

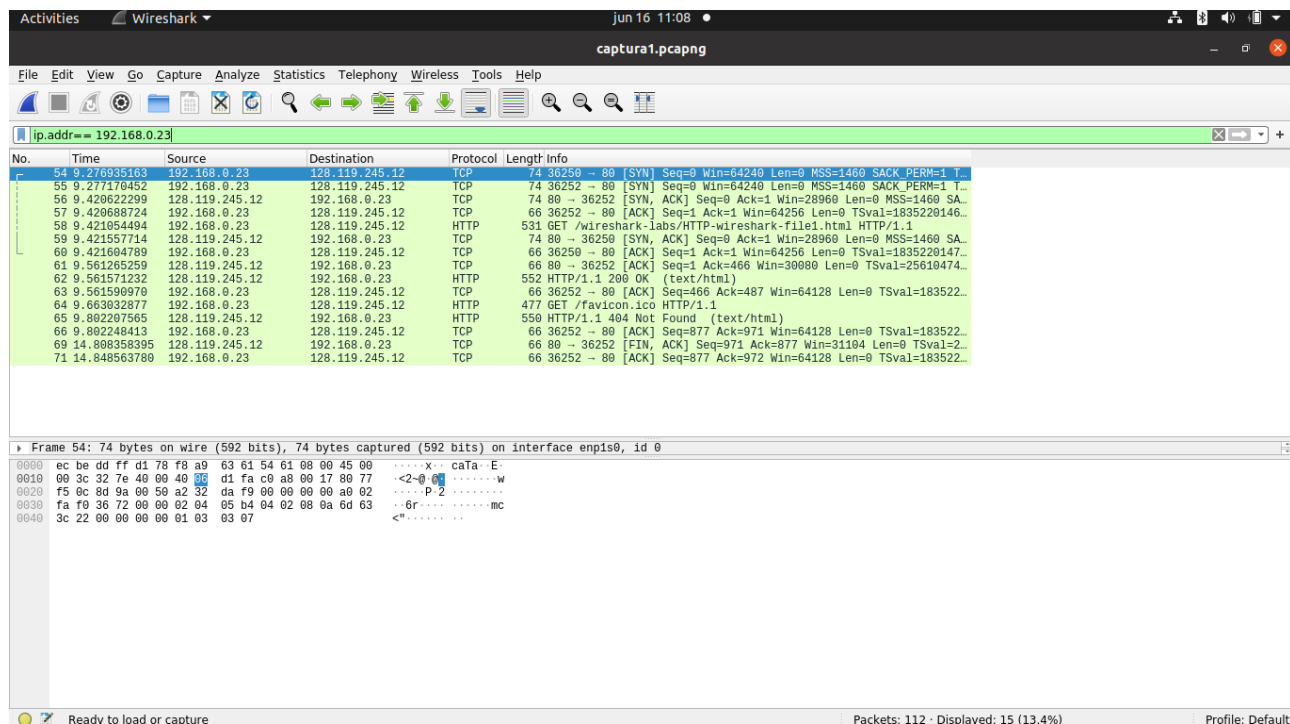
Redes de Computadores I (CK0249) 2021.1 - PPE
Prof. Dr. Emanuel Bezerra Rodrigues

ATIVIDADE PRÁTICA I
CAMADA DE APLICAÇÃO

Aluna: Fernanda Costa de Sousa
Matrícula: 485404

CAPTURA 1

1. Inicie seu navegador. Não acesse nenhuma página ainda!
 2. Inicie o Wireshark e digite o filtro "ip.addr == seu_ip" (sem aspas). Esse filtro vai fazer com que apenas sejam exibidos pacotes que tenham origem ou sejam destinados ao seu computador.
 3. Inicie a captura de pacotes no Wireshark.
 4. Vá ao navegador e digite o endereço:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
Espere o site carregar completamente.
 5. Vá no wireshark e pare a captura.
 - a. Quantos pacotes foram capturados? Anexe um print da captura no relatório.
- Uma dica: Salve a captura.



