Instituto Tecnológico de Aeronáutica – ITA
CES-35

Lab 1:
Conhecendo protocolos - Wireshark

Membros da equipe:

Bryan Diniz Borck

Prof. Dra. Cecília de Azevedo

Segundo Semestre de 2023

Sumário

Lab 1: Conhecendo protocolos - Wireshark

1 Questão 1

Inicie o seu navegador (browser). Inicie o Wireshark e selecione a interface onde vai capturar pacotes que deve ter acesso a Internet. Inicie a capture (Start).

Resposta:

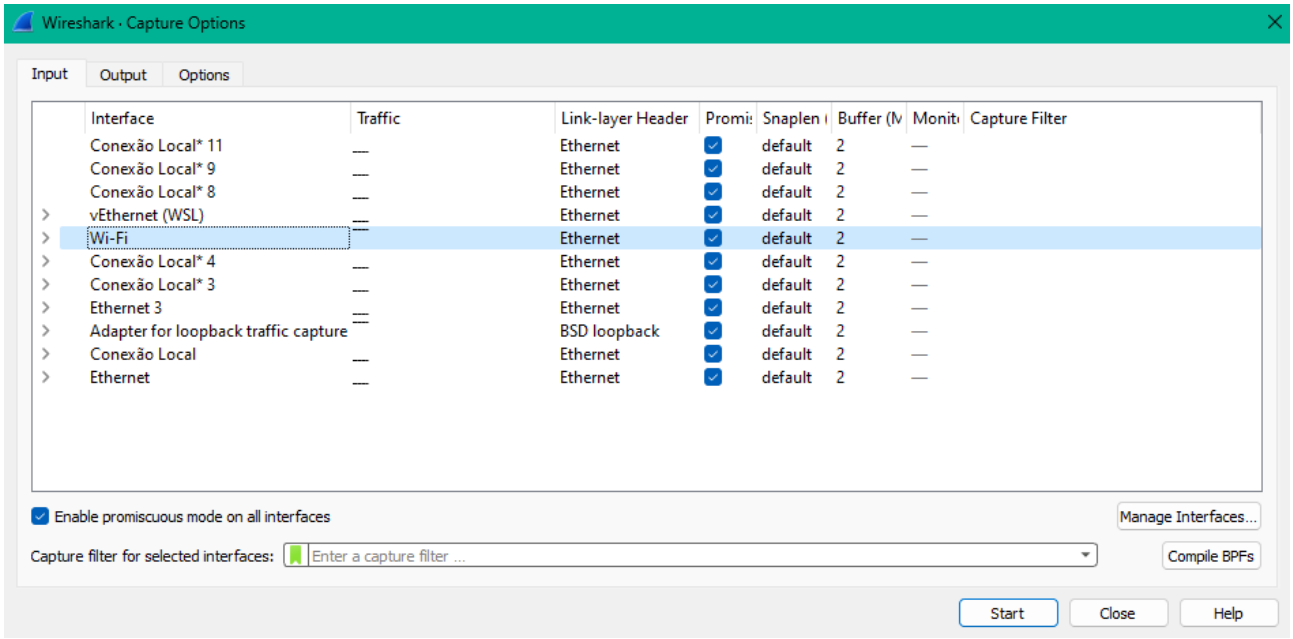

Figura 1: Screenshot do início de captura da minha rede Wifi.

2 Questão 2

Acesse a URL do site do Kurose: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html no navegador. Pare a captura (Stop).

Você pode salvar esta captura para ir respondendo as perguntas abaixo em diferentes momentos. Para salvar File→ Save as → salve no formato próprio do wireshark que usa a biblioteca pcapng. Não se esqueça de outras vezes que tiver que trabalhar com esta mesma captura de abri-lo.

Resposta:

