
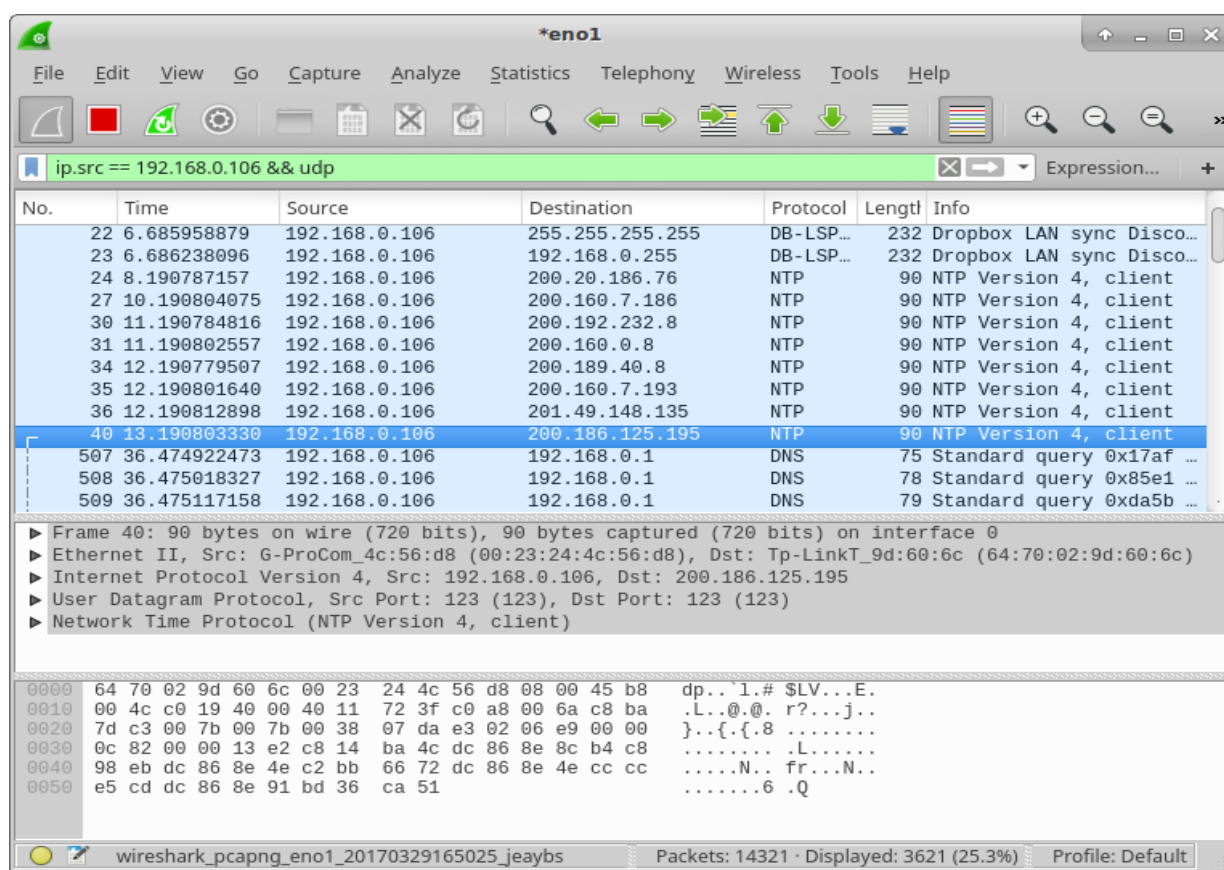
 INSTITUTO DE INFORMÁTICA UFG	<b>Universidade Federal de Goiás</b> <b>Instituto de Informática</b>	 <b>UFG</b>
<b>Professor:</b> Kleber Vieira Cardoso		
<b>Laboratório:</b> captura e análise de pacotes; Web/HTTP.		

A menos que haja alguma orientação contrária, os exercícios devem ser realizados na máquina virtual (Kali Linux) disponibilizada para uso no VirtualBox (usuário: **root**, senha: **toor**).

1. Como foi estudado no laboratório anterior, a captura de pacotes de uma rede de computadores é uma prática comum com diferentes propósitos. Um desses propósitos é entender o funcionamento dos protocolos de comunicação e da própria rede. Há várias ferramentas disponíveis para realizar essa tarefa, uma delas é o **Wireshark**, o qual é ilustrado na figura abaixo.



O **Wireshark** oferece uma interface gráfica amigável que facilita bastante seu uso. Além disso, o software oferece extensa documentação que pode ser acessada a partir da ferramenta (*menu => help*) ou diretamente no site: [wireshark.org/docs/](http://wireshark.org/docs/) e [wiki.wireshark.org/DisplayFilters](http://wiki.wireshark.org/DisplayFilters)

Caso não tenha usado o **Wireshark** antes, navegue na ferramenta e consulte a documentação para se familiarizar antes de iniciar os demais exercícios. Se tiver dificuldades com o **Wireshark**, acesse a primeira atividade de laboratório e realize os exercícios.

