Thomas Merkel, Arthur Henkel

Aufgaben Wireshark

1. Capture-Filterstrings
   a) **`host 141.69.209.31 and port 53`**
   IP-Quell- oder IP-Ziel-Adresse 141.69.209.21 und Port-Quell- oder Port-Ziel 53 (DNS)
   b) **`icmp`**
   Pakete mit dem „icmp“ Protokoll
   c) **`ip[0] & 0xf0 = 0x40`**
   IPv4 Pakete, ersten 8 Byte der IP Adresse undiert mit 0xf0 ergibt 4
   d) **`ether[0] & 1 = 0`**
   Unicast Paket, LSB (iG-Bit) der MAC DA auf 0
   e) **`ether[12] = 0x08 and ether[13] = 0x00`**
   IPv4 Paket, 0x0800 entspricht beim 13 und 14 Byte IPv4
   f) **`ether[12:2] = 0x0806`**
   ARP Pakete (0x0806), ether[12:2] entspricht dem Ethernet Type Feld
   g) **`host 141.69.201.205 and (port 20 or port 21)`**
   IP-Quell- oder IP-Ziel-Adresse 141.69.201.205 und Port-Quell- / Port-Ziel 20 (FTP Data) oder Port-Quell- / Port-Ziel 21 (FTP Control)

2. Display-Filterstrings
   a) **`pop`**
   IP-Datenpakete mit dem POP Protokoll
   b) **`ip.addr == 192.168.0.10 && tcp.port == 80`**
   IP-Datenpakete von und zu 192.168.0.10 und TCP-Datenverkehr zum und vom TCP -Port 80 (HTTP)
   c) **`udp.port == 53`**
   UDP-Datenverkehr zum und vom UDP-Port 53 (DNS) von allen Rechnern
   d) **`icmp.type == 0 || icmp.type == 8`**
   ICMP Datenpakete mit dem Typ 0 (Echo-Reply) oder Typ 8 (Echo-Request)

3. Bezeichnung und Beziehung folgender Adressen
   a) **`FF:FF:FF:FF:FF:FF`**
   MAC Adresse, alle 48 Bits auf 1, entspricht Broadcast Adresse und wird an alle Geräte im LAN gesendet.
   b) **`01-80-C2-00-00-10`**
   MAC Adresse, Bridge Management Group Address (deprectated)
   Quelle: http://standards.ieee.org/regauth/groupmac/Standard_Group_MAC_Address_assignments.pdf
   c) **`255.255.255.255`**
   Flooded Broadcast, Limited Broadcast
   d) **`141.69.1.255`**
   (Subnet-) Directed Broadcast
   e) **`141.69.255.255`**
   All-Subnet-Directed-Broadcast
   f) **`224.0.0.1`**
   Multicast Adresse, alle Hosts im selben Netzwerksegment