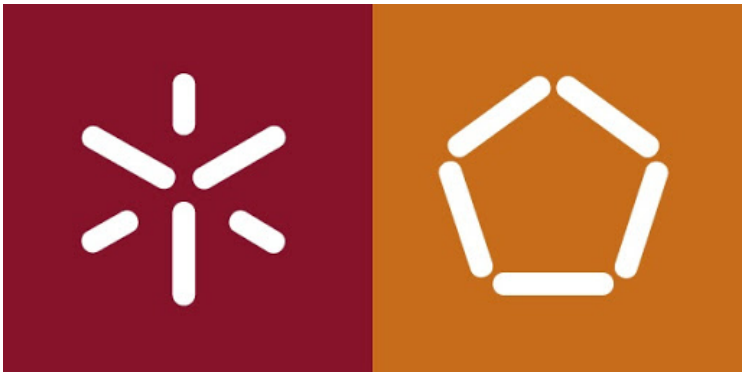
Tarefa Prática 2

Modelação e Caracterização de Tráfego

PG39254 - Igor Araújo
PG39255 - Matheus Gonçalves
PG41017 - I-Ping



Departamento de Informática
Universidade do Minho
Braga - Portugal
13 de março de 2020

Sumário

Objetivo

Realizar a captura, visualização, análise e filtragem de tráfego de rede, onde no final desse relatório o grupo vai estar mais familiarizado com as ferramentas e os conceitos de captura e análise de tráfego.

Parte I - Captura e análise de tráfego

a) Inicie a captura de tráfego na interface de rede disponível. Faça uma primeira análise comparativa dos cabeçalhos e formatos dos PDUs do protocolos TCP, UDP e IP. Identifique para cada um deles os campos geralmente utilizados na classificação de tráfego:

O protocolo TCP possui header que contém diversos campos, mas os campos que são utilizados geralmente para identificação e classificação de um tráfego são as portas de origem e destino, e da mesma maneira para o UDP. Além destas, para a melhor classificação do tráfego é utilizado também os campos da PDU da camada de redes IP, que utilizam os endereços de origem e destino IP o número de protocolo, assim é formada a 5 tupla. Em posse desses parâmetros é possível em muitos casos classificar o tráfego. Porém a cada dia novas aplicações com diversos tipos de tráfegos são enviadas através de tráfegos encriptados o que torna ainda mais difícil sua identificação e classificação. Pode-se observar tais campos mencionados na figura 1.

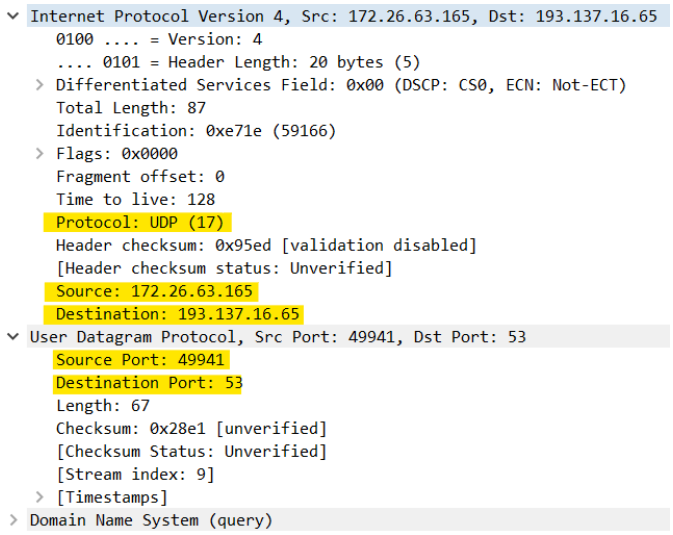


Figura 1. Exemplificação de PDU.

b) Utilizando o sniffer em modo de captura, proceda à invocação de várias aplicações conhecidas, nomeadamente:

- Acesso via browser ao URL: http://marco.uminho.pt
- Acesso ftp (anonymous): ftp.di.uminho.pt
- Acesso em tftp para router-ext (193.136.9.33)
- Acesso via telnet para router-ext (193.136.9.33) ou para router-lab (192.168.90.254)
- Acesso ssh para qualquer host da sala de aula
- Resolução de nomes usando nslookup www.uminho.pt
- traceroute cisco.uminho.pt

e construa uma tabela onde, para cada aplicação, conste o protocolo de transporte e a porta de atendimento do servidor (quando aplicável).

