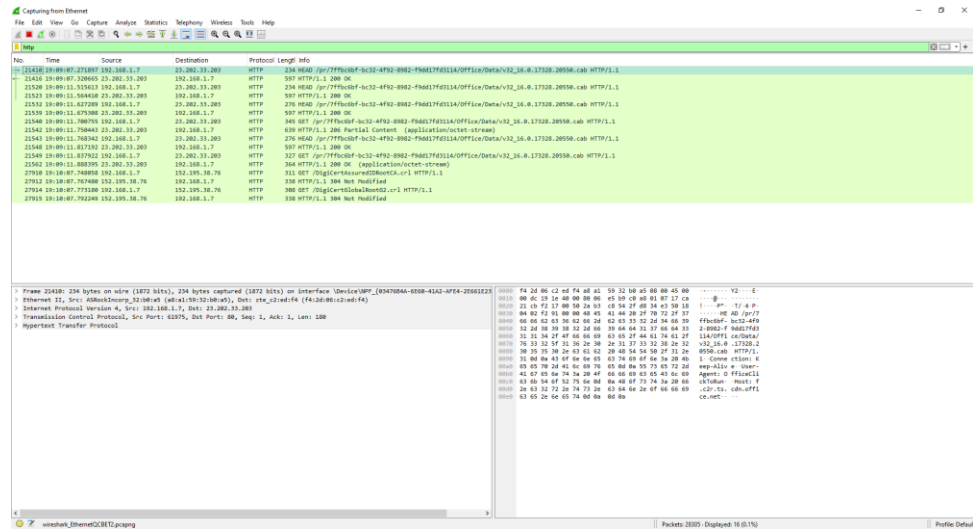


Name: Zuriel G. Montallana

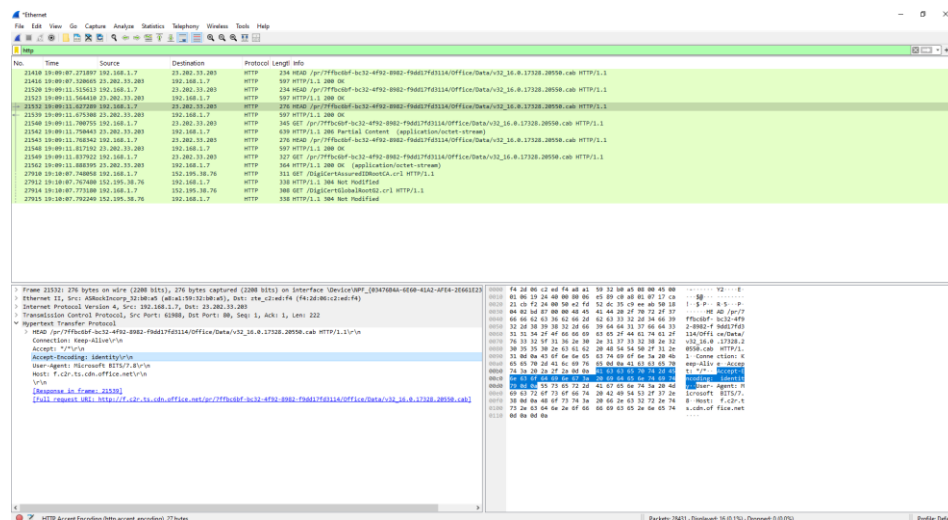
Year/Block: BSIT3 – B1

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



My browser is running version 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?



It didn't show any languages that accepts to the server.

192.168.1.7 and 23.202.33.203

4. What is the status code returned from the server to your browser?

200 OK

5. When was the HTML file that you are retrieving last modified at the server?

[illegible]

Tue, 13 Aug, 2024 07:09:53 GMT

6. How many bytes of content are being returned to your browser?

[illegible]

11447

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

The image shows a Wireshark packet capture of an HTTP GET request. The packet listing window displays a list of packets, with packet 21416 selected. The packet details window shows the structure of the HTTP request, including the Host, User-Agent, and Accept-Range headers. The packet bytes window shows the raw hex and ASCII data of the packet, including the 'IF-MODIFIED-SINCE' header.

