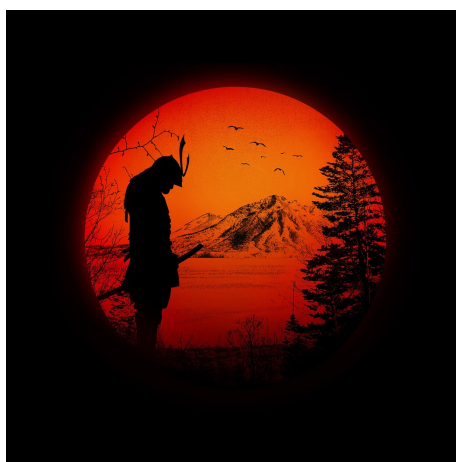


Se protéger !



Version Stagiaire

Version 1.0

Eric BERTHOMIER
eric.berthomier@free.fr

24 mai 2020

Table des matières

1	Préambule	3
1.1	Consignes	3
1.2	Avertissement	3
1.3	Roue de secours	3
1.4	Historique	3
2	Vol et perte	4
2.1	Câble anti-vol	4
2.2	Chiffrement	4
2.2.1	Bitlocker	4
2.2.2	TrueCrypt	4
3	Sauvegarde	10
3.1	FreeFileSync	10
3.1.1	Synchronisation manuelle	10
3.1.2	Synchronisation automatisée	11
3.2	CloneZilla	11
4	Protection du système d'exploitation	12
4.1	Antivirus	12
4.1.1	Testons	12
4.2	Connexions réseaux	12
5	Protection / destruction du matériel	14
5.1	Onduleur	14
5.2	Récupération de données	14
6	Protection de mes informations	17
6.1	Protection des mots de passe	17
6.1.1	Création de la base et premier élément	17
6.1.2	Utilisation de KeyPass	19
6.2	Protection des fichiers	20
6.2.1	Usage basique	20
6.2.2	Un partage de documents privés	22
7	Conclusion	25

CHAPITRE 1

Préambule

1.1 Consignes

Afin de se réserver un périmètre de manipulation, merci de créer un répertoire SSI dans Documents.

1.2 Avertissement

Tous les outils présentés dans ce document sont "normalement" sans danger pour votre ordinateur. Le danger c'est **VOUS** ...si **VOUS** ne suivez pas les instructions ...

1.3 Roue de secours

Il peut arriver que la situation nous échappe, aussi avant d'arriver à l'irréparable, il vous est possible de télécharger le logiciel [TeamViewer QuickSupport](#) pour que l'instructeur puisse prendre la main rapidement sur votre poste.

1.4 Historique

04 Mai 2020 Version initiale



Vol et perte

2.1 Câble anti-vol

1. Rechercher les caractéristiques des câbles anti-vol.
2. Quelle est l'erreur courante réalisée par les usagers ?
3. Quelle précaution dois-je prendre dans l'usage d'un anti-vol ?

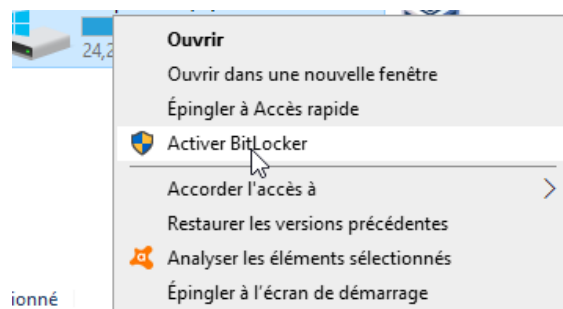
2.2 Chiffrement

- Qu'entraîne la mise en place du chiffrement de votre disque dur pour votre ordinateur ?

2.2.1 Bitlocker

- Quelle est la version de Windows nécessaire pour avoir cette fonctionnalité ?

Si Bitlocker est actif, il vous est possible de le lancer en réalisant un clic droit sur le disque dur puis "Activer Bitlocker". Ceci entraînera le début de la procédure de chiffrement du disque.



Il est conseillé de s'entraîner avec le chiffage d'une clé USB avant celui de son disque dur.

2.2.2 TrueCrypt

Création d'un espace sécurisé

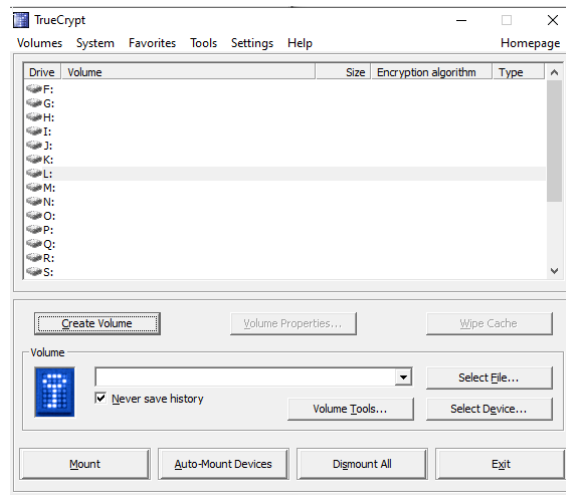
TrueCrypt permet comme Bitlocker de chiffrer disque dur / clé USB ou tout autre périphérique de stockage. A l'inverse de Bitlocker c'est un produit Open Source.

Un disque dur une clé USB ou tout périphérique de stockage se définit comme un ensemble d'octets agencées d'une façon que le système peut comprendre.

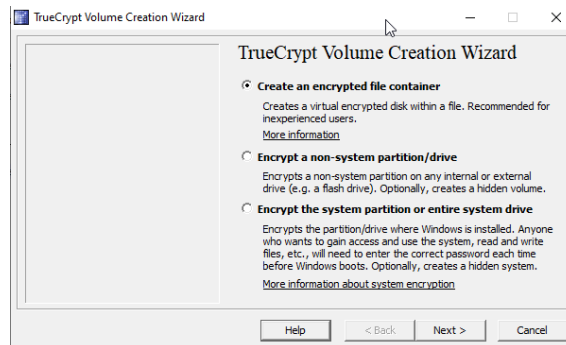
En résumé, un disque dur est construit comme un livre, une table des matières, une liste de chapitres.

Afin de montrer le fonctionnement de TrueCrypt sans pour autant faire des manipulations qui pourraient se révéler hasardeuse sur l'ordinateur, nous allons construire un espace de stockage chiffré sur notre disque dur.

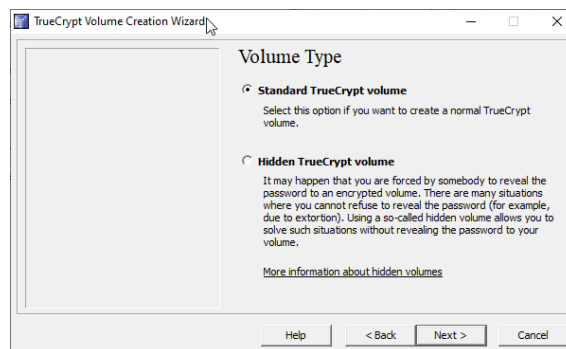
1. Télécharger TrueCrypt, installer le par défaut et lancer le.



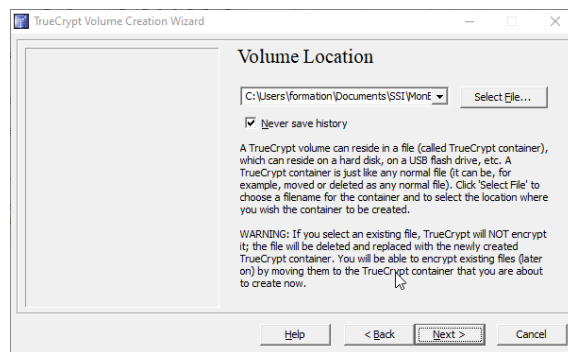
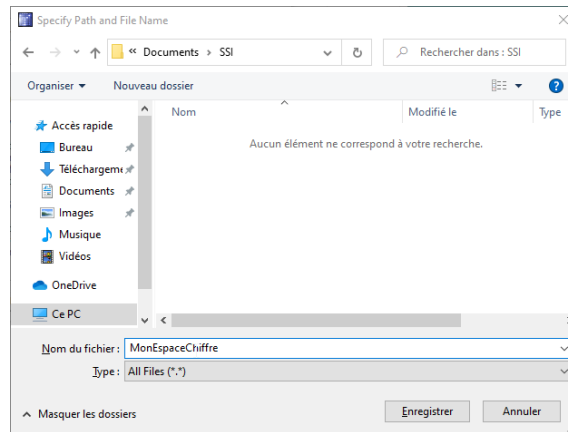
2. Cliquer sur Create Volume
3. Cliquer sur Create an encrypted file container puis Next



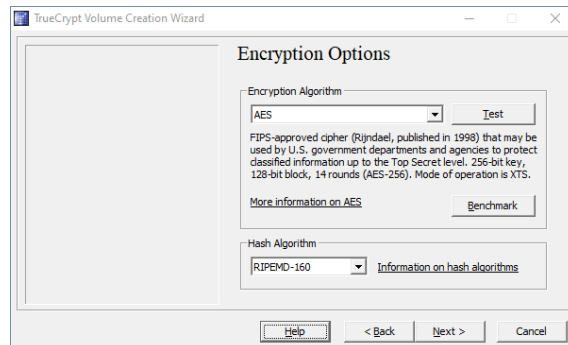
4. Sélectionner Standard TrueCrypt volume puis Next



5. Dans VolumeLocation, indiquer le répertoire Documents\SSI et un nom de fichier : ...

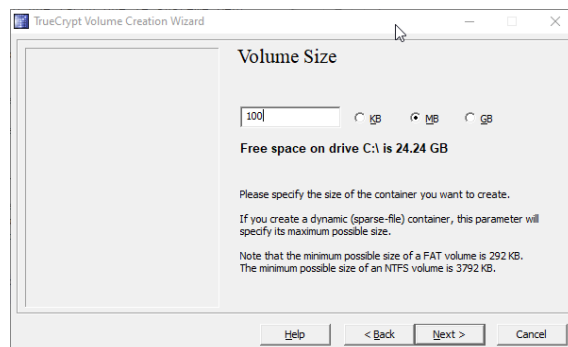


6. Puis Next

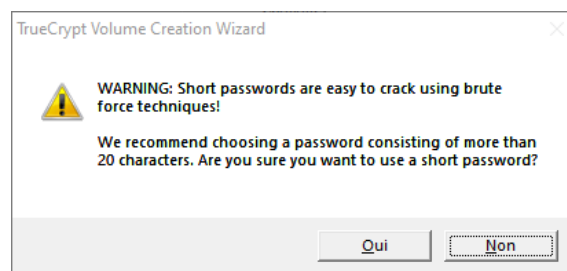
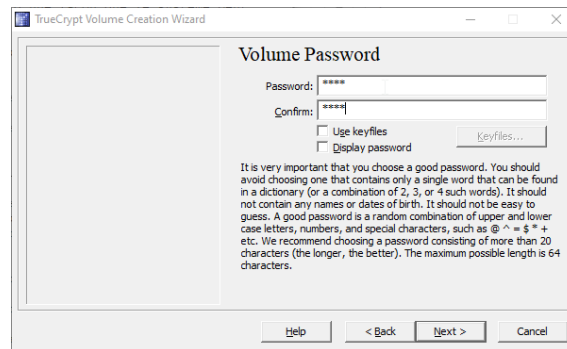


7. Après avoir jeter un œil à l'ensemble des chiffrements possible, cliquer sur Next

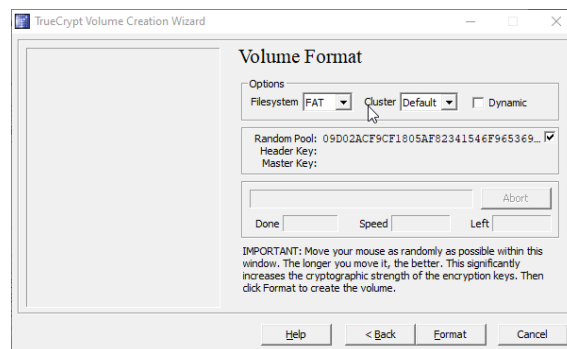
8. Comme indiqué précédemment TrueCrypt va créer un volume, une sorte de disque sur votre disque dur. Il lui est donc nécessaire d'avoir la taille de ce dernier. Pour la démonstration nous allons mettre 100 MB (100 mégaoctets).



9. Saisir un mot de passe basique pour la démonstration. TrueCrypt vous avertit qu'il ne peut pas gérer des mots de passe de plus de 64 caractères ! Comme tout bon informaticien mon mot de passe sera : "toto"



10. Ah oui je me fais engueuler, la norme est de 20 caractères minimum.

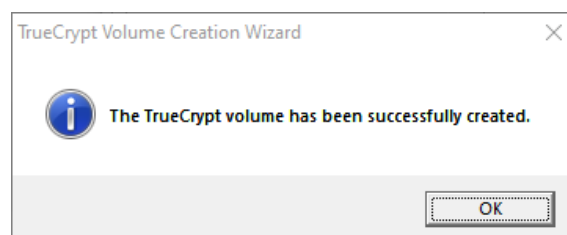


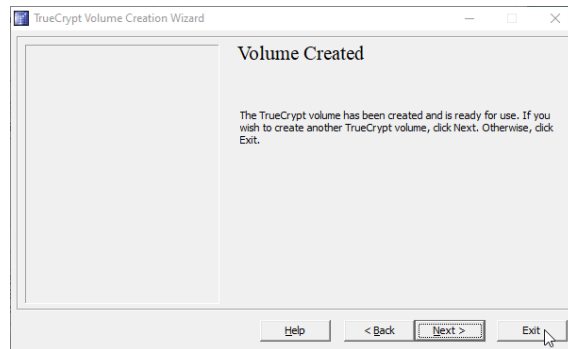
Remarquez la proposition de type de partition.

Exercice

🐭 Pourquoi dois je bouger ma souris ? Comment est créé le hasard en informatique ?

11. Cliquer sur Format





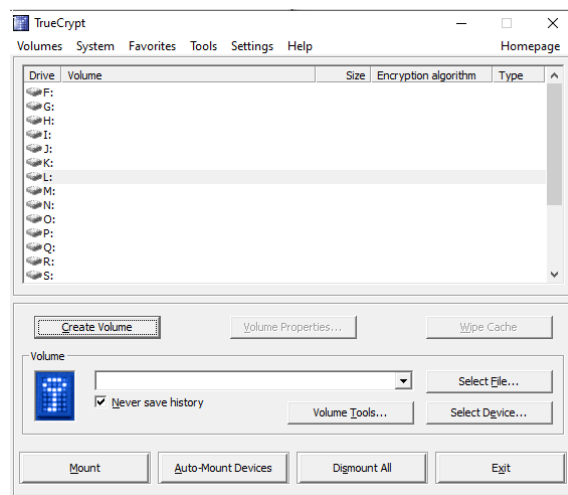
12. Cliquer sur Exit

Exercice

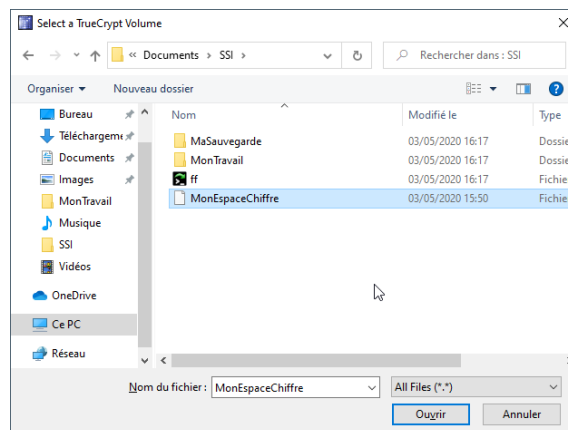
👤 Qu'avons nous créé ? Vérifier le contenu du répertoire Documents\SSI

Utilisation d'un espace sécurisé

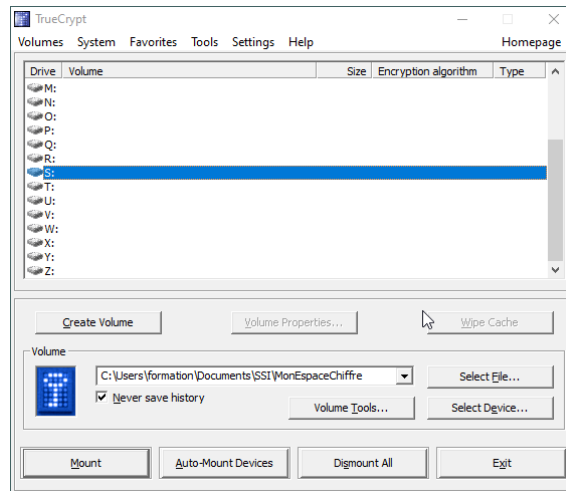
1. Ouvrir TrueCrypt



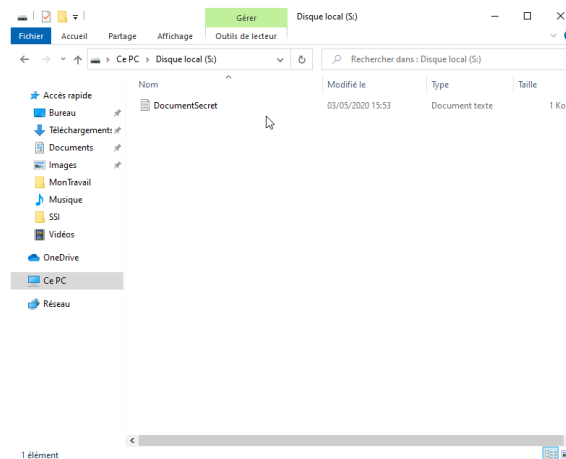
2. Sélectionner une lettre de lecteur (comme une clé USB) S: (comme Secret)
3. À l'aide du bouton Select File..., sélectionner notre espace chiffré



4. Cliquer sur mount



5. Indiquer votre mot de passe
6. Sortir par Exit
7. Ouvrir l'explorateur de fichier et constater la présence d'un lecteur S :



A l'aide d'un éditeur de texte, créer un fichier contenant un message ultra-secret :

Par exemple :



Mon document Ultra-Secret

et enregistrez le sur S :

1. Ouvrir TrueCrypt, cliquer sur DismountAll.
2. Votre fichier est maintenant protégé dans un espace chiffré.

Exercice



Réitérer les opérations pour retrouver votre fichier.

Sauvegarde

3.1 FreeFileSync

Ce logiciel va vous permettre de sauvegarder sur un disque externe vos données et ceci de manière très rapide.

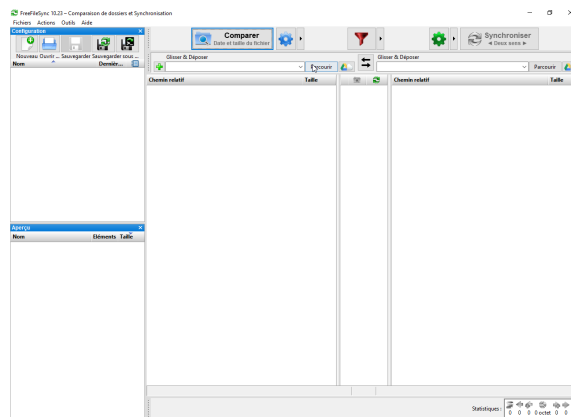
À des fins de démonstration nous allons utiliser 2 répertoires à créer dans Documents\SSI.

- MonTravail
- MaSauvegarde

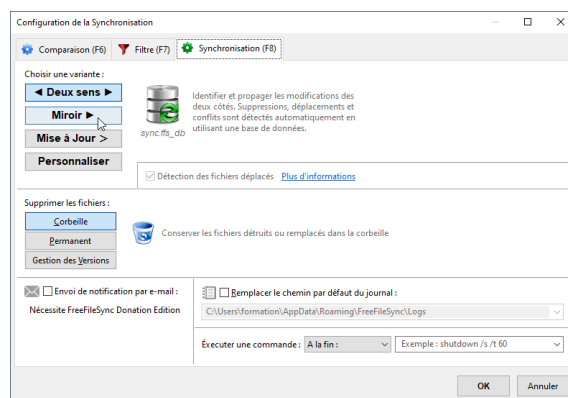
Peupler votre répertoire MonTravail de ce que vous désirez mais avec au moins un document (on pourra reprendre notre document ultra-secret de l'exercice précédent).

3.1.1 Synchronisation manuelle

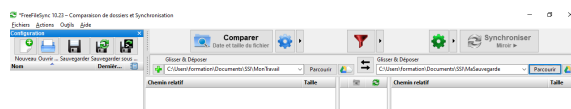
1. Télécharger, installer puis ouvrir FreeFileSync



2. À l'aide du bouton Parcourir de la fenêtre de Gauche, sélectionner le répertoire MonTravail
3. À l'aide du bouton Parcourir de la fenêtre de Droite sélectionner le répertoire MaSauvegarde
4. À l'aide de la roue crantée sélectionner Miroir



5. À l'aide du bouton Synchroniser, lancer la copie



6. Vérifier la bonne exécution de la sauvegarde

7. Supprimer un fichier de la sauvegarde
8. Relancer l'opération
9. Tester

Note



N'hésiter pas à appuyer sur le bouton "Comparer" car nous ne sommes pas dans un cas "standard"

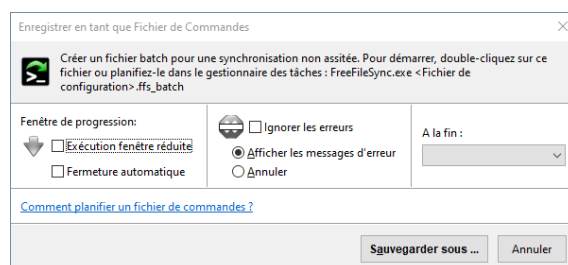
Exercice



Modifier le document et répéter l'opération

3.1.2 Synchronisation automatisée

1. Cliquer sur le bouton Enregistrer en tant que fichier de commandes et sauvegarder le fichier ainsi crée dans Documents\SSI



2. Exécuter le fichier de commande en double-cliquant sur ce dernier.

Exercice



Pour qu'une sauvegarde soit valable qu'est il nécessaire de faire de manière régulière ?

3.2 CloneZilla

CloneZilla vous permet de sauvegarder votre disque chiffré ou non sur un disque dur externe.

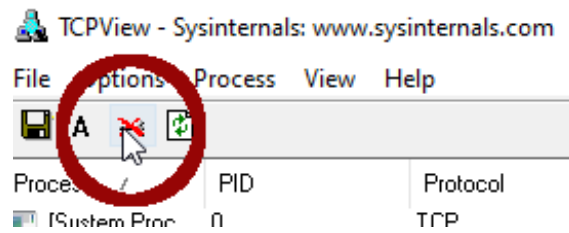
Il existe une signature de test nommée EICAR qui vous permet de voir si votre antivirus fonctionne toujours et ceci sans risque puisque cette chaîne de caractère est :

- Les fichiers eicarxxxx.zip sont des fichiers Eicar compressés de multiples fois.
- Les fichiers noteicarxxx.zip sont des fichiers qui ne sont pas Eicar compressés de multiples fois.

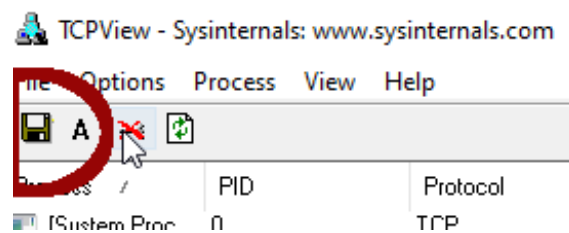
Pour se faire on utilise des connexions réseau ... Un petit coup d'œil, on garde la capture d'écran quelque part ou on sauvegarde à un instant t , puis à un autre moment, un autre coup d'œil pour voir si un intrus ne s'est pas glissé dans mon ordinateur.

Wireshark: System:Port:0												
#	System:Port:0	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Recv Packets	Recv Bytes	
1	System:Port:0	TCP	denying-icmp	43976	15.108.1.2	*	Time_wait	0	0	0	0	
2	System:Port:0	TCP	denying-icmp	43976	15.108.1.2	*	Time_wait	0	0	0	0	
3	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
4	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
5	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
6	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
7	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
8	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
9	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
10	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
11	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
12	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
13	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
14	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
15	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
16	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
17	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
18	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
19	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
20	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
21	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
22	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
23	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
24	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
25	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
26	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
27	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
28	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
29	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
30	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
31	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
32	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
33	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
34	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
35	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
36	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
37	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
38	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
39	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
40	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
41	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
42	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
43	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
44	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
45	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
46	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
47	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
48	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
49	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
50	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
51	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
52	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
53	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
54	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
55	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
56	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
57	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
58	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
59	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
60	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
61	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
62	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
63	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
64	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
65	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
66	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
67	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
68	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
69	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
70	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
71	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
72	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
73	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
74	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
75	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
76	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
77	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
78	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
79	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
80	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
81	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
82	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
83	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
84	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
85	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
86	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
87	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
88	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
89	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
90	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
91	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
92	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
93	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
94	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
95	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
96	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
97	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
98	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
99	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
100	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
101	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
102	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
103	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
104	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
105	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
106	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
107	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
108	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
109	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
110	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
111	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
112	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
113	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
114	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
115	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
116	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
117	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
118	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
119	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
120	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
121	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
122	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
123	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
124	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
125	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
126	System:Port:0	TCP	denying-icmp	43976	40.123.20.2	*	Time_wait	0	0	0	0	
127	System:Port:0	TCP	denying-icmp</									

2. À l'aide du bouton indiqué ci-dessous, ne prendre en compte que les connexions établies.



3. Pour un usage futur ... sauvegarde l'état de vos connexions.



Exercice



Tentez d'identifier les différentes connexions établies ...

Protection / destruction du matériel

5.1 Onduleur

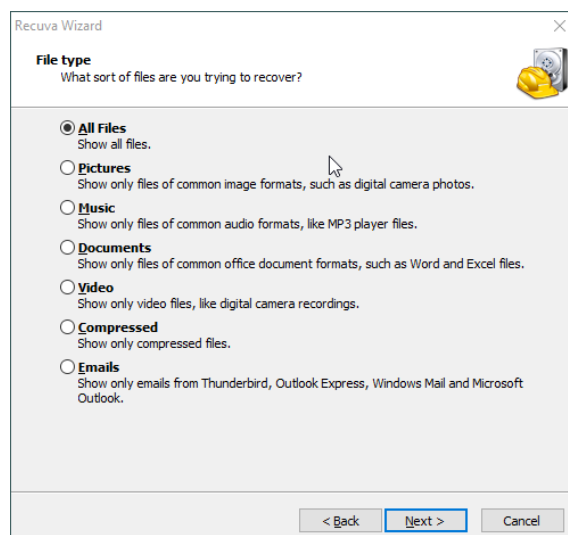
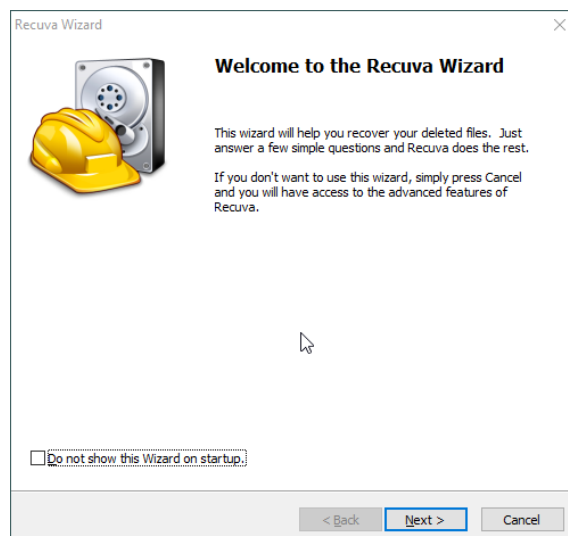
1. Rechercher les caractéristiques d'un onduleur.
2. Résumez ce qui fait le prix d'un onduleur.
3. Quels sont les éléments que l'onduleur peut protéger ?
4. Quelle est la différence avec un prise parafoudre ?

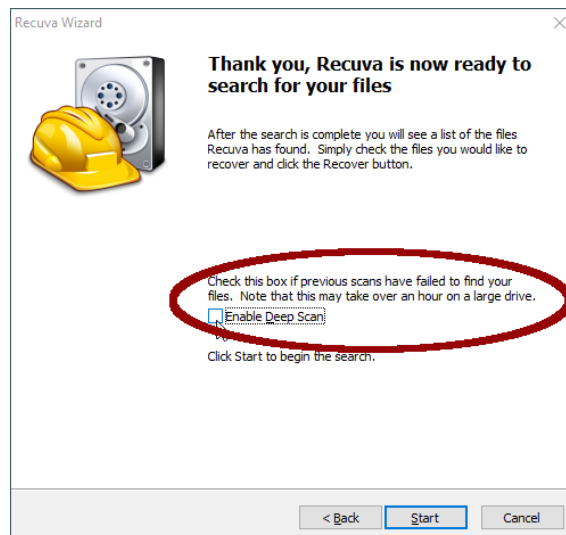
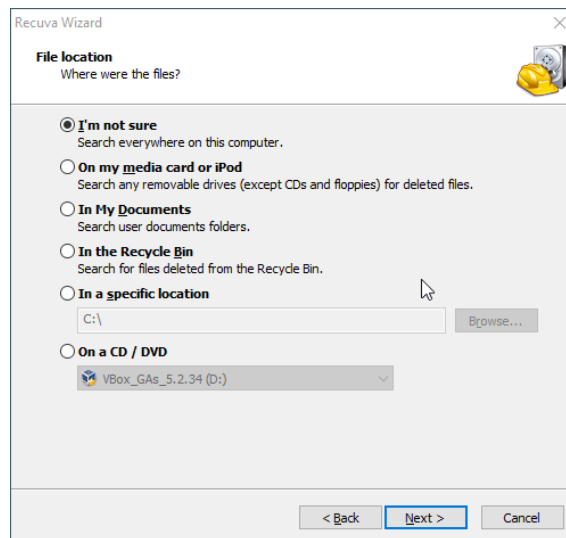
5.2 Récupération de données

Il est recommandé d'utiliser le logiciel DBAN sur les disques durs avant de transmettre un bien à l'extérieur.

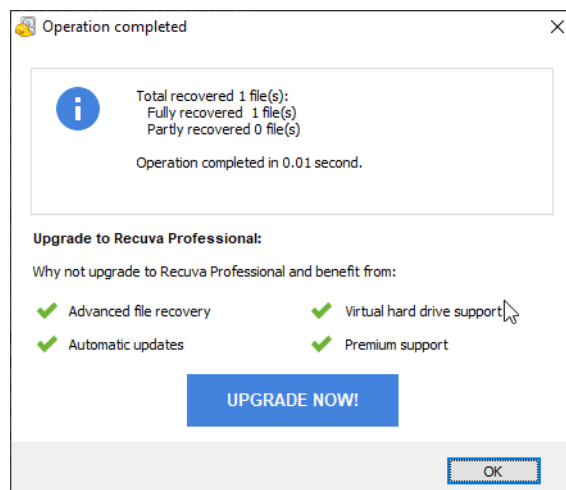
Nous allons en voir la raison ...

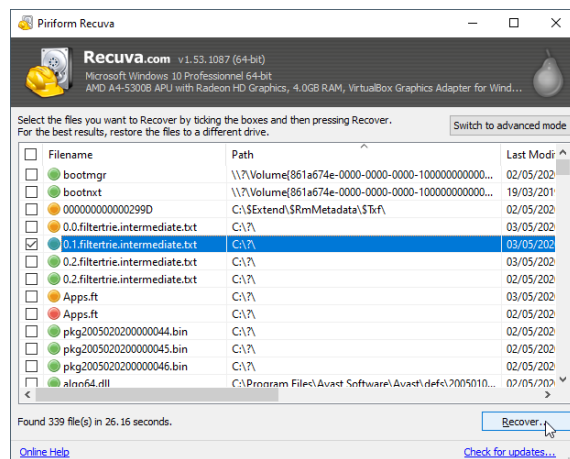
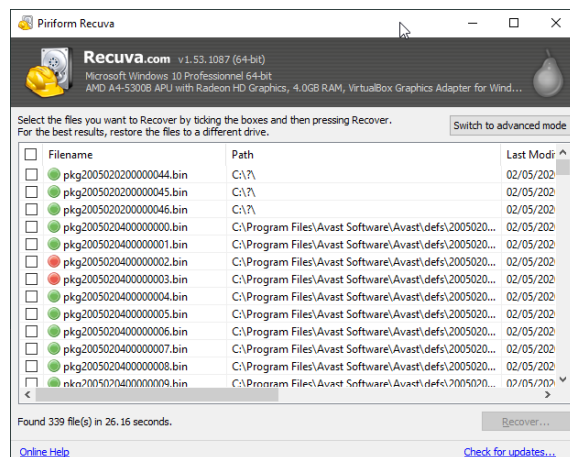
1. A défaut d'avoir un CD Linux qui nous permettrait de faire les choses avec moins d'adhérence, télécharger puis exécuter Recuva (de Microsoft)





2. On remarquera la possibilité de faire un "Deep Scan" ou un scan en profondeur qui va rechercher des fragments de résultats.
3. Observer les résultats et restaurer un fichier effacé.





Exercices



- Pourquoi la restauration d'un fichier a t'elle moins de chance d'aboutir en travaillant sur le même espace de stockage que le fichier que l'on désire restaurer ?
- PhotoRec et TestDisk sont deux utilitaires connus du monde libre Linux, mais quelle est la différence entre ces deux logiciels qui appartiennent à la même suite ?
- Rechercher la définition du Forensic et des logiciels qui lui sont associés

Protection de mes informations

6.1 Protection des mots de passe

KeyPass est un logiciel validé par l'ANSSI.

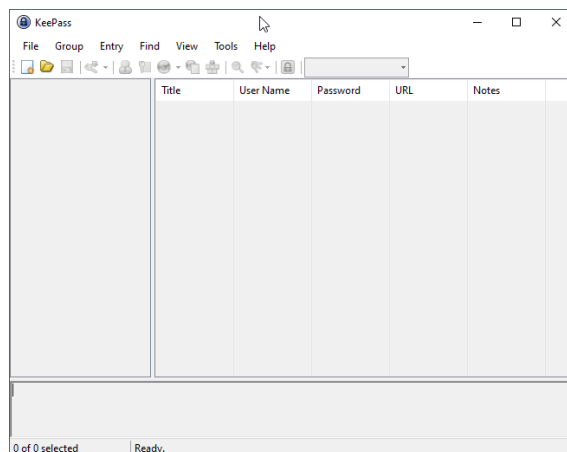
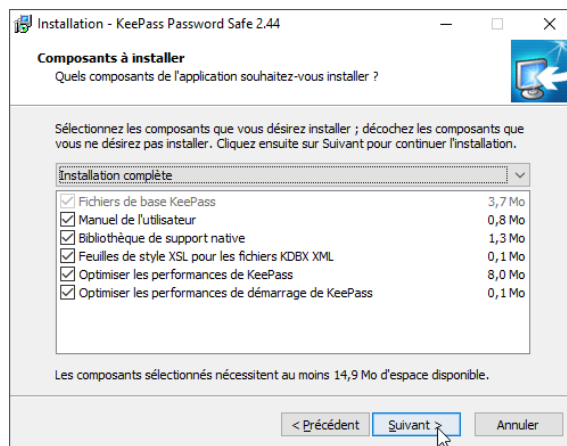
Exercice



En quoi consiste une validation par l'ANSSI ?

6.1.1 Création de la base et premier élément

Télécharger et installer KeePass v2



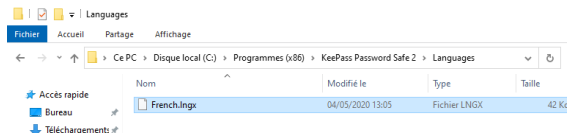
Exercice



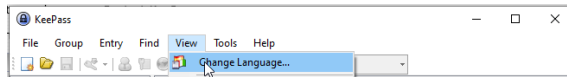
Que signifie Optimiser KeePass ?

Appliquons un petit coup de francisation bien méritée ...

- Télécharger la langue désirée
- Placer le fichier dans le répertoire lang de Keypass

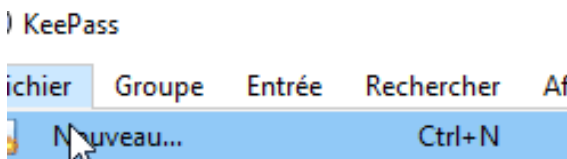


- Dans le menu View, changer le langage

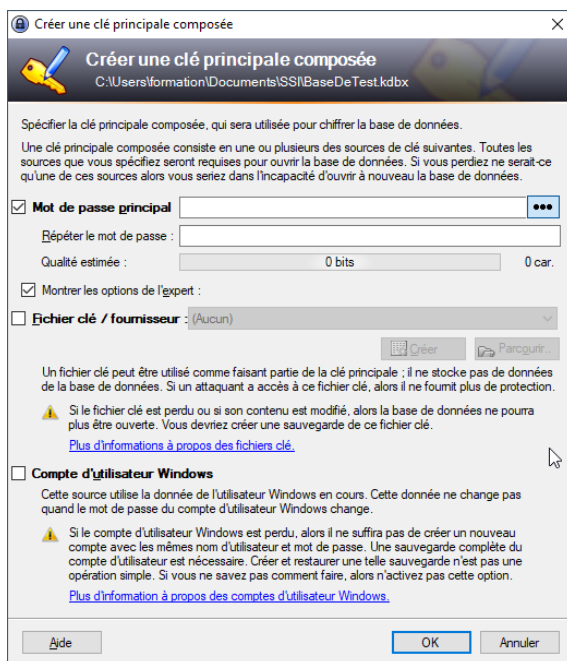


Keypass peut gérer un grand nombre de bases de données de mots de passe, ce qui permet de mutualiser des mots de passe sans ouvrir l'ensemble du portefeuille.
Nous allons donc créer une première base.

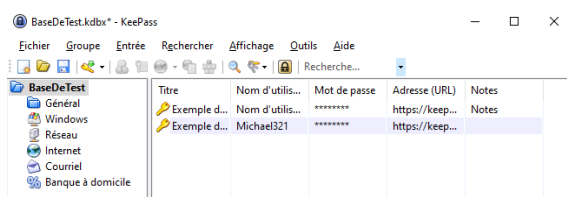
- Fichier – > Nouveau



- Nommer la base "BaseDeTest" et enregistrer là dans le répertoire Documents\SSI
- En cliquant sur Montrer les options de l'expert, consulter les différents moyens de protéger votre coffre-fort à mot de passe.



- Un mot de passe permettant de protéger la base vous est demandé. On parle ici de "passphrase" car ce mot de passe doit être très fort, en général 24 caractères minimum.
- Une fois la base créée une feuille de secours est proposée à l'impression. En effet perdre le mot de passe de votre base de données de mot de passe signifie perdre **TOUS SES MOTS DE PASSE**.



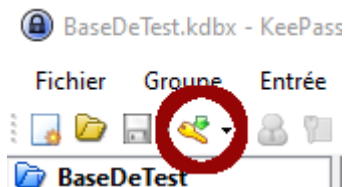
- Nous allons maintenant créer un exemple d'entrée dans KeyPass.
- Voici les éléments transmis pour accéder à une page Web :
URL : <http://cours.ericberthomier.fr/authentification/>

User : cours

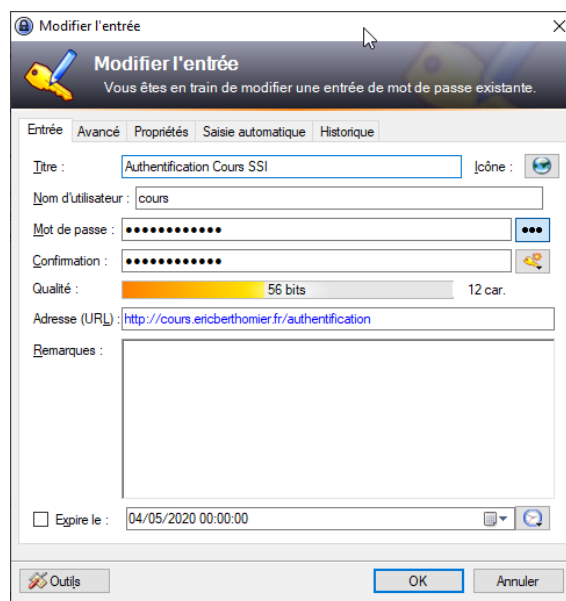
Password : coursSSI2020

— Nous allons indiquer ces renseignements dans notre base.

1. Je me positionne dans l'arborescence concernée
2. Je clique sur "Ajouter une entrée"



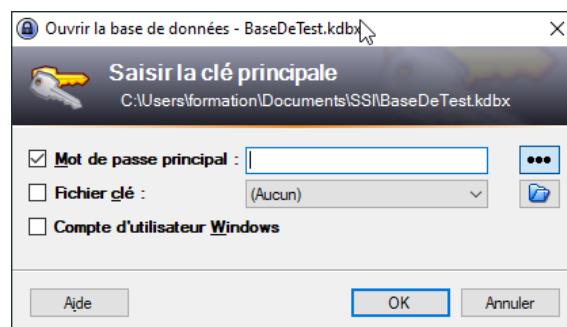
3. Je renseigne l'ensemble des champs nécessaires



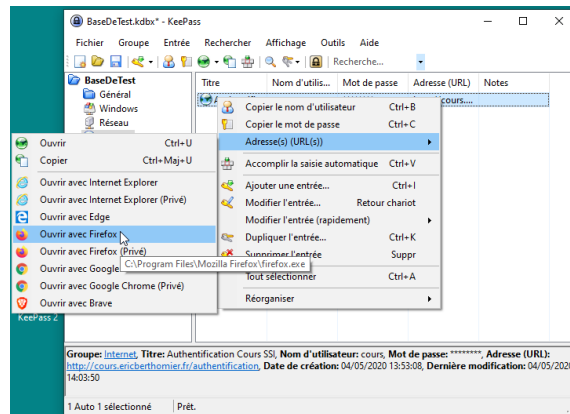
— Enregistrer et quitter KeyPass

6.1.2 Utilisation de KeyPass

1. Ouvrir KeyPass



2. Dans l'arborescence, sélectionner Internet puis faire un clic droit sur notre enregistrement pour ouvrir L'URL avec Firefox



3. Revenir sur KeyPass puis à l'aide du clic droit faire copier le nom de l'utilisateur. Colle ce dernier dans la zone de saisie de l'authentification.
4. Faire de même avec le mot de passe.
5. Valider l'authentification

Exercice

🔒 Fermer Firefox puis reconduire l'opération sauf pour le mot de passe où vous allez procéder ainsi :

1. Clic droit – > Copier le mot de passe
2. ⌚ Attendre 20 secondes
3. Coller le mot de passe, observer

Pour quelle raison KeyPass a-t-il mis en place cette "contrainte" ?

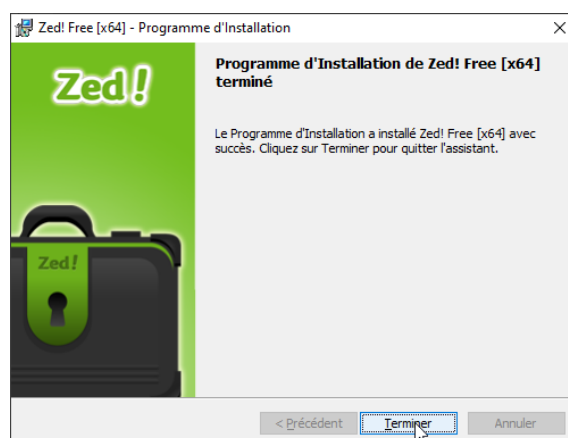
6.2 Protection des fichiers

6.2.1 Usage basique

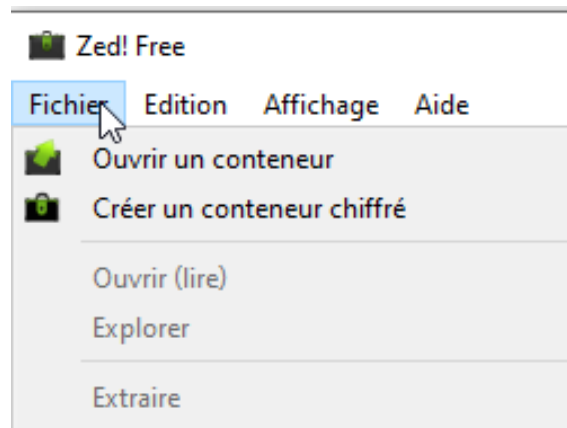
Zed! est un logiciel validé par l'ANSSI vous permettant de créer des containers sécurisés (un peu comme dans TrueCrypt) mais avec plus de facilité.

TrueCrypt est en effet prévu pour des volumes et non pour des fichiers.

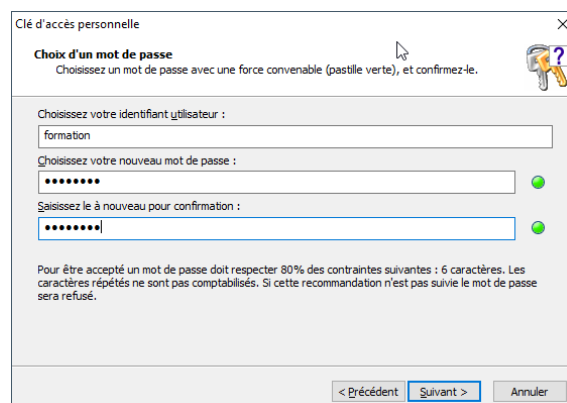
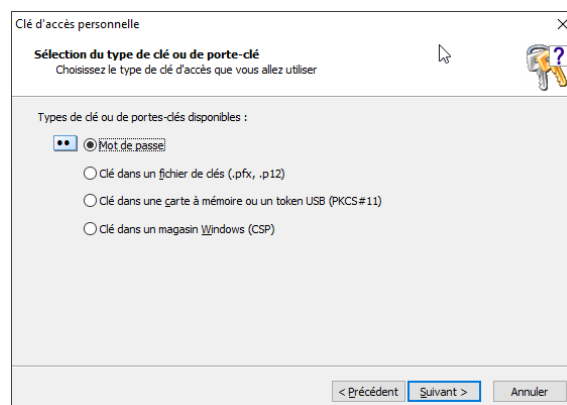
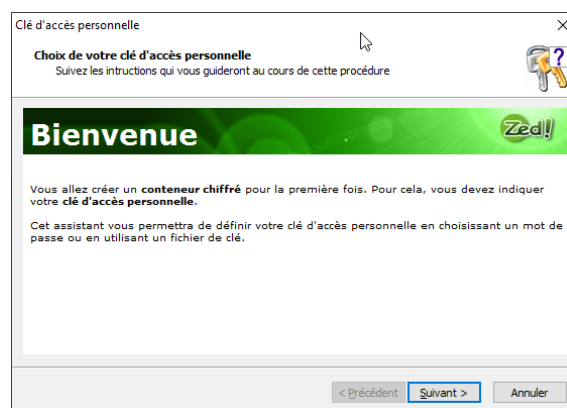
1. Télécharger et installer Zed!



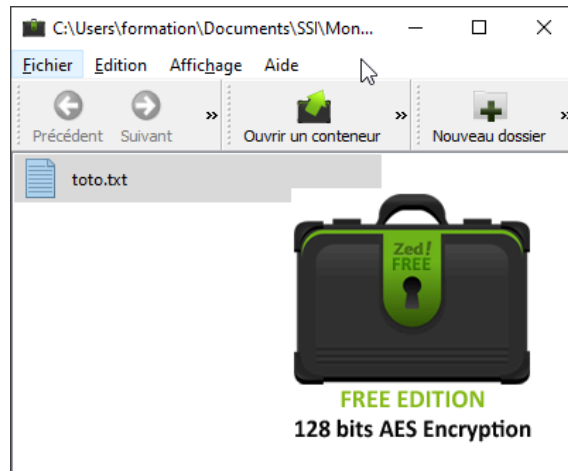
2. Exécuter Zed!
3. Dans le menu Fichier, cliquer sur Créer un conteneur chiffré.



4. Enregistrer le conteneur dans Documents\SSI

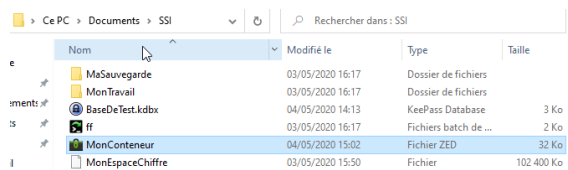


5. Déposer un fichier dans le conteneur chiffré



6. Fermer Zed! (ce qui ferme le conteneur)

7. Observer le fichier ainsi généré dans Documents\SSI



8. Ouvrir le conteneur à l'aide de votre mot de passe.

Exercice

👤 Créer un nouveau container ... Qu'en est-il de l'authentification ?

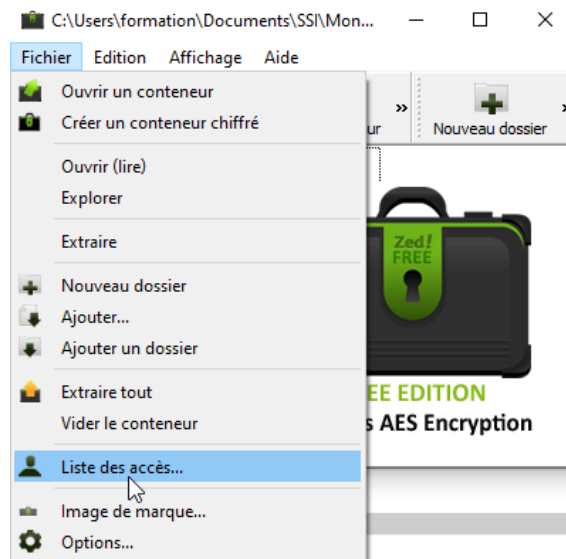
Exercice

👤 Zed! propose un chiffrement par clé ... mais qu'est ce que sont ces clés de chiffrements ?

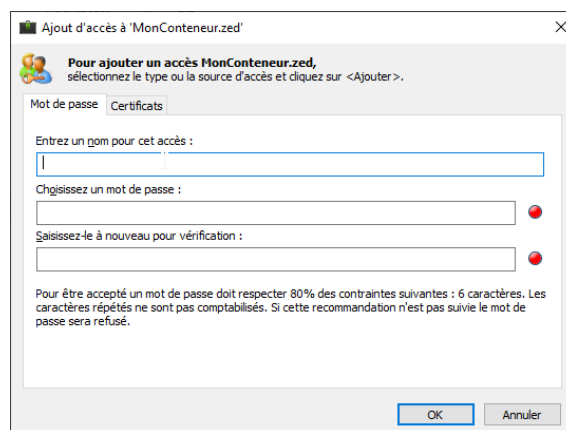
6.2.2 Un partage de documents privés

Pour l'instant, rien de bien intéressant, nous venons de créer un conteneur chiffré dont moi seul connaît le mot de passe.

— Ouvrir un conteneur Zed!



- Fichier – > Gestion des accès, ajouter un compte "Copain"



- Fermer le conteneur
- Ouvrir le conteneur avec le compte "copain"

Exercice

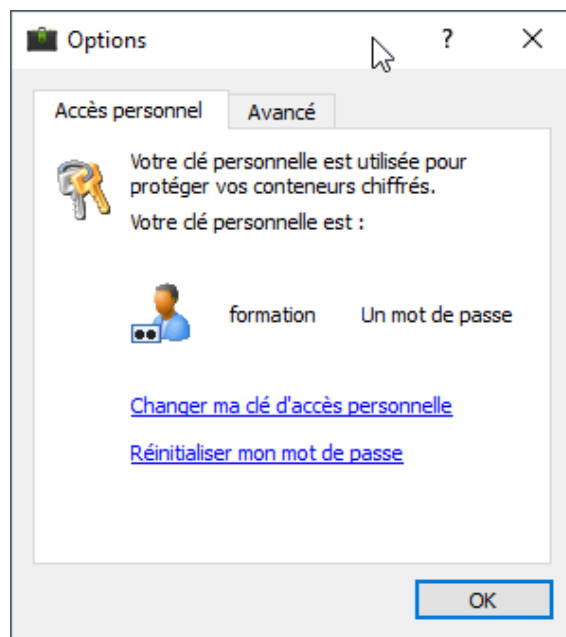


À vous de réaliser la conclusion...

Note



Il est possible de changer son mot de passe de chiffrement enregistré par Zed! en allant sur Fichier – > Options.



Attention cependant tous les conteneurs précédemment créés nécessiteront l'ancien mot de passe.

Conclusion

Cette série de travaux pratiques n'a pas abordé la sécurisation des échanges de courriels ou la sécurisation "industrielle" des données... Vos échanges d'information par mail ne sont donc pas protégés ...mais vous disposez maintenant d'éléments pour protéger les pièces jointes.

Concernant la sécurisation des courriels et bien plus, il est possible d'utiliser une solution de clés privées / clés publiques et notamment le logiciel recommandé et libre est Gpg4Win.



À suivre dans un autre cours...



Ne devenez pas un ronin, rejoignez le Libre !