Roteiro para a Aula de Laboratório – Redes de Computadores 1 – Profa. Michelle Wangham

Atividade individual. Cada aluno deverá redigir um relatório respondendo cada item das atividades listadas a seguir. O relatório deve ser postado no ambiente.

Aluno: Maurício Macário de Farias Junior

Parte I – Iniciando a captura de pacotes com o Wireshark (www.wireshark.org)

1. Qual o número IP da sua máquina? E o número do MAC address?
   a. Comando (MS-DOS): ipconfig /all

   R: MAC: 64-32-A8-10-86-59

   IP: 192.168.15.10
2. Ative o Wireshark
3. No menu Capture opção Options, habilite as opções "*Enable **MAC name** resolution*", e "*Enable **transport name** resolution*" e desabilite a opção "*Enable **network name** resolution*".
4. No menu **Analyze**, na opção **Enabled Protocols** clique no botão *"**Enable All**"* e clique no botão *"Ok"*.
5. Ative a captura de pacotes (Menu Capture/Interface/Start). Procure a interface com atividade (p.ex WiFi).
6. Observe que agora existe uma "janela de captura" ativada.
7. Acesse a rede por alguns segundos (exemplo: acesse o site https://www.internet2.edu/). Não precisa demorar (basta acessar uma única página).
8. Pare a captura de pacotes clicando no botão **Stop** da janela de captura.
9. Caso você queira salvar os pacotes capturados, acesse Menu File-->Save As...
10. **Analise os pacotes e responda:**

    a) Quantos pacotes foram capturados?

    R: 572

    b) Cite alguns protocolos que foram listados na janela de captura?

    R: TCP, UDP, TLSv1.2 e ARP

    c) Quais os principais endereços IP (fonte e destino) nos pacotes que utilizam o protocolo TCP?

    R:

Fonte	Destino
35.174.78.146	192.168.15.10
3.93.42.209	192.168.15.10
192.168.15.10	35.174.78.146
192.168.15.10	3.93.42.209
192.168.15.10	207.74.164.248
207.74.164.248	192.168.15.10

Parte II - **Filtros de visualização – Display Filter**

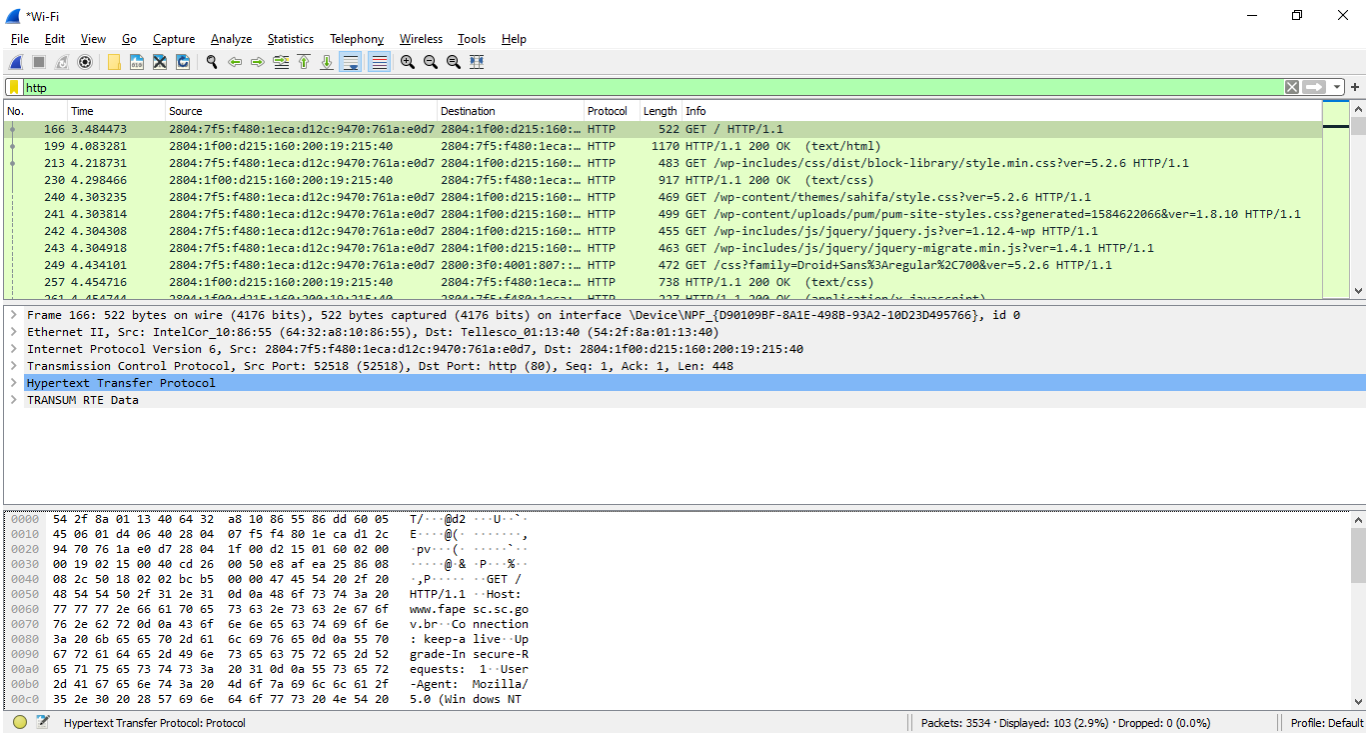
Estabeleça alguns filtros de visualização (display filter). Atenção: alguns filtros podem não mostrar nenhum pacote, em função da atividade da rede naquele momento. Vamos ver como se faz isso:

11. Na parte superior esquerda da janela do Wireshark, você pode ver um botão “Filter” com um espaço em branco ao lado dele. Nele você colocará os filtros que desejar, em letras minúsculas, e pressionará ENTER para aplicá-los e o botão CLEAR para “resetar” o filtro. Use os nomes dos protocolos do item 10.b, por exemplo.

Parte III – Protocolo http

Agora iremos acompanhar um fluxo HTTP entre o seu computador e um servidor web na Internet, a fim de ver como são realizadas as trocas de mensagens do protocolo HTTP.

12. Inicie a captura do wireshark, abra uma aba anônima em seu navegador e acesse a página da FAPESC usando o protocolo HTTP (http://www.fapesc.sc.gov.br/). Após carregar as páginas, clique no botão STOP, para parar a captura de pacotes.
13. Inclua um filtro para apresentar apenas os pacotes HTTP na janela de captura (campo FILTER = http). Isso permitirá que você visualize as trocas de requisições e respostas HTTP que foram feitas entre a sua máquina e o servidor HTTP da FAPESC.
14. Apresente um *printscreen* da sua tela do Wireshark e responda:



a. Qual a versão do protocolo HTTP está sendo utilizada nas trocas de mensagens?

R: HTTP 1.1

b. As trocas estão sendo realizadas de maneira segura, com uso de criptografia? Como é possível saber disso?

R: Até o acesso do site, só é solicitado dados, sem nenhum envio de dados não é possível saber se dados são enviados

c. A primeira mensagem enviada do seu computador para o servidor HTTP da Univali foi feita utilizando qual método HTTP?