All headers are present.

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

The image shows a Wireshark packet capture of an HTTP GET request. The packet listing window displays a list of packets, with packet 21416 selected. The packet details window shows the structure of the HTTP request, including the Host, User-Agent, and Accept-Range headers. The packet bytes window shows the raw hex and ASCII data of the packet, including the 'IF-MODIFIED-SINCE' header.

Yes

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

It didn't, because it didn't show the body of html which should be like <html><body>This is a simple HTML file</body></html>

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list on the left shows a GET request from 192.168.1.7 to 192.168.1.203 on port 80. The packet details pane on the right shows the request structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows the request line: GET /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1. The packet bytes pane on the right shows the raw data of the request, including the GET line and various headers.

No.	Time	Source	Destination	Protocol	Length	Info
21418	19:09:07.278007	192.168.1.7	23.202.33.203	HTTP	204	HEAD /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1
21419	19:09:07.320605	23.202.33.203	192.168.1.7	HTTP	507	HTTP/1.1 200 OK
21528	19:09:11.510613	192.168.1.7	23.202.33.203	HTTP	204	HEAD /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1
21529	19:09:11.564420	23.202.33.203	192.168.1.7	HTTP	507	HTTP/1.1 200 OK
21532	19:09:11.627299	192.168.1.7	23.202.33.203	HTTP	276	HEAD /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1
21533	19:09:11.675388	23.202.33.203	192.168.1.7	HTTP	507	HTTP/1.1 200 OK
21540	19:09:11.708705	192.168.1.7	23.202.33.203	HTTP	345	GET /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1
21541	19:09:11.720463	23.202.33.203	192.168.1.7	HTTP	639	HTTP/1.1 200 Part11 Content (application/octet-stream)
21543	19:09:11.760342	192.168.1.7	23.202.33.203	HTTP	276	HEAD /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1
21546	19:09:11.827292	23.202.33.203	192.168.1.7	HTTP	507	HTTP/1.1 200 OK
21549	19:09:11.837022	192.168.1.7	23.202.33.203	HTTP	327	GET /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1
21552	19:09:11.888395	23.202.33.203	192.168.1.7	HTTP	364	HTTP/1.1 200 OK (application/octet-stream)
27910	19:10:07.740806	192.168.1.7	192.195.18.76	HTTP	311	GET /img/center/measure/20070624.crl HTTP/1.1
27912	19:10:07.767408	192.195.18.76	192.168.1.7	HTTP	338	HTTP/1.1 304 Not Modified
27914	19:10:07.773108	192.168.1.7	192.195.18.76	HTTP	308	GET /img/center/measure/20070624.crl HTTP/1.1
27915	19:10:07.792249	192.195.18.76	192.168.1.7	HTTP	338	HTTP/1.1 304 Not Modified

Frame 21540: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on Interface Device\NPF {8347684A-6E6B-41A2-4F54-0E661E22} (en0)
Ethernet II, Src: iGigabitEthernet0/24 (08:00:00:0C:00:00:00:00:00), Dst: 23.202.33.203 (f4:2d:8c:12:ed:f4)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 23.202.33.203
Transmission Control Protocol, Src Port: 61088, Dst Port: 80, Seq: 223, Ack: 544, Len: 291
Hypertext Transfer Protocol
GET /pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab HTTP/1.1\nConnection: keep-alive\nAccept: */*\nAccept-Encoding: identity\nRange: bytes=0-1\nUser-Agent: Microsoft IE75.7.81\nHost: c2c-ts.cdm.office.net/v32_36_8-17328-28558 cab\n[Full request URI: http://c2c-ts.cdm.office.net/pr/7ffbc0df-bc32-4f92-8982-f86817f6d314/Office/Data/v32_36_8-17328-28558 cab]

