CSE 5382: Secure Programming - Spring 2020
Capture the Flag Bonus Exercise

Student Name: Goutami Padmanabhan
Student ID: 1001669338

Flag Table

Placed the flags once found them in the appropriate table entries below.

	Cryptography	Malware	Network Capture	Reverse Engineering	Steganography
Level 1 (2 Points)	backoff_malware	flag{sandworm_apt}	M0d1c0nF14G	lm	flag{covert_channel}
Level 2 (3 Points)	WANNACRY	2e1afcef9baa15b8db764274b0e45d3f	YWRtaW46YWRtaW4=	ClippyHasReturned	flag{cookies_n_milk}
Level 3 (4 Points)		flag{duqu_aint_dooku}	NTLMSSP_NEGOTIATE	infected flag	R0075RUS
Level 4 (5 Points)		123123	1255	73C972DF8DB0E1EDC289F491A09AF330	flag{alan_turing_edm}
Level 5 (6 Points)		flag{kragany_uses_up$x}	passwordBasisk		

Explanation of Approaches

Cryptography

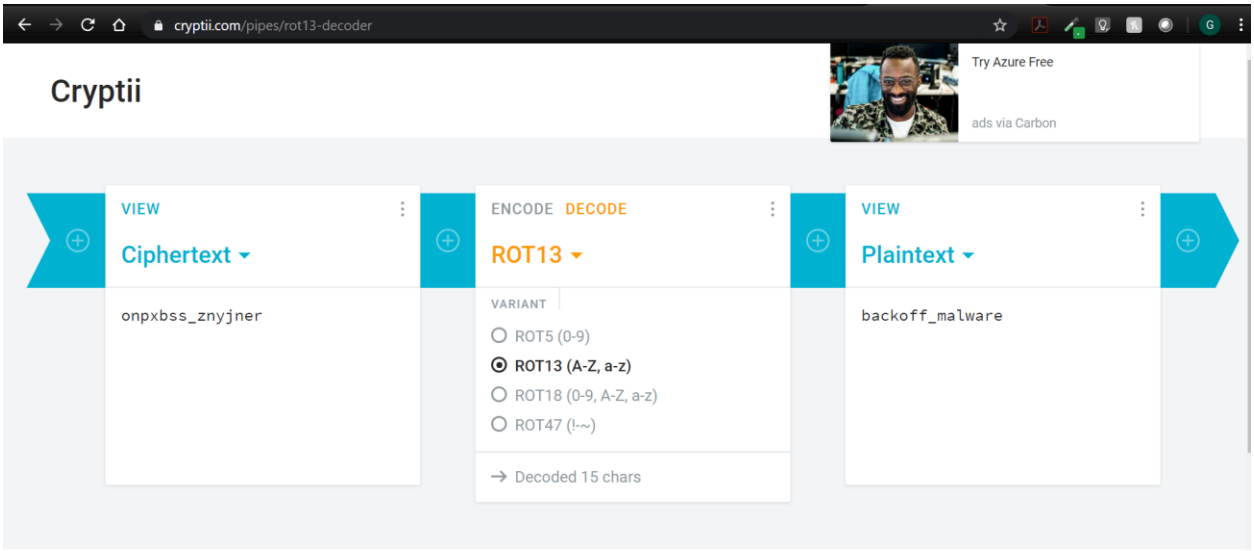
Level 1 – Orange Julius

Cipher test to plain text decryptor

To decrypt the flag synt{onpxbss_znyjner}, I googled for cipher text decryptor and got a website to decrypt the flag.

https://cryptii.com/pipes/rot13-decoder

After decrypting, we get plain text 'backoff_malware' as shown in the screenshot below



Level 2 – Block Chain

In this task, with the phrase "the pawn can beat the king", we get a hint that we should use a chess board and the malware is hidden in the letters given. So, I designed a chess board with 8 squares. If we arrange all the letters in this chess board row by row, we will get MALWARE in last column. This is shown below.

I	L	P	L	N	C	W	N
N	U	H	A	A	H	E	**M**
T	M	E	G	C	I	L	**A**
H	N	R	I	R	S	L	**L**
I	A	T	S	Y	N	K	**W**
S	R	H	W	W	O	N	**A**
C	C	E	A	H	W	O	**R**
O	I	F	N	I	A	W	**E**

But we did not get any flag in this chess board. Hence, I tried to use online base 64 decoder to find if I get any flag.

From the screenshot, we can see that we get a list of decoded strings to the left. If we check the first string we have got, we can see the flag in that string as highlighted below.

INTHISCOLUMNARCIPHERTHEFLAGIS**WANNACRY**WHICHISNOWAWELLKNOWNMALWARE

The hidden flag in this string is WANNACRY

Level 3 – DASH DOT COM

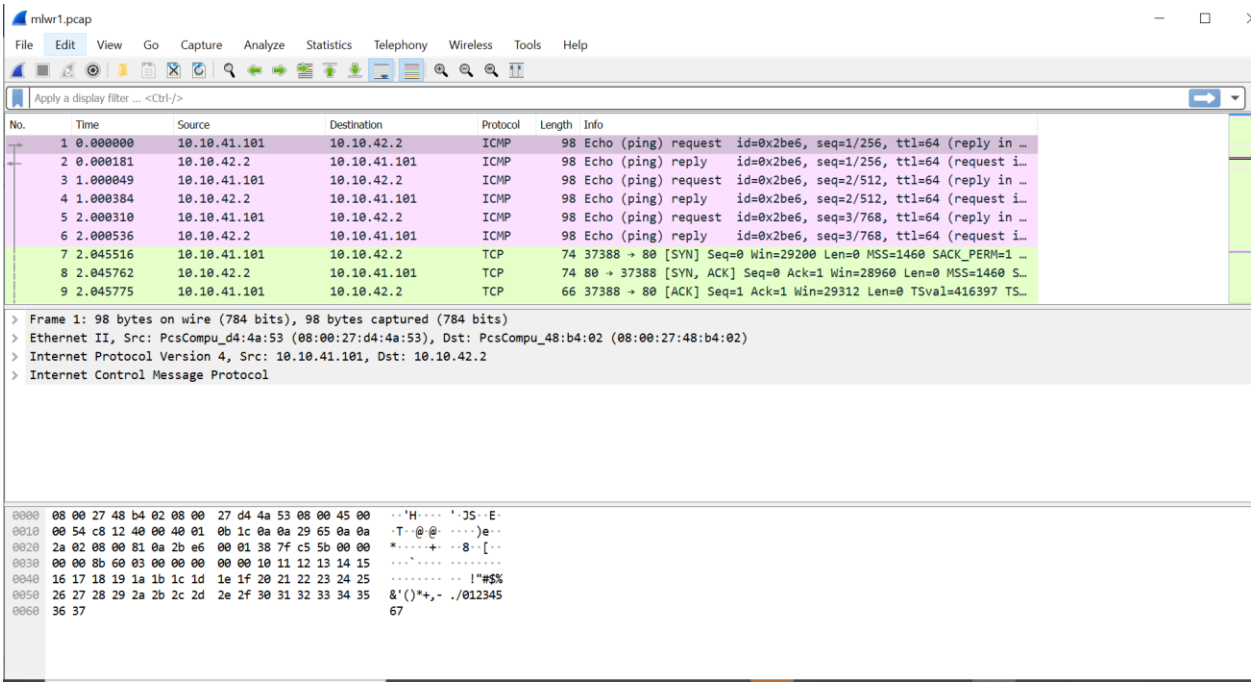
Level 4 – VIII A Small Example

Level 5 – Big Blue Randu

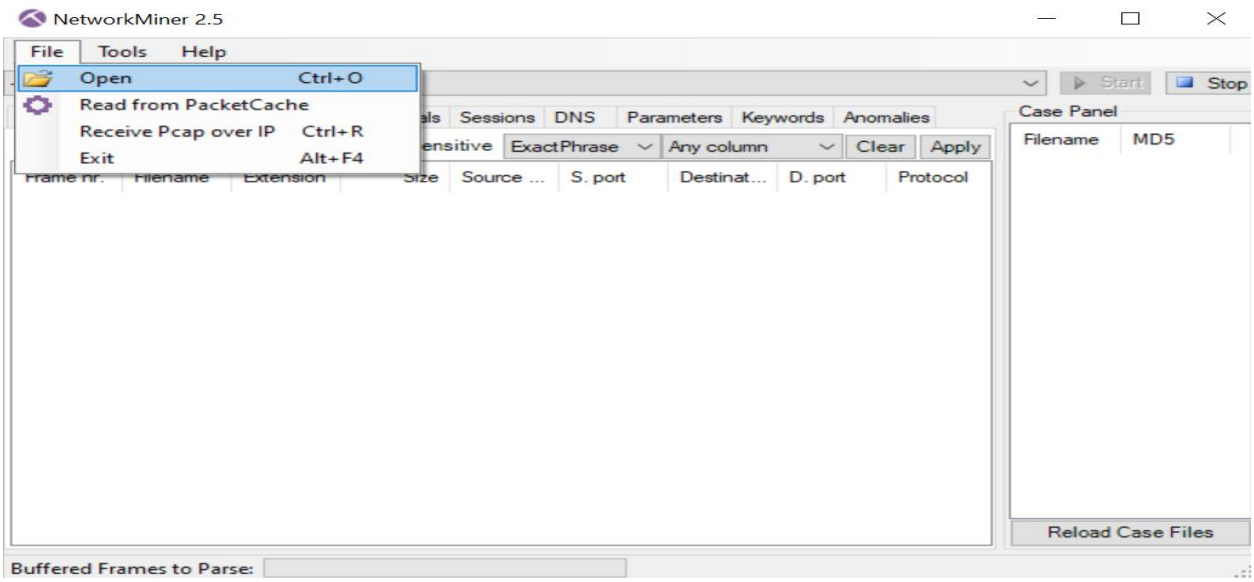
Malware

Level 1

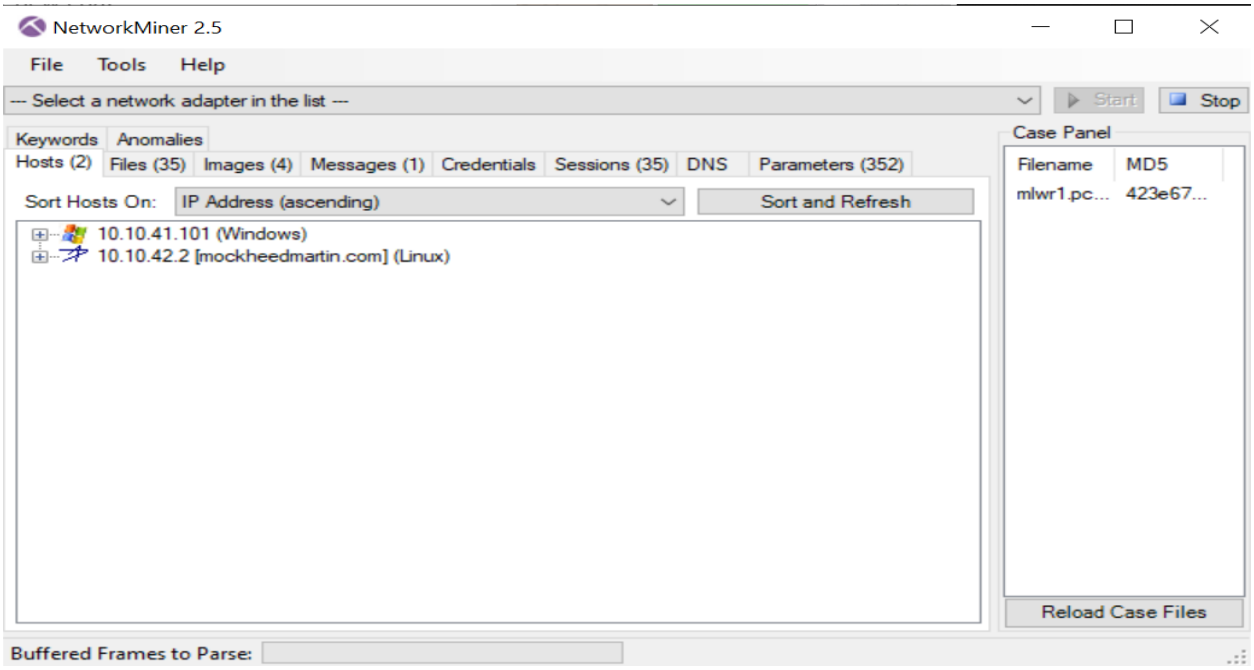
In this task, we have to find the hidden flag in the zip file. I tried to open the given Wireshark capture file in Wireshark as shown in the below screenshot. But I was unable to find any flag.



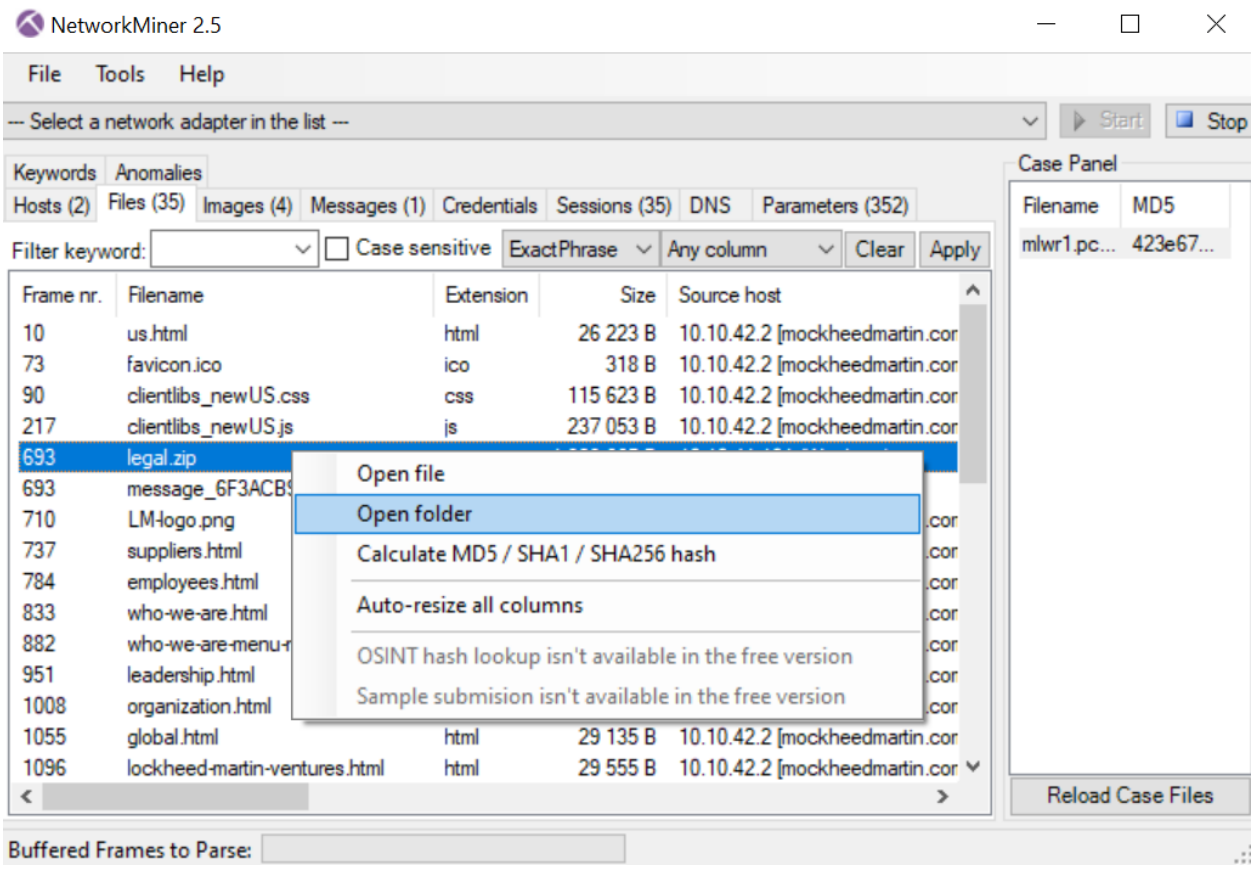
I browsed through to find if there is nay other software which can find zip file from Wireshark capture file. In found an application called Network Miner. I used it to open the file.



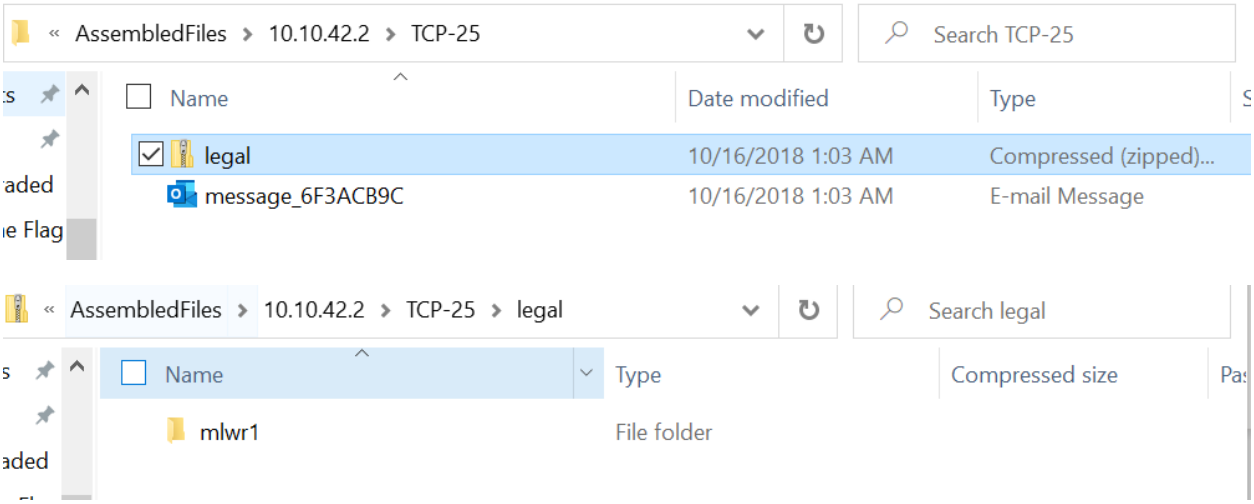
When I opened it showed 2 hosts as shown in the screenshots.



