questão 1:
Snort: É um IDS de código aberto que pode ser utilizado para a análise de pacotes em tempo real e para a detecção de ataques e sondagens de rede. Ele é amplamente usado devido à sua flexibilidade e eficácia em identificar tráfego de rede suspeito.
Suricata: Outro IDS de código aberto, o Suricata é conhecido por seu desempenho em alta velocidade e suas capacidades avançadas de detecção. Ele pode analisar tráfego de rede, detectar intrusões e até mesmo funcionar como um sistema de prevenção de intrusões (IPS) quando configurado adequadamente.

referências: https://suricata.io/, https://www.snort.org/

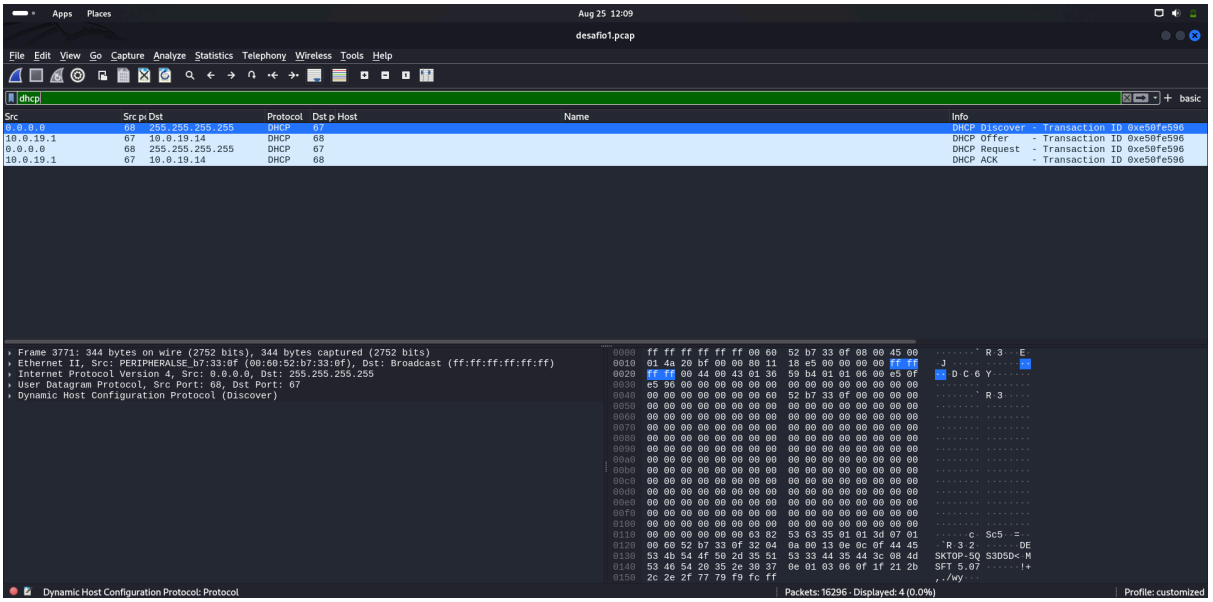
questão 2:
Função Principal:

- **IDS (Sistema de Detecção de Intrusões)**: Tem o objetivo de monitorar e identificar atividades suspeitas ou maliciosas na rede ou sistema. Ele gera alertas quando detecta uma possível intrusão, mas não toma ações diretas para bloquear ou prevenir a ameaça.
- **IPS (Sistema de Prevenção de Intrusões)**: Além de detectar atividades maliciosas, o IPS pode tomar ações automáticas para prevenir ou bloquear essas ameaças em tempo real. Isso pode incluir o bloqueio de pacotes, o encerramento de sessões ou a reconfiguração de dispositivos de rede.

Ação em Tempo Real:

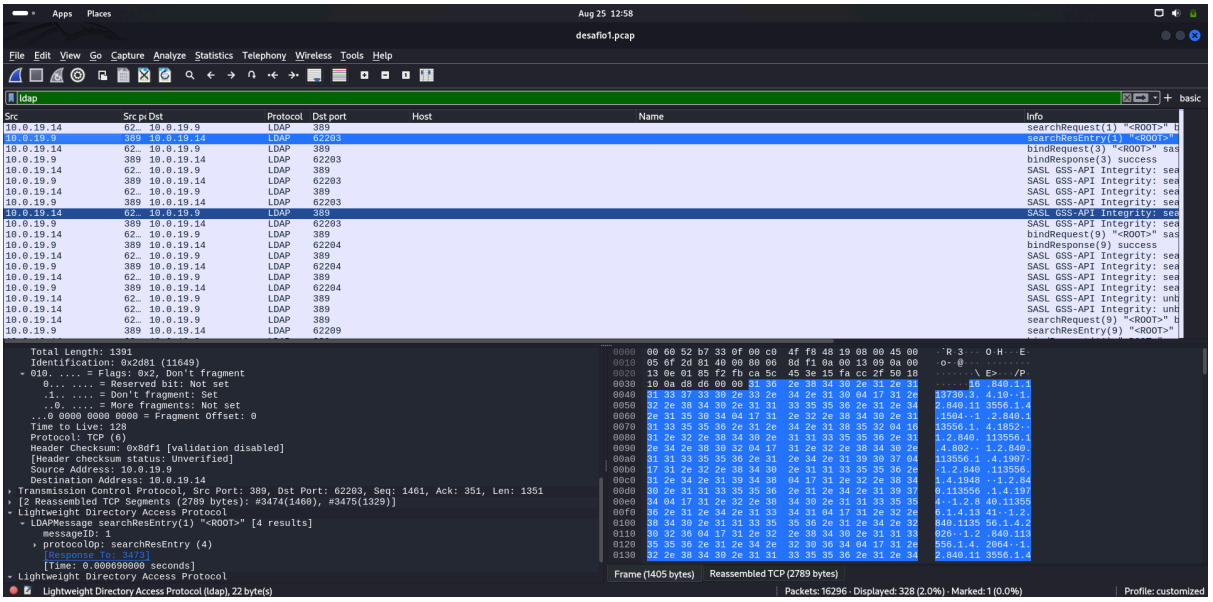
- **IDS**: Opera de forma passiva. Ele monitora e analisa o tráfego, mas não interfere diretamente no tráfego de rede. As ações corretivas devem ser tomadas manualmente por administradores de segurança com base nos alertas gerados.
- **IPS**: Opera de forma ativa. Ele é inserido diretamente no caminho do tráfego de rede e pode interromper, modificar ou redirecionar pacotes suspeitos em tempo real, proporcionando uma defesa mais imediata e automatizada.

pergunta 3:



IP do servidor DHCP: 10.0.19.1

pergunta 4:



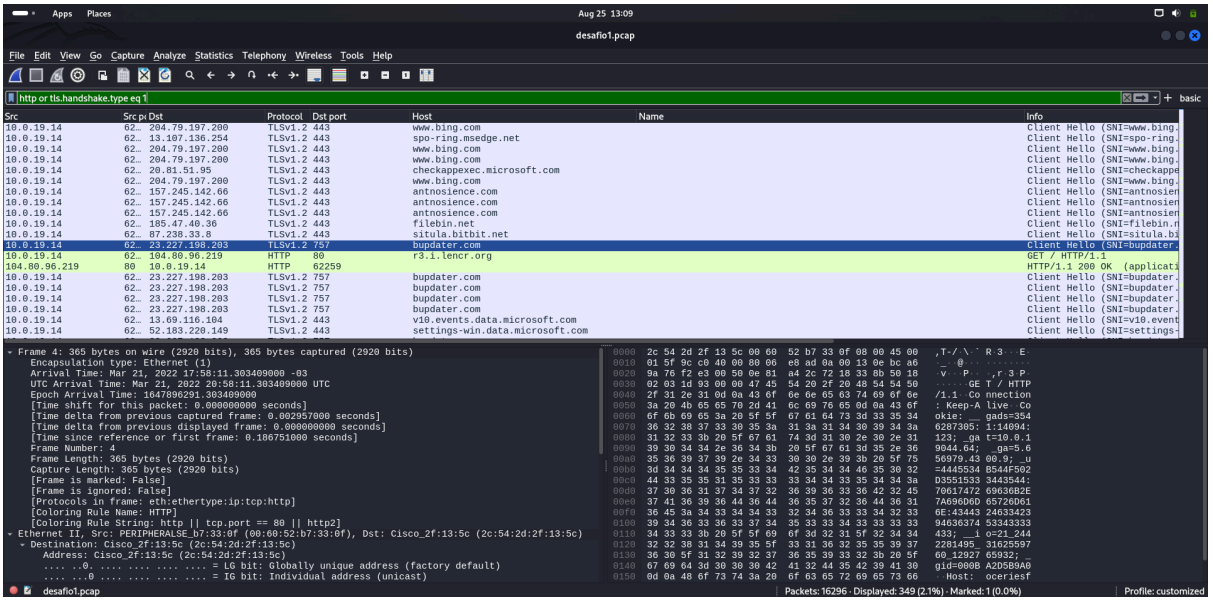
DC = burnincandle-dc

DNS Hostname: O texto menciona "dnsHostName1....". BURNINCANDLE-DC.burnincandle.com, que indica que o nome do host do servidor é "BURNINCANDLE-DC" e pertence ao domínio "burnincandle.com".

