

Rendez-vous 4n6s

La pomme en 2021, digeste ou indigeste ?

29 Janvier 2021

Jean-Philippe Noat, Senior Director of Intl training chez Cellebrite

Johann Polewczyk, Responsable de recherche à l'Université de Lausanne

Format des rendez-vous

- Votre rendez-vous d'échange
- Proposer les sujets qui vous intéressent
- Poser des questions techniques, si toutes ne peuvent être répondues elles le seront lors du prochain rendez-vous.
- Faites vous plaisir et échangez
- Mettre l'humain au coeur de la technique
- N'hésitez pas à présenter un sujet si vous le souhaitez



Que faire en cas de pépin ?

En cas de perturbation technique :

mon portable +33 6 08 98 08 94

Pour toute question sur le thème (et les thèmes à venir)

jean-philippe.noat@cellebrite.com

johann@polewczyk.fr

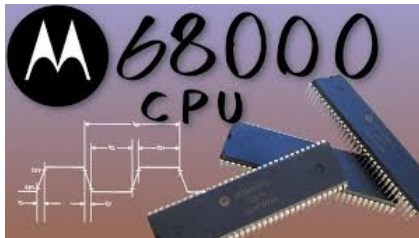
VOYAGE AU PAYS DE LA POMME QUELS CHANGEMENTS ?

UNE ÉVOLUTION DU MATÉRIEL

TRANSITION VERS DES PROCESSEURS MAISON

PROCESSEURS

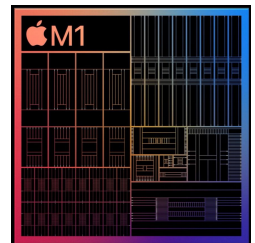
- 1984 – 1994 : Processeurs Motorola
- 1994 – 2006 : Processeurs PowerPC
- De juin 2005 à début 2007 : Transition vers les processeurs INTEL
 - Compatibilité pour les logiciels PowerPC avec la technologie « Rosetta »
 - Bootcamp permet d'installer nativement Microsoft Windows



TRANSITION VERS DES PROCESSEURS MAISON

PROCESSEURS ARM

- À partir de 2007 dans les iOS Devices
 - Processeurs Samsung (iPhone à iPhone 3GS)
 - Processeurs Apple
 - Ax : iPhone (depuis iPhone 4), iPad, AppleTV (depuis Apple TV 2^{ème} génération), HomePod
 - Sx : Apple Watch
- Transition depuis novembre 2020 dans les Mac
 - Processeur M1
 - MacBook Air (M1, 2020) → Model A2337 (EMC 3598) → MacBookAir10,1
 - MacBook Pro (13 pouces, M1, 2020) → Model A2338 (EMC 3578) → MacBookPro17,1
 - Mac mini (M1, 2020) → Model A2348 (EMC 3569) → Macmini9,1
 - *Mac mini Developer Transition Kit (DTK) → Model A2330 (EMC 3568) → ADP3.2*



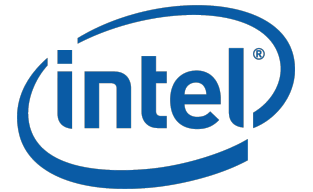
IDENTIFICATION DU MATÉRIEL

DOCUMENTATION APPLE

- Identification des modèles d'iMac
 - <https://support.apple.com/fr-fr/HT201634>
- Identification des modèles de Mac mini
 - <https://support.apple.com/fr-fr/HT201894>
- Identification des modèles de Mac Pro
 - <https://support.apple.com/fr-fr/HT202888>
- Identification des modèles de MacBook Air
 - <https://support.apple.com/fr-fr/HT201862>
- Identification des modèles de MacBook Pro
 - <https://support.apple.com/fr-fr/HT201300>
- Identification des modèles de MacBook
 - <https://support.apple.com/fr-fr/HT201608>
- Comment localiser le numéro de série de votre matériel Apple
 - http://support.apple.com/kb/HT1349?viewlocale=fr_FR

INTERRUPTION DE LA SÉQUENCE DE BOOT

MAC INTEL

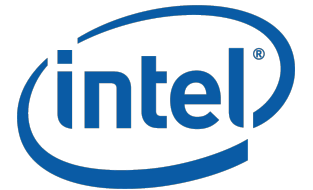


- Gestionnaire de démarrage (Boot manager)
 - Appuyer sur la touche '⌥ option' pendant le son de démarrage

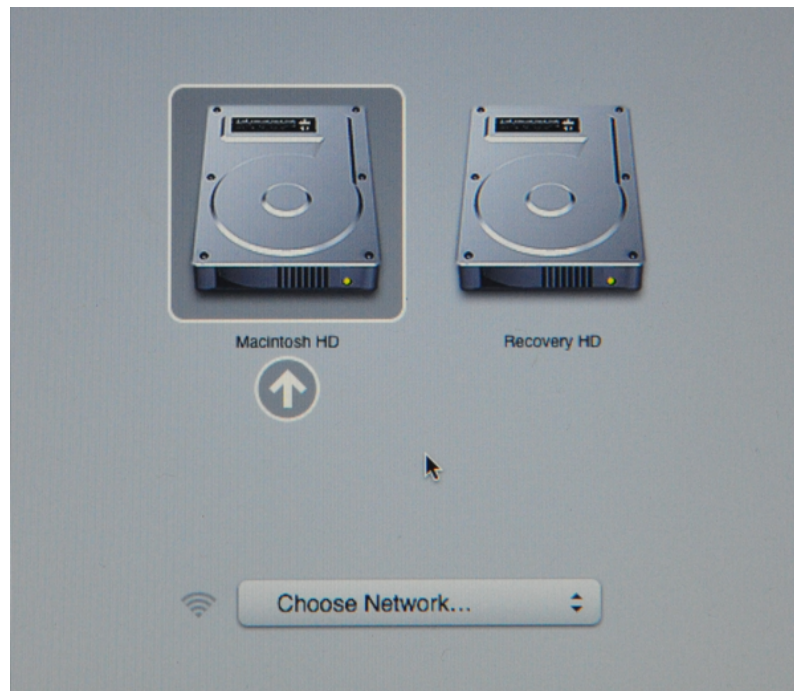


INTERRUPTION DE LA SÉQUENCE DE BOOT

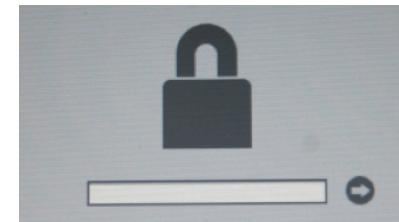
MAC INTEL



- Gestionnaire de démarrage (Boot manager)



