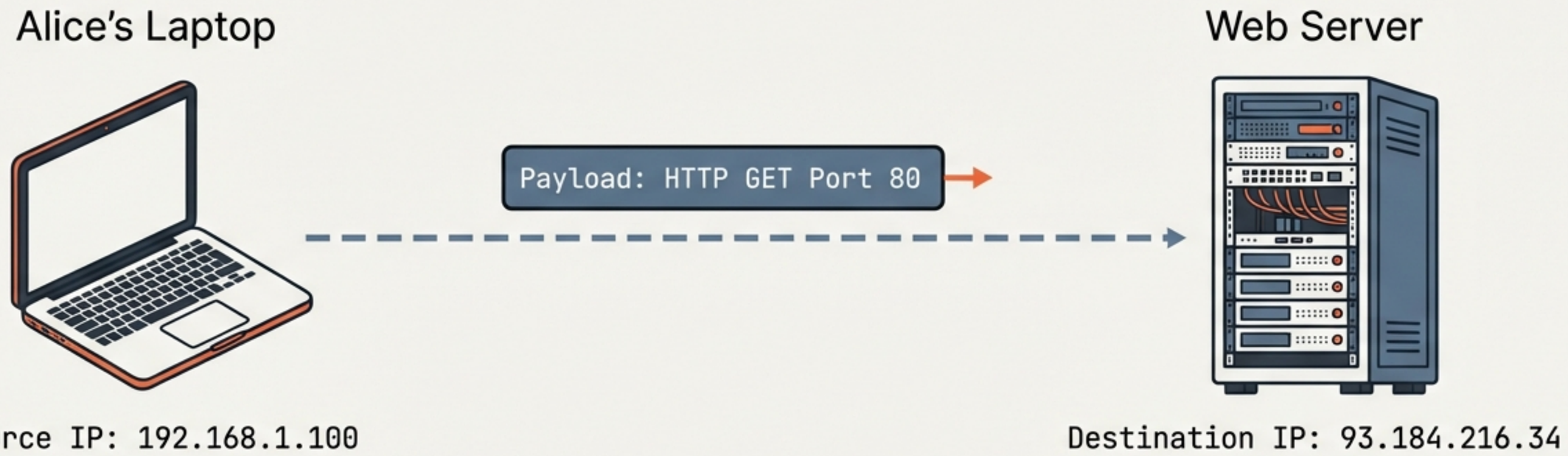
The Life of an IP Packet

An invisible courier's journey across the world in milliseconds.

