LABOLinx

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
31 JANVIER 2017

CNEJITA EXPERTS

OUTILS D'ANALYSE DE SUPPORT NUMÉRIQUE STANDARD

UNE ANALYSE STANDARD

Extraction du support

Clonage Bloqueur

Traitement et préparation

Fichiers présents

Fichiers et Données supprimées

Dossier d'instruction

0 -1 h

Extraction des données (typage, archive, vignette, registre, artefact ...)
Visualisation des différents formats
Recherche par mot clé
Recherche multicritères: par type factuel ou calculé (skin color)
Recherche par méta donnée
Recherche dans les mails
Table de Hash (NIST)
OCR
Historique web / Appli com
...

2 - 3h
avec des outils forensics

Analyse

8 - 16h

Rédaction
Mise au clair

LE CLONAGE

mission du Juge d'Instruction:

« Procéder à une copie par tous moyens techniques appropriés de nature à garantir une reproduction à l'identique, intègre et infalsifiable, du contenu des supports de données informatiques renfermés dans les scellés examinés »

L'accès au disque dur / la recopie / le calcul du Hashcode

- gratuit :
  - suite forensic : DEFT / CAINE montage readonly Linux
  - outil de copie forensic : dcfldd / ddrescue / guymager / FTK Imager / ...
- payant et plus confortable :
  - bloqueur en écriture électronique (débit) 400 €
  - logiciel de blocage ?
- plus rapide, mais plus cher :
  - duplicateur 1500 €

TABLEAU

Intelligent Computer Solutions

wiebeTECH
A Brand of CRU-DataPort

L'accès au clone

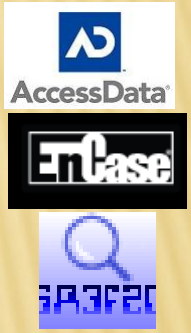
- gratuit :
  - FTK Imager / P2 Explorer
  - Les outils forensics

LES SUPER BROWSERS

Outils permettant de traiter / catégoriser / parcourir / trier / visualiser / rechercher par multi-critéres / extraire …

- Les payants les plus connus et les plus utilisés
  - FTK 6 — 3800 €
  - ENCASE 7 — 3500 €
  - XWAYS FORENSICS — 1650 €

  + la maintenance annuelle



- Les payants moins connus mais aussi utilisés
  - BLACKBAG ? — 3500 €
  - NUIX ?

- Les gratuits dignes d'intérêt
  - SLEUTKIT / AUTOPSY — 0 €
  - DFF (ArxSys) ?

- Un nouveau (pour faire plaisir à Fabien)
  - FORENSIC EXPLORER — 1200 €

AXIOM (IEF)

Le spécialiste de la recherche de traces d'utilisation

Outil indispensable sans vraiment de concurrent à son niveau

ARTÉFACTS D'ORDINATEUR

TOUT SUPPRIMER

- ☑ CHIFFREMENT (2 of 2)
- ☑ CLOUD (7 of 7)
- ☑ CONSOLES DE JEUX VIDÉO (1 of 1)
- ☑ COURRIER ÉLECTRONIQUE (11 of 11)
- ☑ DOCUMENTS (7 of 7)
- ☑ FORUM (26 of 26)
- ☑ LIÉS AU WEB (17 of 17)
- ☑ MÉDIAS (3 of 3)
- ☑ POSTE À POSTE (10 of 10)
- ☑ RÉSEAUX SOCIAUX (10 of 10)
- ☑ SAUVEGARDES MOBILES (2 of 2)
- ☑ SYSTÈME D'EXPLOITATION (21 of 21)

