**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**



**LAB 2:**

***Wireshark HTTP***

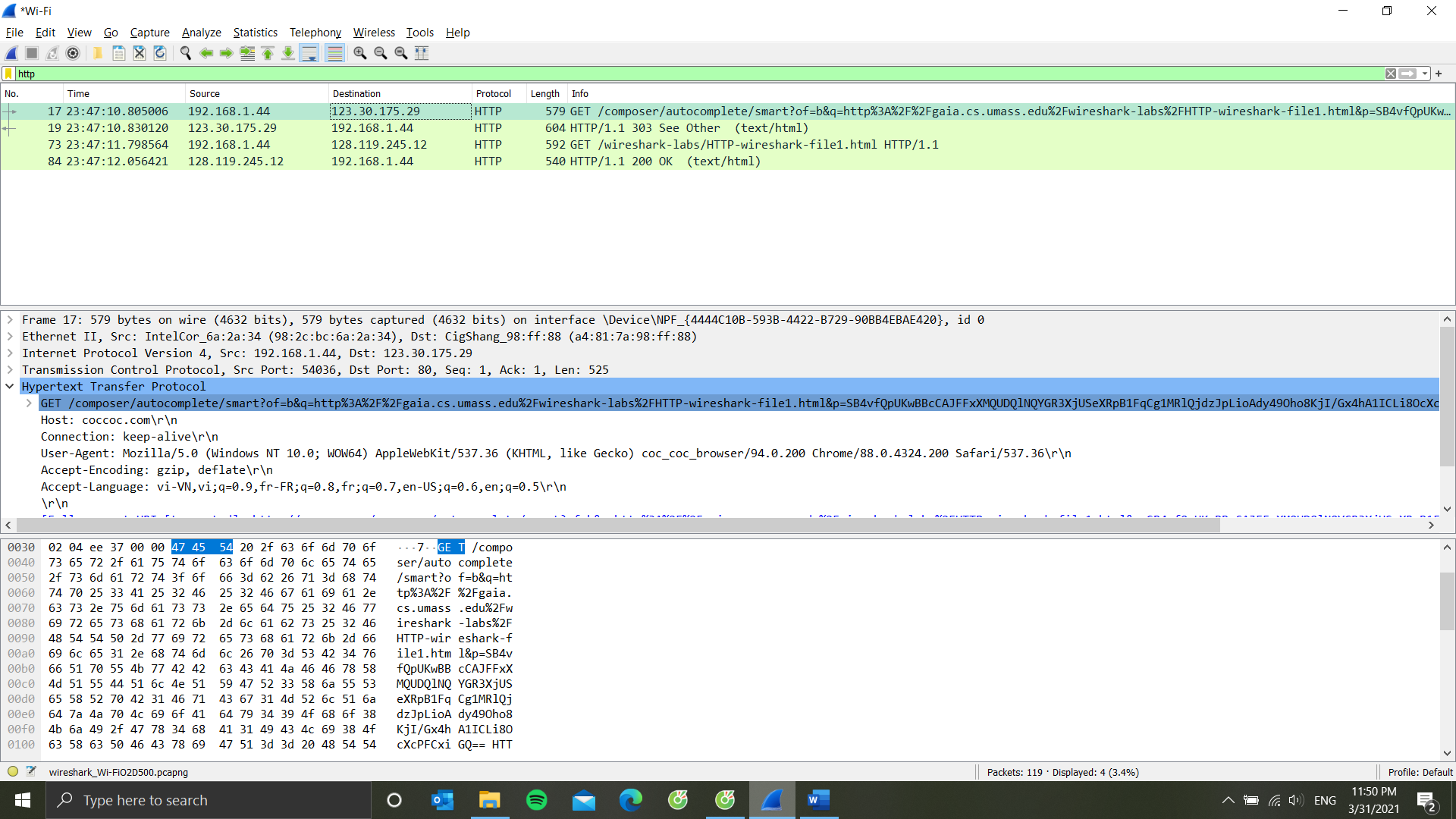
**Môn :** KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

Giảng viên: Sam Nguyen Xuan

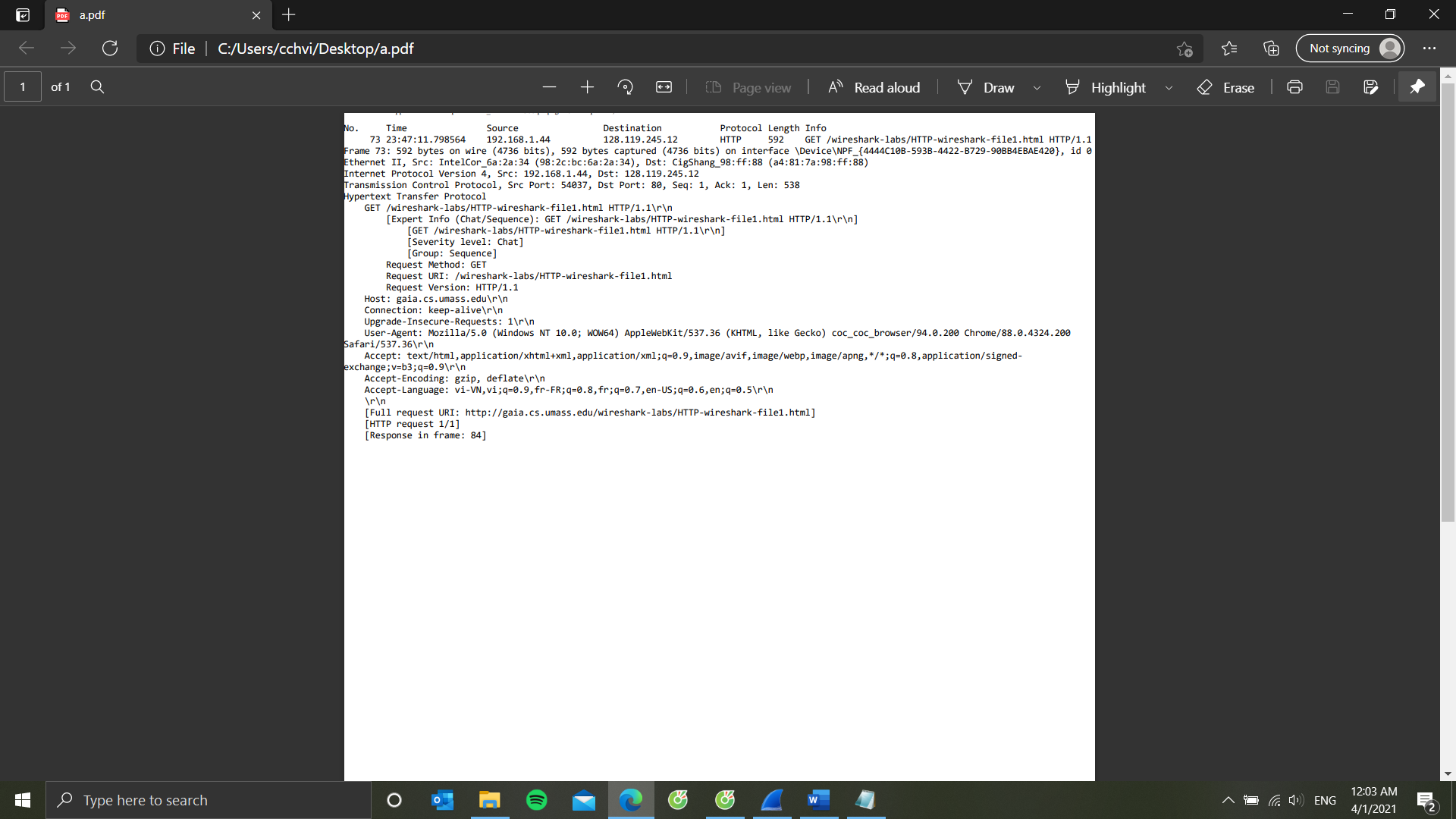
Họ tên: Chế Công Hậu – N17DCAT023

*Ngày 31 tháng 3 năm 2021*

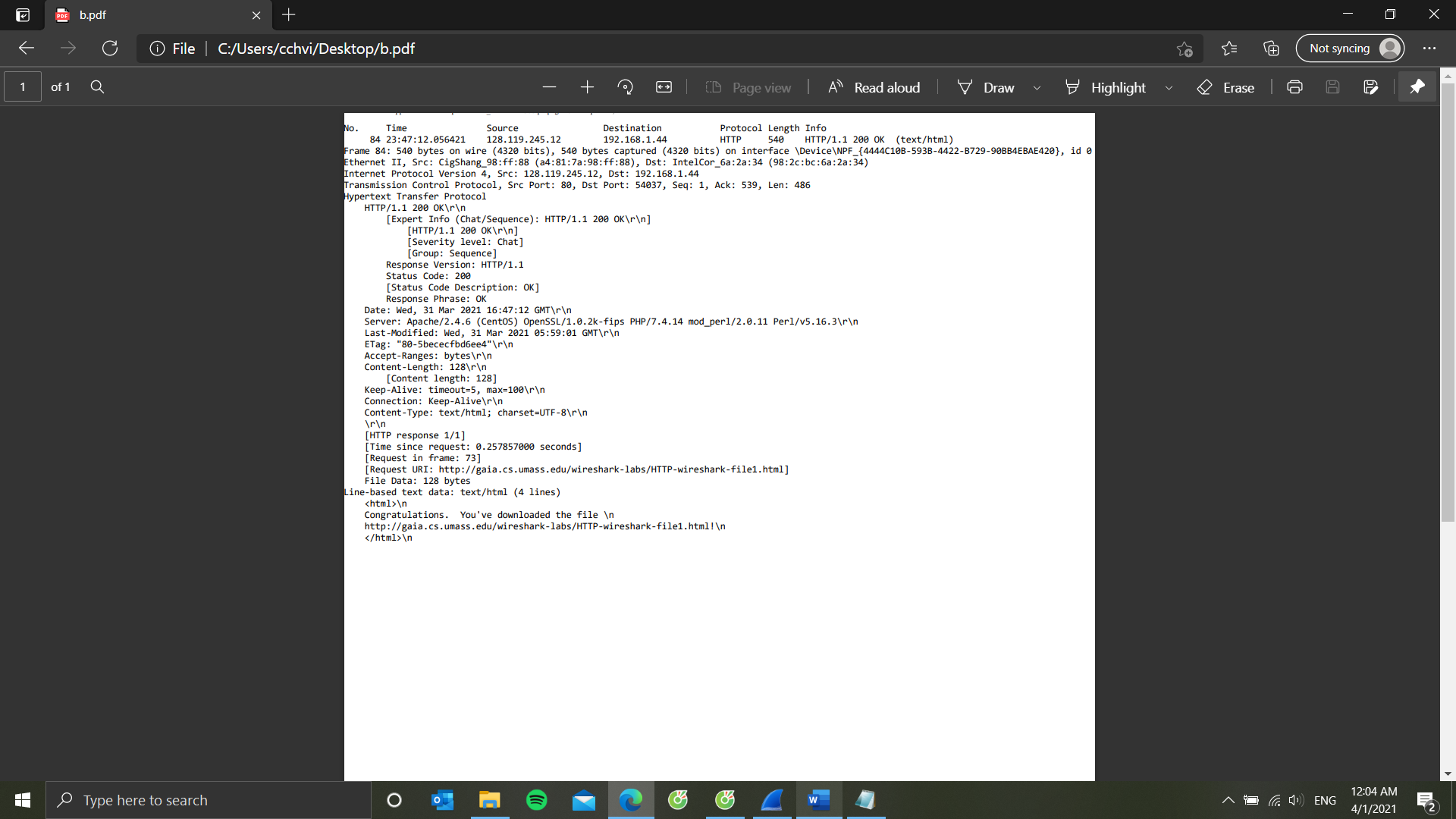
Các gói HTTP bắt được khi truy cập: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>



