CSE 5382: Secure Programming - Fall 2018 **Student Name**: Biswa Ranjan Nanda

Capture the Flag Bonus Exercise **Student ID**: 1001558251

# Flag Table

Place the flags once you find them in the appropriate table entries below. Each category has a maximum of 20 points with each higher level of difficulty granting an increasing number of points. Maximum score for all challenges completed is 100 points.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Cryptography** | **Malware** | **Network Capture** | **Reverse Engineering** | **Steganography** |
| **Level 1 (2 Points)** | flag{backoff\_malware} | flag{sandworm\_apt} | M0d1c0nF14G | lm | flag{convert\_channel} |
| **Level 2 (3 Points)** |  | 2e1afcef9baa15b8db764274b0e45d3f | admin |  | flag{cookies\_n\_milk} |
| **Level 3 (4 Points)** |  | flag{duqu\_aint\_dooku} |  | flag{infected} |  |
| **Level 4 (5 Points)** |  |  |  |  | flag{alan\_turing\_edm} |
| **Level 5 (6 Points)** |  |  |  | flag{Sacako iph} |  |

# **Explanation of Approaches**

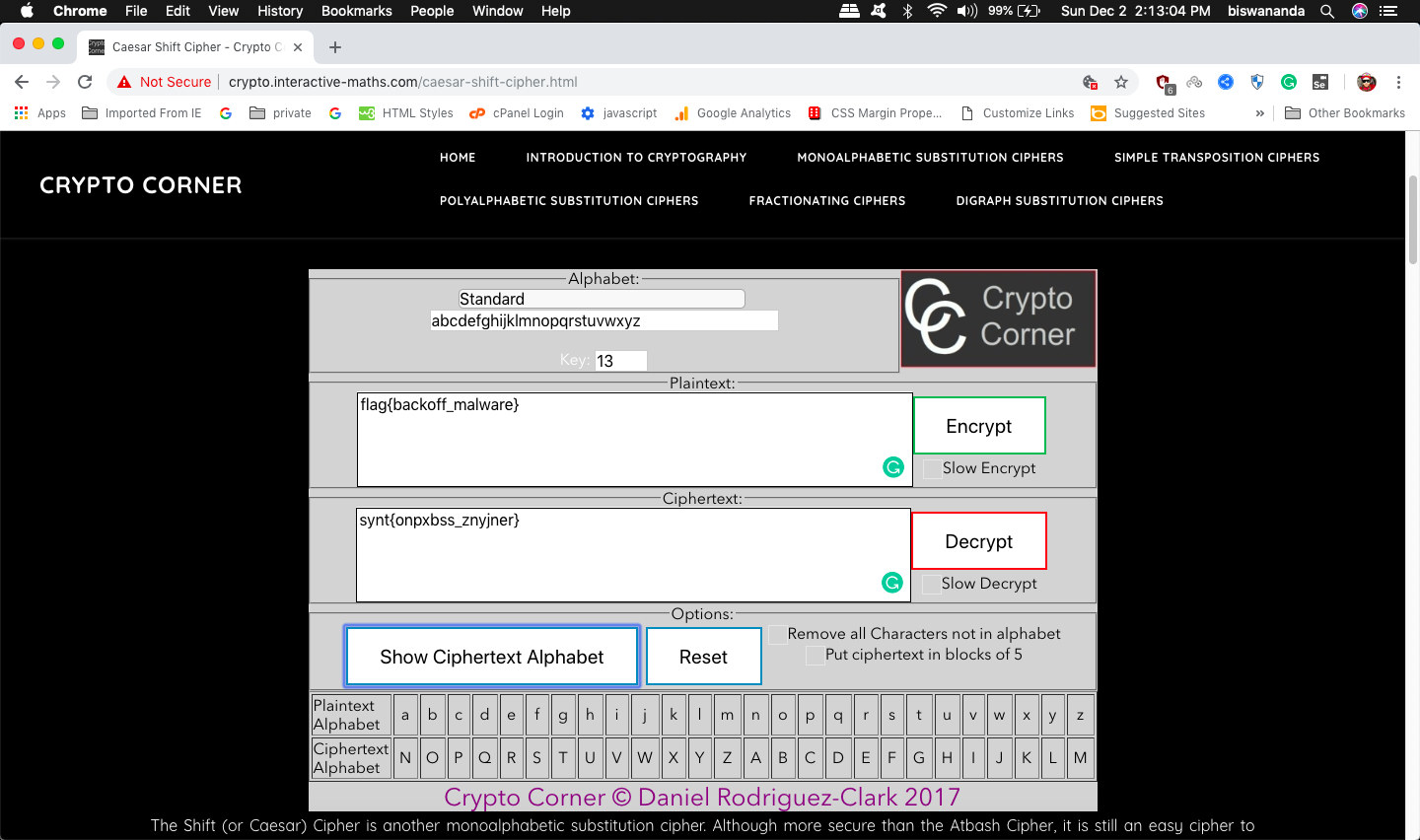
Include descriptions along with screen shots of the approaches you took to solve these challenges.

## **Cryptography**

### **Level 1 – Orange Julius**

### I went to the website for crypto.interactive-maths.com/Caesar-shift-cipher.html and used our instruction to decrypt the same with key as “13”. Screenshot is mentioned below.