Achat
Axiom Complete
4100 €

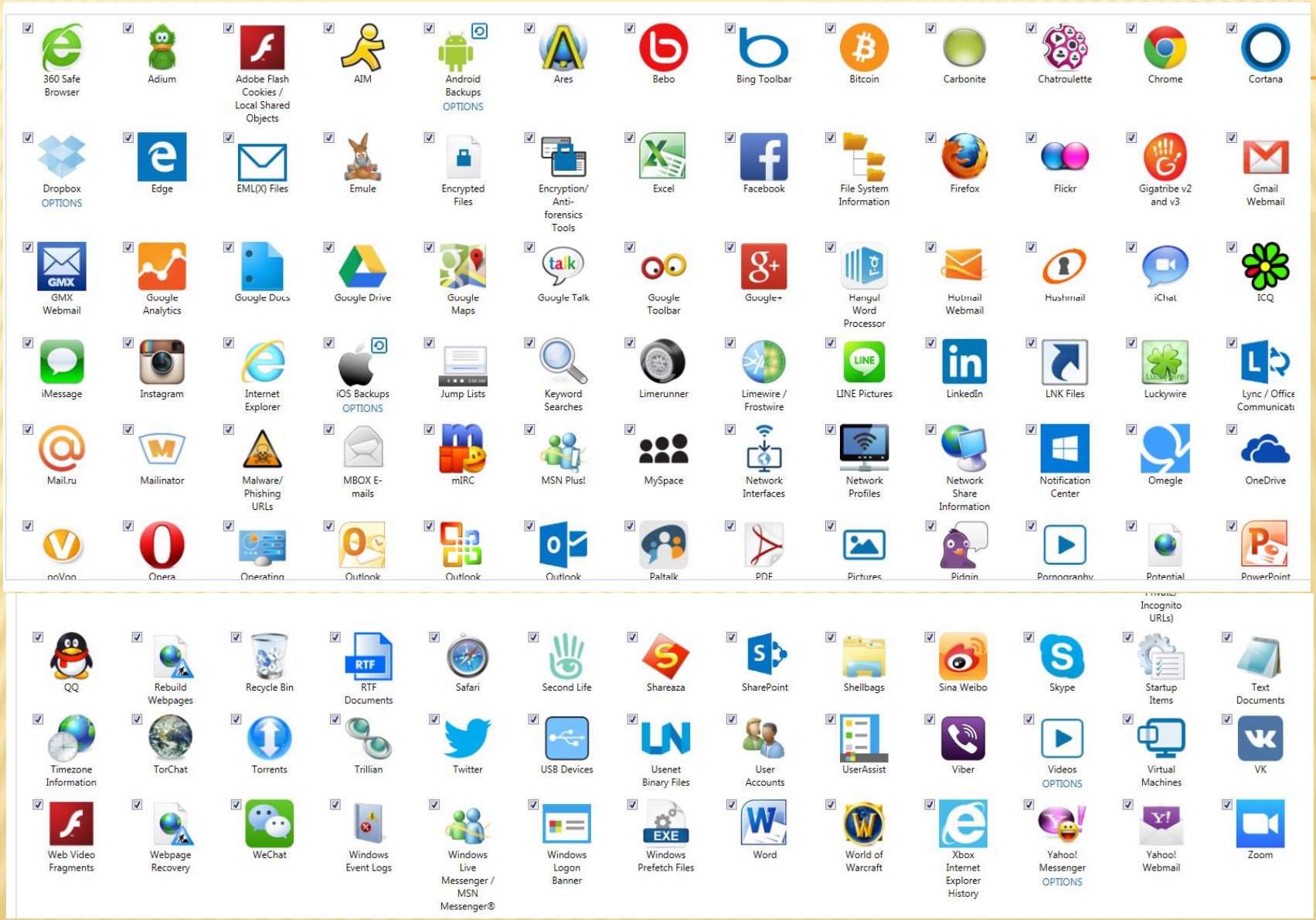
Maint.
1100 € / an

Achat
Axiom Computer
3000 €

Maint.
700 € / an

Achat
Axiom Smartphone
2000 €

Maint.
550 € / an


360 Safe Browser
Adium
Adobe Flash Cookies / Local Shared Objects
AIM
Android Backups OPTIONS
Ares
Bebo
Bing Toolbar
Bitcoin
Carbonite
Chatroulette
Chrome
Cortana
Dropbox OPTIONS
Edge
EML(X) Files
Emule
Encrypted Files
Encryption/ Anti-forensics Tools
Excel
Facebook
File System Information
Firefox
Flickr
Gigatribe v2 and v3
Gmail Webmail
GMX Webmail
Google Analytics
Google Docs
Google Drive
Google Maps
Google Talk
Google Toolbar
Google+
Hangul Word Processor
Hotmail Webmail
Hushmail
iChat
ICQ
iMessage
Instagram
Internet Explorer
iOS Backups OPTIONS
Jump Lists
Keyword Searches
Limerunner
Limewire / Frostwire
LINE Pictures
LinkedIn
LNK Files
Luckywire
Lync / Office Communicat
Mail.ru
Mailinator
Malware/ Phishing URLs
MBOX E-mails
mIRC
MSN Plus!
MySpace
Network Interfaces
Network Profiles
Network Share Information
Notification Center
Omegle
OneDrive
ooVoo
Opera
Operating
Outlook
Outlook
Outlook
Paltalk
PDF
Pictures
Pidgin
Pornography
Potential
PowerPoint
Incognito URLs)
QQ
Rebuild Webpages
Recycle Bin
RTF Documents
Safari
Second Life
Shareaza
SharePoint
Shellbags
Sina Weibo
Skype
Startup Items
Text Documents
Timezone Information
TorChat
Torrents
Trillian
Twitter
USB Devices
Usenet Binary Files
User Accounts
UserAssist
Viber
Videos OPTIONS
Virtual Machines
VK
Web Video Fragments
Webpage Recovery
WeChat
Windows Event Logs
Windows Live Messenger / MSN Messenger®
Windows Logon Banner
Windows Prefetch Files
Word
World of Warcraft
Xbox Internet Explorer History
Yahoo! Messenger OPTIONS
Yahoo! Webmail
Zoom

