



Had some fun with @blackbagtech Blacklight and F-Response Universal, thanks for the opportunity guys!
[Follow on Twitter](#)

HOME SUPPORT CONTACT CLOUD SERVICES SOFTWARE BUY F-RESPONSE ABOUT



F-Response Universal

Integrated, Centralized, Powerful solution for Remote Forensics, Incident Response, and E-Discovery

[Click here for more information](#)

computing

OSX
OSX

computing

win
WINDOWS

computing

lin
LINUX

mobile
and
ANDROID

1 2 3 4

"Your immediate responses have far exceeded our expectations. If only all other organizations were as responsive you guys are."

Samir Cortes, HARRIS BEACH PLLC, www.harrisbeach.com

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.



Support



[More Support Options](#)

[Mission Guides](#)

What is F-Response?



News & Blog

[F-Response 6.0.3.3, Universal 2.0.1.11](#)

[Now Available](#) We've just about made it through another year. It was a very exciting and fast paced year at...

[Powering up your F-Response with](#)

[PowerForensics](#) We are always on the look out for new and interesting tools to couple with F-Response. Especially...

[F-Response Universal and Black Bag Technologies Blacklight](#)

In the current release of F-Response Universal/Now (2.0.1.6) we added the ability to access remote...

[A Trio of New Releases](#)

We are very pleased to announce a trio of exciting new product releases at F-Response. There's a...

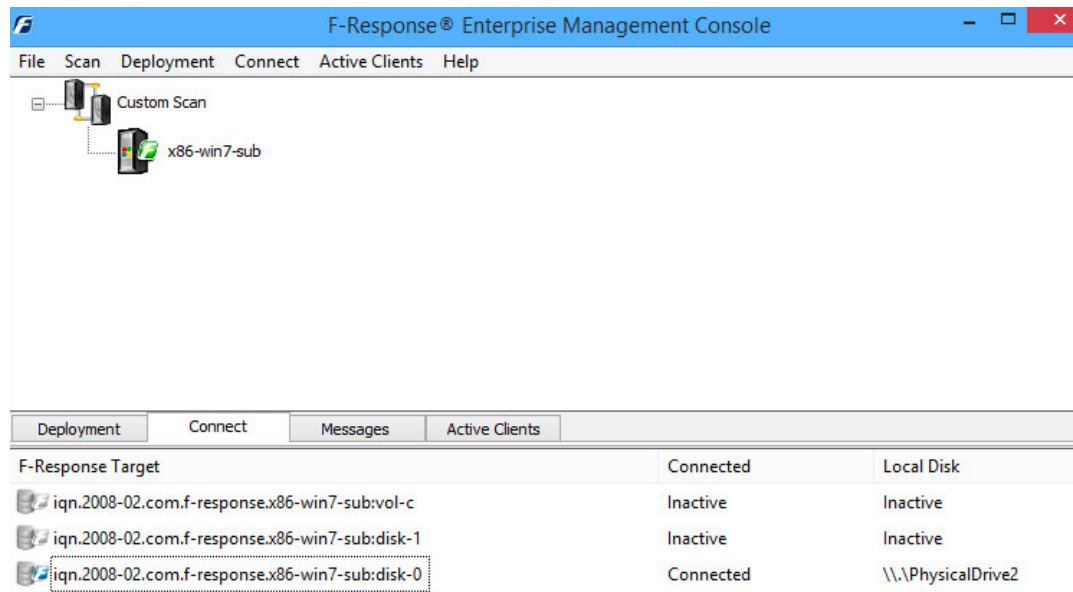
```

Administrator: Windows PowerShell

PS C:\Windows\system32> Get-Command -Module PowerForensics

CommandType      Name
-----
Cmdlet            ConvertFrom-ForensicBinaryData
Cmdlet            ConvertTo-ForensicTimeline
Cmdlet            Copy-ForensicFile
Cmdlet            Get-ForensicAlternateDataStream
Cmdlet            Get-ForensicAmcache
Cmdlet            Get-ForensicAttrDef
Cmdlet            Get-ForensicBitmap
Cmdlet            Get-ForensicBootSector
Cmdlet            Get-ForensicChildItem
Cmdlet            Get-ForensicContent
Cmdlet            Get-ForensicEventLog
Cmdlet            Get-ForensicFileRecord
Cmdlet            Get-ForensicFileRecordIndex
Cmdlet            Get-ForensicFileSlack
Cmdlet            Get-ForensicGuidPartitionTable
Cmdlet            Get-ForensicMasterBootRecord
Cmdlet            Get-ForensicMftSlack
Cmdlet            Get-ForensicNetworkList
Cmdlet            Get-ForensicPartitionTable
Cmdlet            Get-ForensicPrefetch
Cmdlet            Get-ForensicRegistryKey
Cmdlet            Get-ForensicRegistryValue
Cmdlet            Get-ForensicScheduledJob
Cmdlet            Get-ForensicShellLink
Cmdlet            Get-ForensicSid
Cmdlet            Get-ForensicTimezone
Cmdlet            Get-ForensicTypedUrl
Cmdlet            Get-ForensicUnallocatedSpace
Cmdlet            Get-ForensicUserAssist
Cmdlet            Get-ForensicUsnJrnl
Cmdlet            Get-ForensicUsnJrnlInformation
Cmdlet            Get-ForensicVolumeBootRecord
Cmdlet            Get-ForensicVolumeInformation
Cmdlet            Get-ForensicVolumeName
Cmdlet            Invoke-ForensicDD
Cmdlet            Invoke-ForensicTimeline
  