- Vérification de la présence d'un mot de passe de l'EFI



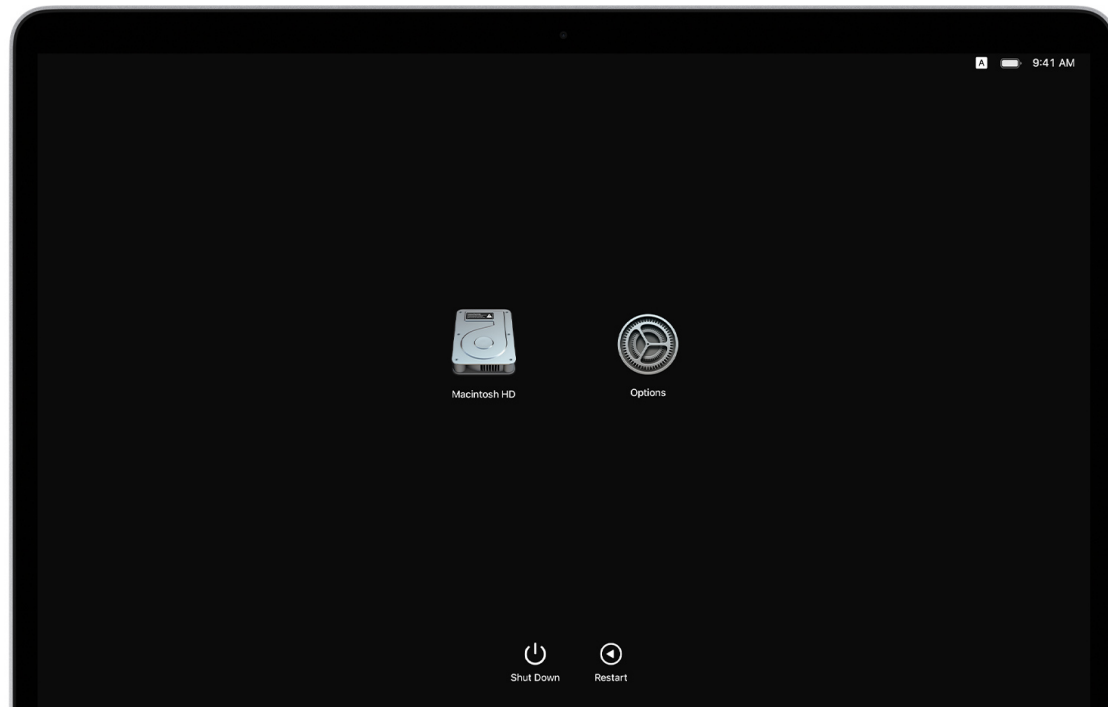
- Affichage de la liste des volumes bootables (partitions amorçables) des supports de stockage internes et externes (USB, FireWire et Thunderbolt).
- Appui sur la touche T pour basculer en Target Disk Mode

INTERRUPTION DE LA SÉQUENCE DE BOOT

MAC M1



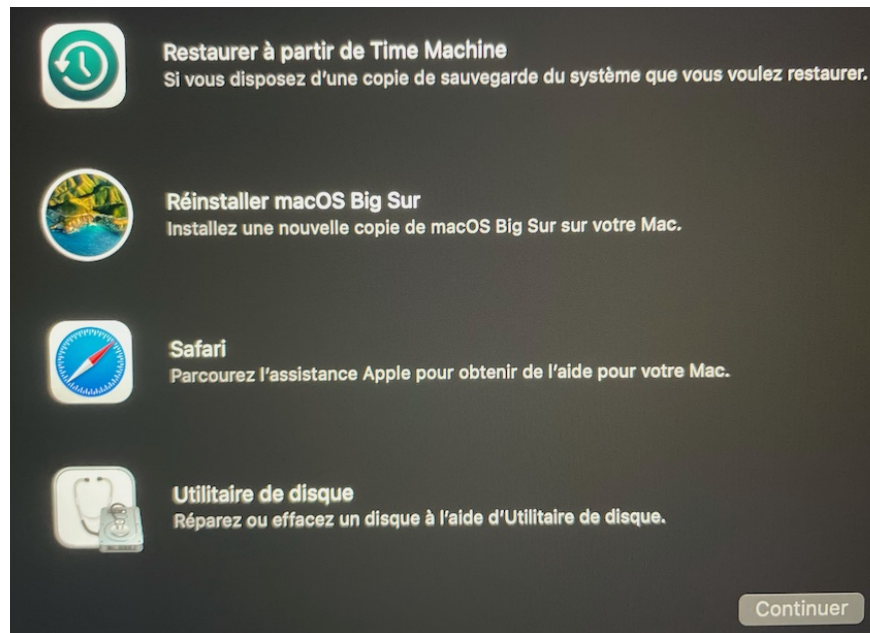
- Options de démarrage (Startup options)



- Maintenir le bouton de marche/arrêt enfoncé pendant au moins 10 secondes...
- Attention : Si filevault est activé, nécessité de fournir le mot de passe d'un compte utilisateur autorisé pour démarrer en Recovery Mode

RECOVERY MODE – PARTAGE DE DISQUE

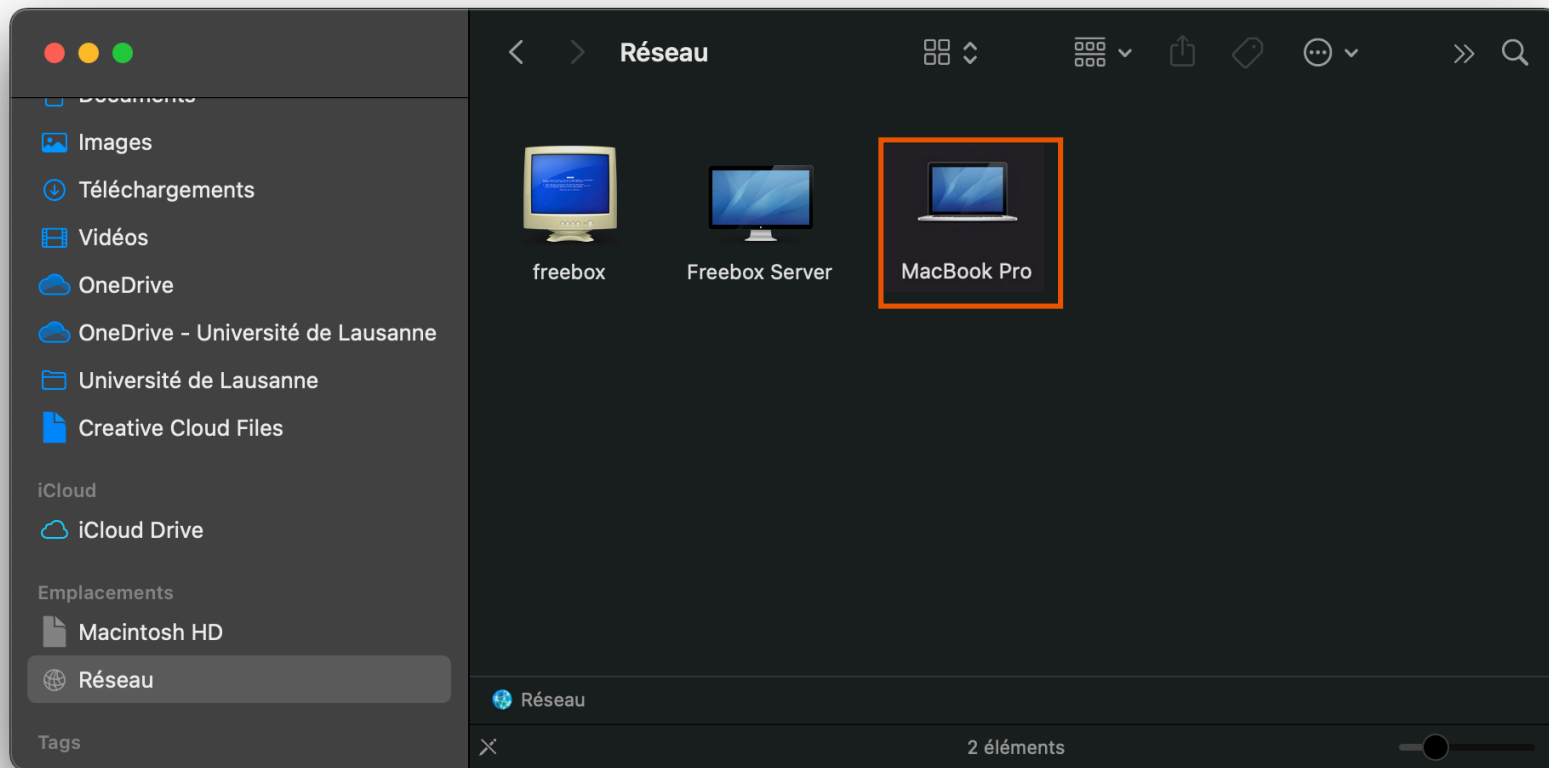
MAC M1



- Plus de Target Disk Mode mais partage de disque
 - Dans la barre des menus
 - Cliquer sur Utilitaires (Utilities)
 - Puis sélectionner Partage de disque... (Share Disk)
 - Sélectionner le volume à partager
 - Apparaît comme un disque réseau dans macOS
 - Utilisation du protocole SMB

