NVS

Laborprotokoll – 05 –Einführung in Wireshark

Alexander Brenner

2015

Inhaltsverzeichnis

[1. Aufgabenstellung für dieses Labor 2](#_Toc472287167)

[2. Setup für das Labor 2](#_Toc472287168)

[3. Fragen zum Labor 05 2](#_Toc472287169)

[4. Aufgabenstellung für dieses Labor 3](#_Toc472287170)

[4.1. Die Installation von Wireshark 3](#_Toc472287171)

[4.2. Starten von Wireshark und Identifizieren der einzelnen Teile 3](#_Toc472287172)

[4.3. Abspeichern des Mitschnitts 3](#_Toc472287173)

[4.4. Untersuchung des Packet-Detailbereiches 4](#_Toc472287174)

[4.5. Beantwortung der Fragen 5](#_Toc472287175)

Einführung in Wireshark

# Aufgabenstellung für dieses Labor

* Installation des Netzwerksniffers – Wireshark
* Durchführen und Speichern eines Mitschnitts
* Identifizieren der Bereiche von Wireshark
* Mitschnitt mit Optionen
* Einsatz eines Capure-Filters
* Verwendung eines Display-Filters

# Setup für das Labor

Für das Labor wird der nachfolgende Übungsaufbau mit den angegebenen IPv4 Adressen verwendet.

* Die Übung wird von VM-Lab01 durchgeführt. Auf diesem PC ist Wireshark installiert.
* Auf VM-Lab02 muss für den letzten Teil der Übung ein Web-Server installiert werden. Bitte kontrollieren Sie dies und installieren Sie gegebenenfalls den Web-Server auf VM-Lab02 nochmals.
* Deaktivieren Sie auf beiden VM´s die Windows Firewall

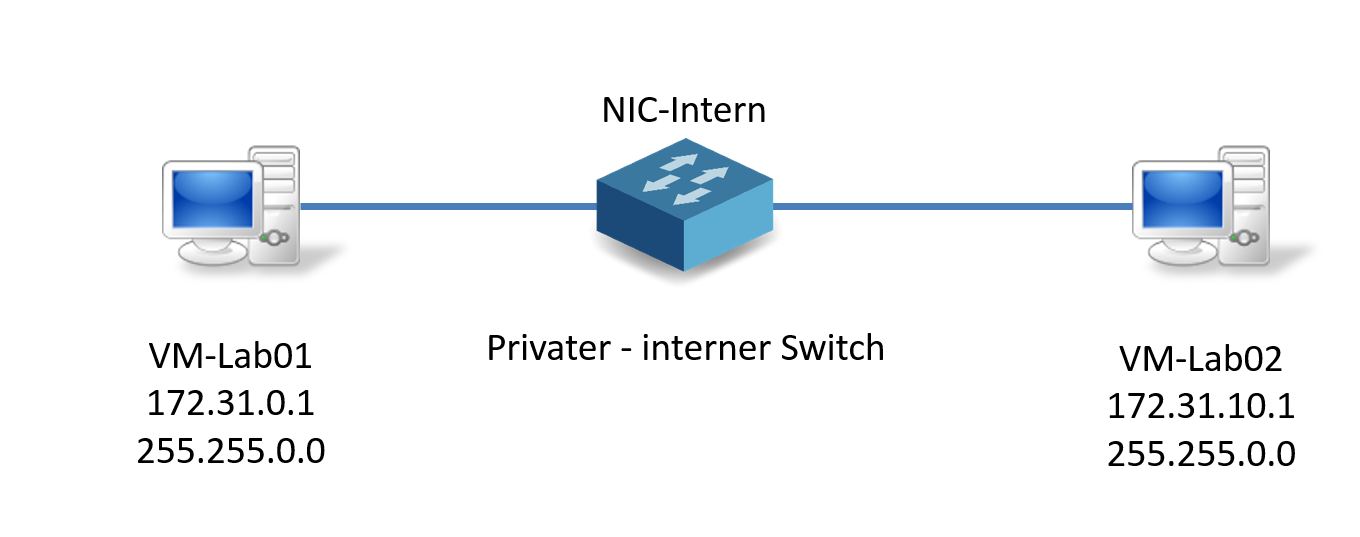


Abbildung: PCs und IP-Adressen für das Labor 05

* Überprüfen Sie die Kommunikationsfähigkeit indem Sie einen ping auf VM-Lab02 durchführen.

