DIGITAL FORENSICS & INCIDENT RESPONSE

PROF. Adel KHALDI

By,

Bharani MOORTHY M.E(SNS)

Step 1:

Downloaded the Exercise from http://www.adeleda.com/epita/dfir_digital_forensics_and_incident_response/exercises/poupees_russes.txt

Step 2:

- Identified the file format RZIP by this command

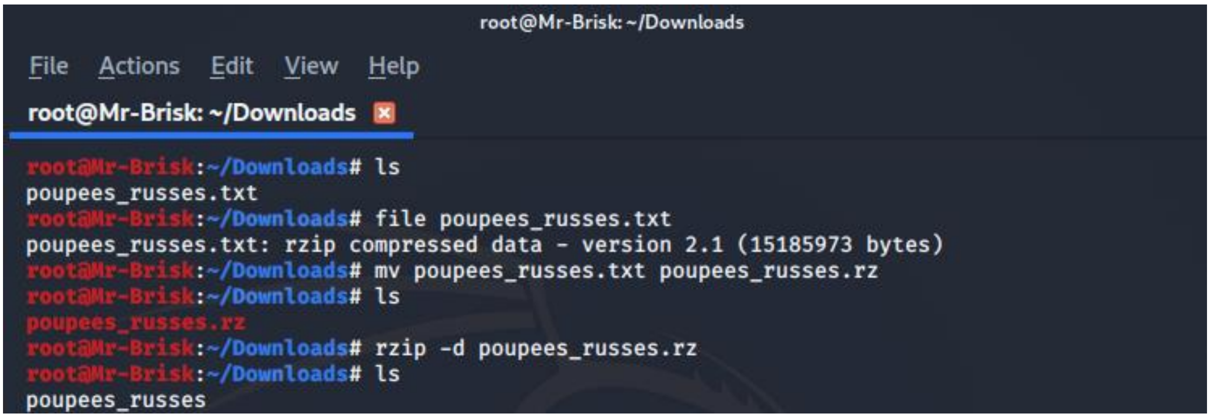
  File poupees_russes.txt

- Moved the file into rz format by this command

  mv poupees_russes.txt poupees_russes.rz

- Decompressed the rzip file by this command

  rzip -d poupees_russes.rz



```
root@Mr-Brisk:~/Downloads# ls
poupees_russes.txt
root@Mr-Brisk:~/Downloads# file poupees_russes.txt
poupees_russes.txt: rzip compressed data - version 2.1 (15185973 bytes)
root@Mr-Brisk:~/Downloads# mv poupees_russes.txt poupees_russes.rz
root@Mr-Brisk:~/Downloads# ls
poupees_russes.rz
root@Mr-Brisk:~/Downloads# rzip -d poupees_russes.rz
root@Mr-Brisk:~/Downloads# ls
poupees_russes
```

Step 3:

- Identified the file format LHarc by this command

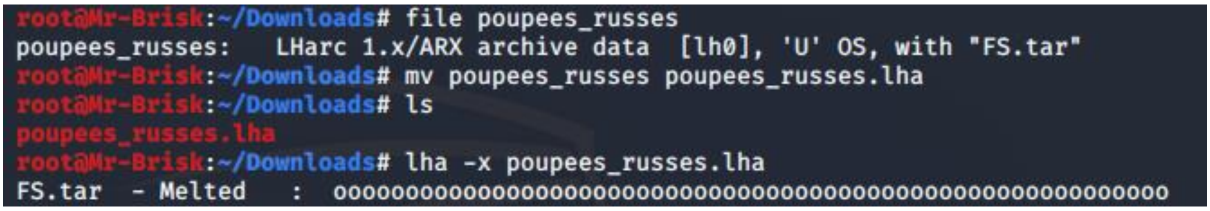
  File poupees_russes

- Moved the file into lha format by this command

  mv poupees_russes poupees_russes.lha

- Melted the lha file by this command

  lha -x poupees_russes.lha



```
root@Mr-Brisk:~/Downloads# file poupees_russes
poupees_russes:   LHarc 1.x/ARX archive data  [lh0], 'U' OS, with "FS.tar"
root@Mr-Brisk:~/Downloads# mv poupees_russes poupees_russes.lha
root@Mr-Brisk:~/Downloads# ls
poupees_russes.lha
root@Mr-Brisk:~/Downloads# lha -x poupees_russes.lha
FS.tar  - Melted   :  ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
```