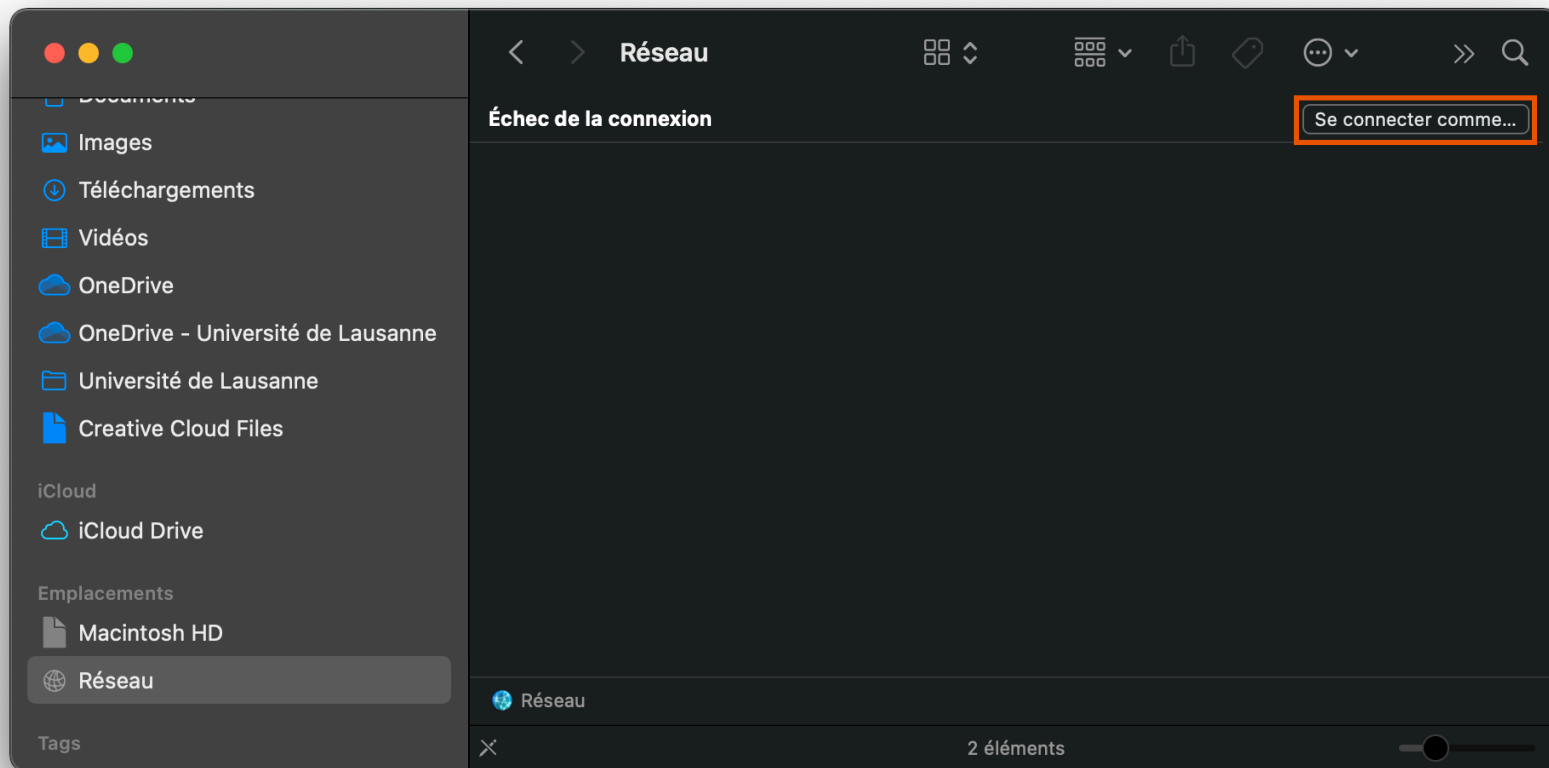
PARTAGE DE DISQUE

MAC M1



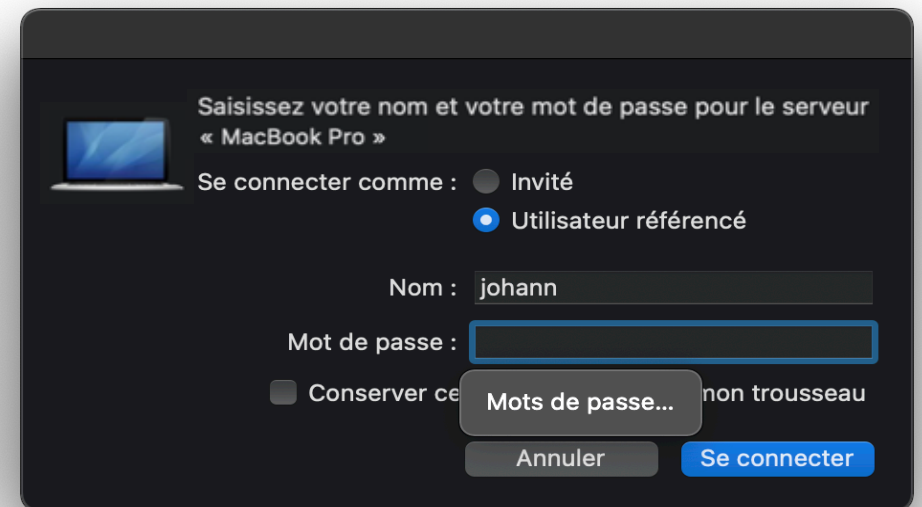
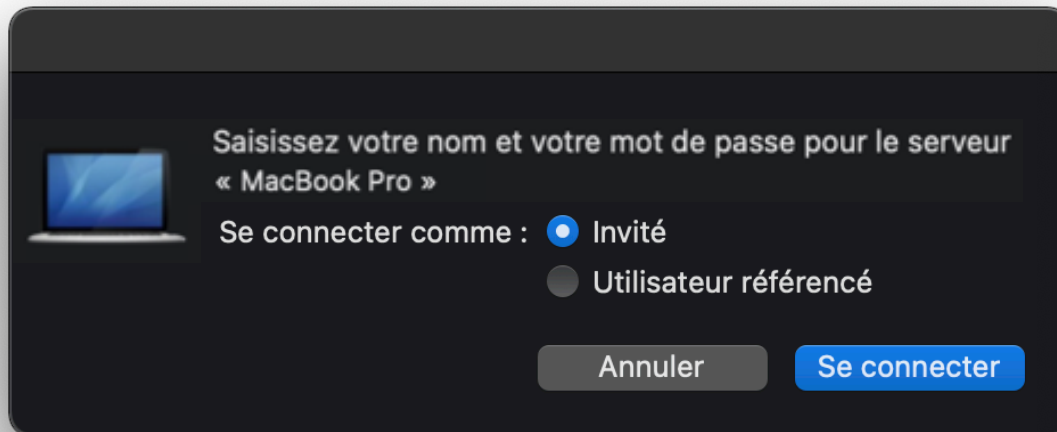
PARTAGE DE DISQUE