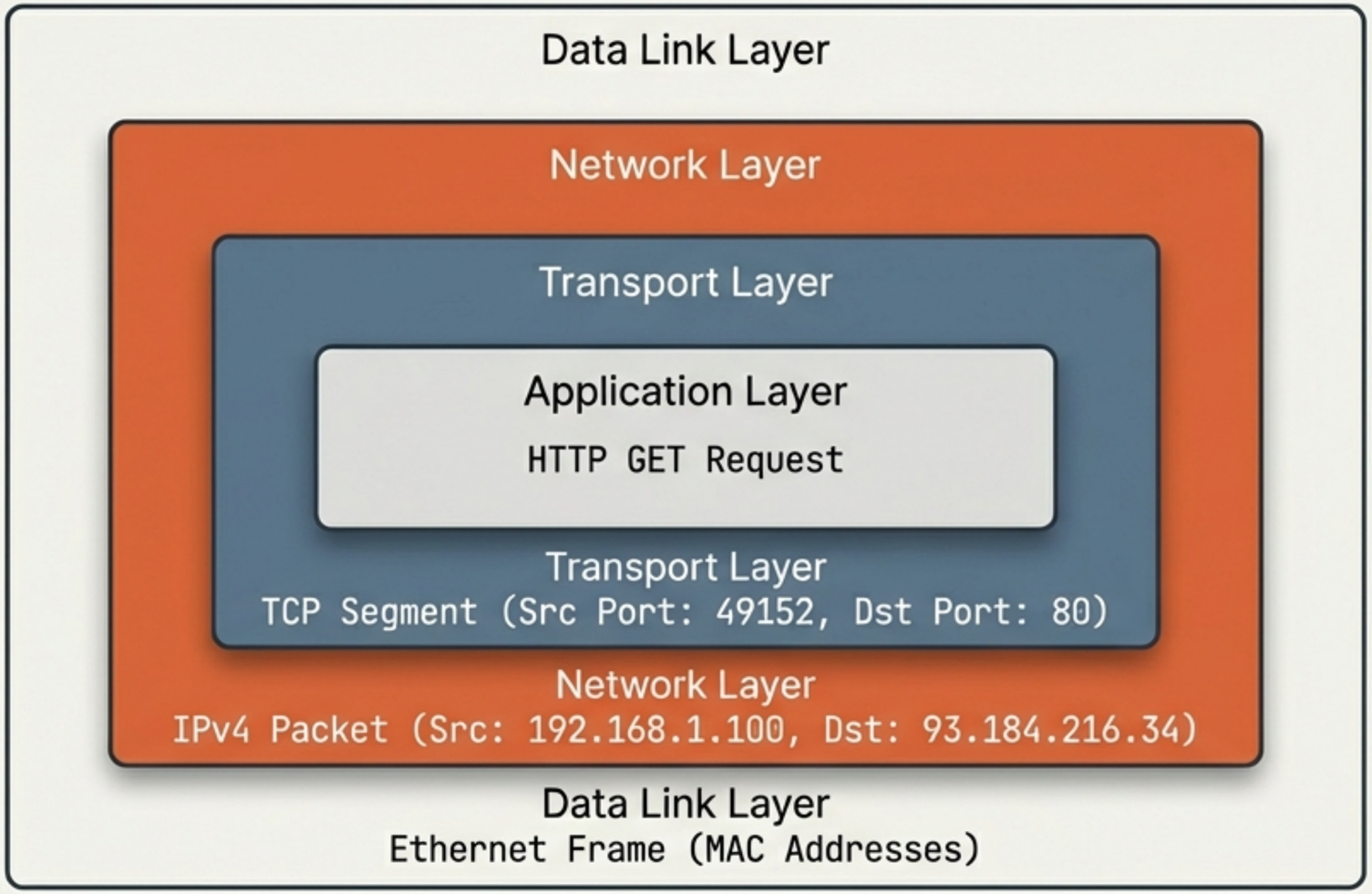
This deck traces the lifecycle of a single IPv4 packet carrying an HTTP GET request. We will follow its creation, its journey through the physical infrastructure of the internet, and the specific anatomy of its header. Finally, we will demonstrate how to capture and analyse this traffic forensically using `Wireshark`.

The Mission: Alice Requests a Webpage



The journey begins with a simple human action. Alice wants to visit www.example.com. Her browser initiates an HTTP GET request, triggering a chain reaction across the network stack.

