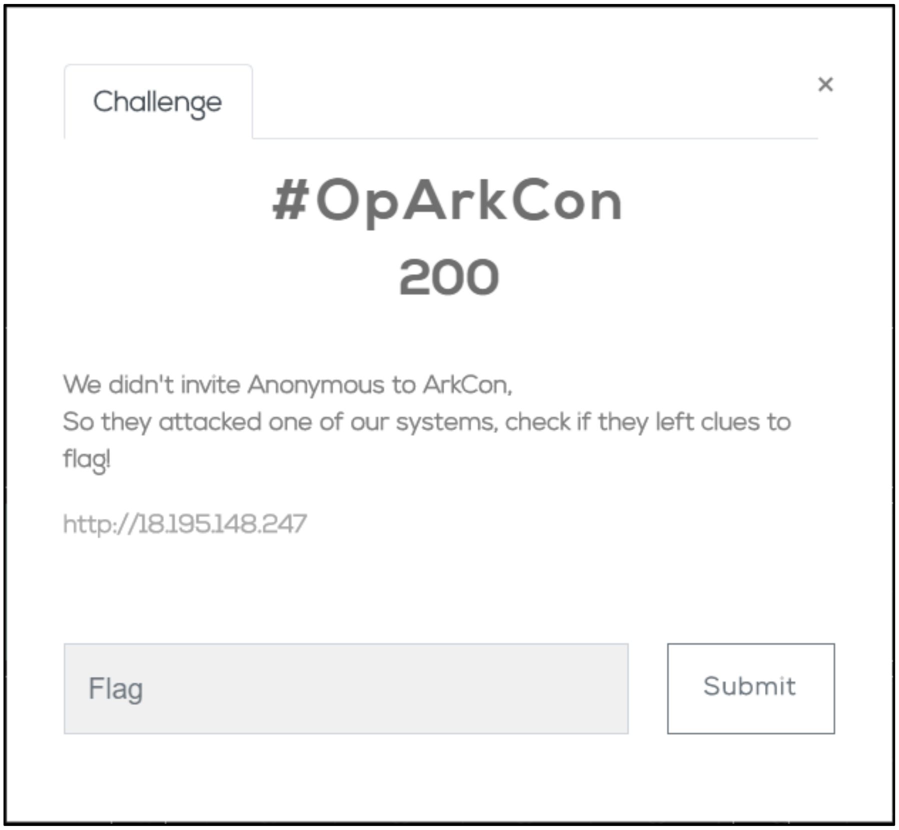
OpArkCon

Author: Tomer Zait



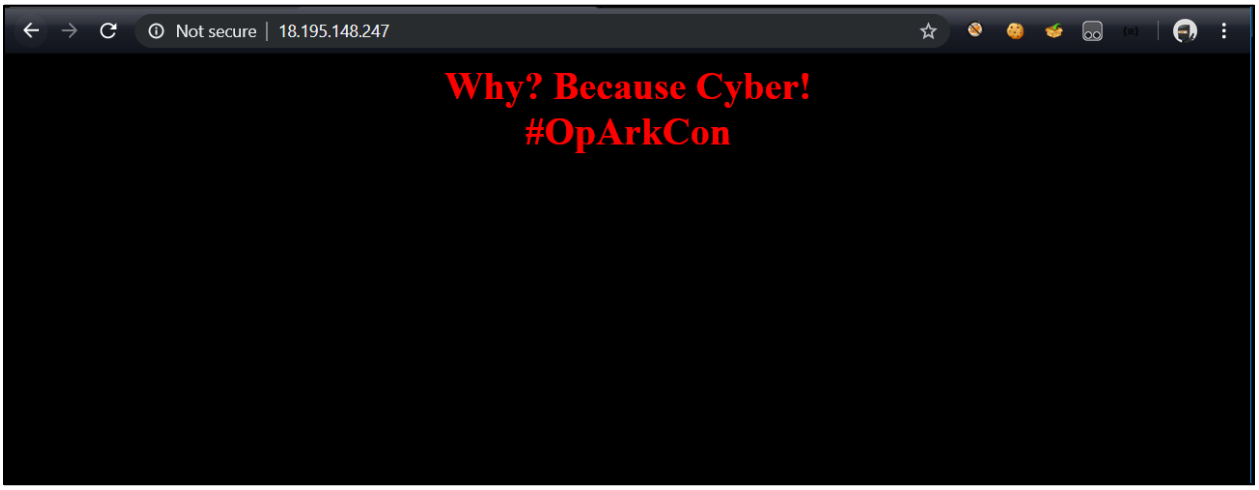
#OpArkCon

200

We didn't invite Anonymous to ArkCon,
So they attacked one of our systems, check if they left clues to flag!