MAC M1



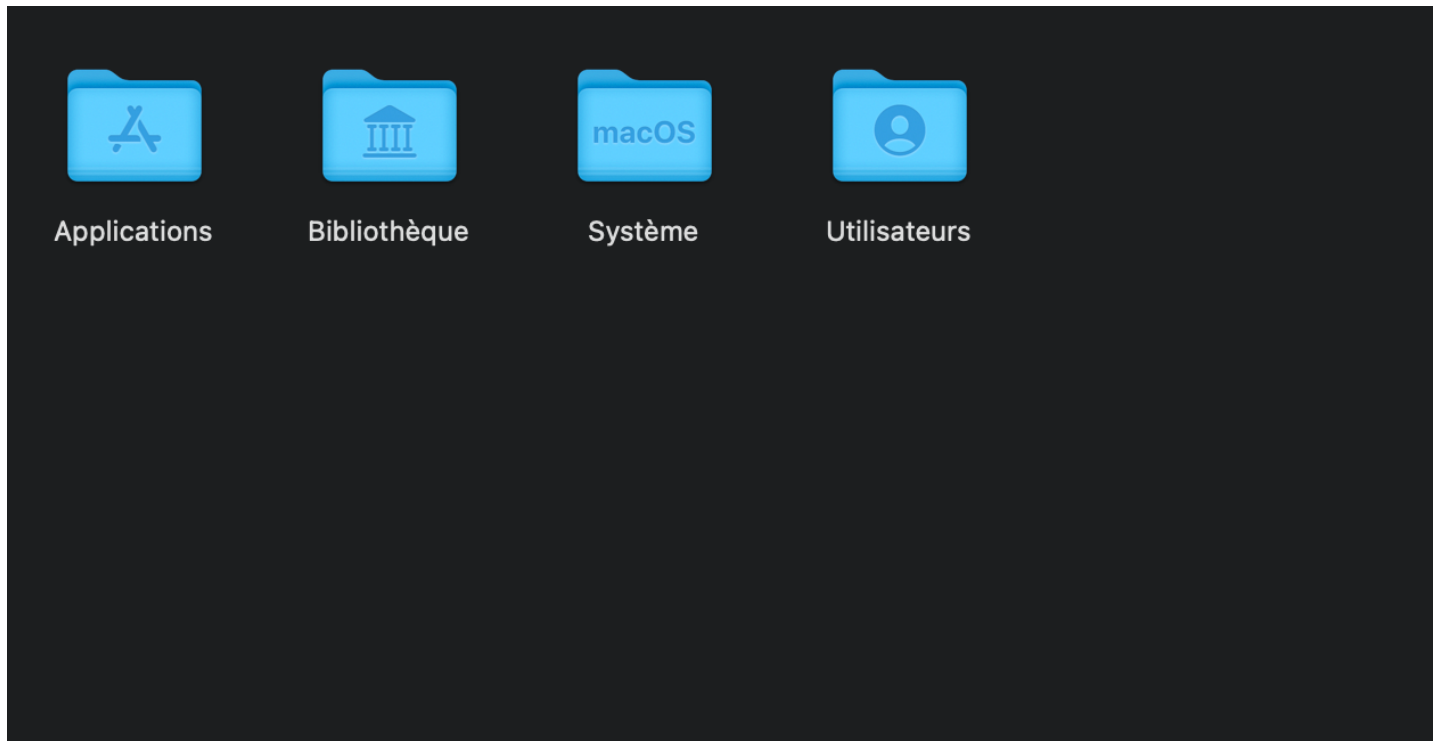
PARTAGE DE DISQUE

MAC M1



PARTAGE DE DISQUE

MAC M1



ET SUR MAC OS ?

QUELQUES RAPPELS

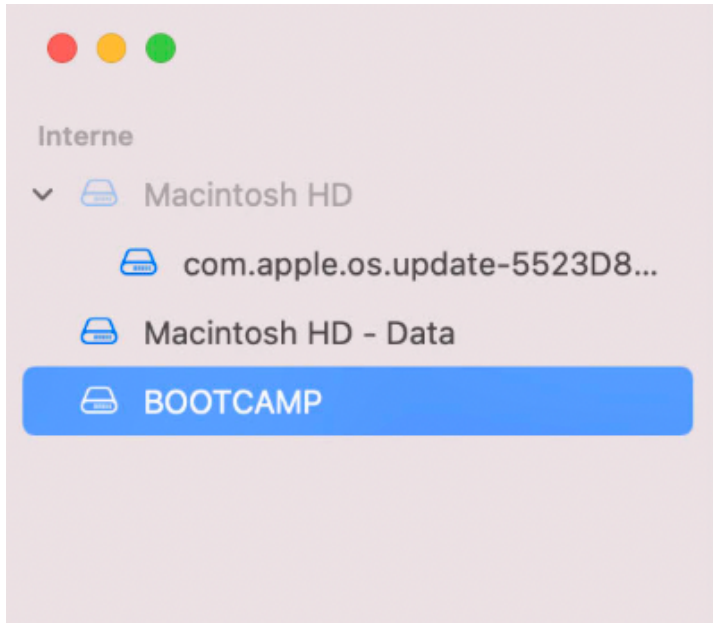
Nous sommes actuellement en macOS 11.1 (11.2 arrive / accessible en RC2)

Le nouveau système de fichiers APFS est apparu avec macOS 10.13 (volumes externes et SSD) et iOS 10.3

Depuis macOS 10.15 nous avons 2 volumes :

- Un volume système en lecture seule (Macintosh HD) (non accessible à compter de la version 11)
- Un volume en lecture / écriture (données utilisateurs) (Macintosh HD-Data)
- Pour l'utilisateur un seul volume est visible (le volume système est caché et protégé)

LE VOLUME SYSTÈME CACHÉ



Invisible à l'utilisateur

Montage en lecture seule

Contient les plist et bases de données de base du système d'exploitation

Contient les applicatifs système (les applications préinstallées par Apple)

Créé automatiquement dès la maj vers 10.15 (ou l'installation de macOS 11.x)

Avec macOS 11 BigSur il est Signed System Volume (SSV)

Chaque fichier pour garantir son intégrité a son propre hash SHA-256

Ce hash est stocké dans les métadonnées du système de fichier (APFS)

Cette information est elle aussi hashée

Quand un fichier du SSV est lu le hash du fichier est comparé à celui stocké pour détecter tout changement / modification. En cas de différence le fichier n'est pas exécuté.

LE VOLUME SYSTÈME EST SCELLÉ

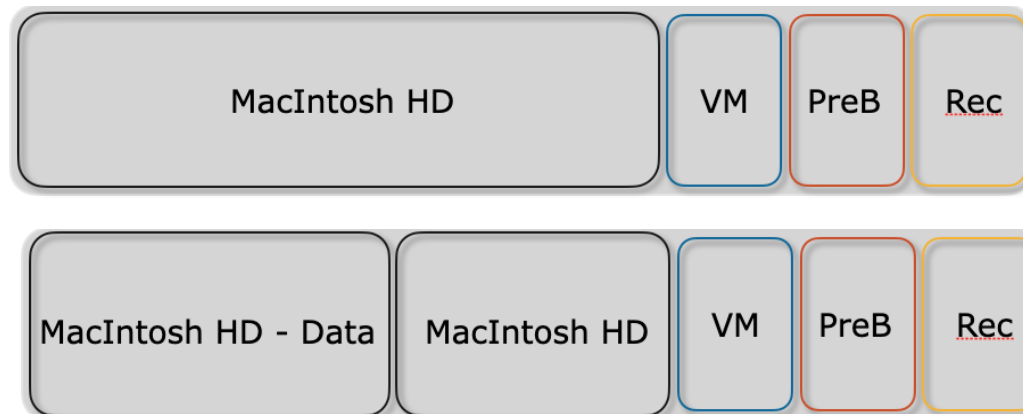
La valeur de hash du nœud root est considérée comme étant sous scellé par Apple

Il contient le hash du système de fichier pour le volume Système

Au boot le scellé (donc le hash) est comparé à l'état réel du volume système afin de tester si le volume a été modifié.

Si la vérification échoue la réinstallation de macOS est obligatoire.

Si pendant la mise à jour la vérification échoue, il y a retour à la version précédente en utilisant la technologie des snapshots.



