



An incident responder who's seeking opportunities to work in technology company!

Operator in Cookie Han Hoan

Admin in Cyber Mely

# OSCTF 2024 - Forensic

📌 OSCTF   📌 Writeup   📌 Command and Control   📌 Powershell   📌 Blue Team

Published on 13 Jul 2024

> All solved forensic challenges\_

Hi guys, this time I joined HITCON CTF with my team: World Wide Union, but because of no forensic challenges, I had to go here and try to solve some challenges. Now it's my writeup for them, let's go!

## The Lost Image Mystery

They gave us a corrupted image and we need to recover it. I used `xxd` to check hex values inside:

```
(odin@DFIR)-[~/Downloads]
$ xxd image.png | head -n 10
00000000: d8e0 0049 4600 0101 0000 0100 0100 00ff  ... IF.....
00000010: e201 d849 4343 5f50 524f 4649 4c45 0001  ... ICC_PROFILE..
00000020: 0100 0001 c800 0000 0004 3000 006d 6e74  .....0..mnt
00000030: 7252 4742 2058 595a 2007 e000 0100 0100  rRGB XYZ .....
00000040: 0000 0000 0061 6373 7000 0000 0000 0000  .....acsp.....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000060: 0000 0000 0100 00f6 d600 0100 0000 00d3  .....
00000070: 2d00 0000 0000 0000 0000 0000 0000 0000  -.....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  .....

(odin@DFIR)-[~/Downloads]
$
```

You can guess easily it must be JPG or JPEG file because of `...IF`. From here you can use this [list](#) to check the signature for the file:

FF D8 FF DB	ÿøÿÔ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format <sup>[16]</sup>
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿøÿàNULDLEJFIFNULSOH			
FF D8 FF EE	ÿøÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿøÿá??ExifNULNUL			

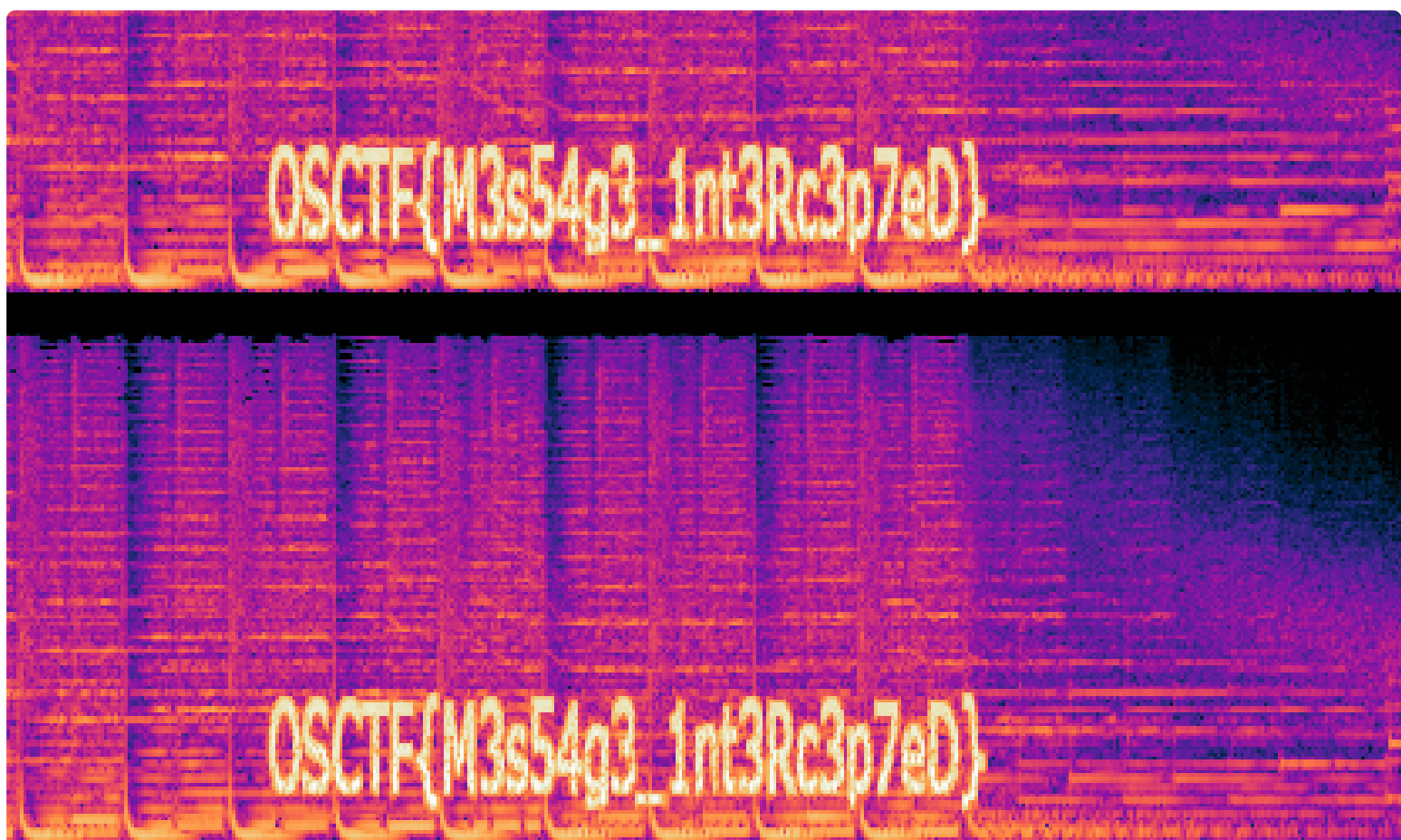
Use `hexedit` to edit hex value, open the file again and enjoy your result:



