

Protokollanalyse mit Wireshark - Einführung

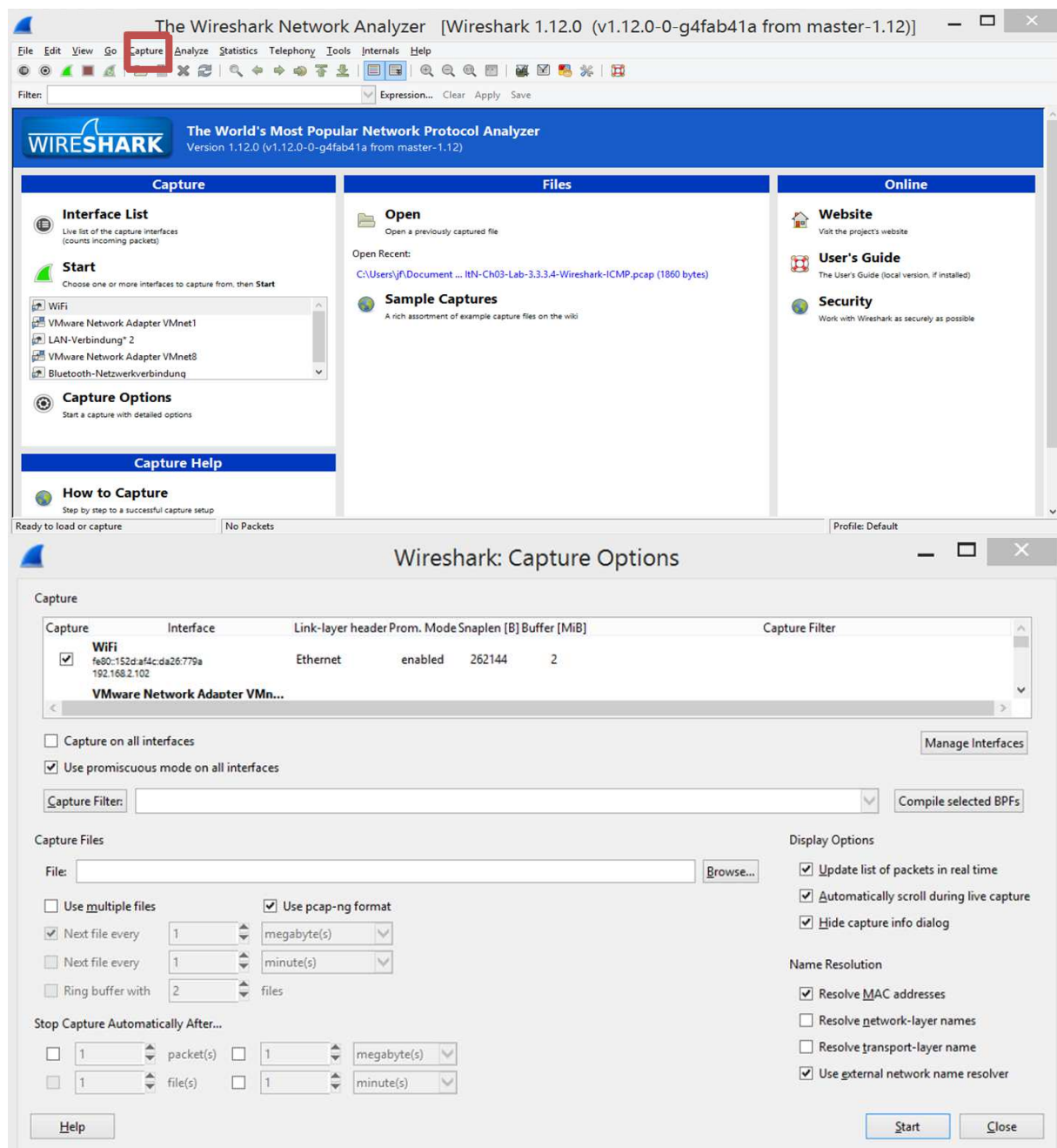
Wireshark ist ein Netzwerk-Protokoll-Analysator, mit dem die Vorgänge beim Senden und Empfangen von Daten visualisiert werden. Dieses Tool besitzt eine Aufzeichnungsfunktion (Capture), die die Möglichkeit bietet, alle Frames, die eine Schnittstelle passieren, zu Analysezwecken aufzuzeichnen. Damit leistet er in der Ausbildung und bei der Fehlersuche wertvolle Dienste.

