Live demonstrations

of privacy issues in DNS, TLS, and email

Kaspar Etter · 25 April 2026 · CC BY 4.0

Outline

- Refresher from the Internet article
- Inspecting network traffic
- Remote content in email

Acknowledgment

These slides were created with help from GPT-5.4.

Refresher from the Internet article

Enough context to follow the demonstrations

Internet layers

Name	Purpose	Example
Application layer	Application logic	HTTP
Security layer	Encryption and authentication	TLS
Transport layer	Typically reliable data transfer	TCP
Network layer	Packet routing across the Internet	IP
Link layer	Handling of the physical medium	Wi-Fi

Each layer solves "one" specific networking problem.

Various protocols per layer, making the stack modular.

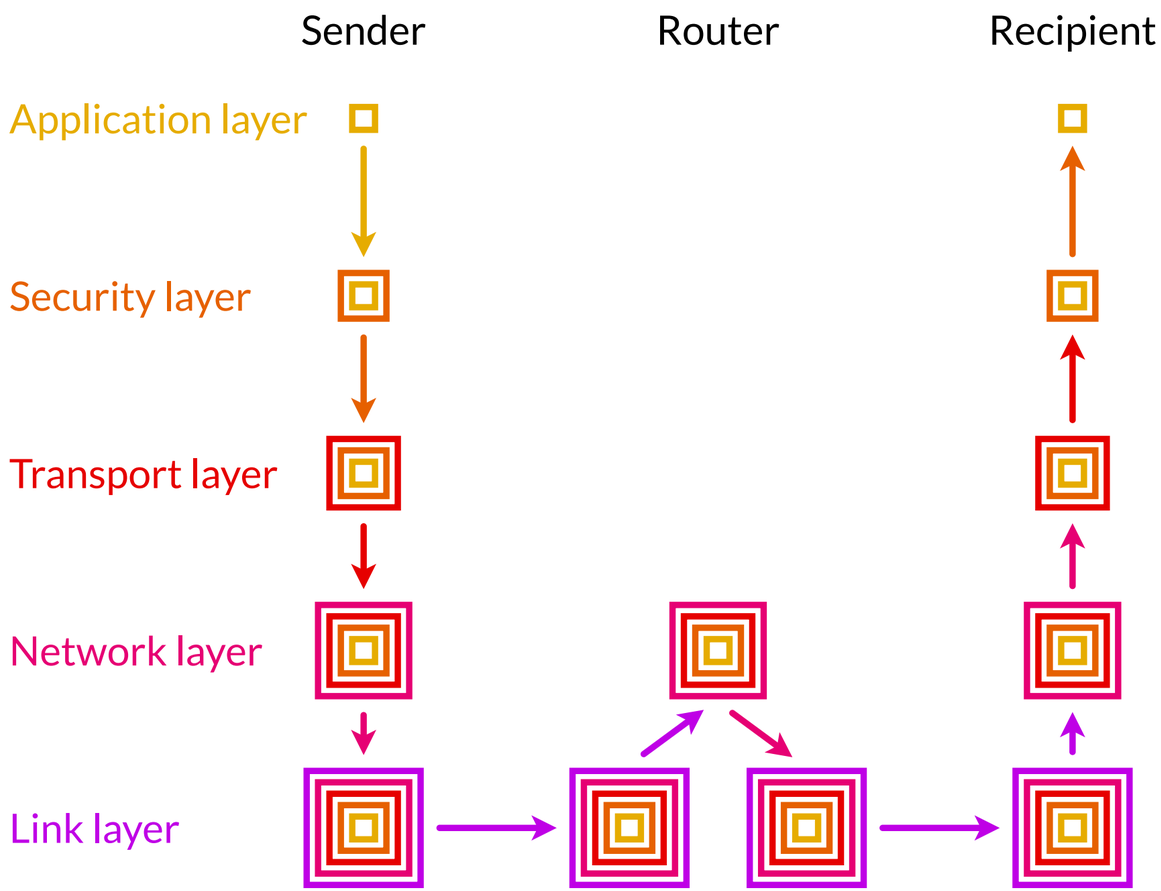
Packet wrapping

Each layer adds its own header to the data from the layer above.

The graphic misleads in two ways. Protocols can:

– transform the payload (compression, encryption, error correction),

– split the payload & transfer smaller chunks separately.