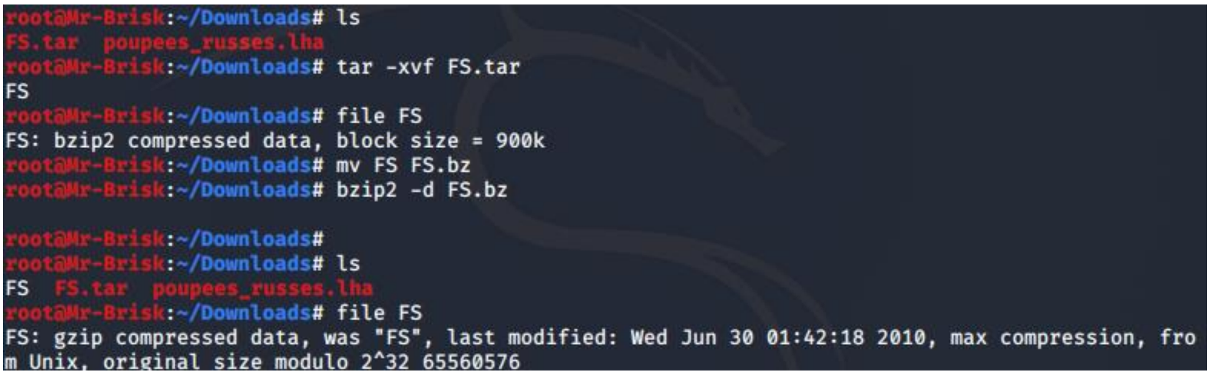
Step 3:

- After the decompression, there is a new file name FS.tar and unzipped by following command

  tar -xvf FS.tar

- It’s again bzip2 formatted file , its unzipped by

  bzip2 -d FS.bz



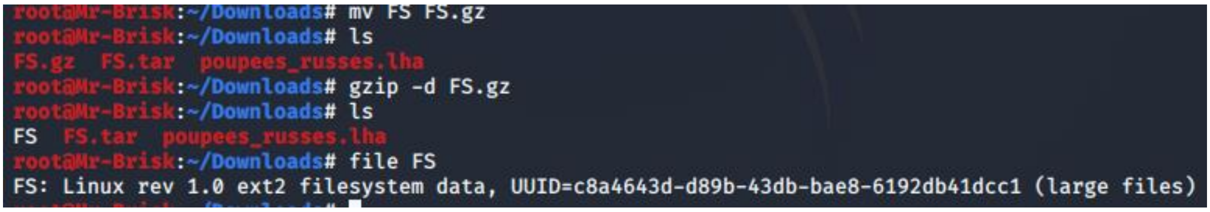
```
root@Mr-Brisk:~/Downloads# ls
FS.tar  poupees_russes.lha
root@Mr-Brisk:~/Downloads# tar -xvf FS.tar
FS
root@Mr-Brisk:~/Downloads# file FS
FS: bzip2 compressed data, block size = 900k
root@Mr-Brisk:~/Downloads# mv FS FS.bz
root@Mr-Brisk:~/Downloads# bzip2 -d FS.bz

root@Mr-Brisk:~/Downloads#
root@Mr-Brisk:~/Downloads# ls
FS  FS.tar  poupees_russes.lha
root@Mr-Brisk:~/Downloads# file FS
FS: gzip compressed data, was "FS", last modified: Wed Jun 30 01:42:18 2010, max compression, fro
m Unix, original size modulo 2^32 65560576
```

Step 4:

- It’s again gzip formatted file, its unzipped by

  gzip -d FS.gz

- Its unzipped into Linux file system data



```
root@Mr-Brisk:~/Downloads# mv FS FS.gz
root@Mr-Brisk:~/Downloads# ls
FS.gz  FS.tar  poupees_russes.lha
root@Mr-Brisk:~/Downloads# gzip -d FS.gz
root@Mr-Brisk:~/Downloads# ls
FS  FS.tar  poupees_russes.lha
root@Mr-Brisk:~/Downloads# file FS
FS: Linux rev 1.0 ext2 filesystem data, UUID=c8a4643d-d89b-43db-bae8-6192db41dcc1 (large files)
root@Mr-Brisk:~/Downloads#
```

