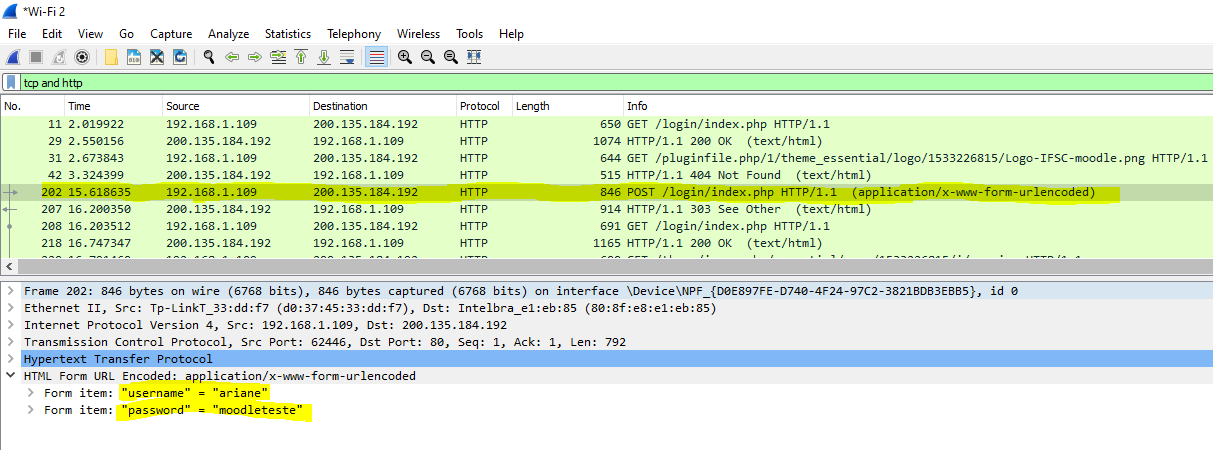
1. Na sua opinião, você considera seguro o acesso à servidores e redes internas da web?

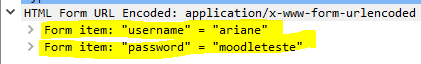
**Depende, pois precisaria conferir se os protocolos de segurança estão implementados, e o tipo de criptografia utilizado.**

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.
2. Analise os pacotes tcp e http da conexão. Pode-se dizer que esta é uma conexão

segura? Justifique sua resposta.

**Não é segura, pois quando capturei o pacote e analisei, pude ler o usuário e senha que usei no moodle, não havia criptografia. Então qualquer um que conseguir acessar a rede que usei para realizar o login, pode capturar o pacote e ver os dados do login.**

****



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>

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?

**Um dos desafios são os *hardwares* limitados em memória e/ou processamento, que não suportam criptografias mais robustas ou que levariam muito mais tempo para executá-las. Então é necessário estudar algoritmos de criptografia que são viáveis para estes *hardwares*, minimizando custos e inseguranças dos dados.**