Übungsblatt Nr. 4

Aufgabe 4

Beobachten von Paketen mit Wireshark:
In Wireshark sieht man mithilfe einer Paketliste jedes einzelne Paket, das von dem Computer versendet oder empfangen wurde, auf dem das Programm installiert ist. Neben dem Sender, Empfänger und Protokoll bekommt man zusätzlich folgende Informationen über ein Paket:

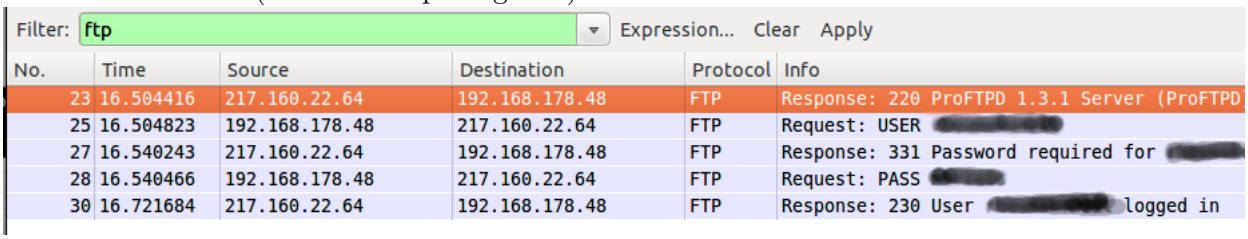
- Informationen zum Frame : Größe, Ankunftszeit, Frame-Nummer und Protokolle (z.B. eth, ip, tcp, ftp)
- Informationen zum OSI-Layer 2 (Ethernet): MAC-Adressen von Sender und Empfänger
- Informationen zum Layer 3 (IP): Version, Headergröße, Time to live, Checksumme,...
- Informationen zu TCP: Ports, Header, Checksummen,..
- Inhalt des Paketes (wie man im Folgenden sieht, zum Teil unverschlüsselt!)

Getestet habe ich drei Programme: einen FTP-Client, Browser und Email-Client.

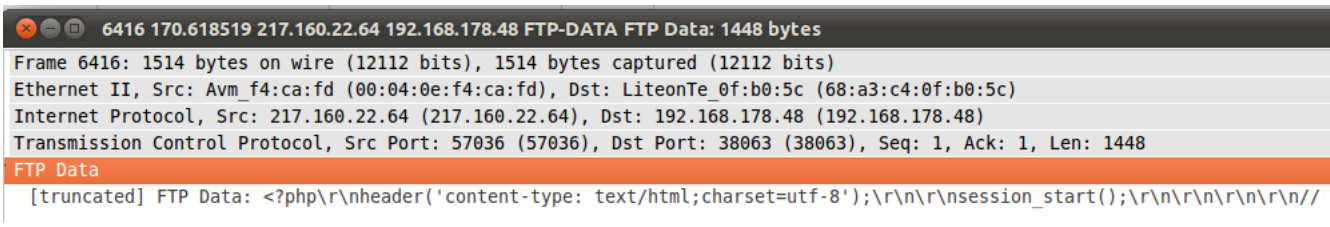
1. Programm: FTP-Client Filezilla

Ablauf: Download einer Datei von einem Server per FTP. Folgenden Traffic kann man mit Wireshark beobachten.

1. Verbindungsaufbau mit dem Server:
   Zunächst werden Benutzerdaten und Passwort angefordert und gesendet. Diese sind in Wireshark in Klartext zu sehen(!)
   Mithilfe eines Filters lasse ich mir von Wireshark nur alle Pakete anzeigen, die das FTP-Protokoll benutzen (bei Filter 'ftp' eingeben).

