PR Rechnernetze und Netzwerkprogrammierung 621.801/621.802	WS 2017 / 2018
Institut für Informationstechnologie (ITEC)	Rainer/Timmerer
Übungsblatt 03	

U 3.1 Protokolle der Anwendungsschicht

Konsultieren Sie sogenannte RFCs der IETF (erklären Sie die Bedeutung dieser Abkürzungen) um folgende Fragestellungen zu beantworten:

- Beschreiben Sie die folgenden Protokolle hinsichtlich ihrer Eigenschaften und wesentlichen Unterschiede: HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2.0.
- Beschreiben Sie die folgenden Protokolle und wie sie benutzt werden: SMTP, POP3, IMAP. Geben Sie ein konkretes Beispiel für SMTP an und demonstrieren Sie dies mit Hilfe von telnet und mailsrv.uni-klu.ac.at.
- Beschreiben Sie das DNS-Protokoll.

U 3.2 Einführung zu Wireshark

Wireshark (www.wireshark.org) ist ein für viele Plattformen verfügbares Tool zur Aufzeichnung von Netzwerkpaketen bzw. für deren weitere Analyse. Installieren Sie sich eine aktuelle Version dieser Software und machen Sie sich mit der Handhabung vertraut. Laden Sie dazu die Datei dump_protocols.pcap aus dem Moodle Kurs auf Ihren Rechner und öffnen Sie diese Datei mit Wireshark.

- Erklären Sie kurz die Ausgabe des Programms bzw. die Funktionalität der einzelnen Ansichten.
- Welche Möglichkeiten zur Filterung bietet Ihnen Wireshark? Geben Sie ein Beispiel für eine Filterbedingung an.
- Starten Sie selbst eine Aufzeichnung (capture) ihres Netzwerkverkehrs. Erklären Sie die Schritte, die dazu notwendig sind.
- Wozu dient beim Aufzeichnen der promiscuous mode?

U 3.3 Protokolle mit Wireshark

Analysieren Sie die Datei dump_protocols.pcap mit Wireshark und beantworten Sie folgende Fragestellungen:

- Welche Netzwerkprotokolle werden in der Kommunikation verwendet?
- Ordnen Sie jedes der Protokolle einer Schicht im TCP/IP-Referenzmodell zu und stellen Sie die Hierarchie der einzelnen Protokolle graphisch dar.

U 3.4 Wireshark – HTTP

Laden Sie die Datei dump_http.pcap aus dem Moodle-Kurs herunter und analysieren Sie die Datei mit Wireshark. Die Datei beschreibt den Download einer recht trivialen Webseite durch einen HTTP-Client. Beantworten Sie folgende Fragestellungen:

- Welche Objekte werden vom Client via HTTP angefordert?
- Recherchieren Sie die Bedeutung der einzelnen Header-Felder bei den Anfragen bzw. Antworten des Servers.
- Wie viele TCP-Verbindungen werden insgesamt aufgebaut? Wie unterscheidet sich das von dump_protocols.pcap?
- Bestimmen Sie, wie viele Bytes in jeder Verbindung ausgetauscht werden und wie lange die einzelnen Verbindungen bestehen.

U 3.5 Wireshark – HTTP

Verbinden Sie sich mit YouTube, Netflix, Amazon Prime Video oder Maxdome und analysieren Sie grob die Vorgänge beim Streamen eines Videos. Beantworten Sie folgende Fragestellungen:

- Welche Objekte werden vom Client via HTTP angefordert? Hinweis: nur jene beim Videostreaming, andere Objekte (z.B. HTML, Text, Bilder) können vernachlässigt werden.
- Versuchen Sie die Verbindung über unterschiedliche Zugangsnetzwerke (z.B. LAN, WLAN, 3/4G sofern möglich) herzustellen und dokumentieren Sie allfällige Unterschiede.