PUC CAMPINAS
PONTIFÍCIA UNIVERSIDADE CATÓLICA

Redes de computadores A

Campinas, 09 de abril de 2019

5ª Atividade

NOME:	**RA:**
Ettore Biazon Baccan	16000465
Mateus Henrique Zorzi	16100661
Matheus Martins Pupo	16145559
Murilo Martos Mendonça	16063497
Victor Hugo do Nascimento	16100588

PDF1:

1. Liste os diferentes protocolos que aparecem na coluna Protocol na janela de listagem de pacotes após o passo 7;

Protocolos: UDP, TCP, IGMPv2, DNS, GQUIC, TLSv1.2, TLSv1.3, AJP13, HTTP, MDNS, NBNS, SSDP.

2. **Quanto tempo passou de quando a mensagem HTTP GET foi enviada até que a resposta OK foi recebida? (por default, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde que a captura iniciou). Para exibir o campo Time no formato hora do dia, selecione o menu View,depois Time Display Format, então selecione Time of day.**

0.272250357 segundos

3. **qual é o endereço IP do site www.aw.com? Qual é o endereço IP da interface de rede do seu computador?**

Ip do site: 18.217.103.17

Ip da interface de rede: 192.168.0.102

4. **imprima as mensagens HTTP GET e a resposta a ela (HTTP/1.1 200 OK). Para fazer isso, selecione Print no menu File, e depois "Selected Packet Only" e "Print as Displayed". Ok (ou Imprimir) para confirmar.**

No arquivo anexo: "impressaoPDF1.pdf".

PDF2:

1. **O seu navegador executa HTTP 1.0 ou 1.1? Qual a versão de HTTP do servidor?**

Http 1.1

2. **Quais linguagens (se alguma) o seu navegador indica que pode aceitar ao servidor?**

En-US e pt-BR

3. **Qual o endereço IP do seu computador? E do servidor gaia.cs.umass.edu?**

Meu computador: 192.168.0.102

Servidor: 128.119.245.12

4. **Qual o código de status retornado do servidor para o seu navegador?**

200 OK

5. **Quando o arquivo em HTML que você baixou foi modificado no servidor pela última vez?**

Segunda, 8 de abril de 2019 - 05:59: 01GMT (alguns segundos antes da execução).

6. **Quantos bytes de conteúdo são retornados ao seu navegador?**

126 Bytes.

7. **Inspecionando os dados na janela de conteúdo do pacote, você vê algum cabeçalho dentro dos dados que não são exibidos na janela de listagem de pacotes? Caso a resposta seja afirmativa, indique um.**

Aparentemente, as requisições tem um cabeçalho e as respostas, outro.

GET: ec 08 6b 88 90 36 30 24 32 23 86 ce 08 00 45 00.

Res: 30 24 32 23 86 ce ec 08 6b 88 90 36 08 00 45 00.

8. **Inspecione o conteúdo da primeira mensagem HTTP GET do seu navegador para o servidor. Você vê uma linha "IF-MODIFIED-SINCE"?**

Não há.

9. **Inspecione o conteúdo da resposta do servidor. O servidor retornou explicitamente o conteúdo do arquivo? Como você pode dizer isso?**

Na primeira vez que a pagina foi carregada, o conteudo do arquivo foi retornado completo. Já quando atualizamos a página, ele não baixa novamente todos os arquivos, ele retorna uma mensagem de "NOT MODIFIED".

10. **Agora inspecione o conteúdo da segunda mensagem HTTP GET do seu navegador para o servidor. Você vê uma linha "IF-MODIFIED-SINCE"? Caso a resposta seja afirmativa, qual informação segue o cabeçalho "IF-MODIFIED-SINCE"?**

Sim, compara com a data: Segunda, 8 de abril de 2019 - 05:59: 01GMT

11. **Qual é o código de status e a frase retornada do servidor na resposta à segunda mensagem HTTP GET? O servidor retornou explicitamente o conteúdo do arquivo? Explique.**

O codigo de status é o 304 – Not Modified. Ele nao retorna o arquivo novamente

12. **Quantas mensagens HTTP GET foram enviadas pelo seu navegador?**

Na primeira execução, foram realizados 2 HTTP GET pelo navegador, apos atualizar a página, apenas um foi realizado.

