ATIVIDADE WIRESHARK – PROTOCOLOS – PARTE I:

Nome: Mikael Akira S. Matos RA: 1680971711012

Nome: Vitor Kiomassa Kina RA: 1680971711028

Nome: Antonio Duarte RA: 1680971711031

Topologia

Objetivos

Parte 1: Captura e visualização de um tráfego FTP

Parte 2: Captura e visualização de um tráfego HTTP

Parte 3: Captura e visualização de um tráfego HTTPS

1. Para um cenário de captura com o Wireshark com o protocolo ftp do exemplo de

tutorial da Cisco (tutorial 4 - Wireshark – FTP disponível no siga), considere o

seguinte procedimento:

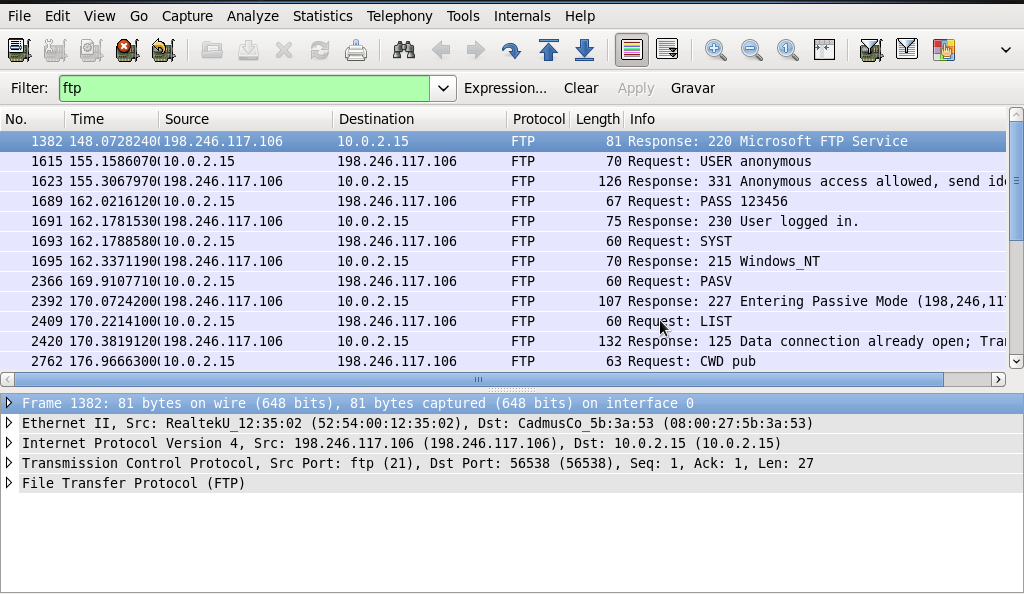
1.1. Iniciar a captura com o Wireshark  abrir o prompt do msdos no Windows 

digitar ftp <ftp.cdc.gov>  usuário: anonymous e senha: 123456  dir  cd pub  dir

 get XX06CBRFS\_SAS.zip  quit  finalizar a captura com o Wireshark.

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

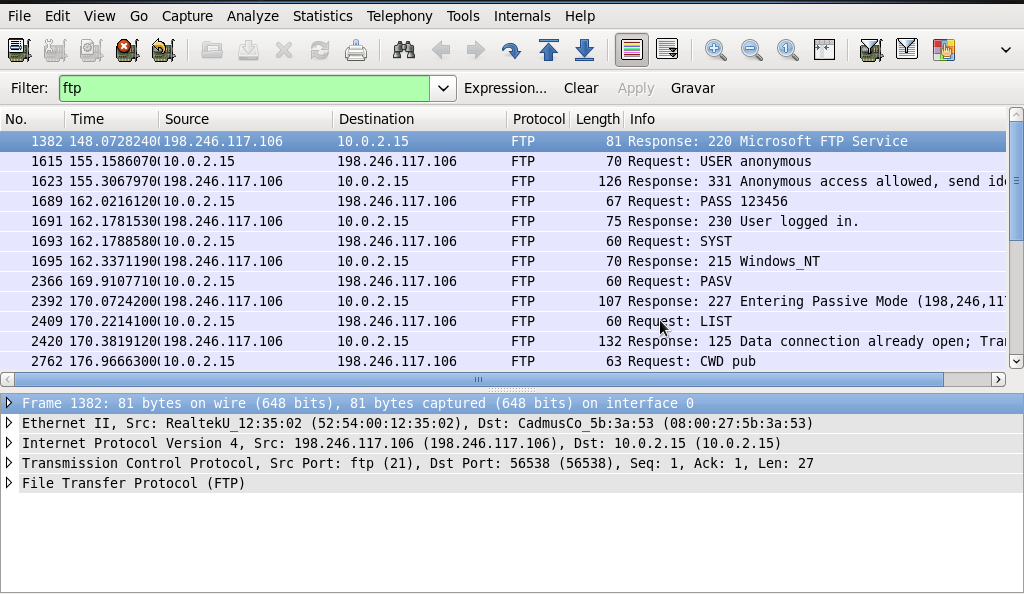
foram.



