

Roadmap 01 - Analysis on network traffic (Wireshark)

Author: Enricco Gemha

Date: 02/28/2024

Question 01

Both Cisco and Trend Micro offer solutions on IDS, as Trend Micro having the most market share.

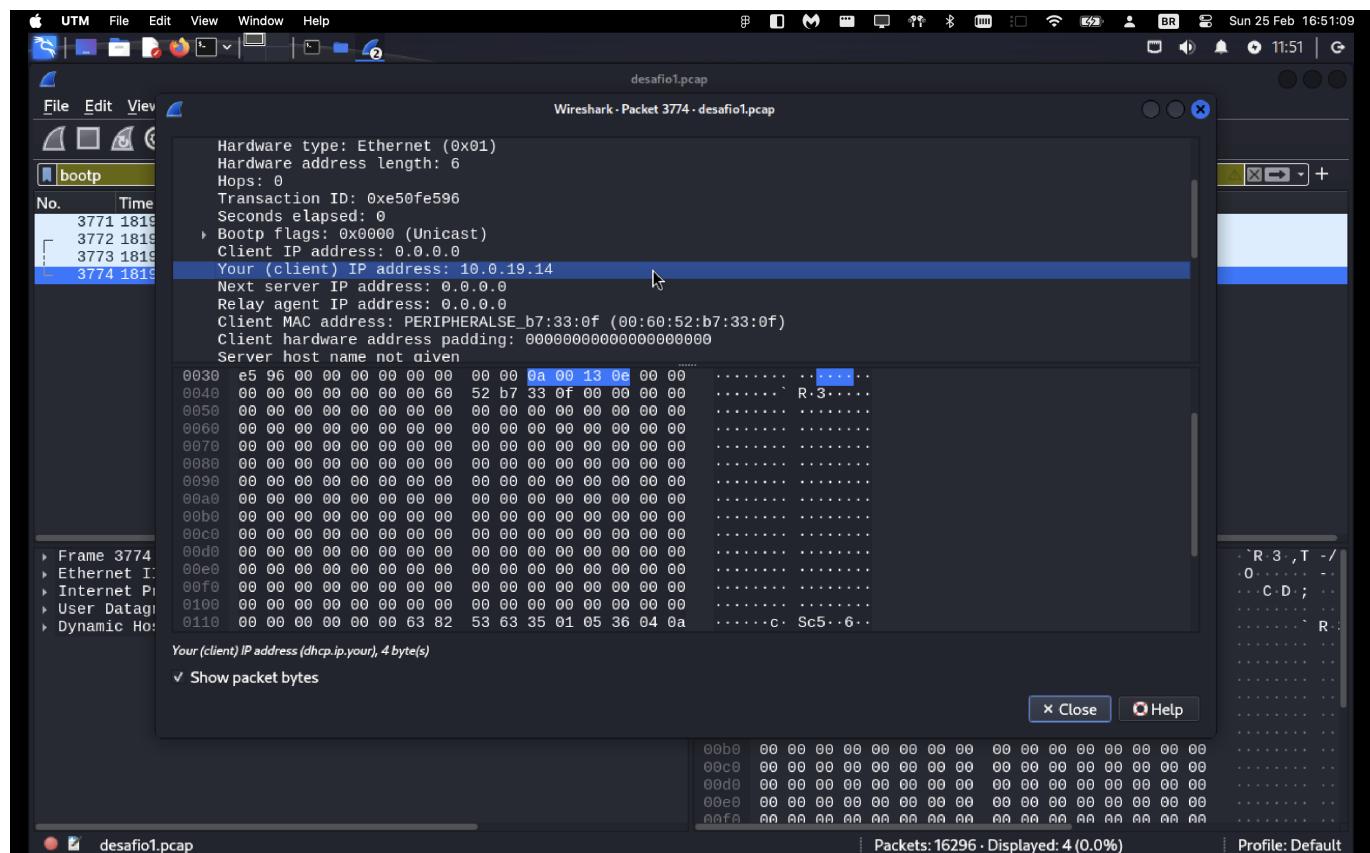
- TrendMicro
- Cisco

Question 02

While the IDS provides only alerts on possible threats and intrusions, therefore, requiring manual intervention, the IPS also blocks connections that may present suspicious behavior, based on **digital vaccine signatures**. Also, it is possible to configure the IPS with custom parameters to quarantine and block connections.

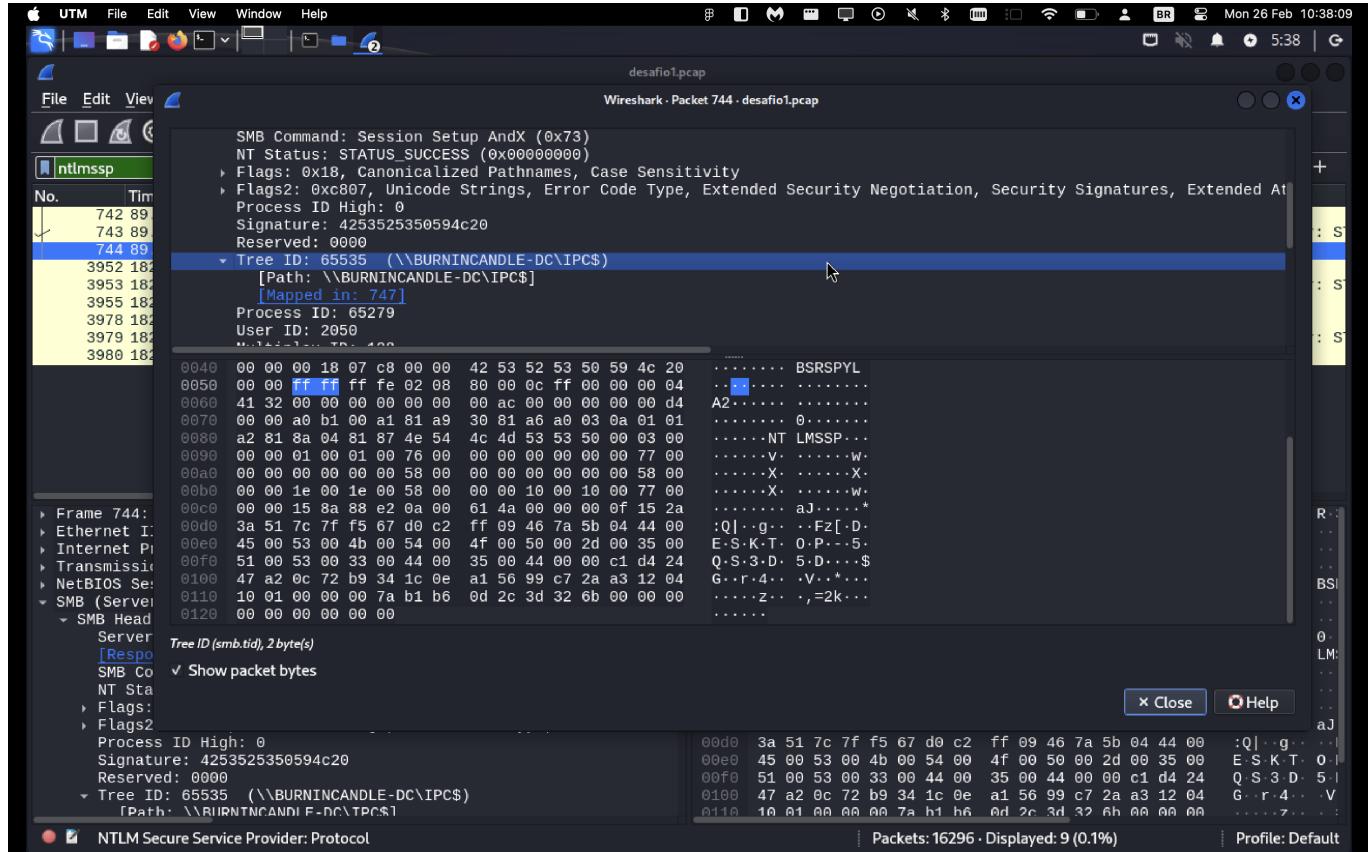
Question 03

The DHCP's IP on this network is **10.0.19.1**, while our PC IP is 10.0.19.14.



