**Engenharia de Computação - Redes de Computadores A**

**Atividade 5**

|  |  |
| --- | --- |
| **Participantes** | **RA** |
| Bruno Camilo Silvério | 16080293 |
| Bruno Vicente Donaio Kitaka | 16156341 |
| Marcelo Dib Coutinho | 16023673 |
| Rafael Fioramonte | 16032708 |

**Sumário**

* **Introdução ……………………………. 2**
* **Fundamentação Teórica ……………………………. 2**
* **Resultados ……………………………. 3**
* **Conclusão ……………………………. 17**

1. **Introdução**

O experimento possibilitou um estudo inicial e a familiarização com o Wireshark, para que possamos responder a todas as perguntas relacionadas a análise de pacotes.

Wireshark nos permite exibir os conteúdos das mensagens sendo enviadas/recebidas de/por protocolos em diferentes camadas da pilha de protocolos.

1. **Fundamentação Teórica**

As redes de computadores são constituídas por múltiplas máquinas (computadores) ligadas entre si de modo que possam trocar informações a partir dessa ligação, tais dados pode ser enviados *bit* a *bit* ou na forma de pacotes.

Os pacotes de dados são constituídos por uma sequência de bytes formatados de modo que possam ser transmitidos juntos e ao chegarem a seu destino possam ser reorganizados para montar a “mensagem” enviada.

O modelo utilizado pelas redes de computadores hoje em dia é o Modelo OSI (Open System Interconnection), padrão de comunicação onde elas são dividas em 7 camadas de abstração: camada física, camada de enlace de dados, camada de rede, camada de transporte, camada de sessão, camada de apresentação e camada de aplicação. Tais abstrações são feitas para que máquinas heterogêneas possam comunicar entre si e não importe a tecnologia utilizada.

O Wireshark é um programa que analisa o tráfego de rede, e o organiza por protocolos. Através desta aplicação é possível controlar o tráfego de uma rede e monitorar a entrada e saída de dados do computador, em diferentes protocolos, ou da rede à qual o computador está ligado.

Também é possível controlar o tráfego de um determinado dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos. Se você estiver a rede local, com micros ligados através de um hub ou switch, outro usuário pode usar o Wireshark para capturar todas as suas transmissões.

1. **Resultados**

**RCA-Wireshark01-Intro.pdf**

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

R: Após a captura dos pacotes foi possível observar vários protocolos, sendo eles:

HTTP, TCP, DNS, TLSv1.2.

