Analyse de Mac

Un Mac n'est pas un PC

- C'est joli, design, ergonomique
- Mais…
  - Le clavier est différent
  - Les raccourcis claviers sont différents
  - Les caractères spéciaux sont cachés
  - Les logiciels ne sont comportent pas pareil que leur version PC
  - Les logs ne sont pas gardés de la même façon
  - La base registre n'existe pas
  - Et beaucoup d'autres différences

D'autres différences avec le PC

http://www.computer-forensics.net/Computer-Forensics/macintosh-forensics.html

- Les fichiers effacés
  - OSX basé sur Linux … Les fichiers effacés sont rarement récupérables
  - Pas de de relai Info2 pour gérer la poubelle – quand la poubelle est vidée, c'est vidé
  - Beaucoup moins d'information dans l'espace non alloué que windows lié à la façon dont les fichiers sont effacés
  - Il y a un effaceur sécurisé intégré au Mac…

Les traces d'utilisation

- Le Mac ne gère pas de liste de « recent »
- Le Mac ne crée pas d'Alias sans intervention de l'utilisateur
- Le Mac ne crée pas d'entrée chaque fois qu'un périphérique est branché. Il faut attendre qu'il soit effectivement utilisé.
- Il n'y pas de date d'accès, juste les dates de création et de modification
- Priorité au dossier utilisateur dans la sauvegarde des fichiers
- Enregistrement d'un File ID incrementé à chaque création/enregistrement sur le disque dur

D'autres différences avec le PC (2)

- Les mails
  - Pas d'outil de traitement des mails issus des OS Mac – iMail et Outlook (moins vrai avec Thunderbird)
  - Il faut extraire, convertir et traiter à l'extérieur
- Internet
  - Le cache internet est géré sous la forme d'un fichier unique de taille limitée (vs multitude de fichiers sur le PC)
- Base de registre
  - Il n'y en a pas – multitude de plist et autres fichiers de paramètres

Revisiter les pratiques

- Démonter pour extraire le disque dur
- Faire une image
- Contourner les sécurités
- Rechercher des fichiers
- Sauvegarder des fichiers
- Le mac dans son environnement

Démonter un Mac

- Design, spécifique
- Pas de recherche systèmatique d'interopérabilité
- … Difficile à démonter
- http://www.ifixit.com/
- Parfois même très difficile – macBook Air
- …Préférer l'acquisition logique

Image d'un Mac - target Mode

- Le target Mode
  - Le mac devient un disque dur Firewire (Thunderbolt)

- Utiliser le target Mode
  - Démarrer le mac en appuyant sur la touche T
  - Icône FireWire affichée
  - Le mode target est activé ..

Acquérir – target mode

- Préparer une machine d'acquisition qui n'écrira pas sur le disque cible
  - Bloqueur en écriture
  - Mac - Disk Arbitrator
  - PC – USB Block
  - Ou … Une machine bootée sur un Linux Forensics
- Brancher le Mac sur une machine d'acquisition - Cable Firewire ou Thunderbolt
- Acquérir
  - PC – FTK Imager
  - Mac – dd et ses variantes
  - Linux – DD et ses variantes

