

# Day 2 Challenge 1

By Bingsu Strawberry from IIUM

## Step 1:

We are given a powershell script only. First step we do is try to understand what the script does.

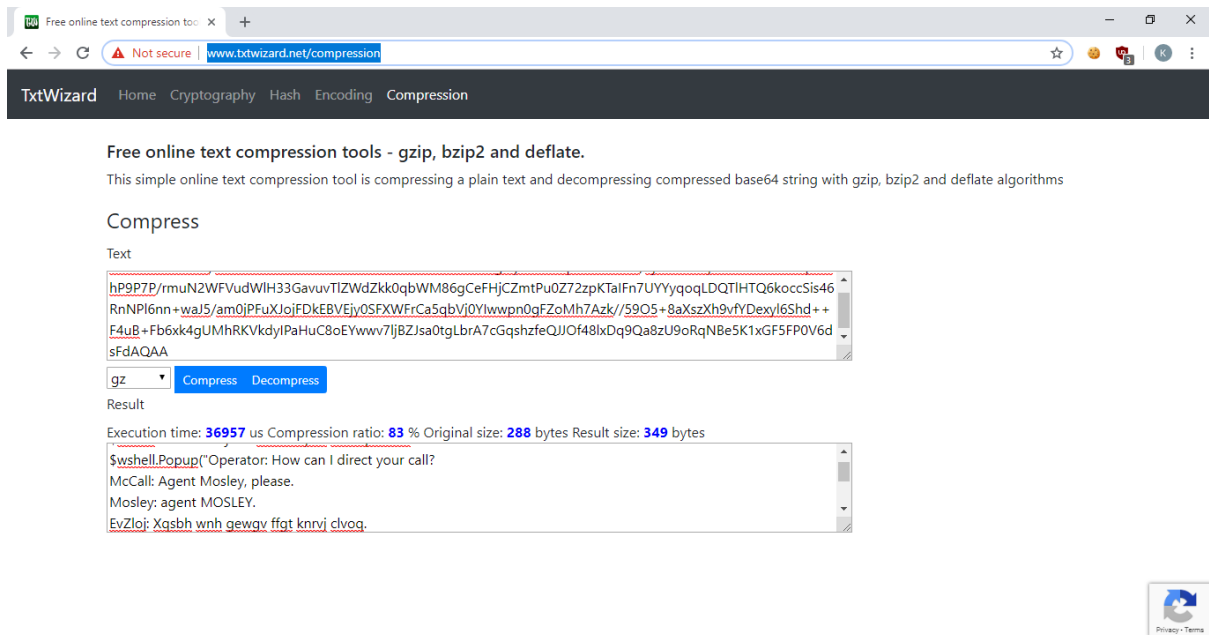


```
powershell.exe -nop -w hidden -c "$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName='powershell.exe';  
$s.Arguments='-noni -nop -w hidden -c &{[scriptblock]::create((New-Object IO.StreamReader(New-Object  
IO.Compression.GzipStream((New-Object IO.MemoryStream([Convert]::FromBase64String  
( 'H4sIAAAAAAAAA/z1OW2vCMBh97684iLANNChuCIUhZsk2mHPgwy4v0savqTE2TdI01rH/vjrHns4dTje4nJTCLV4o9JepJF6hP9P7P/rmuN2WFVudW1H33Gav  
uvT1ZwdZkk0qbWm86gCeFHjCZmtPu0Z72zpKTaIFn7UYyYqoqLDQT1HTQ6koccSis46RnNP16nn  
+waJ5/am0jPFuXJojFDkEBVEjy0SFXWFrCa5qbVj0YIwwpn0gFZoMh7Azk//5905+8aXszXh9vfYDexy16Shd++F4uB  
+Fb6xk4gUMhRKVkyIPaHuC8oEYwvv71jBZJsa0tgLbrA7cGqshzfeQJJ0f481xDq9Qa8zU9oRqNB5K1xGF5FP0V6dsFdAQAA' )))),  
[IO.Compression.CompressionMode]::Decompress))).ReadToEnd()}';$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;  
$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```

## Step 2:

We decompress the compressed part of the script to make sure it is not anything malicious.

