Cloakify

Information Security Inc.

Contents

- About Cloakify
- Testing Environment
- Why Cloakify?
- Installing Cloakify
- Using Cloakify
- References

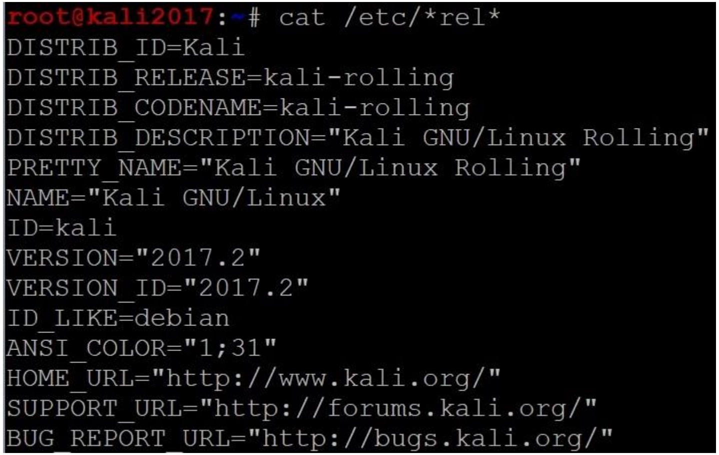
About Cloakify

- CloakifyFactory & the Cloakify Toolset - Data Exfiltration & Infiltration In Plain Sight; Evade DLP/MLS Devices
- CloakifyFactory transforms any filetype (e.g. .zip, .exe, .xls, etc.) into a list of harmless-looking strings. This lets hiding the file in plain sight, and transfer the file without triggering alerts

```
 (\~---.
 /   (\-`-/)
(      ' '  )
 \ (  \_Y_/\
  ""\ \___//
     `W   "
```

