

## Secure-Contain-Protect Challenge

Challenge

44 Solves



# Secure-Contain-Protect

## 10

You have successfully gotten into the file.. Find the information that John left behind regarding his whereabouts.

Flag Format: SBTVIP{---}

Flag

Submit

**Answer:** This challenge is a second part of the Switching Teams Challenge. Let start by looking at all the files that came out of admin.zip

```
root@kali:/home/kali/Pictures/John# ls -lRah
.:
total 36K
drwxrwxrwx  6 root root 4.0K Feb 21 17:36 .
drwxrwxrwx 11 kali kali 12K Mar 16 08:16 ..
-rw-r--r--  1 root root  30 Feb 21 17:52 Flag1.txt
drwx-----  3 root root 4.0K Feb 21 18:16 Homework
drwx-----  3 root root 4.0K Feb 21 17:38 'Personal Stuff'
drwx-----  2 root root 4.0K Feb 21 17:31 Pictures
drwx-----  2 root root 4.0K Feb 21 17:36 Work

./Homework:
total 12K
drwx-----  3 root root 4.0K Feb 21 18:16 .
drwxrwxrwx  6 root root 4.0K Feb 21 17:36 ..
drwx-----  2 root root 4.0K Feb 21 18:16 Churchill

./Homework/Churchill:
total 392K
drwx-----  2 root root 4.0K Feb 21 18:16 .
drwx-----  3 root root 4.0K Feb 21 18:16 ..
-rw-r--r--  1 root root 105K Feb 21 18:16 .jpeg
-rw-r--r--  1 root root 266K Feb 21 18:16 Winston-Churchill-1.jpg
-rw-r--r--  1 root root 243 Feb 21 18:16 'Winston Churchill Biography, World War II, & Facts ....URL'
-rw-r--r--  1 root root 236 Feb 21 18:16 'Winston Churchill - Wikipedia.URL'

'./Personal Stuff':
total 16K
drwx-----  3 root root 4.0K Feb 21 17:38 .
drwxrwxrwx  6 root root 4.0K Feb 21 17:36 ..
drwx-----  3 root root 4.0K Feb 21 17:40 Certifications
-rw-r--r--  1 root root 228 Feb 21 17:38 How-To-Build-NGINX-Server.txt

'./Personal Stuff/Certifications':
total 16K
drwx-----  3 root root 4.0K Feb 21 17:40 .
drwx-----  3 root root 4.0K Feb 21 17:38 ..
-rw-r--r--  1 root root 257 Feb 21 17:40 ITFUNDAMENTALS.txt
drwx-----  2 root root 4.0K Feb 21 17:41 SBT

'./Personal Stuff/Certifications/SBT':
total 12K
drwx-----  2 root root 4.0K Feb 21 17:41 .
drwx-----  3 root root 4.0K Feb 21 17:40 ..
-rw-r--r--  1 root root 168 Feb 21 17:41 rant.txt
```

```
./Pictures:  
total 16M  
drwx----- 2 root root 4.0K Feb 21 17:31 .  
drwxrwxrwx 6 root root 4.0K Feb 21 17:36 ..  
-rw-r--r-- 1 root root 2.8M Feb 21 17:30 dan-gold-P_0R02ArdLE-unsplash.jpg  
-rw-r--r-- 1 root root 884K Feb 21 17:30 davisco-5E5N49RWtbA-unsplash.jpg  
-rw-r--r-- 1 root root 2.8M Feb 21 17:31 gatis-marcinkevics-a5uptAdUmjE-unsplash.jpg  
-rw-r--r-- 1 root root 1.5M Feb 21 17:31 ivan-bandura-5cwigXmGWTTo-unsplash.jpg  
-rw-r--r-- 1 root root 6.2M Feb 21 17:31 matteo-bernardis-QpIay05KIRE-unsplash.jpg  
-rw-r--r-- 1 root root 1.3M Feb 21 17:31 mohamed-nashah-GIsFHopvbPA-unsplash.jpg
```

We have a few files including a hidden jpeg.



Nothing special about this image.