Question 04

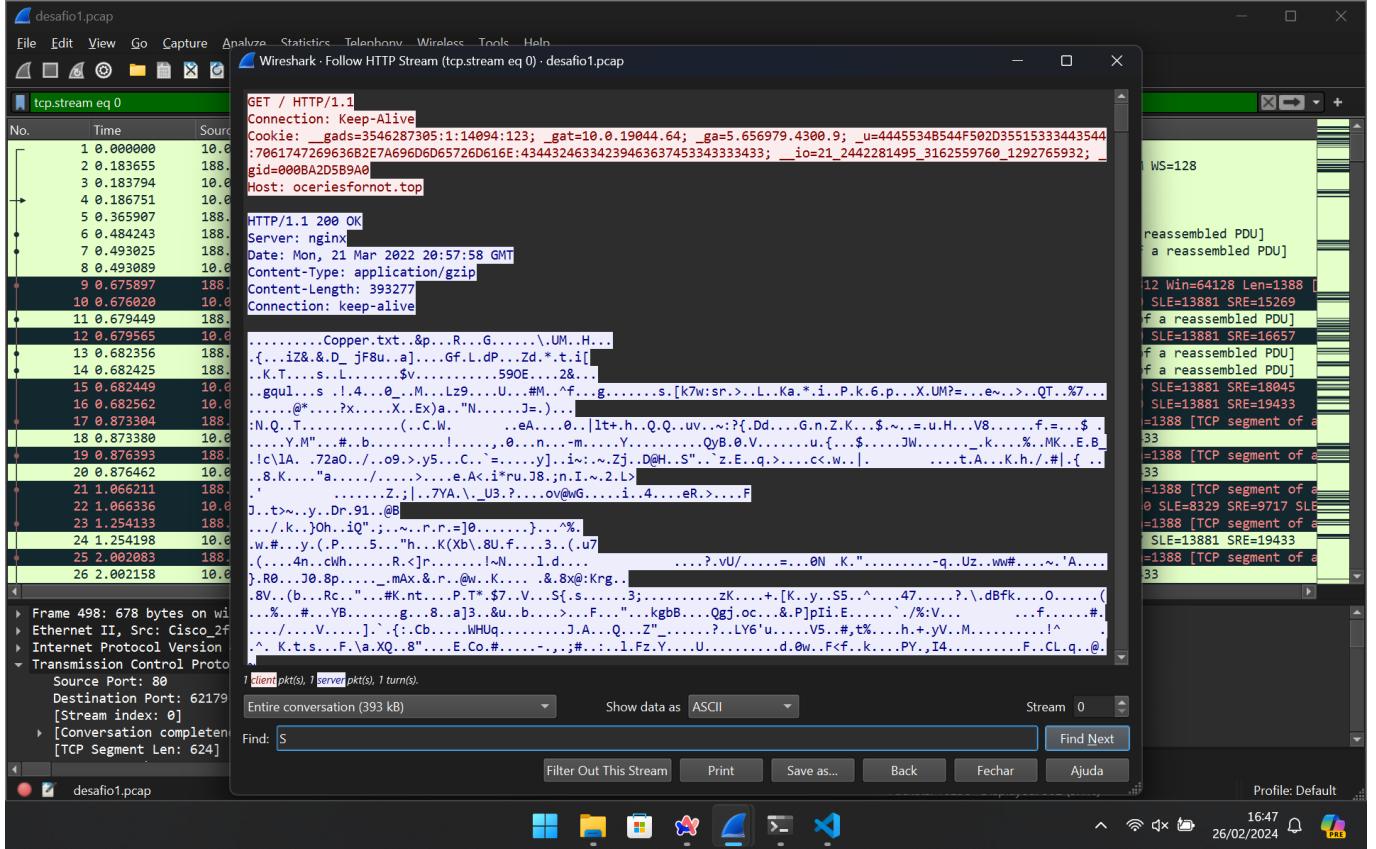
The domain controller (DC) name on this network is **BURNINCANDLE-DC**.



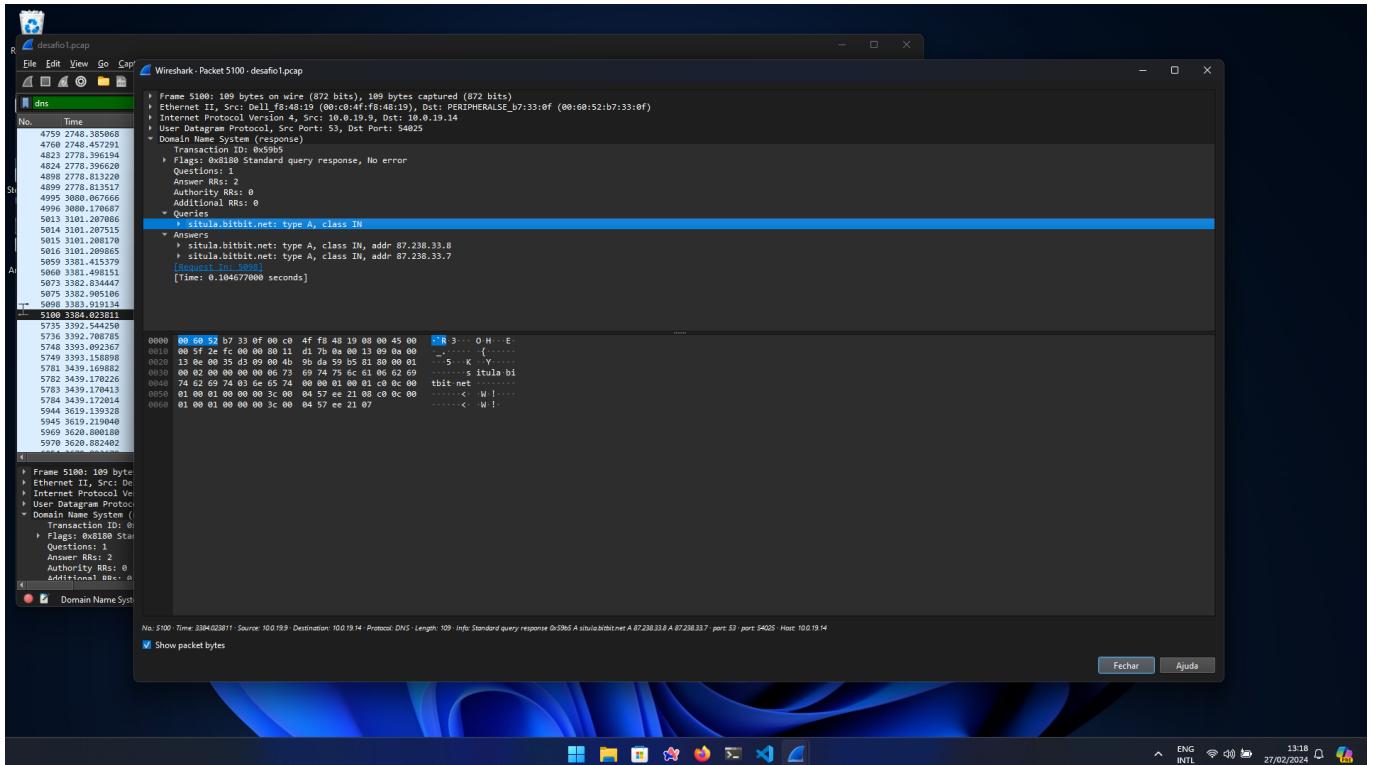
Question 05

I found two connections that can be classified as potential malicious:

- Connection 1: HTTP GET request to suspicious hostname, **oceriesfornot.top**, which was described in Internet searches as a hostname that hosts malware. Besides that, if we follow the HTTP stream we can observe a request resulting in the download of a text file **Cooper.txt**, which appears to be facade. More than that, it can be related to decripting the zip file that was also downloaded in the same connection.