Testing Environment

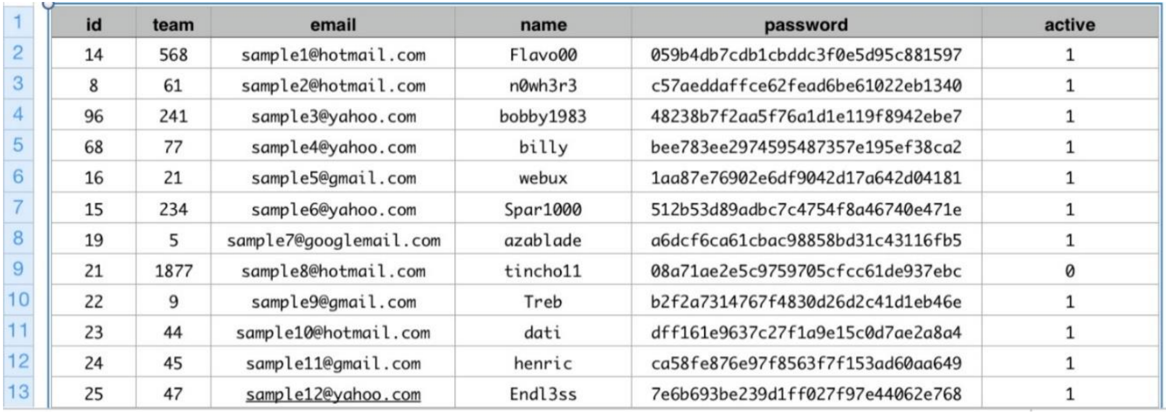
- Kali Linux 2017



```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Why Cloakify

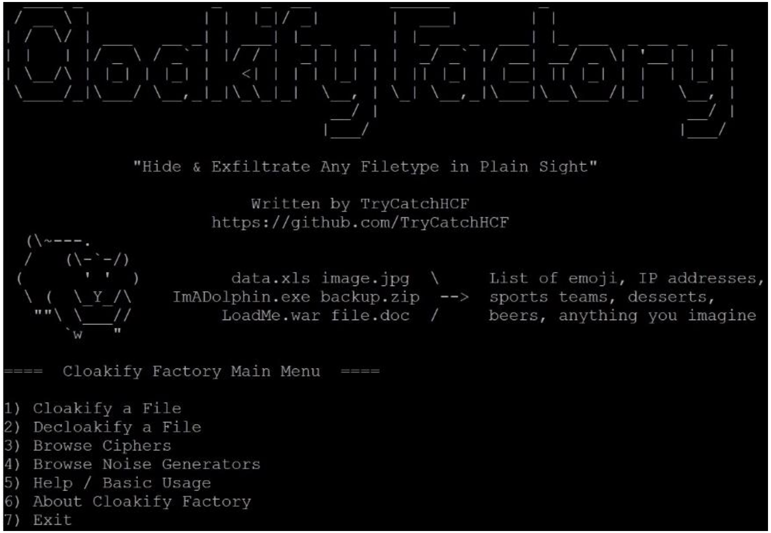
- DLP systems, MLS devices, and SecOps analysts know what data to look for:



1	id	team	email	name	password	active
2	14	568	sample1@hotmail.com	Flavo00	059b4db7cdb1cbddc3f0e5d95c881597	1
3	8	61	sample2@hotmail.com	n0wh3r3	c57aeddaffce62fead6be61022eb1340	1
4	96	241	sample3@yahoo.com	bobby1983	48238b7f2aa5f76a1d1e119f8942ebe7	1
5	68	77	sample4@yahoo.com	billy	bee783ee2974595487357e195ef38ca2	1
6	16	21	sample5@gmail.com	webux	1aa87e76902e6df9042d17a642d04181	1
7	15	234	sample6@yahoo.com	Spar1000	512b53d89adbc7c4754f8a46740e471e	1
8	19	5	sample7@googlemail.com	azablade	a6dcf6ca61cbac98858bd31c43116fb5	1
9	21	1877	sample8@hotmail.com	tincho11	08a71ae2e5c9759705cfcc61de937ebc	0
10	22	9	sample9@gmail.com	Treb	b2f2a7314767f4830d26d2c41d1eb46e	1
11	23	44	sample10@hotmail.com	dati	dff161e9637c27f1a9e15c0d7ae2a8a4	1
12	24	45	sample11@gmail.com	henric	ca58fe876e97f8563f7f153ad60aa649	1
13	25	47	sample12@yahoo.com	Endl3ss	7e6b693be239d1ff027f97e44062e768	1

Why Cloakify

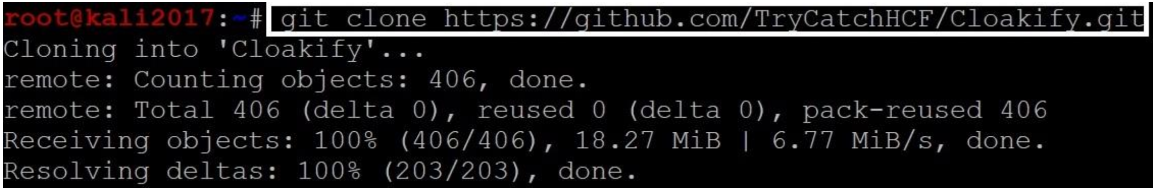
- So transform that data into something they're **not** looking for:



```
           "Hide & Exfiltrate Any Filetype in Plain Sight"

                     Written by TryCatchHCF
                 https://github.com/TryCatchHCF
  (\~---.
  /   (\-`-/)
 (      ' '  )        data.xls image.jpg  \     List of emoji, IP addresses,
  \ (  \_Y_/\    ImADolphin.exe backup.zip  -->  sports teams, desserts,
   ""\ \___//        LoadMe.war file.doc  /     beers, anything you imagine
      `w   "