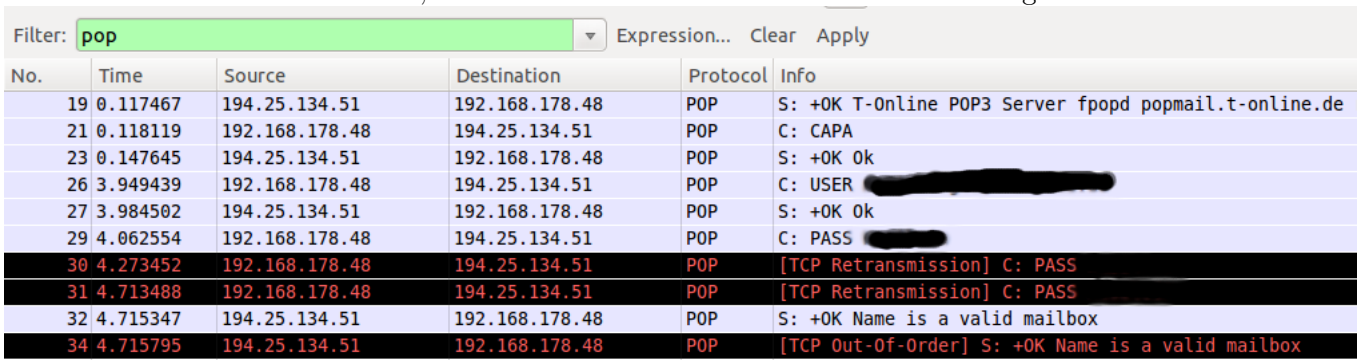


2. Übertragung der Datei:
   Um den Inhalt der gesendeten Pakete zu sehen, muss als Filter 'ftp-data' eingestellt sein. Der Inhalt der übertragenen Datei ist ebenfalls in Klartext zu sehen (in diesem Beispiel eine php-Datei):



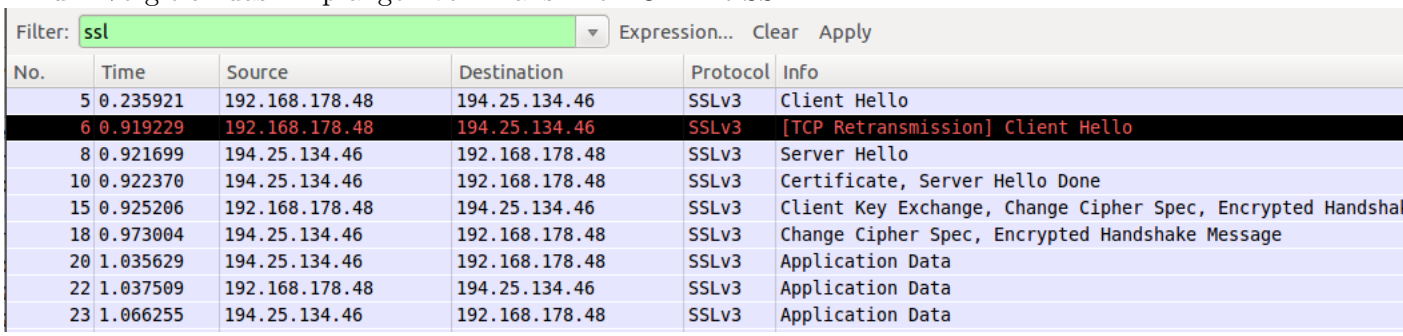
   Eine FTP-Übertragung ist somit nicht mehr sicher, wenn andere Endgeräte im Netzwerk Zugriff auf die Pakete der Übertragung haben.

2. Programm: Email-Client Thunderbird:
Versuch: Empfangen von Mails mit POP ohne SSL:
Auch hier werden Benutzername, Passwort und Inhalt der Mail unverschlüsselt gesendet.


Filter: pop — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19	0.117467	194.25.134.51	192.168.178.48	POP	S: +OK T-Online POP3 Server fpopd popmail.t-online.de
21	0.118119	192.168.178.48	194.25.134.51	POP	C: CAPA
23	0.147645	194.25.134.51	192.168.178.48	POP	S: +OK Ok
26	3.949439	192.168.178.48	194.25.134.51	POP	C: USER [redacted]
27	3.984502	194.25.134.51	192.168.178.48	POP	S: +OK Ok
29	4.062554	192.168.178.48	194.25.134.51	POP	C: PASS [redacted]
30	4.273452	192.168.178.48	194.25.134.51	POP	[TCP Retransmission] C: PASS
31	4.713488	192.168.178.48	194.25.134.51	POP	[TCP Retransmission] C: PASS
32	4.715347	194.25.134.51	192.168.178.48	POP	S: +OK Name is a valid mailbox
34	4.715795	194.25.134.51	192.168.178.48	POP	[TCP Out-Of-Order] S: +OK Name is a valid mailbox