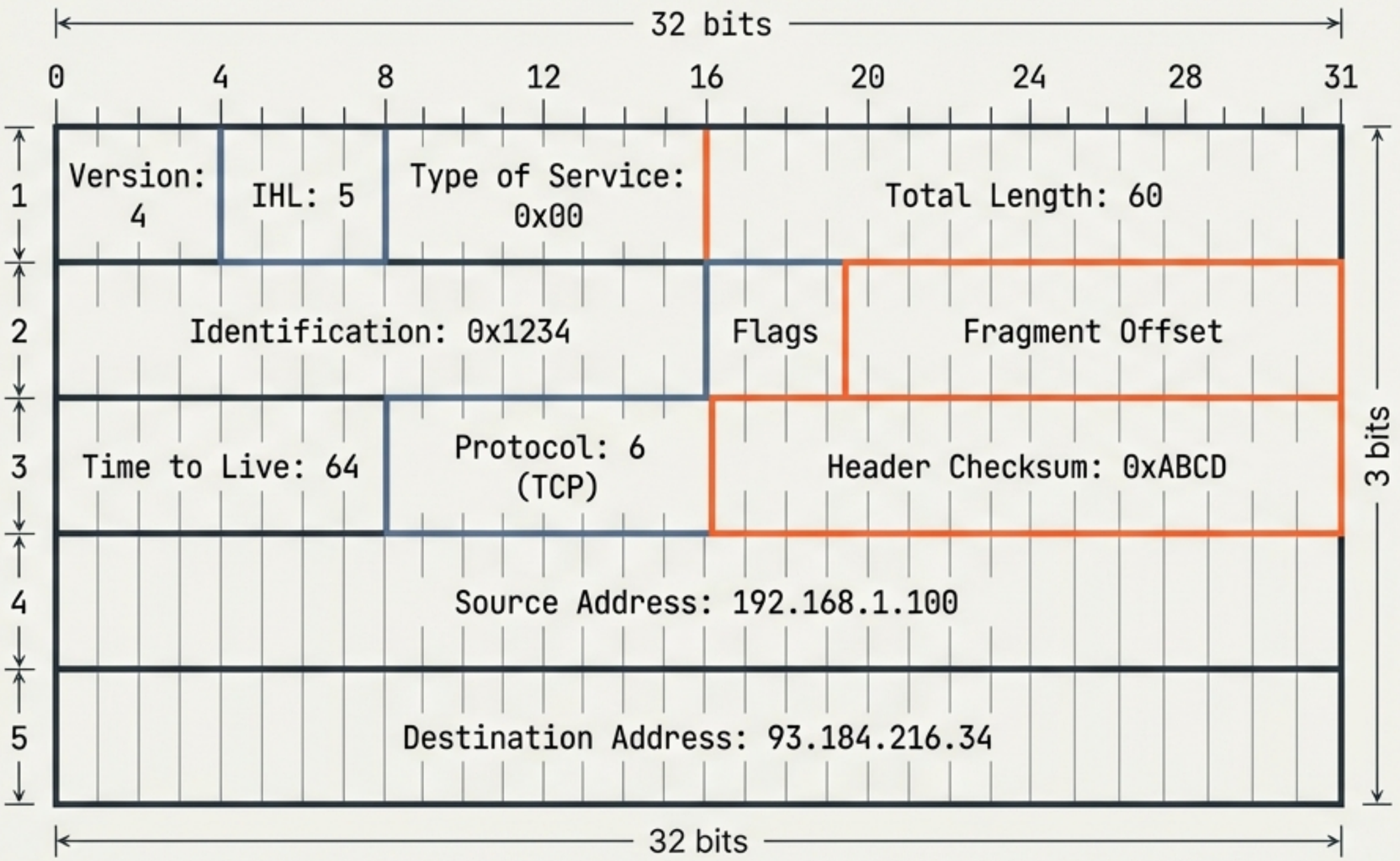
Packet Creation and Encapsulation



The operating system resolves the domain name to an IP address.

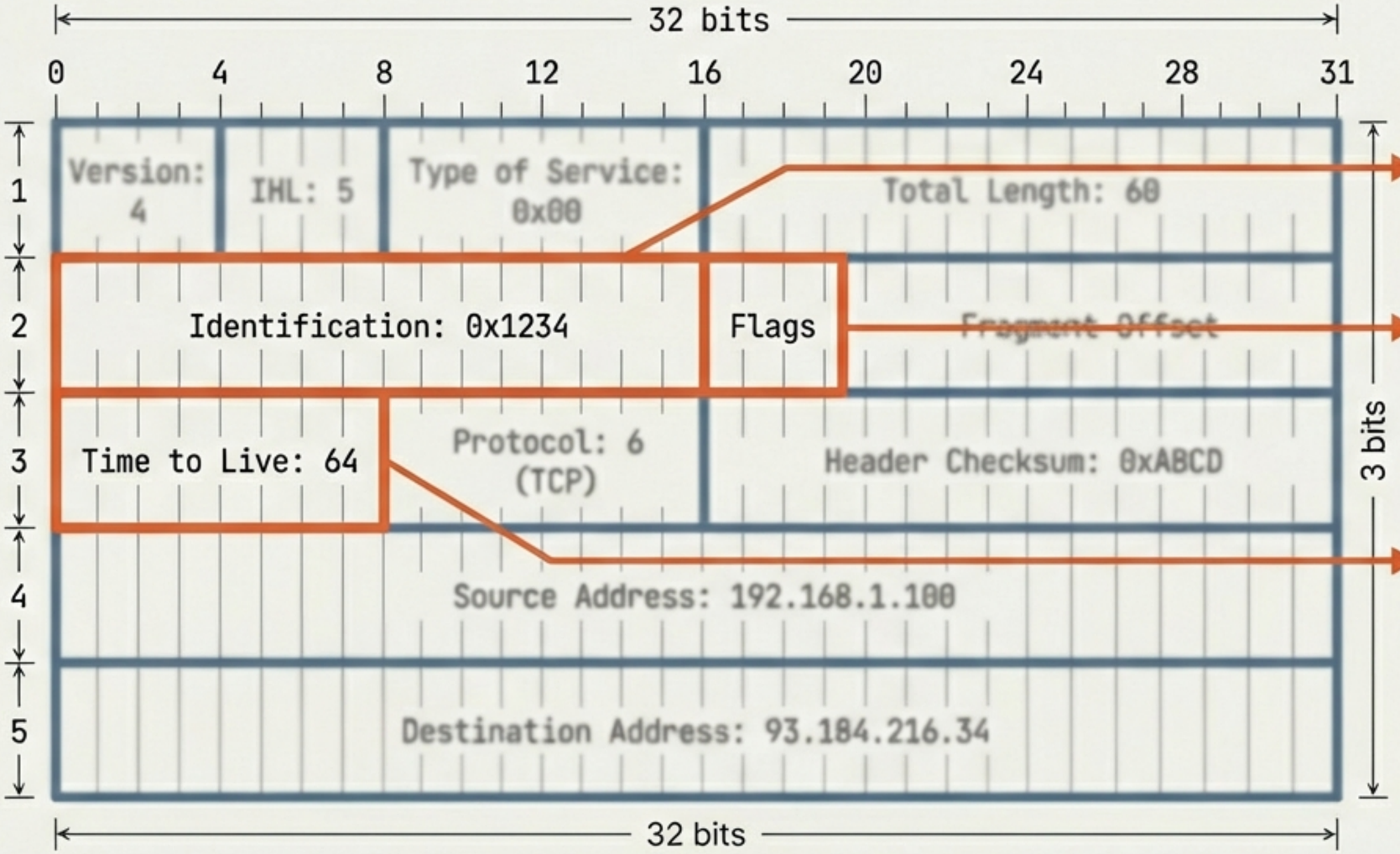
Before leaving the network interface, the data is encapsulated. The TCP segment ensures reliable delivery, while the IP packet provides the addressing logic for the journey ahead.