====  Cloakify Factory Main Menu  ====

1)  Cloakify a File
2)  Decloakify a File
3)  Browse Ciphers
4)  Browse Noise Generators
5)  Help / Basic Usage
6)  About Cloakify Factory
7)  Exit
```

Installing Cloakify

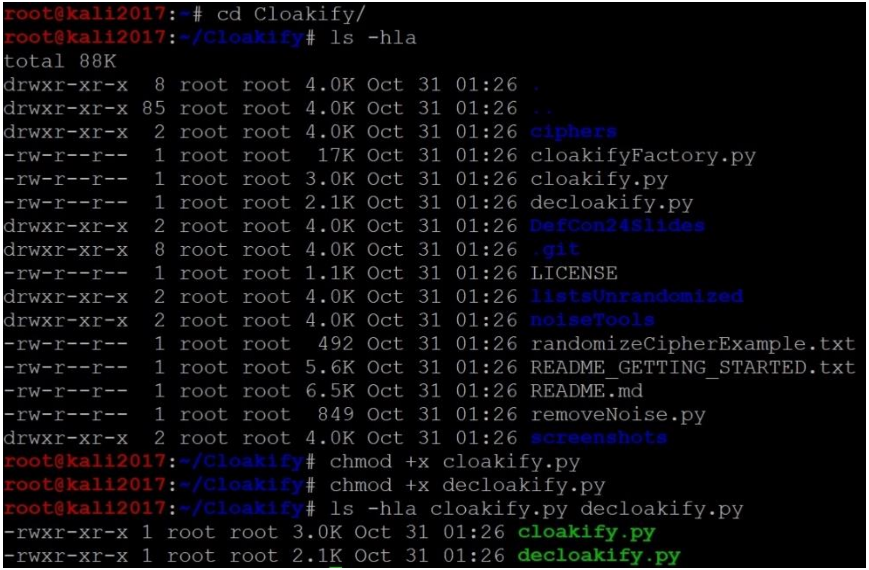
- Clone the GitHub repository



```
root@kali2017:~# git clone https://github.com/TryCatchHCF/Cloakify.git
Cloning into 'Cloakify'...
remote: Counting objects: 406, done.
remote: Total 406 (delta 0), reused 0 (delta 0), pack-reused 406
Receiving objects: 100% (406/406), 18.27 MiB | 6.77 MiB/s, done.
Resolving deltas: 100% (203/203), done.
```

Installing Cloakify

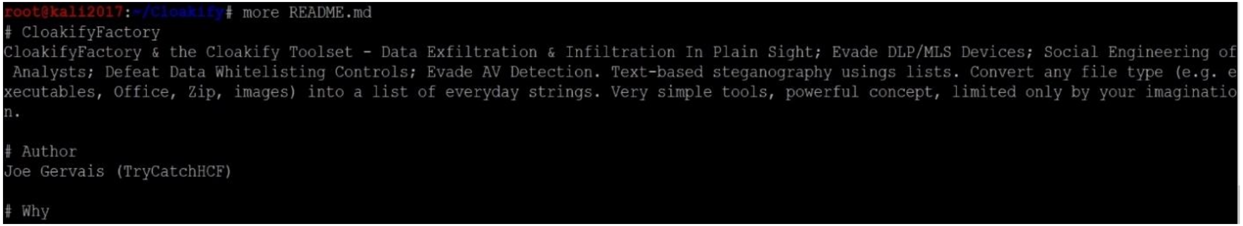
- Make the cloakify scripts executable



