

**Vorlesung Rechnernetze**

**AIN 5**

**Laborübung**

**Paketanalyse mit Wireshark**

**Prof. Dr. Dirk Staehle**

Die Abgabe erfolgt durch Hochladen der bearbeiteten Word-Datei in Moodle.

**Bearbeitung in Zweier-Teams**

**Team-Mitglied 1: Janko Varga**

**Team-Mitglied 2: Ludwig Kaftan**

* **Einleitung**

WireShark ist ein Werkzeug, um Pakete, die über die Netzwerkkarte eines Rechners laufen, aufzuzeichnen und zu analysieren. In dieser Übung sollen Sie ein erstes Gefühl für WireShark bekommen und die Grundzüge der Datenübertragung im Internet auf den verschiedenen Protokollschichten zu verstehen.

WireShark ist auf den Rechnern im Labor bereits installiert, steht aber auch auf der Seite <https://www.wireshark.org/download.html> zum Download zur Verfügung.

* **WireShark-Umgebung**

Um mit WireShark vertraut zu werden, folgen wir dem Einstiegsversuch, wie er in der Laborübung zum Buch „Computer Networks“ von J.F. Kurose und K.W. Ross spezifiziert ist. Die Beschreibung finden Sie anbei.

Änderungen im Vergleich zur Angabe aufgrund der Situation im Labor:

* wenn Sie als „Display-Filter“ http eingeben, werden weiterhin Protokolle wie z.B. SSDP (Simple Service Discovery Protocol) angezeigt. SSDP können Sie abschalten, indem Sie den Filter auf   
   http && !(udp.port==1900)  
  erweitern.
* SSDP wird übrigens von UPnP (Universal Plug and Play) zur Erkennung von Geräten in IP-Netzen genutzt.
* **Fragen**

Nachdem wir einen ersten Einblick in WireShark gewonnen haben, ein paar Fragen:

* Nennen Sie mindestens 5 Protokolle, die WireShark erkannt hat.

-IP, TCP, HTTP, Ethernet II, TLS(Transport Layer Security)

* Wie lange hat es vom Senden des HTTP Requests bis zum Erhalt der HTTP Response gedauert?

36.863637 - 36.809005 = 0,054s

* Was ist die Internet-Adresse ihres Rechners? Was ist die Ethernet-Adresse (MAC-Adresse, physikalische Adresse) ihres Rechners? Welches ist die Ziel-MAC-Adresse, zu der ihr Rechner Pakete sendet? Vergleichen Sie die Ziel-MAC-Adresse für verschiedene Ziel-IP-Adressen. Welchem Netzknoten können Sie die Ziel-MAC-Adresse zuordnen?

Meine-IPv6: 2003:cb:2704:9d00:45c1:d903:67e9:6815.

Meine-MAC: 4c:cc:6a:0a:cb:e4. Ziel-MAC: c0:25:06:1a:b1:e6

* Betrachten Sie ein HTTP Paket. Welche weiteren Protokolle werden genutzt, um ein http Paket zu übertragen? Welchen Schichten des ISO/OSI Schichtenmodells können Sie die Pakete zuordnen?

1. Ethernet II -> Physical Layer

2. IP -> Network Layer

3. TCP -> Transport Layer

* **Analyse eines Pakets**

Pakete werden von mehreren Protokollschichten verarbeitet und jede Protokollschicht dem Paket, das sie von der höheren Protokollschicht erhält, einen Header hinzu. WireShark greift Pakete an der Netzwerkkarte ab. Wir sehen also alle Protokolle, die dem Paket einen Header hinzugefügt haben.

Das folgende HTTP Paket wurde von Wireshark aufgezeichnet und ist wie im unteren Bereich von WireShark als Hexadezimal-Code und ASCII-Zeichen dargestellt.

Analysieren sie dieses Paket, indem Sie es mit einem anderen http Paket vergleichen, das in WireShark dargestellt ist. Wenn Sie in WireShark zu einem ausgewählten Paket, Header und Header-Felder im Fenster "details of selected packet headers" markieren, so werden die entsprechenden Bytes des Pakets ebenfalls markiert.

* Markieren Sie im obigen Paket Ethernet, IP und TCP Header

Ethernet : L.j ...%......

IP: `......{\* .P@... . . .'.. a>G.[.F.

TCP: P....8... 0P...r|

* Was sind die Quell- und Ziel-MAC-Adressen Adressen des dargestellten Pakets?

Quell-MAC: c0:25:06:1a:b1:e6

Ziel-MAC: 4c:cc:6a:0a:cb:e4

* Was sind die Quell- und Ziel-IP-Adressen des dargestellten Pakets?