HTTP GET

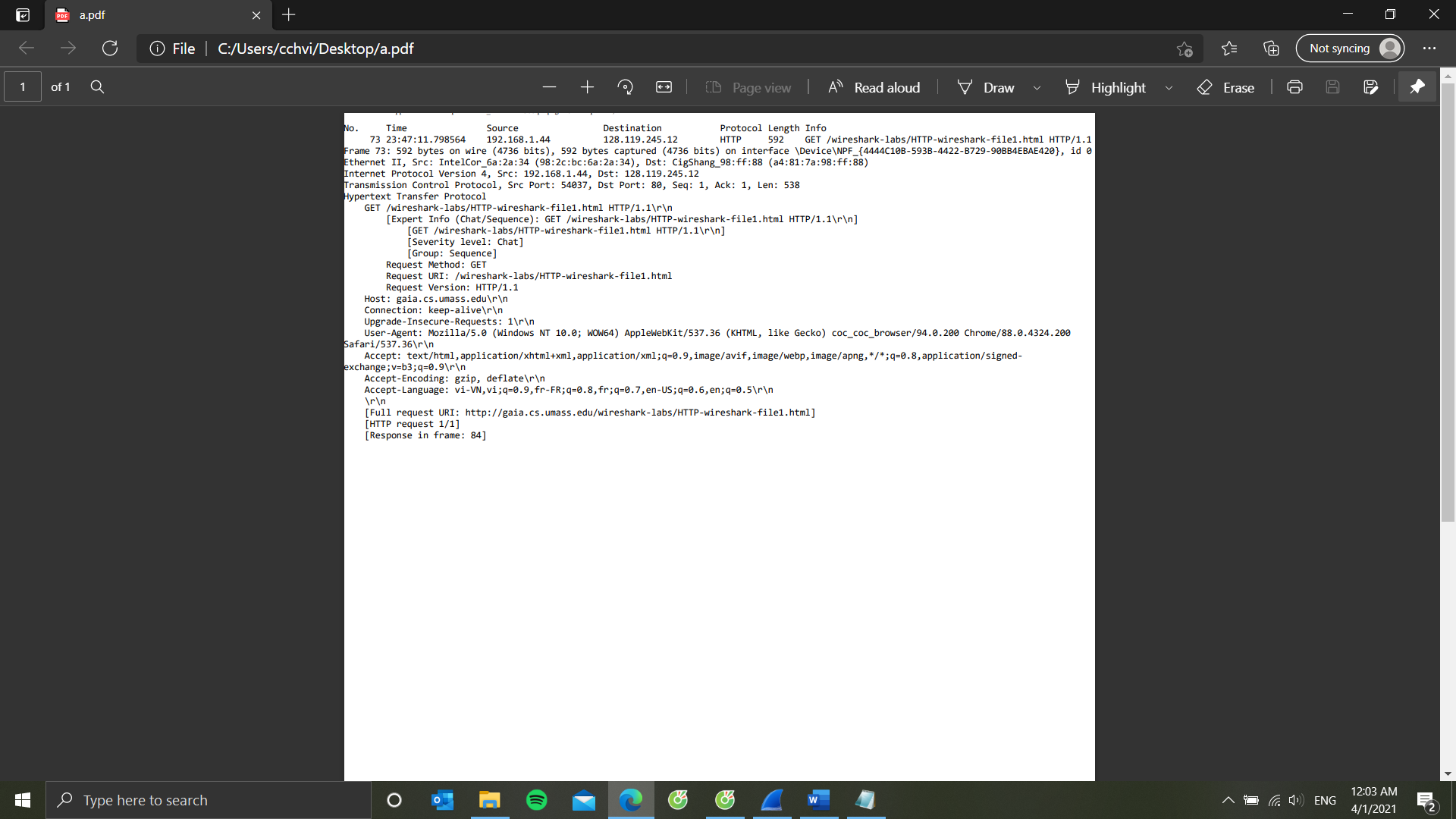


HTTP OK

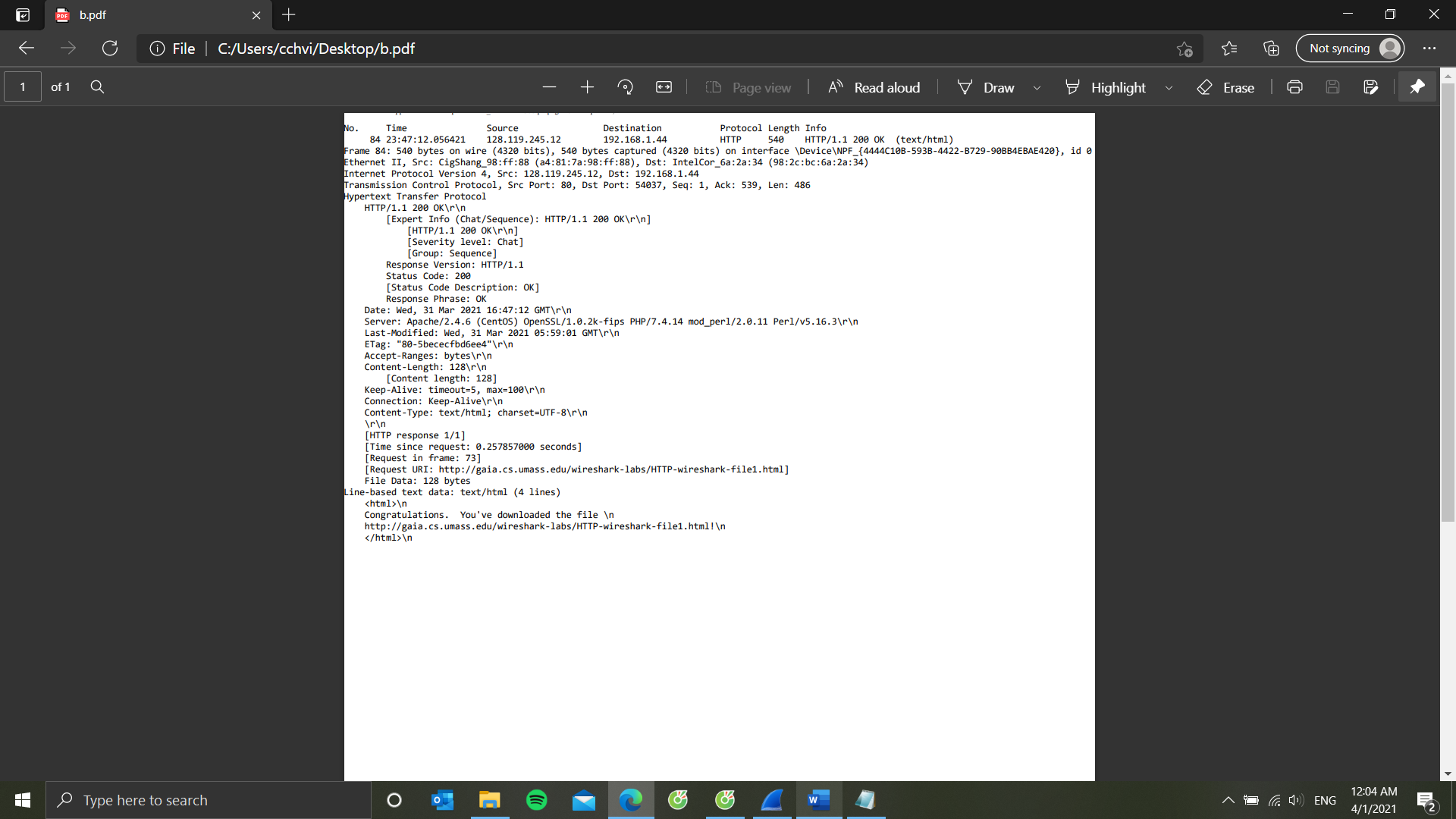


**Trả lời câu hỏi:**

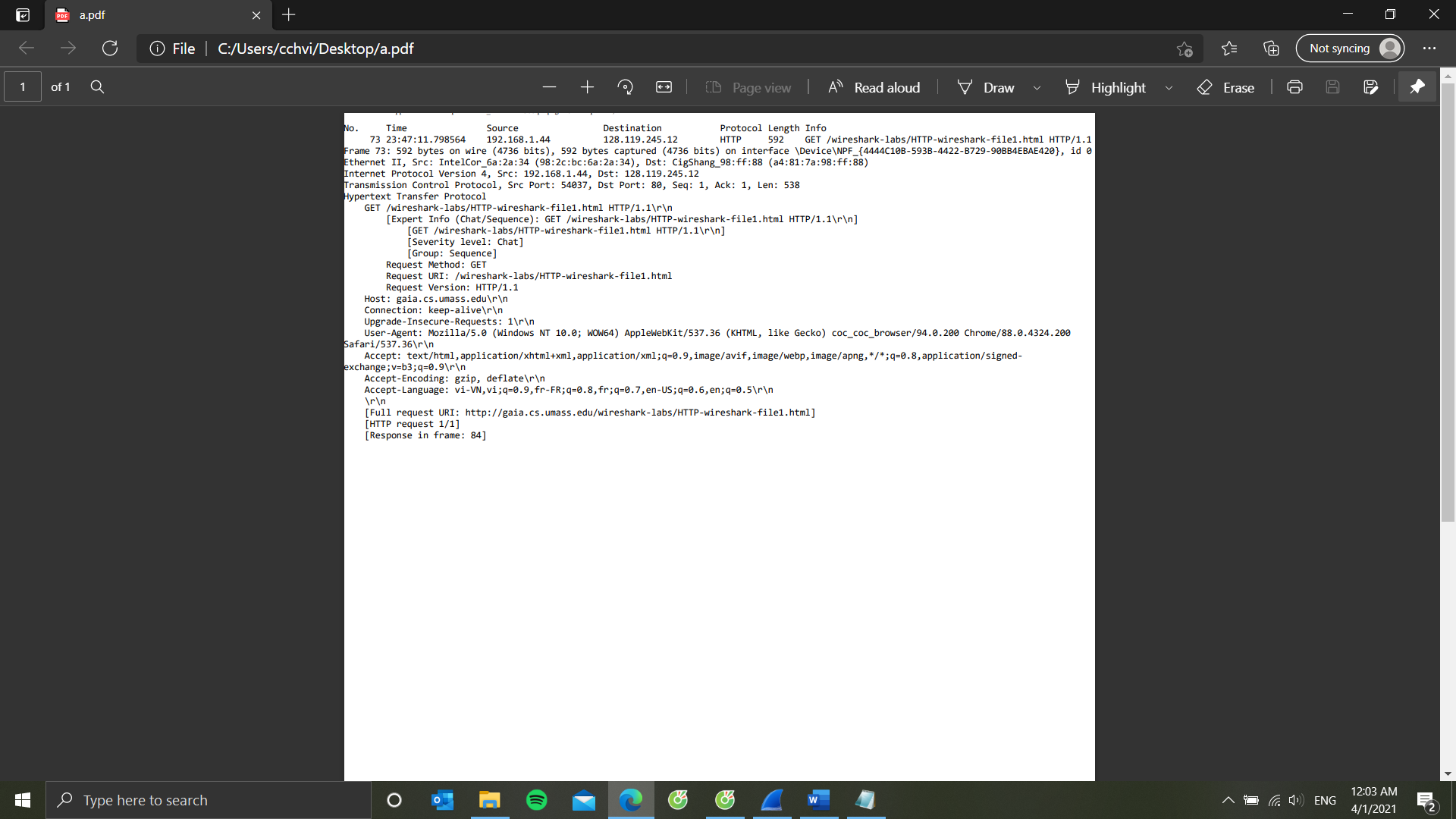
1. **The Basic HTTP GET/response interaction**
2. Trình duyệt đang chạy phiên bản HTTP 1.1.