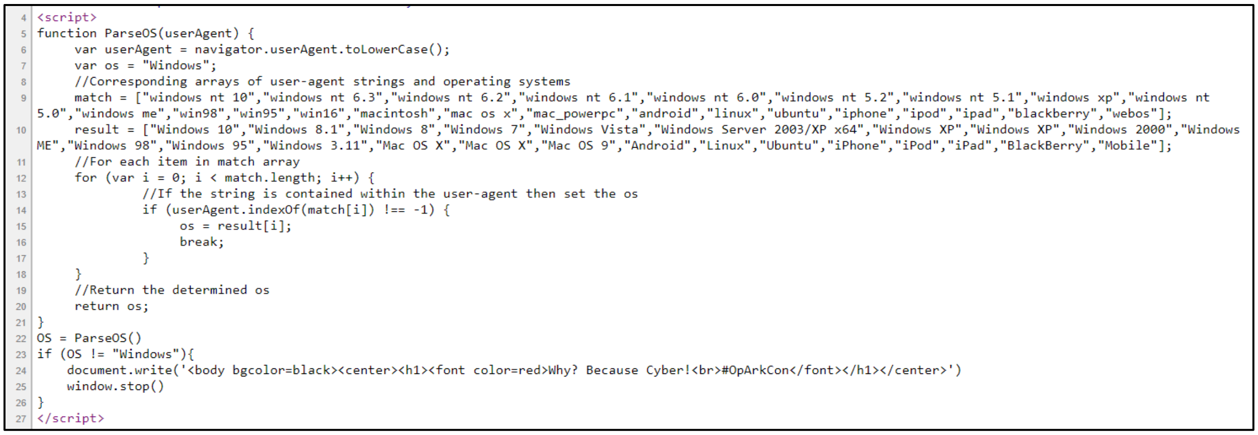
http://18.195.148.247

The challenge starts with a URL: http://18.195.148.247
When we go to the URL in our browser we see an anonymous message:



Why? Because Cyber!
#OpArkCon

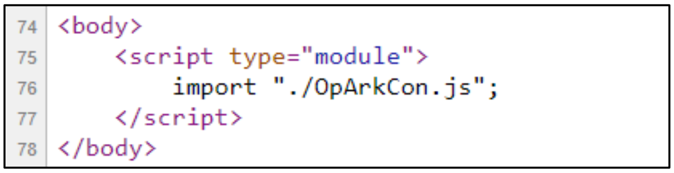
When we view the page source we can see a JavaScript Code that should have worked but had a tiny bug that made it useless…



```
<script>
function ParseOS(userAgent) {
     var userAgent = navigator.userAgent.toLowerCase();
     var os = "Windows";
     //Corresponding arrays of user-agent strings and operating systems
     match = ["windows nt 10","windows nt 6.3","windows nt 6.2","windows nt 6.1","windows nt 6.0","windows nt 5.2","windows nt 5.1","windows xp","windows nt 5.0","windows me","win98","win95","win16","macintosh","mac os x","mac_powerpc","android","linux","ubuntu","iphone","ipod","ipad","blackberry","webos"];
     result = ["Windows 10","Windows 8.1","Windows 8","Windows 7","Windows Vista","Windows Server 2003/XP x64","Windows XP","Windows XP","Windows 2000","Windows ME","Windows 98","Windows 95","Windows 3.11","Mac OS X","Mac OS X","Mac OS 9","Android","Linux","Ubuntu","iPhone","iPod","iPad","BlackBerry","Mobile"];
     //For each item in match array
     for (var i = 0; i < match.length; i++) {
              //If the string is contained within the user-agent then set the os
              if (userAgent.indexOf(match[i]) !== -1) {
                   os = result[i];
                   break;
              }
     }
     //Return the determined os
     return os;
}
OS = ParseOS()
if (OS != "Windows"){
    document.write('<body bgcolor=black><center><h1><font color=red>Why? Because Cyber!<br>#OpArkCon</font></h1></center>')
    window.stop()
}
</script>
```

