Challenge Name: Fraudulent

Category: Forensics
Difficulty: Medium
Developer: Aman Jain

Description: I got ditched by someone and I need your help!!!

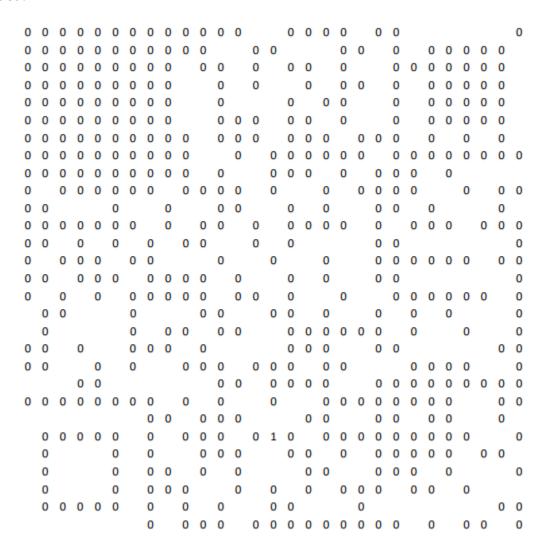
The bill amount that was charged to me was not correct. The image of the bill was corrupted. Sources said that some PIXELS of the image were FORRENSICALLY manipulated or edited, Leading to changes in the total bill amount.

You have to reach the image to see what happened. Remember to analyze every pixel of the Image carefully.

Flag Format: VishwaCTF{actual_total_amount}

P.S.: Round off the actual total amount to the nearest integer value.

Files Provided:

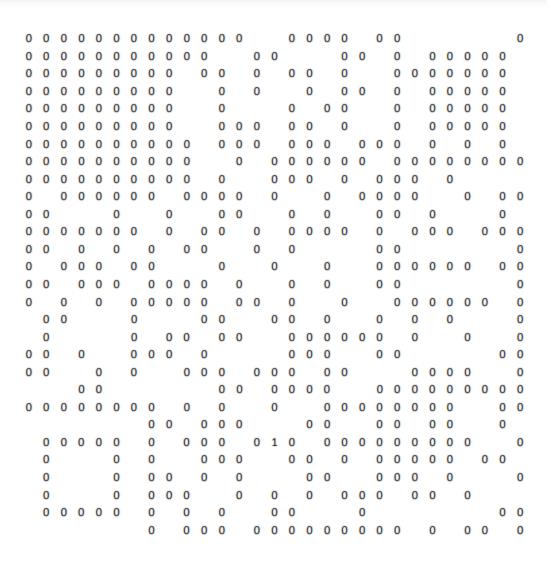


Write Up-

1. After getting the frames of the gif we get the idea that it's a QR code with 1's representing Black and 0's representing white pixels and it is a 29X29 version 3 QR.

Frames:

														1	1					1			1	1	1	1	1	1	
												1	1			1	1	1			1		1						1
										1			1		1			1		1	1								1
										1	1		1		1	1		1			1		1						1
										1	1		1	1	1		1			1	1		1						1
										1	1				1			1		1	1		1						1
											1				1				1				1		1		1		1
											1	1		1							1								
											1		1	1										1		1	1	1	1
		1							1					1			1												
			1	1	1		1	1		1	1			1	1		1		1	1			1		1	1	1		1
1								1		1			1		1					1		1				1			
			1		1		1		1			1	1		1									1		1	1	1	
1		1				1			1	1	1		1	1		1	1		1	1							1		
			1				1					1		1	1		1		1	1			1	1	1	1	1	1	
		1		1		1						1			1													1	
1				1	1	1		1									1		1	1		1		1		1	1	1	
1			1	1	1	1		1			1			1	1							1		1	1		1	1	
			1		1	1				1		1	1							1			1	1	1	1	1		
			1	1		1		1	1				1				1			1	1	1					1	1	
1	L	1	1			1	1	1	1	1	1			1					1	1									
									1		1		1	1		1	1									1	1		
1		1	1	1	1	1	1			1				1	1	1			1	1			1			1	1		1
1	L						1						1				1										1	1	
1			1	1	1		1		1	1				1	1			1		1									
1	L		1	1	1		1			1		1		1												1	1	1	
1	L		1	1	1		1															1			1		1	1	1
1	L						1		1		1		1	1			1	1	1		1	1	1	1	1	1	1		
1		1	1	1	1	1	1		1				1										1		1			1	



