

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:

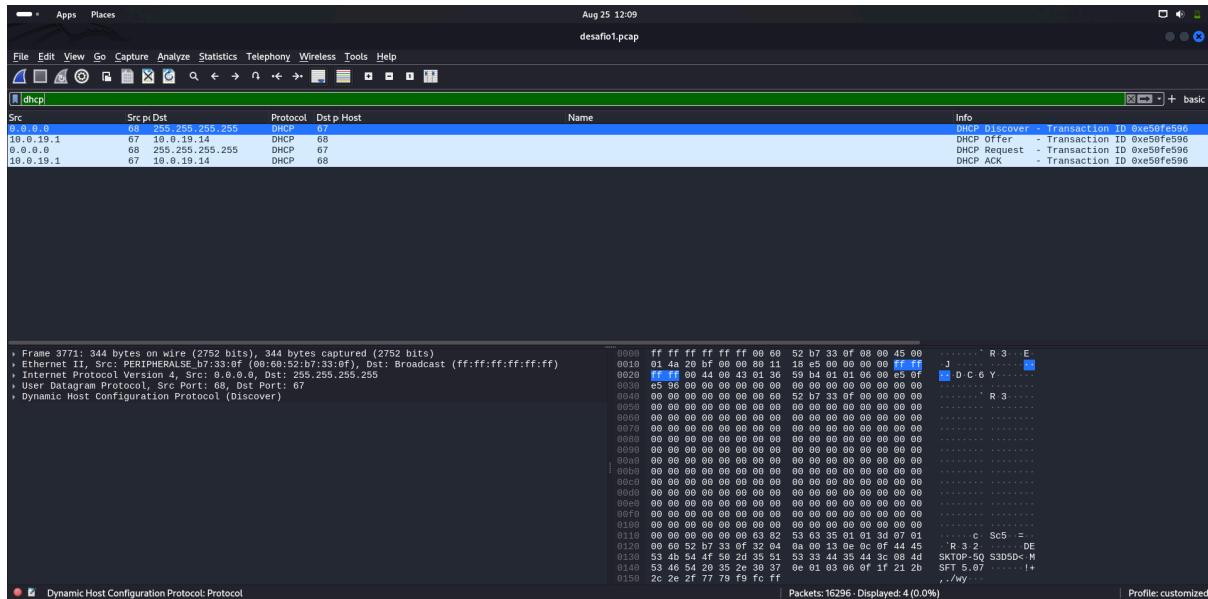
### **Função Principal:**

- **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:**

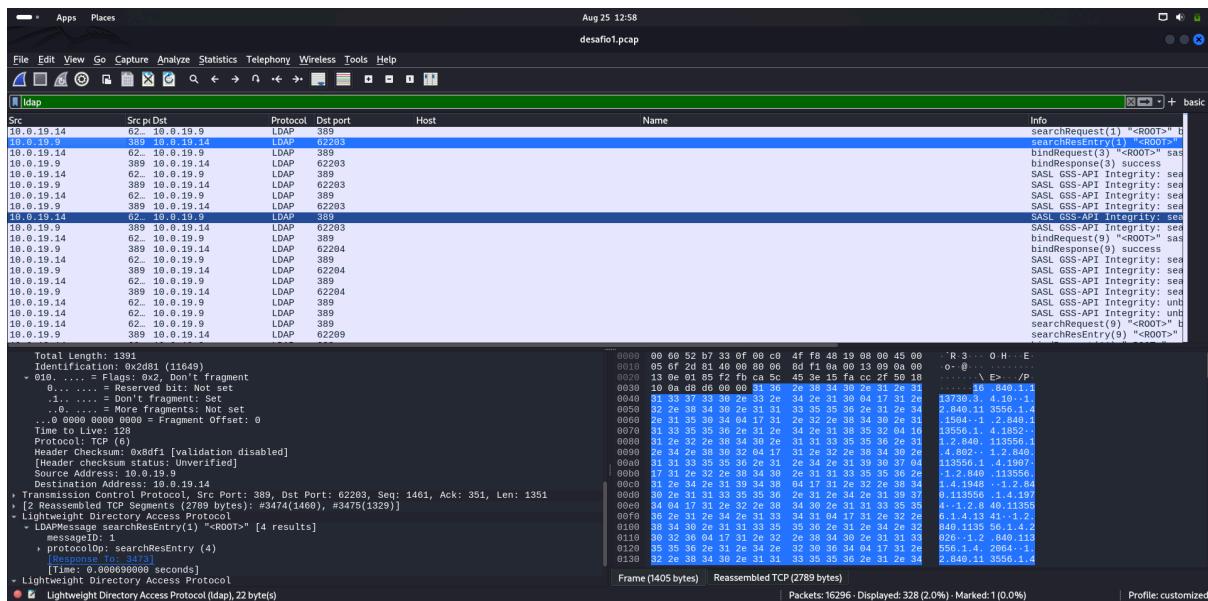
- **IDS:** Opera de forma passiva. Ele monitora e analisa o tráfego, mas não interfere diretamente no tráfego de rede. As ações corretivas devem ser tomadas manualmente por administradores de segurança com base nos alertas gerados.
- **IPS:** Opera de forma ativa. Ele é inserido diretamente no caminho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

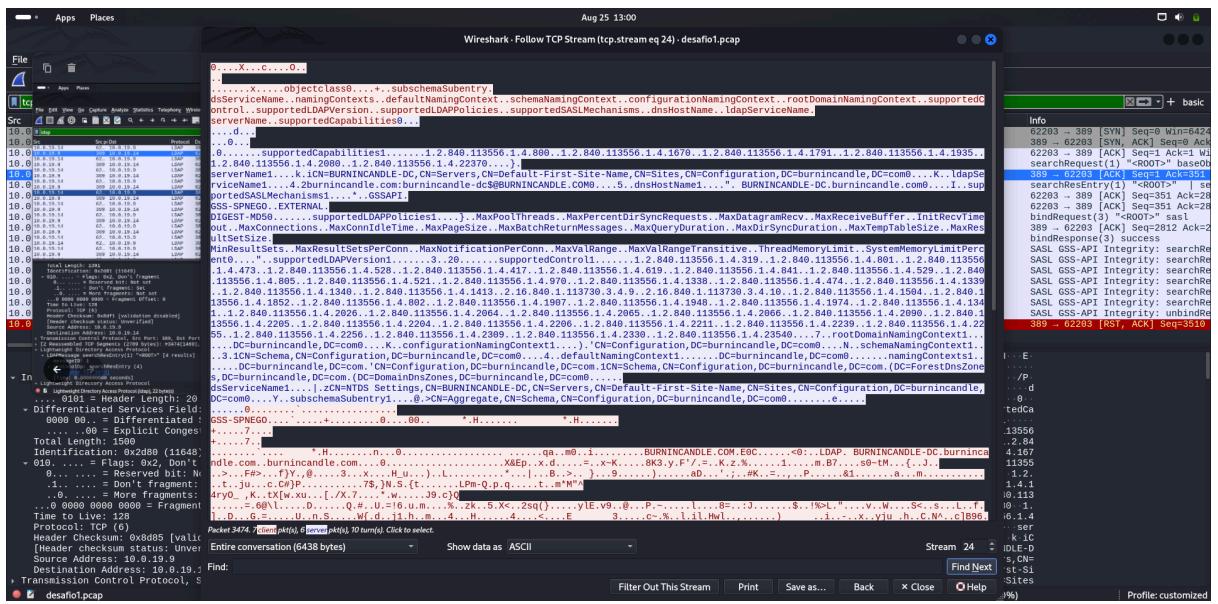
### pergunta 3:



