NVS

Laborprotokoll – 04 – Winsocket Verbindung

Alexander Brenner

2015

Inhaltsverzeichnis

[1. Aufgabenstellung für dieses Labor 2](#_Toc469177818)

[2. Fragen zum Labor 04 2](#_Toc469177819)

[3. Durchführung des Labors 3](#_Toc469177820)

[3.1. Allgemeines zu Thema Socket Verbindung 3](#_Toc469177821)

[3.2. Installation eines Web-Servers auf VM-Lab02 4](#_Toc469177822)

[3.3. Einsatz diverser Netzwerk-Tools um Win-Socket Verbindungen anzuzeigen 5](#_Toc469177823)

[3.3.1 Netstat 5](#_Toc469177824)

[3.3.2 Netscan 7](#_Toc469177825)

[3.3.3 CurrPort, TCP-View – Nachweis der Win-Socket Verbindung 7](#_Toc469177826)

[3.3.4 TCPLogView 9](#_Toc469177827)

[3.3.4 httpNetworkSniffer 9](#_Toc469177828)

Untersuchen von Windows Socket Verbindungen mit diversen Tools

# Aufgabenstellung für dieses Labor

* Was ist eine Win-Socket Verbindung?
* Wie viele und welche Ports gibt es zu einer IP-Adresse?
* Installation eines Web-Servers – Internet Information Server – auf der Workstation VM-Lab01
* Verwendung diverser Tools zur Untersuchung von Win-Socketverbindungen wie zBsp.: netstat, TCPView, currport, Socketsniff, httpnetworksniffer

