Writeup for “The Lost City” TrojanCTF Challenge:

1) Convert the 500 ms frequencies in the file to ascii characters (“Hear the Trojan song”). The file was first converted to wav format in this case:

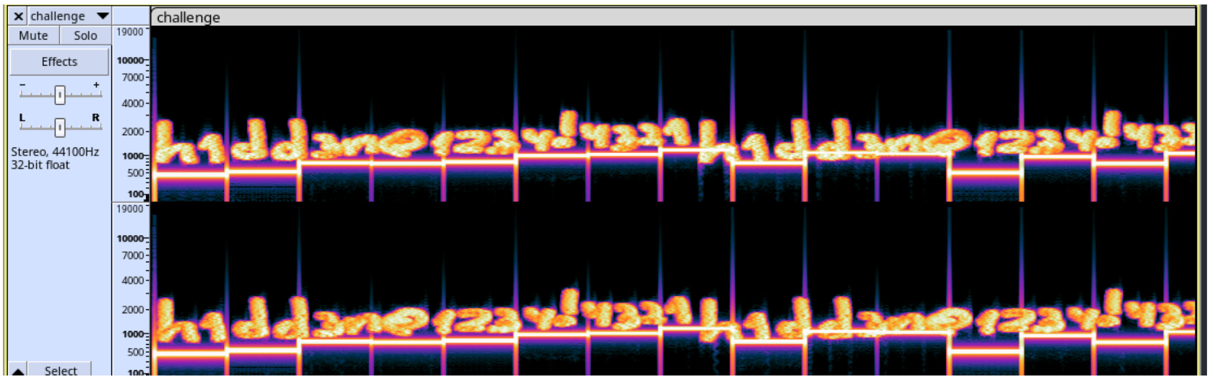
Example script:

```
import numpy as np
from scipy.io import wavfile

def detect_frequency(segment, sample_rate):
    # Perform FFT on the audio segment
    fft_result = np.fft.fft(segment)
    freqs = np.fft.fftfreq(len(segment), d=1/sample_rate)

    # Use only the positive half of the spectrum
    magnitude = np.abs(fft_result[:len(segment)//2])
    positive_freqs = freqs[:len(segment)//2]

    # Find the peak frequency
    peak_index = np.argmax(magnitude)
    return int(round(positive_freqs[peak_index]))

# Read the .wav file
sample_rate, data = wavfile.read("challenge.wav")

# Ensure mono audio
if data.ndim > 1:
    data = data[:, 0]

# Split the audio into 1-second chunks
chunk_size = int(sample_rate * 0.5)  # 1 second
frequencies = []

for i in range(0, len(data), chunk_size):
    segment = data[i:i + chunk_size]
    if len(segment) < chunk_size:
        break  # Skip incomplete chunks at the end
    freq = detect_frequency(segment, sample_rate)
    frequencies.append(int(freq / 10))

# Output detected frequencies (Ascii characters)
print("Detected frequencies (Hz) / 10:", frequencies)
```