Protocolo de Transporte	Porta de Origem	Porta de Destino
HTTP	6	87837
FTP	7	78
TFTP		69
TELNET	545	23
SSH	88	22
DNS	88	53
ICMP	88	53

Tabela 1. Tabela de aplicações

Parte II - Filtragem de tráfego

a) Explore e descreva:

i A utilidade dos filtros de captura e visualização;

ii A sintaxe e semântica dos filtros.

Dê alguns exemplos simples de utilização dos mesmos.

Os filtros, tal como sugere, são opções que nos permitem selecionar um conjunto de informação a ser apresentadas no visualizador. Esse filtro pode ser utilizado por protocolo, endereço de rede, por porta, por endereço MAC. Eles possuem uma forma bem simples de se utilizar, basta aplicarmos no campo de pesquisa o que queremos mostrar. No exemplo a seguir iremos filtrar pelo protocolo TELNET.

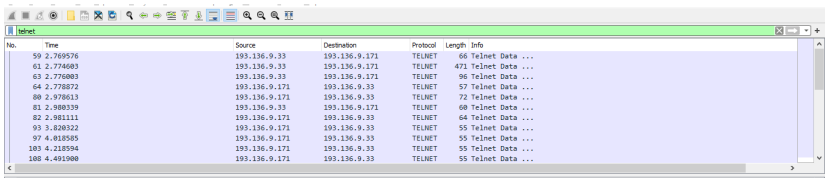


Figura 2. Exemplo aplicação do filtro TELNET.

Como exemplo utilizamos o protocolo TELNET, e sua semântica de pesquisa, nesse caso, é bem simples, bastando apenas escrever o protocolo, mas caso queremos procurar o ip, a semântica permite adicionar outras informações, como o ip.dst, que seria o IP destino.

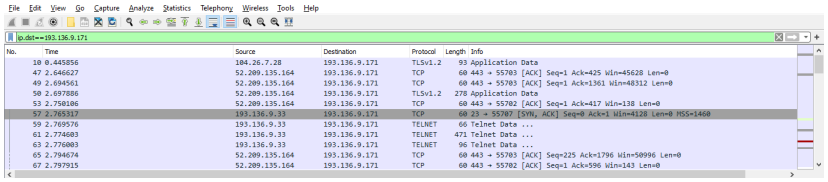


Figura 3. Exemplo aplicação do filtro IP.DST.

Também permite adicionar operadores lógicos, por exemplo o símbolo || que permite pesquisar dois protocolos ao mesmo tempo.

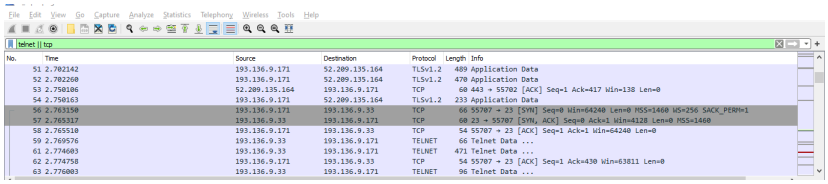


Figura 4. Exemplo aplicação do filtro com duplo parâmetros.

E por fim, o Wireshark possui uma opção no menu onde é possível consultar todos os filtros que existem para ser aplicado, e montar qual o filtro melhor se encaixa na pesquisa que deseja realizar.

b) Baseando-se nas tramas capturadas acima (1.b), e em outros exemplos que achar conveniente, explore a utilidade e utilização dos filtros de captura e visualização, nomeadamente na captura/visualização de:

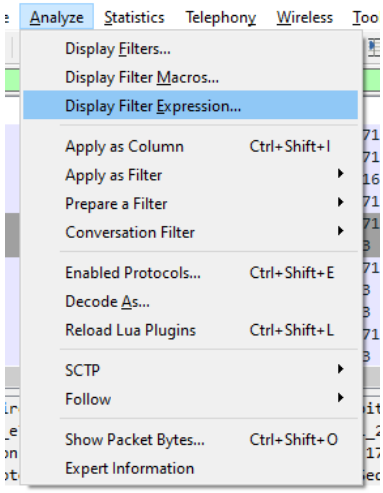


Figura 5. Aba para acesso ao menu avançado com todos os filtros.

- protocolos aplicacionais;
- protocolos de transporte;
- endereços IP;
- pacotes com valores específicos nos campos principais dos cabeçalhos de transporte e rede (ver opção "+Expression");
- pacotes com flags de iniciação e termino de conexões TCP;

Exemplifique a exploração que realizou, indicando a sintaxe utilizada nos filtros e, muito sucintamente os resultados obtidos.

