

Advanced 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 only collecting only what you need



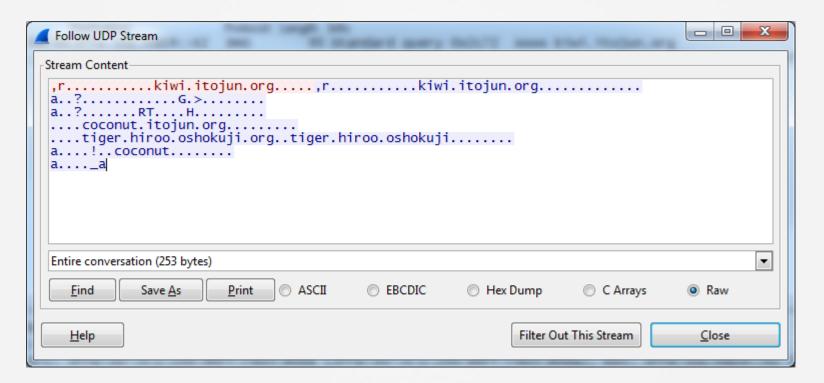
Wireshark Advanced Filters

» Filter types

- Capture and display
- Streams (TCP and UDP)
- Macros
- Conversation filters
- Others



Configuring an Advanced Filter





Configuring a Capture Filter

```
Follow TCP Stream
Stream Content
SSH-1.5-1.2.26
SSH-1.5-1.2.26
..i'=`.....J....m.z.....;/..u.q..p....2.fN...zl......{?E..h..|
%...|.!...z.e.;).....ob..|..!.r.#N1..s.
.....f.w..^ ".Y.....d
I..Nm. ._.y....$o.[..'..b.....
               +kkD.Gs.*.36...)q.....Z...:c.Q.f@>%r....'R...'...H..r.Y...]v.AN@.g.z.
+.8.4..s.y..`K...2...\"..}...W.Y...n1mya....4....G}..*d.o...f......
$..a@h....8.....&.m|I.P....;T...M.m.{..oh...N.._P5.5.O.L.F....w."<...,0
.v....@..5....>.V...mt.%
Entire conversation (4626 bytes)
                           ASCII
  Find
                                     EBCDIC
                                                 Hex Dump
                                                              C Arrays
           Save As
                     Print
                                                                          Raw
                                                      Filter Out This Stream
  Help
                                                                           Close
```



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?