OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Fakultät Informatik und Mathematik

COMLAB
Datenkommunikation und Netzwerke

Prof. Dr. Waas

Praktikum zum Fach

**Kommunikationssysteme/
Rechnernetze**

Übung

TCPIP 4

TCP und UDP

Linux

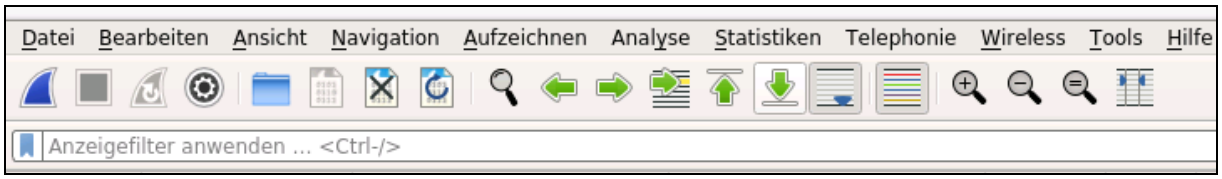
(Version 21.06.2023 KVM)

1 EINFÜHRUNG

Ziel dieser Übung ist es, sich mit dem TCP- bzw. UDP-Protokoll vertraut zu machen. Zuerst sollen Sie vorbereitete Capture-Dateien analysieren und dabei die Besonderheiten und spezielle Mechanismen des Protokollablaufs untersuchen und sich verdeutlichen. Hervorzuheben sind dabei Datensicherung und Flusskontrolle. Dies soll durch die Verwendung von geeigneten Filtern unterstütz werden. Kontrollfragen sollen Ihnen bei der Einschätzung des Erreichens des gesetzten Lernzieles unterstützen. Danach sollen Sie Ihre Kenntnisse anhand eigener Messungen im Internet vertiefen.

2 ANALYSE DER TCP SCHICHT

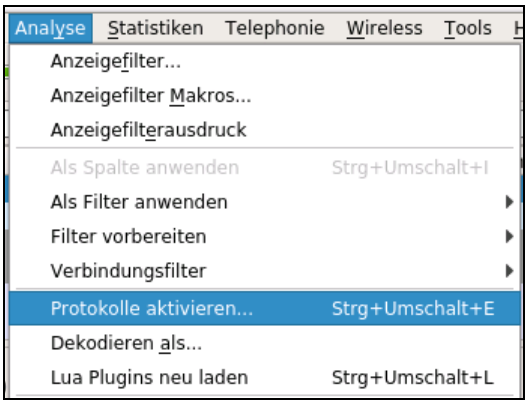
- Starten Sie auf dem lokalen Labor-PC das Programm **WireShark**
- Öffnen Sie das **Datei Menü** und wählen Sie **Öffnen...** aus.



- Wählen Sie im geöffneten Dateibrowser von Wireshark die Datei **/home/kurs/D/captures/FTP.ENC**. Diese Datei enthält die Aufzeichnung einer FTP-Session.

Um die TCP-Schicht besser untersuchen zu können, wird zunächst die darüber liegende FTP-Schicht im Summary-Fenster ausgeblendet. Vergessen Sie bitte nicht diese Änderungen am Ende der Übung wieder **rückgängig zu machen**.

- Öffnen Sie das **Analyse** Menü und wählen Sie **Protokolle aktivieren...**



- Suchen Sie in der Liste der Protokolle die Einträge für **FTP** und **FTP-Data** und **disablen** Sie beide. Klicken Sie dann auf **OK**.

Nun sehen Sie im Summary-Fenster bei allen FTP-Paketen nur noch die zur TCP-Schicht gehörenden Informationen.

- Filtern Sie nun alle Pakete, die zur FTP-Session gehören und blenden Sie alle übrigen aus

Displayfilter: tcp

- Vollziehen Sie nun den Sequence/Acknowledgement Ablauf für die Datenrichtung vom **FTP-Server 131.188.3.71 zum Host 194.95.109.136** bis einschließlich Paket Nr. 19 nach. Versuchen Sie die Sequenznummern und Acknowledgenummern nachzuvollziehen.
- Nutzen Sie nun die Wireshark Unterstützung **Flow Graphs**. Klicken Sie auf einen FTP-Paket im Summary-Fenster. Öffnen Sie das Menü **Statistiken** und wählen Sie **Flow Graph**.
- Nehmen Sie die Einstellungen im Flow Graph Fenster analog dem folgenden Bild vor.

- Interpretieren Sie die Anzeige. Ist diese Form hilfreich?
- Speichern Sie die Darstellung auf Ihrem Memorystick o.Ä.
- Klicken Sie auf **Schließen** und gehen Sie zurück zur Summary-Darstellung und beantworten Sie die folgenden Kontrollfragen.