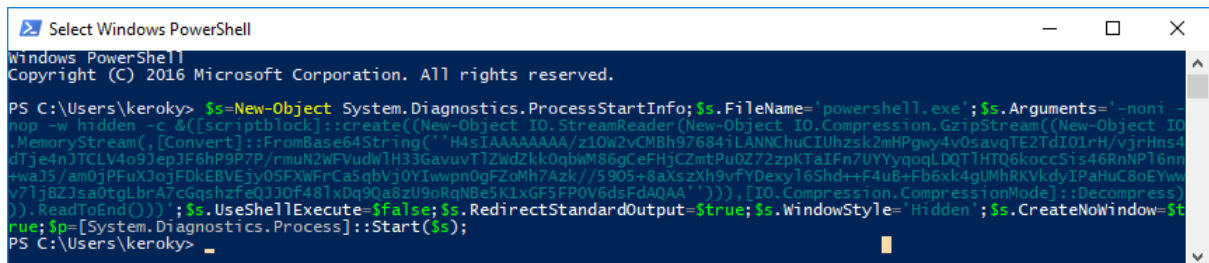
We used a website online to decompress it. [Link here](#)



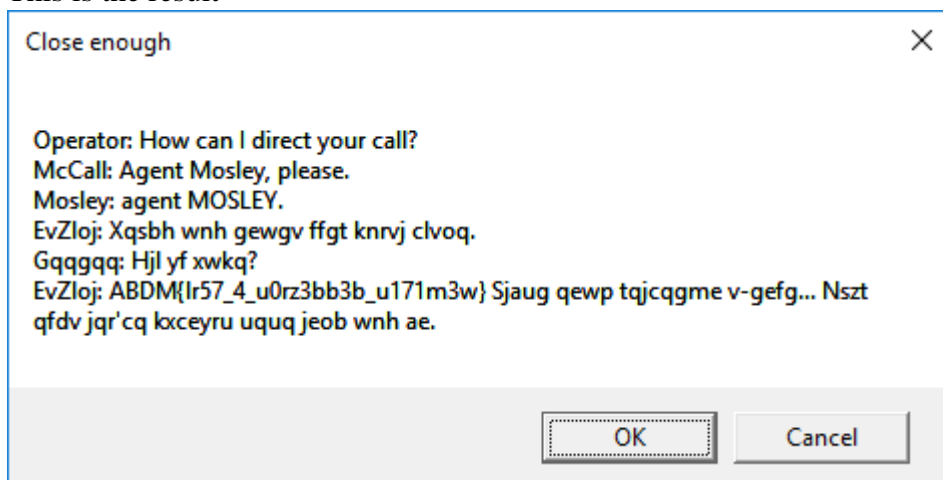
The code doesn't seem to pose any threats. We think it's just used to display a message. Time to put it to test!

### Step 3:

Remove the unnecessary part from the code and put it into powershell and run it.



This is the result



It seems to be a dialog of some sort.

The bottom part seems to be encrypted. We are not sure what type of encryption is used here.

#### **Step 4:**

A quick google search of the dialog showed that it is from a movie called The Equalizer from the year 2014.

#### **Quotes**

**FBI Operator** : FBI. How can I direct your call?

**Robert McCall** : Agent Mosley, please.

**Agent Mosley** : Agent Mosley.

**Robert McCall** : Heard you found some money today.

**Agent Mosley** : Who is this?

**Robert McCall** : Concerned citizen. Check your personal e-mail... Make sure you're sitting down when you do.

Now we can see a relation between the dialog we have and the actual dialog. The last part seemed to contain our flag.

#### **Step 5:**

The relation of the flag to the actual dialog :

ABDM{lr57\_4\_u0rz3bb3b\_u171m3w} = concerned citizen

We can assume the last part of the flag to be concerned citizen.

u0rz3bb3b\_u171m3w = concerned citizen

We can try to verify this.