6. No Wireshark, na barra de filtros, digite o "ip.addr == seu_ip and http" (sem aspas). Esse filtro vai exibir apenas os pacotes referentes ao protocolo HTTP.

7. Analise o primeiro pacote HTTP request. Anexe um print desse pacote no relatório.

captura1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr== 192.168.0.23 and http

No.	Time	Source	Destination	Protocol	Length	Info
58	9.421054494	192.168.0.23	128.119.245.12	HTTP	531	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
62	9.561571232	128.119.245.12	192.168.0.23	HTTP	552	HTTP/1.1 200 OK (text/html)
64	9.663032877	192.168.0.23	128.119.245.12	HTTP	477	GET /favicon.ico HTTP/1.1
65	9.802207565	128.119.245.12	192.168.0.23	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 58: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface enp1s0, id 0
 Ethernet II, Src: CompalIn_61:54:61 (f8:a9:63:61:54:61), Dst: Sagemcom_ff:d1:78 (ec:be:dd:ff:d1:78)
 Internet Protocol Version 4, Src: 192.168.0.23, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 36252, Dst Port: 80, Seq: 1, Ack: 1, Len: 465
 Hypertext Transfer Protocol

100 ec be dd ff d1 78 f8 a9 63 61 54 61 08 00 45 00x...caTa..E..
 110 02 05 86 15 40 00 40 06 7c 9a c0 a8 00 17 80 77@..|.....w
 120 f5 0c 8d 9c 00 50 d9 a1 43 e8 53 d2 d1 1c 80 18P...C:S.....
 130 01 f6 38 3b 00 00 01 01 08 0a 6d 63 3c b3 98 a6 ..8;.....mc<...
 140 7b 3a 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b {}GET /w ireshark
 150 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73 -labs/HT TP-wires
 160 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c 20 hark-fil e1.html
 170 40 54 54 50 2f 24 2a 24 0d 0a 40 6f 72 74 2a 20 HTTP/1.1 404 Not Found

Responda:

a) Qual tamanho do pacote?

531 bytes

b) Qual o endereço IP de destino?

128.119.245.12

c) Qual o método utilizado?

GET

d) Qual a versão do HTTP está sendo executada no seu navegador?

HTTP/1.1

e) Quais formatos de arquivos o seu navegador indica aceitar?

