**ALUNO: THIAGO SANTOS DE LIRA**

1. Na sua opinião, você considera seguro o acesso à servidores e redes internas

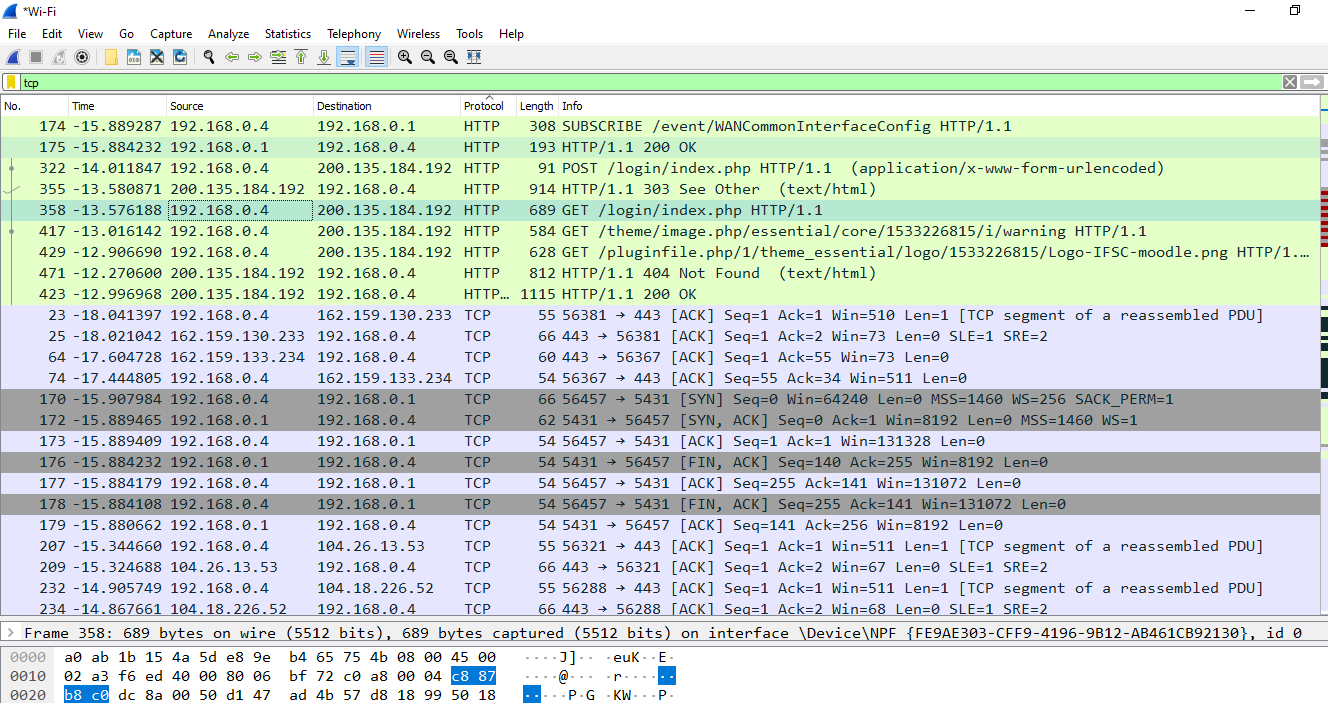
da web?

**RESPOSTA:** Atualmente não acho segura, mesmo tendo inúmeras formas de gerar uma proteção maior além da criptografia de pacotes, existem também a possibilidade de fazer teste de vulnerabilidade do roteador, teste de conectividade do servidor ou até mesmo habilitar mais opções de segurança de conexão.  
 No entanto na medida que é possível gerar mais seguranças, também está sendo criado novas forças para “burlar” essa segurança. A melhor forma é ter cuidado e não acessar sites “não ideais”

1. Inicie uma captura da interface de rede ativa no Wireshark e em seguida faça o

login no sistema moodle do campus IFSC Florianópolis

(http://moodle.florianopolis.ifsc.edu.br/). OBS.: Não é necessário ter uma

conta ativa para fazer a tarefa. Basta digitar um login e senha quaisquer.**RESPOSTA:**

1. Analise os pacotes tcp e http da conexão. Pode-se dizer que esta é uma conexão segura? Justifique sua resposta.

**RESPOSTA:** Por razão da comunicação tcp ser uma padronização de todas as comunicações de rede, e principalmente da comunicação web, creio que não seja relativamente segura, pois conseguindo de alguma forma essa key de acesso conseguiu a informação necessária suficiente para acessar a conta.

1. Faça a leitura do artigo Towards Acceptable Public-Key Encryption in

Sensor Networks

<http://telematics.tm.kit.edu/publications/Files/85/blass-sensor-public-key-encryption-2005.pdf>  
**RESPOSTA:** FEITO

1. Analisando os dados do artigo, na sua opinião quais são os principais desafios

de segurança em uma rede na qual diferentes hardwares estão conectados?

**RESPOSTA:**

A principal dificuldade é a redes de sensores para fazer a interligação dos hardwares estar necessitando de novos protocolos além dos hardware estarem falhando para proporcionar um desempenho relativamente satisfatório com um consumo baixo de memória.