INTRODUCTION TO INTERNET PROGRAMMING

ROWLAND DANJI

C024/401455/2023

ASSIGNMENT 2: ANALYZING HTTP HEADERS

a) Use a network packet sniffer (Wireshark or equivalent) to analyze HTTP headers.
b) Capture an HTTP GET and POST request.
c) Identify:
1) Request and response headers.
2) MIME type of the response.
3) HTTP status code and explanation.
Submit a detailed report with screenshots.

Introduction

This report uses Wireshark to capture and analyse an HTTP GET and POST request in order to analyse HTTP headers. The experiment, which was carried out on February 26, 2025, uses screenshots to identify the MIME types, HTTP status codes, and request and response headers for interactions with vbsca.ca.

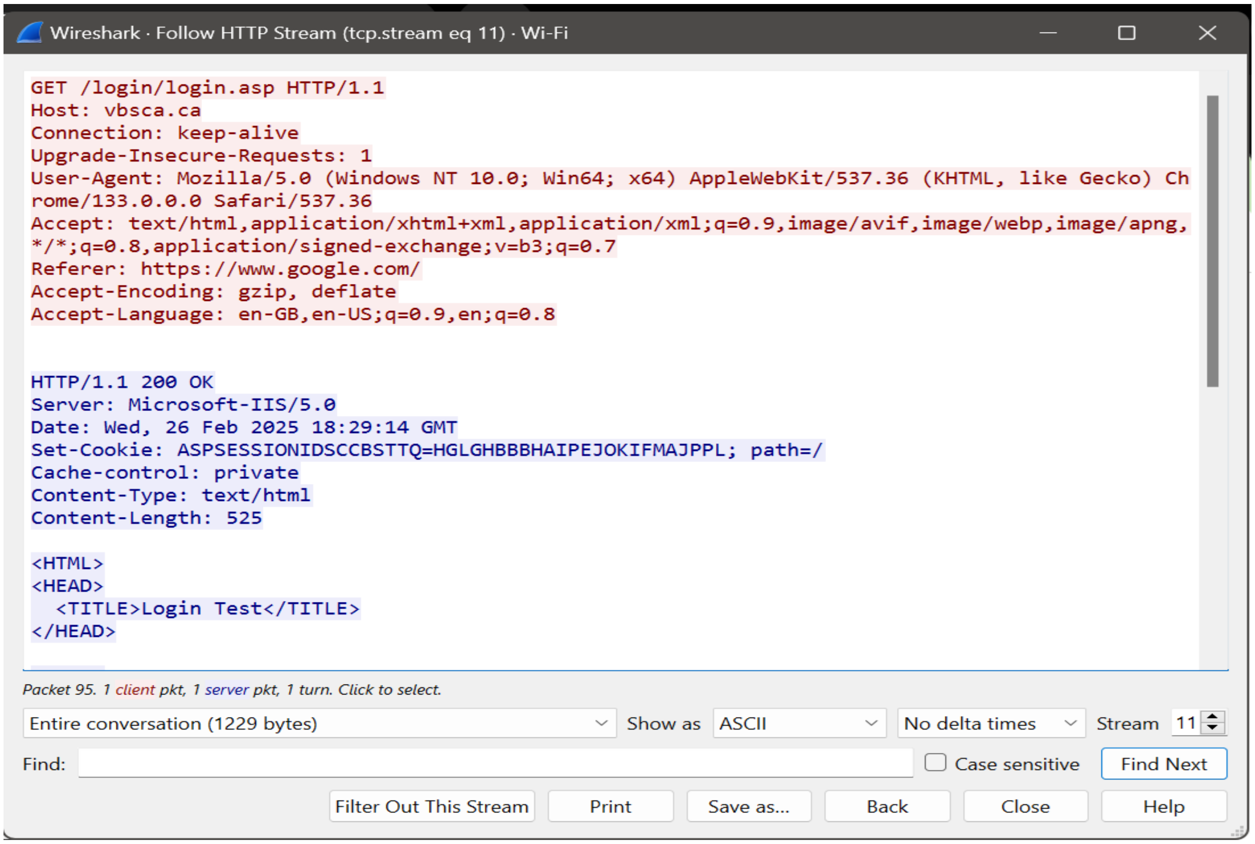
Approach:

- **Tool**: Wireshark, installed on a Windows system
- **Setup**: Captured traffic on an active network interface with the filter http applied.
- **Procedure**:
  - GET: Navigated to http://vbsca.ca/login/login.asp
  - POST: Submitted a login form on http://vbsca.ca/login/login.asp with credentials (txtUsername=dan&txtPassword=1234).
  - Analyzed packets using Wireshark's TCP Stream feature

Results and Analysis

a) HTTP GET Request

- **Request Headers**:



```
GET /login/login.asp HTTP/1.1
Host: vbsca.ca
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
rome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 26 Feb 2025 18:29:14 GMT
Set-Cookie: ASPSESSIONIDSCCBSTTQ=HGLGHBBBHAIPEJOKIFMAJPPL; path=/
Cache-control: private
Content-Type: text/html
Content-Length: 525

<HTML>
<HEAD>
  <TITLE>Login Test</TITLE>
</HEAD>
```

Packet 95. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1229 bytes) · Show as: ASCII · No delta times · Stream: 11

- **Notes**: Requests the login page; Host specifies the domain, Referer indicates the user came from Google, and Accept lists supported content types.