IP do servidor DHCP: 10.0.19.1

#### pergunta 4:





**DC = burnincandle.com**

**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:

Aug 25 13:22

6 / 96

6/96 security vendors flagged this URL as malicious

http://bpupdate.com/  
bpupdate.com

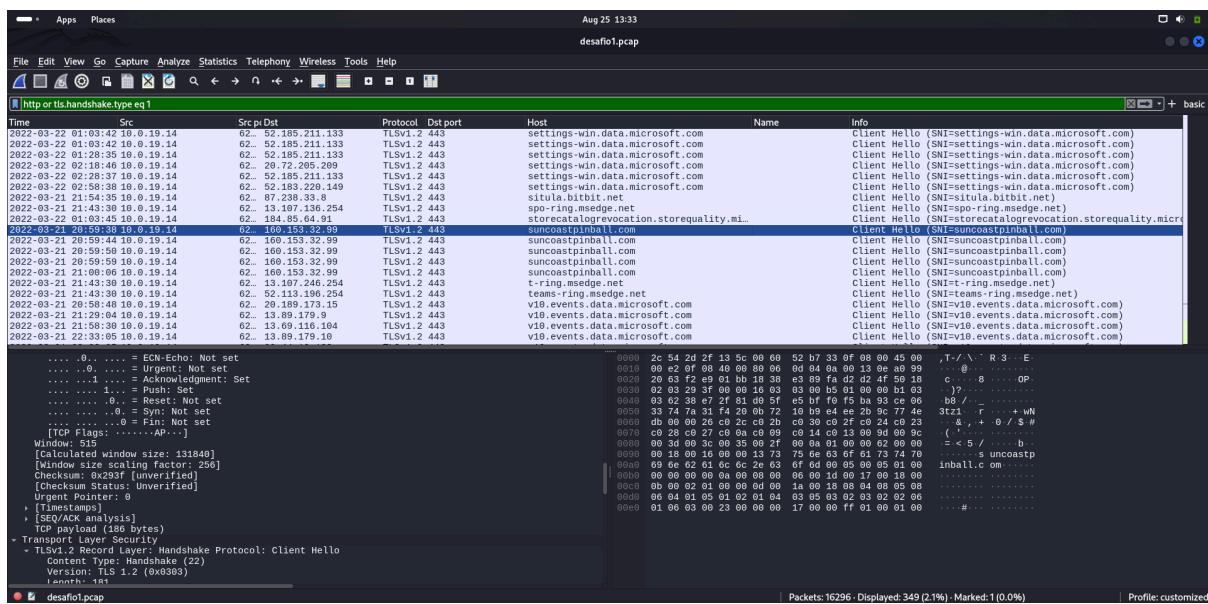
Last Analysis Date  
3 days ago

DETECTION DETAILS COMMUNITY

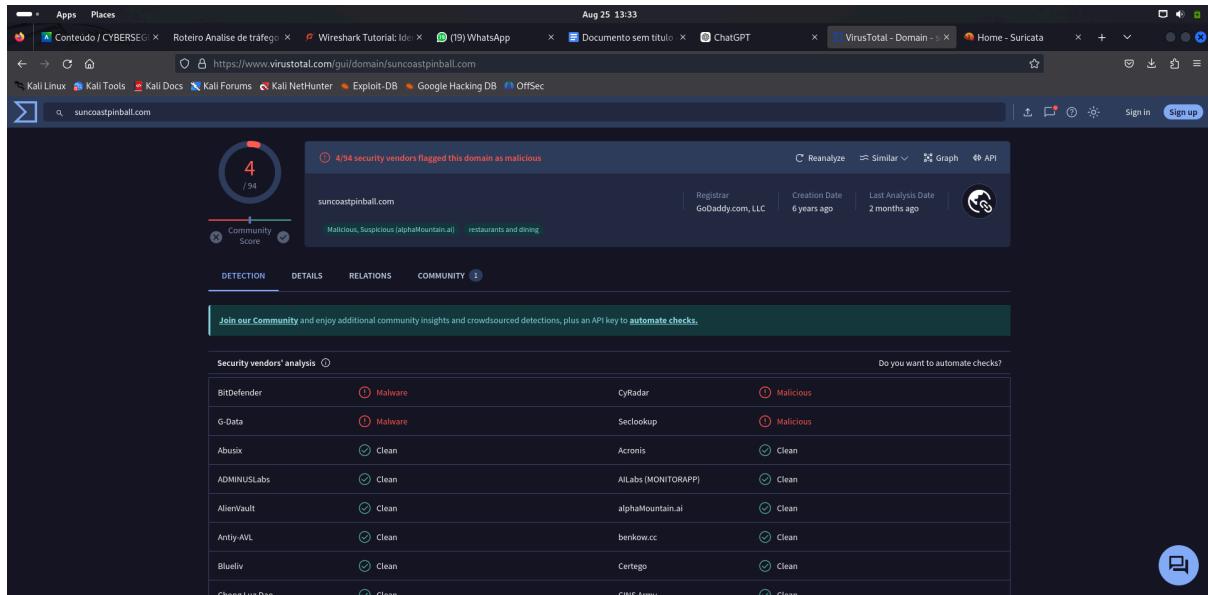
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendor's analysis		Do you want to automate checks?
Arity-AVL	Malicious	Malware
CyRadar	Malicious	Malware
Seclookup	Malicious	Malware
Abusik	Clean	Clean
ADMINUSLabs	Clean	Clean
AlienVault	Clean	Clean
Artists Against 419	Clean	Clean
BlockList	Clean	Clean
BitDefender		
G-Data		
Sophos		
Acronis		
AllLabs (MONITORAPP)		
alphaMountain.ai		
berinkow.cc		
Blueliv		