* The Code and the page design taken from a real anonymous attack that happened on March 2019. You can read more about it here: https://www.cyberark.com/threat-research-blog/opjerusalem-flashinstaller-ransomware/

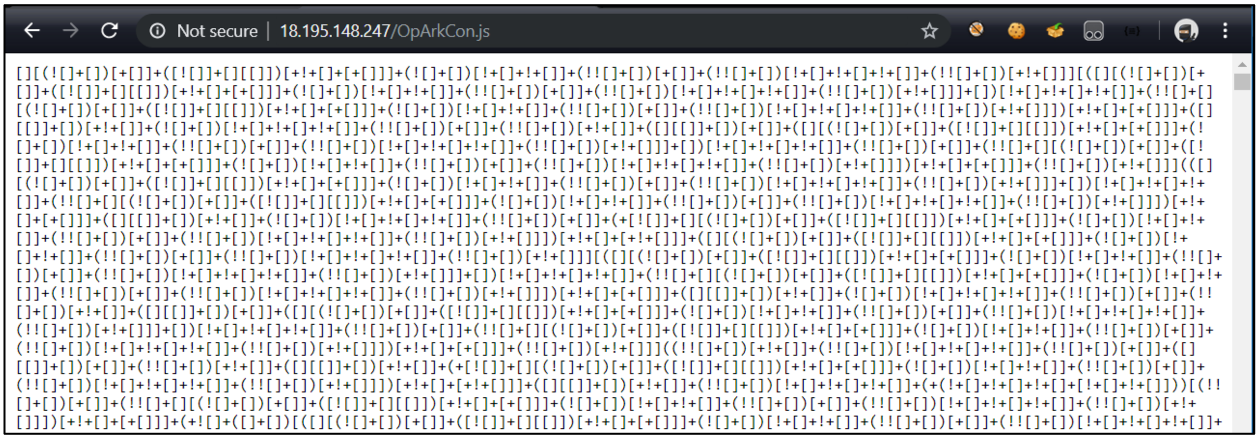
If the script didn't have a bug, this code was running when we opened the page on Windows (also found in the page source):



```
<body>
    <script type="module">
        import "./OpArkCon.js";
    </script>
</body>
```

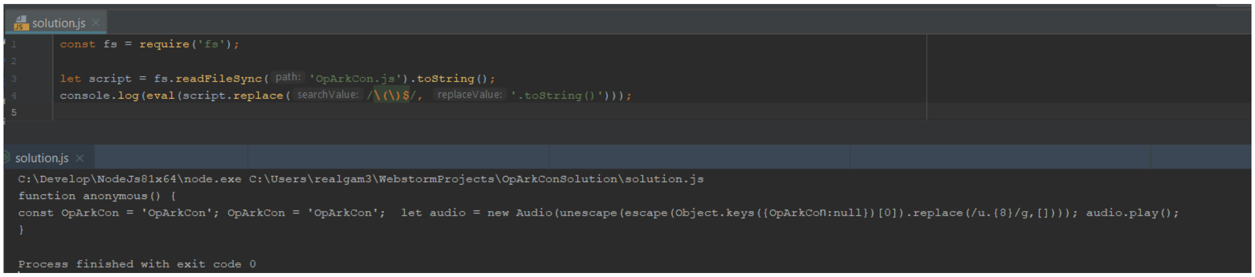
This is a ES6 import of the **OpArkCon.js** file.