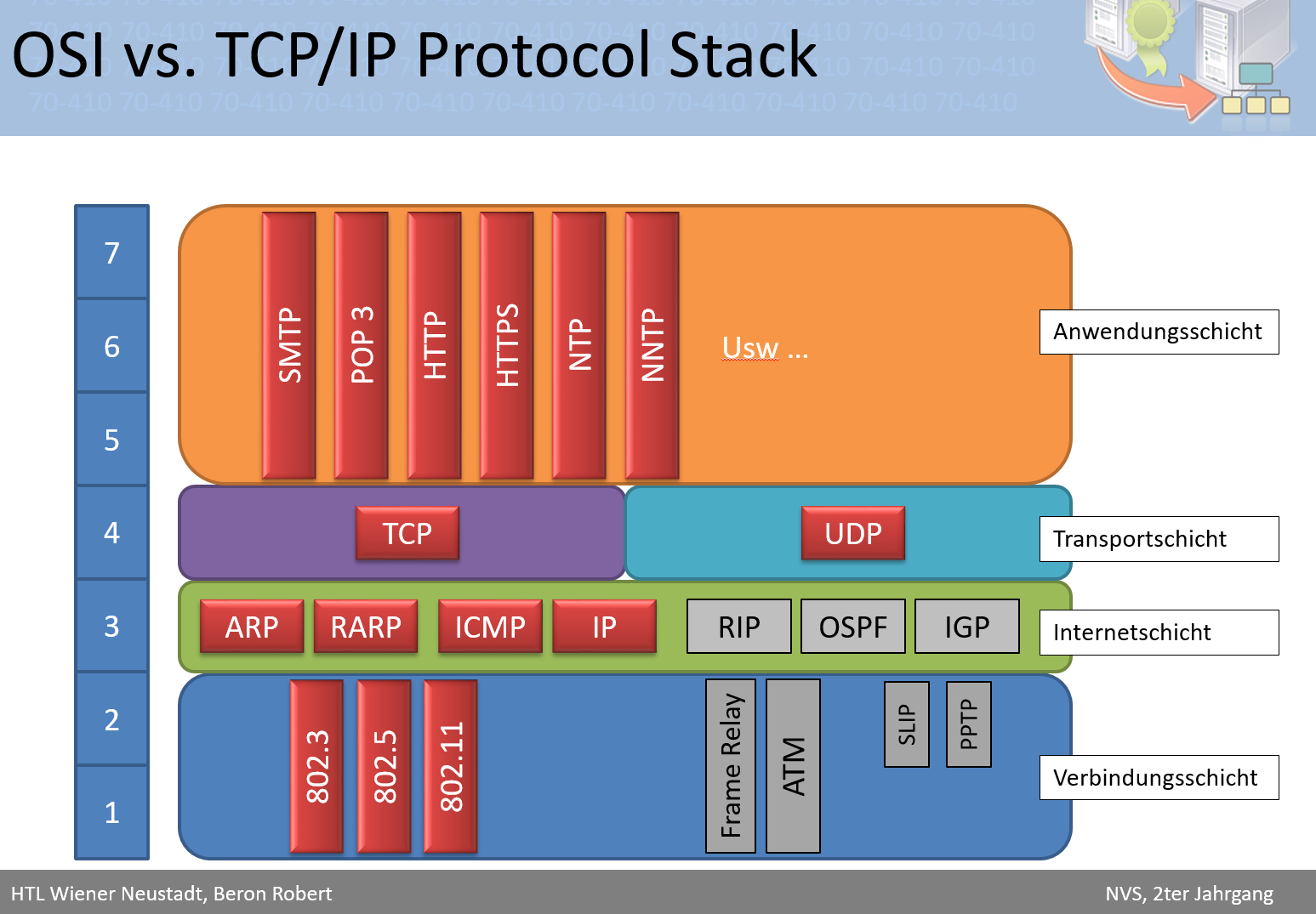
# Fragen zum Labor 04

1. Welche Transportprotokolle kennen Sie?
2. Wie heißen die vier Schichten des TCP/Ip Protocol Stacks
3. Wie viele Ports gibt es?
4. Die Ports werden in drei Kategorien eingeteilt. Wie heißen diese Kategorien und welche Art von Ports verwendet ein Browser der auf eine Antwort von einem Web-Server wartet
5. Wie nennt man die Protokolle http, ftp, smtp mit einem gemeinsamen Namen
6. Was versteht man unter dem Begriff Win-Socket Verbindung?
7. Warum ist es absolut notwendig, dass ein Web-Server als well-known Service auf TCP-Port 80 läuft?
8. Könnte ein Web-Server auch auf einem anderen Port betrieben werden? Was würde das für den Endanwender der ja einen Browser verwendet bedeuten?
9. Mit welcher Methode fordert ein Web-Browser die Startseite von einem Web-Server an?

# Durchführung des Labors

## Allgemeines zu Thema Socket Verbindung

Ein Socket ist ein vom Betriebssystem bereitgestelltes Objekt und dient als Kommunikationsendpunkt einer TCP oder UDP Verbindung. Allgemein existieren 65536 TCP bzw. UDP Ports hinter denen ein Dienst oder ein Client auf Datenpakete wartet.



*Abb.: OSI vs. TCP/IP Protokoll Stack mit diversen Protokollen in den unterschiedlichen Schichten*

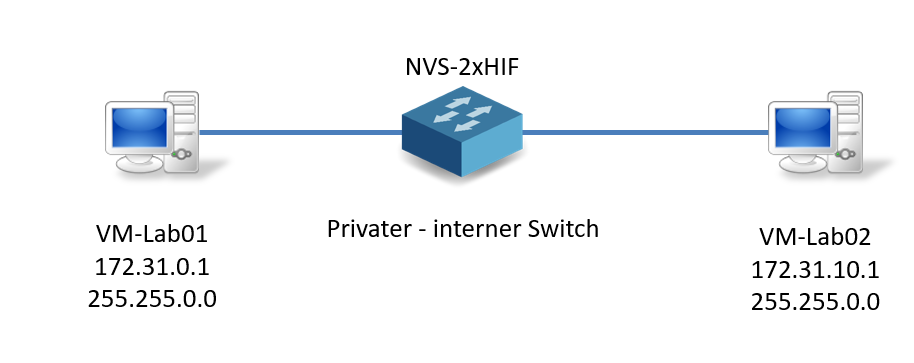
Ein Dienst verwendet dabei ein bestimmtes Transportprotokoll und einen oder mehrere Ports