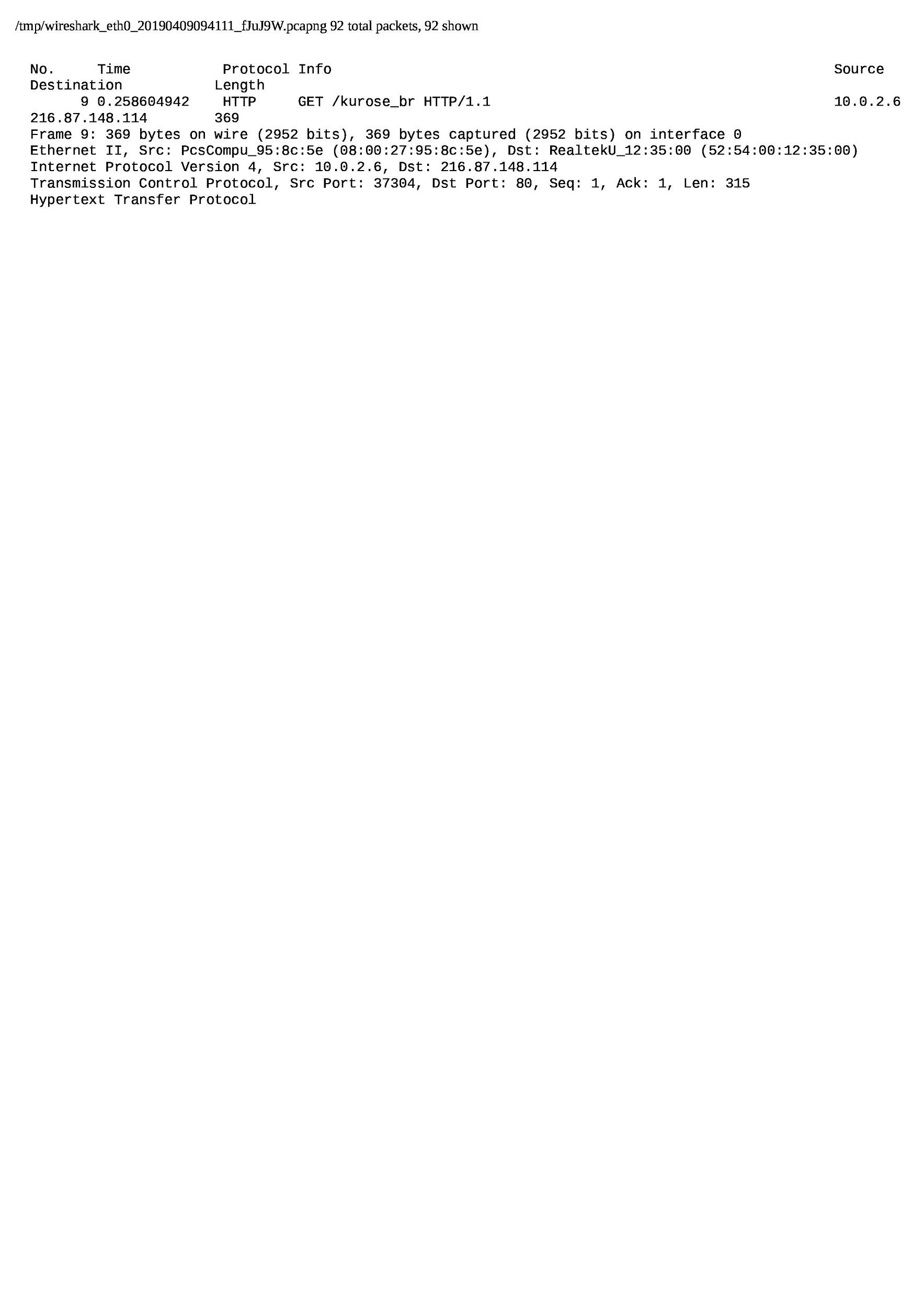
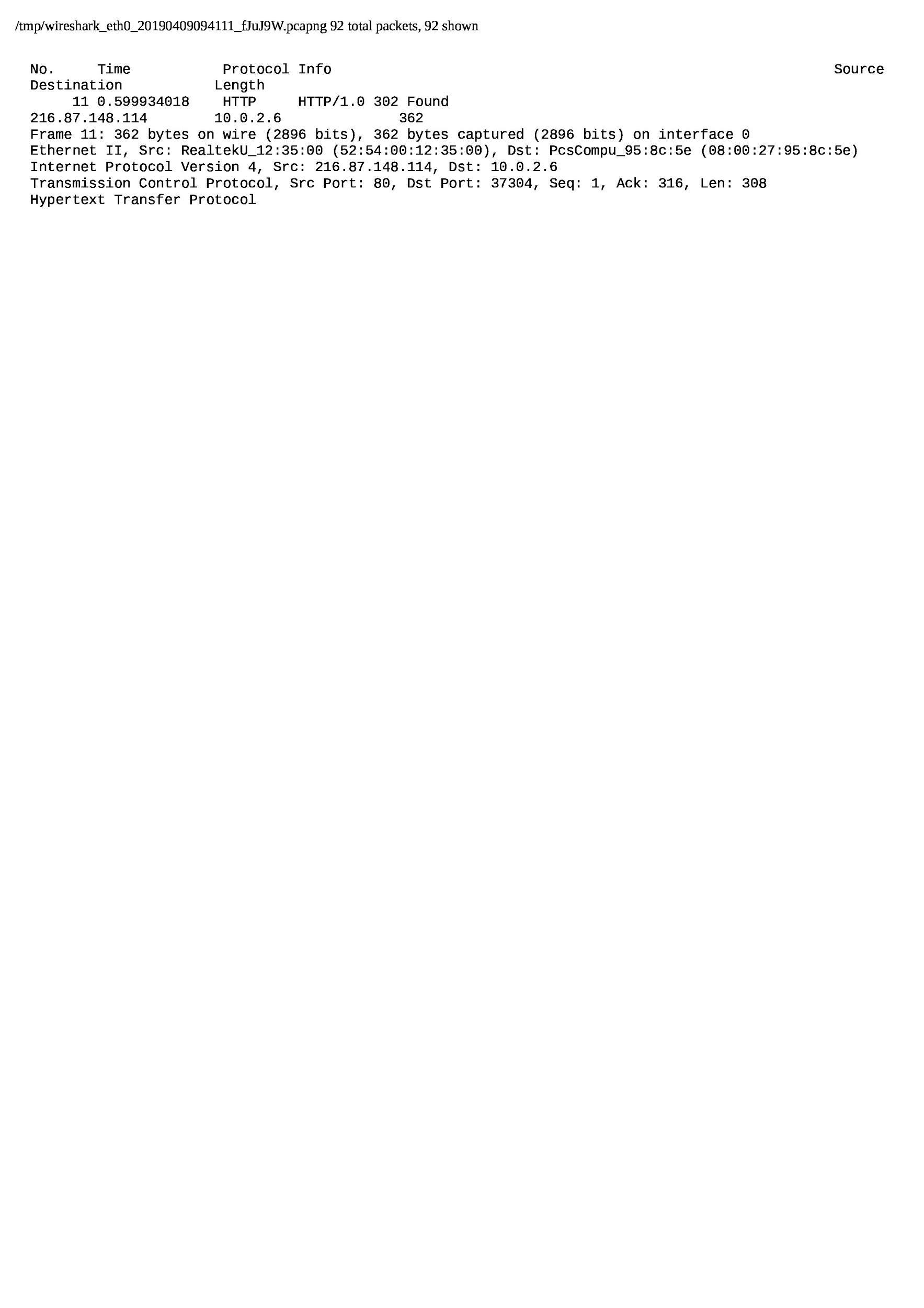
**2. quanto tempo passou de quando a mensagem HTTP GET foi enviada até que a resposta OK foi recebida? (por default, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde que a captura iniciou). Para exibir o campo Time no formato hora do dia, selecione o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

