Nome do alunos (grupos com até 2 elementos): Matheus Canever Fernandes e Aicha
Curso: **Graduação em Engenharia de Computação**
Disciplina: **DEC7557 - Redes de Computadores**
Assuntos: **a) Protocolo HTTP e arquiteturas de serviços em Web** **b) Protocolo HTTP: visualização de mensagens através do programa Wireshark** **c) Protocolo DNS: práticas com resolução de endereços e análise de mensagens via Wireshark** **d) Protocolo NTP**
Entrega: arquivo contendo as respostas aos questionamentos apresentados além de arquivos do Wireshark (conforme definido nas questões).
Data de entrega: 20 junho de 2023 (terça-feira)

Práticas em redes e questões teóricas

HTTP: análise de pacotes usando Wireshark

Para esta atividade, seguem recomendações antes de iniciar o teste:
a) Evitar navegações paralelas, para facilitar a visualização dos pacotes exclusivos à navegação fim. Além disso, apagar a cache do navegador.

b) Fazer a instalação do Wireshark e durante esse processo, selecionar a biblioteca/driver Npcap, pois ela é que é a interface para captura de pacotes. Também, dependendo da versão do Windows/Npcap, será questionado se o acesso ao driver Npcap será exclusido do administrador. Se for marcado esse checkbox, então, lembrar de iniciar o programa com uma conta com direitos de administrador.
Obs.: sobre o Wireshark, há duas questões: a primeira, é que se trata de um programa com interface rica para visualizar, filtrar, dissecar e apresentar pacotes, que pode ser executado como usuário comum; a segunda, se for necessário fazer captura online, então o Wireshark usará o driver do Npcap para realizar esse processo. Neste último caso, dependendo da instalação, deve ser executado como administrador.

Para responder aos questionamentos a seguir, executar os seguintes passos do teste:
a) Iniciar o Wireshark e iniciar a captura de pacotes.
b) Copiar no navegador o seguinte endereço:
http://noctilucentis.com.br/
c) Após finalizado o download das duas imagens, parar a captura de pacotes.

d) Usando o programa nslookup, encontrar o endereço IP referente ao domínio noctilucentis.com.br
e) Na barra de filtros do Wireshark, inserir ip.addr == END_ENCONTRADO_ANTERIORMENTE e dar ENTER. Serão apresentados pacotes referentes aos protocolos HTTP e TCP. Para facilitar a visualização, pode-se incluir a string http na barra de filtros e dar ENTER. No programa, menu File > Export Specified Packets, exportar para um arquivo somente os pacotes que aparecem na visualização. Este arquivo deve ser enviado junto com a tarefa: **NOME_ALUNO-pratica_redes-wireshark-http** (a extensão é adicionada automaticamente pelo Wireshark, normalmente pcapng).

Questão 1: na requisição inicial da página web, o navegador web informa cabeçalhos sobre que tipos e formatos serão aceitos. Especificamente, qual tipo de conteúdo tem *q-factor* igual a 1 e qual linguagem aceita tem *q-factor* igual a 1.

Resposta:

```
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\r\n
```

text/html e application/xhtml+xml são 1

```
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
```

pt-BR é 1.

Questão 2: foram geradas três requisições HTTP. O navegador usou um único endpoint de origem ou mais de um endpoint? Se foi mais de um, indique a linha de requisição e o respectivo endoint.

Resposta: Foram usados dois endpoints. As 3 requisições tinham o mesmo endereço de ip. Para entrar na página usou um endpoint e para baixar as duas outras imagens usou outro endpoint.

entrar na página:

```
Src Port: 56202,
```

baixar imagem 1 e 2:

```
Src Port: 56203,
```

Questão 3: sobre a mensagem HTTP que continha a imagem img-b-low.png, informe:
a) Qual o tamanho reportado e qual cabeçalho usado?
b) Se a mensagem continha cabeçalhos condicionais, quais eram e que valores continham?