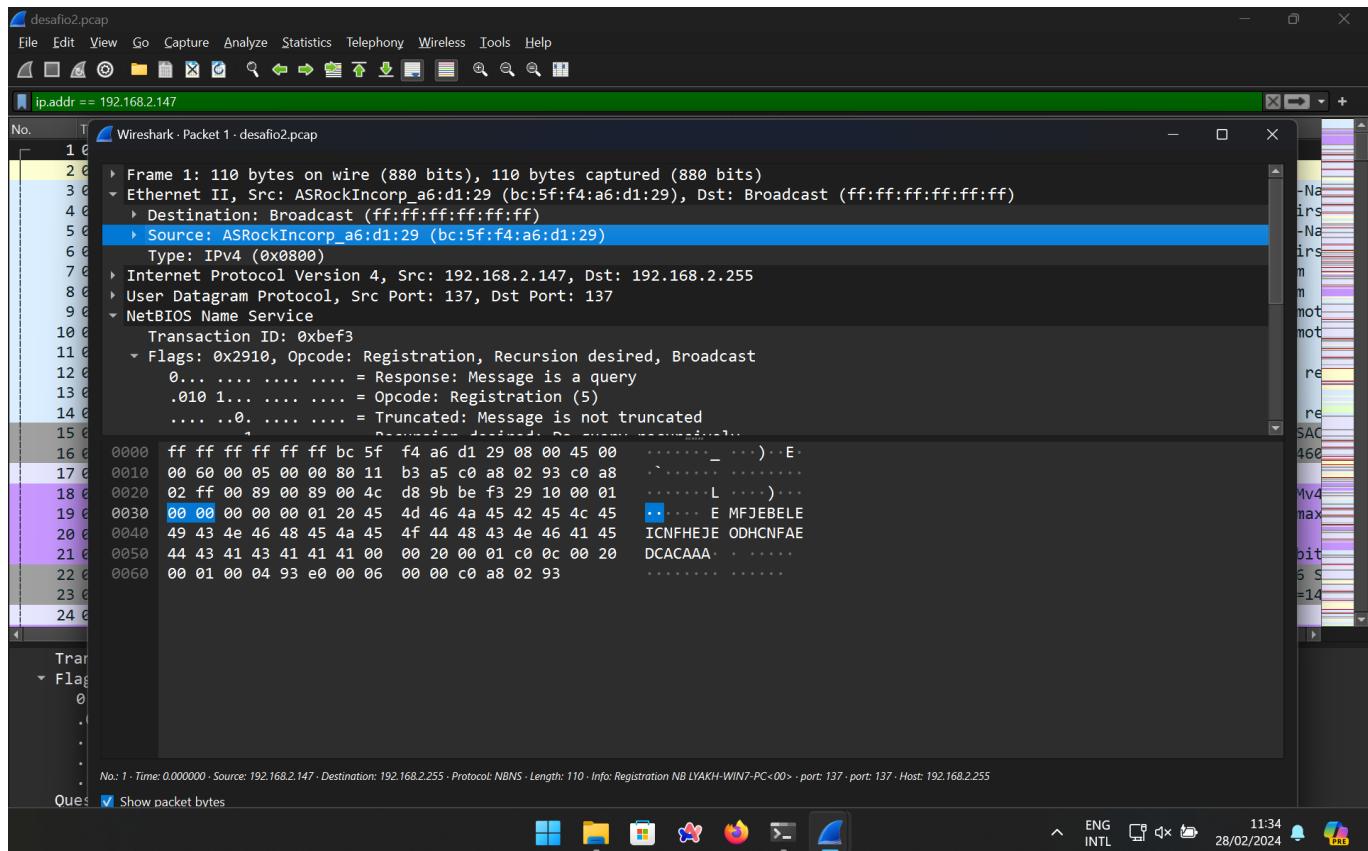


- Connection 2: HTTPS traffic to file sharing website, which might indicate that an infection occurred after the download of such compromised file, in the domain **situla.bitbit.net**.



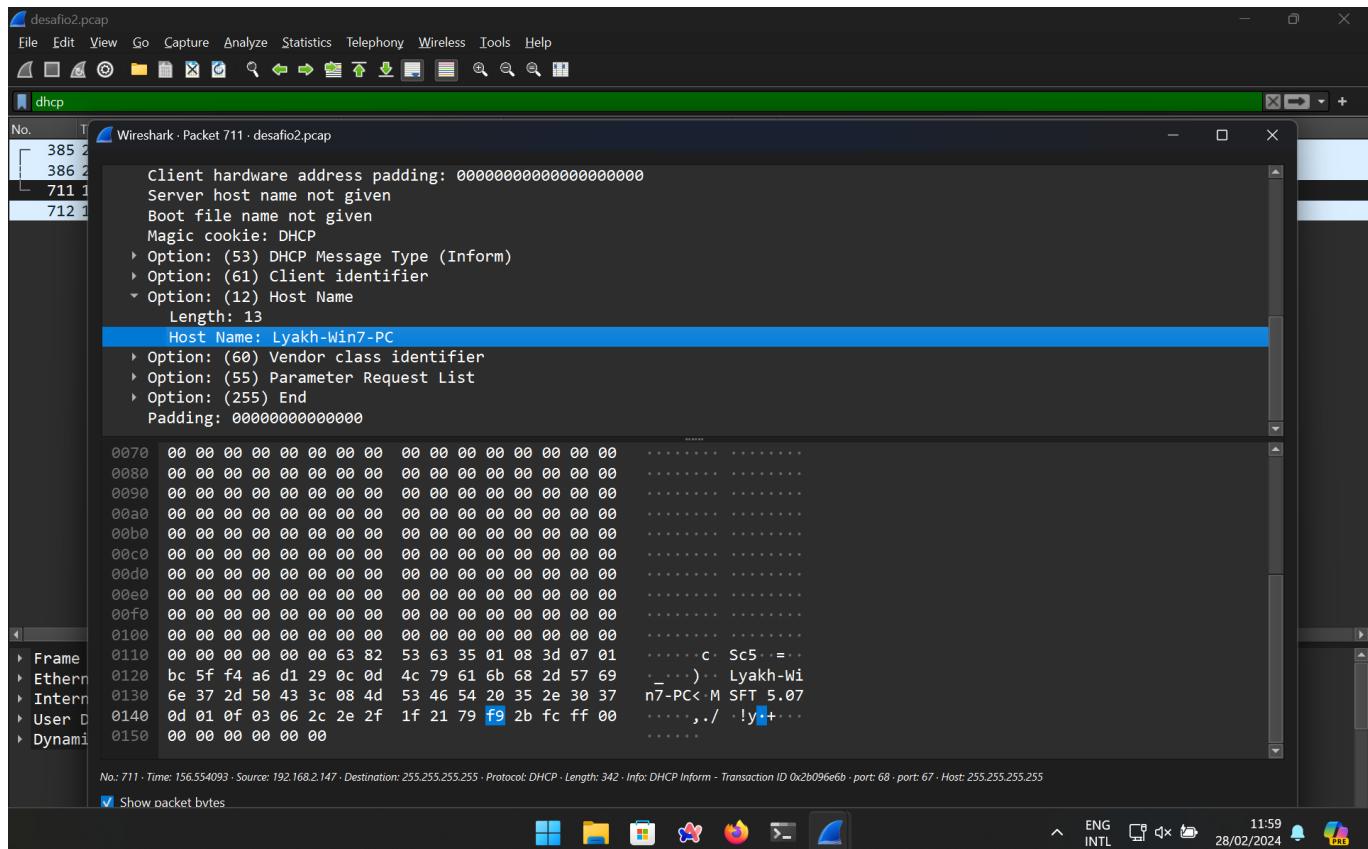
Question 06

The MAC address is **bc:5f:f4:a6:d1:29** for the host 192.168.2.4, achieved through inspecting a packet from host, in section ethernet II.



