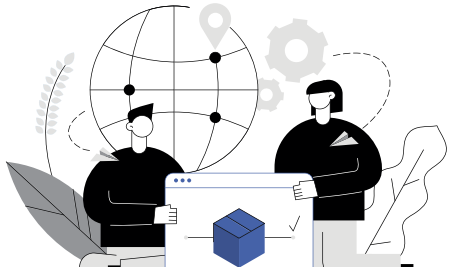
Basque CyberSecurity Centre



Wireshark cheat sheet

Sareko protokoloak aztertzeko doako tresna. Ekipo batean sartzen eta irteten den guztia xehetasunez aztertzeko aukera ematen du.

1. Wiresharkeko bistaratze-iragazkiak

- Wiresharken atzipenak egiteko moduak

a. Modu nahasia

Lotutako sare-segmentu batean pakete guztiak atzitzeko interfazea ezartzen du.

b. Monitore-modua

Haririk gabeko interfazea konfiguratzen du, jaso dezakeen trafiko guztia (Unix/Linux soilik) atzitzeko.

- Iragazki-motak

a. Atzipen-iragazkia

Atzipenean paketeak iragazten ditu.

b. Bistaratze-iragazkia

Atzipen-pantaila bateko paketeak ezkutatzen ditu.

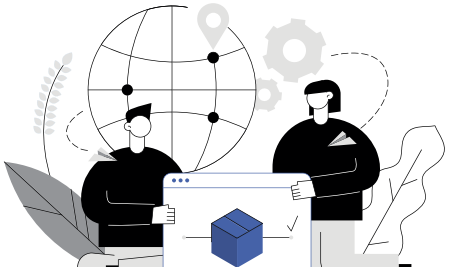
- Atzipen-iragazkiaren sintaxia

Adibidea	Protokoloa	Helbidea	Ostalariak	Balioa	Eragile logikoa	Adierazpena
204.163.20.3	tcp	src	192.168.1.1	80	and	tcp dst

- Bistaratze-iragazkiaren sintaxia

Sintaxia	Protokoloa	1. katea	2. katea	Eragilearen konparazioa	Eragile logikoa	Adierazpena
[redacted]	http	dest	ip	==	and	tcp port

Basque CyberSecurity Centre



2. Protokoloak - Balioak

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

3. Paketeen iragazpena (bistaratze-iragazkiak)

Eragilea	Azalpena	Adibidea
eq o ==	Berdina da	ip.dest == 192.168.1.1
ne o !=	Ez da berdina	ip.dest != 192.168.1.1
gt o >	Baino handiagoa da	frame.len > 10
lt o <	Baino txikiagoa da	frame.len <10
ge o >=	Baino handiagoa edo berdina da	frame.len >= 10
le o <=	Baino txikiagoa edo berdina da	frame.len <= 10

4. Miszelanea

- **Slice eragilea**
  [...] - Balioen barrutia

  Adibidea:
  eth.src[1-2] == 00:83
- **Kidetasun-eragilea**
  {} - Lekua

  Adibidea:
  tcp.port in {80, 443, 8080}
- **Atzipena hastea/gelditzea**
  CTRL+E

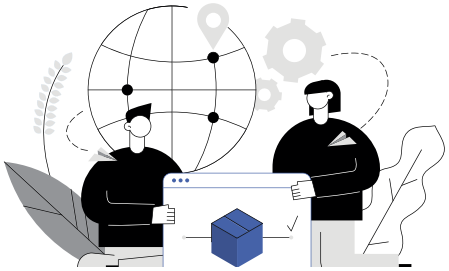
5. Eragile logikoak

Eragilea	Azalpena	Adibidea
And o &&	And lodikoa	Se deben cumplir todas las condiciones
Or o ||	Or logikoa	Una o todas las condiciones se deben cumplir
Xor o ^^	Xor logikoa	Sólo una de las condiciones se debe cumplir
Not o !	Ukapena	No es igual a
[n] [...]	Azpikate-eragilea	Filtrar una palabra o texto específico

6. Aurrez zehaztutako zutabeak pakete-atzipenaren irteera batean

- **No**
  Bilbe-zenbakia, pakete-atzipenaren hasieratik zenbatzen hasita
- **Time**
  Lehen fotogramatik igarotako segundoak
- **Source (src)**
  Jatorriko helbidea; eskuarki IPv4, IPv6 edo Ethernet helbide bat
- **Destination (dst)**
  Xede-helbidea
- **Protocol**
  Etherneteko bilbean, IP paketean edo TCP segmentuan erabilitako protokoloa
- **Length**
  Bilbearen luzera bytetan

Basque CyberSecurity Centre



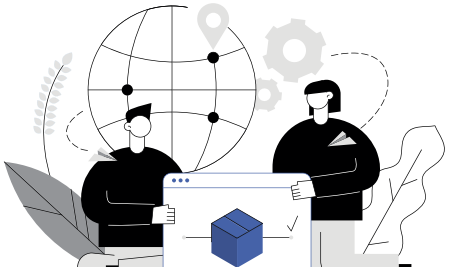
7. Teklatuko metodo laburtuak: leiho nagusia

