Outils pour la forensique

Tanguy Gernot

OUTILS POUR LA FORENSIQUE

Tanguy Gernot
Ingénieur de recherche CNRS

tanguy.gernot@cnrs.fr
https://gernot.fr

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

Plan

Plan

Que veut-on faire ?

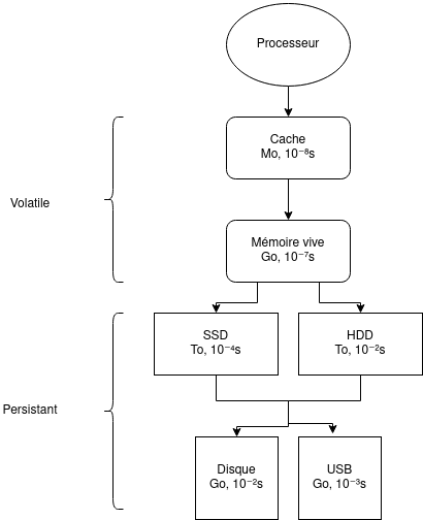
- Utiliser des informations numériques comme preuve légale.
- Comprendre (et neutraliser) une attaque.
- Informations numériques = Données binaires stockées ou transmises.
- Différents types de données : disque, ram, fichiers, photos, email, sms, chat...
- 4 branches : ordinateurs, téléphones, EEPROM (Electrically Erasable Programmable Read-Only Memory), réseau.

Quelles étapes ?

1. Préserver : figer la scène, empêcher toute altération, tout vol. Collecter les preuves (intégrité, authenticité).
2. Transporter : mesures de protection physique, cage de Faraday (manipulations distantes). WiFi, Bluetooth, 4G and co, RFID, NFC, radio.
3. Examiner (brute).
4. Analyser (sémantique).
5. Rapport.
6. Restitution du matériel.

Introduction

Types de stockage



Dans quel ordre ?

1. Copier les données volatiles (si allumé)
2. Coper les données persistantes
3. Exception : processus destructeur en cours (data wiping, encryption), exfiltration ?

Plan

Qu’est-ce que la mémoire persistante ?

- HDD, SSD, disc, mdisc, clé usb...
- Non volatile : conserve les données même sans alimentation électrique.
- Vitesse d’accès et de transfert plus lent que la mémoire volatile (centaine de microsecondes).
- Données à conserver à long terme (OS, programmes, données utilisateurs).
- Moins coûteux que la mémoire volatile.

Combien de temps ces données sont-elles intègres ?

Support de stockage	Durée de vie
CD/DVD	$<$ 7ans
Disque dur	$<$ 10ans
Flash (clé, SD, SSD)	$<$ 10ans
Bande magnétique	$<$ 30 ans
M-DISC	$>$ 1000ans

Table: Durée de vie des données archivées

Comment récupérer les données persistantes ?

- Bloqueur l'écriture !
- *ddfldd ou dc3dd if=/dev/sda of=/dev/sdb* : pourquoi ?
- Autre logiciel "Imager" type *FTK Imager*
- Matériel "Duplicator"

Figure: Tableau TD4 (duplicateur)

Comment récupérer les données persistantes ?

Différents formats de dump :

- raw image : format ouvert (dd)
- EWF : ancêtre E01
- E01 : EnCase, standard, compression, index, segmentable.
- AFF : nouveau format ouvert, compression (*affconvert* tool)

Comment analyser les données capturées ?

Boîte à outils (cas classique, limites !)

- Boîte à outils ouverte : autopsy, the sleuth kit.
- Boîte à outils propriétaire : XWAYS, AXIOM, EnCase, FTK, OSForensics, Cellebrite, ...

Fonctionnalités :

- Capture intègre et authentique
- Suivi de cas : plusieurs device, croisement, rapports
- File carving (réassemblage)
- Timeline de fichiers
- Type de fichiers
- Carte des photos
- Email
- Logiciels communs...

Comment analyser les données capturées ?