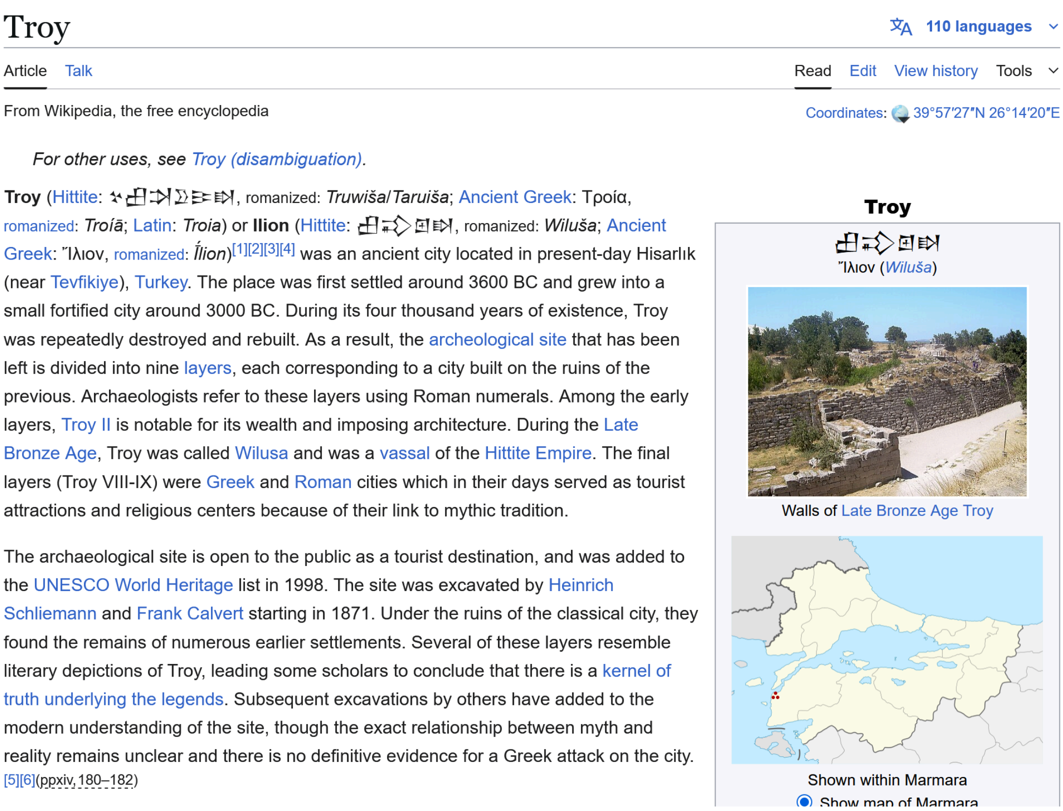
Output:
Detected frequencies (Hz) / 10: [47, 55, 78, 76, 81, 100, 104, 120, 78, 110, 107, 52, 97, 76, 108, 65, 84, 111, 110, 69, 104, 106, 73, 66, 82, 43, 82, 76, 110, 75, 57, 78, 109, 68, 81, 100, 51, 82, 109, 87, 112, 43, 69, 61]

After ascii conversion, we get a ciphertext:
/7NLQdhxNnk4aLIATonEhjIBR+RLnK9NmDQd3RmWp+E=

2) Look at the spectrogram of the challenge.mp3 recording provided to find a secret passphrase: h1dd3n@1234!4321 ("see the energy behind it")



3) OSINT part of the challenge: locate the lost city of Troy and the Trojan horse ("Enter the Trojan horse")



Troy

110 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

Coordinates: 39°57′27″N 26°14′20″E

For other uses, see Troy (disambiguation).

Troy (Hittite: , romanized: *Truwiša*/*Taruiša*; Ancient Greek: Τροία, romanized: *Troíā*; Latin: *Troia*) or **Ilion** (Hittite: , romanized: *Wiluša*; Ancient Greek: Ἴλιον, romanized: *Ī́lion*)[1][2][3][4] was an ancient city located in present-day Hisarlık (near Tevfikiye), Turkey. The place was first settled around 3600 BC and grew into a small fortified city around 3000 BC. During its four thousand years of existence, Troy was repeatedly destroyed and rebuilt. As a result, the archeological site that has been left is divided into nine layers, each corresponding to a city built on the ruins of the previous. Archaeologists refer to these layers using Roman numerals. Among the early layers, Troy II is notable for its wealth and imposing architecture. During the Late Bronze Age, Troy was called Wilusa and was a vassal of the Hittite Empire. The final layers (Troy VIII-IX) were Greek and Roman cities which in their days served as tourist attractions and religious centers because of their link to mythic tradition.

The archaeological site is open to the public as a tourist destination, and was added to the UNESCO World Heritage list in 1998. The site was excavated by Heinrich Schliemann and Frank Calvert starting in 1871. Under the ruins of the classical city, they found the remains of numerous earlier settlements. Several of these layers resemble literary depictions of Troy, leading some scholars to conclude that there is a kernel of truth underlying the legends. Subsequent excavations by others have added to the modern understanding of the site, though the exact relationship between myth and reality remains unclear and there is no definitive evidence for a Greek attack on the city.[5][6](ppxiv, 180–182)

