# Wireshark

أداة الـWireshark هي أداة مفتوحة المصدر لتحليل حركة البيانات والشبكات، وتعتبر واحدة من أشهر الأدوات في مجال الشبكات، خاصة في اختبارات الاختراق وتحليل الأمان. بتسمح لك الأداة بمراقبة وتحليل البيانات المتنقلة عبر الشبكة بشكل تفصيلي

في Wireshark، تقدر تشوف حزم البيانات (packets) التي بتتحرك بين الأجهزة على الشبكة، وتستطيع تحليل هذه الحزم لفهم طبيعة البيانات المتنقلة، مثل البروتوكولات المستخدمة، عناوين الـ IP، وأماكن حدوث الاتصال

# Wireshark Filter Commands

## Filter by Protocol:

- `http` : To display only HTTP packets.
- `tcp` : To display only TCP packets.
- `udp` : To display only UDP packets.
- `dns` : To display only DNS packets.
- `smb || nbns || dcerpc || nbss || dns` : To display packets for any of these protocols.

## Filter by IP Address:

- `ip.src == 192.168.0.0/16 or ip.dst == 192.158.0.0/16` : To display packets with source or destination in this range.
- `ip.addr == 10.43.54.65` : To display packets related to this specific IP.
- `ip.addr != 10.43.54.65` : To display all packets except those related to this IP.
- `ip.src != 10.43.54.65 or ip.dst != 10.43.54.65` : To exclude packets with this IP as source or destination.

- `!(ip.addr == 10.43.54.65)` : To exclude packets related to this IP.
- `!(ip.src == 10.43.54.65 or ip.dst == 10.43.54.65)` : To exclude packets with this IP as source or destination.

## Filter by Port:

- `tcp.port eq 25 or icmp` : To display packets using port 25 or ICMP protocol.
- `tcp.port in {80,443,8080}` : To display packets using any of the ports 80, 443, or 8080.
- `tcp.srcport == 443` : To display packets originating from port 443.
- `udp.port == 53` : To display packets using port 53 (DNS).

## Filter by Text within Packets:

- `tcp.payload contains "GET"` : To display packets containing the text "GET".
- `tcp.payload contains "pass"` : To display packets containing the text "pass".
- `http contains "https://www.wireshark.org"` : To display packets containing this URL.
- `frame contains "password"` : To display packets containing the text "password".

## Filter HTTP:

- `http.request.method == "POST"` : To display requests using the POST method.
- `http.request.method in {"HEAD", "GET"}` : To display requests using the HEAD or GET methods.

## Filter by Range:

- `ip.addr in {10.0.0.5 .. 10.0.0.9, 192.168.1.1 .. 192.168.1.9}` : To display packets within this range of addresses.

## Filter by Destination:

- `ip.dst ne 224.1.2.3` : To display packets not destined for this address.
- `not ip.dst or ip.dst ne 224.1.2.3` : To display packets with no specific destination or not destined for this address.
- `ip.dst and ip.dst ne 224.1.2.3` : To display packets with a destination that is not this address.

## Filter Lost Packets or Errors:

- `tcp.analysis.retransmission` : To display retransmitted packets.
- `tcp.analysis.flags` : To display packets with flags or issues.

## Filter by Header or User Agent:

- `wsp.header.user_agent matches "cldc"` : To display packets with this text in the User-Agent.

## Filter by Time:

- `frame.time >= "2025-01-16 14:00:00" && frame.time <= "2025-01-16 15:00:00"` : To display packets captured within a specific time range.

## Filter by Time and HTTP:

- `http.request.method == "POST" && frame.time >= "2025-01-16 14:00:00"` : To display packets containing a POST request at a specific time.

## Symbol Explanation:

- `eq` : equal.
- `ne` : not equal.
- `in` : specify a value within a set or range.
- `contains` : search for text within packets.