- **Response Headers**:

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0

Date: Wed, 26 Feb 2025 18:29:14 GMT

Set-Cookie: ASPSESSIONIDSCCBSTTQ=HGLGHBBBHAIPEJOKIFMAJPPL; path=/

Cache-control: private

Content-Type: text/html

Content-Length: 525

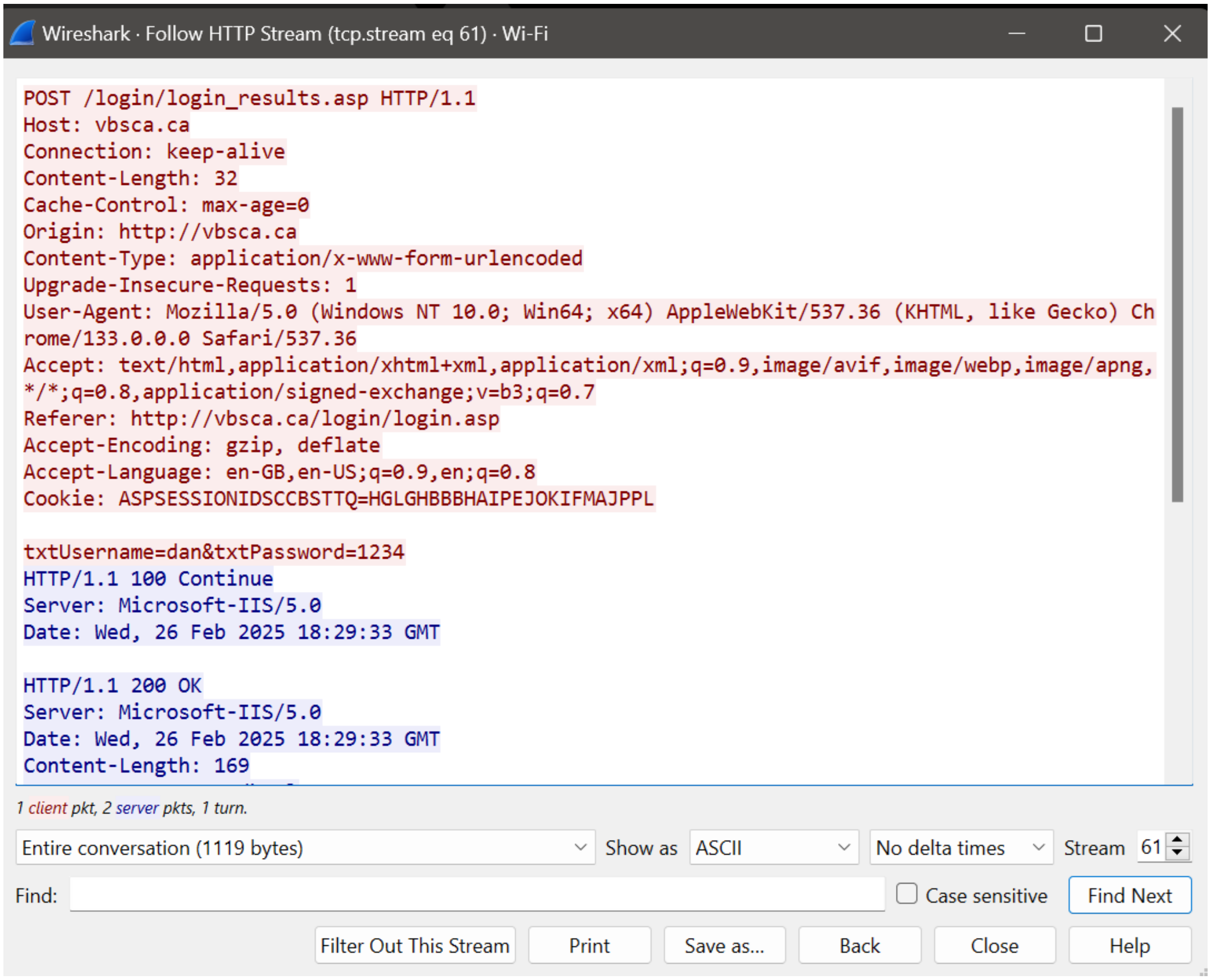
Notes: Returns the login page HTML; Set-Cookie assigns a session ID.

MIME Type: text/html—an HTML document (login page).

HTTP Status Code: 200 OK—Request succeeded, resource delivered.

b) HTTP POST Request

- **Request Headers**:



```
POST /login/login_results.asp HTTP/1.1
Host: vbsca.ca
Connection: keep-alive
Content-Length: 32
Cache-Control: max-age=0
Origin: http://vbsca.ca
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
rome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://vbsca.ca/login/login.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ASPSESSIONIDSCCBSTTQ=HGLGHBBBHAIPEJOKIFMAJPPL

txtUsername=dan&txtPassword=1234
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Wed, 26 Feb 2025 18:29:33 GMT

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 26 Feb 2025 18:29:33 GMT
Content-Length: 169
```

1 client pkt, 2 server pkts, 1 turn.

Entire conversation (1119 bytes) | Show as: ASCII | No delta times | Stream: 61

Find:

  - **Notes**: Submits login credentials; Content-Type indicates form data, Cookie ties to the session, and Refer links to the login page.

Response headers;

```
HTTP/1.1 100 Continue
   Server: Microsoft-IIS/5.0

Date: Wed, 26 Feb 2025 18:29:33 GMT
```

  - **Notes**: Signals the server is ready to process the POST data.
  - **Notes**: Confirms successful login processing; no Content-Type specified, but likely text/html based on context.

MIME Type: Assumed text/html (login result page), though not explicitly stated in the response headers provided.

HTTP Status Code: 200 OK—Server processed the POST successfully.

c) Key Findings

- **Headers**: GET retrieves the login page (no body), while POST submits credentials (body: txtUsername=dan&txtPassword=1234). Common headers include Host, User-Agent, and Connection.
- **MIME Types**: Both responses are likely text/html (GET explicitly states it; POST implied).
- **Status Codes**: 200 OK for both indicates success; POST includes a 100 Continue interim response, showing the server’s two-step handling of the request.