Outra conexão suspeita foi a de baixo:



verificando no virustotal.com:



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

Aug 25 13:39  
desafio2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**dhcp**

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Info
2018-11-13 01:59:39	192.168.2.147	68	255.255.255.255	DHCP	67			DHCP Inform
2018-11-13 02:02:19	192.168.2.147	67	192.168.2.147	DHCP	66			DHCP ACK
2018-11-13 02:02:19	192.168.2.147	68	255.255.255.255	DHCP	67			DHCP Inform
2018-11-13 02:02:19	192.168.2.4	67	192.168.2.147	DHCP	68			DHCP ACK

```

> Frame 386: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
   Ethernet II, Src: Dell (90:b1:1c:96:d2:c8), Dst: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
-> Destination: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
  + Source: Dell 90:d2:c8 (90:b1:1c:96:d2:c8)
  + Address: Dell 90:d2:c8 (90:b1:1c:96:d2:c8) [factory default]
  + ... .0 .. . = L6 bit: Globally unique address (factory default)
  + ... .0 .. . = Ig bit: Individual address (unicast)
  + Type: IPv4 (0x0800)
-> Internet Protocol Version 4, Src: 192.168.2.4, Dst: 192.168.2.147
  + User Datagram Protocol, Src Port: 67, Dst Port: 68
  + Destination Port: 68
  + Length: 368
  + Checksum: 0xc8ef [unverified]
    [Checksum Status: Unverified]
    [Timestamp Index: 17]
  + [Timestamps]
  + UDP payload (368 bytes)
-> Dynamic Host Configuration Protocol (ACK)
  + Source or Destination Hardware Address (eth.addr), 6 byte(s)

```

Packets: 1541 - Displayed: 4 (0.3%) | Profile: customized

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

Aug 25 13:40  
desafio2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**dhcp**

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Info
2018-11-13 01:59:39	192.168.2.4	67	255.255.255.255	DHCP	68			DHCP Inform
2018-11-13 02:02:13	192.168.2.147	68	255.255.255.255	DHCP	67			DHCP ACK
2018-11-13 02:02:13	192.168.2.4	67	192.168.2.147	DHCP	68			DHCP Inform

```

> Frame 385: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
   Ethernet II, Src: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
-> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  + Address: Broadcast (ff:ff:ff:ff:ff:ff) [group/mcast/broadcast]
  + ... .A .. . = L6 bit: Locally administered address (this is NOT the factory default)
  + ... .1 .. . = Ig bit: Group address (multicast/broadcast)
  + Source: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
  + Address: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29) [factory default]
  + ... .0 .. . = L6 bit: Globally unique address (factory default)
  + ... .0 .. . = Ig bit: Individual address (unicast)
  + Type: IPv4 (0x0800)
-> Internet Protocol Version 4, Src: 192.168.2.147, Dst: 255.255.255.255
  + User Datagram Protocol, Src Port: 68, Dst Port: 67
  + Destination Port: 67
  + Length: 368
  + Checksum: 0x88c8 [unverified]
    [Checksum Status: Unverified]
    [Timestamp Index: 16]
  + [Timestamps]
  + UDP payload (368 bytes)
-> Dynamic Host Configuration Protocol (ACK)
  + Source or Destination Hardware Address (eth.addr), 6 byte(s)

```

Packets: 1541 - Displayed: 4 (0.3%) | Profile: customized

pergunta 8:Host=LYAKH-WIN7-PC

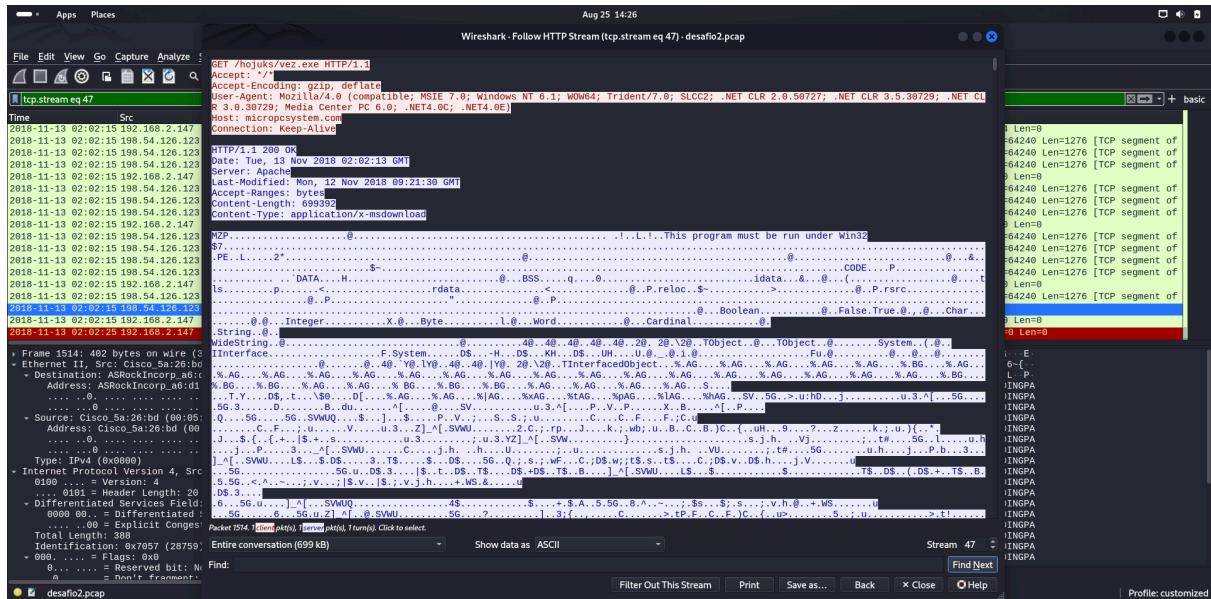
## Pergunta 9: jermija.lyakh

The Wireshark interface displays a sequence of network packets. The timeline pane shows the following sequence of events:

