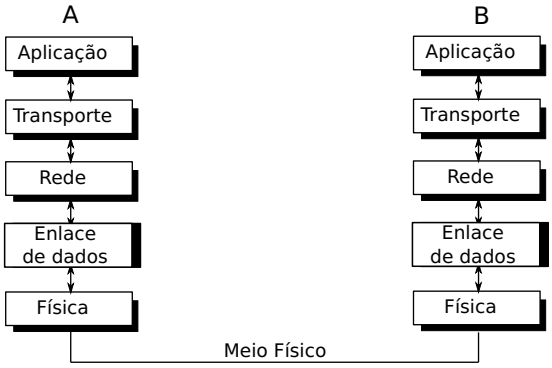
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Redes de Computadoores
Prática 03: Análise da Pilha TCP/IP com o Wireshark

Olá turma bonita, hoje compreenderemos a estrutura da pilha de protocolos TCP/IP e identificaremos os principais protocolos em cada camada da pilha TCP/IP. Para isso utilizaremos o Wireshark para capturar e analisar pacotes de rede. Vamos lá??

Pilha TCP/IP

A pilha TCP/IP é uma arquitetura de protocolos usada para comunicação entre dispositivos em redes de computadores, especialmente na Internet. Ela organiza os processos de comunicação em camadas hierárquicas, onde cada camada é responsável por uma parte específica da tarefa de envio e recepção de dados.



As camadas são: Aplicação, Transporte, Rede (ou Internet), Enlace e Física. Alguns autores consideram as camdas de Enlace e Física sendo uma única camada chamada de Acesso à Rede.

Camada de Aplicação

É a camada mais próxima do usuário ou do software de aplicação. Fornece serviços de rede diretamente para os programas que precisam se comunicar pela Internet ou por redes locais. Os protocolos mais comuns são:

- HTTP/HTTPS: Navegação na web.
- DNS: Tradução de nomes de domínio para endereços IP.
- SMTP, POP3, IMAP: Envio e recebimento de e-mails.
- FTP/SFTP: Transferência de arquivos.

Camada de Transporte

Esta camada garante a comunicação fim a fim entre dois programas (origem e destino). É responsável por endereçamento de portas, estabelecimento de conexões, controle de fluxo e congestionamento, segmentação e remontagem de dados e detecção de erros. Os protocolos mais comuns são:

- TCP (Transmission Control Protocol): protocolo orientado à conexão, garante a entrega correta dos dados, na ordem correta, com retransmissão em caso de falhas. Usado em navegação web, e-mail e arquivos.
- UDP (User Datagram Protocol): protocolo sem conexão, não garante entrega nem ordem, mais rápido, utilizado em transmissões de áudio, vídeo e DNS.

Camada de Rede (ou Internet)

A camada e Rede trata do endereçamento lógico (endereços IP) e do roteamento de pacotes entre diferentes redes. É essa camada que garante que os dados cheguem ao destino, mesmo que passem por várias redes intermediárias. O protocolo desta camada é:

- IP (Internet Protocol): responsável pelo endereçamento e roteamento dos pacotes.

Camada de Enlace

Esta camada realiza a comunicação entre dispositivos na mesma rede física. Ela garante que os dados sejam entregues corretamente entre duas máquinas diretamente conectadas, para isso realiza o endereçamento físico (endereços MAC), detecção e correção de erros, controle de acesso ao meio físico e controle de fluxo. Os principais protocolos desta camada são:

- Ethernet (IEEE 802.3): redes com fio.
- Wi-Fi (IEEE 802.11): redes sem fio.

Camada Física

Ela é responsável pela transmissão real dos bits (0s e 1s) através de meios físicos, como cabos ou ondas de rádio. Converte os quadros da camada de enlace em sinais elétricos, ópticos ou eletromagnéticos. Ela definir a representação dos bits, os padrões físicos (conectores, cabos, frequências, voltagens), realiza a transmissão e recepção de sinais analógicos ou digitais e a sincronização de bits.

Wireshark

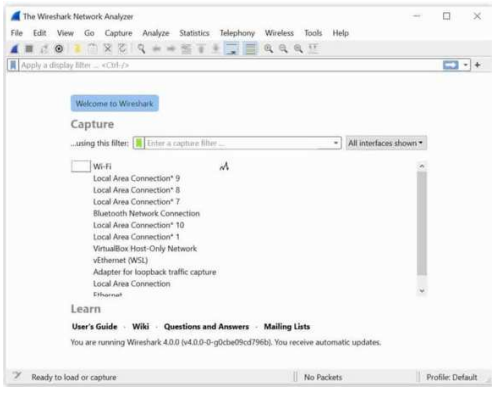
O Wireshark é uma ferramenta para análise de tráfego de rede. Com ele, é possível capturar e inspecionar pacotes da rede em tempo real, permitindo a visualização detalhada do tráfego em cada camada do modelo TCP/IP. O programa captura o tráfego de entrada e saída e organiza-os por protocolo. O Wireshark suporta uma ampla variedade de protocolos de rede, tornando-o uma ferramenta versátil para profissionais de redes, administradores de sistemas e estudantes que desejam entender melhor como as redes de computadores funcionam.

