PFDump Forensic Tool
Member of Malware-Hunters Forensic Toolkit

Quick-Start Guide

Version 1.0.0
April 19,, 2011

Michael G. Spohn
mspohn@malware-hunters.net

Table of Contents

Table of Tables

Table of Figures

Introduction

This document describes the features of the *PFDump* forensic tool. This tool provides a quick and easy way to extract forensic metadata from Windows prefetch files. It is designed to supplement your forensic tools such as EnCase, FTK, Hex-Ways Forensic, etc. Be sure to read the *PFDump* FAQ document to learn more about the design of the tool.

The tool has the following features:

- Lightweight, fast, and flexible command line tool.
- Extracts forensic metadata from a Windows prefetch file.
- Analyzes a single prefetch file or a folder containing multiple prefetch files.
- Analyzes prefetch files on a live system for incident responders.
- Dumps prefetch metadata to stdout, TXT, HTML, or XML files.
- Computes MD5 and SHA1 hashes for each prefetch file.
- Self-contained binary – no other dependencies.
- Runs on Windows XP, Vista, 7.

The tool is used by forensic examiners and incident responders who need a quick method to examine valuable forensic metadata from a Windows file. Common uses include:

- Identifying applications run on a Windows host and when.
- Identifying the full path to an executable run on a Windows host.
- Identifying how many times and application has been run.
- Searching and sorting application execution time.
- Creating a timeline of applications run on a Windows host.

Tool Use

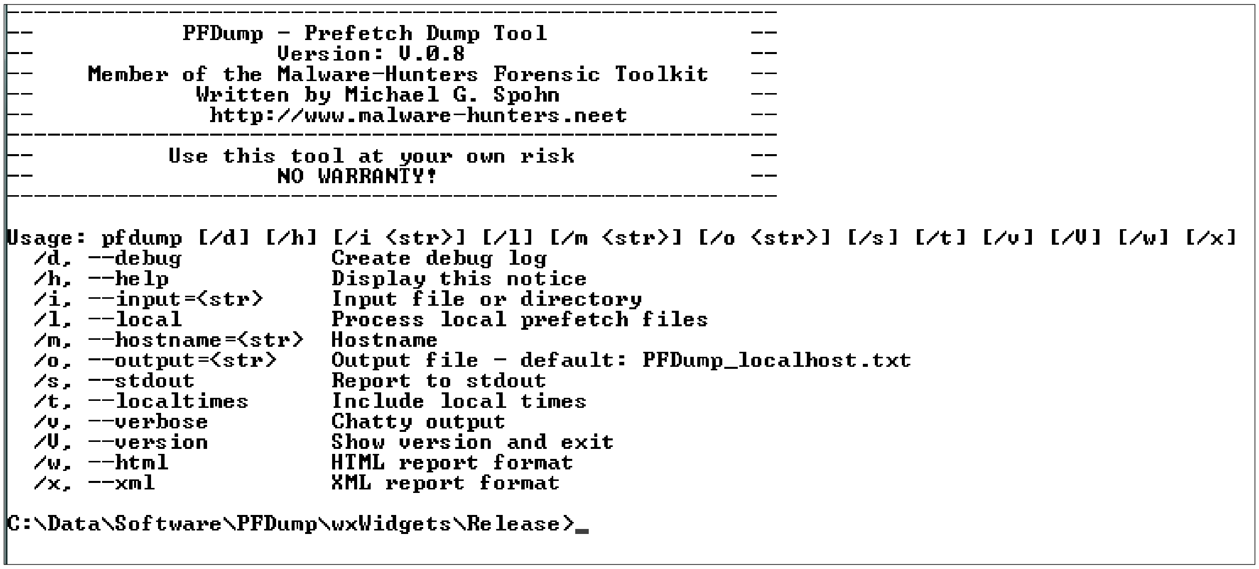
PFDump is designed to be fast and easy to use. All you need is the tool binary. You can extract the Windows prefetch folder from an acquired forensic image using any capable forensic tool such as EnCase, FTK, Hex-Ways Forensic and the Sleuthkit.

You can analyze the \Windows\Prefetch folder from a live host by simply copying the folder to a USB thumb drive or a network share. You can also analyze the prefetch files on a live system by passing the /l command line parameter.