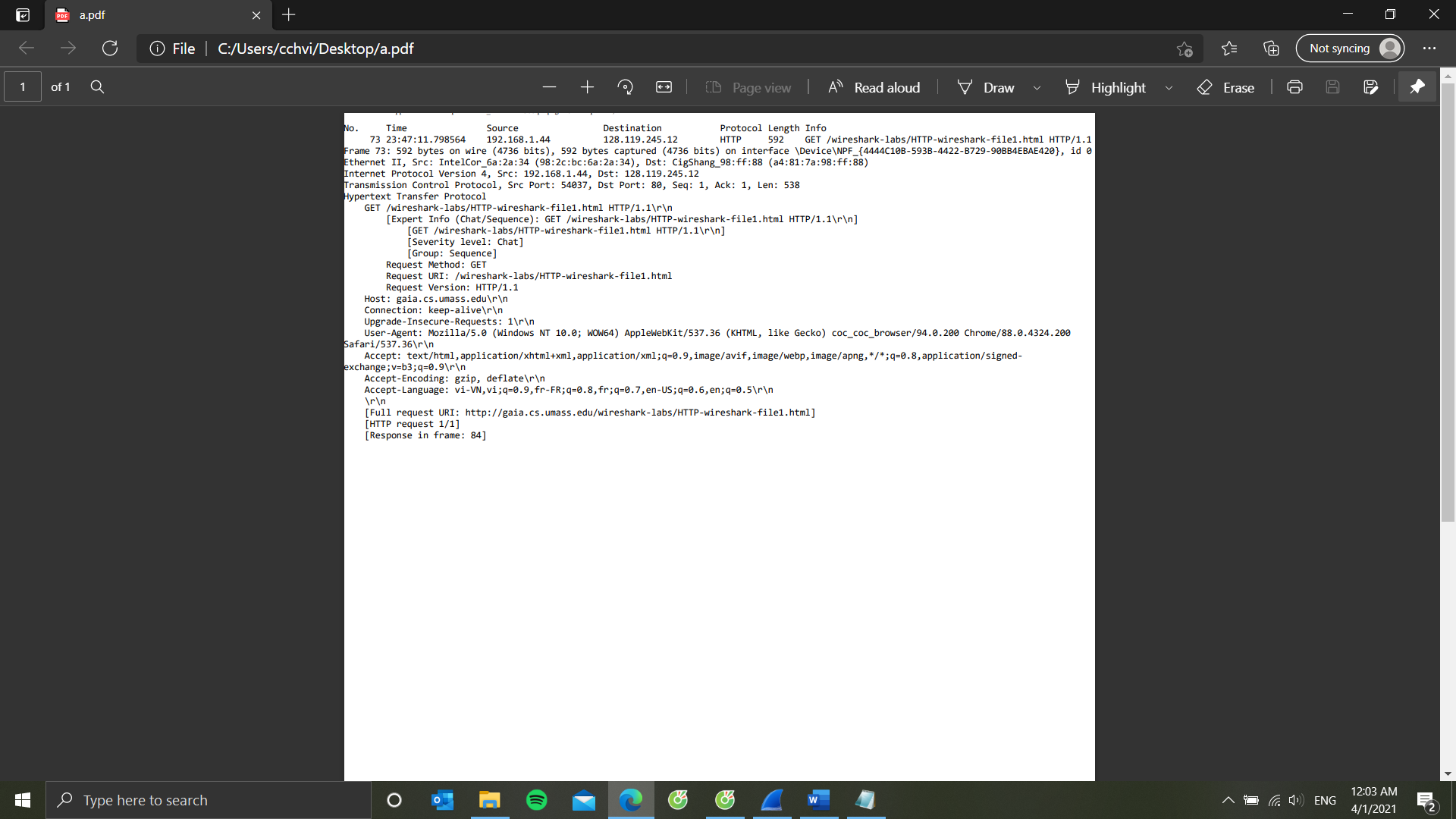
Phiên bản HTTP của server: 1.1.



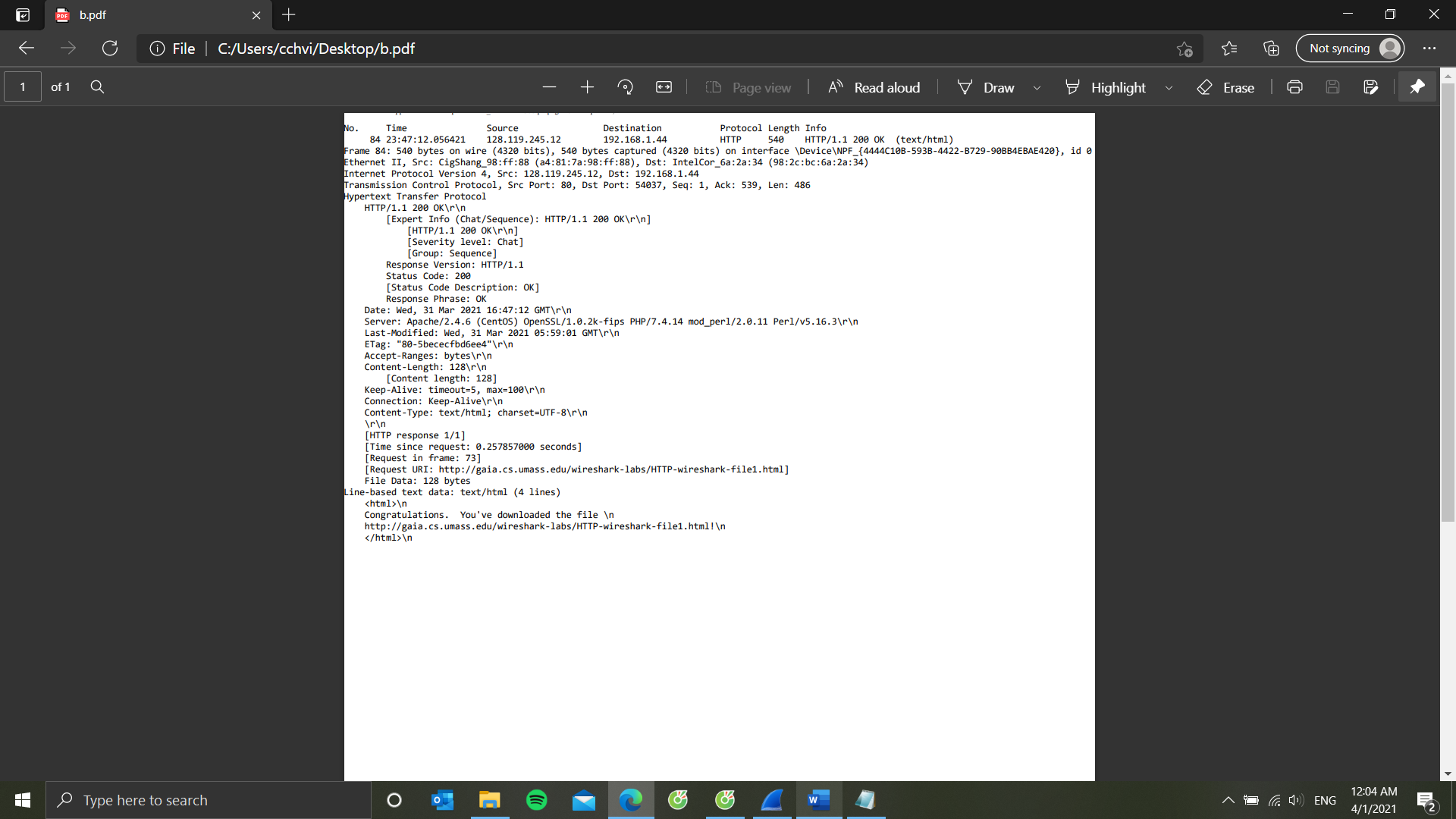
1. Những ngôn ngữ nào (nếu có) mà trình duyệt cho phép sử dụng ở máy chủ?



