# Vertiefung in Wireshark

## Informationsquellen zu Wireshark

Wireshark spezifische Informationsquellen und Beispiel-Capture-Dateien

- https://ask.wireshark.org/ → Wissensdatenbank
- https://wiki.wireshark.org/ → Wiki zu Wireshark (hier sind auch Samples)
- https://wiki.wireshark.org/SampleCaptures

Weitere Informationsquellen zu Netzprotokollen

- RFC-Datenbank: http://www.rfc-editor.org/
- Port-Liste: http://www.iana.org/assignments/service-names-port-numbers
- IP-Verwaltung: https://apps.db.ripe.net/search/query.html

## Wichtige Einstellungen

`Edit → Preferences → Name Resolution` `Resolve MAC addresses: DISABLE (default: ENABLE)` Ist Geschmacksache; Schnittstellenhersteller wird dann nicht mehr angezeigt.

`Use external network name resolver: DISABLE (default: ENABLE)` Hostnamen werden nicht mehr per DNS aufgelöst; vermindert Traffic im Netz

`Resolve transport names: ENABLE (default: DISABLE)` Protokollnamen werden anhand der Ports aufgelöst.

Optional: `GeoIP database directories`: Datenbank einbinden DB unter http://dev.maxmind.com/geoip/geolite runterladen und auspacken. In `wireshark` einbinden Zeigt den Standort der IP an. ????BILD????

### Profile

Hat man sich besondere Einstellungen oder Filter erarbeitet, so kann man diese in einem eigenen Profil abspeichern, um sie später wiederzuverwenden. Rechtsklick am unteren rechten Rand des Programmfensters auf `Profile: Default`.

????BILD????

## Umgang mit Filtermöglichkeiten

Wireshark kennt im wesentlichen drei Filterebenen:

1. `wiretap` → Quelle Datenträger mit Kommentarfunktionen (aufgezeichnete Caputures)

2. dumpcap → Live-Capture über Schnittstellen; Capture-Filter wirken bereits zur Aufnahme
3. Coreengine → Dissectoren; Plugins über LUA-Scripte; Display-Filter wirken nur auf Anzeige

Bei den Filtern sollte darauf geachtet werden, wie viele Daten anfallen. Bei Langzeitmitschnitten sollte man mit Capture-Filtern Pakete verwerfen, die nicht von Interesse sind. Will man das Netz analysieren, sollten hingegen mit Display-Filtern gearbeitet werden, da diese Pakete dynamisch ein- und ausblenden, ohne diese zu verwerfen.

Jedes Protokollfeld kann als Filter verwendet werden. Oft kennt man nicht den genauen Dissectornamen bzw. die Struktur in der Wireshark diese abgelegt hat.

**TIPP:** Mit einem Rechtsklick auf das betreffende Feld kann man dieses als Filter einfügen `Apply as Filter Selected`. Dabei stehen mehrere Möglichkeiten zur Wahl. Mit Prepare a Filter wird der Wert nur in den Filter übernommen, aber noch nicht aktiviert. Durch `Not` oder **…**`and Selected` lassen sich so komplexe Filter zusammenbauen.

????BILD????

Eine weitere Möglichkeit ist das Hinzufügen von Protokollfeldern als Anzeigespalte. Dies geschieht ebenfalls mittels Rechtsklick und `Apply as Column`.

Hierdurch ist es möglich wie bei Listen üblich die neue Spalte als Sortierkriterium auszuwählen. Damit kann man vor allem in großen Paketmengen sehr leicht Häufungen von Protokollinhalten erkennen.

`Conversations` ist ebenfalls eine sehr interessante Informationsquelle. Dieses Menü befindet sich unter `Statistics → Conversations`. Der Dialog ist mit Reitern für die unterschiedlichen mitgeschnittenen Protokolle versehen. Auf jedem Reiter werden die Detailinformationen zu den erkannten Kommunikationsbeziehungen aufgeführt (Anzahl Pakete, Bytes; Dauer etc.). Aus dieser Tabelle lassen sich Rückschlüsse über das lokale Netz machen. Welche PCs verwenden ARP oder `NetBIOS`? Diese können nur im lokalen Netz sein, in dem sich der Wireshark-PC befindet. Über die Ethernet-Tabelle lassen sich Schnittstellen finden, die per Filter auf weitere Kommunikationsbeziehungen untersucht werden können. PCs mit hohem Paketaufkommen deuten auf Server hin usw.

**TIPP:** Auch in diesem Dialog funktioniert Rechtsklick und `Apply as Filter`. **TIPP:** Hat man im mittleren Packet Details-Bereich ein Protokollfeld ausgewählt, so wird der von Wireshark verwendete Feldname in der Statuszeile unten links angezeigt.

????BILD????

Links neben diesem Feld befindet sich ein grün, gelb oder roter Kreis, der Auskunft über den Zustand des sogenannten Expertensystem gibt. Dieses kann ebenfalls zu Analysezwecken herangezogen werden. Wireshark verfügt über eine Heuristik, die auf Unregelmäßigkeiten aufmerksam macht. Hierdurch kann man schnell zu Fehlern oder Warnings navigieren.

Eine weitere Informationsquelle ist die `Statistics → Protocol Hierarchy`. Hier werden alle mitgeschnittenen Protokolle nach ihrer Häufigkeit aufgeführt. Auch hier lassen sich Unregelmäßigkeiten entdecken. Z.B. Warum werden viele ARP-Anfragen durchgeführt, wenn nur wenige IP-Adressen aktiv sind?

