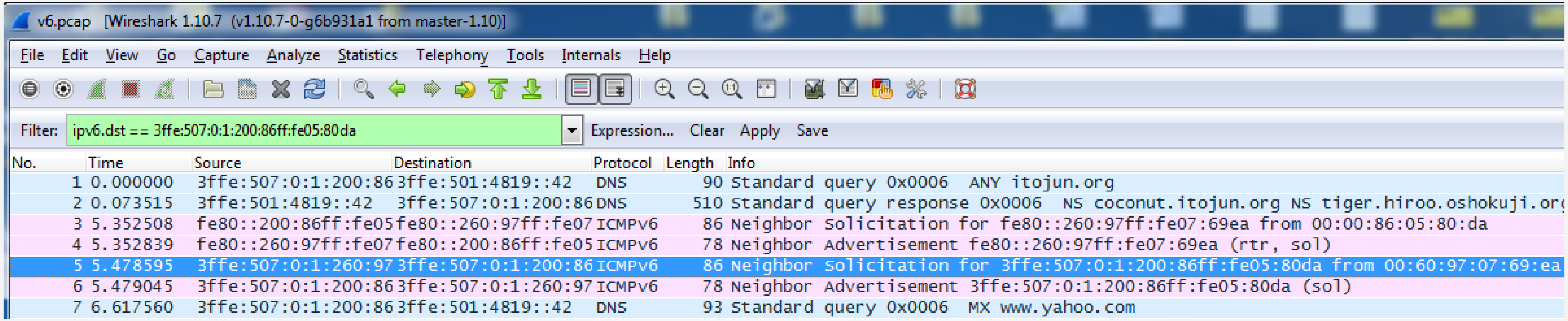
Setting Filters

Wireshark Filters

- What is a filter?
  - Used to limit what appears in the Packets List pane
- Wireshark filters are used to
  - Aid in troubleshooting efforts
  - Refine the view
  - Assist with collecting only what you need

Applying a Filter



Filter: ipv6.dst == 3ffe:507:0:1:200:86ff:fe05:80da

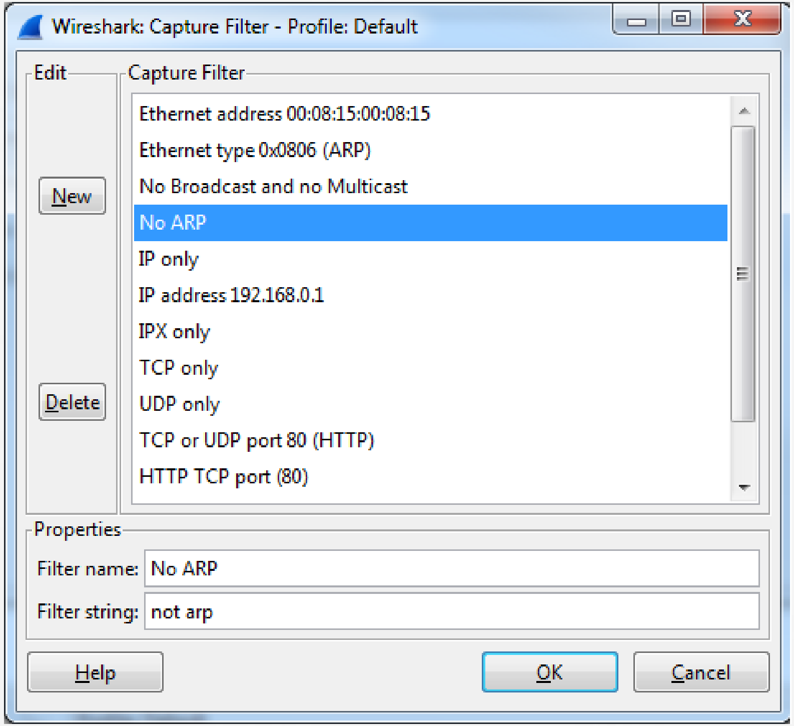
```
No.  Time      Source              Destination         Protocol Length Info
   1 0.000000  3ffe:507:0:1:200:86 3ffe:501:4819::42   DNS          90 Standard query 0x0006  ANY itojun.org
   2 0.073515  3ffe:501:4819::42   3ffe:507:0:1:200:86 DNS         510 Standard query response 0x0006  NS coconut.itojun.org NS tiger.hiroo.oshokuji.org
   3 5.352508  fe80::200:86ff:fe05 fe80::260:97ff:fe07 ICMPv6       86 Neighbor Solicitation for fe80::260:97ff:fe07:69ea from 00:00:86:05:80:da
   4 5.352839  fe80::260:97ff:fe07 fe80::200:86ff:fe05 ICMPv6       78 Neighbor Advertisement fe80::260:97ff:fe07:69ea (rtr, sol)
   5 5.478595  3ffe:507:0:1:260:97 3ffe:507:0:1:200:86 ICMPv6       86 Neighbor Solicitation for 3ffe:507:0:1:200:86ff:fe05:80da from 00:60:97:07:69:ea
   6 5.479045  3ffe:507:0:1:200:86 3ffe:507:0:1:260:97 ICMPv6       78 Neighbor Advertisement 3ffe:507:0:1:200:86ff:fe05:80da (sol)
   7 6.617560  3ffe:507:0:1:200:86 3ffe:501:4819::42   DNS          93 Standard query 0x0006  MX www.yahoo.com
```