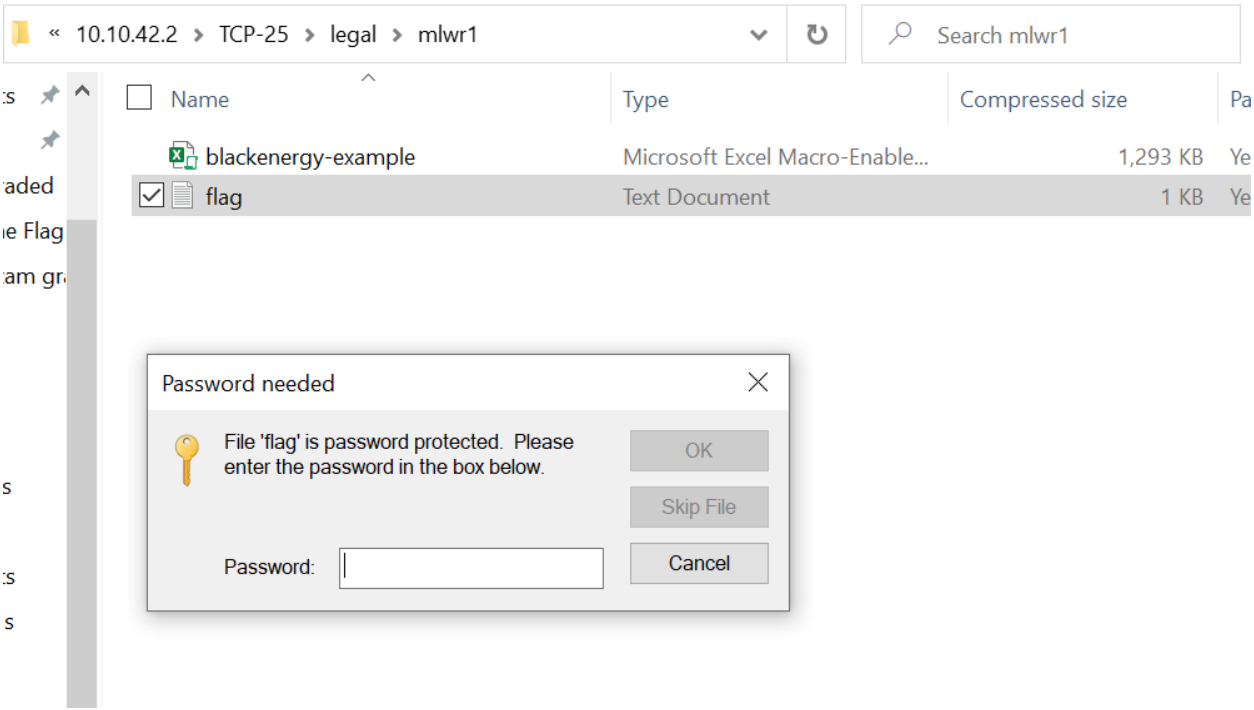
I navigated to Files section to find the zip file named legal.zip. I opened the folder as shown below.



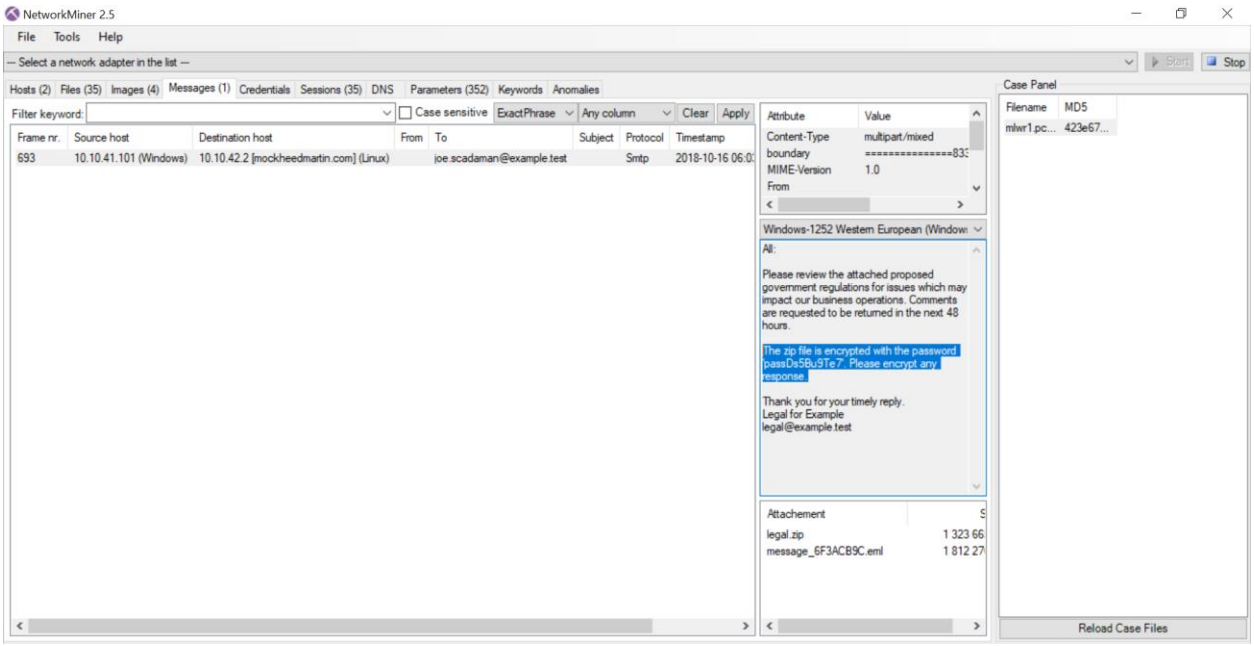
I navigated through the legal.zip file to get mlwr1 folder.



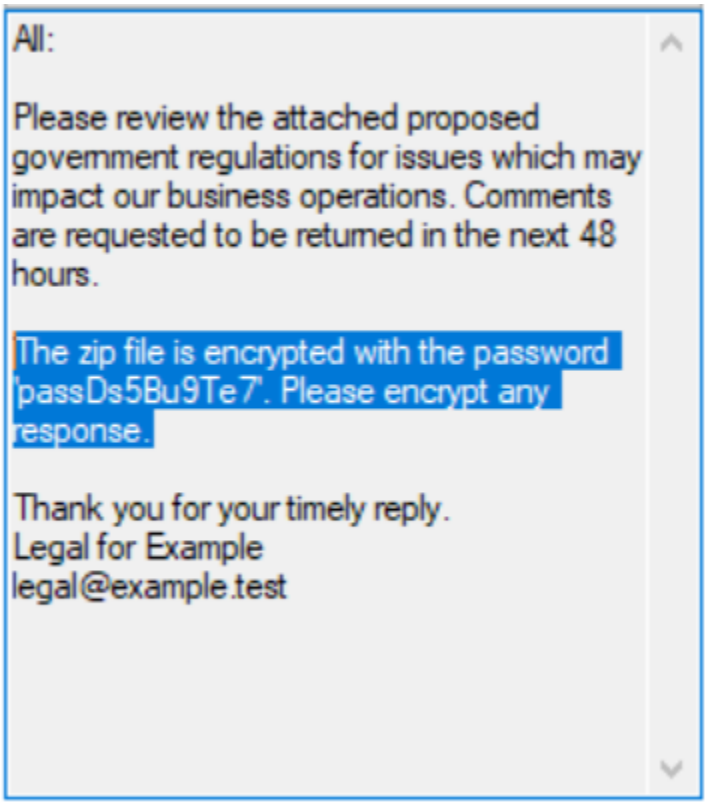
In the mlwr1 folder we see one excel file and one text file named flag. I clicked on that and it asked for password.



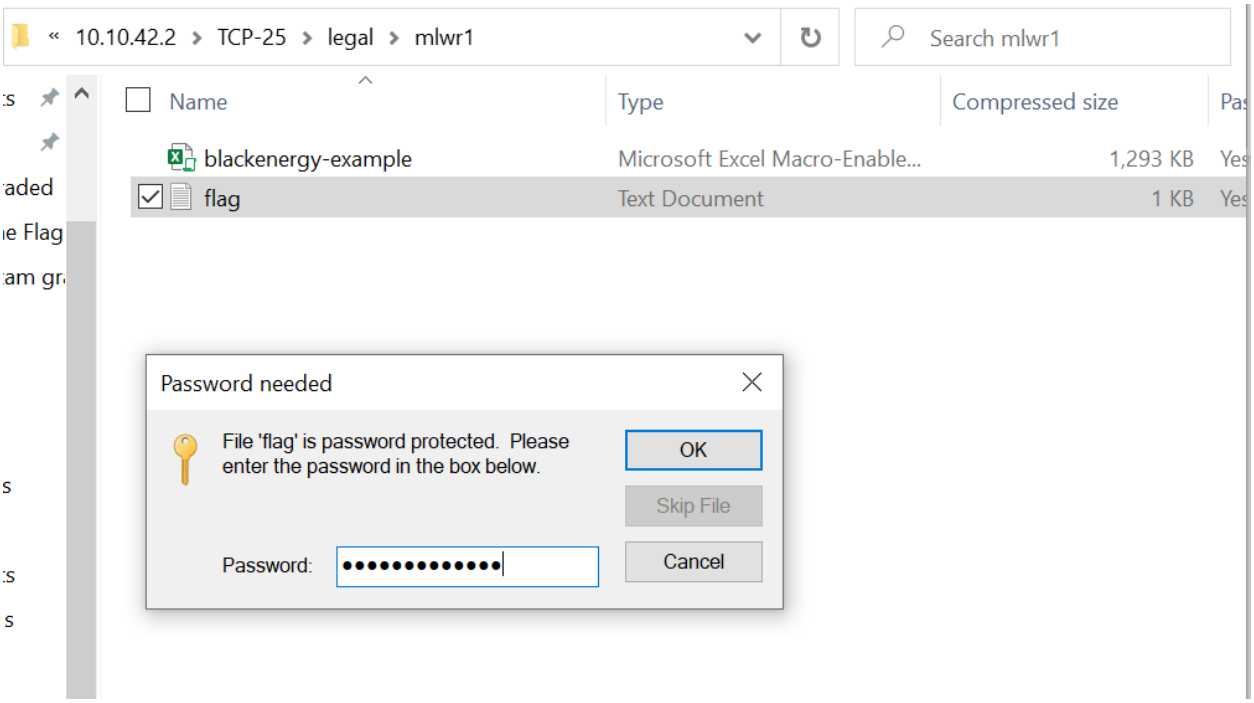
So, I went back to NetworkMiner and checked all other tabs. In the Messages tab I found the password, as highlighted in the screenshot below.



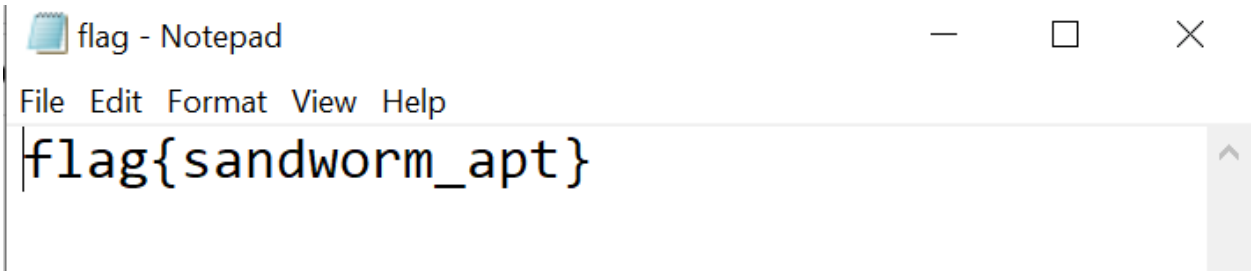
A zoomed view of the message is seen in the below screenshot.



Give the password passDs5Bu9Te7 for the flag text file I mentioned before.



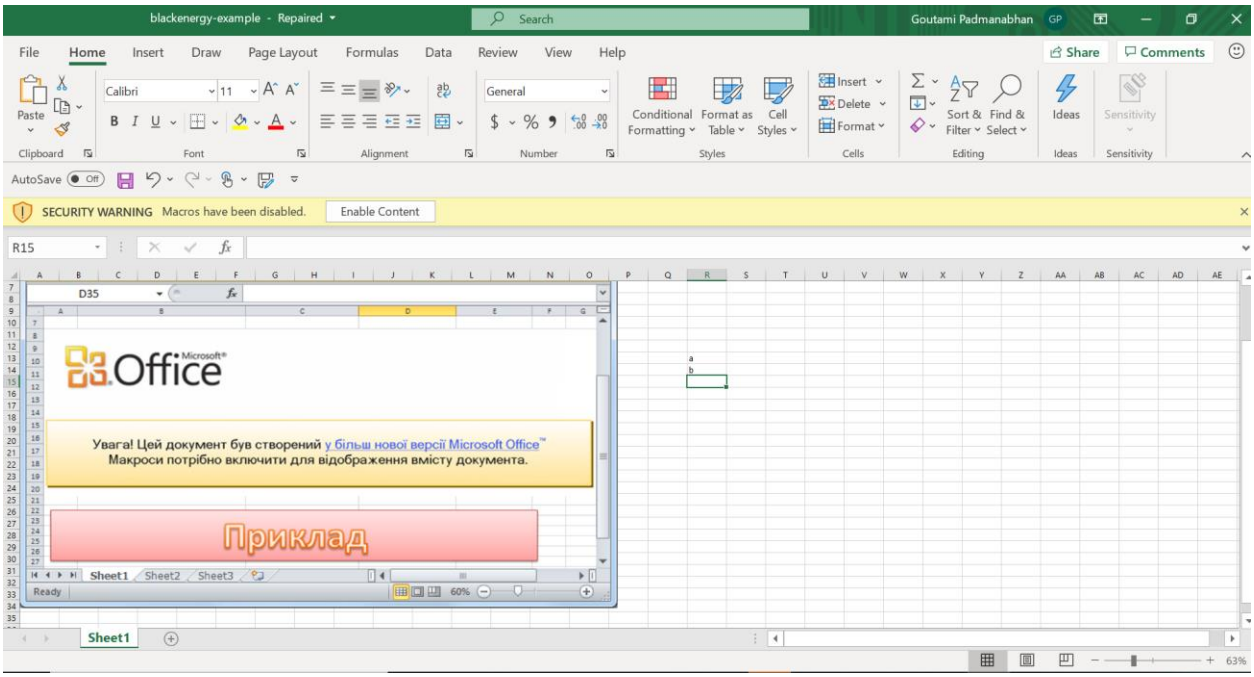
We can see the flag given in this text file as shown in the screenshot.



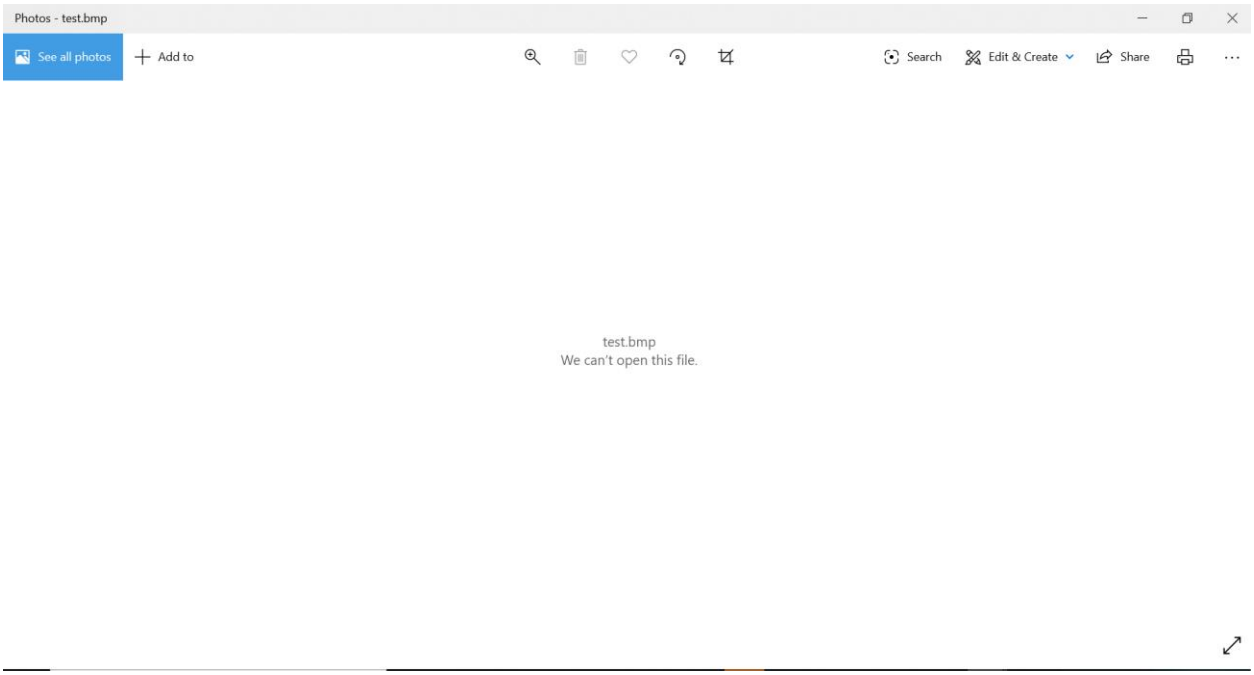
The hidden flag to be found in this task is flag{sandworm_apt}

Level 2

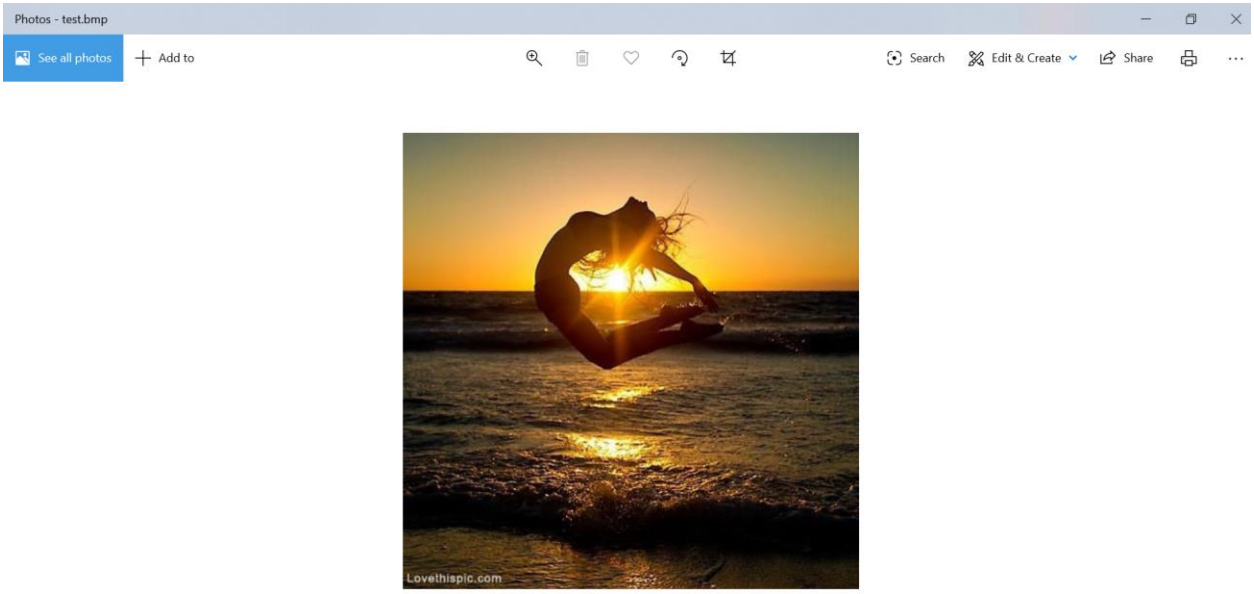
In this task we are asked to use the excel file found in Level 1 to find the flag. We open the excel sheet and check the data.