Once you have a prefetch file or a folder containing prefetch files you want to examine, run *PFDump* passing the name of the file or folder file on the command line with the /I switch.

If you run the tool without any command line parameters, you will see a usage printout shown in Figure 1.

Figure 1: PFDump usage printout



```
----------------------------------------------------------
--            PFDump - Prefetch Dump Tool               --
--                 Version: V.0.8                       --
--     Member of the Malware-Hunters Forensic Toolkit   --
--             Written by Michael G. Spohn              --
--              http://www.malware-hunters.neet         --
----------------------------------------------------------
--           Use this tool at your own risk             --
--                    NO WARRANTY!                      --
----------------------------------------------------------

Usage: pfdump [/d] [/h] [/i <str>] [/l] [/m <str>] [/o <str>] [/s] [/t] [/v] [/V] [/w] [/x]
  /d, --debug            Create debug log
  /h, --help             Display this notice
  /i, --input=<str>      Input file or directory
  /l, --local            Process local prefetch files
  /m, --hostname=<str>   Hostname
  /o, --output=<str>     Output file - default: PFDump_localhost.txt
  /s, --stdout           Report to stdout
  /t, --localtimes       Include local times
  /v, --verbose          Chatty output
  /V, --version          Show version and exit
  /w, --html             HTML report format
  /x, --xml              XML report format

C:\Data\Software\PFDump\wxWidgets\Release>_
```

To analyze a prefetch file or folder use the /i switch followed by the name of the prefetch file or folder containing multiple prefetch files.

The command line switches *PFDump* uses are described in Table 1 below:

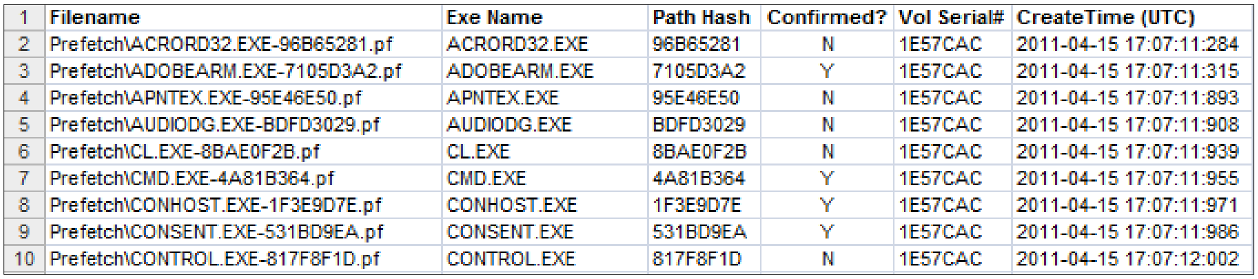
Table 1: PFDump command line switches

Switch	Description
/d	Run in debug mode - creates a log file named PFDump.log
/h	Prints usage text and exits.
/i	The prefetch file or folder containing multiple prefetch files to analyze
/l	Analyze the prefetch file on the localhost (e.g. \Windows\Prefetch)
/m	Use the provided hostname string in output filename and report hostname field.
/o	Use the provided filename as the output filename.
/s	Print tab delimited report to stdout.
/t	Include local times in report.
/v	Verbose mode - describes application actions.
/V	Prints tool version number and exits.
/w	Output report in HTML format.
/x	Output report in XML format.

Report Formats

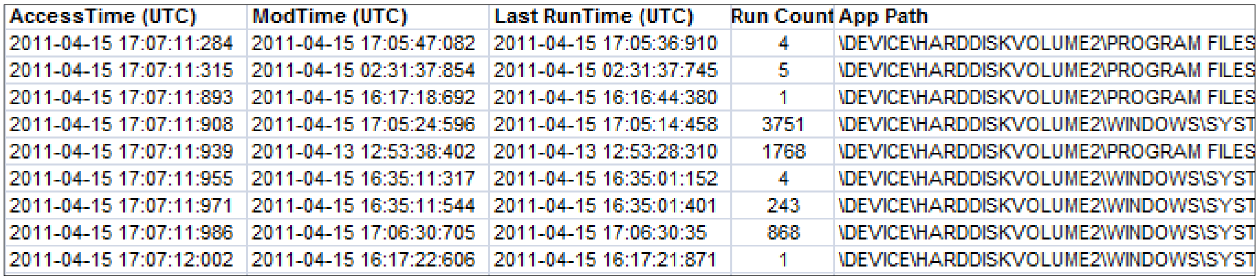
PFDump provides three report formats; tab-delimited text, HTML, or XML, If you do not provide the /w (HTML) or /x (XML) switches on the command line, the output report will be in tab-delimited text. Samples of the three report formats are shown in the below tables.