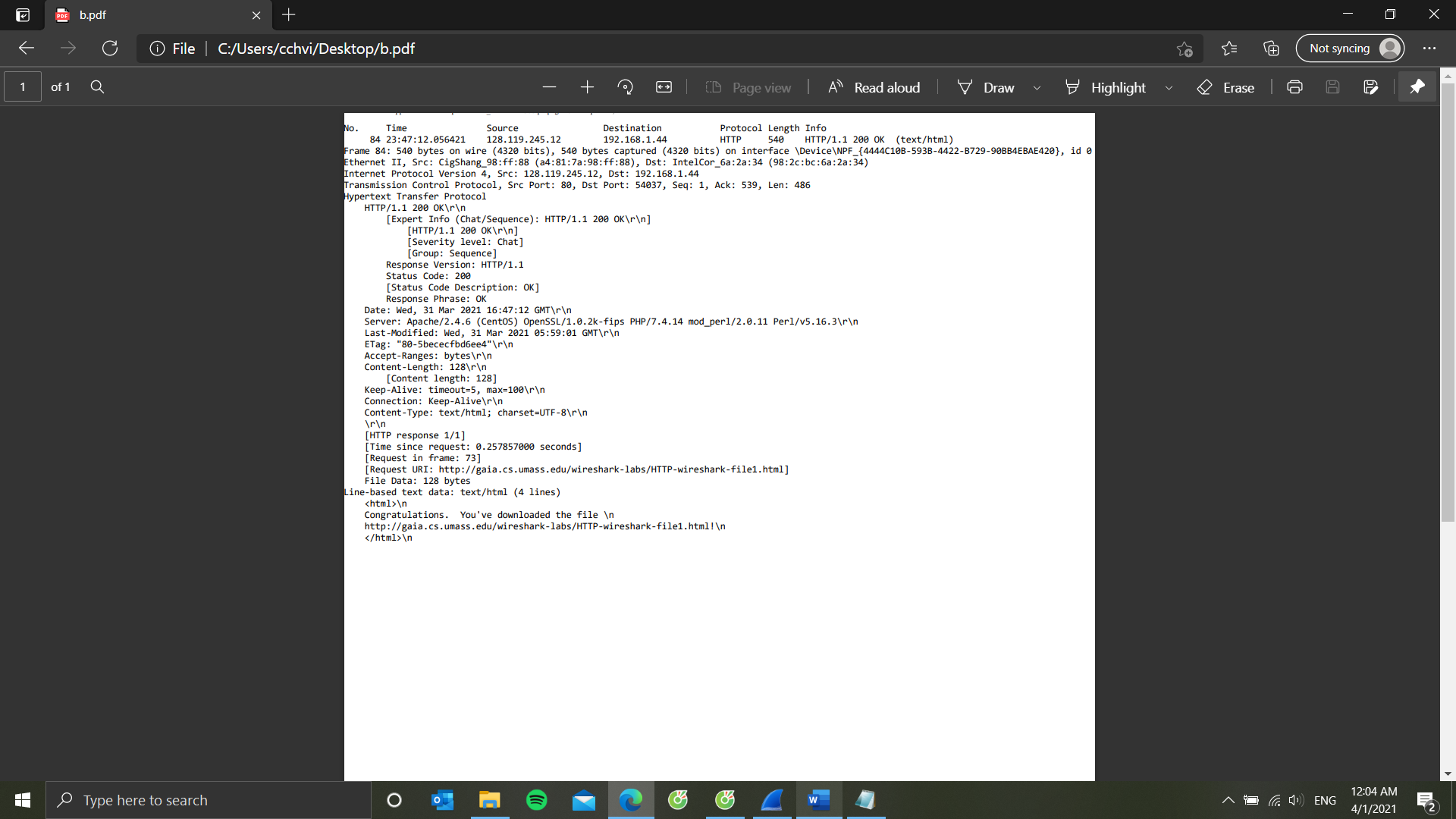
1. Địa chỉ IP của máy tính: 192.168.1.44 . Địa chỉ IP của gaia.cs.umass.edu server: 128.119.245.12 .



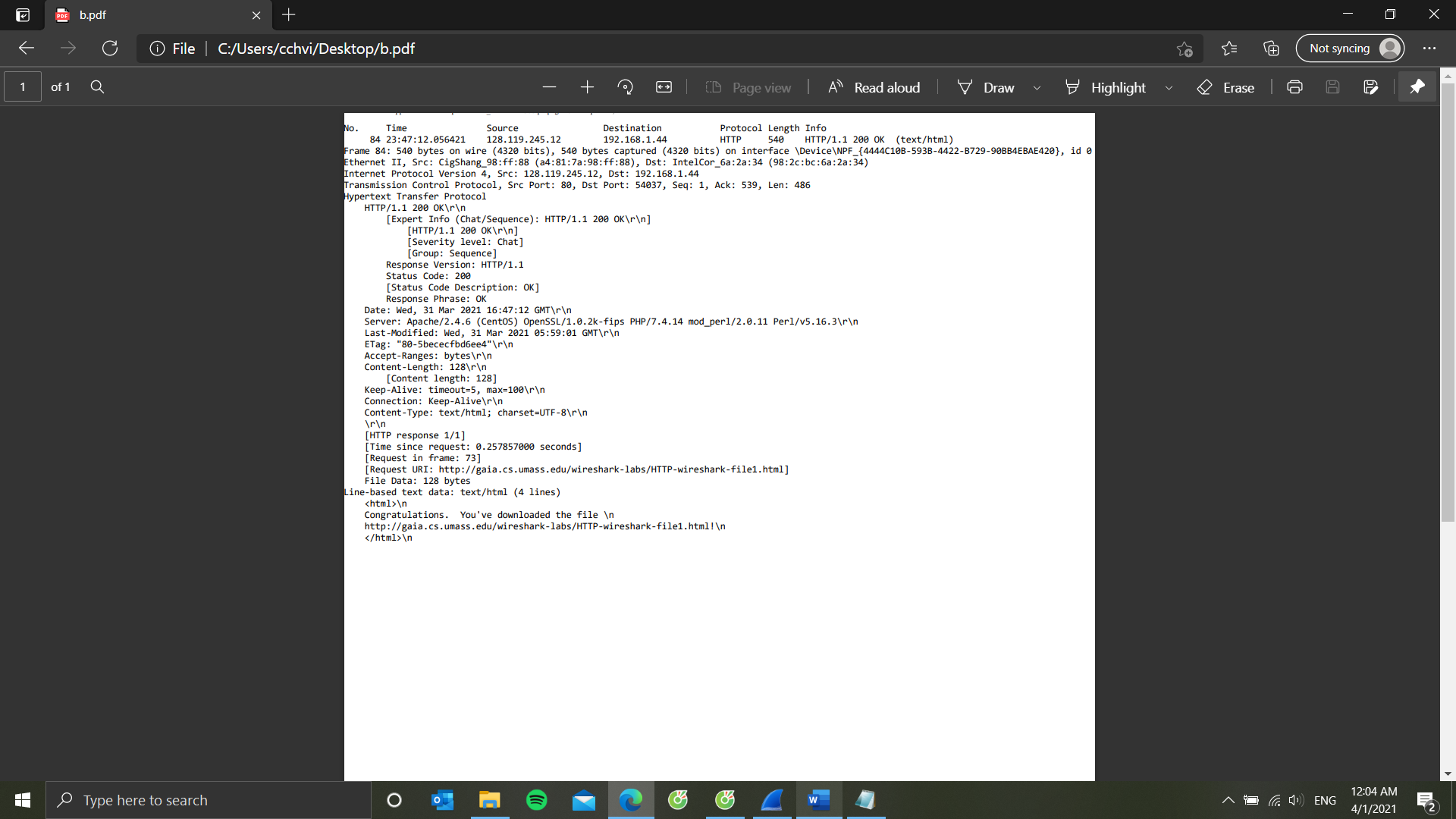
1. Status code được trả về từ máy chủ đến trình duyệt: 200