LES AUTRES OUTILS

Ma vision est ancienne
Je n'utilise presque plus ces outils

Voir l'excellent travail du groupe Constat

- La récupération de fichier supprimé
  - gratuit : Recuva /…
  - payant : GetDataBack / R-Studio / Stellar Phoenix / …
- Le file carving : PhotoRec / Scalpel / Foremost
- Historique / Cache / Messagerie instantanée
  - gratuit : Pasco, Galleta, Nirsoft, Index.dat, PhotoRec
  - payant : X-Ways Trace (n'est plus mis à jour), NetAnalysis, Paraben Chat Examiner
- Email (recherche / récupération / conversion / lecture)
  - gratuit : Nirsoft, les Mailer
  - payant : AtoutMail, Emailchemy, Stellar Phoenix, Paraben E-Mail Examiner

NirSoft

LES AUTRES OUTILS

- L'analyse de l'activité
  - gratuit: Nirsoft et une multitude d'autres outils
- La recherche par mot clé
  - gratuit: Nirsoft SearchMyFiles
- Les casseurs de mots de passe (rarement utile ?)
  - gratuit mais limité: OphCrack
  - de nombreux produits payants: OphCrack / Passware / ElcomSoft
  - des solutions hardware onéreuses
- Les logiciels de compta ou métier
  - Les versions démos
  - Le démarrage de la machine avec un clone
- La virtualisation / l'utilisation du poste avec un HD clone

UN RETOUR D'EXPÉRIENCE

Les outils forensics pro

- Font gagner beaucoup de temps car ils sont dédiés à notre activité
- Ont une couverture large de notre besoin contrairement à des outils individuels
- Savent gérer de gros volume de données

Mais

- Ponctuellement des petits outils sont plus pointus sur des cas très spécifiques
- Les prix assez stables jusqu'à présent commencent à monter

LABOLinx

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
31 JANVIER 2017

CNEJITA EXPERTS

OUTILS D'ANALYSE DE SUPPORT NUMÉRIQUE STANDARD

FIN