Internet Protocol (IP)

IP routes packets across connected (sub-)networks.

It gives packets source and destination addresses so routers can forward them toward the right network.

IPv4 uses a 32-bit address to identify a network interface of a device. Example: `74.125.29.102`

IPv6 uses much longer 128-bit addresses, mainly because the Internet needed far more addresses. Example: `2a00:1450:400a:1000::71`

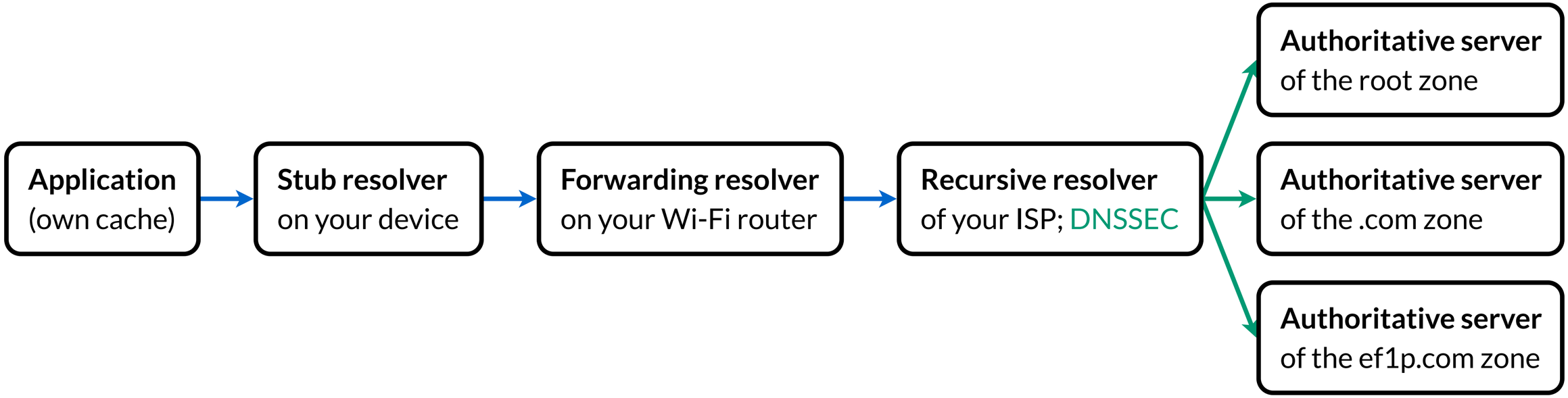
Internet Protocol, IPv4, IPv6

Domain Name System (DNS)

DNS maps human-friendly names to IP addresses.

It is the Internet's distributed telephone book.

Caching and hierarchy make these lookups scale.



