

LinkedIn: [Kelvin Kimotho](#)

CYBER TALENTS

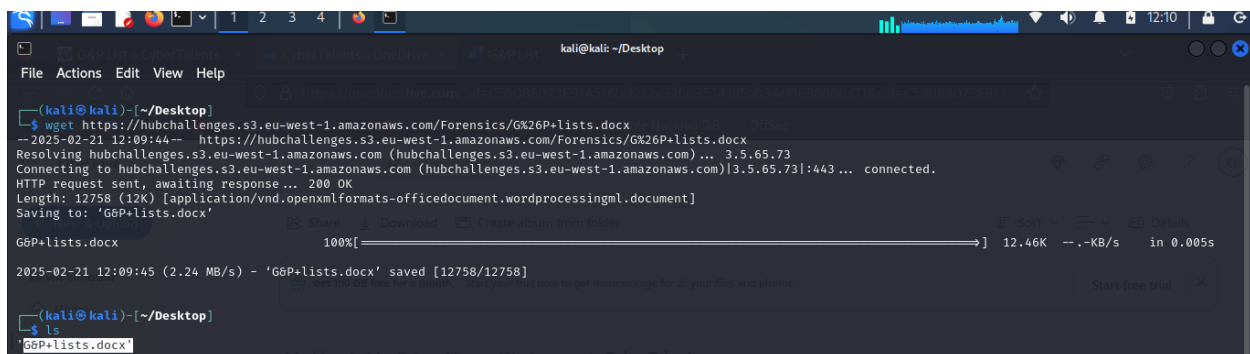
Challenge Name: G&P List

Challenge Description

Just Open the File and Capture the flag . Submission in MD5

Solution

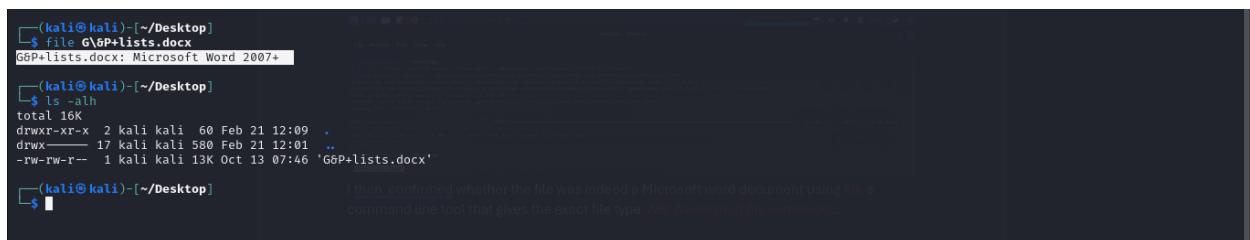
I began by downloading the challenge files using **wget** tool a command-line tool for downloading files.



```
(kali@kali)-[~/Desktop]
$ wget https://hubchallenges.s3.eu-west-1.amazonaws.com/Forensics/GX26P+lists.docx
--2025-02-21 12:09:44-- https://hubchallenges.s3.eu-west-1.amazonaws.com/Forensics/GX26P+lists.docx
Resolving hubchallenges.s3.eu-west-1.amazonaws.com (hubchallenges.s3.eu-west-1.amazonaws.com) ... 3.5.65.73
Connecting to hubchallenges.s3.eu-west-1.amazonaws.com (hubchallenges.s3.eu-west-1.amazonaws.com)[3.5.65.73]:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12758 (12K) [application/vnd.openxmlformats-officedocument.wordprocessingml.document]
Saving to: 'G6P+lists.docx'
G6P+lists.docx
100%[====>] 12.46K --.-KB/s in 0.005s
2025-02-21 12:09:45 (2.24 MB/s) - 'G6P+lists.docx' saved [12758/12758]

(kali@kali)-[~/Desktop]
$ ls
'G6P+lists.docx'
```

I then confirmed whether the file was indeed a Microsoft word document using **file** a command line tool that gives the exact file type. *NB: Never trust file extensions.*



```
(kali@kali)-[~/Desktop]
$ file G\6P+lists.docx
G6P+lists.docx: Microsoft Word 2007+

(kali@kali)-[~/Desktop]
$ ls -alh
total 16K
drwxr-xr-x 2 kali kali 60 Feb 21 12:09 .
drwx----- 17 kali kali 580 Feb 21 12:01 ..
-rw-rw-r-- 1 kali kali 13K Oct 13 07:46 'G6P+lists.docx'
```

Since this challenge was a digital forensics challenge, I went ahead and examined the file's meta data using a tool called **exiftool**. I didn't find anything suspicious.