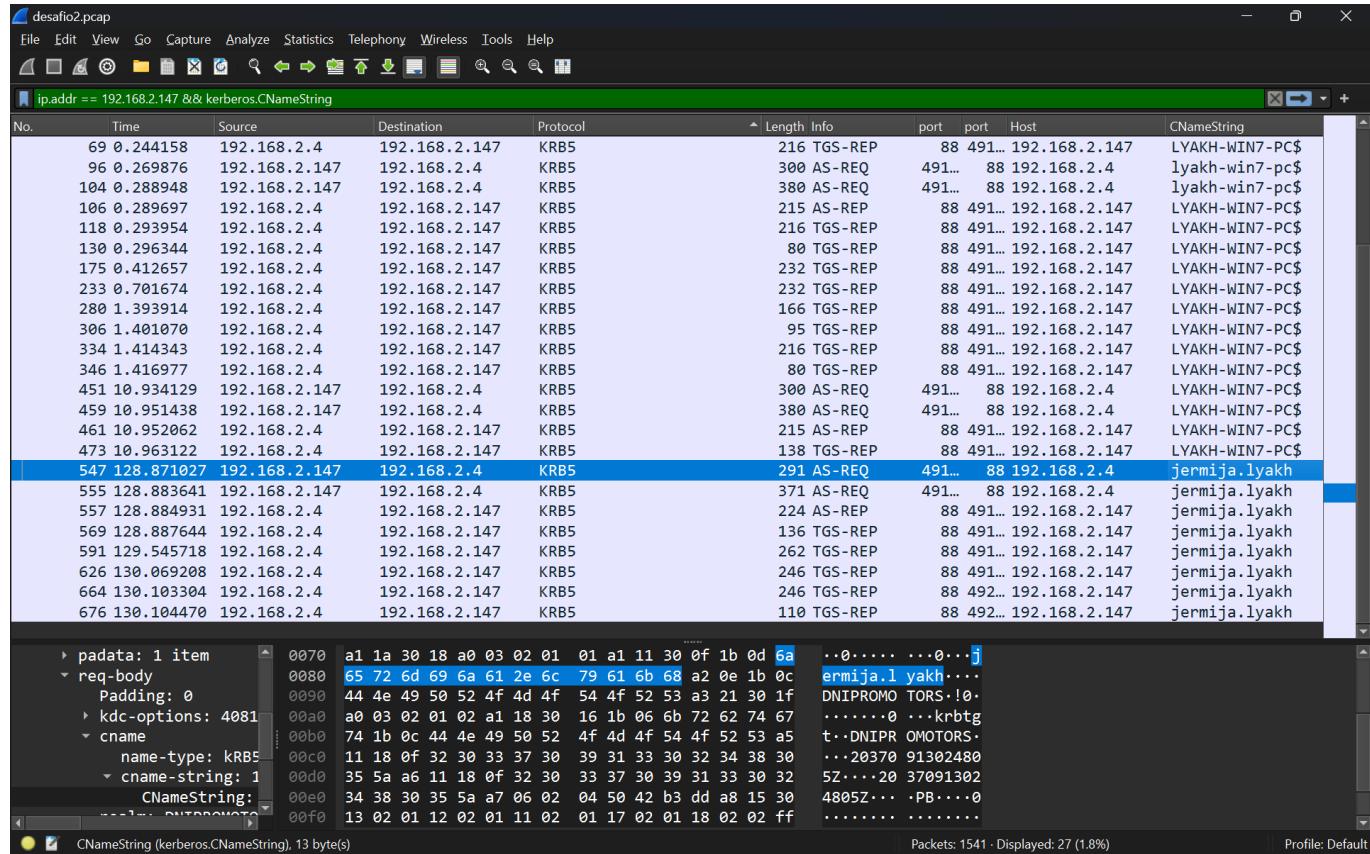
Question 07

The hostname for the Windows client in 192.168.2.147 is **Lyakh-Win7-PC**. I achieved this through inspecting the DHCP logs, which show the hostname information.



Question 08

The Windows username used in 192.168.2.147, based on the inspection of the packets with Kerberos protocol, is **jermija**.

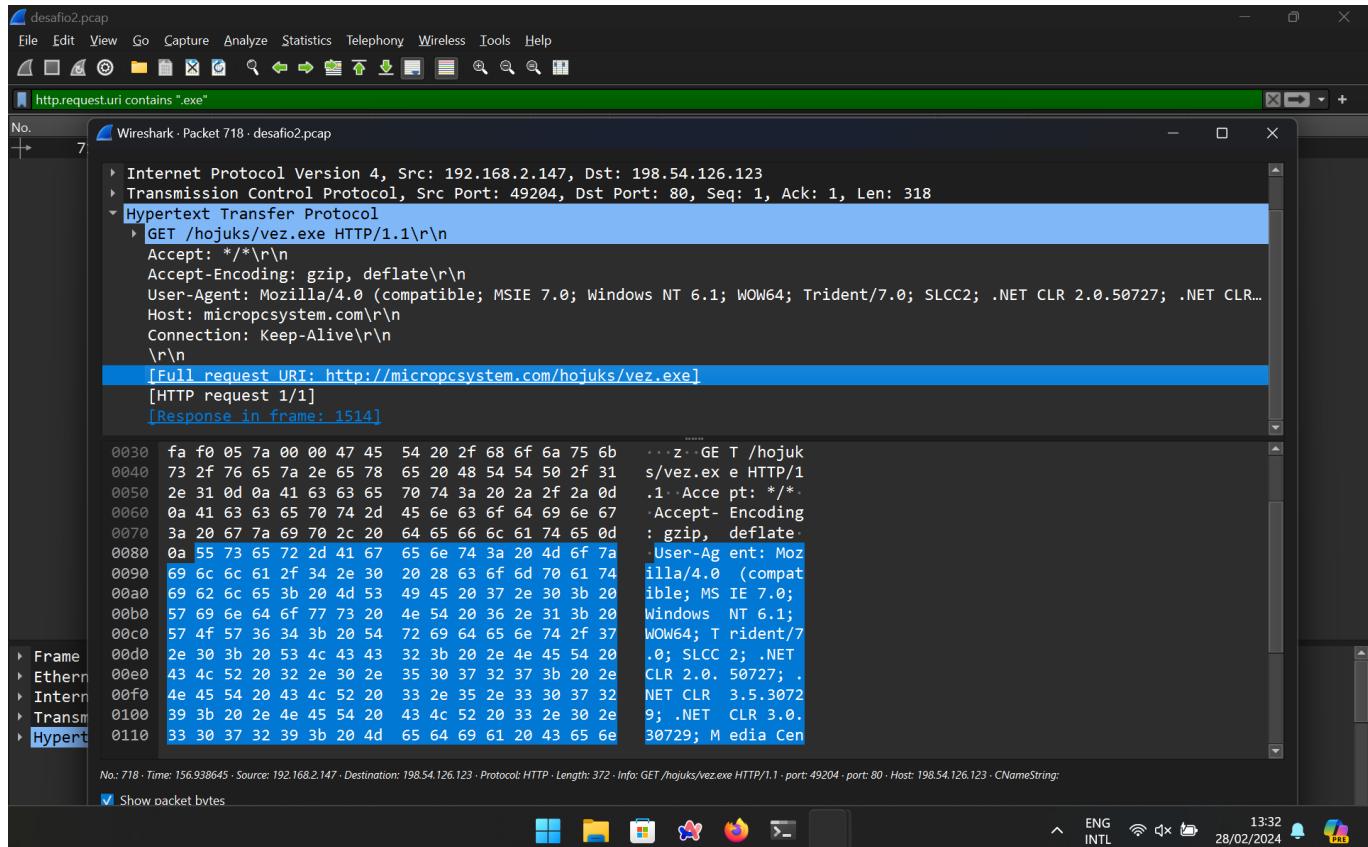


Question 09

Kerberos protocol function is authenticating service requests between two or more trusted hosts across an untrusted network, like the internet. Kerberos employs secret-key cryptography and a trusted third party, the Key Distribution Center (KDC), to authenticate client-server applications and verify user identities. The KDC provides authentication and ticket-granting services, issuing "tickets" for secure identity verification. This process uses shared secret cryptography, protecting against eavesdropping and replay attacks. [Based on SimpliLearn](#).