- 2018-11-13 01:59:47.132, Src: 192.168.2.4, Dst: 192.168.2.147, Protocol: LDAP, Port: 389, Info: UnboundResponse(10) success
- 2018-11-13 01:59:47.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: AS-REQ, KRB Error: KRB5KDC\_ERR\_PREAMUTH\_REQUIRED
- 2018-11-13 01:59:47.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: AS-REP
- 2018-11-13 01:59:47.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: TGS-REQ
- 2018-11-13 01:59:47.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: TGS-REP
- 2018-11-13 02:01:49.132, Src: 192.168.2.4, Dst: 192.168.2.147, Protocol: Kerberos, Port: 464, Info: AS-REQ, KRB Error: KRB5KDC\_ERR\_PREAMUTH\_REQUIRED
- 2018-11-13 02:01:49.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: AS-REP
- 2018-11-13 02:01:49.132, Src: 192.168.2.4, Dst: 192.168.2.147, Protocol: Kerberos, Port: 464, Info: TGS-REQ
- 2018-11-13 02:01:49.132, Src: 192.168.2.4, Dst: 192.168.2.147, Protocol: Kerberos, Port: 464, Info: TGS-REP
- 2018-11-13 02:01:49.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: AS-REQ, KRB Error: KRB5KDC\_ERR\_PREAMUTH\_REQUIRED
- 2018-11-13 02:01:49.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: AS-REP
- 2018-11-13 02:01:49.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: TGS-REQ
- 2018-11-13 02:01:49.132, Src: 192.168.2.147, Dst: 192.168.2.4, Protocol: Kerberos, Port: 464, Info: TGS-REP

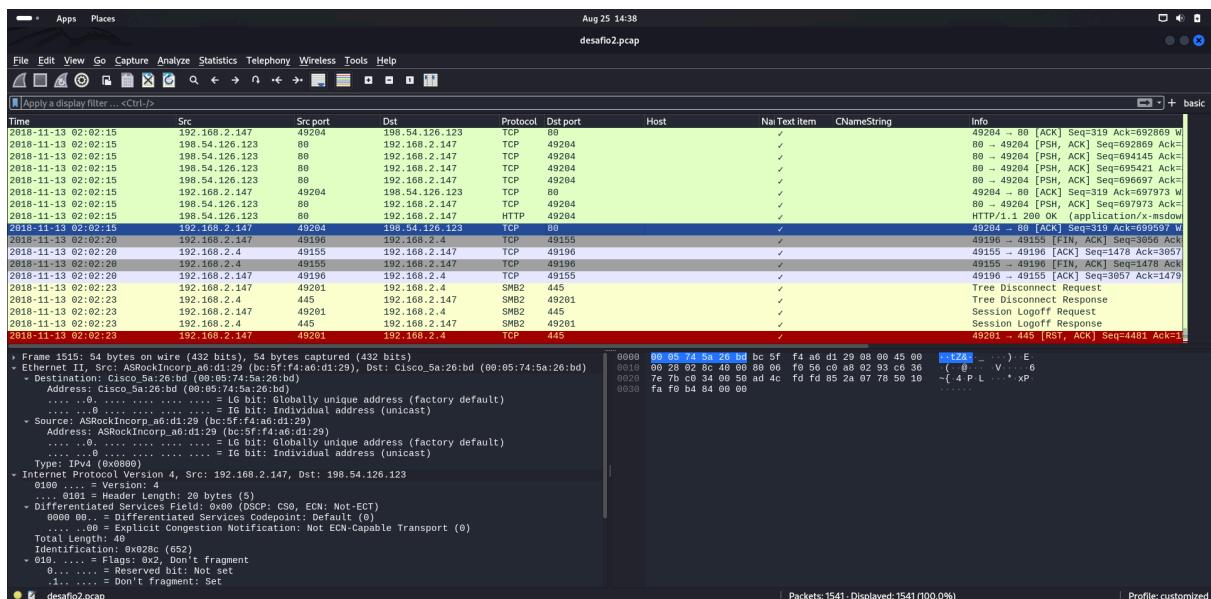
The details pane shows the structure of the Kerberos messages, including fields like cNameString, realm, and ticket-tkt-vno. The bytes pane shows the raw binary data for each packet.

## Resposta 10: [micropcsystem.com/hojuks/vez.exe](http://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

Aug 25 14:43  
desafio3.pcap

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[ ip.addr == 172.17.1.129 ] basic
Time Src Src/Dst Protocol Dstport Host NaiText Item CNameString Info
2018-11-12 21:01:15 172.17.1.129 137 172.17.1.255 NBNS 137 ✓ Registration NB NALYVAIKO-PC<0>
2018-11-12 21:01:15 172.17.1.129 137 172.17.1.255 NBNS 137 ✓ Registration NB KYIVARTWORKS<0>
2018-11-12 21:01:15 172.17.1.129 60.. 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 66888 -- Standard query response 0x109 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 59478 -- Standard query response 0x109 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 DNS 53 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.129 DNS 53548 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53556 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53552 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49156 .. 49156 [SYN] Seq=0 Win=0 MSS=1468
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 TCP 49155 -- 49155 [SYN ACK] Seq=0 Ack=1 Win=8192 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49155 .. 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.129 DCERPC 135 Bind: call_id: 2, Fragment: Single, 3 context it
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 DCERPC 49155 Bind: ack: call_id: 2, Fragment: Single, max_xmit
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 EPM 135 Map request, RPC_NETLOGON, 32bit NDR

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Intel 4a:d7:5c (00:1e:67:4a:d7:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
Address: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
..... . . . . . = L6 bit: Globally unique address (factory default)
..... . . . . . = I6 bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.1.129, Dst: 172.17.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Flags: 0x0000, 0x0000
Flags: 0x0000, 0x0000
Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
  - NALYVAIKO-PC<0>: type NB, class IN
    Name: NALYVAIKO-PC<0> (Workstation/Redirector)
    Type: NB (32)
    Class: IN (1)
Source Hardware Address (eth.src), 6 byte(s)

```

Packets: 19928 - Displayed: 19928 (100.0%) | Profile: customized

## Resposta 14: NALYVAIKO-PC

Aug 25 14:43  
desafio3.pcap