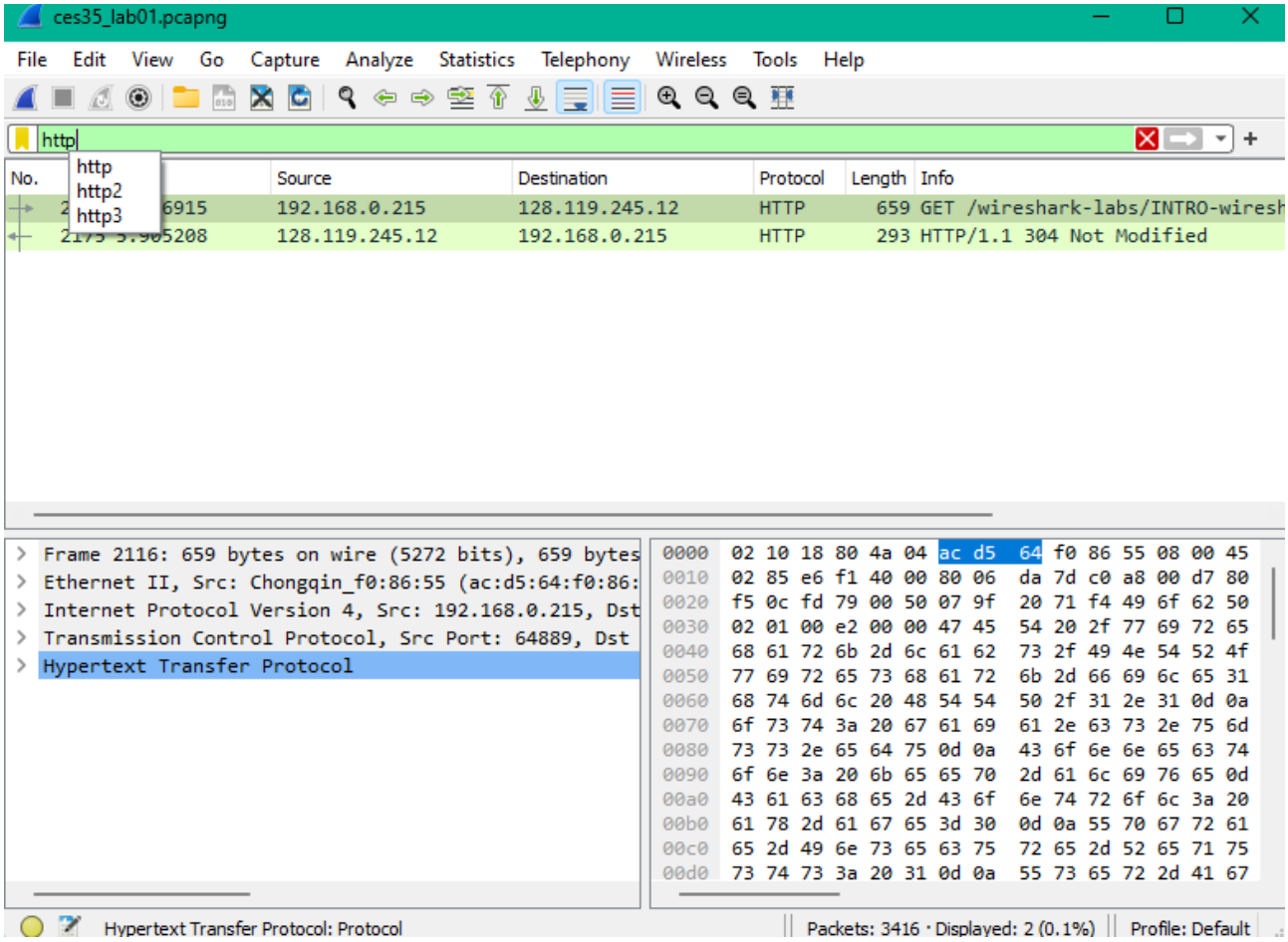

Figura 2: Screenshot da captura do protocolo HTTP.

3 Questão 3

Responda as perguntas gerais:

(A) Quais destes protocolos aparecem na lista de pacotes: TCP, QUIC, HTTP, DNS, UDP, TLS?

Se você não viu o protocolo DNS na lista, talvez a requisição necessária não foi feita pois já estava no seu cache. Esvazie o cache de seu browser e recomece do passo

Resposta:

Todos os protocolos aparecem: TCP, QUIC, HTTP, DNS, UDP, TLS.

(B) Quanto tempo transcorreu desde quando a mensagem HTTP GET foi enviada até quando a resposta HTTP OK foi recebida?

Observação: Por padrão, o valor da coluna "Time" (na janela de listagem de pacotes capturados) é a quantidade de tempo que passou (em segundos) desde que a captura de pacotes começou. Para exibir a hora do dia na coluna "Time", selecione a opção "Time Display Format" do menu "View" e, em seguida, selecione a opção "Time-of- day" no menu emergente.

Resposta:

Tempo decorrido: 01,89 segundos

(C) Aponte para a mensagem que tem o GET e expanda a porção HTTP da mensagem. Olhando os detalhes do pacote, qual a utilidade do campo User-Agent? E na resposta, o que significa o campo Server?

