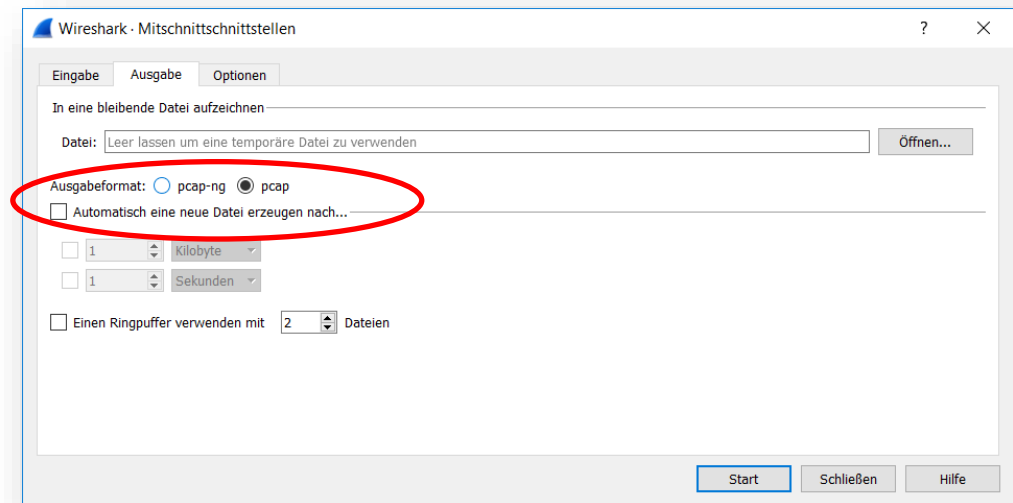


Abbildung 9: Ausgabeformat "pcap" oder "pcap-ng" auswählen.

2.3.3 Mitschnittlänge, Limit each packet to

Hier kann die Grösse eines jeden Pakets beschränkt werden. In der Grössenangabe sind u.a. auch die Headerinformationen enthalten. Ist der Punkt auf **"standard"** eingestellt, gibt es keine Begrenzung.

Wir sind immer noch bei Wireshark auf **"Aufzeichnen | Optionen ..."** Register **Eingabe**. Hier legen Sie weitere Kriterien fest, nach welchen Mustern Sie den Datenverkehr scannen möchten.

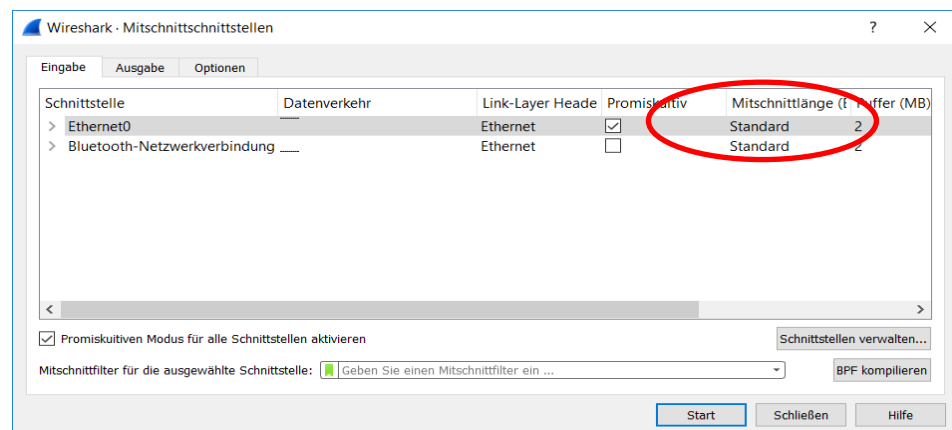


Abbildung 10: Die Paketlänge bei der Aufzeichnung begrenzen (Mitschnittlänge).

M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

2.4

Capture Prozess auch zeitlich begrenzen

Sie können den Capture Prozess auch zeitlich begrenzen. Hierzu wählen Sie das entsprechende Format (Pakete, Kilobytes, Minuten) und tragen einen entsprechenden Wert ein.