Flag: OSCTF{W0ah\_F1l3\_h34D3r5}

### The Hidden Soundwave

We got an audio file, and as the title, you need to find hidden information inside the audio file. Very basic, I always check **spectrogram** because it appeared in many CTFs 🤔🤔🤔. From here I used **audacity** to open audio file, change to spectrogram view and I got the flag:



Flag: OSCTF{M3s54g3\_1nt3Rc3p7eD}

### Mysterious Website Incident

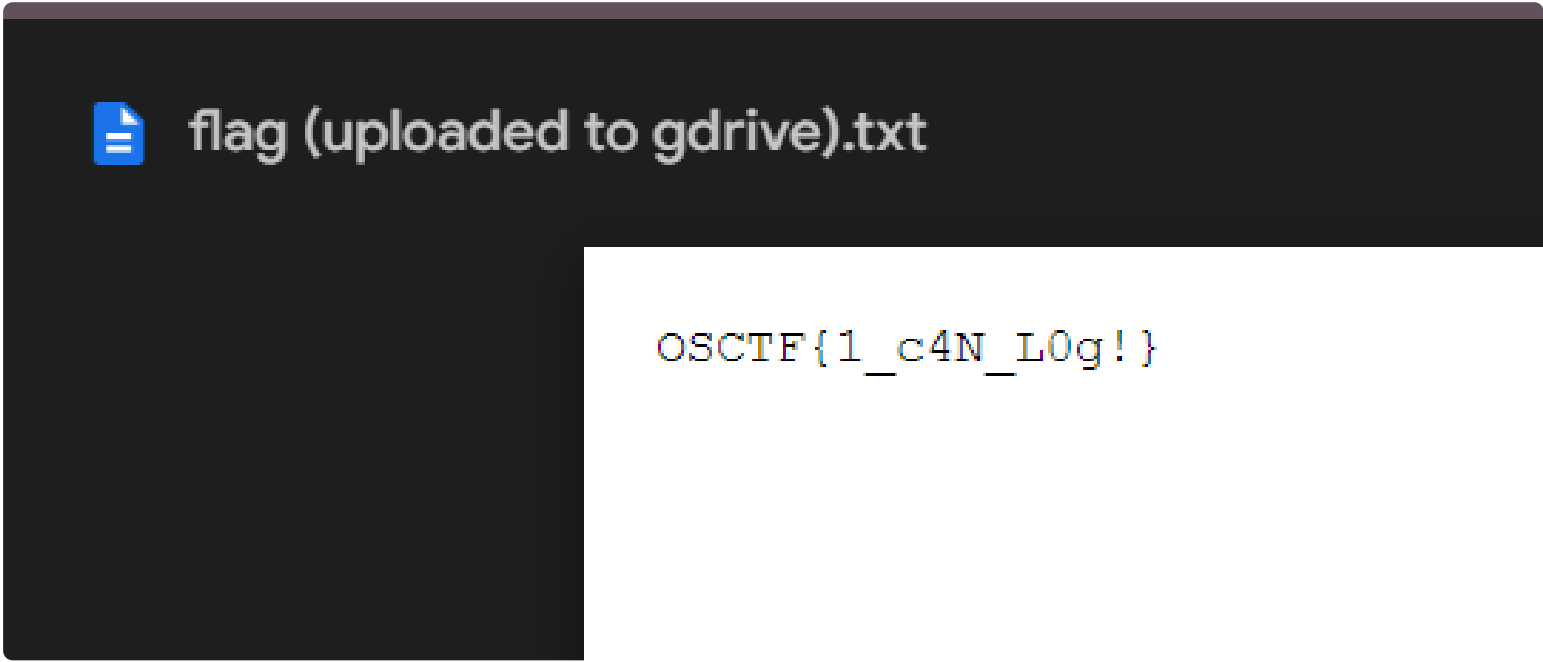
Now we had a nginx log, and very simple, we just open in text editor and analyse it:

```
-D\Downloads\nginx_logs.txt - Mousepad
File Edit Search View Document Help
[Icons] [Address Bar] [Search] [Back] [Forward] [Home] [Stop] [Reload] [Print] [Fullscreen] [Close]

1 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "GET /submit_form HTTP/2.0" 200 2894 "http://example.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
2 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "POST /index.html HTTP/2.0" 302 4859 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
3 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "PUT /index.html HTTP/1.1" 200 1451 "http://example.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
4 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "DELETE /robots.txt HTTP/1.0" 302 1385 "http://test.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
5 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "GET /robots.txt HTTP/1.1" 404 3638 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
6 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/2.0" 200 4931 "http://localhost" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
7 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "POST /submit_form HTTP/1.0" 302 661 "http://test.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
8 192.168.1.3 - - [14/Jun/2024:07:47:14 +0000] "DELETE /image.jpg HTTP/1.0" 200 4169 "http://example.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
9 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/1.1" 302 4116 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
10 192.168.1.3 - - [14/Jun/2024:07:47:14 +0000] "PUT /submit_form HTTP/1.0" 200 2670 "http://test.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
11 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/2.0" 302 3261 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
12 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "DELETE /index.html HTTP/1.0" 404 4942 "http://example.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
13 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "GET /robots.txt HTTP/1.0" 302 1323 "http://localhost" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
14 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/2.0" 302 3746 "http://example.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
15 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "GET /index.html HTTP/1.1" 404 4470 "http://test.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
16 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "PUT /index.html HTTP/2.0" 302 4283 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
17 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "PUT /submit_form HTTP/2.0" 200 922 "http://localhost" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
18 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/1.1" 302 2224 "http://localhost" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
19 192.168.1.3 - - [14/Jun/2024:07:47:14 +0000] "GET /robots.txt HTTP/1.0" 200 523 "http://localhost" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
20 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "POST /robots.txt HTTP/1.0" 302 160 "http://localhost" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