*13. **Quantos segmentos TCP foram necessários para carregar a resposta?**

Na primeira vez que a pagina é carregada, são usados dois segmentos TCP, e a cada vez que a página é recarregada, é usado apenas um.

14. **Qual é o código de status e a frase associada com a resposta à mensagem HTTP GET?**

Código 200 – OK

Código 404 – NOT FOUND (no caso do favicon)

*15. **Há alguma linha de status HTTP nos dados transmitidos associados com um "Continuation" TCP?**

Sim, dois continuations.

16. **Quantas mensagens HTTP GET foram enviadas pelo seu navegador? Para quais endereços na Internet estas mensagens foram enviadas?**

Quatro GETs foram enviados. Endereço 128.119.245.12

17. **Você consegue dizer se o seu navegador baixou as duas imagens em seqüência, ou se foram baixadas dos dois locais distintos em paralelo? Explique.**

As requisições são sequenciais, porém, a ordem de chegada depende do tamanho dos pacotes e a distância que eles estão de quem os requisitou.

```
   701 3.007154332   192.168.1.111     159.182.31.51     HTTP     441 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
   728 3.185156603   159.182.31.51     192.168.1.111     HTTP     600 HTTP/1.1 403 Forbidden  (text/html)
   755 3.313318074   192.168.1.111     128.119.245.12    HTTP     425 GET /~kurose/cover.jpg HTTP/1.1
  1004 3.890548680   128.119.245.12    192.168.1.111     HTTP     662 HTTP/1.1 200 OK  (JPEG JFIF image)
```

18. **Qual é a resposta do servidor (código de status e frase) para a primeira mensagem HTTP GET do seu navegador?**

401 – Unauthorized.

19. **Quando o seu navegador envia a mensagem HTTP GET pela segunda vez, qual o novo campo que está incluído na mensagem?**

É incluído um campo authorization, seguido por uma linha que parece estar criptografada.

PDF3:

Execute o nslookup para cada uma das questões, e escreva os resultados:

1. **obtenha o endereço IP de um servidor web na Ásia;**

```
victor@victor-TUF-GAMING-FX504GE-FX80GE:~$ nslookup www.aiit.or.kr
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 58.229.6.225
```

Obtivemos o IP do servidor www.aiit.or.kr representado por 58.229.6.225

2. **determine os servidores DNS autoritários para uma universidade na Europa;**

Determinamos os servidores DNS autoritários para a universidade de Oxford na Inglaterra e obtemos os seguintes endereços:

dns2.ox.ac.uk 163.1.2.190

```
victor@victor-TUF-GAMING-FX504GE-FX80GE:~$ nslookup dns2.ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   dns2.ox.ac.uk
Address: 163.1.2.190
```

ns2.ja.net 193.63.105.17

dns1.ox.ac.uk 129.67.1.191

auth5.dns.ox.ac.uk 93.93.128.67

auth4.dns.ox.ac.uk 45.33.127.156

dns0.ox.ac.uk 129.67.1.190

auth6.dns.ox.ac.uk 185.24.221.32

E o servidor DNS Mestre:

nighthawk.dns.ox.ac.uk 163.1.2.189

3. **utilize um dos servidores DNS obtidos na questão 2 e consulte pelo endereço IP do Yahoo! Mail.**

Executamos o comando nslookup br.yahoo.com nighthawk.dns.ox.ac.uk e obtivemos o endereço **********.

