htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

htl donaustadt

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**

Inhaltsverzeichnis

1 Aufgabenstellung

Frame Analyse mit Wireshark

2 Zusammenfassung

3 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.

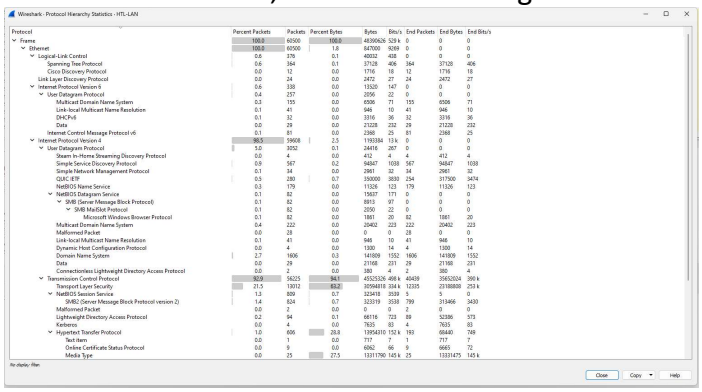

Abbildung 1:Protokoll Hierachie

Type = Protokoll
Smb, Dns, NetBIOS
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: 0.000000000 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 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:bf:56 (c8:d9:d2:8c:bf:56), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.23.38.14, Dst: 10.23.38.255
> User Datagram Protocol, Src Port: 138, Dst Port: 138
> NetBIOS Datagram Service
v SMB (Server Message Block Protocol)
  > SMB Header
  > Trans Request (0x25)
v SMB MailSlot Protocol
    Opcode: Write Mail Slot (1)
    Priority: 0
    Class: Unreliable & Broadcast (2)
    Size: 50
    Mailslot Name: \MAILSLOT\BROWSE
> Microsoft Windows Browser Protocol
```

Abbildung 2:Smb Frame

Dns frame:

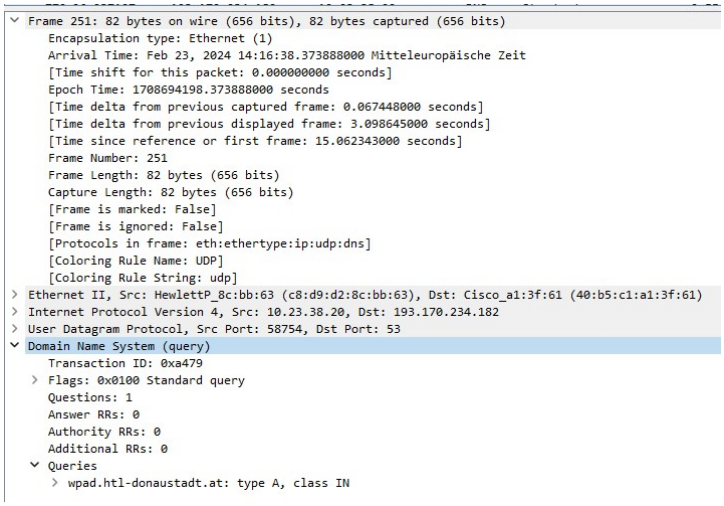

Abbildung 3: Dns Frame

NetBios(nbns)frame:

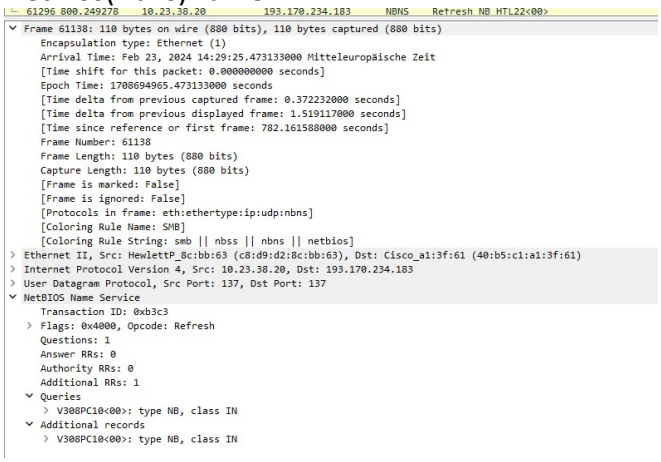

Abbildung 4:nbns frame

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.

4 Vollständige Konfigurationsdateien (optional)

4.1 <Überschrift>

5 Abbildungsverzeichnis

6 Anhang

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