Figure 2:   Tab-Delimited Report Format (Cols 1-6)



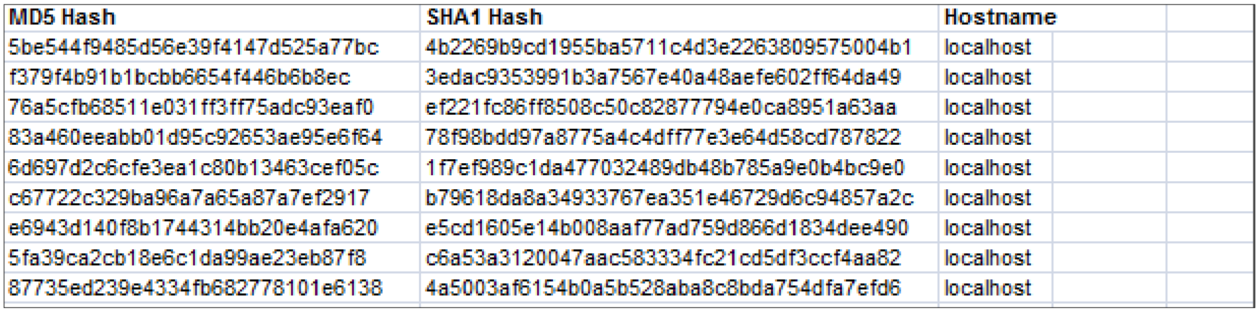
1	Filename	Exe Name	Path Hash	Confirmed?	Vol Serial#	CreateTime (UTC)
2	Prefetch\ACRORD32.EXE-96B65281.pf	ACRORD32.EXE	96B65281	N	1E57CAC	2011-04-15 17:07:11:284
3	Prefetch\ADOBEARM.EXE-7105D3A2.pf	ADOBEARM.EXE	7105D3A2	Y	1E57CAC	2011-04-15 17:07:11:315
4	Prefetch\APNTEX.EXE-95E46E50.pf	APNTEX.EXE	95E46E50	N	1E57CAC	2011-04-15 17:07:11:893
5	Prefetch\AUDIODG.EXE-BDFD3029.pf	AUDIODG.EXE	BDFD3029	N	1E57CAC	2011-04-15 17:07:11:908
6	Prefetch\CL.EXE-8BAE0F2B.pf	CL.EXE	8BAE0F2B	N	1E57CAC	2011-04-15 17:07:11:939
7	Prefetch\CMD.EXE-4A81B364.pf	CMD.EXE	4A81B364	Y	1E57CAC	2011-04-15 17:07:11:955
8	Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE	1F3E9D7E	Y	1E57CAC	2011-04-15 17:07:11:971
9	Prefetch\CONSENT.EXE-531BD9EA.pf	CONSENT.EXE	531BD9EA	Y	1E57CAC	2011-04-15 17:07:11:986
10	Prefetch\CONTROL.EXE-817F8F1D.pf	CONTROL.EXE	817F8F1D	N	1E57CAC	2011-04-15 17:07:12:002

Figure 3: Delimited Report Format (Cols 7-11)