Step 5:

- Created the directory JK to mount the file system

  mkdir jk

- Mounted the file in jk directory by following command

  mount-o loop ./FS ./jk/

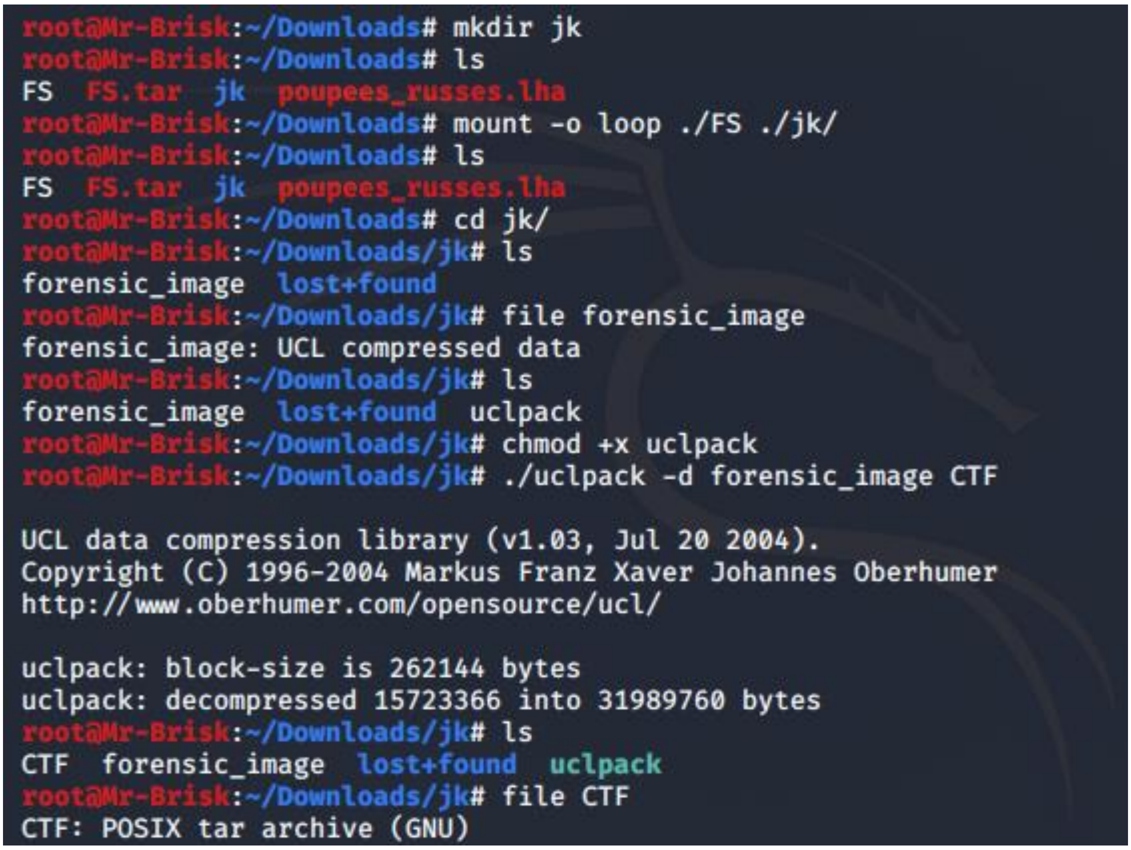
- After mounting, there is **forensic_image** file in UCL compressed data format.