QUELQUES PRINCIPES DE L'APFS

MacSSD
180GB

Data 20GB

Pooled Free
Space
800GB

On travaille au niveau d'un
container

Les volumes sont dynamiques

L'espace libre est partagé

MacSSD
180GB

Data
100GB

Pooled Free
Space
720GB

APFS (SUITE)

APFS	Macintosh HD - Data Snap 1	76806	181699454
APFS	Macintosh HD - Data Snap 2	76806	181699454
APFS	Macintosh HD - Data Snap 3	76806	181699454
APFS	Macintosh HD - Data Snap 4	76806	181699454
APFS	Macintosh HD - Data Snap 5	76806	181699454
APFS	Preboot	76806	181699454
APFS	Recovery	76806	181699454
APFS	VM	76806	181699454
APFS	Macintosh HD	76806	181699454
APFS	Update	76806	181699454
APFS	Unallocated	76806	181699454

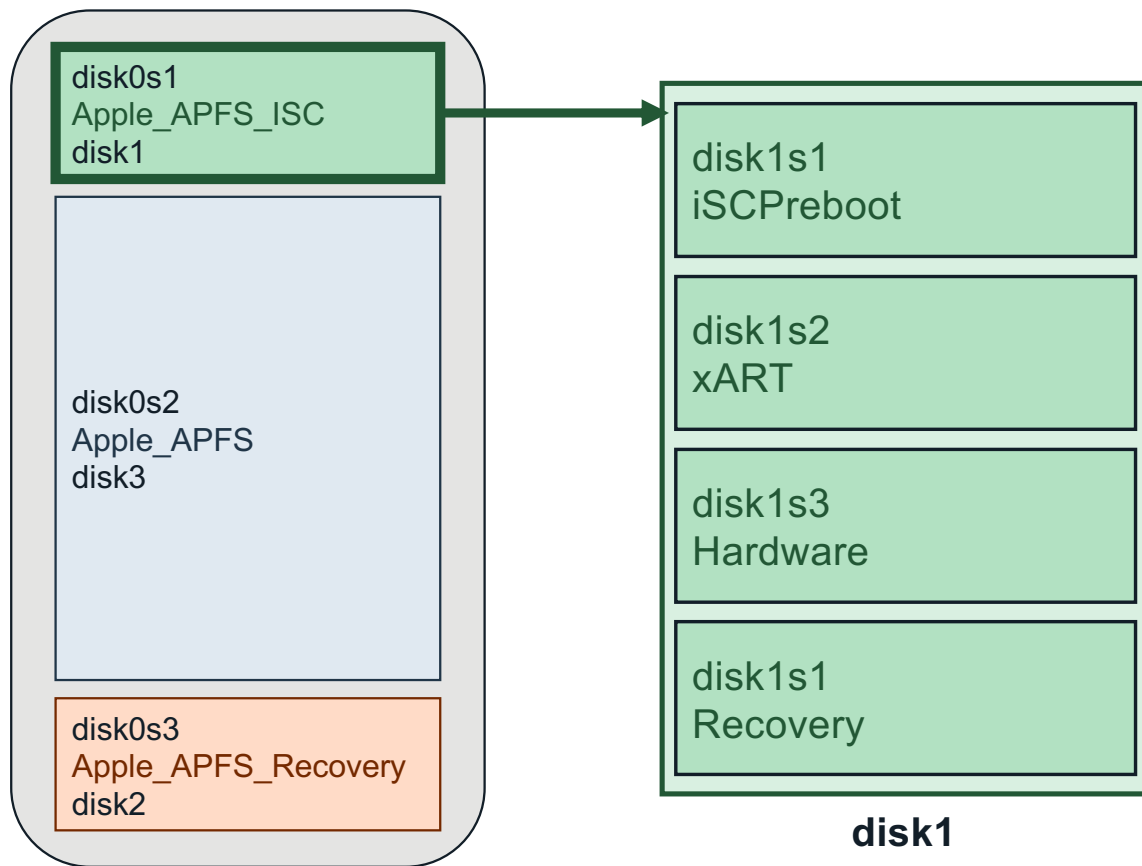
APFS (SUITE)

	HFS+	APFS
Nb de blocs	2^{32} (4.29 billion)	2^{63} (9 quintillion)
File ID	32-bit	64-bit
Taille maximum d'un fichier	2^{63} bytes	2^{63} bytes
Protection en cas de crash	journalisé	Ecriture à la demande
Format date/heure	1 seconde	1 nanoseconde



APFS
Apple File System

APFS (PARTICULARITÉS DU MAC M1)



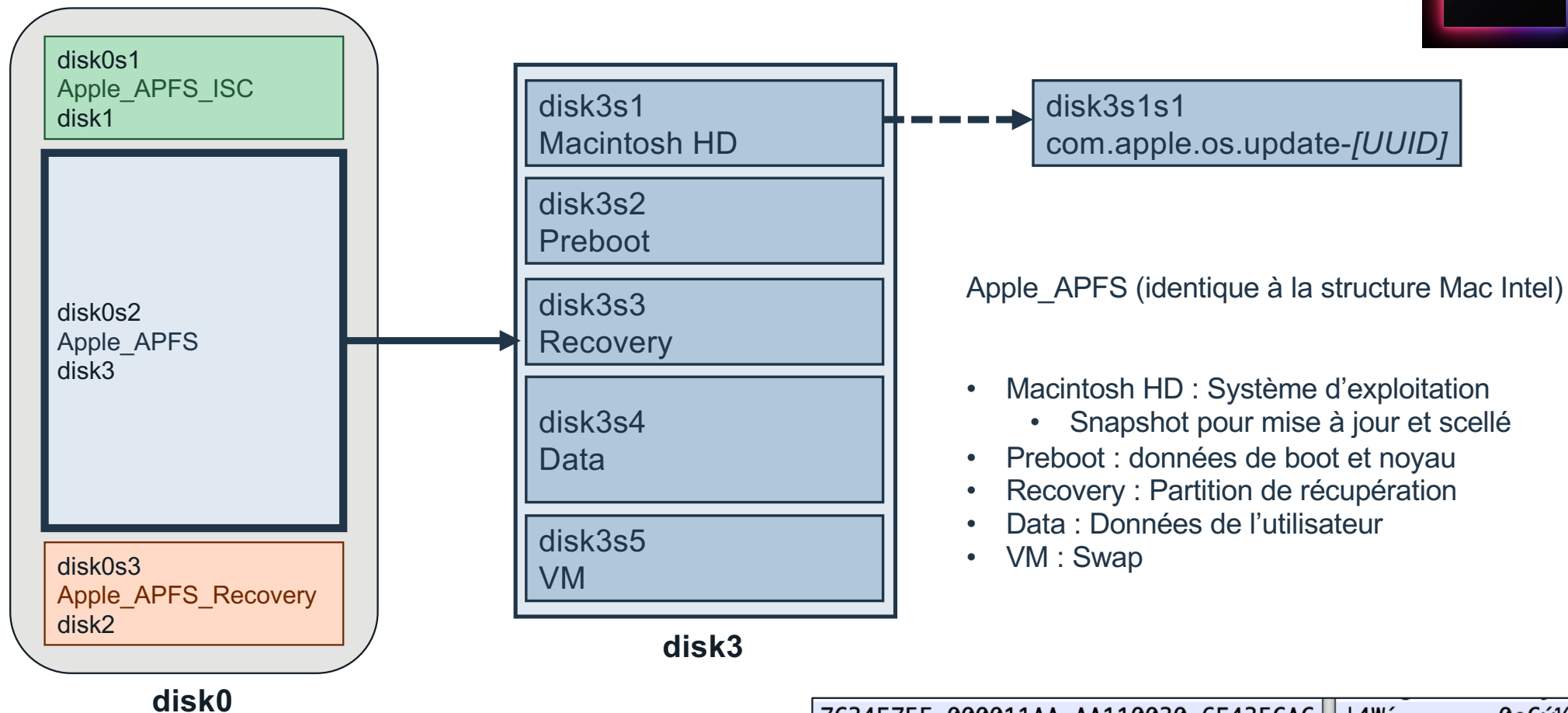
Apple_APFS_ISC : iBoot System Container

- iCSPPreboot : iBoot
- xART : stockage SEP
- Hardware : Infos relatives au matériel (logs et données d'activation)
- Recovery : Vide