Wireshark Filters

» Filter types

- Capture – Used to filter data before it is captured by Wireshark. For example, you could configure Wireshark to capture only data supplied by a specific IP address.
- Display – Used to filter data after it is captured. This will help you refine the display to show only what you need to see.

Configuring a Capture Filter



Wireshark: Capture Filter - Profile: Default

Edit

Capture Filter

- Ethernet address 00:08:15:00:08:15
- Ethernet type 0x0806 (ARP)
- No Broadcast and no Multicast
- No ARP
- IP only
- IP address 192.168.0.1
- IPX only
- TCP only
- UDP only
- TCP or UDP port 80 (HTTP)
- HTTP TCP port (80)

Properties

Filter name: No ARP

Filter string: not arp

Wireshark Filters

» Simple filter expression examples

- Capture traffic to or only from a specific IP address.

host 10.1.1.1

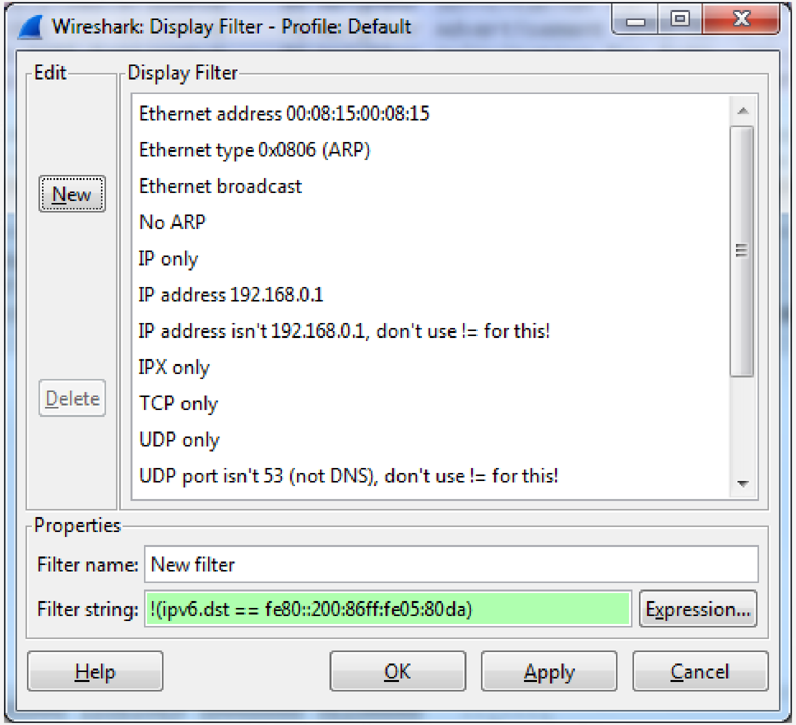
- Capture traffic to a range of IP addresses

net 10.1.1.0 mask 255.255.255.0

- Capture traffic on a specific port

port 8080

Display Filters



Wireshark: Display Filter - Profile: Default

Display Filter

- Ethernet address 00:08:15:00:08:15
- Ethernet type 0x0806 (ARP)
- Ethernet broadcast
- No ARP
- IP only
- IP address 192.168.0.1
- IP address isn't 192.168.0.1, don't use != for this!
- IPX only
- TCP only
- UDP only
- UDP port isn't 53 (not DNS), don't use != for this!

Properties

Filter name: New filter

Filter string: !(ipv6.dst == fe80::200:86ff:fe05:80da)

Wireshark Filters

» Troubleshooting with filters

- Streamline viewable traffic to find exactly what you need
- Remove anything that could cause confusion
- Give the analyst a clearer view of the root cause data

Questions?