1. **localize as mensagens de solicitação e resposta DNS. Foram enviadas com TCP ou UDP?**

Todas as mensagens foram enviadas com TCP

2. **qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte da mensagem de resposta DNS?**

443 a porta destino

32862 a porta origem no desktop do Murilo Martos

38958 a porta origem no desktop do Matheus Pupo

3. **a qual endereço IP a mensagem de consulta DNS é enviada? Utilize ipconfig para determinar o endereço IP do seu servidor DNS local. Estes endereços são os mesmos?**

104.20.1.85 - Destino

192.168.0.107 - Origem (IP do servidor local)

Sim, o endereço de origem é o mesmo obtido pelo comando ipconfig e o endereço destino é o mesmo obtido pelo *nslookup www.ietf.org*

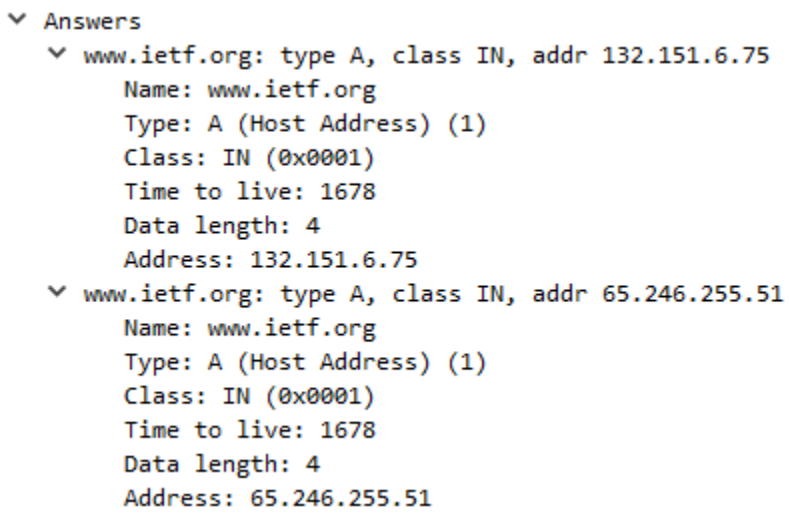
4. **examine a mensagem de consulta DNS. Qual o campo "type" desta mensagem? A mensagem de consulta contém algum campo "answer"?**

Type = IPv4

Não, as mensagens de consultam não possuem campo answer

5. **examine a mensagem de resposta DNS. Quantos campos com "answer" existem? O que há em cada uma destas mensagens?**

Existem dois campos answer



6. **considere o segmento TCP SYN subseqüente enviado pelo seu host. O endereço IP de destino do pacote SYN corresponde a algum dos endereços IP fornecidos na mensagem de resposta DNS?**

Não, o endereço enviado na resposta DNS é diferente do endereço de segmento TCP SYN

7. **a página web visitada contém imagens. Antes de recuperar cada imagem, o host realiza novas consultas DNS?**

Não, a consulta é realizada somente uma vez

1. **qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte da mensagem de resposta DNS?**

A fonte é o próprio endereço de IP local (192.168.0.104) e o destino seria o endereço de gateway padrão (192.168.0.1)

2. **a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?**

Sim, é o endereço de gateway padrão

3. **examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?**

Type = IPv4

Não, as mensagens de consulta não possuem campo answer

4. **examine a mensagem de resposta DNS. Quantos campos com “answer” existem? O que há em cada uma destas mensagens?**

As mensagens de respostas possuem 3 campos answer

```
▼ Answers
  ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.38.154.77
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: 23.38.154.77
```