21 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /robots.txt HTTP/1.0" 404 4983 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
22 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/2.0" 302 1513 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
23 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "POST /image.jpg HTTP/1.0" 302 186 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
24 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "GET /submit_form HTTP/2.0" 500 2029 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
25 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /submit_form HTTP/1.0" 302 771 "http://test.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
26 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "PUT /robots.txt HTTP/1.1" 302 3496 "http://example.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
27 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /submit_form HTTP/2.0" 200 4951 "http://test.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
28 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "GET /index.html HTTP/1.1" 200 2706 "http://example.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
29 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "GET /index.html HTTP/2.0" 500 4559 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
30 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "PUT /image.jpg HTTP/1.0" 500 2059 "http://localhost" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
31 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "GET /submit_form HTTP/1.1" 302 4134 "http://test.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
32 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "DELETE /robots.txt HTTP/2.0" 302 1922 "http://test.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
33 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "GET /index.html HTTP/1.1" 302 4489 "http://localhost" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
34 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "POST /image.jpg HTTP/1.1" 200 3519 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
35 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /robots.txt HTTP/1.1" 500 3629 "http://example.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
36 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "GET /index.html HTTP/1.0" 200 797 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
37 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /robots.txt HTTP/1.1" 302 4045 "http://localhost" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
38 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "GET /image.jpg HTTP/2.0" 404 273 "http://test.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
39 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /submit_form HTTP/2.0" 404 1573 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
40 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "POST /image.jpg HTTP/1.0" 302 2407 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
41 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /submit_form HTTP/1.1" 500 402 "http://example.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
42 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "PUT /submit_form HTTP/1.1" 404 1543 "http://test.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
43 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "POST /image.jpg HTTP/1.1" 404 691 "http://example.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
44 192.168.1.3 - - [14/Jun/2024:07:47:14 +0000] "GET /submit_form HTTP/1.0" 200 3436 "http://localhost" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
```

