????

????

?????

```
==
!=
>
<
>=
<=
in
```

?????

```
&&  # AND
||    # OR
!     # NOT
```

?????

- type: host, port
- dir: src, dst
- proto: tcp, udp, ftp, http

SIP ??

tcpdump

```
timeout 6m tcpdump -i eth0 host <sip-trunk-ip> -n -s 0 -vvvv  -w carrier.pcap
```

Wireshark

- ??? sip ??? filter ???https://www.wireshark.org/docs/dfref/s/sip.html

??? REGISTER ??Filter: `sip.CSeq.method == REGISTER`

??

??????

```
ssh root@192.168.0.1 tcpdump -n -i any -w- 'not \( port 22 and host 192.168.0.1 \)' |etherape -r-
```

Filter ???

Wireshark Display Filter Cheat Sheet

www.cellstream.com www.netscionline.com

Operators and Logic

eq or ==
ne or !=
gt or >

lt or <
ge or >=
le or <=

and or && Logical AND
or or || Logical OR
xor or ^^ Logical XOR

not or ! Logical NOT
[n] [ ] Substring operator

LAYER 1

frame
frame.cap_len
frame.coloring_rule.name
frame.coloring_rule.string
frame.file_off

frame.ignored
frame.len
frame.link_nr
frame.marked
frame.md5_hash

frame.number
frame.p2p_dir
frame.protocols
frame.ref_time
frame.time

frame.time_delta
frame.time_delta_displayed
frame.time_epoch
frame.time_invalid
frame.time_relative

LAYER 2

Ethernet

eth.addr
eth.dst
eth.ig
eth.len
eth.lg

eth.multicast
eth.src
eth.trailer
eth.type

ARP

arp.dst.hw_mac
arp.dst.proto_ipv4
arp.hw.size
arp.hw.type
arp.opcode

arp.proto.size
arp.proto.type
arp.src.hw_mac
arp.src.proto_ipv4

802.1Q VLAN

vlan.cfi
vlan.etype
vlan.id

vlan.len
vlan.priority
vlan.trailer

PPP

ppp.address
ppp.control

ppp.direction
ppp.protocol

VLAN Trunking Protocol

vtp.code
vtp.conf_rev_num
vtp.followers
vtp.md
vtp.md5_digest
vtp.md_len
vtp.neighbor
vtp.seq_num
vtp.start_value
vtp.upd_id
vtp.upd_ts

vtp.version
vtp.vlan_info.802_10_index
vtp.vlan_info.isl_vlan_id
vtp.vlan_info.len
vtp.vlan_info.mtu_size
vtp.vlan_info.status.vlan_susp
vtp.vlan_info.tlv_len
vtp.vlan_info.tlv_type
vtp.vlan_info.vlan_name
vtp.vlan_info.vlan_name_len
vtp.vlan_info.vlan_type

DTP

dtp.neighbor
dtp.tlv_len

dtp.tlv_type
dtp.version

MPLS

mpls.bottom
mpls.cw.control
mpls.cw.res
mpls.exp
mpls.label
mpla.aom.bip16

mpls.oam.defect_location
mpls.oam.defect_type
mpls.oam.frequency
mpls.oam.function_type
mpls.oam.ttsi
mpls.ttl

Frame Relay

fr.becn
fr.chdlctype
fr.control
fr.control_f
fr.control.ftype
fr.control.n_r
fr.control.n_s

fr.control.p
fr.control.s_ftype
fr.control.u_modifier_cmd
fr.control.u_modifier_resp
fr.cr
fr.dc
fr.de