```
root@kali2017:~# cd Cloakify/
root@kali2017:~/Cloakify# ls -hla
total 88K
drwxr-xr-x  8 root root 4.0K Oct 31 01:26 .
drwxr-xr-x 85 root root 4.0K Oct 31 01:26 ..
drwxr-xr-x  2 root root 4.0K Oct 31 01:26 ciphers
-rw-r--r--  1 root root  17K Oct 31 01:26 cloakifyFactory.py
-rw-r--r--  1 root root 3.0K Oct 31 01:26 cloakify.py
-rw-r--r--  1 root root 2.1K Oct 31 01:26 decloakify.py
drwxr-xr-x  2 root root 4.0K Oct 31 01:26 DefCon24Slides
drwxr-xr-x  8 root root 4.0K Oct 31 01:26 .git
-rw-r--r--  1 root root 1.1K Oct 31 01:26 LICENSE
drwxr-xr-x  2 root root 4.0K Oct 31 01:26 listsUnrandomized
drwxr-xr-x  2 root root 4.0K Oct 31 01:26 noiseTools
-rw-r--r--  1 root root  492 Oct 31 01:26 randomizeCipherExample.txt
-rw-r--r--  1 root root 5.6K Oct 31 01:26 README_GETTING_STARTED.txt
-rw-r--r--  1 root root 6.5K Oct 31 01:26 README.md
-rw-r--r--  1 root root  849 Oct 31 01:26 removeNoise.py
drwxr-xr-x  2 root root 4.0K Oct 31 01:26 screenshots
root@kali2017:~/Cloakify# chmod +x cloakify.py
root@kali2017:~/Cloakify# chmod +x decloakify.py
root@kali2017:~/Cloakify# ls -hla cloakify.py decloakify.py
-rwxr-xr-x 1 root root 3.0K Oct 31 01:26 cloakify.py
-rwxr-xr-x 1 root root 2.1K Oct 31 01:26 decloakify.py
```

Using Cloakify

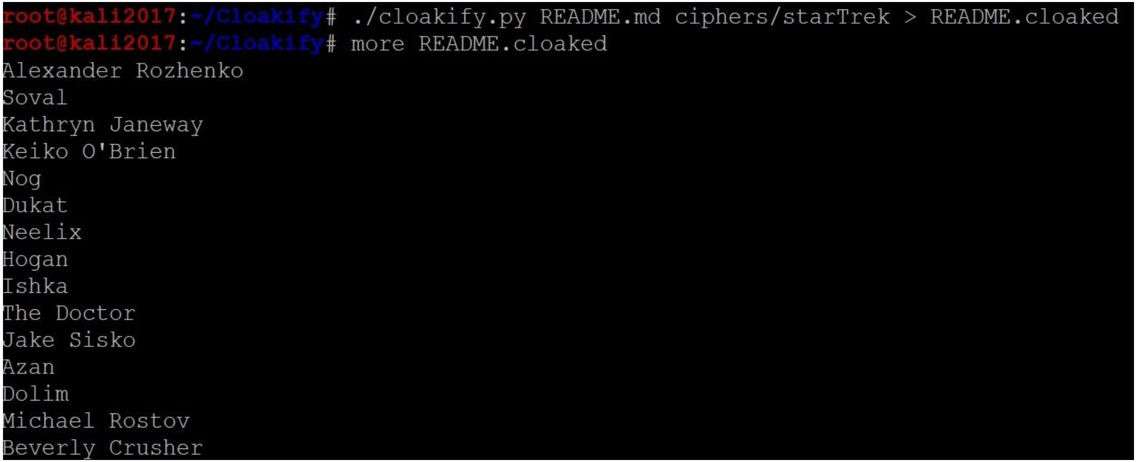
- Standalone scripts -> cloakify.py (README.md as payload)



```
root@kali2017:~/Cloakify# more README.md
# CloakifyFactory
CloakifyFactory & the Cloakify Toolset - Data Exfiltration & Infiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of
 Analysts; Defeat Data Whitelisting Controls; Evade AV Detection. Text-based steganography usings lists. Convert any file type (e.g. e
xecutables, Office, Zip, images) into a list of everyday strings. Very simple tools, powerful concept, limited only by your imaginatio
n.

# Author
Joe Gervais (TryCatchHCF)

# Why
```

Using Cloakify

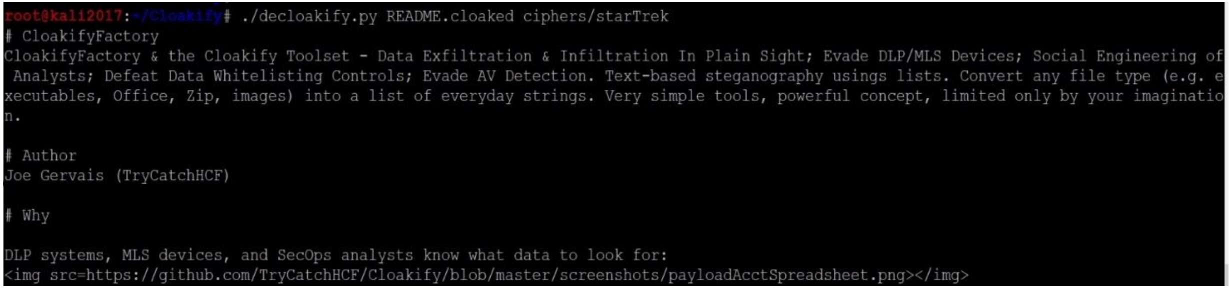
- Standalone scripts -> cloakify.py (README.md as payload)