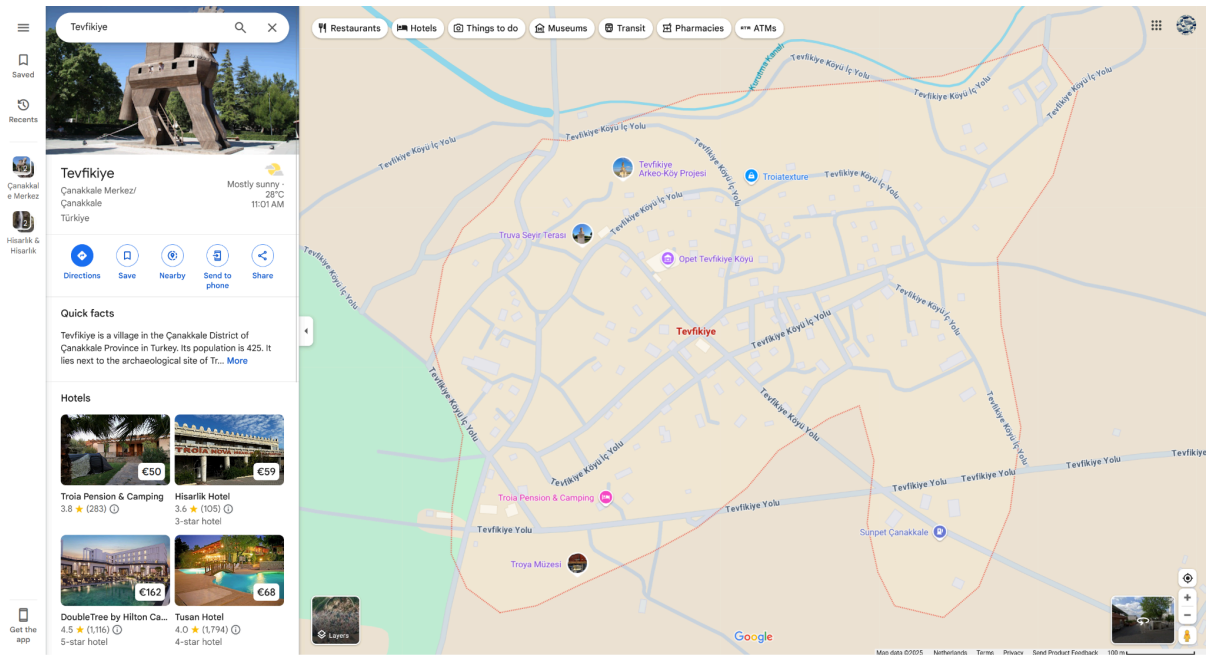
Troy

Ἴλιον (*Wiluša*)

