

Pontifícia Universidade Católica do Paraná Escola Politécnica

Bacharelado em Ciência da Computação Bacharelado em Sistema de Informação Bacharelado em Engenharia de Software

Disciplina: Clínica de Tecnologia da Informação e Comunicação

Carga Horária: 4ha/3ha Professor: Alison Luis Lando

Estudante: Gustavo Furini, Gabriel Maron, Theo Cesar e Thomas Frentzel_

TDE II – Trabalho Discente Efetivo

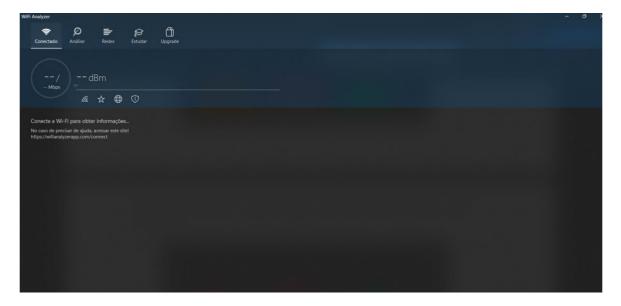
Identificação de ferramentas de análise de redes de computadores

Descrição da Atividade:

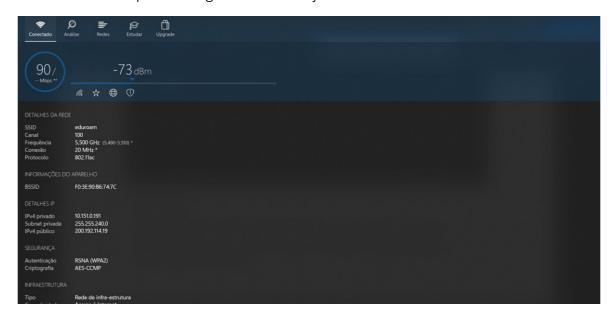
Montar Tutorial para a utilização de ferramentas de análise de redes de computadores.

1. Identificar uma ferramenta para análise de redes sem fio e criar um tutorial passo a passo sobre seu funcionamento. Responda como a ferramenta pode ajudar a identificar instabilidade e lentidão em uma rede sem fio.

Ao entrar no wifi analyzer uma aba como essa irá aparecer, é necessário que você esteja concetado a uma rede para conseguir utilizar da plataforma



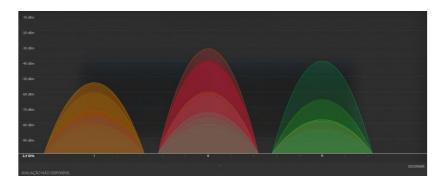
Ao conectar irá aparecer algumas informações sobre a sua rede:



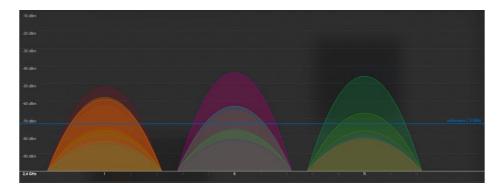
Aba de Análise:

Você pode verificar o gráfico momentaneo ao clicar em "Análise" para ver quais canais estão mais congestionados e quais não estão. A linha mais grossa representa a rede conectada, e, se quiser ver apenas as redes sobrepostas em cores, desative "Mais cores".

- Laranja: Escala para a intensidade do sinal (mais detalhes no meu tutorial "Fundamentos do Wi-Fi").
- Verde: Banda atual visualizada.
- Amarelo: Números dos canais (mais detalhes no meu tutorial "Fundamentos do Wi-Fi").
- Branco: Redes encontradas por canal (ativado pelo botão "Visualizar").

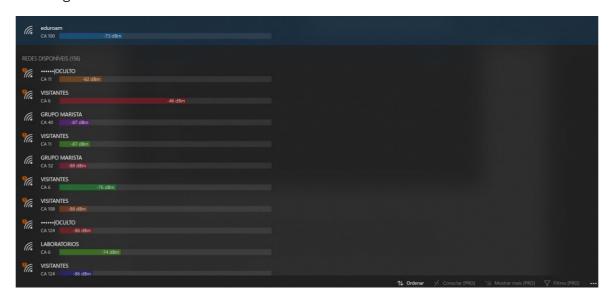


Caso apareça uma linha azul no gráfico ela mostra que você está conectado em outra banda, tornando a avaliação indisponível por falta de referência na mesma frequência:



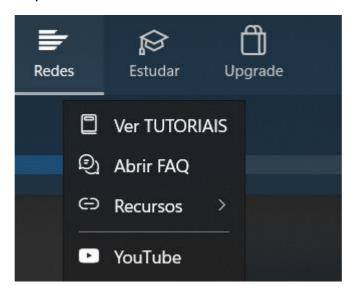
Aba de Redes:

Ao clicar na aba "Redes" você pode visualizar todas as redes disponíveis, como na imagem abaixo:



Aba Estudar:

Aqui você consegue assistir mais alguns tutorias no site do WifiAnalyzer, ver algumas perguntas frequentes caso esteja em dúvida e visualizar os recursos disponíveis.