R: 0,34 segundos.

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

R: 216.87.148.114 (www.aw.com); 10.0.2.6 (Maquina utilizada).

**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.**



**RCA-Wireshark02-http.pdf**

**A Interação Básica GET/Resposta do HTTP**

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

R: O navegador executa com HTTP 1.1, porém o servidor respondeu com o a versão 1.0.

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

****

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

R: 10.22.10.6 (Maquina utilizada), 128.119.245.12

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

R: 304 Not Modified

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

R: 

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

R: Dos 293 bytes da mensagem toda, 119 bytes do protocolo HTTP são retornados ao navegador.

**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.**

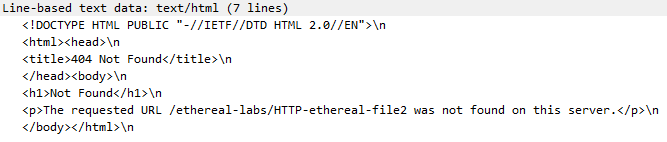
R: Não.

**A Interação HTTP GET Condicional/Resposta**

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

R: Não

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

R:

**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”?**

R: 

**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**

R: 304 Not modified, O servidor não retornou explicitamente o conteúdo do arquivo pois ele foi para a cache do navegador na primeira requisição.

**Baixando Documentos Longos**

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

R: Tres.

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

R: Nove.

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

R: 200 OK

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

R: Sim.

**Documentos HTML com Objetos Incluídos**

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

R: 3 mensagens get para os ips 128.119.245.112, 159.182.31.35, 128.119.245.112

**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.**

R: Foram baixados de dois locais em sequência, a ordem de requisições foi respectiva a ordem das urls no arquivo html.

**Autenticação HTTP**

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

R: 401 Unauthorized

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

R: 200 OK e o corpo da mensagem (página HTML).

**RCA-Wireshark03-DNS.pdf**

**nslookup**

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

R: Primeiro comando: *nslookup -type=NS cn.* (servidores da China). Usamos então o nome de uma das máquinas retornadas no segundo comando: *nslookup a.dns.cn.* . Então nos é retornado Name: a.dns.cn Address: 203.119.25.1.

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

R: Comando utilizado: *nslookup -type=NS edu.eu.* . Nos foi retornado:

ns7.dnsmadeeasy.com internet address = 208.80.126.13

ns7.dnsmadeeasy.com has AAAA address 2600:1802:7::1

ns6.dnsmadeeasy.com internet address = 208.80.124.13

ns6.dnsmadeeasy.com has AAAA address 2600:1801:6::1

ns5.dnsmadeeasy.com internet address = 208.94.148.13

ns5.dnsmadeeasy.com has AAAA address 2600:1800:5::1

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

R: Comando utilizado: *nslookup mail.yahoo.com ns7.dnsmadeeasy.com*. Reposta: “\*\* server can't find mail.yahoo.com: REFUSED”

**Rastreando DNS com o Wireshark**

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

R: UDP

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

R:



