

Tecnologias Hacker - Roteiro 1

Arthur Carvalho

Pergunta 1: Pesquise e registre aqui dois exemplos de IDS.

Dois exemplos de IDS são:

- Snort: serviço de detecção de intrusão que é baixável no windows. Ele utiliza de regras básicas que são baixadas diretamente do site do Snort e você pode configurar as regras a partir do seu próprio gosto
- Suricata: Diferente do Snort, o Suricata realiza a detecção na camada de aplicação e, além disso, consegue ler protocolos como HTTP, SMB e FTP.

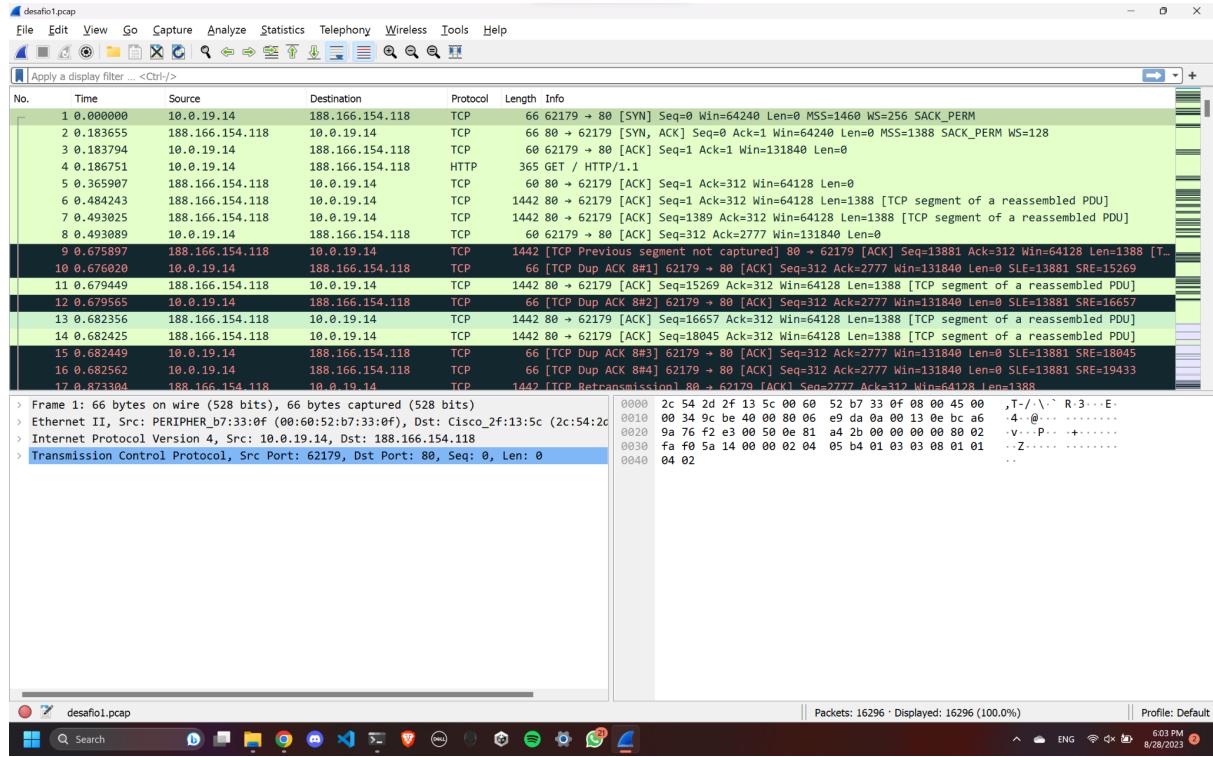
Pergunta 2: Quais as diferenças entre IDS e IPS?

O IDS(Intrusion Detection System) e o IPS(Intrusion Protection System) são sistemas de segurança para um computador. O IDS consiste em detectar possíveis ameaças no sistema, permitindo ao usuário maior flexibilidade e liberdade em relação a como tratar a segurança própria em seu sistema. Já o IPS tem, em seu escopo, além da detecção de vulnerabilidades, a proteção pró-ativa do sistema, assim comprometendo a liberdade e flexibilidade do usuário e trocando-a por maior prevenção dada pelo provedor do serviço.

DESAFIO 1

1 - Pergunta: Qual o IP do controlador de domínio desta rede?