Kontrollfragen:

- ☑ Welche Nummer hat der FTP-Server Port? Welchen Port verwendet der Client?
- ☑ Was ist bezüglich der Seq/Ack Nummerierung bei den Paketen 4 bis 6 geschehen? Warum blieb der Zähler stehen?
- ☑ Wie wird eine TCP-Verbindung eröffnet? Welche Bits im TCP-Header sind dafür nötig? Wie viele Pakete werden dafür benötigt (3-Way-Handshake)?
- ☑ Wie wird eine TCP-Verbindung geschlossen? Welche Bits im TCP-Header sind dafür nötig? Wie viele Pakete werden dafür benötigt?
- ☑ Was ist bei den Paketen 85 bis 87 geschehen?
- ☑ Ist es möglich, dass IP-Pakete nicht in derselben Reihenfolge ankommen, wie sie abgeschickt wurden?
- ☑ Mit welcher Sequenznummer startet die TCP-Verbindung wirklich?
- ☑ Wie könnten Sie die Anzahl der mit TCP übertragenen Bytes in Paket Nr. 10 ermitteln, wenn Sie die Angabe der Länge (Len=...) nicht hätten?
- Verwenden Sie den folgenden Displayfilter um nach Out-Of-Order-Pakete in der Datei zu suchen:

  Display Filter: tcp.analysis.out_of_order

- Verwenden Sie den folgenden Displayfilter um in der Datei nach doppelten Acknowledge zu suchen:

  Display Filter: tcp.analysis.duplicate_ack

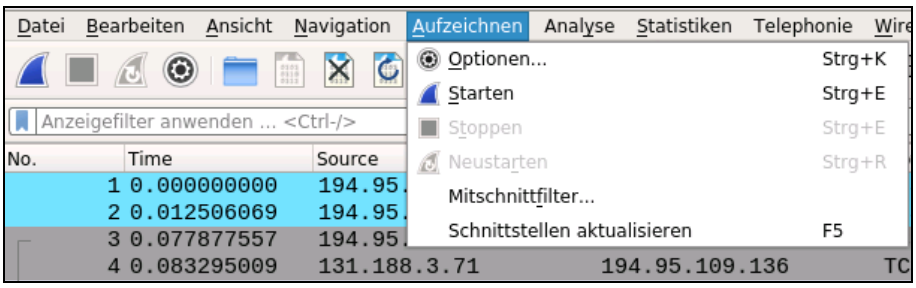
- Verwenden Sie einen geeigneten Displayfilter und überprüfen Sie, ob Datenpakete verloren gingen und wiederholt werden mussten (Retransmission).

- Verwenden Sie einen geeigneten Displayfilter und überprüfen Sie, ob andere Probleme bei der Übertragung aufgetreten sind.
- Machen Sie das Ausblenden der FTP und FTP-Data Protokolls wieder rückgängig.

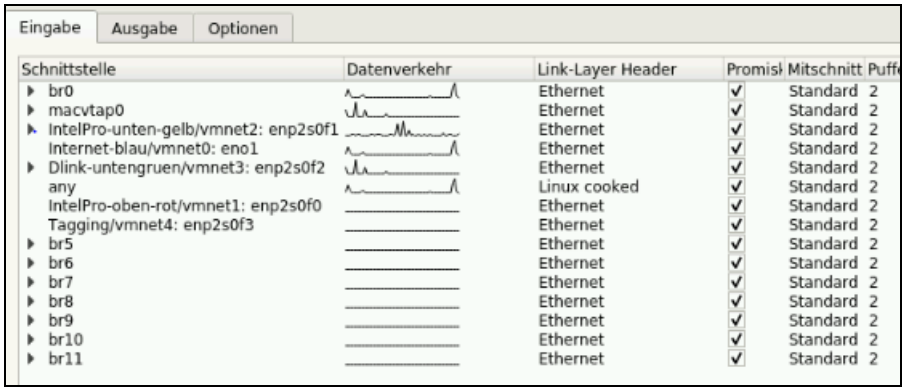
- Löschen Sie den Display-Filter.

3 EIGENE MESSUNGEN IM INTERNET

- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Optionen...** aus.



- Überprüfen Sie, dass der sog. **Promiscuous mode** aktiviert ist bzw. aktivieren Sie ihn.
- Wählen Sie das Interface **Internet blau** aus.



- Öffnen Sie den Webbrowser aber geben Sie noch keine URL ein.
- Klicken Sie auf **Start** um die Messung zu beginnen. Sofort sehen Sie, dass Pakete aufgezeichnet und angezeigt werden.
- Geben Sie nun im Webbrowser die folgende URL ein (IPv4):

http://ipv4server.oth-regensburg.de

- Stoppen Sie die Aufzeichnung in Wireshark und untersuchen Sie die DNS-Auflösung des Internetnamens. Welcher Recordtype (A oder AAAA) brachte bei der DNS-Namensauflösung Erfolg?
- Analysieren Sie die aufgezeichneten Datenpakete auf TCP-Ebene. Verwenden Sie geeignete Displayfilter um nur die Pakete von und zum HTTP-Server anzuzeigen.