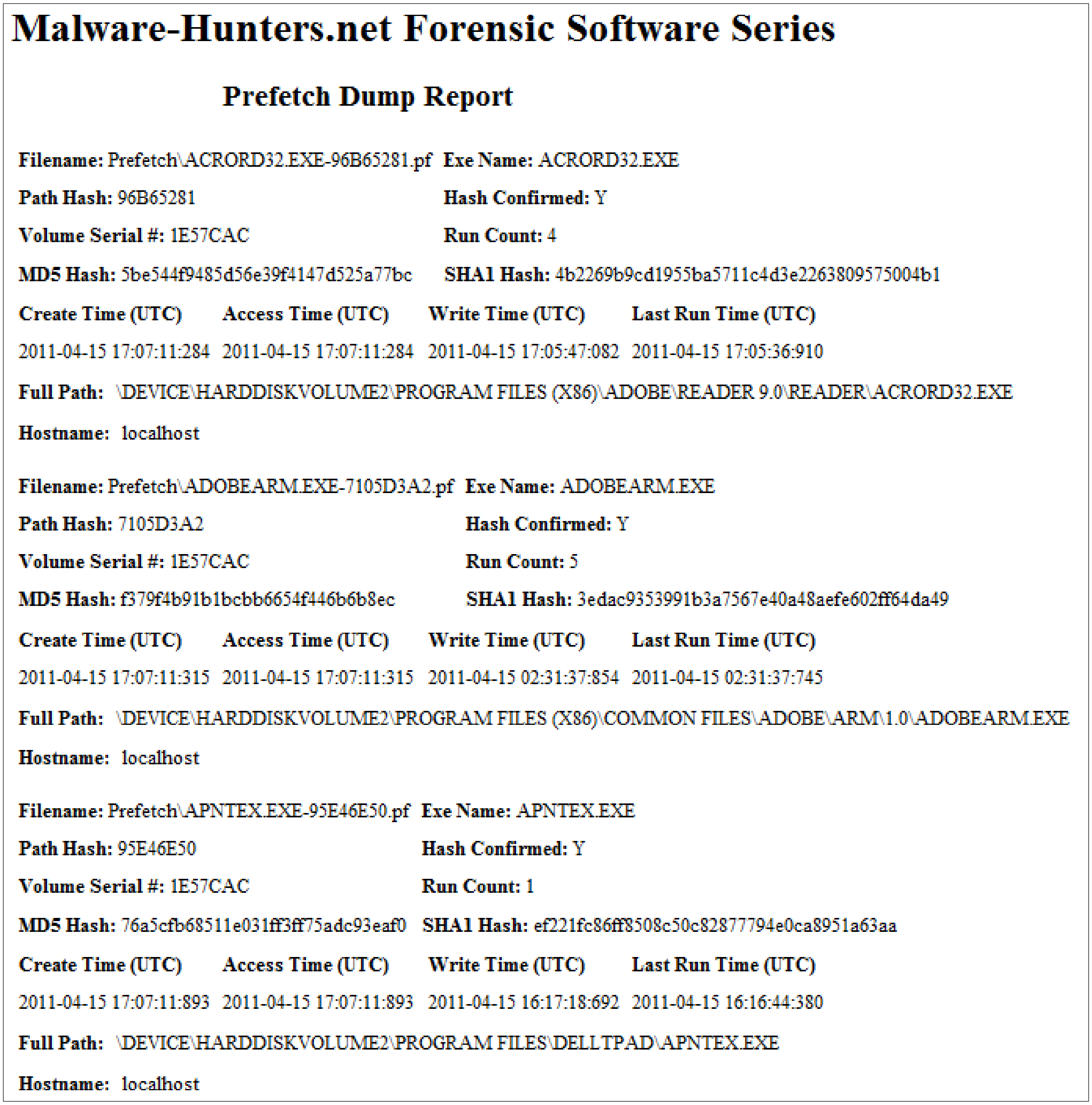
AccessTime (UTC)	ModTime (UTC)	Last RunTime (UTC)	Run Count	App Path
2011-04-15 17:07:11:284	2011-04-15 17:05:47:082	2011-04-15 17:05:36:910	4	\DEVICE\HARDDISKVOLUME2\PROGRAM FILES
2011-04-15 17:07:11:315	2011-04-15 02:31:37:854	2011-04-15 02:31:37:745	5	\DEVICE\HARDDISKVOLUME2\PROGRAM FILES
2011-04-15 17:07:11:893	2011-04-15 16:17:18:692	2011-04-15 16:16:44:380	1	\DEVICE\HARDDISKVOLUME2\PROGRAM FILES
2011-04-15 17:07:11:908	2011-04-15 17:05:24:596	2011-04-15 17:05:14:458	3751	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYST
2011-04-15 17:07:11:939	2011-04-13 12:53:38:402	2011-04-13 12:53:28:310	1768	\DEVICE\HARDDISKVOLUME2\PROGRAM FILES
2011-04-15 17:07:11:955	2011-04-15 16:35:11:317	2011-04-15 16:35:01:152	4	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYST
2011-04-15 17:07:11:971	2011-04-15 16:35:11:544	2011-04-15 16:35:01:401	243	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYST
2011-04-15 17:07:11:986	2011-04-15 17:06:30:705	2011-04-15 17:06:30:35	868	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYST
2011-04-15 17:07:12:002	2011-04-15 16:17:22:606	2011-04-15 16:17:21:871	1	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYST

Figure 4: Tab-Delimited Report Format (Cols 12-14)



MD5 Hash	SHA1 Hash	Hostname
5be544f9485d56e39f4147d525a77bc	4b2269b9cd1955ba5711c4d3e2263809575004b1	localhost
f379f4b91b1bcbb6654f446b6b8ec	3edac9353991b3a7567e40a48aefe602ff64da49	localhost
76a5cfb68511e031ff3ff75adc93eaf0	ef221fc86ff8508c50c82877794e0ca8951a63aa	localhost
83a460eeabb01d95c92653ae95e6f64	78f98bdd97a8775a4c4dff77e3e64d58cd787822	localhost
6d697d2c6cfe3ea1c80b13463cef05c	1f7ef989c1da477032489db48b785a9e0b4bc9e0	localhost
c67722c329ba96a7a65a87a7ef2917	b79618da8a34933767ea351e46729d6c94857a2c	localhost
e6943d140f8b1744314bb20e4afa620	e5cd1605e14b008aaf77ad759d866d1834dee490	localhost
5fa39ca2cb18e6c1da99ae23eb87f8	c6a53a3120047aac583334fc21cd5df3ccf4aa82	localhost
87735ed239e4334fb682778101e6138	4a5003af6154b0a5b528aba8c8bda754dfa7efd6	localhost

Figure 5: HTML Report Format



Malware-Hunters.net Forensic Software Series

Prefetch Dump Report

Filename: Prefetch\ACRORD32.EXE-96B65281.pf **Exe Name:** ACRORD32.EXE

Path Hash: 96B65281 **Hash Confirmed:** Y

Volume Serial #: 1E57CAC **Run Count:** 4

MD5 Hash: 5be544f9485d56e39f4147d525a77bc **SHA1 Hash:** 4b2269b9cd1955ba5711c4d3e2263809575004b1

Create Time (UTC)	Access Time (UTC)	Write Time (UTC)	Last Run Time (UTC)
2011-04-15 17:07:11:284	2011-04-15 17:07:11:284	2011-04-15 17:05:47:082	2011-04-15 17:05:36:910

Full Path: \DEVICE\HARDDISKVOLUME2\PROGRAM FILES (X86)\ADOBE\READER 9.0\READER\ACRORD32.EXE

Hostname: localhost

Filename: Prefetch\ADOBEARM.EXE-7105D3A2.pf **Exe Name:** ADOBEARM.EXE

Path Hash: 7105D3A2 **Hash Confirmed:** Y

Volume Serial #: 1E57CAC **Run Count:** 5

MD5 Hash: f379f4b91b1bcbb6654f446b6b8ec **SHA1 Hash:** 3edac9353991b3a7567e40a48aefe602ff64da49

Create Time (UTC)	Access Time (UTC)	Write Time (UTC)	Last Run Time (UTC)
2011-04-15 17:07:11:315	2011-04-15 17:07:11:315	2011-04-15 02:31:37:854	2011-04-15 02:31:37:745