5. **grave a tela de captura de pacotes**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.104	35.232.53.48	TCP	62	56251 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	1.495703	192.168.0.104	13.89.220.65	TLSv1.2	157	Application Data
3	1.661664	13.89.220.65	192.168.0.104	TLSv1.2	180	Application Data
4	1.703291	192.168.0.104	13.89.220.65	TCP	54	53473 → 443 [ACK] Seq=104 Ack=127 Win=63540 Len=0
5	3.000864	192.168.0.104	35.232.53.48	TCP	62	[TCP Retransmission] 56251 → 1688 [SYN] Seq=0 Win=64240 Len=0 MS
6	3.248009	35.232.53.48	192.168.0.104	TCP	60	1688 → 56251 [SYN, ACK] Seq=0 Ack=1 Win=28400 Len=0 MSS=1420
7	3.248123	192.168.0.104	35.232.53.48	TCP	54	56251 → 1688 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8	3.248252	192.168.0.104	35.232.53.48	DCERPC	214	Bind: call_id: 2, Fragment: Single, 3 context items: 51c82175-84
9	3.270763	192.168.0.104	64.233.186.125	TCP	55	53528 → 5222 [ACK] Seq=1 Ack=1 Win=64516 Len=1 [TCP segment of a
10	3.323733	64.233.186.125	192.168.0.104	TCP	66	5222 → 53528 [ACK] Seq=1 Ack=2 Win=65366 Len=0 SLE=1 SRE=2
11	3.497984	35.232.53.48	192.168.0.104	TCP	60	1688 → 56251 [ACK] Seq=1 Ack=161 Win=29480 Len=0
15	3.774437	35.232.53.48	192.168.0.104	DCERPC	162	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv:
16	3.774590	192.168.0.104	35.232.53.48	DCERPC	126	Alter_context: call_id: 2, Fragment: Single, 1 context items: 51
19	3.998475	35.232.53.48	192.168.0.104	TCP	60	1688 → 56251 [ACK] Seq=109 Ack=233 Win=29480 Len=0
20	4.026484	35.232.53.48	192.168.0.104	DCERPC	110	Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840
21	4.026635	192.168.0.104	35.232.53.48	DCERPC	346	Request: call_id: 2, Fragment: Single, opnum: 0, Ctx: 0 51c82175
24	4.256209	35.232.53.48	192.168.0.104	DCERPC	354	Response: call_id: 2, Fragment: Single, Ctx: 0 51c82175-844e-475
26	4.298370	192.168.0.104	35.232.53.48	TCP	54	56251 → 1688 [ACK] Seq=525 Ack=465 Win=65320 Len=0
27	4.475725	192.168.0.104	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
28	4.482031	192.168.0.1	192.168.0.104	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-a
29	4.483081	192.168.0.104	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
30	4.491696	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.e
31	4.494357	192.168.0.104	192.168.0.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
32	4.500364	192.168.0.1	192.168.0.104	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.ed
33	5.905435	192.168.0.104	192.168.1.255	TCP	62	56252 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

1. **a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?**

A fonte é o endereço IP local e o destino é o endereço de gateway padrão.

2. **examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?**

Type = IPv4

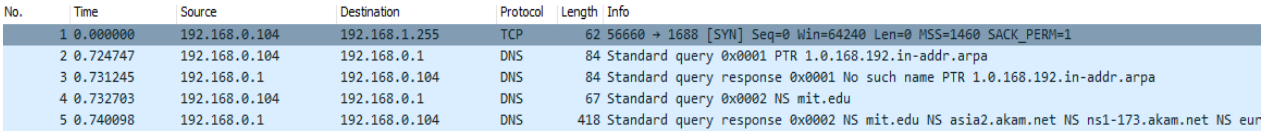
Não há campo answer na consulta

3**. examine a mensagem de resposta DNS. Quantos campos com "answer" existem? O que há em cada uma destas respostas?**

Existem 8 campos answers

- Answers
  - mit.edu: type NS, class IN, ns asia2.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 1767
    - Data length: 16
    - Name Server: asia2.akam.net
  - mit.edu: type NS, class IN, ns ns1-173.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 1767
    - Data length: 10
    - Name Server: ns1-173.akam.net
  - mit.edu: type NS, class IN, ns eur5.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 1767
    - Data length: 7
    - Name Server: eur5.akam.net
  - mit.edu: type NS, class IN, ns asia1.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 1767
    - Data length: 8
    - Name Server: asia1.akam.net
  - mit.edu: type NS, class IN, ns use5.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 1767
    - Data length: 7
    - Name Server: use5.akam.net
  - mit.edu: type NS, class IN, ns usw2.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 1767
    - Data length: 7
    - Name Server: usw2.akam.net
  - mit.edu: type NS, class IN, ns ns1-37.akam.net
    - Name: mit.edu
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)

4. **grave a tela de captura de pacotes.**



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.104	192.168.1.255	TCP	62	56660 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	0.724747	192.168.0.104	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
3	0.731245	192.168.0.1	192.168.0.104	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
4	0.732703	192.168.0.104	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
5	0.740098	192.168.0.1	192.168.0.104	DNS	418	Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS ns1-173.akam.net NS eur