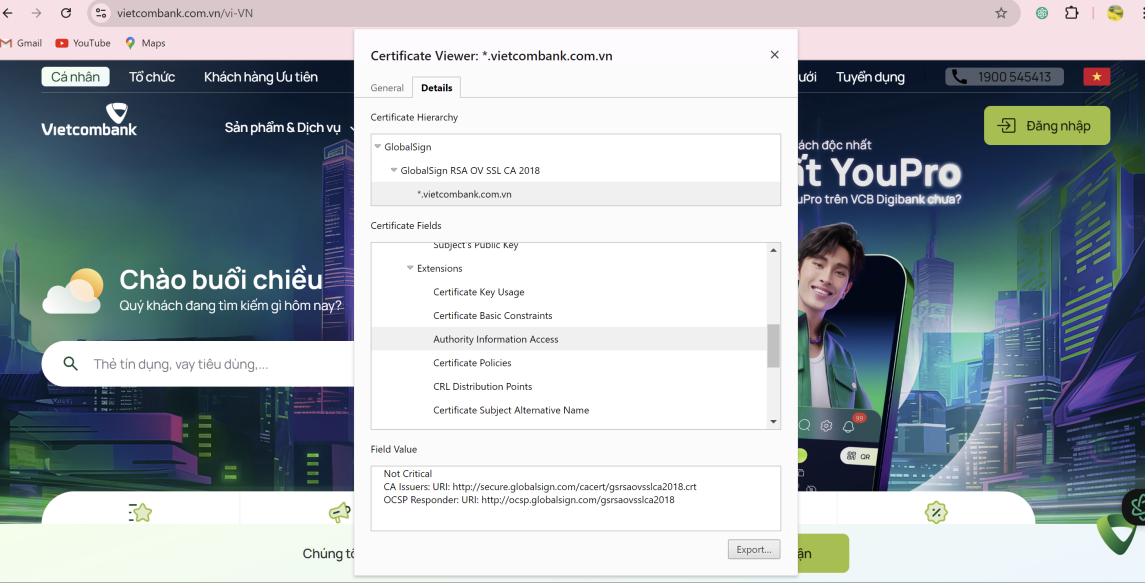
Lê Ngọc Kiều Anh - 22520047

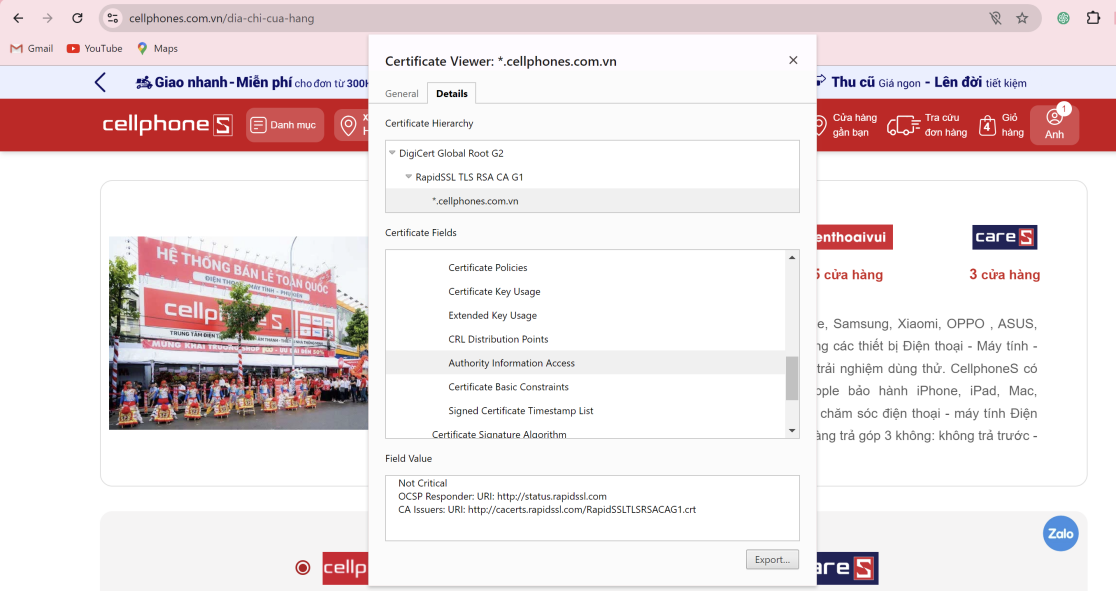
**BÀI TẬP AN TOÀN MẠNG BUỔI 6**

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

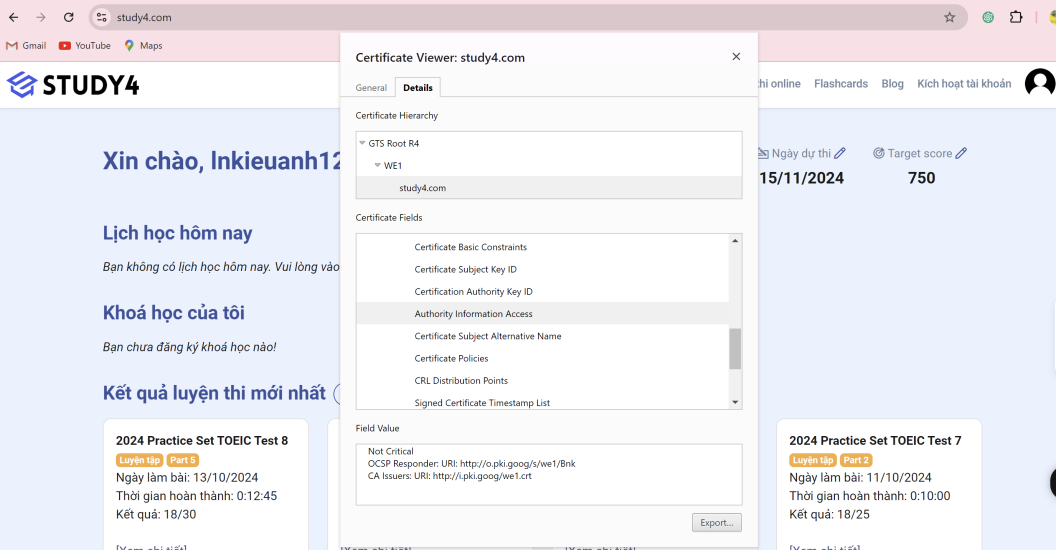
1. Web Vietcombank

****

1. Web CellphoneS



1. Web Study4



**Câu 2. Mô tả quá trình trao đổi khóa của giao thức SSL.**

1. **Client Hello**:  
   Quá trình bắt đầu khi **client** gửi thông điệp **ClientHello** tới **server**. Thông điệp này chứa các thông tin như phiên bản SSL/TLS mà client hỗ trợ và danh sách các **cipher suites** (tổ hợp thuật toán mã hóa) mà nó có thể sử dụng. Ngoài ra, nó gửi các thông số ngẫu nhiên cần thiết cho quá trình trao đổi khóa.
2. **Server Hello**:  
   **Server** phản hồi bằng thông điệp **ServerHello**. Thông điệp này xác nhận phiên bản SSL/TLS sẽ được sử dụng và chọn một bộ mã hóa từ danh sách client đã đề xuất. Đồng thời, nó gửi thêm một giá trị ngẫu nhiên riêng từ server.
3. **Server Certificate**:  
   Server gửi chứng chỉ số của mình cho client. Chứng chỉ này chứa **public key** và được cấp bởi một **Certificate Authority (CA)** đáng tin cậy. **Client** kiểm tra chứng chỉ này để đảm bảo rằng nó hợp lệ và có hiệu lực (chưa hết hạn).