Aufgabe 1

1.1 Starten Sie Wireshark und die Eingabeaufforderung (CMD).

1.2 Wählen Sie die Schnittstelle aus.

Im Menü Capture / Options können verschiedene Optionen zum Aufzeichnungsprozess eingestellt werden, wie z.B. das Interface, von dem aufgenommen werden soll, Capturefilter zur Steuerung der Aufnahme, Capturefile zum Speichern, Displayoptionen und automatische Abbruchbedingungen. Beginnen Sie mit der Aufzeichnung (Start).



Geben Sie auf der Befehlszeile des PCs (Konsolenfenster, CMD) den Befehl **nslookup** ein und geben Sie dann die Domäne **cisco.com** ein, um die IP-Adresse zu erhalten.

```
C:\>nslookup
Standardserver:  fxns01.t-d1-wap.de
Address:  10.74.83.22

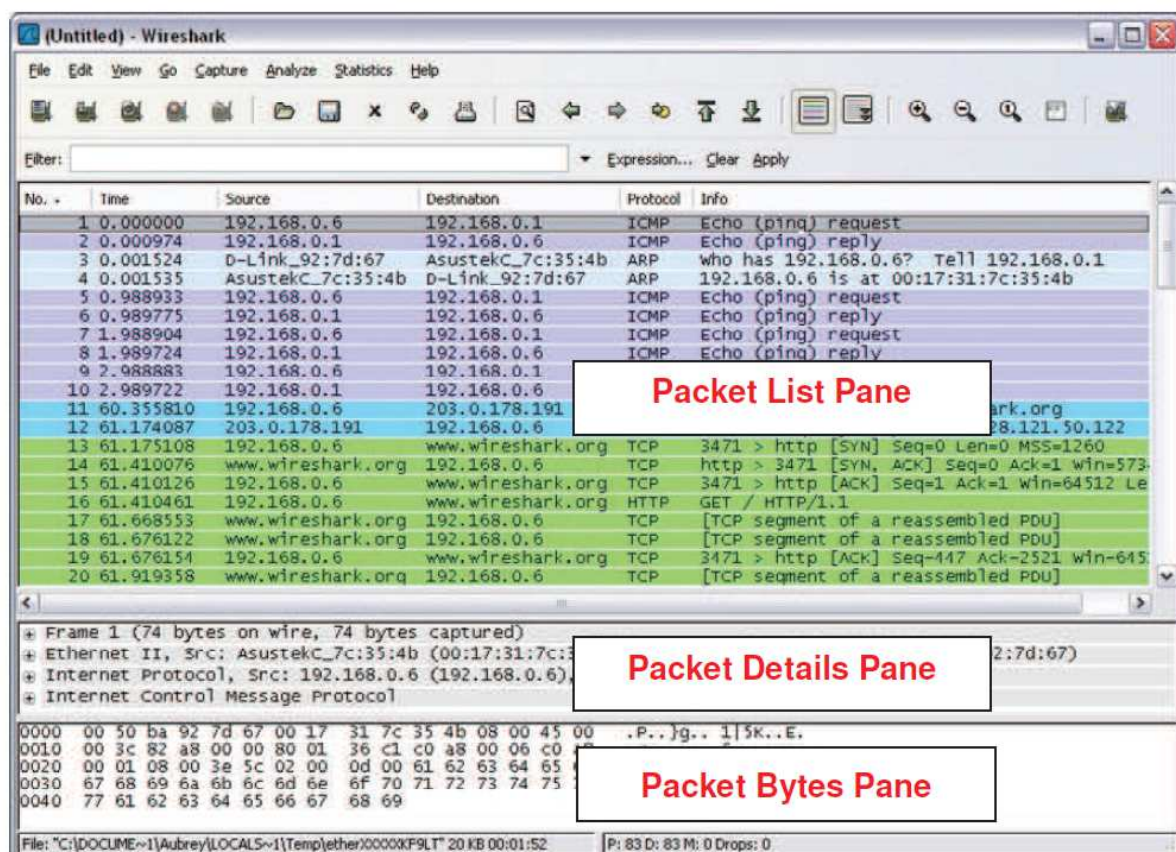
> cisco.com
Server:  fxns01.t-d1-wap.de
Address:  10.74.83.22

Nicht autorisierte Antwort:
Name:      cisco.com
Address:   198.133.219.25
```

Stoppen Sie die Aufzeichnung. (Capture / Stop).