To decompress this format , found the file in http://www.oberhumer.com/opensource/ucl/ and some idea in (**DefCon CTF** 2008 Qualifiers) page https://nopsr.us/ctf2008qual/walk-forensics.html

- Downloaded uclpack is moved into jk directory and gave executable access by Chmod and started decompression by following command

  . /uclpack -d forensic-image CTF

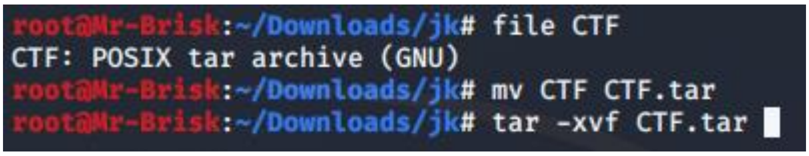
- The decompressed UCL file is in tar format.



```
root@Mr-Brisk:~/Downloads# mkdir jk
root@Mr-Brisk:~/Downloads# ls
FS  FS.tar  jk  poupees_russes.lha
root@Mr-Brisk:~/Downloads# mount -o loop ./FS ./jk/
root@Mr-Brisk:~/Downloads# ls
FS  FS.tar  jk  poupees_russes.lha
root@Mr-Brisk:~/Downloads# cd jk/
root@Mr-Brisk:~/Downloads/jk# ls
forensic_image  lost+found
root@Mr-Brisk:~/Downloads/jk# file forensic_image
forensic_image: UCL compressed data
root@Mr-Brisk:~/Downloads/jk# ls
forensic_image  lost+found  uclpack
root@Mr-Brisk:~/Downloads/jk# chmod +x uclpack
root@Mr-Brisk:~/Downloads/jk# ./uclpack -d forensic_image CTF

UCL data compression library (v1.03, Jul 20 2004).
Copyright (C) 1996-2004 Markus Franz Xaver Johannes Oberhumer
http://www.oberhumer.com/opensource/ucl/

uclpack: block-size is 262144 bytes
uclpack: decompressed 15723366 into 31989760 bytes
root@Mr-Brisk:~/Downloads/jk# ls
CTF  forensic_image  lost+found  uclpack
root@Mr-Brisk:~/Downloads/jk# file CTF
CTF: POSIX tar archive (GNU)
```

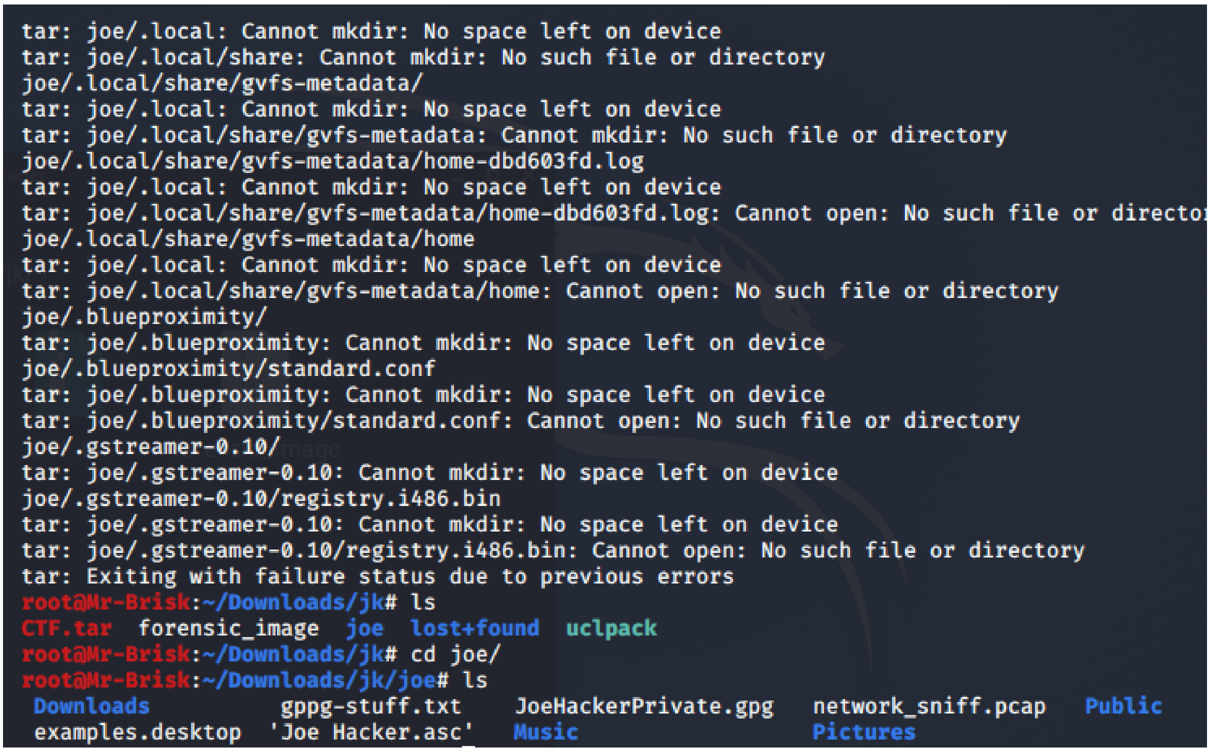
Step 6: *Again, the Tar format is unzipped by following command*