disk1

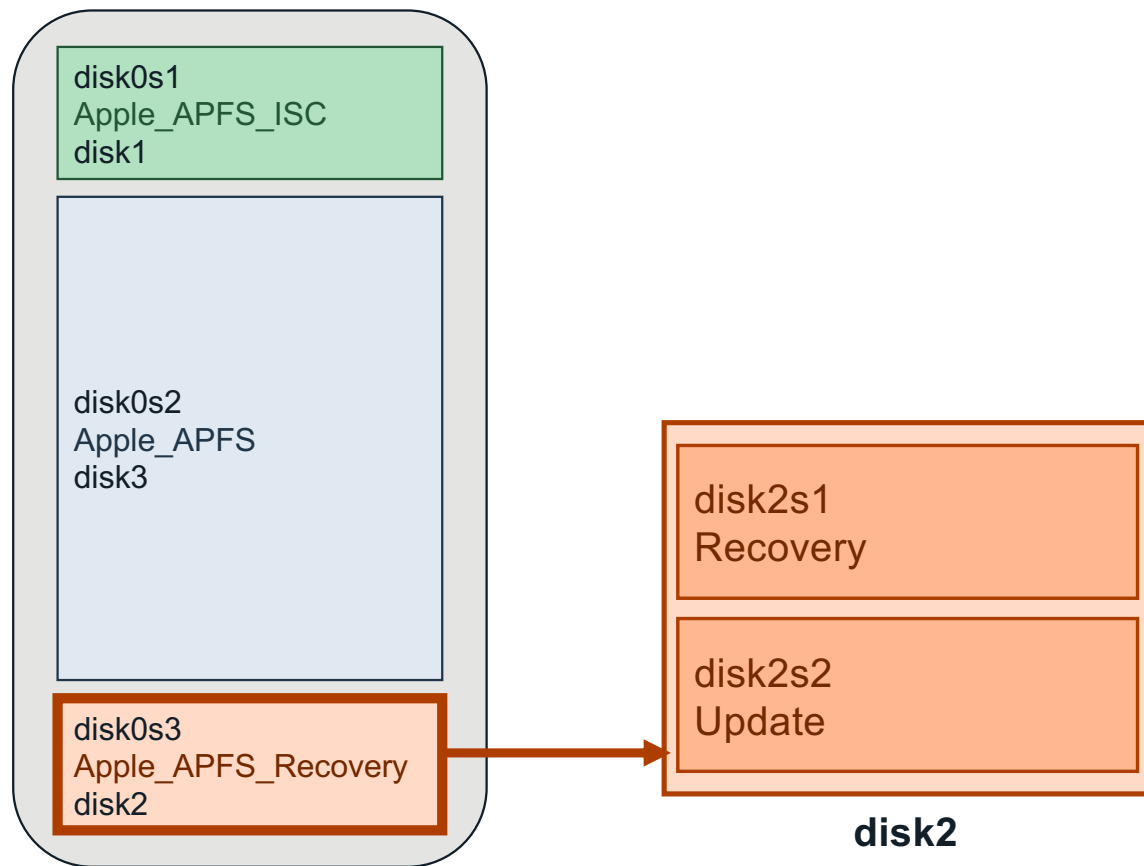
69646961 670011AA AA110030 6543ECAC | iddiag ↔ 0eCý%

APFS (PARTICULARITÉS DU MAC M1)



- Macintosh HD : Système d'exploitation
 - Snapshot pour mise à jour et scellé
- Preboot : données de boot et noyau
- Recovery : Partition de récupération
- Data : Données de l'utilisateur
- VM : Swap

APFS (PARTICULARITÉS DU MAC M1)



Apple_APFS_Recovery (Recovery OS)

- Recovery : One True Recovery
 - Contient notamment l'utilitaire de sécurité au démarrage (Startup Security Utility)
- Update :
 - Fichiers temporaires de mise à jour du firmware
 - Logs
 - ...

LES TRÉSORS DU PREBOOT

Preboot/<GUID>/System/Library/Caches/com.apple.corestorage/EncryptedRoot.plist.wipekey et recherche dans User information from <username>.plist /private/var/db/dslocal/nodes/default/user/ (Disque Data)

Key	Type	Value
Root	Dictionary	(2 items)
CryptoUsers	Array	(2 items)
Item 0	Dictionary	(6 items)
EFILoginGraphics	Dataavatar.png.....:avatar@2x.png.....
PassphraseHint	String	old
UserFullName	String	Mac Tester
Userid	String	0E7E9192-57B4-40A9-B936-6FD028014AA2
UserNamesData	Array	(4 items)
Item 0	Data	Mac Tester
Item 1	Data	mactester
Item 2	Data	macexamimer@icloud.com
Item 3	Data	com.apple.idms.appleid.prd.61706d3254584e7843426169352f54474c2f417152513d3d
UserType	Number	268828674
Item 1	Dictionary	(3 items)
WrappedVolumeKeys	Array	(1 item)

Utilisateur iCloud

Key	Type	Value
Root	Dictionary	(2 items)
0E7E9192-57B4-40A9-B936-6FD028014...	Dictionary	(6 items)
FullName	String	Mac Tester
PasswordHint	String	old
PictureData	Data	<View Picture>
PictureFormat	String	JPEG
ShortName	String	mactester
UserType	String	OpenDirectory
EBC6C064-0000-11AA-AA11-00306543E...	Dictionary	(1 item)

Preboot/GUID/System/Library/CoreServices/SystemVersion.plist

Key	Type	Value
Root	Dictionary	(6 items)
ProductBuildVersion	String	20B5022a
ProductCopyright	String	1983-2020 Apple Inc.
ProductName	String	macOS
ProductUserVisibleVersion	String	11.0.1
ProductVersion	String	11.0.1
IOSSupportVersion	String	14.2