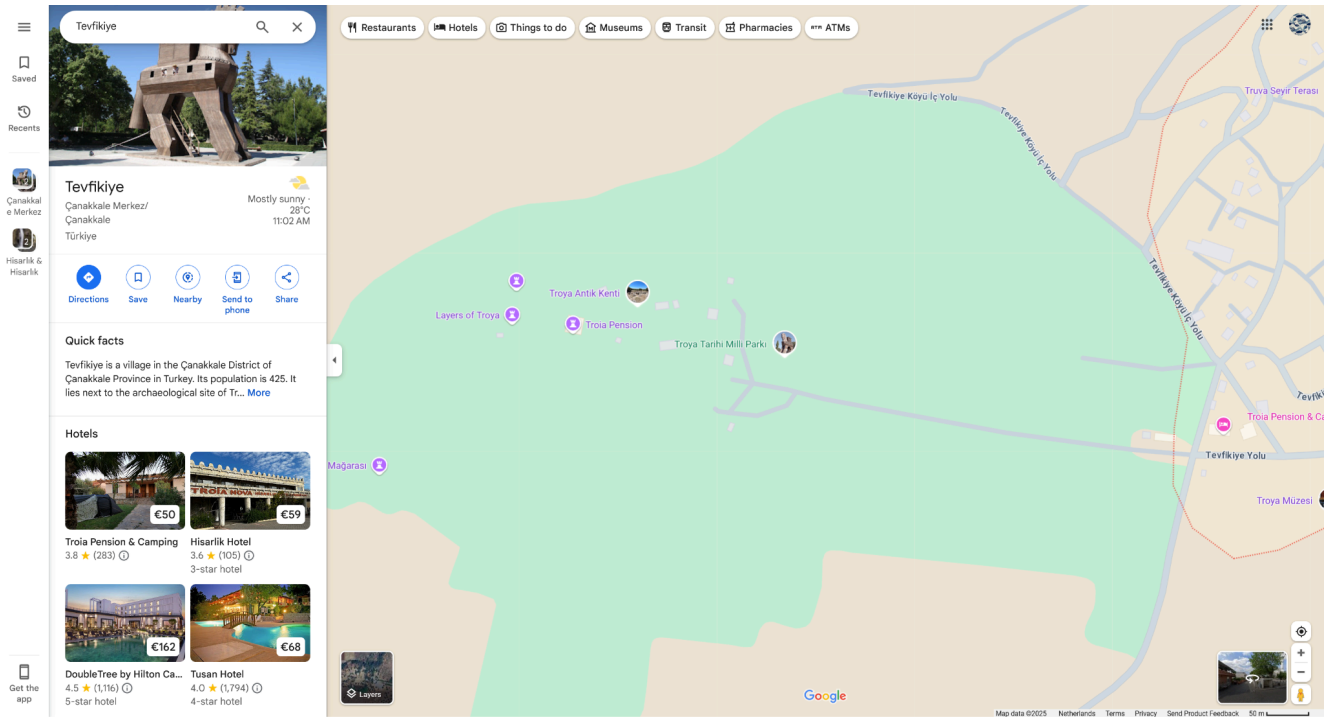
Walls of Late Bronze Age Troy

Shown within Marmara

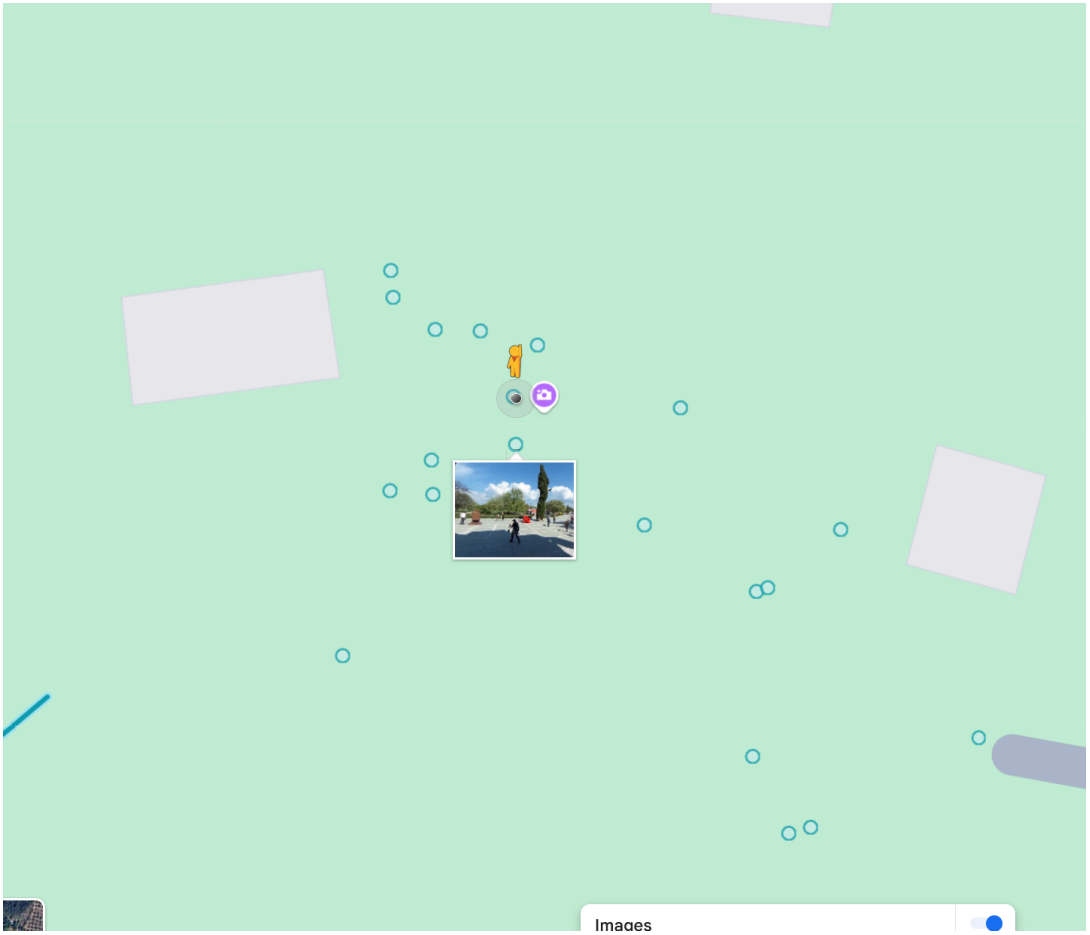
Show map of Marmara

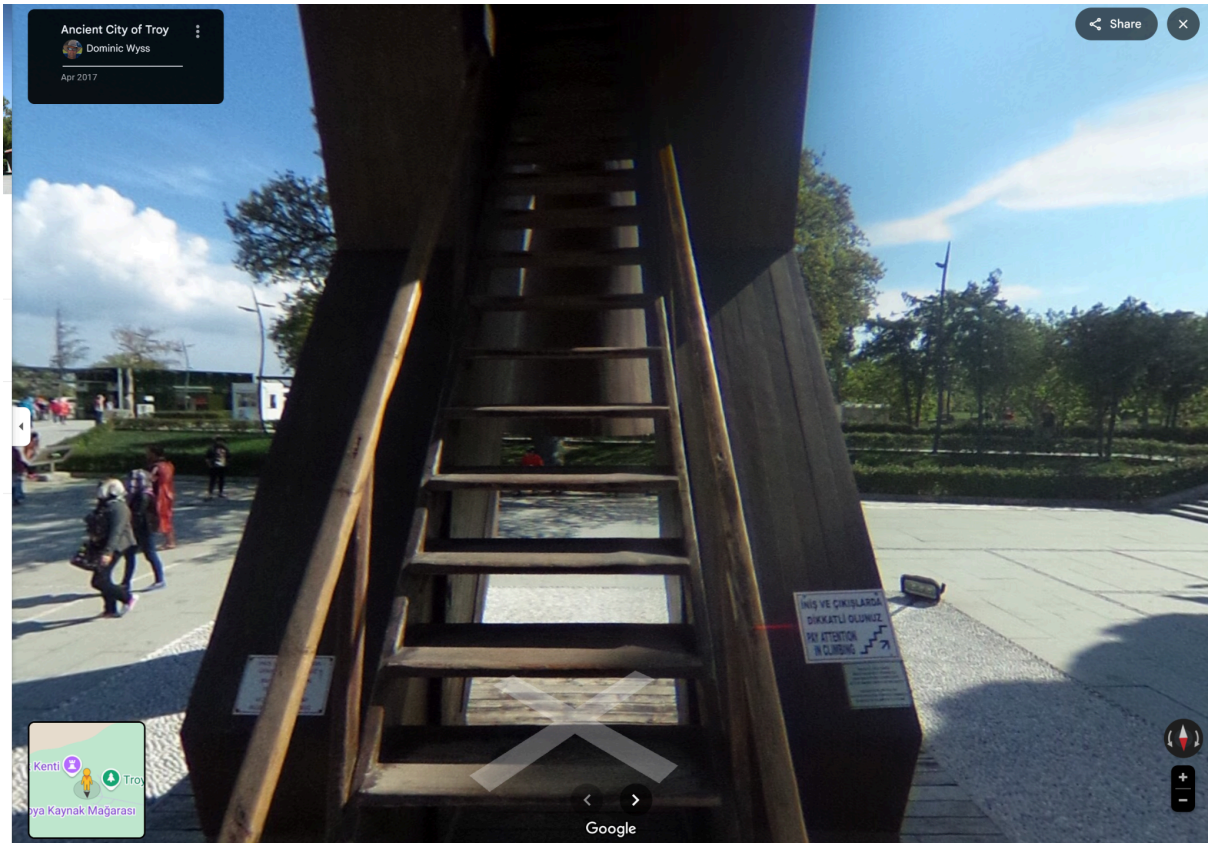


Here’s the location of our Trojan horse:



4) Time to enter the horse:





Go forward on the previous picture to enter:

5) Take note of the “Bangladesh” graffiti (“many have flocked to it. The faraway land of your fellow soldier will guide you,”).

6) AES decrypt the ciphertext with the passphrase (“all ends soon.”), using “Bangladesh******” as an IV (“but you must fill the rest of your path with stars.”):

AES Decryption

AES Encrypted Text

/7NLQdhxNnk4aLlATonEhjIBR+RLnK9NmDQd3RmWp+E=

Select Cipher Mode of Decryption

CBC

Select Padding

PKCS5Padding

Enter IV Used During Encryption(Optional)

Bangladesh******

Key Size in Bits

128

Enter Secret Key used for Encryption

h1dd3n@1234!4321

Output Text Format (•) Plain-Text ( ) Base64

Decrypt

AES Decrypted Output

Trojan{L05t_C1Ty_n0W_f0uNd}