tar -xvf CTF.tar



```
root@Mr-Brisk:~/Downloads/jk# file CTF
CTF: POSIX tar archive (GNU)
root@Mr-Brisk:~/Downloads/jk# mv CTF CTF.tar
root@Mr-Brisk:~/Downloads/jk# tar -xvf CTF.tar
```

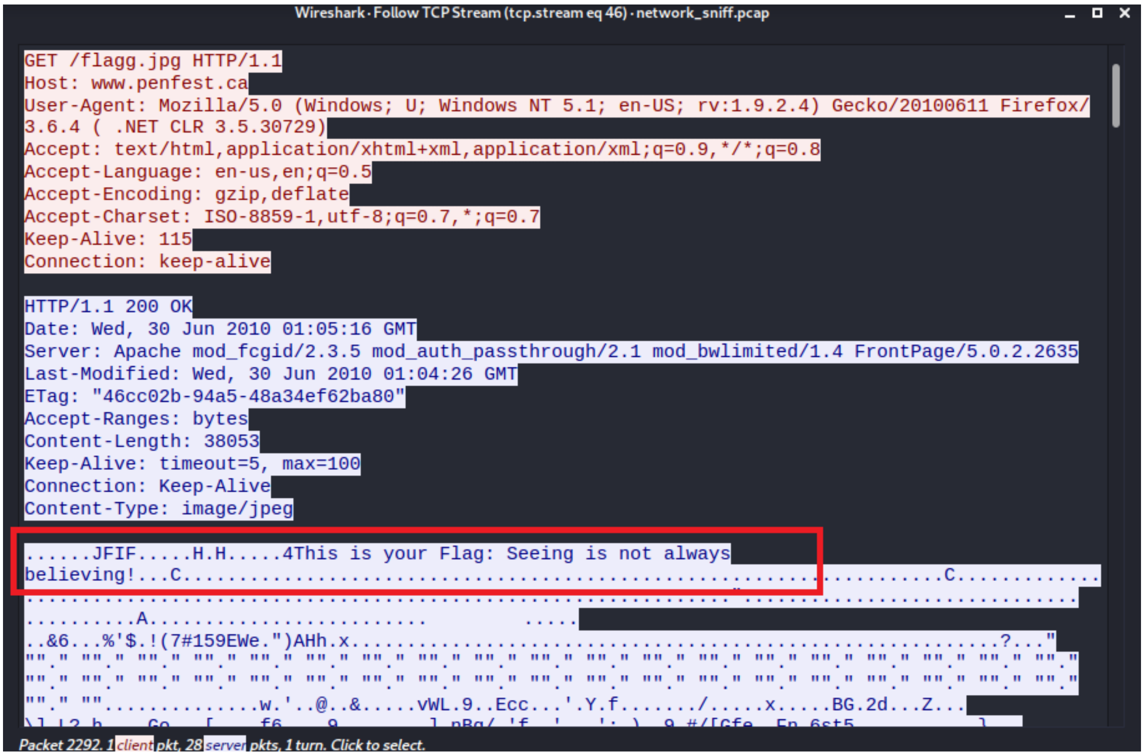
- During unzipping, it seems there is no space on the device,but, we can see joe folder



```
tar: joe/.local: Cannot mkdir: No space left on device
tar: joe/.local/share: Cannot mkdir: No such file or directory
joe/.local/share/gvfs-metadata/
tar: joe/.local: Cannot mkdir: No space left on device
tar: joe/.local/share/gvfs-metadata: Cannot mkdir: No such file or directory
joe/.local/share/gvfs-metadata/home-dbd603fd.log
tar: joe/.local: Cannot mkdir: No space left on device
tar: joe/.local/share/gvfs-metadata/home-dbd603fd.log: Cannot open: No such file or directo
joe/.local/share/gvfs-metadata/home
tar: joe/.local: Cannot mkdir: No space left on device
tar: joe/.local/share/gvfs-metadata/home: Cannot open: No such file or directory
joe/.blueproximity/
tar: joe/.blueproximity: Cannot mkdir: No space left on device
joe/.blueproximity/standard.conf
tar: joe/.blueproximity: Cannot mkdir: No space left on device
tar: joe/.blueproximity/standard.conf: Cannot open: No such file or directory
joe/.gstreamer-0.10/
tar: joe/.gstreamer-0.10: Cannot mkdir: No space left on device
joe/.gstreamer-0.10/registry.i486.bin
tar: joe/.gstreamer-0.10: Cannot mkdir: No space left on device
tar: joe/.gstreamer-0.10/registry.i486.bin: Cannot open: No such file or directory
tar: Exiting with failure status due to previous errors
root@Mr-Brisk:~/Downloads/jk# ls
CTF.tar  forensic_image  joe  lost+found  uclpack
root@Mr-Brisk:~/Downloads/jk# cd joe/
root@Mr-Brisk:~/Downloads/jk/joe# ls
 Downloads          gppg-stuff.txt    JoeHackerPrivate.gpg   network_sniff.pcap   Public
 examples.desktop  'Joe Hacker.asc'   Music                  Pictures
```