### Flag - flag{backoff\_malware}



### **Level 2 – Block Chain**

### **Level 3 – DASH DOT COM**

### **Level 4 – VIII A Small Example**

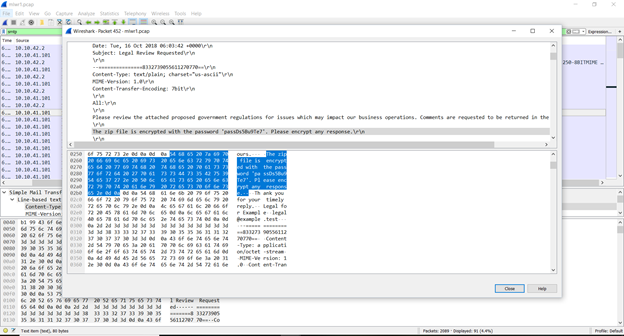
### **Level 5 – Big Blue Randu**

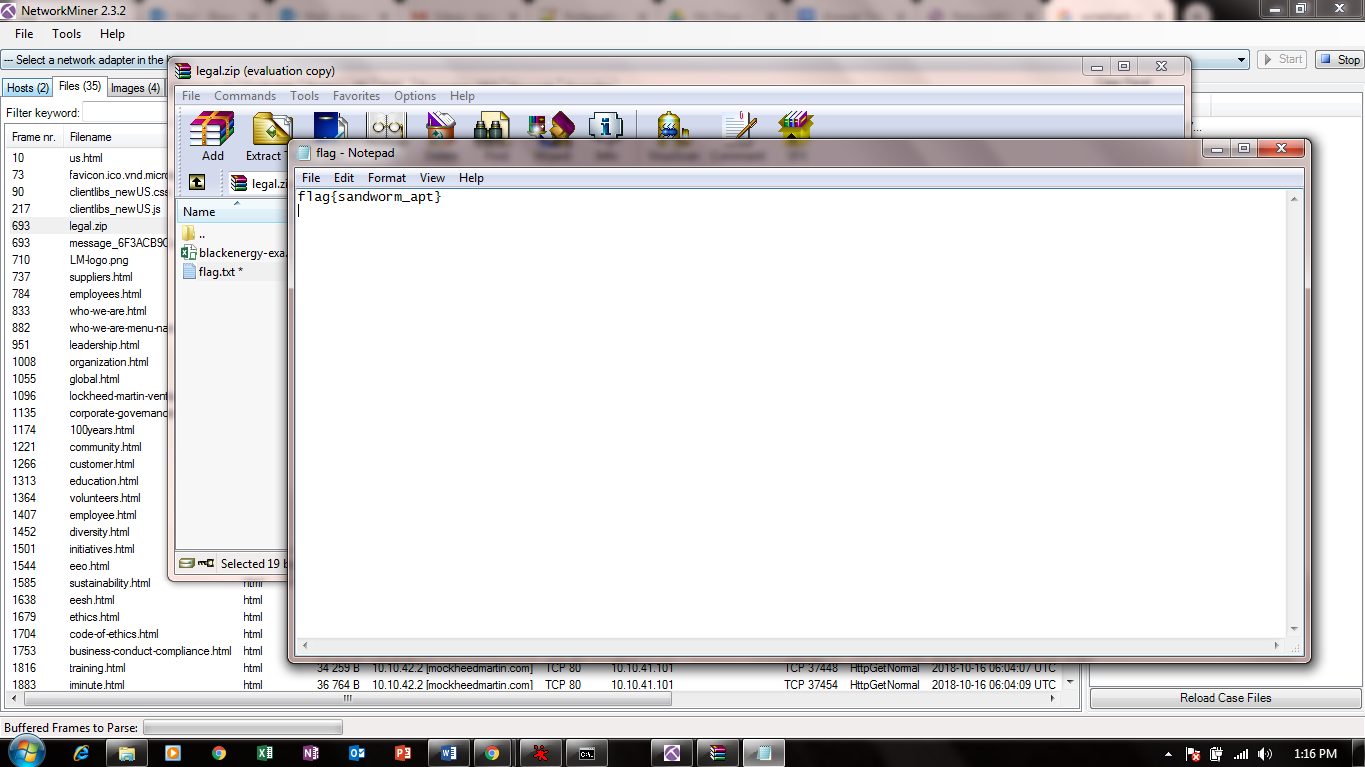
## **Malware**

### **Level 1**

Using Wireshark we open the file to check the password and using the same password, then using Networkminer, the legal.zip file is extracted and using the previous password for the flag.txt to get the flag.