```

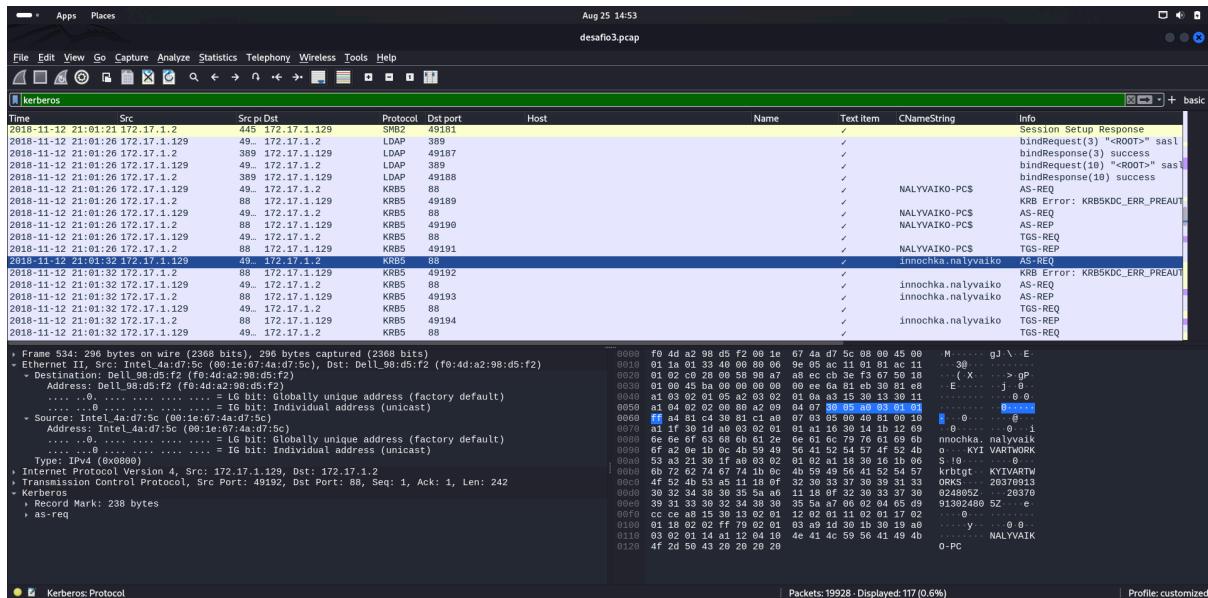
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[ ip.addr == 172.17.1.129 ] basic
Time Src Src/Dst Protocol Dstport Host NaiText Item CNameString Info
2018-11-12 21:01:15 172.17.1.129 137 172.17.1.255 NBNS 137 ✓ Registration NB NALYVAIKO-PC<0>
2018-11-12 21:01:15 172.17.1.129 60.. 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 66888 -- Standard query response 0x109 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 59478 -- Standard query response 0x109 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 DNS 53 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.129 DNS 53548 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53556 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53552 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49156 .. 49156 [SYN] Seq=0 Win=0 MSS=1468
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 TCP 49155 -- 49155 [SYN ACK] Seq=0 Ack=1 Win=8192 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49155 .. 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.129 DCERPC 135 Bind: call_id: 2, Fragment: Single, 3 context it
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 DCERPC 49155 Bind: ack: call_id: 2, Fragment: Single, max_xmit
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 EPM 135 Map request, RPC_NETLOGON, 32bit NDR

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Intel 4a:d7:5c (00:1e:67:4a:d7:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
Address: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
..... . . . . . = L6 bit: Globally unique address (factory default)
..... . . . . . = I6 bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.1.129, Dst: 172.17.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Flags: 0x0000, 0x0000
Flags: 0x0000, 0x0000
Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
  - NALYVAIKO-PC<0>: type NB, class IN
    Name: NALYVAIKO-PC<0> (Workstation/Redirector)
    Type: NB (32)
    Class: IN (1)
Source Hardware Address (eth.src), 6 byte(s)

