Wireshark Analysis Quick Reference Guide

For Ethical Hackers

Essential Filters

Basic Filtering

```
ip.addr == 192.168.1.1      # Specific IP
tcp.port == 80              # HTTP traffic
dns                         # DNS queries
http                        # HTTP only
tcp.flags.syn == 1          # SYN packets
```

Attack Detection

```
tcp.flags.syn == 1 and tcp.flags.ack == 0   # SYN flood
arp.duplicate-address-detected              # ARP spoofing
dns and frame.len > 512                     # DNS tunneling
http.request.method == POST                 # Form submissions
```

Common Attack Patterns

SYN Flood: High volume SYN packets without ACK responses **DNS Spoofing:** Multiple IP responses for same domain **ARP Spoofing:** Same IP claimed by different MAC addresses **DNS Tunneling:** Unusually large DNS packets **MITM:** HTTP traffic that should be HTTPS

Quick Investigation Steps

1. **Overview:** Statistics > Protocol Hierarchy
2. **Top Talkers:** Statistics > Conversations
3. **Suspicious Traffic:** Use attack detection filters
4. **Follow Stream:** Right-click > Follow > TCP Stream

Integration Commands

With nmap:

```bash
nmap -sS 192.168.1.0/24
# Then filter: tcp.flags.syn == 1
```

With tcpdump:

```bash
sudo tcpdump -w capture.pcap -i eth0
# Open in Wireshark: File > Open
```

Incident Response

Immediate Actions:

1. Start capture immediately
2. Apply relevant filters
3. Export evidence: File > Export Objects
4. Document timestamps and patterns

Key Evidence Filters:

```
tcp.stream eq X          # Follow connection
frame.time >= "2024-01-01"    # Time filtering
ip.addr == <suspicious_ip>    # Focus on host
```