Issesion CTF 2023 Write Up

Michael N.

Team /root is proud to have come in 28th place in the ISSESSION CTF 2023 with a total of 546 points! We worked hard to take on the challenges presented to us and were able to demonstrate our skills and knowledge in cybersecurity. Despite the difficulties, our team remained determined and found success. In this write-up, we will discuss the strategies and techniques we utilized to solve the challenges, as well as provide an overview of our overall experience. We hope this write-up will be useful to other teams competing in the future.

List of Flags

Challenge	Category	Value	Time
[KPMG] Very Simple OSINT	OSINT	30	January 14th, 10:53:22 AM
Vacation Spot	OSINT	30	January 14th, 11:18:33 AM
Basic Permissions	Beginner Zone	20	January 14th, 11:37:54 AM
Ghost File	Beginner Zone	20	January 14th, 11:51:11 AM
Crack Me	Beginner Zone	20	January 14th, 12:01:38 PM
Find my car Marty	OSINT	30	January 14th, 12:15:02 PM
Fileception	Beginner Zone	20	January 14th, 12:47:09 PM
Decontamination	MISC	56	January 14th, 1:54:20

			PM
Video-Rental-0	PWN	44	January 14th, 2:04:16 PM
VaultChallenge	REVERSING	30	January 14th, 2:45:25 PM
You Get What You Give	Forensics	30	January 14th, 6:55:33 PM
CryptoTools2 (CyberChef)	Cryptography	30	January 14th, 7:17:49 PM
CryptoTools1	Cryptography	30	January 14th, 8:32:28 PM
RSA_1	Cryptography	30	January 14th, 8:48:51 PM
1337	Cryptography	30	January 14th, 8:58:04 PM
The Man Who Sold the World	Cryptography	96	January 15th, 10:26:05 AM

[KPMG] Very Simple OSINT

I was new to CTFs and wanted to go for the challenges with the highest points, so the [KPMG] Very Simple OSINT challenge was a great choice.

FIGURE 1. [KPMG] OSINT

When tackling an OSINT challenge, I like to think of the world as a large database. This database contains entities, which are people, places, objects, and concepts. Each entity has attributes, for example, some attributes I was given about this entity(person) I was looking for in this challenge were they had a podcast and they were a KPMG partner, they also had 20+ years of experience, along with being ranked in the top 100 most influential people in government technology.

I needed to find a way to create a unique identifier with the attributes/facts I was given about the individual/entity.

Some insights I was able to draw using the provided information, a unique identifier could be created using all the provided information and combining them, using the attributes alone to search for the individual will lead me onto a goose chance with the result being very vague, for example searching for the individual by only using the attribute of them being a KPMG partner would return a bunch of different results since there are many different KPMG partners, but there is only one KPMG partner that has 20+ years experience, a Podcast, and was ranked in top 100 most influential people in government technology. What I wanted to accomplish was to filter my search result by creating a very specific Unique identifier to make the query return only

entities(people) who share all of these same exact attributes. For example, the identifier I used was "KPMG-Partner-Cyber-Leader-20+-Years-Digital-Government-Top-100".

Upon combining the attributes of the individual, a unique identifier was created which allowed me to narrow down my search within Google. The first result of my search was the individual's name on the KPMG website. From there, I had all the information I needed to submit my first Flag of the competition.