fr.dlci
fr.dlcore_control
fr.ea
fr.fecn
fr.lower_dlci
fr.nlpid
fr.second_dlci

fr.snap.oui
fr.snap.pid
fr.snaptype
fr.third_dlci
fr.upper_dlci

LAYER 3

IP v4

ip.addr
ip.checksum
ip.checksum_bad
ip.checksum_good
ip.dsfield

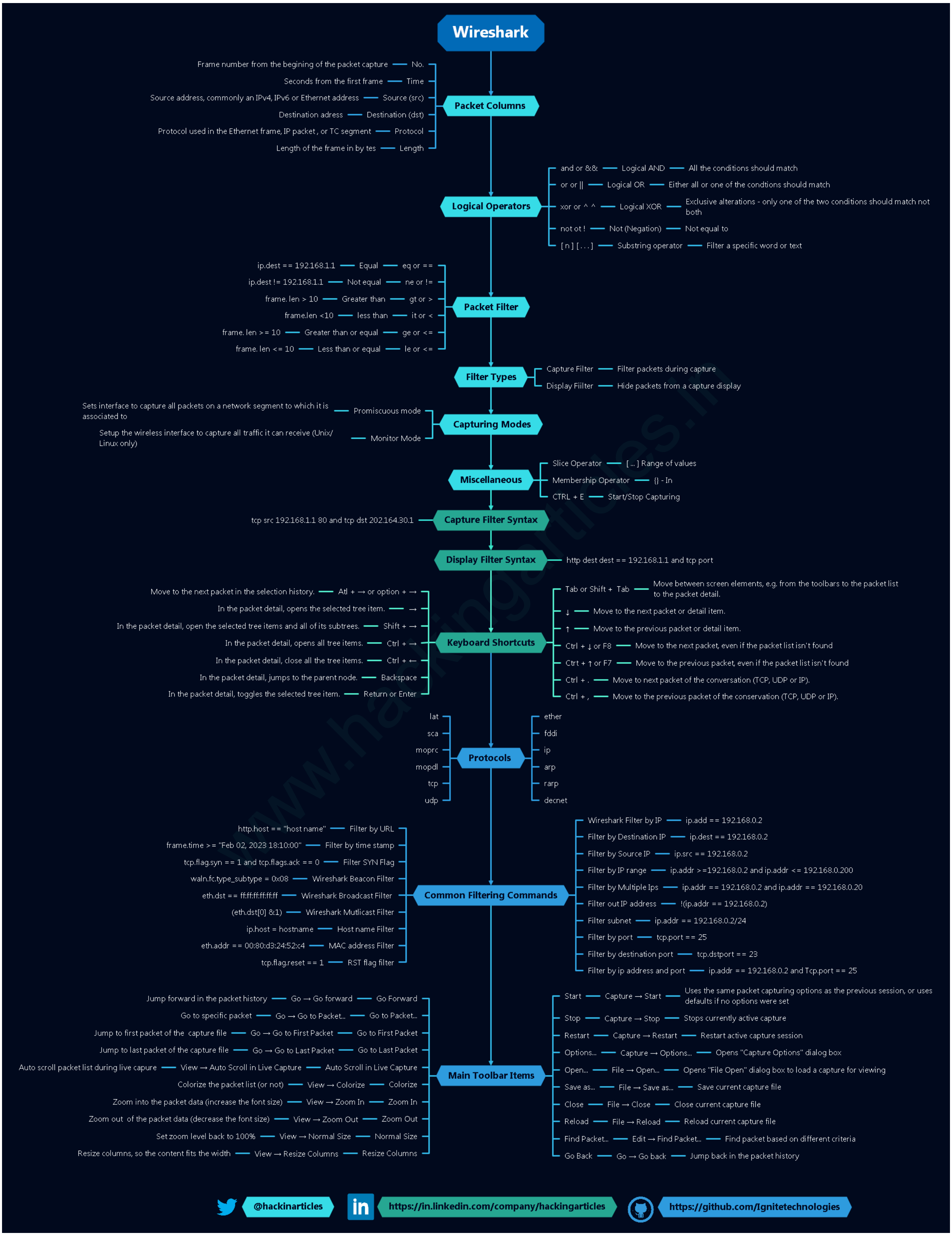
ip.fragment.overlap.conflict
ip.fragments
ip.fragment.toolongfragment
ip.hdr_len
ip.host

IP v6

ipv6.addr
ipv6.class
ipv6.dst
ipv6.dst_host
ipv6.dst_opt

ipv6.hop_opt
ipv6.host
ipv6.mipv6_home_address
ipv6.mipv6_length
ipv6.mipv6_type

(c)1998-2021 CellStream, Inc.



Wireshark

Packet Columns

- Frame number from the begining of the packet capture — No.
- Seconds from the first frame — Time
- Source address, commonly an IPv4, IPv6 or Ethernet address — Source (src)
- Destination adress — Destination (dst)
- Protocol used in the Ethernet frame, IP packet , or TC segment — Protocol
- Length of the frame in by tes — Length

Logical Operators

- and or && — Logical AND — All the conditions should match
- or or || — Logical OR — Either all or one of the condtions should match
- xor or ^ ^ — Logical XOR — Exclusive alterations - only one of the two conditions should match not both
- not ot ! — Not (Negation) — Not equal to
- [n] [. . .] — Substring operator — Filter a specific word or text

Packet Filter

- ip.dest == 192.168.1.1 — Equal — eq or ==
- ip.dest != 192.168.1.1 — Not equal — ne or !=
- frame. len > 10 — Greater than — gt or >
- frame.len <10 — less than — it or <
- frame. len >= 10 — Greater than or equal — ge or <=
- frame. len <= 10 — Less than or equal — le or <=

Filter Types

- Capture Filter — Filter packets during capture
- Display Fiilter — Hide packets from a capture display

