# CCF LAB 1

06.01.2017

Ali Abdulmadzhidov

## Report N.12478651

06:51 - Got white/blue USB stick SanDisk Cruzer Facet 3.73GiB/4GB capacity with s/n: 4C532000060912115265 and evidence sticker on it. Order # 32144123

10:12 - Acquired image from it with calcultaion of MD5, SHA-1, SHA-256 and verifications.

10:35 - Mounted EWF format image with ewgtool.

```
> ewfmount evidence.E01 /media/disk0
```

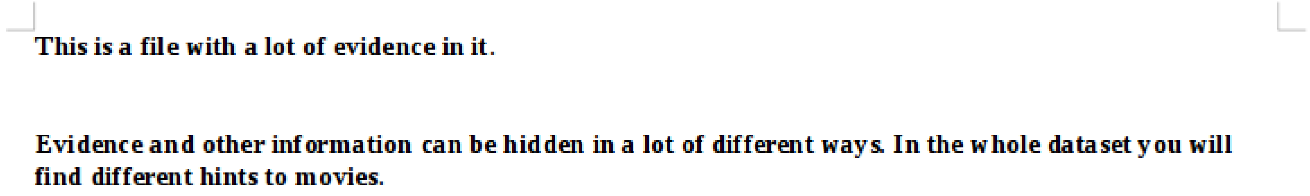
10:40 - Found ntfs partition image in that dump. "ewf1". Knowin offset we can mount it.

```
> sudo fdisk -l ewf1
Disk ewf1: 3,7 GiB, 4004511744 bytes, 7821312 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x629e70e5

Device     Boot Start     End Sectors Size Id Type
ewf1p1            128 6285439 6285312   3G  7 HPFS/NTFS/exFAT

> sudo losetup -o65536 -r /dev/loop0 ewf1
> sudo mount /dev/loop0 /media/disk1
```

11:00 - This is Windows parition. "Two" users, many images with cats. Also images from sites about politic news and sports. One interesting document with evidence.



This is a file with a lot of evidence in it.

Evidence and other information can be hidden in a lot of different ways. In the whole dataset you will find different hints to movies.

## P.S. Tried to make acquire image with console commands.

```
> ddrescue /dev/sdb1 image.img
> sha256sum image.img
7494847d12568e94b26262e666e4eb56a19a000dba301976a31d6f055556293a  image.img
```