



Capture Filters

Capture Filters

» What are capture filters?

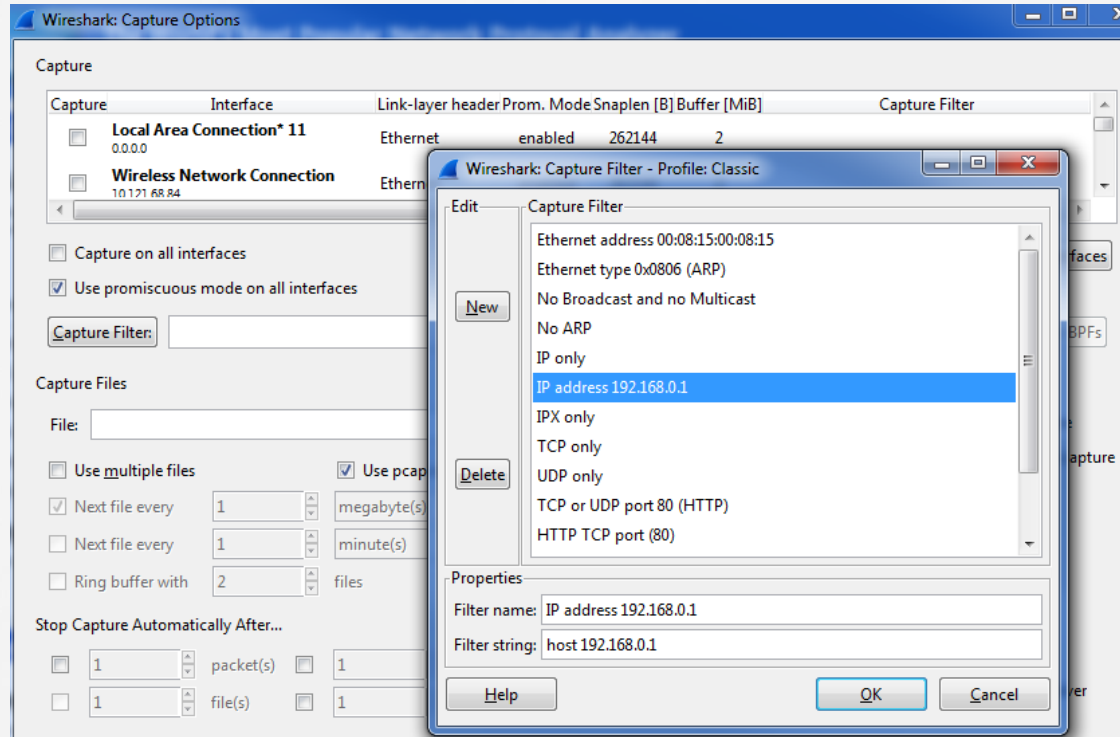
» Capture filter rules

- Only applied before capture, not after
- Different syntax than display filters
- Use Berkeley Packet Filter (BPF) format

» Using capture filters

- Found in Launch Pad | Capture Options

Capture Filters



Capture Filters

» How can I edit cfilters?

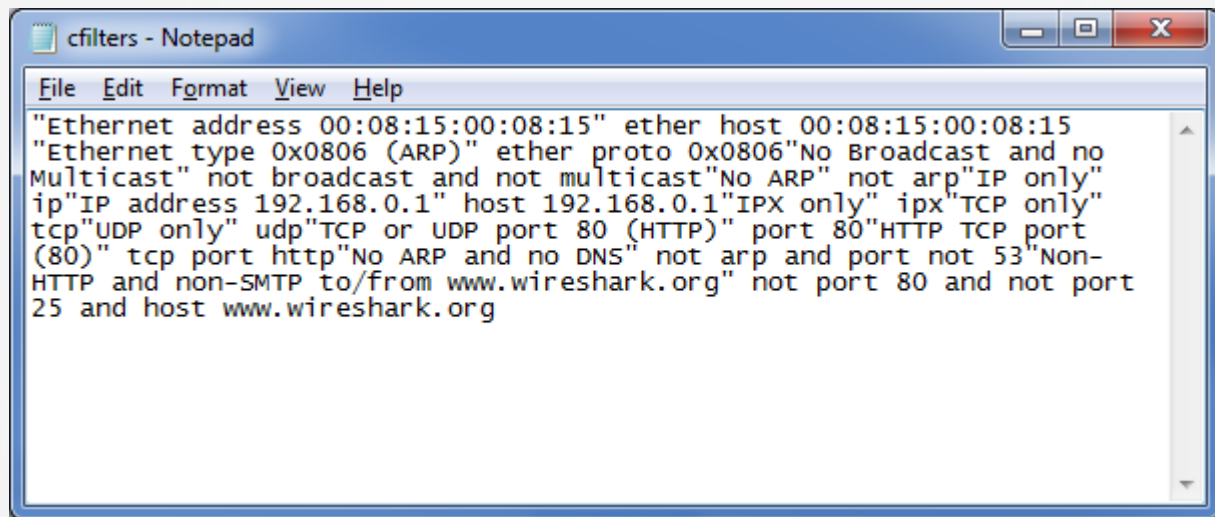
» GUI

- You can add filter strings as needed—example: udp
- You can copy other strings and add them to the dialog box

» Notepad

- You can add filter strings manually to the file
- You can make a copy of another cfilters file or the contents within one to your files

Capture Filters



```
"Ethernet address 00:08:15:00:08:15" ether host 00:08:15:00:08:15
"Ethernet type 0x0806 (ARP)" ether proto 0x0806"No Broadcast and no
Multicast" not broadcast and not multicast"No ARP" not arp"IP only"
ip"IP address 192.168.0.1" host 192.168.0.1"IPX only" ipx"TCP only"
tcp"UDP only" udp"TCP or UDP port 80 (HTTP)" port 80"HTTP TCP port
(80)" tcp port http"No ARP and no DNS" not arp and port not 53"Non-
HTTP and non-SMTP to/from www.wireshark.org" not port 80 and not port
25 and host www.wireshark.org
```

Questions?