Anatomy of the Vessel: The IPv4 Header



Just as a shipping container has a manifest, the IP header contains 20 bytes of critical routing instructions. Every bit serves a purpose for survival and delivery.

Critical Fields for Survival and Reassembly

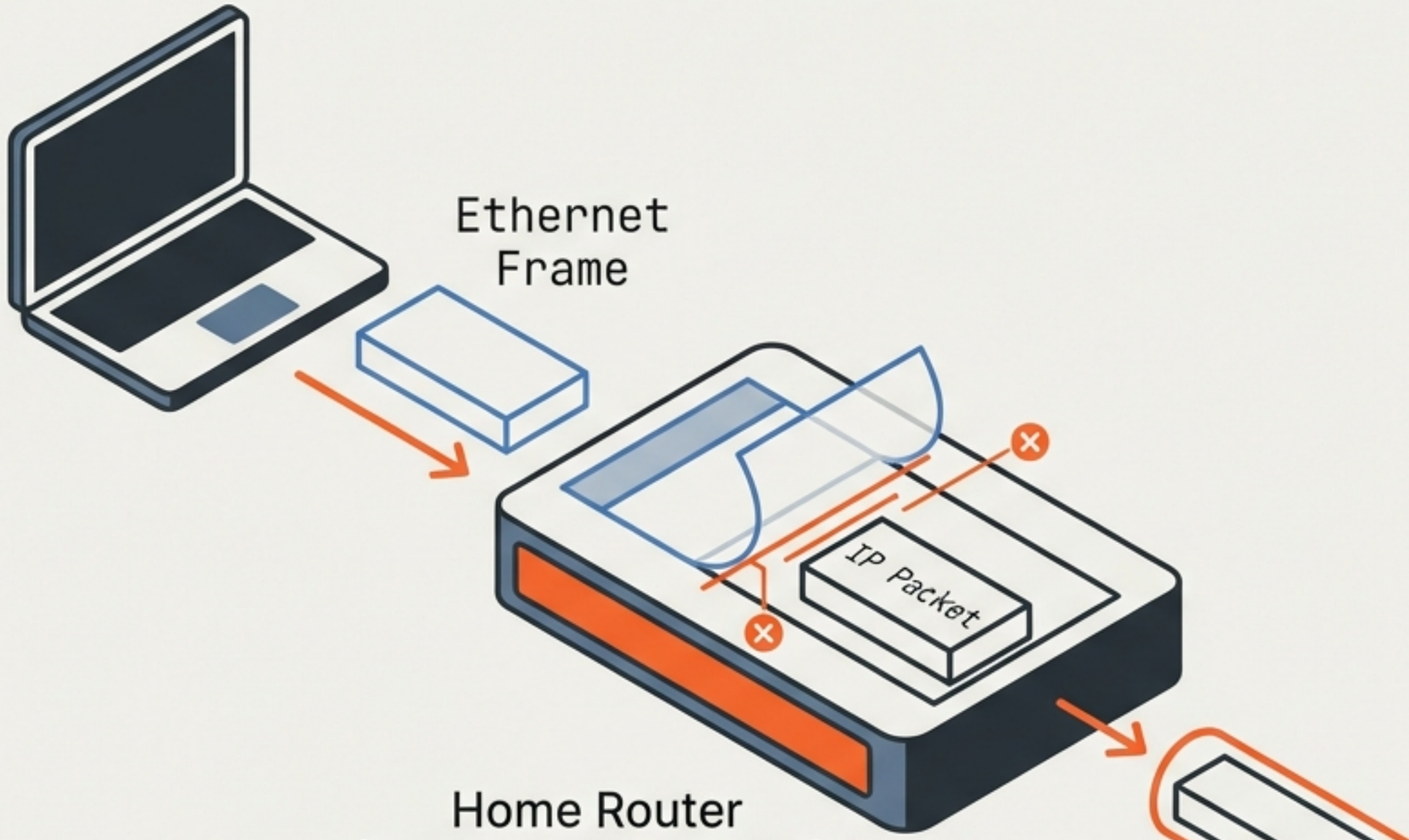


Identification (0x1234): A unique ID used to reassemble the packet if it gets fragmented (chopped up) during the journey.

Flags (0x4000): Specifically, the 'Don't Fragment' bit is set. This tells routers: Do not break me apart.

Time to Live (TTL): Starts at 64. This is a hop limit, not a time in seconds. It acts as a kill-switch to prevent undeliverable packets from circling the internet forever.

Departure: The Local Gateway



The packet leaves the laptop via Ethernet.

Upon reaching the router, the Ethernet frame is stripped off and discarded.

The router checks the destination IP (93.184.216.34), consults its internal routing table, and forwards the bare IP packet to the Internet Service Provider.

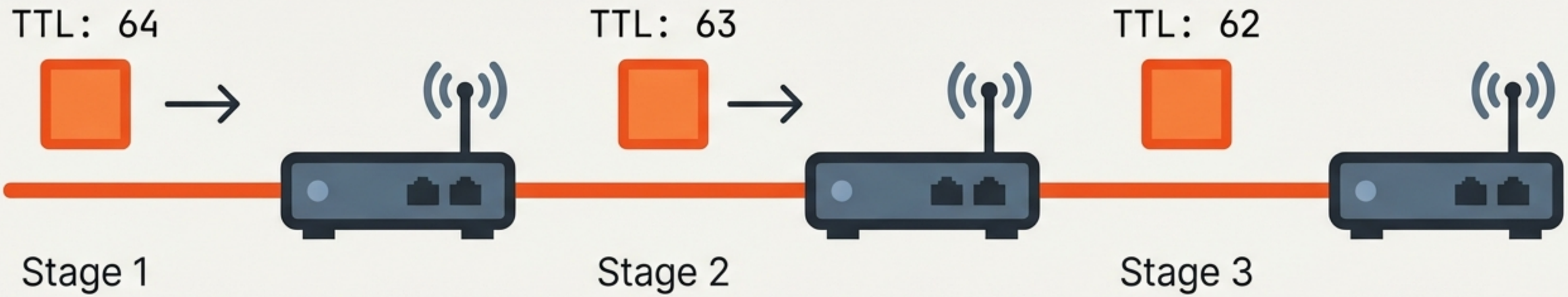
ISP Uplink

Routing Across the Wild Open

The packet does not travel in a straight line. It is passed like a baton through a chain of routers across multiple autonomous networks.

