Network Recorder – Write Up

Difficulty – Medium

**Challenge:**

I captured some network traffic from Alice. I am sure there is some secret inside. Can you help me to find out what’s the secret?

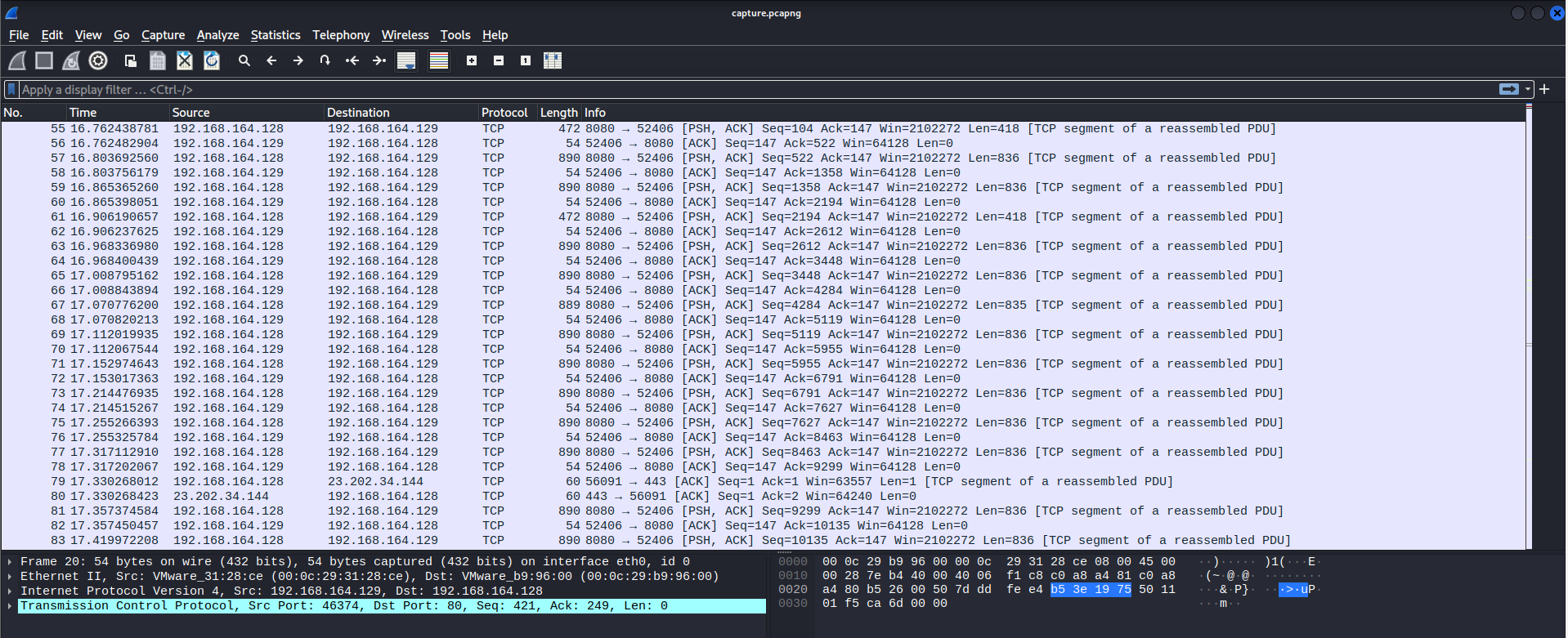
Note: Flag format is MOCSCTF{XXXXXX} and XXXXXX only include capital letters and digits.

Flag: MOCSCTF{Y0uF0UND7HEC0DEG00DJ0B!}

**Solution:**

First, open the packet capture file with Wireshark:





The beginning packets are port 80 HTTP traffic, but then you can find later the packet belongs to a TCP port 8080 stream which is also based on HTTP protocol.