O IP do host é 10.0.19.14

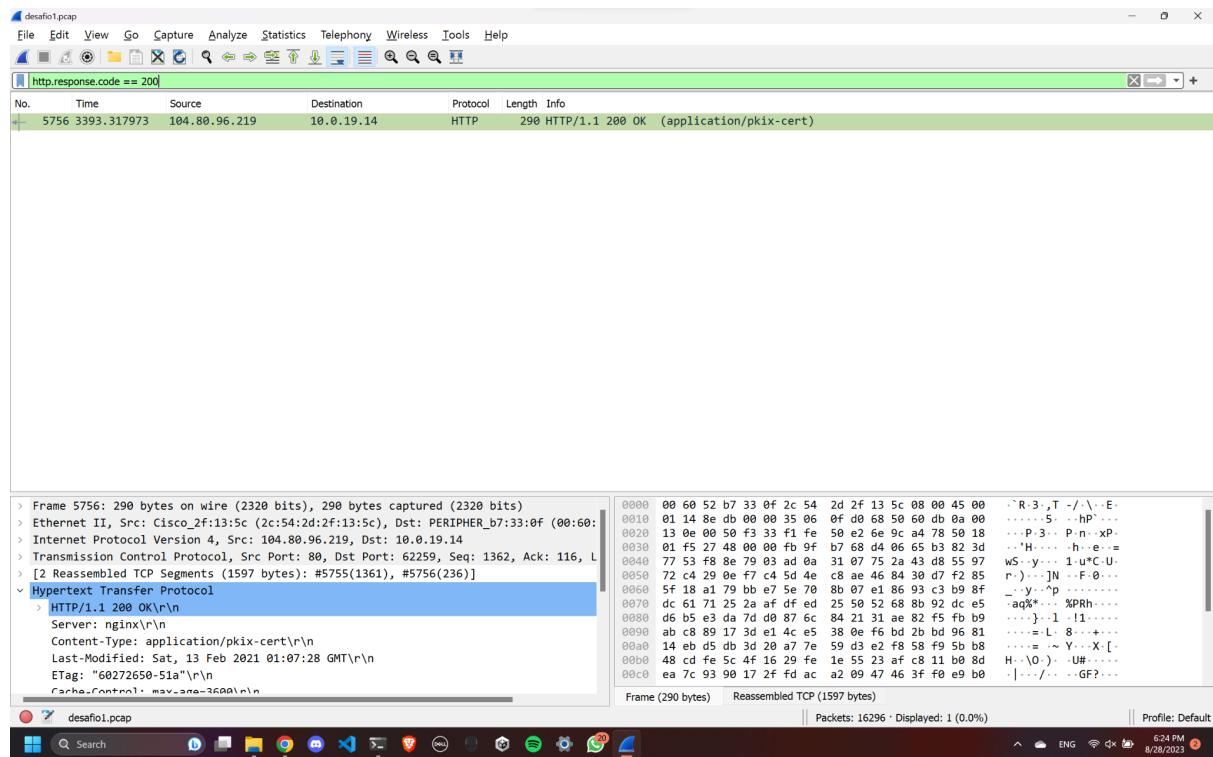


2 - Pergunta: Liste as conexões que você julga suspeitas.

- 10.0.19.9
- 104.80.96.219
- 209.197.3.8
- 69.28.162.0
- 69.28.162.128
- 68.142.107.1

3 - Pergunta: Qual conexão baixou o código malicioso?