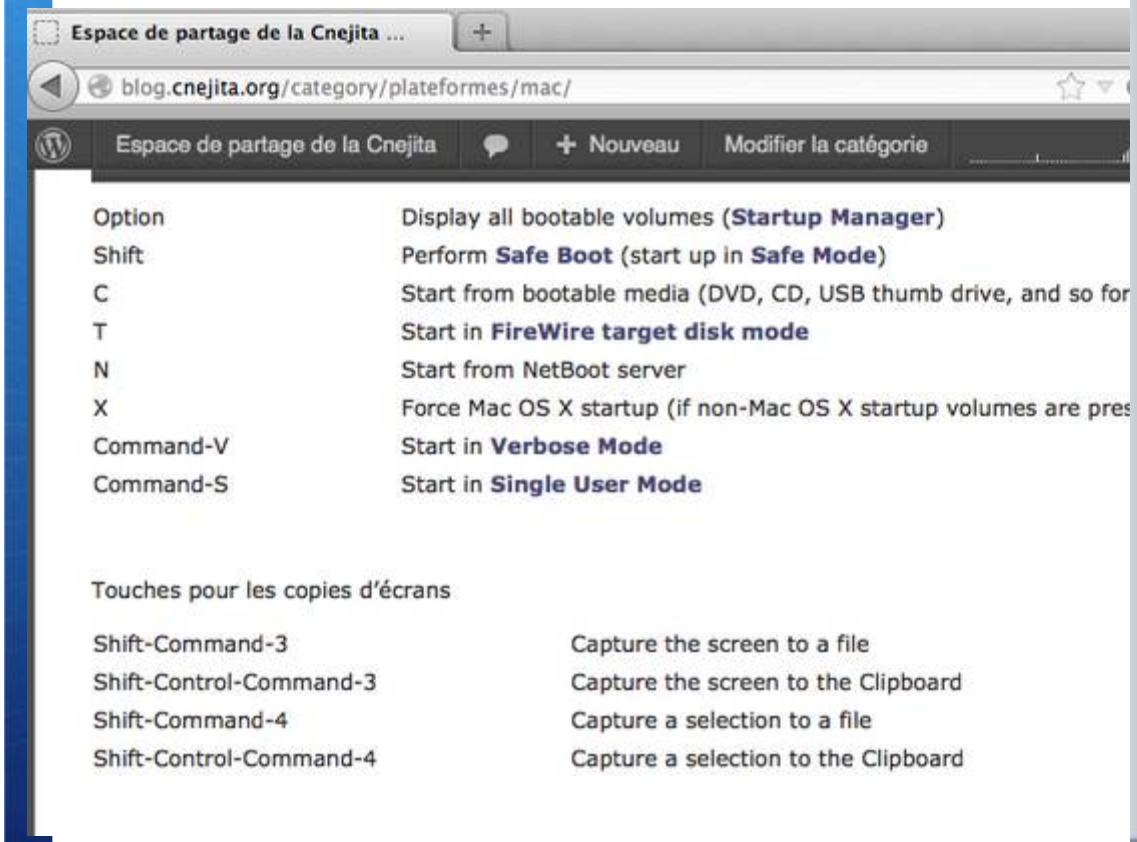
Acquérir – boot linux avec Usb

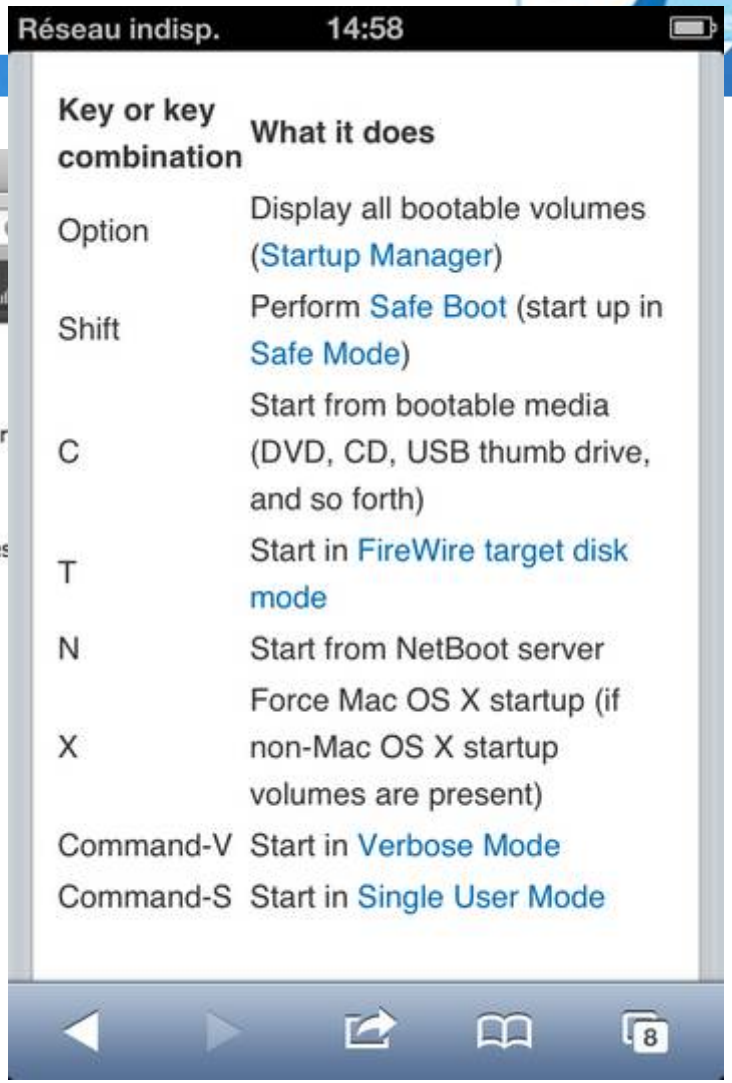
- Démarrer sur une clé USB
  - Mettre la clé USB
    - Caine 2.5.1 marche bien
  - Démarrer en appuyant sur « alt » ou «C »
  - Choisir la clé USB
- Passer par l'imager de la distribution
  - Dcfldd
  - Ou … Guymager

Acquérir

- Le démarrage en mode commande – une option?