After searching, I found a GG drive link, open it and I got the flag:

```
262 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /image.jpg HTTP/1.1" 302 637 "http://test.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
263 192.168.1.3 - - [14/Jun/2024:07:47:14 +0000] "PUT /robots.txt HTTP/2.0" 302 1758 "http://example.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
264 192.168.1.4 - - [14/Jun/2024:07:47:14 +0000] "GET /index.html HTTP/2.0" 500 1336 "http://example.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
265 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /index.html HTTP/1.1" 404 1477 "http://test.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
266 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "POST /submit_form HTTP/1.0" 200 459 "http://localhost" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
267 my_secret :D - - [14/Jun/2024:07:47:14 +0000] "GET https://drive.google.com/file/d/15tWd7Q1SKtvmW7KG2gYkdmW0bXxBgdj/view?usp=drive_link HTTP/1.0" 200 3625 "http://test.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
268 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "POST /robots.txt HTTP/1.1" 200 2385 "https://test.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
269 192.168.1.3 - - [14/Jun/2024:07:47:14 +0000] "GET /submit_form HTTP/1.1" 500 3247 "http://test.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
270 192.168.1.2 - - [14/Jun/2024:07:47:14 +0000] "PUT /index.html HTTP/2.0" 404 4113 "http://example.com" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
271 10.0.0.1 - - [14/Jun/2024:07:47:14 +0000] "DELETE /image.jpg HTTP/2.0" 500 3042 "http://localhost" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
272 192.168.1.1 - - [14/Jun/2024:07:47:14 +0000] "PUT /robots.txt HTTP/1.0" 200 4054 "http://test.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36"
```



Flag: OSCTF{1\_c4N\_L0g!}

## Phantom Script Intrusion

For this challenge, they gave us a PHP code, and it was obfuscated:

```
1 c?php
2 goto L56v2; apeWK: ${"\x70\x141\x72\x61"} = str_rot13("\x24\x7b\x22\x14\x78\x34\x37\x134\x78\x34\x143\x5c\x78\x164\x66\x5c\x170\x34\x32\x134\x78\x64\x61\x5c\x170\x34\x63\x134\x78\x35\x33\x42\x7d"); goto G9fZX; L56v2: $
{"\x47\x4c\x4f\x42\x101\x141\x23"} = "\x50\x58\x58\x70\x73\x72\x2f\x57\x163\x158\x30\x162\x164\x75\x72\x6c\x56\x61\x164\x2f\x73\x31\x146\x57\x62"; goto apeWK; XT2kv: if (strlen("${\x70\x141\x72\x32}") > 0) { ${"\x166\x61\x72\x33"} = $
{"\x76\x61\x72\x32"}; } else { ${"\x166\x141\x72\x63"} = ''; } goto ZYamk; VZP30: foreach (str_split("${\x166\x141\x72\x33}") as ${"\x166\x61\x72\x35"}) { ${"\x166\x141\x162\x34"} .= chr(ord("${\x166\x141\x162\x65"} - 1)); } goto Ly_yq; G9fZX: $
{"\x70\x141\x162\x32"} = base64_decode("${\x166\x61\x162\x31}"); goto XT2kv; Ly_yq: eval("${\x70\x61\x72\x34}"); goto IFMxz; ZYamk: ${"\x166\x141\x162\x64"} = ''; goto VZP30; IFMxz: ?>
```