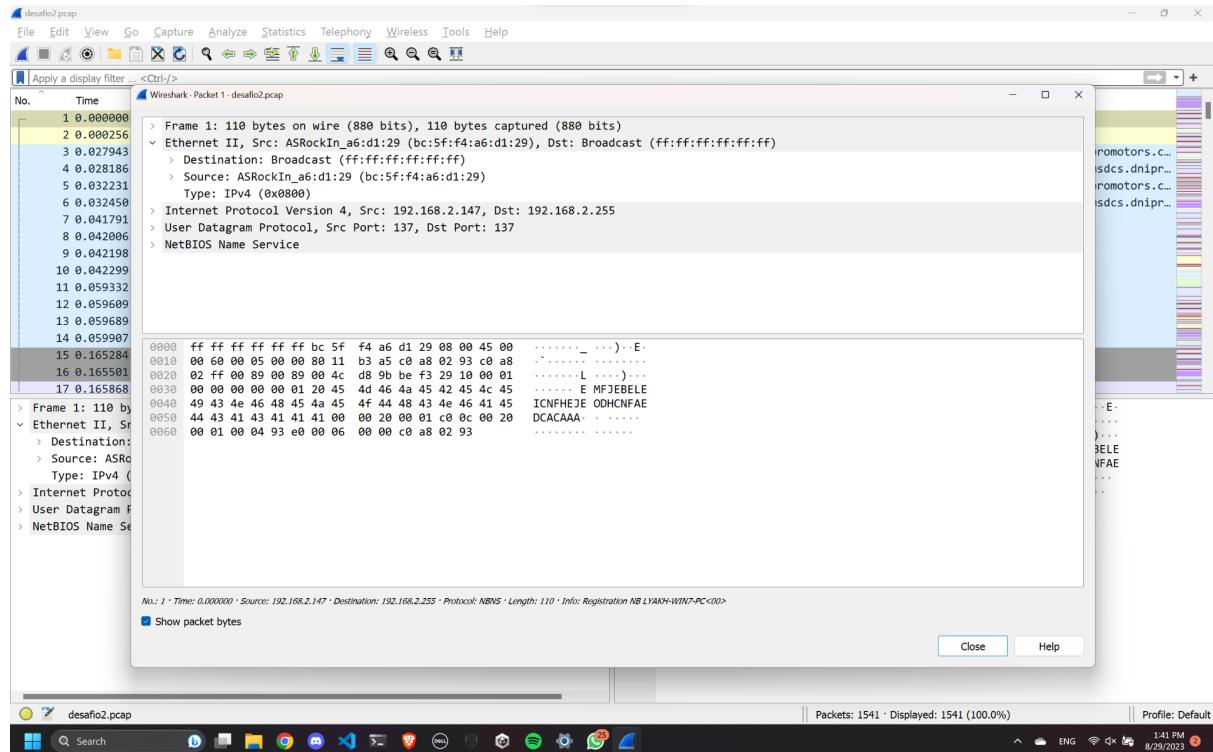
A conexão é: 104.80.96.219



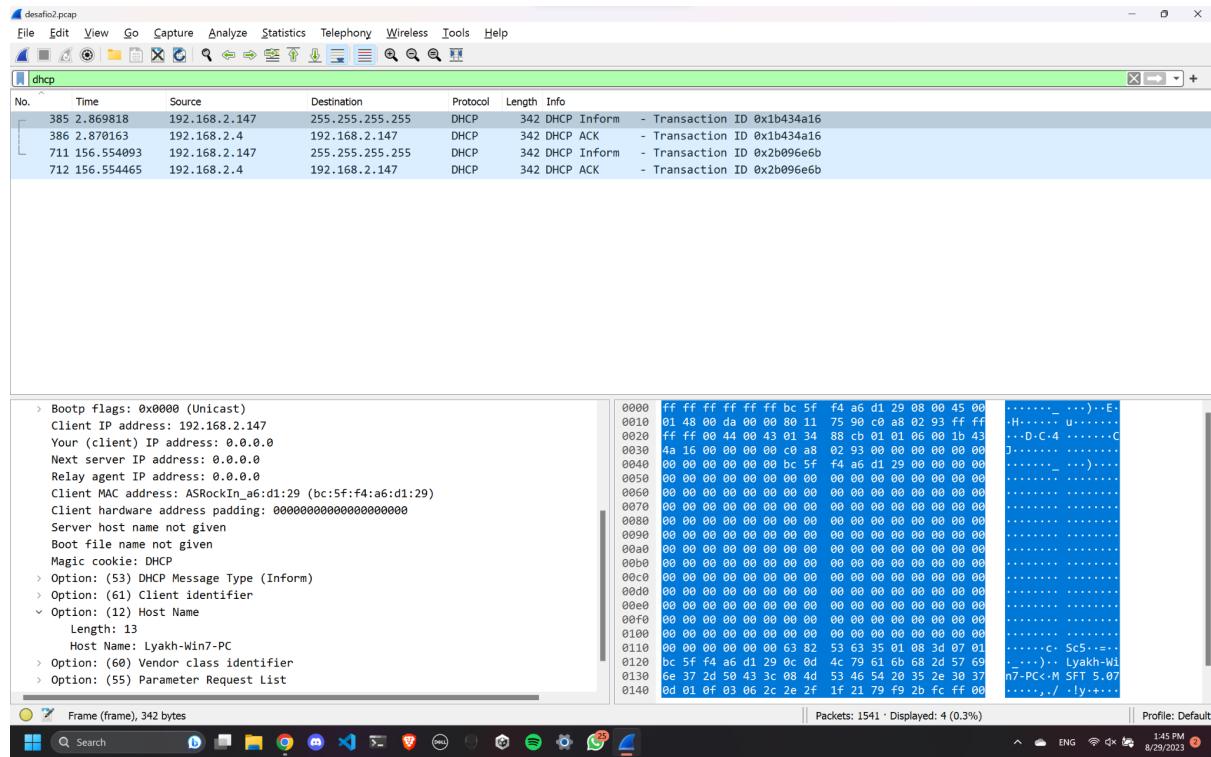
DESAFIO 2

Pergunta 3: Qual é o endereço MAC do cliente Windows em 192.168.2.147?

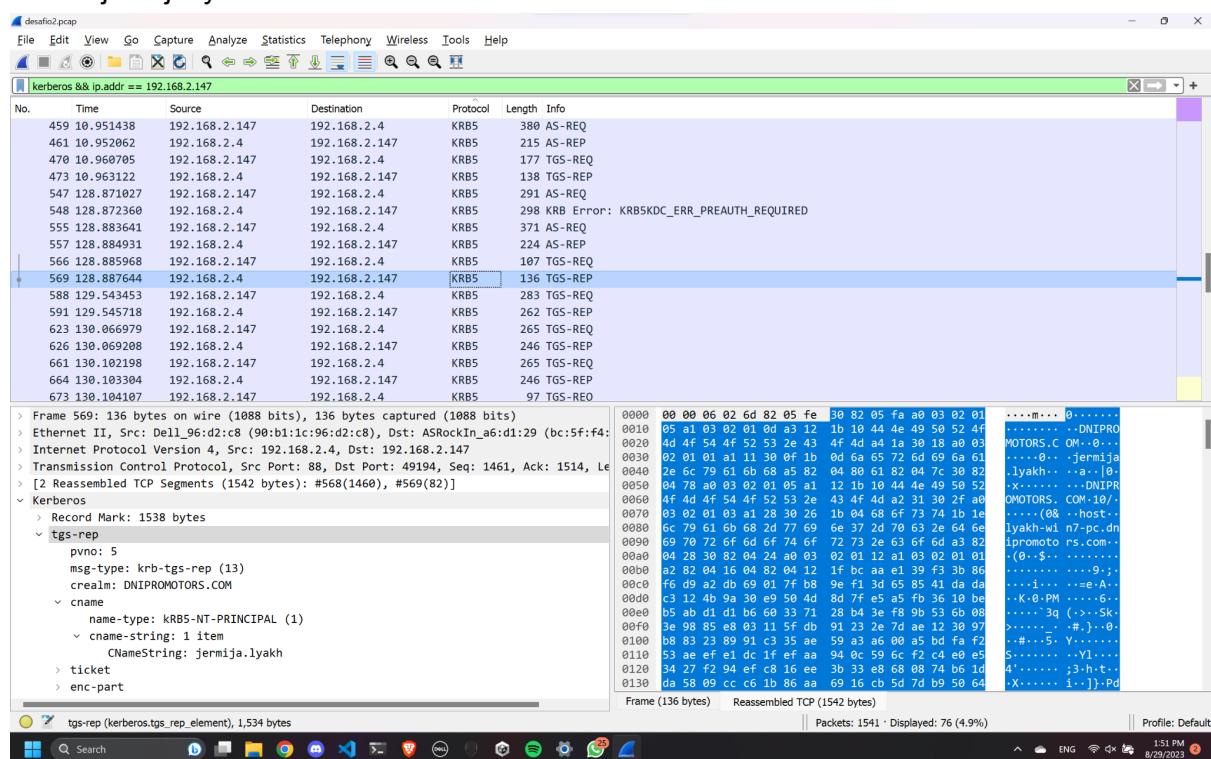
bc:5f:f4:a6:d1:29



Pergunta 4: Qual é o nome do host para o cliente Windows em 192.168.2.147?
host name : Lyakh-Win7-PC