Resposta:
a)

```
HTTP/1.1 200 OK
Content-Type: image/png
Content-Length: 70724
```

b)

```
Last-Modified: Sun, 04 Jun 2023 17:51:55 GMT
ETag: "647ccf3b-11444"
```

HTTP e Web

Questão 4: encontrar casos de uso para cada uma das seguintes arquiteturas de software da Web: SOAP, REST, GraphQL e gRPC e discutir as vantagens da adoção

Resposta:
SOAP: O SOAP é frequentemente usado em cenários em que a comunicação entre diferentes sistemas é necessária. Também, é muito adotado em sistemas de pagamento e serviços bancários online, pois oferece segurança e suporte a protocolos de criptografia avançados. Suas vantagens são um rigoroso suporte a padrões de comunicação e uma segurança avançada.

REST: O REST é uma arquitetura muito utilizada para construir APIs (Interfaces de Programação de Aplicativos) que fornecem acesso a recursos de aplicativos web e móveis. Também, é amplamente adotado em arquiteturas de microserviços. Suas vantagens são simplicidade, leveza e alta escalabilidade.

GraphQL: O GraphQL é uma alternativa ao REST quando há necessidade de recuperar e modificar dados complexos e em uma única chamada de API. Também, é adequado para cenários em que os dados são provenientes de várias fontes ou serviços, permitindo que o cliente solicite todos os dados necessários em uma única consulta. Suas vantagens são flexibilidade de consulta e evolução contínua do esquema.

gRPC: O gRPC é uma arquitetura adequada para aplicações distribuídas, onde há uma necessidade de comunicação eficiente e confiável entre serviços. Também, é amplamente utilizado em cenários de IoT, onde há uma variedade de dispositivos e serviços que precisam se comunicar de forma eficiente e confiável. Suas vantagens são alta performance

e suporte a várias linguagens de programação.

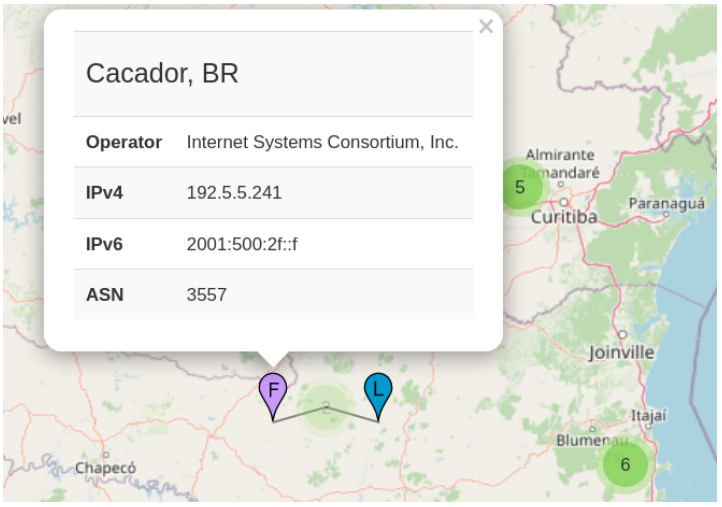
DNS

Questão 5: encontrar informações de delegação do nome .br no sítio da IANA; coletar e transcrever as informações consideradas as mais importantes

Resposta:

ccTLD Manager
Comitê Gestor da Internet no Brasil
Av. das Nações Unidas, 11541, 7. andar
São Paulo SP 04578-000
Brazil

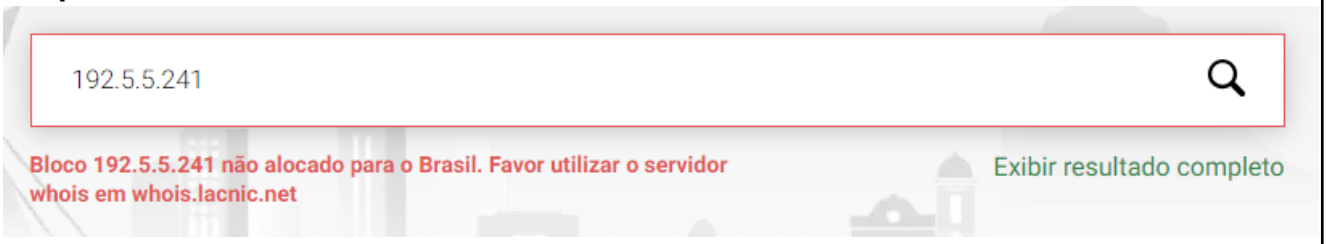
A figura ao lado apresenta um mapa com as réplicas dos 13 servidores DNS, conforme informação disponibilizada no sítio: https://root-servers.org/