To make it easier to follow, I deobfuscated it and this is my final script:

```

{"GLOBALS"} = "hXXps://sh0rtur1.at/s1fW2";
{"var1"} = str_rot13("${"\x47\x4c\x4f\x42\x101\x141\x23"}");
{"var2"} = base64_decode("${{"var1"}});
if (strlen("${"var2"}) > 0) {
    {"var3"} = {"var2"};
} else {
    {"var3"} = "";
}
{"var4"} = "";
foreach (str_split("${"var3"}) as {"var5"}) {
    {"var4"} .= chr(ord("${"var5"}) - 1);
}
eval("${{"var4"}});
```

There's a **shorturl** link, access it and got the flag:



 flag.txt

```
OSCTF{M4lW4re_0bfU5CAt3d}
```

Flag: OSCTF{M4lW4re\_0bfU5CAt3d}

## PDF Puzzle

Just check the metadata of the file => get the flag:

```
(odin@DFIR)-[~/Downloads]
$ exiftool My_pdf.pdf
ExifTool Version Number      : 12.76
File Name                    : My_pdf.pdf
Directory                   : .
File Size                    : 18 kB
File Modification Date/Time  : 2024:07:13 08:27:41-07:00
File Access Date/Time       : 2024:07:13 08:27:42-07:00
File Inode Change Date/Time  : 2024:07:13 08:15:39-07:00
File Permissions             : -rwxrwx---
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.7
Linearized                   : No
Author                       : OSCTF{H3il_M3taD4tA}
Create Date                  : 2008:07:01 07:24:47+02:00
Creator                      : Pages
Modify Date                   : 2008:07:01 07:24:47+02:00
```

Flag: OSCTF{H3il\_M3taD4tA}

## Seele Vellerei

In this challenge we had a docx file. At first I tried to find out VBA code inside, but there's nothing, so I think maybe flag was hidden somewhere inside the file. Because word structure is same with zip file, you can use **binwalk** to extract all files inside:

```
(odin@DFIR)-[~/Downloads/_SeeleVollerei.docx.extracted]
$ ls -la
total 1692
drwxr-xr-x  5 odin odin   4096 Jul 13 08:18 .
drwxr-xr-x 18 odin odin   4096 Jul 13 08:18 ..
-rw-r--r--  1 odin odin 1706635 Jul 13 08:18 0.zip
-rw-r--r--  1 odin odin  1362 Jan  1 1980 '[Content_Types].xml'
drwxr-xr-x  2 odin odin   4096 Jul 13 08:18 _rels
drwxr-xr-x  2 odin odin   4096 Jul 13 08:18 docProps
drwxr-xr-x  5 odin odin   4096 Jul 13 08:18 word

(odin@DFIR)-[~/Downloads/_SeeleVollerei.docx.extracted]
$ cd word

(odin@DFIR)-[~/Downloads/_SeeleVollerei.docx.extracted/word]
$ ls
_rels  document.xml  fontTable.xml  media  settings.xml  styles.xml  theme  webSettings.xml
```

Navigate to **document.xml** where content of file was stored, use **grep** and I found the flag:

```
<w:rsidR="00B4326E" w:rsidP="00B4326E"><w:pPr><w:ind w:left="2880" w:firstLine="7" lag: OSCTF{V3l10n4_1s_Gr43t}</w:tR="00B4326E" w:rsidRPr="00B4326E" D64B" w14:textId="77777777" w:rsid="00B4326E" w14:paraId="152
```

Flag: OSCTF{V3l10n4\_1s\_Gr43t}

FOR101

I love this challenge most, so I will explain it carefully. In this challenge we had a zip file contains datas inside an User directory. I opened it by 7z:

C:\Users\Admin\Downloads\Users.zip\Users\Administrator\							
Name	Size	Packed Size	Modified	Created	Accessed	Attributes	
3D Objects	298	160	2024-07-13...			RD	
AppData	220 363 706	95 179 694	2024-07-13...			HD	
Application Data	0	0	2024-06-29...			HSD	
Contacts	412	180	2024-07-13...			RD	
Cookies	0	0	2024-06-29...			HSD	
Desktop	584 234	579 157	2024-07-13...			RD	
Documents	4 498	501	2024-07-13...			RD	
Downloads	332 567 903	320 356 403	2024-07-13...			RD	
Favorites	690	423	2024-07-13...			RD	
Links	1 961	1 131	2024-07-13...			RD	
Local Settings	0	0	2024-06-29...			HSD	
Music	504	190	2024-07-13...			RD	
My Documents	0	0	2024-06-29...			HSD	
NetHood	0	0	2024-06-29...			HSD	

After searching, I found an .eml file at \Users\Administrator\Downloads\Outlook Files named Notifications.eml:

C:\Users\Admin\Downloads\Users.zip\Users\Administrator\Downloads\Outlook Files\						
Name	Size	Packed Size	Modified	Created	Accessed	
Notifications.eml	526 985	400 336	2024-07-08...			