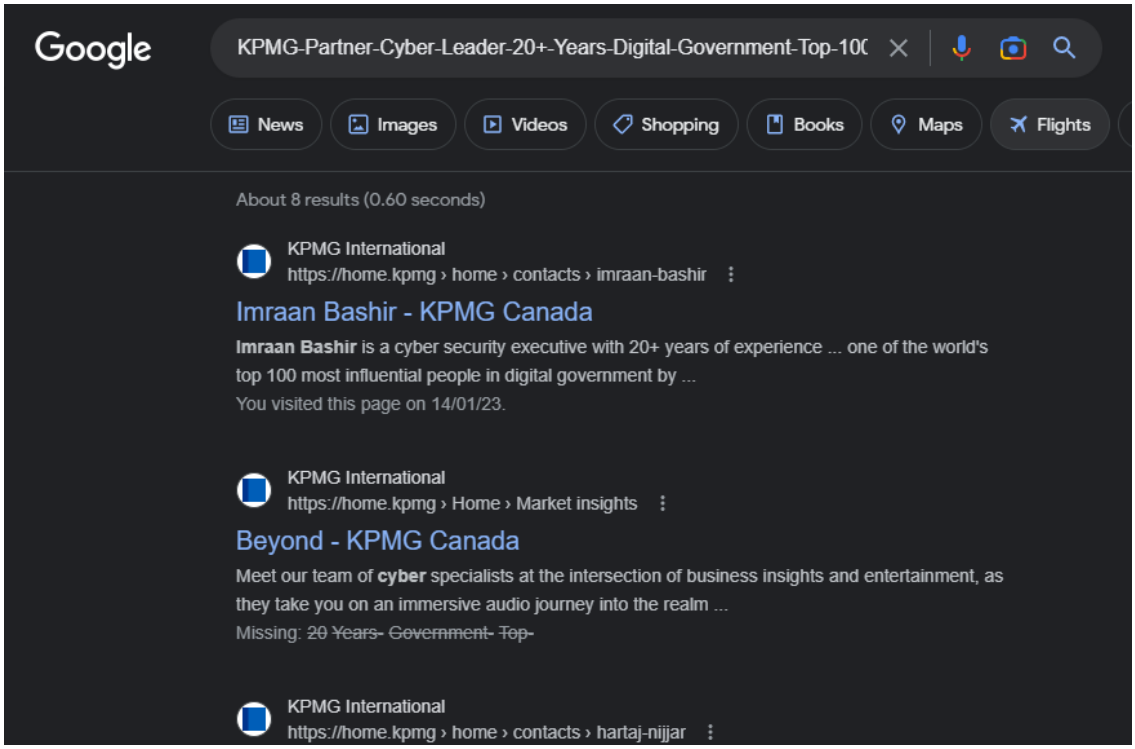


FIGURE 2. GOOGLE SEARCH RESULT

Find My Car Marty

I thoroughly enjoyed completing the first OSNIT challenge, so I decided to take on another one: Find My Car Marty!

Find my car Marty

30

Easy

Help me Marty!

My DeLorean has been stolen! I parked it when I went to grab a drink with a friend and when I came out it was gone. I cannot believe this. The scummy thief even had the audicity to send me a gloating picture of him with my car. Maybe I can get some information from this picture though?

Use this picture and help me find my car Marty.

Format: retroCTF{Street Name} Each first letter of each word must be capitalized!

FIGURE 3. Find My Car Challenge Description

This challenge requires me to identify the most recent location of a vehicle, based on an image of the car in that location. I have no other information about the location, just the image of the car and the location in the background. Therefore, I must utilize image analysis to identify the location

FIGURE 4. Image Provided from the Challenge (Image.jpg)

When I see this image, the first thing I do is identify any unique identifiers that will help me form a connection to the place depicted in the challenge. By looking closer and zooming into ***FIGURE 4*** the first unique identifiers I find are road signs.

FIGURE 5. Circling The Clues

Upon zooming into the image I get a better view of the signs, information I can gather was from the sign of the LA river, so I know this is somewhere in Los Angeles where there is a bike path near a river. I also know that it must be near FWY 134 and Interstate 5(I-5).

