

# ACCA7031 - Hands On Activity 3

By Mehdi BIZET  
Kevin

### How the challenge has been made:

- Generate the ~7000 files with different names and different sizes (between 50 – 100 bytes) with two bash commands to obfuscate the file exploration.

```
i=0; while [ $i -lt 2300 ]; do touch $(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | head -c 16).txt; i=$((i+1)); done
```

```
i=0; while [ $i -lt 2300 ]; do touch $(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | head -c 16).jpeg; i=$((i+1)); done
```

```
i=0; while [ $i -lt 2300 ]; do touch $(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | head -c 16).png; i=$((i+1)); done
```

```
for i in $(ls); do echo $(cat /dev/urandom | head -c $(shuf -i 50-100 -n 1)) > $i; done
```

- Add randomly 900000 – 2200000 bytes between 5 and 10 files to consolidate the obfuscation.

```
echo $(cat /dev/urandom | head -c $(shuf -i 900000-2200000 -n 1)) > NAME_OF_THE_FILE
```

- Create a dead end to confuse the challenger.
- Download from the internet some images to confuse further.
- Create 4 file documents and insert random content.
- Create one file documents about Edmond Locard.
- Create the hint containing the name of 4 random <1KB files in the challenge, hide it inside the image using « openstego » with the password « locard », and convert the image file into a text file with base64.
- By saving, closing, and reopening the document with 7zip, search inside the « manifest » directory the XML file to edit it.
- Open an XML comment at the end and insert the base64 encoded image.
- Create the flag of the challenge and download an image.
- Hide the flag inside the image using « openstego » with a password associated with the image (in the created challenge, the password is « megumin »).
- Divide the file into 4 parts and move the parts into the files indicated in the hint with a hexadecimal editor.