## Speicherorte

Wireshark speichert seine Konfiguration an verschiedenen Stellen im System. Diese können über den `Help → About Wireshark → Folders` angezeigt werden.

Will man globale Profile oder Konfigurationen vornehmen, so geschieht dies unter Linux im Ordner `/usr/share/wireshark`

Hier liegen u.a. die Dateien: - `dfilters`: enthält einige Basis Filter - `colorfilters`: enthält die Farbregeln für die unterschiedlichen Protokolle

## Weitere interessante Tools

- `tshark` → Kommandozeilen alternative zu `wireshark`
- `tcpdump` → Kommandozeilen alternative zu `wireshark`

# Übungen zum Umgang mit Wireshark

## traceroute

Wie gelingt es `traceroute`, dass alle Zwischenstationen auf dem Weg zu einem entfernten System einzeln aufgeführt werden können?

Führen Sie einen traceroute zu einer entfernten Adresse aus (nicht außerhalb des Schulnetzes möglich). Beobachten Sie die Felder des IP-Headers. Durch welches Feld steuert traceroute, die Rückmeldung der einzelnen Router.

## ARP

Einfache Übung zum Verständnis über den Zusammenhang zwischen MAC und IP-Adressen. Ping von einem Client über einen Router hin zu einem Server.

## Telnet Passwort mitschneiden

Schneiden Sie das Passwort einer `telnet`-Verbindung mit. Eine `telnet`-Verbindung können Sie z.B. auf die Raum-Switche aufbauen.

Filter: tcp.stream eq 0 && frame contains „login“

Beim Filter muss zunächst aus den `Conversations` der richtige Stream gefunden werden. bedeutet erster Stream.

Alternativ: Rechtsklick auf entsprechende `Conversation` und als Filter aktivieren.

Im `Conversations-Dialog` lässt sich eine beliebige Stream auswählen und unten per `Follow stream` in einem eigenen Fenster anzeigen.

**Hinweis:** Eingaben des Benutzers werden bei `telnet` normalerweise als ECHO zurückgeschickt. Daher kommt es an einigen Stellen zu Dopplungen.

## Dateien aus Streams speichern

Werden im Mitschnitt Dateien von einem Fileserver (SMB) geladen, so werden diese im Klartext per SMB transportiert. Nun könnte man die einzelnen SMB-Nachrichten suchen und diese mühselig zusammensetzen.

`Wireshark` bietet aber ein wesentlich mächtigere Option. Diese findet man unter `File → Export Objects → SMB`. In diesem Dialog tauchen alle Share-Freigaben ausgetauschten Dateien auf. Sie können dort per Save oder Save all gespeichert werden. Die Dateinamen können Sonderzeichen enthalten, der Inhalt ist jedoch identisch.

## Firewall-Regeln aus einzelnen Paketen

Unter `Tools → Firewall ACL Rules` verbirgt sich ein sehr praktische Tool, mit dessen Hilfe man sich die Syntax für eine Firewall-Regel anzeigen lassen kann. Dabei stehen unterschiedliche Firewall-Produkte zu Wahl.

Bei `iptables` sollte allerdings kontrolliert werden, ob die richtige `chain` angezeigt wird. Meist wird hier die `INPUT` bzw. `OUTPUT-Chain` angeboten. Bei Router ist dies häufig auf `FORWARD` zu ändern.

Beispiel: `iptables -A INPUT -i eth0 -d 192.168.0.19/32 -j ACCEPT`

## Amplification attack (gefährlich)

DNS-Angriff, bei dem der Absender gefälscht wird und das Opfer angegeben wird. Der Angreifer stellt eine DNS-Anfrage für sehr viele Domains und lässt die Antwort auf der Opfer „prasseln“.

# Analyse des testdump

Zunächst müssen Sie den testdump im wireshark öffnen. Der testdump befindet sich auf dem Server im Austausch-Ordner. Sie erreichen diesen über folgende Adresse: http://raumserver/~lehrer

# Überblick verschaffen

Zunächst verschaffen wir uns einen Überblick darüber welche Maschinen sich im lokalen Netz befinden

- Wie viele Maschinen befinden sich im lokalen Netz?
- Welche MAC- und welche IP-Adressen haben diese?
- Welche Aufgabe haben die einzelnen Maschinen vermutlich?

**TIP:** `Conversations-Dialog`

# Protokolle überprüfen

- Welche Protokolle kommen zum Einsatz?
- Gibt es auffällige Häufungen bei einzelnen Protokollen?

**TIP:** Protocol-Hierarchy

# Ein Client betritt die Domain

Es ist bekannt, dass ein Client während des Mitschnitts einer Domaine beigetreten ist.

- Wie lautet die Domaine?
- Wie lautete der Hostname vor und nach dem Domainenbeitritt?
- Wie lautet der Hostname des Active Directory-Servers?
- Welche Maschinen waren dabei noch beteiligt?

**TIP:** Suchen Sie nach häufigen Ziel-IP-Adressen. Suchen Sie nach FQDN [1)] und identifizieren Sie, welche Rolle diese Rechner einnehmen.

# Vorbereitung eines Hacker-Angriffs

Während des Mitschnitts fand der Versuch eines Hacker-Angriffs statt.

- Woran kann man dies identifizieren?
- Wie lautet die IP-Adresse des Angreifers?
- Was könnte er gefunden haben?

**TIP:** Suchen Sie nach Häufungen bei den Protokollen. Suchen Sie nach Häufungen bei den Sende-IP-Adressen.

1)

FQDN: Full qualified domain name; Rechnername inkl. Domain