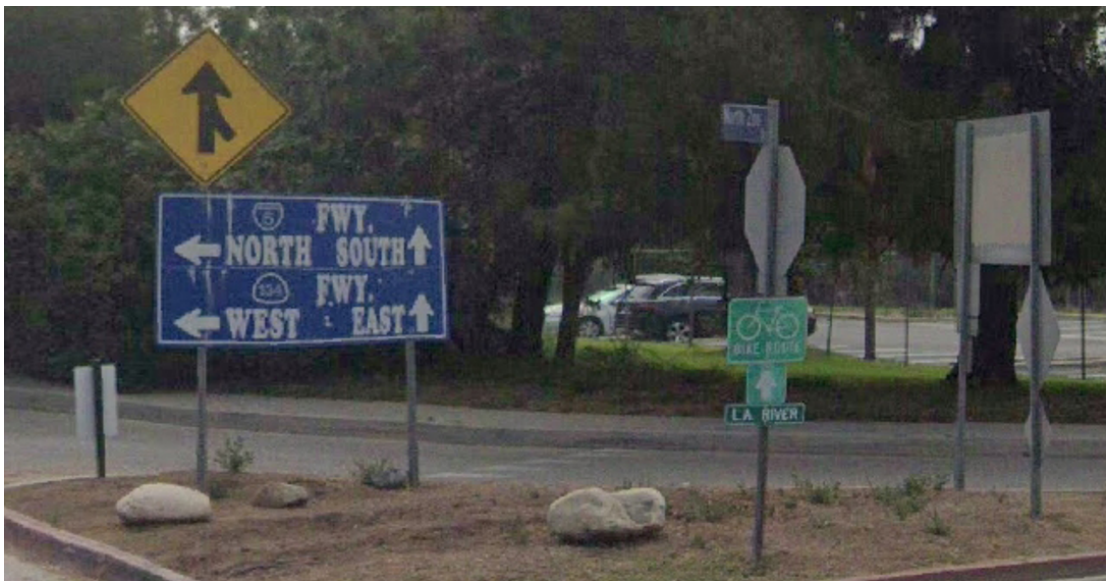


FIGURE 6. Zoomed In Street Signs

By using the street signs and some help from google maps you can begin to narrow down where exactly this image was taken. So by combining all these facts I created a unique identifier that brought me to this location in google maps. I searched for “Interstate 5 near LA River with FWY 134” and got to this general location

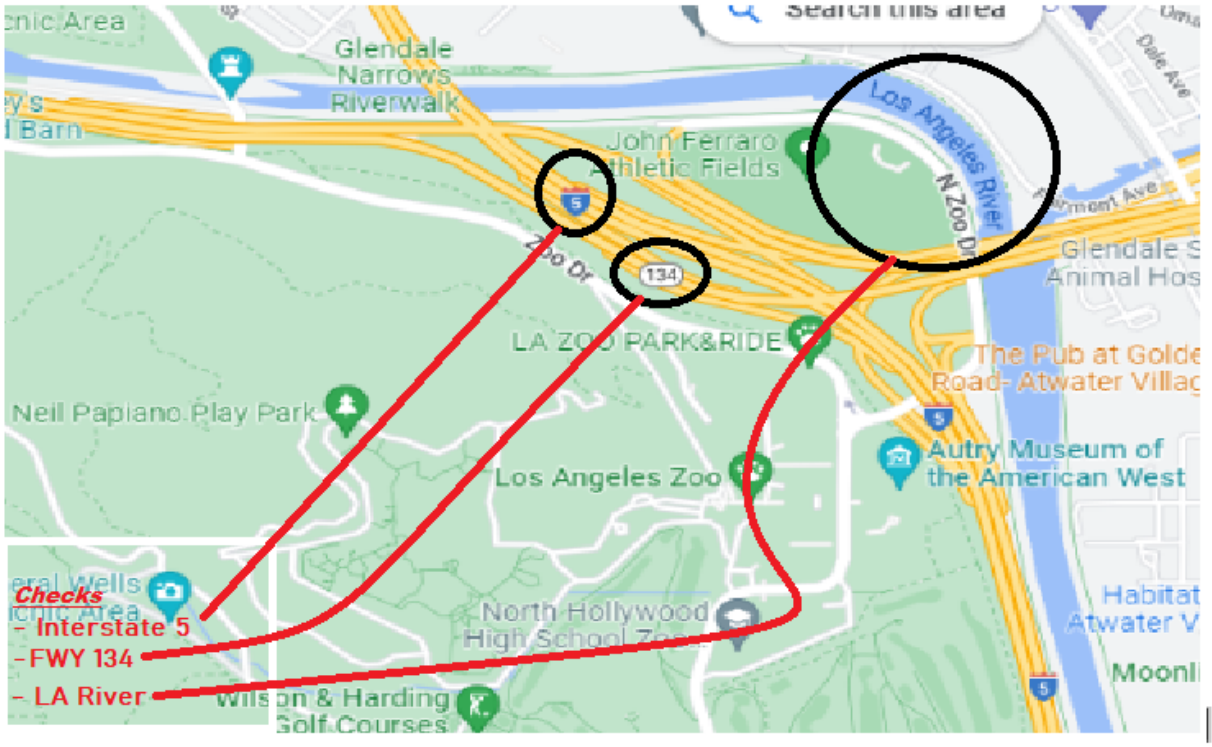


FIGURE 7. Google Maps Image of Location

As you can see FWY 134, LA river, And the I-5, along with trails are present so I know I'm near the location in the image, now to narrow down which exact street it is I will look back at my image for another clue, there was a street sign that had the name of a road but it was blurred, you could only make out a few letters from it, ‘N’, and ‘Z’, and I knew that the word that began with the letter ‘z’ only contained 3 characters.