2. O HTTP (*HyperText Transfer Protocol*) é um protocolo da camada de aplicação que utiliza mensagens em texto ASCII (*American Standard Code for Information Interchange*). Portanto, é possível interagir com um servidor *Web* diretamente, sem auxílio de um cliente específico (ou seja, sem um navegador ou similar). Novamente, utilize o **Wireshark** para capturar os pacotes enquanto você utiliza o **netcat** (ou **nc**) para interagir com alguns servidores *Web*. O uso de filtros também é útil nesse exercício. Escolha uma das sequências que você capturou para responder o que é pedido.

- Comente sobre o que você observou do HTTP, descrevendo que informação está sendo transportada e o que você deveria ver se estivesse usando um navegador.
- Tudo que você espera ver em um navegador foi trazido pelo **nc** ou parece estar faltando “dados”? Comente sua resposta.
- Para auxiliar na compreensão do que está sendo capturado, o **Wireshark** apresenta comentários na coluna **Info** (mais à direita na tela) e tenta reconstruir os “diálogos” estabelecidos na camada de aplicação. Para o iniciante, esse auxílio pode causar alguma confusão, pois parece haver uma camada extra, por exemplo, a **[Reassembled TCP Segments ...]** que aparece nesse exercício. Portanto, responda por que o **Wireshark** realizou essa remontagem dos segmentos TCP com a requisição que você enviou? Essa remontagem também apareceria em um cliente *Web* convencional (por exemplo, **Firefox** ou **wget**)? Faça testes com um desses clientes para confirmar sua resposta e comente-a.

Dicas:

- por padrão, os servidores *Web* aguardam conexões TCP na porta 80;
- o HTTP é um protocolo que espera por requisições para as quais sempre gera resposta (exemplo da requisição mais simples: **GET / HTTP/1.0<ENTER><ENTER>**).

### 3. Análise de um pequeno arquivo HTML.

Realize os seguintes passos:

- inicie um navegador *Web* (e.g., **Firefox**);
- aguarde algum tempo após o navegador ter sido iniciado, pois é comum o navegador carregar uma página ou buscar alguma informação sobre atualização e não estamos interessados nessa informação;
- inicie a captura de pacotes com **Wireshark**;
- acesse o seguinte endereço: <http://www.inf.ufg.br/~kleber/wshark-labs/HTTP-arquivo1.html>;
- pare a captura de pacotes do **Wireshark**.

Responda o que é pedido nas questões a seguir.

- Qual é a versão do HTTP do seu navegador (1.0 ou 1.1)? Qual é versão do servidor *Web* do INF?
- Quais idiomas (se houver algum) o seu navegador indica que ele pode aceitar do servidor?
- Qual é o endereço IP do seu computador? Qual é o endereço IP do servidor [www.inf.ufg.br](http://www.inf.ufg.br)?
- Qual é o código de *status* retornado pelo servidor?
- Quando o arquivo HTML foi modificado pela última vez no servidor?
- Quanto *bytes* de conteúdo foram trazidos na mensagem de resposta?

### 4. Análise de um grande arquivo HTML.

De maneira semelhante ao exercício anterior, realize os seguintes passos:

- inicie a captura de pacotes com **Wireshark**;
- acesse o seguinte endereço: <http://www.inf.ufg.br/~kleber/wshark-labs/HTTP-arquivo2.html>;
- pare a captura de pacotes do **Wireshark**.

O arquivo HTML transportado na mensagem de resposta HTTP enviada pelo servidor *Web* é muito grande para caber em único pacote IP, portanto, a mensagem é dividida pelo TCP em múltiplos segmentos. Cada segmento TCP é registrado como um pacote separado pelo **Wireshark** e o fato que uma única resposta HTTP foi fragmentada em múltiplos segmentos TCP é indicado pela frase “**TCP segment of a reassembled PDU**” na coluna de informação (**Info**) do software. Vale salientar que não existe nenhuma mensagem desse tipo (“**TCP segment of a reassembled PDU**”) no HTTP.

Responda o que é pedido nas questões a seguir.

- Quantas mensagens HTTP GET foram enviadas pelo seu navegador?
- Quanto segmentos de dados TCP foram necessários para transportar uma única mensagem de resposta HTTP?
- Qual é o código de *status* e frase associada com a resposta para a requisição HTTP GET?
- Como o **Wireshark** identifica que vários pacotes transportam parte de uma resposta HTTP e quando é o fim da resposta?