Flag: flag{sandworm\_apt}

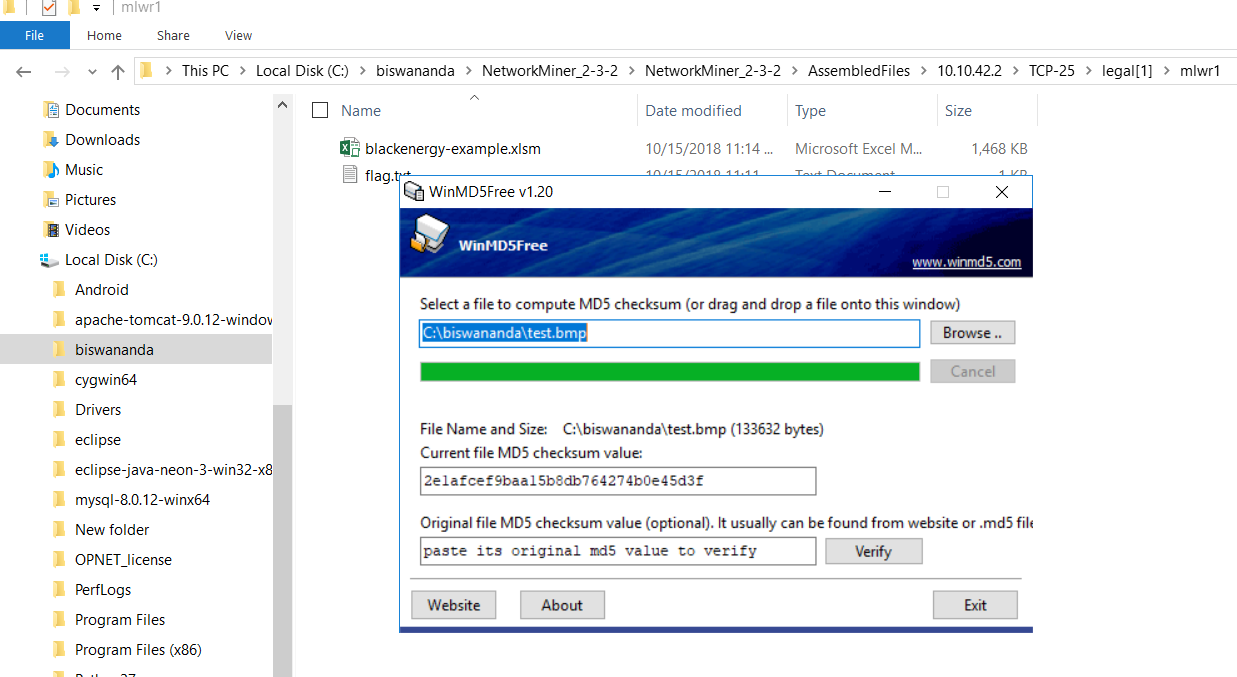




### Level 2

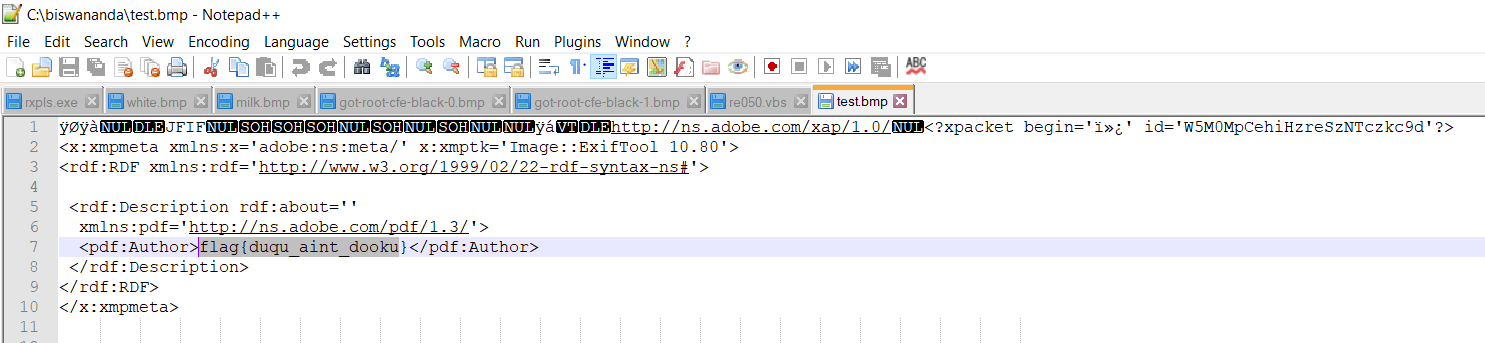
Using WinMD5 to get the md5 value of the image that is dropped from the excel file.

Flag - 2e1afcef9baa15b8db764274b0e45d3f



### **Level 3**

Open the image file dropped from excel, and open it using notepad++.