Pergunta 5: Com base no tráfego do protocolo Kerberos, qual é o nome da conta de usuário do Windows usado em 192.168.2.147?
jermija.lyaki



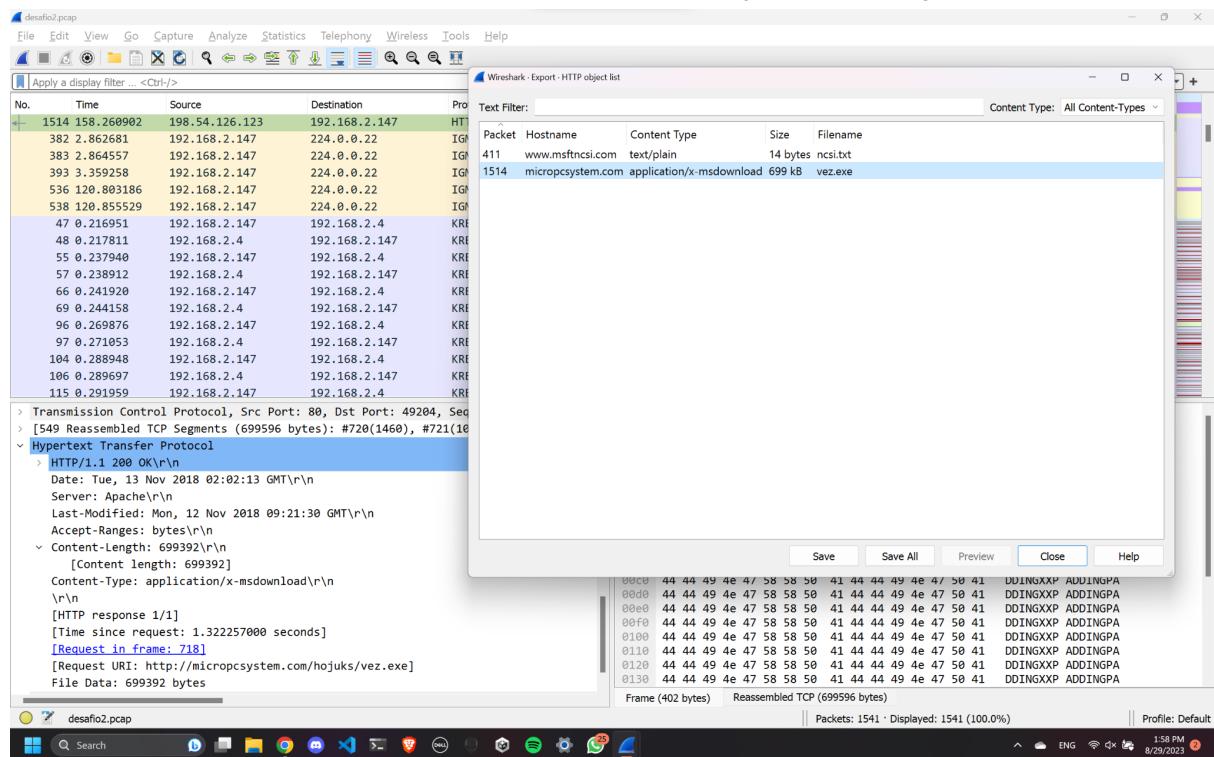
Após erro no número 548, a máquina faz a autenticação e o nome passa a ser jermija.lyaki ao invés do nome da máquina (Lyakh-Win7-PC).

Pergunta 6: Qual a função do protocolo Kerberos?

O protocolo Kerberos serve para realizar a autenticação entre cliente e servidor em uma rede não segura.