1.3. Identificar endereço MAC (origem e destino), endereço IP (origem e destino),

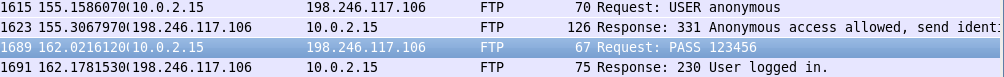
fabricante das placas de rede (origem e destino), portas de comunicação ou sockets

(origem e destino), informações de camada de aplicação (sinalização ftp).



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.



1.5. Esse protocolo é considerado seguro? Justifique.

Não, porque ele não usa nenhum tipo de criptografia para o login do usuário.

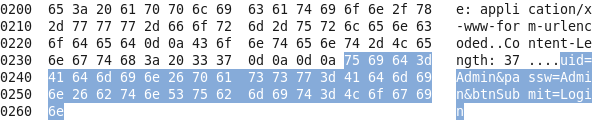
2. Para um cenário http para acesso ao servidor http. Considere o seguinte procedimento:

2.1. Iniciar a captura com o Wireshark  acessar a seguinte página http:

<www.altoromutual.com/bank/login.aspx>

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

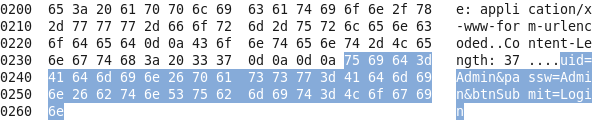
b. Fechar o browser e fechar o Wireshark.



2.2. Qual o método http usado (GET ou POST)? Quais as informações capturadas que

são consideradas vulneráveis? Realizar o print das telas do Wireshark para demonstrar.





3. Para um cenário https para acesso ao servidor https. Considere o seguinte

procedimento:

3.1. Iniciar a captura com o Wireshark  acessar uma página https (Office 365 ou outro

local https)  finalizar a conexão da página  finalizar a captura com o Wireshark.

3.2. Após a captura no Wireshark, filtre o tráfego https na porta 443. Entre com

tcp.port==443 com um filtro, e clique Apply.

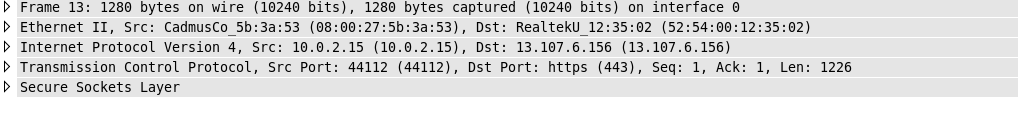
Navegue por diferentes mensagens HTTPS e selecione uma mensagem de Application

Data.

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

3.2.1. Qual a porta de comunicação usada nessa comunicação?





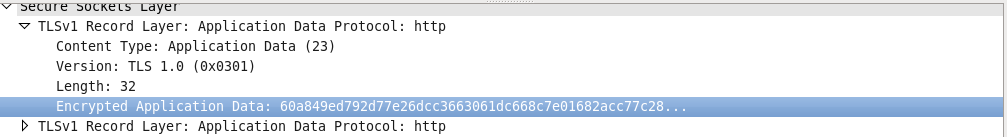
3.2.2. Qual o protocolo que está sendo usado ao invés do HTTP (protocolo acima do TCP)?



3.3.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.



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

Porque o HTTPS criptografa as informações acessadas ao contrário do HTTP.

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

Não, porque nenhum site é seguro.