Wir sind immer noch bei Wireshark auf **"Aufzeichnen | Optionen ..."** Register **Optionen**. Hier legen Sie die Werte für die zeitliche Begrenzung, die Paketmenge resp. Aufzeichnungsmenge fest.

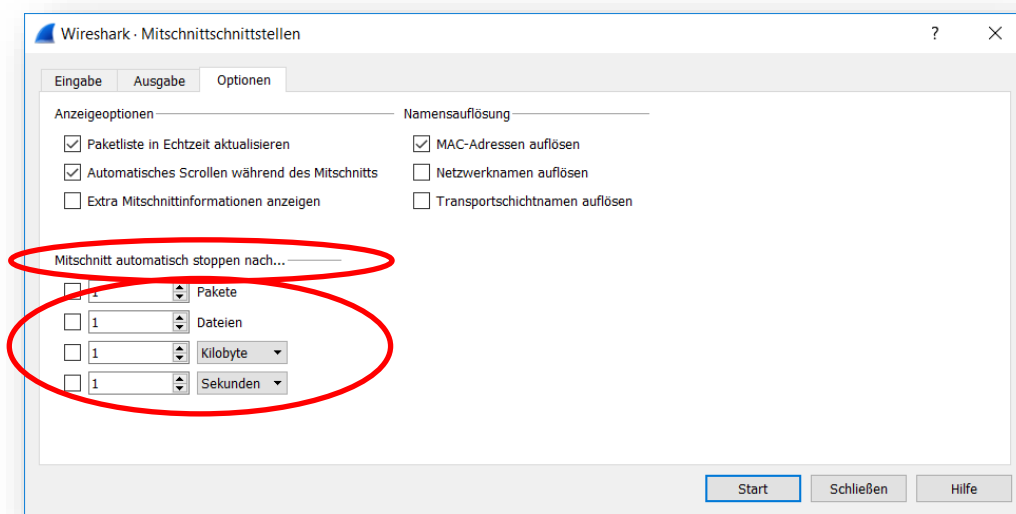


Abbildung 11: Grösse eines jeden Datenpaketes beschränken.

M129	LAN-Komponenten in Betrieb nehmen	Theorie
Wireshark Anleitung		

2.5 Filter für bestimmte Paketsorten einsetzen

Um die sehr umfangreiche Ausgabe etwas einzuschränken, können Sie in Wireshark Filter definieren. Wenn Sie nur nach HTTP Traffic suchen, können Sie den vordefinierten Filter für HTTP benutzen.

Wählen Sie den gewünschten Filter, in unserem Fall fahren wir mit dem HTTP TCP Port (80) Filter fort. Sie können auch eigene Filter definieren oder mehrere Filter mit dem + - Symbol kombinieren.

Klicken Sie dazu auf "**Aufzeichnen | Mitschnittfilter ...**" resp. "**Capture | Filter ...**".