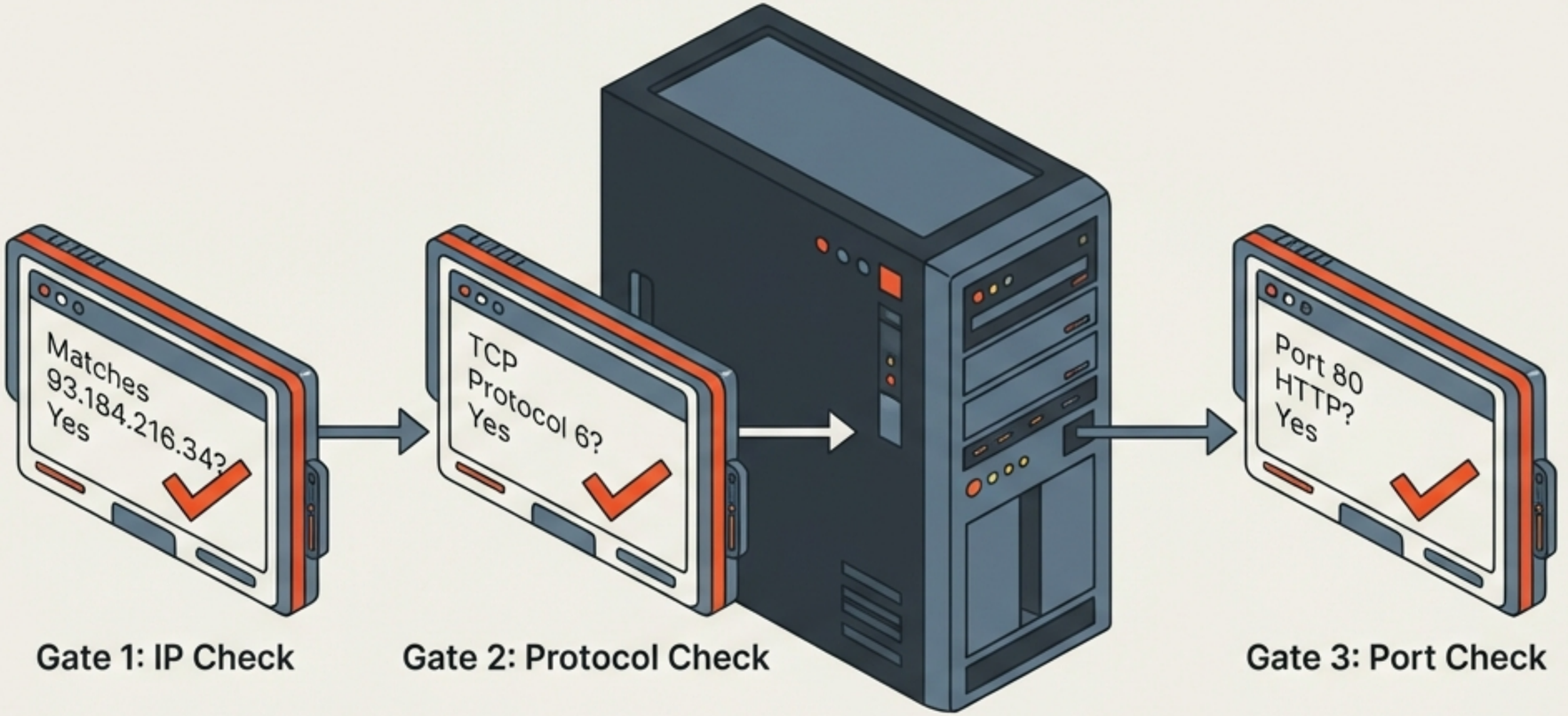
- 1. Router examines destination IP.
- 2. Router looks up best "next hop".
- 3. Packet forwarded closer to destination.

The Cost of Travel: Time to Live (TTL)



To survive the journey, the packet must reach the destination before its energy runs out. At every single hop, the TTL field is decremented by 1. If the TTL reaches 0, the packet is discarded to prevent “zombie packets” from looping infinitely.