When we open this file in our browser we see a **JSFuck** Obfuscated Code:



```
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[]
[(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([]
[[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(!
[]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([!
[]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]](([]
[(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+
[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+
[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+
[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!!
[]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+
(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([]
[[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+
(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+([][[]]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(+(!+[]+!+[]+!+[]+[!+[]+!+[]]))[(!!
[]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+
[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+
```

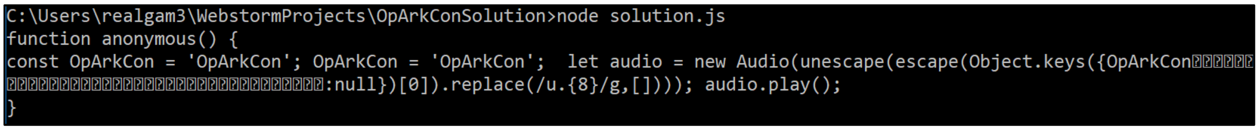
We will download the **OpArkCon.js** file and write a script that will deobfuscate the code.



```
const fs = require('fs');

let script = fs.readFileSync( path: 'OpArkCon.js').toString();
console.log(eval(script.replace( searchValue: /\(\)$/,  replaceValue: '.toString()')));
```

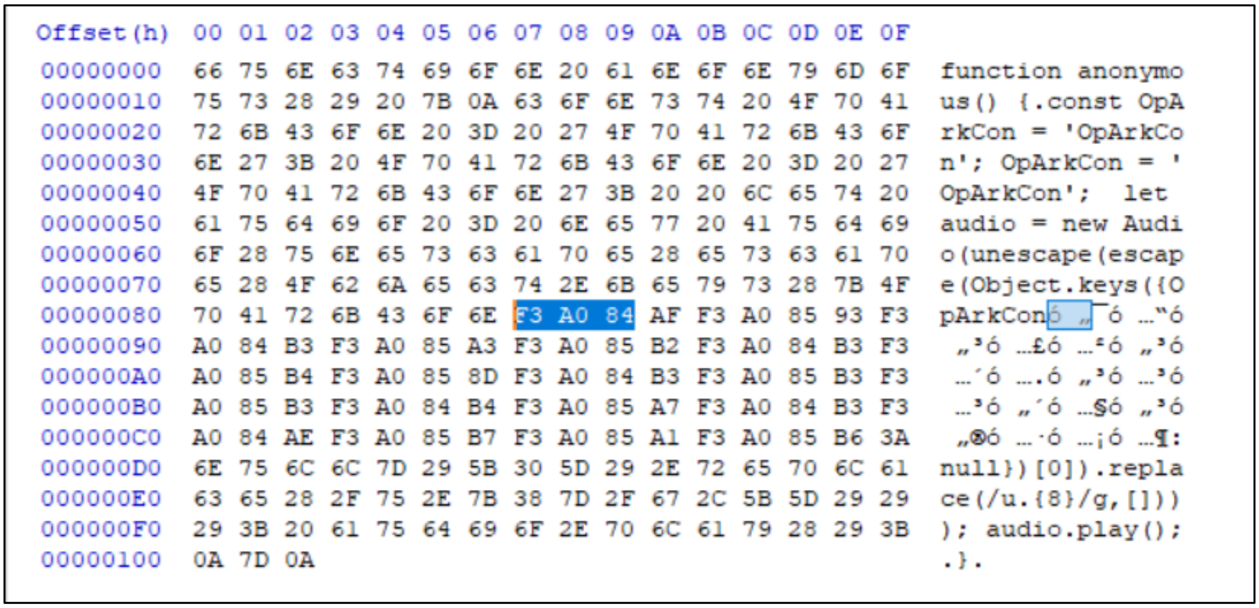
```
C:\Develop\NodeJs81x64\node.exe C:\Users\realgam3\WebstormProjects\OpArkConSolution\solution.js
function anonymous() {
const OpArkCon = 'OpArkCon'; OpArkCon = 'OpArkCon';  let audio = new Audio(unescape(escape(Object.keys({OpArkCon:null})[0]).replace(/u.{8}/g,[]))); audio.play();
}

Process finished with exit code 0
```

The script worked but there is something strange in the output….
Let’s run the same script in **cmd.exe**



```
C:\Users\realgam3\WebstormProjects\OpArkConSolution>node solution.js
function anonymous() {
const OpArkCon = 'OpArkCon'; OpArkCon = 'OpArkCon';  let audio = new Audio(unescape(escape(Object.keys({OpArkCon⍰⍰⍰⍰⍰⍰
⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰:null})[0]).replace(/u.{8}/g,[]))); audio.play();
}
```