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\r\n

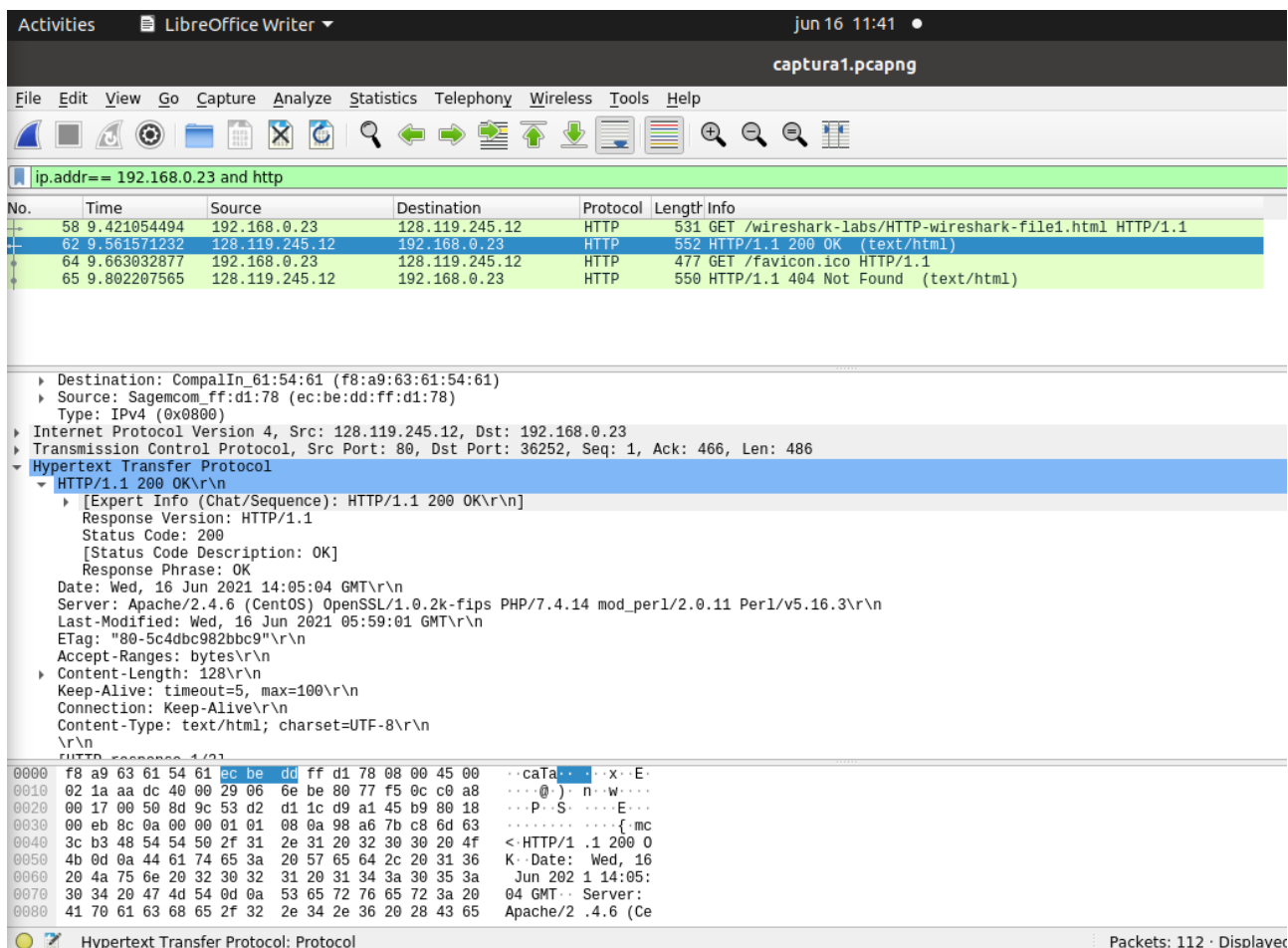
f) Quais linguagens (se houver) o seu navegador indica ao servidor?

En-US, en

g) O que contém a linha de requisição do HTTP?

GET /wireshark-labs/HTTP-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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 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

8. Analise o primeiro pacote HTTP response. Anexe um print desse pacote no relatório.



Responda:

a) Qual a versão do HTTP executada no servidor?

HTTP/1.1

b) Qual o nome do servidor e seu sistema operacional?

Apache e CentOS

c) Qual linha informa a data e a hora do servidor?

A linha de cabeçalho Date

d) Qual a data em que o conteúdo solicitado foi modificado pela última vez?

Wed, 16 jun 2021 05:59:01 GMT

e) Qual o tamanho e tipo de conteúdo enviado na resposta HTTP?

128 e text/html

f) Qual o conteúdo retornado?

text/html

9. Na barra de filtros do Wireshark, digite o seguinte: "ip.addr == seu_ip and dns" (sem aspas).

Esse filtro vai fazer com que sejam exibidos apenas os pacotes referentes ao protocolo DNS.

10. Analise o pacote que contém a requisição de resolução de nome "gaia.cs.umass.edu". Esse pacote está assinalado com query. Anexe um print desse

pacote no relatório. Responda:

a) Qual o tamanho do pacote?

124 bytes

b) Qual o endereço IP de destino? A quem corresponde esse endereço?

Destination: CompalIn_61:54:61 (f8:a9:63:61:54:61)

c) A requisição é do tipo recursiva ou iterativa? Qual linha indica isso? Recursiva. A linha de Query.

11. Analise a resposta à requisição DNS. Ele está assinalado com query response.

Responda:

a) Qual o endereço do emissor desse pacote? É o mesmo do destinatário da requisição anterior? Por quê?

b) Qual o endereço do "gaia.cs.umass.edu"? servidor autoritativo responsável pelo domínio

12. Responda : Analisando a captura de pacotes como um todo, quais pacotes vieram primeiro: HTTP ou DNS? Por quê?