Wireshark é multiplataforma, sendo compatível com Windows, macOS e Linux, tornando-o acessível a uma ampla gama de usuários. Ele pode ser obtido gratuitamente em: `http://www.wireshark.org`.

Nas máquinas do laboratório ele já está instalada. Para iniciar o Wireshark:

1. Clique em iniciar e digite Wireshark.

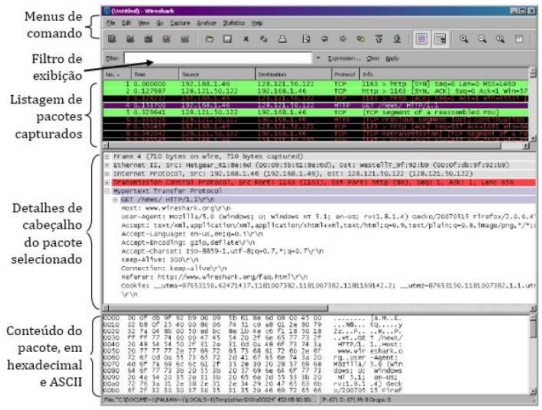
Você pode precisar de permissões elevadas, como administrador, para capturar pacotes em algumas plataformas. Será apresentado uma tela para selecionar a interface de rede.



2. Selecione a interface de rede que deseja usar para capturar pacotes (no nosso caso será Ethernet ou Conexão Local).

3. Clique em “Capture” e depois em “Start” para iniciar a captura.

Ao iniciar a ferramenta, você verá os pacotes sendo exibidos na tela principal do Wireshark.



4. Observe os pacotes que estão entrando e saindo da sua placa de rede em tempo real.

5. Selecione um pacote específico e visualize os protocolos de cada camada e seus respectivos campos (informações).

Atividade

1. Em dupla, começe ( ) ou reiniciar a captura ( ) dos tráfegos na placa de rede de acesso a Internet;

2. Com o Wireshark ainda em execução, abra o seu navegador e acesse a seguinte `http://www.exemplo.com`.

Seu computador irá trocar mensagens DNS e HTTP com o servidor para fazer o download dessa página. As mensagens trocadas entre o seu computador e o servidor serão então capturadas e exibidas pelo Wireshark na janela de captura.

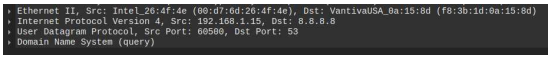
3. Após a página ser exibida interrompa a captura de pacotes no wireshark com o ícone de parar captura( ).

4. Na janela de filtro do Wireshark digite o filtro a seguir e selecione o botão “Apply”.

```
dns.qry.name == ”www.exemplo.com”
```

5. Procure e selecione a mensagem “ query ... A example.com OPT”. Esta mensagem é uma requisição feita pelo seu computador para a um servidor DNS (Domain Name System) para resolver o nome de domínio do site (exemplo.com) em seu endereço IP correspondente.

Observe que o seu Sistema Operacional para realizar a consulta para resolver o endereço, ele utilizou vários protocolos na camada de Aplicação (Domain Name Server - DNS), Transporte (User Datagram Protocol - UDP), Rede (Internet Protocol - IP) e Enlace (Ethernet). Se você clicar em um protocolo deste verá o que cada um envie de informações para os equipamentos que estão no meio do caminho e para o destino final.

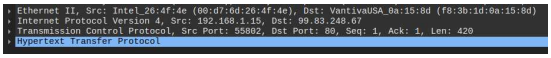


6. Descubra a mensagem de resposta e identifique qual foi o endereço IP retornado.

7. Na janela de filtro do Wireshark agora digite o filtro a seguir e selecione o botão "Apply".

ip.addr == 99.83.248.67 && http

Observe que o seu Sistema Operacional para solicitar a página web utilizou vários protocolos na camada de Aplicação (Hypertext Transfer Protocol - HTTP), Transporte (Transmission Control Protocol - TCP), Rede (Internet Protocol - IP) e Enlace (Ethernet). Se você clicar em um protocolo deste verá o que cada um envie de informações para os equipamentos que estão no meio do caminho e para o destino final.



Agora abra um arquivo de texto e responda os seguintes questionamentos.

7. Cite três informações que são inseridas na mensagem HTTP GET na solicitação da página web, são elas:

- Request Method:
- User Agent:
- Accept-Language:

8. Observe as informações do protocolo Transmission Control Protocol (TCP) e responda:

- Source Port:
- Destination Port:
- Windows:
- Checksum:

9. Observe as informações do protocolo Internet Protocol (IP) e responda:

- Source Address:
- Destination Address:

Coloque o arquivo com as respostas no Google Sala de Aula. Informe também os componentes do grupo.