1. Tệp HTML được sửa đổi lần cuối tại máy chủ: 05:59:01 GMT thứ tư, 31/03/2021.

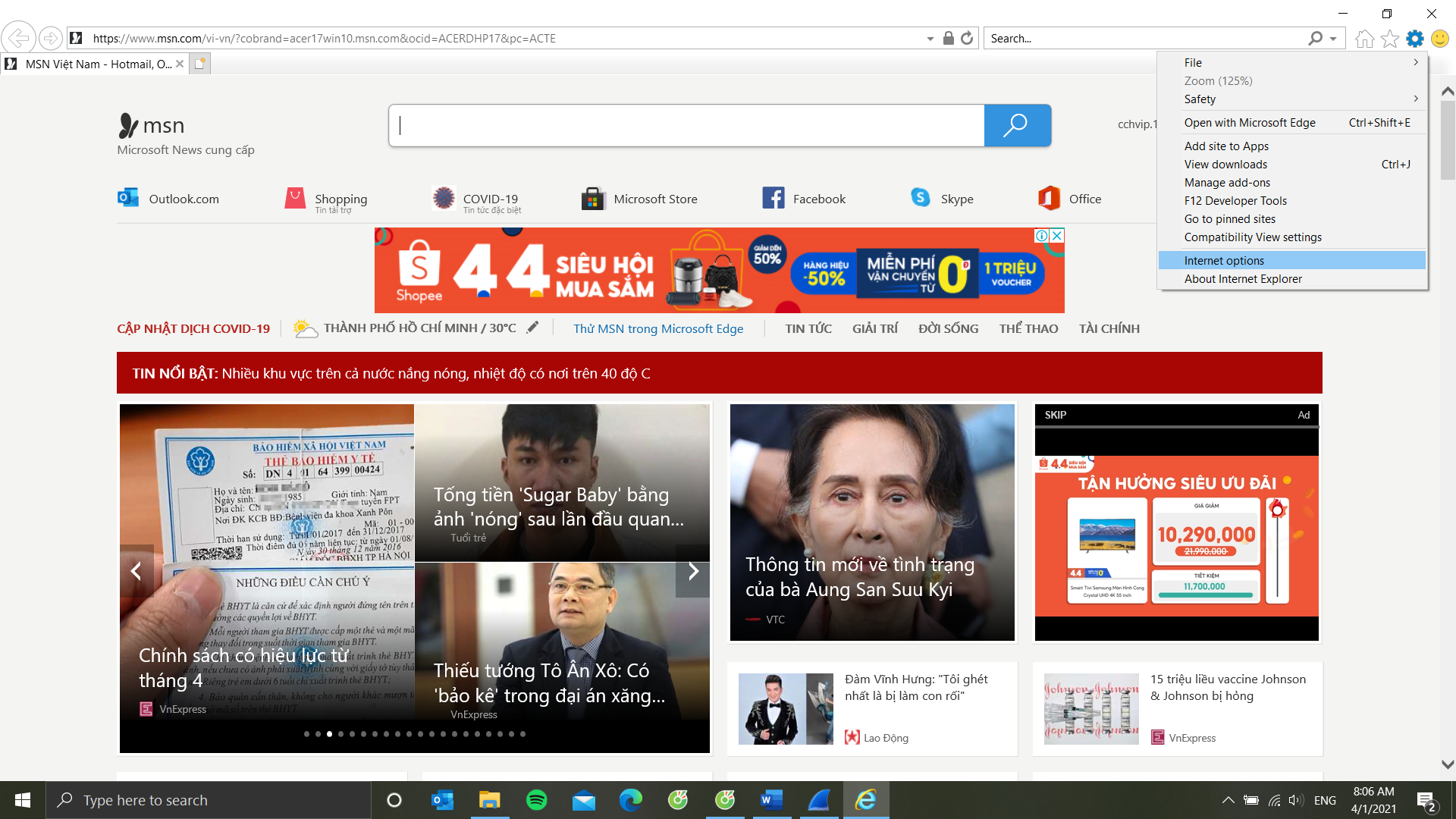


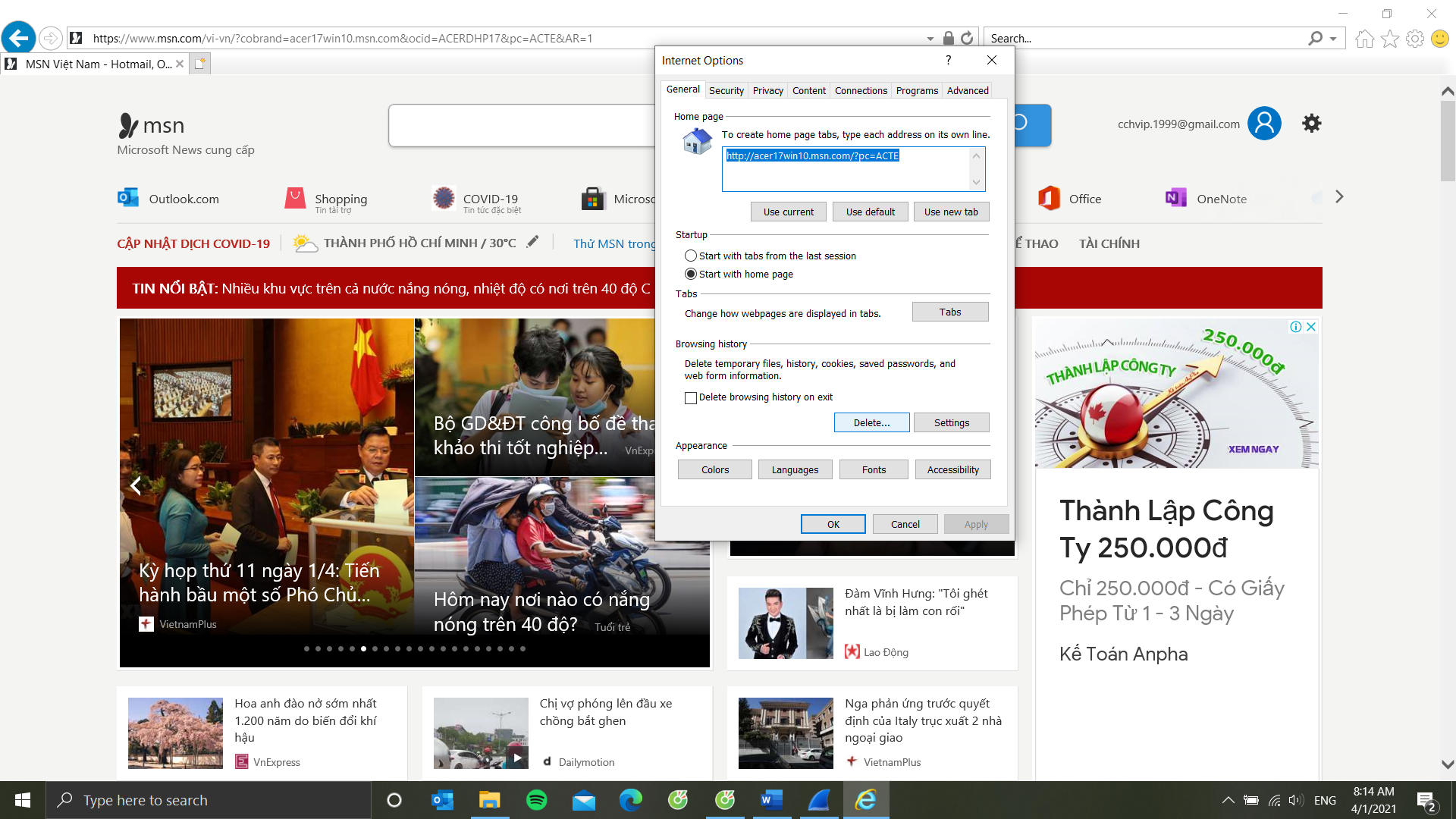
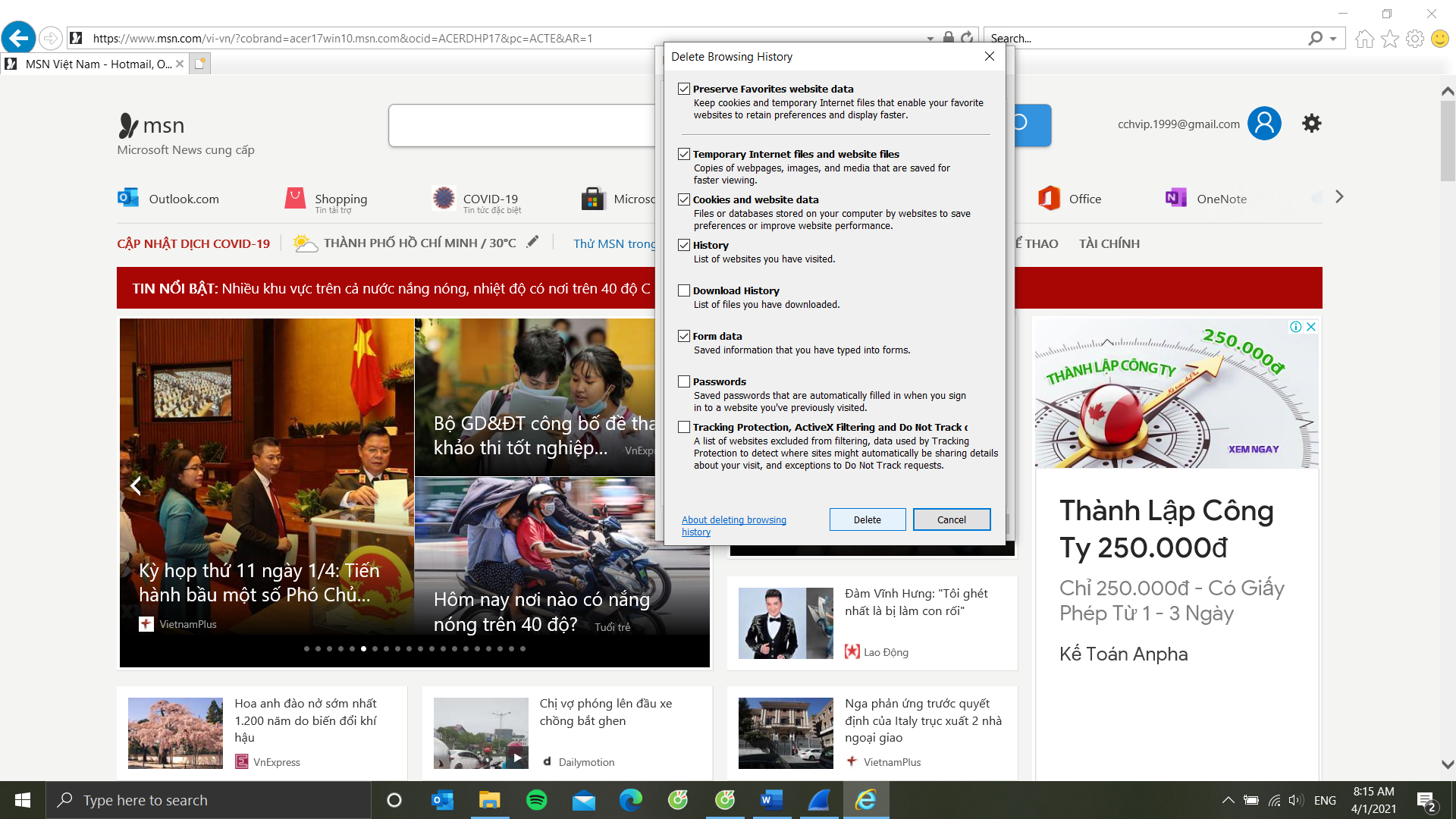
1. Có bao nhiêu byte nội dung đang được trả về trình duyệt: 128.



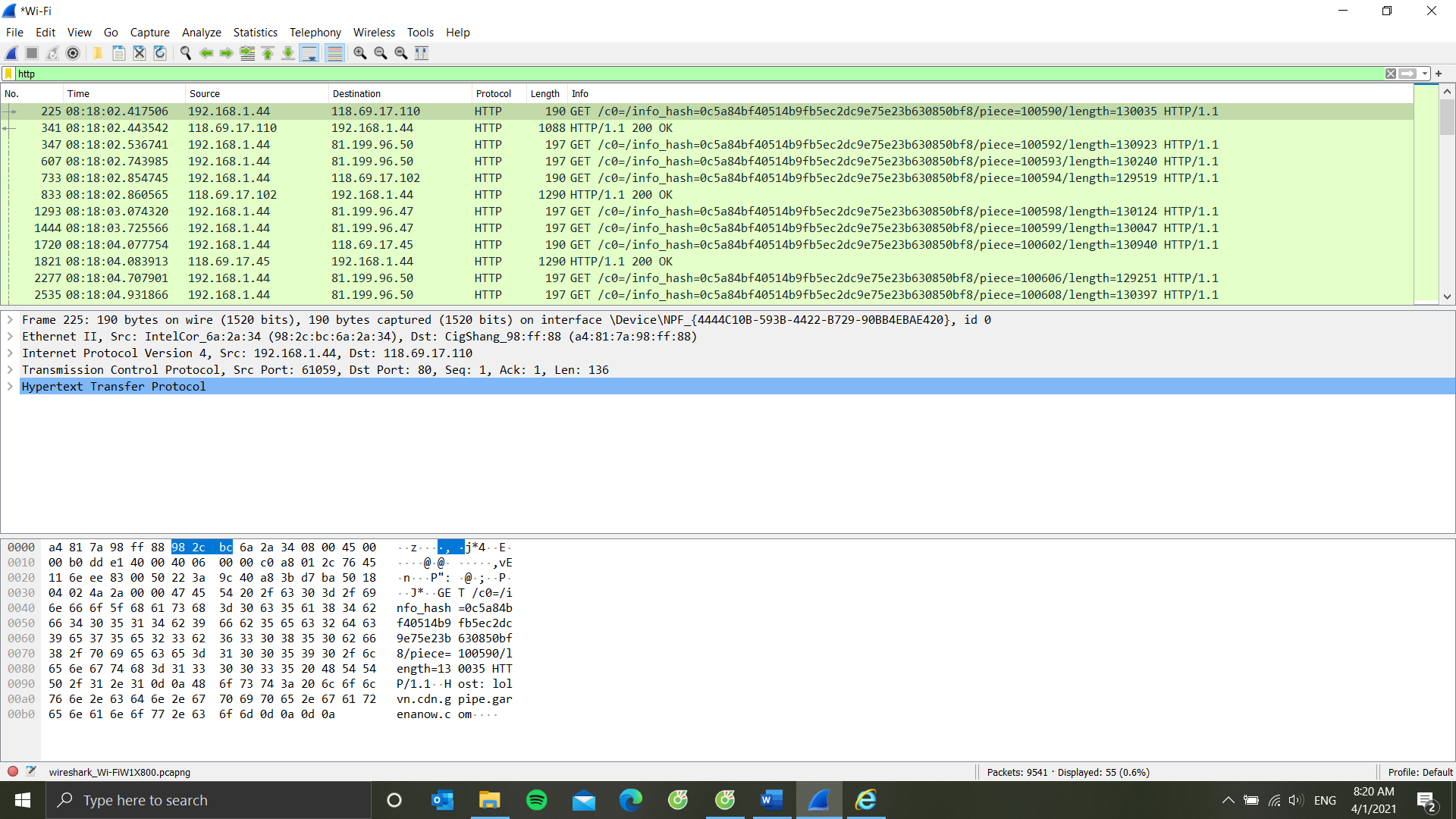
1. Không thấy tiêu đề nào trong dữ liệu không được hiển thị trong cửa sổ liệt kê gói.
2. **The HTTP CONDITIONAL GET/response interaction**

Sẽ sử dụng Internet Explorer để truy cập vào url: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> nhưng trước hết cần phải xóa bộ nhớ đệm của trình duyệt.