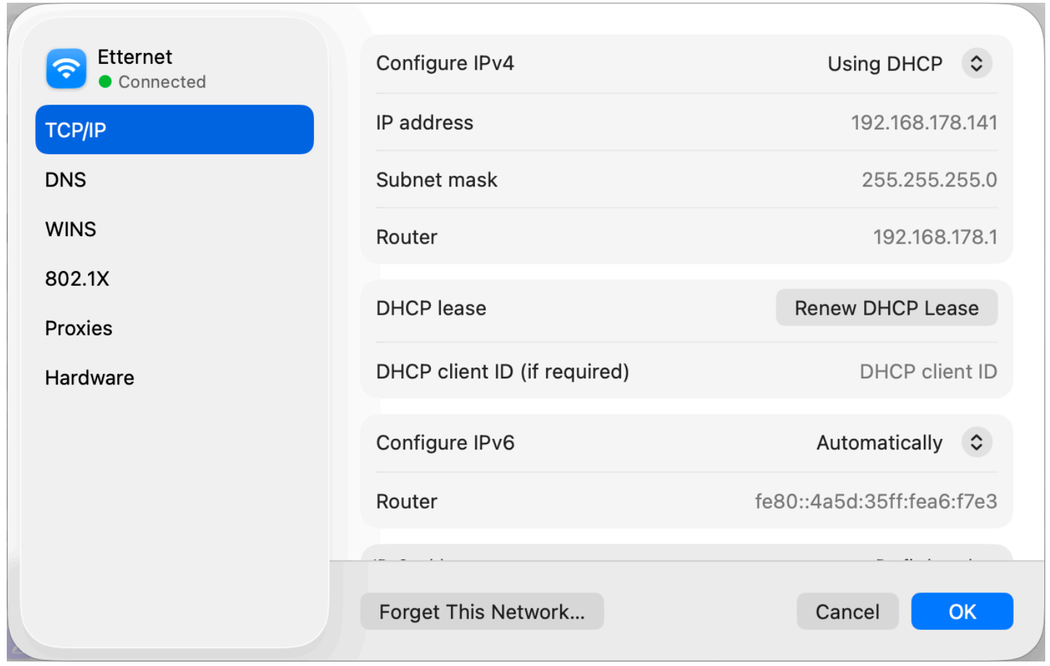
Domain Name System, DNS stub resolvers

Dynamic Host Configuration Prot. (DHCP)

It lets devices join a network without manual setup.

The router assigns an IP address and related settings.

This is why Wi-Fi "just works" when you connect.



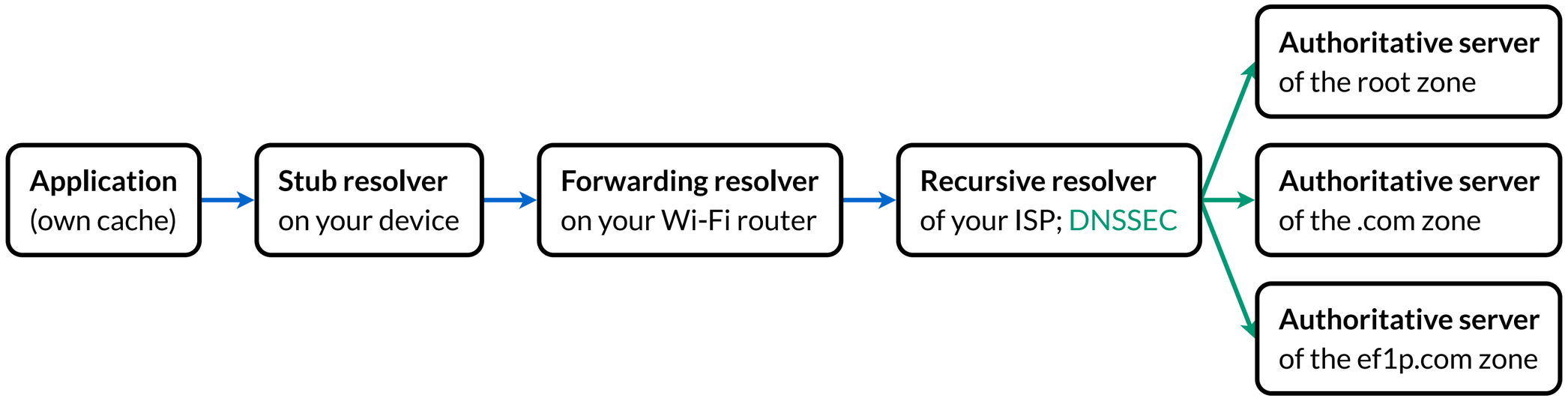
Problems with router-provided classic DNS

Most devices let DHCP configure their DNS resolver.

On public Wi-Fi, the router cannot be trusted (evil twin).

Plaintext DNS leaks what domain names you look up.

Bogus DNS replies can misdirect you before TLS starts.



Problems with plaintext DNS, evil twin attack

Transport Layer Security (TLS)

TLS encrypts the traffic between a client and a server.

It also authenticates the server with a certificate, which was issued by a trusted certificate authority (CA).

TLS also prevents message tampering in transit.

It does not hide all metadata of the connection.

Transport Layer Security, public key infrastructure, certificate authority

Server Name Indication (SNI)

One server can host many sites behind one IP address.

Clients have to tell the server which site they want with the TLS extension SNI to get the matching certificate.

Without Encrypted Client Hello (ECH), which has been published as a standard only in March 2026, the name of the site is not encrypted and visible to all bystanders.

Thus, others can see which sites you visit, as I will show.

Server Name Indication, Encrypted Client Hello

Wi-Fi Protected Access (WPA)

WPA protects the link between your device and the router by encrypting the radio signals with a password.

It does not replace end-to-end security, such as TLS.