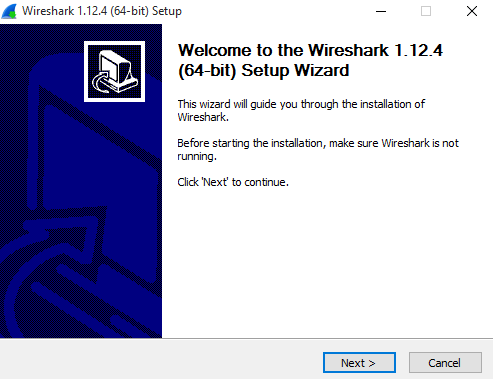
# Fragen zum Labor 05

1. Aus wie vielen Bit besteht die MAC-Adresse einer Netzwerkkarte
2. Auf welcher OSI-Ebene findet der Vergleich zwischen der MAC-Adresse im Datenpaket und der MAC-Adresse der Netzwerkkarte statt?
3. Wie nennt man den Modus in dem die Netzwerkkarte geschalten werden muss, damit alle Datenpaket aufgenommen werden
4. Welche Aufgabe hat ein Capture Filter in Wireshark?
5. Welche Aufgabe hat ein Display Filter in Wireshark?
6. Was versteht man unter dem Begriff Datenframe?
7. Was versteht man unter dem Begriff Datenpacket?
8. Was versteht man unter dem Begriff Datensegment?
9. Welchen Dateityp verwendet Wireshark um einen Mitschnitt in einer Datei zu speichern?
10. Wie heißen die drei Fensterteile die bei einem Mitschnitt in Wireshark angezeigt werden?

# Aufgabenstellungen für dieses Labor

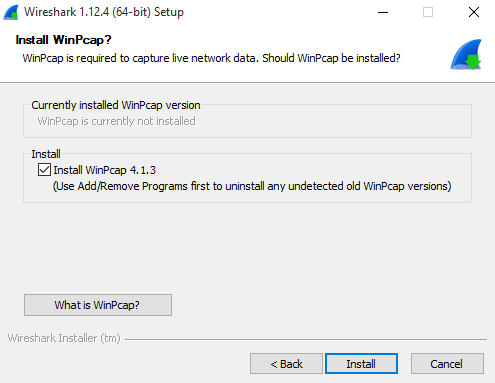
## Die Installation von Wireshark

* Das Setup führt sie durch die „straightforward“ Installation von Wireshark.

**

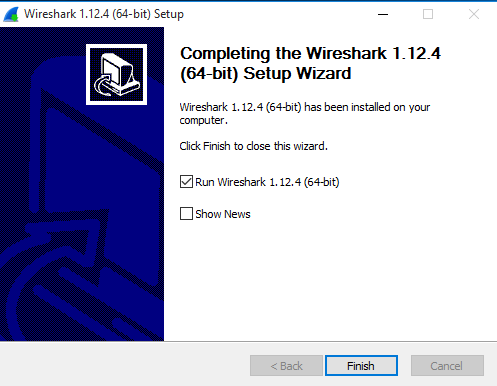
*Abb.1: Wireshark Setup – Erster Schritt*

* Wenn Sie bei der Auswahl zur Installation von WinPcap angelangt sind, setzen Sie ein Häckchen bei „Install WinPcap [Aktuelle Version]“.