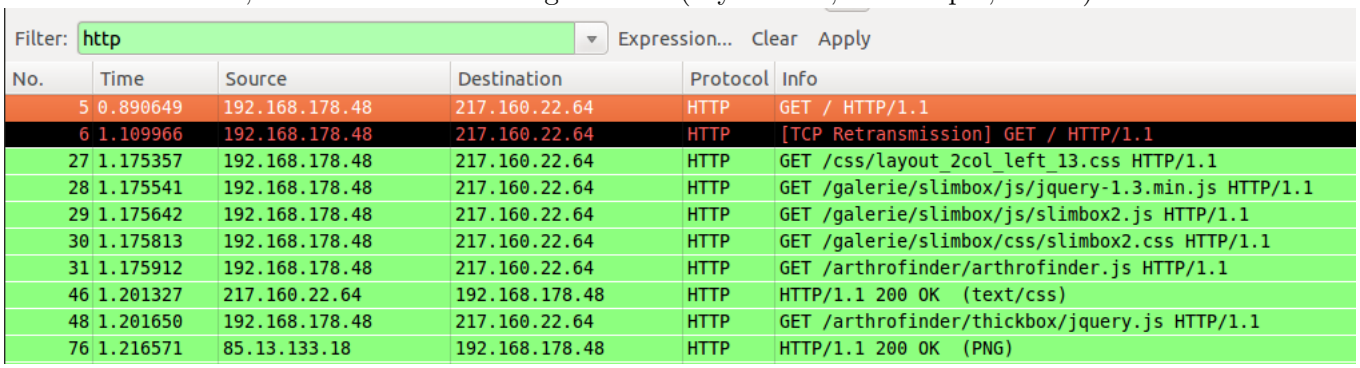
Zum Vergleich das Empfangen von Mails mit POP mit SSL:


Filter: ssl — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5	0.235921	192.168.178.48	194.25.134.46	SSLv3	Client Hello
6	0.919229	192.168.178.48	194.25.134.46	SSLv3	[TCP Retransmission] Client Hello
8	0.921699	194.25.134.46	192.168.178.48	SSLv3	Server Hello
10	0.922370	194.25.134.46	192.168.178.48	SSLv3	Certificate, Server Hello Done
15	0.925206	192.168.178.48	194.25.134.46	SSLv3	Client Key Exchange, Change Cipher Spec, Encrypted Handshal
18	0.973004	194.25.134.46	192.168.178.48	SSLv3	Change Cipher Spec, Encrypted Handshake Message
20	1.035629	194.25.134.46	192.168.178.48	SSLv3	Application Data
22	1.037509	192.168.178.48	194.25.134.46	SSLv3	Application Data
23	1.066255	194.25.134.46	192.168.178.48	SSLv3	Application Data

