**Lab 1: Testen von Firmen-Netzwerken** [Pascal Schwarz, Yanick Eberle]

1. **Wireshark**

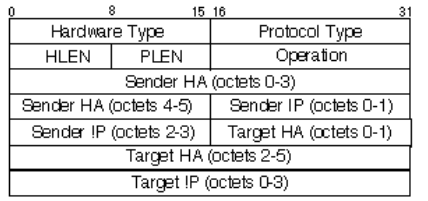
****

Bild 1:ARP-Message

* 1. 6 Byte
  2. ARP request
  3. Ja
  4. Operation (Opcode)
  5. arp -n

**Address HWtype HWaddress Flags Mask Iface**

10.196.134.1 ether ee:ee:ee:01:07:06 C eth0

10.196.134.127 ether 54:42:49:56:7c:bc C eth0

**Address**: zu welcher IP gehört der Rest der Information in der Zeile?

**HWType**: gibt layer1/2 typ an

**HWAddress**: der IP (Spalte 1) zugeordnete Hardwareadresse (hier MAC-Adresse)

**Flags**: C steht für Complete (ARP Anfrage abgeschlossen), M wäre permanent, P publish

**Mask**: würde zusammen mit publish benutzt

**Iface**: über welches Interface ist die HWAddr erreichbar

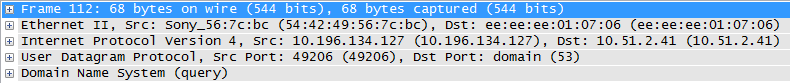
1. **ping, hping3, dig, traceroute**
   1. Perl Script
   2. **DNS Protokoll**

a)UDP

Vorteile:

-geringeren Verlustleistung

-besserer Performance



b) Auf Zielhost wird auf Port 53 abgehört. Da es eine Anfrage ist, ist der Destination Port 53.



c) Felder und Bedeutung

**Time**: Antwortzeit

**Transaction** **ID**: eindeutige Nummer, übereinstimmend mit Transaction ID der DNS Request

**Flags**: Flags, ob Request, Response, Error, no Error, ...

**Questions**: Anzahl Anfragen

**Answer** **RRs**: Anzahl Antworten

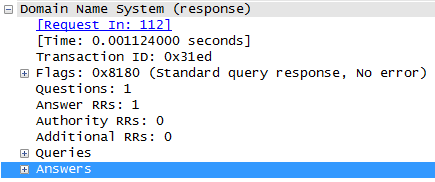
**Authority RRs**: RRs, die auf verantwortliche Server deuten

**Additional RRs:** RRs mit weiteren Informationen/Records

RR steht hier für **Resource Record**, ein Format zur Angabe des Mappings von IP-Adresse zu Name bzw. umgekehrt - oder weitere Information. Resource Records sind die Einträge in den Datenbank-Files des Name Servers.

**Queries**: Anfrage

**Answers**: Antwort



d) Felder und Bedeutung

**NAME**: Der Domain-Name, zu der dieser RR gehört.

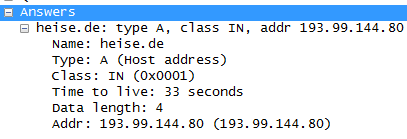
**TYPE**: Der RR-Typ Code. Spezifiziert die Bedeutung des Feldes RDATA. Zwei Oktets.

**CLASS**: RR-Klasse. Spezifiziert die Bedeutung des Feldes RDATA. Zwei Oktets.

**TTL**: Time To Live - eine 32-bittige Zahl, die die Anzahl der Sekunden angibt, für die man diesen Record im Cache behalten darf. Null bedeutet, das dieser RR nur für die aktuelle Transaktion gilt.

**RDLENGTH**: Eine 16-bittige Zahl, die die Anzahl der Oktets im RDATA Feld angibt.

**RDATA**: Ein String variabler Länge (Oktets), der die Resource beschreibt. Das Format hängt von den Setzungen in TYPE und CLASS ab. Bei TYPE = A und CLASS = IN wäre das also eine normale 4 Oktet (32-bittige) ARPA Internet Adresse.



**Quelle: http://doc-tcpip.org/Dns/named.dns.message.html**

* 1. **tracert**



Die geographische Lage der Router kann insbesondere in diesem Beispiel über die reverse DNS Einträge festgelegt werden.

Bsp: \*.zrh1.he.net ist in Zürich

Der Sprung passiert folglich zwischen Hop 13 und 14, also zwischen Amsterdam und Washington.

Grundsätzlich sollte der Sprung an der Latenzzeit ersichtlich sein. In diesem Fall ist die Latenzzeit der Router in Frankfurt und Amsterdam jedoch schon sehr hoch, was ev. auf eine Überlastung am Übergang zwischen he.net und xo.net in Frankfurt (am DE-CIX) zurückzuführen ist.

3) black

4) metasploit black

5) Scan

**Footprinting-Phase**

4.1nettools1

**WHOIS**

Domain name:  
fhnw.ch  
  
Holder of domain name:  
Fachhochschule Nordwestschweiz FHNW  
Graf Heinz  
ICT Kommunikation  
Steinackerstrasse 5  
CH-5210 Windisch  
Switzerland  
Contractual Language: German  
  
Technical contact:  
Fachhochschule Nordwestschweiz FHNW  
Graf Heinz  
ICT Kommunikation  
Steinackerstrasse 5  
CH-5210 Windisch  
Switzerland  
  
DNSSEC:N  
  
Name servers:  
ns.inwx.de  
ns1.fhnw.ch [147.86.3.20]  
ns2.fhnw.ch [147.86.3.21]

**Scanning-Phase**

**Zusammenstellung Ergebnisse**