WPA2 & WPA3 are different versions of this protection.

WPA3 is more secure but not yet widely used in 2026.

WPA2 is widespread but not secure

Everyone nearby receives the same radio signal.

If the password is known and the handshake was captured, WPA2 traffic can be decrypted afterwards.

Attackers can often trigger a fresh handshake at will.

Sharing your Wi-Fi password weakens your privacy.

Inspecting network traffic

Seeing computer networks in action

Disclaimer

Unauthorized interception of third-party traffic is usually illegal because most jurisdictions protect the secrecy of correspondence.

Capture only your own devices on your own network or a network where you have explicit permission to do so.

Don't wiretap other people without their consent!

The tool we'll use: Wireshark

Wireshark is a free and open-source packet analyzer.

In monitoring mode, your device records all packets on the network, not just those addressed to your device.

We'll let macOS capture the traffic and then use Wireshark to analyze the captured packets.

Wireshark, packet analyzer

Monitoring mode on macOS

Open the app "Wireless Diagnostics", use its "Sniffer".

Match the Wi-Fi channel and channel width from the menu bar (alt-click on the Wi-Fi icon to see this info).

Start the capture and stop once you have enough data.

Packet capture (.pcap) files

macOS stores the capture in a ".pcap" file in "/var/tmp".

In Finder, use "Go" > "Go to Folder..." & enter "/var/tmp".

Then open the file in Wireshark to analyze the packets.

Delete the ".pcap" file afterwards, as it may be sensitive.

WPA2 decryption in Wireshark

Skip this step if the Wi-Fi network is not encrypted.

In Wireshark "Preferences" > "Protocols" > "IEEE 802.11":

– Make sure decryption is enabled.
– Add a "wpa-pwd" key as "password:network-name".

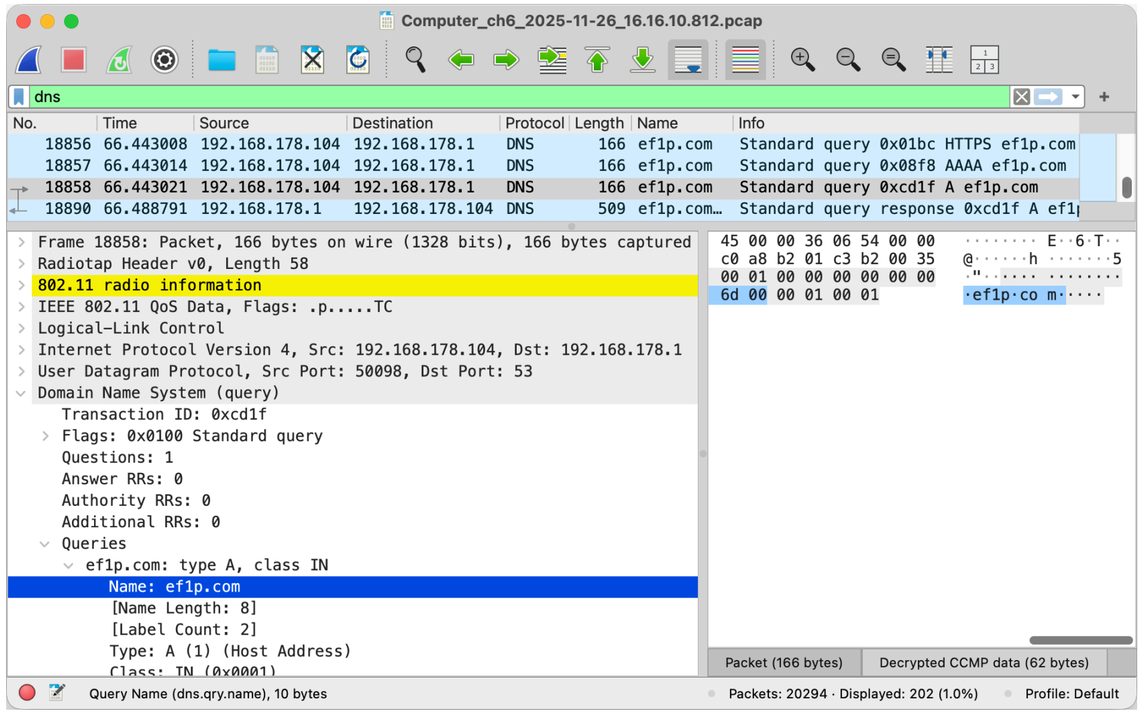
Decryption works only if the four EAPOL handshake packets between a device and the router were captured.

