UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS E TECNOLOGIA
CIÊNCIA DA COMPUTAÇÃO

DANIEL XAVIER BRITO DE ARAÚJO
LUCAS DE LUCENA SIQUEIRA
JOAO VICTOR GOMES BARBOSA

Atividade 01

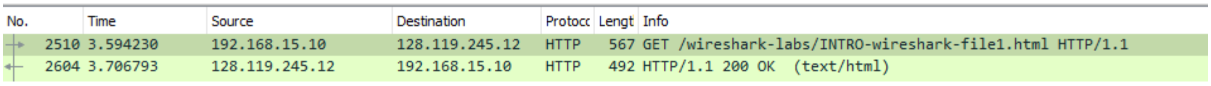
CAMPINA GRANDE
2022

Projeto prático 1

1 - Quais dos seguintes protocolos são mostrados como aparecendo (ou seja, estão listados na coluna “Protocol” do Wireshark) em seu arquivo de rastreamento: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

- TCP, UDP, RTCP, ARP, TLSv1.2, HTTP, DNS, ICMPv6, QUIC e DNS.

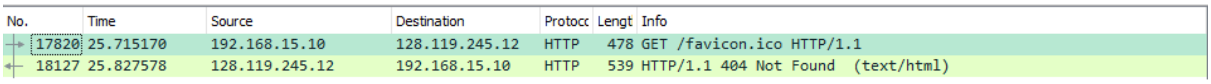
2 - Quanto tempo levou desde o envio da mensagem HTTP GET até o recebimento da resposta HTTP OK? (Por padrão, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde que o rastreamento do Wireshark começou. menu para baixo, selecione Formato de exibição de hora e selecione Hora do dia.)



No.	Time	Source	Destination	Protocc	Lengt	Info
2510	3.594230	192.168.15.10	128.119.245.12	HTTP	567	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2604	3.706793	128.119.245.12	192.168.15.10	HTTP	492	HTTP/1.1 200 OK (text/html)

- Foram necessários 0.112563 segundos entre a requisição HTTP GET e a resposta HTTP OK.

3 - Qual é o endereço de Internet do gaia.cs.umass.edu (também conhecido como www-net.cs.umass.edu)? Qual é o endereço de Internet do seu computador ou (se você estiver usando o arquivo de rastreamento) do computador que enviou a mensagem HTTP GET?



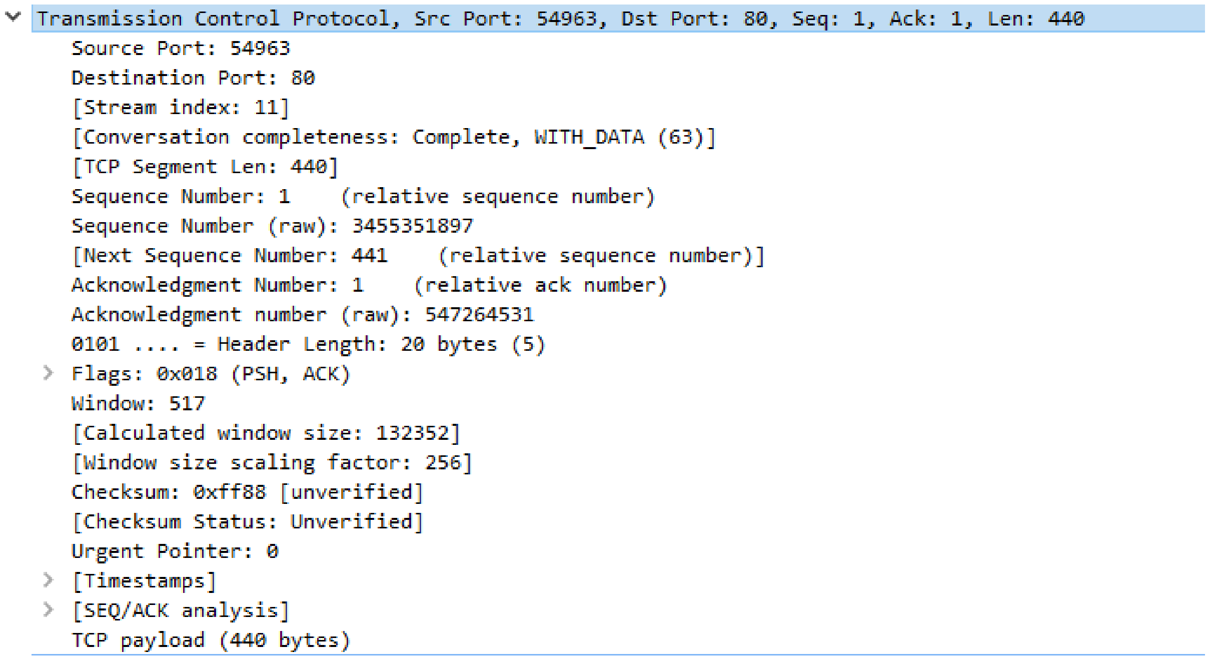
No.	Time	Source	Destination	Protocc	Lengt	Info
17820	25.715170	192.168.15.10	128.119.245.12	HTTP	478	GET /favicon.ico HTTP/1.1
18127	25.827578	128.119.245.12	192.168.15.10	HTTP	539	HTTP/1.1 404 Not Found (text/html)