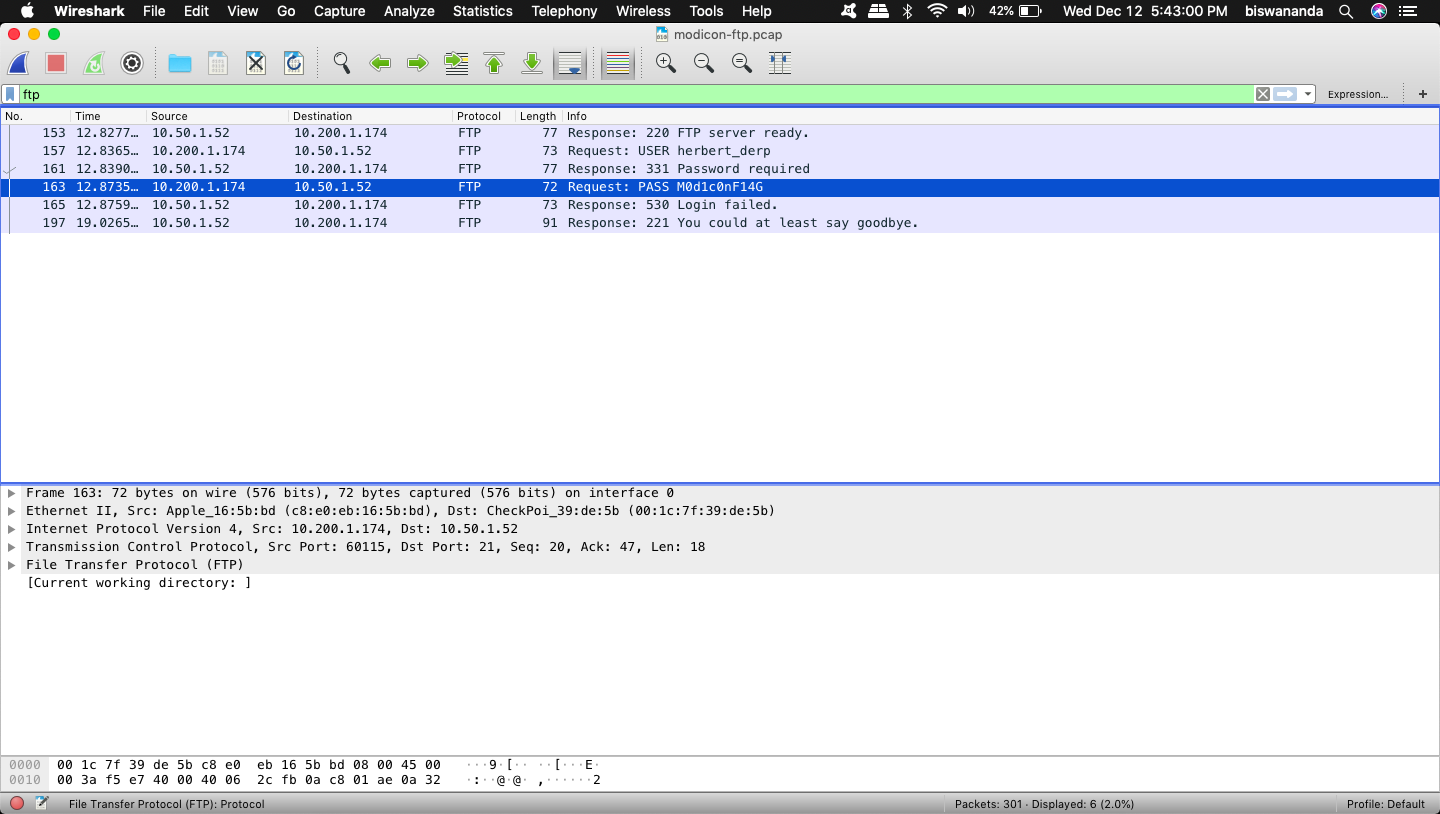
### **Level 4**

### **Level 5**

## **Network Capture**

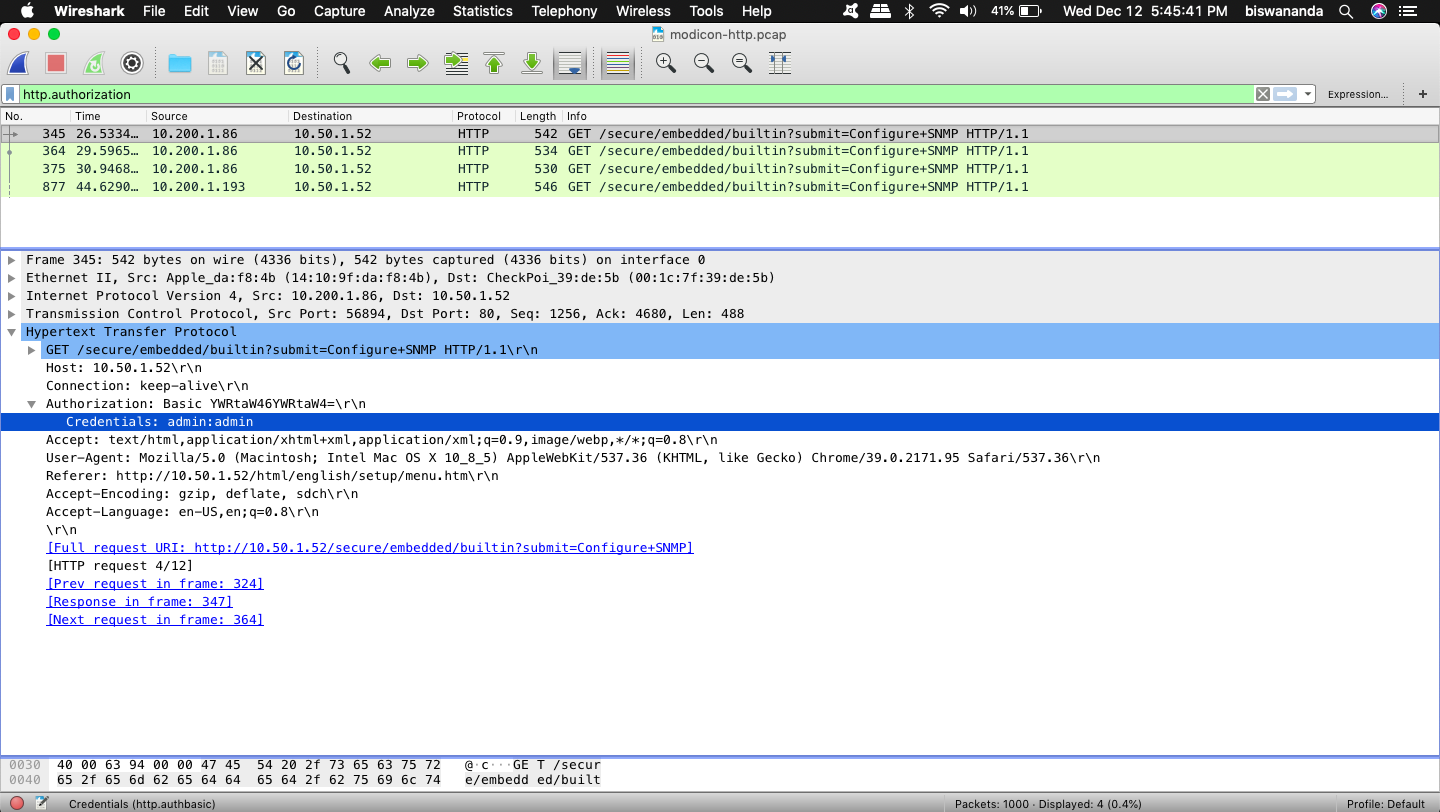
### **Level 1 – Modicon-FTP**

Using Wireshark, Open the capture and filter for “ftp” because of title of the task, I got to see the password and I have highlighted the same.