4. **Trao đổi khóa (Key Exchange)**:  
   Client và server tiến hành trao đổi khóa bằng cách sử dụng **public key** từ server. Mục tiêu là tạo ra một **khóa bí mật phiên (session key)** để mã hóa dữ liệu trong suốt phiên giao dịch.
5. **Session Key**:  
   Khóa bí mật (session key) được thiết lập thành công sau khi hoàn tất quá trình trao đổi. Khóa này được cả hai bên sử dụng để mã hóa và giải mã dữ liệu trong suốt phiên.
6. **Lựa chọn Cipher Suite**:  
   Client và server đồng thuận về một bộ **cipher suite** duy nhất. Bộ này bao gồm các thuật toán mã hóa, hàm băm (hash functions), và thuật toán xác thực để đảm bảo tính bảo mật của dữ liệu.
7. **Kết thúc bắt tay (Finish Handshake)**:  
   Sau khi tất cả các thỏa thuận đã hoàn thành, cả client và server gửi thông điệp xác nhận **"Finished"**. Bắt tay kết thúc và từ thời điểm này, dữ liệu trao đổi được mã hóa bởi session key.
8. **Trao đổi dữ liệu an toàn**:  
   Sau khi thiết lập thành công phiên, dữ liệu được mã hóa và truyền giữa hai bên thông qua SSL/TLS.
9. **Khôi phục phiên (Session Resumption)**:  
   Để cải thiện hiệu suất, SSL/TLS cho phép sử dụng lại phiên đã thiết lập trước đó mà không cần trải qua toàn bộ quá trình bắt tay từ đầu.