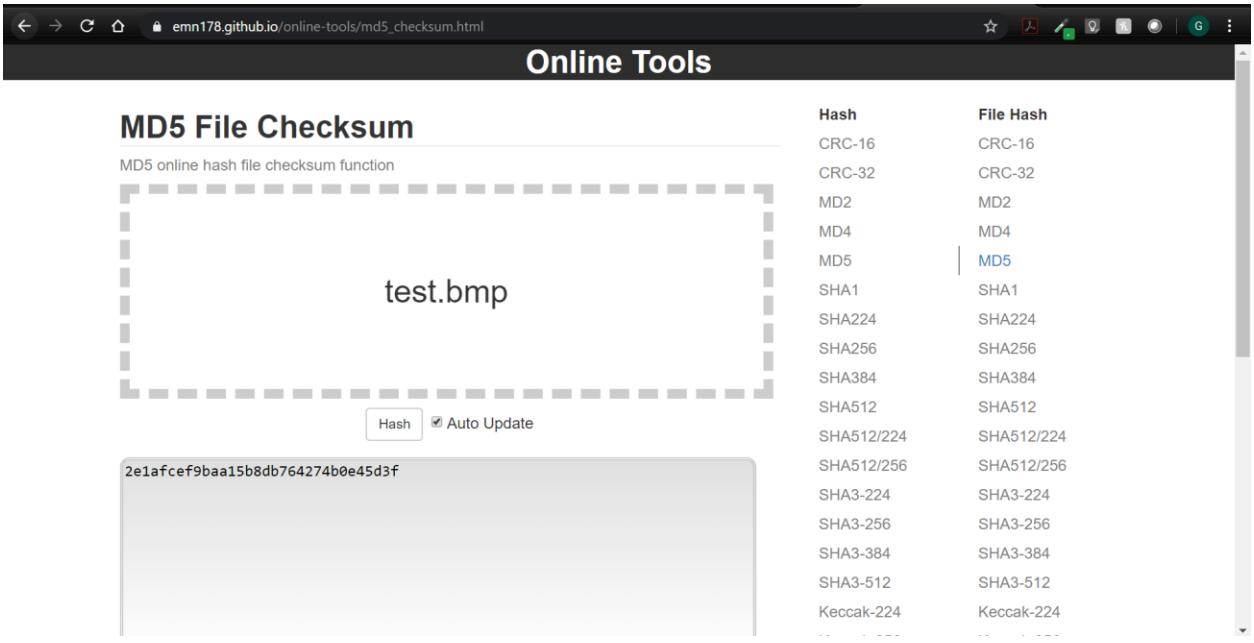
When I opened the excel sheet, teher was another image file that was trying to be opened as shown below



So, I enabled the macros in the excel sheet and immediately an image named test.bmp opened as shown below.



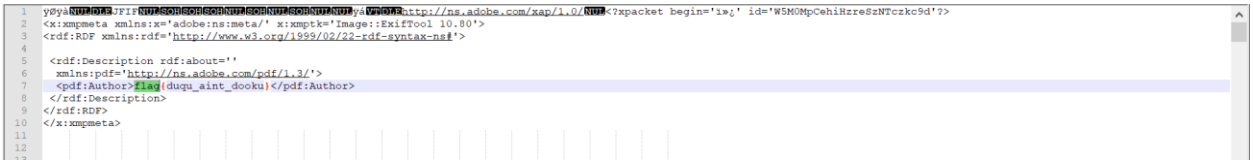
I saved the test.bmp file. It is given that the flag is the MD5SUM of the file that the spreadsheet drops. I browsed for MD5SUM and got a tool to upload the test.bmp file and check. I got the flag which is the hash code.



The hidden flag in this task is 2e1afcef9baa15b8db764274b0e45d3f

Level 3

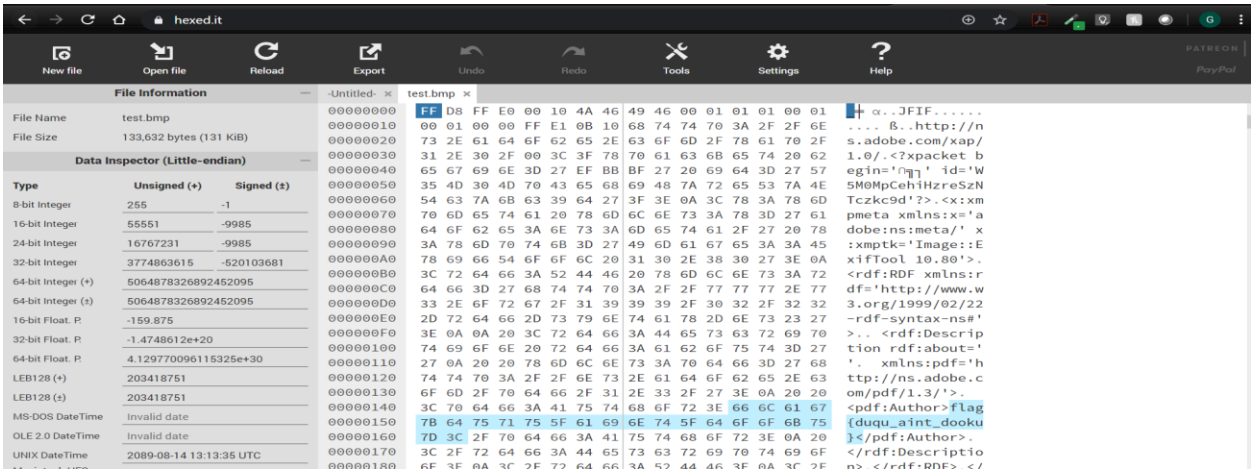
I tried to open the bmp file in Notepad++ text editor as shown in the screenshot.



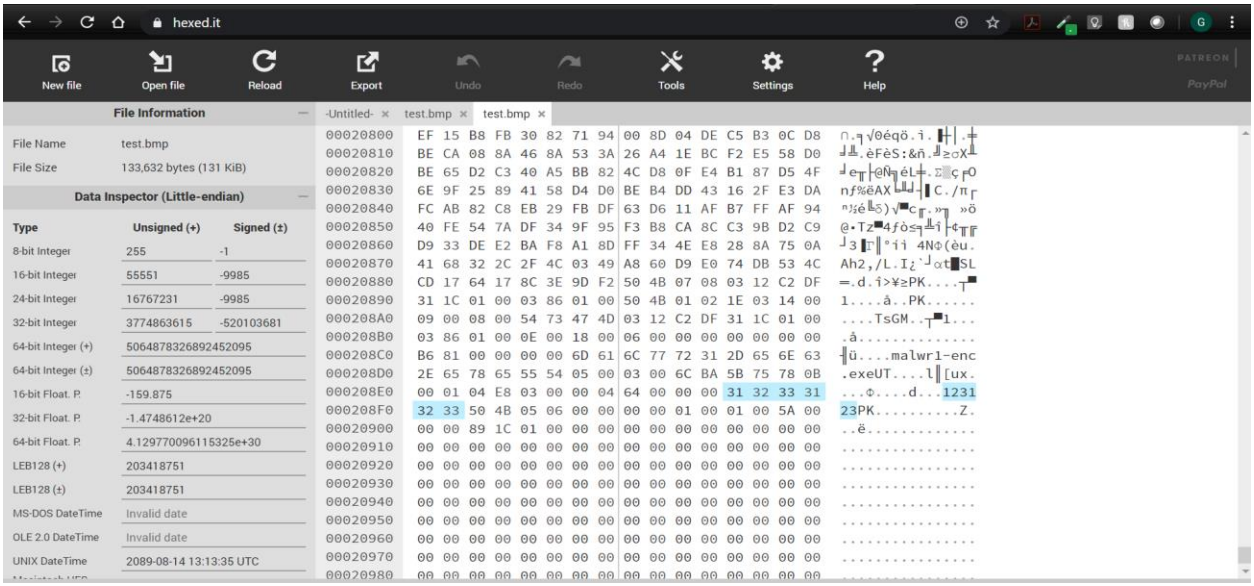
We find that flag is hidden in this bmp file. The hidden flag is flag{duqu_aint_dooku}

Level 4

In this task, we have to find the hidden password from the test.bmp file. I opened the test.bmp file in online hex-editor as well and could find the same flag. See screenshot below.



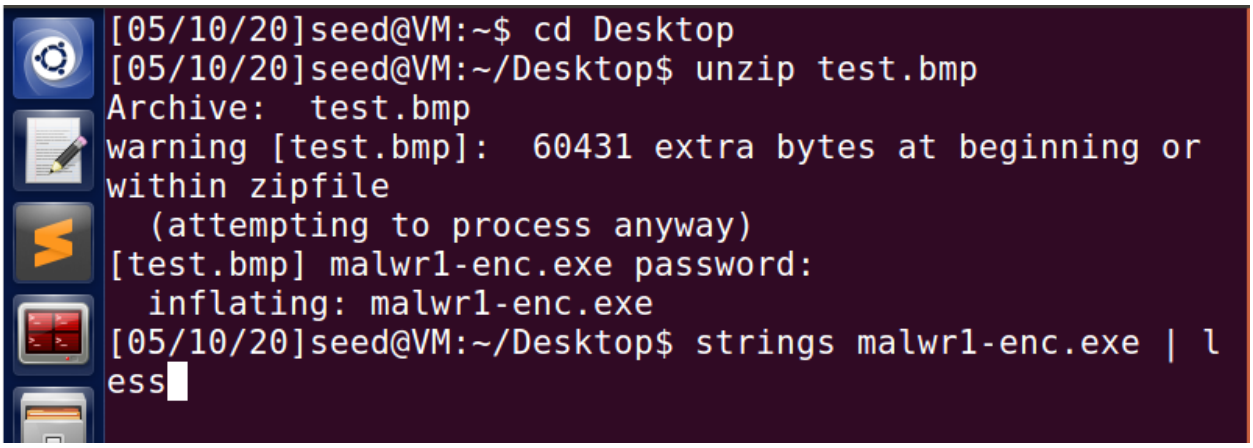
I scrolled over the entire file till the and to find the password. It is written malwr1-enc.exe. Using this hint, I guessed that the highlighted text is the password. See the screenshot below.



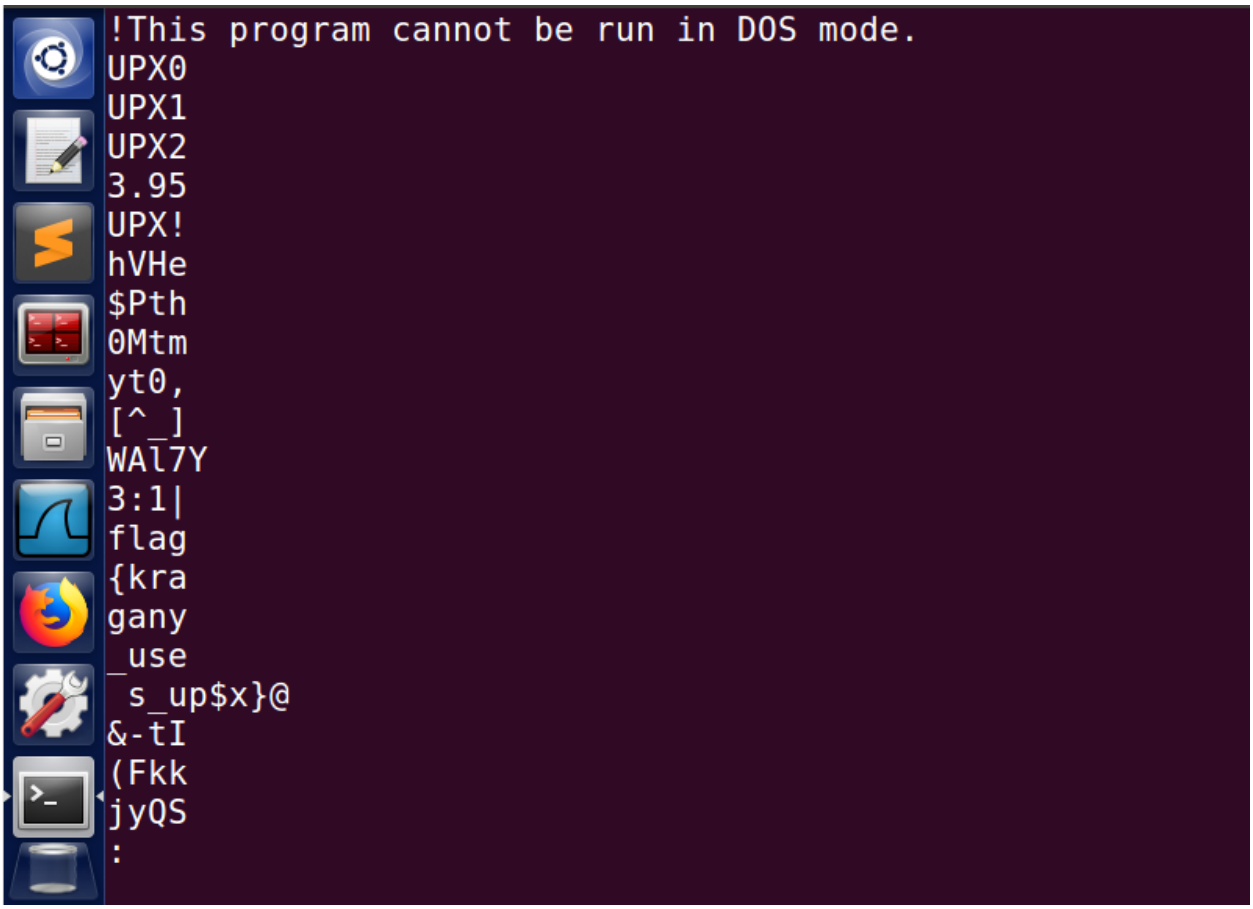
The hidden flag in this task is the password 123123

Level 5

In this task we are told that the final malware flag is in the file extracted. We try to unzip the test.bmp file and give the password we found from the previous level.



We get a prompt that the file is inflating: malwr1-enc.exe. So, this extracted file is used and opened with strings command.

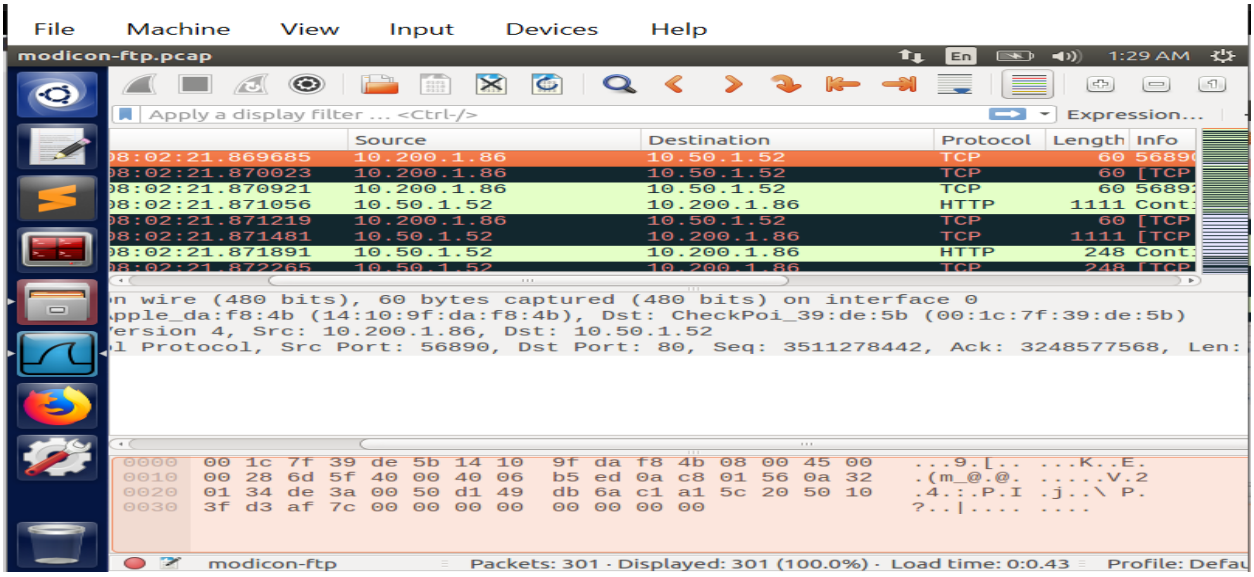


We immediately see a flag in that exe file. The hidden flag as per the screenshot is flag{kragany_use s_up$x}

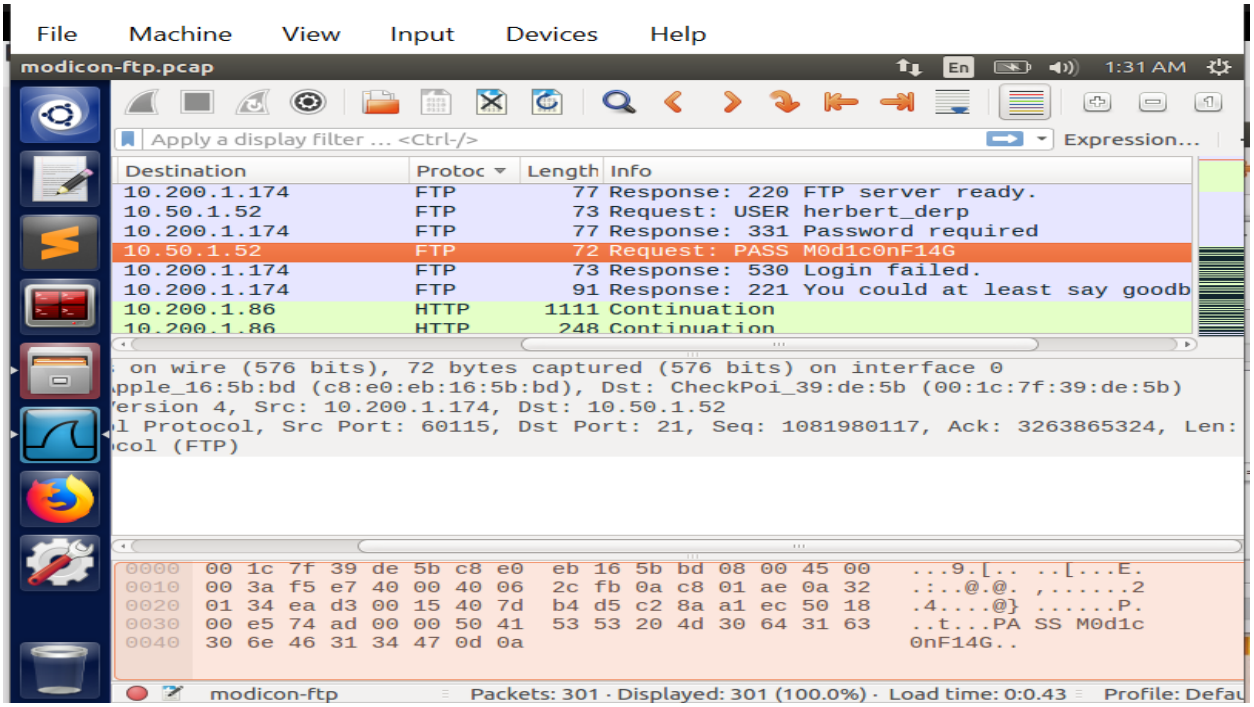
Network Capture

Level 1 – Modicon-FTP

In this task, we must find the FTP password used in the failed login attempt. We have been given a pcap file. We can use Wireshark to find out the failed login attempt. I have installed the Wireshark in my VM and imported the pcap file given.