```
root@kali2017:~/Cloakify# ./cloakify.py README.md ciphers/starTrek > README.cloaked
root@kali2017:~/Cloakify# more README.cloaked
Alexander Rozhenko
Soval
Kathryn Janeway
Keiko O'Brien
Nog
Dukat
Neelix
Hogan
Ishka
The Doctor
Jake Sisko
Azan
Dolim
Michael Rostov
Beverly Crusher
```

Using Cloakify

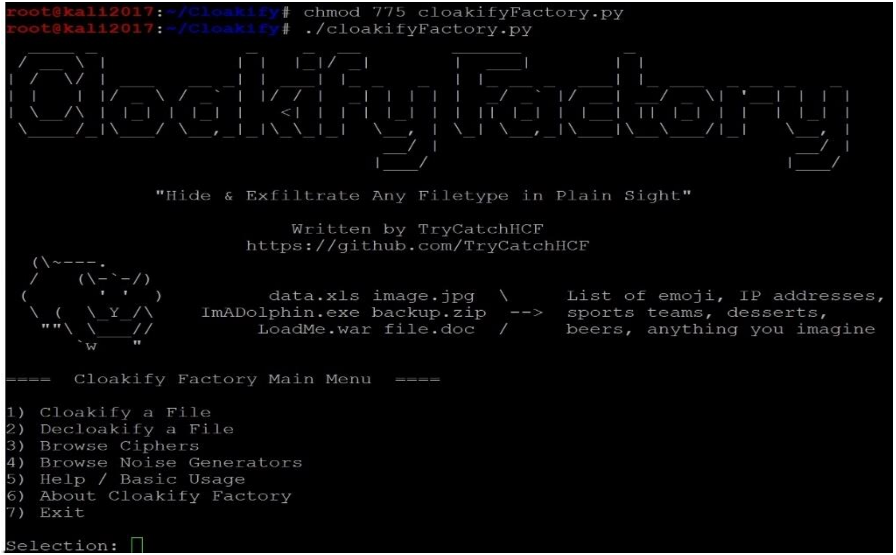
- Standalone scripts -> decloakify.py



```
root@kali2017:~/Cloakify# ./decloakify.py README.cloaked ciphers/starTrek
# CloakifyFactory
CloakifyFactory & the Cloakify Toolset - Data Exfiltration & Infiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of
 Analysts; Defeat Data Whitelisting Controls; Evade AV Detection. Text-based steganography usings lists. Convert any file type (e.g. e
xecutables, Office, Zip, images) into a list of everyday strings. Very simple tools, powerful concept, limited only by your imaginatio
n.

# Author
Joe Gervais (TryCatchHCF)

# Why

DLP systems, MLS devices, and SecOps analysts know what data to look for:
<img src=https://github.com/TryCatchHCF/Cloakify/blob/master/screenshots/payloadAcctSpreadsheet.png></img>
```

Using Cloakify

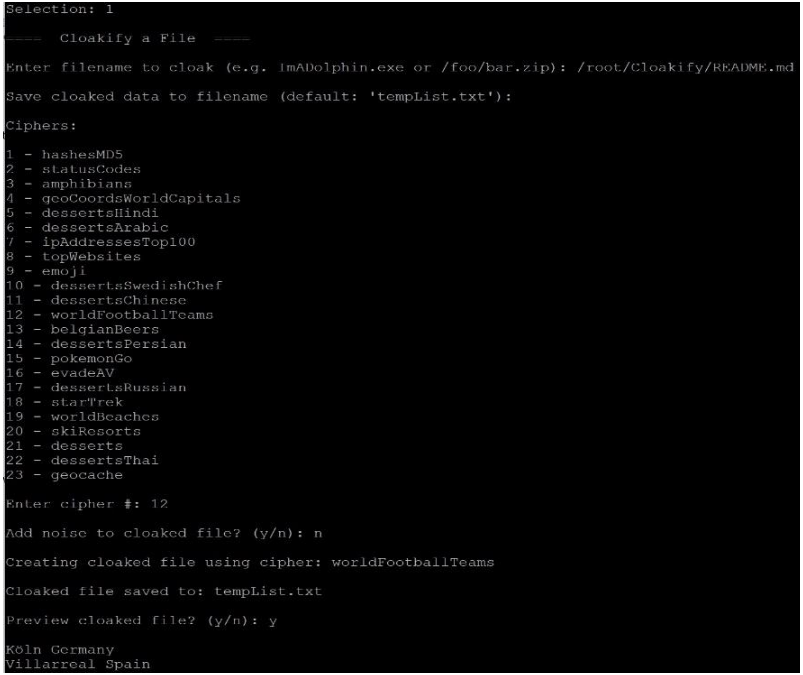
- Running Cloakify Factory



