Wireshark

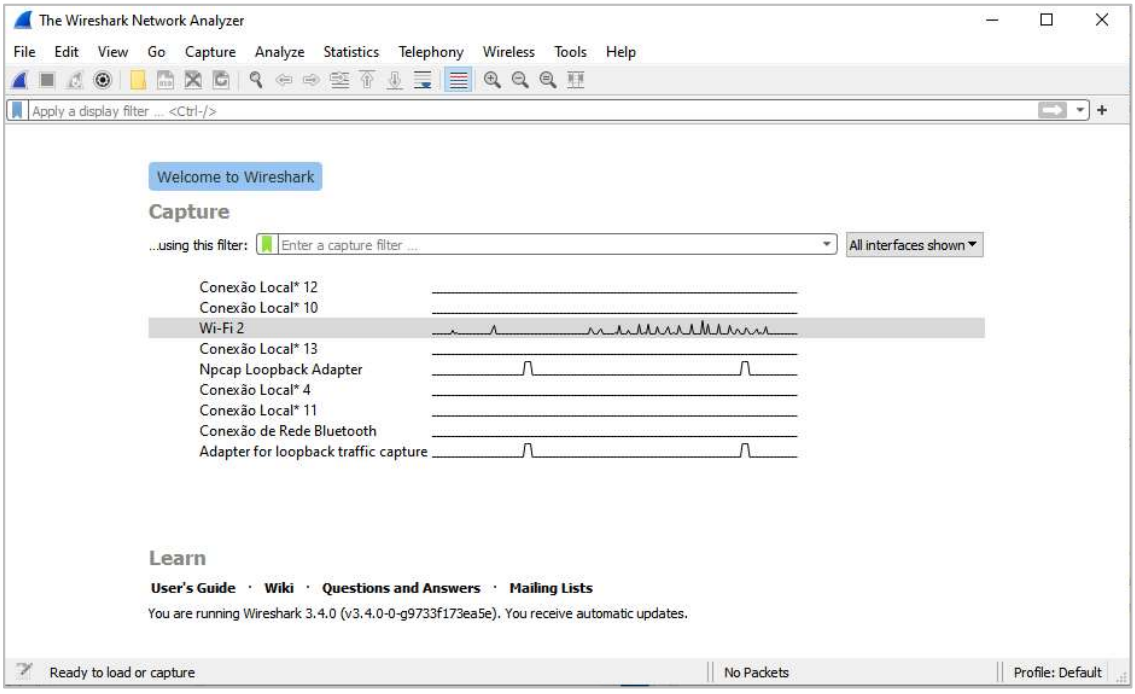
Exemplo de programa farejador, ou *sniffer*, de rede

O *Wireshark* é uma ferramenta de análise de tráfego de rede, chamada de farejador ou *sniffer*. Ele permite que um administrador da rede analise protocolos e tráfego da rede, assim como capture seus dados. Também permite que você navegue e capture informações da rede interativamente durante o tempo de execução dos sistemas utilizando um computador comum.

Esta é uma ferramenta útil para administradores de rede, considerando que é possível detectar o comportamento do tráfego da rede, problemas ou conexões suspeitas. Com ele, pode-se fazer testes de senhas e análise de segurança, observando a criptografia de dados em alguns protocolos, como o HTTPS (*HyperText Transfer Protocol Secure*).

Para utilizá-lo, primeiramente, é necessário fazer o download do software e, em seguida, instalá-lo em um computador na rede. Ao abri-lo, você deverá selecionar a interface de rede que deseja monitorar. A figura a seguir mostra a tela do *Wireshark* e a opção de Wi-Fi 2 selecionada como interface de rede.

Wireshark – escolha da interface de rede.

