



2e Rendez-vous 4n6s

05 Mai 2020

Jean-Philippe Noat Directeur international du training chez Cellebrite

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

SHADOW COPY

C'est quoi ce truc ?

- VSS (ou Volume Snapshot Service) a été introduit depuis Windows XP
- Le but premier est de pouvoir faire un retour arrière du système quand c'est nécessaire.
- 64 snapshots peuvent être stockés sur un système
- Windows 7 crée des sauvegardes automatiquement tous les 24h par défaut et à chaque changement de configuration
- Les sauvegardes sont incrémentales
- Possibilité pour l'utilisateur de retrouver d'anciennes versions de documents.
- On travaille au niveau « bloc » c'est à dire par groupes de cluster (en général les blocs font 16Ko).
- Attention au comportement qui est différent suivant le système d'exploitation
- Jusqu'à présent compliqué à exploiter complètement.



1ère version avec Windows XP

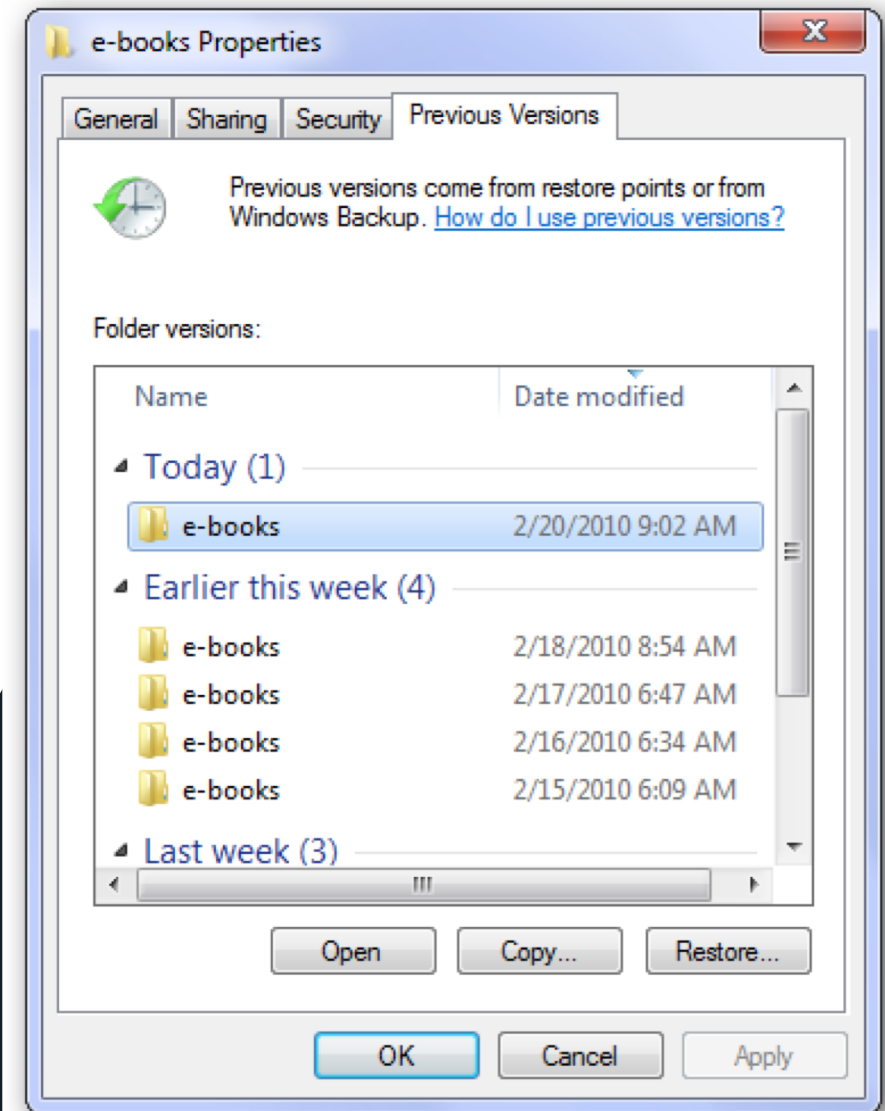
- Ne concerne que les fichiers systèmes
- Se nomme point de restauration
- Permet de récupérer les différentes versions du registre
- Manuels ou automatiques
- Fichiers utilisateurs non concernés

To begin, select the task that you want to perform:

- ☒ Restore my computer to an earlier time
- ☐ Create a restore point

Amélioration avec Vista et Windows 7

- Restauration du Système + Windows Backup
- Fonctionne au niveau Bloc (16 K octets) pour gérer des sauvegardes incrémentales
- Le terme se nomme VSCs
- Concerne cette fois tous les fichiers



Définition complète

Le Service Volume Shadow Copy est un mécanisme intégré à Windows qui permet la création de sauvegardes ponctuelles des données connues en tant que shadow copies ou aussi snapshot

Les sauvegardes se font au niveau bloc pour tout ce qui a été modifié.

