

zertifiziert nach ISO 14001 validiert nach EMAS

# Frame analyse mit Wireshark

Laborprotokoll

Hier bitte ein originelles Gruppen-Logo einfügen.				

Unterrichtsgegenstand: <NWT1|ZIVK>

Jahrgang: 2BHIT

Name: Stefan Fürst

Betreuer: ZIVK

 Übungsdaten:
 23.02.2024

 Abgabedatum:
 23.02.2024



zertifiziert nach ISO 14001 validiert nach EMAS

### Inhaltsverzeichnis

1	Aufgabenstellung		
2			
3 Übungsdurchführung			
	3.1.1	Finden Sie drei Frames mit Unterschiedlichen "Type" Inhalten	
	3.1.2	Mehr infos zu den Protokollen (von wiki.wireshark.com)	6
	3.1.3 und woz	Recherchieren Sie welches Layer-3 Protokoll in dem Type-Feld verwendet vu es dient.	
4	Vollständ	dige Konfigurationsdateien (optional)	7
	4.1 <Ük	perschrift>	7
5	Abbildur	ngsverzeichnis	8
6	Anhang.		<u>9</u>



zertifiziert nach ISO 14001 validiert nach EMAS

## 1 Aufgabenstellung

Frame Analyse mit Wireshark

### 2 Zusammenfassung

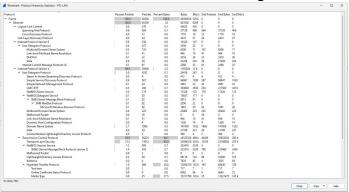


zertifiziert nach ISO 14001 validiert nach EMAS

### Übungsdurchführung

### 3.1.1 Finden Sie drei Frames mit Unterschiedlichen "Type" Inhalten

Um das Protokoll auszusuchen, habe ich auch Statistics und dann Protocol Hierarchy geklickt, in dem Fenster dann, die Protokolle ausgesucht.



**Abbildung 1:Protokoll Hierarchie** 

Type = Protokoll Smb, Dns, NetBIOS

#### Smb frame:

```
Smb frame:

Frame 50357: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Feb 23, 2024 14:24:22.118190000 Mitteleuropäische Zeit
[Time shift for this packet: 0.0000000000 seconds]
Epoch Time: 1708694662.118190000 seconds
[Time delta from previous captured frame: 0.460098000 seconds]
[Time delta from previous displayed frame: 14.564235000 seconds]
[Time since reference or first frame: 478.806645000 seconds]
Frame Number: 50357
Frame Length: 243 bytes (1944 bits)
Capture Length: 243 bytes (1944 bits)
[Frame is marked: False]
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:nbdgm:smb:browser]
[Coloring Rule Name: SMB]
[Coloring Rule String: smb || nbss || nbns || netbios]

Ethernet II, Src: Hewlettp-8c:ibf:56 (c8:d9:d2:8c:bf:56), Dst: Broadcast (ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.23.38.14, Dst: 10.23.38.255

NetBIOS Datagram Service

SMB (Server Message Block Protocol)
> SMB Hailslot Protocol
Opcode: Write Mail Slot (1)
Priority: 0
Class: Unreliable & Broadcast (2)
                                                   Priority: 0
       Class: Unreliable & Broadcast (2)
Size: 50
Mailslot Name: \MAILSLOT\BROWSE
> Microsoft Windows Browser Protocol
```

#### **Abbildung 2:Smb Frame**



zertifiziert nach ISO 14001 validiert nach EMAS

#### Dns frame:

```
Dns frame:

Frame 251: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Feb 23, 2024 14:16:38.373888000 Mitteleuropäische Zeit
[Time shift for this packet: 0.0000000000 seconds]
Epoch Time: 1708694198.373888000 seconds
[Time delta from previous displayed frame: 0.067448000 seconds]
[Time delta from previous displayed frame: 3.098645000 seconds]
[Time since reference or first frame: 15.062343000 seconds]
Frame Number: 251
Frame Length: 82 bytes (656 bits)
Capture Length: 82 bytes (656 bits)
[Frame is marked: False]
[Frame is marked: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HewlettP &scib:63 (c8:d9:d2:8c:bb:63), Dst: Cisco_a1:3f:61 (40:b5:c1:a1:3f:61)

Internet Protocol Version 4, Src: 10.23.38.20, Dst: 193.170.234.182

User Datagram Protocol, Src Port: 58754, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xa479

> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Additional RRs: 0

Queries

> wpad.htl-donaustadt.at: type A, class IN
                        → Queries

> wpad.htl-donaustadt.at: type A, class IN
```