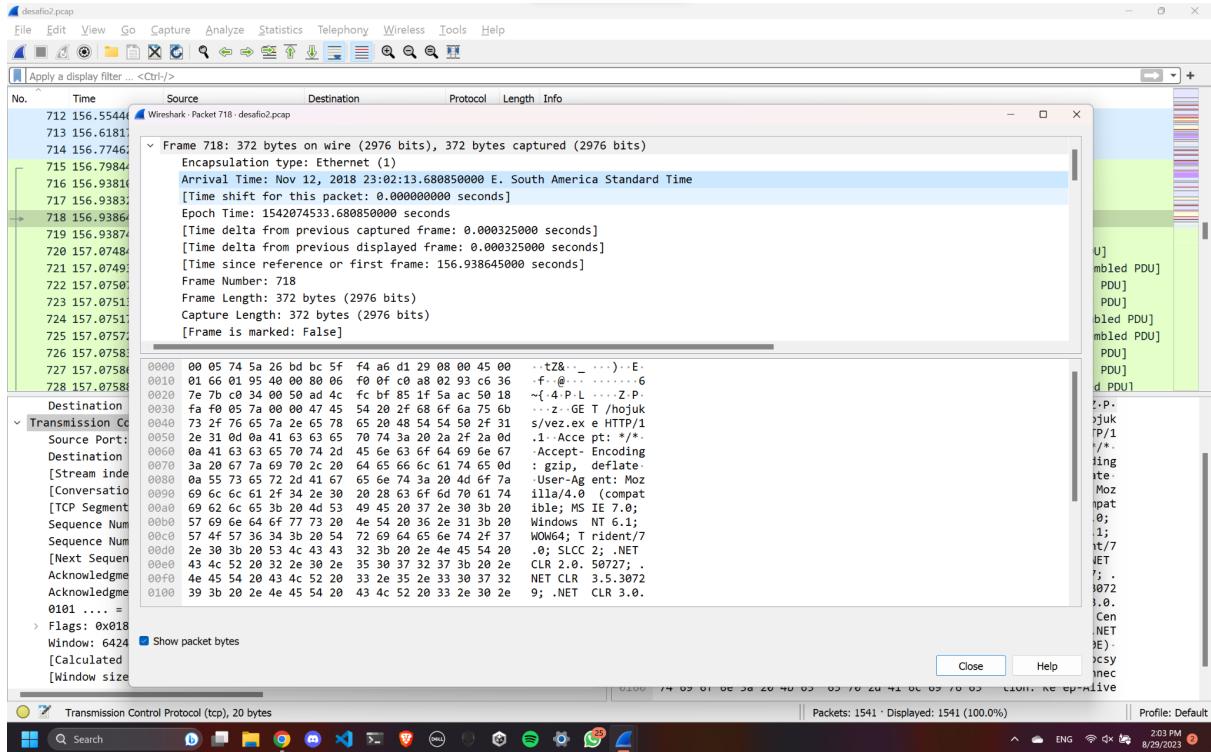
Pergunta 7: Qual é a URL que retornou um arquivo executável do Windows?

A URL que retorna o executável é <http://micropcsystem.com/hojuks/vez.exe>



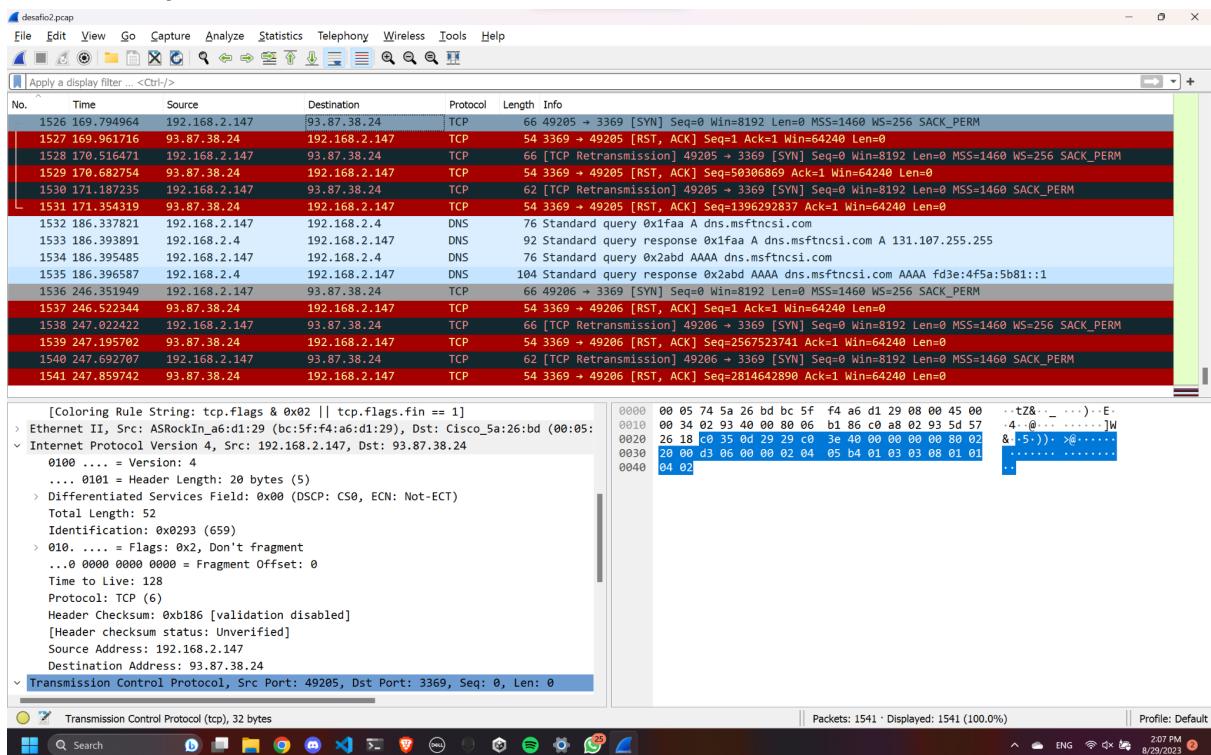
Pergunta 8: Qual data e hora que a URL foi acessada?

O timestamp de acesso da URL é dia 12/11/2018 às 23:02:13 no horário de E. South America Standard Time (UTC -3:00)



Pergunta 9: Depois de receber o arquivo executável, com qual endereço IP o host infectado do Windows tentou estabelecer uma conexão TCP?