2003 Serveur : les utilisateurs ont la possibilité de récupérer des versions précédentes de leurs documents au niveau d'un mappage réseau.

Vista : Les utilisateurs ont la possibilité de récupérer des anciennes versions de leur fichier (version Entreprise / Business / Ultimate)

Windows 7 : toutes versions

Windows 10 : seule la protection du système est activée par défaut. Les sauvegardes doivent être activées manuellement et sur un autre lecteur.

Les vieilles versions sont écrasées. Les shadows peuvent être sur le disque local ou sur un disque externe.

Windows 10

Historique des fichiers

← → ↕ ↑ > Panneau de configuration > Tous les Panneaux de configuration > Historique des fichiers

Page d'accueil du panneau de configuration

Restaurer des fichiers personnels

Sélectionner un lecteur

Exclure des dossiers

Paramètres avancés

Conservez un historique de vos fichiers.

L'historique des fichiers enregistre des copies de vos fichiers ; vous pouvez ainsi les récupérer s'ils sont perdus ou endommagés.

L'historique des fichiers est désactivé.

Copier les fichiers à partir de : Bibliothèques, Bureau, Contacts et Favoris

Copier les fichiers vers :



Disque local (D:)
320 Go disponible(s) sur 930 Go

Activer

Exemple de Shadow Copy

<Volume>\System Volume Information

System Volume Information	2016-11-24 00:01:00 (UTC)	2018-02-14 08:04:39 (UTC)	2018-02-14 08:04:39 (UTC)	--
MountPointManagerRemoteDat...	2016-11-24 00:01:00 (UTC)	2016-11-24 00:01:00 (UTC)	2016-11-24 00:01:00 (UTC)	0 Bytes
SPP	2016-11-23 15:31:10 (UTC)	2018-02-13 08:25:07 (UTC)	2018-02-13 08:25:07 (UTC)	--
Syscache.hve	2016-11-23 15:24:38 (UTC)	2018-02-15 09:52:29 (UTC)	2018-02-15 09:52:29 (UTC)	768,0 KB hve
Syscache.hve.LOG1	2016-11-23 15:24:38 (UTC)	2018-02-15 09:52:12 (UTC)	2016-11-23 15:24:38 (UTC)	161,0 KB LOG1
Syscache.hve.LOG2	2016-11-23 15:24:38 (UTC)	2016-11-23 15:24:38 (UTC)	2016-11-23 15:24:38 (UTC)	0 Bytes LOG2
tracking.log	2016-11-23 15:24:36 (UTC)	2016-11-23 15:25:10 (UTC)	2016-11-23 15:24:36 (UTC)	20,0 KB log
Windows Backup	2017-11-08 08:21:39 (UTC)	2017-11-08 08:21:39 (UTC)	2017-11-08 08:21:39 (UTC)	--
{05cdeead-0fc5-11e8-9766-f4066...	2018-02-13 08:24:58 (UTC)	2018-02-15 09:42:17 (UTC)	2018-02-13 08:24:58 (UTC)	1,1 GB
{2237554f-ff44-11e7-b5eb-f40669...	2018-01-29 09:16:42 (UTC)	2018-02-05 13:06:36 (UTC)	2018-01-29 09:16:42 (UTC)	619,4 MB
{3808876b-c176-4e48-b7ae-0404...	2017-03-16 07:19:01 (UTC)	2017-03-16 07:19:01 (UTC)	2017-03-16 07:19:01 (UTC)	64,0 KB
{3a4b29c8-f9c4-11e7-b4b8-f4066...	2018-01-18 12:05:05 (UTC)	2018-01-29 09:16:46 (UTC)	2018-01-18 12:05:05 (UTC)	657,3 MB
{4a02293b-d8c2-11e7-b643-f4066...	2017-12-07 09:49:11 (UTC)	2017-12-14 10:05:52 (UTC)	2017-12-07 09:49:11 (UTC)	593,9 MB
{4d1acbbc-eee2-11e6-b473-f4066...	2017-02-14 08:14:31 (UTC)	2017-02-21 15:55:06 (UTC)	2017-02-14 08:14:31 (UTC)	3,3 GB
{5c54bbb6-f056-11e7-b332-f4066...	2018-01-03 08:38:26 (UTC)	2018-01-11 09:46:48 (UTC)	2018-01-03 08:38:26 (UTC)	601,5 MB
{6d3172c5-f444-11e7-b296-f4066...	2018-01-11 09:46:45 (UTC)	2018-01-18 12:05:07 (UTC)	2018-01-11 09:46:45 (UTC)	636,0 MB
{6d95fea7-c843-11e7-b799-f4066...	2017-11-14 09:15:24 (UTC)	2017-11-22 08:19:01 (UTC)	2017-11-14 09:15:24 (UTC)	602,3 MB
{9ba1c12a-ce89-11e7-b217-f4066...	2017-11-22 08:18:58 (UTC)	2017-11-29 09:52:40 (UTC)	2017-11-22 08:18:58 (UTC)	525,3 MB
{9ba1c174-ce89-11e7-b217-f4066...	2017-11-29 09:52:37 (UTC)	2017-12-07 09:49:13 (UTC)	2017-11-29 09:52:37 (UTC)	672,4 MB
{a221d79c-5662-11e7-af6d-f4066...				0 Bytes
{a221d89e-5662-11e7-af6d-f4066...				0 Bytes
{c6021af4-a737-11e7-8406-f4066...				0 Bytes
{c6021b37-a737-11e7-8406-f4066...	2017-10-11 07:33:57 (UTC)	2017-10-19 09:07:23 (UTC)	2017-10-11 07:33:57 (UTC)	650,8 MB
{cce1951a-c2be-11e7-b336-f4066...	2017-11-06 09:40:30 (UTC)	2017-11-14 09:15:27 (UTC)	2017-11-06 09:40:30 (UTC)	703,3 MB
{cf4de91d-de46-11e7-b030-f4066...	2017-12-14 10:05:50 (UTC)	2018-01-03 08:38:27 (UTC)	2017-12-14 10:05:50 (UTC)	861,4 MB
{d9ef5b45-0a4a-11e8-b0e8-f4066...	2018-02-05 13:06:33 (UTC)	2018-02-13 08:25:00 (UTC)	2018-02-05 13:06:33 (UTC)	617,8 MB
{dcc60620-b237-11e7-aeb6-f4066...	2017-10-19 09:07:17 (UTC)	2017-10-27 10:24:11 (UTC)	2017-10-19 09:07:17 (UTC)	506,2 MB
{dcc60663-b237-11e7-aeb6-f4066...	2017-10-27 10:24:08 (UTC)	2017-11-06 09:40:34 (UTC)	2017-10-27 10:24:08 (UTC)	611,5 MB
{03a9ccc5-4ff9-11e7-b529-f40669...	2017-06-13 08:45:37 (UTC)	2017-06-21 08:56:07 (UTC)	2017-06-13 08:45:37 (UTC)	409,2 MB
{03a9ccc3-4ff9-11e7-b529-f40669...	2017-06-21 08:56:02 (UTC)	2017-06-28 09:40:13 (UTC)	2017-06-21 08:56:02 (UTC)	628,6 MB
{146ee747-0310-11e7-0279-f4066...	2017-03-16 07:19:01 (UTC)	2017-03-27 07:01:02 (UTC)	2017-03-16 07:19:01 (UTC)	434,0 MB