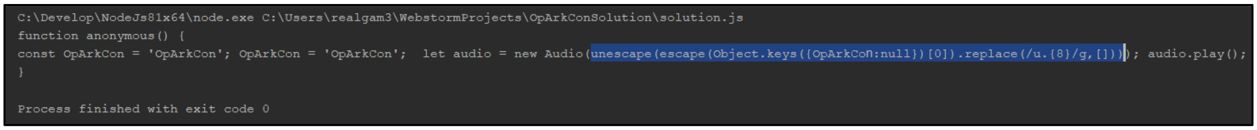
Now its little bit better we can see that there are special utf-8 characters that we cannot see in the browser and the IDE (WebStrorm), But we can see in **cmd.exe** or hex editor



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  66 75 6E 63 74 69 6F 6E 20 61 6E 6F 6E 79 6D 6F  function anonymo
00000010  75 73 28 29 20 7B 0A 63 6F 6E 73 74 20 4F 70 41  us() {.const OpA
00000020  72 6B 43 6F 6E 20 3D 20 27 4F 70 41 72 6B 43 6F  rkCon = 'OpArkCo
00000030  6E 27 3B 20 4F 70 41 72 6B 43 6F 6E 20 3D 20 27  n'; OpArkCon = '
00000040  4F 70 41 72 6B 43 6F 6E 27 3B 20 20 6C 65 74 20  OpArkCon';  let 
00000050  61 75 64 69 6F 20 3D 20 6E 65 77 20 41 75 64 69  audio = new Audi
00000060  6F 28 75 6E 65 73 63 61 70 65 28 65 73 63 61 70  o(unescape(escap
00000070  65 28 4F 62 6A 65 63 74 2E 6B 65 79 73 28 7B 4F  e(Object.keys({O
00000080  70 41 72 6B 43 6F 6E F3 A0 84 AF F3 A0 85 93 F3  pArkConó „¯ó …“ó
00000090  A0 84 B3 F3 A0 85 A3 F3 A0 85 B2 F3 A0 84 B3 F3   „³ó …£ó …²ó „³ó
000000A0  A0 85 B4 F3 A0 85 8D F3 A0 84 B3 F3 A0 85 B3 F3   …´ó ….ó „³ó …³ó
000000B0  A0 85 B3 F3 A0 84 B4 F3 A0 85 A7 F3 A0 84 B3 F3   …³ó „´ó …§ó „³ó
000000C0  A0 84 AE F3 A0 85 B7 F3 A0 85 A1 F3 A0 85 B6 3A   „®ó …·ó …¡ó …¶:
000000D0  6E 75 6C 6C 7D 29 5B 30 5D 29 2E 72 65 70 6C 61  null})[0]).repla
000000E0  63 65 28 2F 75 2E 7B 38 7D 2F 67 2C 5B 5D 29 29  ce(/u.{8}/g,[]))
000000F0  29 3B 20 61 75 64 69 6F 2E 70 6C 61 79 28 29 3B  ); audio.play();
00000100  0A 7D 0A                                         .}.
```

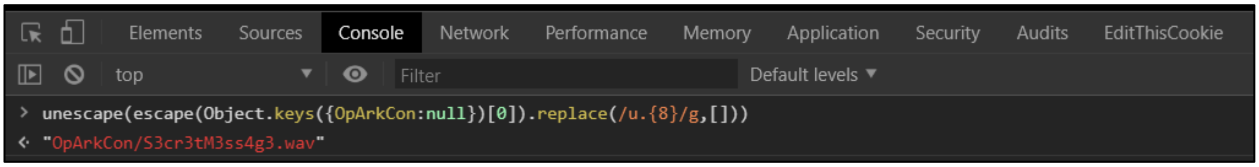
This Is a known technique to hide secrets in JavaScript. You can read more about it here: https://www.stefanjudis.com/blog/hidden-messages-in-javascript-property-names/

We understand that even if we can’t see it we can copy it to the clipboard



```
C:\Develop\NodeJs81x64\node.exe C:\Users\realgam3\WebstormProjects\OpArkConSolution\solution.js
function anonymous() {
const OpArkCon = 'OpArkCon'; OpArkCon = 'OpArkCon';  let audio = new Audio(unescape(escape(Object.keys({OpArkCon:null})[0]).replace(/u.{8}/g,[]))); audio.play();
}