À la main :

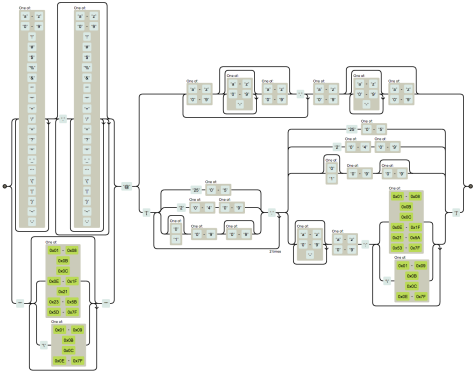
- Un bon éditeur hexadécimal
- strings, awk, egrep, fdisk, dd, sed
- ...

Outils spécialisés (logiciel par logiciel, type par type) :

- Dumpzilla (cookie, cache, download, thumbnails, ssl, session).
- ...

Comment analyser les données capturées ?

```
(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*|"(?:[\x01-
\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-
z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?|\[(?:(?:(2(5[0-5]|[0-4][0-9])|
1[0-9][0-9]|[1-9]?[0-9]))\.){3}(?:(2(5[0-5]|[0-4][0-9])|1[0-9][0-9]|[1-9]?[0-9])|[a-z0-9-]*[a-
z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+)\])
```



https://emailregex.com/

Comment analyser les données capturées ?

Recherche de texte :

- Apache Tika : détecte, extrait, structure métadonnées de nombreux documents.
- Optical Character Recognition (OCR) : tesseract
  tesseract fichier_source.png fichier_resultat.txt -l fra

Fichiers supprimés ?

Que se passe-t-il lorsque l'on supprime un fichier ?

Suppression de métadonnées (nom, date, heure), et suppression d'emplacement du premier bloc.
Conséquence : le fichier n'est pas vraiment supprimé, seule sa localisation l'est (un nouveau fichier peut prendre cette place et écrasé l'existant !).

PhotoRec

Logiciel libre de récupération de données supprimées. Spécialisé dans les fichiers de type photo, vidéo et document.
Récupère les données même si la table ou le système de fichiers sont altérés.
Utilise les magic numbers pour détecter les fichiers.

Partitions supprimées ?

TestDisk

Logiciel libre de récupération de partitions perdues.
Travaille avec la table de partitions, même si altérée.
Tente de reconstruire les partitions perdues.

Plan

Qu'est-ce que la mémoire vive ?

- RAM, cache.
- Rapide (dizaine de nanosecondes).
- Volatile.
- Coûteux.
- Contient :
  - Une partie de l'OS (noyau, pilotes)
  - Les programmes essentiels (codes exécutables, variables, fichiers temporaires)
  - D'autres applications en cours d'exécution (données générées, cache, presse-papier, contexte...)
  - La pile, le tas...
  - "Ce qui se passe en ce moment sur l'ordinateur"

Tout ceci peut être très intéressant à récupérer et à analyser.

Comment récupérer les données présentes en RAM ?

- SWAP : lorsque la RAM est trop pleine, on peut déplacer une partie des vieilles données inactives sur une partition (ou un fichier) dédiée sur le disque dur / SSD / ... : lenteur (mais récupérable) !
- Veille prolongée ('powercfg -h on' puis C:/.hiberfil.sys) :
  - Veille classique = consommation électrique pour garder la RAM
  - Veille prolongée = copie du contenu de la RAM dans le disque dur, extinction (pas de consommation électrique), et à la sortie de veille : restitution du disque vers la RAM.
- FireWire : DMA (Direct Memory Access)
- VM : *'VBoxManage debugvm 'windows 11' dumpvmcore –filename=dump.elf*
- Crash Dump *MEMORY.DMP*
- LiME (Linux Memory Extractor) pour téléphone Android.
- Cold boot attack !

Cold boot attack

- Combien de temps la RAM conserve-t-elle l'information sans alimentation ?

(a) 0 sec / 100% **(b)** 2 sec / 99.2% **(c)** 3 sec / 93.4% **(d)** 4 sec / 93.1% **(e)** 5 sec / 61.4% **(f)** 6 sec / 51.9%

Figure: Performances à température ambiante

doi.org/10.1109/ARES.2013.52

Cold boot attack

- Comment faire pour augmenter cette performance ?
- Refroidir !