Ce qui n'est pas sauvegardé

- Espace non alloué
- Slack
- Pagefile.sys
- Hiberfil.sys
- Autres éléments....

Fréquence d'exécution des Shadow copies ?

A chaque windows update

A chaque installation de nouveaux logiciels / drivers

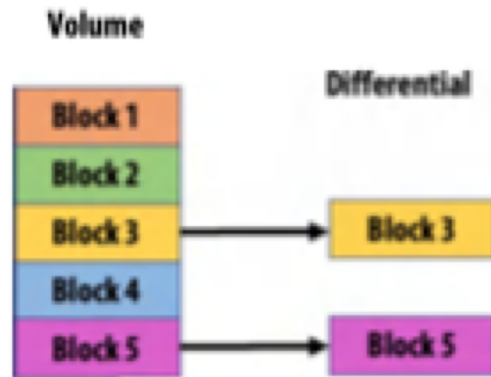
Chaque 24h sur certains systèmes (Vista)

Une fois par semaine (Windows 7)

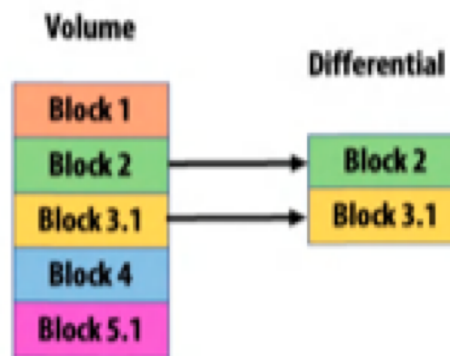
Entre 7h et minuit sur des OS de type serveur

A la demande

Principe des copies différentielles par bloc



Snapshot 1 : les blocs 3 et 5 sont modifiés les autres intacts



Snapshot 2 : les blocs 3.1 et 2 sont modifiés les autres intacts



Les valeurs de registre importantes

SYSTEM\ControlSet00x\Services\VSS

VssAccessControl : liste les utilisateurs ayant accès aux volumes des shadow copies

SYSTEM\ControlSet00x\Services\VolSnap

Éditeur du Registre

Fichier Edition Affichage Favoris ?

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\volsnap\Enum

	Nom	Type	Données
> vhdmp			
> vhf			
> Vid			
> vmibus			
> VMBusHID			
> vmgid			
> vmicguestinterface			
> vmicheartbeat			
> vmickvpexchange			
> vmicrdv			
> vmicshuttdown			
> vmictimesync			
> vmicvmsession			
> vmicvss			
> vncserver			
> volmgr			
> volmgrx			
> volsnap			
Enum			
	(par défaut)	REG_SZ	(valeur non définie)
	0	REG_SZ	STORAGE\Volume\{80e8a331-23cf-11ea-b91d-806e6f6e6963}#000000000100000
	1	REG_SZ	STORAGE\Volume\{80e8a331-23cf-11ea-b91d-806e6f6e6963}#000000000650000
	2	REG_SZ	STORAGE\Volume\{63117c04-228b-11ea-b919-806e6f6e6963}#000000000100000
	3	REG_SZ	STORAGE\Volume\{80e8a332-23cf-11ea-b91d-806e6f6e6963}#000000000100000
	4	REG_SZ	STORAGE\Volume\{80e8a332-23cf-11ea-b91d-806e6f6e6963}#000000002120000
	5	REG_SZ	STORAGE\Volume\{80e8a332-23cf-11ea-b91d-806e6f6e6963}#000000002750000
	6	REG_SZ	STORAGE\Volume\{80e8a332-23cf-11ea-b91d-806e6f6e6963}#000000002850000
	7	REG_SZ	STORAGE\Volume\{63117c06-228b-11ea-b919-806e6f6e6963}#000000000100000
	8	REG_SZ	STORAGE\Volume\??_USBSTOR#Disk&Ven_USB&Prod_Flash_Disk&Rev_1100#FBX1010201401434&0#{53f56307-b6bf-11d0-94f2-00a0c9...
	9	REG_SZ	STORAGE\Volume\??_USBSTOR#Disk&Ven_SanDisk&Prod_Extreme&Rev_1.00#4C530001261123111000&0#{53f56307-b6bf-11d0-94f2-0...
	Count	REG_DWORD	0x0000000a (10)
	NextInstance	REG_DWORD	0x0000000a (10)

Les valeurs de registre importantes

SYSTEM\ControlSet00x\Control\BackupRestore

FilesNotToBackup

FilesNotToSnapshot

KeysNotToRestore

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore

Quelques clés peuvent (ou pas être présentes)

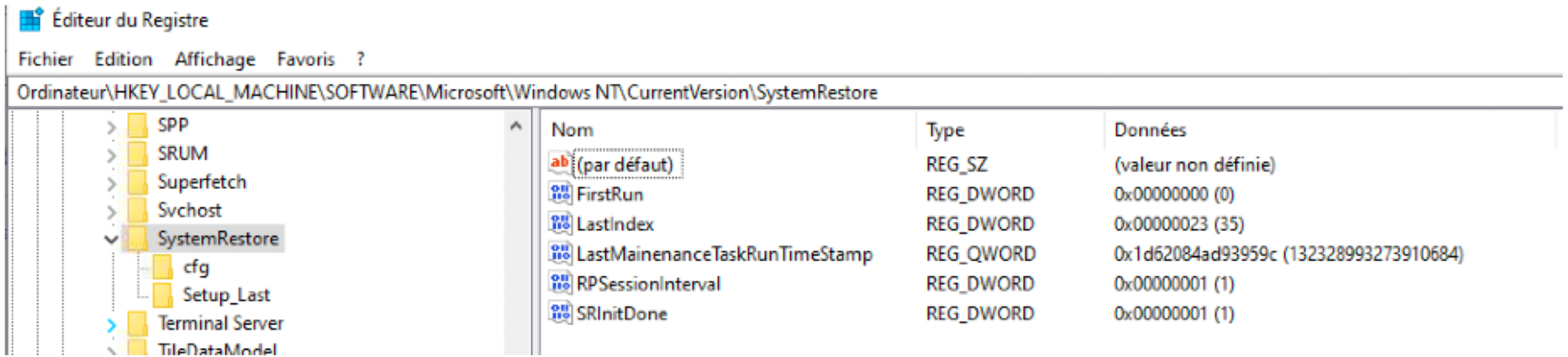
DisableSR (à 1 : les points de restauration sont désactivés)

DiskPercent: (% max de l'espace disque utilisé par System Restore sur un disque)

RPGlovalInterval (Fréquence en secondes entre 2 points de restauration)

RPLifeInterval (Durée de vie en secondes pendant lequel le système va conserver le point de restauration)

Les valeurs de registre importantes



Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
FirstRun	REG_DWORD	0x00000000 (0)
LastIndex	REG_DWORD	0x00000023 (35)
LastMaintenanceTaskRunTimeStamp	REG_QWORD	0x1d62084ad93959c (132328993273910684)
RPSessionInterval	REG_DWORD	0x00000001 (1)
SRInitDone	REG_DWORD	0x00000001 (1)

Quelques lignes de commande

vssadmin list shadowstorage /on=c:

```
C:\Windows\system32>vssadmin list shadowstorage /on=c:
vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume
(C) Copyright 2001-2013 Microsoft Corp.

Association de stockage de cliché instantané
  Pour le volume : (C:)\?\Volume{fb0cc499-128e-4ecf-bc6a-1baff4855838}\
  Volume de stockage de cliché instantané : (C:)\?\Volume{fb0cc499-128e-4ecf-bc6a-1baff4855838}\
  Espace du volume de stockage de cliché instantané utilisé : 4,52 Go (0%).
  Espace du volume de cliché instantané alloué : 4,82 Go (0%).
  Espace maximal du volume de cliché instantané : 93,1 Go (10%)

C:\Windows\system32>
```

Quelques lignes de commande

vssadmin list shadows: **AFFICHAGE en HEURE LOCALE**

Vssadmin list shadows /for=c: pour un volume spécifique

```
C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume
(C) Copyright 2001-2013 Microsoft Corp.

Contenu du jeu de clichés instantanés n° : {d5172e15-3722-459c-8392-b48dbcca74b1}
  Contenait 1 clichés instantanés à la date de création : 16/04/2020 17:05
    ID du cliché instantané : {06afc893-3181-4f36-92fd-6c121d6ddcbb}
    Volume original : (C:)\?\Volume{fb0cc499-128e-4ecf-bc6a-1baff4855838}\
    Volume de cliché instantané : \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
    Ordinateur d'origine : JPN0AT-DELLWK
    Ordinateur de service : JPN0AT-DELLWK
    Fournisseur : 'Microsoft Software Shadow Copy provider 1.0'
    Type : ClientAccessibleWriters
    Attributs : Persistent, Accessible par client, Pas de libération automatique, Différentielle, Récupération automatique

Contenu du jeu de clichés instantanés n° : {9c5d307b-3835-4d17-be3b-a550bbbb02fb}
  Contenait 1 clichés instantanés à la date de création : 26/04/2020 07:46
    ID du cliché instantané : {03a15433-c308-4d9f-8897-8a3c9a30f520}
    Volume original : (C:)\?\Volume{fb0cc499-128e-4ecf-bc6a-1baff4855838}\
    Volume de cliché instantané : \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
    Ordinateur d'origine : JPN0AT-DELLWK
    Ordinateur de service : JPN0AT-DELLWK
    Fournisseur : 'Microsoft Software Shadow Copy provider 1.0'
    Type : ClientAccessibleWriters
    Attributs : Persistent, Accessible par client, Pas de libération automatique, Différentielle, Récupération automatique
```

Les sauvegardes / restauration

S'appuient sur les shadow copies

Stockées dans des fichiers zip multiples classés dans des répertoires par date et heure de création

<Nom ordinateur> Backup Set <Date Backup Created> \ avec un fichier GlobalCatalog.wbcat dans le répertoire Catalogs contenant les fichiers sauvegardés avec la date et heure.

Utilité d'un point de vue forensic

- Versions précédentes de base de registre (**NTUSER**)
- Analyse de malware (date installation malware)
- Des données telles que typedURLs sont effacées
- Prouver un changement d'heure / date
- Vol de documents / utilisateur effacé

Exploitation des shadows par nos outils préférés

X-Ways ne gère que partiellement les shadows par défaut

Exemple concret : complexité à reconstituer plusieurs fichiers de registre / documents sur un Windows 7 avec shadow activé.

-> documentation utilisateur + RVS

-> Axiom : reprocesser le cas mais tous les artifacts sont testés.

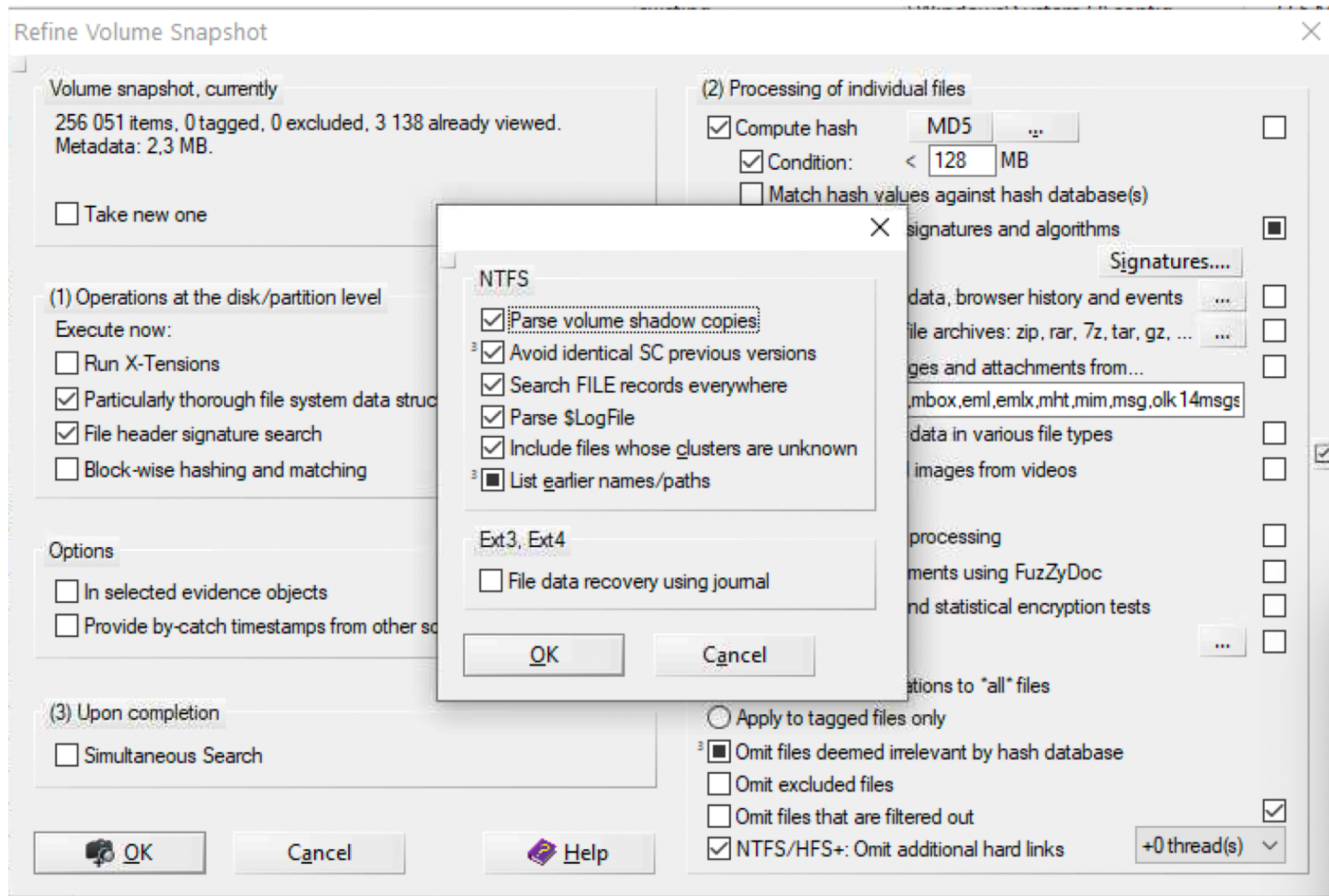
Exploitation des shadows par nos outils préférés

NTFS: Volume shadow copies can be parsed optionally, with a forensic license. Existing and previously existing volume shadow copy host files are checked for valuable information that would not be available otherwise, such as files that cannot be found in the current \$MFT any more or previous versions of files whose contents have changed. Those files will be reconstructed up to 1 GB in length according to the shadow copy. Processing of volume shadow copies, if any, occurs before all the other operations that are part of the particularly thorough file system data structure search (parsing \$LogFile, optionally searching for FILE record outside of \$MFT and outside of VSC, searching for index records in the slack of INDX buffers). If there are volume shadow copies, the caption of the small progress indicator window will tell you when they are being parsed. Volume shadow copy host files that you exclude before processing will be omitted.