Die Datenaufzeichnung von Wireshark wird angehalten. Da für die Aufzeichnung keine Filter gesetzt wurden, wurde sämtlicher Netzwerkverkehr mitgeschnitten.

Das Hauptfenster von Wireshark teilt sich in drei Bereiche: die Paketliste (Packet List Pane), die Paketdetails (Packet Details Pane) und die Hexadezimale Paketanzeige (Packet Bytes Pane).



Im oberen Bereich werden u.a. der Sender (Source), der Empfänger (Destination) und das Protokoll eines Frames angezeigt.

Im mittleren Bereich werden die Details zum ausgewählten Frame angezeigt.

Ergänzen Sie folgende Tabelle, indem Sie nur DNS-Protokoll filtern und die angezeigten Frames analysieren.

IP-Adresse Ihres Rechners	
IP-Adresse des DNS-Servers	
IP-Adresse der Domäne <i>cisco.com</i>	
DNS-Port	
Transportprotokoll (TCP oder UDP)	

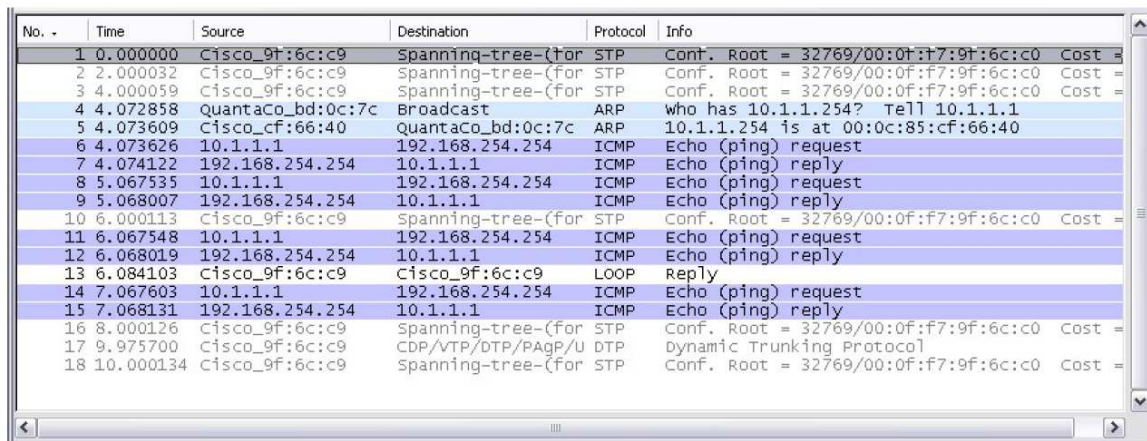
Aufgabe 2: Ping PDU Capture

Starten Sie Wireshark und die Eingabeaufforderung (CMD).

Wählen Sie die richtige Schnittstelle und starten Sie die Paketerfassung. Über die Befehlszeile des Computers, pingen Sie die IP- Adresse eines anderen im Netzwerk verbunden Endgeräts. In diesem Fall pingen Sie den Cisco Server mit der Adresse aus Aufgabe 1. Nach Erhalt der erfolgreichen Antworten auf den Ping, stoppen Sie die Paketerfassung in Wireshark.

Untersuchung der Paketliste

Der Listenbereich im Wireshark sollte nun in etwa so aussehen:



No. ->	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for STP	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for STP	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for STP	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for STP	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for STP	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAGP/U DTP	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for STP	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Schauen Sie sich die oben aufgeführten Pakete an, uns interessieren die Paketnummern 6, 7, 8, 9, 11, 12, 14 und 15. Suchen Sie die gleichwertigen Pakete auf der Paketliste auf Ihrem Computer.

Beantworten Sie mithilfe der Wireshark Packet Liste folgende Fragen:

Welches Protokoll wird vom Ping Befehl verwendet? _____

Wie lautet der vollständige Protokollname? _____

Wie lauten die Namen der zwei Ping Nachrichten? _____

Sind die Source und Destination IP-Adressen wie erwartet? Ja / Nein

Warum? _____

Markieren Sie das erste Echo Request-Paket auf der Liste mit der Maus.