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ exiftool G6P+lists.docx
ExifTool Version Number      : 12.76
File Name                    : G6P+lists.docx
Directory                    : 
File Size                     : 13 kB
File Modification Date/Time   : 2024:10:13 07:46:28+00:00
File Access Date/Time        : 2025:02:21 12:09:45+00:00
File Inode Change Date/Time   : 2025:02:21 12:09:45+00:00
File Permissions              : -rw-rw-r--
File Type                    : DOCX
File Type Extension          : docx
MIME Type                    : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version         : 20
Zip Bit Flag                 : 0
Zip Compression              : None
Zip Modify Date              : 2016:06:21 05:38:30
Zip CRC                     : 0x00000000
Zip Compressed Size          : 0
Zip Uncompressed Size        : 0
Zip File Name                : docProps/
Template                     : Normal
Total Edit Time              : 0
Pages                        : 1
Words                       : 504
Characters                   : 2873
Application                  : Microsoft Office Word
Doc Security                 : None
Lines                       : 23
Paragraphs                   : 6
Scale Crop                   : No
Company                     : 
Links Up To Date             : No
Characters With Spaces       : 3371
Shared Doc                   : No
Hyperlinks Changed          : No
App Version                  : 14.0000
Title                       : 
Subject                     : 
Creator                     : 7
Keywords                     :
```

I then used strings tool against the file trying to look for printable strings in the file. I realized that there were some other files hidden within this word document some were directories containing xml files but i was interested with a file named **Flag.txt**.

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ strings G6P+lists.docx
docProps/PK
docProps/app.xml

)6pZ#
UynII
[Content_Types].xml
Gk{RK
VITf+
DEZU
"+G
_rels/PK
_rels/.rels
INNB
@e!oi
iCr$
}-2.
docProps/
docProps/app.xml
docProps/core.xml
Flag.txt
word/
word/document.xml
$~_n
$~_n
word/fontTable.xml
word/settings.xml
word/styles.xml
word/stylesWithEffects.xml
word/theme/
word/theme/theme1.xml
word/webSettings.xml
word/_rels/
word/_rels/document.xml.rels
[Content_Types].xml
_rels/
hB}_n
hB}_n
hB}_n
_rels/.rels
hB}_n
hB}_n

(kali@kali)-[~/Desktop]
$
```

I then used **Binwalk** tool to extract files and data that were embedded inside this word file.

```
kali@kali: ~/Desktop/_G6P+lists.docx.extracted
File Actions Edit View Help

(kali@kali) ~/Desktop
$ binwalk -e G6P+lists.docx

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0            Zip archive data, at least v2.0 to extract, name: docProps/
39            0x27           Zip archive data, at least v2.0 to extract, compressed size: 371, uncompressed size: 713, name: docProps/app.xml
456           0x1C8          Zip archive data, at least v2.0 to extract, compressed size: 348, uncompressed size: 729, name: docProps/core.xml
851           0x353          Zip archive data, at least v1.0 to extract, compressed size: 32, uncompressed size: 32, name: Flag.txt
921           0x399          Zip archive data, at least v2.0 to extract, name: word/
956           0x3BC          Zip archive data, at least v2.0 to extract, compressed size: 2098, uncompressed size: 8734, name: word/document.xml
3101          0xC1D          Zip archive data, at least v2.0 to extract, compressed size: 490, uncompressed size: 1717, name: word/fontTable.xml
3639          0xE37          Zip archive data, at least v2.0 to extract, compressed size: 855, uncompressed size: 2343, name: word/settings.xml
4541          0x118D         Zip archive data, at least v2.0 to extract, compressed size: 1586, uncompressed size: 14983, name: word/styles.xml
6172          0x181C         Zip archive data, at least v2.0 to extract, compressed size: 1693, uncompressed size: 15736, name: word/stylesWithEffects.xml
7921          0x1EF1         Zip archive data, at least v2.0 to extract, name: word/theme/
7962          0x1F1A         Zip archive data, at least v2.0 to extract, compressed size: 1460, uncompressed size: 7076, name: word/theme/theme1.xml
9473          0x2501         Zip archive data, at least v2.0 to extract, compressed size: 373, uncompressed size: 859, name: word/webSettings.xml
9896          0x26A8         Zip archive data, at least v2.0 to extract, name: word/_rels/
9937          0x26D1         Zip archive data, at least v2.0 to extract, compressed size: 273, uncompressed size: 953, name: word/_rels/document.xml.rels
10268         0x281C         Zip archive data, at least v2.0 to extract, compressed size: 358, uncompressed size: 1422, name: [Content_Types].xml
10675         0x2983         Zip archive data, at least v2.0 to extract, name: _rels/
10711         0x29D7         Zip archive data, at least v2.0 to extract, compressed size: 233, uncompressed size: 590, name: _rels/.rels
12736         0x31C0         End of Zip archive, footer length: 22

(kali@kali) ~/Desktop
$ ls
'G6P+lists.docx'  '_G6P+lists.docx.extracted'
```

I then used `cd` command to navigate to the location where the flag.txt resided then used `cat` command to read the contents of the flag.txt file.

```
(kali@kali) ~/Desktop
$ cd _G6P+lists.docx.extracted
(kali@kali) ~/Desktop/_G6P+lists.docx.extracted
$ ls
0.zip  '[Content_Types].xml'  docProps  Flag.txt  _rels  word
(kali@kali) ~/Desktop/_G6P+lists.docx.extracted
$ cat Flag.txt
877c1fa0445adaedc5365d9c139c5219
(kali@kali) ~/Desktop/_G6P+lists.docx.extracted
$
```

The contents of the flag.txt file was ” 877c1fa0445adaedc5365d9c139c5219” which appeared to be a hash. I was supposed to submit a MD5 to complete this challenge as stated in the Challenge description.

Challenge Description

Just Open the File and Capture the flag . Submission in MD5

To confirm whether the contents of the flag.txt file was a MD5 hash, I used `hash-identifier` tool on kali which confirmed that the file was md5. And that's how i captured the flag.

[illegible]