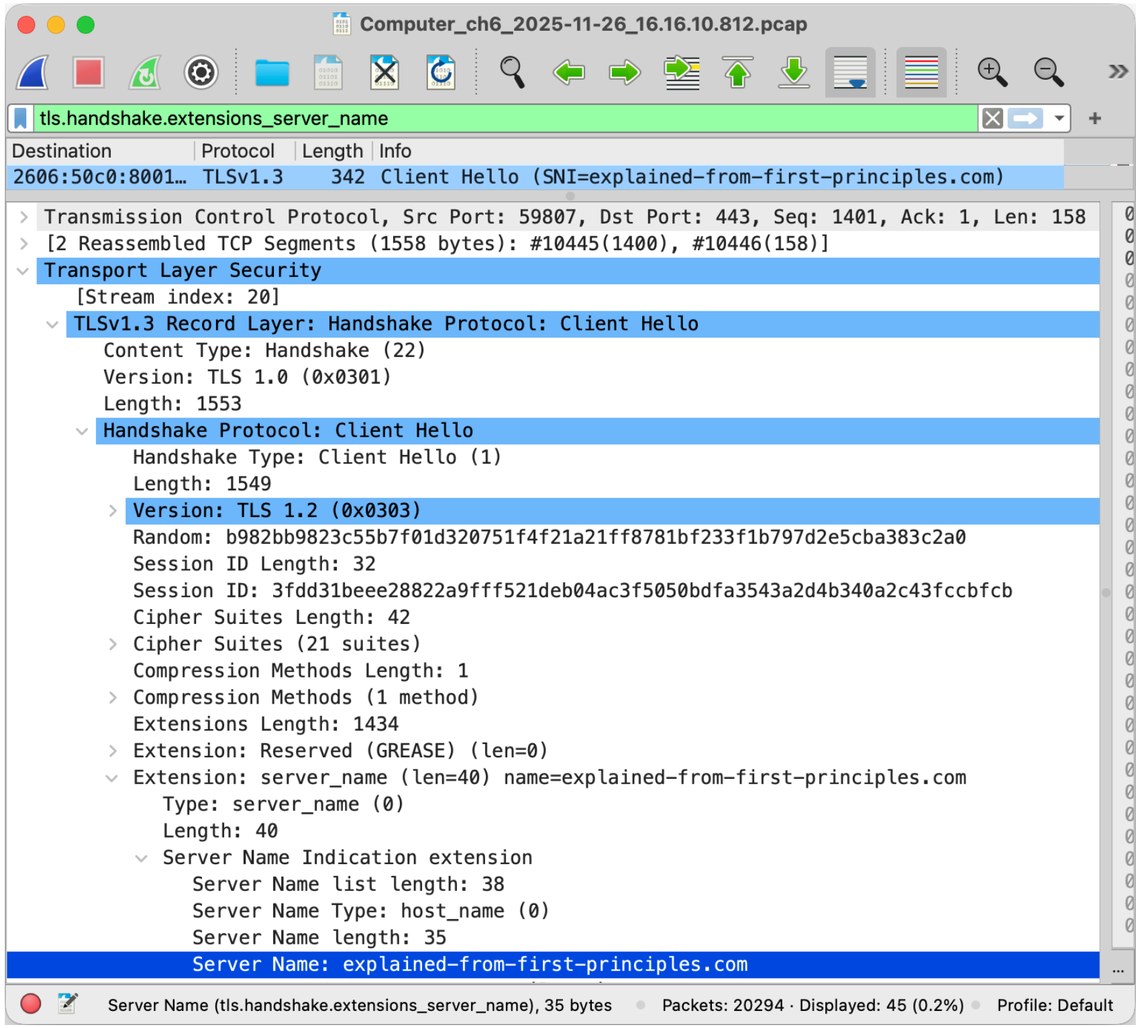
Wireshark filters

- WPA2 handshake: `eapol`
- One device: `wlan.addr == aa:bb:cc:dd:ee:ff`
- Core protocols: `tls`, `dhcp`, `dns`, `http`
- SNI field (this includes initial QUIC packets):
  `tls.handshake.extensions_server_name`
- DNS queries only: `dns.flags.response == 0`
- Combine filters with `&&` (and) or `||` (or).

