Investigate Packet Details with Wireshark - Summary

# 1. IP Headers – IPv4 vs IPv6

- IPv4 Header (13 fields): Includes fields like Version, IHL, ToS, TTL, Protocol, Source/Destination Address, etc.  
- IPv6 Header (8 fields): Includes Version, Traffic Class, Flow Label, Payload Length, Hop Limit, Source/Destination Address, etc.  
- These headers are critical for investigations and can be viewed in tools like Wireshark.

# 2. What is Wireshark?

Wireshark is an open-source network protocol analyzer with a GUI.  
It is used to inspect packet captures (pcaps) for suspicious or unusual activity.  
It allows display filtering to isolate relevant packets from large datasets.

# 3. Using Wireshark Filters

Comparison Operators:  
- Equal: == or eq  
- Not Equal: != or ne  
- Greater Than: > or gt  
- Less Than: < or lt  
- Greater Than or Equal: >= or ge  
- Less Than or Equal: <= or le  
  
Boolean Logic Support:  
- Combine filters using 'and', 'or', and parentheses () for complex queries.

# 4. Filter Examples

- All DNS packets: dns  
- Source IP 10.10.10.10: ip.src == 10.10.10.10  
- Destination IP 4.4.4.4: ip.dst == 4.4.4.4  
- Any match for IP 172.21.224.2: ip.addr == 172.21.224.2  
- MAC address: eth.addr == 00:70:f4:23:18:c4  
- UDP port 53 (DNS): udp.port == 53  
- TCP port 25 (SMTP): tcp.port == 25  
- Text in payload (contains): http contains "moved"  
- Regex match (matches): http matches "regex"

# 5. Follow Streams

Stream (or conversation): Series of packets exchanged using a protocol.  
Use “Follow Stream” in Wireshark to view the entire conversation (e.g., HTTP request & response).  
Helpful in understanding context, not just individual packets.

# Key Takeaways

- Packet headers (IPv4/IPv6) are crucial in detecting issues and tracing behavior.  
- Wireshark provides powerful filtering and stream analysis tools to inspect traffic efficiently.  
- Mastering display filters allows for focused investigations of suspicious network activity.