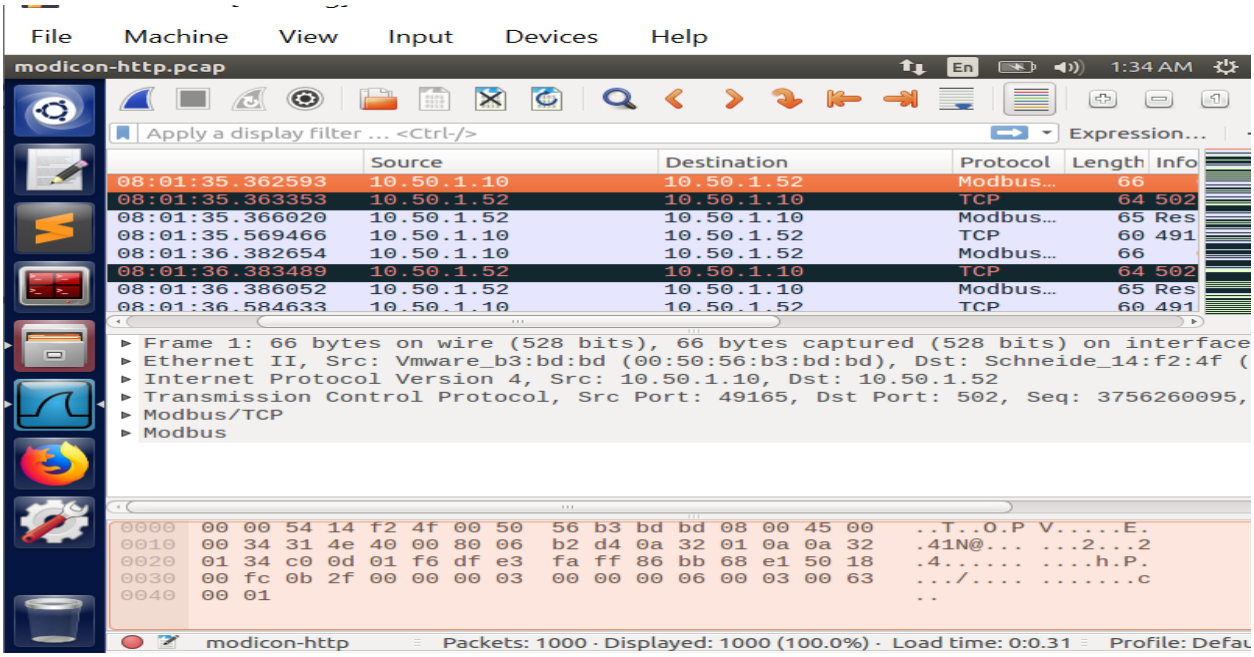


Since we are going to find the FTP password, we order the records with protocol used. If we scroll over, we see that we get the password explicitly written in the Info column. Password is M0d1c0nF14G as shown in the screenshot.

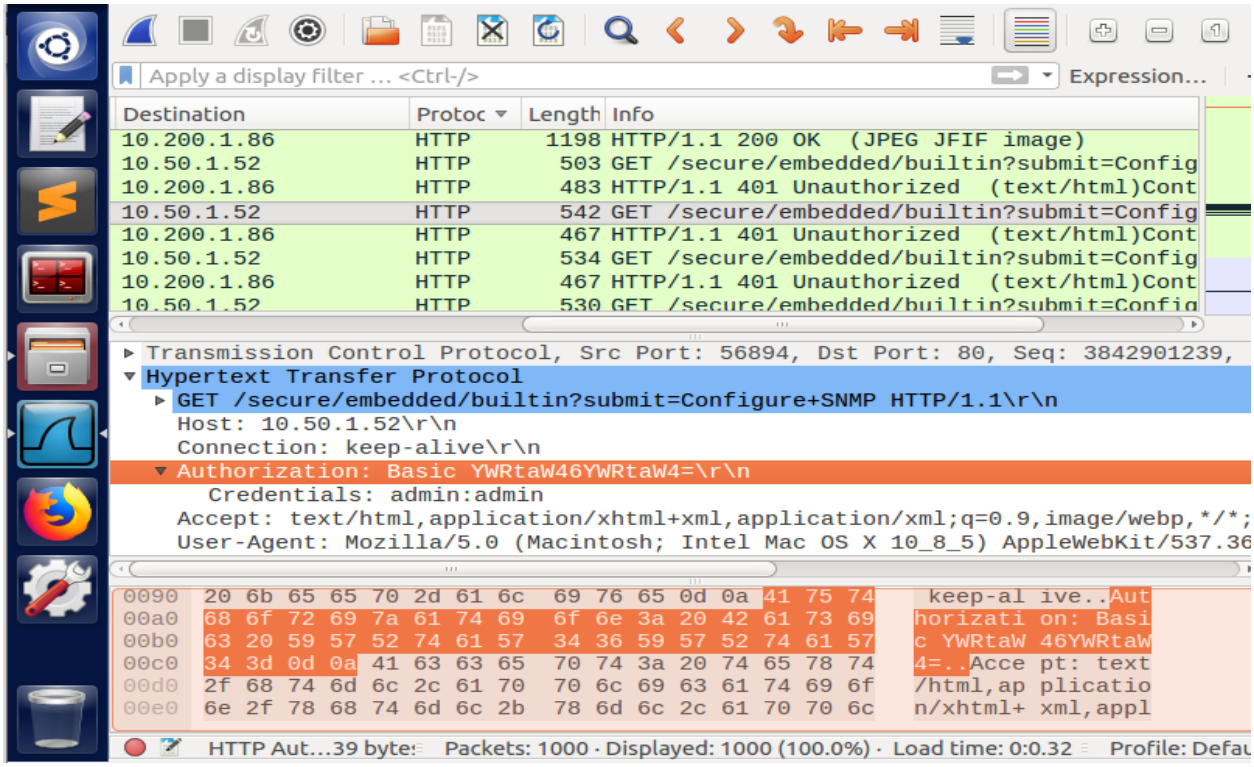


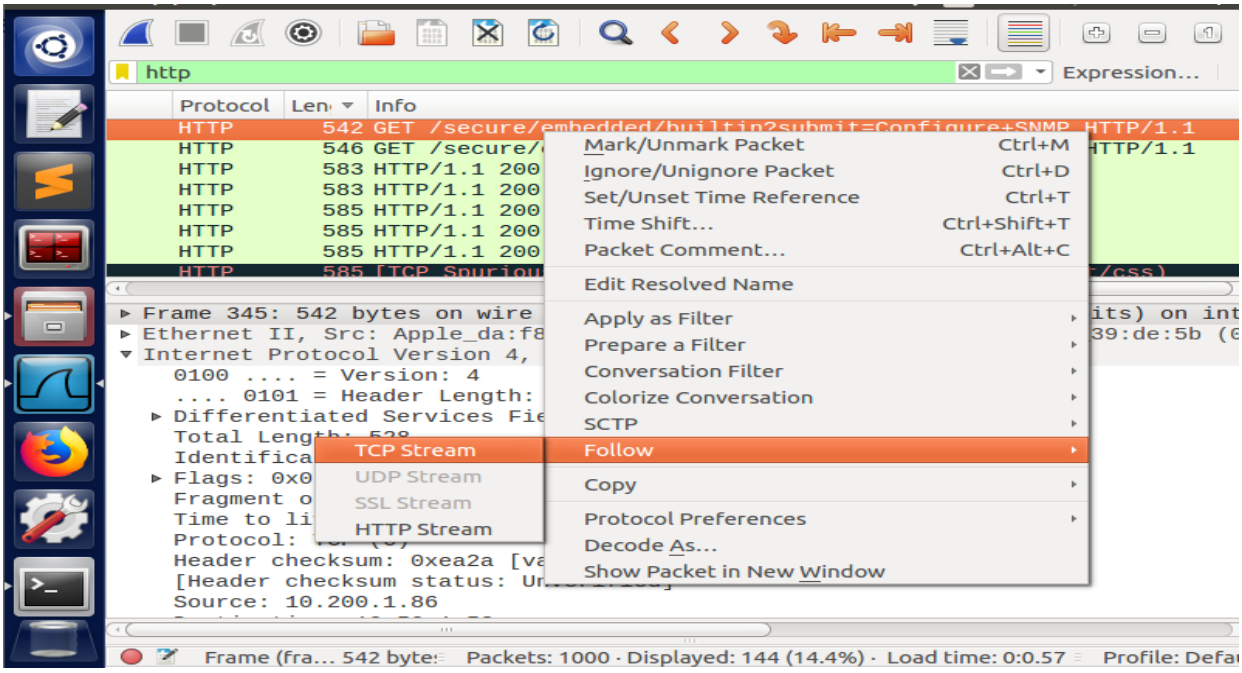
Level 2 – Modicon-HTTP

In this task, we must find HTTP Basic Authorization password used in failed user login attempt. We have been given a pcap file. We can use Wireshark to find out the password by importing the pcap file given.

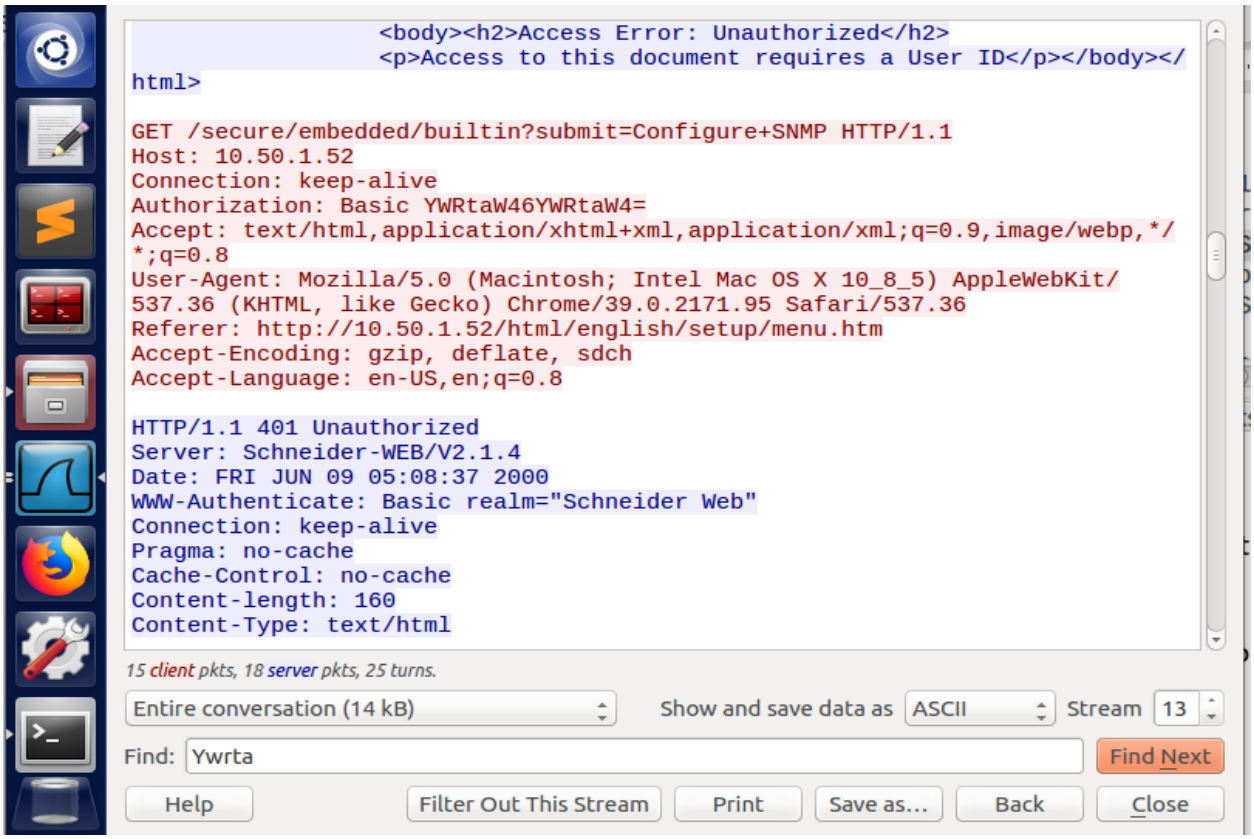


Since we are going to find the HTTP password, we order the records with HTTP protocol. If we scroll over, we see 'Unauthorized' written in the Info column. When we click on the record below that, it has a GET request with the password Authorization: Basic YWRtaW46YWRtaW4=\r\n



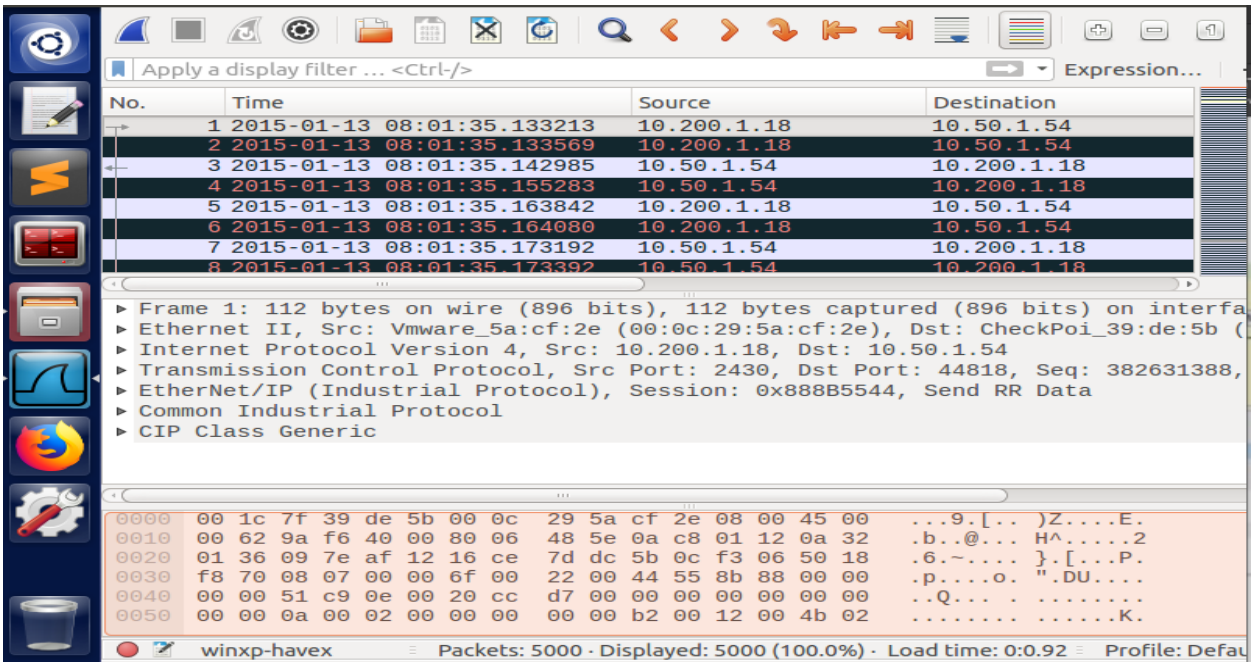


I browsed through a lot of YouTube videos to find the options to use in Wireshark. When we right click on that record and click Follow->TCP Stream, we see a separate window that shows failed login attempt in red when we search for the password YWRt. It has the details like Authorization: Basic YWRtaW46YWRtaW4=

