

BAI4-RNP	Praktikum Rechnernetze	KRF/SLZ
SS 2017	Aufgabe 1 – Protokolle / Einfacher SMTP-Client	Seite 1 von 2

1 Protokolle

Das Programm **wireshark** (<http://www.wireshark.org>) dient dem Monitoring des Netzwerkverkehrs („Netzwerksniffer“). Sie finden im Pub-Verzeichnis von Hartmut Schulz eine Kurzanleitung für die Laborumgebung und eine komplette Dokumentation (<http://users.informatik.haw-hamburg.de/~schulz/pub/Rechnernetze/>).

1.1 Erzeugen Sie einen Netzwerk-„Sniff“:

- Starten Sie **wireshark** (siehe Kurzanleitung)
- Starten Sie das Monitoring des Netzverkehrs (Capture)
- Starten Sie einen Webbrowser (z.B. Firefox) und besuchen Sie 3 verschiedene Websites
- Speichern Sie den „Sniff“ als Textdatei (csv-Format).
- Beenden Sie **wireshark**

1.2. Analysieren Sie den gespeicherten Netzwerk-„Sniff“:

- Öffnen Sie die gespeicherte „Sniff“-Datei mit einem Tabellenkalkulationsprogramm (z.B. *Excel oder Calc - passen Sie ggf. das Trennzeichen an bzw. verteilen Sie den Text in Spalten*).
- Sortieren Sie die Tabelle nach der Spalte „Protocol“.
- Ermitteln Sie für jedes Protokoll, wie häufig es in der Sniff-Tabelle auftritt, d.h. wie viele Zeilen mit dem Protokoll-Namen es jeweils gibt.
(*Tipp: „Teilergebnis“ – Auswertung in Excel benutzen*).
- Informieren Sie sich über die 6 am häufigsten aufgeführten Protokolle und beschreiben Sie kurz, welche Funktion das Protokoll hat und auf welcher Schicht des Internet-Schichtenmodells es einzuordnen ist.

2 SMTP-Client

2.1 Implementieren Sie eine JAVA-Klasse **MailFile**, die als „User Agent“ einen festgelegten Nachrichtenbody sowie einen beliebigen Dateianhang mittels SMTP-Protokoll zur Weiterleitung an einen SMTP-Server überträgt.

Die Kommandozeilen-Syntax ist wie folgt:

```
java -cp . MailFile <recipient mail address> <file path>
```

Argumente:

- **<recipient mail address>**: Die komplette Mailadresse des Empfängers
- **<file path>**: Der komplette Dateipfad des zu versendenden Dateianhangs

Beispiel:

```
java -cp . MailFile fritz.mueller@haw-hamburg.de C:/Temp/Test.docx
```

Randbedingungen:

- Die Kontodaten des Absenders sowie der Betreff und der Nachrichtenbody sollen aus einer Konfigurationsdatei gelesen werden (*Tipp: Klasse `Properties` verwenden*).
Zu den Kontodaten des Absenders gehören:
 - Mailadresse
 - Benutzername
 - Passwort
 - Hostname (DNS-Name) des SMTP-Servers, der zum Versenden benutzt wird
 - Portnummer für SMTP (25) oder SMTPS (465)
- Wenn die Verbindung zum Mailserver verschlüsselt werden muss (Port 465), verwenden Sie einen TLS(SSL)-Socket!

BAI4-RNP	Praktikum Rechnernetze	KRF/SLZ
SS 2017	Aufgabe 1 – Protokolle / Einfacher SMTP-Client	Seite 2 von 2

- Zur Anmeldung verwenden Sie den SMTP-Authentifizierungsbefehl AUTH mit Angabe von Benutzername und Passwort (AUTH PLAIN), wobei Benutzername und Passwort Base64-codiert übergeben werden müssen (zur Syntax siehe RFC 4954).
- Verwenden Sie MIME 1.0 (RFC 2045) mit dem Content-Type: multipart/mixed und codieren Sie den Datei-Anhang mit Base64!
- Lassen Sie alle gesendeten / empfangenen Nachrichten in einer Log-Datei protokollieren!

2.2 Testen Sie Ihre Implementierung *mindestens* folgendermaßen:

- Verwenden Sie das folgende Konto für den Absender¹:
 - Mailadresse: **rnsose2017@informatik.haw-hamburg.de**
 - Benutzername: **rnsose2017**
 - Passwort: **Aufgabe1**
 - Hostname (DNS-Name) des SMTP-Servers: **mailgate.informatik.haw-hamburg.de**
 - Portnummer: **465**
- Senden Sie mit Ihrer **MailFile**-Implementierung eine Datei im Binärformat (z.B. docx) an den HAW-Mailer-Account Ihres Teampartners (Empfänger-Adresse).
- Führen Sie bei der Abnahme das Absenden sowie das Öffnen der empfangenen Mail inkl. Anhang sowie das Sendeprotokoll (Log-Datei) vor.

Tipps und Hinweise

Ab Java 8 gibt es eine Base64-Implementierung im Package `java.util`!

Wireshark im Labor Raum 765

- Für den Zugriff auf die Netzwerkkarten benötigt Wireshark Administratorprivilegien („Root Privileges“).
- Um mit Root Privileges im Labor 765 arbeiten zu können, müssen Sie den Rechner mit der Linux-Partition "BRV-Special" starten und sich als "networker" (Passwort gibt es im Praktikum oder bei Herrn Schulz) einloggen. Sie werden dann aufgefordert, das Passwort zu ändern. Dieses gilt dann für die Dauer der Sitzung.
- Weiter müssen Sie sich im zweiten Teil der Authentifizierung mit Ihrem persönlichen Benutzernamen und Passwort legitimieren.
- Root-Rechte bekommen Sie grundsätzlich nur mit dem „sudo“-Kommando in einer Terminal-Shell. Als Parameter geben Sie dabei den auszuführenden Befehl (ggf. mit dessen Parametern) an, also zum Starten von wireshark: **`sudo /usr/bin/wireshark`**

Weitere Hinweise für das Labor Raum 765:

- Es nur ausgewählte Befehle mit sudo zugelassen!
- Sie arbeiten unter "BRV-Special" als lokaler Benutzer. Aus Sicherheitsgründen werden nach Sitzungsende alle (!) lokalen Daten gelöscht! Ebenso wird das Passwort zurückgesetzt.
- Ihre persönlichen Daten auf dem Server finden hinter dem Desktopsymbol "MyHome" (diese sind von o.g. Löschung natürlich nicht betroffen).
- Nähere Informationen über die Laborumgebung finden Sie im Public-Bereich von Herrn Schulz:
 - zum Thema Rechnernetze:
<http://users.informatik.haw-hamburg.de/~schulz/pub/Rechnernetze/>
 - zu Linux in Raum 765:
<http://users.informatik.haw-hamburg.de/~schulz/pub/Linux-Einfuehrung/>

Viel Spaß!

¹ Sie können auch Ihren Informatik Mail Account verwenden. Stellen Sie in diesem Fall vorher bitte Ihr Passwort um.