**ATIVIDADE 3 - CAPTURA HTTP E HTTPS:**

**Nome: Igor Correa RA: 15.00588-7**

**Nome: Rodrigo Franciozi RA: 14.04014-0  
Nome: RA:**

1. Topologia



1. Objetivos

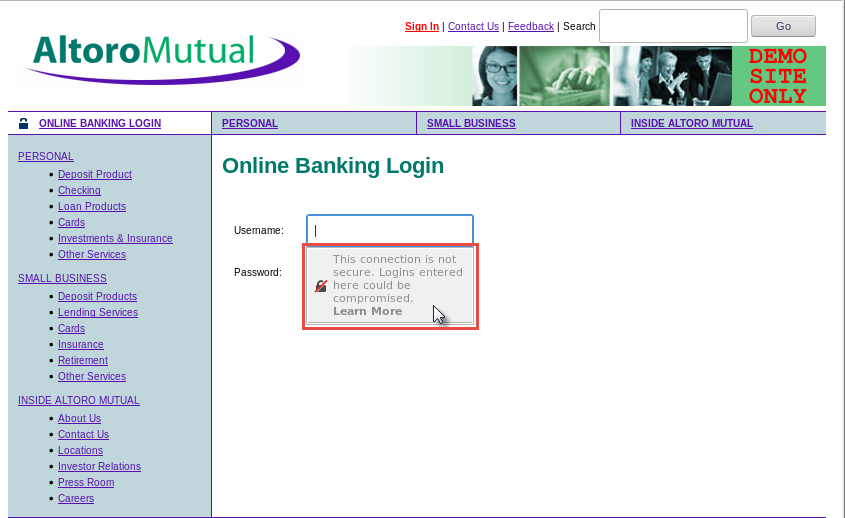
Parte 1: Captura e visualização de um tráfego HTTP

Parte 2: Captura e visualização de um tráfego HTTPS

1. Para um cenário **http** para acesso ao servidor http. Considere o seguinte procedimento:

1.1. Iniciar a captura com o Wireshark 🡪 acessar a seguinte página http:

[**www.altoromutual.com/bank/login.aspx**](http://www.altoromutual.com/bank/login.aspx)



a. Entrar com o usuário **Admin** e a senha **Admin** e clique em **Login**.

1.2. Quais as camadas do modelo TCP/IP foram usadas nessa captura? Identifique quais foram.

As camadas usadas foram todas as 4: aplicação (por se conectar no site http), transporte (para poder fazer a conexão), internet (por usar protocolo TCP) e a enlace (por ter conexões físicas) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3. Identificar endereço MAC (origem e destino), endereço IP (origem e destino), fabricante das placas de rede (origem e destino), portas de comunicação ou sockets (origem e destino), informações de camada de aplicação (métodos utilizados, POST ou GET).

MAC 🡪 origem: 64:1c:67:68:20:d0 destino: e4:6f:13:41:18:bc

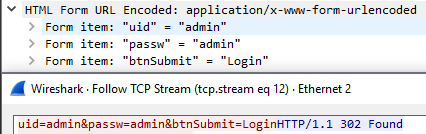
IP 🡪 origem: 192.168.0.101 destino: 65.61.137.117

Fabricante 🡪 origem: Digibras\_68:20:d0 destino: D-LinkIn\_41:18:bc

Portas 🡪 origem: 53723 destino: 80

Os dois métodos foram utilizados, GET e POST.

1.4. Verificar se é possível capturar nome de **usuário** e **senha** usando Wireshark? Se sim, como? Demonstrar com o **print** das telas no Wireshark. Dica: usar a seguinte sequência: Analyse 🡪 Follow 🡪 TCP Stream

Sim, analisando o método POST do HTTP.  


1.5. Esse protocolo é considerado seguro? Justifique.

Não, pois como pudemos ver, o nome de usuário e senha não estão escondidos nem criptografados.

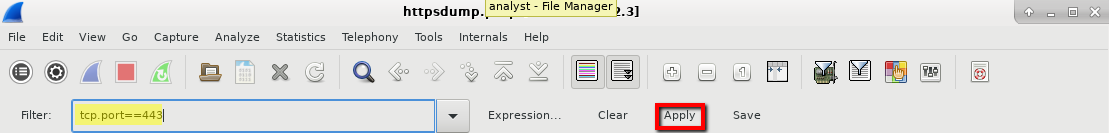
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

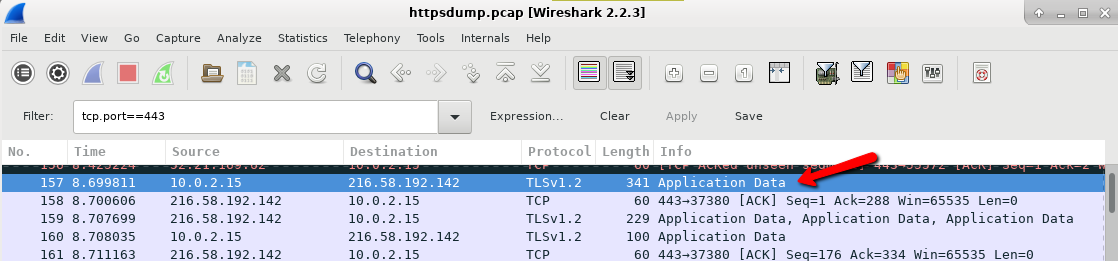
2. Para um cenário **https** para acesso ao servidor https. Considere o seguinte procedimento:

2.1. Iniciar a captura com o Wireshark 🡪 acessar uma página https (Office 365 Mauá ou outro local https) 🡪 finalizar a conexão da página 🡪 finalizar a captura com o Wireshark.

2.2. Após a captura no Wireshark, filtre o tráfego https na porta 443. Entre com **tcp.port==443** com um filtro, e clique **Apply**.



Navegue por diferentes mensagens HTTPS e selecione uma mensagem de **Application Data**.



Na janela abaixo do Wireshark (janela do meio), responda;

2.2.1. Qual a porta de comunicação usada nessa comunicação?

53901\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

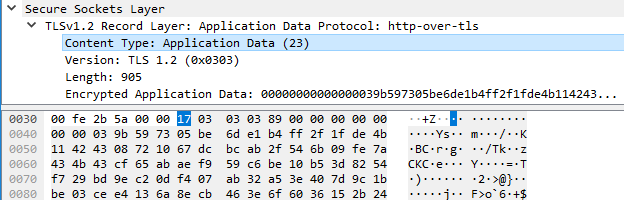
2.2.2. Qual o protocolo que está sendo usado ao invés do HTTP (protocolo acima do TCP)?

TLSv1.2 (Transmission Control Protocol)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Expandindo a seção **Secure Sockets Layer,** clicar em **Encrypted Application Data**.

Essa aplicação de dados é considerada de texto puro? Justifique com **print** da janela do Wireshark.

Não, os dados estão encriptografados.



* 1. Quais as vantagens de usar o HTTPS ao invés do HTTP?

A vantagem é a segurança (como o próprio S diz “seguro”), pois os dados do HTTPS são transmitidos encriptografados.

* 1. Todos os sites WEB que usam HTTPS são considerados seguros? Justifique.

Com relação a transmissão dos dados, sim, pois eles vão ser transmitidos criptografados, mas o site pode utilizar seus dados da forma que desejar, então não necessariamente eles são seguros.