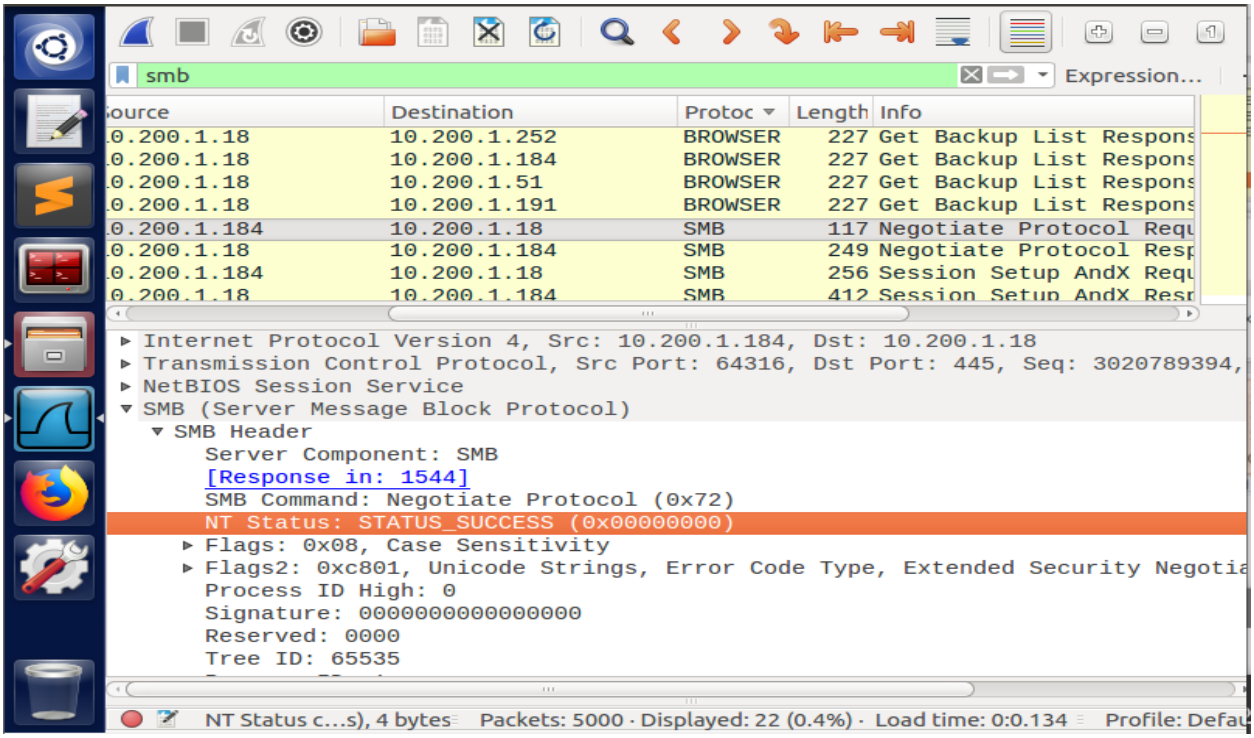


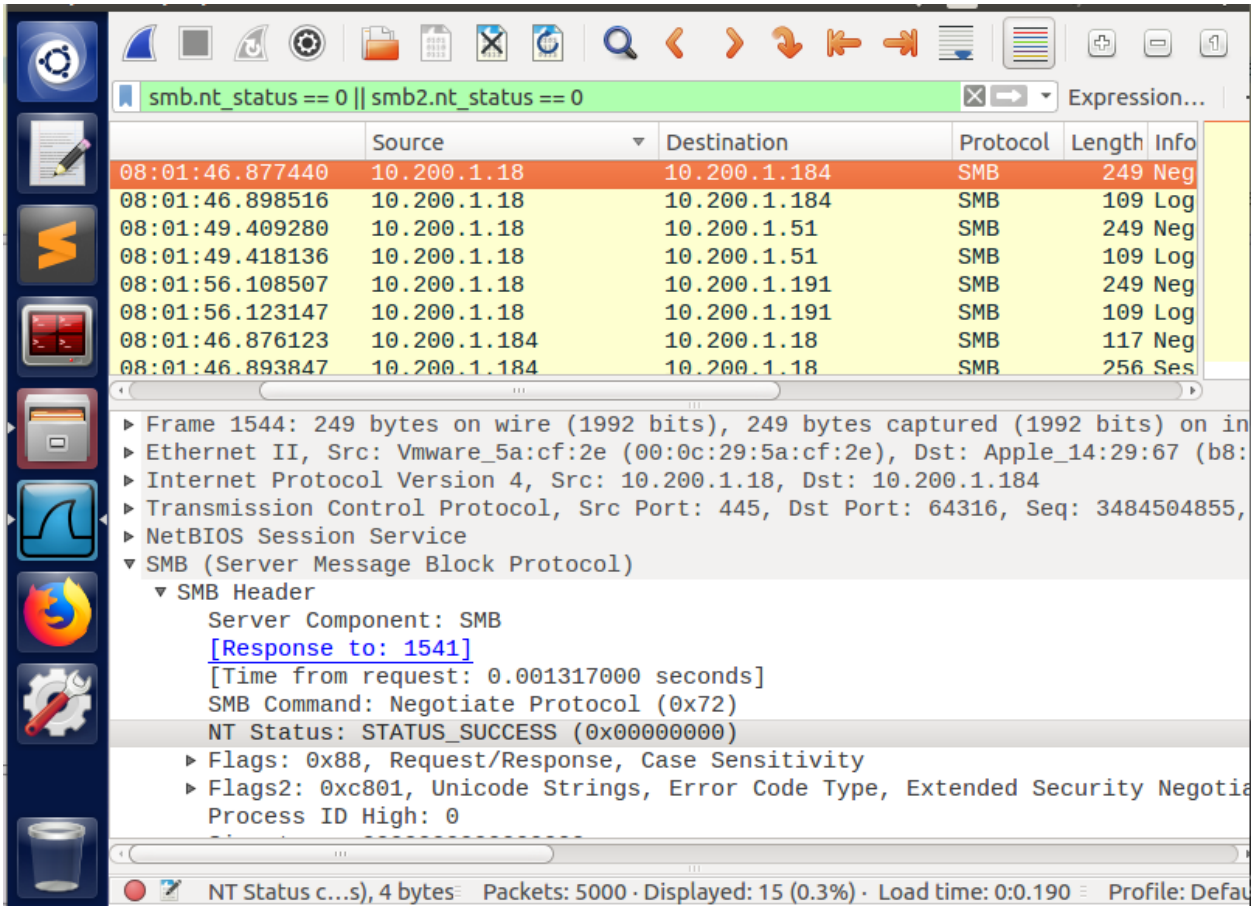
Level 3 – WinXP-HAVEX

In this task, we must find the HAVEX malware IOC. We have been given a pcap file. We can use Wireshark to find out by importing the pcap file given.



WinXP-HAVEX is Backdoor threat. Windows Defender detects and removes this threat. This threat can give a malicious hacker unauthorized access and control of your PC. SMB protocol provides unauthorized access to a remote machine. So we order the records with SMB protocol.

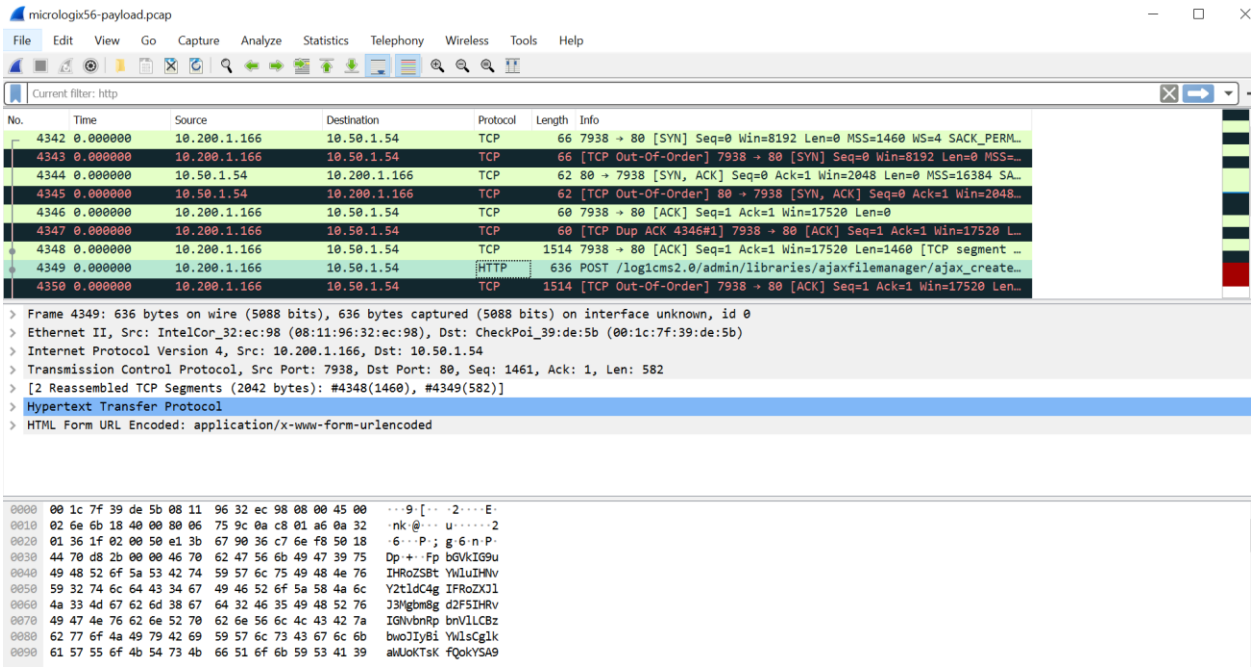




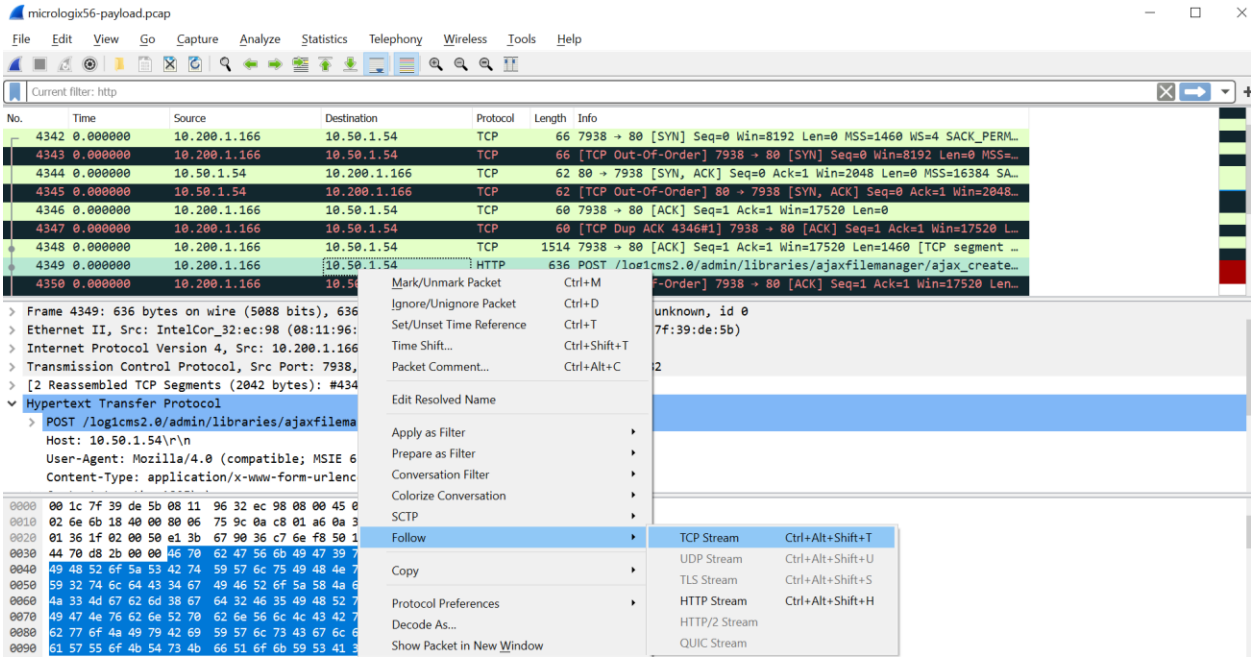
We see NT Status (Negotiate status) as STATUS_SUCCESS. This means unauthorized access has been given successfully. From the screenshot we have found the HAVEX malware IOC.

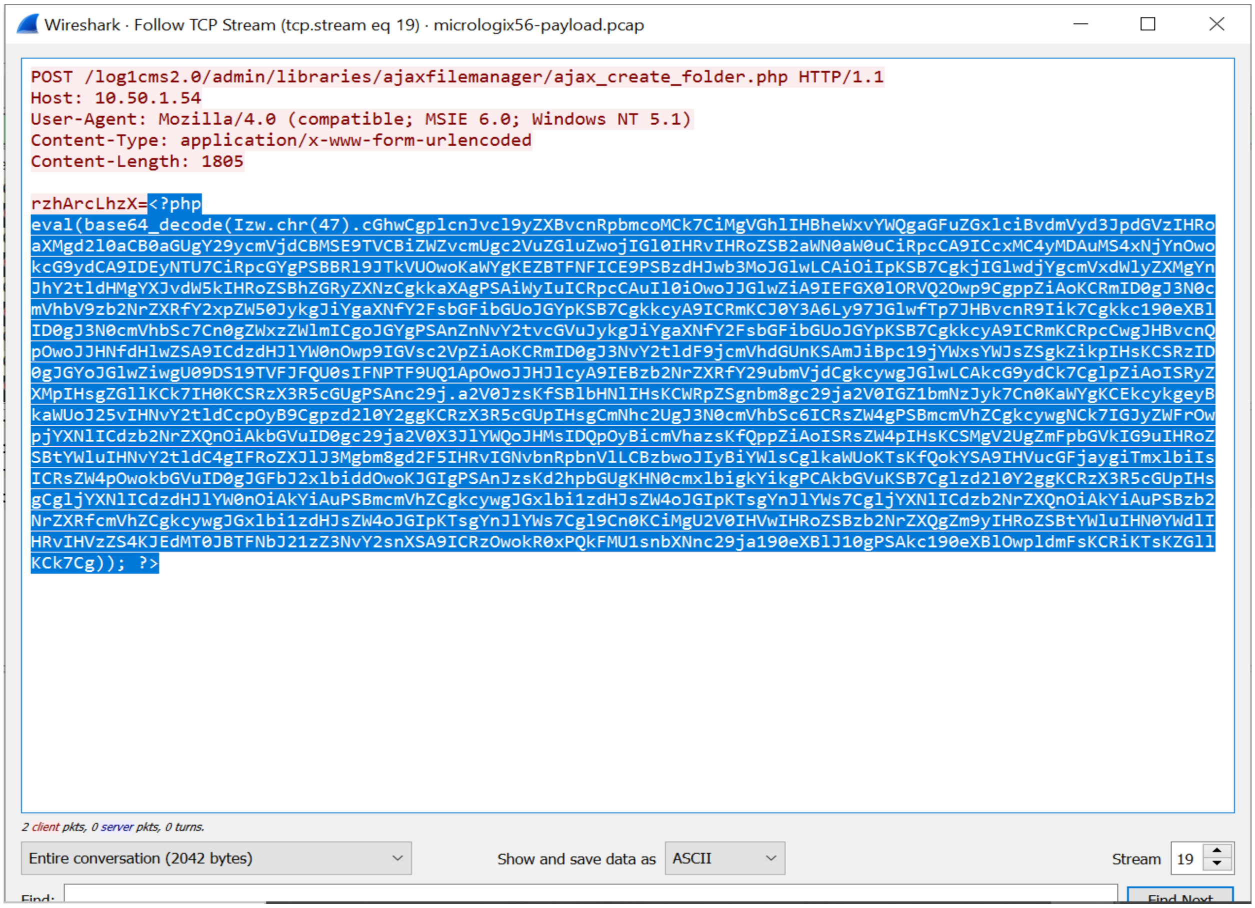
Level 4 – MICROLOGIX56

The purpose of this task is to find the port number of the backdoor that an attacker attempted to install. We have been given a pcap file. We can use Wireshark to find out by importing the pcap file given.

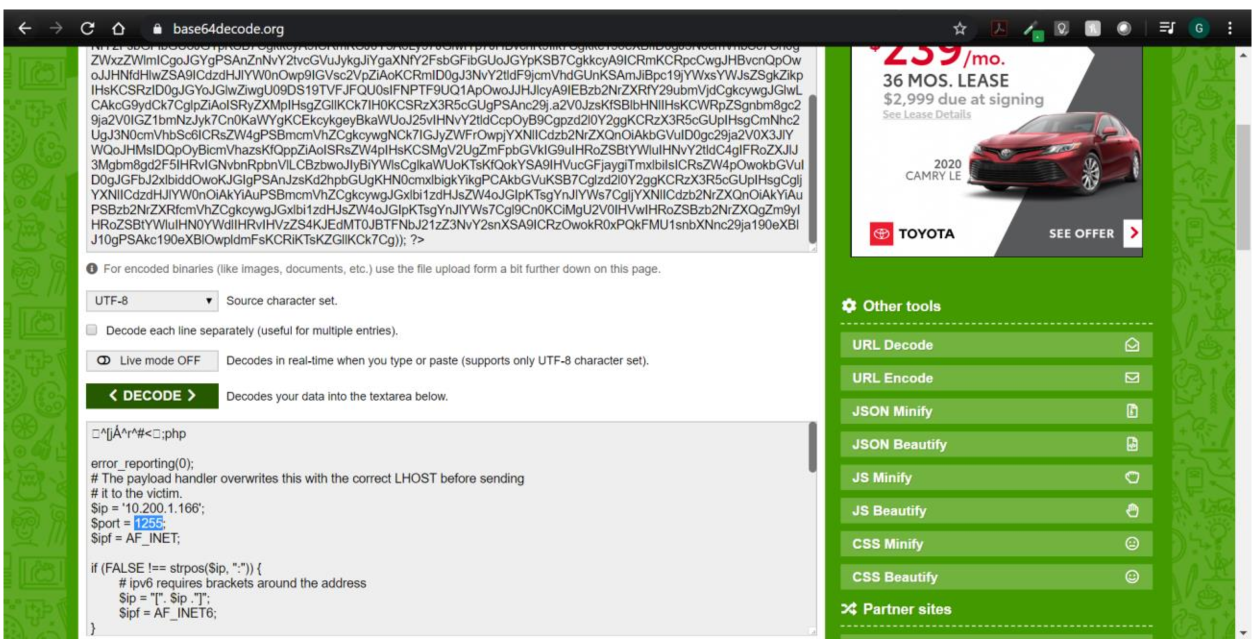


When I checked through the records, I saw HTTP protocol. When I followed the TCP stream I saw a PHP script that should not be there in the TCP stream.