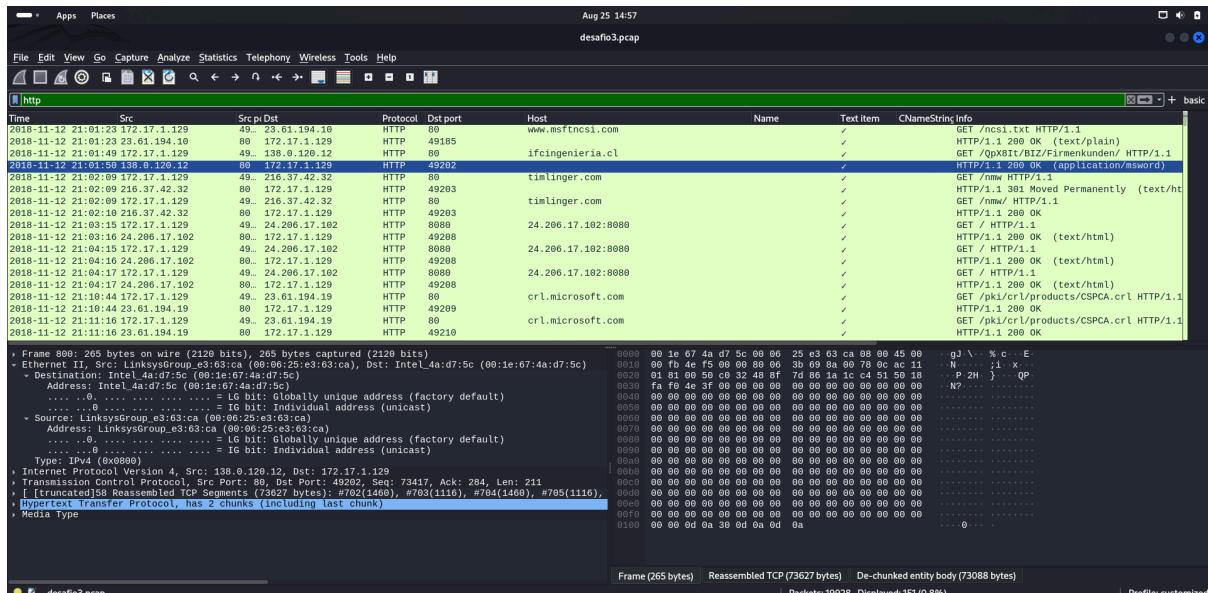
```

Packets: 19928 - Displayed: 19928 (100.0%) | Profile: customized

## Resposta 15: innochka.nalyvaiko



## Resposta 16:<http://ifcingenieria.cl/QpX8lt/BIZ/Firmenkunden>



## Pergunta 17:

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

## Pergunta 18:[timlinger.com/nmw/](http://timlinger.com/nmw/) retornou o eecutável 6169583.exe

Wireshark Screenshot showing a TCP Stream (eq 46) with 11 captured frames. The timeline shows traffic from 2018-11-12 21:02:18 to 2018-11-12 21:02:19. The details pane displays the TCP header fields for each frame, including Source Port, Destination Port, Sequence Number, and Acknowledgment Number. The bytes pane shows the raw binary data of the frames. The status pane at the bottom right indicates the connection state as established.

Resposta 19: 192.168.1.2

## Resposta 20:steve.smith

The screenshot displays a Wireshark capture of a Kerberos authentication exchange. The timeline pane shows the sequence of messages:

- 2022-01-07 16:04:19 192.168.1.2 → 192.168.1.216 KRBS 49679 DESKTOP-GXWY02S AS-REP
- 2022-01-07 16:04:19 192.168.1.216 → 192.168.1.2 KRBS 49670 DESKTOP-GXWY02S AS-REQ
- 2022-01-07 16:04:19 192.168.1.216 → 192.168.1.2 KRBS 49673 DESKTOP-GXWY02S AS-REP
- 2022-01-07 16:04:20 192.168.1.2 → 192.168.1.216 KRBS 49709 DESKTOP-GXWY02S AS-REP

The packet details pane highlights the CNameString field in the AS-REP message, which contains "steve.smith". The bytes pane shows the raw hex and ASCII data for each frame.

## Pergunta 21:desktop-gxmyno2

The screenshot shows a network capture in Wireshark. The timeline pane displays a sequence of messages:

- 0x0000 20 47 A7 62 ae 26 9c 5c Be 32 58 f9 08 00 45 00 Ggb & ZX - E
- 0x0010 01 1c cb a8 09 89 06 aa 0a c9 b0 d8 c0 00 00 @
- 0x0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .xy S Zr P
- 0x0030 68 14 77 1f 00 00 00 00 00 5d 00 00 00 01 ed 30 00 00 j 0
- 0x0040 a1 03 02 01 05 a2 02 02 01 01 a3 15 36 13 30 11 0 0
- 0x0050 a1 04 02 02 00 89 09 00 04 07 39 05 00 a3 01 01 0 0
- 0x0060 a1 04 02 02 00 89 09 00 04 07 39 05 00 a3 01 01 0 0
- 0x0070 a1 04 02 02 00 89 09 00 04 07 39 05 00 a3 01 01 0 0
- 0x0080 65 73 0b 74 6f 70 2d 67 78 6d 79 0e 06 32 24 04 esktop-g zmxny02s
- 0x0090 10 1b 73 70 67 6f 67 67 71 64 03 68 2e 66 65 spoon watch.ne
- 0x00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
- 0x00b0 68 72 62 74 67 74 10 00 13 70 06 0f 6e 77 61 74 krbtgt - spoonwat
- 0x00c0 63 66 0e 65 74 55 11 08 03 32 33 37 30 00 286709
- 0x00d0 31 33 30 32 34 38 39 55 a6 11 18 0f 32 30 33 13824985 Z ... 203
- 0x00e0 35 36 37 77 81 00 00 19 13 02 11 12 02 01 11 02 01 70913024 8052 .
- 0x00f0 17 02 01 18 02 02 ff 79 02 01 03 a9 1d 30 1b 00 00 00 00 0Kw .
- 0x0100 19 a9 03 02 01 14 a1 12 04 10 44 45 53 4b 54 4f .. v 0 0
- 0x0110 56 2d 47 58 4d 59 4e 4f 32 20 . DESKTO
- 0x0120 P-GXMYNO 2

The details pane shows the structure of the messages, including the 'Ticket' field which contains the session key and other authentication information.

## Pergunta 22:

Aug 25 16:41

desafio4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.content\_type>0

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Text item	CNameString	Info
2022-01-07 16:07:34 2.56.57.108	89	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK (image/jpeg)
2022-01-07 16:07:35 2.56.57.108	89	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK
2022-01-07 16:07:36 2.56.57.108	89	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:07:39 2.56.57.108	89	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:18 23.38.189.225	89	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:22 23.38.189.225	89	192.168.1.216		HTTP	49749					HTTP/1.1 206 Partial Content
2022-01-07 16:14:22 23.38.189.225	89	192.168.1.216		HTTP	49759					HTTP/1.1 206 Partial Content
2022-01-07 16:14:22 23.38.189.225	89	192.168.1.216		HTTP	49749					HTTP/1.1 206 Partial Content
2022-01-07 16:07:32 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/6.jpg HTTP/1.1
2022-01-07 16:07:32 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/1.jpg HTTP/1.1
2022-01-07 16:07:32 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/2.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/3.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/4.jpg HTTP/1.1
2022-01-07 16:07:34 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/5.jpg HTTP/1.1