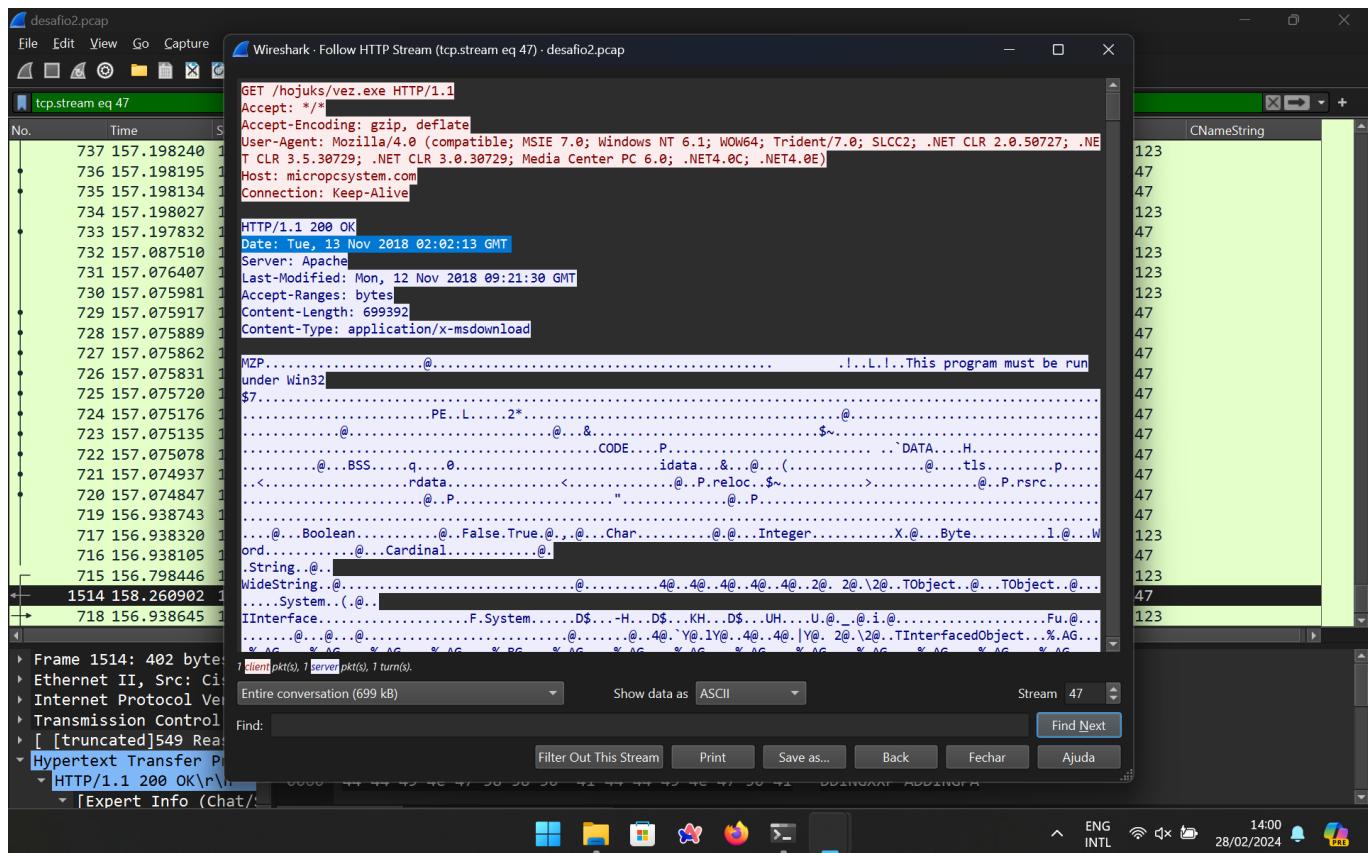
Question 10

The URL that returned an executable file is <http://micropcsystem.com/hojuks/vez.exe>.



Question 11

The URL was accessed in **11/13/2018 02:02:13 GMT**, as shown in this picture with the HTTP stream.



Question 12

After infection, the host tried to establish a TCP connection with IP **198.54.126.123**.

The screenshot shows a list of network packets captured in Wireshark. The traffic is primarily between the client (192.168.2.147) and the target host (198.54.126.123). Key interactions include:

- Multiple SMB2 requests and responses, indicating file operations.
- DHCP requests and responses, showing the client obtaining an IP address (192.168.2.147).
- TCP connections being established to port 123 (NTP), port 80 (HTTP), and port 443 (HTTPS).
- A DNS query for 'vez.exe' resulting in a redirect to 'hojuks/vez.exe'.
- File download requests for 'vez.exe' and 'hojuks/vez.exe'.

The packet details and bytes panes provide the raw binary data for each selected frame.

Question 13

The MAC address for the Windows client at 172.17.1.129 is **00:1e:67:4a:d7:5c**.

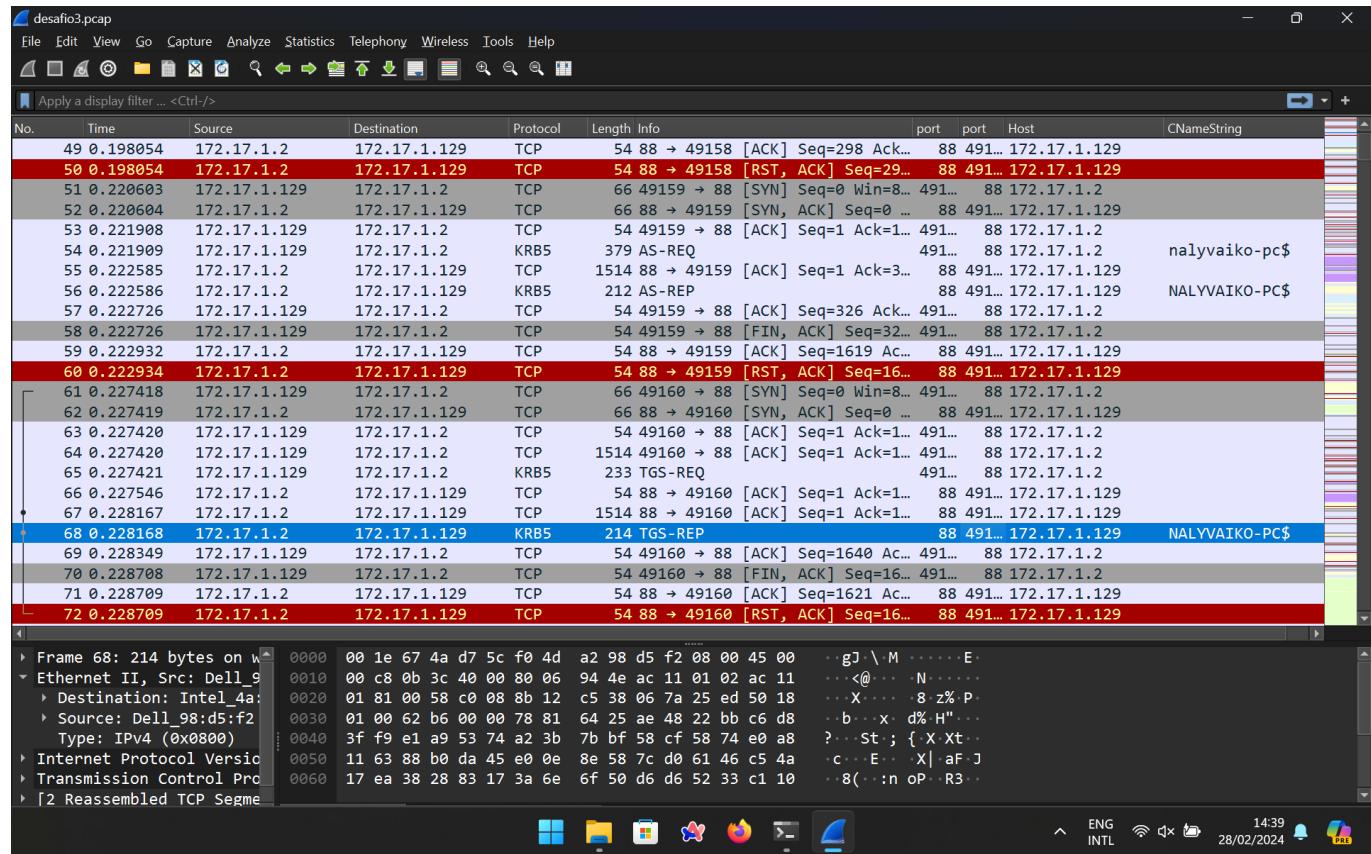
The screenshot shows a list of network packets captured in Wireshark. The traffic is primarily between the client (172.17.1.129) and the target host (172.17.1.2). Key interactions include:

- Registration NB messages to NALYVAIKO-PC and KIVIARTWORKS.
- DNS queries for SRV records.
- HTTP traffic, including a POST request to 'http://172.17.1.2:8088/'.
- Domain Name System (query).