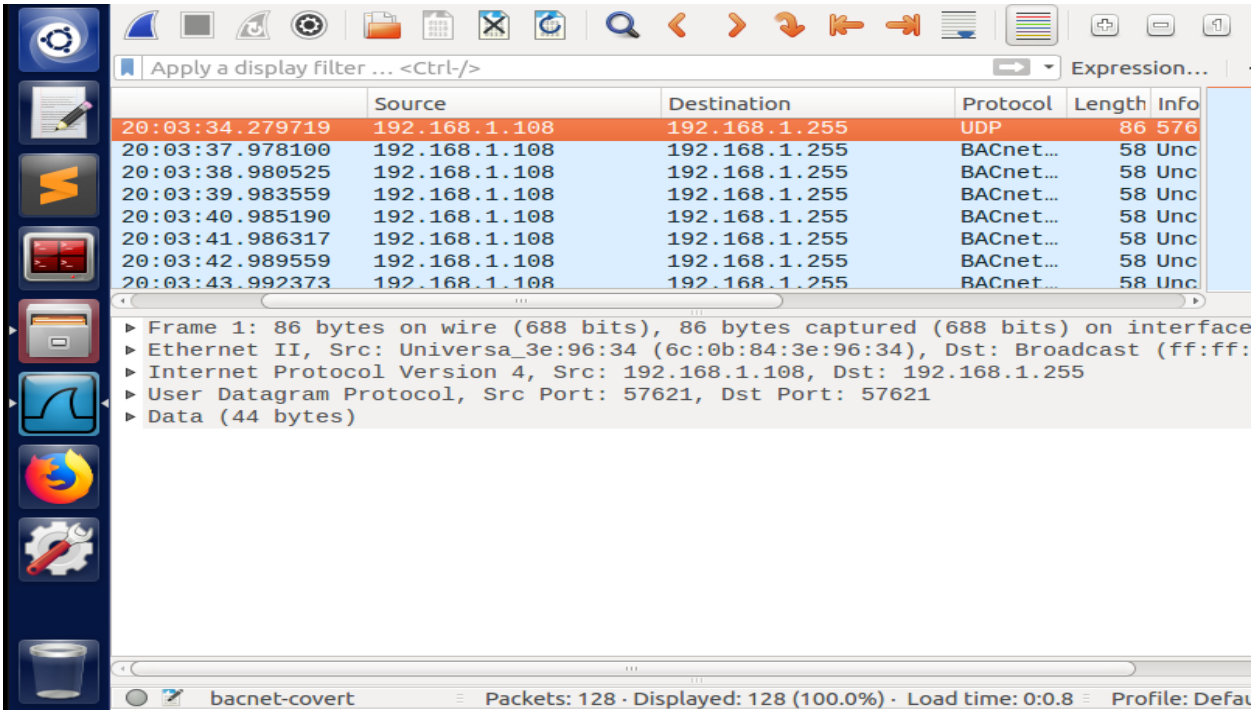
I copied the PHP script and used a base64 decoder to decode this script.



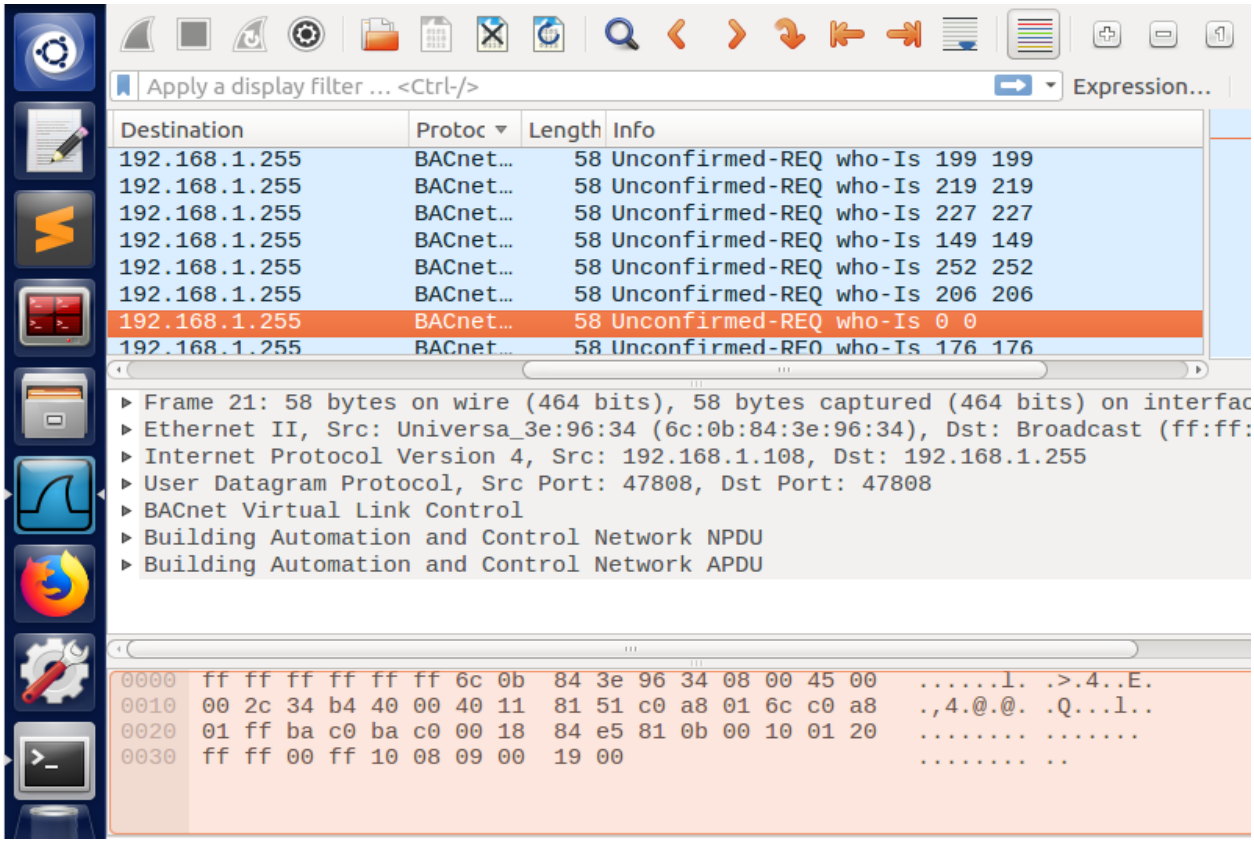
As highlighted in the screenshot, when I tried to decode the script, I found the port 1255 as shown in the screenshot. The port number of the backdoor that an attacker attempted to install is 1255.

Level 5 – BACNET-COVERT

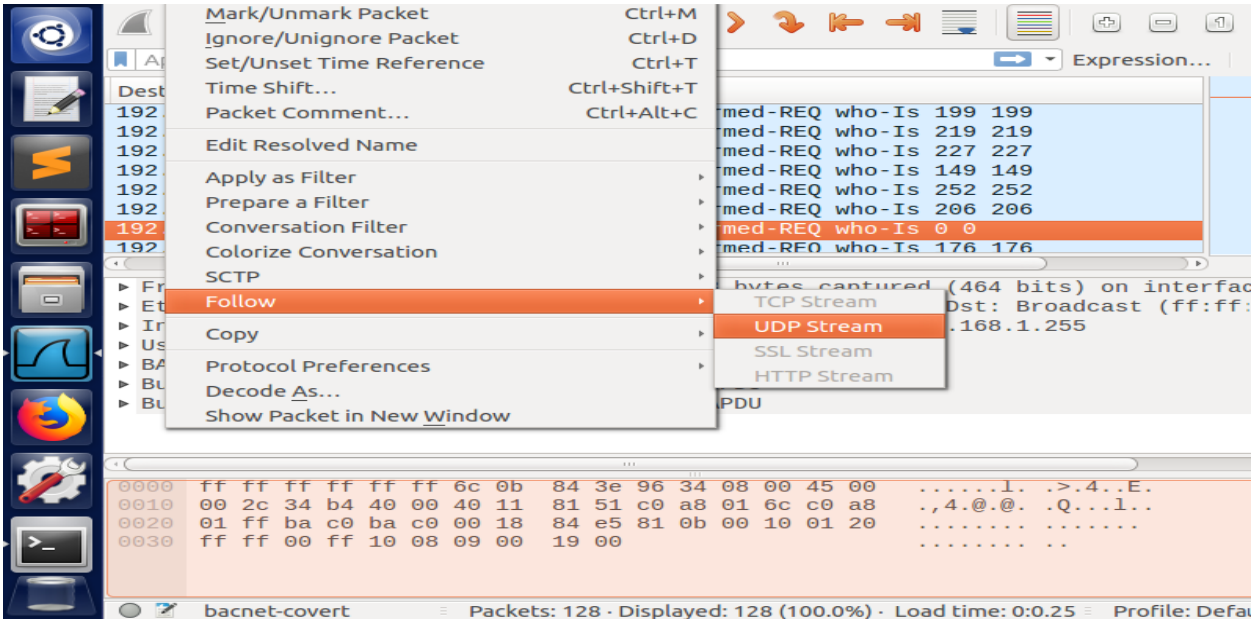
The purpose of this task is to find the covert message that was passed via the BACnet communication protocol. We have been given a pcap file. We can use Wireshark to find out by importing the pcap file given. Then we order the records with BACnet protocol.



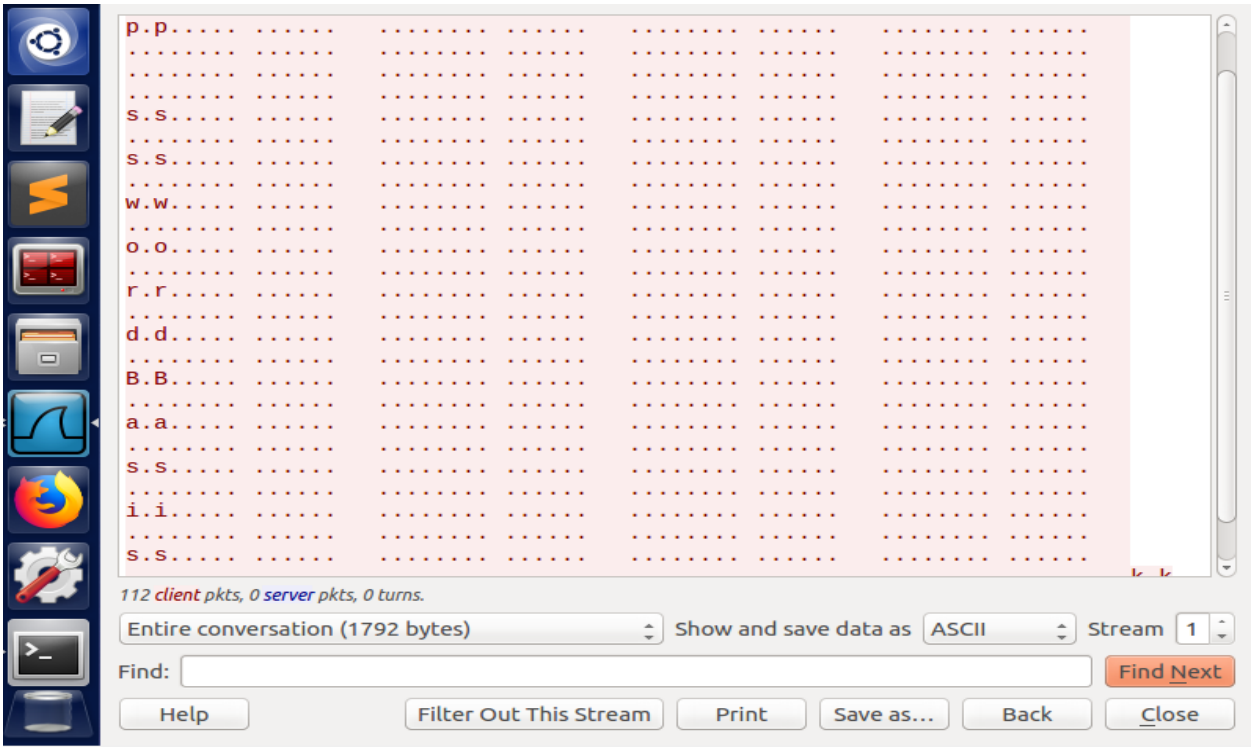
BACnet protocol is a data communication protocol is a set of rules governing the exchange of data over a computer network that covers everything from what kind of cable to use to how to form a particular request or command in a standard way.

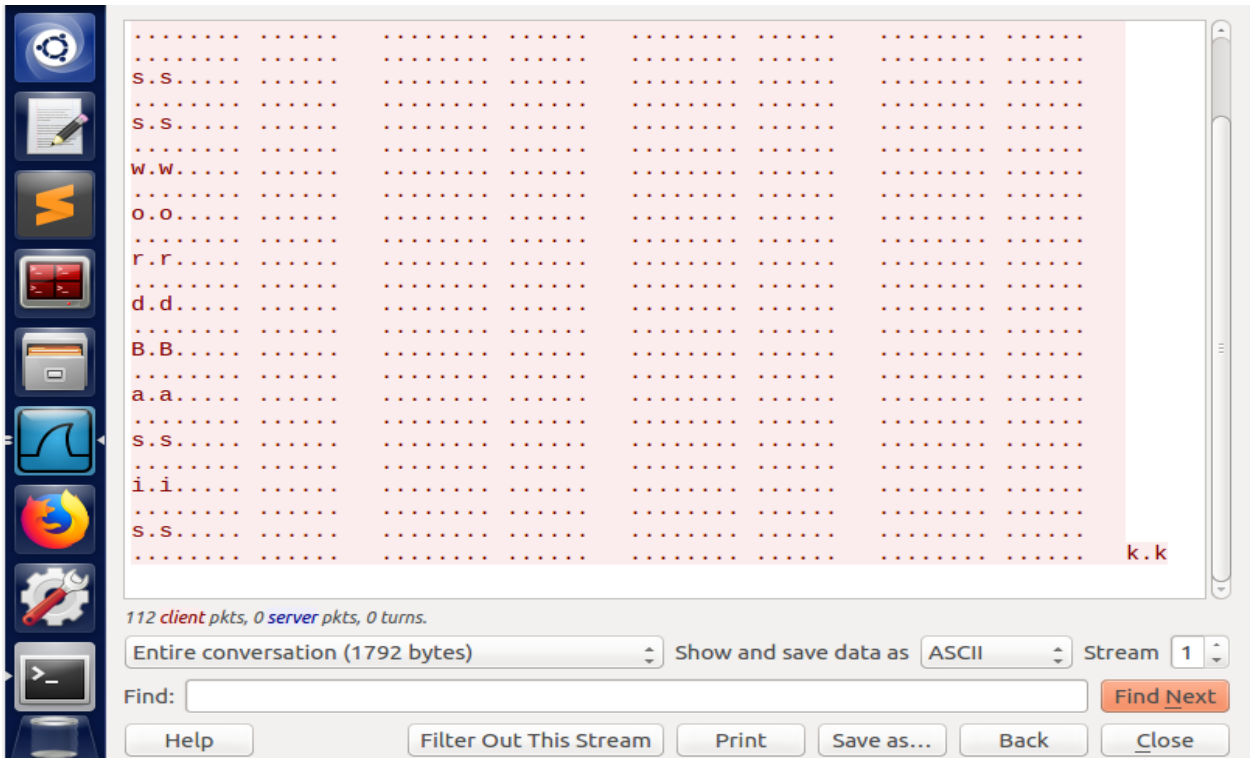


We find out that Info column has “Unconfirmed-REQ who-Is 0 0” message. This clearly shows that it is an attacker. We open the UDP stream as shown in the screenshot below.



If we open the UDP stream, we get the covert message passwordBasisk. The hidden flag is the covert message.





This is the covert message that was passed via the BACnet communication protocol – passwordBasisk

Reverse Engineering

Level 1 – Script Kiddie

In this task, we must read the code and find the password. By reading the code we can say that password starts from 12th position of contents in strPass and ends after 2 positions. 12th and 13th position is lm. So the flag password is lm

```
Dim strPass
Dim strIn

strPass="abcdefghijklmnopqrstuvwxyz"
strIn = InputBox("Enter password:", "password")

DO UNTIL IsEmpty(strIn) Or Mid(strPass,12,2) = strIn
    strIn = InputBox("Wrong password:"+strIn+vbCrlf++vbCrlf+"Try Again:", "password")
LOOP
```

Level 2 – The PDF Your Parents Warned You About I

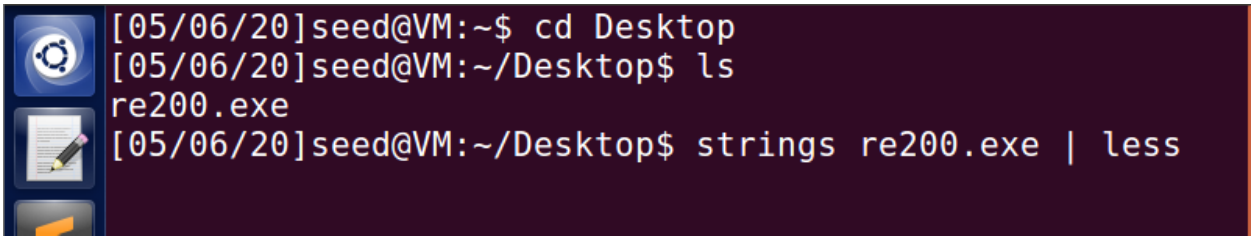
In this task we must find who created the PDF file given. I opened the PDF in Photos application. I could not find anything. Then I opened in Notepad++ in a text format. When I checked through the text, I found the tag creator.

