Get Memory Image for Volatility

Run Windows PowerShell as administrator, and change directory to VirtualBox installation path, then execute VBoxManage.exe with `list vms` command to see the name list of all available operating systems.

```
cd C:\"Program Files"\Oracle\VirtualBox
./VBoxManage.exe list vms
```

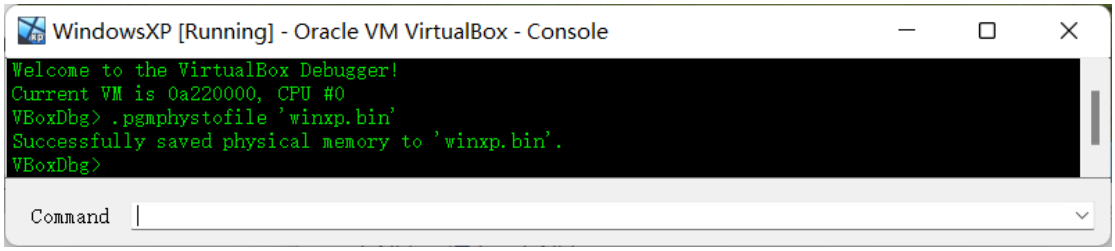
```
"Ubuntu" {4b7721a6-57c8-478e-a6b4-b16522c614d9}
"Win10_1909" {961542fe-313f-4325-85e9-718117b394f0}
"WindowsXP" {96d6eef8-4c4f-4b63-9e86-fce8df93bb92}
```

Then open VirtualBoxVM.exe, specify "WindowsXP" to `--startvm` command, and make sure to add `--dbg` at the end of the command to enable debugging mode, which is necessary for dumping VirtualBox memory.

```
PS C:\Program Files\Oracle\VirtualBox> ./VirtualBoxVM.exe --startvm WindowsXP --dbg
```

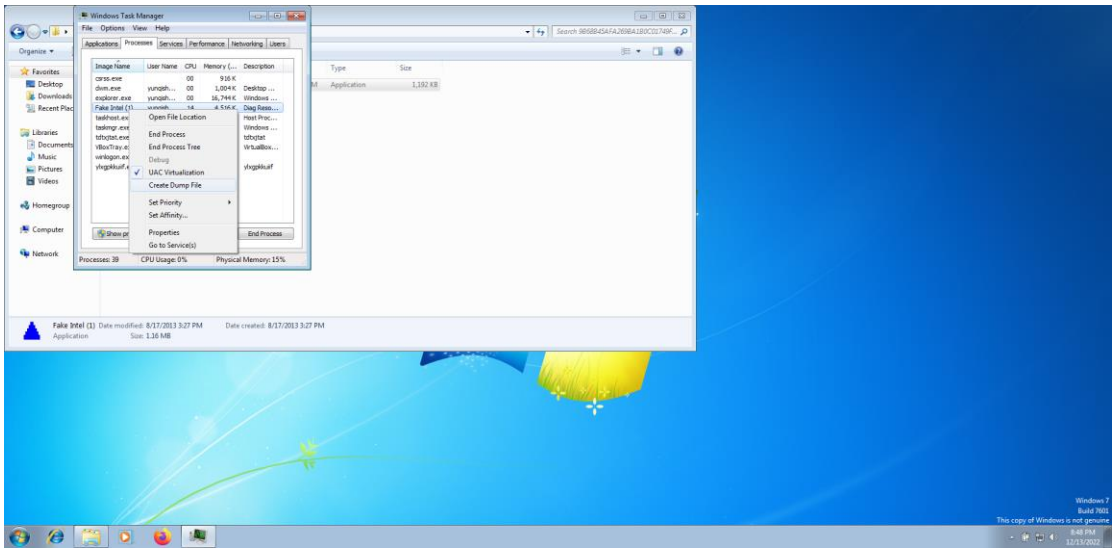
Run shelly.exe on Windows XP virtual machine and launch the VirtualBox debug console by navigating to "Debug" menu an select "Command Line". To create a memory dump, issue the below command (say the name of the dump file is "winxp.bin"):

```
.pgmphystofile 'winxp.bin'
```



Get Memory Image for Forecast

First run the malware sample in 32-bit Windows 7 virtual machine. Then go to windows task manager and find the malware process in "Processes" tab, right click, and click "create dump file".



The dump file created by task manager can be found at the path

`C:\Users\your_username\AppData\Local\Temp`

in your virtual machine. Please make sure you have enabled displaying hidden files in system setting.