Si vous n'avez pas noté les raccourcis clavier





Les ports de sortie du Mac

- FireWire 2 ou 3
  - Il y a des docks sur le marché
- Thunderbolt
  - Il y a des disques thunderbolt sur le marché
  - Pas encore de docks thunderbolt pour les disques Sata
  - Il y a des adaptateurs d' ExpressCard – voir Sonnet mais… Drivers à installer
- Usb3
  - Ouf!
  - Mais perfs pas toujours au rendez vous

Pour brancher un disque Sata

/ay > Stockage > Boîtier > Convertisseur > Sonnet Echo Pro - Adaptateur Expresscard/34 Thunderbolt (PCIe 2.0)

Sonnet Echo Pro - Adaptateur Expresscard/34 Thunderbolt (PCIe 2.0) - Convertisseur - Sonnet

169,90 €

Dont 0,03 € d'écotaxe

Livraison à partir de **5,40 €**

Ajouter au panie

3x CB Paiement en 3x

Total : 177,50 €

(mensua

Avantages MacWay Club

20pts

Devenir membre

Commandez par téléphor

03 88 182 182

(prix d'un appel local)

Sauvegarder des fichiers

- Monter un disque externe manuellement
  - sudo diskutil list
- La limite des 4 Go – FAT32
  - Couper les grands fichiers … Split
  - Archiver
    - Zip de l'IHM ou en manuel tar
  - Découper
    - split -b 2000m grandfichier.tar seg
  - Remonter
    - Sur windows : copy /b seg* grandfichier_reconstitue.tar
    - Sur mac/linux : join

Contourner les mots de passe

- Le mode commande
- A la main
  - C'est parfois possible – voir fiches internet
- Avec des suites logiciel
  - Koon Boot – Fred ?
  - John the Ripper Pro pour mac (pas testé)
- Attention – firevault est facile à activer sur un Mac
  - Pas possible de lire les fichiers (id TrueCrypt ou autre)
  - Mais toujours possible de faire une image en attendant que le mot de passe soit communiqué