Guide to analyzing the captured packets, QUIC

Screenshots of Wireshark





Tip 1: Configure a secure DNS resolver

Public Wi-Fi usually chooses your DNS resolver for you.

Configure a public recursive resolver you trust instead, using DNS over HTTPS (DoH) or DNS over TLS (DoT).

Configure the operating system, not only the browser.

I recommend Quad9: Use DoH (HTTPS) either

– with ECS (`9.9.9.11`, better routing)

– or without (`9.9.9.9`, better privacy).

Then visit on.quad9.net to see if it worked.

DNS configuration recommendations, EDNS Client Subnet (ECS), Quad9 setup guides

Tip 2: Enable warnings for insecure HTTP

Never log in to a website over HTTP: Anyone in the same network can steal your password or hijack your session.

Websites can signal that browsers should use only HTTPS with HTTP Strict Transport Security (HSTS).

First visits to some important websites are protected by HSTS preload lists in browsers. (Hosts have to opt in.)

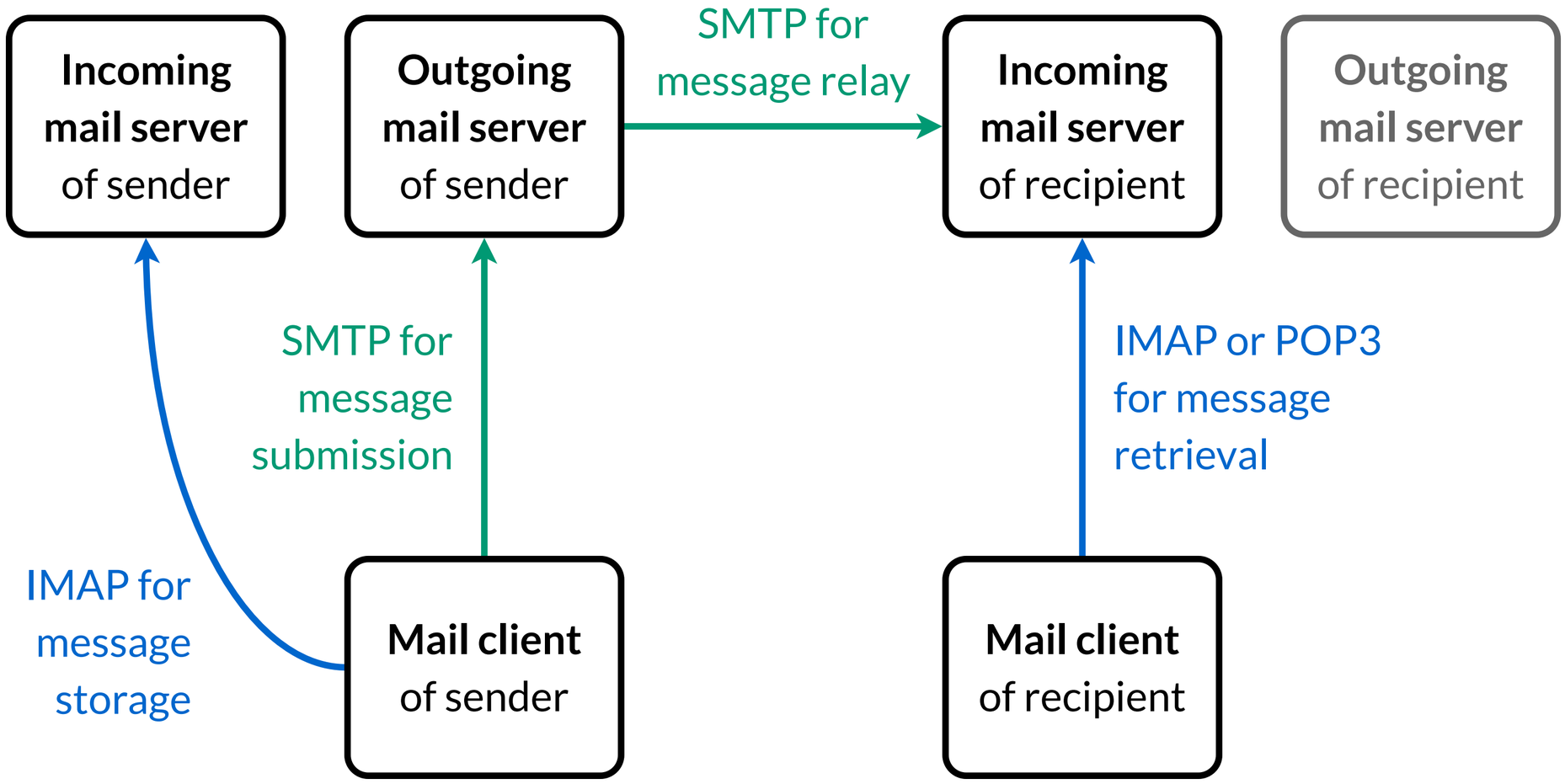
Better be safe than sorry: Enable warnings for insecure HTTP connections in your browser (see the links below).

