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 3](#_Toc159593617)

[2 Zusammenfassung 3](#_Toc159593618)

[3 Übungsdurchführung 4](#_Toc159593619)

[3.1.1 Finden Sie drei Frames mit Unterschiedlichen "Type" Inhalten 4](#_Toc159593620)

[3.1.2 Mehr infos zu den Protokollen (von wiki.wireshark.com) 6](#_Toc159593621)

[3.1.3 Recherchieren Sie welches Layer-3 Protokoll in dem Type-Feld verwendet wird und wozu es dient. 6](#_Toc159593622)

[4 Vollständige Konfigurationsdateien (optional) 7](#_Toc159593623)

[4.1 <Überschrift> 7](#_Toc159593624)

[5 Abbildungsverzeichnis 8](#_Toc159593625)

[6 Anhang 9](#_Toc159593626)

# Aufgabenstellung

Frame Analyse mit Wireshark

# Zusammenfassung

# Übungsdurchführung

### 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.

Ein Bild, das Text, Screenshot, Zahl, Software enthält.

Automatisch generierte Beschreibung

Abbildung :Protokoll Hierarchie

Type = Protokoll

Smb, Dns, NetBIOS

Smb frame:

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Abbildung :Smb Frame

Dns frame:

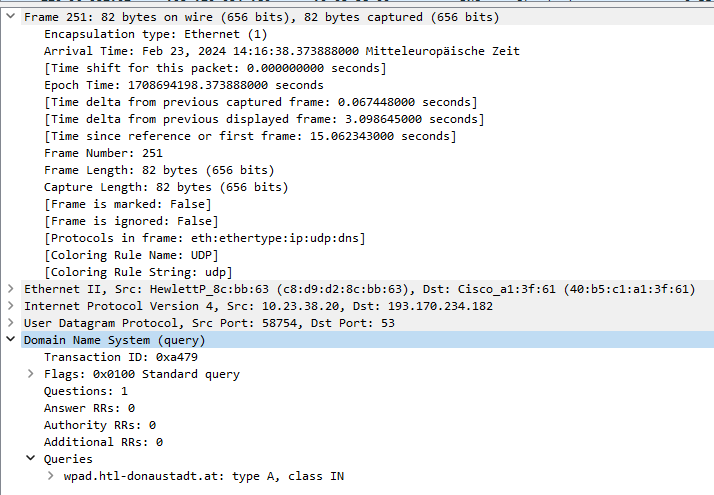


Abbildung : Dns Frame

NetBios(nbns)frame:

Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

Automatisch generierte Beschreibung

Abbildung :nbns frame

### 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

### 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.

# Vollständige Konfigurationsdateien (optional)

## <Überschrift>

# Abbildungsverzeichnis

[Abbildung 1:Protokoll Hierarchie 4](#_Toc159593685)

[Abbildung 2:Smb Frame 4](#_Toc159593686)

[Abbildung 3: Dns Frame 5](#_Toc159593687)

[Abbildung 4:nbns frame 6](#_Toc159593688)

# Anhang

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