Step-9:

- And, we can see **network-sniff.pcap** so, its time to investigate the packets.



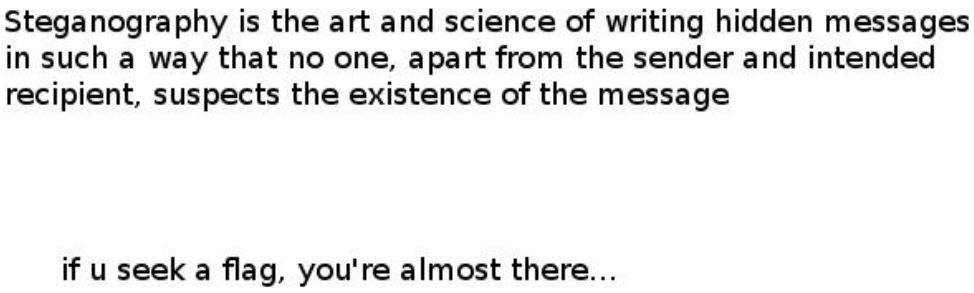
Wireshark · Follow TCP Stream (tcp.stream eq 46) · network_sniff.pcap

```
GET /flagg.jpg HTTP/1.1
Host: www.penfest.ca
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.4) Gecko/20100611 Firefox/
3.6.4 ( .NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive

HTTP/1.1 200 OK
Date: Wed, 30 Jun 2010 01:05:16 GMT
Server: Apache mod_fcgid/2.3.5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Last-Modified: Wed, 30 Jun 2010 01:04:26 GMT
ETag: "46cc02b-94a5-48a34ef62ba80"
Accept-Ranges: bytes
Content-Length: 38053
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg

......JFIF.....H.H.....4This is your Flag: Seeing is not always
believing!...C..........................................................C............
...............................................................................................
..........A.........................          .....
..&6...%'$.!(7#159EWe.")AHh.x.......................................................?..."
"".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".".
"".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".". "".".
"".". ""..............w.'..@..&.....vWL.9..Ecc...'.Y.f......./.....x.....BG.2d...Z...
```

Packet 2292. 1 client pkt, 28 server pkts, 1 turn. Click to select.

CTF!!!

By exporting this packet by export its objects, we are almost there I guess



Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message

if u seek a flag, you're almost there...