FIGURE 8. Images of the location I found in google maps compared to Figure 3

With these facts along with the fact that N Zoo Dr was the closes road to FWY 183 and I-5 that meant that the flag was retroCTF{North Zoo Dr}

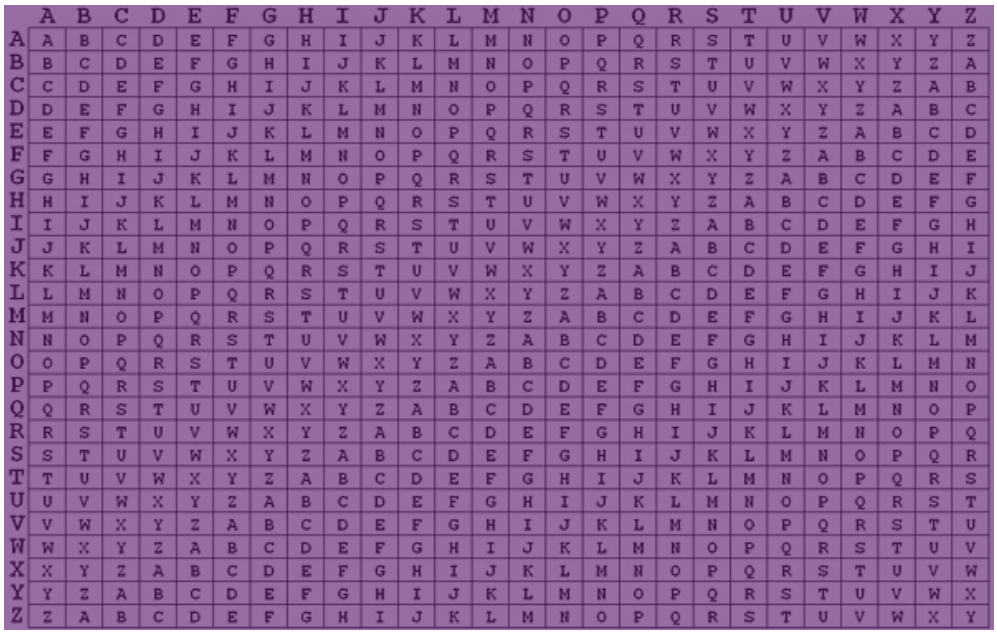
The Man Who Sold the World

FIGURE 9. The Man Who Sold The World Challenge Description

The man who Sold the world Challenge was a Cryptography challenge. I was given an audio file, of what seemed to be morse code, and I was also provided an image of a purple chart. First thing I did was look at the names of files to see if there were any hints, sadly there were none.

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
message.wav	72,924	723	WAV File	1/12/2023 8:25 ...	173BDF5F
table.png	241,315	240,311	PNG File	1/12/2023 8:25 ...	6A3482E1

FIGURE 10. Name of Files Downloaded



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE 11. Png from the Challenge (image.png) “Purple Chart”

I was not familiar with Morse code, so I looked online for a tool that could convert an audio file to text by analyzing the audio waves. Fortunately, I was able to find a suitable program that could help me accomplish this task. It was a Spectrum Analyzer so I could visualize the radio waves to translate the patterns to morse by using a morse code chart.