### **Level 2 – Modicon-HTTP**

Open the capture using Wireshark, I have used “http” filter, to filter out http packets, by the hint I opened the packet which was denied authorization, In the Authorization part there is encrypted string, using basic 64 decoder I captured the flag and the wrong password is admin.



### Level 3 – WinXP-HAVEX

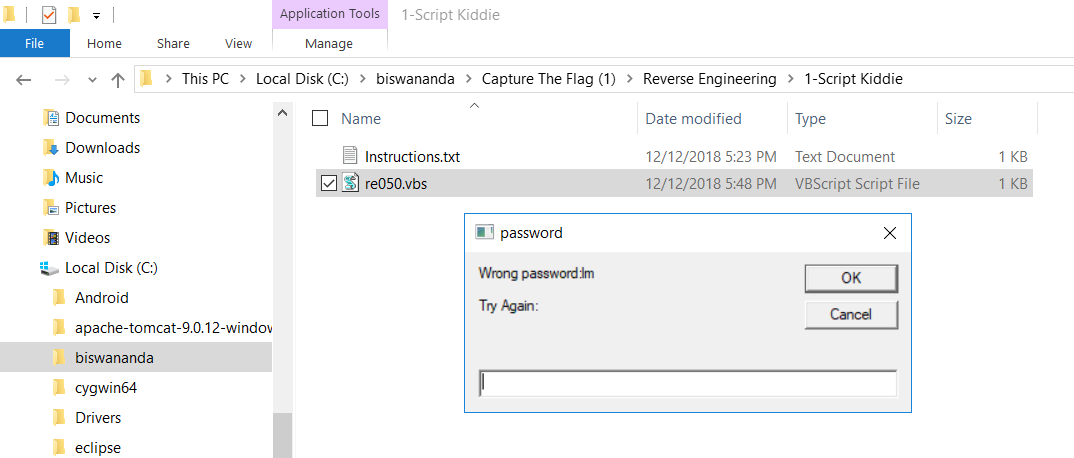
### Level 4 – MICROLOGIX56

### Level 5 – BACNET-COVERT

## Reverse Engineering

### Level 1 – Script Kiddie

Making changes in the string compare of program code, we get to know correct password “lm”.



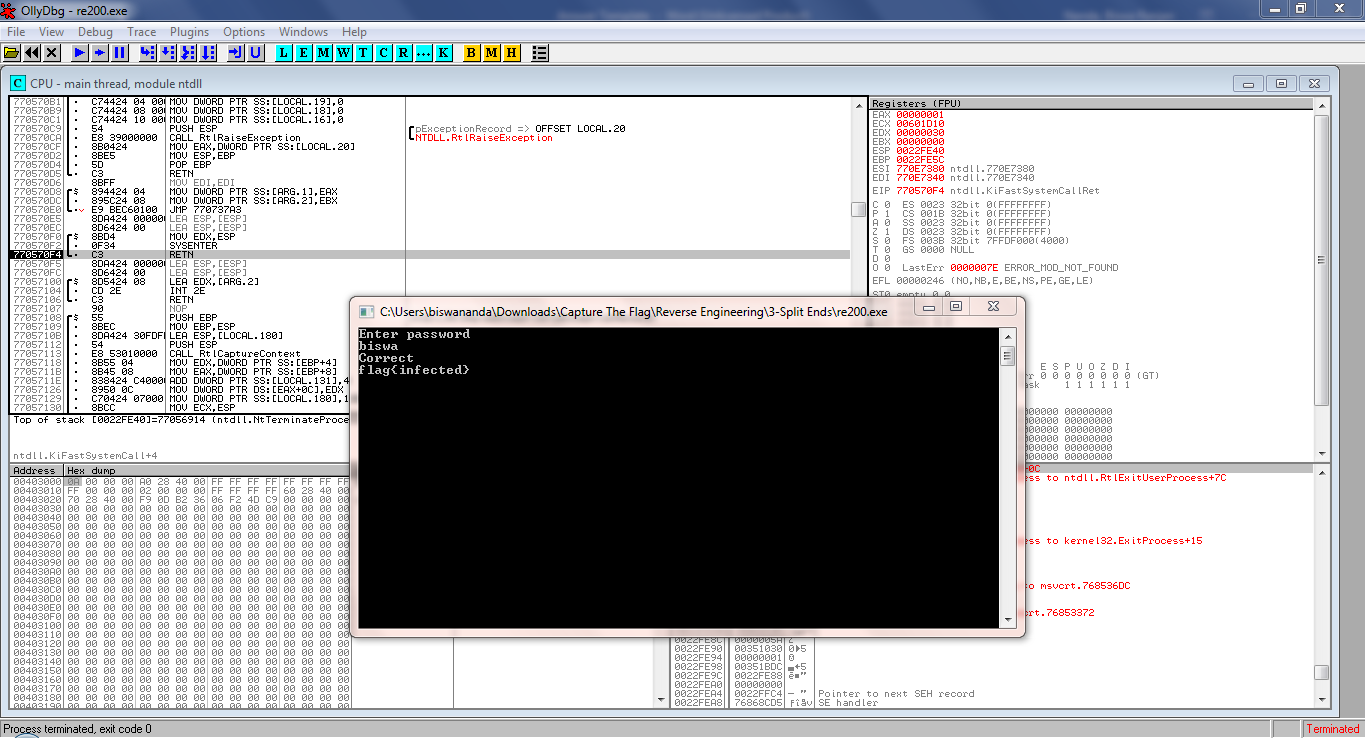
### **Level 2 – The PDF Your Parents Warned You About I**

### **Level 3 – Split Ends**

Using olly debugger v2.0, and open the application, run the program, search for the password string comparison line and make some changes in the code as a jump statement to the “*correct*” line, by which we can get the flag.