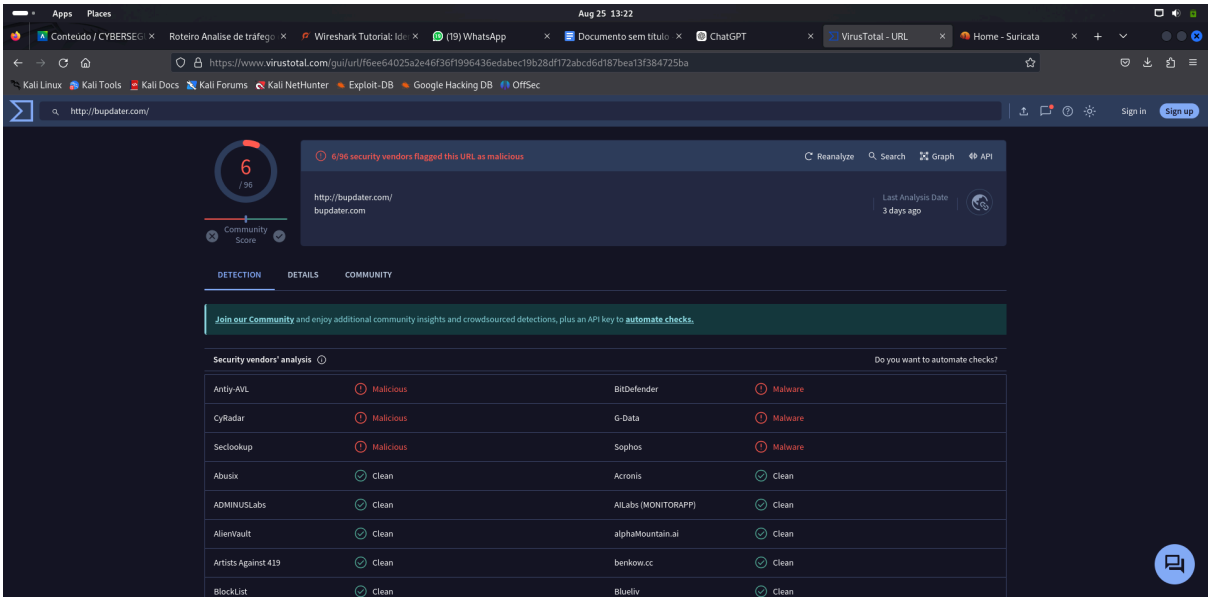
LDAP Service Name: A linha "ldapServiceName1....4.2burnincandle.com:burnincandle-dc$@BURNINCANDLE.COM" mostra que o serviço LDAP está associado ao domínio "burnincandle.com", reforçando que este domínio é gerido pelo servidor "burnincandle-dc".

Server Name: "serverName1....k.iCN=BURNINCANDLE-DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites, CN=Configuration,DC=burnincandle,DC=com". Isso mostra que o servidor controlador é identificado como "BURNINCANDLE-DC" dentro do contexto de configuração do domínio "burnincandle.com".

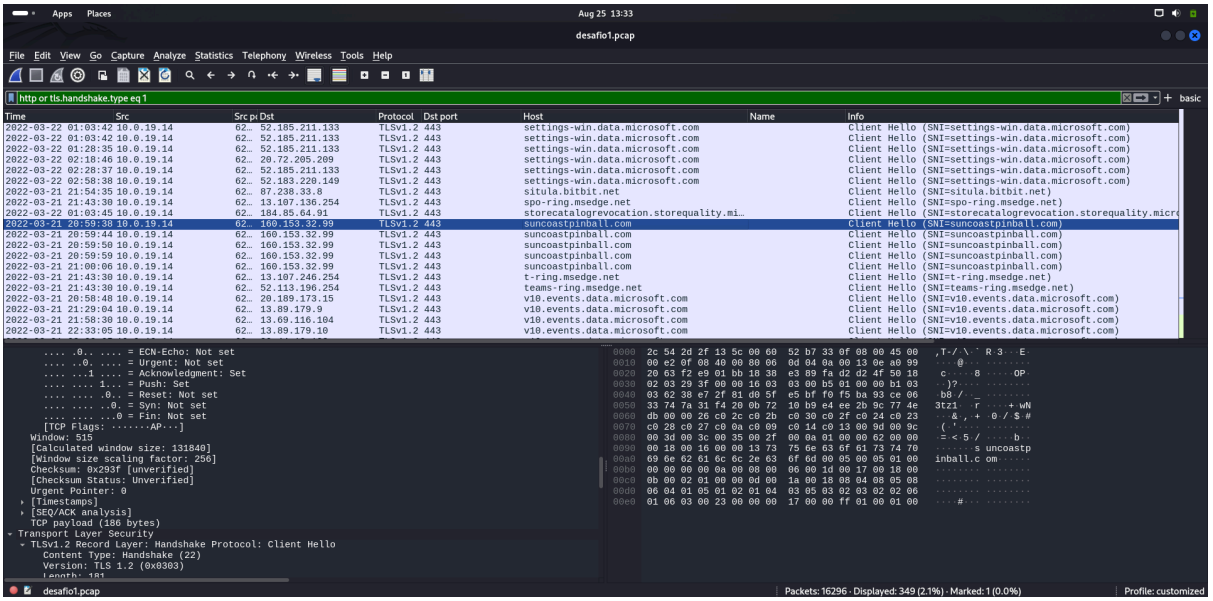
Pergunta 5:



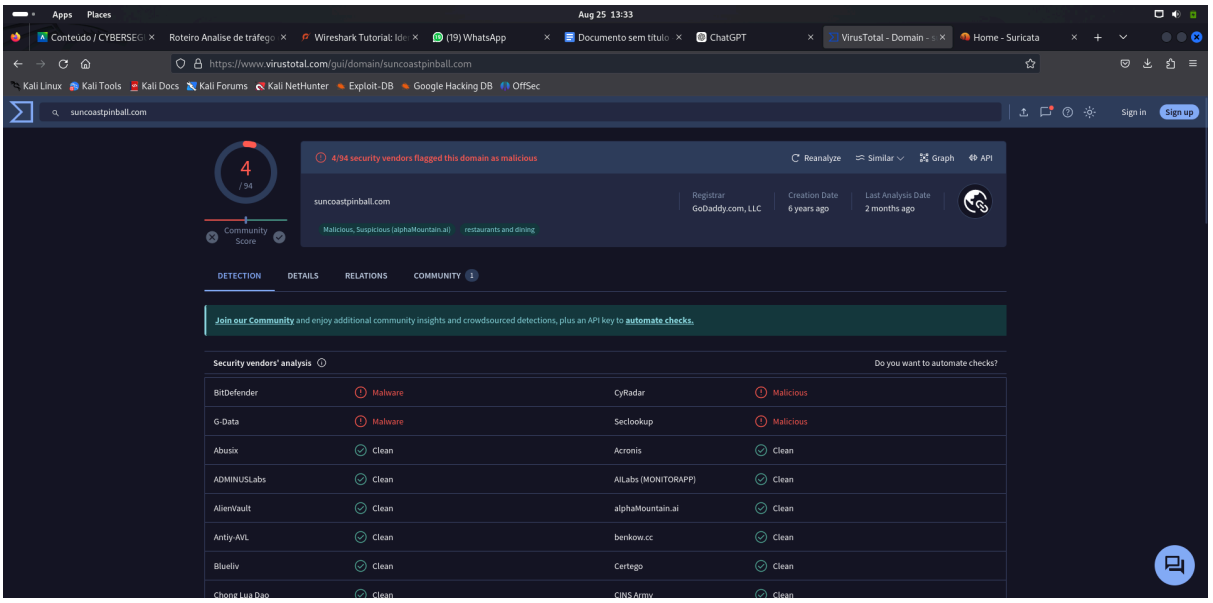
A conexão pra bupdater.com é suspeita, olhando a porta vemos que é 757 e não 80 ou 443 e filtrei por http ou https. Olhando na internet, no site virustotal.com analisei o domínio:



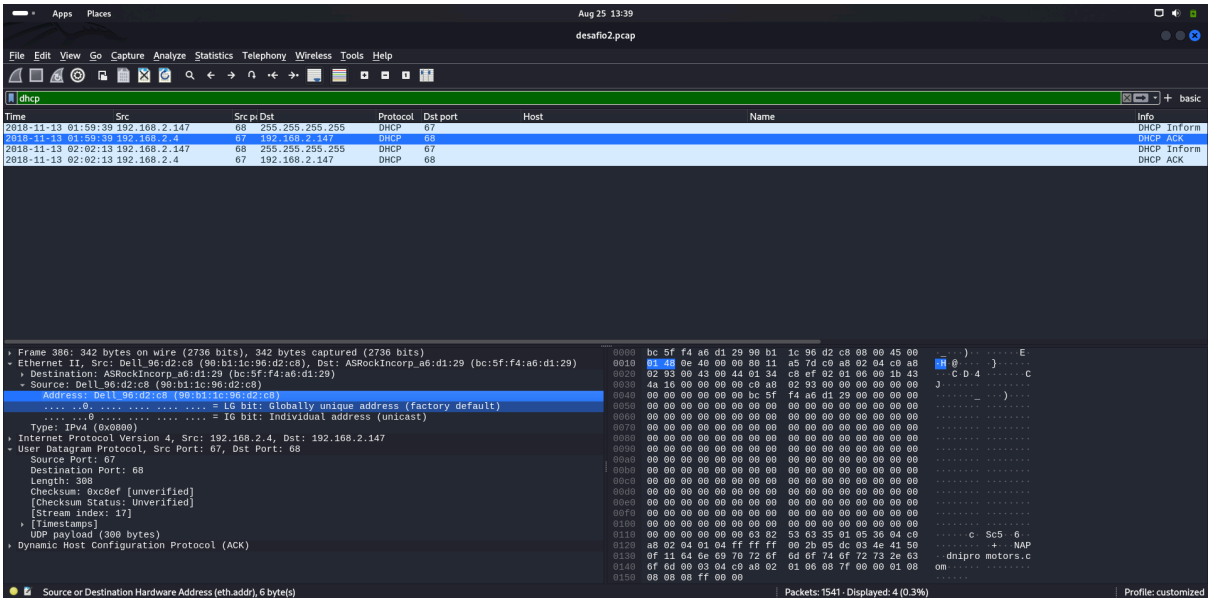
Outra conexão suspeita foi a de baixo:



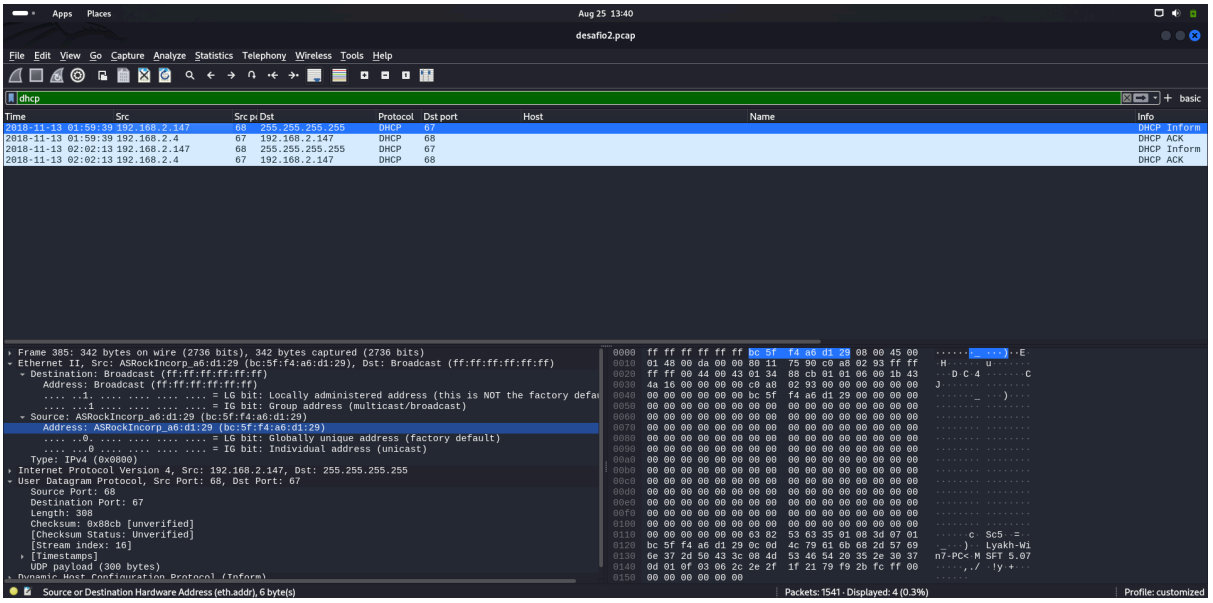
verificando no virustotal.com:



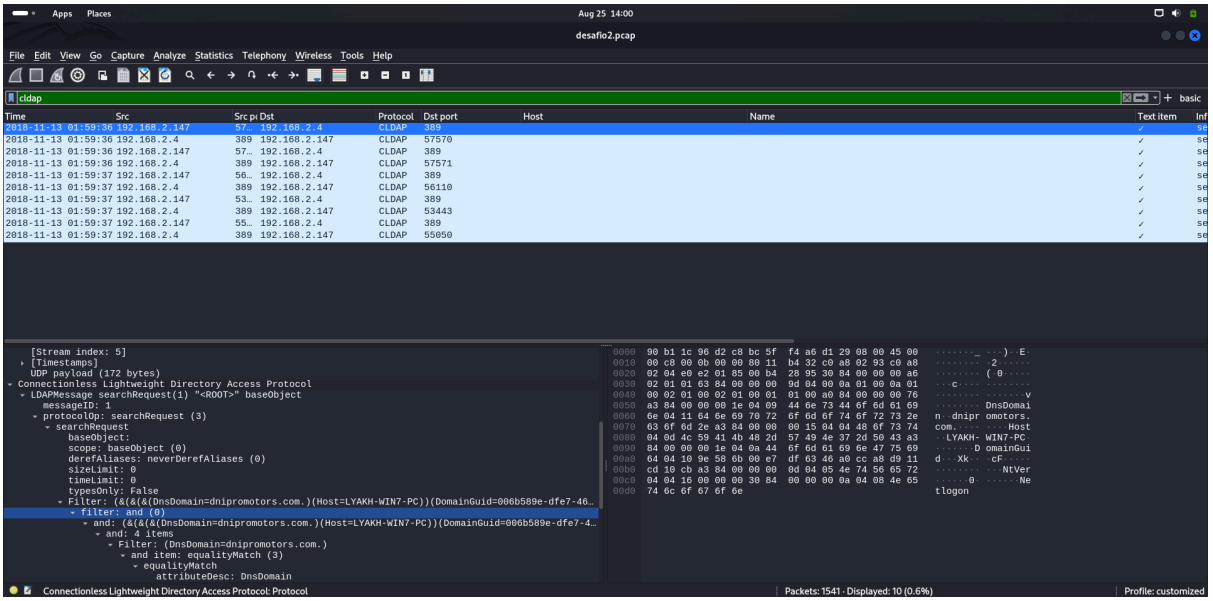
pergunta 6: 90:b1:1c:96:d2:c8



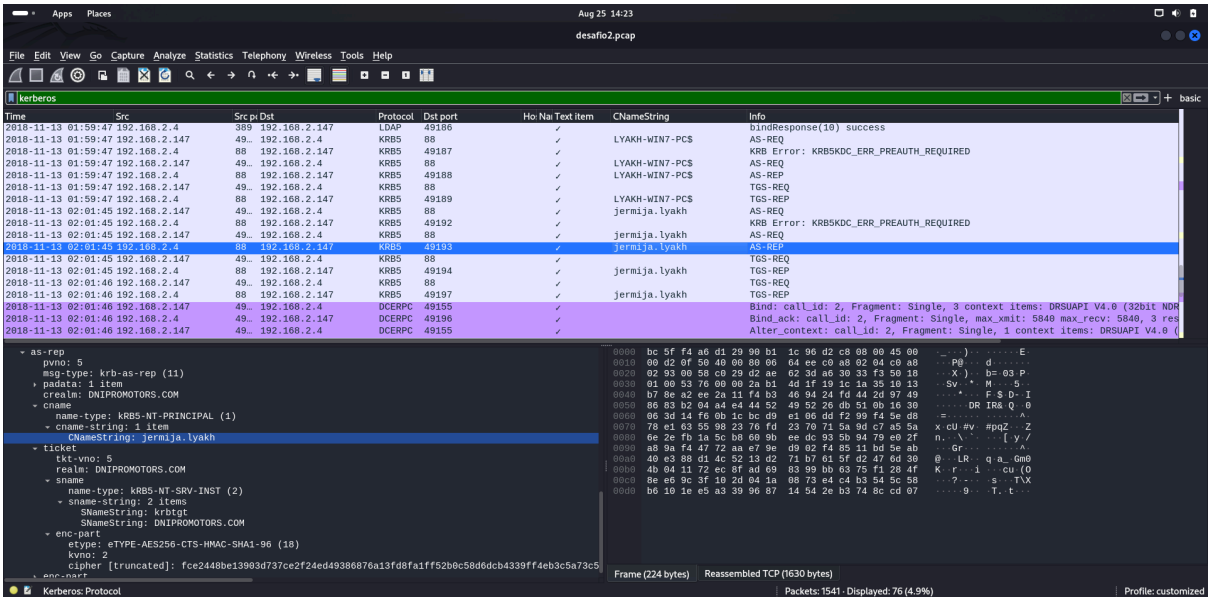
pergunta 7: bc:5f:f4:a6:d1:29



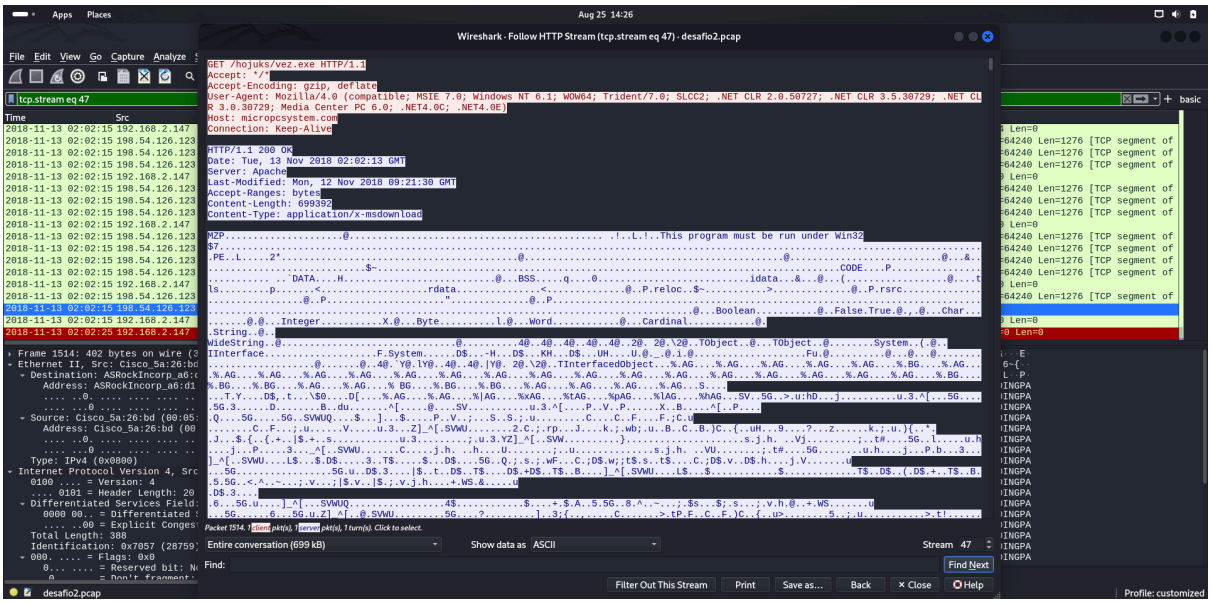
pergunta 8:Host=LYAKH-WIN7-PC



Pergunta 9: jermija.lyakh

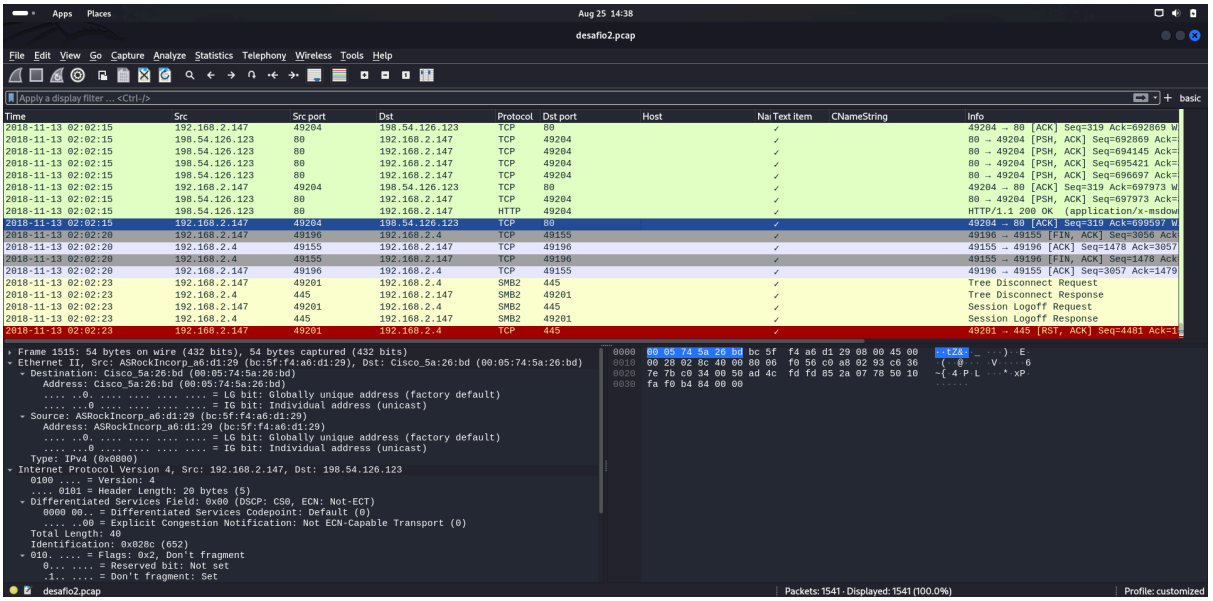


Resposta 10:micropcsystem.com/hojuks/vez.exe o nome do arquivo é vez.exe