Les recherches

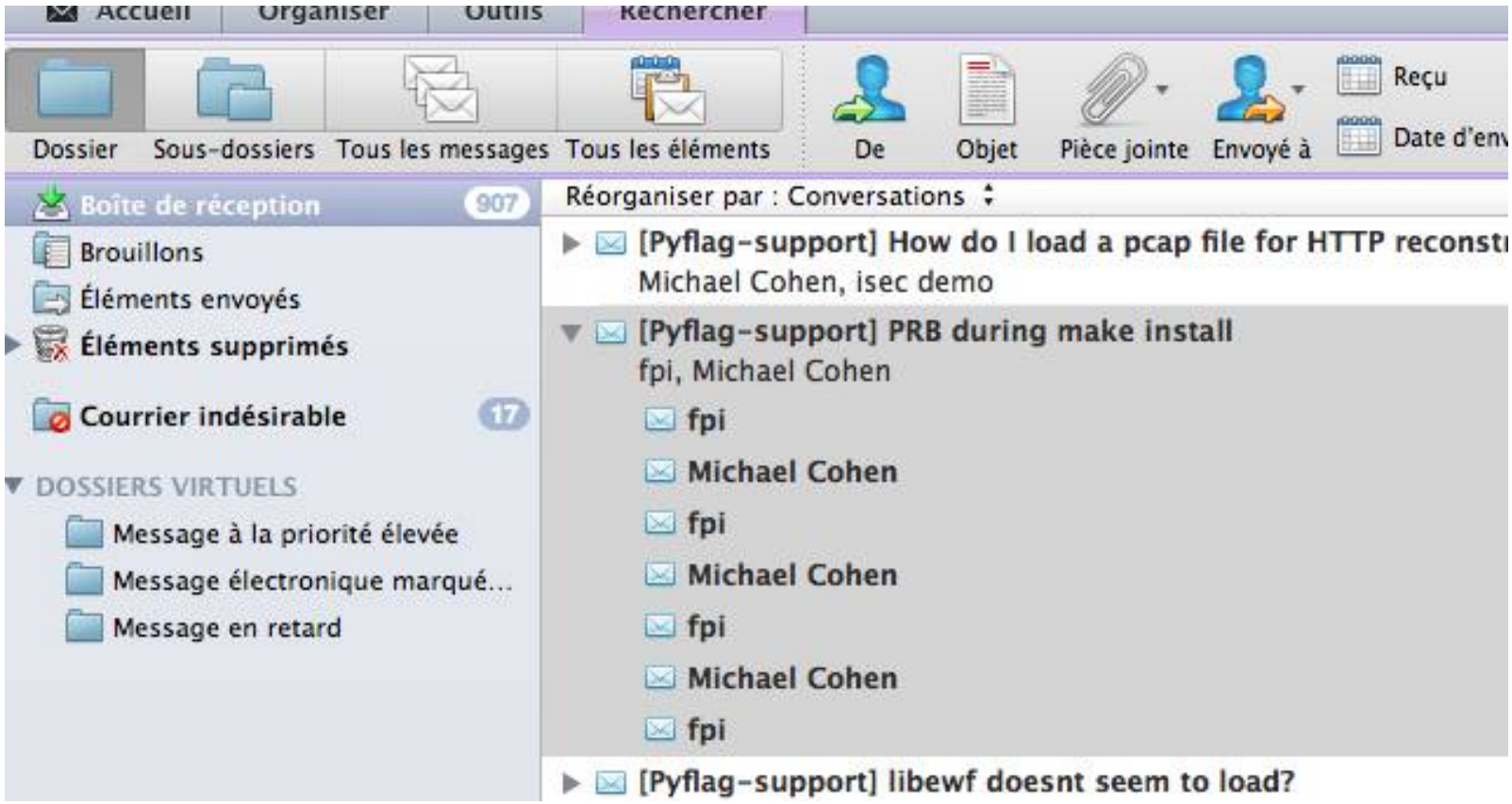
- Spotlight – IHM
- Spotlight – ligne de commande
  - Mdfind toto
  - Mdfind –onlyin /Users/philippe/Documents/cible toto
- Grep, Find
  - Grep –ir toto /Users/philippe/Documents/cible toto
  - Find /Users/philippe/Documents/cible –iname « *.txt » -exec grep –i toto {} \;