diskutil APFS updatePreboot



QUELQUES PLIST INTÉRESSANTS

com.apple.finder.plist

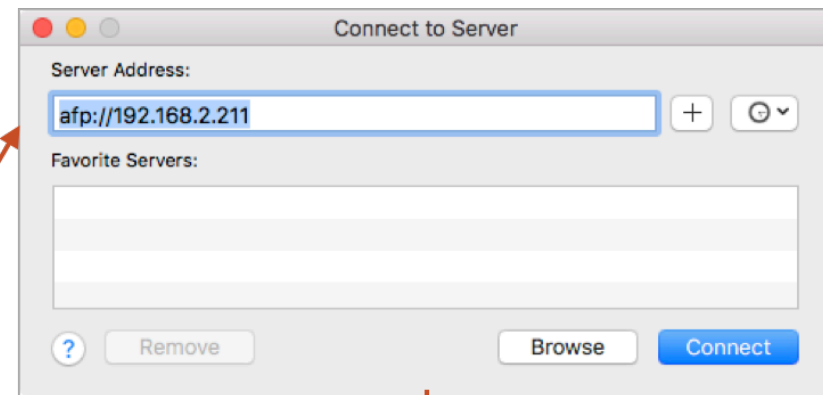
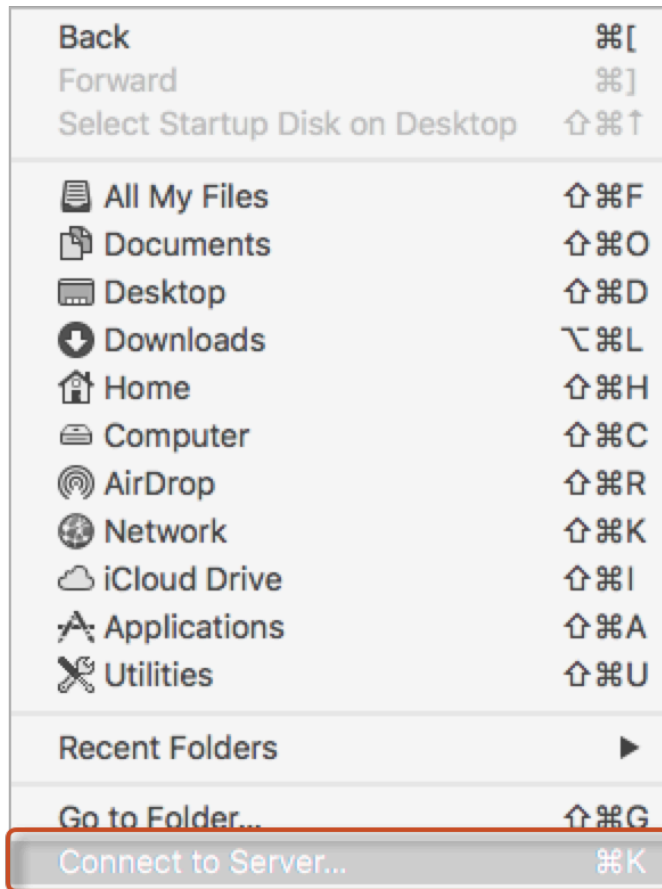
▼ FXRecentFolders	Array	(3 items)
▼ Item 0	Dictionary	(2 items)
file-bookmark	Data	book\.....0.....X.....Volumes.....Gambling.....ob.....
name	String	Gambling
▼ Item 1	Dictionary	(2 items)
file-bookmark	Data	book.....0.....t.....Users.....mactester.....Library.....Preferences
name	String	Preferences
▼ Item 2	Dictionary	(2 items)
file-bookmark	Data	bookX.....0.....<.....Users.....mactester.....Library..... ..4.....
name	String	Library

Liste les dossiers récemment ouverts (FXRecentFolders), à noter le nom du volume qui est listé comme un dossier

QUELQUES PLIST INTÉRESSANTS

com.apple.finder.plist

(FXConnectToLastURL)



▼ Root	Dictionary	(25 items)
CopyProgressWindowLocation	String	{640, 245}
▶ DesktopViewSettings	Dictionary	(1 item)
FXArrangeGroupViewBy	String	Name
FXConnectToBounds	String	{{597, 617}, {486, 231}}
FXConnectToLastURL	String	afp://192.168.2.211

QUELQUES PLIST INTÉRESSANTS

com.apple.finder.plist

▼ RecentMoveAndCopyDestinations	Array	(3 items)
Item 0	String	file:///Users/mactester/Downloads/
Item 1	String	file:///Users/mactester/Documents/
Item 2	String	file:///Volumes/BuzzWord/

Fichiers récemment déplacés / copiés

QUELQUES PLIST INTÉRESSANTS

com.apple.finder.plist

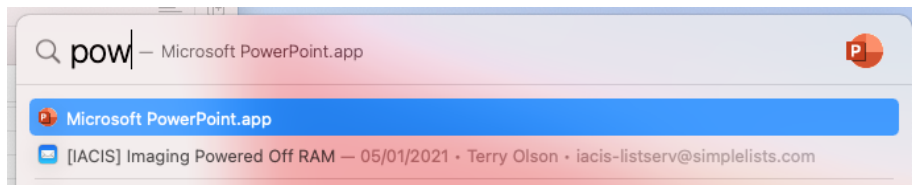
The image illustrates the connection between a Finder search and the underlying plist data. The top part shows a Finder window with a search for 'NAME good' on the Desktop, yielding the result 'GoodOne'. A red box highlights the search bar, which is then shown in a larger, detailed view on the right. Below this, a table represents the 'SGTRecentFileSearches' plist array. The second item in the array is highlighted with a red box, showing its attributes and values.

▼ SGTRecentFileSearches	Array	(2 items)
▼ Item 0	Dictionary	(7 items)
▼ attributes	Array	(1 item)
Item 0	String	kMDItemDisplayName
enforceStrictMatch	Boolean	False
exactMatch	Boolean	False
name	String	Wow
scope	Number	4
type	String	com.apple.finder
▼ values	Array	(1 item)
Item 0	String	Wow
▼ Item 1	Dictionary	(7 items)
▼ attributes	Array	(1 item)
Item 0	String	kMDItemDisplayName
enforceStrictMatch	Boolean	False
exactMatch	Boolean	False
name	String	good
scope	Number	4
type	String	com.apple.finder
▼ values	Array	(1 item)
Item 0	String	good

Recherches effectuées

QUELQUES PLIST INTÉRESSANTS

~/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3



Key	Type	Value
> photos	Dictionary	(3 items)
> plans	Dictionary	(3 items)
▼ po	Dictionary	(3 items)
DISPLAY_NAME	String	Microsoft PowerPoint.app
LAST_USED	Date	2020-11-16T12:05:22Z
URL	String	/Applications/Microsoft PowerPoint.app
▼ pow	Dictionary	(3 items)
DISPLAY_NAME	String	Microsoft PowerPoint.app
LAST_USED	Date	2021-01-28T13:44:44Z
URL	String	/Applications/Microsoft PowerPoint.app
▼ powe	Dictionary	(3 items)
DISPLAY_NAME	String	Microsoft PowerPoint.app
LAST_USED	Date	2020-10-26T05:29:34Z
URL	String	/Applications/Microsoft PowerPoint.app
▼ pre	Dictionary	(3 items)
DISPLAY_NAME	String	Adobe Premiere Pro 2020.app
LAST_USED	Date	2020-11-30T08:04:22Z
URL	String	/Applications/Adobe Premiere Pro 2020/Adobe Premiere Pro 2020.app

▼ pow	Dictionary	(3 items)
DISPLAY_NAME	String	Microsoft PowerPoint.app
LAST_USED	Date	2021-01-28T13:44:44Z
URL	String	/Applications/Microsoft PowerPoint.app

Recherches Spotlight effectuées

QUELQUES PLIST INTÉRESSANTS

/Users/<username>/Library/Application Support/com.apple.LSSharedfilelist/

RecentApplications.sfl

RecentDocuments.sfl2 : RecentDocuments.sfl

RecentHosts.sfl

RecentServers.sfl2

iCloudItems.sfl

FavoriteServers.sfl2

Les fichiers sfl / sfl2 sont en fait des fichiers plist

Key	Type	Value
✓ Root	Dictionary	(4 items)
✓ \$archiver	NSMutableDictionary...	(2 items)
✓ items	NSArray	(1 item)
✓ Item 0	NSMutableDictionary...	(5 items)
> Bookmark	Bookmark	bookp.....0.....ftp://ftp.dell.com.....
> CustomItemProperties	NSMutableDictionary...	(0 item)
Name	String	ftp://ftp.dell.com
uuid	String	61497769-B940-4AFD-BBF0-209698CE4DC5
visibility	Number	0
> properties	NSMutableDictionary...	(1 item)
> \$objects	Array	(21 items)
> \$top	Dictionary	(1 item)
\$version	Number	100000

