

Vorname:

## Hinweise zu Wireshark

- 1. Selektieren Sie für die Überwachung das Symbol
- 2. Wählen Sie dann die Verbindung aus, die auch eine IP-Adresse besitzt und starten Sie das Abhören.
- 3. Beenden Sie das Abhören mit dem Symbol
- 4. Um den Datenverkehr zu filtern, geben Sie unter Filter den Namen des Filters ein, also entweder arp, http, smtp oder pop.

📶 (Untitled) - Wireshark
<u>File Edit View Go Capture Analyze Statistics H</u> elp
≝≝≝≝≦≦© ⊒ × % ≞ © ≎ ⇔ ⇔ ൷ ⊈ [≡ ⊒ ( , , , , , ) ≝
Eilter: arp Expression Clear Apply
No Time Source Destination Protocol Info
108 21.838471 Fujitsus_75:95:64 Broadcast ARP Who has 192.108.2.3? Tell 192.108.1.250
109 21.838481 QuantaCo_36:a8:13 Fujitsu5_75:95:64 ARP 192.168.4.23 is at 00:c0:9f:36:a8:13
199 25.010096 Netronix_51:6d:40 Broadcast ARP who has 192.168.2.3? Tell 192.168.2.100
200 25.131855 Fujitsus_75:95:64 Broadcast ARP Who has 192.168.0.6? Tell 192.168.1.250 415 32.510721 Netronix 51:6d:40 Broadcast ARP Who has 192.168.2.3? Tell 192.168.2.100
540 40.009938 Netronix_51:6d:40 Broadcast ARP Who has 192.168.2.3? Tell 192.168.2.100
■ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: FujitsuS_/S:93:cf (00:30:05:/S:93:cf), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff) Address Resolution Protocol (request)
Eile Edit Wew Go Capture Apaluze Statictics Help
Lie Far Jew 30 Cabrate Buaixes Starizaria
Eiker: http
No Time Source Destination Protocol Info
112 21.841760 192.168.4.23 85.13.129.171 HTTP GET / HTTP/1.1
132 23.309197 192.168.4.23 85.13.129.171 HTTP GET /style.css HTTP/1.1
136 23.311252 85.13.129.171 192.168.4.23 HTTP HTTP/1.1 200 OK (text/css) 138 23.579613 192.168.4.23 85.13.129.171 HTTP GET /images/eule.gif HTTP/1.1
143 23.580987 85.13.129.171 192.168.4.23 HTTP HTTP/1.1 200 OK (GIF89a)
143 25.391167 192.106.4.25 63.15.129.1/1 ППР GET / IIIdges/preti_ex.gli ППР/1.1 1 // либ 22 502152 85 12 120 171 102 168 // 22 НТТВ НТТВ/1 1 200 ок (стеябы)
Hypertext Transfer Protocol
via: 1.1 SERVER02\r\n
Content-Length: 6448
Age: 284\r\n
Content-Type: text/html\r\n
Server: Apache/1.3.2/ (Linux/SuSE) mod_fastcgi/2.4.2 FrontPage/4.0.4.3 PHP/4.4.1 mod_peri/1.2/ mod_ssi, Last-Modified: Tue, 30 oct 2007 12:57:38 GMT\r\r
ETag: "138f37-1930-47272a42"\r\n
Accept-Ranges: bytes\r\n Keen-Alive: timeout-1max-100\r\n
\r\n
□ Line-based text data: text/html
<pre><!--uocitype Hime Public =//w3C//DID HIME 4.01 Transitional//EN --></pre>
0000 00 c0 9f 36 a8 13 00 30 05 75 95 64 08 00 45 0060 .u.dE.
0020 04 17 00 50 04 6d 42 85 f6 4a a1 8e 53 a2 50 18P.mBJS.P.
PO220  to So do bt 00 00 74 69 25 20 25 21 20 70 72 2b  to St 0pv+    Frame (462 bytes)  Reassembled TCP (6836 bytes)
File: "C:\DOKUME~1\thempel\LOKALE~1\Temp\etherXXX88T32T" 245 KB 00:00:43 P: 594 D: 85 M: 0 Drops: 0