**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

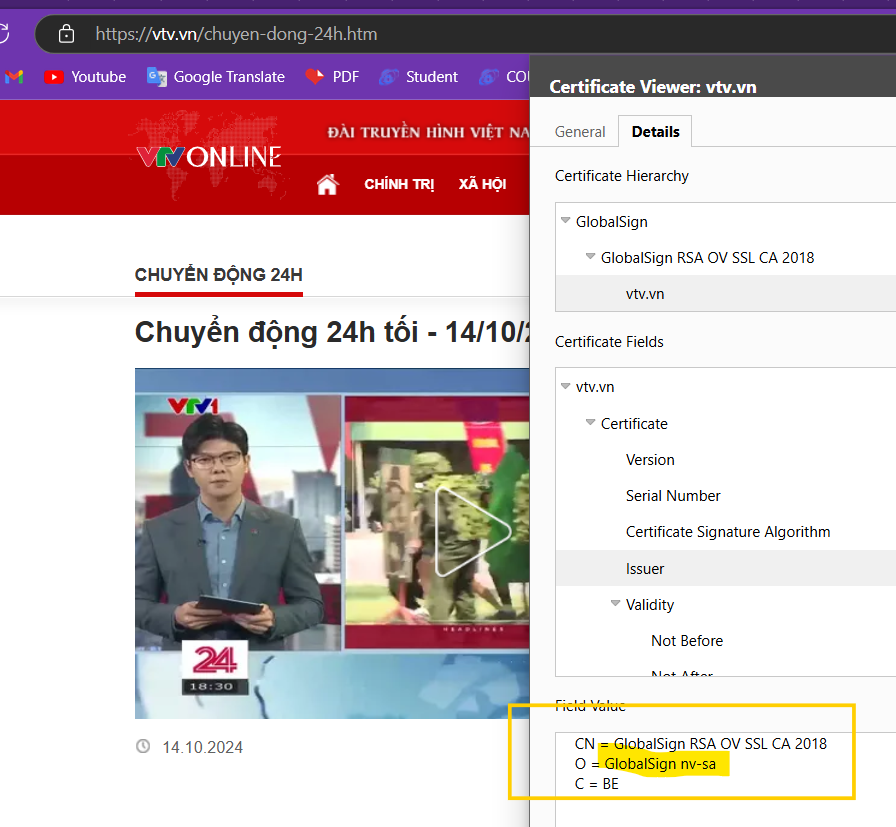
1. **Tìm kiếm các trang web (3-4 trang) được chứng thực bởi các nhà cung cấp chứng chỉ số khác nhau (trong và ngoài nước).**

