

**AB-Protokollanalyse**

gibb HF Informatik & Telekom

Aeby, Marc

Inhalt

[Inhalt 1](#_Toc85786295)

[Ausgangslage 2](#_Toc85786296)

[DHCP 3](#_Toc85786297)

[ARP 5](#_Toc85786298)

[DNS Lookup / http Request 6](#_Toc85786299)

[FTP Filetransfer 7](#_Toc85786300)

[SNMP Überwachung 8](#_Toc85786301)

[Zusatzaufgabe für Profis 9](#_Toc85786302)

Ausgangslage

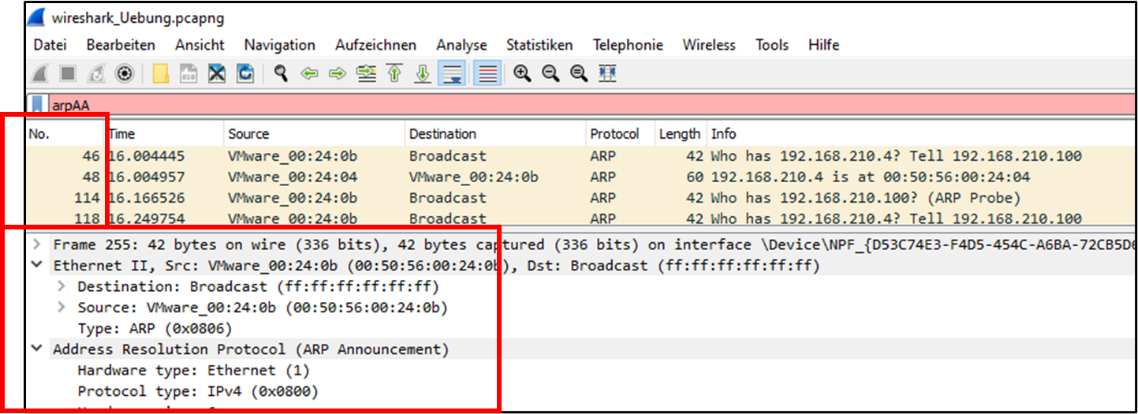
Ziel der Aufgabe ist das Handling von Wireshark aufzufrischen. Es geht darum sich im TCP/IP Schichtenmodell wiederzufinden und Informationen zu einzelnen Protokollen im Datenverkehr zu suchen. Die Aufzeichnung wurde auf dem Windows PC mit Wireshark durchgeführt.

Folgende Umgebung wurde eingesetzt:



Die Aufzeichnung (File wireshark\_Uebung.pcapng) befindet sich unter folgendem Link auf ILIAS im Tag 4/5:

<https://ilias.iet-gibb.ch/goto.php?target=file_18021_download&client_id=tsbe01>

Suche im Wireshark Trace Antworten zu den nachfolgenden Fragen. Dafür muss der Wireshark auf dem BYOD PC oder auf der Smartlearn SSD Windows PC vmWP installiert sein. Die Antworten können in der Aufzeichnung gesucht werden. Bei den Antworten immer die Paketnummer angeben wo die Information gefunden wurde.

Als Refresh vom Wireshark kann das Linkedin eLearning konsultiert werden.

<https://www.linkedin.com/learning/netzwerkanalyse-mit-wireshark/wireshark-effektiv-zur-netzwerkanalyse-und-problembehebung-nutzen?autoAdvance=true&autoSkip=false&autoplay=true&resume=true&u=76376906>

DHCP

Beantworte folgende Fragen zum Thema DHCP:

Welche Adresse wurde vom DHCP Server an den Windows PC übergaben:

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 3 | Der DHCP Server antwortet Broadcast Message mit einem DHCP Offert und übergibt die IP Adresse 192.168.210.100 |

Welche Adresse hat der Standard Gateway?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 3 | Router IP ist in Option 3 ersichtlich und hat IP= 192.168.210.4 |

Was ist die MAC Adresse vom Windows PC?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 1 | Source Adresse im Ethernet Frame hat MAC Adresse 00:50:56:00:24:0B |

Was ist die MAC Adresse vom DHCP Server?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 3 | Source Adresse im Ethernet Frame hat MAC Adresse 00:50:56:00:24:04 |

Wie lange ist die vergebene Lease Time?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 3 | Lease Time ist in Option 51 ersichtlich und ist 7200sekunden = 2 Stunden |

Ist der DHCP Request ein UDP oder ein TCP Paket?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 1 | Der PC sendet ein UDP Paket von Source Port 68 auf Destination Port 67 |

Zeichne den Verlauf der DHCP Meldungen mit Pfeilen auf und benenne die Meldungen:

Win PC DHCP Server

|  |
| --- |
|  |

IP Adresse WinPC IP Adresse DHCP Server

Pfeile vom Sender zum Empfänger und Name der Meldung (z.B http GET Request) bezeichnen.