Full Path: \DEVICE\HARDDISKVOLUME2\PROGRAM FILES (X86)\COMMON FILES\ADOBE\ARM\1.0\ADOBEARM.EXE

Hostname: localhost

Filename: Prefetch\APNTEX.EXE-95E46E50.pf **Exe Name:** APNTEX.EXE

Path Hash: 95E46E50 **Hash Confirmed:** Y

Volume Serial #: 1E57CAC **Run Count:** 1

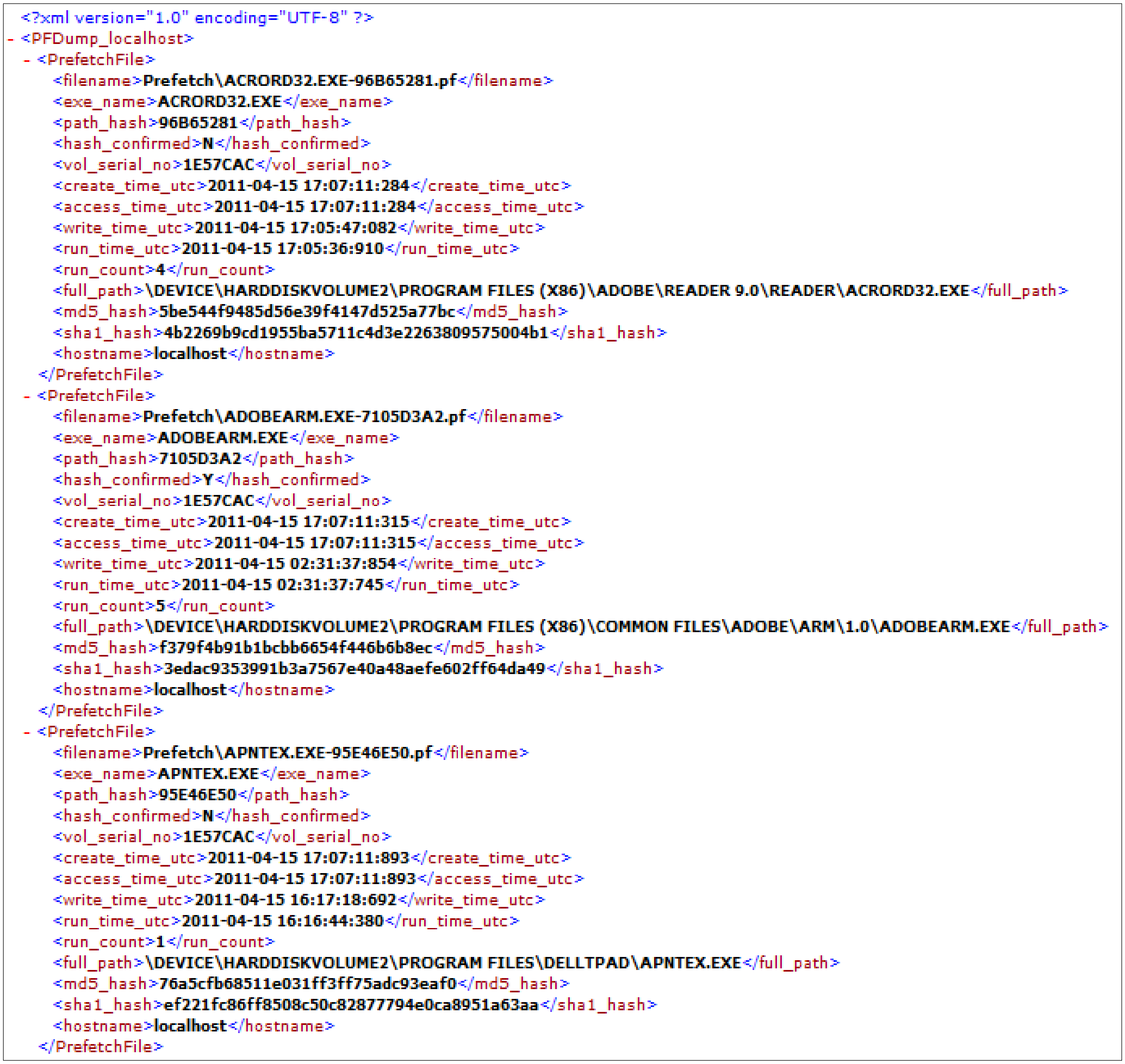
MD5 Hash: 76a5cfb68511e031ff3ff75adc93eaf0 **SHA1 Hash:** ef221fc86ff8508c50c82877794e0ca8951a63aa