**

*Abb.2: Wireshark-Setup – WinPcap Auswahl*

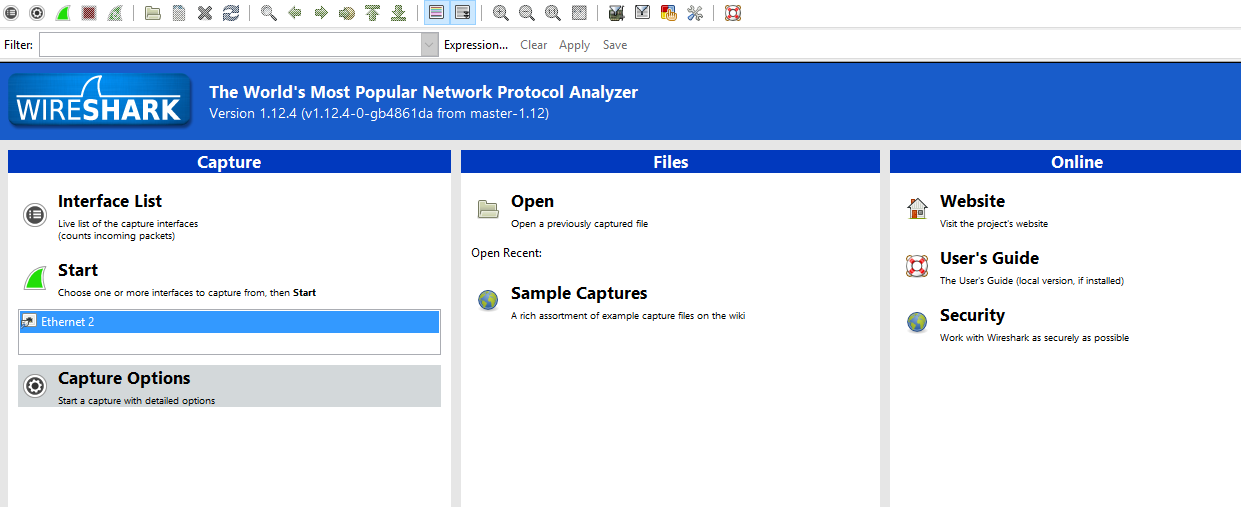
* Um die Installation fertig zu stellen klicken sie auf „Finish“.

**

*Abb.3: Wireshark-Setup – Installation fertig stellen*

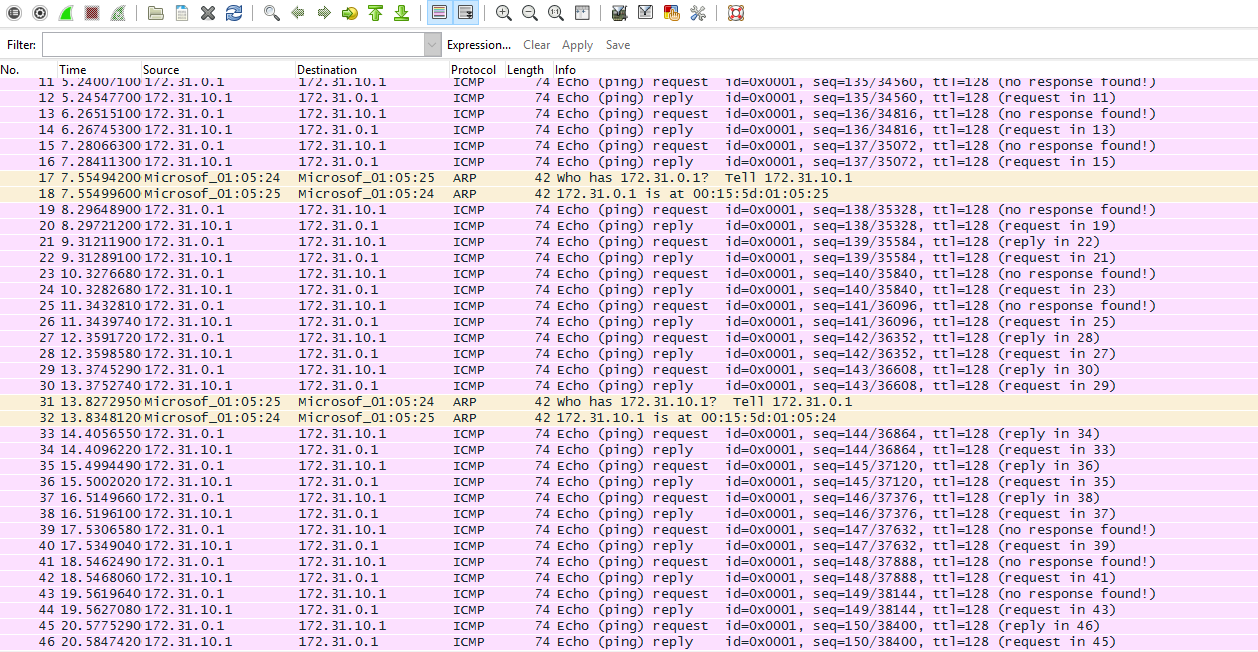
## Starten von Wireshark und Identifizieren der einzelnen Teile