Hilfsmittel  
<https://www.elektronik-kompendium.de/sites/net/0812221.htm>

ARP

Beantworte folgende Fragen zum Thema ARP:

Mit welchem Befehl kann ich auf dem Windows PC die ARP Tabelle löschen?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| Nicht relevant | In einer Comand Line kann mit dem Befehl  *arp -d arp -d <ip Adresse>* die ARP Tabelle gelöscht werden  In Powershell: *netsh interface ip delete arpcache* |

Wann wurden ARP Anfragen ausgeführt und was war aus deiner Sicht der Grund dazu?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 9  61  328ff | PC will Verbindung auf Router IP 192.168.210.4 machen und muss seine MAC Adresse wissen. Er kriegt die MAC Adresse im nachfolgenden Paket.  Router will auf PC IP 192.168.210.100 eine Verbindung machen und braucht seine MAC Adresse. Es ist aber keine Antwort ersichtlich.  PC will auf IP 192.168.210.3 eine Verbindung machen und fragt nach der MAC Adresse. Es antwortet aber niemand |

Hilfsmittel  
<https://www.elektronik-kompendium.de/sites/net/0901061.htm>

DNS Lookup / http Request

Der Windows PC hat eine Webseite in der Schweiz abgefragt. Einige Antworten findet man nicht im Trace sondern müssen extern mit anderen Tools gesucht werden.

Welche Webseite (URL) wurde vom Browser aufgerufen?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 352 | Nach dem DNS Request wurde nach www.cardinal.ch gesucht. |

Was ist die IP Adresse des Web Servers?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 357 | Der DNS Server übergibt dem PC die IP 185.139.240.11 für die Adresse [www.cardinal.ch](http://www.cardinal.ch) |

In welchem Land wird die Domain gehostet und was ist der Anbieter und wo hast du diese Information gefunden?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| Nicht Releavant | Ein whois Lookup auf <https://nic.chwhois> zeigt folgende Adressen:  Key-Systems GmbH  Im Oberen Werk 1  DE-66386 St. Ingbert  Phone +49 68949396870  info@key-systems.net |

Wie heisst der Nameserver, der diese Webseite verwaltet?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| Nicht Relevant | ns01.brandshelter.com  ns02.brandshelter.net |

Hilfsmittel  
<https://www.elektronik-kompendium.de/sites/net/0902231.htm>

FTP Filetransfer

Der Windows PC hat auf einem FTP Server ein File abgeholt.

Auf welchen FTP Server hat sich der Windows PC verbunden (Name Server, IP-Adresse)?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 498 | 195.144.107.198 |

Mit welchem Username und Passwort wurde bei der FTP Verbindung unverschlüsselt kommuniziert?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 499  501 | Username= demo Passwort=password |

In welches Verzeichnis wurde auf dem FTP Server gewechselt?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 518 | FTP Befehl CWD (Change Working Direktory) auf /pub/example |

Wie heisst die Datei die transferiert wurde und von wo nach wo wurde das File gesendet?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 525  530 | Es wird nach File readme.txt gefragt File wird gesendet |

Hilfsmittel  
<https://www.elektronik-kompendium.de/sites/net/0902241.htm>

SNMP Überwachung

Der Linux Server hat einen SNMP Agent konfiguriert. Der Windows Server hat via SNMP mehrere Parameter überprüft und via SNMP Get Befehl abgesetzt.

Mit welcher SNMP Version hat der SNMP Server (Windows PC) auf den SNMP Agent (Linux Server) kommuniziert?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 539 | Der SNMP Request wird mit Version 2c gesendet |

Was ist die IP Adresse die via SNMP abgefragt wurde?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 539 | Es wird ein SNMP Request auf IP 192.168.210.100 gesendet |

Was ist die SNMP Community (Password das in Klartext übermittelt wurde)

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 539 | Die SNMP Community heisst «Cardinal1 » |

Auf welche SNMP OIDs wurden ein GET Request gemacht und was war die Antwort? Welche Information könnte gesucht werden? (OID wie z.B. .1.3.1.4.1.9)

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 539  540 | 1.3.6.1.2.1.1.3.0  Gemäss oid-info.com ist dies die «sysUpTimeInstance»  1.3.6.1.2.1.25.1.1.0  Gemäss oid-info.com ist dies die «hrSystemUptime»  Es sind keine Antworten im Trace ersichtlich |

Hilfsmittel  
<https://www.manageengine.com/de/network-monitoring/what-is-snmp.html>

Zusatzaufgabe für Profis

Diese Aufgabe ist freiwillig. Lade die folgende Telefonaufzeichnung runter und beantworte die nachfolgenden Fragen.

<https://ilias.iet-gibb.ch/goto.php?target=file_18022_download&client_id=tsbe01>

Welche Rufnummer wurde gewählt

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 18 | 161 |

Welche Rufnummer hat gewählt

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 18 | 0265085325 |

In welcher Sprache wird im Anruf gesprochen?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| Nicht Relevant | Wenn man im Wireshark den Call anhört, dann ist dieser Französisch |

Bei welchem Provider ist der SIP Anschluss?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 18 | SIP Provider ist Netvoip.ch |

Mit welchem CODEC wurde der RTP Stream gesendet?

|  |  |
| --- | --- |
| **PKT-NR** | **Antwort** |
| 25 | Aus dem Flowsequence im Wireshark ist ersichtlich, dass G.711a aus den verschiedenen Codes ausgewählt wurde. Man sieht auch, dass Paket 25 mit RTP Paket mit dem Codec G711 sendet. |

Hilfsmittel  
<https://www.elektronik-kompendium.de/sites/net/1305281.htm>