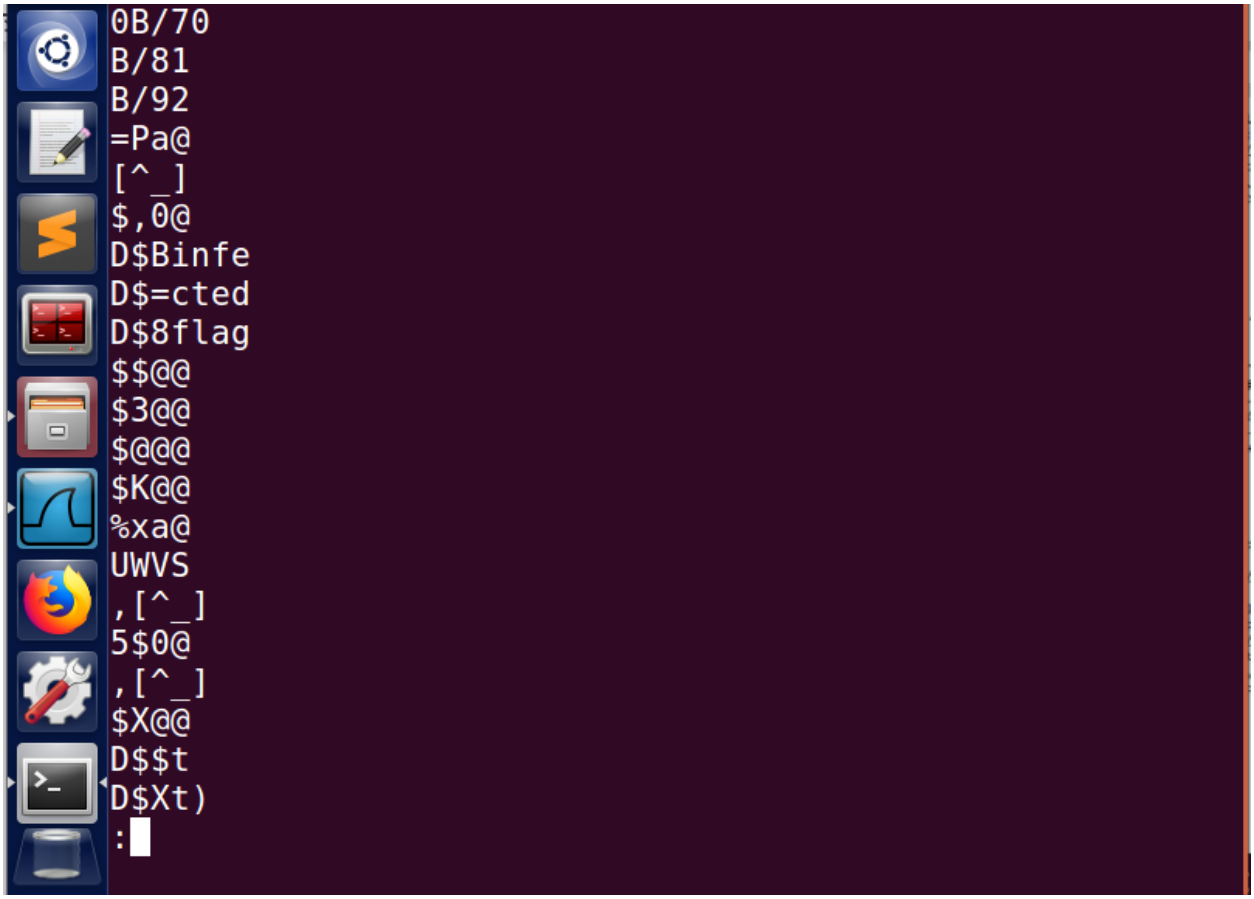
The creator tag had the creator name as ClippyHasReturned. This was like the picture seen in the PDF if we open it in PDF format itself.

The creator named “ClippyHasReturned” created this PDF file.

Level 3 – Split Ends

In this task, we must find the compiled flag. We are given with the exe file. I tried to open in text Notepad++ and Photos application. It did not work. I was not able to find anything. So I tried the strings command to find the flag.

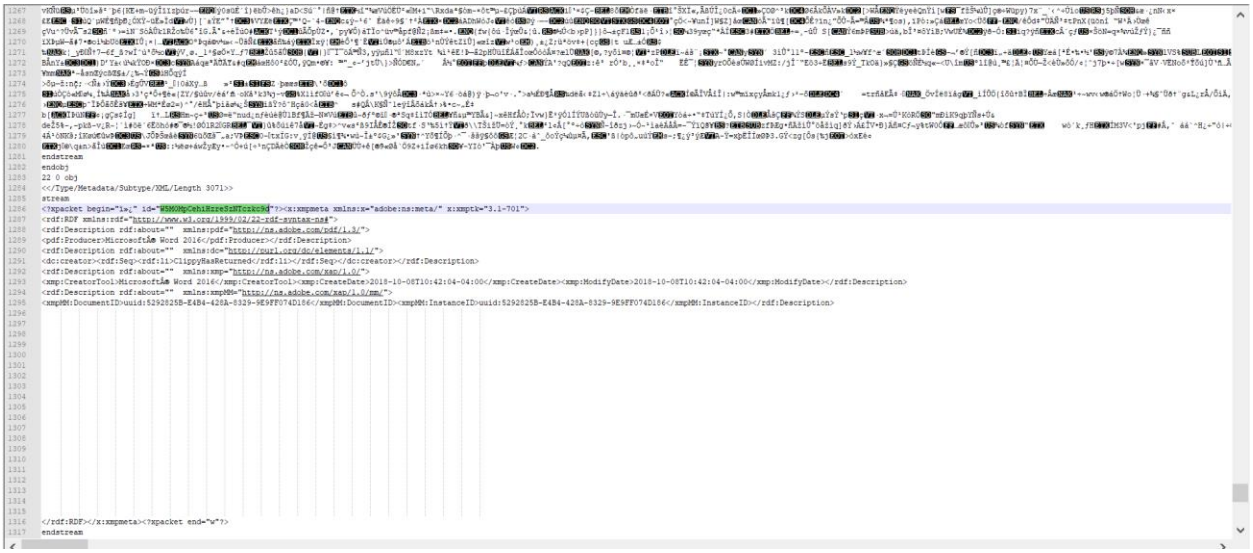




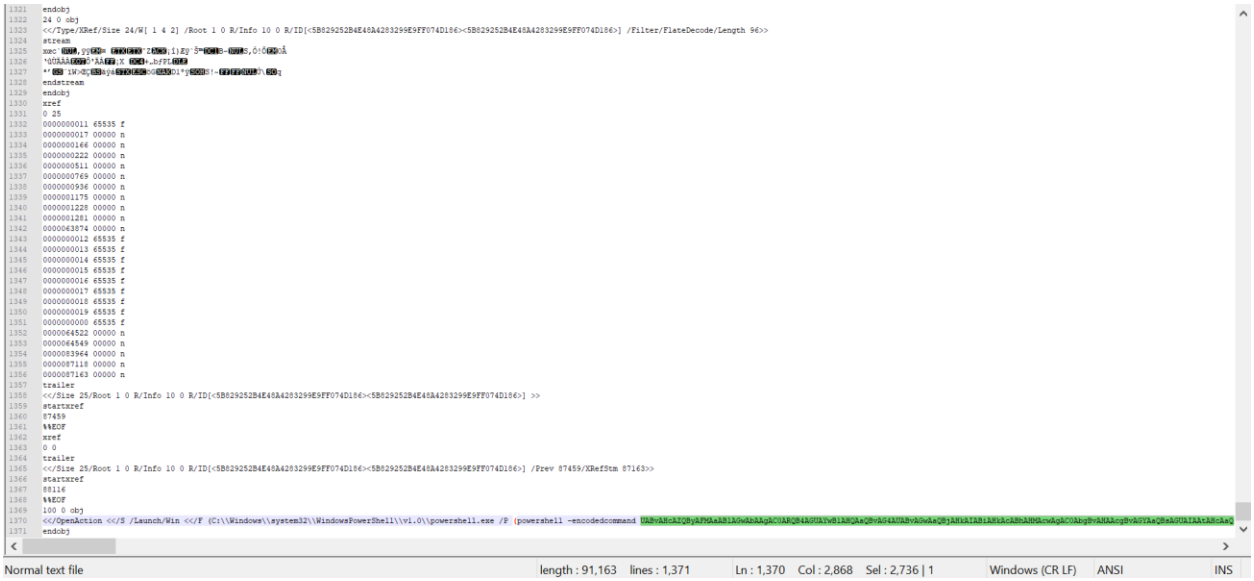
When we keep on moving through the file, we can see the text “infected flag” towards the end of the strings split in 3 parts. This is like the hint SPLIT ENDS given to us. The compile flag is infected flag as shown in the screenshot.

Level 4 – The PDF Your Parents Warned You About II

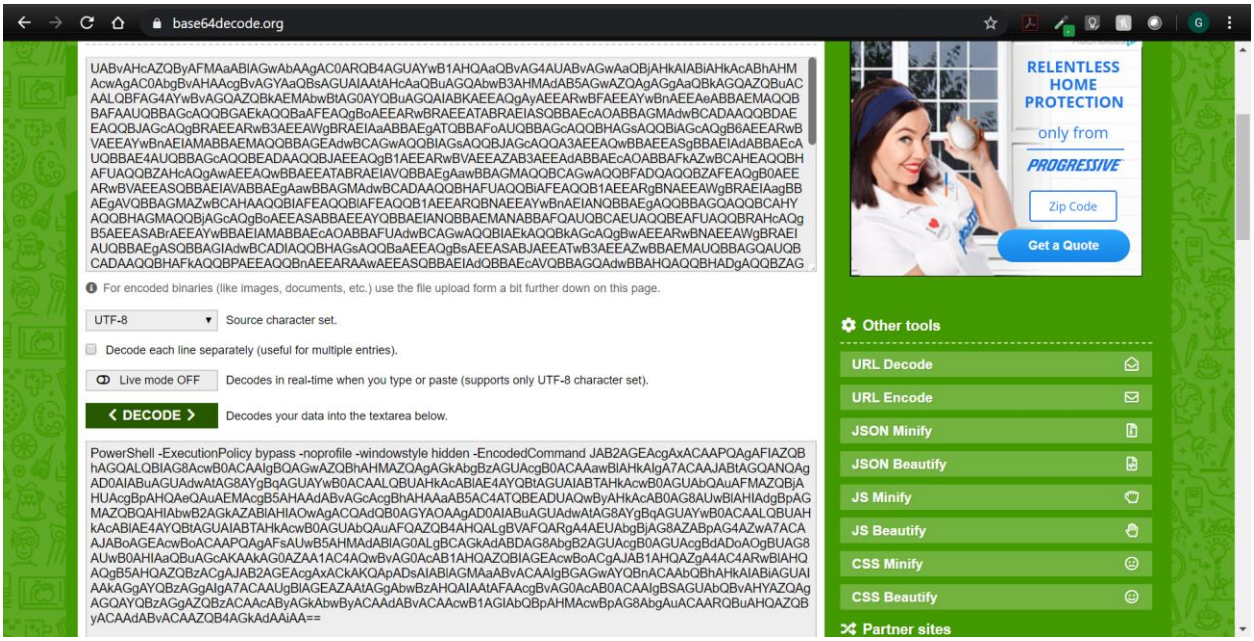
In this task we must find the hidden flag from a PDF file. If we open the PDF in a text editor like Notepad++, we will be able to see an id field which is W5M0MpCehiHzreSzNTczkc9d as shown in the screenshot.



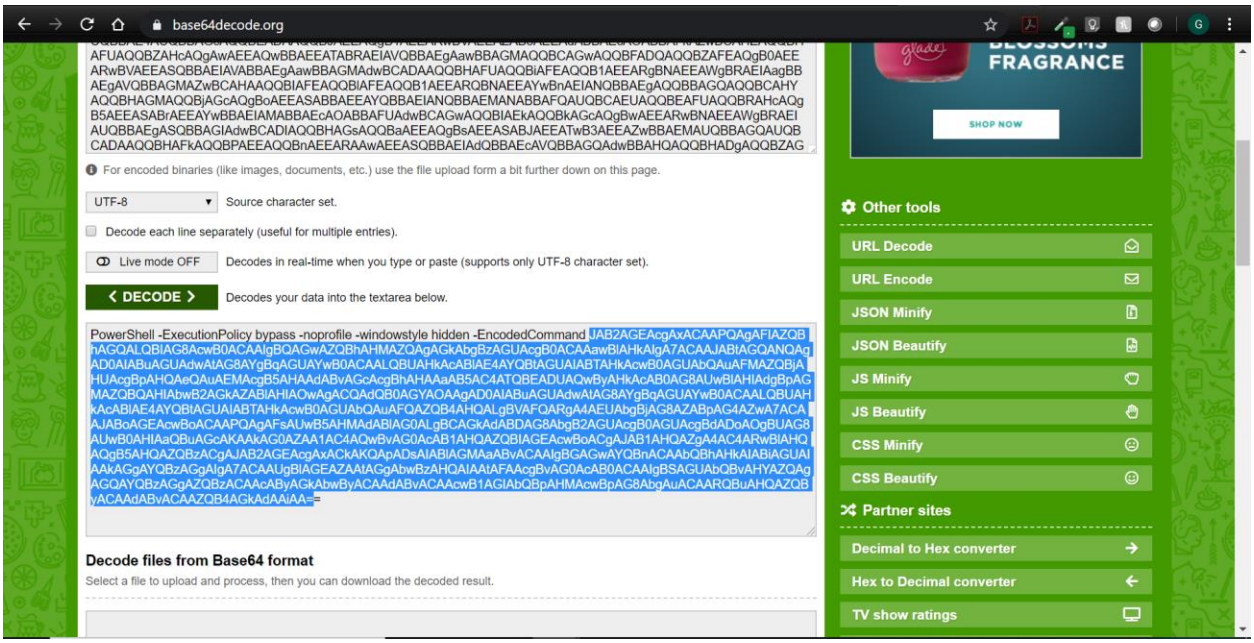
When we go towards the end of this file, we see a powershell path and a huge string as shown in the screenshot below.



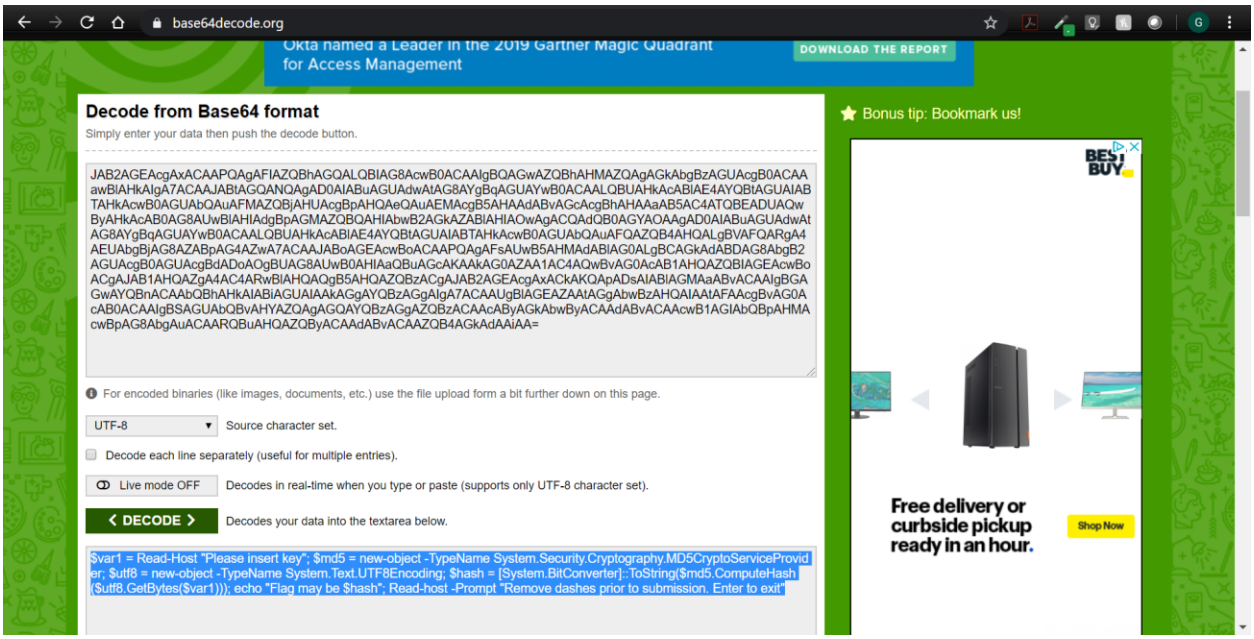
We try to decode this string in a base64 decoder.



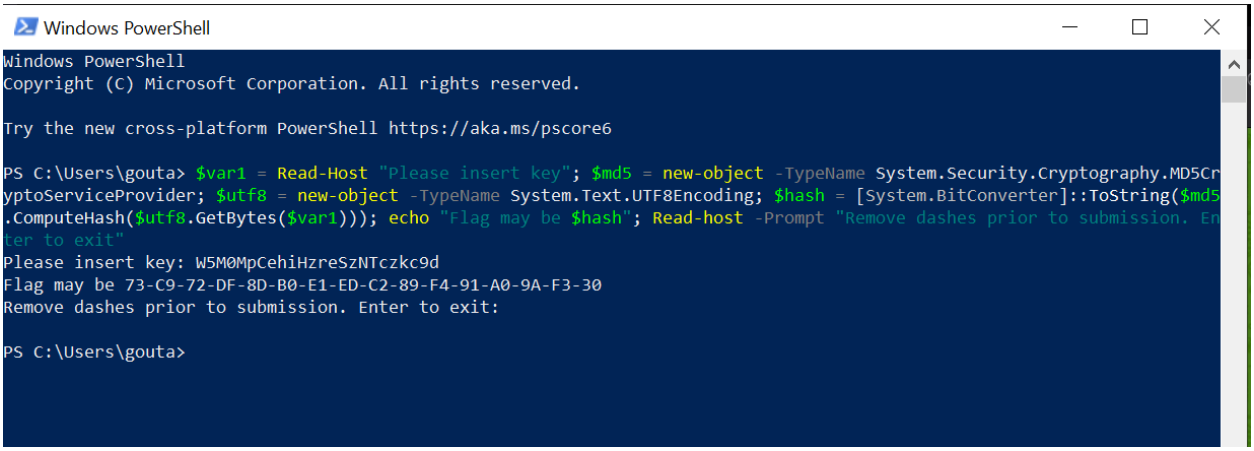
When we decode this huge string, we get another string as highlighted below.



We try to decode this string again in base64 decoder and we get a code as highlighted in the screenshot.



By opening the PDF in Notepad++, we know that this string is for a powershell path. So we enter this code in powershell. It asks to insert a key. For this key, we enter the id field value W5M0MpCehiHzreSzNTczkc9d which we got initially.