Aqui podemos mostrar a análise do arquivo gerado anteriormente. Em nosso exemplo vamos procurar a utilização de um protocolo para transferência de um ficheiro. Começamos por filtrar a captura, utilizando a sintaxe mais simples possível: TFTP. Podemos ver o resultado obtidos na imagem 7

Indo para a análise de um pacote, visualizando suas informações, podemos verificar que ele utiliza como protocolo de transporte o UDP (figura 8), em seguida podemos verificar os endereços MAC dos dispositivos e os Ips utilizados (origem/Destino – figura 9).

E por último, nesse exemplo utilizado, podemos conferir as portas da aplicação que são utilizadas e como se trata de um protocolo com mensagem junto, ele nós informa qual o código enviado pela origem (figura 10).

E claro, ao montar o stream desse filtro(figura 11), podemos acompanhar qual foi a solicitação e a mensagem retornada pelo destino, conforme a figura 12.

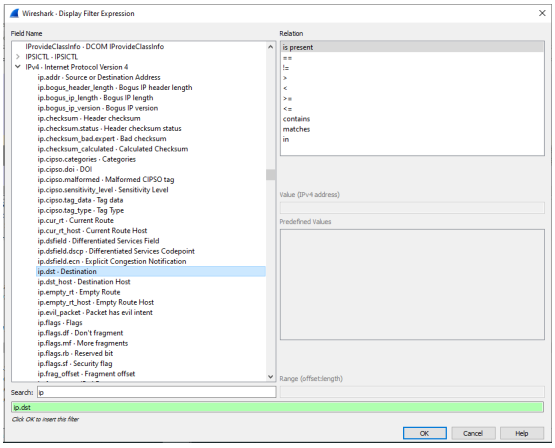


Figura 6. Display com todos os filtros.

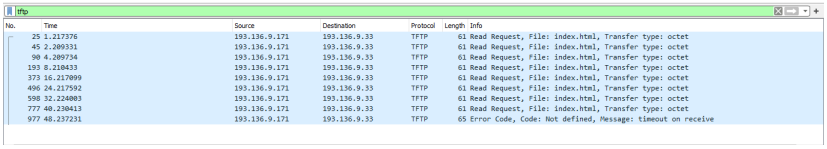


Figura 7. Aplicando o filtro para o protocolo TFTP.

c) Para uma das aplicações que usam o protocolo TCP (e.g. Telnet router-ext), explore a opção "Analyse - Follow TCP Stream". Indique os filtros automaticamente aplicados por essa opção. Discuta eventuais fragilidades de segurança e confidencialidade dos dados.

Com a opção de filtragem via menu Analyse > Follow > TCP Stream, é possível selecionar um pacote entra vários capturados e reunir todos os pacotes que pertencem ao mesmo stream de dados. Neste caso foi feito inicialmente uma filtragem pelo protocolo Telnet, conforme visto na figura 13 abaixo:

Em seguida foi utilizado o menu Analyse > Follow > TCP Stream, mencionado anteriormente e com isso foi possível agrupar todos os pacotes pertencentes ao stream de pacotes pertencentes ao stream do pacote selecionado, inclusive aqueles que não são exclusivamente de protocolo Telnet, conforme visto a seguir na figura 14.

Como pode também ser visto na figura 14 o filtro que é gerado pelo menu executado basicamente é filtrar na captura pelo stream TCP de número 6 que sintaticamente possui a expressão (tcp.stream eq 6), o trecho tcp.stream

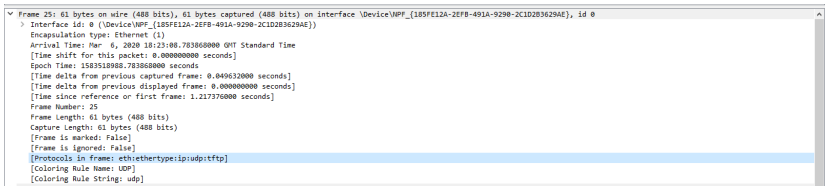


Figura 8. Protocolo de transporte UDP.