There are a few txt files, one of interest is the Work/To-Do.txt. Inside there is a link  
<https://pastebin.com/DaA5uvk4>

```
root@kali:/home/kali/Pictures/John/Work# cat To-Do.txt  
1. Rename Business to Secure in the Deep Blue  
2. Steal BT1 Plan  
3. Evade any feds  
4. Rick Roll some investigators  
5. Hack the World  
6. 4kvu5AaD\moc.nibetsap\\:sptth
```

If you go to that site we see the following.

1010001010101  
A GUEST FEB 21ST, 2020 125 NEVER

Not a member of Pastebin yet? [Sign Up](#), it unlocks many great features!

text 0.04 KB

```
1. uggcf://jjj.erqqvg.pbz/e/FrphervagurQrrc0yhr
```

#### RAW Paste Data

```
uggcf://jjj.erqqvg.pbz/e/FrphervagurQrrc0yhr
```

This looks to be a URL that is ROT13 encoded, let's use hURL to decode.

```
root@kali:/home/kali/Pictures/John/Work# hURL -7 uggcf://jjj.erqqvg.pbz/e/FrphervagurQrrc0yhr
Original string :: uggcf://jjj.erqqvg.pbz/e/FrphervagurQrrc0yhr
Converted to ROT13 :: https://www.reddit.com/r/SecureintheDeepBlue
```

Another url to a reddit page that contains some binary.

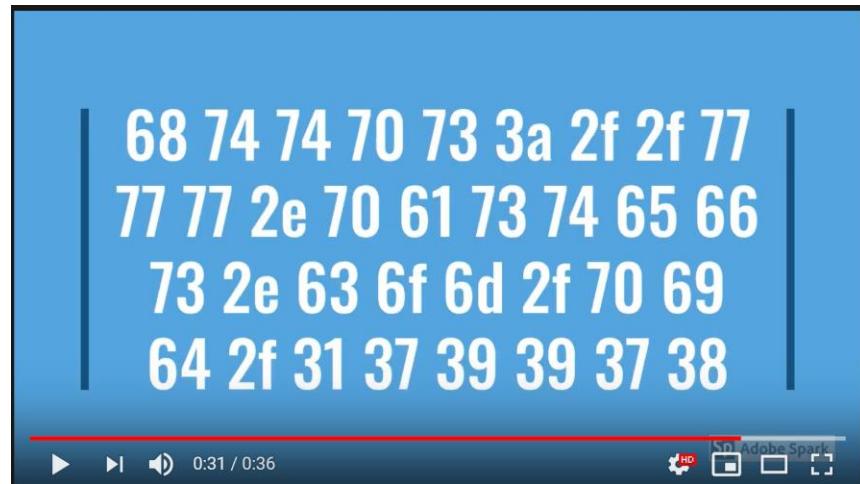
A screenshot of a Reddit post. The title is "10101101001" and the author is "(self.SecureintheDeepBlue)". It was submitted 23 days ago by cyberneticwired. The post body contains the following binary code:

```
01101000 01110100 01110100 01110000 01110011 00111010 00101111 00101111
01110111 01110111 01110111 00101110 01111001 01101111 01110101 01110100
01110101 01100010 01100101 00101110 01100011 01101111 01101101 00101111
01110111 01100001 01110100 01100011 01101000 00111111 01110110 00111101
01001111 01110011 01110111 01010000 00110111 01001010 01110000 01010001
01111010 01101101 01001101
```

Below the post are standard Reddit interaction buttons: comment, share, save, hide, give award, report, and crosspost.

Decoding the binary gives us the following. <https://www.youtube.com/watch?v=OswP7JpQzmM>

The YouTube video looks like a confession tape with one important frame that contains a hex string. 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 61 73 74 65 66 73 2e 63 6f 6d 2f 70 69 64 2f 31 37 39 39 37 38 decoded to <https://www.pastefs.com/pid/179978>





PasteFS



new



recent



trends

search

👤 guest on 22 Feb, 2020

1. SBTVIP{3vidence\_acquir3D}
- 2.
3. I give up.
4. I John Kelvin stole work from SBT because I didn't study hard enough.
- 5.
6. I have seen the content.
- 7.
8. I can't believe how much effort was put into it.
- 9.
10. I did something WRONG.
- 11.
12. I'm sorry SBT. Forgive me.
- 13.
14. <https://securityblue.team/why-btl1/>

When you visit the site you see the final confession and the flag.

FLAG: SBTVIP{3vidence\_acquir3D}