CES-35 – Redes de Computadores e Internet

Laboratório número 1
Conhecendo protocolos - Wireshark

Em seu relatório siga rigorosamente o roteiro abaixo. Inclua as perguntas na ordem em que aparecem seguidas das respectivas respostas. Não precisa introdução nem conclusão.

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).

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.

3. Responda as perguntas gerais:
3.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 start da captura (Passo 1).

Na lista de protocolos obtida entre o início (Start) e o fim (Stop) da captura, aparecem os seguintes pacotes da lista em questão: DNS, HTTP, QUIC, TCP e TLS. Não aparece UDP.

3.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.

Tempo decorrido: GET: 17:38:38,826978 – OK: 17:38:38,975665

3.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?

O User-Agent é um campo que o cliente (navegador ou software que faz a requisição) envia para "se identificar", fornecendo, dentre outras informações, que navegador está sendo usado e qual sistema operacional, para auxiliar o servidor a como formatar a resposta.

Já o Server é um campo enviado pelo servidor web para indicar, dentre outras informações, qual software está rodando para atender a requisição e sua versão, ou seja, para o cliente saber "quem" respondeu.

3.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:

Num. de Bytes do cabeçalho de Aplicação (HTTP): 357B.
Num. de Bytes do cabeçalho de Transporte (TCP): 20B.
Num. de Bytes do cabeçalho de Rede (Internet Protocol): 20B.
Num. de Bytes do cabeçalho de Enlace (Ethernet): 14B.
Assim, o total do número de bytes dedicados aos cabeçalhos foi: 411B.
Dados "úteis" carregados pela resposta (a página de resposta): 81B.

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

Aprox. 16,46%.

3.E) Inclua no relatório o print das mensagens HTTP (GET e OK) referentes ao acesso feito em (3). Para isso, no wireshark selecione as mensagens, seleciona File→ Print, selecione "Selected Packet Only" e "All expanded" para que eu possa conferir os campos a que você se refere.

3.F) Através do Wireshark, você pode gravar arquivos presentes em comunicações de rede capturadas. Clique em "File", "Export Objects" e depois em "HTTP..." e escreva abaixo quais os arquivos o Wireshark idenficou nas mensagens trocadas com o IP do site do Kurose:

INTRO-wireshark-file1.html
Favicon.ico

Salve o arquivo HTML da página web desse site em seu computador.

3.G) 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.

A mensagem indica que a página está armazenada na cache do cliente e, dessa forma, não precisa retornar uma nova requisição diretamente do servidor, pois este informou que não houve modificações desde a última vez em que foi acessada pelo cliente. Dessa forma, economiza-se no tráfego de dados.

Para forçar a transferência da página novamente (e evitar a mensagem 304), deve-se esvaziar a cache ou forçar o navegador a recarregar sem utilizá-la (como fazer essa ação varia para cada navegador).

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

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

Porta de destino: 80

E qual o número da porta de origem?

Porta de origem: 62890

4.B) Liste o nome dos campos da camada TCP que encontrou neste pacote:

Source Port, Destination Port, Sequence Number, Acknowledge Number, Header Length, Flags, Windows Size, Checksum, Urgent Pointer e Payload.

4.C) 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).

São os pacotes de número 209 (SYN), 237 (SYN, ACK) e 242 (ACK).

Em ordem do menor tempo para o maior. Preencha:
Flag(s) de controle ligado(s) no primeiro pacote do handshake

Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
[TCP Flags: ··········S·]

Flag(s) de controle ligado(s) no segundo pacote:

Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
[TCP Flags: ·····A··S·]

Flag(s) de controle ligado(s) no terceiro pacote:

Flags: 0x010 (ACK)
000. .... = Reserved: Not set

...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····A····]

Você vai entender melhor este mecanismo quando estudarmos o nível de transporte, por enquanto basta saber que há diversos pacotes trocados para controlar a conversa.

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

Porta de origem: 80
Porta de destino: 62890

4.E) Depois da transferência da página normalmente acontece a desconexão que envolve os flags FIN e ACK. Há pacotes ligados às 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.

Os pacotes de handshake de despedida são os pacotes 318 (ACK), 523 (FIN, ACK) e 527 (ACK). O que está com o bit FIN ligado é o pacote 523. Assim:

Nº: 318
Time: 17:38:39,332266
Flag ligada: ACK

Nº: 523
Time: 17:38:44,286980
Flag ligada: FIN, ACK

Nº: 527
Time: 17:38:44,287320
Flag ligada: ACK

4.F) Agora vamos ver a quantidade de pacotes e de dados que essa conexão TCP transportou. Clique em "Statistics" e depois em "Conversations". Selecione a tab "TCP" e registre abaixo:

Considerando apenas o fluxo entre as portas 80 e 62890, temos:

Quantidade total de pacotes trocados nessa conexão: 12
Quantidade de bytes trocados nessa conexão: ~3kB
Quantidade de bytes enviados pelo cliente para o servidor: ~1 kB (7 packets)
Quantidade de bytes enviados pelo servidor para o cliente: ~1 kB (5 packets)

4.G) Que tal entender exatamente o que os dados transmitidos significam? Clique com o botão direito em qualquer pacote TCP que faz parte da comunicação entre o seu

computador e o IP do site do Kurose, selecione “Follow” e depois “TCP Stream”. Copie o output e cole aqui embaixo.