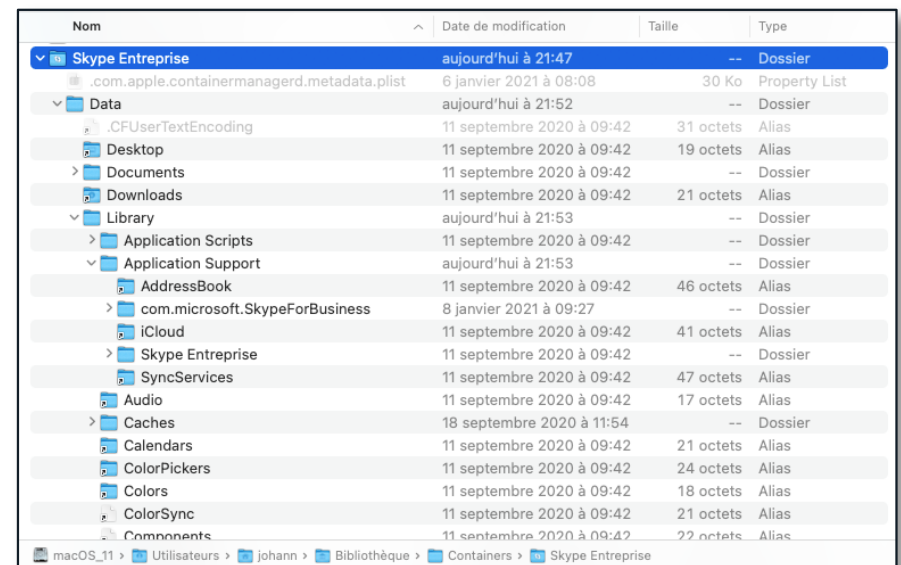
QUELQUES PLIST INTÉRESSANTS

FS ID	Name	Size	Date Created	Date Modified
72082	com.apple.LSSharedFileList.RecentServers.sfl2	1.7 KB	20 Dec 2017 14:42:30 (UTC)	20 Dec 2017 14:42:30 (UTC)
72081	com.apple.LSSharedFileList.RecentDocuments.sfl	3.2 KB	1 Apr 2016 18:41:05 (UTC)	1 Apr 2016 18:41:05 (UTC)
725215	com.apple.LSSharedFileList.FavoriteVolumes.sfl2	25.6 KB	5 Nov 2020 23:08:49 (UTC)	5 Nov 2020 23:08:49 (UTC)
72082	com.apple.LSSharedFileList.RecentServers.sfl2	1.7 KB	20 Dec 2017 14:42:30 (UTC)	20 Dec 2017 14:42:30 (UTC)
72081	com.apple.LSSharedFileList.RecentDocuments.sfl	3.2 KB	1 Apr 2016 18:41:05 (UTC)	1 Apr 2016 18:41:05 (UTC)
725215	com.apple.LSSharedFileList.FavoriteVolumes.sfl2	25.6 KB	5 Nov 2020 23:08:49 (UTC)	5 Nov 2020 23:08:49 (UTC)
46849	com.apple.LSSharedFileList.RecentApplications.sfl	10.1 KB	29 Nov 2017 20:07:10 (UTC)	29 Nov 2017 20:07:10 (UTC)
46845	com.apple.LSSharedFileList.FavoriteServers.sfl2	782 Bytes	4 Nov 2019 21:50:06 (UTC)	4 Nov 2019 21:50:06 (UTC)
650636	com.apple.LSSharedFileList.RecentServers.sfl2	1.6 KB	2 Nov 2020 16:14:12 (UTC)	2 Nov 2020 16:14:12 (UTC)
608931	com.apple.LSSharedFileList.RecentDocuments.sfl2	9.5 KB	30 Oct 2020 19:50:49 (UTC)	30 Oct 2020 19:50:49 (UTC)
46808	com.apple.ibooksx.sfl	446 Bytes	26 Oct 2016 12:59:01 (UTC)	26 Oct 2016 12:59:01 (UTC)
46830	com.apple.systempreferences.sfl	446 Bytes	26 Oct 2016 12:59:02 (UTC)	26 Oct 2016 12:59:02 (UTC)
46836	com.microsoft.autoupdate2.sfl	446 Bytes	5 Jul 2016 17:27:57 (UTC)	5 Jul 2016 17:27:57 (UTC)
46819	com.apple.nbagent.sfl	446 Bytes	26 Oct 2016 12:42:25 (UTC)	26 Oct 2016 12:42:25 (UTC)
46829	com.apple.systemevents.sfl	446 Bytes	21 Aug 2016 16:46:41 (UTC)	21 Aug 2016 16:46:41 (UTC)
46835	com.google.chrome.sfl	446 Bytes	25 May 2016 13:50:26 (UTC)	25 May 2016 13:50:26 (UTC)
46804	com.apple.backup.launcher.sfl	446 Bytes	26 Oct 2016 12:59:01 (UTC)	26 Oct 2016 12:59:01 (UTC)
46826	com.apple.safari.sfl	446 Bytes	26 Oct 2016 12:59:02 (UTC)	26 Oct 2016 12:59:02 (UTC)
46840	org.libreoffice.scrit.sfl2	11.9 KB	10 May 2020 21:07:47 (UTC)	10 May 2020 21:07:47 (UTC)

TRACES DES APPLICATIONS

OÙ RECHERCHER ?

- /Users/[username]
 - Library/[Nom_Application]
 - Library/Application Support/[Nom_Application]
 - Library/Application Support/[Bundle_Identifier]
 - Library/Containers/[Nom_Application]
 - Library/Containers/[Bundle_Identifier]
 - Library/Group Containers/[Bundle_Identifier]
 - Library/Preferences/[Bundle_Identifier].plist



Nom	Date de modification	Taille	Type
Skype Entreprise	aujourd'hui à 21:47	--	Dossier
.com.apple.containermanagerd.metadata.plist	6 janvier 2021 à 08:08	30 Ko	Property List
Data	aujourd'hui à 21:52	--	Dossier
.CFUserTextEncoding	11 septembre 2020 à 09:42	31 octets	Alias
Desktop	11 septembre 2020 à 09:42	19 octets	Alias
Documents	11 septembre 2020 à 09:42	--	Dossier
Downloads	11 septembre 2020 à 09:42	21 octets	Alias
Library	aujourd'hui à 21:53	--	Dossier
Application Scripts	11 septembre 2020 à 09:42	--	Dossier
Application Support	aujourd'hui à 21:53	--	Dossier
AddressBook	11 septembre 2020 à 09:42	46 octets	Alias
com.microsoft.SkypeForBusiness	8 janvier 2021 à 09:27	--	Dossier
iCloud	11 septembre 2020 à 09:42	41 octets	Alias
Skype Entreprise	11 septembre 2020 à 09:42	--	Dossier
SyncServices	11 septembre 2020 à 09:42	47 octets	Alias
Audio	11 septembre 2020 à 09:42	17 octets	Alias
Caches	18 septembre 2020 à 11:54	--	Dossier
Calendars	11 septembre 2020 à 09:42	21 octets	Alias
ColorPickers	11 septembre 2020 à 09:42	24 octets	Alias
Colors	11 septembre 2020 à 09:42	18 octets	Alias
ColorSync	11 septembre 2020 à 09:42	21 octets	Alias
Components	11 septembre 2020 à 09:42	22 octets	Alias



Pour en savoir plus

Rendez-vous sur le cours CAF / CAAF
(Cellebrite Apple Investigation / Cellebrite
Advanced Apple Investigation) qui peuvent
être donnés en français

Digital Collector

EX MACQUISITION

Feature	Digital Collector	Sumuri	ADF Triage
Démarrage au boot Windows	✓	✗	✓
Démarrage au boot sur Mac	✓	✓	✓
Analyse live sur Windows	✓	✗	✓
Analyse live pour Mac	✓	✓	✗
Récupération du contenu du disque sur Windows	✓	✗	✓
Récupération du contenu du disque sur Mac	✓	✗	✓
Récupération selective pour Windows et Mac	✓	✓	✓

PA Over DB (PA 8.0) arrive

LA NOUVELLE GENERATION DES OUTILS DE DECODAGE

Des performances grandement améliorées (tout est en base de données et plus en mémoire)

Conservation des données de décodage et ouverture instantanée du cas

Nouvelle interface utilisateur



Le webinar est enregistré

le service CAS est disponible en France

2ème surprise : vous allez avoir accès en exclusivité à la version beta de PA 8.0 et pouvoir avoir un impact sur son développement