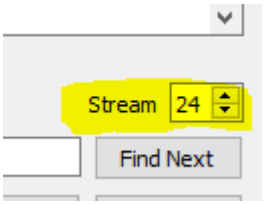
R: GET

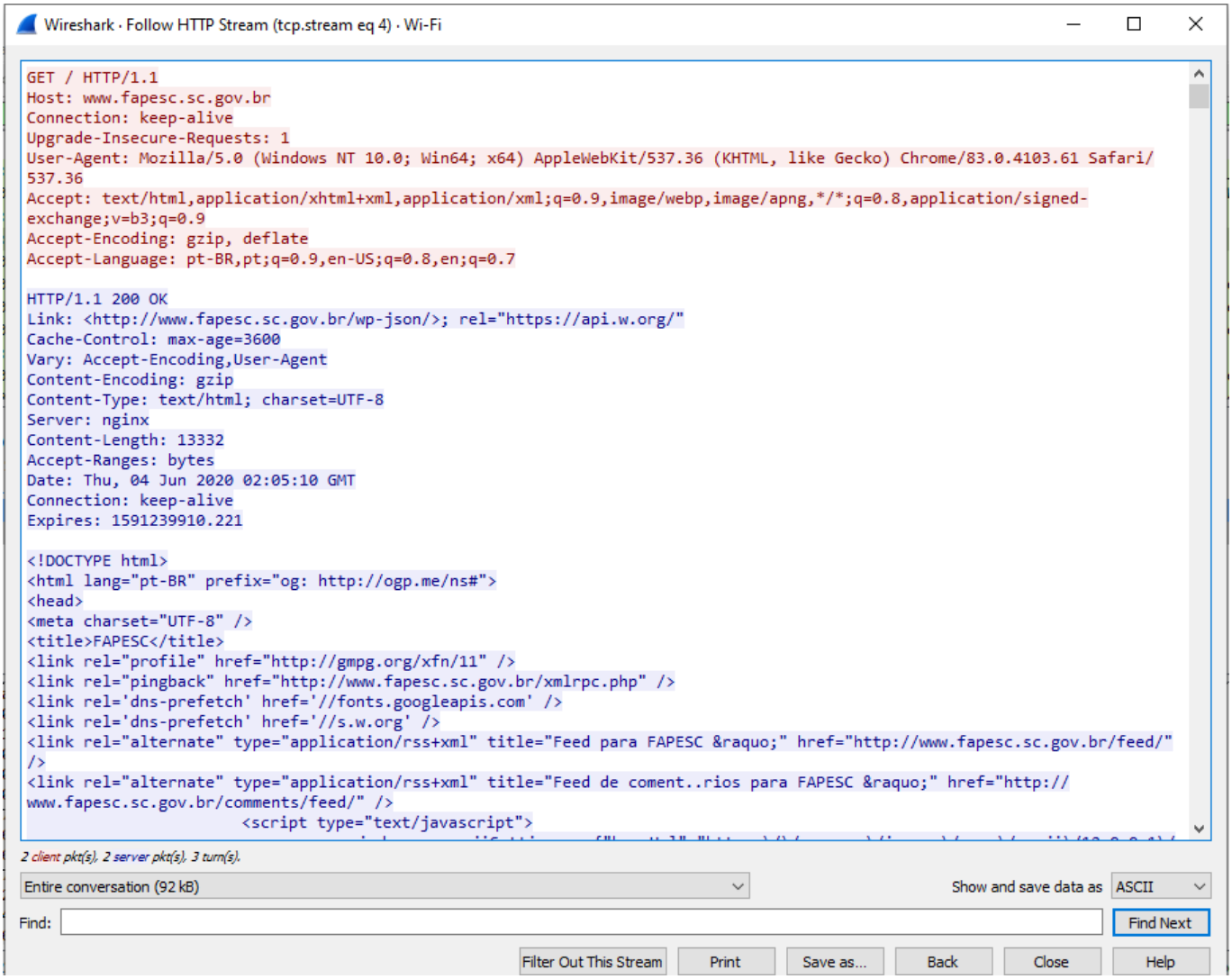
d. A resposta HTTP para essa primeira mensagem contém que tipo de conteúdo e