2022-01-07 16:07:34 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/7.jpg HTTP/1.1
2022-01-07 16:07:35 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/main.php HTTP/1.1
2022-01-07 16:07:36 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/1.zip HTTP/1.1

Frame 1639: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits) Encapsulation type: Ethernet (1) Src/Mac: Cisco Switch/Firewall (08:00:27:00:00:00) Dst/Mac: 2.56.57.108 (08:00:27:00:00:08) **Frame is marked: False** [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000000000 seconds] [Time delta from previous displayed frame: 0.033d460000 seconds] [Time since reference or first frame: 16.033d460000 seconds] Frame Number: 1639 Frame Length: 708 bytes (5664 bits) Capture Length: 708 bytes (5664 bits) **Frame is ignored: False** [Protocols in frame: eth:ether:ip:tcp:http:media] [Coloring Rule Name: HTTP ||| tcp.port == 80 ||| http] -> Ethernet II, Src: Cisco\_f6:df:0a (1c:17:d3:06:f6:0a), Dst: ASUSTekCOMPU\_32:58:f9 (9c:5c:8e:32:58:f9) -> Destination: ASUSTekCOMPU\_32:58:f9 (9c:5c:8e:32:58:f9) Address: ASUSTekCOMPU\_32:58:f9 (9c:5c:8e:32:58:f9) . . . . . L bit: Globally Unique address (factory default) A = In host T=Individual address (implied) Frame 708 bytes) Reassembled TCP (145194 bytes) Packets: 5880 - Displayed: 24 (0.4%) Profile: customized

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 arquivo executável windows.

Aug 25 16:43

Wireshark - Follow HTTP Stream (tcp.stream eq 65) - desafio4.pcap

File Edit View Go Capture Analyze : POST /osk/6.jpg HTTP/1.1

Accept: text/html, application/xhtml+xml, application/xml;q=0.9, application/rss+xml;q=0.9

Accept-Charset: iso-8859-1, utf-8, utf-16, \*;q=0.9

Accept-Encoding: deflate, gzip, x-gzip, identity, \*;q=0

Content-Type: multipart/form-data; boundary=18EF0A57BE110FD467A

Host: 2.56.57.108

Cache-Control: no-cache

Connection: Keep-Alive

Content-Length: 0

Content-Type: image/jpeg

Last-Modified: Thu, 06 Jun 2019 04:01:52 GMT

ETag: "18EF0A57BE110FD467A"-

HTTP/1.1 200 OK

Date: Fri, 07 Jan 2022 16:07:32 GMT

Content-Type: application/x-tar

Content-Length: 144049

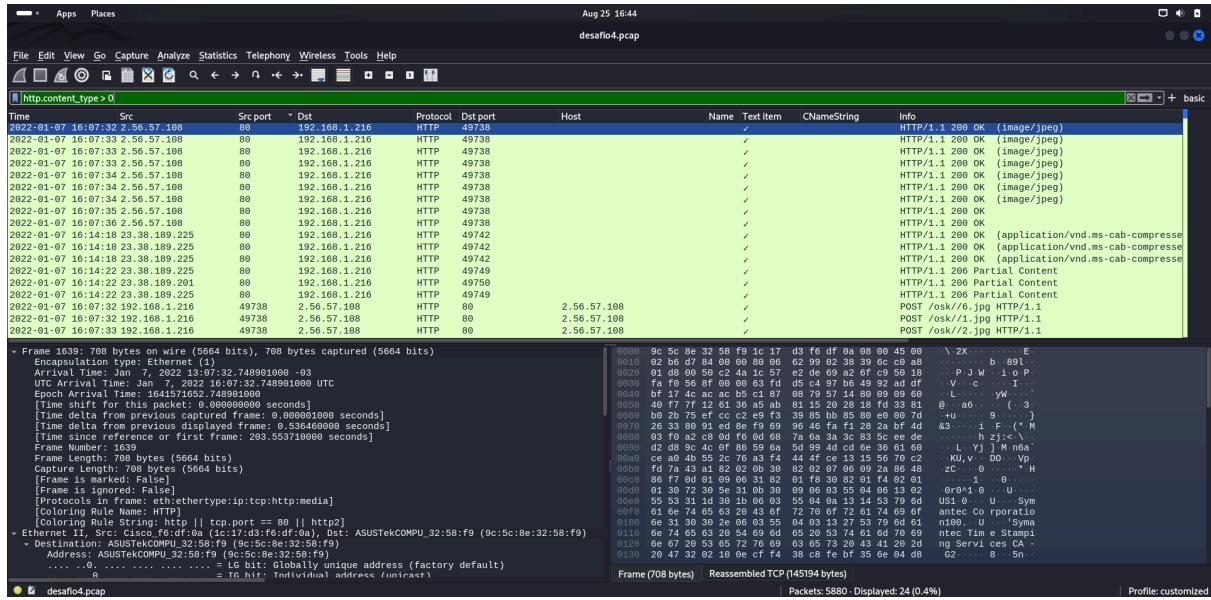
Content-Security-Policy: default-src 'self'; script-src 'self' 'strict-dynamic' 'nonce-1'; style-src 'self' 'strict-dynamic' 'unsafe-inline' 'unsafe-style-src'; font-src 'self' 'strict-dynamic'; img-src 'self' 'strict-dynamic'; object-src 'self' 'strict-dynamic'; frame-src 'self' 'strict-dynamic'; media-src 'self' 'strict-dynamic'; child-src 'self' 'strict-dynamic'; manifest-src 'self' 'strict-dynamic'; script-src-elem 'self' 'strict-dynamic'; style-src-elem 'self' 'strict-dynamic'; font-src-elem 'self' 'strict-dynamic'; img-src-elem 'self' 'strict-dynamic'; object-src-elem 'self' 'strict-dynamic'; frame-src-elem 'self' 'strict-dynamic'; media-src-elem 'self' 'strict-dynamic'; child-src-elem 'self' 'strict-dynamic'; manifest-src-elem 'self' 'strict-dynamic';

NZ.....@.....!..!..!This program cannot be run in DOS mode.

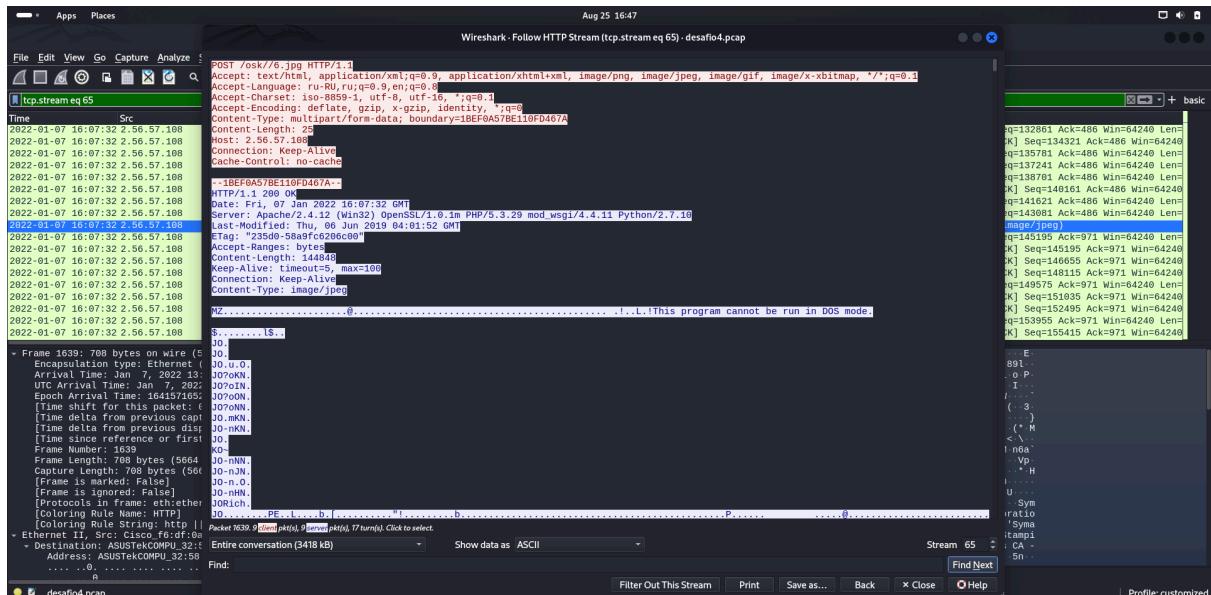
\$.....\$..

Frame 1639: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits) Encapsulation type: Ethernet (1) Arrival Time: Jan 7, 2022 16:07:32.567000000 UTC Arrival Time: Jan 7, 2022 16:07:32.567000000 Epoch Arrival Time: 1644571652.748091000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000000000 seconds] [Time delta from previous displayed frame: 0.033d460000 seconds] [Time since reference or first frame: 16.033d460000 seconds] Frame Number: 1639 Frame Length: 708 bytes (5664 bits) Capture Length: 708 bytes (5664 bits) **Frame is marked: False** [Protocols in frame: eth:ether:ip:tcp] [Coloring Rule Name: HTTP ||| tcp.port == 80 ||| http] -> Ethernet II, Src: Cisco\_f6:df:0a (1c:17:d3:06:f6:0a), Dst: ASUSTekCOMPU\_32:58:f9 (9c:5c:8e:32:58:f9) -> Destination: ASUSTekCOMPU\_32:58:f9 (9c:5c:8e:32:58:f9) Address: ASUSTekCOMPU\_32:58:f9 (9c:5c:8e:32:58:f9) . . . . . L bit: Globally Unique address (factory default) A = In host T=Individual address (implied) Stream 65 Find Next Filter Out This Stream Print Save as... Back × Close Help Profile: customized

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 conteúdo e ver com o comando file o tipo de arquivo, se é uma jpeg ou um executável ou dll:

Aug 25 18:01  
fernando@fernando: ~/Downloads