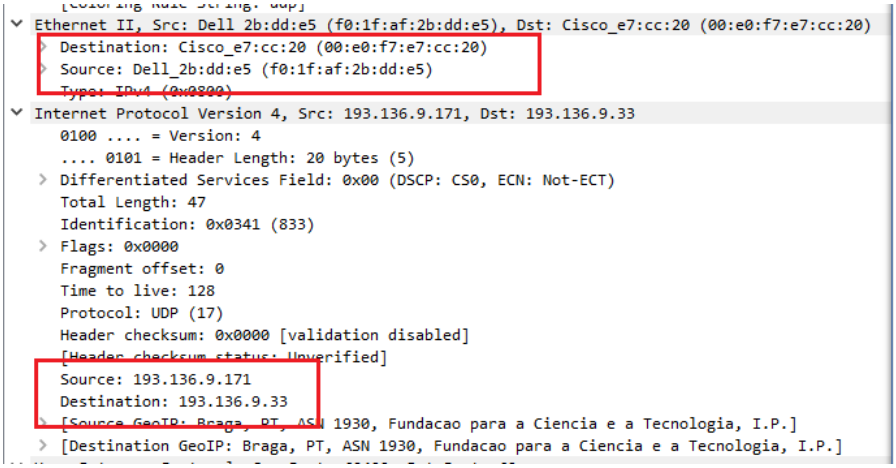


Figura 9. Exibindo o MAC e IP dos hosts origem e destinos.

indica intuitivamente que quer se filtrar por streams TCP e a parte (eq 6) indica que o stream especifico que se deseja é o de número igual (eq) a 6. E o mais interessante do resultado da ação executado pelo menu selecionado é a reconstrução e apresentação das trocas de mensagens trocadas entre origem e destino, de tal forma que seja possível capturar e entender uma troca de mensagens por completo, se forem enviados em texto claro, que é o caso do protocolo Telnet. Tal resultado é visualizado na figura 15

Os trechos apresentados marcados em azul foram recebidos pelo destinatário e em vermelho pela a origem, que está a tentar aceder ao equipamento via protocolo Telnet. Assim vemos de forma clara o password que foi digitado pelo utilizador. Desta forma mostra a fragilidade do protocolo Telnet, bem como outros protocolos que transmitem suas mensagens via texto claro, caso sejam transmitidos conteúdos sensíveis como senhas, informações bancárias e outros, tais dados estarão expostos e a comprometer a confidencialidade das informações caso haja um utilizador malicioso a sniffar os pacotes que são transmitidos pela rede.

d) Analise e identifique dados estatísticos da sua captura de pacotes.

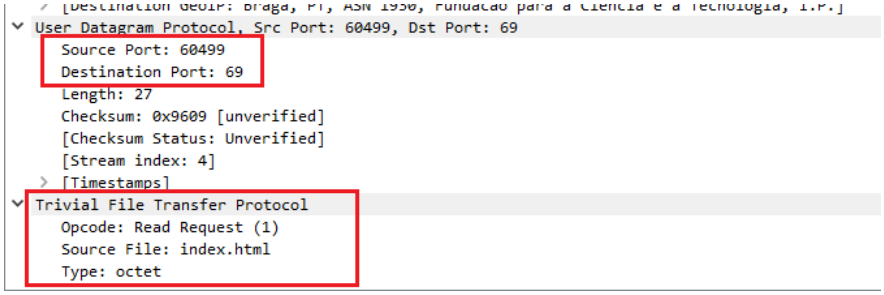


Figura 10. Exibindo a porta de origem e destino para identificar a aplicação.

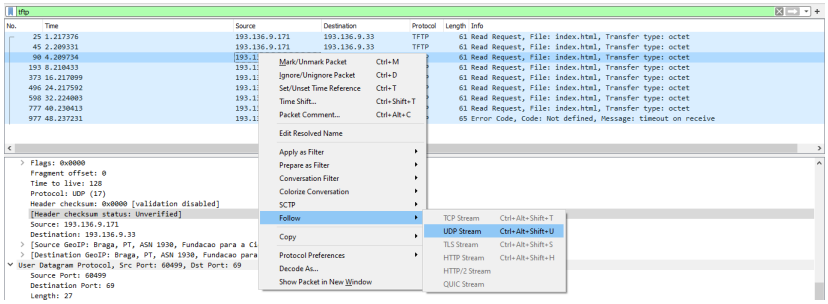


Figura 11. Menu para seguir o stream.

Dentre as capturas realizadas selecionou-se a referente ainda ao Telnet. Na tela principal já é possivel verificar a quantidade de pacotes capturados no total e quantos estão sendo exibidos, quando há um filtro aplicado.
CRIAR TABELA AQUI:
Quantidade de pacotes capturados: 352
Total de pacotes exibidos: 50(14.2%)
Outra opção para se obter mais estatísticas é utilizar o menu Statistics, nele há uma lista de opções. Uma delas que é interessante é o Conversation, nesta são compiladas todas as conversas entre origm X e destindo Y para os protocolos Ethernet, Ipv4, Ipv6, TCP e UDP, sendo essas opções distribuídas em abas, conforme visto abaixo na figura 16.