|  |  |  |  |
| --- | --- | --- | --- |
| Dienst | Beschreibung | Transportprotokoll | Port |
| Web-Server | Host einer Website | TCP/UDP | 80 |
| FTP-Server | File Transfer Protocol | TCP | 21 |
| Ping  (auch Echo bzw. ICMP) | (Command-Line Befehle) | TCP/UDP | 7 |
| DNS | Domain Name System | TCP/UDP | 53 |
| SMTP | Simple Mail Transfer Protocol | TCP | 25 |
| POP3 | Post Office Protocol – Version 3 | TCP | 110 |
| IMAP4 | Internet Message Access Protocol | TCP | 143 |

Öffnen Sie dazu die Datei Services im Ordner C:\windows\system32\drivers\etc. In dieser Datei finden Sie die von der IANA als well-known Services definierten Ports.

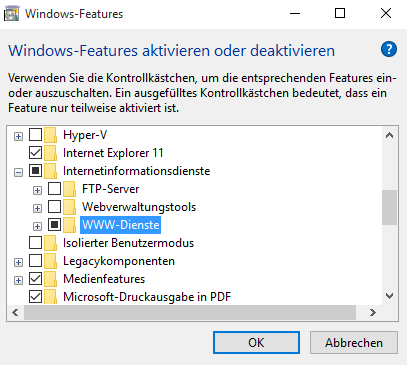
## Installation eines Web-Servers auf VM-Lab02

Die nachfolgende Konfiguration ist auch den beiden Workstations durchzuführen:



*Abb.: Konfiguration der virtuellen Maschinen des Labors*

*Installieren Sie in weiterer Folge über Programme und Features – Windows Features aktivieren einen Web-Server auf der Workstation VM-Lab 02 und beschreiben Sie diesen Vorgang der Installation. Sie finden den Web Server unter Internetinformationsdienste – WWW-Dienste*

**

*Abb.: Windows-Features aktivieren oder deaktivieren*

## Einsatz diverser Netzwerk-Tools um Win-Socket Verbindungen anzuzeigen

### 3.3.1 Netstat

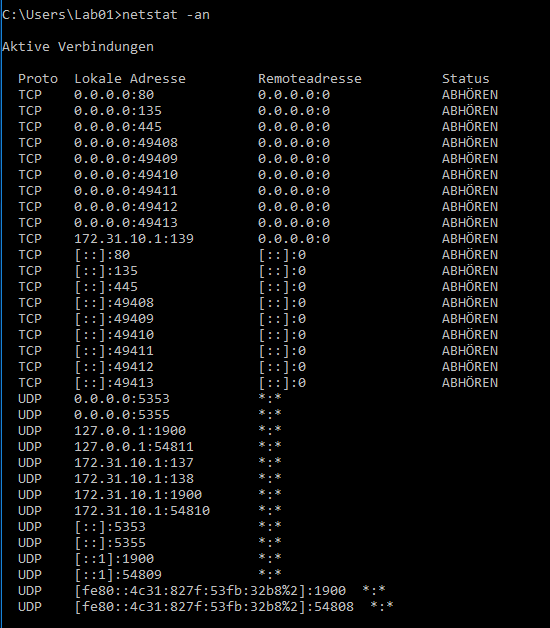
Stellen Sie mit Hilfe von netstat fest welche Dienste auf den beiden Rechner VM-Lab01 und VM-Lab02 laufen