Process finished with exit code 0
```

And then we run it in our browser

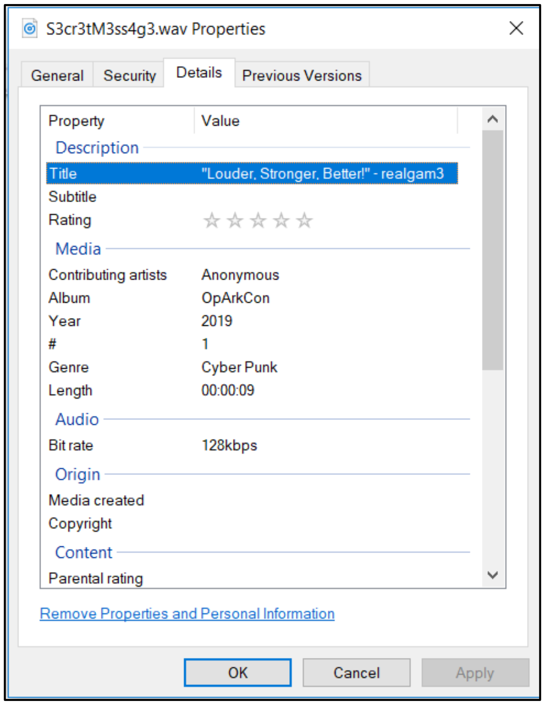