- Endereço do “gaia.cs.umass.edu”: 128.119.245.12
- Endereço do computador local: 192.168.15.10

4 - Expanda as informações sobre a mensagem HTTP na janela "Detalhes do pacote selecionado" do Wireshark para que você possa ver os campos na mensagem de solicitação HTTP GET. Que tipo de navegador da Web emitiu a solicitação HTTP? A resposta é mostrada na extremidade direita das informações após o campo “User-Agent:” na tela de mensagem HTTP expandida. (Este valor de campo na mensagem HTTP é como um servidor web aprende que tipo de navegador você está usando: Firefox, Safari, Microsoft Internet Edge, Outros).

- Imformações exibidas à direita do User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33\r\n
- Navegador utilizado para realizar a requisição HTTP GET: Microsoft Edge.

5 - Expanda as informações sobre o Transmission Control Protocol para este pacote na janela "Detalhes do pacote selecionado" do Wireshark para que você possa ver os campos no segmento TCP que transportam a mensagem HTTP. Qual é o número da porta de destino (o número após “Dest (ou Destination) Port:” para o segmento TCP que contém a solicitação HTTP) para a qual esta solicitação HTTP está sendo enviada?



```
v Transmission Control Protocol, Src Port: 54963, Dst Port: 80, Seq: 1, Ack: 1, Len: 440
     Source Port: 54963
     Destination Port: 80
     [Stream index: 11]
     [Conversation completeness: Complete, WITH_DATA (63)]
     [TCP Segment Len: 440]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 3455351897
     [Next Sequence Number: 441    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 547264531
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x018 (PSH, ACK)
     Window: 517
     [Calculated window size: 132352]
     [Window size scaling factor: 256]
     Checksum: 0xff88 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > [Timestamps]
   > [SEQ/ACK analysis]
     TCP payload (440 bytes)
```