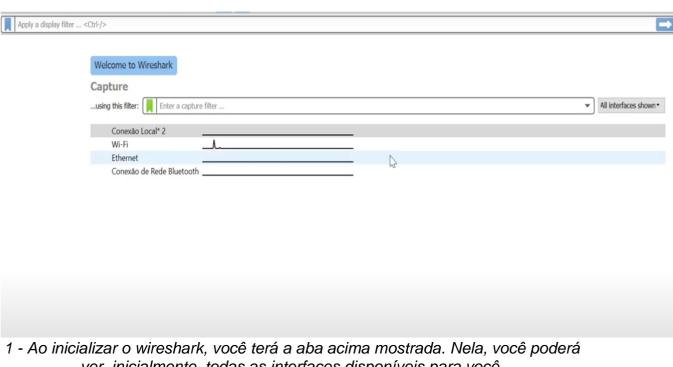


Há muitas funções como filtrar as redes, mostrar SSID em gráficos, mostrar BSSID em gráficos, contar as redes, importar as redes e etc.... que facilitam muito na análise, mas que você consegue ter acesso somente com o Pro.

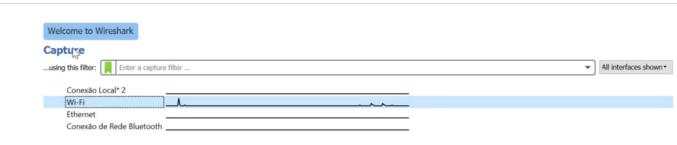
OPÇÕES DO PRO Suporte a Live Tiles * 믊 序 Mostrar o SSID em gráficos Ð Mostrar o BSSID em gráficos (9) Contagem de rede (iD Bip para a intensidade do sinal 5< Importar redes 7 Usar filtros Detalhes da rede \Box Definir o tempo limite da tela ** € Rotação da tela de bloqueio ** 园 Intensidade do sinal Experimente 1h ATUALIZAÇÃO PARA O PRO *** Compre as opções PRO para uma melhor experiência. Pagar R\$ 36,95 * https://wifianalyzerapp.com/livetile ** Isso deve ser ativado nas configurações antes de usar *** As compras no app são válidas para todos os dispositivos que você usar com esta conta da Microsoft. No caso de precisar de ajuda, acessar este site! https://wifianalyzerapp.com/upgrade / Sair

2. Pesquisar sobre a ferramenta Wireshark (https://www.wireshark.org/) e criar um tutorial passo a passo sobre seu funcionamento

O Wireshark é um analisador de rede de código aberto amplamente utilizado que pode capturar e exibir detalhes em tempo real do tráfego de rede.



ver, inicialmente, todas as interfaces disponíveis para você.