**Trang báo điện tử Tiên Phong**

A screenshot of a certificate

Description automatically generated

**Trang VTV 24**

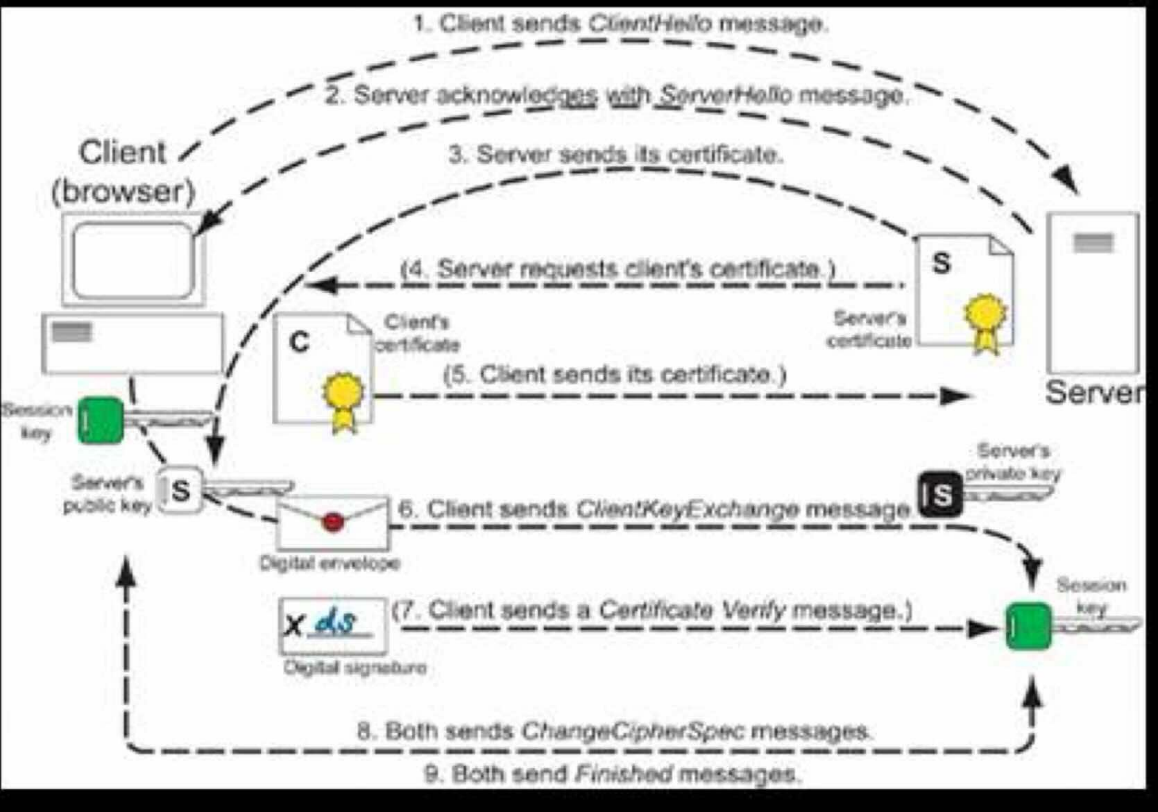
****

**Trang bán hàng Amazon**

**A screenshot of a computer

Description automatically generated**

1. **Mô tả quá trình trao đổi khóa của giao thức SSL**



1. Client gữi lời chào muốn làm việc với server bằng gói tin Client hello: client gửi message tới server, chứa thông tin về SSL/TLS version hổ trợ, thuật toán mã hóa, ...
2. Server xác nhận lời chào bằng gói Server hello: server gửi message tới client, chứ thông tin về SSL/TLS version sẽ được dùng, thuật toán mã hóa được chọn, về digital certificate của server (nếu có).
3. Server gữi chứng chỉ số (S) Server certificate: chứa public key được cung cấp bởi trusted Certificat Authority (CA), client sẽ kiểm tra certificate.
4. Server yêu cầu Client trao đổi Key exchange: trao đổi khóa để tạo ra một khóa bí mật, sẽ được dùng để mã hóa và giải mã trong suốt quá trình trao đổi thông tin.
5. Session key: trong khi chia sẻ khóa bí mật, cả client và server sẽ nhận được session key. Session key dùng để mã hóa và giải mã trong suốt quá trình. Mỗi session sẽ có một session key riêng.
6. Cipher suite selection: Client và server cùng thỏa thuận về bộ giải mã, bao gồm thuật toán giải mã, thuật toán hàm băm và các thuật toán khác trong suốt quá trình trao đổi.
7. Chứng nhận lại khoá xanh này là do chính xác client gữi

Clietn băm bao thư ra được chuỗi băm, dùng khoá bí mật của mình mã hoá chuỗi băm rồi gữi đi

Server sẽ dùng mã công khai để mã hoá ra chuỗi băm

So sánh 2 chuỗi băm để xem khoá xanh này là toàn vẹnFinish handshake: sau khi thỏa thuận xong bộ giải mã và các keys, client và server cùng gửi FINISH message để kết thúc quá trình bắt tay. Từ thời điểm này, SSL/TLS đảm bảo bảo mật và mã hóa.

1. Secure data exchange: sau bước bắt tay, dữ liệu có thể được trao đổi thông qua các giao thức bảo mật.
2. Session resumption: SSL/TLS cho phép nối lại phiên, nhằm cải thiện hiệu suất bằng cách sử dụng lại các phiên đã sử dụng mà không cần qua bước bắt tay.