Kontrollfragen:

- ☑ Wer beginnt den Verbindungsaufbau auf TCP Ebene?
- ☑ Wie viele TCP-Verbindungen werden für die Übertragung dieser einen Webseite geöffnet? Versuchen Sie mit geeigneten Displayfiltern die Anzahl der angezeigten Pakete einzuschränken, sodass hauptsächlich die gesuchten Pakete übrigbleiben.
- ☑ Welche Optionen werden auf IP- und TCP Ebene ausgehandelt?
- ☑ Können Sie den Inhalt der übertragenen Webseite erkennen?
- ☑ Welcher Recordtype (A oder AAAA) brachte bei der DNS-Namensauflösung Erfolg?
  Hinweis: Falls Sie keine passenden DNS Pakete in Wireshark finden können, löschen Sie den DNS-Cache mit folgendem Befehl und wiederholen Sie die Messung:
  `sudo resolvectl flush-caches`

- Wiederholen Sie nun die Messung mit IPv6. Starten Sie in Wireshark die Aufzeichnung wieder und geben Sie im Webbrowser die folgende URL ein. Benutzen Sie entweder die Schreibweise des Domainnamens oder der IPv6 Adresse:

  http://ipv6server.oth-regensburg.de
  oder
  http://[2001:638:a01:3f80:0:0:0:8089]

- Stoppen Sie die Aufzeichnung in Wireshark und untersuchen Sie die DNS-Auflösung der Internetadresse. Welcher Recordtype brachte jetzt bei der DNS-Namensauflösung Erfolg?
- Analysieren Sie die aufgezeichneten Datenpakete auf TCP-Ebene.
- Vergleichen Sie die beiden Messungen (IPv4 und IPv6) auf TCP- und HTTP-Ebene.

Kontrollfragen:

- ☑ Sind die TCP-Daten bei IPv4 wesentlich anders als bei IPv6?
- ☑ Sind die http-Daten bei beiden Protokollen unterschiedlich?
- ☑ Welcher Recordtype brachte bei der DNS-Namensauflösung Erfolg?
- ☑ Was ist der Unterschied zwischen Recordtgype A und AAAA?
  Hinweis: Falls Sie keine passenden DNS Pakete in Wireshark finden können, löschen Sie den DNS-Cache mit folgendem Befehl und wiederholen Sie die Messung:
  `sudo resolvectl flush-caches`

4 MESSUNG MIT DATENVERSCHLÜSSELUNG

Setzen Sie die Messung von Vorher fort, nun aber mit einem anderen Protokoll. Es ist unerheblich ob dabei IPv4 oder IPv6 verwendet wird.

- Öffnen Sie den Webbrowser aber geben Sie noch keine URL ein.
- Klicken Sie auf **Start** um die Messung zu beginnen. Sofort sehen Sie, dass Pakete aufgezeichnet und angezeigt werden.
- Geben Sie nun im Webbrowser die folgende URL ein (IPv4 oder IPv6):

https://ipv4server.oth-regensburg.de

oder

https://ipv6server.oth-regensburg.de

- Stoppen Sie die Aufzeichnung in Wireshark wieder und analysieren Sie die aufgezeichneten Datenpakete auf http-Ebene. Verwenden Sie geeignete Displayfilter um nur die Pakete von und zum HTTPS-Server anzuzeigen.
  Hinweis: HTTPS läuft über tcp port 443.

Kontrollfragen:

- ☑ Können Sie auf HTTP-Ebene den Inhalt der Webseite erkennen?
- ☑ Was wurde am Anfang zusätzlich übertragen bzw. ausgehandelt?

5 ANALYSE DER UDP-SCHICHT

- Öffnen Sie das **Datei Menü** und wählen Sie **Öffnen...** aus.
- Wählen Sie im geöffneten Dateibrowser von Wireshark die Datei **/home/kurs/D/captures/udp.enc**. Diese Datei enthält die Aufzeichnung einiger UDP Pakete.

Wählen Sie einen UDP-Paket aus und Betrachten Sie ihn in der Detaildarstellung.

Kontrollfragen:

- ☑ Welche Felder hat der UDP-Header im Wesentlichen?
- ☑ Lässt das vermuten, dass es eine Datensicherung und/oder eine Flusskontrolle gibt?
- ☑ Was ist eigentlich die Aufgabe eines UDP-Protokolls?
- ☑ Was könnten Vorteile von UDP gegenüber TCP sein?
- ☑ Was sind die Vorteile von TCP gegenüber UDP?

6 ENDE DER ÜBUNG

- Beenden Sie alle **Programme** und **virtuelle Maschinen**! Im Rahmen der Übung an Ihrem Arbeitsplatz erzielte Messergebnisse können Sie im Labor auf Ihren Memorystick zur späteren Nachbearbeitung abspeichern. Gewonnene sicherheitsrelevante Informationen insbesondere Passwörter, dürfen nicht weitergegeben oder unbefugt verwendet werden. Geht leider nicht im Remotebetrieb.
- **Loggen** Sie sich aus dem Labor-PC **aus!**
- Lassen Sie den PC weiterlaufen. Er wird automatisch ausgeschaltet.

Bitte hinterlassen Sie Ihren Arbeitsplatz in ordentlichem Zustand!
Entsorgen Sie Mitgebrachtes selbst!
Schieben Sie den Stuhl an den Tisch!