Create Time (UTC)	Access Time (UTC)	Write Time (UTC)	Last Run Time (UTC)
2011-04-15 17:07:11:893	2011-04-15 17:07:11:893	2011-04-15 16:17:18:692	2011-04-15 16:16:44:380

Full Path: \DEVICE\HARDDISKVOLUME2\PROGRAM FILES\DELLTPAD\APNTEX.EXE

Hostname: localhost

Figure 6: XML Report Format



```
  <?xml version="1.0" encoding="UTF-8" ?>
- <PFDump_localhost>
  - <PrefetchFile>
      <filename>Prefetch\ACRORD32.EXE-96B65281.pf</filename>
      <exe_name>ACRORD32.EXE</exe_name>
      <path_hash>96B65281</path_hash>
      <hash_confirmed>N</hash_confirmed>
      <vol_serial_no>1E57CAC</vol_serial_no>
      <create_time_utc>2011-04-15 17:07:11:284</create_time_utc>
      <access_time_utc>2011-04-15 17:07:11:284</access_time_utc>
      <write_time_utc>2011-04-15 17:05:47:082</write_time_utc>
      <run_time_utc>2011-04-15 17:05:36:910</run_time_utc>
      <run_count>4</run_count>
      <full_path>\DEVICE\HARDDISKVOLUME2\PROGRAM FILES (X86)\ADOBE\READER 9.0\READER\ACRORD32.EXE</full_path>
      <md5_hash>5be544f9485d56e39f4147d525a77bc</md5_hash>
      <sha1_hash>4b2269b9cd1955ba5711c4d3e2263809575004b1</sha1_hash>
      <hostname>localhost</hostname>
    </PrefetchFile>
  - <PrefetchFile>
      <filename>Prefetch\ADOBEARM.EXE-7105D3A2.pf</filename>
      <exe_name>ADOBEARM.EXE</exe_name>
      <path_hash>7105D3A2</path_hash>
      <hash_confirmed>Y</hash_confirmed>
      <vol_serial_no>1E57CAC</vol_serial_no>
      <create_time_utc>2011-04-15 17:07:11:315</create_time_utc>
      <access_time_utc>2011-04-15 17:07:11:315</access_time_utc>
      <write_time_utc>2011-04-15 02:31:37:854</write_time_utc>
      <run_time_utc>2011-04-15 02:31:37:745</run_time_utc>
      <run_count>5</run_count>
      <full_path>\DEVICE\HARDDISKVOLUME2\PROGRAM FILES (X86)\COMMON FILES\ADOBE\ARM\1.0\ADOBEARM.EXE</full_path>
      <md5_hash>f379f4b91b1bcbb6654f446b6b8ec</md5_hash>
      <sha1_hash>3edac9353991b3a7567e40a48aefe602ff64da49</sha1_hash>
      <hostname>localhost</hostname>
    </PrefetchFile>
  - <PrefetchFile>
      <filename>Prefetch\APNTEX.EXE-95E46E50.pf</filename>
      <exe_name>APNTEX.EXE</exe_name>
      <path_hash>95E46E50</path_hash>
      <hash_confirmed>N</hash_confirmed>
      <vol_serial_no>1E57CAC</vol_serial_no>
      <create_time_utc>2011-04-15 17:07:11:893</create_time_utc>
      <access_time_utc>2011-04-15 17:07:11:893</access_time_utc>
      <write_time_utc>2011-04-15 16:17:18:692</write_time_utc>
      <run_time_utc>2011-04-15 16:16:44:380</run_time_utc>
      <run_count>1</run_count>
      <full_path>\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\DELLTPAD\APNTEX.EXE</full_path>
      <md5_hash>76a5cfb68511e031ff3ff75adc93eaf0</md5_hash>
      <sha1_hash>ef221fc86ff8508c50c82877794e0ca8951a63aa</sha1_hash>
      <hostname>localhost</hostname>
    </PrefetchFile>
```

Support

PFDump has been an extremely useful tool in our incident response forensic work. We believe it will be a valuable addition to your forensic toolkit.

Please send bug reports and future enhancement requests to: mspohn@malware-hunters.net.