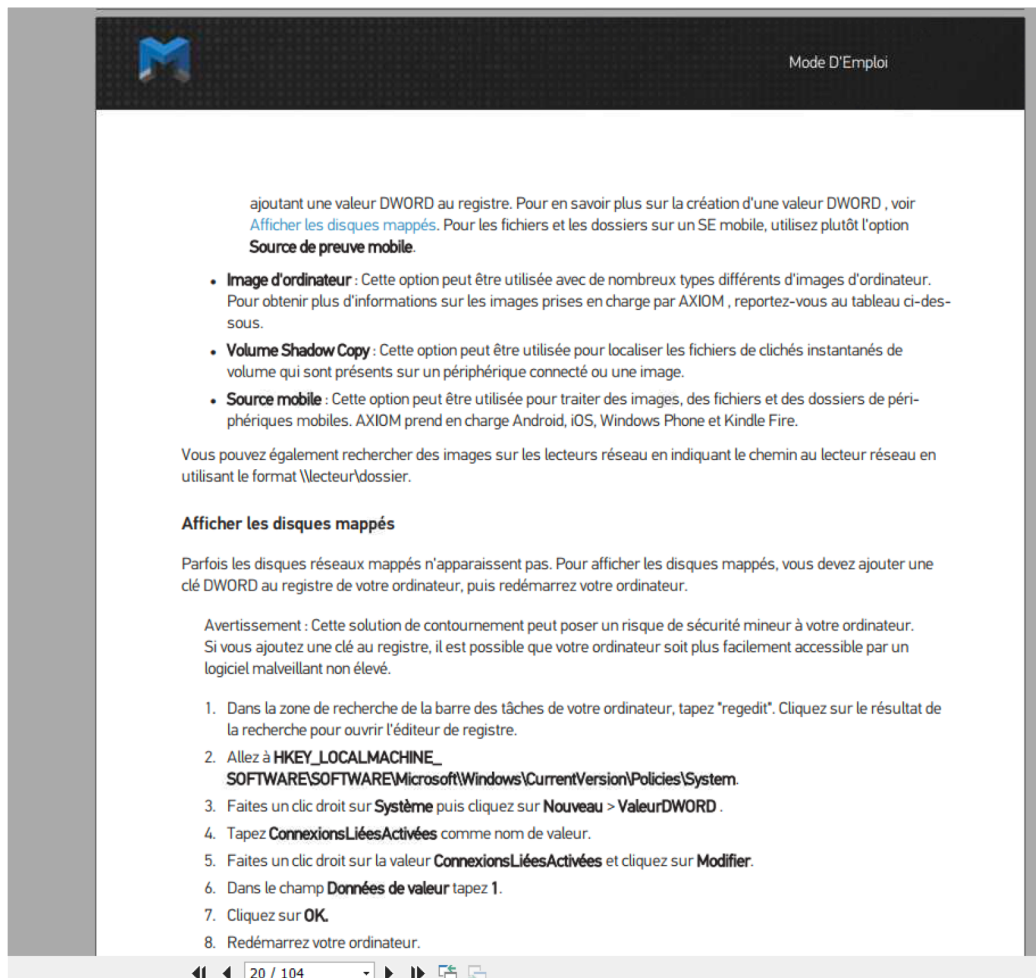
Files found in volume shadow copies are specially marked with "SC #" in the Attr. column, or "SC #, prev. version" if they are previous versions of files that were known to the volume snapshot already before the thorough file system data structure search, so that it is easy to filter them in or out. # stands for the sequential number of the snapshot in which these files were found. Remember you can sort by ID to see the files they are a previous version of next to them. You can also easily navigate to the VSC host by using the command Navigation | Find related file in the directory browser context menu, for example so that in Details mode learn more about that particular snapshot. You could then invoke the same command once more to navigate to the corresponding snapshot properties file, where in Details mode you learn even more, e.g. description and official creation date.

Optionally avoid that previous versions of files in volume shadow copies are added to the volume snapshot if they are exact duplicates (identical file contents) so that it is much easier to focus on files for which actually previous data is still available. Even if modification dates are different, the file contents are often the same for files installed by the operation system. If fully selected, X-Ways Forensics will compare files up to 128 MB, if half selected, only up to 16 MB, as to not waste too much time on this feature.

Exploitation des shadows par nos outils préférés



Exploitation des shadows par nos outils préférés



ajoutant une valeur DWORD au registre. Pour en savoir plus sur la création d'une valeur DWORD , voir [Afficher les disques mappés](#). Pour les fichiers et les dossiers sur un SE mobile, utilisez plutôt l'option **Source de preuve mobile**.

- **Image d'ordinateur** : Cette option peut être utilisée avec de nombreux types différents d'images d'ordinateur. Pour obtenir plus d'informations sur les images prises en charge par AXIOM , reportez-vous au tableau ci-dessous.
- **Volume Shadow Copy** : Cette option peut être utilisée pour localiser les fichiers de clichés instantanés de volume qui sont présents sur un périphérique connecté ou une image.
- **Source mobile** : Cette option peut être utilisée pour traiter des images, des fichiers et des dossiers de périphériques mobiles. AXIOM prend en charge Android, iOS, Windows Phone et Kindle Fire.

Vous pouvez également rechercher des images sur les lecteurs réseau en indiquant le chemin au lecteur réseau en utilisant le format \\lecteur\dossier.

Afficher les disques mappés

Parfois les disques réseaux mappés n'apparaissent pas. Pour afficher les disques mappés, vous devez ajouter une clé DWORD au registre de votre ordinateur, puis redémarrez votre ordinateur.

Avertissement : Cette solution de contournement peut poser un risque de sécurité mineur à votre ordinateur. Si vous ajoutez une clé au registre, il est possible que votre ordinateur soit plus facilement accessible par un logiciel malveillant non élevé.

1. Dans la zone de recherche de la barre des tâches de votre ordinateur, tapez "regedit". Cliquez sur le résultat de la recherche pour ouvrir l'éditeur de registre.
2. Allez à **HKEY_LOCAL_MACHINE\SOFTWARE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.
3. Faites un clic droit sur **Système** puis cliquez sur **Nouveau > ValeurDWORD** .
4. Tapez **ConnexionsLiéesActivées** comme nom de valeur.
5. Faites un clic droit sur la valeur **ConnexionsLiéesActivées** et cliquez sur **Modifier**.
6. Dans le champ **Données de valeur** tapez **1**.
7. Cliquez sur **OK**.
8. Redémarrez votre ordinateur.