Arrival at 93.184.216.34

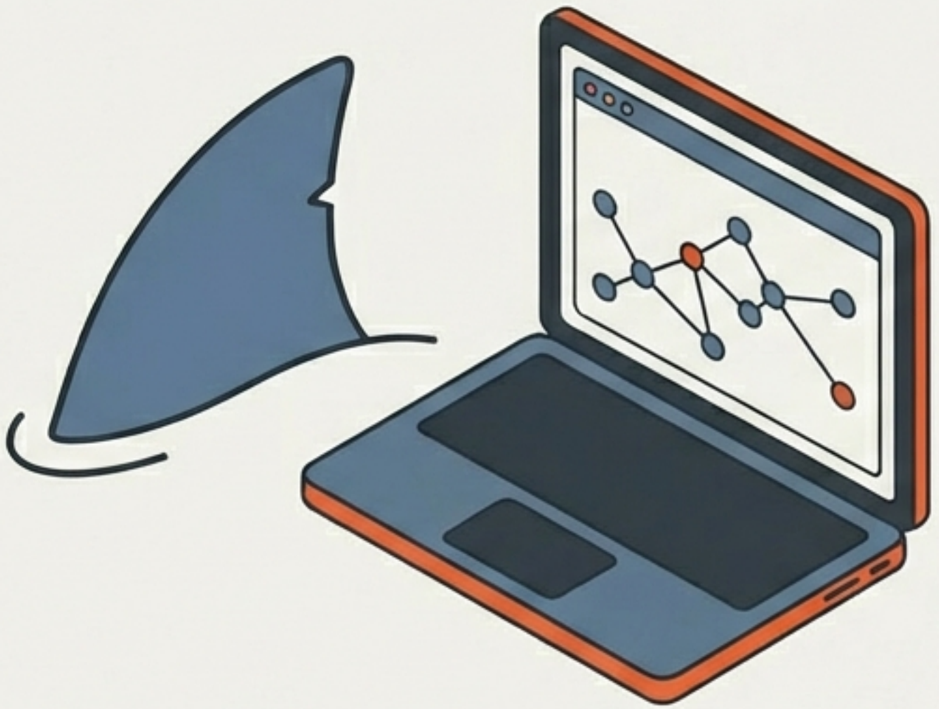


The server receives the packet and performs a security and identity check. Once it confirms the IP, Protocol, and Port match its expectations, it accepts the payload and hands the HTTP `GET` request to the web server software.

The Return Journey & NAT

The server creates a response packet. When it reaches Alice's router, the router uses Network Address Translation (NAT) to remember that Alice's specific laptop initiated the request, forwarding the data to her private IP address.

Forensic Analysis with Wireshark

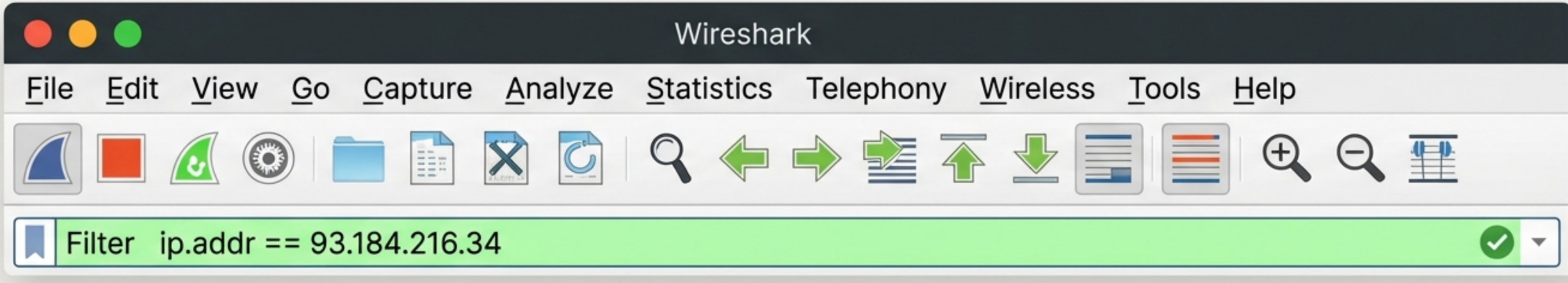


Don’t just take our word for it.

Wireshark is the industry-standard tool for capturing and analysing network packets. It allows us to see this invisible story in real-time.

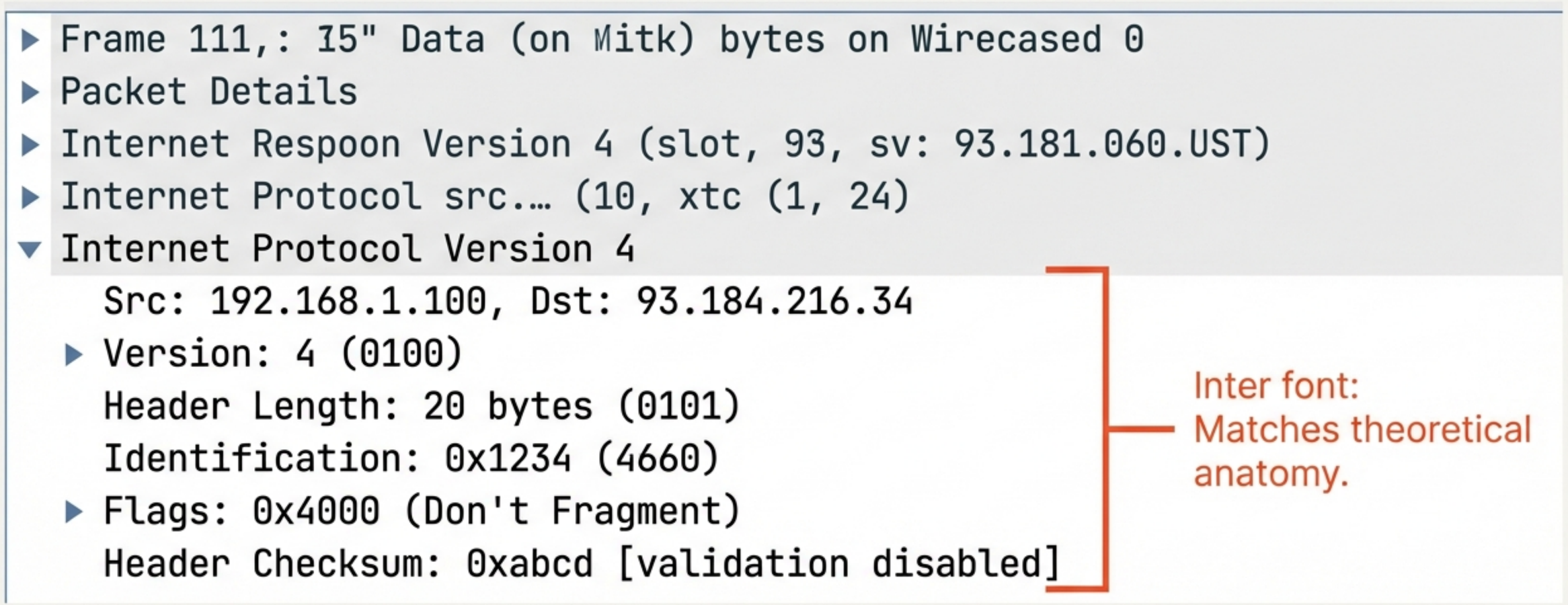
- ☑ 1. Install Wireshark.
- ☑ 2. Select active interface (Wi-Fi/Ethernet).
- ☑ 3. Start Capture.