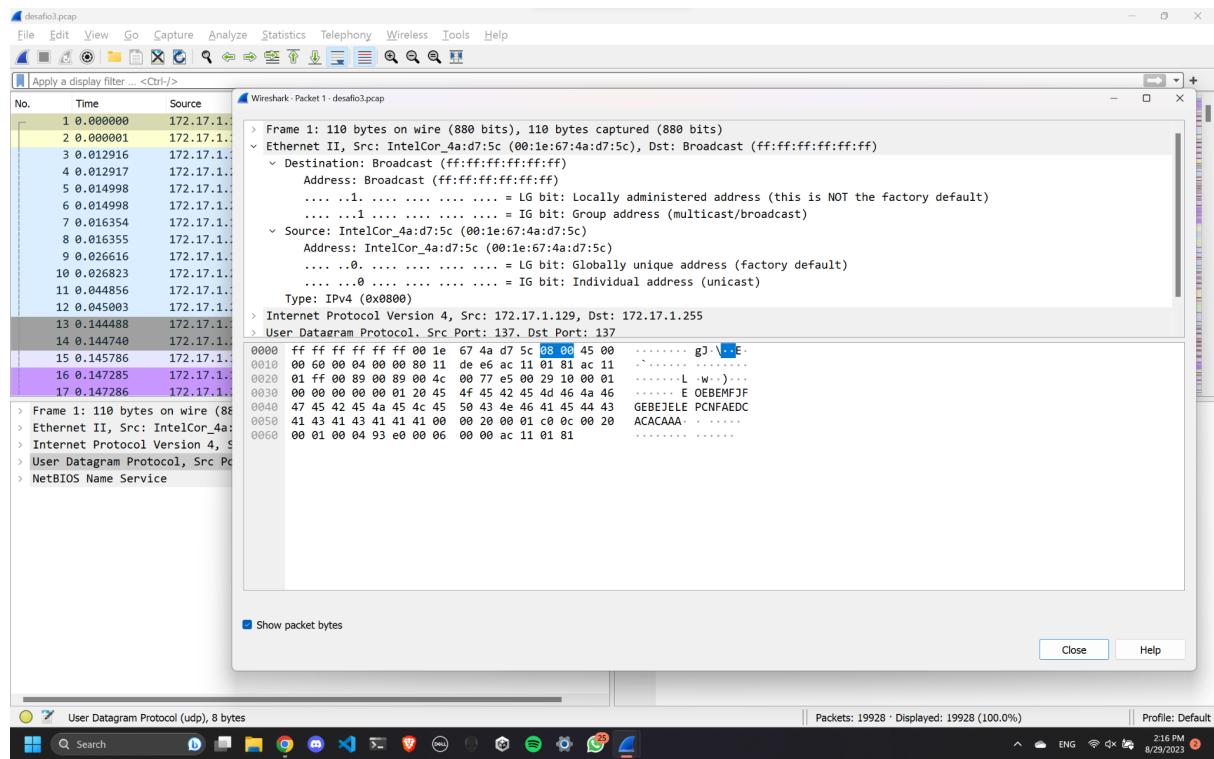
O endereço IP é 93.87.38.24, pois, completado o download do arquivo, o handshake (SYN) começa utilizando esse IP.



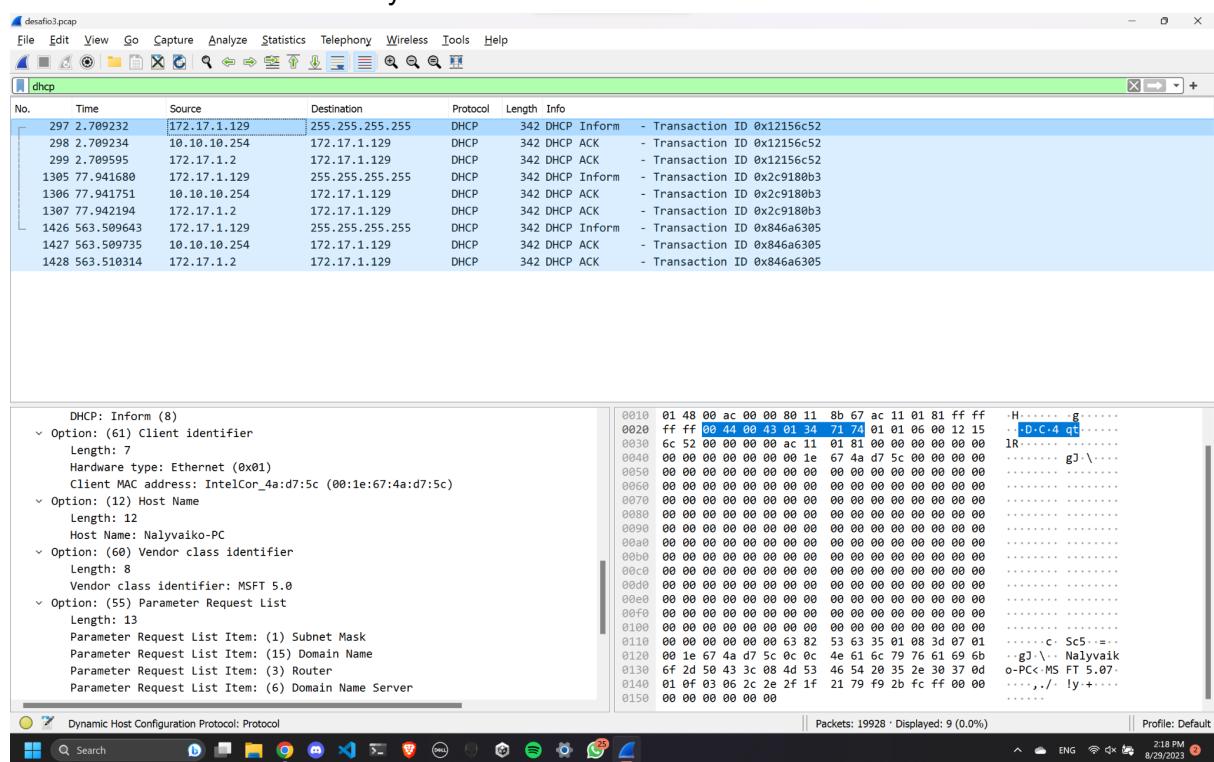
DESAFIO 3

Pergunta 10: Qual é o endereço MAC do cliente Windows em 172.17.1.129?