*Listen Sie die Parameter und die Bedeutung dieser Parameter des Netstat-Befehls auf:*

|  |  |
| --- | --- |
| Parameter | Bedeutung |
| -an | Zeigt alle laufenden Verbindungen(-a), Ports(-a) & Portnummer(-n) und Adressen(-n) |
| -ano | Zeigt alle laufenden Verbindungen, Ports & Portnummer, Adressen und die mit jeder Verbindung verknüpfte, übergeordnete Prozesserkennung an |
| -o 5 | Zeigt in 5 Sekunden Abständen die „Statistik“ Informationen neu an |

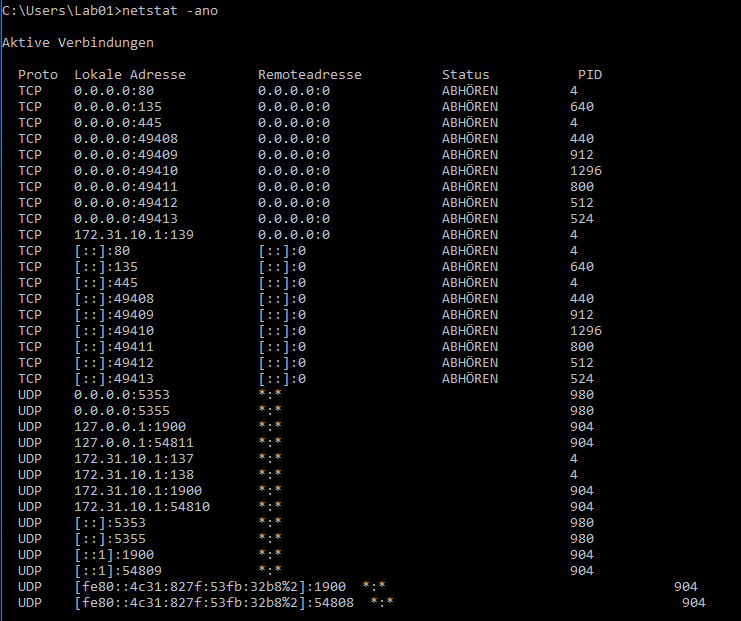
Erstellen Sie Screenshot bei VM-Lab02 für die nachfolgenden Befehle und erklären Sie die Anzeige