Isolating the Signal



The internet is noisy. To see the specific interaction with the server, apply a filter. Alternatively, filter by protocol: '`http`'. Then, navigate to www.example.com in your browser to capture the handshake.

The Capture: Verifying the Header



Key Observations from the Capture

TTL Reduction

If capturing at intermediate points, you would see the TTL (e.g., 58) lower than the starting value (64), proving the packet has traversed multiple hops.

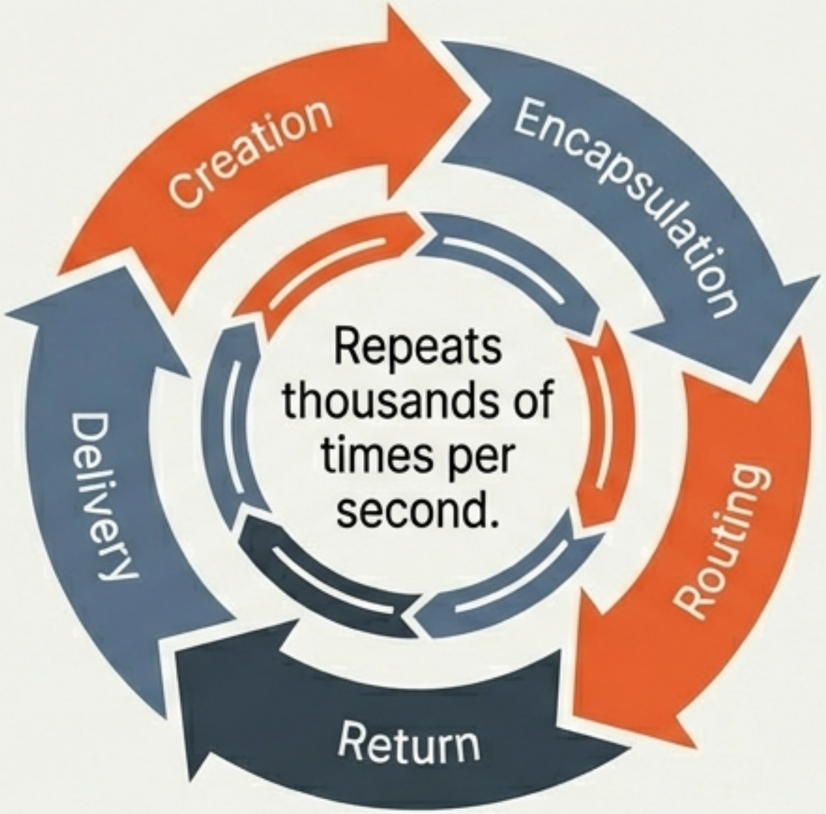
Integrity

The Header Checksum (`0xabcd`) confirms the header was not corrupted in in transit.

NAT Effects

If captured outside the local network, the Source IP would show the Router's Public IP, not Alice's local `192.168.1.100`.

The Internet in Motion



The life of an IP packet is a complex orchestration of precision engineering. Understanding the header structure and routing logic demystifies how the global internet functions.

CALL TO ACTION

Download Wireshark. Capture traffic to www.example.com. See the invisible couriers for yourself.