Flag - flag{infected}

Tools : VMWare, windows 7, ollydebugger tool



Reference: 1) http://www.ollydbg.de/download.htm

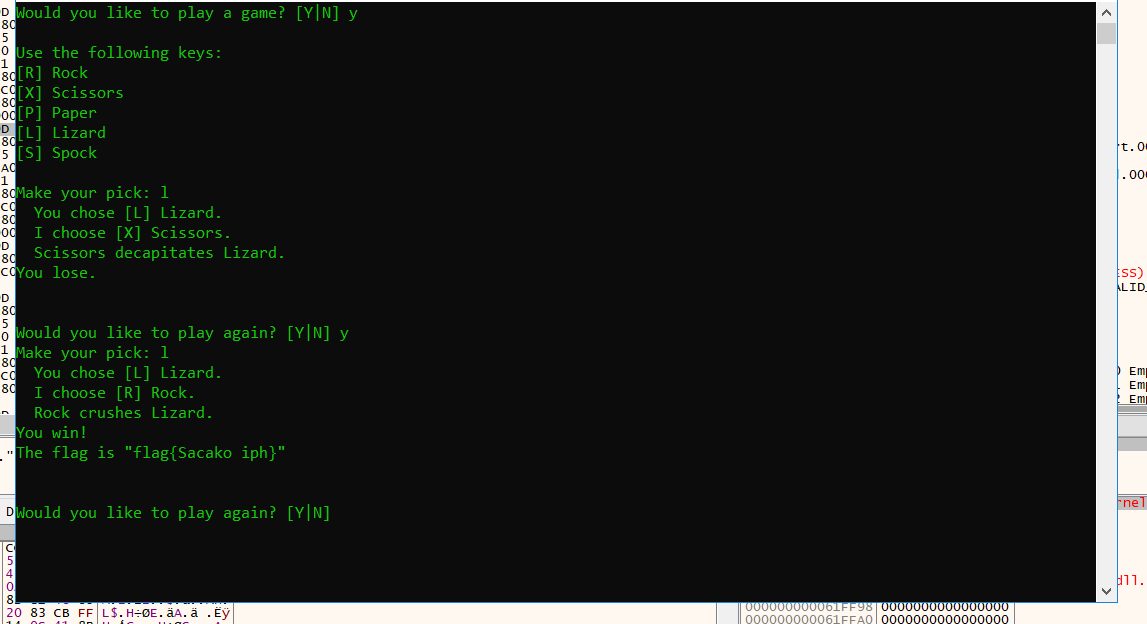
2) http://www.ollydbg.de/version2.html

### **Level 4 – The PDF Your Parents Warned You About II**

### **Level 5 – Rock Scissors Paper Lizard Spock**

Used debugger to view the machine code, making the changes using jump statement from Lizard to the win statement, I got the flag. In short editing the machine code.