Outra estatistica interessante é listagem hierárquica dos protocolos, nela pode-se ver a representatividade de cada protocolo e subprotocolo no total da captura. Essa estatística pode ser visualizada na figura 17.

E outra forma de visualizar estatísticas é na opção File Properties do menu Statistics, que pode ser visualizado na figura 18
Quantidade de pacotes capturados: 352
Total de pacotes exibidos: 50(14.2%)

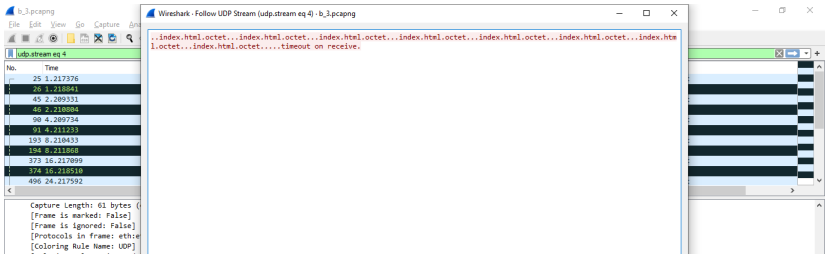


Figura 12. Ao montar o stream, é apresentado as informações.

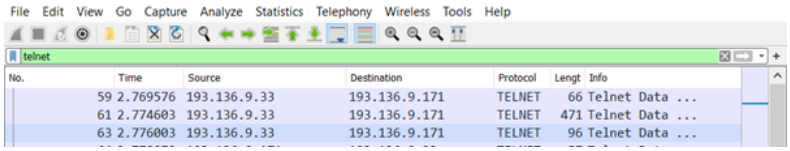


Figura 13. Exemplo lista de stream.

Conclusão

Ao longo desse trabalho, tivemos a oportunidade de desenvolver nossas habilidades na análise do tráfego gerado. Com fácil aprendizado, a ferramenta Wireshark se mostra extremamente poderosa e eficaz, nos mostrando os detalhes das capturas geradas, com isso conseguimos caracterizar o tráfego, identificar as portas utilizadas e com isso qual o serviço utilizado, por exemplo. No relatório mostramos como podemos verificar tais informações, filtra os dados da captura, mostrando sua sintaxe e complexidade na geração dos filtro. Claro, estamos longe de sermos especialistas na caracterização e análise, mas podemos afirmar que estamos caminhando na direção correta.

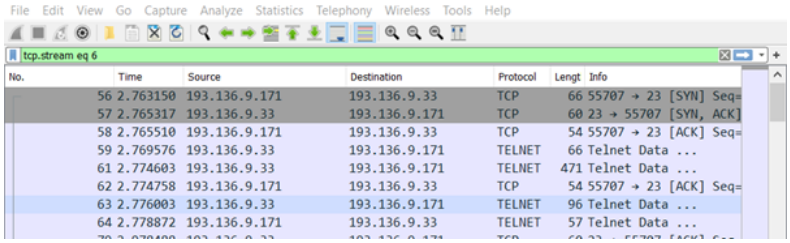


Figura 14. Exemplo lista de stream.

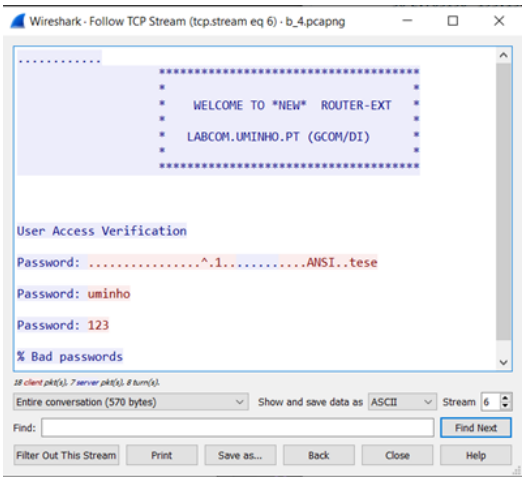


Figura 15. Montando o stream.