* Netstat –an



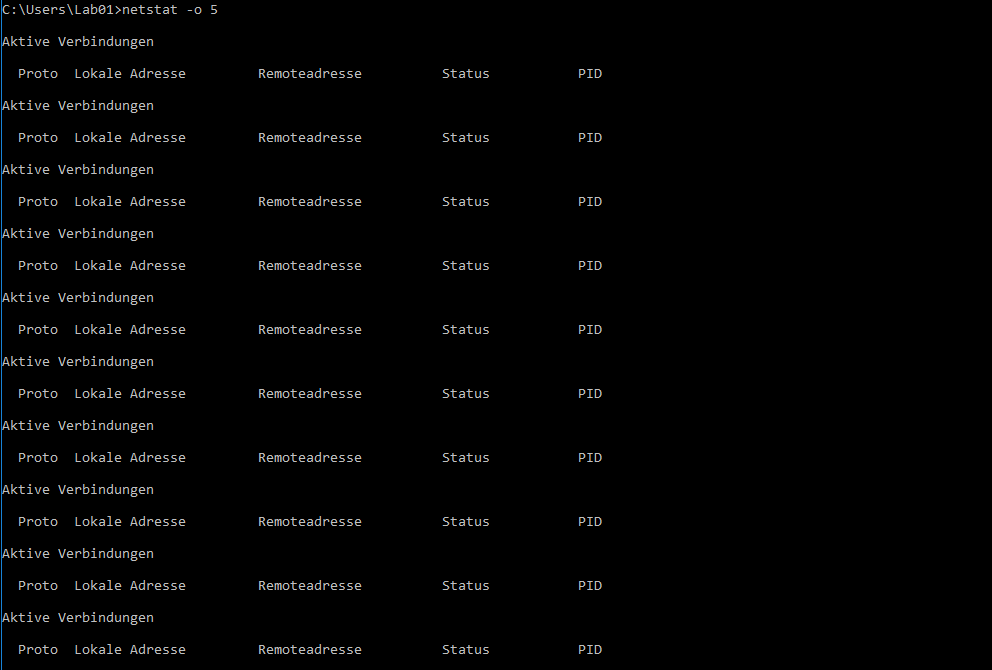
*Abb.: „netstat -an“ Befehl*

* Bei diesem Parameter bekommen wir Auskunft über TCP/UDP-Verbindungen und von welcher Adresse mit welchem Port diese kommen.
* Netstat –ano



*Abb.: „netstat -ano“ Befehl*

* Bei diesem Parameter bekommen wir Auskunft über TCP/UDP-Verbindungen und von welcher Adresse mit welchem Port diese kommen. Zusätzlich wird uns noch die Prozess-ID angezeigt.
* Netstat –o 5



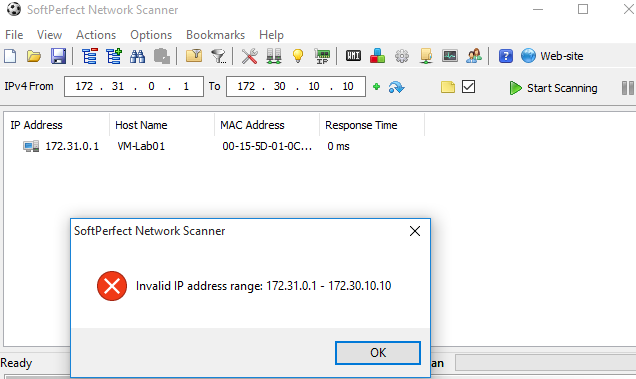
*Abb.: „netstat -o 5“ Befehl*

* Hier sehen wir, dass sich der „netstat“ Befehl alle fünf Sekunden „aktualisiert“. Da wir jedoch keine weiteren Parameter mitgegeben haben, sehen wir hier nur eine Art leere Tabelle.

### Netscan

Verwenden Sie den SoftPerfect Networkscanner VM-Lab01 Ordner C:\LaborSoftware\netscan\64-bit. Führen Sie einen Scann für den Bereich 172.31.0.1 bis 172.30.10.10 durch

Erstellen Sie einen Screenshot des Ergebnisses des Scans dar



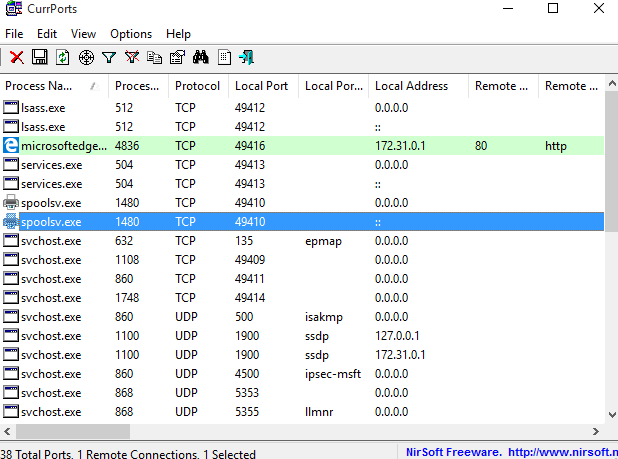
*Abb.: Ausschnitt aus dem Programm „SoftPerfect Network Scanner“*

### CurrPort, TCP-View – Nachweis der Win-Socket Verbindung

Mittels CurrPort bzw. TCPView soll die Win-Socket Verbindung zwischen dem Edge Browser und dem Web-Server nachgewiesen werden.

