Powering up your F-Response with PowerForensics

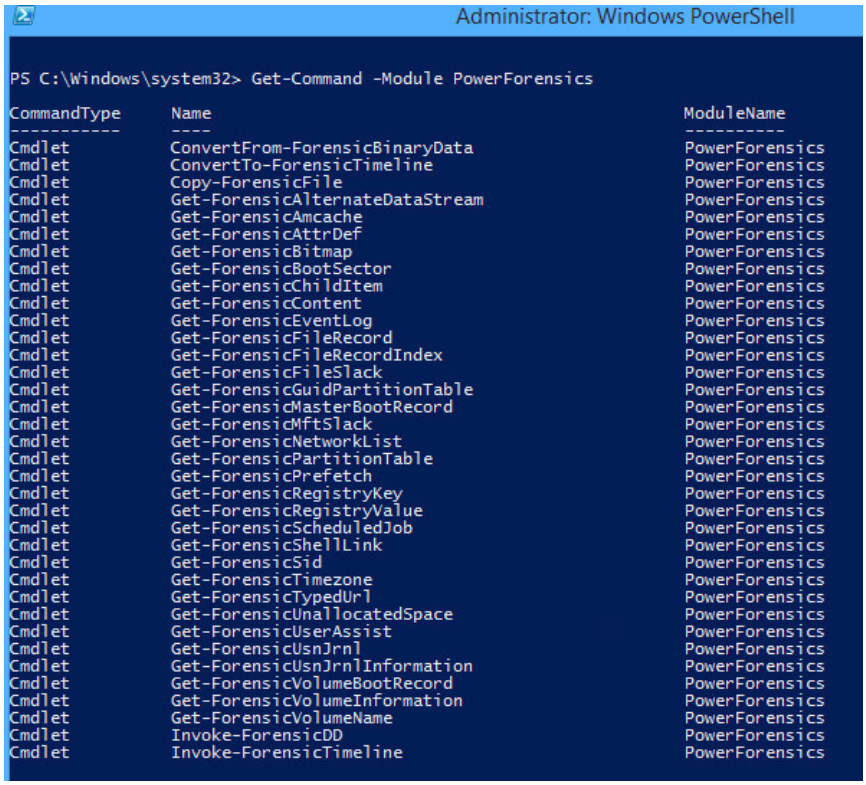
Dec/07/2015

We are always on the look out for new and interesting tools to couple with F-Response. Especially tools that highlight the flexibility of F-Response and the power of scripting.

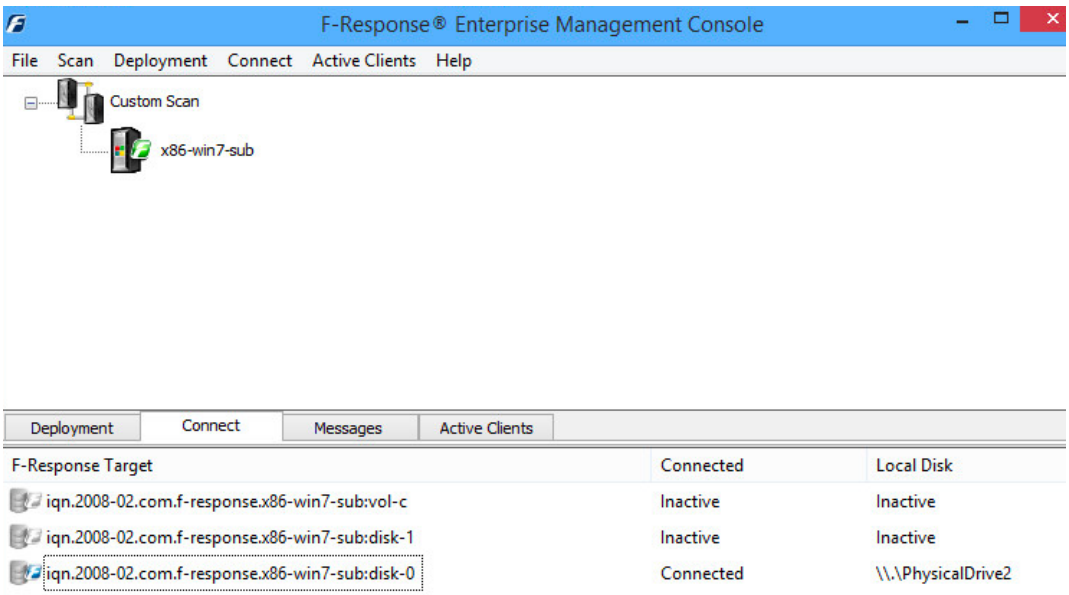
Therefore it was very exciting to stumble across "PowerForensics" from Jared Atkinson and Invoke-IR.

After a brief call with Jared we took some time to play with PowerForensics and try at least one interesting F-Response enabled usage case.

After loading up the PowerShell module, you'll see there is a considerable number of different options. There are more than enough interesting features here to fill many blog posts. We encourage you to explore the PowerForensics framework in more depth when the time allows.



Eager for a test drive, we then started F-Response Enterprise and connected to a test subject:



With the remote machine's disk zero now connected as \.\PhysicalDrive2 to our examiner machine, we decided to look at the details of the possibilities above. The PowerShell standard "Get-Help" Cmdlet can be applied to any of the cmdlets to get the scoop:

For those following along on their computer, sometimes Windows will assign a drive letter to the newly attached drive volumes automatically other times you have to use diskpart.exe. We've gone over that process before here.

Hrm.. would be cool to see if we can grab the remote machine's SAM key from the registry and dump it to a text file on our examiner machine.

Well will you look at that:

"PowerForensics" would make a nice addition to any toolkit, and coupling it with F-Response really ups the "Power"! We look forward to seeing to see how Jared and his team continue to expand this useful framework.

Thanks for taking the time to share this with us Jared!

Warmest Regards,

M Shannon, F-Response

Back...