2 - Se você quiser analisar umas dessas interfaces em específico, você pode clicar duas vezes com o mouse encima dela ou clicar uma vez e, em seguida apertar em Capture (como mostrado na imagem).

```
282 Unknown operation (12) 0x7236 Unknown (11543) <Root>[Malformed Packet] 60 443 \rightarrow 54867 [ACK] Seq=1 Ack=3218 Win=65535 Len=0 60 443 \rightarrow 54731 [ACK] Seq=1 Ack=1610 Win=385 Len=0
      44 2.467043
                                        177.47.27.152
                                                                                192,168,15,6
      45 2.535820
46 2.544318
                                        50.16.174.43
34.197.12.217
                                                                                192.168.15.6
192.168.15.6
      47 2.544318
                                        34.197.12.217
                                                                                192.168.15.6
                                                                                                                                            246 Application Data
      48 2.581044
49 2.585801
                                       50.16.174.43
192.168.15.6
                                                                                192.168.15.6
34.197.12.217
                                                                                                                        TLSv1...
TCP
                                                                                                                                           879 Application Data
879 Application Data
54 54731 → 443 [ACK] Seq=1610 Ack=193 Win=257 Len=0
54 54867 → 443 [ACK] Seq=3218 Ack=826 Win=64515 Len=0
      50 2.627192
                                        192.168.15.6
                                                                                50.16.174.43
      51 3.770252
52 3.800602
53 3.982368
                                       2804:7f1:e 99:c5c9...
2606:4700:e4::ac40...
192.168.15.6
                                                                                                                                             To Satis 443 [ACK] Seq=1 Ack= Win=26 Lens [TCP segment of a reassembled PDU]

86 443 + S8154 [ACK] Seq=1 Ack=2 Win=29 Lens [TCP segment of a reassembled PDU]

85 58123 + 443 [ACK] Seq=1 Ack=1 Win=25 Lens [TCP segment of a reassembled PDU]

75 S8117 - 443 [ACK] Seq=1 Ack=1 Win=260 Lens [TCP segment of a reassembled PDU]
                                                                                2606:4700:e4::ac40... TCP
                                                                                2804:7f1:e109:c5c9...
151.101.92.157
                                        2804:7f1:e109:c5c9... 2800:3f0:4001:801:...
      54 4.056068
                                       151.101.92.157 192.168.15.6
192.168.15.6 104.244.42.5
2800:3f0:4001:801:... 2804:7f1:e109:c5c9...
                                                                                                                                              56 443 + 58123 [ACK] Seq=1 Ack=2 Win=61 Len=0 SLE=1 SRE=2

55 58126 + 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment

86 443 + 58117 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2
      55 4.056517
      56 4.073140
57 4.088556
      58 4.105592
                                        104.244.42.5
                                                                                192.168.15.6
                                                                                                                                              66 443 → 58126 [ACK] Seg=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
                                   2804:7f1:e109:c5c9... 2600:9000:2025:180... TCP
                                                                                                                                             75 58157 + 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HonHaiPr_a6:80:eb (68:14:01:a6:89:eb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
     ff ff ff ff ff 68 14 01 a6 89 eb 08 06 00 01 08 00 06 04 00 01 68 14 01 a6 89 eb c0 a8 0f 06 00 00 00 00 00 c0 a8 0f 01
```

3 - Ao clicar na interface, a tela do analisador de pacotes se abrirá para você.

No.		Time	Source	Destination	Protocol	Length	Info
	222	21.512658	77.234.42.239	192.168.15.6	HTTP	234	4 HTTP/1.1 200 OK
	223	21.515730	192.168.15.6	77.234.42.239	HTTP	356	GET /R/A3gKIGIwYzN10TI3NTRjOTRiMmNhYWRjMmY3YTY4NzY0ZmEyEgQCBQQZGIUCIgEFKgcIBBDN855tKgcIAxCO45
	224	21.600606	2800:3f0:4001:814:	2804:7f1:e109:c5c9	TLSv1	137	7 Application Data
	225	21.600606	2800:3f0:4001:814:	2804:7f1:e109:c5c9	TCP	74	4 443 → 55045 [FIN, ACK] Seq=64 Ack=2 Win=124 Len=0
	226	21.601085	2804:7f1:e109:c5c9	2800:3f0:4001:814:	TCP		4 55045 → 443 [ACK] Seq=2 Ack=65 Win=256 Len=0
	227	21.601338	2804:7f1:e109:c5c9	2800:3f0:4001:814:	TCP	74	4 55045 → 443 [FIN, ACK] Seq=2 Ack=65 Win=256 Len=0
	228	21.601624	2804:7f1:e109:c5c9	2800:3f0:4001:814:	TCP	74	1 55045 → 443 [RST, ACK] Seq=3 Ack=65 Win=0 Len=0
	229	21.634913	2800:3f0:4001:814:	2804:7f1:e109:c5c9	TCP	74	4 443 → 55045 [ACK] Seq=65 Ack=3 Win=124 Len=0
	230	21.635194	2804:7f1:e109:c5c9	2800:3f0:4001:814:	TCP	74	1 55045 → 443 [RST] Seq=3 Win=0 Len=0
	231	21.652686	77.234.42.239	192.168.15.6	TCP	60	0 80 → 51732 [ACK] Seq=181 Ack=303 Win=5 Len=0
	232	21.800380	54.230.227.183	192.168.15.6	TLSv1	100	Application Data
	233	21.800381	54.230.227.183	192.168.15.6	TLSv1	85	5 Encrypted Alert
	234	21.800382	54.230.227.183	192.168.15.6	TCP	60	0 443 → 55006 [FIN, ACK] Seq=78 Ack=2 Win=226 Len=0
	235	21.800775	192.168.15.6	54.230.227/183	TCP	54	4 55006 → 443 [ACK] Seq=2 Ack=78 Win=260 Len=0
	236	21.801089	192.168.15.6	54.230.227.183	TCP		\$ 55006 → 443 [ACK] Seq=2 Ack=79 Win=260 Len=0
	237	21.801765	192.168.15.6	54.230.227.183	TCP	54	4 55006 → 443 [RST, ACK] Seq=2 Ack=79 Win=0 Len=0