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,el-GR;q=0.8,el;q=0.7,ja-JP;q=0.6,ja;q=0.5,es-ES;q=0.4,es;q=0.3,el-CY;q=0.2,en-US;q=0.1,en;q=0.1


HTTP/1.1 200 OK
Date: Sun, 24 Aug 2025 20:38:35 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sun, 24 Aug 2025 05:59:01 GMT
ETag: "51-63d1622bb91a0"
Accept-Ranges: bytes
Content-Length: 81
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations! You've downloaded the first Wireshark lab file!
</html>

GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,el-GR;q=0.8,el;q=0.7,ja-JP;q=0.6,ja;q=0.5,es-ES;q=0.4,es;q=0.3,el-CY;q=0.2,en-US;q=0.1,en;q=0.1


HTTP/1.1 404 Not Found
Date: Sun, 24 Aug 2025 20:38:35 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Content-Length: 209
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /favicon.ico was not found on this server.</p>
</body></html>
```

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. Coloque em negrito a interface que realizou as comunicações com o IP do site do Kurose**.

```
Microsoft Windows [versão 10.0.26100.4946]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\UlissesLS>ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet:

   Estado da mídia. . . . . . . . . . . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . :

Adaptador Ethernet vEthernet (WSL (Hyper-V firewall)):

   Sufixo DNS específico de conexão. . . . . . :
   Endereço IPv6 de link local . . . . . . . . : fe80::95d7:ceef:7c5a:b37f%99
   Endereço IPv4. . . . . . . . . . . . . . . . : 172.26.240.1
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.240.0
   Gateway Padrão. . . . . . . . . . . . . . . :

Adaptador desconhecido Conexão Local 2:

   Estado da mídia. . . . . . . . . . . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . :

Adaptador Ethernet Ethernet 2:

   Sufixo DNS específico de conexão. . . . . . :
   Endereço IPv6 de link local . . . . . . . . : fe80::1b1f:3911:637d:de6d%19
   Endereço IPv4. . . . . . . . . . . . . . . . : 192.168.56.1
   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* 1:

Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Conexão Local* 2:

Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Wi-Fi:

Sufixo DNS específico de conexão. . . . . :
Endereço IPv6 . . . . . : 2804:1b3:a9c3:97d8:481f:7ed0:9d43:63d7
Endereço IPv6 Temporário. . . . . : 2804:1b3:a9c3:97d8:fda5:7fd:3604:ccb7
Endereço IPv6 de link local . . . . . : fe80::5c15:bed7:5cba:a2ea%4
Endereço IPv4. . . . . : 192.168.15.32
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : fe80::96ea:eaff:fee0:ae7a%4
192.168.15.1

Adaptador Ethernet Conexão de Rede Bluetooth:

Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

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

6.A)

Endereço IP de gaia.cs.umass.edu : 128.119.245.12
Endereço IP de seu computador: 192.168.15.32

6.B) O campo inet na saída do ifconfig é o mesmo do endereço IP que o wireshark mostrou? Espero que sim, pois o Sistema Operacional usa esta configuração ligada à sua placa de rede na hora de montar os pacotes que emite para a rede.

Sim, considerando que meu computador estava usando o Wi-Fi no momento.

6.C) Liste o nome dos campos da camada IP que encontrou neste pacote:

Version, Header Length, Differentiated Services Field, Total Length, Identification, Flags, Fragment Offset, Time to Live, Protocol, Header Checksum, Source Address, Destination Address

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:

7.A)

Endereço MAC de origem: Intel_b2:c4:60 (50:84:92:b2:c4:60)
Endereço MAC de destino: TellescomInd_e0:ae:7a (94:ea:ea:e0:ae:7a)

7.B) Liste o nome dos campos da camada MAC que encontrou neste pacote:

Destination, Source e Type.

7.C) O campo ether na saída do ifconfig é o mesmo do endereço de origem que o wireshark mostrou? Espero que sim, pois o Sistema Operacional usa esta configuração de sua placa de rede na hora de montar os pacotes que emite para a rede.

Sim, considerando que meu computador estava usando o Wi-Fi no momento.

Note como, com um simples GET quanta coisa você aprendeu da relação entre os protocolos!

7.D) Que tal bisbilhotar um pouco a sua rede local? Aplique o filtro "arp" e observe os pacotes filtrados. (Obs: ainda que você esteja usando o modo promíscuo para o wireshark fazer a captura, na rede sem fio seria preciso ativar o modo monitor e o driver teria que ser configurado para dar suporte a captura completa de todos os pacotes na vizinhança. Não é isso que estamos fazendo, aqui pegamos pacotes apenas da comunicação onde estamos envolvidos).