Exploitation des shadows par nos outils préférés

WINDOWS SÉLECTIONNER SOURCE DE PREUVES



DISQUE



IMAGE



FICHIERS ET DOSSIERS



COPIE REPÈRE DE
VOLUME

WINDOWS AJOUTER UNE COPIE REPÈRE DE VOLUME TOUT SUPPRIMER

^ ☒ lenovo.E01

Partition 1 (Microsoft NTFS, 1,46 GB) SYSTEM_DRV

^ ☒ Partition 2 (Microsoft NTFS, 448,35 GB) Windows7_OS

- ✓ ☒ Shadow Copy Creation Time: 2017-10-11 07:34:00 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {7e234ea8-9b13-44d3-b989-f094fab6c490}
- ✓ ☒ Shadow Copy Creation Time: 2017-10-19 09:07:23 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {5c70a2f5-0d73-4ed0-9c51-bc17743f323e}
- ✓ ☒ Shadow Copy Creation Time: 2017-10-27 10:24:11 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {b91528c1-5b0b-4251-970f-d0a16cd22469}
- ✓ ☒ Shadow Copy Creation Time: 2017-11-06 09:40:33 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {2aff14a5-1ca5-4607-80f3-b37ccd3a693c}
- ✓ ☒ Shadow Copy Creation Time: 2017-11-14 09:15:26 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {e1c231e6-18e7-40d4-9e0b-3721ffb41a10}
- ✓ ☒ Shadow Copy Creation Time: 2017-11-22 08:19:01 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {60584bed-5931-4940-b55c-e4a72e5301d9}
- ✓ ☒ Shadow Copy Creation Time: 2017-11-29 09:52:39 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {f52df4ff-537a-46ab-872e-62424096533e}
- ✓ ☒ Shadow Copy Creation Time: 2017-12-07 09:49:13 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {cc8bc503-031d-49a6-bb54-7e4620ccad0b}
- ✓ ☒ Shadow Copy Creation Time: 2017-12-14 10:05:52 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {e4fdbfb8-f50a-43d1-873e-b53aa65f5019}
- ✓ ☒ Shadow Copy Creation Time: 2018-01-03 08:38:27 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {9d81ad91-6204-4d37-a2b4-cbc7ca23552c}
- ✓ ☒ Shadow Copy Creation Time: 2018-01-11 09:46:48 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {c73acc07-6c82-46b5-a7aa-c3d8b8c28de6}
- ✓ ☒ Shadow Copy Creation Time: 2018-01-18 12:05:07 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {70f1b15a-c7a2-4e09-b0c6-ab7cc9845408}
- ✓ ☒ Shadow Copy Creation Time: 2018-01-29 09:16:46 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {69161713-f016-4932-9c9a-518a80009c59}
- ✓ ☒ Shadow Copy Creation Time: 2018-02-05 13:06:36 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {bb5df431-e6cc-422b-be74-30dbec739b0c}
- ✓ ☒ Shadow Copy Creation Time: 2018-02-13 08:25:00 UTC (yyyy-mm-dd), Machine: commander-PC, ID: {002a39db-a8fd-4d9e-afd6-93a5a79b1119}

Partition 3 (Microsoft NTFS, 15,95 GB) Lenovo_Recovery

Retour d'expérience sur 4 approches différentes

X--Ways gère le shadows une fois les bonnes options trouvées dans le RVS. Pas d'indexation simple par contre et perte d'info si recherche mots clés.

Axiom gère le shadow intégralement une fois les options trouvées dans Axiom Process. Les recherches par index restent toutefois limitées aux possibilités d'Axiom. Par contre tous les artifacts d'Axiom peuvent être utilisés.

Forensic Explorer : propose de monter des volumes avec fichiers différents, attention le montage n'est pas complet et il y a des pertes d'information.

Blacklight : Permet de retrouver les données sous forme d'evidence avec les traitements associés. Les traitements sont plus longs mais par contre beaucoup plus complets (indexation, historiques, mails....) et l'exploitation est faite complètement.

Références

Définition du shadow copy: https://en.wikipedia.org/wiki/Shadow_Copy

Harlan Carvey : Windows Forensic Analysis Toolkit (version 4)

Nihad Ahmad Hassan : Data Hiding Techniques in Windows OS

Cours Windows Forensic Investigation : Blacklight

La semaine prochaine...

Extraction avancée, découverte de la nouvelle interface de Physical Analyzer et analyse de malware sur téléphone portable

Heather Mahalik se joindra à nous. (Formatrice SANS / Senior Director of Digital Intelligence chez Cellebrite (Attention rendez-vous décalé à 16h)

Prenez soin de vous et de ceux que vous aimez



La parole est à vous !