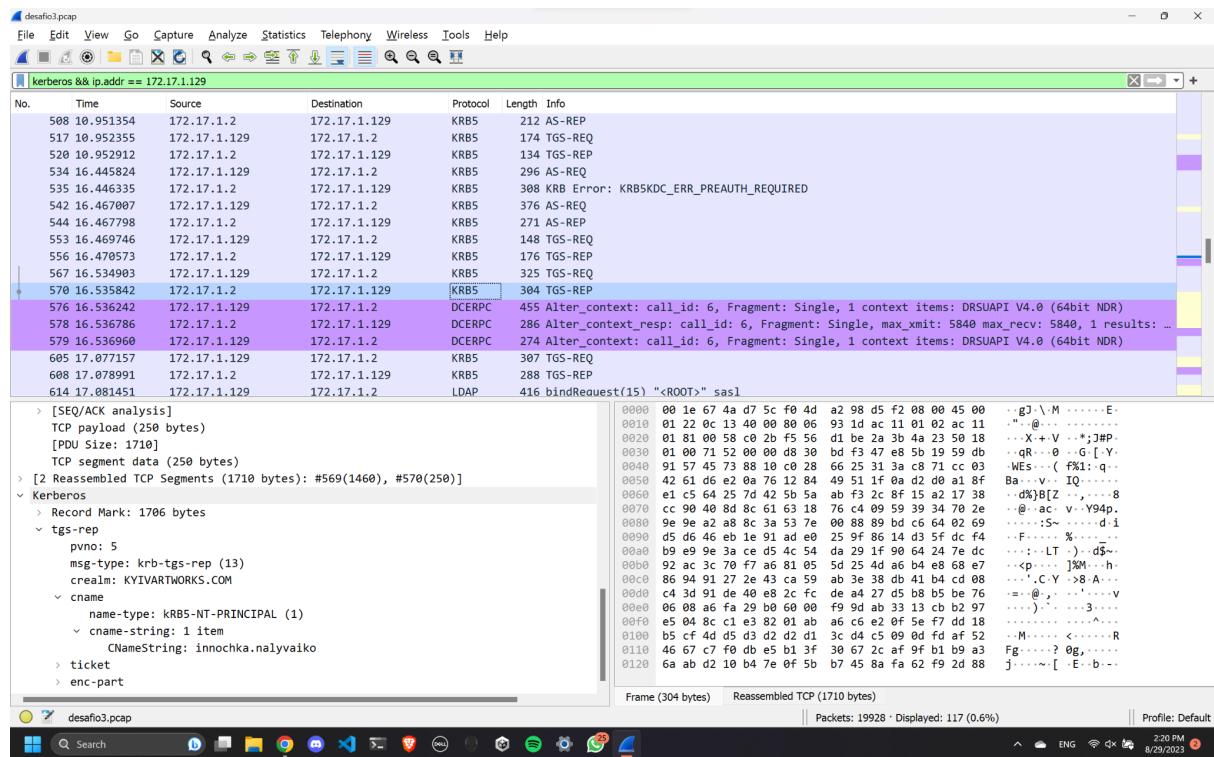
O endereço MAC é 00:1e:67:4a:d7:5c



Pergunta 11: Qual é o nome do host para o cliente Windows em 172.17.1.129?
O nome do host é Nalyvaiko-PC.