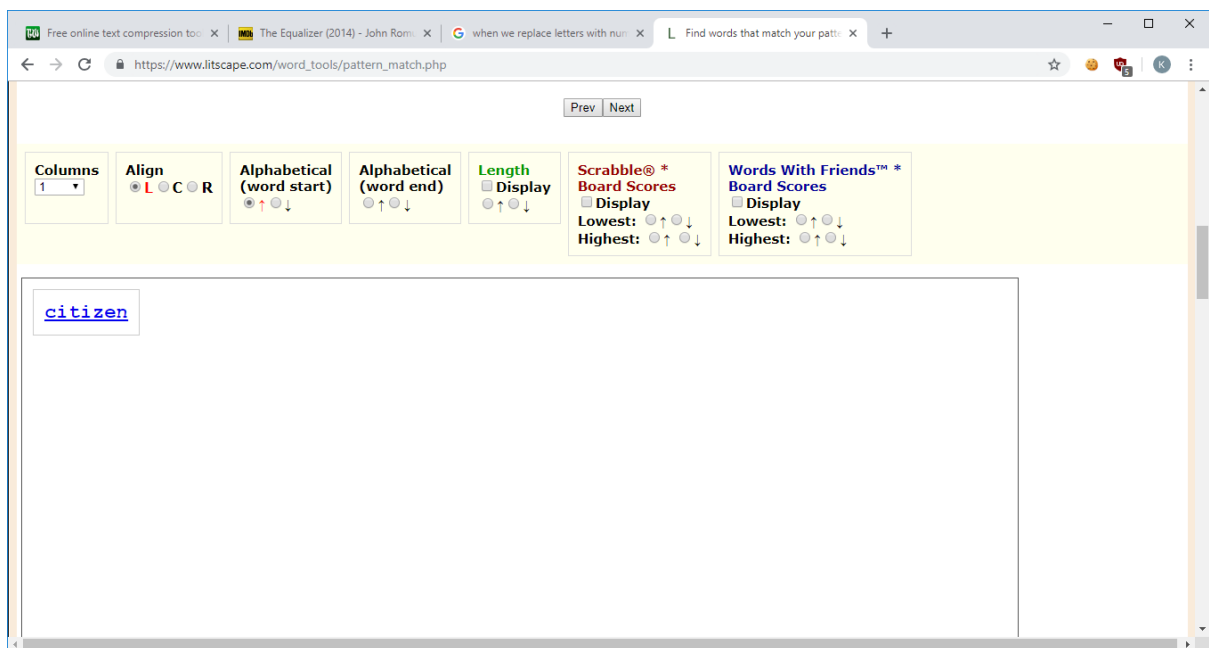
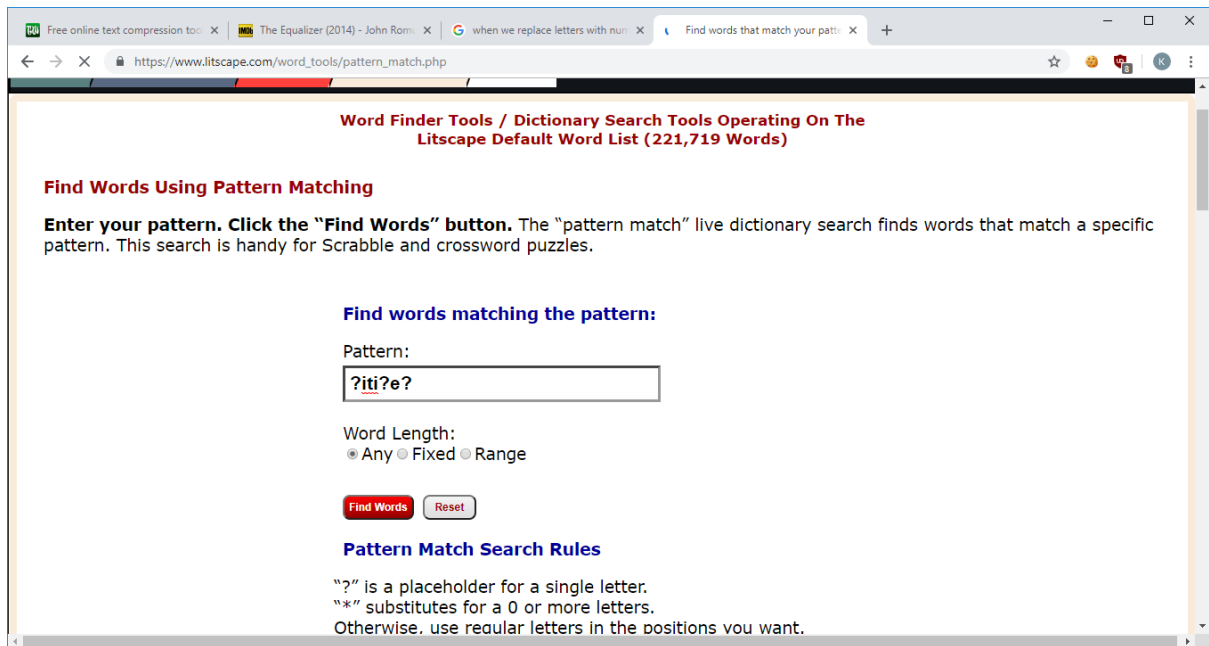
#### **Step 6:**

We believe the flag is written in leet speak or the act of changing letters with numbers .