Resposta:

O User-Agent é responsável pelas informações do dispositivo que iniciou o request, indicando sistema operacional e browser por exemplo. E acredito que na resposta, Server indique exatas mesmas informações do lado do servidor que hospeda o site acessado.

(D) Aponte para a mensagem que tem o OK, ou seja, a resposta do HTTP GET. Escreva aqui o tamanho em bytes do cabeçalho de cada camada:

Resposta:

Num. de Bytes do cabeçalho de Aplicação (HTTP): 605

Num. de Bytes do cabeçalho de Transporte (TCP): 20

Num. de Bytes do cabeçalho de Rede (Internet Protocol): 20

Num. de Bytes do cabeçalho de Enlace (Ethernet): 14

Assim, o total do número de bytes dedicados aos cabeçalhos foi 659

Dados "úteis"carregados pela resposta (a página de resposta): 293

Portanto, do total de bytes transferidos nesta mensagem, quanto se refere aos dados úteis em porcentagem? 44

(E) Defina um filtro no campo de filtro da tela principal do wireshark para observar apenas as mensagens que vêm do IP do site do kurose (ip.addr==xxx.xxx.xxx.xxx). Em seguida, acesse novamente a mesma página citada no item (2) do roteiro.

Você deve obter um pacote de resposta do tipo HTTP 1.1/304 Not Modified. Explique do que se trata. O que fazer para evitar esta mensagem e ter a página transferida novamente? Faça isso.

Resposta:

Basicamente significa que desde o último request, a página não foi modificada, de modo que o cliente recebe uma versão com o cache histórico utilizado. Para evitar a mensagem, deve-se limpar o cache do browser.

4 Questão 4

Responda as perguntas gerais:

(A) Expandindo a porção TCP, qual o número da porta de destino para o qual a requisição HTTP foi enviada?

Resposta:

Porta de destino: 80 E qual o número da porta de origem? Porta de origem: 64889

(B) Os protocolos criam sua maneira de conversar, por exemplo, através de bits ligados nas mensagens trocadas, os chamados flags. Há pacotes de controle do TCP que não carregam dados de aplicação. Estão nesta categoria 3 pacotes TCP anteriores ao pacote do HTTP GET. Estes pacotes formam o chamado 3-way handshake e são usados para estabelecer a conexão com o outro lado antes de fazer a requisição propriamente dita. Este handshake envolve os flags SYN e ACK no cabeçalho. Encontre 3 pacotes anteriores ao GET que usam as mesmas portas do item (5A). Em ordem do menor tempo para o maior. Preencha:

Resposta:

Flag(s) de controle ligado(s) no primeiro pacote do handshake: SYN Flag(s) de controle ligado(s) no segundo pacote: SYN e ACK Flag(s) de controle ligado(s) no terceiro pacote: ACK

(C) No pacote HTTP OK quais são as portas envolvidas?

Resposta:

Porta de origem: 80 Porta de destino: 64889

(D) No pacote HTTP OK quais são as portas envolvidas?

Depois da transferência da página normalmente acontece a desconexão que envolve os flags FIN e ACK. Há pacotes ligados as mesmas portas do item (5A) com o bit FIN? Mencione o instante de tempo, os pacotes e os flags ligados nos pacotes encontrados depois da transferência.

Resposta:

Sim, cerca de 0,2 s após o GET há um pacote TCP com a flag ACK ligada mas com a flag FIN desativa encontrado após a transferência, com mesmas portas.

5 Questão 5

O comando ifconfig (Linux) traz os endereços das suas interfaces de rede. Coloque aqui a saída do ifconfig. No Windows o comando equivalente é ipconfig.

Resposta:

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

Estado da mídia. . . . . : mídia desconectada

Sufixo DNS específico de conexão. . . . . :

Adaptador Ethernet Ethernet 3:

Sufixo DNS específico de conexão. . . . . :

Endereço IPv6 de link local . . . . . : fe80::303:81e2:e533:307c%11

Endereço IPv4. . . . . : 192.168.220.1

Máscara de Sub-rede . . . . . : 255.255.255.0

Gateway Padrão. . . . . :

Adaptador desconhecido Conexão Local:

Estado da mídia. . . . . : mídia desconectada

Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Conexão Local* 3:

Estado da mídia. . . . . : mídia desconectada

Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Conexão Local* 4:

Estado da mídia. . . . . : mídia desconectada

Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Wi-Fi:

Sufixo DNS específico de conexão. . . . . :

Endereço IPv6 . . . . . : 2804:14d:688c:4f23:a1bf:7267:1afd:44fe

Endereço IPv6 . . . . . : 2804:14d:688c:4f23:bfb7:743f:5dbf:4931

Endereço IPv6 Temporário. . . . . : 2804:14d:688c:4f23:c0f4:f114:6995:97a7

Endereço IPv6 de link local . . . . . : fe80::2f57:a50b:7e9f:2bc1%22

Endereço IPv4. . . . . : 192.168.0.215

Máscara de Sub-rede . . . . . : 255.255.255.0

Gateway Padrão. . . . . : e80::10:18ff:fe80:4a04%22

192.168.0.1

Adaptador Ethernet vEthernet (WSL):

Sufixo DNS específico de conexão. . . . . :

Endereço IPv6 de link local . . . . . : fe80::a716:f5f2:7cdb:739c%67

Endereço IPv4. . . . . : 172.17.144.1

Máscara de Sub-rede . . . . . : 255.255.240.0

Gateway Padrão. . . . . :

6 Questão 6

Para estudar superficialmente a Camada de Rede, selecione a mensagem com o GET novamente e responda:

Resposta:

(A) Endereço IP de gaia.cs.umass.edu : 128.119.245.12

Endereço IP de seu computador: 192.168.0.215

(B) O campo inet na saída do ifconfig é o mesmo do endereço IP que o wireshark mostrou?

Sim, é o mesmo

7 Questão 7

Para estudar superficialmente a Camada de Enlace, selecione a mensagem com o GET novamente. Na camada de enlace os endereços não se referem ao endereçamento mundial IP, mas ao endereço de sua placa de rede que será usado localmente. Responda:

Resposta:

(A) Endereço MAC de origem: ac:d5:64:f0:86:55

Endereço MAC de destino: 02:10:18:80:4a:04

(B) O campo ether na saída do ifconfig é o mesmo do endereço de origem que o wireshark mostrou?

Sim, é o mesmo. Não tem no ipconfig, porém o endereço está nas Propriedades de Rede do Windows.

8 Questão 8

Faça um traceroute para o site do Kurose que está no item (2) acima. Quantos saltos foram necessários até chegar lá? Inclua a saída do traceroute no relatório.

Resposta:

Foram necessário 22 saltos. Segue a saída:

1 9 ms 8 ms 9 ms 192.168.0.1

2 19 ms 18 ms 17 ms 10.59.0.1

3 19 ms 15 ms 19 ms bb6a9031.virtua.com.br [187.106.144.49]

4 23 ms 23 ms 21 ms embratel-T0-5-0-0-uacc01.spoph.embratel.net.br [200.245.154.145]

5 22 ms 20 ms 20 ms ebt-B1102-core01.spo.embratel.net.br [200.230.243.32]

6 139 ms 139 ms 134 ms ebt-B11121-intl02.nyk.embratel.net.br [200.230.251.254]

7 * * * Esgotado o tempo limite do pedido.

8 157 ms 158 ms 158 ms be3362.ccr41.jfk02.atlas.cogentco.com [154.54.3.9]

9 156 ms 160 ms 161 ms be4076.ccr21.alb02.atlas.cogentco.com [154.54.90.98]

10 173 ms 157 ms 166 ms be2734.rcr51.orh01.atlas.cogentco.com [154.54.81.230]

11 164 ms 165 ms 160 ms 38.104.218.14

12 167 ms 172 ms 173 ms 69.16.0.8

13 142 ms 140 ms 140 ms 69.16.1.0

14 141 ms 139 ms 141 ms core1-rt-et-8-3-0.gw.umass.edu [192.80.83.109]

15 214 ms 140 ms 139 ms n1-rt-1-1-et-0-0-0.gw.umass.edu [128.119.0.216]

16 254 ms 142 ms 139 ms 128.119.7.74

17 143 ms 143 ms 147 ms 128.119.7.66

18 141 ms 146 ms 141 ms core2-rt-et-7-2-1.gw.umass.edu [128.119.0.121]

19 144 ms 145 ms 142 ms n5-rt-1-1-xe-2-1-0.gw.umass.edu [128.119.3.33]

20 142 ms 146 ms 145 ms cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]

21 152 ms 141 ms 143 ms nscs1bbs1.cs.umass.edu [128.119.240.253]

22 143 ms 143 ms 141 ms gaia.cs.umass.edu [128.119.245.12]