

Computer Forensics, Malware Analysis & Digital Investigations

Wednesday, May 28, 2008

F-Response to the rescue!

A few weeks ago, I received an evaluation version of the new F-Response tool. Although I knew it was coming and I was excited to try it out, I received it while I was out of town and when I returned I was inundated with work and could not play with it immediately as I had hoped, so instead it sat in the shipping envelope in my car.

Last week, I was called by a company who has been the victim of the SQL injection attack. They were frantic and wanted help immediately. I saddled up and grabbed my response kit and met with the company. After getting all the particulars, I responded to the data center where there were two computers that needed to be imaged.

As I setup my gear, the system admin explained that their main back-end SQL server was tied to *everything* and there was no cluster or back-up server, so I could not shut the system down or even reboot it, as it would interrupt their business. I thought, no problem, I will image it live. As I looked at the Dell 2U rack server, I noticed one USB port on the front and two on the back. I collected volatile data and saved the data off to a small USB flash disk. I noticed that the volatile data collection was taking a lot longer than normal. I then asked how old the server was and if the USB was 2.0 or 1.1.....uh-oh...

I then examined the installed hard drives and found there were 5 SCSI hard drives making up a RAID 5 system. The operating system saw one physical disk, consisting of two logical partitions, totaling 1.1TB

After he told me it was USB 1.1, I paused for a bit thinking through all the possible scenarios:

- A. Use USB 1.1 and save the live image off to a removable USB hard drive
- B. Insert a USB 2.0 card (required a reboot and this was not an option)
- C. Insert a Firewire card (required a reboot and this was not an option)
- D. Use netcat/cryptcat to throw the image across the network to another device
- E. Use FTK imager and save the image to a network share.

I figured I would try option A and see how long the image would take. After setting everything up, I started FTK imager and it began

Blogs I read

[Computer Forensics/E-Discovery Tip/Tricks and Information](#)

[Didier Stevens](#)

[Forensic Incident Response](#)

[int for\(ensic\) {blog}:](#)

[Jamie Morris' Blog](#)

[Robert Hensing's Blog](#)

[Windows Incident Response Blog](#)



email: lance (at) forensickb.com
phone: (888) 567-8417

All EnScripts are provided as-is, with no guarantees or promises to find all the evidence, solve your problems, fix your marriage or help you win the lottery.

Security & Investigative links

[NHTCU Good Practices Guide for Computer based Electronic Evidence](#)

[USSS Best Practices Guide to Seizing Electronic Evidence v3](#)

[VirusTotal online virus scanner](#)

[Jotti online virus scanner](#)

[SANS](#)

[Ghostship InfoSec](#)

to level out at 440 hours....hmmm...440/24 = 18.3 days... ouch!

So option A was out. After thinking a bit, I decided to use option F, F-Response! I remember that I had the package with me, but had not tried it out yet. I retrieved the package from my car and set up a VMware machine on my forensic laptop and went through the installation. I then tested it out using EnCase as the imaging platform and found it worked flawlessly.

I was still concerned about sending 1.1TB of data across the network wire that was being actively being used by clients and the web server. After digging around a bit, I found a separate gigabit NIC adapter on the back of the server that was not being used, so I used a crossover cable connected directly to my laptop and statically setup some IP addresses. I then copied the F-Response client application to a flash disk and ran it on the target server. Two minutes later, I had a direct connection and the 1.1TB drive was showing up on my forensic laptop as a local drive. I started EnCase and previewed the drive. I started the imaging process using EnCase and it reported 30 hours until completion, much better than 18 days..;)

--fast forward-->

28 hours later the image was done. When the dust settled, I had an EnCase image file sitting on a Lacie 2 TB removable drive that was complete and verified correctly.

The F-Response setup process took all of about 5 minutes and was extremely easy. There is a very small learning curve in order to understand how it works. The best part of it is that it allows you to use whatever forensic platforms you normally use, the F-Response tool is not a forensic analysis tool itself, but instead is a type of conduit that connects remote hard drives to your local workstation so that your traditional tools can be used.

Hogfly posted a cool video of using F-Response here:
<http://forensicir.blogspot.com/2008/04/ripping-registry-live.html>

Harlan also posted a blog about this tool here:
<http://windowsir.blogspot.com/2008/05/f-response.html>

There is also a great little demo video on how the tool works on the F-Response website: <http://www.f-response.com/>

If you have not seen this tool yet, I highly recommend you take advantage of their [\\$100 trial version](#). Their field kit, consultant and enterprise versions are insanely priced compared to the price point of other forensic tools. Once you see or try this tool I think it will find a permanent home in your response kit, like mine has!

Posted by Lance Mueller at [Wednesday, May 28, 2008](#) 

0 comments:

[Post a Comment](#)

Links to this post

Blog Archive

▼ 2008 (22)

▼ May (3)

[F-Response to the rescue!](#)

[Summary report of file types by extension](#)

[Find duplicate files](#)

► April (1)

► March (4)

► February (5)

► January (9)

► 2007 (36)

About Me

[View my complete profile](#)

[Create a Link](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)