Flag - flag{Sacako iph}

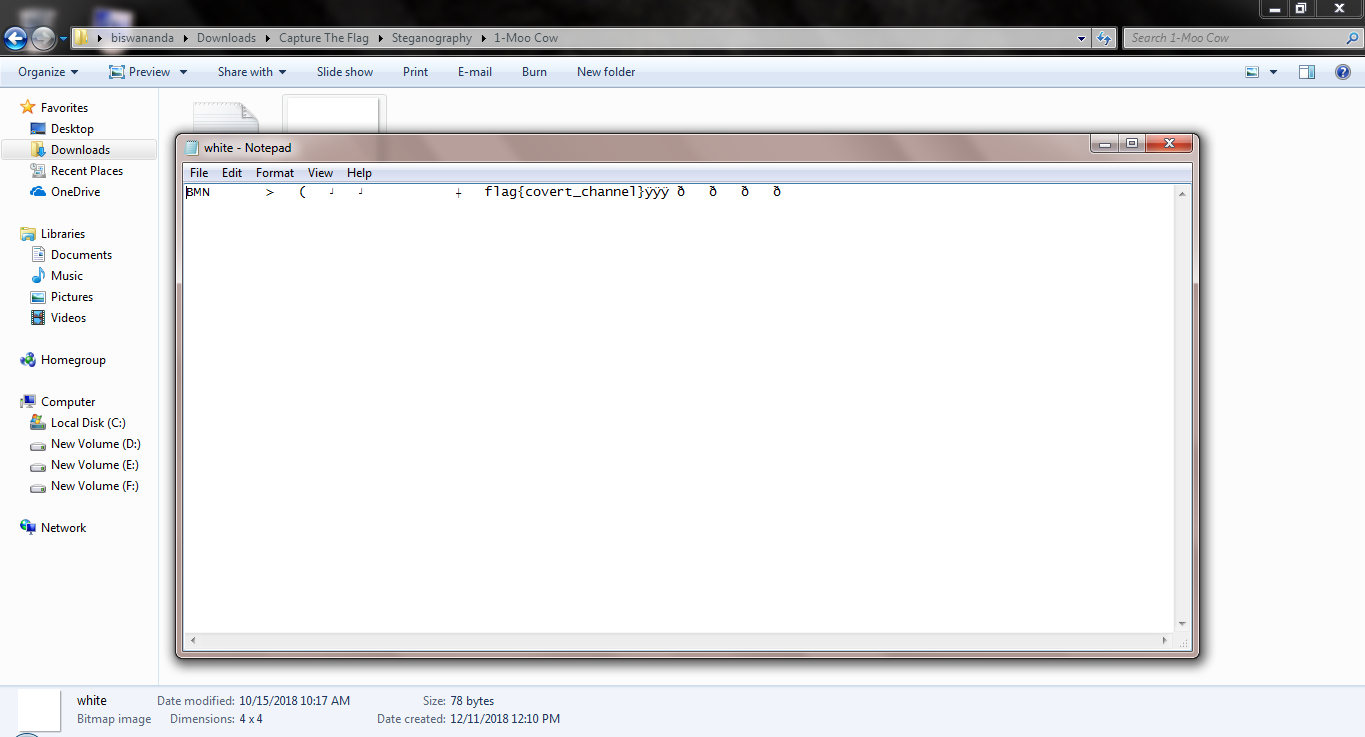


## **Steganography**

### **Level 1 – Moo Cow**

Simply open the image with notepad.

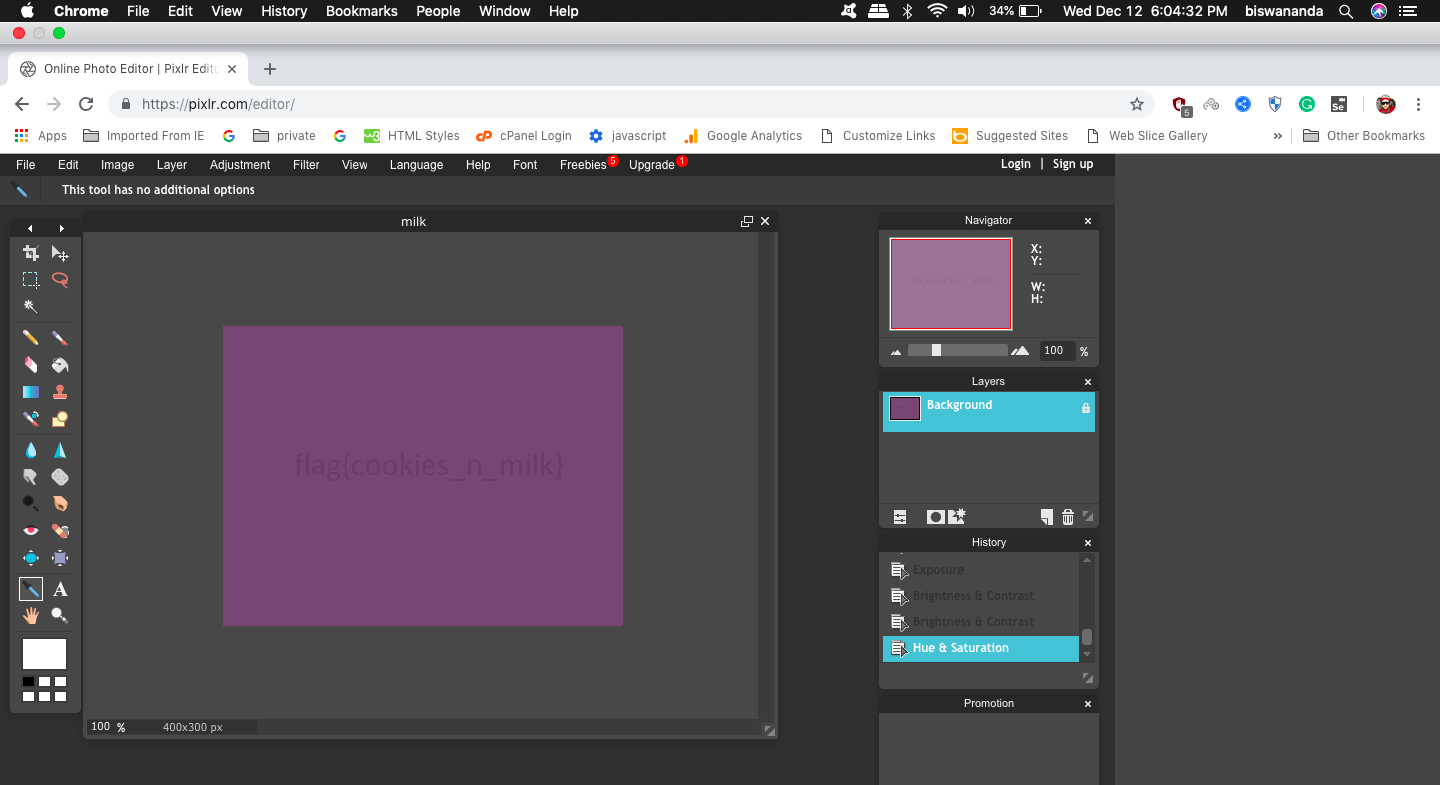
Flag - flag{convert\_channel}



### Level 2 – Milk Run

Open the image with photo editor and do the adjustments in brightness, contrast,shadows, Hue etc You’ll see the flag.

