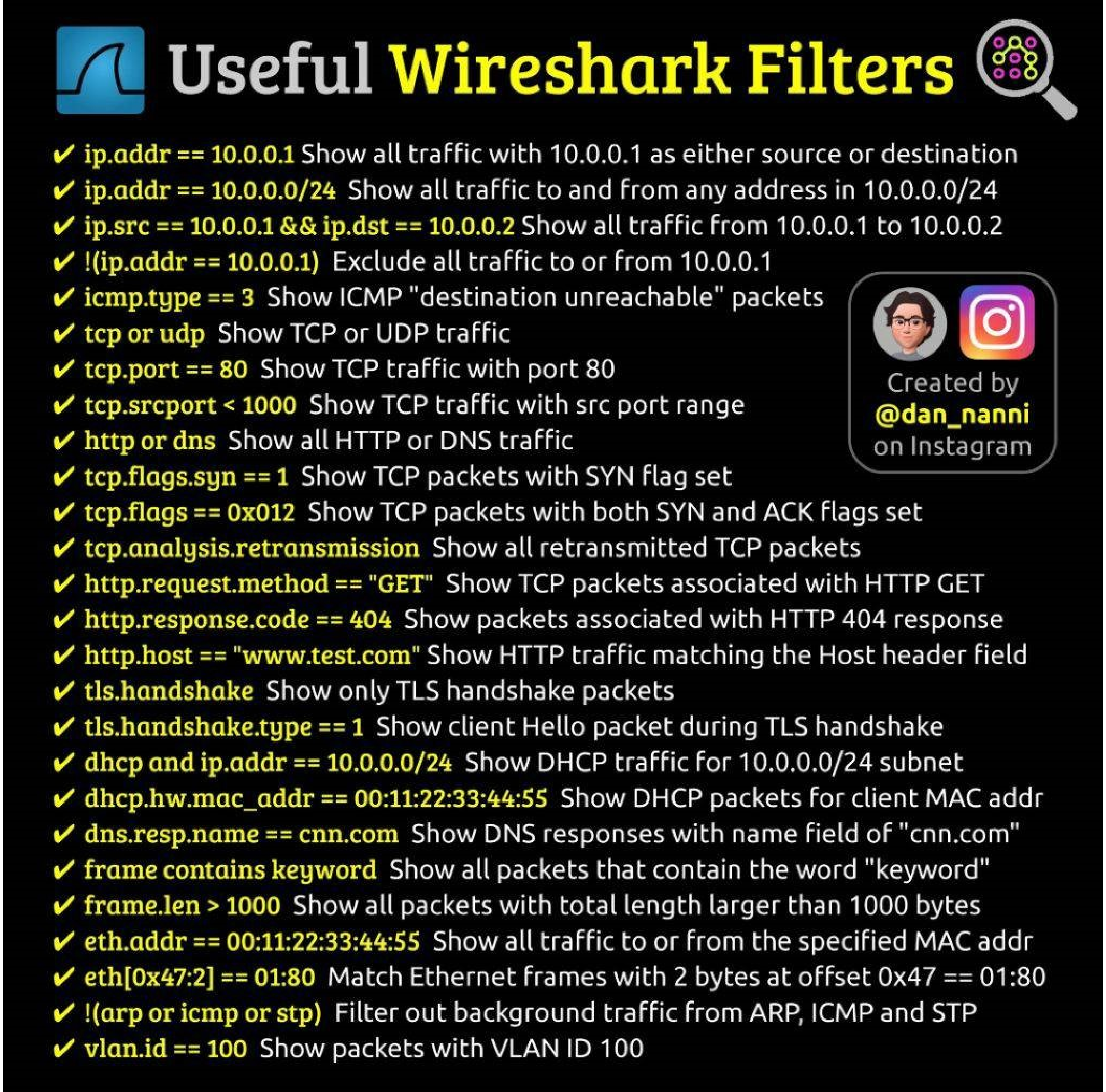

Useful Wireshark Filters

✔ ip.addr == 10.0.0.1 Show all traffic with 10.0.0.1 as either source or destination

✔ ip.addr == 10.0.0.0/24 Show all traffic to and from any address in 10.0.0.0/24

✔ ip.src == 10.0.0.1 && ip.dst == 10.0.0.2 Show all traffic from 10.0.0.1 to 10.0.0.2

✔ !(ip.addr == 10.0.0.1) Exclude all traffic to or from 10.0.0.1

✔ icmp.type == 3 Show ICMP "destination unreachable" packets

✔ tcp or udp Show TCP or UDP traffic

✔ tcp.port == 80 Show TCP traffic with port 80

✔ tcp.srcport < 1000 Show TCP traffic with src port range

✔ http or dns Show all HTTP or DNS traffic

✔ tcp.flags.syn == 1 Show TCP packets with SYN flag set

✔ tcp.flags == 0x012 Show TCP packets with both SYN and ACK flags set

✔ tcp.analysis.retransmission Show all retransmitted TCP packets

✔ http.request.method == "GET" Show TCP packets associated with HTTP GET

✔ http.response.code == 404 Show packets associated with HTTP 404 response

✔ http.host == "www.test.com" Show HTTP traffic matching the Host header field

✔ tls.handshake Show only TLS handshake packets

✔ tls.handshake.type == 1 Show client Hello packet during TLS handshake

✔ dhcp and ip.addr == 10.0.0.0/24 Show DHCP traffic for 10.0.0.0/24 subnet

✔ dhcp.hw.mac_addr == 00:11:22:33:44:55 Show DHCP packets for client MAC addr

✔ dns.resp.name == cnn.com Show DNS responses with name field of "cnn.com"

✔ frame contains keyword Show all packets that contain the word "keyword"

✔ frame.len > 1000 Show all packets with total length larger than 1000 bytes

✔ eth.addr == 00:11:22:33:44:55 Show all traffic to or from the specified MAC addr

✔ eth[0x47:2] == 01:80 Match Ethernet frames with 2 bytes at offset 0x47 == 01:80

✔ !(arp or icmp or stp) Filter out background traffic from ARP, ICMP and STP

✔ vlan.id == 100 Show packets with VLAN ID 100

Created by
@dan_nanni
on Instagram