Wireshark - filtry

Bardzo ważnym elementem pracy z analizatorem protokołu jest korzystanie z filtrów przechwytywania i wyświetlania. W programie Wireshark filtry tworzy sie w oparciu o następujące zasady:

[pole operator_relacji wartosc] operator_logiczny [pole operator_relacji wartosc] ...

Przy czym wartość w nawiasie [] może odpowiadać także protokołowi. W takim wypadku w nawiasie [] umieszczana jest tylko nazwa protokołu.

Operatory relacji:

- == - równe,
- != - rózne,
- > - wieksze,
- < - mniejsze,
- >= - wieksze lub równe,
- <= - mniejsze lub równe.

Operatory logiczne

- and, && - logiczne AND
- or, || - logiczne OR
- not, ! - logiczne NOT

Nazwy protokołów

arp, dns, tcp, udp, ip, ipv6, irc, idp, ipx, http, pop, smtp, ftp, gnutella, kerberos, l2tp, netlogon, smb, ...

Przykładowe pola - Ethernet

- eth.addr ==
- eth.dst ==
- eth.len ==
- eth.src ==
- eth.trailer ==
- eth.type ==

Przykładowe pola - IP

- ip.dst eq www.mit.edu
- ip.src == 192.168.1.10
- ip.addr == 129.110.0.0/16
- ip.fragment ==
- ip.id ==
- ip.len ==
- ip.ttl ==

Przykładowe pola - TCP

- tcp.port == 80
- tcp.dstport ==
- tcp.srcport ==
- tcp.ack == numer potwierdzenia
- tcp.flags == flaga 8-bit
- tcp.flags.reset ack, syn, fin,
- tcp.len == ???
- tcp.window_size ==

Przykładowe pola - UDP

- udp.checksum ==
- udp.checksum_bad ==
- udp.dstport ==
- udp.length ==
- udp.port ==
- udp.srcport ==

Przykładowe pola - HTTP

- http.cookie ==
- http.host ==

Przykładowe pola - Echo

- echo.data ==
- echo.request ==
- echo.response ==