Session hijacking; always use secure connections in Chrome; HTTPS-only mode in Firefox

Remote content in email

Modern email violates your privacy

Email architecture



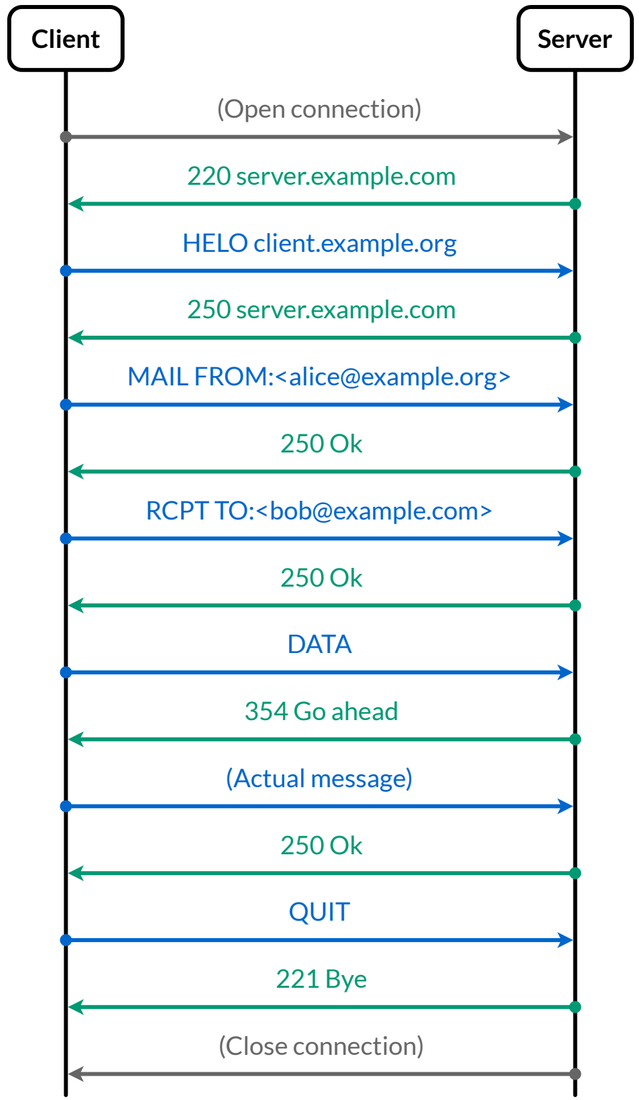
Submission, relay, and retrieval are separate interactions.

Extended Simple Mail Transfer Pr. (ESMTP)

SMTP sequence diagram on the right:

ESMTP (1993) is SMTP (1982) with backward-compatible extensions.