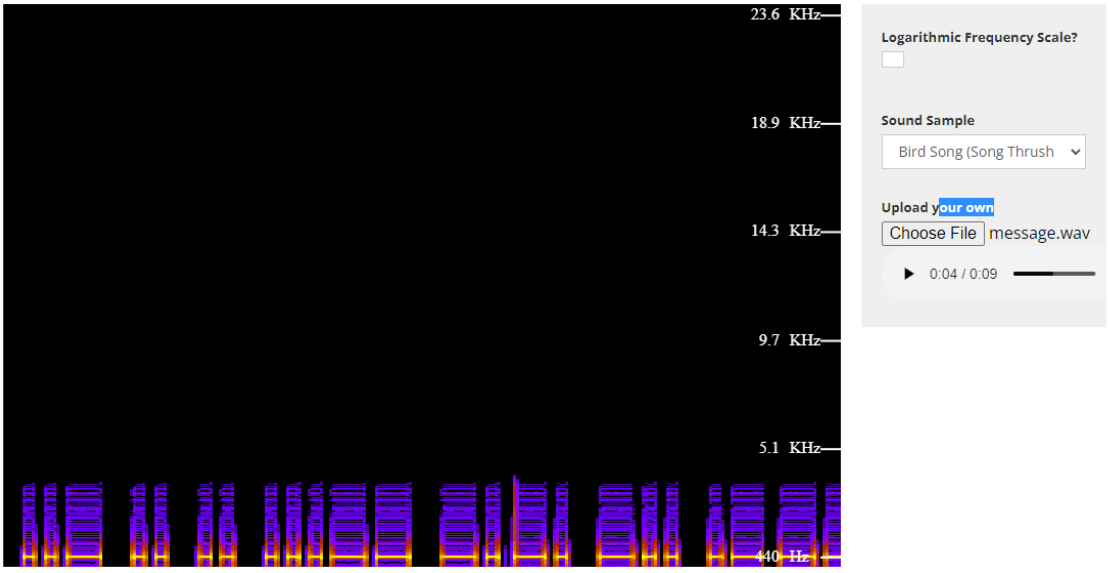


FIGURE 12. EXAMPLE OUTPUT from (*https://academo.org/demos/spectrum-analyzer/*)

To translate waveforms to text, I needed to figure out how to distinguish when one letter begins and ends. After some research on YouTube, I learned that each letter in Morse code is separated by a space the size of a dash.

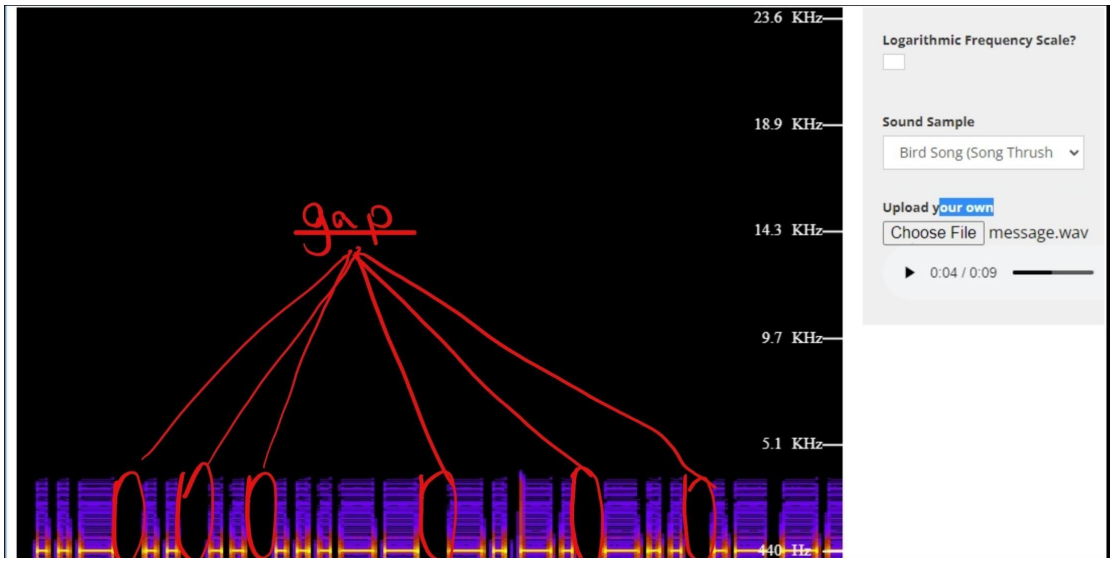


FIGURE 13. Dash Sized Gaps between Letters in Morse Code

Now since I knew when one letter ends and begins I can pull out a morse code chart and begin to translate, a hint I got from a ticket I opened in the CTF Discord was that the morse code in this challenge was International morse code not American. So I downloaded an image of an international morse code chart and began translating.