**Verwendung von CurrPort**

1. *Starten Sie CurrPort. Sie finden die Software auf VM-Lab01 im Ordner C:\LaborSoftware\NirSoft\*
2. *Starten Sie auf VM-Lab01 den Edge Browser*
3. *Geben Sie den URL* [*http://172.31.10.1*](http://172.31.10.1) *ein*
4. *Wechseln Sie zu CurrPort – erstellen Sie einen Screenshot und analysieren Sie diesen. Wo und durch was können Sie erkennen, dass der Edge Browser eine Verbindung zum Web-Server aufgenommen hat?*

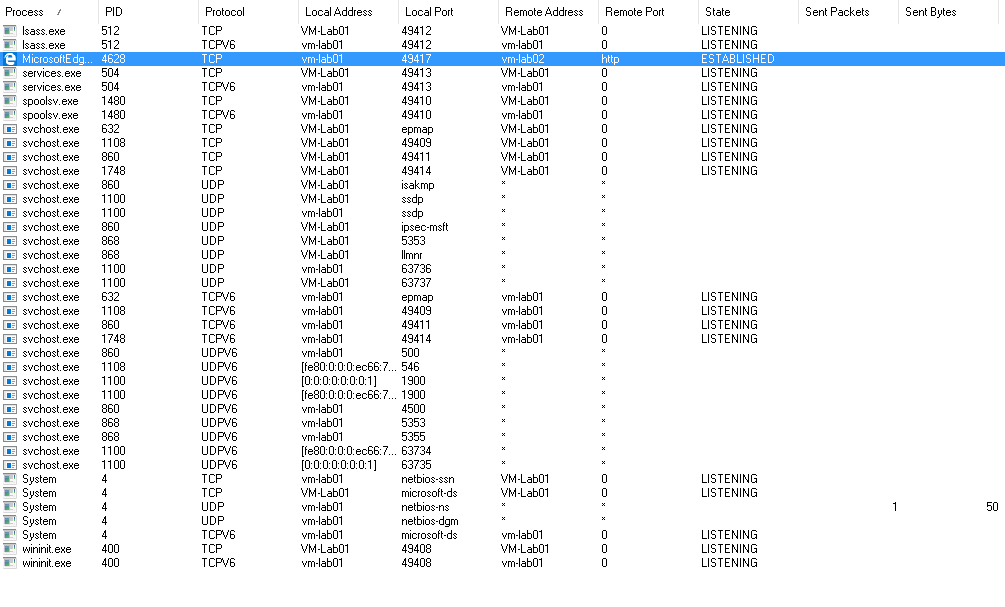
**

*Abb.: Ausschnitt aus dem Programm „CurrPorts“*

* Man sieht den Edge-Browser und die IP-Adresse unserer „VM-Lab01“. Das Feld ist grün hinterlegt und somit erkennen wir, dass er eine Verbindung zum Web-Server aufgebaut hat.

**Verwendung von TCP-View**

*Führen Sie dieselbe Aufgabe mit TCPView durch*

****

*Abb.: Ausschnitt aus dem Programm „TCP-View“*

* Man sieht den Edge-Browser, die Prozess-ID und das Protokoll. In der letzten Spalte unter dem Punkt „Status“ (State) steht bei dem Prozess „ESTABLISHED“ und daran erkennen wir, dass er eine Verbindung zum Web-Server aufgebaut hat.

### 3.3.4 TCPLogView

Verwenden Sie TCPLogView um das Öffnen und Schließen einer Web-Verbindung anzuzeigen. Sie finden die Software auf VM-Lab01 im Ordner C:\LaborSoftware\NirSoft\....