* Melden Sie sich auf VM-Lab01 an
* Setzen Sie einen Dauerping auf 172.31.10.1 ab
* Starten sie Wireshark

**

*Abb.4: Ausschnitt aus dem Startfenster von Wireshark*

* Starten Sie das Capturen – auf dem Symbol der blauen Haifischflosse - und beenden Sie nach einigen Sekunden den Vorgang durch einen Klick auf dem roten, viereckigen Symbol

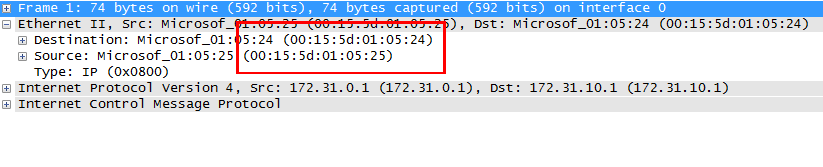
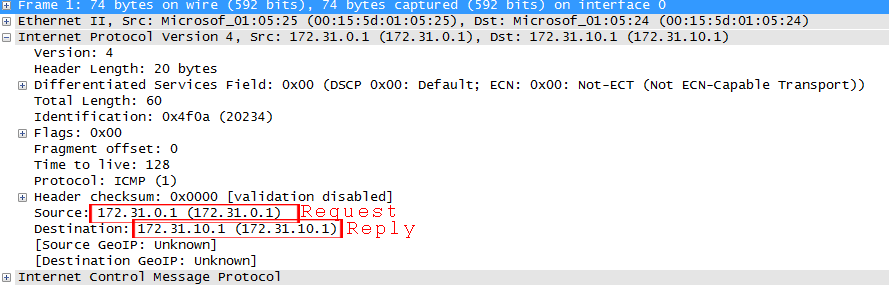
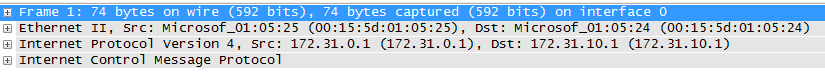


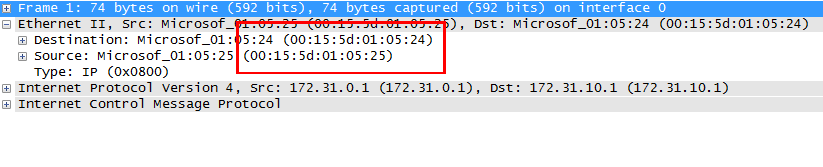
*Abb.5: Ausschnitt aus Wireshark, nach dem Capturen*

## Abspeichern des Mitschnitts

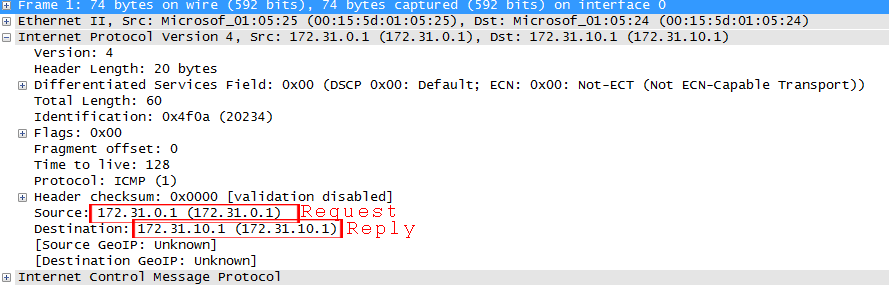
* Speichern Sie den Mitschnitt unter dem Dateinamen 01Cap ab