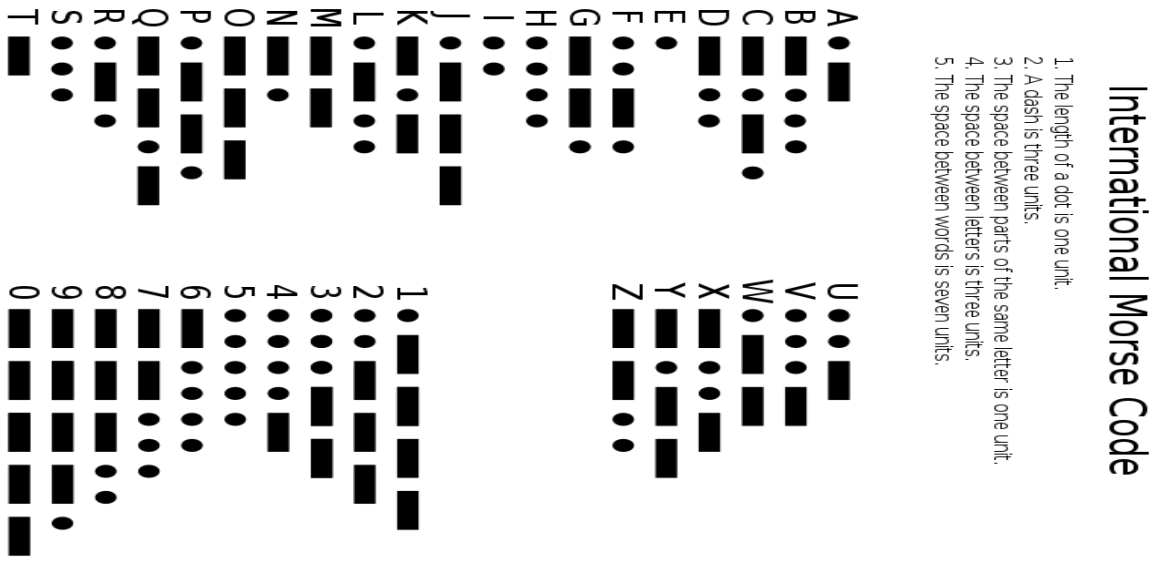


FIGURE 14. International Morse Code Chart from Google

Now armed with this chart, and images of the audio waveforms I can analyze these to translate them to dots and dashes to match these codes to the letter codes within the chart as seen in ***FIGURE 14***

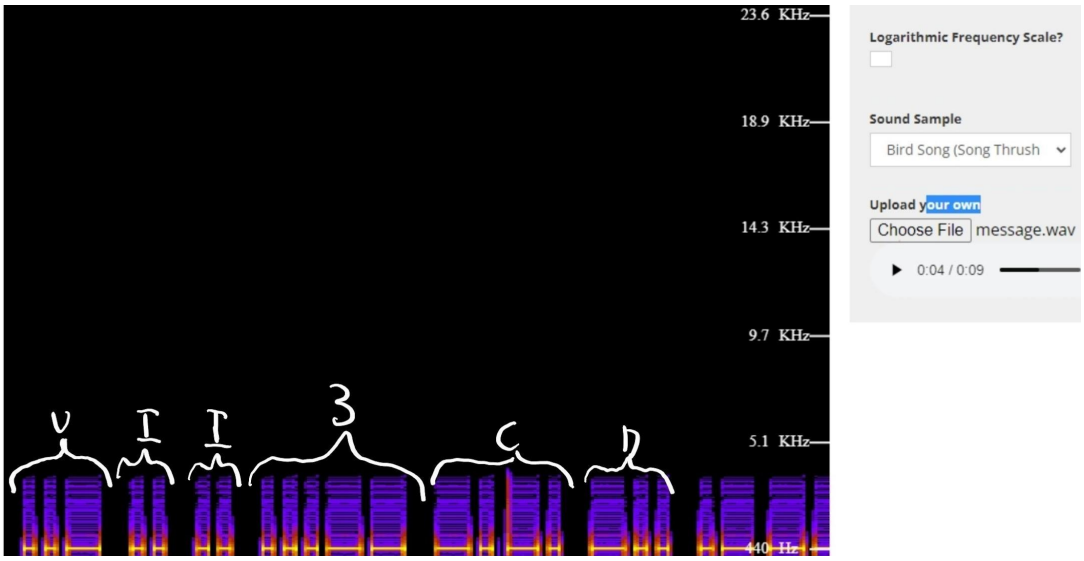


FIGURE 15. Translation of Morse code

As you can see above every small wave is a dot, and every large wave is a dash. I did this for the entire audio file. After about 45 minutes of writing a bunch of codes on a piece of paper I ended up with the code "U I I 3 C D 1 G T R G 3 G E" I was confused at first and double-checked it was correct because I wasn't sure. While searching on google about morse code to make sure I was doing the translation right I found out there was an online tool that does the translation for you…