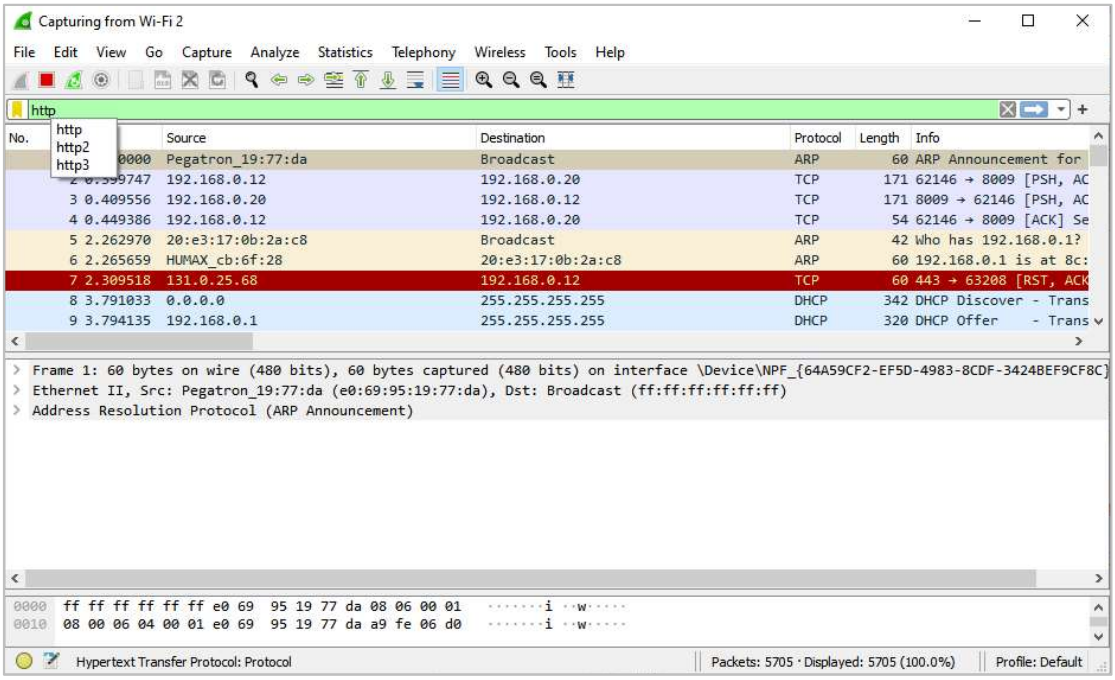


Fonte: captura de tela da ferramenta *Whireshark* elaborada pelo autor.

Com a interface de rede escolhida, você pode selecionar a opção ***Enable promiscuous mode***, para que o programa capture todos os pacotes da rede conectados à interface. Em seguida, clique no botão ***Start*** para iniciar a análise da rede. Você pode digitar um determinado filtro na linha de comando apresentada na figura a seguir, na qual houve a

definição do HTTP para ser analisado. Também é possível inserir um endereço IP, para que seja exclusivamente analisado.

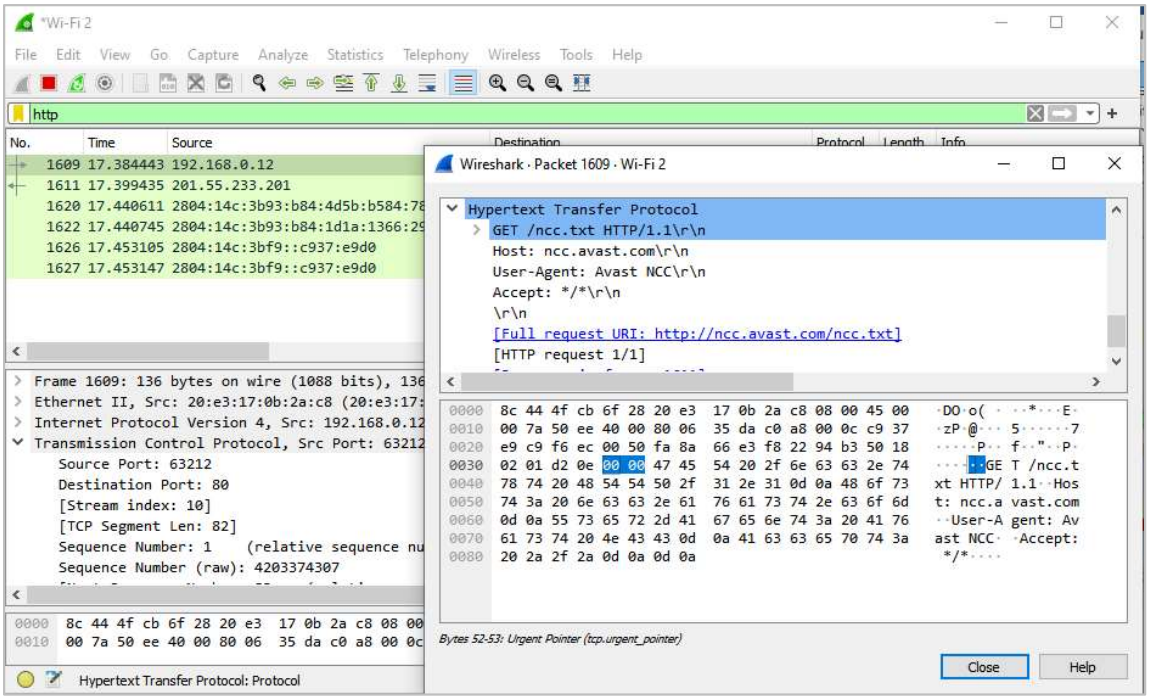
Wireshark – escolha de filtro de HTTP para análise