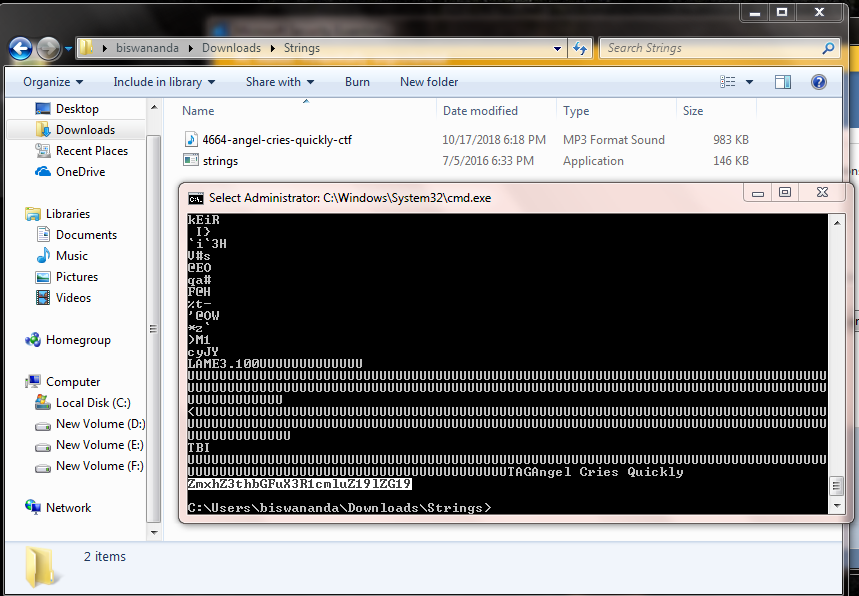
Flag - flag{cookies\_n\_milk}

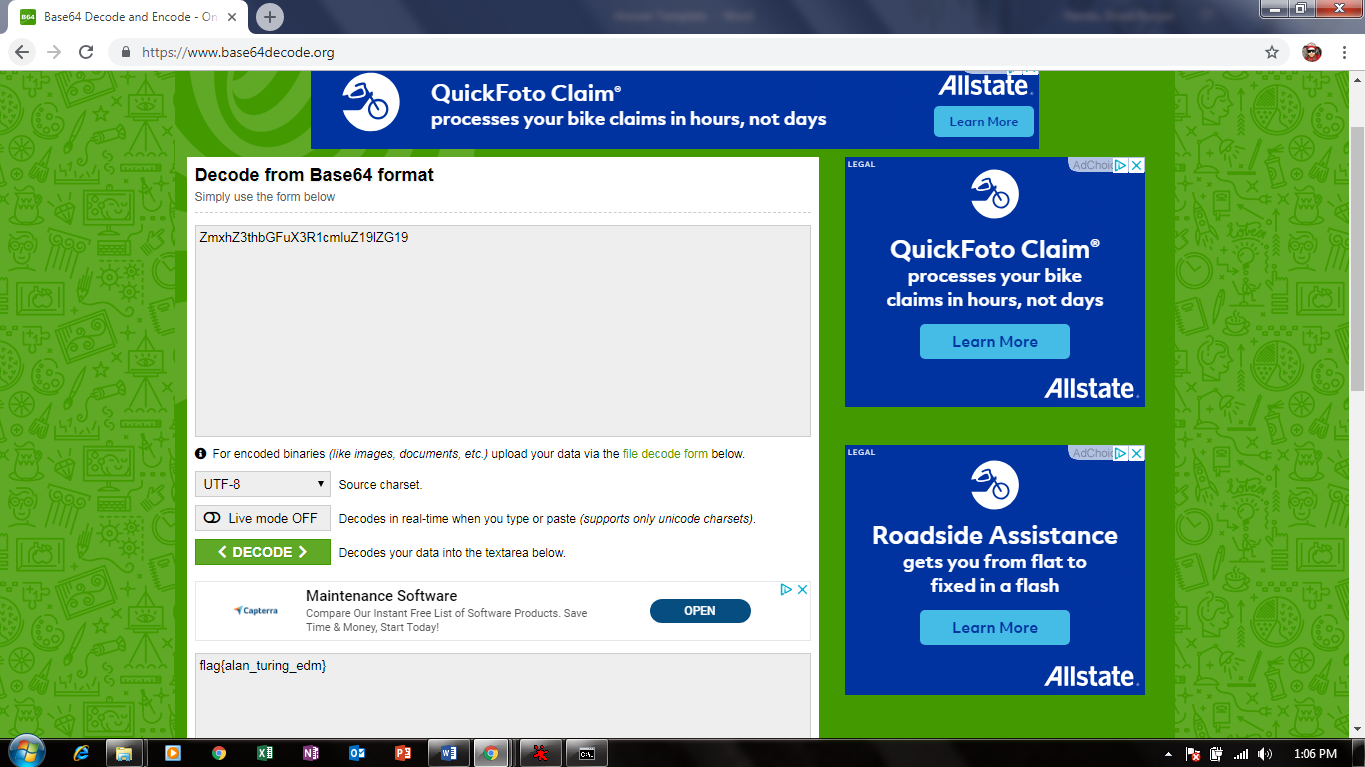


### Level 3 – Got Root

### Level 4 – AI EDM

I used Strings command from command prompt, and the encrypted data is seen, decrypting same with basic 64 decoder I got the flag.





### Level 5 – Final Frontier

**Note:** Screenshots are taken using both Macbook Air and Windows Laptop, due to the unavailability of some softwares like x64 debugger, Olly debugger, Networkminer are not available for Macbook.