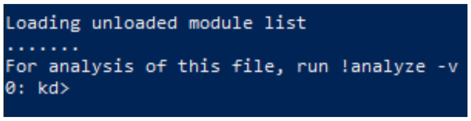
Hyper-V acquisition

1 Preparation (On Hyper-V Host)

1. Download and install the Debugging Tools for Windows package from Microsoft's web site: https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/
2. Download livekd from Windows SysInternals: https://docs.microsoft.com/en-gb/sysinternals/downloads/livekd
3. Extract the content of the downloaded livekd.zip to the location where the debugging tools were installed. *Note: By default, on a 64 bit system, the correct path would be "C:\Program Files (x86)\Windows Kits\10\Debuggers\x64"*
4. Once the extraction is complete, check that "livekd.exe" and "kd.exe" are present in the same folder.
5. From an administrative command prompt, execute the previously downloaded and extracted "livekd.exe"
6. If prompted to collect symbols automatically from the Microsoft symbol server, type "y" and press Enter.
7. At the following prompt, press Enter to keep the default path.
8. Download of the symbols will then commence and will likely take a few minutes to complete. On completion the prompt should appear as below:



```
Loading unloaded module list
.......
For analysis of this file, run !analyze -v
0: kd>
```

9. Once the above prompt has appeared, press CTRL + C or close the command prompt window

2 RAM acquisition

1. From an administrative command prompt, navigate to the folder that holds "livekd.exe", and run the following command:

```
livekd -hvl
```

2. This command lists the virtual machines running on that host. Identify the name of the virtual machine being investigated and then type the following command, replacing <VM> with the name of the VM being acquired:

```
livekd -hv <VM> -p -o C:\<VM>-RAM.dmp
```

3. The output path "-o" can be modified to an alternative suitable location.

3 Disk image acquisition

1. From an administrative PowerShell prompt, run the following command, replacing <VM> with the name of the VM being acquired:

```
Export-VM -Name <VM> -Path C:\
```

2. The output path "-Path" can be modified to an alternative suitable location.

4 Preparation for delivery

1. Move the files acquired during the RAM and Disk image acquisition steps (.dmp, .vhd, .avhd, .vhdx, .avhdx) to a single separate directory.

Calculate hash values of acquired files

1. Open a PowerShell prompt and navigate to the directory that contains the acquired files.
2. Run the following command:

```
Get-ChildItem . -recurse -exclude
hashes.txt | Get-FileHash -Algorithm
SHA1 | Select-Object -Property Path,
Hash, Algorithm | Out-File hashes.txt
```

Compress and encrypt files

1. Ensure you have access to compression software capable of creating encrypted ZIP archives. If not, IBM Security X-Force IR recommends using 7-Zip Portable, available from the official website: http://portableapps.com/apps/utilities/7-zip_portable or any other tool of your choice.
2. Compress the entire folder containing the acquired files into a single encrypted archive utilising a strong complex password
   a. Use the method approved within your organization to securely erase original files extracted from VM.

Delivering files to IBM Security X-Force IR

1. The compressed, encrypted archive can be delivered to the IBM Security X-Force IR team via the agreed method of delivery.
2. Share complex password used to for encryption with the IBM Security X-Force IR team using a different communication channel than used to share the acquired data.
3. Use the method approved within your organization to securely erase original files extracted from VM.
4. (Optional) Uninstall and/or remove the Debugging tools, livekd and associated materials.