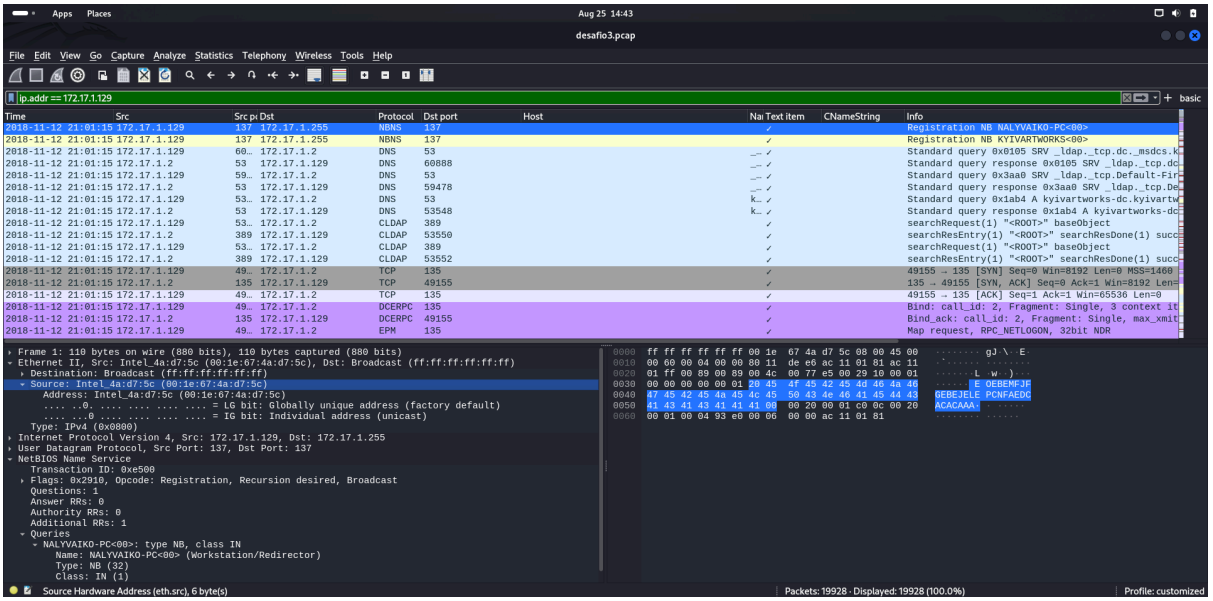


Resposta 11: 2018-11-13 02:02:13

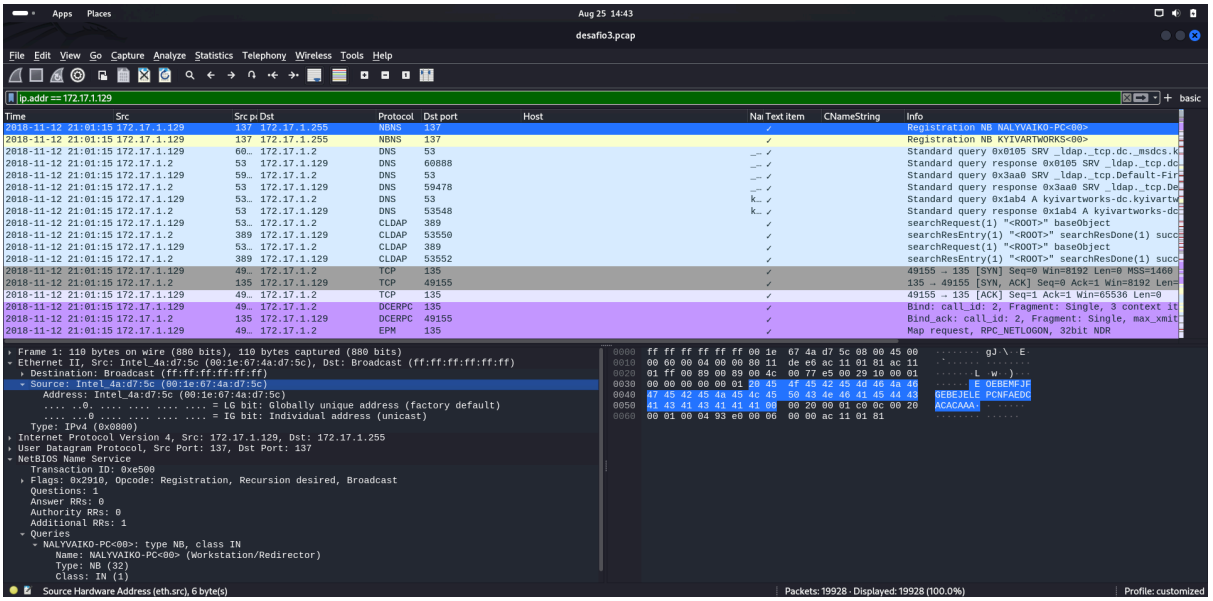
Resposta 12: 198.54.126.123



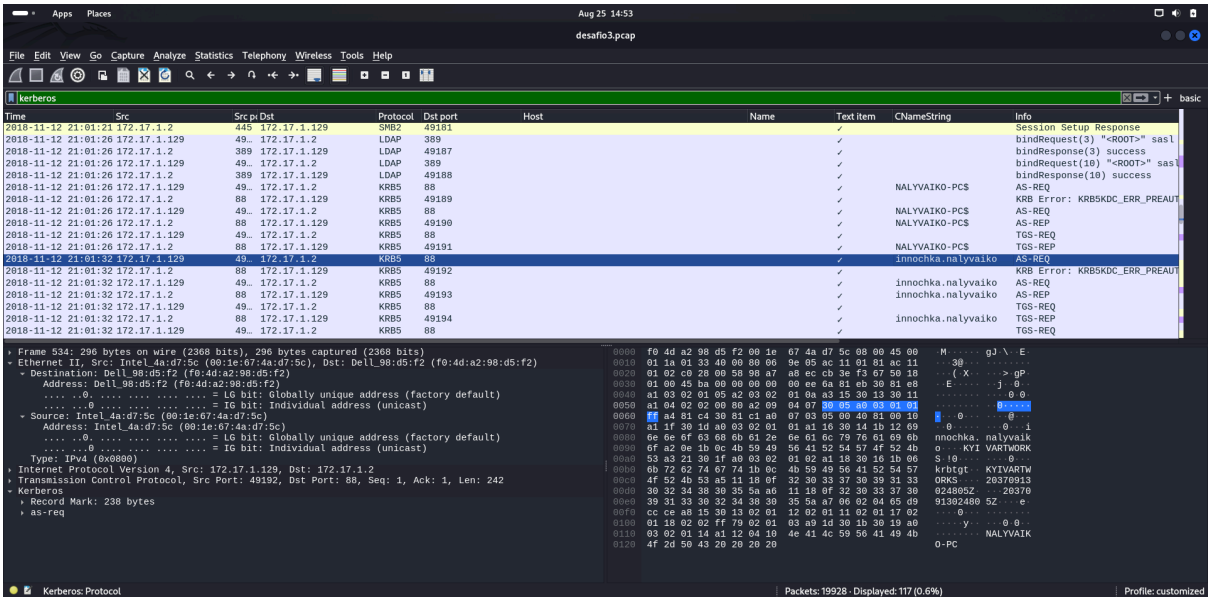
Resposta 13: 00:1e:67:4a:d7:5c



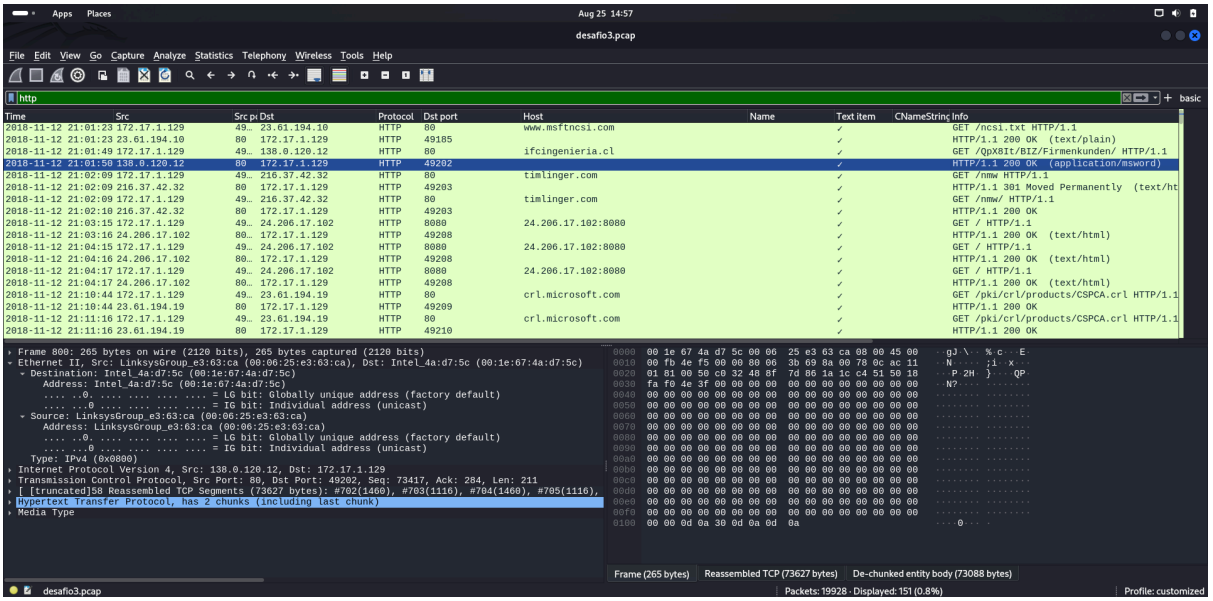
Resposta 14: NALYVAIKO-PC