Der Packet Detailbereich sollte nun in etwa so aussehen:

```
+ Frame 6 (74 bytes on wire, 74 bytes captured)
+ Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40 (00:0c:85:cf:66:40)
+ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
+ Internet Control Message Protocol
```

Klicken Sie nun auf jedes der vier "+", um die Information zu erweitern.
Das Paket -Detail -Fenster sollte nun in etwa so aussehen:

```
- Frame 6 (74 bytes on wire, 74 bytes captured)
  Arrival Time: Jan 10, 2007 01:54:07.860436000
  [Time delta from previous packet: 0.000017000 seconds]
  [Time since reference or first frame: 4.073626000 seconds]
  Frame Number: 6
  Packet Length: 74 bytes
  Capture Length: 74 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp]
+ Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  Destination: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  Source: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c)
  Type: IP (0x0800)
+ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 60
  Identification: 0x0bf7 (3063)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (0x01)
  Header checksum: 0x6421 [correct]
  Source: 10.1.1.1 (10.1.1.1)
  Destination: 192.168.254.254 (192.168.254.254)
+ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x2a5c [correct]
  Identifier: 0x0300
  Sequence number: 0x7000
```

Wie Sie nun sehen, sind die Einzelheiten für jeden Abschnitt und Protokoll sichtbar. Verbringen Sie einige Zeit um durch diese Informationen zu Scrollen und notieren Sie sich die Informationen, die Sie erkennen.

Suchen Sie die zwei verschiedenen Arten von "Quelle" und "Ziel". Warum gibt es zwei Typen?

Welche Protokolle sind im Ethernet-Frame enthalten?

Wenn Sie eine Zeile in dem Paket Detailbereich oder einen Teil der Informationen auswählen, wird diese auch im Paket Bytes Bereich hervorgehoben.
Zum Beispiel, wenn die zweite Zeile (+ Ethernet II) in den Details ausgewählt wird, werden auch die entsprechenden Werte (Bytes) ausgewählt.

```
0000 00 0c 85 cf 66 40 00 c0 9f bd 0c 7c 08 00 45 00  f0...E.
0010 00 3c 0b f7 00 00 80 01 64 21 0a 01 01 01 c0 a8  <.....dl....
0020 fe fe 08 00 2a 5c 03 00 20 00 61 62 63 64 65 66  ...*...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdefgh
```

Dies zeigt insbesondere die binären Werte, die diese Informationen in der PDU darstellen.

Speichern Sie Ihre Aufzeichnung und schließen Sie Wireshark.

Aufgabe 3: Untersuchung ICMP-Paket - Format

ICMP Packet – Common Message Header Information

0	7	8	16	24	31
Type		Code		Checksum	

Die Abbildung zeigt den ICMP Header. Jede ICMP Nachricht startet mit einem 8-bit Type Feld, einem 8-bit Code Feld, und einer berechneten 16-bit Checksumme. Der ICMP Nachricht type beschreibt die folgenden ICMP Felder. Die folgende Abbildung zeigt die ICMP Nachrichtentypen (RFC 792)

Value	Meaning
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

Das Code Feld enthält weitere Informationen zum Type Feld. Zum Beispiel, ist der Wert des Type Feld 3 (Destination unreachable) wird zusätzliche Information zu diesem Problem im Code Feld zurückgegeben.

Die folgende Tabelle enthält die Message Codes für eine ICMP Type 3 Nachricht (destination unreachable, RFC 1700)

Code Value	Meaning
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service

Analyse ICMP (Response)

Öffnen Sie Ihren Mitschnitt aus der vorigen Aufgabe und halten Sie die Informationen (Feldname und Werte) aus dem ersten Ping fest (Echo und Echo Reply).

ICMP Packet – echo

0	7	8	16	24	31
DATA ...					

ICMP Packet – echo reply

0	7	8	16	24	31
DATA ...					

Welche Felder haben sich möglicherweise im echo reply geändert?

Auf der TCP / IP- Netzwerkschicht, wird die Kommunikation zwischen den Geräten nicht gewährleistet. Dennoch stellt ICMP kleine Prüfungen für eine Anfrage zur Verfügung.

Wie weiß der Absender, aus den Angaben in der ICMP Nachricht, dass es eine Antwort auf eine spezifische Echo Nachricht ist?