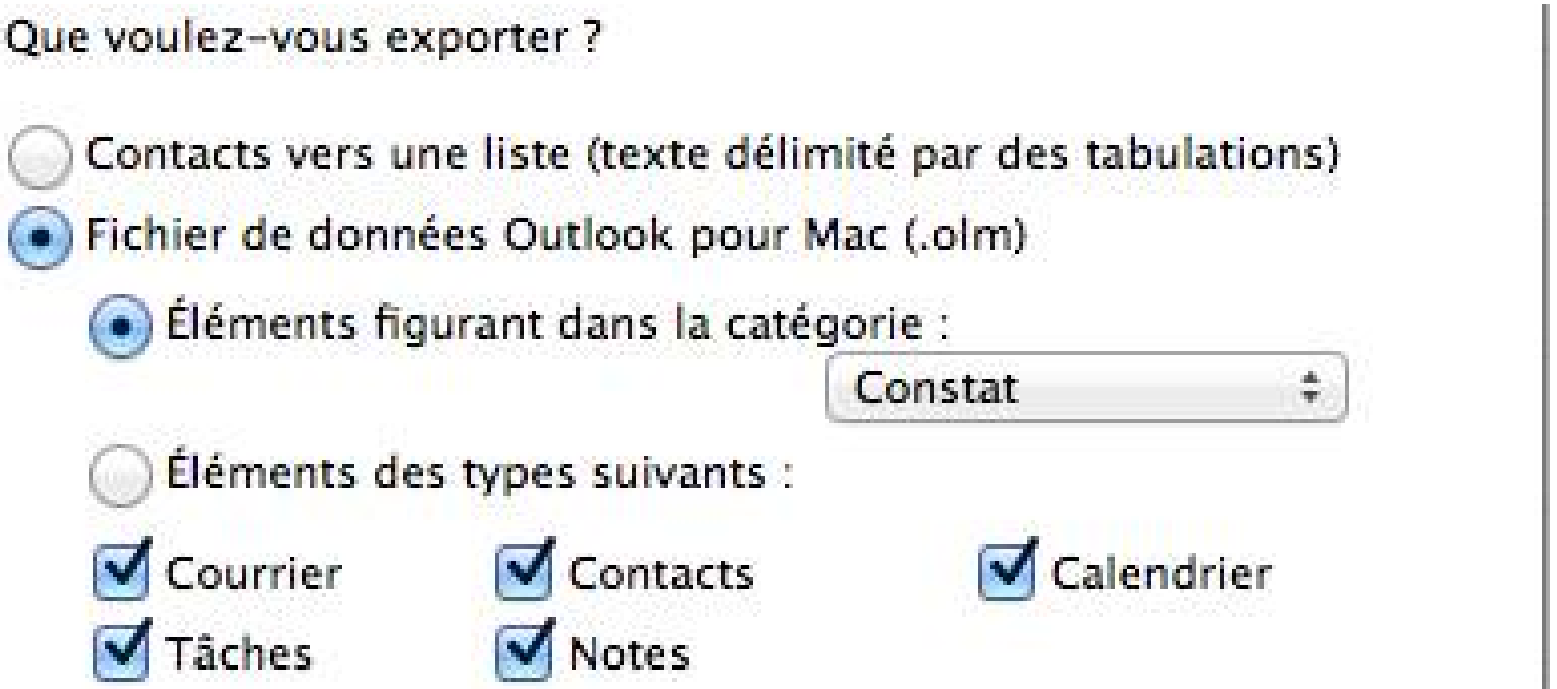
Les mails

- Stockage réparti entre mail et pièces jointes – nécessité de passer par les IHM
- Rechercher des mails
  - Spotlight
  - Le moteur de recherche intégré au client Mail
- Sauvegarder depuis Spotlight
  - Glisser sur le disque USB – attention cas de figure avec des sauvegardes partielles
- Imail
  - Copier dans un dossier puis exporter le dossier → une mbox qui peut être exploitée par ailleurs

Outlook

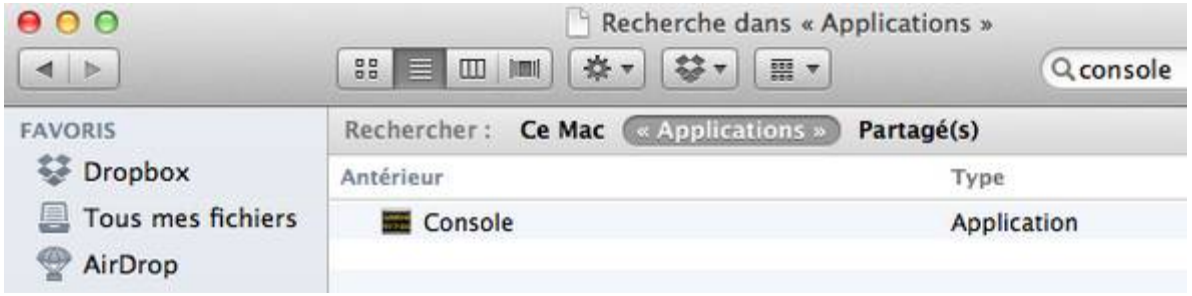
- Sauvegarder des mails depuis Spotlight
  - Glisser sur le disque USB
    - Attention – cf Serge
- Outlook
  - Glisser les mails à l'extérieurs, mais ne glisse pas les dossiers
  - Pour récupérer un dossier et sa hiérarchie – version lourde
    - Exporter toute la base
    - Importer dans Outlook Windows (cf outils Olm to PST)
  - Pour récupérer un dossier et sa hiérarchie – version modif
    - Rechercher les mails dans le sous dossier
    - Sélectionner les mails antérieurs à 2050
    - Focaliser la recherche sur le dossier et les sous dossiers
    - Sélectionner les messages restitués
    - Leur donner la catégorie « Constat »
    - Exporter la catégorie Constat


Accueil
Organiser
Outils
Rechercher
Dossier
Sous-dossiers
Tous les messages
Tous les éléments
De
Objet
Pièce jointe
Envoyé à
Reçu
Date d'env
Boîte de réception 907
Brouillons
Éléments envoyés
Éléments supprimés
Courrier indésirable 17
DOSSIERS VIRTUELS
Message à la priorité élevée
Message électronique marqué...
Message en retard
Réorganiser par : Conversations
[Pyflag-support] How do I load a pcap file for HTTP reconstr
Michael Cohen, isec demo
[Pyflag-support] PRB during make install
fpi, Michael Cohen
fpi
Michael Cohen
fpi
Michael Cohen
fpi
Michael Cohen
fpi
[Pyflag-support] libewf doesnt seem to load?