```
> unescape(escape(Object.keys({OpArkCon:null})[0]).replace(/u.{8}/g,[]))
< "OpArkCon/S3cr3tM3ss4g3.wav"
```

Now we download the **S3cr3tM3ss4g3.wav** file and listen to it:
We hear the message:

You made a CTF without inviting us,
We are anonymous,
We are legion,
We do not forgive,
 We do not forget,
expect us!

We can hear the message almost clearly but its still a CTF so maybe there is something hidden in this file….
Let's check the file details (meta data):

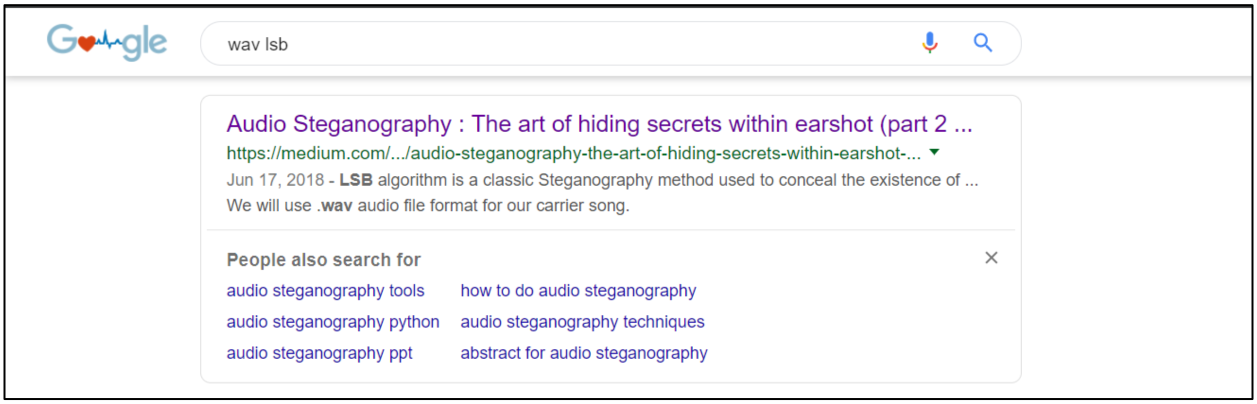

S3cr3tM3ss4g3.wav Properties
General
Security
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

Property	Value
Description	
Title	"Louder, Stronger, Better!" - realgam3
Subtitle	
Rating	☆ ☆ ☆ ☆ ☆
Media	
Contributing artists	Anonymous
Album	OpArkCon
Year	2019
#	1
Genre	Cyber Punk
Length	00:00:09
Audio	
Bit rate	128kbps
Origin	
Media created	
Copyright	
Content	
Parental rating	

We can see the title of the song: “**L**ouder, **S**tronger, **B**etter!” – realgam3

We can understand from this quote that this stage is a steganography stage and we will need to use **LSB (Last Significant Bit)** algorithm in order to get the secret text hidden inside the wav file.

Let’s search it in google



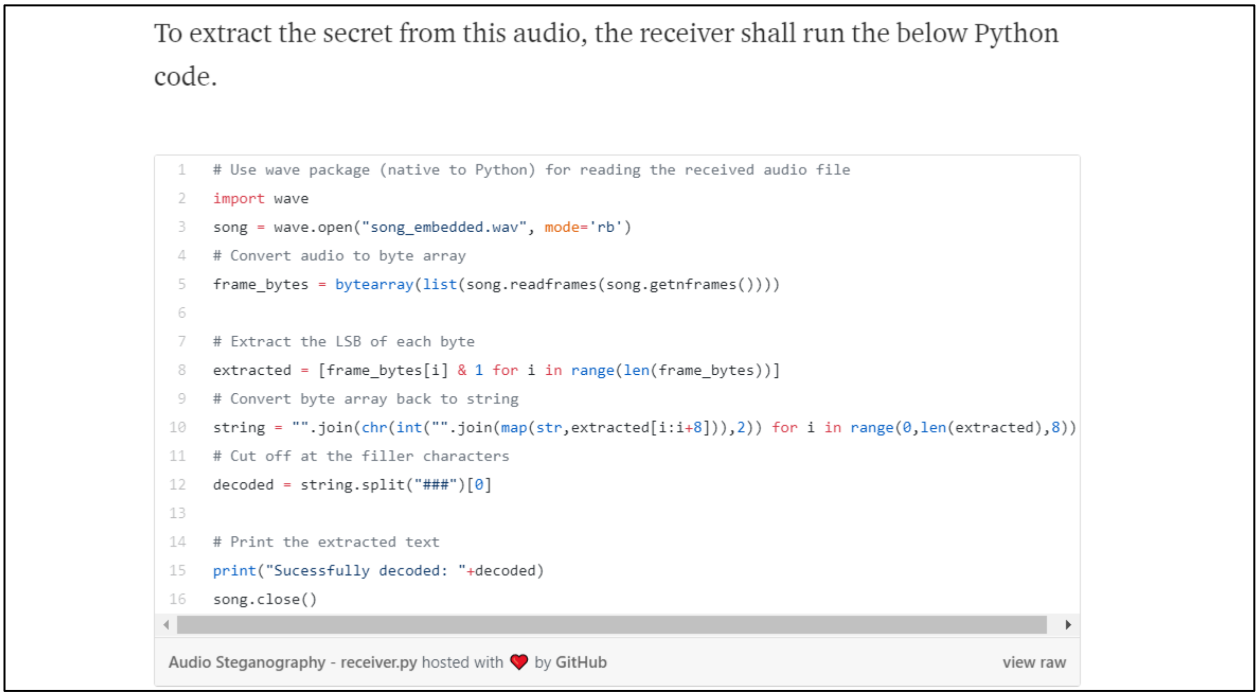
wav lsb

Audio Steganography : The art of hiding secrets within earshot (part 2 ...
https://medium.com/.../audio-steganography-the-art-of-hiding-secrets-within-earshot-...
Jun 17, 2018 - **LSB** algorithm is a classic Steganography method used to conceal the existence of ... We will use .**wav** audio file format for our carrier song.

People also search for

audio steganography tools	how to do audio steganography
audio steganography python	audio steganography techniques
audio steganography ppt	abstract for audio steganography

We found an article, now let’s see if there is code that decode our file…

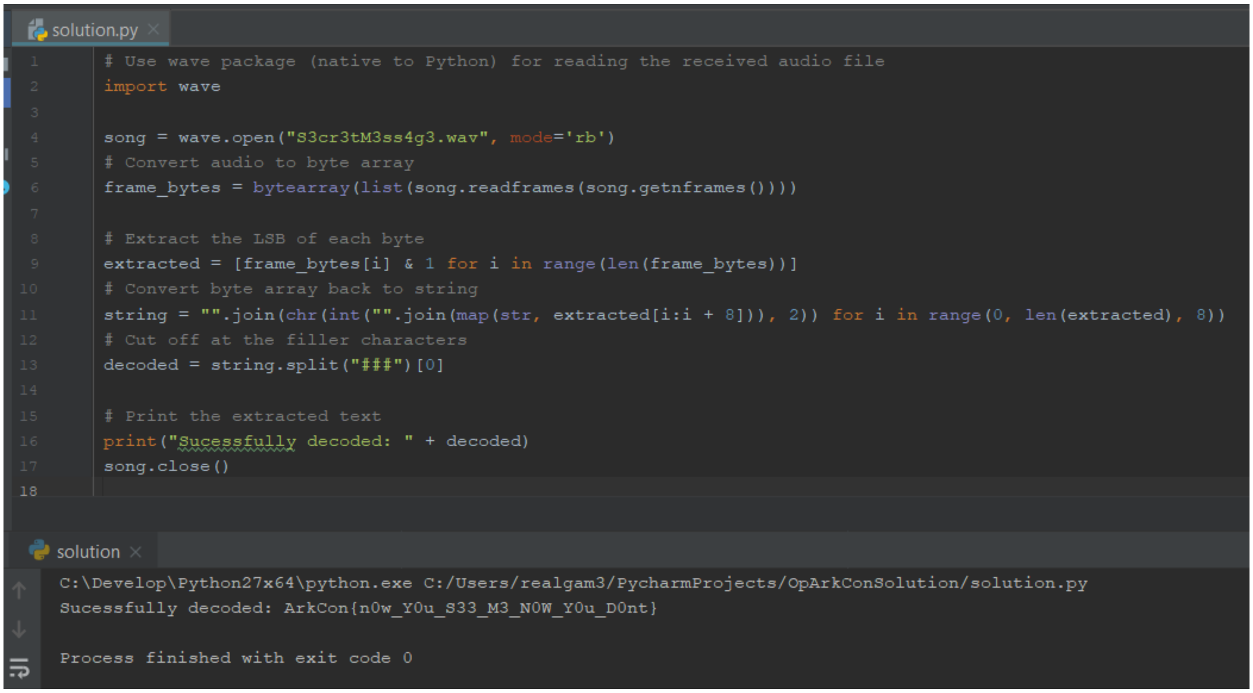


To extract the secret from this audio, the receiver shall run the below Python code.