Fonte: captura de tela da ferramenta *Whireshark* elaborada pelo autor.

Como a intensidade das análises é grande, o fluxo de informações será constantemente atualizado na ferramenta. Para verificar os detalhes das requisições e dos pacotes transferidos na rede, você pode clicar em uma requisição do endereço 192.168.0.12, como mostra a figura a seguir, para analisar os dados com mais detalhes.

Figura | *Wireshark* – análise de uma requisição do IP 192.168.0.12

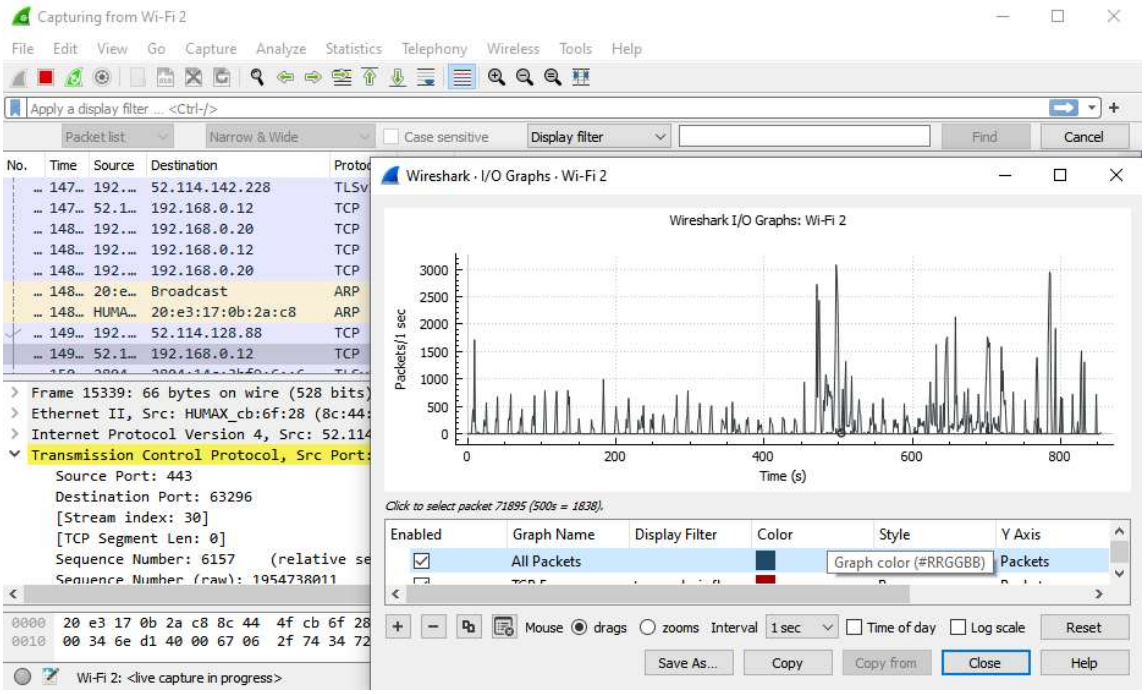


Fonte: captura de tela da ferramenta *Whireshark* elaborada pelo autor.

Há muitas opções na ferramenta, inclusive, gerar relatórios em formato de arquivo para posterior análise.

Outra forma de verificar a performance e fazer análise da rede é gerar estatísticas de acesso. A próxima figura mostra uma tela, na qual foi selecionada uma estatística de acesso via menu ***Statistics – I/O Graphics***.

Wireshark – análise e estatísticas de acesso



Fonte: captura de tela da ferramenta *Whireshark* elaborada pelo autor.

O *Wireshark* é uma ferramenta complexa, que permite um grande volume de filtros e análises, e pode ser explorada de forma simples e intuitiva.

Explore as ferramentas e análises de forma consciente, em prol da segurança de sistemas de redes de computadores.