**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?**

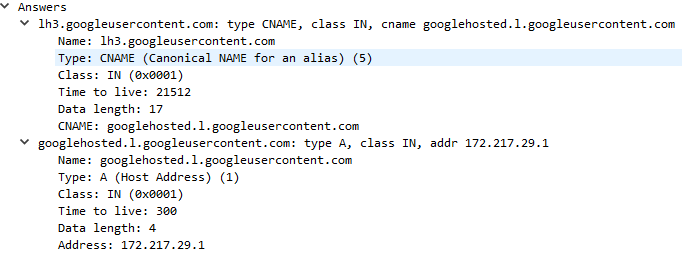
R: 



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

R:

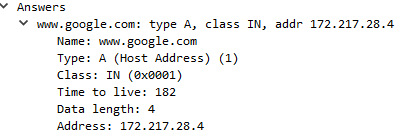
**5. examine a mensagem de resposta DNS. Quantos campos com “answer” existem? O que há em cada uma destas mensagens?**

R:

**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?**

R:





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

R: Sim.

**A figura 7 mostra o resultado da captura dos pacotes. Nela estão a mensagem de consulta e a resposta DNS. Responda às questões:**

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

R: Fonte: 34152 Destino: 53

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

R: 200.225.157.105, Não.

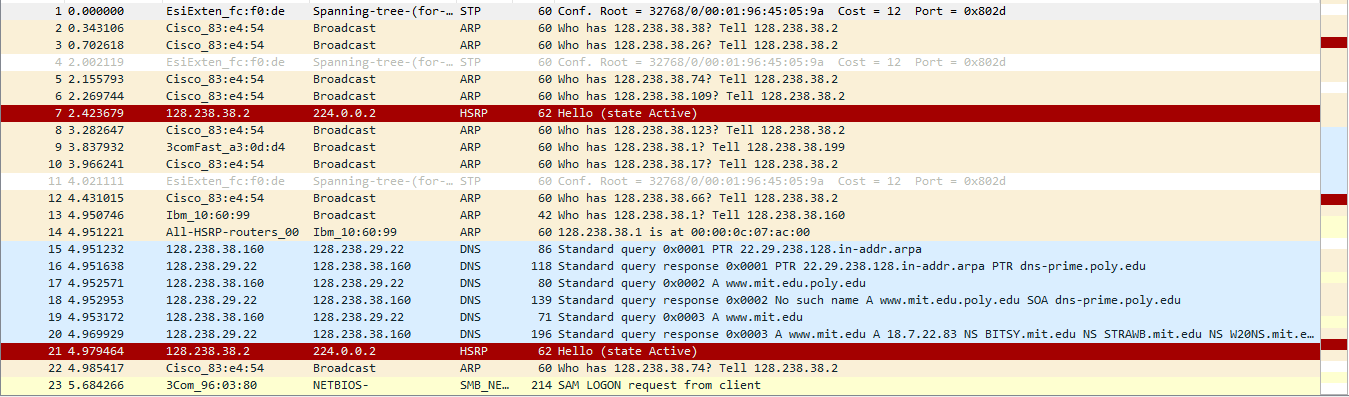
**3. examine a mensagem de consulta DNS. Qual o campo “type” que há nela? A mensagem de consulta contém algum campo “answer”?**

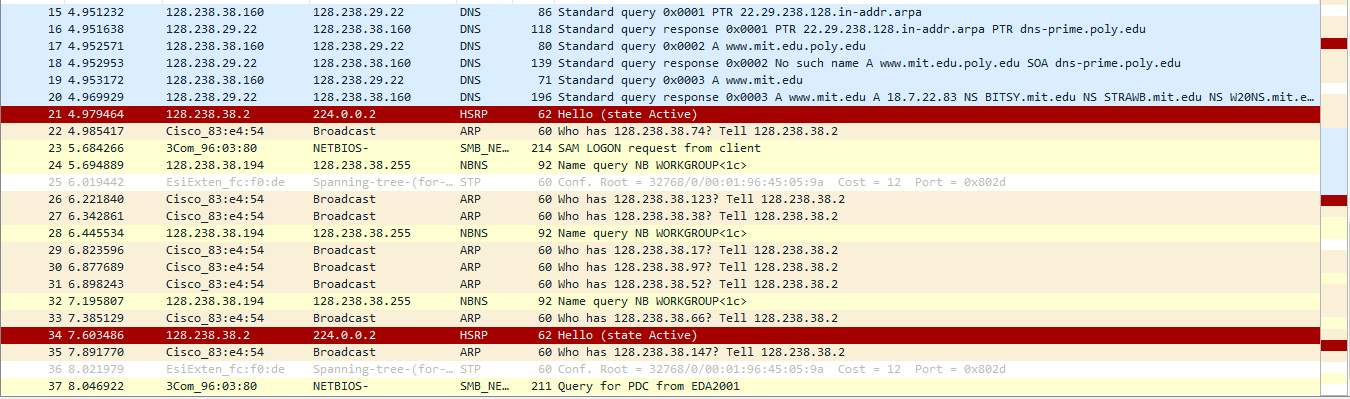
R: A (host address)

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

R: Não há campos answer.