- **Zuriunea edo Shift+Zuriunea**
  Pantailako elementuen artean mugitzea, adibidez, tresna-barratik pakete-zerrendara eta paketearen xehetasunera.
- **Alt+→ edo Option+→**
  Hautaketa-historiako hurrengo paketera joatea.
- **↓**
  Hurrengo paketera edo xehetasun-elementura joatea.
- **→**
  Paketearen xehetasunean, hautatutako zuhaitz-elementua irekitzea.
- **↑**
  Aurreko paketera edo xehetasun-elementura joatea.
- **Shift+→**
  Paketearen xehetasunean, hautatutako zuhaitz-elementua eta haren azpizuhaitz guztiak irekitzea.
- **Ctrl+↓ edo F8**
  Hurrengo paketera joatea, baita paketeen zerrenda bideratuta ez badago ere.
- **Ctrl+→**
  Paketearen xehetasunean, zuhaitzaren elementu guztiak irekitzea.
- **Ctrl+↑ edo F7**
  Aurreko paketera joatea, baita paketeen zerrenda bideratuta ez badago ere.
- **Ctrl+←**
  Paketearen xehetasunean, zuhaitzaren elementu guztiak ixtea.
- **Ctrl+**
  Elkarrizketaren hurrengo paketera joatea (TCP, UDP edo IP).
- **Backspace (atzera-tekla)**
  Paketearen xehetasunean, lehen nodora jauzi egitea.
- **Ctrl+,**
  Elkarrizketaren aurreko paketera joatea (TCP, UDP edo IP).
- **Itzuli tekla**
  Paketearen xehetasunean, hautatutako zuhaitz-elementua txandakatzea.

8. Ohiko iragazpen-komandoak

- **IP bidezko Wireshark iragazkia**
  ip.addr == 10.20.70.1
- **Helmugako IParen arabera iragaztea**
  ip.dest == 10.20.70.1
- **Jatorrizko IParen arabera iragaztea**
  ip.src == 10.20.70.1
- **IParen barrutiaren arabera iragaztea**
  ip.addr >= 10.20.70.1 and ip.addr <= 10.20.70.100
- **Hainbat IPren arabera iragaztea**
  ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100
- **IP helbidea iragaztea/baztertzea**
  !(ip.addr == 10.20.100.1)
- **IP azpisarea iragaztea**
  ip.addr == 10.10.50.1/24
- **Zehaztutako zenbait IP azpisarreren arabera iragaztea**
  ip.addr == 10.10.50.1/24 and ip.addr == 10.10.51.1/24
- **Protokoloaren arabera iragaztea**
  Dns, http,ftp, ssh, arp, telnet, icmp
- **Atakaren arabera iragaztea (TCP)**
  tcp.port == 25
- **Helmugako atakaren arabera iragaztea (TCP)**
  tcp.dstport == 23
- **IP helbidearen eta atakaren arabera iragaztea**
  ip.addr == 10.200.80.1 and Tcp.port == 25
- **URLaren arabera iragaztea**
  http.host == "host name"
- **Timestamp-aren arabera iragaztea**
  frame.time >= "June 02, 2019 18:04:00"
- **SYN flag iragazkia**
  tcp.flags.syn == 1
  tcp.flags.syn == 1 and tcp.flags.ack == 0
- **Wireshark Beacon iragazkia**
  wlan.fc.type_subtype = 0x08
- **Broadcast Wireshark iragazkia**
  eth.dst == ff:ff:ff:ff:ff:ff
- **Multicast iragazkia**
  (eth.dst[0] & 1)
- **Ostalariaren izenaren iragazkia**
  ip.host = hostname
- **MAC helbideen iragazkia**
  eth.addr == 00:70:f4:23:18:c4
- **RST adierazlearen iragazkia**
  tcp.flags.reset == 1

Basque CyberSecurity Centre



9. Tresna-barraren elementu nagusiak

Tresna-barraren ikonoa	Tresna-barraren elementua	Menuko elementua	Azalpena
	Hasi	Capture → Start	Aurreko saioan paketeak atzitzeko erabilitako aukera berak erabiltzen ditu, edo aurrez zehaztutako balioak erabiltzen ditu aukerarik ezarri ez bada
	Gelditu	Capture → Stop	Uneko atzipena geldiarazten du
	Berrekin	Capture → Restart	Uneko atzipen-saioa hasten du berriro
	Aukerak...	Capture → Options...	«Atzipen-aukerak» elkarrizketa-koadroa irekitzen du
	Ireki...	File → Open...	«Fitxategi irekia» elkarrizketa-koadroa irekitzen du, atzipen bat kargatu eta bistaratzeko
	Gorde honela...	File → Save As...	Uneko atzipen-fitxategia gordetzen du
	Itxi	File → Close	Uneko atzipen-fitxategia ixten du
	Birkargatu	View → Reload	Uneko atzipen-fitxategia birkargatzen du
	Bilatu paketea...	Edit → Find Packet...	Paketeak zenbait irizpideren arabera bilatzen ditu
	Itzuli	Go → Go Back	Paketeen historiara itzultzen du
	Aurreratu	Go → Go Forward	Paketeen historian aurrera egiten du
	Joan paketera...	Go → Go to Packet...	Pakete espezifiko batera eramaten du
	Joan lehen paketera	Goe → First Packet	Atzipen-fitxategiko lehen paketera eramaten du
	Joan azken paketera	Go → Last Packet	Atzipen-fitxategiko azken paketera eramaten du
	Desplazamendu automatikoa Live Capture-n	View → Auto Scroll in Live Capture	Desplazamendu automatikoko paketeen zerrenda, zuzeneko atzipenean zehar
	Margotu	View → Colorize	Pakete-zerrenda margotzen du (edo ez)
	Hurbildu	View → Zoom In	Paketearen datuak zabaltzen ditu (letra-tamaina handitzen du)
	Urrundu	View → Zoom Out	Paketearen datuak urruntzen ditu (letra-tamaina txikitzen du)
	Tamaina normala	View → Normal Size	% 100eko zoom-maila ezartzen du berriz
	Aldatu zutabeen tamaina	View → Resize Columns	Zutabeen tamaina aldatzen du, edukia zabalerara egokitzeko