Figure: Illustration

doi.org/10.1145/1506409.1506429

Cold boot attack

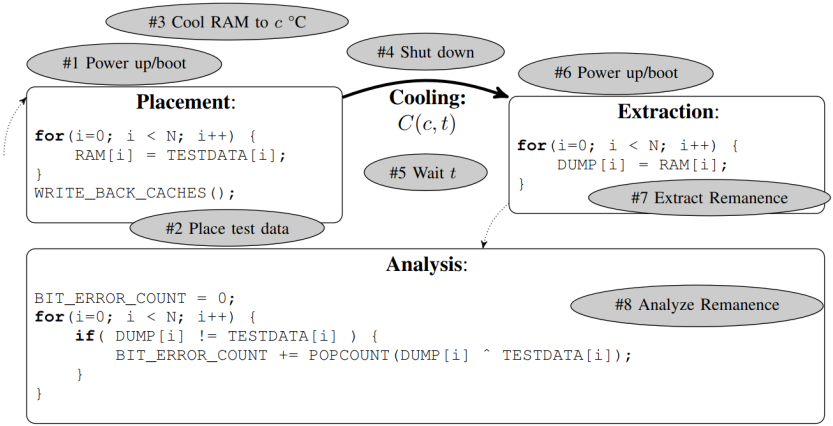


Figure: Protocole

doi.org/10.1109/ARES.2013.52

Cold boot attack

	Seconds w/o power	Error % at operating temp.	Error % at −50 °C
A	60	41	(no errors)
	300	50	0.000095
B	360	50	(no errors)
	600	50	0.000036
C	120	41	0.00105
	360	42	0.00144
D	40	50	0.025
	80	50	0.18

Figure: Performances

doi.org/10.1145/1506409.1506429

Cold boot attack

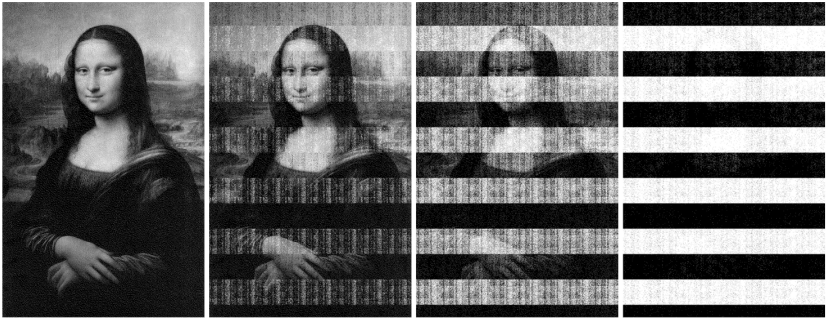


Figure: Performances (5s, 30s, 60s, 300s)

doi.org/10.1145/1506409.1506429

Cold boot attack

Demo :
https://www.youtube.com/watch?v=XfUlRsE3ymQ&ab_channel=LukeClarke
Défense : https://veracrypt.eu/en/VeraCrypt%20RAM%20Encryption.html

Cold boot attack

Contre-mesure

- Chiffrement de la RAM et supprimer uniquement la clé au verrouillage.
- Attendre avant de laisser un PC fraichement éteint sans surveillance.
- Écraser la RAM au démarrage avant de booter sur le disque ou une clé : attaque possible en reparamétrant la puce avant de remettre sous tension.

Comment analyser les données capturées ?

La donnée volatile est capturée, qu'en fait-on maintenant ?

Volatility

Logiciel opensource permettant l'analyse de dump mémoire. Nécessite un *profil* décrivant comme les informations stockées en RAM sont organisées (OS, noyau, versions). Il permet de :

- Lister les processus actifs : PID, nom, privilèges, ...
- Lister les modules chargés (DLL) : pour analyser le comportement d'une attaque.
- Connexions réseaux actives : IP/PORT/...
- Fichiers ouverts.
- Données des registres.
- Dumper un exécutable et son environnement mémoire ! (éditeur hexa)

Profil inconnu ?

Plan

Différents types de transferts

Analogiques

- Anciennes lignes téléphoniques
- Radio
- Télévision analogique
- (Vinyles)

Numériques

- WiFi a b g n ac
- Bluetooth
- xG

Différents types de transferts

Deux modes très différents de transfert :

- Filaire : man in the middle, découpe, soudure...
- Sans fil : capture plus aisée (matériels spécifiques)

(a) Alpha

(b) Yagi

Figure: Exemples d'antenne spécifiques

GREYC
Laboratoire de recherche en sciences du numérique

[Merci]

Questions ?

tanguy.gernot@cnrs.fr
https://gernot.fr