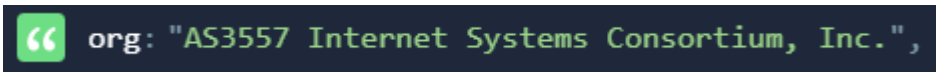
Questão 6: procurar em serviços Whois informações sobre o número ASN apresentado na figura acima:

Assunto: registro de nomes/domínios/números de AS (Autonomous System Number)
Ajuda: buscar por serviços de whois nas registradoras nacionais (Registro.br), regionais (LACNIC) e a nível mundial (IANA)
Obs.: inserir no seguinte campo somente as informações consideradas relevantes

Resposta:



Pesquisado e não encontrado no registro.br



Já no ipinfo.io consta a organização e asn.

Questão 7: pesquisar pelos seguintes **recursos** a respeito do domínio: us-east-1.console.aws.amazon.com usando a ferramenta definida a seguir.
A, AAAA, SOA, CNAME, DNSKEY, MX, PTR
Assunto: pesquisa por registros de recursos em servidores DNS
Ajuda: usar o serviço Google Admin Toolbox e a ferramenta dig para fazer a buscas pelos respectivos recursos: https://toolbox.googleapps.com/apps/main/
Obs.: inserir no seguinte campo somente as informações consideradas relevantes para cada registro de recurso obtido.

Respostas:

- A:
  - TLL: 4 minutos e 37 segundos
  - IPV4: 3.3.9.1
- AAAA: só aparece o CNAME
- SOA: só aparece o CNAME
- CNAME:
  - TLL: 55 seconds
  - IPV4: (não tem)

- DNSKEY: só aparece o CNAME
- MX: só aparece o CNAME
- PTR: só aparece o CNAME

Questão 8: fazer requisições **iterativas** em servidores DNS para resolver o seguinte nome **videira.ifc.edu.br.** ou seja, se quer o endereço IP (registro **A**).

Assunto: pesquisa por registros de recursos em servidores DNS simulando um servidor recursivo.

Ajudas: usar o programa nslookup (ou o dig, se for no Linux; existe uma versão do dig para ser instalada no Windows):
Comando:
`nslookup -type=soa|mx|a|aaaa|any nome_a_resolver  endereço_IP_server_DNS`
Ao final deste documento há um extrato de comandos nslookup.
Alguns exemplos podem ser obtidos em:
https://www.cloudns.net/blog/10-most-used-nslookup-commands

Obs.:
a) Inserir no seguinte campo as seguintes informações:
- Resposta ao questionamento; e
- Se a resposta é autoritativa ou não
b) Importante: um servidore DNS recursivo já teria essa informação, mas neste caso, pode ser necessária uma consulta recursiva para obter o endereço IP de servidores da zona root. O exemplo a seguir poderia o primeiro comando a ser executado.

Exemplo de resposta:
Comando: ***$ nslookup -type=ns .***
nameserver = m.root-servers.net.
Resposta não autoritativa

Respostas:

DNS: análise de pacotes usando Wireshark

Para esta atividade, o cache local do sistema contendo as resoluções DNS mais recentes deve ser limpo:
No Windows:
> ipconfig /flushdns
No Linux:
$ resolvectl flush-caches

Para responder aos questionamentos a seguir, executar os seguintes passos do teste:
a) Iniciar o Wireshark e iniciar a captura de pacotes.
b) No terminal, executar o seguinte comando: nslookup google.com
c) Depois de apresentada a resposta DNS no terminal, parar a captura de pacotes no Wireshark
d) Na barra de filtros do Wireshark, inserir dns e dar ENTER. Somente pacotes referentes ao protocolo DNS devem ser exibidos. No programa, menu File > Export Specified Packets, exportar para um arquivo somente os pacotes que aparecem na visualização. Este arquivo deve ser enviado junto com a tarefa: **NOME_ALUNO-pratica_redes-wireshark-dns** (a extensão é adicionada automaticamente pelo Wireshark, normalmente pcapng).