#### **Abbildung 3: Dns Frame**



zertifiziert nach ISO 14001 validiert nach EMAS

NetBios(nbns)frame:

```
NetBios(nbns)frame:

61296.809.29278 10.23.38.20 193.170.234.183 NBNS Retresh NB HTL22<00>

▼ Frame 61138: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Feb 23, 2024 14:29:25.473133800 Mitteleuropäische Zeit
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1708069965.473133000 seconds
[Time delta from previous captured frame: 0.372232000 seconds]
[Time delta from previous displayed frame: 1.159117000 seconds]
[Time delta from previous displayed frame: 1.159117000 seconds]
[Time since reference or first frame: 782.161588000 seconds]
Frame lumber: 61138
Frame Length: 110 bytes (880 bits)

Capture Length: 110 bytes (880 bits)

[Frame is marked: False]
[Protocols in frame: ethiethertype:ipiudp:nbns]
[Coloring Rule String: smb | [ nbns | [ netbios]

Tethernet IT, Sec: Hewlette Re: ebb653 (sciela/22.86:bbis3), Dst: (isco_al:3f:61 (40:b5:cl:al:3f:61)

Internet Protocol Version 4, Sec: 18-23.38.20, Dst: 193.170.234.183

VBLED Dataggma Protocol, Src Port: 137, Dst Port: 137

NetBOS Name Service

Fransaction ID: 0xb3c3

> lags: 0x4000, Opcode: Refresh
Questions: 1
Answer RRs: 0
Additional RRs: 0
Additional RRs: 0
Additional RRs: 0
Additional RRs: 0
> V380EC18
                Additional Rhs. 1

V Queries

> V308PC10<00>: type NB, class IN

Additional records

> V308PC10<00>: type NB, class IN
```

#### Abbildung 4:nbns frame

#### 3.1.2 Mehr infos zu den Protokollen (von wiki.wireshark.com)

Dns: Domain name System -> Namesauflösung, Ips zu domains.

Smb: Server Message Block Protocol. Benutzt, um Zugriff auf zb Dateien oder Drucker zu teilen.

Nbns: Dasselbe wie dns, mit dem Unterschied, aber ist dafür da, um smb Verbindungen zu machen, bevor es Smb über tcp gab. Deshalb wird es noch in vielen Windoof netzwerken verwendet, wo noch ältere Windoof geräte sind, die smb over tcp noch nicht unterstützen

#### 3.1.3 Recherchieren Sie welches Layer-3 Protokoll in dem Type-Feld verwendet wird und wozu es dient.

Logischerweise wird ipv4 benutzt. (Ipv6 hater sind idioten und es sollte man endlich mehr adopted werden, damit wir dumme nat scheiße endlich mal los sind)

Ipv4 ist dazu da, um packets von einer ip adresse zu einer anderen zu bekommen, dass Ip Protokoll sorgt, dann für die Übertragung unabhängig von der darunterliegenden Netzwerk Hardware. Wenn lokal, wird arp benutzt, um die Kommunikation über mac adressen zu machen.



zertifiziert nach ISO 14001 validiert nach EMAS

- 4 Vollständige Konfigurationsdateien (optional)
- 4.1 <Überschrift>

#### htl donaustadt Donaustadtstraße 45

1220 Wien

Abteilung: Informationstechnologie Schwerpunkt: Netzwerktechnik



zertifiziert nach ISO 14001 validiert nach EMAS

## 5 Abbildungsverzeichnis

Abbildung 1:Protokoll Hierarchie	. 4
Abbildung 2:Smb Frame	. 4
Abbildung 3: Dns Frame	. 5
Abbildung 4:nbns frame	. 6

htl donaustadt Donaustadtstraße 45 1220 Wien

Abteilung: Informationstechnologie Schwerpunkt: Netzwerktechnik



zertifiziert nach ISO 14001 validiert nach EMAS

6 Anhang <br/>
<Hier werden alle zusätzlichen Beilagen angefügt. Dies sind zum Beispiel die ausgefüllten Cisco Laborblätter!>