Introduction à la forensique

Ian-Kyle Wagner

Club de Sécurité Informatique, Université Laval

Automne 2019

Table des matières

Section 1

Introduction

Qu'est-ce la forensique

- Analyzer les différents médias informatique
- Trouver des preuves pour les enquêtes
- Analyzer les données non visibles pour des indices (métadonnées, fichiers supprimés)
- comprendre ce qui c'est passé lors d'une cyberattaque ou incident affectant des systèmes informatiques.

Pourquoi la forensique

- Permettre de déterminer l'origine des attaques
- Prévention de futures attaques
- Utiliser en droit et enquête pour trouver les coupables d'un acte
- Peut être utilisé en analyse de logiciels malveillants (Malware Analysis) pour trouver le vecteur d'origine d'une infection (IOC)

Section 2

Les métadonnées et paradonnées

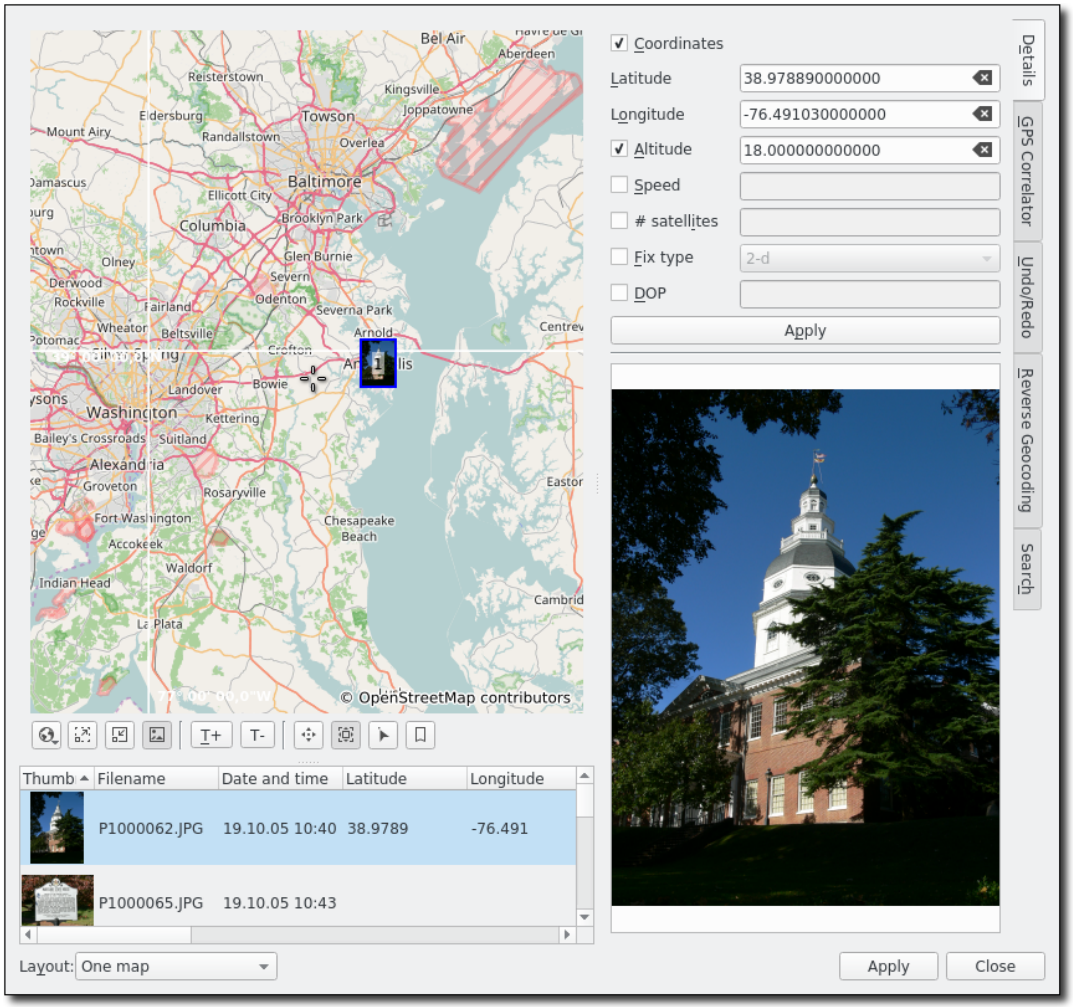
Les paradonnées

- Données externes décrivant des fichiers (origine, auteur)
- peuvent êtres supprimés ou modifiés
- Différents types de données: coordonnées GPS, auteur, date de création
- Sous le format exif pour les fichiers des images photo
- Pour les documents propriétés visibles à partir de logiciels permettant la lecture et l'édition
- outils: exiftool, Okular, ...