- Destination Port: 80

6 - Imprima as duas mensagens HTTP (GET e OK) referidas na questão 2 acima. Para fazer isso, selecione Imprimir no menu de comando Arquivo Wireshark e selecione os botões radiais “Somente pacote selecionado” e “Imprimir conforme exibido” e clique em OK.

```
No.     Time           Source                Destination           Protocol Length Info
   1500 11.925742      192.168.0.104         128.119.245.12        HTTP     527    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 1500: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{37804717-F72E-4805-9195-
A70E69E42C20}, id 0
Ethernet II, Src: IntelCor_82:08:75 (cc:f9:e4:82:08:75), Dst: Shenzhen_16:ae:55 (38:6b:1c:16:ae:55)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61212, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
    Source Port: 61212
    Destination Port: 80
    [Stream index: 21]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 473]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3749260976
    [Next Sequence Number: 474    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 952223551
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 514
    [Calculated window size: 131584]
    [Window size scaling factor: 256]
    Checksum: 0xd711 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (473 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
    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=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1510]
    [Next request in frame: 1550]
No.     Time           Source                Destination           Protocol Length Info
   1510 12.043095      128.119.245.12        192.168.0.104         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 1510: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{37804717-F72E-4805-9195-
A70E69E42C20}, id 0
Ethernet II, Src: Shenzhen_16:ae:55 (38:6b:1c:16:ae:55), Dst: IntelCor_82:08:75 (cc:f9:e4:82:08:75)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104
Transmission Control Protocol, Src Port: 80, Dst Port: 61212, Seq: 1, Ack: 474, Len: 438
    Source Port: 80
    Destination Port: 61212
    [Stream index: 21]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 952223551
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 474    (relative ack number)
    Acknowledgment number (raw): 3749261449
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xcadd [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 16 Sep 2022 19:28:44 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT\r\n
    ETag: "51-5e8c50f0beb89"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.117353000 seconds]
    [Request in frame: 1500]
    [Next request in frame: 1550]
    [Next response in frame: 1563]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
No.     Time           Source                Destination           Protocol Length Info
   1550 12.359901      192.168.0.104         128.119.245.12        HTTP     473    GET /favicon.ico HTTP/1.1 
Frame 1550: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{37804717-F72E-4805-9195-
A70E69E42C20}, id 0
Ethernet II, Src: IntelCor_82:08:75 (cc:f9:e4:82:08:75), Dst: Shenzhen_16:ae:55 (38:6b:1c:16:ae:55)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61212, Dst Port: 80, Seq: 474, Ack: 439, Len: 419
    Source Port: 61212
    Destination Port: 80
    [Stream index: 21]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 419]
    Sequence Number: 474    (relative sequence number)
    Sequence Number (raw): 3749261449
    [Next Sequence Number: 893    (relative sequence number)]
    Acknowledgment Number: 439    (relative ack number)
    Acknowledgment number (raw): 952223989
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0xb23a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (419 bytes)
Hypertext Transfer Protocol
    GET /favicon.ico HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
    [HTTP request 2/2]
    [Prev request in frame: 1500]
    [Response in frame: 1563]
No.     Time           Source                Destination           Protocol Length Info
   1563 12.476012      128.119.245.12        192.168.0.104         HTTP     538    HTTP/1.1 404 Not Found  (text/html)
Frame 1563: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{37804717-F72E-4805-9195-
A70E69E42C20}, id 0
Ethernet II, Src: Shenzhen_16:ae:55 (38:6b:1c:16:ae:55), Dst: IntelCor_82:08:75 (cc:f9:e4:82:08:75)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104
Transmission Control Protocol, Src Port: 80, Dst Port: 61212, Seq: 439, Ack: 893, Len: 484
    Source Port: 80
    Destination Port: 61212
    [Stream index: 21]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 484]
    Sequence Number: 439    (relative sequence number)
    Sequence Number (raw): 952223989
    [Next Sequence Number: 923    (relative sequence number)]
    Acknowledgment Number: 893    (relative ack number)
    Acknowledgment number (raw): 3749261868
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 245
    [Calculated window size: 31360]
    [Window size scaling factor: 128]
    Checksum: 0x03e9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (484 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 404 Not Found\r\n
    Date: Fri, 16 Sep 2022 19:28:45 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.116111000 seconds]
    [Prev request in frame: 1500]
    [Prev response in frame: 1510]
    [Request in frame: 1550]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 209 bytes
Line-based text data: text/html (7 lines)
```