```

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...](#)

```
Administrator: Windows PowerShell

PS C:\Windows\system32> get-help get-forensicregistrykey

NAME
    Get-ForensicRegistryKey

SYNOPSIS
    Gets the keys of the specified registry hive.

SYNTAX
    Get-ForensicRegistryKey -HivePath <String> [-Key [<String>]] [<CommonParameters>]
    Get-ForensicRegistryKey -HivePath <String> [-Recurse [<SwitchParameter>]] [<CommonParameters>]

DESCRIPTION
    The Get-ForensicRegistryKey cmdlet parses a registry hive and returns the subkeys of the specified key.

    Except as noted, the cmdlets in the PowerForensics module require the permissions of a member of the
    Administrators group on the computer. To run them, start Windows PowerShell with the 'Run as administrator' option.

RELATED LINKS

REMARKS
    To see the examples, type: "get-help Get-ForensicRegistryKey -examples".
    For more information, type: "get-help Get-ForensicRegistryKey -detailed".
    For technical information, type: "get-help Get-ForensicRegistryKey -full".

PS C:\Windows\system32> _
```

```
Administrator: Windows PowerShell

PS C:\Windows\system32> get-forensicregistrykey -hivepath e:\windows\system32\config\SAM -recurse |Out-file c:\SubjectSAMkey
```

```
SubjectSAMkey - Notepad

File Edit Format View Help

HivePath      : e:\windows\system32\config\SAM
WriteTime     : 7/5/2012 2:37:40 AM
NumberOfSubKeys : 3
NumberOfVolatileSubKeys : 0
NumberOfValues : 2
FullName      : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}\SAM
Name          : SAM
Allocated     : True

HivePath      : e:\windows\system32\config\SAM
WriteTime     : 7/14/2009 4:02:18 AM
NumberOfSubKeys : 2
NumberOfVolatileSubKeys : 0
NumberOfValues : 1
FullName      : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}\SAM\Domains
Name          : Domains
Allocated     : True

HivePath      : e:\windows\system32\config\SAM
WriteTime     : 9/4/2014 2:54:57 PM
NumberOfSubKeys : 3
NumberOfVolatileSubKeys : 0
NumberOfValues : 2
FullName      : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}\SAM
```

Client Support

support at f-response.com

1-800-317-5497

Follow Us

Facebook

Twitter

LinkedIn

YouTube

F-Response products are protected by one or more patents or patents-pending, including U.S. Patent Nos. 7,899,882; 8,171,108; 9,037,630; and 9,148,418.