Capturing Modes

- Sets interface to capture all packets on a network segment to which it is associated to — Promiscuous mode
- Setup the wireless interface to capture all traffic it can receive (Unix/ Linux only) — Monitor Mode

Miscellaneous

- Slice Operator — [...] Range of values
- Membership Operator — {} - In
- CTRL + E — Start/Stop Capturing

Capture Filter Syntax

- tcp src 192.168.1.1 80 and tcp dst 202.164.30.1

Display Filter Syntax

- http dest dest == 192.168.1.1 and tcp port

Keyboard Shortcuts

- Move to the next packet in the selection history. — Atl + → or option + →
- In the packet detail, opens the selected tree item. — →
- In the packet detail, open the selected tree items and all of its subtrees. — Shift + →
- In the packet detail, opens all tree items. — Ctrl + →
- In the packet detail, close all the tree items. — Ctrl + ←
- In the packet detail, jumps to the parent node. — Backspace
- In the packet detail, toggles the selected tree item. — Return or Enter
- Tab or Shift + Tab — Move between screen elements, e.g. from the toolbars to the packet list to the packet detail.
- ↓ — Move to the next packet or detail item.
- ↑ — Move to the previous packet or detail item.
- Ctrl + ↓ or F8 — Move to the next packet, even if the packet list isn't found
- Ctrt + ↑ or F7 — Move to the previous packet, even if the packet list isn't found
- Ctrl + . — Move to next packet of the conversation (TCP, UDP or IP).
- Ctrl + , — Move to the previous packet of the conservation (TCP, UDP or IP).

Protocols

- lat
- sca
- moprc
- mopdl
- tcp
- udp
- ether
- fddi
- ip
- arp
- rarp
- decnet

Common Filtering Commands

- http.host == "host name" — Filter by URL
- frame.time >= "Feb 02, 2023 18:10:00" — Filter by time stamp
- tcp.flag.syn == 1 and tcp.flags.ack == 0 — Filter SYN Flag
- waln.fc.type_subtype = 0x08 — Wireshark Beacon Filter
- eth.dst == ff:ff:ff:ff:ff:ff — Wireshark Broadcast Filter
- (eth.dst[0] &1) — Wireshark Mutlicast Filter
- ip.host = hostname — Host name Filter
- eth.addr == 00:80:d3:24:52:c4 — MAC address Filter
- tcp.flag.reset == 1 — RST flag filter
- Wireshark Filter by IP — ip.add == 192.168.0.2
- Filter by Destination IP — ip.dest == 192.168.0.2
- Filter by Source IP — ip.src == 192.168.0.2
- Filter by IP range — ip.addr >=192.168.0.2 and ip.addr <= 192.168.0.200
- Filter by Multiple Ips — ip.addr == 192.168.0.2 and ip.addr == 192.168.0.20
- Filter out IP address — !(ip.addr == 192.168.0.2)
- Filter subnet — ip.addr == 192.168.0.2/24
- Filter by port — tcp.port == 25
- Filter by destination port — tcp.dstport == 23
- Filter by ip address and port — ip.addr == 192.168.0.2 and Tcp.port == 25

Main Toolbar Items

- Jump forward in the packet history — Go → Go forward — Go Forward
- Go to specific packet — Go → Go to Packet... — Go to Packet...
- Jump to first packet of the capture file — Go → Go to First Packet — Go to First Packet
- Jump to last packet of the capture file — Go → Go to Last Packet — Go to Last Packet
- Auto scroll packet list during live capure — View → Auto Scroll in Live Capture — Auto Scroll in Live Capture
- Colorize the packet list (or not) — View → Colorize — Colorize
- Zoom into the packet data (increase the font size) — View → Zoom In — Zoom In
- Zoom out of the packet data (decrease the font size) — View → Zoom Out — Zoom Out
- Set zoom level back to 100% — View → Normal Size — Normal Size
- Resize columns, so the content fits the width — View → Resize Columns — Resize Columns
- Start — Capture → Start — Uses the same packet capturing options as the previous session, or uses defaults if no options were set
- Stop — Capture → Stop — Stops currently active capture
- Restart — Capture → Restart — Restart active capture session
- Options... — Capture → Options... — Opens "Capture Options" dialog box
- Open... — File → Open... — Opens "File Open" dialog box to load a capture for viewing
- Save as... — File → Save as... — Save current capture file
- Close — File → Close — Close current capture file
- Reload — File → Reload — Reload current capture file
- Find Packet... — Edit → Find Packet... — Find packet based on different criteria
- Go Back — Go → Go back — Jump back in the packet history

@hackinarticles

https://in.linkedin.com/company/hackingarticles

https://github.com/Ignitetechnologies

www.hackingarticles.in

Revision #10
Created 28 May 2022 13:15:18 by Admin
Updated 15 September 2023 13:10:28 by Admin