The text now looks like this

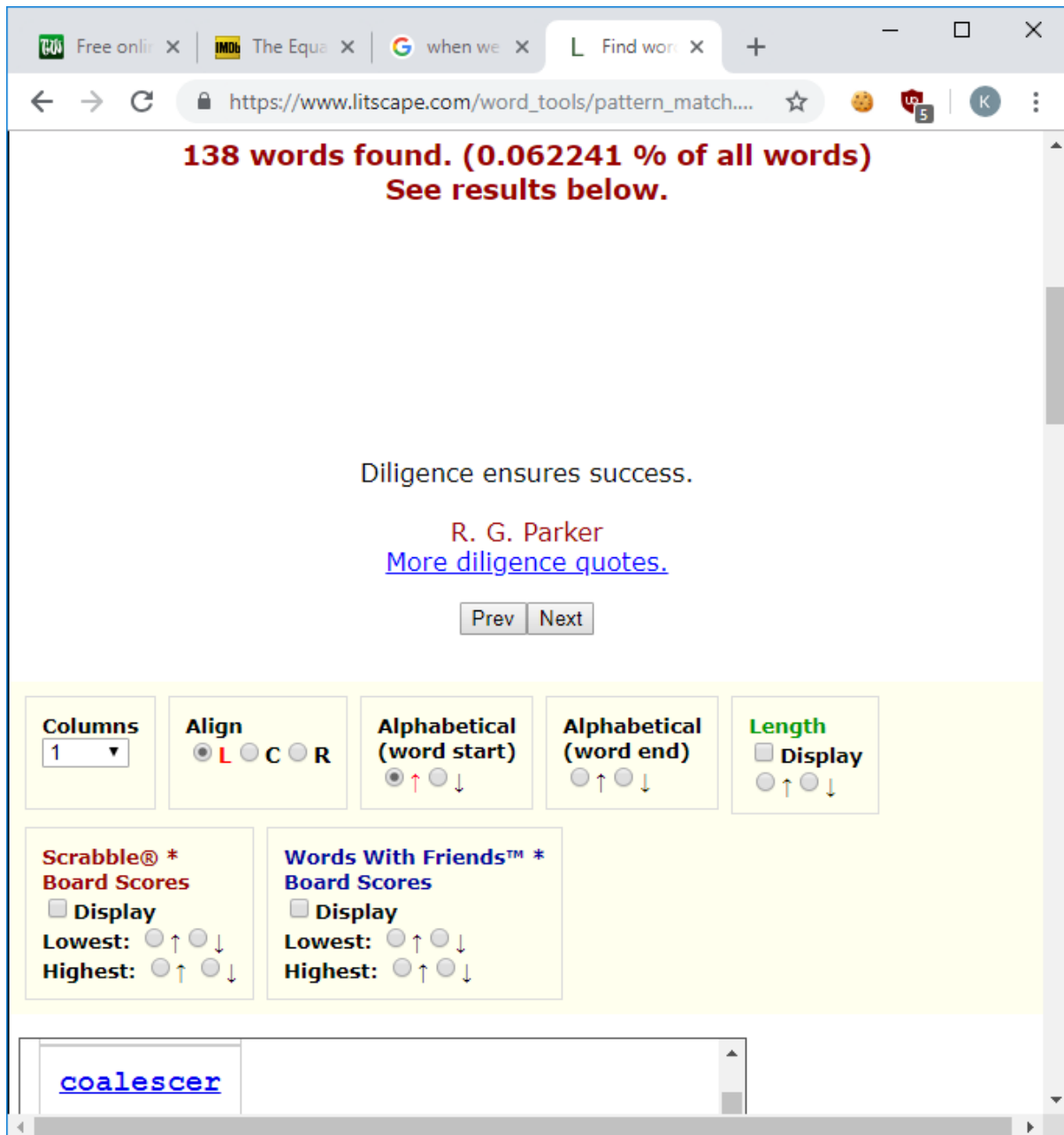
uOrzEbbEb and uITImEw

Try to do a pattern search for the words we have



The result is uITImEw = citizen

For the case of uOrzEbbEb , we found 138 words



But if we refer back to the original dialog, we can safely assume that `uOrzEbbEb` = concerned,

Now for the rest of the text, 4 is A .

Doing a pattern finder for `lrST` yields us 37 words but the most probable word we assume is just. Leaving us with `lrST` = just.

#### **Step 7:**

Now our flag looks like `ABDM{just_a_concerned_citizen}`

Try to convert it back to the format it usually is and we get

KPMG{ju57\_4\_c0nc3rn3d\_c171z3n} as our flag