* *Starte den TCPLogView als Administrator*
* *Starten Sie den Edge-Browser und stellen Sie eine Verbindung mit dem Web-Server auf VM-LOAb02 her.*
* *Öffne die Startseite von http://172.31.10.1 mit einem Browser. Da der Inhalt aus dem lokalen Cache kommen kann müssen Sie unbedingt eine Aktualisierung der Startseite erzwingen.*
* *Wechseln Sie zu TCPLogView und warten Sie einige Zeit bis der Event Type „Close“ eingetragen wird.*
* *Erstellen Sie einen Screenshot der Anzeige*



*Abb.: Ausschnitt aus dem Programm „TCPLogView“*

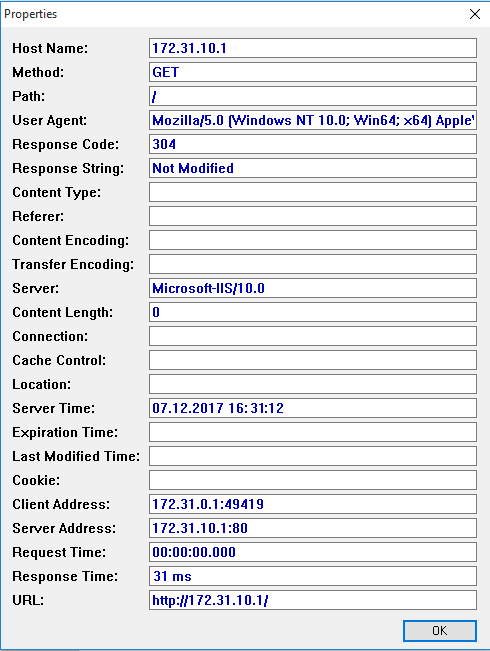
### httpNetworkSniffer

Verwenden Sie den httpNetworkSniffer auf VM-Lab01 Ordner C:\LaborSoftware\NirSoft\...

* *Starte den Sniffer als Administrator*
* *Öffne die Startseite von* <http://172.31.10.11>
* *Wechsle zum Sniffer und erstelle einen Screenshot der Anzeige*
* *Führe anschließend einen Doppelklick auf dem ersten Eintrag durch und erstelle von dem sich öffnenden Fenster ebenfalls einen Screenshot*

**

*Abb.: Ausschnitt aus dem Programm „httpNetworkSniffer“*



*Abb.: Ausschnitt des, sich beim Doppelklick öffnendem, Fenster*

## Beantwortung der Fragen zum LAB-04

1. Welche Transportprotokolle kennen Sie?

TCP/UDP

1. Wie heißen die vier Schichten des TCP/Ip Protocol Stacks

Application Layer – Transport Layer – Internet Layer – Link Layer

1. Wie viele Ports gibt es?

65536

1. Die Ports werden in drei Kategorien eingeteilt. Wie heißen diese Kategorien und welche Art von Ports verwendet ein Browser der auf eine Antwort von einem Web-Server wartet.(unterstrichen)

Standardisierte Ports, Registrierte Ports, Dynamische Ports

1. Wie nennt man die Protokolle http, ftp, smtp mit einem gemeinsamen Namen

Application Layer Protocol

1. Was versteht man unter dem Begriff Win-Socket Verbindung?

Winsock oder Windows Sockets ist eine Windows-Programmierschnittstelle (API) zum Zugriff auf Rechnernetze über Sockets.

1. Warum ist es absolut notwendig, dass ein Web-Server als well-known Service auf TCP-Port 80 läuft?

Weil wenn sich ein User dann mit dem Web-Server verbinden will muss er den speziellen Port extra eingeben. Es ist eine Norm.

1. Könnte ein Web-Server auch auf einem anderen Port betrieben werden? Was würde das für den Endanwender der ja einen Browser verwendet bedeuten?

Weil wenn sich ein User dann mit dem Web-Server verbinden will muss er den speziellen Port extra eingeben. Es ist eine Norm.

1. Mit welcher Methode fordert ein Web-Browser die Startseite von einem Web-Server an?

Sobald der User ein URL eingibt, stellt der Browser eine Verbindung zum Web-Server her, auf dem das angeforderte Dokument liegt. (http-Request)