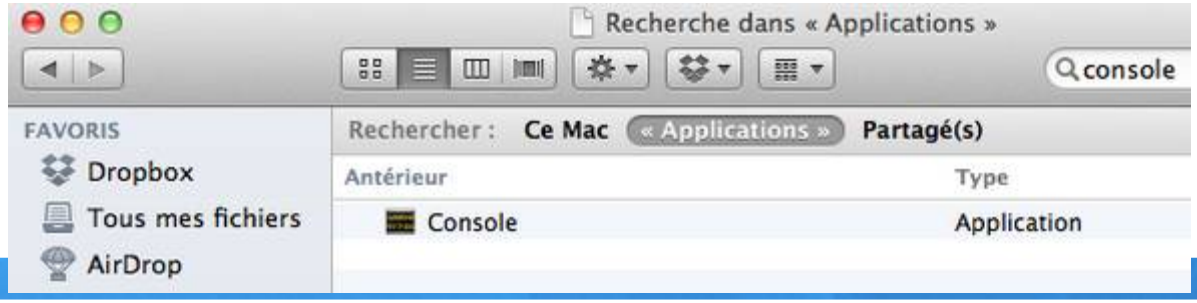

Que voulez-vous exporter ?
Contacts vers une liste (texte délimité par des tabulations)
Fichier de données Outlook pour Mac (.olm)
Éléments figurant dans la catégorie :
Constat
Éléments des types suivants :
Courrier
Contacts
Calendrier
Tâches
Notes