4 - Aqui nós temos três "seções": A primeira delas é a de cima, na qual é mostrado os pacotes que estão chegando um por um pela rede. Temos também diversas colunas: No (Número de sequência); Time (Intervalo de tempo); Source (endereço de origem) e Destination (endereço de destino), podendo ser endereço IP ou endereço MAC; Protocol (protocolo); Length (tamanho do pacote); Info (informações adicionais do pacote ou do protocolo).

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: HonHaiPr_a6:89:eb (68:14:01:a6:89:eb), Dst: Broadcast (ff:ff:ff:ff:ff:)
> Address Resolution Protocol (request)
```

5 - Essa aqui é a segunda "seção". Aqui são mostrados detalhes de cada pacote (primeira "seção"). Ao pressionar qualquer um dos pacotes apresentados na primeira seção, essa tela mostrará os detalhes do pacote escolhido, exemplo mostrado na imagem abaixo.

```
866 141.361956 192.168.15.6 162.220.63.163 TCP 54 58173 → 443 [RST, ACK] Seq=2 Ack=79 Win=0 Len=0

81 7.035705 2804:7f1:e109:c5c9... 2a03:2880:f0ff:2:f... TCP 75 58174 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of the control of the cont
```

6 - Ao selecionar qualquer um dos cabeçalhos apresentado na imagem acima, você poderá informações adicionais sobre eles.

```
Transmission Control Protocol, Src Port: 58173, Dst Port: 443, Seq: 1, Ack: 1,
    Source Port: 58173
    Destination Port: 443
    [Stream index: 17]
    [TCP Segment Len: 1]
    Sequence number: 1 (relative sequence number)
    [Next sequence number: 2 (relative sequence number)]
0000 10 72 23 eb fa 86 68 14 01 a6 89 eb 08 00 45 00  r#··h·····E·
```

7 – TCP: Abrindo as informações do protocolo TCP podemos ver a porta de destino 443, que é a porta do protocolo HTTPS (destino com criptografia e autenticação, no caso).

```
Internet Protocol Version 4, Src: 192.168.15.6, Dst: 162.220.63.163
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0x0aa3 (2723)
    Flags: 0x4000, Don't fragment
```

8 - IP

```
Ethernet II, Src: HonHaiPr_a6:89:eb (68:14:01:a6:89:eb), Dst: Tellesco_eb:fa:86 (10:72:23:eb:fa:86)

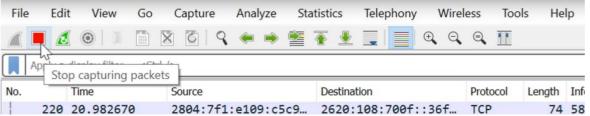
Destination: Tellesco_eb:fa:86 (10:72:23:eb:fa:86)

Source: HonHaiPr_a6:89:eb (68:14:01:a6:89:eb)

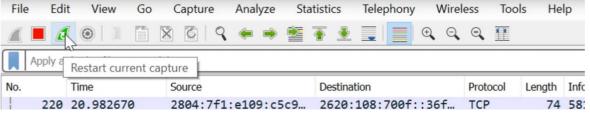
Type: IPv4 (0x0800)
```

9 - Ethernet

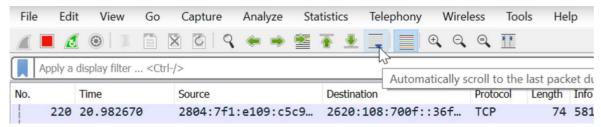
10 - Aqui temos a terceira "seção", que vai mostrar a informação em hexadecimal.



11 - Aqui nós temos botões que também são importantes para o uso do Wireshark. Esse primeiro é responsável por parar a captura de pacotes.



12 - Esse aqui reinicia a captura de pacotes.



13 - Esse aqui ao ser ativado, mantém a barra de scroll estabilizada nos últimos pacotes que estão chegando. Isso permite verificar em tempo real o recebimento dos pacotes.



14 - Esse aqui permite ao usuário colocar cores nos pacotes e suas informações. Por exemplo: Cores vermelhas ou pretas representam algum tipo de incidente ou problema momentâneo.

REFERÊNCIAS

Wireshark: https://www.youtube.com/watch?v=zp45Qv2nLWU