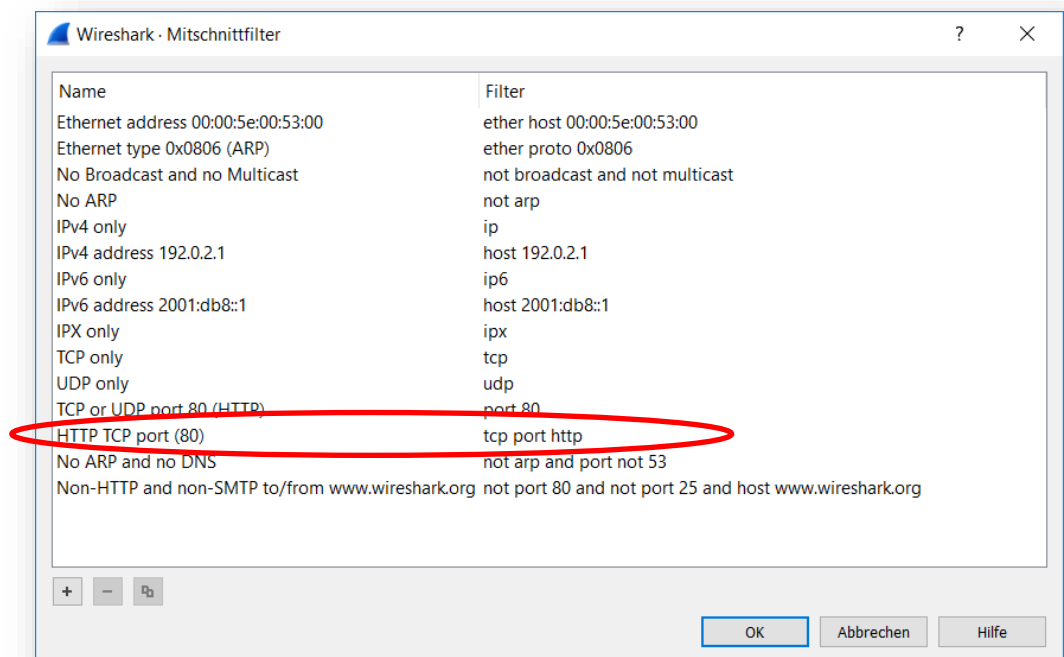
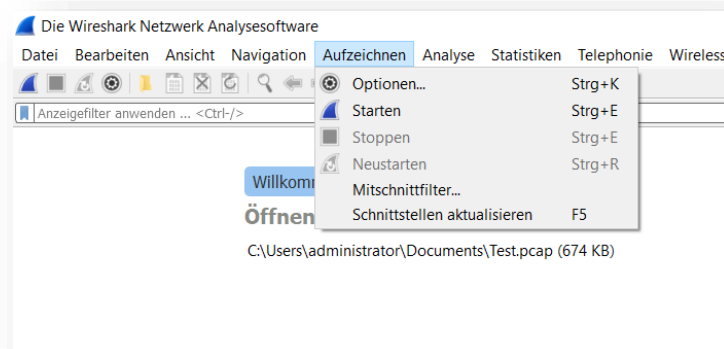


Abbildung 12: Wählen Sie das Filter HTTP TCP Port (80).

Klicken sie anschliessend auf "OK".

2.6 Aufzeichnung starten

Starten Sie nun den Capture Vorgang, indem Sie auf "Start" klicken.



M129	LAN-Komponenten in Betrieb nehmen	T heorie
Wireshark Anleitung		

Anschliessend haben Sie die Möglichkeit, die aufgezeichneten Pakete je nach Bedarf zu analysieren und auszuwerten.

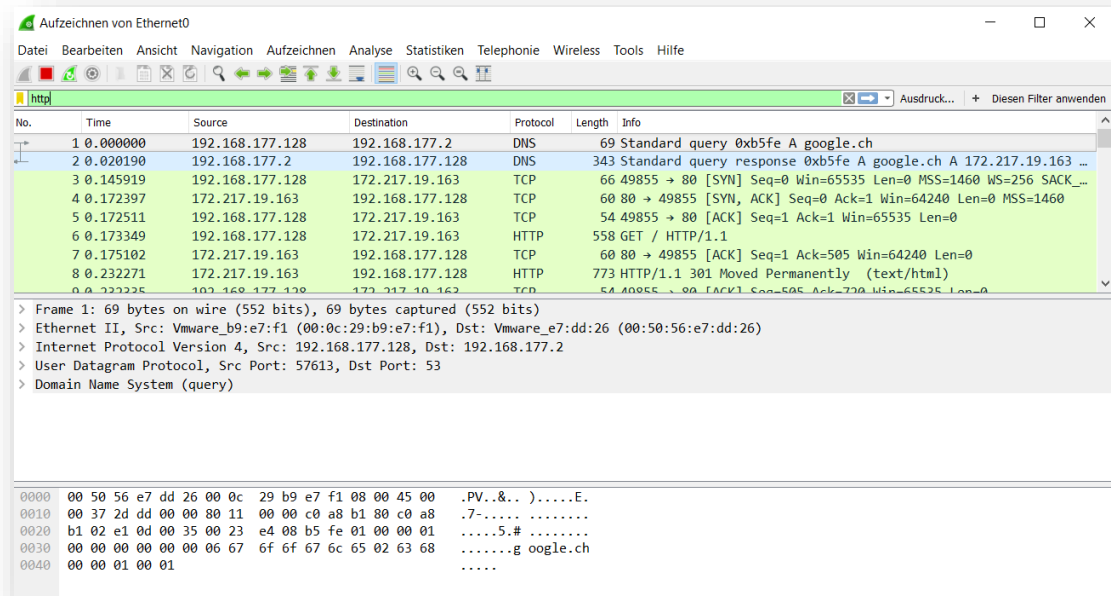


Abbildung 13: Aufgezeichnete Pakete mit aktivem "http-Filter".