Truy cập vào: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> sau đó refresh lại trang. Các gói bắt được ở Wireshark:



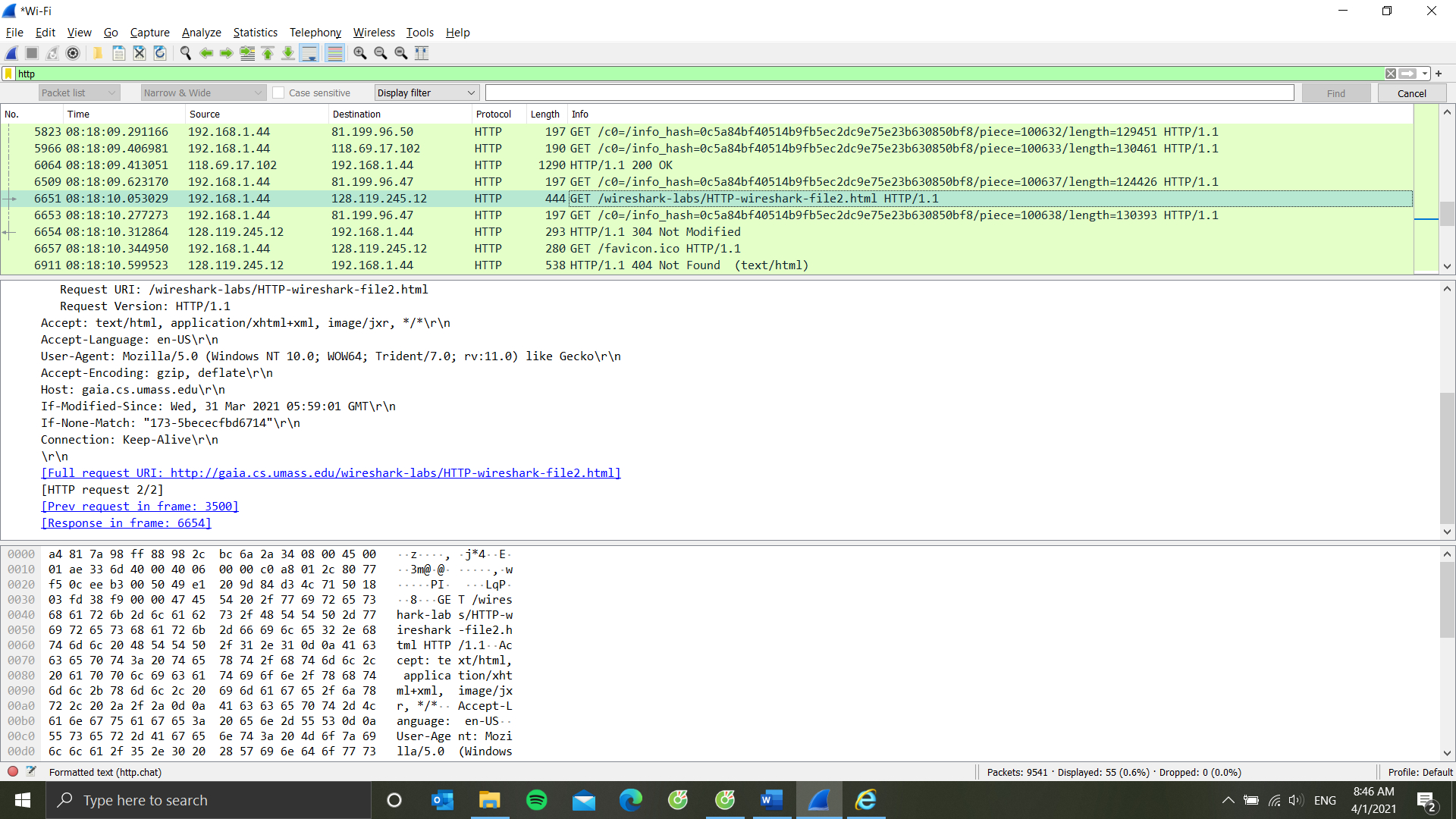
1. Kiểm tra nội dung của yêu cầu HTTP GET đầu tiên từ trình duyệt đến máy chủ. Có thấy dòng “IF-MODIFIED-SINCE” trong HTTP GET không? Trả lời : không thấy.
2. Kiểm tra nội dung phản hồi của máy chủ. Máy chủ có trả về nội dung của tệp một cách rõ ràng không? Làm thế nào để biết?

Trả lời : có trả về nội dung một cách rõ ràng, dựa vào Content length: 371 và nội dung trang đọc được rõ ràng.



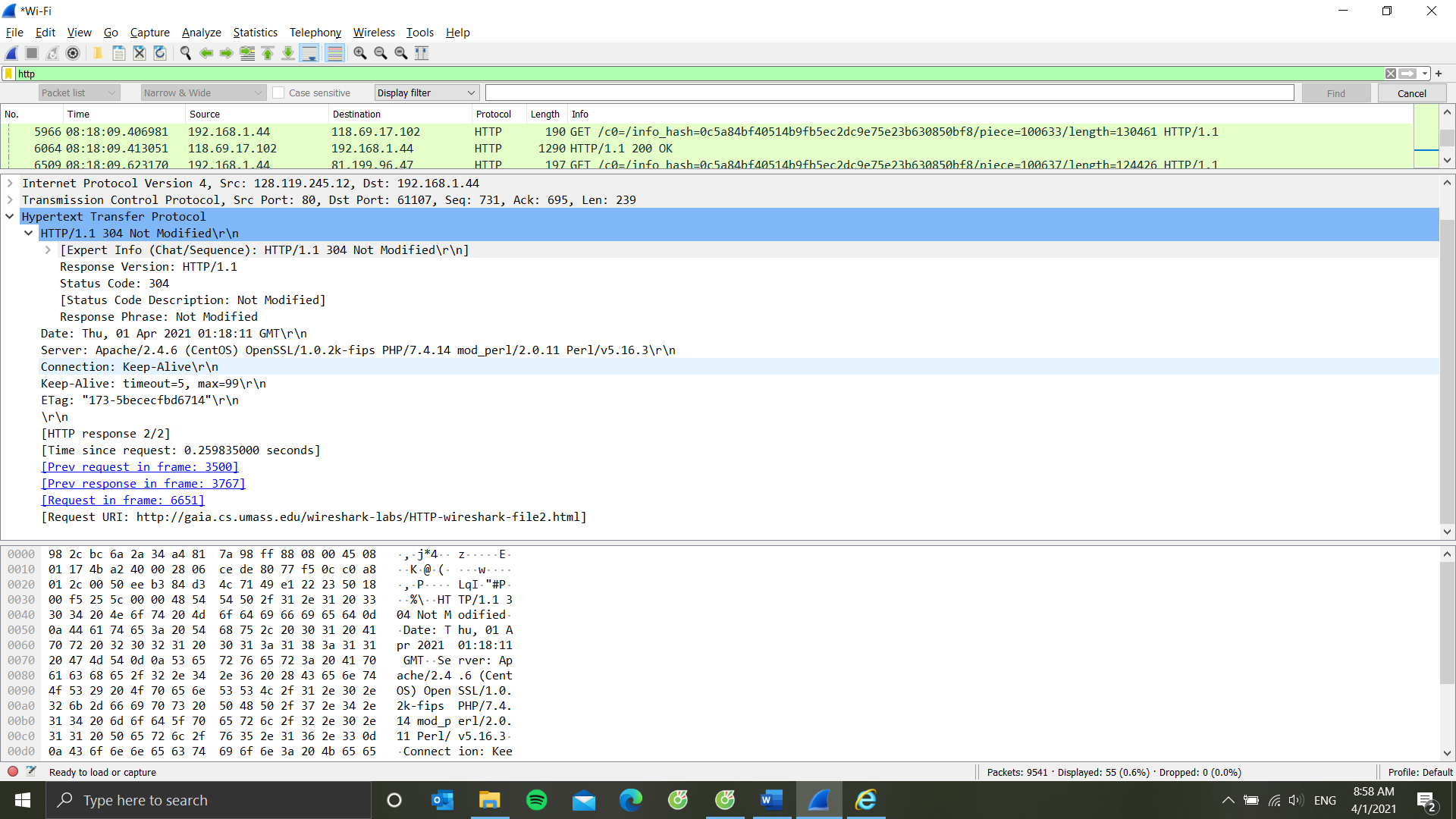
1. Kiểm tra nội dung của yêu cầu HTTP GET thứ hai từ trình duyệt đến máy chủ. Có thấy dòng “IF-MODIFIED-SINCE:” trong HTTP GET không? Nếu có, thông tin nào sau tiêu đề “IF-MODIFIED-SINCE:”?

Trả lời: Có thấy dòng “IF-MODIFIED-SINCE:”. Thông tin : Wed, 31 Mar 2021 05:59:01 GMT.