Questão 9: colar nesta a saída do programa nslookup

```
C:\Users\mathe>ipconfig /flushdns

Configuração de IP do Windows

Liberação do Cache do DNS Resolver bem-sucedida.

C:\Users\mathe>nslookup google.com
Servidor:  ns1.contato.net
Address:  201.76.0.2

Não é resposta autoritativa:
Nome:    google.com
Addresses:  2800:3f0:4001:826::200e
          142.251.132.14
```

Obs.: caso o sistema tenha configurado tanto endereço IPv4 quanto IPv6, o nslookup fará consultas considerando ambos os sistemas, logo, aparecerão duas requisições.

Questão 10: qual o identificador da transação referente à requisição pelo recurso A?

```
Transaction ID: 0x0002
```

Questão 11: qual o identificador da transação referente à requisição pelo recurso AAAA? Caso tenha.

```
Transaction ID: 0x0003
```

Questão 12: quais as informações de endpoint de origem e destino da requisição pelo recurso A? E qual protocolo de transporte usado?

```
Source Port: 49896
Destination Port: 53
Length: 36
```

<- UDP

Questão 13: referente à requisição pelo recurso A, informe o seguinte:
a) Quais flags estão ativas e qual o significado das mesmas?

```
Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
```

(Recursion Desired), que indica se o cliente deseja que o servidor DNS realize a consulta recursivamente.

b) Qual a quantidade de questões que estão na requisição?

```
Questions: 1
```

c) Qual o conteúdo do campo Queries?

```
Queries
  google.com: type A, class IN
      Name: google.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

Questão 14: referente à resposta à requisição pelo recurso A, informe o seguinte:

a) Quais flags estão ativas e qual o significado das mesmas?

```
Flags: 0x8180 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .0.. .... .... = Authoritative: Server is not an authority for domain
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive queries
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
```

(Response), que indica se é uma consulta (0) ou uma resposta (1).
(Recursion Desired), que indica se o cliente deseja que o servidor DNS realize a consulta recursivamente.
(Recursion Available), que indica se o servidor DNS suporta recursão.

b) Qual a quantidade de recursos que estão na resposta DNS?

```
Answers
  > google.com: type A, class IN, addr 142.251.132.14
```
= 1 recurso

c) Há algum recurso autoritativo?

```
Authority RRs: 0
```
= não

d) Qual o conteúdo da resposta?

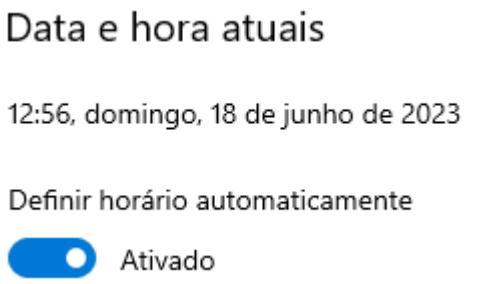
```
Answers
  google.com: type A, class IN, addr 142.251.132.14
      Name: google.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 85 (1 minute, 25 seconds)
      Data length: 4
      Address: 142.251.132.14
```

NTP (Network Time Protocol)

O Windows permite configurar a sincronizaçao de data e hora através do serviço NTP.

Questão 15: identificar:

a) Se a sincronização de tempo via NTP está ativa?



= Não sei

b) Qual o endereço do servidor de horário, se ativa?

Servidor de horário: time.windows.com

c) Quando foi a última sincronização bem sucedida?

Última sincronização de horário bem-sucedida: 14/06/2023 17:11:19

Obs.: para alterar, há necessidade de ir no Painel de Controle > Relógio e Região > Data e Hora > aba Horário na Internet. Servidores de tempo do serviço NTP.br (pertencente ao NIC.br): a.ntp.br, b.ntp.br e c.ntp.br

O leapsecond é o procedimento para atrasar ou adiantar um segundo (SI) do horário de relógio devido à diferença entre o tempo solar devido às diferenças na rotação da terra e o tempo transcorrido de um relógio atômico.

Questão 16: quando foi a última vez quando houve essa alteração e como está relacionado ao protocolo NTP?

12/31/2016

Past Leap Seconds

UTC Date	UTC Time	Difference TAI vs. UTC
6/30/2012	23:59:60	35 secs
6/30/2015	23:59:60	36 secs
12/31/2016	23:59:60	37 secs

O NTP tem suporte para a inserção de Leap Seconds em seus cálculos de tempo. Quando um Leap Second é anunciado, os servidores NTP podem transmitir essa informação para os clientes, permitindo que eles ajustem seus relógios adequadamente.