|  |
| --- |
| OTO Oefening |
|  |
| Technische oefening |
|  |
|  |
|  |

# Doel van de oefening

Het doel van deze OTO-sessie is het oefenen van het uitvoeren van een digitaal forensisch onderzoek. Deze training is gebaseerd op een onderdeel van de JSCU 2018 Winter Challenge (nu offline). Deze oefening combineert diverse methodieken, technieken en kennis. De ‘win condition’ van de oefening is het vinden van de ‘flag’, herkenbaar als ‘*jscu{…}*’ met een MD5-waarde op de plek van de punten.

# Vereisten

* Een werkruimte
* Aantal USB-keys voor verspreiding van het image
* Tijdsbesteding: 3-4 uur – max. 15 minuten uitleg over uitvoering, +/- 15 min evaluatie
* Per deelnemer:
  + Laptop met daarop een installatie (VM of anderszins) van een Linux-distributie die geschikt is voor digitaal forensisch onderzoek. Voorbeelden: DEFT, SIFT, Kali

## Opzet

* Twee begeleiders die zowel de inhoudelijke als procesbewakingsrol vervullen
* Deelnemers vervullen hun reguliere rol (SOC, Security dan wel CERT)

## Spelregels

* Samenwerking is beperkt toegestaan, probeer te voorkomen dat:
  + Antwoorden worden voorgezegd
  + Slechts enkelen daadwerkelijk bezig zijn met het onderzoek
* Schrijf de acties/beslissingen op

# Beschrijving

Een zoeking heeft geleid tot een inbeslagname van een drager. Deze inbeslagname is op een forensisch verantwoorde manier gebeurd:

1716f58487962f7b62a26e5e872aa29b cat\_scene\_investigation.e01.gz

798ba8ec92df9b335b31aa2ac3590fcf3728bc73 cat\_scene\_investigation.e01.gz

4bb1e43471333b81fb5668ac0642708dcdaa3abe70e544b11d4d22f10ceac7f6 cat\_scene\_investigation.e01.gz

Op de drager werd een Post-It Note aangetroffen met daarop de tekst: “*Forensicats*”

## Working with the raw disk image

Image is in EWF formaat (Encase forensics file, bevat automatische verificatie). Deze images kunnen direct worden gemount met behulp van ewftools/libewf: <http://www.forensicswiki.org/wiki/Libewf>.

1. mkdir /mnt/ewf (of vergelijkbaar)
2. gunzip cat\_scene\_investigation.e01.gz
3. ewfmount cat\_scene\_investigation.e01 /mnt/ewf

## Finding the partitions

Image is vrijwel exact 100MB en bevat twee partities: ééntje is in DOS-formaat en direct leesbaar, de andere is in een ander formaat. De DOS-partitie kan worden bekeken als volgt:

1. fdisk -l ./ewf1
2. mkdir /mnt/catscene1
3. mount -o offset=$((40\*512)) ./ewf1 /mnt/catscene1

Hierop is een aantal cat pictures te vinden, maar dit is grotendeels een dood spoor, anders dan dat het een baseline aan plaatjes geeft waar de andere plaatjes later mee kunnen worden vergeleken.

## Support for APFS

De tweede partitie is een APFS-encrypted partitie.

1. losetup --offset $((97696\*512)) /dev/loop1 ./ewf1
2. head -c128 /dev/loop1 | xxd

In de header is meermaals een NXSB ‘magic value’ terug te vinden; zoeken via Google zal opleveren dat dit wordt geassocieerd met een APFS-partitie. Er is weinig ondersteuning te vinden, maar er is een library die het mogelijk maakt deze partities te mounten onder Linux met behulp van deze library: <https://github.com/sgan81/apfs-fuse.git>. De installatie hiervan gaat als volgt:

1. apt-get install git build-essential cmake libicu-dev libfuse-dev libattr1-dev
2. git clone https://github.com/sgan81/apfs-fuse.git
3. mkdir -p apfs-fuse/build
4. cd apfs-fuse/build
5. cmake ..
6. make
7. mkdir /mnt/catscene2

## Mounting the APFS-encrypted partition

1. […] bin/apfs-fuse /dev/loop1 /mnt/catscene2

Het wachtwoord voor de APFS-encrypted volume is ‘*Forensicats*’.

## Discovering the RAR file

Op het gemounte APFS-volume is weer een grote collectie kattenfoto’s te vinden. Het vergelijken en analyseren van de individuele foto’s toont één file die een ongewone grootte heeft, maar desalniettemin zonder fouten opent in een image viewer.

Met behulp van *binwalk* of vergelijkbare tooling (*xxd*, etc.) is te zien dat er een RAR-file is verborgen na de datablokken van het plaatje.

## Extracting the RAR file

*binwalk* geeft aan dat er een RAR file is verborgen in *cute\_cat.jpg*. Door middel van *dd* is het eenvoudig om die file er uit te splitsen. Omdat *apfs-fuse* alleen read-only kan mounten, moet de RAR file op een andere locatie worden opgeslagen.

1. cd /mnt/catscene2/root
2. binwalk cute\_cat.jpg
3. mkdir ~/oto\_work
4. dd if=cute\_cat.jpg of=~/oto\_work/archive.rar bs=1 skip=8993
5. cd ~/oto\_work

De RAR file heeft een wachtwoord. Dit is echter gemakkelijk te raden (common weak password)!

1. unrar x archive.rar

Het wachtwoord voor de RAR file is ‘*123456*’.

## Contents of the RAR file, NTFS trickery

Eén van de files in het RAR archief bevat weer een verborgen stuk data. Dit is opnieuw te achterhalen met bijvoorbeeld *binwalk*, en het aparte gedeelte kan worden geknipt met *dd*. Op die manier is uit de file *cute\_cats\_009.jpg* een ODF document te halen, te herkennen aan de structuur van een ZIP-file met daarin een aantal elementen. Het openen van deze .ODF is echter niet mogelijk, doordat er een wachtwoord op zit. Het wachtwoord is niet te raden, en brute-forcing is niet realistisch/mogelijk op korte termijn.

Eén van de files heeft als extensie ‘*.jpg*’, maar blijkt eigenlijk een tekstfile te zijn met daarin de tekst ‘*NTFS Rules*”. Dit is een hint naar het feit dat RAR als één van de weinige archiefformaten in staat is om Alternate Data Streams op te slaan (ADS).

1. dd if=./cute\_cats\_009.jpg of=./document.odf bs=1 skip=15300
2. cat kittycat.jpg # bevat "NTFS Rules", een hint dat bestanden in RAR files NTFS Alternate Data Streams kunnen bevatten.

## Unpacking the RAR on a Windows system

Na het uitpakken van de RAR file op een Windows systeem, waarbij de ADS blijven bewaard, is er één bestand, *kittycat.jpg*, met daarin een tweede ADS genaamd *cattykit.txt.* Hierin staat een willekeurige stroom aan tekens. Dit is het wachtwoord waarmee de ODF kan worden geopend.

1. notepad kittycat.jpg:cattykit.txt
2. libreoffice --writer document.odf # password: "*Hg&d$sM05GvcwsuUH4@!8(;jaHG*"

## Final step, ODF document

Het ODF document bestaat uit een aantal stukken WordArt, waardoor het niet is uit te lezen met strings. Bij het openen lijkt er slechts ‘Flag’ te staan en een groot kader. Bij het wegslepen van het kader wordt de daadwerkelijke flag zichtbaar.