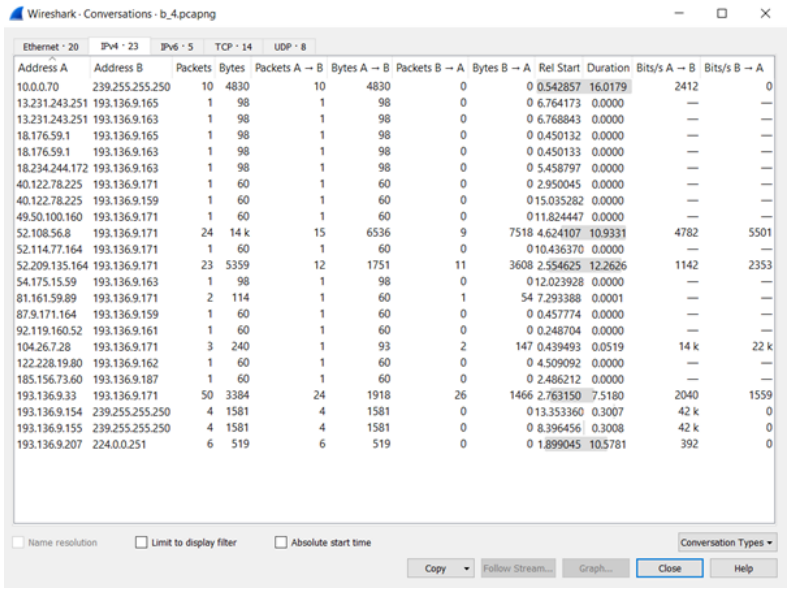


Figura 16. Tabela conversation.

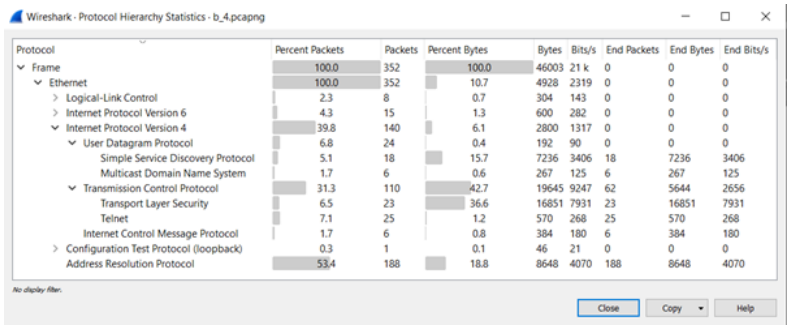


Figura 17. Tabela de estatística hierárquica.

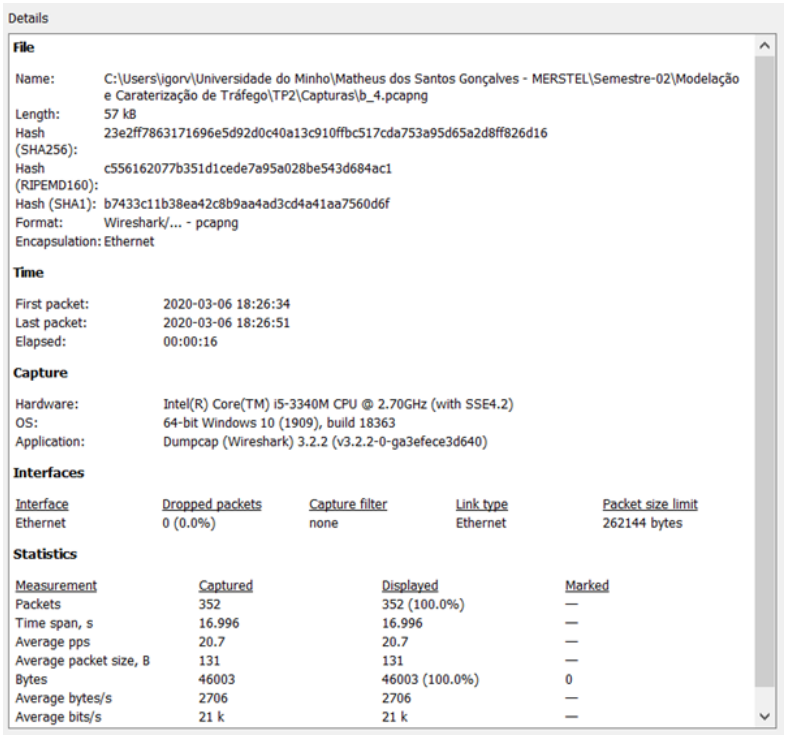


Figura 18. File Properties.