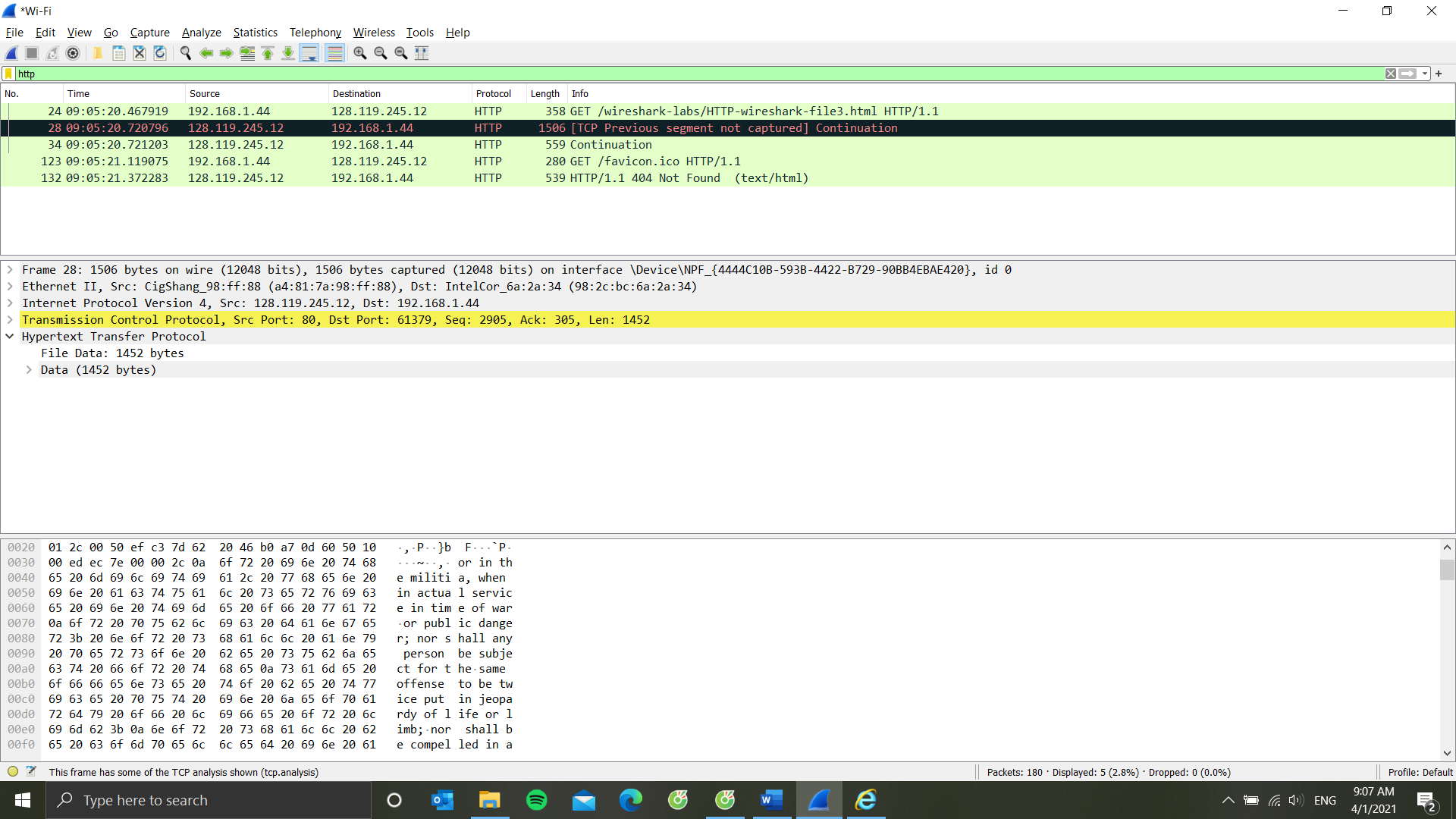
1. HTTP status code và phrase được trả về từ máy chủ để phản hồi HTTP GET thứ hai này là gì? Máy chủ có trả về nội dung của tệp một cách rõ ràng không? Giải thích.

Trả lời : HTTP status code – 304, phrase – Not Modified. Máy chủ không trả về nội dung một cách rõ ràng. Vì nội dung của trang đã được lưu vào cache của trình duyệt khi HTTP get ở lần đầu nên máy chủ chỉ cần lấy từ cache của trình duyệt.



1. **Retrieving Long Documents**

Xóa bộ nhớ đệm (cache) của trình duyệt, sau đó truy cập vào: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>. Wireshark :



1. Trình duyệt đã gửi bao nhiêu thông báo yêu cầu HTTP GET? Số packet nào chứa thông điệp GET cho the Bill or Rights?

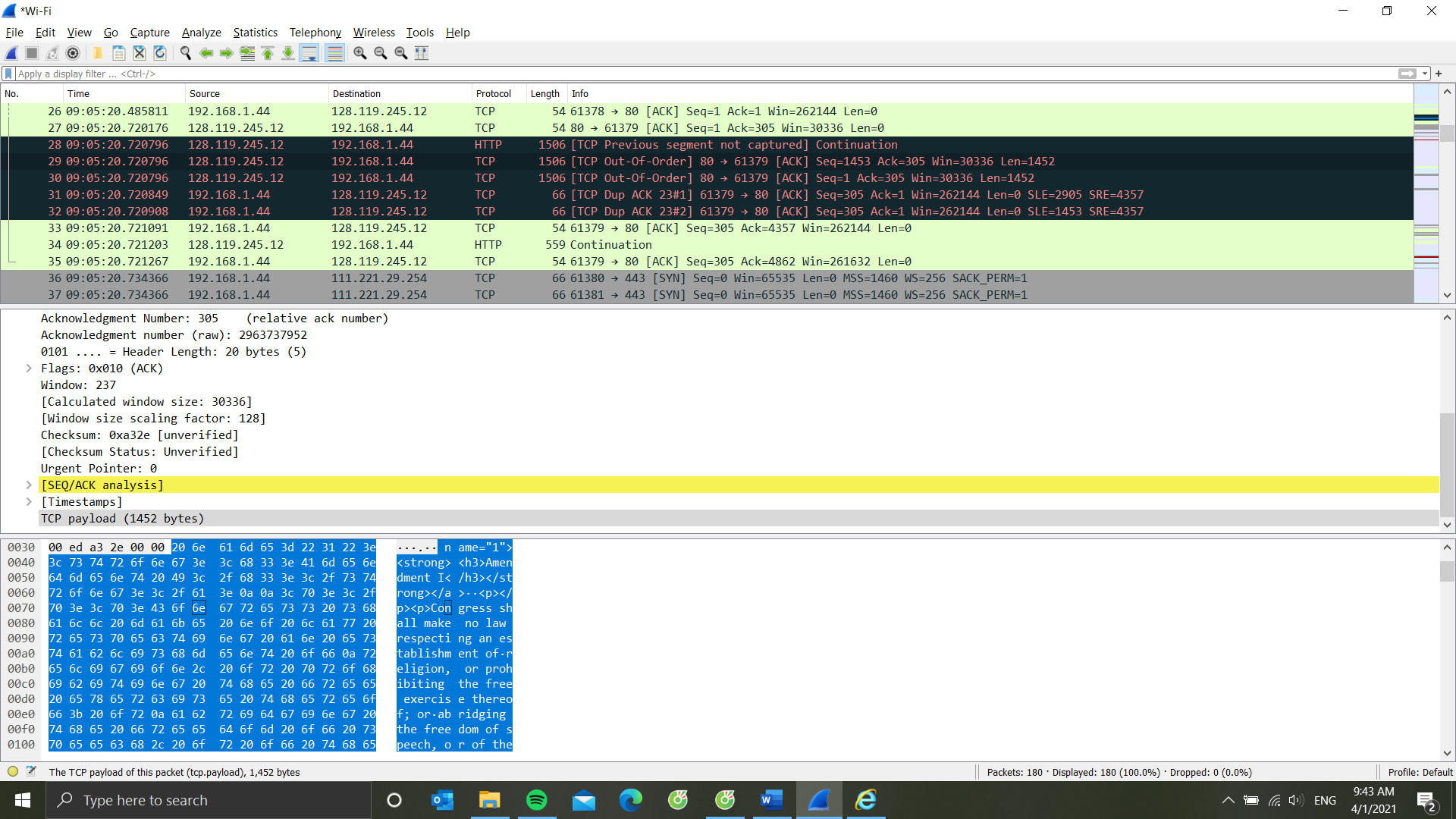
Trả lời : đã gửi hai HTTP GET. Số packet trong hình chứa thông điệp GET cho the Bill or Rights : là gói số 28.

1. Số packet nào chứa status code và phrase được liên kết với phản hồi cho yêu cầu HTTP GET?

Trả lời : không có packet nào.

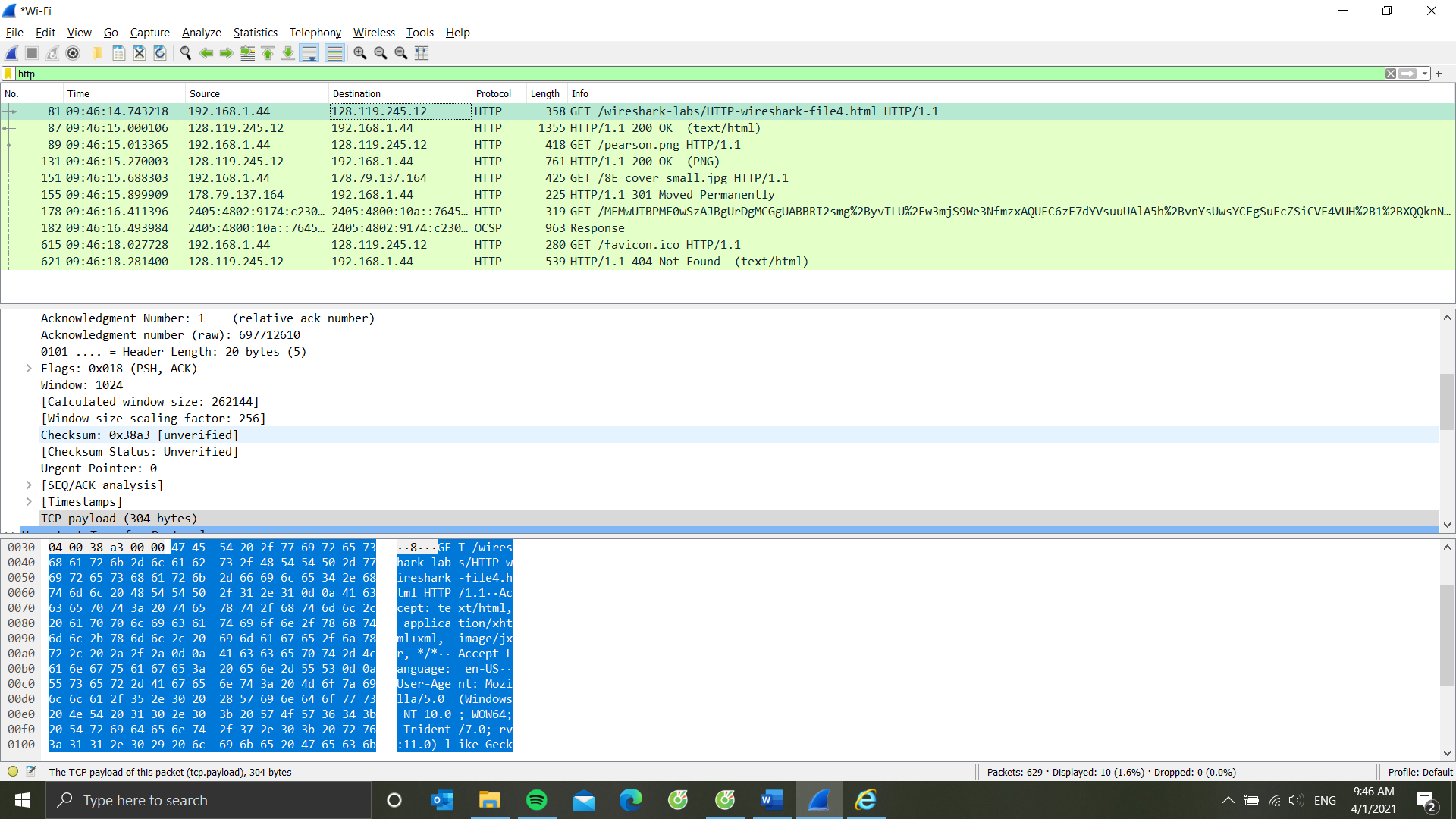
1. Status code và phrase đó là gì? ---- Không thấy.
2. Cần bao nhiêu phân đoạn TCP chứa dữ liệu để thực hiện?