metadonnées de type exif

- Utilisé dans les images de type jpg ainsi que tiff
- possibilité d'obtenir la géolocalisation où que l'image est prise
- indique la caméra qui a prise l'image
- la date de création d'image est indiqué
- plusieurs lecteur d'image peuvent visualiser ces données ainsi que l'outil exiftool
- peut être modifié ou supprimé par la logiciel exiftool

Démonstration exiftool et extraction des métadonnées



Exercices metadonnées

- Télécharger les images du répertoire git des exercices
- À l'aide de l'outil exiftool trouver la localisation où la photo dans l'image jpg a été prise
- Trouver l'auteur qui a créé le document pdf menaçant

Section 3

Les artéfacts images de disque

Les différents types d'images forensique disque

- dd
- E01
- AFF
- RAW

Outils pour monter les images disques

- FTK Imager (Windows)
- Encase Imager (defunct)
- efw-tools
- sleuthkit (Windows/Linux)
- mount

Comment monter une image forensique sous Kali Linux

- sudo apt install ewf-tools
- sudo mkdir /mnt/ewf
- efwmount image /mnt/ewf
- lien pour tutoriel Kali Linux: https://dfir.science/2017/11/EWF-Tools-working-with-Expert-Witness-Files-in-Linux.html

Comment monter une image forensique sous Windows

- Télécharger l'outil FTK imager du lien suivant: https://accessdata.com/product-download/ftk-imager-version-3-4-0-5
- Outil non libre (DFSG), mais gratuit pour son utilisation
- Outil avec une interface graphique

Démo FTK Imager

Exercices images forensiques

- Télécharger l'image forensique du github de la présentation
- Utiliser soit FTK imager ou monter l'image sur Kali Linux pour obtenir le flag.

Section 4

La forensique volatile

Pourquoi la forensique volatile?

- Éléments de preuve ne se trouvant sur le disque
- Volatile peut modifier avec chaque session
- Les preuves comme les mots de passe peuvent retrouvé
- Permet de découvrir certains artéfacts
- Plusieurs outils disponibles: volatility ainsi que belkasoft evidence center

Volatility (description)

- Framework open source en python
- permet de lire des captures de mémoire pour trouver des indices
- Supporte des images .mem et .dmp
- link git: https://github.com/volatilityfoundation/volatility3/
- site internet: https://www.volatilityfoundation.org/

Volatility 2.6 vs 3

- Volatility 3: Framework open source en python 3
- Volatility 2.6: Framework open source en python 2
- volatility 2.6: stable et beaucoup de plugins
- volatility 3: en développement (beta) peu de plugins

Volatility (installation version 2.6)

- télécharger du site: https://www.volatilityfoundation.org/26
- choisir l'option Linux Standalone executables
- désarchiver le fichier zip

Volatility (installation version 3)

- requirements: pefile, yara-python, capstone
- (sous kali): sudo pip3 install pefile yara-python capstone
- git clone https://github.com/volatilityfoundation/volatility3.git
- python3 vol.py -h

Commandes utiles avec le logiciel volatility

- imageinfo
- psslist
- pstree
- psscan
- dlllist
- dlldump
- memdump
- iehistory
- notepad
- connscan (Windows XP)
- sockets (Windows XP)
- netscan (Windows Vista/7)

Démonstration Volatility

Exercices avec Volatility

- Ouvrir la capture mémoire de l'ordinateur avec Windows XP et de trouver la localisation du Flag.
- Ouvrir la capture mémoire de la même image et trouver le navigateur web qui a été utilisé.
- Trouver le logiciel de virtualization hébergant la machine qui a été imagé.