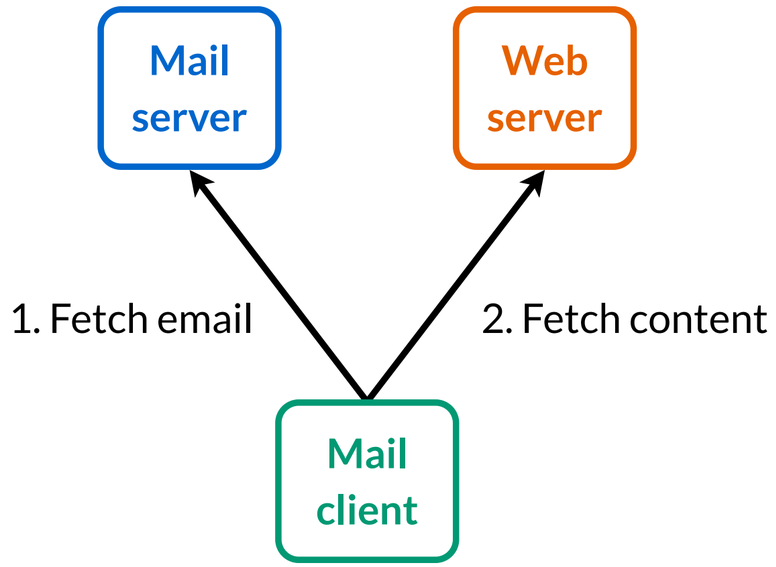
It is used for submission and relay.



Remote content

Remote content breaks three central principles of email:

- **Offline reading**: Parts of emails are missing when you are offline.
- **Immutable content**: The sender can change what loads later.
- **Reading privacy**: Opening mails leaks time, IP, and client details.



Email on the command-line interface (CLI)

Open a TLS connection with `openssl` to the server.

Say `EHLO`, then authenticate for mail submission.

Send `MAIL FROM`, `RCPT TO`, and then `DATA`.

End the message with a single dot on a line.

Close the connection with `QUIT`.

The remote image I add is a transparent 1x1 pixel PNG.

ESMTP tool, email tracking tool

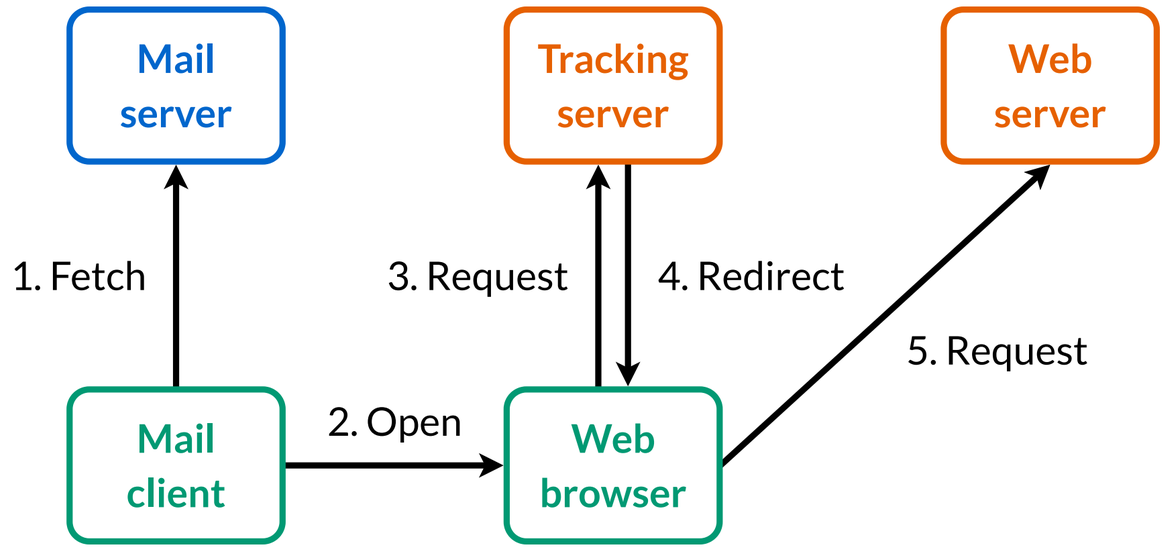
Link tracking

A link can direct you to the sender's tracking server.

That server records the click and then redirects you.

This works even in non-HTML emails and with remote content blocked.

The only thing you can do about link tracking is not clicking on links in emails.



Tip 3: Disable remote content in your client

Knowing your email address shouldn't be enough to determine your approximate location at any time.

Configure all your mail clients to block remote content.

Then load remote content only for messages where you're willing to share your IP address with the sender.

(Some mail clients proxy remote content by default.)

How to disable remote content; proxying remote content

Summary

Local networks reveal more than many people expect.

Wireshark makes DNS, SNI, and weak WPA2 visible.

Remote content in emails leaks private information.

Further reading

- Internet explained from first principles
- Email explained from first principles