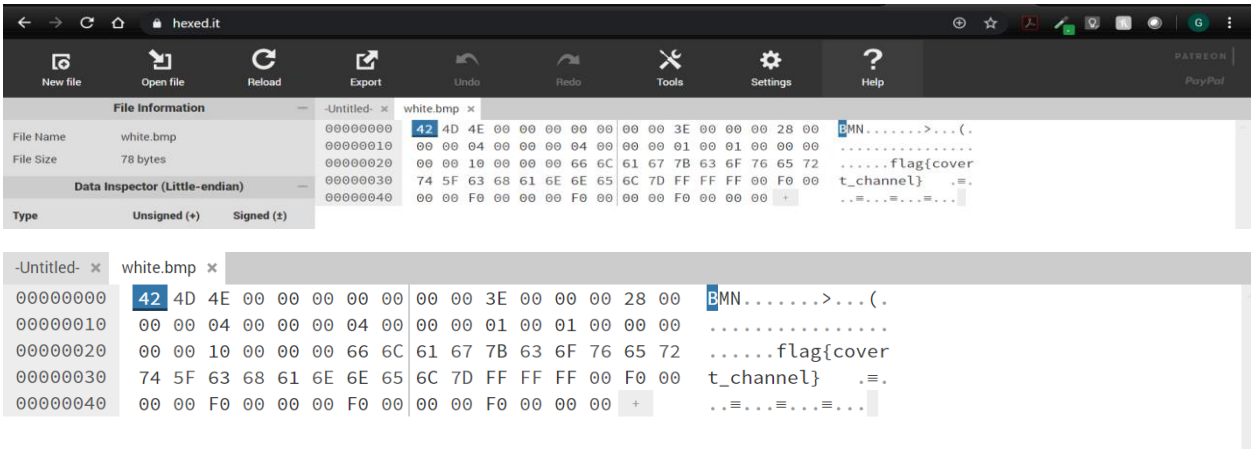
If we enter this vid value, we get the hidden flag 73-C9-72-DF-8D-B0-E1-ED-C2-89-F4-91-A0-9A-F3-30 as shown in the screenshot. We remove the dashes as instructed and it becomes 73C972DF8DB0E1EDC289F491A09AF330

Level 5 – Rock Scissors Paper Lizard Spock

Steganography

Level 1 – Moo Cow

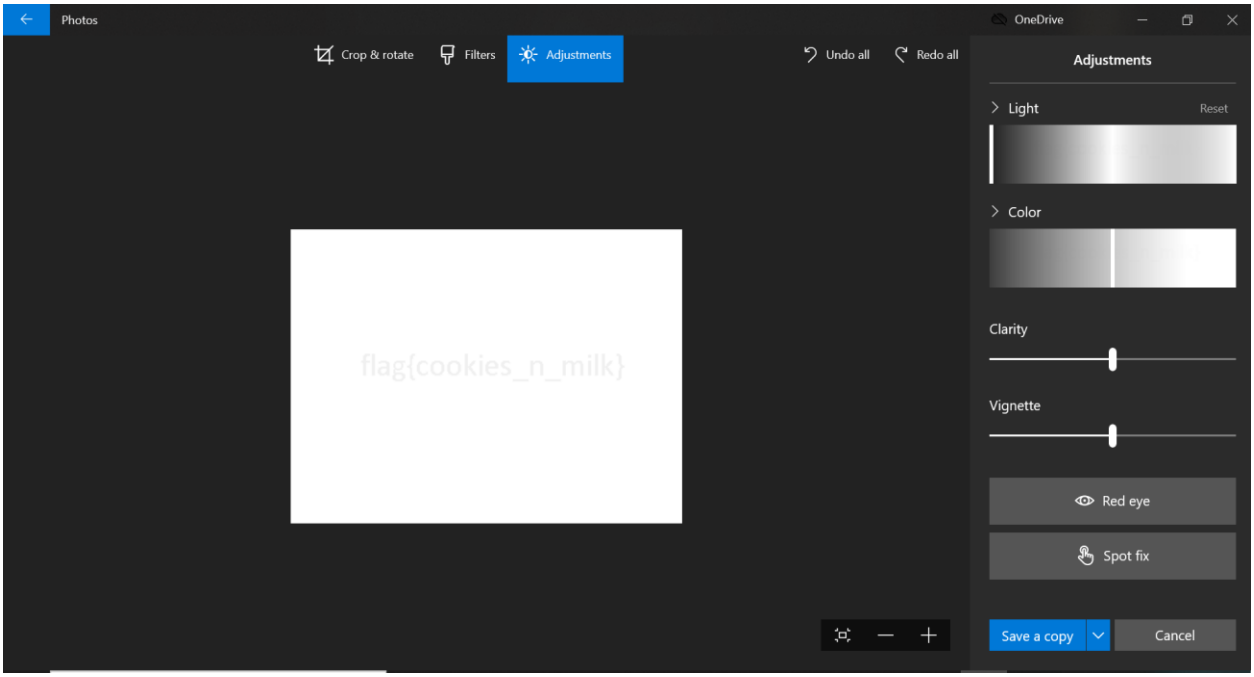
In this task, we must find the flag from bmp file given to us. I tried to open the file in text editor, Notepad++ and Photos application but I was not able to find anything. Then I opened the bmp file in an online hex-editor.



As shown in the screenshot, when the bmp file is opened in a hex-editor, it shows flag{covert_channel}. This is the flag we were supposed to find.

Level 2 – Milk Run

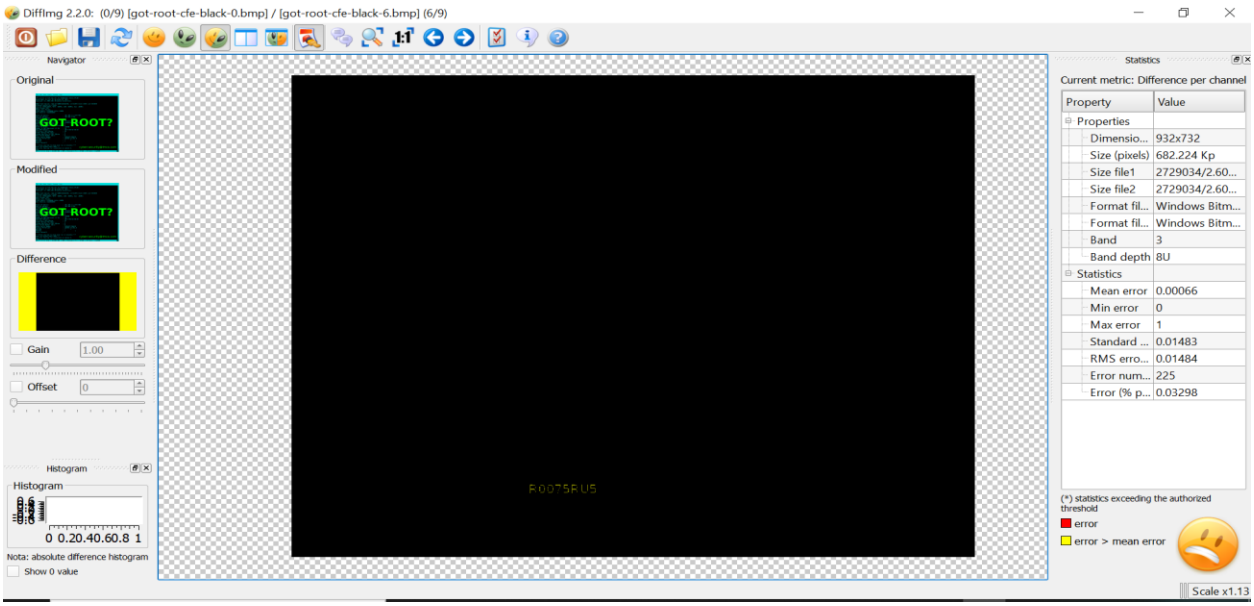
In this task, we must find the white flag in the image of white cows in a snow field.



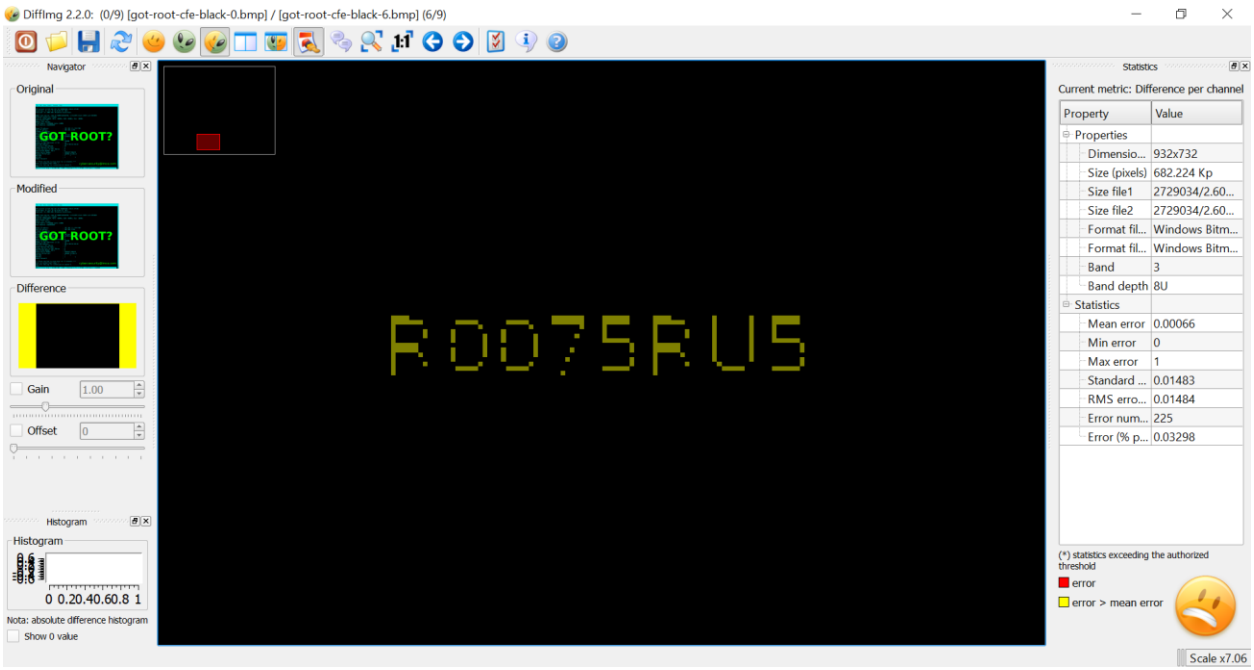
We have been given bmp file. So I opened the bmp file in Photos application. From the hint, I found that flag was white in color. So I made adjustments in the Light. From the screenshot, we can see flag{cookies_n_milk}. This is the white flag we were searching for.

Level 3 – Got Root

In this task, we must find which one of the pics given to us has the hidden password. When I opened the images in Photos application, all the images looked the same. So, I guessed that there might be some difference in the pics.



I googled for the software that finds differences between images. I found the DiffImg software. I used this to compare each image with one other image. By following a Brute force method, I found that there was a difference between Image 0 and Image 6.

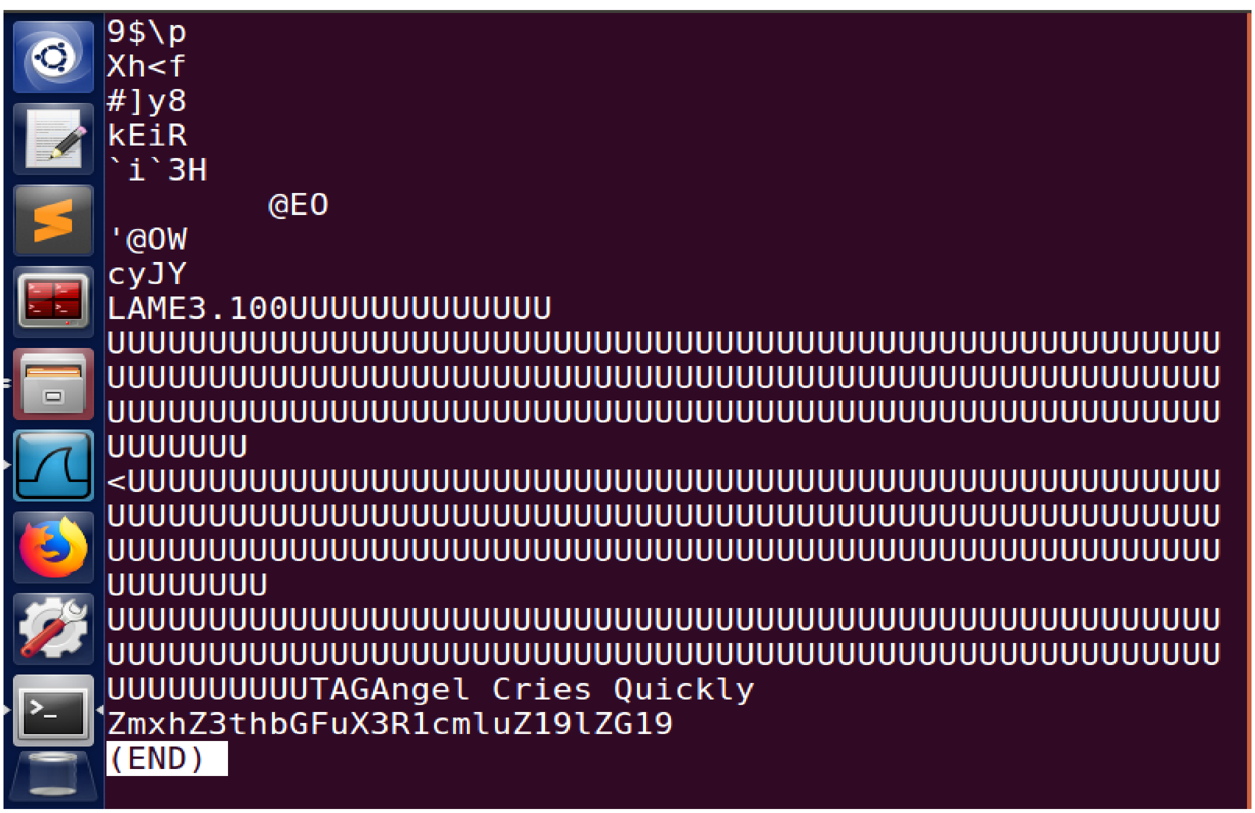


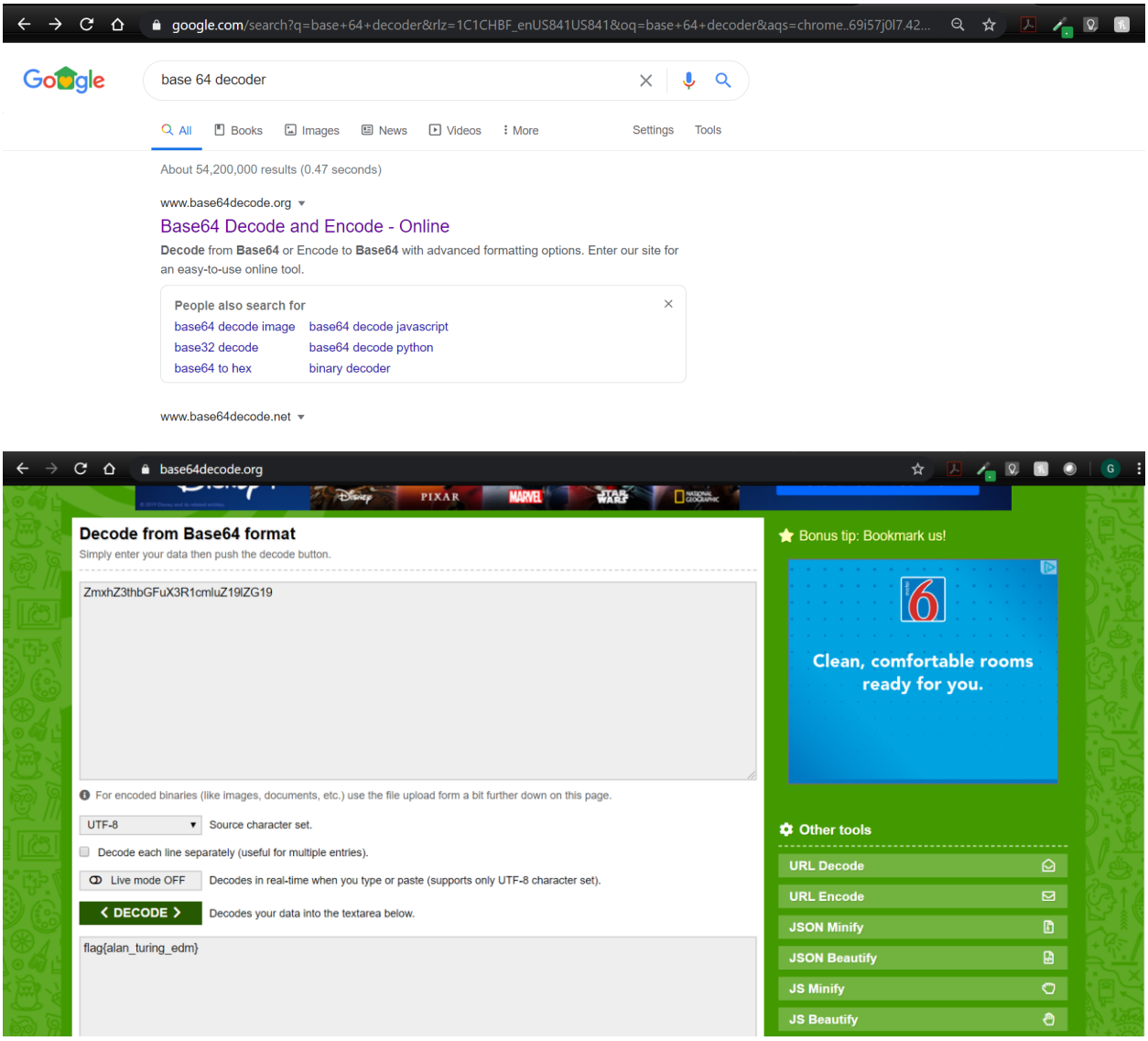
As shown in the screenshot, we could find some code written in the image. When I zoomed I could see the password R0075RUS. This is the flag that we were supposed to find.

Level 4 – AI EDM

In this task, we have to find the hidden flag in the mp3 file given. I opened it in mp3 format itself, but heard only music. So I opened with text editor Notepad++, Photos application and PDF. I was not able to find the flag.

Then I opened with strings command from the command prompt. I browsed through the entire file and I could not find any flag. But I found a string at the end of the file. I browsed the string online to find that it is of the base64 format.





As shown in the screenshots, I tried to decode the base 64 format online and I finally got a flag that was written as flag{alan_turing_edm}. This is the flag we were supposed to find.

Level 5 – Final Frontier