Das Capture kann nach unterschiedlichen Kriterien sortiert und ausgewertet werden. Durch einen Klick auf die Pakete bekommen Sie genauere Informationen angezeigt.

2.7

HTTP-Traffic erzeugen

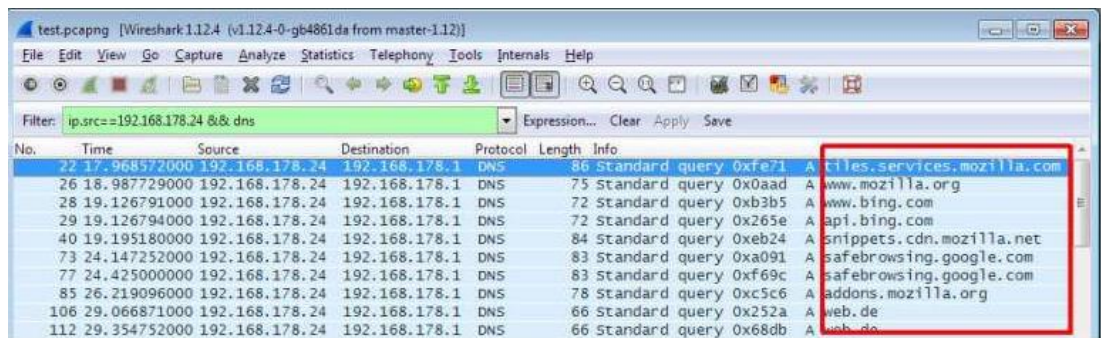


Abbildung 14: Mithilfe eines DNS-Filters zeigt Wireshark die angefragten Domains der Heimnetz-Clients an.

Je nach Anwendungsfall bietet Wireshark von Haus aus weitere und tiefergehendere Möglichkeiten zur Traffic Analyse.

M129	LAN-Komponenten in Betrieb nehmen	Theorie
Wireshark Anleitung		

3 **Abbildungsverzeichnis**

Abbildung 1:	Bei einem Switch mit Monitoring-Port: Wireshark auf Monitoring PC	2
Abbildung 2:	Startbildschirm mit Schnittstellen, bei denen der Datenverkehr aufgezeichnet werden kann.	4
Abbildung 3:	Mögliche Netzwerkadapter für die die Aufzeichnung gemacht werden kann.	4
Abbildung 4:	Startbildschirm im Legacy-Mode mit Schnittstellen, bei denen der Datenverkehr aufgezeichnet werden kann. Der Packet Sniffer Wireshark bietet einen Bereich für die eigenen Mitschnitte (Capture) und einen Bereich (Files), um Capture-Dateien (Mitschnitte) zu analysieren.	5
Abbildung 5:	Legacy-Mode: Schnittstelle auswählen und Aufzeichnung starten.	6
Abbildung 6:	Standard-Farbschema für Datenpakete.	8
Abbildung 7:	Zuerst prüfen wir das ausgewählte Netzwerk Interface.	9
Abbildung 8:	Den Promiscuous Mode ein- oder abschalten.	10
Abbildung 9:	Ausgabeformat "pcap" oder "pcap-ng" auswählen.	11
Abbildung 10:	Die Paketlänge bei der Aufzeichnung begrenzen (Mitschnittlänge).	11
Abbildung 11:	Grösse eines jeden Datenpaketes beschränken.	12
Abbildung 12:	Wählen Sie das Filter HTTP TCP Port (80).	13
Abbildung 13:	Aufgezeichnete Pakete mit aktivem "http-Filter".	14
Abbildung 14:	Mithilfe eines DNS-Filters zeigt Wireshark die angefragten Domains der Heimnetz-Clients an.	14