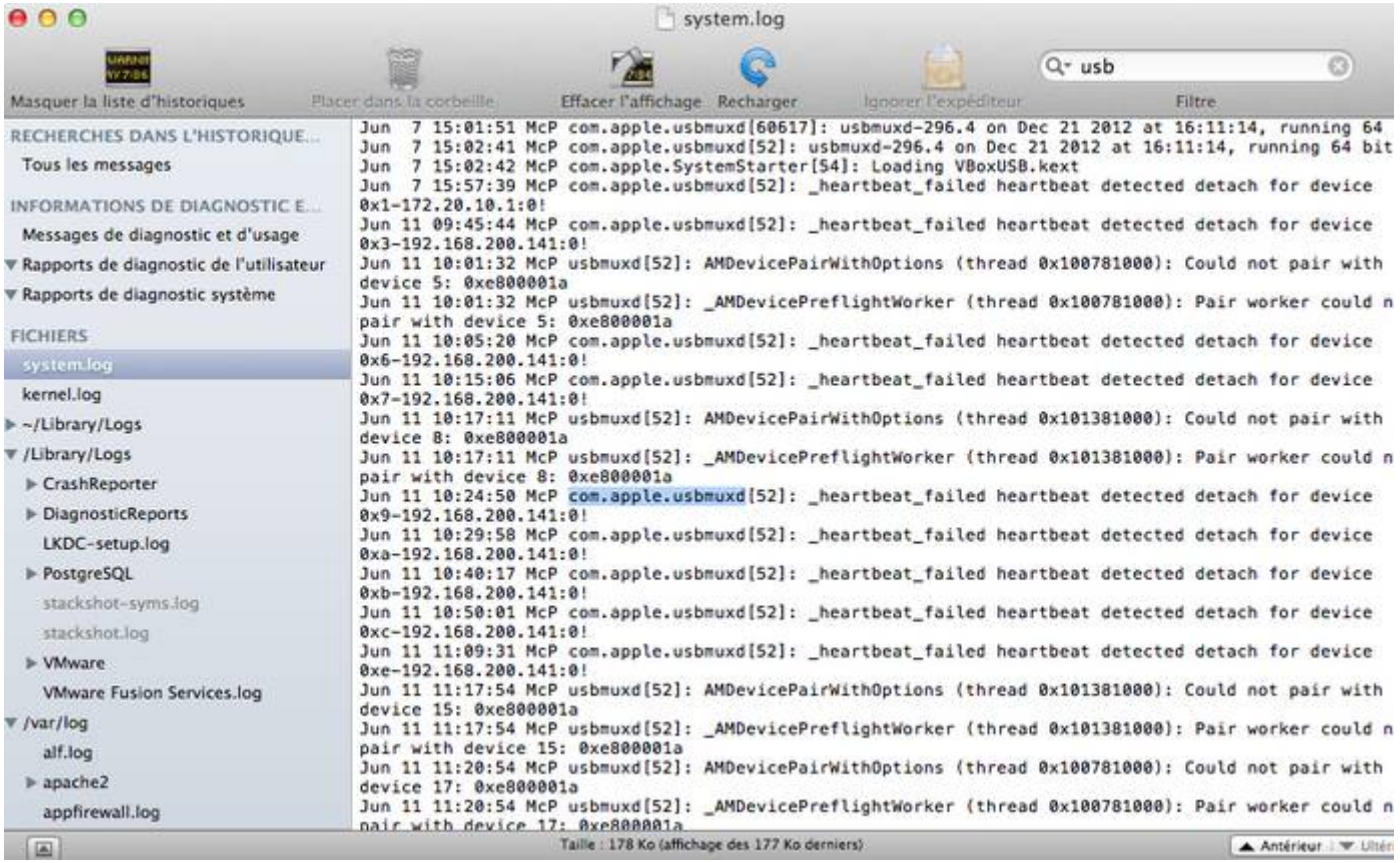
Les logs

- La console



- Les plist
  - Sudo find / -iname *.plist
- La ligne de commande
  - Terminal


Recherche dans « Applications »
console
FAVORIS
Dropbox
Tous mes fichiers
AirDrop
Rechercher :
Ce Mac
« Applications »
Partagé(s)
Antérieur
Type
Console
Application


system.log
Masquer la liste d'historiques
Placer dans la corbeille
Effacer l'affichage
Recharger
Ignorer l'expéditeur
usb
Filtre
RECHERCHES DANS L'HISTORIQUE...
Tous les messages
INFORMATIONS DE DIAGNOSTIC E...
Messages de diagnostic et d'usage
Rapports de diagnostic de l'utilisateur
Rapports de diagnostic système
FICHIERS
system.log
kernel.log
~/Library/Logs
/Library/Logs
CrashReporter
DiagnosticReports
LKDC-setup.log
PostgreSQL
stackshot-syms.log
stackshot.log
VMware
VMware Fusion Services.log
/var/log
alf.log
apache2
appfirewall.log
Jun 7 15:01:51 McP com.apple.usbmuxd[60617]: usbmuxd-296.4 on Dec 21 2012 at 16:11:14, running 64
Jun 7 15:02:41 McP com.apple.usbmuxd[52]: usbmuxd-296.4 on Dec 21 2012 at 16:11:14, running 64 bit
Jun 7 15:02:42 McP com.apple.SystemStarter[54]: Loading VBoxUSB.kext
Jun 7 15:57:39 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0x1-172.20.10.1:0!
Jun 11 09:45:44 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0x3-192.168.200.141:0!
Jun 11 10:01:32 McP usbmuxd[52]: AMDevicePairWithOptions (thread 0x100781000): Could not pair with device 5: 0xe800001a
Jun 11 10:01:32 McP usbmuxd[52]: _AMDevicePreflightWorker (thread 0x100781000): Pair worker could n
pair with device 5: 0xe800001a
Jun 11 10:05:20 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0x6-192.168.200.141:0!
Jun 11 10:15:06 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0x7-192.168.200.141:0!
Jun 11 10:17:11 McP usbmuxd[52]: AMDevicePairWithOptions (thread 0x101381000): Could not pair with device 8: 0xe800001a
Jun 11 10:17:11 McP usbmuxd[52]: _AMDevicePreflightWorker (thread 0x101381000): Pair worker could n
pair with device 8: 0xe800001a
Jun 11 10:24:50 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0x9-192.168.200.141:0!
Jun 11 10:29:58 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0xa-192.168.200.141:0!
Jun 11 10:40:17 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0xb-192.168.200.141:0!
Jun 11 10:50:01 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0xc-192.168.200.141:0!
Jun 11 11:09:31 McP com.apple.usbmuxd[52]: _heartbeat_failed heartbeat detected detach for device 0xe-192.168.200.141:0!
Jun 11 11:17:54 McP usbmuxd[52]: AMDevicePairWithOptions (thread 0x101381000): Could not pair with device 15: 0xe800001a
Jun 11 11:17:54 McP usbmuxd[52]: _AMDevicePreflightWorker (thread 0x101381000): Pair worker could n
pair with device 15: 0xe800001a
Jun 11 11:20:54 McP usbmuxd[52]: AMDevicePairWithOptions (thread 0x100781000): Could not pair with device 17: 0xe800001a
Jun 11 11:20:54 McP usbmuxd[52]: _AMDevicePreflightWorker (thread 0x100781000): Pair worker could n
Taille : 178 Ko (affichage des 177 Ko derniers)
Antérieur