```
[fernando@fernando:~/Downloads]
└─$ file 6.jpg
6.jpg: PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections
[fernando@fernando:~/Downloads]
```

Arquivo Editar Ver inserir Formatar Ferramentas Extensões Ajuda

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 conteúdo e ver com o comando file o tipo de arquivo, se é um jpg ou um executável ou dll.

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 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:

Aug 25 16:50  
desafio4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.content\_type > 0

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Text item	CNameString	Info
2022-01-07 16:07:34 2.56.57.108	80	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK (image/jpeg)
2022-01-07 16:07:35 2.56.57.108	80	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK
2022-01-07 16:07:36 2.56.57.108	80	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:18 23.38.189.225	80	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:19 23.38.189.225	80	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:20 23.38.189.225	80	192.168.1.216		HTTP	49742					HTTP/1.1 200 Partial Content
2022-01-07 16:14:22 23.38.189.225	80	192.168.1.216		HTTP	49749					HTTP/1.1 206 Partial Content
2022-01-07 16:14:23 23.38.189.225	80	192.168.1.216		HTTP	49750					HTTP/1.1 206 Partial Content
2022-01-07 16:14:22 23.38.189.225	80	192.168.1.216		HTTP	49749					HTTP/1.1 206 Partial Content
2022-01-07 16:07:32 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/6.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/2/3.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/3.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/4.jpg HTTP/1.1
2022-01-07 16:07:34 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/5.jpg HTTP/1.1
2022-01-07 16:07:34 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/7.jpg HTTP/1.1
2022-01-07 16:07:35 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/main.php HTTP/1.1
2022-01-07 16:07:36 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/HTTP/1.1 (zip)

- Frame 1501: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)  
Encapsulation type: Ethernet (1)  
Arrival Time: Jan 7, 2022 13:07:32.212441000 -03  
Epoch Arrival Time: 1641571652.212441000 UTC  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.000431000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 263.017250000 seconds]  
Frame Number: 1501  
Frame Length: 539 bytes (4312 bits)  
Encapsulation type: Ethernet (4312 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ether:type:ip:tcp:http:mime multipart]  
[String representation: (Colorized Rule String: http || tcp port == 80 || http2]  
- Ethernet II, Src: ASUSTekCOMPU\_32:58:f9 (0c:5c:8e:32:58:f9), Dst: Cisco\_f0:df:0a (1c:17:d3:f6:df:0a)  
- Destination: Cisco\_f0:df:0a (1c:17:d3:f6:df:0a)  
Address: Cisco\_f0:df:0a (1c:17:d3:f6:df:0a)  
.....0.....16 bits probably unique address (factory default)  
.....0.....a = Tc hit: Individual address (unicast)  
.....0.....a = Tc hit: Individual address (unicast)

0000 1c 17 d3 f6 df 0a 9c 5c 8e 32 58 f9 08 00 45 96 ..... \ 2X .. E  
0010 02 0d cd 68 40 08 80 28 5c c0 a8 01 d8 02 38 ..... h... .A... 8  
0020 39 6c c2 4a 08 59 69 42 6d e4 1c 55 ae 42 50 18 91 J R m m B8  
0030 2f 30 2e 6a 70 57 49 48 54 54 59 2f 31 2e 31 0d 00 POST /osk/  
0040 2f 30 2e 6a 70 57 49 48 54 54 59 2f 31 2e 31 0d 00 /6.jpg H TIP/1.1  
0050 0a 41 63 65 76 74 3a 20 74 65 78 74 2f 6e 74 Accept: text/html  
0060 6d 6c 2c 29 61 78 78 8c 69 63 61 74 69 67 6e 6c m, application/x-  
0070 63 61 74 69 67 6e 2f 78 68 74 6d 6c 2b 78 6d 6c  
0080 2c 29 69 6d 61 67 65 2f 70 66 67 2c 2b 69 6d 61 , image/png, ima  
0090 67 65 2f 6a 68 67 62 29 69 6d 61 67 65 2f 67 ge/jpeg, image/g  
0100 6d 61 70 2c 2b 2a 2f 38 71 3d 30 2e 31 0d 0a map, image/gif  
0090 6d 61 70 2c 2b 2a 2f 38 71 3d 30 2e 31 0d 0a map, / / q=0.1  
0090 41 63 63 65 70 74 2d 4c 61 6b 67 75 61 67 63 3a Accept-L anguage:  
0090 20 72 75 2d 52 55 2c 72 75 3d 71 3d 30 2e 39 2c ru-Ru, r, u;q=0.9,  
0090 05 6c 30 2e 31 0d 0a 05 6c 30 2e 31 0d 0a 05 6c 30 2e 31 0d 0a  
0090 63 61 74 69 67 6e 2f 78 68 74 6d 6c 2b 78 6d 6c  
0090 2c 29 69 6d 61 67 65 2f 70 66 67 2c 2b 69 6d 61 , image/png, ima  
0110 35 39 2d 31 2c 2b 73 74 3d 30 2e 31 0d 0a 05 6c 30 2e 31 0d 0a  
0120 2d 31 36 2c 2b 2a 30 71 3d 30 2e 31 0d 0a 04 63 Chars : 1088  
0130 63 65 2f 6a 68 67 62 29 69 6d 61 67 65 2f 67 6e 64 69 66 67 3d 29 64  
0140 63 65 2f 6a 68 67 62 29 69 6d 61 67 65 2f 67 6e 64 69 66 67 3d 29 64  
0150 67 79 69 78 2c 2b 69 64 65 66 74 69 74 79 2c 28 gzip, id entity,

Packets: 5880 - Displayed: 24 (0.4%)

Profile: customized

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