```
root@kali2017:~/Cloakify# chmod 775 cloakifyFactory.py
root@kali2017:~/Cloakify# ./cloakifyFactory.py

             "Hide & Exfiltrate Any Filetype in Plain Sight"

                          Written by TryCatchHCF
                     https://github.com/TryCatchHCF
   (\~---.
   /    (\-`-/)
  (      ' '  )         data.xls image.jpg  \     List of emoji, IP addresses,
   \  (  \_Y_/\    ImAD0lphin.exe backup.zip  -->  sports teams, desserts,
    ""\ \___//         LoadMe.war file.doc  /     beers, anything you imagine
       `w   "

====  Cloakify Factory Main Menu  ====

1) Cloakify a File
2) Decloakify a File
3) Browse Ciphers
4) Browse Noise Generators
5) Help / Basic Usage
6) About Cloakify Factory
7) Exit

Selection: 
```

Using Cloakify

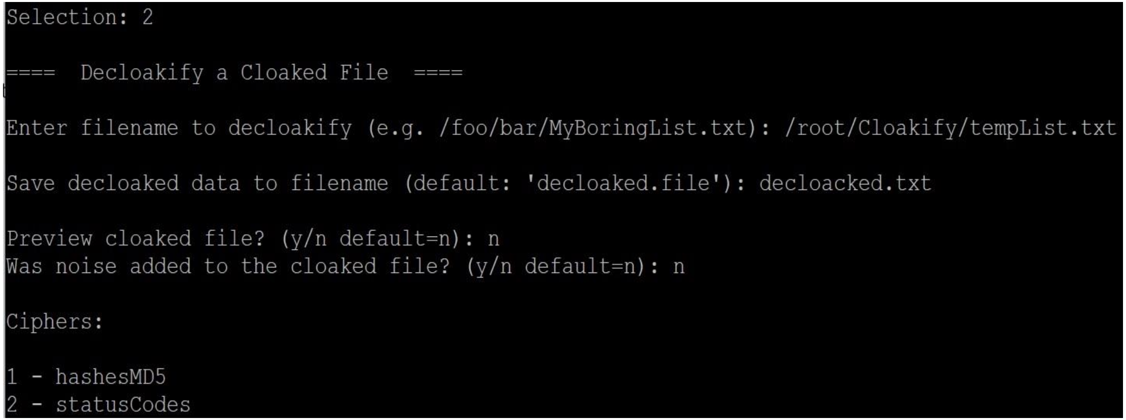
- Cloakify a file



```
Selection: 1

====  Cloakify a File  ====

Enter filename to cloak (e.g. ImADolphin.exe or /foo/bar.zip): /root/Cloakify/README.md

Save cloaked data to filename (default: 'tempList.txt'):

Ciphers:

1 - hashesMD5
2 - statusCodes
3 - amphibians
4 - geoCoordsWorldCapitals
5 - dessertsHindi
6 - dessertsArabic
7 - ipAddressesTop100
8 - topWebsites
9 - emoji
10 - dessertsSwedishChef
11 - dessertsChinese
12 - worldFootballTeams
13 - belgianBeers
14 - dessertsPersian
15 - pokemonGo
16 - evadeAV
17 - dessertsRussian
18 - starTrek
19 - worldBeaches
20 - skiResorts
21 - desserts
22 - dessertsThai
23 - geocache

Enter cipher #: 12

Add noise to cloaked file? (y/n): n

Creating cloaked file using cipher: worldFootballTeams

Cloaked file saved to: tempList.txt

Preview cloaked file? (y/n): y

Köln Germany
Villarreal Spain
```

Using Cloakify

- DeCloakify a file



```
Selection: 2

====  Decloakify a Cloaked File  ====

Enter filename to decloakify (e.g. /foo/bar/MyBoringList.txt): /root/Cloakify/tempList.txt

Save decloaked data to filename (default: 'decloaked.file'): decloacked.txt

Preview cloaked file? (y/n default=n): n
Was noise added to the cloaked file? (y/n default=n): n

Ciphers:

1 - hashesMD5
2 - statusCodes
```

References

- Kitploit
http://www.kitploit.com/2016/09/cloakify-data-exfiltration-in-plain.html

- Kali Linux
https://www.kali.org/downloads/