The packet details and bytes panes provide the raw binary data for each selected frame. The selected frame (Frame 3) shows the source MAC address as **00:1e:67:4a:d7:5c**.

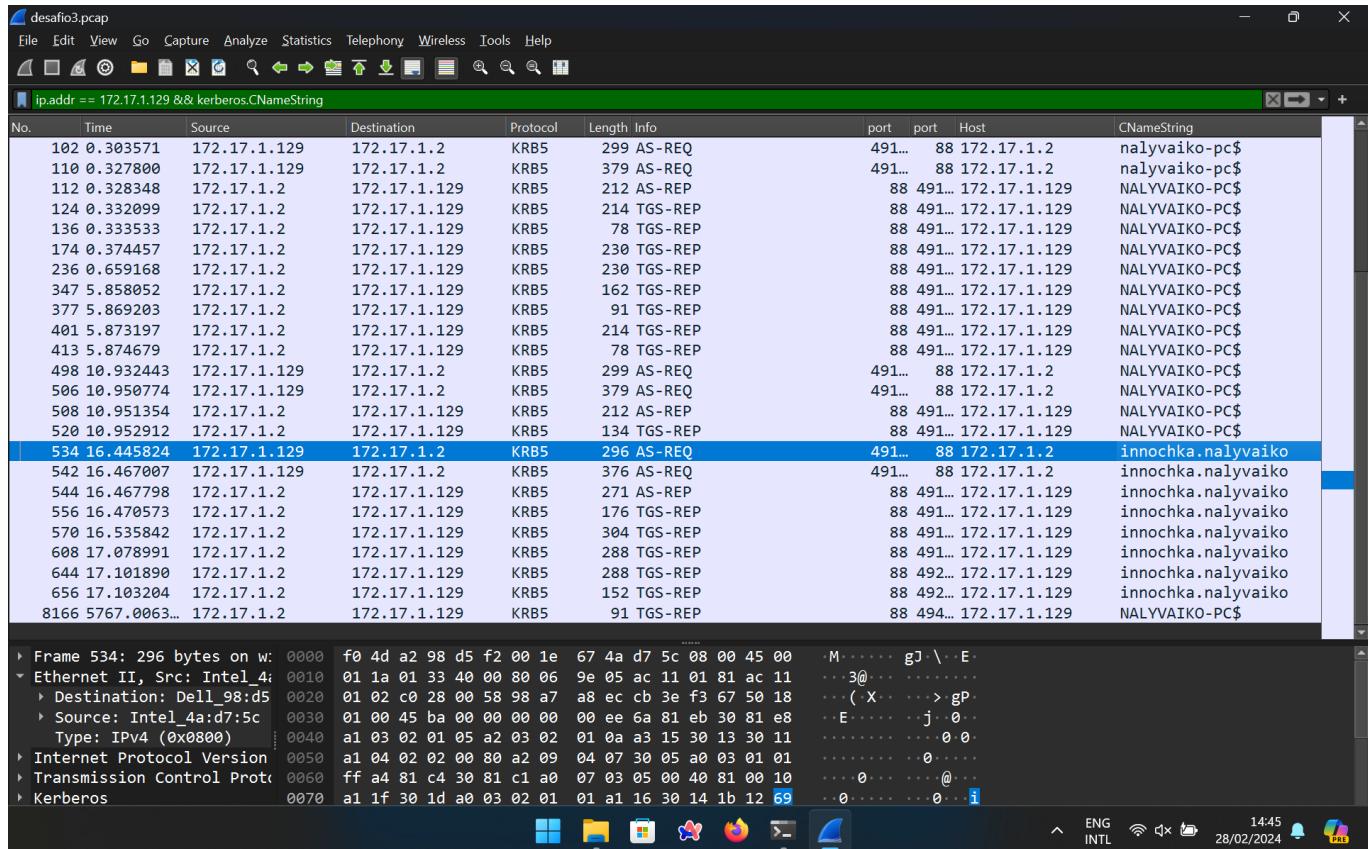
Question 14

The hostname for the Windows client at 172.17.1.129 is **NALYVAIKO-PC**, as it can be observed in the CNameString in the TCP request.



Question 15

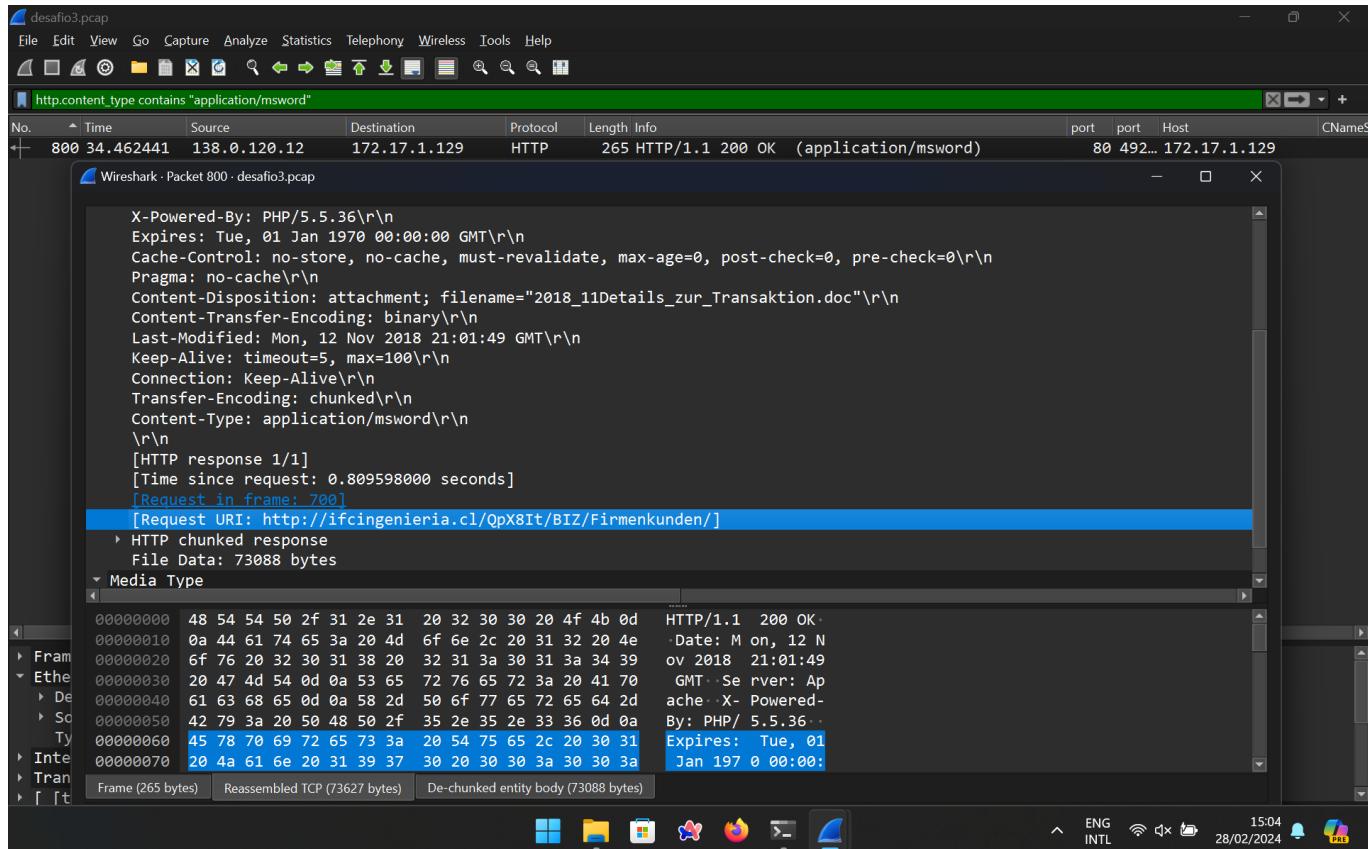
The Windows username used in 172.17.1.129, based on the inspection of the packets with Kerberos protocol, is **innochka**.