It only displayed the date which is Tue, 13 Aug, 2024 07:09:53 GMT

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets, with packet 27914 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
21410	19.09:07.275897	192.168.1.7	23.202.33.203	HTTP	234	HEAD /js/7f9bc8bf-bc32-4f92-8982-f86d27f811a4/Office/Data/v32_36.0.17328.20550.cab HTTP/1.1
21411	19.09:07.320605	23.202.33.203	192.168.1.7	HTTP	587	HTTP/1.1 200 OK
21520	19.09:11.515613	192.168.1.7	23.202.33.203	HTTP	234	HEAD /js/7f9bc8bf-bc32-4f92-8982-f86d27f811a4/Office/Data/v32_36.0.17328.20550.cab HTTP/1.1
21521	19.09:11.564458	23.202.33.203	192.168.1.7	HTTP	587	HTTP/1.1 200 OK
21532	19.09:11.627200	192.168.1.7	23.202.33.203	HTTP	276	HEAD /js/7f9bc8bf-bc32-4f92-8982-f86d27f811a4/Office/Data/v32_36.0.17328.20550.cab HTTP/1.1
21533	19.09:11.675306	23.202.33.203	192.168.1.7	HTTP	587	HTTP/1.1 200 OK
21548	19.09:11.708793	192.168.1.7	23.202.33.203	HTTP	345	GET /js/7f9bc8bf-bc32-4f92-8982-f86d27f811a4/Office/Data/v32_36.0.17328.20550.cab HTTP/1.1
21549	19.09:11.730443	23.202.33.203	192.168.1.7	HTTP	639	HTTP/1.1 200 Partial Content (application/octet-stream)
21561	19.09:11.748242	192.168.1.7	23.202.33.203	HTTP	276	HEAD /js/7f9bc8bf-bc32-4f92-8982-f86d27f811a4/Office/Data/v32_36.0.17328.20550.cab HTTP/1.1
21548	19.09:11.817332	23.202.33.203	192.168.1.7	HTTP	587	HTTP/1.1 200 OK
21549	19.09:11.837622	192.168.1.7	23.202.33.203	HTTP	137	GET /js/7f9bc8bf-bc32-4f92-8982-f86d27f811a4/Office/Data/v32_36.0.17328.20550.cab HTTP/1.1
21562	19.09:11.888393	23.202.33.203	192.168.1.7	HTTP	364	HTTP/1.1 200 OK (application/octet-stream)
27910	19.18:07.740800	192.168.1.7	152.195.38.76	HTTP	311	GET /DigitalCertificateDownload.crl HTTP/1.1
27912	19.18:07.767480	152.195.38.76	192.168.1.7	HTTP	208	HTTP/1.1 304 Not Modified
27914	19.18:07.777330	192.168.1.7	152.195.38.76	HTTP	388	GET /DigitalCertificateDownload.crl HTTP/1.1
27915	19.18:07.792240	152.195.38.76	192.168.1.7	HTTP	338	HTTP/1.1 304 Not Modified

Frame 27912: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits) on interface 'DeviceNPF_{0347686A-6608-41A2-8F6A-25861E23...}'

Ethernet II, Src: Intel(R) Gigabit Ethernet Controller (8:0:0:0:0:0), Dst: 08:00:00:00:00:00 (8:0:0:0:0:0)

Internet Protocol Version 4, Src: 152.195.38.76, Dst: 192.168.1.7

Transmission Control Protocol, Src Port: 80, Dst Port: 8080, Seq: 1, Ack: 208, Len: 204

Hypertext Transfer Protocol

Accept-Ranges: bytes

Age: 6841s

Cache-Control: max-age=7200, public

Date: Wed, 04 Sep 2024 11:18:07 GMT

ETag: "66b7e4b-4357"

Expires: Wed, 04 Sep 2024 13:18:07 GMT

Last-Modified: Tue, 03 Sep 2024 20:15:04 GMT

Server: KSCC (v/0.0.0.0)

X-Cache: HIT

[Request in frame: 27910]

[Time since request: 0.03422800 seconds]

[Request URI: /DigitalCertificateDownload.crl]

[Full request URI: http://cr3.digitcert.com/DigitalCertificateDownload.crl]

The status code is 304 Not Modified. It means that the server did not return the file content because it determined that the file had not changed since the last time it was retrieved by the browser. The browser can use the cached version of the file instead.