Quell-IP: 2a00:1450:4001:81b:200e

Ziel-IP: 2003:cb:2704:9d00:45c1:d903:67e9:6815

* Was sind die verwendeten TCP-Ports des dargestellten Pakets?

Port = 80

* **Filter**

Als nächsten Schritt wollen wir Paketfilter kennenlernen. Es gibt Capture-filter und Display-Filter. Capture-Filter legen fest, welche Pakete WireShark sammelt. Display-Filter legen fest, welche Pakete dargestellt werden. Wir verwenden Display-Filter, um der Vielzahl von Paketen Herr zu werden. Einen Filter haben wir bereits kennengelernt: http. Dadurch werden nur Pakete nach dem HTTP Protokoll dargestellt.

Pakete können generell nach den verwendeten Protokollen und nach dem Inhalt der Felder in den verschiedenen Protokoll-Headern gefiltert werden. Wollen wir beispielweise die Pakete betrachten, bei denen der die Ziel- oder Sendeadresse die 192.140.168.15 ist, dann wäre der Filter  
ip.addr==192.140.168.15. Wenn Sie alle Pakete betrachten wollen, die den UDP-Port 1500 auf Sender- oder Empfängerseite verwenden, dann ist der Filter udp.port==1500.

Versuchen Sie, allen HTTP Verkehr über den verwendeten TCP Port zu filtern.

Mögliche Filteroptionen finden Sie

* bei Eingabe von tcp. im Displayfeld
* indem Sie auf Expression klicken (eher umständlich)
* in der Manpage zu "WireShark Filter" und der Display Filter Übersicht: <https://www.wireshark.org/docs/dfref/>

Fragen:

* Wie lautet der Filter, mit dem Sie über den TCP Port http Verkehr filtern können?

tcp.port == 80

* Erhalten Sie das gleiche Ergebnis wie bei dem Filter HTTP? Erklären Sie ihre Erkenntnis

Nein. mit tcp.port == 80 bekommen wir auch das Packet angezeigt bevor der http- header hinzugeführt wird

* Was bewirkt der Filter: http && !(udp.port==1900)

nur http packete die keinen udp port mit der nummer 1900 anzeigen

* Welcher Filter bewirkt, dass nur Pakete angezeigt, werden, die ihre eigene IP-Adresse als Ziel-Adresse haben?

dst net "myip"

* **Analyse von** [**www.spiegel.de**](http://www.spiegel.de/)

Laden sie die Web-Seite [www.spiegel.de](http://www.spiegel.de/) in ihrem Browser und analysieren Sie den http Verkehr.

* Wie viele Pakete insgesamt übertragen wurden? Unterscheiden Sie Upstream- und Downstream Pakete. Upstream- oder Uplink-Pakete sind Pakete, die von ihrem Rechner ins Internet gesendet werden und Downstream- oder Downlink-Pakete sind Pakete, die aus dem Internet zu ihrem Rechner übertragen werden.

1 Up und 1 Downlink

* Wie viele Bytes an Daten wurden insgesamt auf dem Uplink und Downlink übertragen?

Uplink: 636 bytes

Downlink: 372 bytes(Seite war aber schon im browser cache)

* Von wie vielen IP Adressen hat ihr Rechner Daten empfangen?

1 IP-Adresse

* Über wie viele TCP Sockets hat ihr Rechner die Daten empfangen? Ein Socket wird über Quell-IP-Adresse, Quell-Port sowie Ziel-IP-Adresse und Ziel-Port identifiziert.

1 TCP-Socket. Von Port 80 auf Port 55263

Nutzen Sie dazu die in WireShark angebotenen Tools.

* **Aufzeichnen eines Audio-Streams**

Starten Sie das Webradio von Radio Seefunk und schneiden Sie die übertragenen Pakete mit. Speichern Sie das Ergebnis ab und stellen Sie den Paketstrom von Radio Seefunk zu ihrem Rechner grafisch dar (x-Achse Ankunftszeitpunkt, y-Achse Paketgröße). Beschreiben Sie, nach welchem Muster die Pakete übertragen werden. Analysieren Sie die Pakete, die zwischen ihrer Anwendung und dem Server ausgetauscht werden (Upstream und Downstream) hinsichtlich Bandbreite, Paketgröße und Zeit zwischen Paketen. Können Sie Regelmäßigkeiten feststellen?

Zeit zwischen Packeten = 400ms

Packete werden in regelmaessigen abstaenden in burst gesendet.

Downstream: zwischen 14kbyte und 20kbyte

Upstream: zwischen 280byte und 420byte

Nutzen Sie dazu die in WireShark angebotenen Tools.

Alternativ zu dem Audio-Stream von Radio-Seefunk können sie auch eine andere Anwendung wählen, z.B. ein YouTube-Video oder eine Counterstrike-Session.