```python
# Use wave package (native to Python) for reading the received audio file
import wave
song = wave.open("song_embedded.wav", mode='rb')
# Convert audio to byte array
frame_bytes = bytearray(list(song.readframes(song.getnframes())))

# Extract the LSB of each byte
extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
# Convert byte array back to string
string = "".join(chr(int("".join(map(str,extracted[i:i+8])),2)) for i in range(0,len(extracted),8))
# Cut off at the filler characters
decoded = string.split("###")[0]

# Print the extracted text
print("Sucessfully decoded: "+decoded)
song.close()
```

Audio Steganography - receiver.py hosted with ❤ by GitHub view raw

All we need to do now is to copy the content, change the file name to **S3cr3tM3ss4g3.wav** and run the script!



```python
# Use wave package (native to Python) for reading the received audio file
import wave

song = wave.open("S3cr3tM3ss4g3.wav", mode='rb')
# Convert audio to byte array
frame_bytes = bytearray(list(song.readframes(song.getnframes())))

# Extract the LSB of each byte
extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
# Convert byte array back to string
string = "".join(chr(int("".join(map(str, extracted[i:i + 8])), 2)) for i in range(0, len(extracted), 8))
# Cut off at the filler characters
decoded = string.split("###")[0]

# Print the extracted text
print("Sucessfully decoded: " + decoded)
song.close()

```

```
C:\Develop\Python27x64\python.exe C:/Users/realgam3/PycharmProjects/OpArkConSolution/solution.py
Sucessfully decoded: ArkCon{n0w_Y0u_S33_M3_N0W_Y0u_D0nt}

Process finished with exit code 0
```

* Note: we could also write the LSB script but it’s always more time consuming to write code instead of finding it…

We got the flag: **ArkCon{n0w_Y0u_S33_M3_N0W_Y0u_D0nt}**