## Untersuchung des Packet-Detailbereiches

* Klicken Sie im Packt List-Bereich das erste Packet des Protokolls ICMP an.
* Wo können Sie die MAC Adresse des Absenders und des Empfängers auslesen  
    
  *Abb.6: Mac-Adressen*
* Von welcher IP-Adresse der der ICMP Request aus?
* Welche IP-Adresse hat einen ICMP Reply geschickt?  
    
  *Abb.7: IPv4 - Adressen*
* Wie viele Byte wurden im Frame verschickt?   
  *Abb.8: Byte im Frame*
* Von welcher MAC Adresse an welche MAC Adresse wurde versendet?

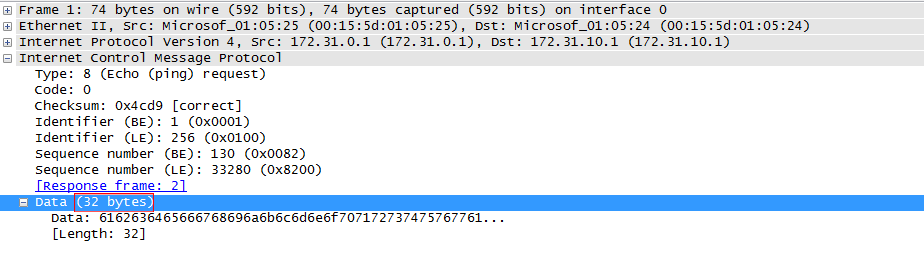
Es wurde von 00:15:5d:01:05:25 an 00:15:5d:01:05:24 (Destination, Ziel) gesendet.  
**  
*Abb.9: Mac-Adressen – gesendet, empfangen*

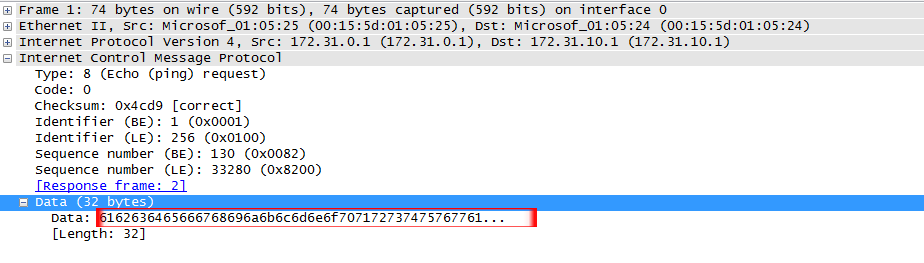
* Von welcher IP-Adresse an welche IP-Adresse wurde gesendet?

Es wurde von 172.31.0.1 an 172.31.10.1 (Destination, Ziel) gesendet.  
**  
*Abb.10: IP-Adressen – gesendet, empfangen*

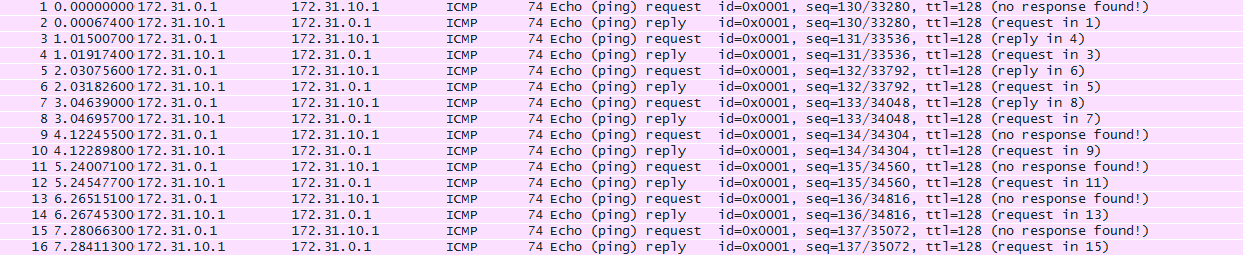
* Wie groß war der Header in der Vermittlungsschicht?