Question 16

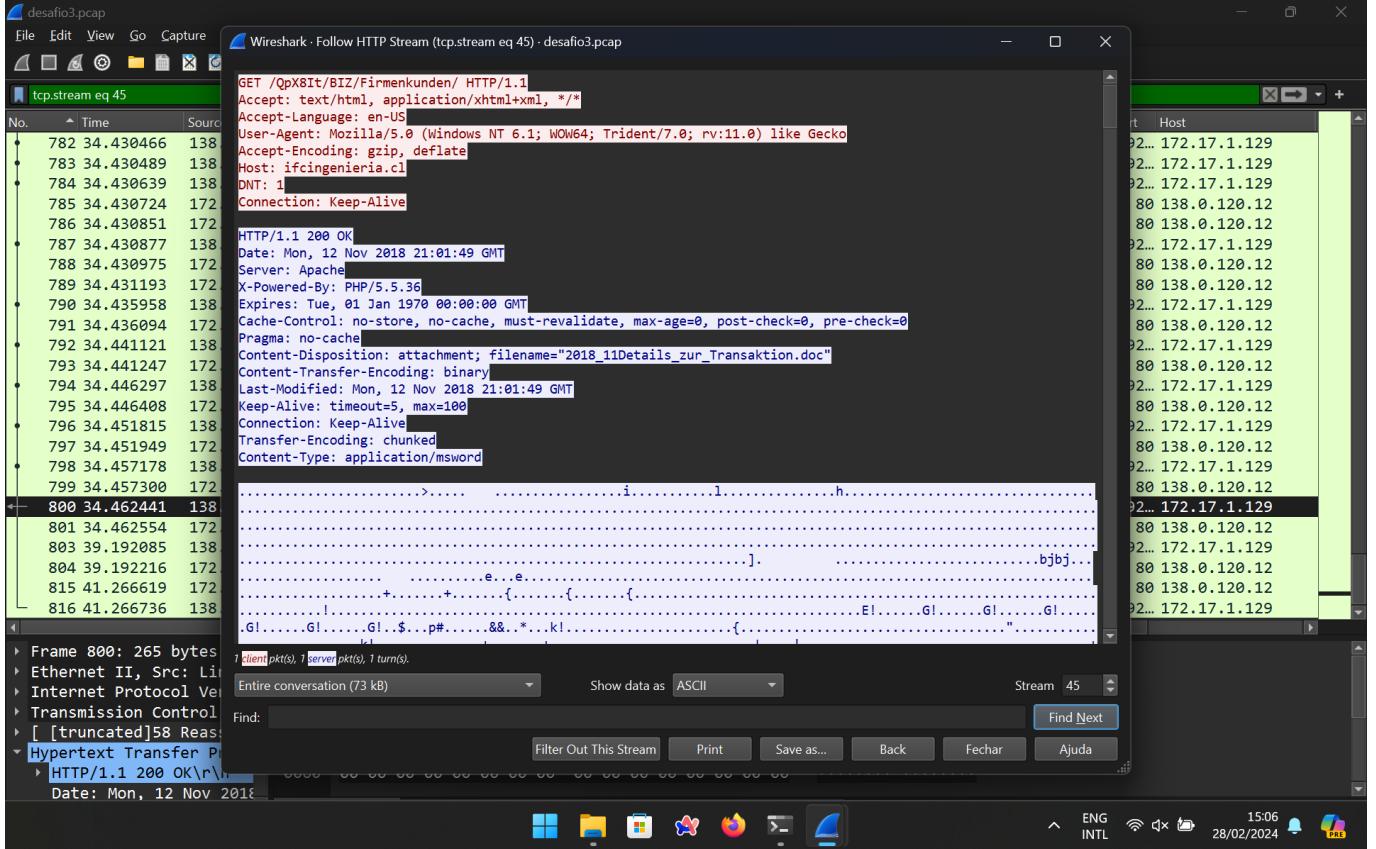
The URL that returned a Microsoft Word document was

<http://ifcingenieria.cl/QpX8It/BIZ/Firmenkunden/>.



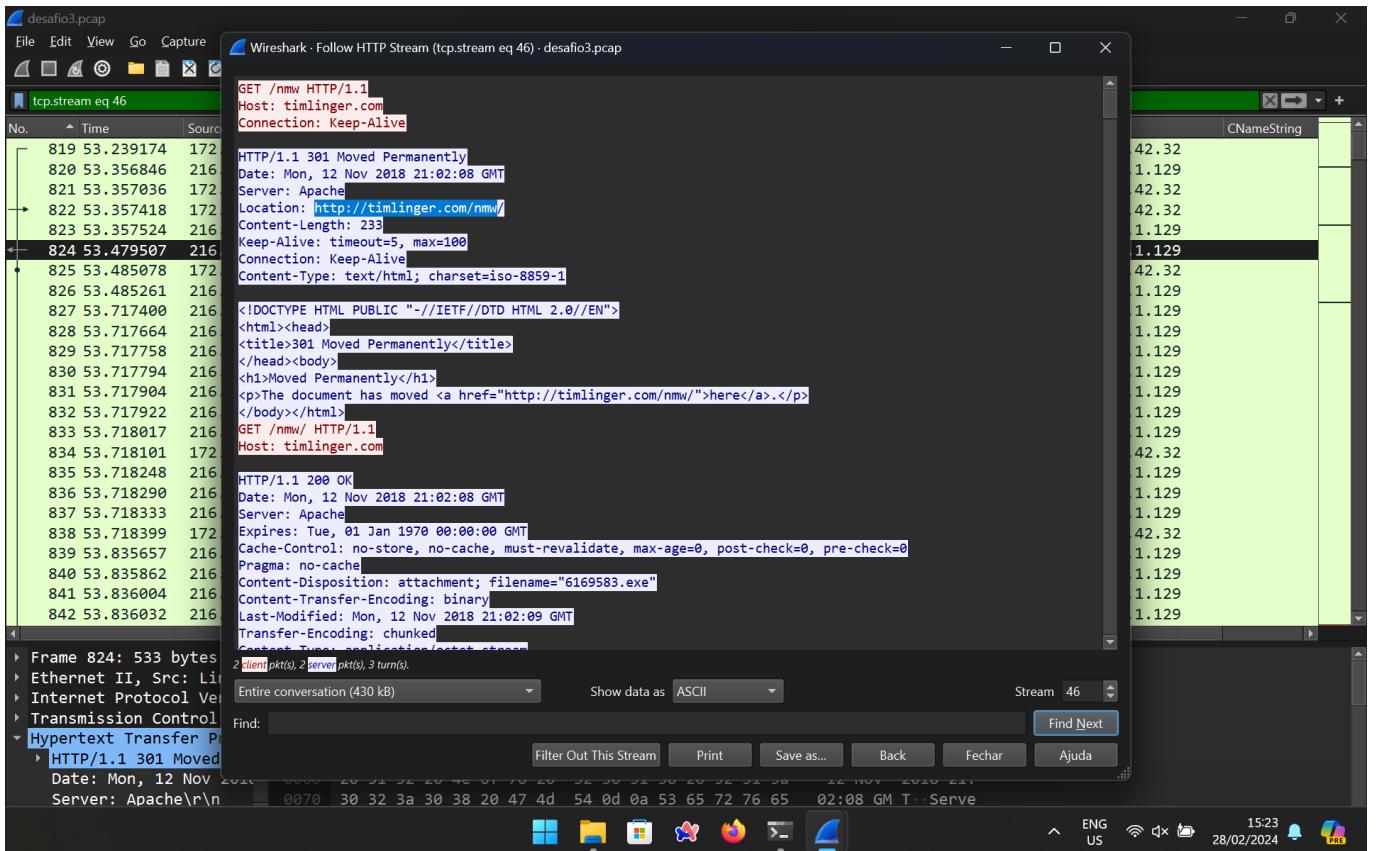
Question 17

The URL was created in **Mon, 12 Nov 2018 21:01:49 GMT**.



