Wireshark Final Exam – Suggested Question Types

DNS-Based Questions

1. **What is the packet number of the DNS query for domain `example.com`? Is it UDP or TCP?**
2. **What is the IP address of the DNS server used in this trace?**
3. **How many questions and answers are in the DNS query/response?**
4. **Is the DNS response authoritative or non-authoritative?**
5. **What is the resolved IP address of `example.edu` from the DNS response?**
6. **What type of DNS record is being queried (e.g., A, AAAA, NS)?**
7. **How many additional records are included in the response? What are they?**
8. **What is the source and destination port of the DNS query and response?**

HTTP-Based Questions

1. **What is the packet number of the HTTP GET request for `index.html`?**
2. **What HTTP version is the browser using?**
3. **What is the status code returned by the server?**
4. **How many bytes of content are returned in the response?**
5. **What is the `Content-Type` of the returned file?**
6. **What is the `User-Agent` string sent by the client?**
7. **Was the requested object found in cache or newly fetched? How can you tell?**
8. **What is the packet number of the GET request for an image (e.g., `logo.jpg`) embedded in the page?**
9. **Does the HTTP response contain authentication headers (e.g., `WWW-Authenticate` or `Authorization`)?**

TCP-Based Questions

1. **What is the 3-way handshake sequence between the client and server? (List packet numbers)**
2. **What are the source and destination ports for the connection?**
3. **What is the sequence number and ACK number in a given TCP segment?**
4. **Is there packet loss or retransmission in the TCP stream? How can you tell?**
5. **What is the window size advertised by the receiver?**
6. **Is TCP segmentation used in this capture? How many segments?**
7. **Are TCP keep-alives or FIN flags used to close the session? Show packet numbers.**

🔹 General Protocol Analysis

1. **What protocols are used in the first 10 packets?**
2. **What is the IP address of the client and the server?**
3. **What is the MAC address of the sender in packet X?**
4. **What is the highest layer protocol present in packet Y?**
5. **Does the trace include IPv6 traffic? If so, what's the IPv6 source address?**

🔹 Reverse Engineering Questions

These are more analytical and might appear in finals:

1. **Identify the full DNS resolution path for a website (e.g., query → response → HTTP GET).**
2. **Compare the packet number of the DNS resolution and the actual HTTP request — was caching used?**
3. **From the captured trace, reconstruct the full URL of a web request.**
4. **Determine whether a site uses HTTPS or HTTP and justify from packet data.**
5. **List all domains resolved in this capture.**

🔹 Specialized / Advanced

1. **Did the HTTP request use persistent (keep-alive) connection?**
2. **How many parallel HTTP connections were made?**
3. **Does the DNS trace involve a recursive or iterative query pattern? How can you tell?**
4. **Are any security-related headers (e.g., `Set-Cookie`, `Authorization`) present in HTTP traffic?**

🧠 Pro Tip for Exam:

If you're given a `.pcap` file:

- Use **filters like** `http`, `dns`, `tcp.port==53`, `ip.addr == x.x.x.x`
- Always note **packet numbers, source/destination IPs, and ports**
- Use **Follow > TCP stream** or **Follow > HTTP stream** to simplify analysis

Where to Find Answers in Wireshark

🔹 DNS Questions

Question	Where to Look in Wireshark
DNS query packet number	Use filter: `dns` → Look for `Standard query A` line in **Info** column
DNS server IP	Expand the DNS packet → look at `Destination IP` or `Address` field
Questions/Answers count	Expand `Domain Name System (response)` → See "Questions", "Answer RRs"
Authoritative?	Check "Authoritative Answer" flag under DNS flags
Resolved IP address	In DNS response → Under "Answers" → look for `A` record
Record type (A, AAAA, NS)	In "Queries" section of DNS → See "Type: A" or "Type: NS"
Additional records	In DNS response → “Additional records” section lists glue records
Source/destination port	Expand UDP layer → Source Port / Destination Port

---

🔹 HTTP Questions

Question	Where to Look
HTTP GET packet number	Filter: `http.request` → Look for `GET` in Info column
HTTP version	Expand HTTP layer → check Request/Response Line: `GET / HTTP/1.1`
Status code	Expand HTTP response packet → see: `HTTP/1.1 200 OK`
Bytes of content	Check `Content-Length:` in response headers
Content-Type	Look for `Content-Type:` in the response headers
User-Agent	In HTTP GET request → expand headers, find `User-Agent: Chrome/...`
Cache behavior	Check for headers like `If-Modified-Since`, `304 Not Modified`
Image GET packet	Filter: `http.request` → Look for filename like `logo.jpg`
Authentication headers	Look for `WWW-Authenticate` (in response) or `Authorization` (in request)

🔹 TCP Questions

Question	Where to Look
3-way handshake	Filter: `tcp.flags.syn == 1` → Find SYN, SYN-ACK, ACK packets
Ports	Expand TCP layer → see "Source Port" and "Destination Port"
SEQ/ACK numbers	In TCP layer → Sequence number and Acknowledgment number
Packet loss or retransmission	Look for `TCP Retransmission` or `Dup ACK` in Info column
Window size	Expand TCP layer → see "Window size value"
Segmentation	Info column might say `TCP segment of a reassembled PDU`
FIN or RST close	Look for TCP flags: `FIN`, `RST` → usually at end of stream

---

🔹 General Protocol Analysis

Question	Where to Look
All protocols used	Use column "Protocol" in Wireshark's top pane
Client/server IP	Use `ip.src`, `ip.dst`, or full connection overview
MAC address	Expand Ethernet II section for source/destination MAC
Highest-layer protocol	Look in Protocol column → e.g., `HTTP`, `DNS`, `TCP`
IPv6 presence	Filter: `ipv6` or check Protocol column for IPv6 packets

---

🔹 Reverse Engineering & Advanced

Question	Where to Look
DNS + HTTP sequence	Use filter `dns
DNS caching	No second DNS query for the same domain indicates caching
Full requested URL	In HTTP GET packet → line will show: `GET /path/file.html HTTP/1.1` with `Host:` header
HTTPS vs HTTP	HTTPS uses `TLS` (look for `Client Hello`) on port 443, HTTP uses port 80
All resolved domains	Filter: `dns` → look for "Standard query A" → list domain names

---

🧪 Tools & Filters to Use:

- `dns` → Only DNS packets
- `http` → Only HTTP
- `tcp.port == 53` → DNS over TCP
- `ip.addr == your_ip` → Packets involving your machine

- `http.request` → HTTP GET/POST
- `http.response` → HTTP responses
- `tcp.flags.syn == 1` → TCP handshakes