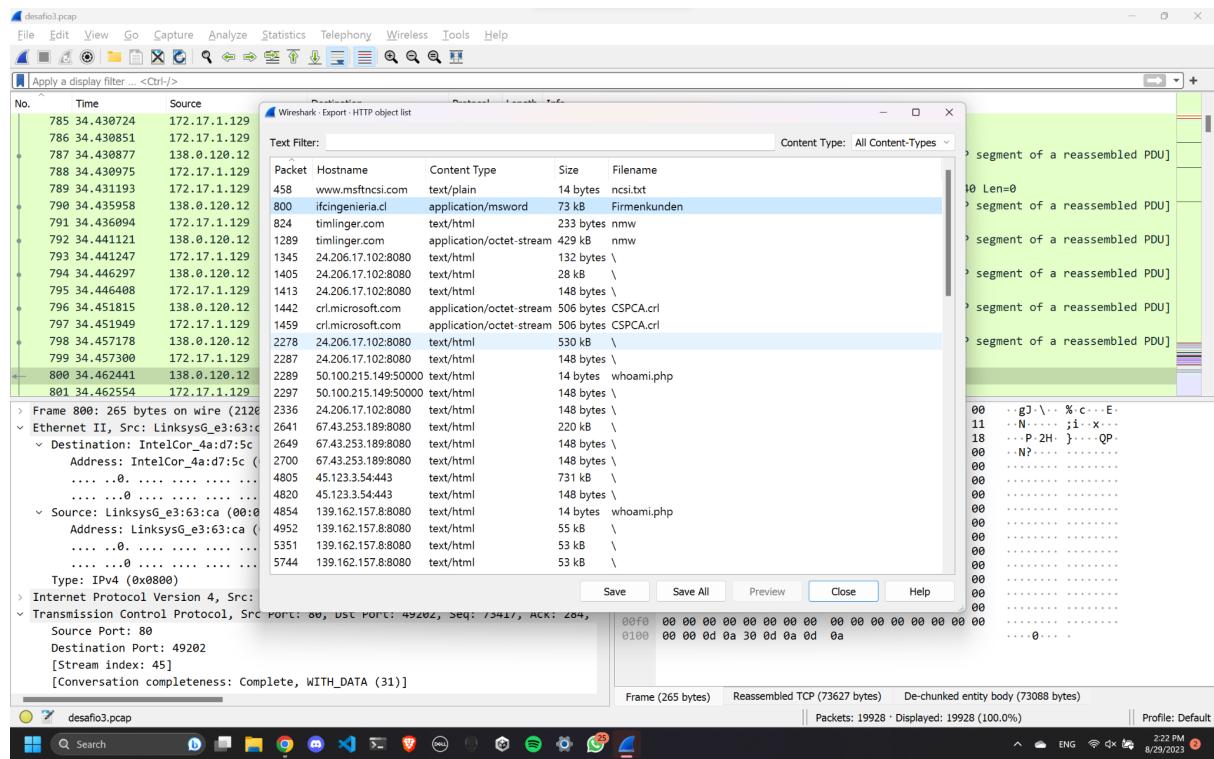


Pergunta 12: Com base no tráfego Kerberos, qual é o nome da conta de usuário do Windows usado em 172.17.1.129?
O nome da conta de usuário é innochka.nalyvaiko.



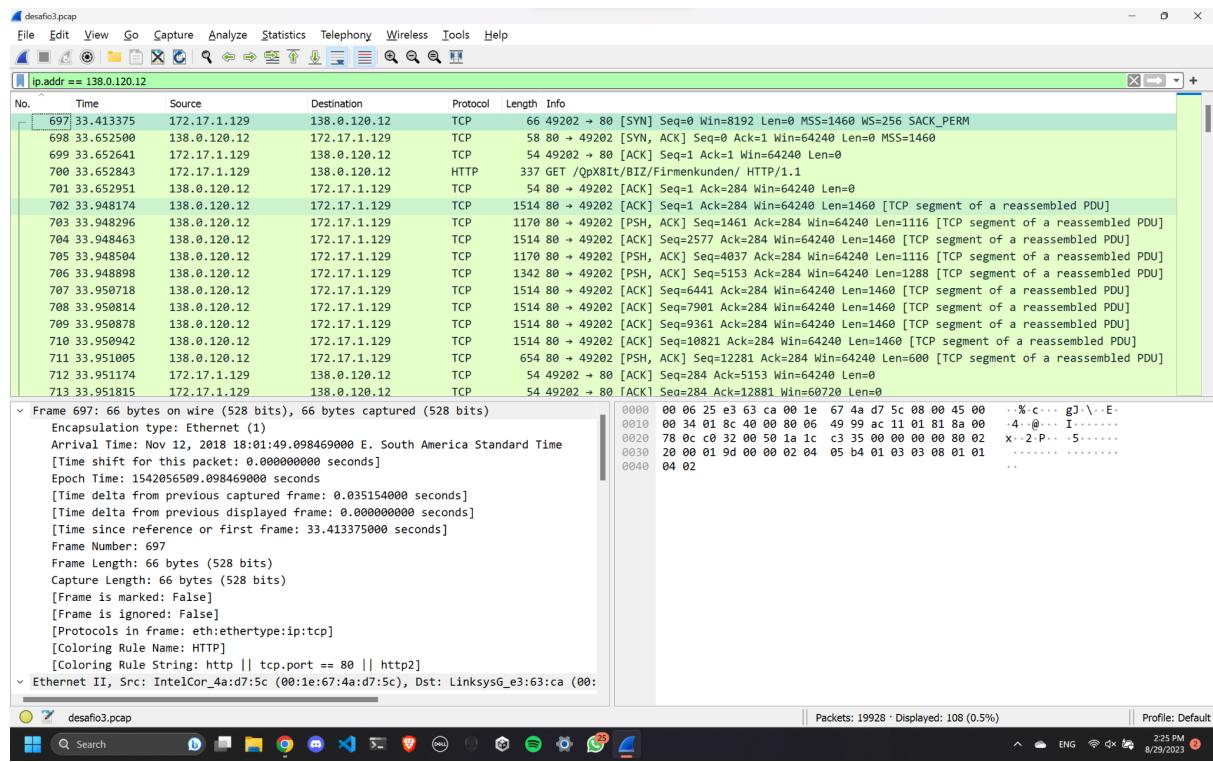
Pergunta 13: Qual URL no pcap retornou um documento do Microsoft Word?

<http://ifcingenieria.cl/QpX8It/BIZ/Firmenkunden/>. Packet número 800.



Pergunta 14: Qual data e hora que a URL foi criada?

O handshake e, consequentemente, a conexão, foi criado às 18:01:49 do dia 12/11/2018.



Pergunta 15: Qual URL no pcap retornou um arquivo executável do Windows?
A url do executável é <http://timlinger.com/nmw/>.