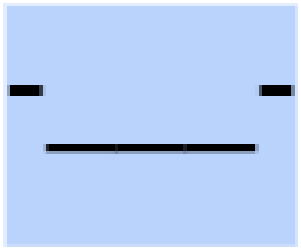


FIGURE 16. Me after finding out there is a tool to do morse code translation for you

The Manual Translation that I did of the morse code was correct so I thought maybe this is a cipher. I went back to the chart that I was provided within a folder with the audio file for this challenge. I was attempting to try to translate the cipher using the Purple chart as seen in **FIGURE 11**, but I had no clue how so I gave up on that. whenever I do a challenge I only like to look at the hint after I tried every possible idea I came up with to solve the challenge, so after trying every possible thing I looked at the hint.

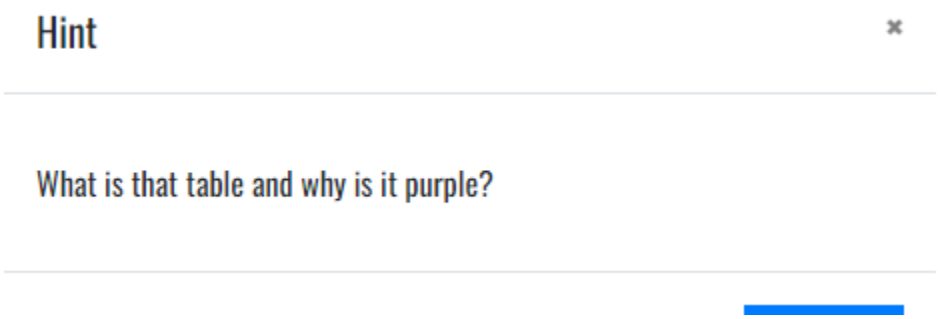


FIGURE 17. HINT

So I knew from this hint that if I could find out what it is, and its name I could use a tool like CyberChef to crack the cipher. I just need to know what cipher it was encrypted with. So I knew that something unique about this chart (Again the unique identifier) was that it was purple and the hint also mentioned the chart being purple so with the hint and information I collected i googled ”purple-chart-with-English-alphabet”, from that I found out that the cipher was a *Vigenere Cipher* so I went on to Cyberchef and after Brute forcing the key I found out that it was the word “purple” and I got my flag…

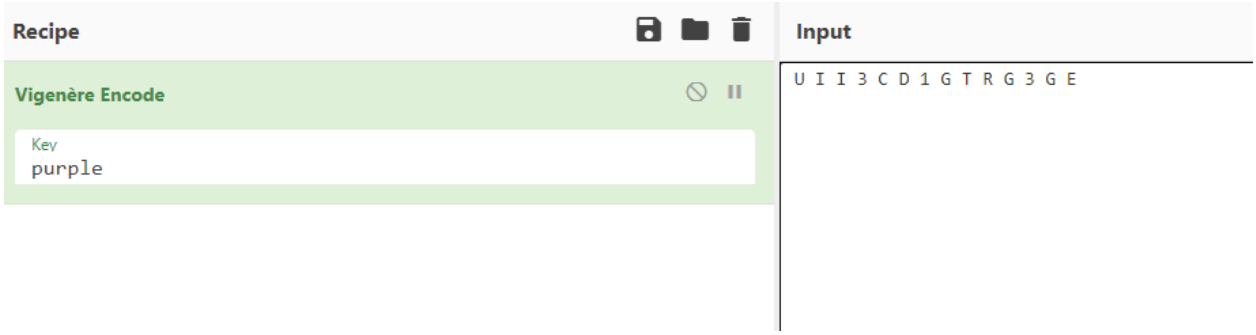


Figure 18. CyberChef | output was “F O R 3 N S 1 C E X P 3 R T**”**

The Flag was “retroCTF{FOR3NS1CEXP3RT}

Thank You!

I'd like to give a huge shout out to the ISSessions team for hosting an amazing 2023 CTF! It was an incredible experience, even while competing from home. The team did an amazing job organizing the entire event. I would also like to thank the sponsors, KPMG, Trend Micro, LARES, Mand Consulting Group, Hyde HR Law, and NineCloudsBeds for their amazing workshops and their generous support.