Trả lời : cần 2 phân đoạn TCP có chứa dữ liệu.



1. **HTML Documents with Embedded Objects**

Xóa cache của trình duyệt. Truy cập <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> . Wireshark :



1. Trình duyệt đã gửi bao nhiêu thông báo yêu cầu HTTP GET? Những yêu cầu GET này đã được gửi đến những địa chỉ Internet nào?

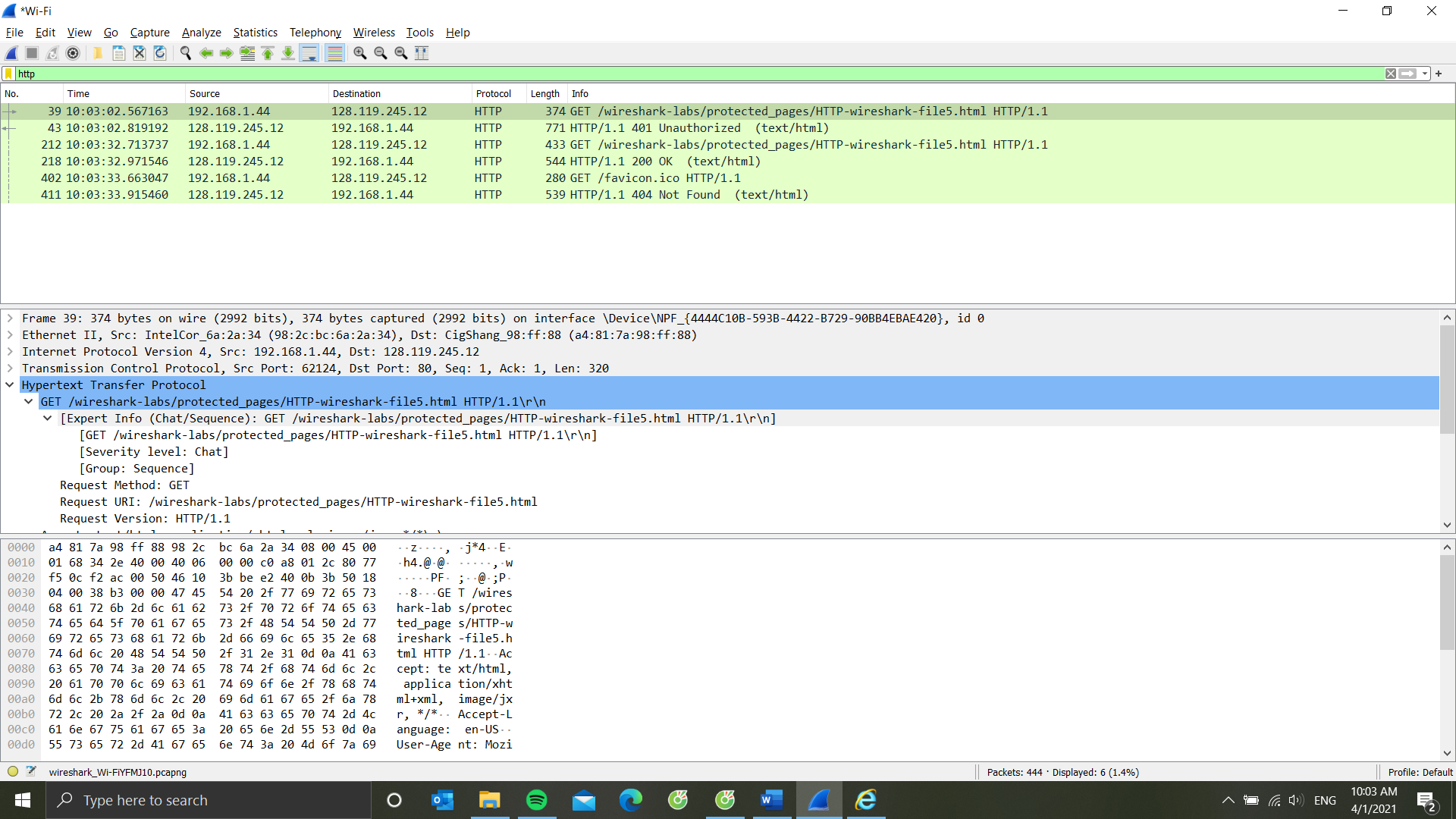
Trả lời : đã gửi bốn HTTP GET (không tính HTTP GET /favicon.ico). Đã gửi đến <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>, <http://gaia.cs.umass.edu/pearson.png>, <http://kurose.cslash.net/8E_cover_small.jpg>, <http://r3.o.lencr.org/MFMwUTBPME0wSzAJBgUrDgMCGgUABBRI2smg%2ByvTLU%2Fw3mjS9We3NfmzxAQUFC6zF7dYVsuuUAlA5h%2BvnYsUwsYCEgSuFcZSiCVF4VUH%2B1%2BXQQknNA%3D%3D>.

1. Có thể biết liệu trình duyệt đã tải xuống hai hình ảnh nối tiếp nhau hay chúng được tải xuống từ hai trang web song song? Giải thích.

Trả lời : được tải xuống từ hai trang web song song. Một ảnh được lấy từ trang web gaia.cs.umass.edu. Một ảnh lấy từ trang web <http://kurose.cslash.net/8E_cover_small.jpg>.

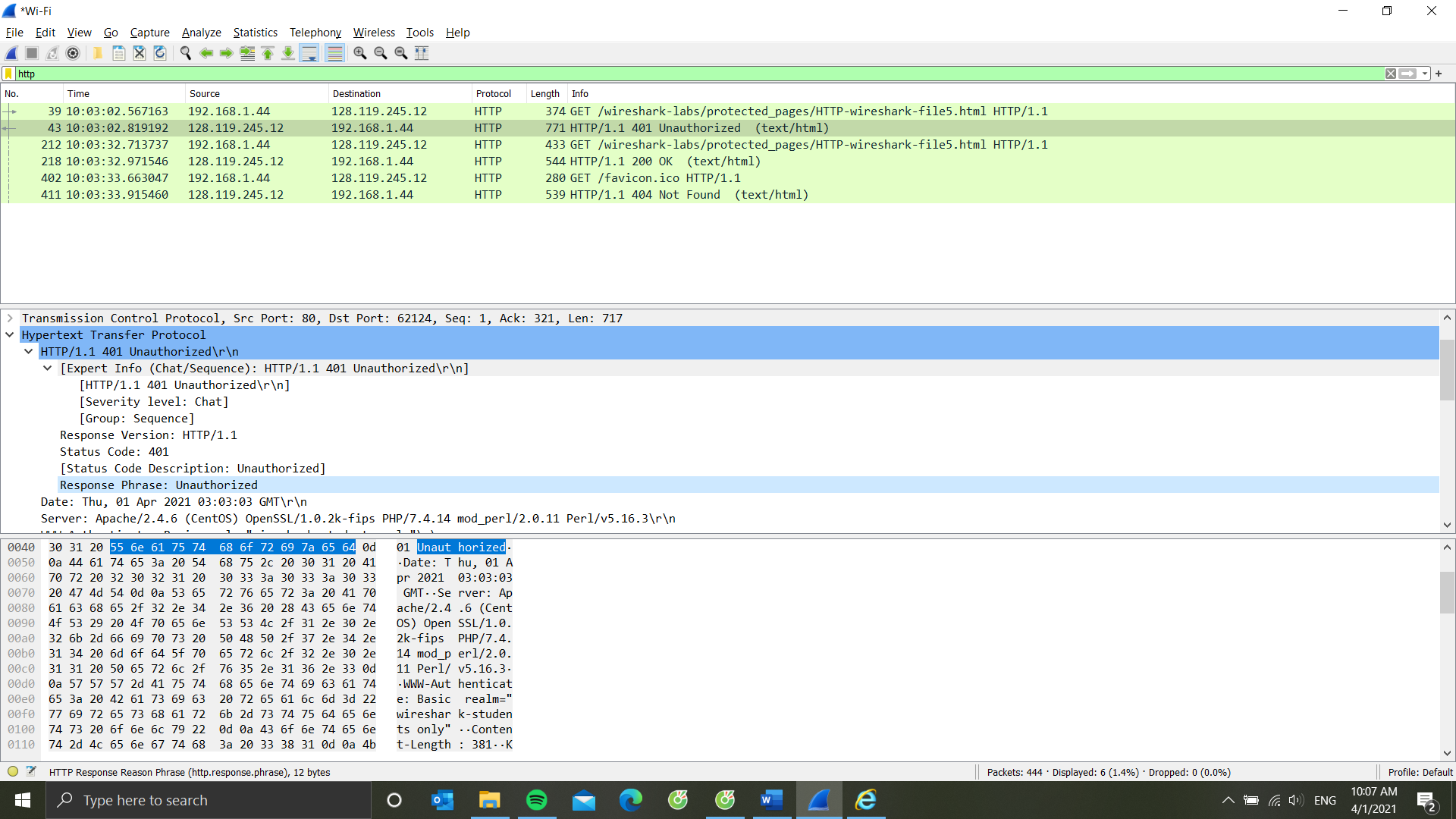
1. **HTTP Authentication**

Xóa cache của trình duyệt. Tắt và mở lại trình duyệt. Truy cập : <http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html>. Nhập username : wireshark-students, password : network. Wireshark :



1. Phản hồi của máy chủ (status code và phrase) phản hồi lại thông báo HTTP GET ban đầu từ trình duyệt là gì?

Trả lời : Status code – 401 , Phrase – Unauthorized.



1. Khi trình duyệt gửi thông báo HTTP GET lần thứ hai, field mới nào sẽ được đưa vào thông báo HTTP GET?

Trả lời : đó là field Authorization: Basic