A screenshot of a computer

Description automatically generated

Try to see if we can export some object from the capture:

Graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated

Save the objects. Check the object from port 8080 traffic:

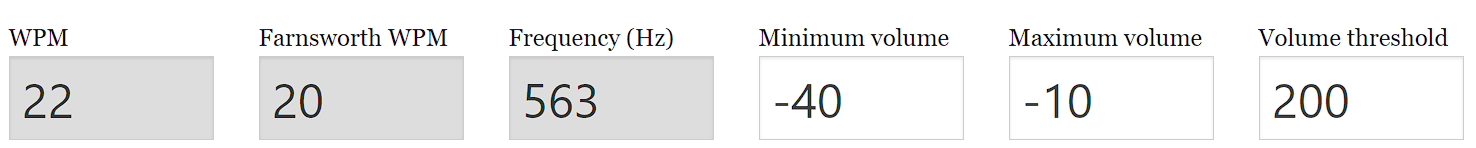


It’s an audio file, let’s open it. We can hear the music from the audio file but at the end of the audio file, we can hear some strange “bi…”, which seems Morse code. Let find an online Morse decoder (In this write up use https://morsecode.world/international/decoder/) to try to decode:

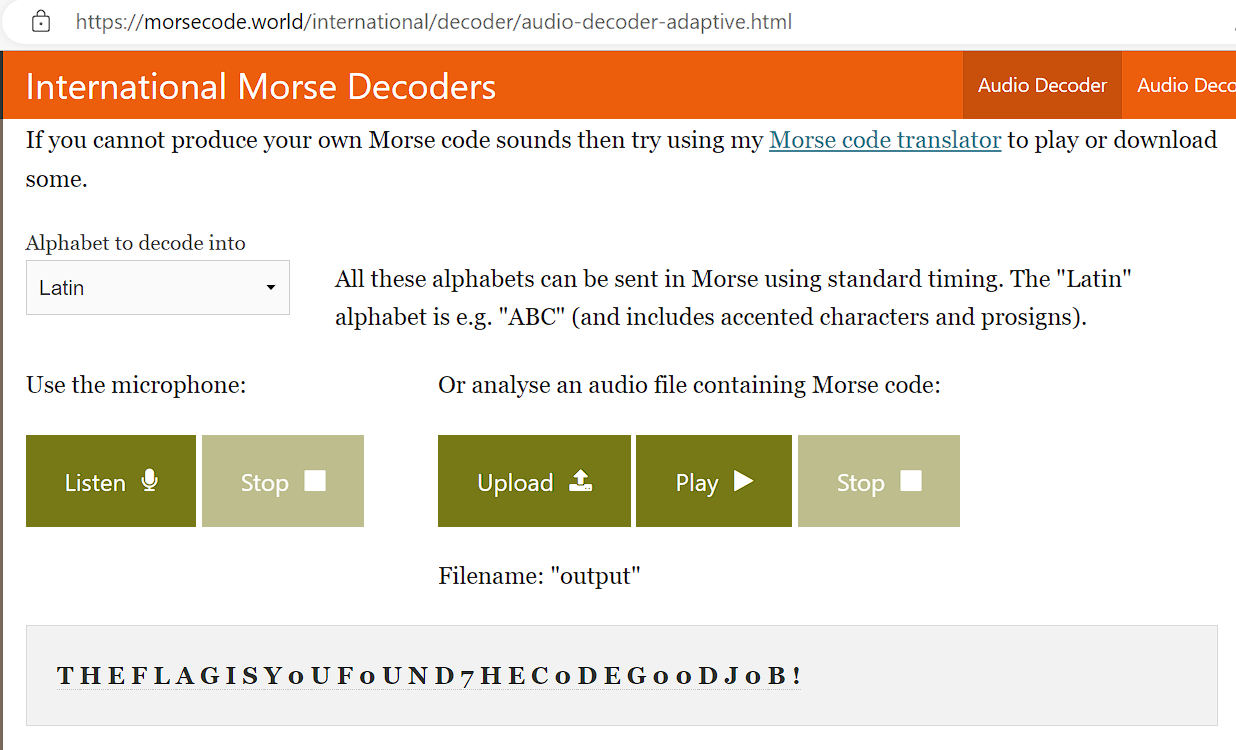
Graphical user interface

Description automatically generated

Seems our direction is correct, it’s Morse code but the output is a bit messy, let’s try to tune a bit the parameters for better sampling:



Try again:



So the flag is MOCSCTF{Y0uF0UND7HEC0DEG00DJ0B!}