Les plist

- Les fichiers conf du mac
- S'ouvre avec TextWrangler sur Mac
- Les répertoires de stockage
  - http://www.appleexaminer.com/MacsAndOS/Analysis/PLIST/PLIST.html
    - Les paramètres utilisateur
      - /Users/username/Library
    - Généralités
      - /Library
      - /Network/Library
      - /System/Library
      - /private/etc
      - /private/var

Les logs

/var/log/crashreporter.log	Application Usage History, information is written here when an application crashes only.
/var/log/cups/access_log	Printer Connection Information
/var/log/cups/error_log	Printer Connection Information
/var/log/daily.out	Network Interface History
/var/log/samba/log.nmbd	Samba (Windows based machine) connection information
~/Library/Logs	Any logs in this area will be specific to the user of this Home directory. Application specific logs will be found here
~/Library/Logs/DiscRecording.log	Log of CD or DVD media burned using the Finder. This is specific to the user of this Home directory.
~/Library/Logs/DiskUtility.log	Log of CD or DVD media burned using the Finder, mount and unmount history of ISO or DMG image files, Permission Repair history. and hard disk partition information.
~/Library/Logs/ iChatConnectionErrors	Log files here contain information of past iChat connection attempts. Data such as username, IP address, and Date&Time of the attempt

/System/Library/CoreServices/SystemVersion.plist	Contains the current version of the installed operating system
/private/var/log/OSInstall.custom	Contains the date and time the operating system was first installed (completion time, not start time)
/private/etc/hosts	Contains defined IP addresses and the associated name

The following PLIST files can be found in the user home directory ~/Library/Preferences/

File	Uses
AddressBookMe.plist	Contains the data this user has entered about him/her self
com.apple.Bluetooth.plist	Contains devices that have connected via Bluetooth. It will show last connection date as well.
com.apple.dashboard.plist	Contains information on installed Widgets for this user.
com.apple.dock.plist	Contains information on applications available in the Dock

Vous n'avez pas tout noté?


SFR
13:29
Espace de partage de la C…
Recherche
Catégories › Mac
juil 21, 2012
Quelques raccourcis clavier pour le Mac
Par Philippe Aymar
Catégories: Mac, Utils Forensics, Utils Rapport
mai 21, 2012
Memento d'acquisition Mac
Par Philippe Aymar
Catégories: Acquisition, Environnement, Image disque, Inventaire, Mac, Recherche fichiers, Recherche mails, Utils Forensics, Utils Rapport
mai 19, 2012
Les distributions forensics du moment
8


Réseau indisp.
14:21
blog.cnejita.org/2012/05
Rechercher
Espace de partage de la C…
Recherche
Guides et sites pour l'analyse de Macs
mai 18th, 2012 @ 07:16 › Philippe Aymar
↓ Laisser un commentaire
La référence
http://peelman.us/files/BasicMacForensics.pc
Un autre plus simple
http://www.appleexaminer.com/Downloads/M
Un annuaire d'utilitaires
http://homepage.mac.com/macbuddy/Forens
Catégories: Acquisition, Mac
8

Le blog – pour écrire

- http://blog.cnejita.org

- Ou un mail à behe106puqi@post.wordpress.com

Le mac dans son environnement

- Réplication avec la Time Machine

Transformer son Mac en machine d'investigation

- Pourquoi?
  - Léger…
  - Thunderbolt
  - Fait les PC et … les Macs
- Les utilitaires bas niveau
  - Installer « MacPort » - http://www.macports.org
  - Depuis Port, installer dcfldd, autopsy, etc.
- Les utilitaires haut niveau
  - Machine virtuelle avec Windows XP (ou > si le disque a de la place)

Les raccourcis clavier

- [- alt-shift-(
- { - alt-(
- | - alt-shift-L
- ~ - alt-shift-N

La protection des supports lus depuis le Mac

- Disk Arbitrator
  - https://github.com/aburgh/Disk-Arbitrator#readme
- Ou à la main
  - Supprimer "/etc/mach_init.d/diskarbitrationd.plist" et redémarrer
  - Prévoir un backup et recopier le fichier une fois les opérations faites

Monter un disque

- Diskutil list pour voir la liste des disques
- HdiUtil partition /dev/disk1
- Mount …
- Attention les drivers ntfs ne permettent pas d'écrire

Quelques autres pratiques non transposées

- La clé USB avec des applications portables
- Le tri par dossier dans le finder

- A vos Macs, prêts?