Resposta 15: innochka.nalyvaiko

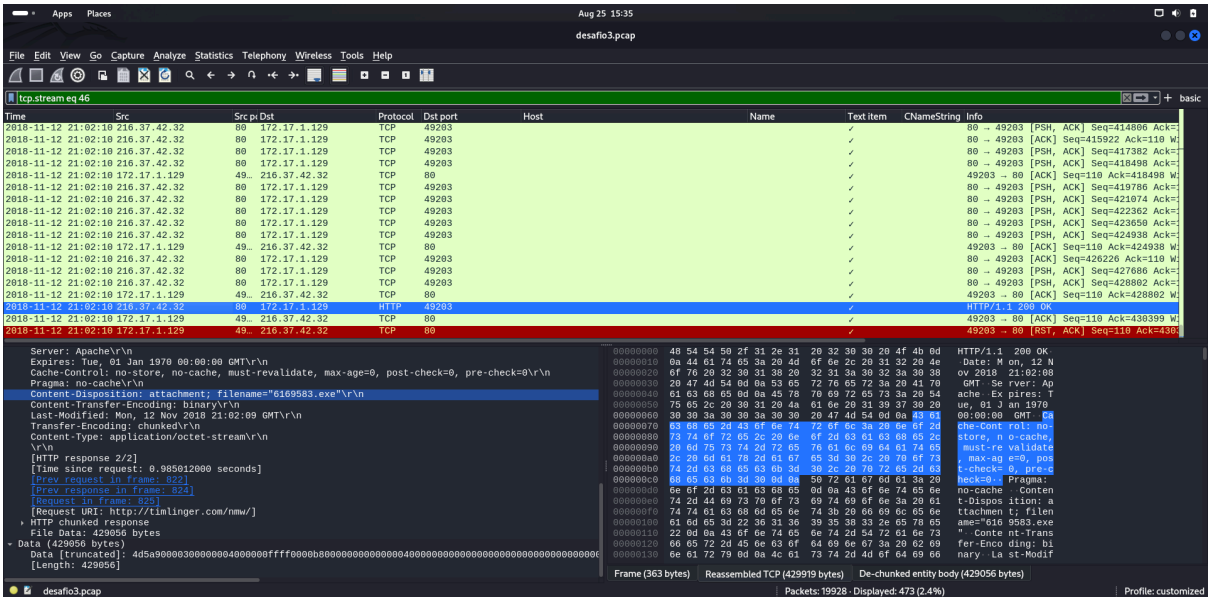


Resposta 16:http://ifcingenieria.cl/QpX8It/BIZ/Firmenkunden

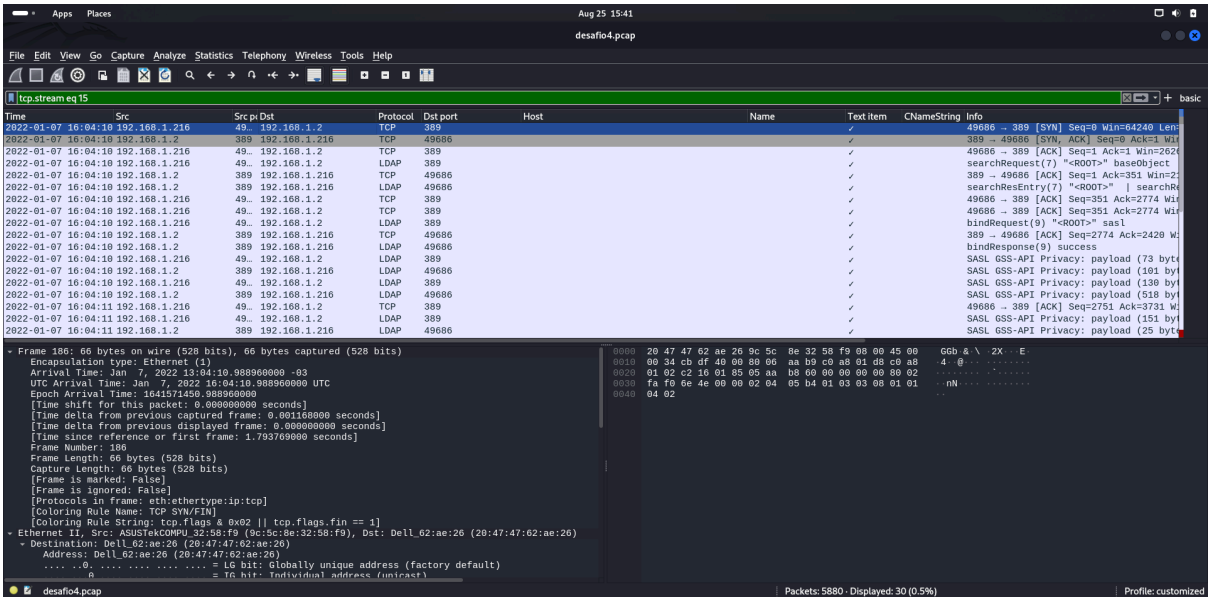


Pergunta 17:
data de acesso:2018-11-12 21:01:49

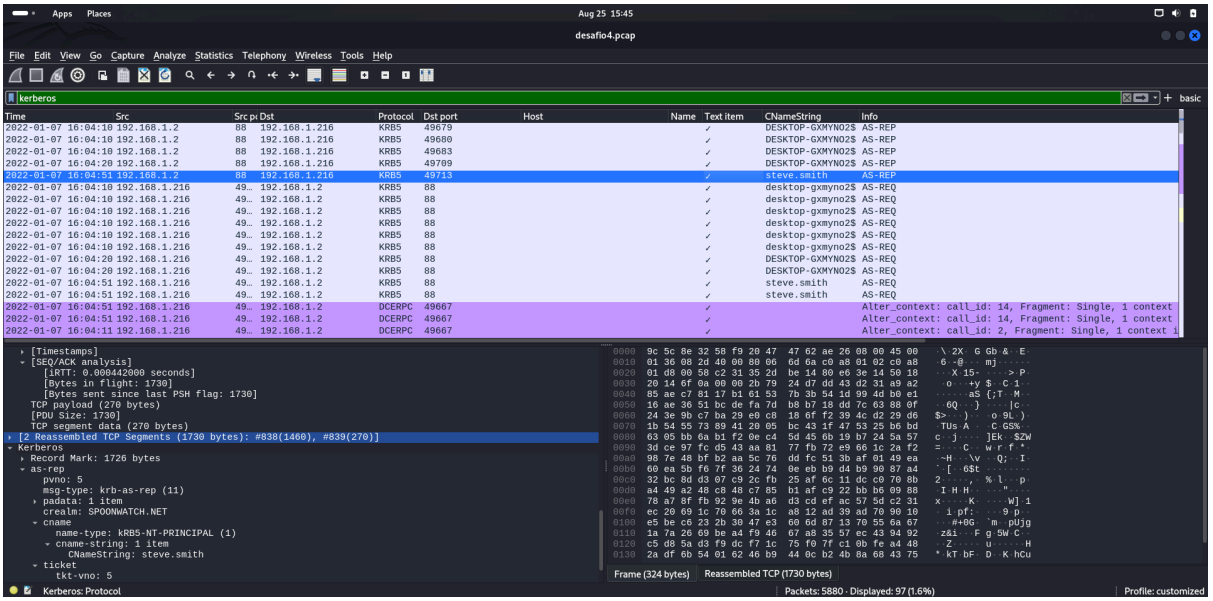
Pergunta 18:timlinger.com/nmw/ retornou o eecutável 6169583.exe