Wie groß ist die Datenmenge? _____

Aufgabe 4: Analyse ICMP (No Response)

Schritt1: Starten Sie eine neue Wireshark Session und senden Sie einen Ping zu einer fiktiven IPv4 Adresse. Diese IP sollte sich im gleichen IP Adress-Bereich befinden wie Ihr Rechner.

Beispiel: IP Rechner 192.168.253.2 – Fiktive IP (nicht vergeben): 192.168.253.1

```
C:\> ping 192.168.253.1
Pinging 192.168.253.1 with 32 bytes of data:
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Ping statistics for 192.168.253.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Wireshark speichert den Verbindungsversuch zu dem fiktiven Ziel. Erweitern Sie das Wireshark - Fenster und analysieren Sie den Eintrag Internet Control Message Protocol.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
2	0.000816	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
3	1.000854	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
4	1.001686	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
5	2.001815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
6	2.002547	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
7	3.002815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
8	3.003588	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)

Welcher ICMP Nachrichtyp wird als Informationen zum Sender gesendet?

Welcher Code ist mit dem Nachrichtyp verbunden?

Schritt2: Capture und Auswertung von ICMP echo Nachrichten die den TTL Wert übersteigen. In diesem Schritt werden pings mit einem geringen TTL Wert versendet, somit wird ein „destination unreachable“ simuliert. Ping Cisco Server, und setzen Sie den TTL Wert auf 1:

```
C:\Users\jff>ping -i 1 cisco.com

Ping wird ausgeführt für cisco.com [72.163.4.161] mit 32 Bytes Daten:
Antwort von 192.168.2.1: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.
Antwort von 192.168.2.1: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.
Antwort von 192.168.2.1: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.
Antwort von 192.168.2.1: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.

Ping-Statistik für 72.163.4.161:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
```

Welches Netzwerkgerät meldet, dass der TTL Wert überschritten wurde?

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
2	0.000701	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
3	1.000003	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	1.000687	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
5	1.999996	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	2.000761	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
7	3.000970	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	3.001723	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

Welcher ICMP Nachrichten Type und welcher Code wird verwendet?

Welches Netzwerkgerät ist für das Dekrementieren des TTL Werts zuständig?

Aufgabe 5: FTP PDU Capture

Unter der Annahme, dass Wireshark immer noch aus den vorherigen Schritten ausgeführt wird, starten Sie die Paketerfassung. Geben Sie in der Eingabeaufforderung: **ftp ftp.fernuni-hagen.de**

Userid: anonymous

Password: <ENTER>

Nach erfolgreichem Login geben Sie: **get /pub/unix/gnu/sunfreeware**

Die Datei wird nun vom FTP- Server heruntergeladen. Beispiel:

```
C:\Documents and Settings\ccna1>ftp eagle-server.example.com
Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP serv
ice. User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

Nach erfolgreichem Download geben Sie **quit** ein:

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccna1>
Stoppen Sie die das PDU capture in Wireshark.
```

Finden Sie die mit dem Datei Download verbundenen PDUs (Layer 4 TCP, Layer 7 FTP) und weisen Sie diese, den Eingaben in der Eingabeaufforderung zu

1. Phase: Connection und Server Login.

Nennen Sie Nachrichten die während dieser Phase ausgetauscht werden.

-
2. Phase: Download Request und Datentransfer.

Nennen Sie Nachrichten die während dieser Phase ausgetauscht werden.

-
3. Phase: Logging out und "breaking the connection".

Nennen Sie Nachrichten die während dieser Phase ausgetauscht werden.

Suchen Sie wiederkehrende TCP Anfragen im gesamten FTP-Prozess. Welche Funktion von TCP wird dadurch angezeigt?

Wählen Sie ein Paket aus der ersten Phase des FTP Prozesses (Details pane).

Welche Protokolle sind in diesem Frame gekapselt?

Wählen Sie die Pakete die den user name und password enthalten (Byte pane).

Was bedeutet das für die Security des FTP login Prozess?

Wählen Sie ein Paket aus der zweiten Phase des FTP Prozesses (Details pane...all).

Der Dateiname ist: _____

Der Inhalt ist: _____

Wählen Sie ein Paket aus der dritten Phase des FTP Prozesses (Details pane...all).

Welche Merkmale weisen diese Pakete auf?

Schließen Sie Wireshark und fahren Sie den Computer herunter.