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





**Repita o experimento anterior para o comando: “nslookup -type=NS mit.edu”, sem as aspas. Depois responda às questões:**

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

R:

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

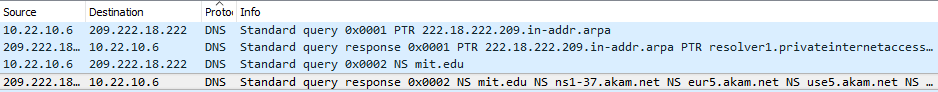
R:

**3. examine a mensagem de resposta DNS. Quais servidores DNS do MIT são fornecidos na resposta? Esta mensagem de resposta também fornece os endereços IP dos servidores DNS do MIT?**

R:



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



**Repita o experimento anterior para o comando: “nslookup www.aiit.or.kr bitsy.mit.edu”, sem as aspas. Depois responda às questões:**

**1. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais? Caso contrário, qual o host para este endereço IP?**

R:



sim

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

R:

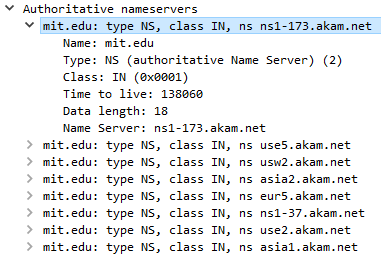
Não.

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

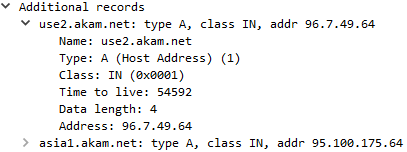
R: 3 campos



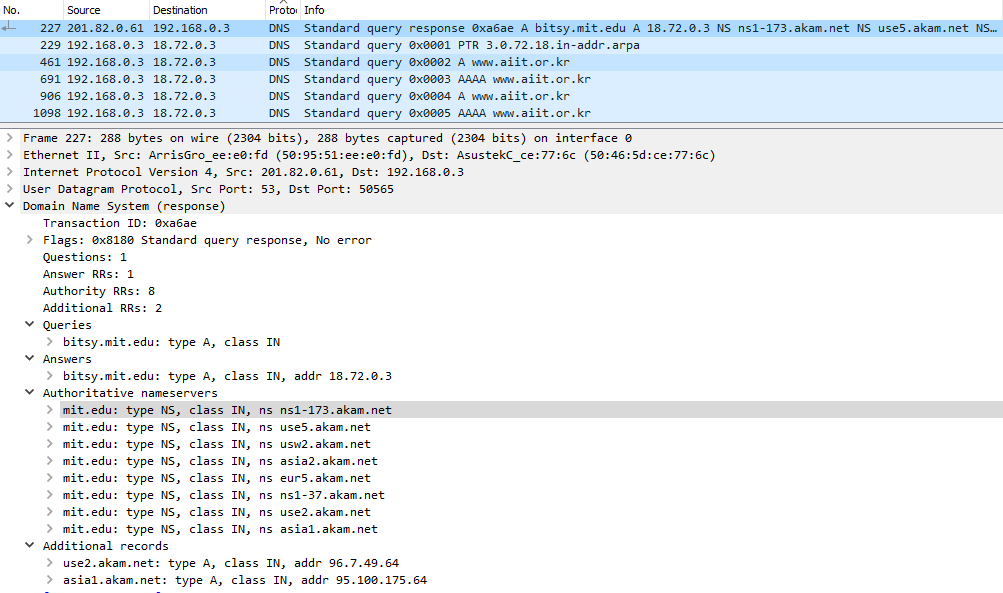
Authoritative nameservers



Additional records



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



1. **Conclusão**

Com esse experimento nos foi apresentado uma ferramenta de análise de pacote chamada Wireshark. Após as instalações do Wireshark e leitura dos PDFs, fizemos a análise da aplicação funcionando, seguindo todas as etapas para melhor entender a ferramenta e para conseguir responder às perguntas propostas pelo professor.

As questões que nos foram propostas foi para testar nossa capacidade a executar o Wireshark e explorar algumas das capacidades dele. Utilizamos o Wireshark para investigar protocolos em operação, tais como protocolo HTTP: a interação básica GET/resposta do HTTP, formatos de mensagens HTTP. E observamos mais de perto o lado cliente do DNS.