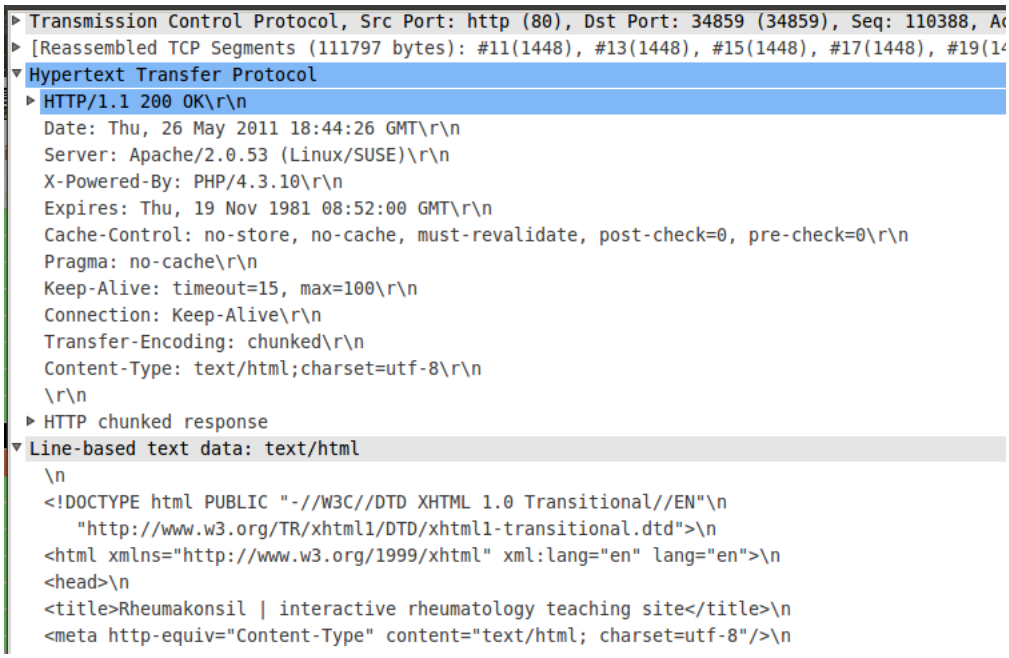
Hier werden keine Daten unverschlüsselt übertragen.
E-Mails mit POP ohne SSL und damit unverschlüsselt zu verschicken, ist somit unsicher. In einem offenen WLAN z.B. haben andere Zugriff auf alle Pakete - sie können somit sehr leicht mit einem Tool wie Wireshark alle Zugangsdaten zu dem Mailaccount mitlesen.

3. Programm: Firefox, HTTP-Zugriff
Bei dem Aufruf einer Website wird zunächst eine HTTP-GET-Anforderung an den Server gesendet. Der Server schickt dann die angeforderte Seite zurück. Dies wird mit allen zusätzlichen Dateien wiederholt, die in der Seite benötigt werden (Stylesheets, Javascripts, Bilder).


Filter: http — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5	0.890649	192.168.178.48	217.160.22.64	HTTP	GET / HTTP/1.1
6	1.109966	192.168.178.48	217.160.22.64	HTTP	[TCP Retransmission] GET / HTTP/1.1
27	1.175357	192.168.178.48	217.160.22.64	HTTP	GET /css/layout_2col_left_13.css HTTP/1.1
28	1.175541	192.168.178.48	217.160.22.64	HTTP	GET /galerie/slimbox/js/jquery-1.3.min.js HTTP/1.1
29	1.175642	192.168.178.48	217.160.22.64	HTTP	GET /galerie/slimbox/js/slimbox2.js HTTP/1.1
30	1.175813	192.168.178.48	217.160.22.64	HTTP	GET /galerie/slimbox/css/slimbox2.css HTTP/1.1
31	1.175912	192.168.178.48	217.160.22.64	HTTP	GET /arthrofinder/arthrofinder.js HTTP/1.1
46	1.201327	217.160.22.64	192.168.178.48	HTTP	HTTP/1.1 200 OK (text/css)
48	1.201650	192.168.178.48	217.160.22.64	HTTP	GET /arthrofinder/thickbox/jquery.js HTTP/1.1
76	1.216571	85.13.133.18	192.168.178.48	HTTP	HTTP/1.1 200 OK (PNG)

In folgendem Screenshot sieht man genauere Details zu einem HTTP-Paket und dessen Protokoll. Außerdem wird auch der HTML-Code angezeigt, eine Verschlüsselung wird an dieser Stelle nicht gebraucht.


Transmission Control Protocol, Src Port: http (80), Dst Port: 34859 (34859), Seq: 110388, Ac
[Reassembled TCP Segments (111797 bytes): #11(1448), #13(1448), #15(1448), #17(1448), #19(14
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 26 May 2011 18:44:26 GMT\r\n
Server: Apache/2.0.53 (Linux/SUSE)\r\n
X-Powered-By: PHP/4.3.10\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Keep-Alive: timeout=15, max=100\r\n
Connection: Keep-Alive\r\n
Transfer-Encoding: chunked\r\n
Content-Type: text/html;charset=utf-8\r\n
\r\n
HTTP chunked response
Line-based text data: text/html
\n
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"\n
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">\n
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">\n
<head>\n
<title>Rheumakonsil | interactive rheumatology teaching site</title>\n
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>\n