2. Taking any frame to construct the QR ultimately leads to nothing cuz the QR code seems to be incomplete.



3. Googling about the QR code, we can find ways to construct it back.

- 4. One of the articles is https://www.robertxiao.ca/hacking/ctf-writeup/mma2015-qrcode/
- 5. Some things can be easily constructed like the position and alignment but still, it's not scannable. Looking at the QR we find that the format information and the timing are also corrupted and we need to fix it.
- 6. The format information is encoded twice. One instance is wrapped around the top-left Finder, and the other instance is split in half between the bottom-left and top-right Finder patterns. The format information consists of exactly 15 bits. Here are the bits we can see in our QR code: 110011000101111 i.e. ECC Level L, Mask Pattern 4.
- 7. And the timing can be easily corrected by putting alternate 1 and 0 wherever missing.



Final QR will be:

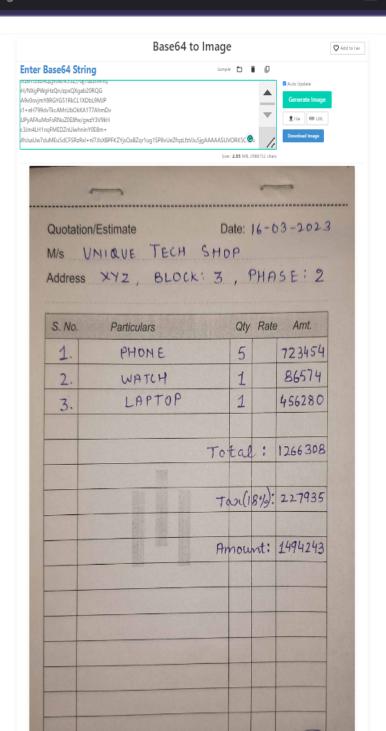


- 8. Finally, we can scan our QR which decodes to a GitHub repo.
- 9. There we find a base64 encoded file which is an image.
- 10. By decoding it, we get an image where we have to reach finally and analyze what is the issue with the amount.





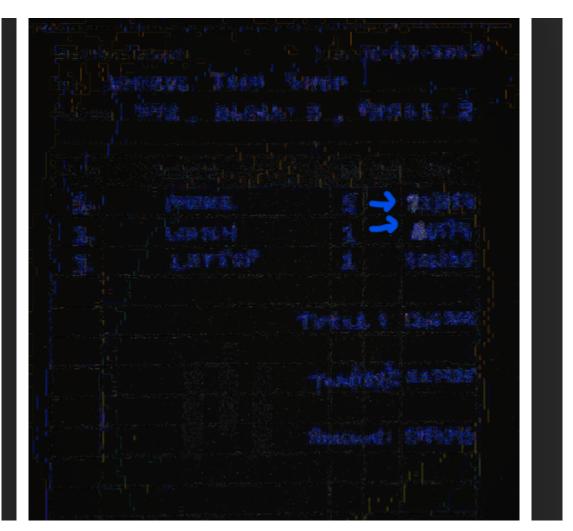




S. No. Particulars Qty Rate	insurates
	: 2
S. No. Particulars Qty Rate	: 2
- Canada	
1. PHONE 5 72	Amt.
	3454
2. WATCH 1 81	6574
3. LAPTOP 1 45	6280
Total: 126	6308
Tan(18%): 22	.7935
0	21 -1 -
Amount: 149	14243
	5
D. BY P. S. PKD. BY R.P. Signature	organ

- 11. The question has a hint about the software that was used to copy or edit the image for charging a false amount, it is <u>FORENSICALLY</u>.
- 12. Other tools can also be used to do the same.

13. In <u>FORENSICALLY</u> by adjusting the Error level analysis we were able to see easily that some figures are copied to other positions as well to change the total amount of the bill. The numbers were 7 and 8.



14. By removing them we can finally calculate the original amount with tax which is the flag.

Calculations: (23454 + 6574 + 456280) * 1.18 = 573843.44It is specified to round off to the nearest Integer in the question, the final amount will be 573843.

15. We have to submit the flag in the flag format VishwaCTF{573843}.