Sem pesquisar na Internet e usando somente o Wireshark, coloque aqui o significado do acrônimo ARP: Address Resolution Protocol

Explique com as suas próprias palavras o que a coluna "Info" está mostrando:

A coluna "info" descreve quem está perguntando por um determinado IP e quem respondeu com qual MAC.

Clique em "Statistics" e depois em "Endpoints". Quantos endereços MAC seu Wireshark detectou? Quem foi o endereço MAC mais ativo da lista?

3 endereços. O mais ativo (com mais pacotes) foi o MAC 94:ea:ea:e0:ae:7a

Selecionando "Name resolution" os endereços MAC recebem nomes um pouco mais inteligíveis. Você acha que esses nomes são atribuídos de fábrica ou existe alguma negociação de rede para que eles sejam estabelecidos?

De fábrica, pois depende do mapeamento dos primeiros bytes do MAC para aquele fabricante.

Você consegue identificar o endereço MAC do computador de algum dos seus colegas? Qual é o seu endereço IP correspondente? Esses endereços são parecidos com os endereços MAC e IP do seu computador?

Essa parte do lab eu fiz em casa, e não havia outras conexões compartilhando minha rede.

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

28 saltos no total, mas apenas 22 “efetivos” (6 tiveram o tempo esgotado).

(b) Há algum passo que tem o valor de tempo menor que o passo anterior? Por que isto aconteceria? Inclua a saída do traceroute no relatório.

Isto pode ocorrer por diversos motivos, tais como: horário do pedido (pois o fluxo na internet pode estar maior ou menor em diferentes períodos do dia); aquele determinado nó estar no momento resolvendo muitas requisições; o caminho escolhido para percorrer os roteadores, etc.

C:\Users\UlissesLS>tracert gaia.cs.umass.edu

Rastreando a rota para gaia.cs.umass.edu [128.119.245.12]
com no máximo 30 saltos:

```
 1    3 ms     4 ms     2 ms  menuvivofibra.br [192.168.15.1]
 2    *        *        *     Esgotado o tempo limite do pedido.
 3   10 ms     9 ms     8 ms  201-1-232-240.dsl.telesp.net.br [201.1.232.240]
 4   26 ms     8 ms     8 ms  187-100-171-226.dsl.telesp.net.br [187.100.171.226]
 5    *        *        *     Esgotado o tempo limite do pedido.
 6    *        *        *     Esgotado o tempo limite do pedido.
 7  125 ms   117 ms   116 ms  5.53.3.143
 8  117 ms   117 ms   116 ms  213.140.43.206
 9    *        *        *     Esgotado o tempo limite do pedido.
10    *        *      135 ms  be2258.ccr82.mia03.atlas.cogentco.com [154.54.168.86]
11  165 ms   140 ms   157 ms  be5577.ccr42.atl01.atlas.cogentco.com [154.54.82.245]
12     133  ms      133  ms      136  ms    port-channel3483.ccr92.dca04.atlas.cogentco.com
[154.54.172.169]
13  137 ms   145 ms   136 ms  be4188.ccr42.jfk02.atlas.cogentco.com [154.54.30.122]
14  174 ms   140 ms   147 ms  be3472.ccr32.bos01.atlas.cogentco.com [154.54.46.33]
15  151 ms   146 ms   147 ms  be8039.rcr71.orh02.atlas.cogentco.com [154.54.170.2]
16  180 ms   146 ms   146 ms  be8628.rcr51.orh01.atlas.cogentco.com [154.54.164.126]
17  152 ms   147 ms   146 ms  38.104.218.14
18  151 ms   146 ms   146 ms  69.16.0.9
19  153 ms   154 ms   158 ms  69.16.3.0
20  161 ms   150 ms   146 ms  core1-rt-et-4-3-0.gw.umass.edu [192.80.83.101]
21  152 ms   147 ms   156 ms  n1-rt-1-1-et-0-0-0.gw.umass.edu [128.119.0.216]
22  148 ms   146 ms   146 ms  n1-fnt-fw-1-1-1-31-vl1092.gw.umass.edu [128.119.77.233]
23    *        *        *     Esgotado o tempo limite do pedido.
24  160 ms   171 ms   150 ms  core2-rt-et-7-2-1.gw.umass.edu [128.119.0.121]
25  152 ms   155 ms   156 ms  n5-rt-1-1-xe-2-1-0.gw.umass.edu [128.119.3.33]
26  154 ms   146 ms   146 ms  cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
27    *        *        *     Esgotado o tempo limite do pedido.
28  155 ms   156 ms   156 ms  gaia.cs.umass.edu [128.119.245.12]
```

Rastreamento concluído.

OBS.: Arquivos porventura necessários para as respostas foram encaminhados juntos a este relatório, compactados na mesma pasta chamada “lab 1”