

# Common Display **Filter** commands

Here are **useful Wireshark display filters** (not capture filters) for **SOC (Security Operations Center)** use cases — short and focused:

## Basic Suspicious Traffic

Purpose	Display Filter
Only HTTP	<code>http</code>
Only DNS	<code>dns</code>
Only TLS (SSL)	<code>tls</code> or <code>ssl</code>
TCP to/from IP	<code>ip.addr == 10.0.0.5 and tcp</code>
Suspicious port (e.g. 4444)	<code>tcp.port == 4444</code>
TCP retransmissions	<code>tcp.analysis.retransmission</code>
Show only GET/POST	<code>http.request.method == "GET"</code>
Large HTTP responses	<code>http.content_length &gt; 100000</code>
<b>Prepare auto commands</b>	Just click specific packet and choose apply filter and auto filter

## C2 / Malware Beaconing Indicators

Purpose	Display Filter
Same interval DNS queries	<code>dns.qry.name == "example.com"</code> + time graph
Long-lived TCP	<code>tcp.analysis.flags &amp;&amp; frame.time_delta &gt; 10</code>
Rare User-Agent	<code>http.user_agent contains "TeslaBrowser"</code>

## Credential / Leak Detection

Purpose	Display Filter
POST with data	<code>http.request.method == "POST"</code>
FTP clear-text	<code>ftp &amp;&amp; ftp.request.command == "USER"</code>
Email sniff (SMTP)	<code>smtp</code> or <code>tcp.port == 25</code>
Possible base64	<code>data-text-lines contains "Authorization: Basic"</code>


## SSL/TLS Analysis



Purpose	Display Filter
TLS handshake only	<code>tls.handshake</code>
Self-signed certs	<code>x509sat.printableString</code>
JA3 fingerprinting	Use plugin or: <code>frame contains "ja3"</code>

## Payload or Specific Strings

Purpose	Display Filter
Contains "powershell"	<code>frame contains "powershell"</code>
Contains <code>.exe</code>	<code>frame contains ".exe"</code>
Contains known IOC domain	<code>frame contains "malicious.com"</code>

## Important Display filter rules commands often:

 Purpose	Display Filter
All HTTP requests	<code>http.request</code>
Only POST requests	<code>http.request.method == "POST"</code>
Only GET requests	<code>http.request.method == "GET"</code>
URI contains suspicious file	<code>http.request.uri contains "audiodg.exe"</code>
DNS query to specific domain	<code>dns.qry.name == "example.com"</code>
HTTP/Traffic on port 80	<code>tcp.port == 80</code>

IP address match (internal or external)	<code>ip.addr == 192.168.0.1</code>
HTTP payload contains login keyword	<code>http contains "login"</code>
HTTP payload contains audiodg.exe	 <code>http contains "audiodg.exe"</code>  (  Correct & Important)


Prepare auto commands refer notion note ( Selected filter , Apply Filter )

Logic Operators ( AND OR NOT )

Mathematics Operators ( < , > , == , != , < = , > = )



### Notes:

-  All filters are valid in **Wireshark Display Filter** format.
- You can **right-click a packet** → **Apply as Filter** → **Selected** to auto-apply.
- Make sure quotes are **straight ASCII**: `"audiodg.exe"` not `"audiodg.exe"`