I extracted it to my machine and use ThunderBird to open the file:



You can see that there's a VBA code and it's obfuscated, and we don't any choice except deobfuscate it by your hand or you can read code by **Ctrl+F+the\_name\_of\_func**. After this I found that function will process a string looks like URL:

[illegible][illegible]

From here I can realise that our function are trying to decode that string. Based on their function, I rewrote a Python script for automatic decoding:

```
def decode_string(encoded_string, decode_table, encoded_substitution):
    decoded_string = ""
    for y in range(len(encoded_string)):
        char_index = decode_table.find(encoded_string[y])
        if char_index > -1:
            decoded_char = encoded_substitution[char_index]
            decoded_string += decoded_char
        else:
            decoded_string += encoded_string[y]
    return decoded_string

encoded_string = "Ü³³Bb://B_b³Ekài~B#/jàEÄ/²_Ä/À60äm_ŠÀ"
decode_table = " ?!@#$$%^&*( )_+|0123456789abcdefghijklmnopqrstuvwxyz,.-~ABCDEFGHIJKLMNOPQRSTUVWXYZ"
encoded_substitution = "äXL1lYU~Üä,Ca²ZfÄ@d0-cq³áoŠäJV9AQn vbj0Ä7WI!RBg$Ho?K_F3.Óp¥ÖePâzkŦÛNØ"
decoded_string = decode_string(encoded_string, decode_table, encoded_substitution)
print(decoded_string)
```



```
ctf.py > ...  
1 def decode_string(encoded_string, decode_table, encoded_substitution):  
2     decoded_string = ""  
3     for y in range(len(encoded_string)):  
4         char_index = decode_table.find(encoded_string[y])  
5         if char_index > -1:  
6             decoded_char = encoded_substitution[char_index]  
7             decoded_string += decoded_char  
8         else:  
9             decoded_string += encoded_string[y]  
10    return decoded_string  
11    encoded_string = "Ü³²Bb://B_b³Ekài~B#/jàEÄ/²_Ä/À6øäm_§À"  
12    decode_table = " ?!@#%$^&*()_|0123456789abcdefghijklmnopqrstuvwxyz.,-~ABCDEFGHIJKLMNOPQRSTUVWXYZ;¡²³´µ¶·¸¹º»¼½¾¿ÀÁÂÃÄÅ Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ø ù ú û ü ý þ ÿ"  
13    encoded_substitution = "äXLllyU~Üä,Ca²ZfÄ@dO~cq³äOsAJV9AQnrbj0Ä7WI!RBg$Ho?K_F3.ÖpyöePázk¶JÜN0%G mü^M&+¡#4)uÀrt8(Sw|T*Â$Eâyhiúx65Dà¿2ÄÖ"  
14    decoded_string = decode_string(encoded_string, decode_table, encoded_substitution)  
15    print(decoded_string)  
16
```

PROBLEMS 7 DEBUG CONSOLE OUTPUT TERMINAL PORTS Python + ▢

- PS C:\Users\Admin\Documents\Code\Python> & C:/Users/Admin/AppData/Local/Programs/Python/Python312/python.exe c:/Users/Admin/Documents/Code/Python/ctf.py https://pastebin.pl/view/ra/8cf50a28
- PS C:\Users\Admin\Documents\Code\Python>

I got a link, now let's open it and see what inside:

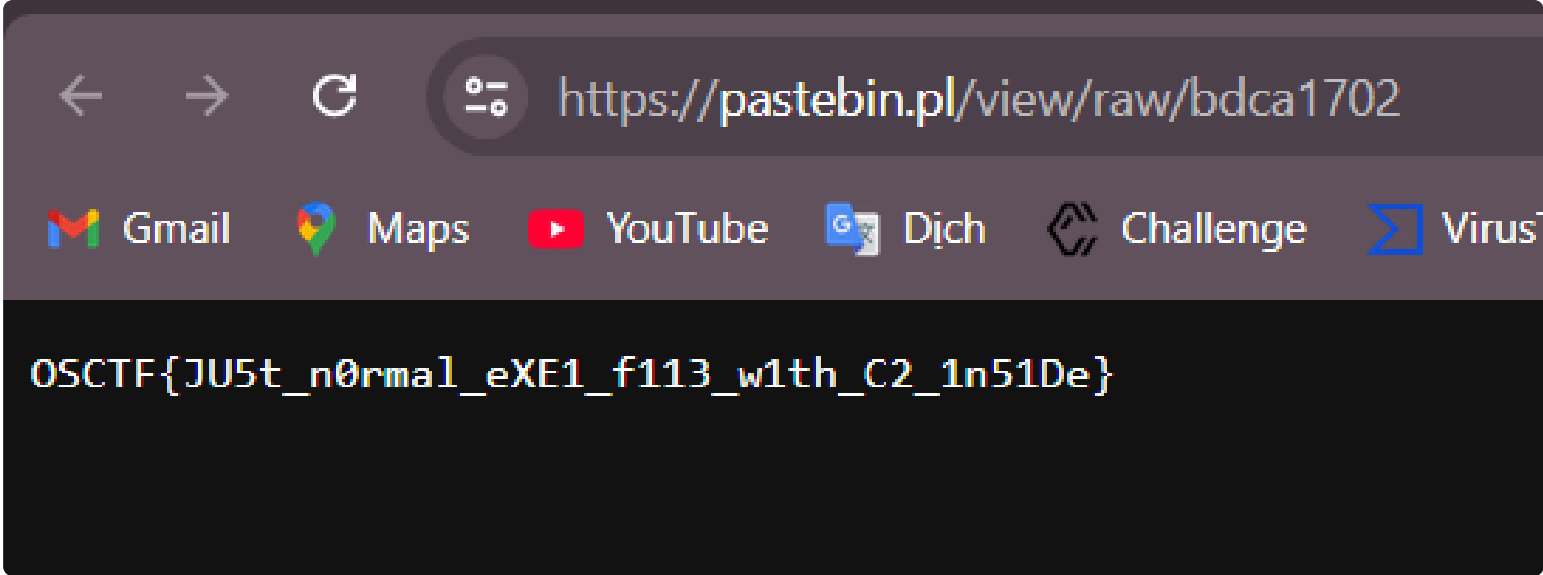
[illegible]

You can see that there's a Powershell script and it will execute a command that was encoded by base64. Now we continue to decode base64 string:









Flag: OSCTF{JU5t\_n0rmal\_eXE1\_f113\_w1th\_C2\_1n51De}

Thank you for watching, hope you enjoy this. I solved other challenges but I still love forensic so I just wrote writeup for it 😂😂😂. See you in other CTFs, bye!!!

### related posts

- 🔧 [DUCTF 2024 - Forensic](#)
- 🔧 [UIUCTF 2024 - SoMeSINT writeup](#)
- 🔧 [WaniCTF 2024 - Forensic](#)

### all tags

- 🔖 AES Decrypt
- 🔖 AKASEC
- 🔖 BITSCTF
- 🔖 BYUCTF
- 🔖 Blue Team
- 🔖 CTFtime
- 🔖 Command and Control
- 🔖 DES3 decrypt
- 🔖 DFIR
- 🔖 DUCTF
- 🔖 Email forensic
- 🔖 Forensic
- 🔖 Git log
- 🔖 HackTheBox
- 🔖 JavaScript
- 🔖 KCSC
- 🔖 Macros
- 🔖 Memory Forensic
- 🔖 MireaCTF
- 🔖 Network Forensic
- 🔖 OSCTF
- 🔖 OSINT
- 🔖 Powershell
- 🔖 Real case
- 🔖 Redis
- 🔖 TheCyberCoopCTF
- 🔖 TrueCrypt
- 🔖 UIUCTF
- 🔖 Virustotal
- 🔖 Volatility
- 🔖 WaniCTF
- 🔖 WannaGame
- 🔖 Wireshark
- 🔖 Word
- 🔖 Writeup

