Fastdump Pro 1.3 FAQ and usage guide 2/7/2009

General Questions and Answers

Q1. What interface/device is fastdump data being written to for the performance metrics listed below?

A1. The in-house FDPro performance tests and metrics are established performing a memory acquisition to the local file system of the machine being analyzed. FDPro was written and optimized to write at USB 2.0 speeds so can write at similar speeds to external thumb drives and hard drives. Speed will always vary depending on different hardware that is installed. It is also possible to acquire RAM to a network share or mapped drive, this relies on Microsoft's SMB protocol and is much much much slower.

Q2. The information you provided indicates a proprietary HPAK format. Is this the default export format for a Memory Acquisition, or will it is a DD RAW type image? What is the HPAK about?

A2. FDPro is capable of exporting in two formats. The first format is industry standard DD RAW format with a ".bin" extension. This process is just a literal zero-to-max_mem_size dump of the physical memory. The second format that is available is known as HPAK. HPAK is an HBGary proprietary format which is capable of several key features, namely the ability to store and archive the RAM and Pagefile in a single archive. HPAK format also supports compression using the gzip format. This is useful during instances where space on the collecting device/system is limited.

Basic usage of FDPro:

Command: **FDPro.exe c:\memdump.bin**

Action: FDPro.exe will acquire the local system physical memory to the file c:\memdump.bin in literal/standard .bin format

Command: **FDPro.exe c:\memdump.hpak**

Action: FDPro.exe will acquire the local system memory into the HPAK archive file c:\memdump.hpak

Compression can be used in the HPAK archive

Command: **FDPro.exe c:\memdump.hpak -compress**

Action: FDPro.exe will acquire the local system memory into the HPAK archive file c:\memdump.hpak in gz-compressed format

Image RAM and Pagefile to an HPAK archive

Command: **FDPro.exe c:\memdump.hpak –page**

Action: FDPro.exe will acquire the local system memory and the Pagefile contents into the HPAK archive file c:\memdump.hpak.

NOTE: The current shipping version of FDPro.exe with Responder Field Edition and Professional ***only support Win XP/2K Pagefile acquisition***. The patch scheduled in the next few weeks will contain complete Pagefile support for all supported operating systems that Responder supports.

List Contents of HPAK

Command: **FDPro.exe c:\memdump.hpak –hpak list**

Action: FDPro.exe will list the contents of the HPAK file

Extract Files from HPAK to file system

Command: **FDPro.exe c:\memdump.hpak –hpak extract memdump.bin**

Action: FDPro.exe extracts the archived file region named "memdump.bin" to the file memdump.bin in the current directory. This file is equivalent to what FDPro.exe c:\memdump.bin would produce. This feature allows specific elements of collected evidence to be extracted from an HPAK archive. The extract feature will automatically decompress the section if it was compressed.

FDPro Performance Metrics as of 1/24/2009:

The average time for a full FDPro dump including Full Pagefile acquisition is ~5 minutes or less in many cases and as much as 10-15 minutes on very high end machines (16GB+). Some preliminary metrics are:

- Dumped 512mb Win2k box + 1gb of Pagefile in ~1.5mins, total file size ~1.5gb
- Dumped 2gb XPSP2 box + 3gb of Pagefile in ~5mins, total file size ~5gb
- Dumped 6gb Vista64 box + 8gb of Pagefile in ~8mins, total file size ~14gb
- Dumped 8gb Vista64 box + 8gb of Pagefile compressed in ~9mins, total file size ~8gb

We have successfully acquired a full RAM acquisition, including Pagefile and completed a successful analysis (complete with integrated paged-in data) on the following platforms:

- Windows 2000 x86 SP0-SP4
- Windows XP x86 SP2 & 3
- Windows XP x64 SP2
- Windows 2K3 X64 SP2
- Windows Vista X86 SP1
- Windows Vista X86 SP1

FDPro Process Probe Feature: *NEW*

GOAL: Force all executable code into RAM for one or all processes on the system. Code that is paged out to the Pagefile.sys or code that is contained in the executable on disk but not in use will be called into RAM prior to acquisition of physical memory.

Process Probe Feature: The process probe feature allows you to control what memory is "paged-in" to RAM from SWAP AND the File System before FDPro does its RAM acquisition. When you use the –probe smart feature FDPro.exe will walk the entire process list and make sure *all* code is called into RAM. The result is that we're able to recover almost 100% of the user-land process memory by causing these pages to be activated & paged in on the fly. The Probe feature will even force code from the file system into RAM for a specific process. We've heard requests for "the code being paged out" which is why we came up with this simple feature. –Probe should dramatically improve the quality and thoroughness of Live Windows Memory Forensic Investigations and Malware Analysis.

Best Practices for Process Probe Feature

Forensic best practices dictate that an investigator or analyst should always acquire RAM first (and the Pagefile too) without running the Probe Feature. After "freezing the current state" of the RAM the investigator or analyst should run FDPro again, this time using the Probe Feature. All paged out code is forced back into RAM prior to the 2nd acquisition of RAM; this 2nd RAM image would contain the code that is paged out to the swap file during the first. This will greatly enhance the quality of the live analysis of the runtime state of the machine.

Example Steps:

1) Arrive at server or workstation suspected in the computer incident or forensic investigation.
2) Take the 1st RAM acquisition for "freezing the state of the machine". This is a full RAM image.
    1. Perform Initial Triage of RAM with Responder. Identify any processes that might require the –Probe feature.
3) Take any number of additional images that use the –probe option to increase the amount of string cross references, code regions, and to enable future full document discovery & extraction/re-construction
    1. If the analyst or investigator doesn't want to take time to analyze the RAM with Responder, they could just simply use fastdump pro a 2nd time right away. The "–Probe smart" feature will move ALL code paged out for all processes into RAM prior to performing the RAM acquisition.

If you're doing any sort of malware analysis, Reverse Engineering, or know for a fact that you will never have to use the RAM acquisition in litigation then you can go ahead and probe –smart on your very first image to save you time but you should know that this technique will contain a larger footprint in RAM than just performing an acquisition.

A large upside of probing is that you can do multiple acquisitions of RAM (assuming you have sustained access to the machine), and pretty much carve out exactly what you want in memory by making sure its active. Find a link to a page that's paged out? No big deal, go back to the machine and run FDPro again and probe the process id. In using this method it's OK to cause data to be paged out because paged out is not the same thing as being lost since we can easily recover anything that's paged in or out by taking new images or going back to older ones. In using this iterative approach you can basically get around the limitations of not having full page-file support (but it will be coming shortly).

Some Thoughts on Acquiring RAM on Large Servers with FDPro

Example System with 128GB RAM and 100GB Pagefile:

Probing can help in "Big Iron" scenarios where a machine has 128GB+ of RAM and obtaining and parsing an accompanying Pagefile would require collecting at least 180-256GB of extra data. Instead of having to collect a huge Pagefile on these jumbo systems you might want to consider the option of smart probing since we can force all *executable code and data* into the physical memory range.

Process Probe Feature Best Practices for Malware Analysis:

When performing any type of malware analysis one should use the probe-smart feature 100% of the time.

Use Probe Feature with HBGary Flypaper & VMware for Malware Analysis: