

UE SEC102

Prise en main VM

Objectif :

- Préparer la machine virtuelle qui sera utilisée tout au long de la formation

Le travail à fournir:

- déployer et configurer la machine d'analyse pour ce cours



Prise en main VM

Téléchargement de la VM

- Téléchargez, depuis l'un des miroirs proposés de [tsurugi](#), le fichier OVA de la VM Tsurugi Linux [Lab]
- Une fois téléchargée, importez la VM dans VirtualBox

Prise en main VM

Configuration minimale requise

Dans les paramètres de la VM, il est recommandé d'utiliser au minimum la configuration suivante :

- 4Go de RAM
- 2 CPU

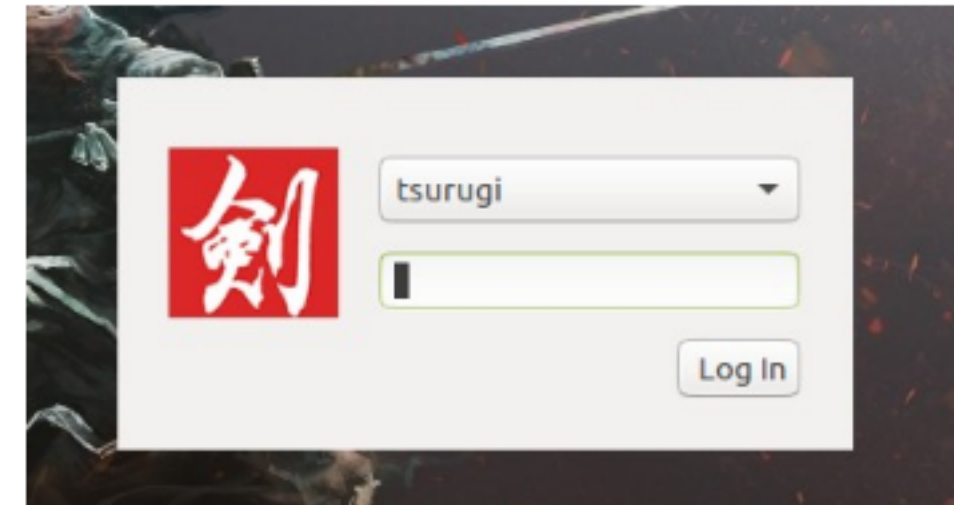
Prise en main VM

Ouverture de session

Mot de passe : tsurugi

Attention à ne pas mettre à jour la VM.

Certains logiciels utilisent des librairies spécifiques à leur fonctionnement



Prise en main VM

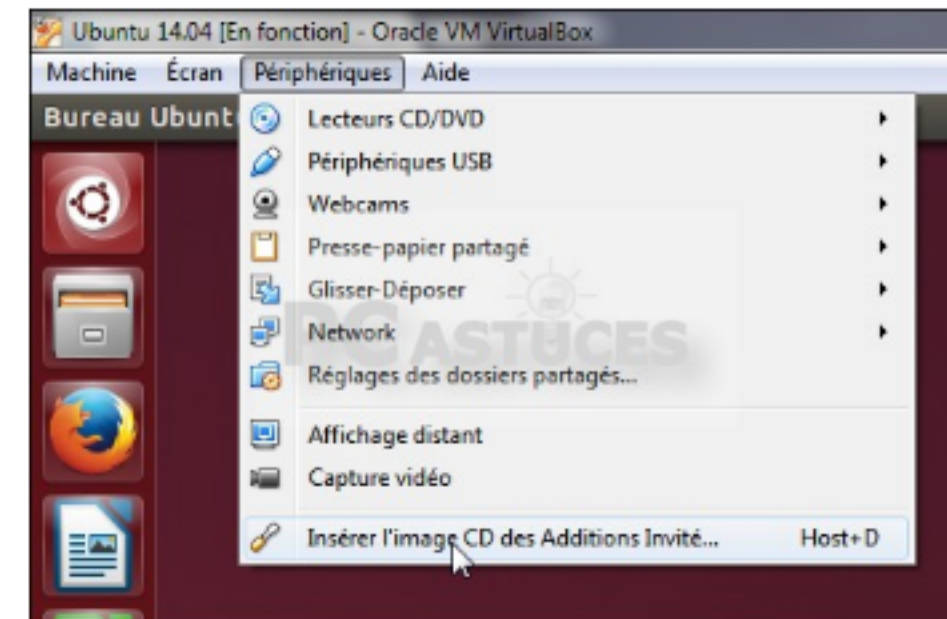
Résolution problème d'affichage

- Une fois que vous êtes connecté :
 - Ouvrir le logiciel « Displays » pour augmenter la résolution d'affichage

Prise en main VM

Ajout des additions invité :

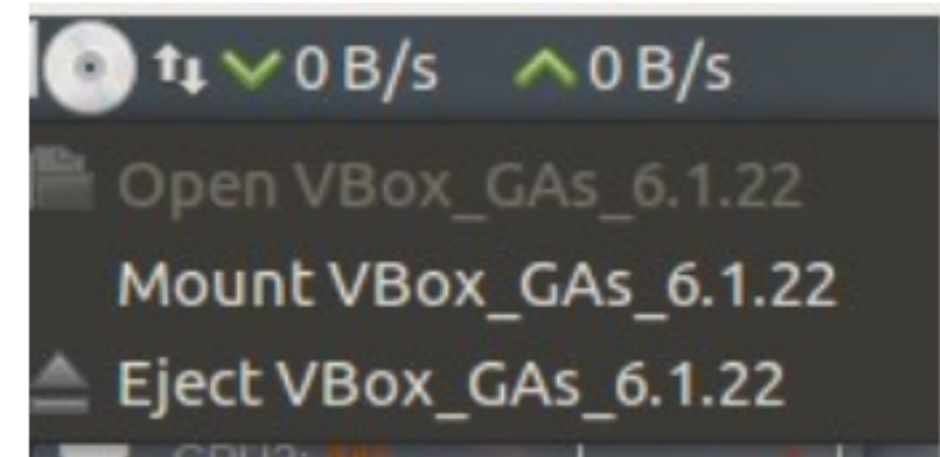
- Périphériques
- Insérer le CD des additions invité



Prise en main VM

Ajout des additions invité :

- Une icône avec un CD apparaît dans l'angle à droite de la VM.
- Cliquez dessus puis « mount »
- Il est possible de monter le CD depuis l'explorateur de fichier
 - Cliquer sur l'icône du CD
 - Mount read-only



Prise en main VM

Ajout des additions invité :

- Dans un terminal en *sudoer* tapez la commande suivante : (remplacez ***** par la version des additions invitées)

```
sh /media/tsurugi/Vbox_Gas_*****/autorun.sh
```

- Éteignez la machine

Prise en main VM

Ajout d'un dossier partagé

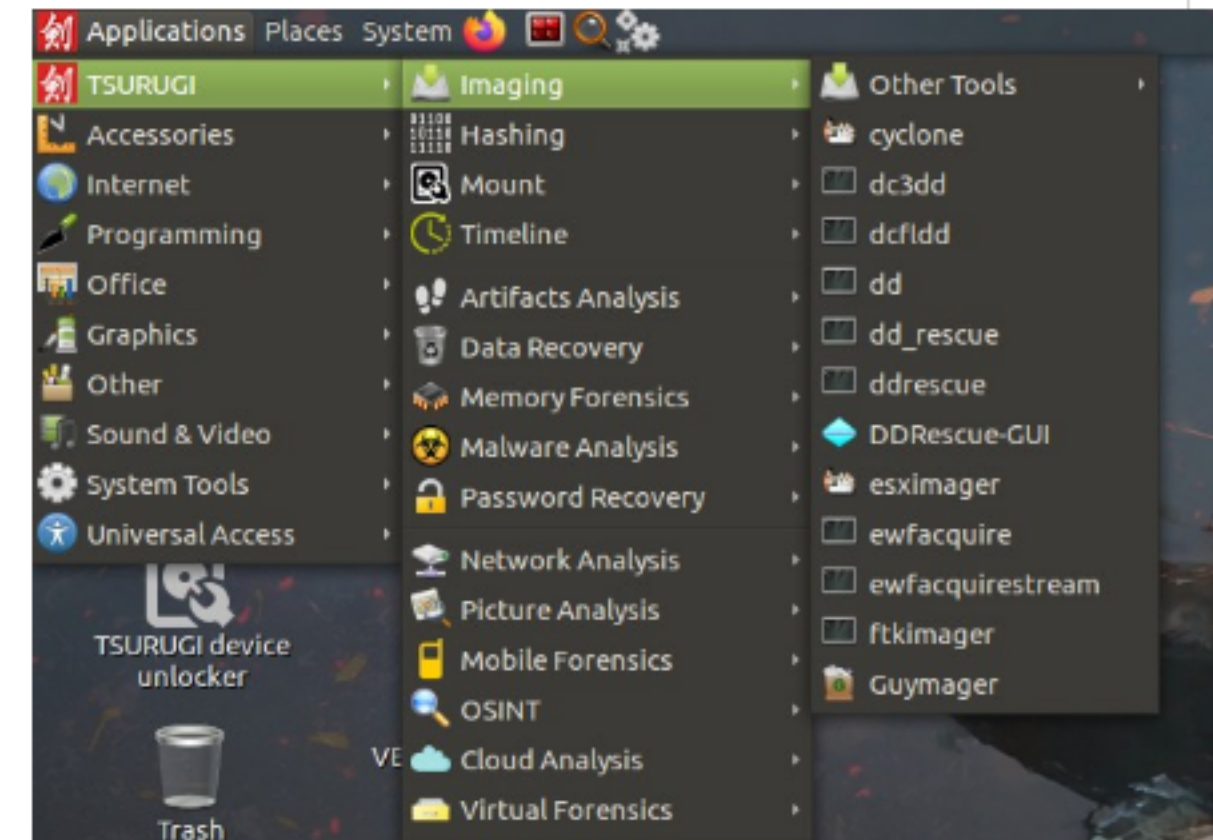
- Ajouter un dossier partagé entre votre hôte et la VM afin d'accéder aux différents dumps s'ils sont téléchargés sur votre machine hôte
- **⚠ Attention lorsque vous souhaitez accéder à votre dossier partagé, vous devez passer par le terminal et par la commande « sudo »**
- Au prochain redémarrage, ajouter votre utilisateur au groupe vboxsf (ouverture en mode user du dossier partagé)

```
sudo adduser $USER vboxsf
```

Prise en main VM

Applications spécifiques de Tsurugi :

- Classées par leurs types d'utilisation



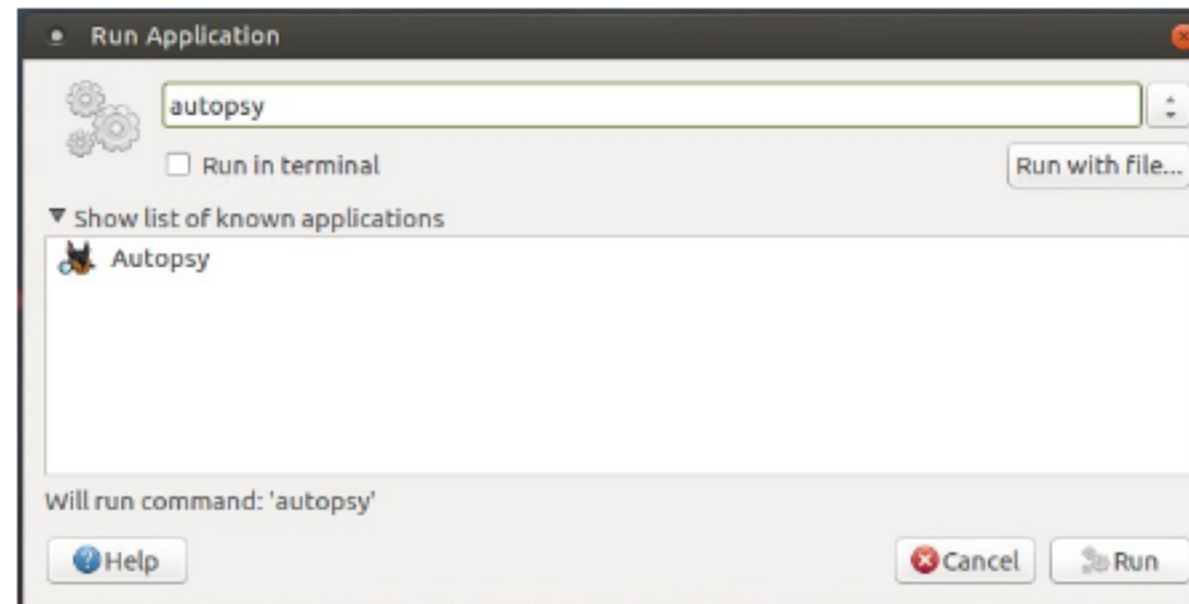
Prise en main VM

Recherche d'une application :

- Cliquez sur l'icône suivant :



- Faire la recherche dans la nouvelle fenêtre



Prise en main VM

Terminal

- Afin d'avoir un terminal, ouvrez le logiciel Terminator via l'icône suivant

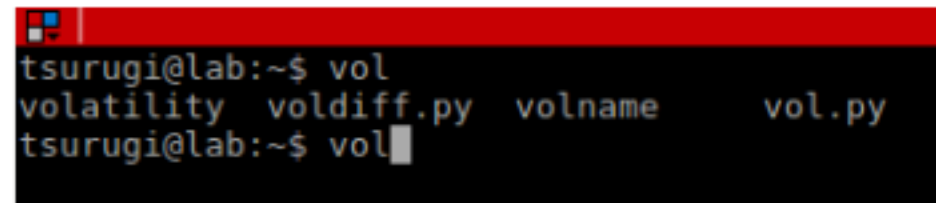


- Un shell de type bash sera alors ouvert et vous pourrez alors utiliser les lignes de commande

Prise en main VM

Terminal

- Utilisez l'indentation avec la touche tab dans le terminal :
 - Tapez le début du nom du logiciel recherché puis utilisez la touche tab



```
tsurugi@lab:~$ vol  
volatility voldiff.py volname vol.py  
tsurugi@lab:~$ vol
```

- Le terminal vous retournera la liste des logiciels commençant par ce que vous avez tapé
- **⚠ Attention vous ne trouverez pas tous les logiciels de cette manière (ex autopsy) vous devez alors utiliser l'icône de recherche d'application**

Prise en main VM

Lignes de commande utiles

- `setxkbmap fr` → passer le clavier en fr
- `ll / ls` → lister les fichiers dans le répertoire courant
- `cd /directory` → aller dans le répertoire
- `whoami` → savoir l'utilisateur
- `ps aux` → lister les processus
- `ip a` → lister les IP par connexions réseau
- `man NameOfSoftware` → manuel d'utilisateur d'un logiciel
- `sudo` → lancer la commande qui suit en tant que root
- `sudo su -` → changement d'utilisateur pour utilisateur root

Prise en main VM

Lignes de commande utiles

- history → affiche l'historique des commandes passées
- pwd → affiche le chemin du répertoire courant
- mkdir FolderName → ajout d'un nouveau dossier dans le répertoire courant
- grep/rgrep → recherche de chaînes de caractères
- find → recherche d'un élément du système
- cat → lire le contenu textuel d'un fichier
- tail → lire les 10 dernières lignes d'un fichier
- head → lire les 10 premières lignes d'un fichier

Prise en main VM

Installation de logiciels supplémentaire

- Depuis un terminal installer

```
sudo apt install libscca1
```

- Les éléments suivants seront utilisés pour l'examen
- Depuis un terminal, installez les éléments suivants :

```
sudo apt install pandoc texlive-latex-base texlive-fonts-recommended texlive-fonts-extra
```


Prise en main VM

Installation de volatility2

- L'élément suivant sera utilisé pour l'analyse de mémoire vive
- Déposer le fichier **Installation Volatility**
- Lancer le en ligne de commande