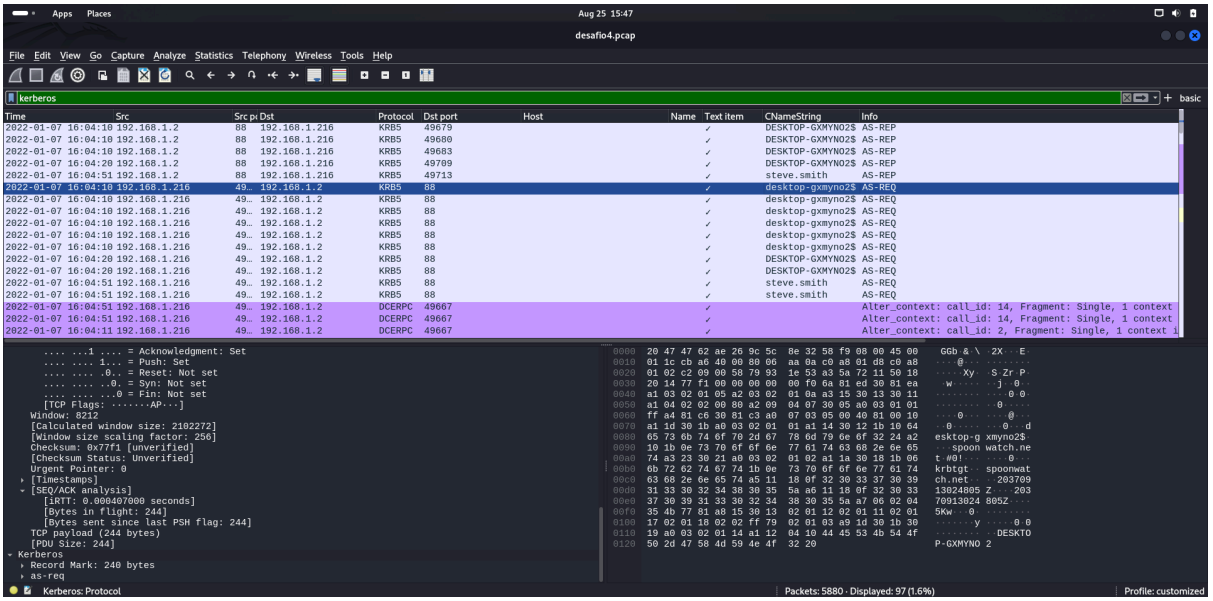
Resposta 19: 192.168.1.2



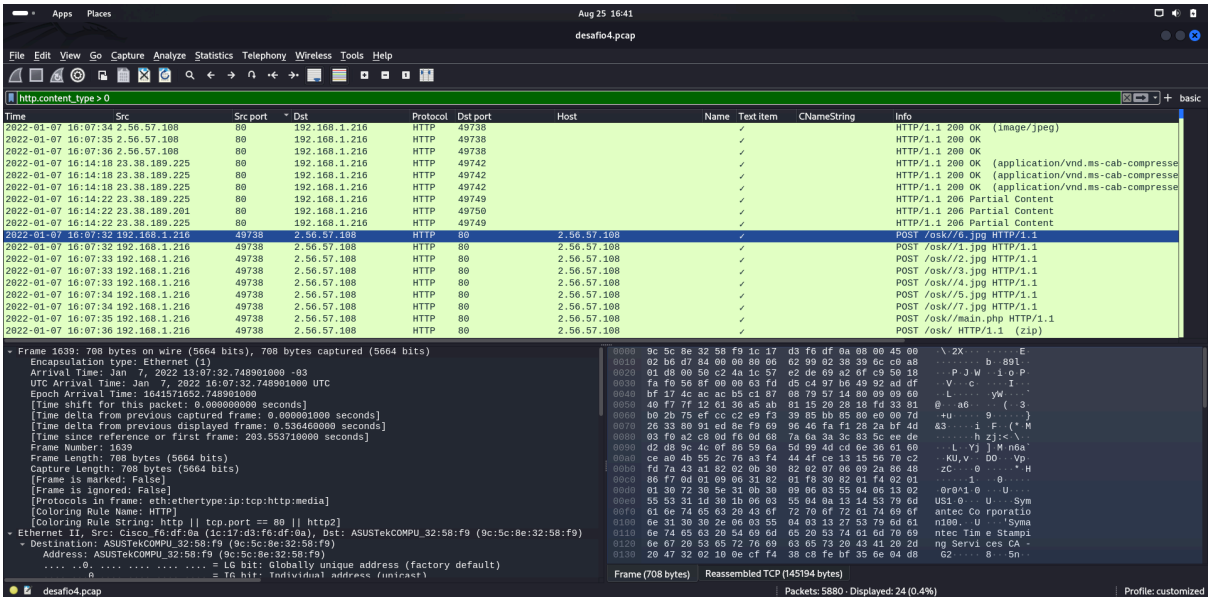
Resposta 20:steve.smith



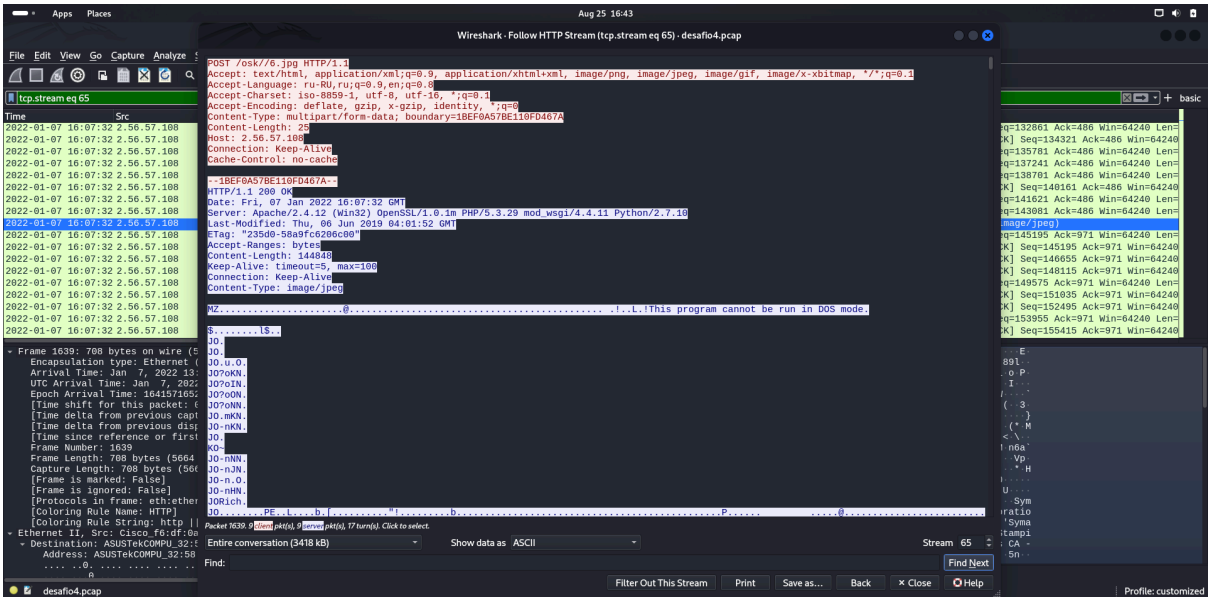
Pergunta 21:desktop-gxmyno2



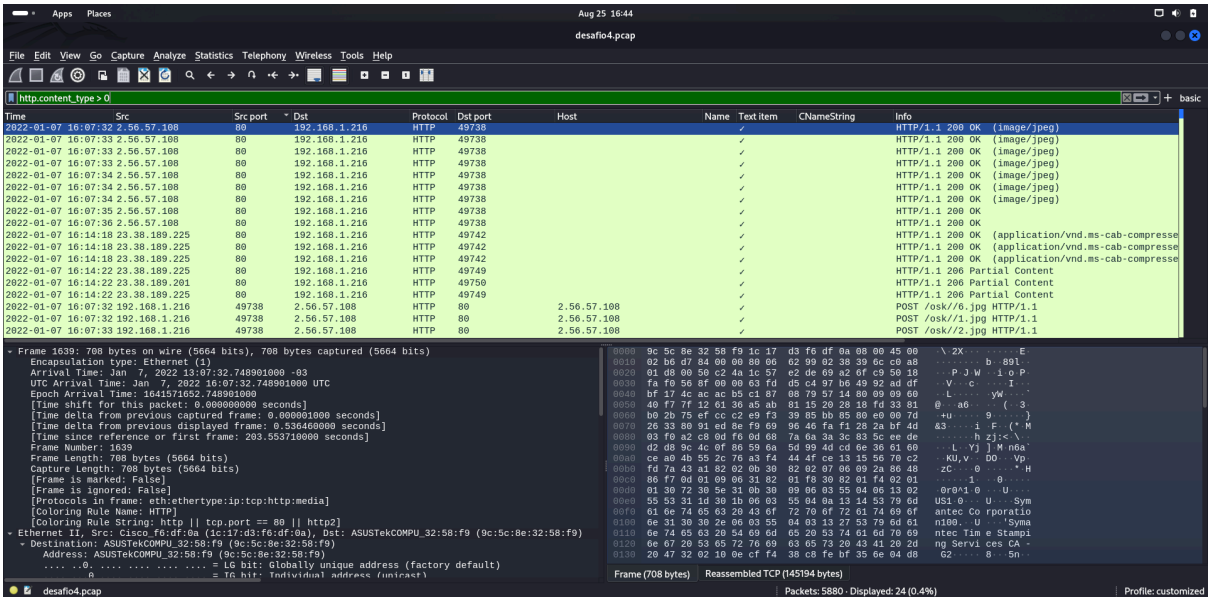
Pergunta 22:



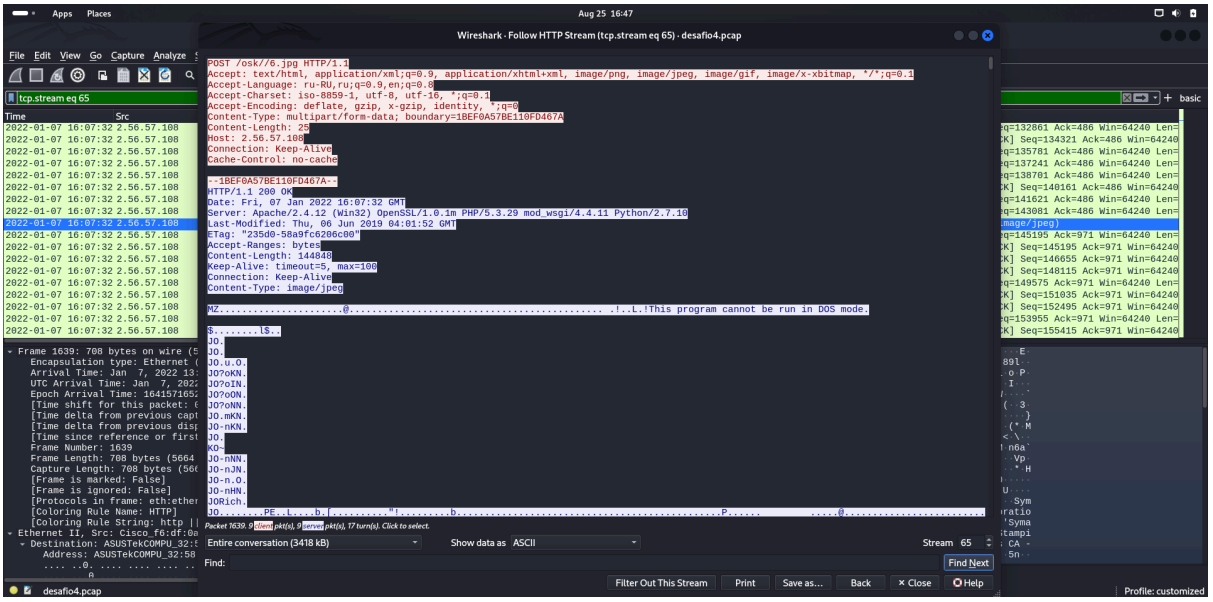
Primeiro podemos ver que o ip 192.168.1.216 fez vários posts suspeitos pro ip 2.56.57.108, são suspeitos porque podemos ver que o content type é image/jpeg mas como vemos abaixo ele está enviando um arquivo que começa com MZ, que é provavelmente um arquvio executável windows.



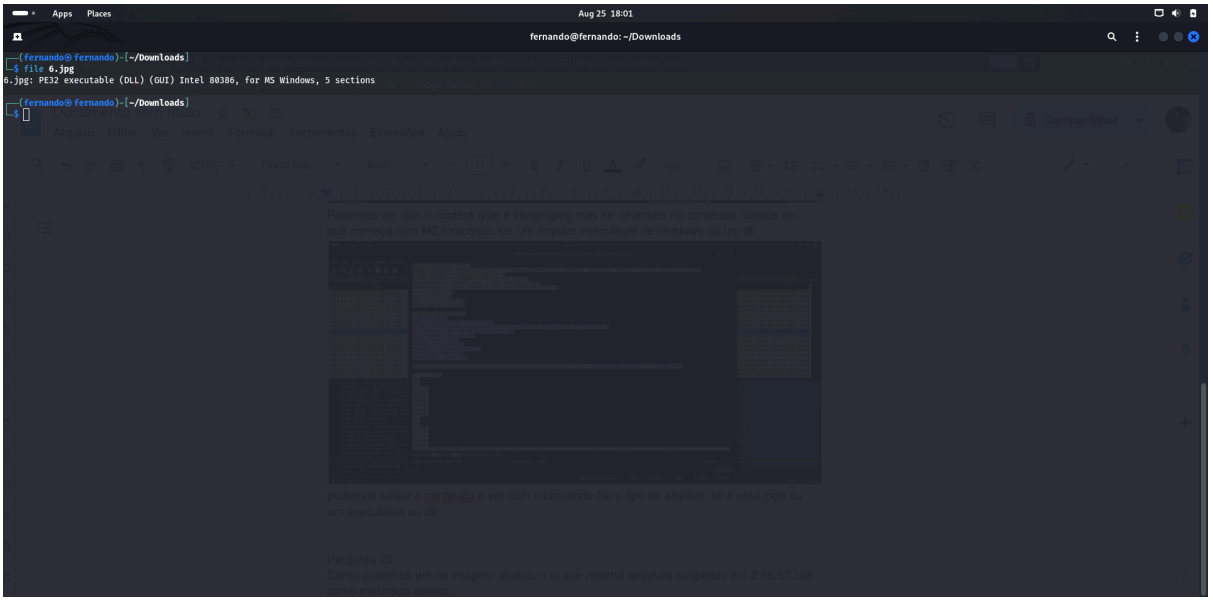
Logo depois vemos a máquina de destino retornar pra máquina de ip 192.168.1.216 arquivos suspeitos também:



Podemos ver que o content type é image/jpeg mas se olharmos no conteúdo, vamos ver que começa com MZ indicando ser um arquivo executável de windows ou um dll:

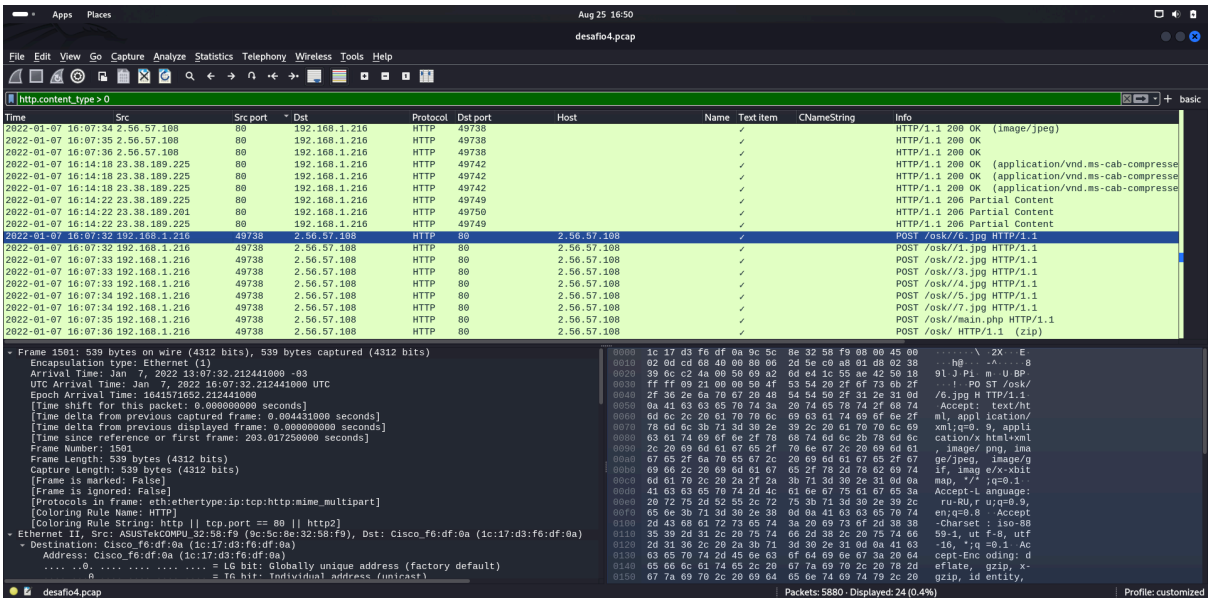


podemos salvar o conteudo e ver com o comando file o tipo de arquivo, se é uma jpge ou um executável ou dll:



vemos que é um dll e não um jpg, portanto é uma conexão suspeita.

Pergunta 23:
Como podemos ver na imagem abaixo, o ip que retorna arquivos suspeitos é o 2.56.57.108 como mostrado abaixo:



Vemos que a porta de conexão foi feita na porta 80.