qual o código de status dessa mensagem?

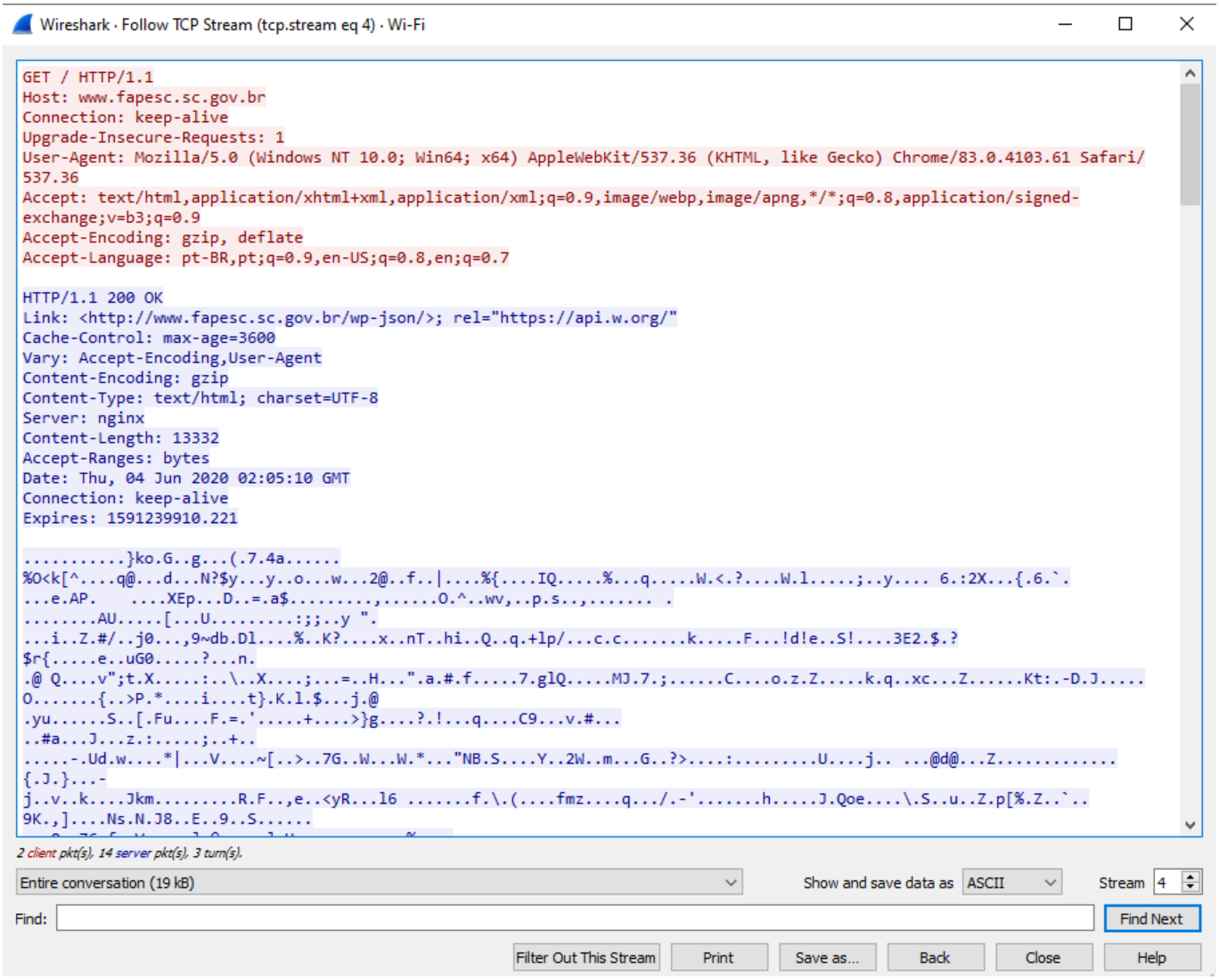
R: Retorna dados de html, sendo dados da pagina a ser mostrada, retornou status 200 (OK)