Question 18

The URL that returned an executable 6169583.exe file is <http://timlinger.com/nmw/>.



Question 19

Given that the domain controller name is SPOONWATCH-DC, we can assume that there is traffic in NetLogon, which leads to filtering traffic in ntlmssp. Inspecting that we can see that the IP for the domain controller is **192.168.1.2**.

The screenshot shows the Wireshark interface with the following details:

- Capture File:** desafio4.pcap
- Selected Filter:** ntlmssp
- Packets:** 912 total, 586 selected.
- Selected Packet:** 914 (42.562717), Session Setup Request, NTLMSSP_NEGOTIATE.
- Selected Hex Data:** 0060 00 00 4d 00 00 00 00 4c 00 00 00 00 00 00 00 00 ..M.....L ..
- Selected ASCII Data:** ..M.....L ..
- Selected Bytes Data:** 0060 00 00 4d 00 00 00 00 4c 00 00 00 00 00 00 00 00 ..M.....L ..
- Selected Description:** Command: Session Setup (1)
Credits requested: 33
Flags: 0x00000010, Priority
Chain Offset: 0x00000000
Message ID: 3
Process Id: 0x0000feff
Tree Id: 0x00000000
Session Id: 0x00004c000000004d Acct:steve.smith Domain:SPOONWATCH Host:DESKTOP-GXMYNO2
Signature: 00
[Response in: 915]
Session Setup Request (0x01)

Question 20

The user account for the 192.168.1.216 IP is **steve.smith**.

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Packet List:** The current capture file is "ntlmssp.pcap". The list shows three SMB2 sessions:
 - 912 42.561478 192.168.1.216 → 192.168.1.2 SMB2 220 Session Setup Request, NTLMSSP_NEGOTIATE
 - 913 42.561991 192.168.1.2 → 192.168.1.216 SMB2 435 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
 - 914 42.562717 192.168.1.216 → 192.168.1.2 SMB2 751 Session Setup Request, NTLMSSP_AUTH, User: SPOONWATCH\steve.smith
- Selected Packet:** The selected packet is the third one (914), which is a "Session Setup Request (0x01)".
 - Details:** Command: Session Setup (1), Credits requested: 33, Flags: 0x00000010, Priority, Chain Offset: 0x00000000, Message ID: 3, Process Id: 0x0000feff, Tree Id: 0x00000000.
 - Hex:** Shows the raw bytes of the packet, including the session ID (0x000004c00000004d) and account information (Acct:steve.smith).
 - Bytes:** Displays the raw binary data.
- Status Bar:** Shows the packet number (914), timestamp (Time: 42.562717), source (Source: 192.168.1.216), destination (Destination: 192.168.1.2), protocol (Protocol: SMB2), length (Length: 751), and info (Info: Session Setup Request, NTLMSSP_AUTH, User: SPOONWATCH\steve.smith). It also indicates the port (port: 445), host (Host: 192.168.1.2), and CNameString.
- Bottom Buttons:** Includes standard Wireshark controls like "Show packet bytes" and "Eng/Intl".

Question 21

The hostname for the 192.168.1.216 IP is **DESKTOP-GXMYNO2**.

The screenshot shows a Wireshark capture of an NTLMSSP session setup request. The packet details pane shows a Session Setup Request (SMB2) from source 192.168.1.216 to destination 192.168.1.2. The bytes pane displays the raw SMB2 message structure, including the command code (4d), flags (0x00000010), and session ID (0x000004c00000004d). The packet list pane shows other related SMB2 packets, such as a Session Setup Response and a User Authentication response.

Question 22

The **2.56.57.108** IP returned a ZIP file via POST request. It's interesting to notice that there's some suspicious information on that file, like the languages supported, like just English and Russian, and the information "This program cannot be run in DOS mode".

Network traffic analysis showing a series of POST requests from 192.168.1.216 to 2.56.57.108, followed by a GET request for a zip file and several M-SEARCH SSDP requests.

No.	Time	Source	Destination	Protocol	Length	Info	port	port	Host
1501	203.017250	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//6.jpg HTTP/1.1	497...	80	2.56.
1641	203.556638	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//1.jpg HTTP/1.1	497...	80	2.56.
2225	204.257253	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//2.jpg HTTP/1.1	497...	80	2.56.
2541	204.548240	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//3.jpg HTTP/1.1	497...	80	2.56.
2691	204.747216	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//4.jpg HTTP/1.1	497...	80	2.56.
3054	205.023863	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//5.jpg HTTP/1.1	497...	80	2.56.
4194	205.559859	192.168.1.216	2.56.57.108	HTTP	539	POST /osk//7.jpg HTTP/1.1	497...	80	2.56.
4275	206.429996	192.168.1.216	2.56.57.108	HTTP	542	POST /osk//main.php HTTP/1.1	497...	80	2.56.
4816	207.181483	192.168.1.216	2.56.57.108	HTTP	83	POST /osk/ HTTP/1.1 (zip)	497...	80	2.56.
5047	609.052177	192.168.1.216	23.38.189.225	HTTP	303	GET /c/msdownload/update/others/2022/01/35969516_5bcfa6f7...	497...	80	23.38
5058	609.074435	192.168.1.216	23.38.189.225	HTTP	303	GET /c/msdownload/update/others/2022/01/35969515_2975e5b...	497...	80	23.38
5069	609.099536	192.168.1.216	23.38.189.225	HTTP	303	GET /c/msdownload/update/others/2022/01/35969632_c422aaa...	497...	80	23.38
5309	613.267252	192.168.1.216	23.38.189.225	HTTP	390	GET /c/msdownload/update/software/defu/2022/01/am_delta_...	497...	80	23.38
5313	613.270748	192.168.1.216	23.38.189.201	HTTP	390	GET /c/msdownload/update/software/defu/2022/01/am_delta_...	497...	80	23.38
5317	613.296742	192.168.1.216	23.38.189.225	HTTP	395	GET /c/msdownload/update/software/defu/2022/01/am_delta_...	497...	80	23.38
5688	616.405816	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5689	616.412839	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5690	616.619551	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5691	619.401261	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5692	619.401485	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5693	619.635176	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5714	622.402498	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5715	622.402683	192.168.1.216	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	530...	1900	239.2
5779	668.719505	192.168.1.216	8.253.189.126	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disalloweds...	497...	80	2.53

The figure shows a Wireshark capture of a POST request to the URL `/osk//6.jpg`. The request is sent via HTTP/1.1 with various headers including Accept, Accept-Language, Accept-Charset, Accept-Encoding, Content-Type, Host, Connection, Cache-Control, and a boundary for multipart/form-data. The response includes status code 200 OK, Date (Fri, 07 Jan 2022 16:07:32 GMT), Server (Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10), Last-Modified (Thu, 06 Jun 2019 04:01:52 GMT), ETag ("235d0-58a9fc6206c00"), and Content-Type (image/jpeg). The response body contains a file named `MZ.....@.....` followed by the message "this program cannot be run in DOS mode." The packet details pane shows the raw hex and ASCII data for the file and the error message.

Question 23

Following the HTTP stream for the suspicious download we can check that all the traffic to the destination went via port **49738**.

