WIRESHARK-HTTP

ASPECTS:

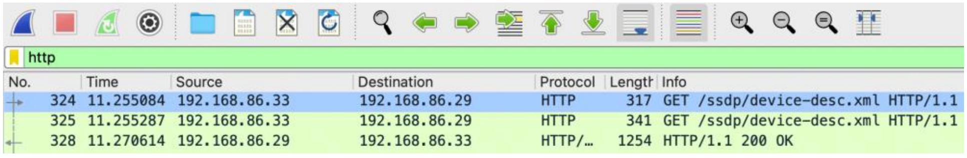
- GET/response interaction
- HTTP message formats
- Retrieving large HTML files
- Retrieving HTML files with embedded objects
- HTTP authentication and security

HTTP GET/response interaction

Steps: to download a HTML file (contains no embedded objects)

a. Start up web browser
b. Start up wireshark and enter HTTP (only captured HTTP messages will be displayed)
c. Wait one minute before starting the wireshark packet capture feature
d. Enter link on browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
e. Stop wireshark packet capture

1. Annotate output on the messages received from wireshark



http

No.	Time	Source	Destination	Protocol	Length	Info
324	11.255084	192.168.86.33	192.168.86.29	HTTP	317	GET /ssdp/device-desc.xml HTTP/1.1
325	11.255287	192.168.86.33	192.168.86.29	HTTP	341	GET /ssdp/device-desc.xml HTTP/1.1
328	11.270614	192.168.86.29	192.168.86.33	HTTP/…	1254	HTTP/1.1 200 OK

- Arrow facing right: **input**
- Arrow facing left: **output**

2. Version of HTTP browser is running: **HTTP 1.1**
3. Languages that browser can accept: **en-us**
4. **IP addresses:**
   - My computer: **ip.src == 192.168.86.33**
   - gaia.cs.umass.edu server: **ip.src == 192.168.86.29**

5. **Status code** returned from the server to my browser: **200, description: OK**
6. Last modification of HTML file (retrieved from gaia.cs.umass.edu server): **Last –modified: fri. 7 Mar 2024 12:30:05 (file was last modified a minute earlier than when file was opened)**
7. Number of bytes being returned to browser: **Content length: 1069 bytes**
8. Headers that are not displayed within the raw data in the packet content window:

No difference between the two windows

HTTP CONDITIONAL GET/RESPONSE INTERACTION

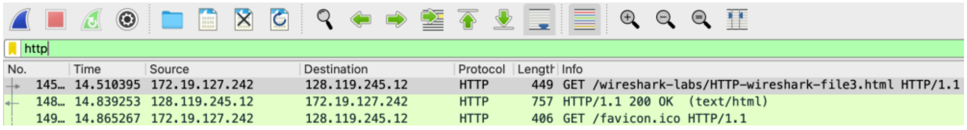
a. Clear browser cache
b. Start up Wireshark packet sniffer
c. Enter given URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
d. Refresh
e. Filter wireshark with HTTP, stop packet sniffing

9. Inspect contents of HTTP GET request, is there a "IF-MODIFIED-SINCE" line? **Yes: If-Modified-Since: Wed, 06 Mar 2024 06:59:02 GMT\r\n**
10. Inspect contents of server response (OK message), did the server return the contents of the file? **Yes**
11. Inspect contents of second HTTP GET request, is there a "IF-MODIFIED-SINCE" header? **Yes: If-Modified-Since: Wed, 06 Mar 2024 06:59:02 GMT\r\n**
    ****Last modified date didn't change**
12. HTTP status code and phrase returned from server (response to second HTTP GET), did the server return the contents of the file? **No: sends a copy of the original file**

RETRIEVING LONG DOCUMENTS

a. Clear browser cache
b. Enter URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
c. Filter, stop packet sniffing

HTTP response message: separated into several packets, since the file is too large: fragmented across multiple TPC segments
*no continuation message in HTTP



http

No.	Time	Source	Destination	Protocol	Length	Info
145…	14.510395	172.19.127.242	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
148…	14.839253	128.119.245.12	172.19.127.242	HTTP	757	HTTP/1.1 200 OK (text/html)
149…	14.865267	172.19.127.242	128.119.245.12	HTTP	406	GET /favicon.ico HTTP/1.1

13. Number of HTTP GET messages browser sent: **1**
    Which packet number in the trace contains the GET message for the Bill or Rights?: P**acket number 145**

14. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request: **Packet number 148**
15. Status code and phrase in the response: **200 OK**
16. How many TCP segments were needed to carry the HTTP response and the text of the Bill of Rights: **[4 Reassembled TCP Segments (4861 bytes): #14892(1386), #14893(1386), #14894(1386), #14895(703)]**

HTML DOCUMENTS WITH EMBEDDED DOCUMENTS

a. Clear browser cache

b. Enter URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
c. Filter, stop packet sniffing

17. Number of HTTP GET request messages browser sent: **2**
Which internet addresses were these GET requests sent:
HTML file internet address: ip.src == 172.19.127.242
Logo picture internet address: ip.src == 128.119.245.12

18. Did the browser download the two images serially** (in a series or sequence), or were they downloaded from the two websites in parallel?: **Downloaded from two websites in parallel (they're being downloaded simultaneously in the same connection, instead of one by one like a persistent connection)**

HTTP AUTHENTICATION

Website is password protected

- Username: wireshark-students
- Password: network

a. Clear browser cache
b. Enter URL: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
c. Filter, stop packet sniffing

19. What's the server's response (status code and phrase) to the HTTP GET message from browser: **_ws.col.info == "HTTP/1.1 401 Unauthorized (text/html)"**

20. When browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?: **Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n- already used password when website was refreshed**