e. Após a primeira requisição e a subsequente resposta, outras mensagens foram trocadas entre o seu computador e o servidor da FAPESC. Explique por que foram necessárias essas trocas de mensagens e quais os métodos utilizados.

R: Foram necessárias por carregamento de componentes presentes na tela, foram utilizados apenas comandos GET.

15. Marque o primeiro frame que tem o comando GET. Com o botão direito do mouse, clique em Follow/HTTP stream. Apresente um *printscreen* do fluxo e analise o fluxo do protocolo. Em seguida, selecione novamente o primeiro frame e clique com o botão direito e selecione Follow/TCP stream. Analise as diferenças. Explore as funcionalidades da janela apresentada. Visualize os streams subsequentes. 

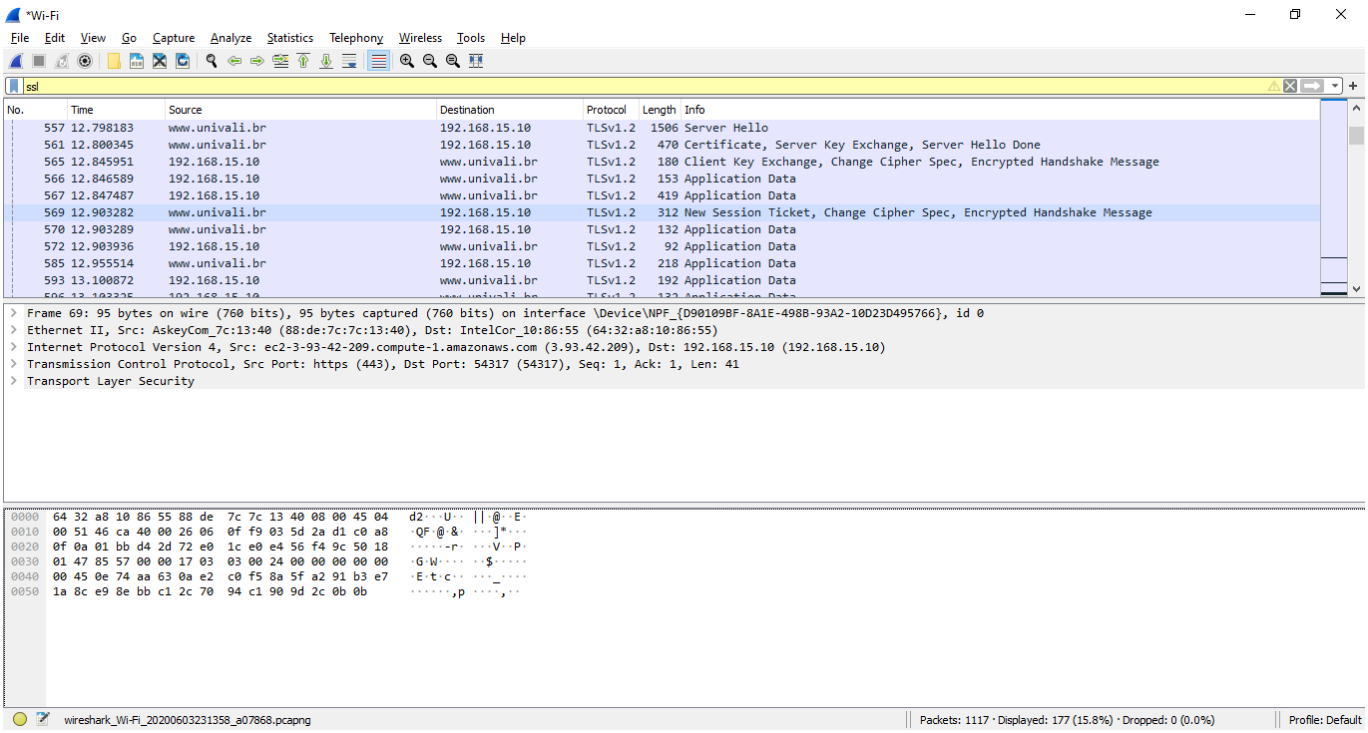

Wireshark · Follow HTTP Stream (tcp.stream eq 4) · Wi-Fi
GET / HTTP/1.1
Host: www.fapesc.sc.gov.br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
HTTP/1.1 200 OK
Link: <http://www.fapesc.sc.gov.br/wp-json/>; rel="https://api.w.org/"
Cache-Control: max-age=3600
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Server: nginx
Content-Length: 13332
Accept-Ranges: bytes
Date: Thu, 04 Jun 2020 02:05:10 GMT
Connection: keep-alive
Expires: 1591239910.221
<!DOCTYPE html>
<html lang="pt-BR" prefix="og: http://ogp.me/ns#">
<head>
<meta charset="UTF-8" />
<title>FAPESC</title>
<link rel="profile" href="http://gmpg.org/xfn/11" />
<link rel="pingback" href="http://www.fapesc.sc.gov.br/xmlrpc.php" />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel='dns-prefetch' href='//s.w.org' />
<link rel="alternate" type="application/rss+xml" title="Feed para FAPESC »" href="http://www.fapesc.sc.gov.br/feed/" />
<link rel="alternate" type="application/rss+xml" title="Feed de coment..rios para FAPESC »" href="http://www.fapesc.sc.gov.br/comments/feed/" />
<script type="text/javascript">
2 client pkt(s), 2 server pkt(s), 3 turn(s).
Entire conversation (92 kB)
Show and save data as
ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help



No protocolo TCP, não é possível visualizar os dados de resposta.

16. No menu **Capture** opção **Options**, habilite *Enable **network name** resolution.* Reinicie a captura de pacotes do Wireshark. Abra uma aba anônima e acesse https://www.univali.br/ . Assim que a página carregar, pare a captura de pacotes.
17. Insira o filtro *http*, que irá apresentar apenas os pacotes HTTP do fluxo de mensagens trocado entre seu computador e o servidor onde o serviço da UNIVALI está hospedado. Responda:
    a. Com esse filtro, há alguma informação sobre as mensagens de requisição e resposta trocadas entre seu computador e o servidor do UNIVALI? Por que isso ocorre, já que a requisição foi enviada e a resposta também?

    R: Nenhum dado foi apresentado, pois não foi usado o protocolo HTTP.
18. Experimente agora trocar o filtro para *ssl*, o qual irá apresentar o fluxo de mensagens entre seu computador e o servidor utilizando o protocolo SSL ou TLS. Apresente um *printscreen* da sua tela do Wireshark e responda:



a. Agora, é possível ter alguma informação sobre o conteúdo das mensagens trocadas entre seu computador e o servidor da UNIVALI? Por que isso ocorre?

R: Sim, é possível, pois é usado o protocolo TSLv1.2

b. Em algum momento, essas trocas de mensagens entre seu computador e o servidor utilizaram o método HTTP?

R: Não

1. Descreva brevemente as principais otimizações que programadores fazem para melhorar o desempenho quando se usa HTTP 1

R: Habilitar o GZIP para comprimir informações, paralelizando as requisições, priorização das requisições.

2. Descreva brevemente as principais características do HTTP2 descritas no vídeo

R: Automatiza e melhora grande parte do HTTP1, como por exemplo, a compressão de informações é automática.

3. Pesquise o que falta para o HTTP 2 ser amplamente usado.

R: Os navegadores e hospedeiros, precisam implementar compatibilidade, a resistência à mudanças do mercado é normal, visto que é necessário um trabalho extra para que seja