Flashcards — What Happens When You Hit Enter

Episode 001 · cut along the lines, or import NetSecViz-001-Flashcards.csv into Anki (Front/Back).

Q Order of DNS lookup locations?
A Browser cache -> OS cache -> recursive resolver -> root -> TLD -> authoritative.

Q What does DNS do?
A Maps a human domain name to a numeric IP address.

Q Recursive resolver vs authoritative server?
A Recursive does the full lookup for you; authoritative holds the real record for the domain.

Q What is a TTL in DNS?
A Time To Live: how long a cached DNS answer stays valid.

Q What does ARP map?
A An IP address to a MAC (hardware) address on the local network.

Q Why is the default gateway needed?
A Your machine can only deliver directly to the LAN; anything off-network goes through the router (gateway).

Q Across the internet, what stays constant and what changes per hop?
A The destination IP stays constant end to end; the MAC address changes at each hop.

Q The three messages of the TCP handshake?
A SYN, then SYN-ACK, then ACK.

Q What does TCP guarantee?
A Reliable, ordered delivery; lost packets are re-sent.

Q Which port does HTTPS use?
A Port 443.

Q What is TLS and what is it for?
A Transport Layer Security: it encrypts the connection (the S in HTTPS).

Q In TLS, how do both sides get the same secret key?
A Each combines its own Diffie-Hellman private half with the other's public half; the secret is never sent on the wire.

Q What does the server's certificate prove?
A Its identity, because it is signed by a trusted Certificate Authority (CA).

Q What is forward secrecy?
A Past recorded traffic stays unreadable even if the server's private key is later stolen.

Q Structure of an HTTP request?
A A method and path (e.g. GET /) plus headers like Host.

Q Structure of an HTTP response?
A A status code (e.g. 200 OK), headers, and the body (the HTML).

Q What does status code 200 mean?
A OK: the request succeeded.

Q What is HTTP/3 built on?
A QUIC, which runs on UDP.

Q How does QUIC speed up setup?
A It merges the TCP and TLS handshakes into a single round trip.

Q What is 0-RTT?
A Zero round-trip time: a returning visitor sends encrypted data in the first packet, with no handshake.

Q Steps of the browser render pipeline?
A HTML->DOM, CSS->CSSOM, combine into render tree, layout, paint, composite.

Q What is the render tree?
A The combined DOM and CSSOM, containing only the elements that are actually visible.

Q What does 'render progressively' mean?
A The browser paints what it can right away instead of waiting for every resource.

Q Three parts of a URL?
A Scheme (https), host (the machine name), and path (the specific resource).

Q What does HSTS do?
A Forces a site to always be loaded over HTTPS, blocking downgrade to http.

Q What is a MAC address?
A A hardware address burned into a network card, used for delivery on the local network.

Q What is a recursive resolver, in one line?
A A DNS server that does the whole lookup on your behalf (e.g. 8.8.8.8).

Q What does the GPU do in rendering?
A It composites the layers into the final image (the composite step).

Q Diffie-Hellman in one line?
A A method letting two parties derive a shared secret without ever transmitting it.

Q Why can a wiretapper not read a TLS session they fully recorded?
A The shared key is derived independently by each side and never crosses the wire.

Q When does ARP actually send a broadcast, and how often?
A Only when the needed IP-to-MAC mapping is not already in the ARP cache. The gateway's MAC is resolved once and reused, refreshed only when the cache entry expires. It is not per request.

Q What is the ARP cache?
A A device's stored list of recently learned IP-to-MAC mappings, so it does not have to ARP every time.

Q Common ARP misconception?
A That ARP runs on every request or connection. It does not; the result is cached and reused.

Q Which DNS record holds an IPv4 vs an IPv6 address?
A A record holds IPv4; AAAA record holds IPv6.

Q What does a CNAME record do?
A Points one domain name to another name.

Q Iterative vs recursive in DNS?
A The resolver's walk down the hierarchy is iterative (referrals); the service it gives you is recursive (it chases the whole chain for you).

Q Why does the TCP handshake need three messages, not two?
A Both sides must announce a starting sequence number and have it acknowledged, which takes three messages.

Q What is a socket?
A An IP address combined with a port; a connection is identified by the pair of sockets at each end.

Q Asymmetric vs symmetric crypto in TLS?
A Asymmetric (Diffie-Hellman) agrees on a key; fast symmetric crypto then encrypts the actual data.

Q In TLS, which part gives secrecy and which gives identity?
A Diffie-Hellman gives secrecy; the CA-signed certificate gives identity.

Q What is SNI?
A Server Name Indication: the field that tells a shared server which site's certificate to present.

Q What does the HTTP Host header enable?
A One server with one IP to host many different sites.

Q What problem does QUIC solve by keeping streams independent?
A Head-of-line blocking: one lost packet no longer stalls every other stream.

Q DOM vs render tree?
A The DOM has every element; the render tree has only the visible ones (no display:none, no <head>).

Q What is the critical rendering path?
A The full sequence from HTML and CSS to pixels; shortening it improves load speed.

Q What do the status code families mean?
A 2xx success, 3xx redirect, 4xx client error, 5xx server error.

Q Why is UDP alone not enough for QUIC, and what does QUIC add?
A UDP is unreliable; QUIC rebuilds reliability and ordering on top of it.

Q Why is 0-RTT data limited to safe requests?
A It can be replayed by an attacker, so it should only carry requests that do not change state (like GET).

Q Reflow vs repaint?
A Reflow recomputes layout (position/size); repaint only redraws pixels. Reflow is more expensive.