  
*Abb.11: Header Lenght*

* Wie viele Bytes wurden unter DATA verschickt?  
    
  *Abb.12: DATA Bytes*
* Welche Daten genau wurden unter DATA im ICMP-Befehl verschickt

  
*Abb.13: DATA Inhalt*

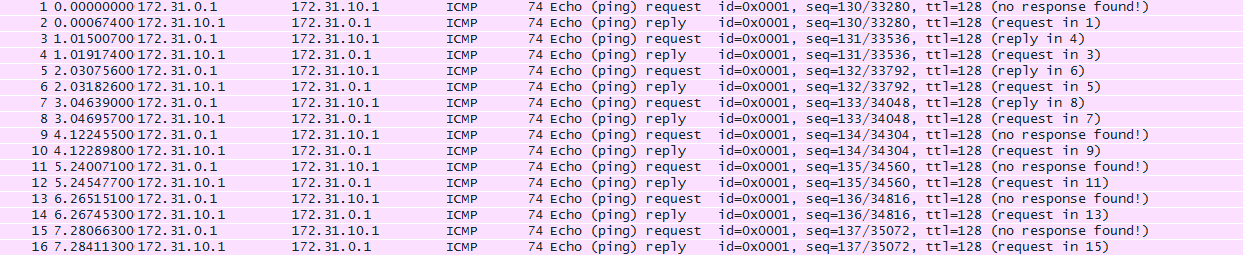
* Wie viele Pakete wurden durch den Ping-Befehl erzeugt?

Die „seq=150/38400“ minus „seq=130/33280“ = 20 Pakete.  


 *Abb.14: Anzahl der Pakete durch Ping Befehl*

* Wie war die Ablauffolge der Pakete zwischen den beiden PCs VM-Lab01 und VM-Lab02?

Request (Anfrage) – Reply (Antwort)



*Abb.15: Abfolge - Request-Reply*

## Beantwortung der Fragen

Aus wie vielen Bit besteht die MAC-Adresse einer Netzwerkkarte?

48 - Bit

Auf welcher OSI-Ebene findet der Vergleich zwischen der MAC-Adresse im Datenpaket und der MAC-Adresse der Netzwerkkarte statt?

Auf Layer 2, der DataLink Layer

Wie nennt man den Modus in dem die Netzwerkkarte geschalten werden muss, damit alle Datenpaket aufgenommen werden?

##### „promiskuitive Modus“

Welche Aufgabe hat ein Capture Filter in Wireshark?

Mit dem Capture Filter kann man bestimmen welche Art von Datenpaketen angezeigt werden soll.

Welche Aufgabe hat ein Display Filter in Wireshark?

Der Display Filter wird für die allgemeine Paketfilterung während der Anzeige verwendet.

Was versteht man unter dem Begriff Datenframe?

Ein Datenframe ist eine Protocol Data Unit auf der Sicherungsschicht des OSI-Modells.

Was versteht man unter dem Begriff Datenpaket?

Ein Datenpaket ist eine in sich geschlossene Dateneinheit, die zwischen zwei Computer (kommunizierenden Dingen) ausgetauscht wird.

Was versteht man unter dem Begriff Datensegment?

Ein Datensegment ist ein Teil von gewissen Dateien. z.B. von Objektdateien

Welchen Dateityp verwendet Wireshark um einen Mitschnitt in einer Datei zu speichern?

.pcapng

Wie heißen die drei Fensterteile die bei einem Mitschnitt in Wireshark angezeigt werden?

Paket List-Bereich, Paket Detail-Bereich, Paket Bytes-Bereich