Analysis of Free Download Manager for Forensic Artefacts

Muhammad Yasin, Muhammad Arif Wahla, and Firdous Kausar

Information Security Department, College of Signals,
National University of Science and Technology, Pakistan
{yaseenyns,arif.wahla,firdous.imam}@gmail.com

Abstract. Free Download Manager (FDM) is one of the most popular download managers due to its free availability, high download speed and versatility. It contains a lot of information that is of potential evidentiary value even if a user deletes web browser history, cookies and temporary internet files. This software records download activities across multiple files saved with .SAV extensions in the User Profile. This paper analyzes: 1) the windows registry entries particularly concerned to configuration and user settings, 2) the log files (with .SAV extension) created by FDM to trace download activities, and 3) RAM and swap files from a forensic perspective. This research work describes a number of traces left behind after the use of FDM such as install location, default download path, downloaded files, and menu extensions to name a few, thus enabling digital investigators to search for and interpret download activities. The widespread use of FDM makes this research work an attractive option for forensic investigators, ranging from law enforcement agencies to employers monitoring personnel.

Keywords: Free Download Manager, Forensic Artefacts, Digital Investigation.

1 Introduction

Free Download Manager (FDM) is a free and open-source download manager released under GNU Public License (GPL). It provides the ability to download files using HTTP, HTTPS, FTP, BitTorrent and Metalink protocols [1], [2]. Its main features include *Upload Manager*, *Site Explorer* and *HTML Spider*. *Upload Manager* facilitates file sharing with other users, *Site Explorer* presents the site structure to download necessary files, and users can download a HTML page or the complete website with *HTML Spider*.

This research work investigates FDM (versions 2.1, 2.3, 2.5 and 3.0) for extracting information about download activities and directories, user's information, as well as date and time the activity was generated. Our investigations are based on Windows registry and log files analysis. Registry analysis facilitate*s* collection of footprints such as FDM configuration and user settings. Log files analysis assists in tracing download activities.

S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 59–68, 2010.

This paper is organized as follows: Section 2 explains using windows registry analysis to discover FDM activities. Section 3 gives details of log files analysis for the same purpose. Section 4 elucidates RAM and swap file analysis for FDM investigation. The paper is concluded in the last section.

2 Windows Registry Analysis

The Windows registry records information necessary to configure the system and is an invaluable source for the digital investigators to examine, investigate and collect evidence from Windows operating systems [3], [4], [5]. Internet-dependent applications commonly utilize the registry to store data. Web browsers such as Internet Explorer records typed URL's, last download directory and reference of *index.dat* file, which keeps record of web activities, and instant messengers also leave limited footprints in the registry [6]. The registry also stores mail client information such as username, password and unread emails [7]. Peer-to-Peer (P2P) networks can either leave minimal footprints of user activity (having no logs of searches and downloaded files), such as Limewire or connection and download path information (e.g. Kazaa) or logs of recently searched keywords or phrases (e.g. Morpheus) [8].

There are many freely available tools for gathering information from Windows Registry such as RegEdit, Resplendent Registrar Lite [9] and Registry Viewer [10]. Microsoft provides RegEdit on Microsoft Windows XP installations with administrative privileges for searching, editing and deleting data within registry hives. These tools are used to analyze the registry to find out traces left by FDM.

A key to access registry information is through knowledge of the registry structure itself [11]. Registry and file system information can be correlated to provide a comprehensive picture of the download activities to examiners. FDM uses consistent registry structure to store configuration and user setting in the Windows registry under single root key. During analysis, analysts need to know the exact installation details of the particular application to refer it in the case. The following *'Free Download Manager'* key has a value *'Path'* which contains the install path of FDM.

HKEY_CURRENT_USER\Software\VicMan Software\Free Download Manager

FDM manages the downloaded files by their file types in several default and user created groups. The default groups of FDM are Music, Software, Video, and Others. All files other than those in predefined file formats are stored in the *Others* group. FDM gives the option to choose the group for download automatically or manually.

Figure 1 illustrates the categorization of downloaded files by FDM. When started initially, all download files are shown in the '*All Groups'* and '*Filters'* folders. When an incomplete download file is deleted by the user, the reference of that file will be removed from '*All Groups'* and shifted to the '*Recycle Bin'*. If this file is restored from '*Recycle Bin',* FDM moves it back to '*All Groups'* and resumes downloading. Upon successful file download, FDM makes a new reference to the downloaded file in '*History'* and also maintains its reference under '*All Groups'*.

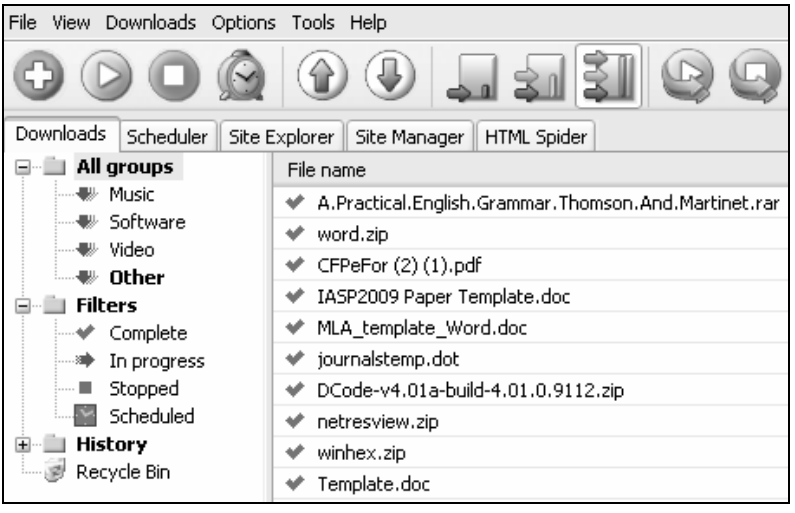


Fig. 1. Graphical User Interface of FDM

The Windows registry creates a separate '*Groups'* key to store '*All Groups'* data as shown in Figure 2. From a forensic perspective, this key can provide important artefacts regarding supported extensions and download directory path (*OutFolder).* The Windows registry creates separate keys with the name as downloaded activity (e.g. the video files which were downloaded by the user are recorded under the '*Video'* key as sub-key of '*Groups'* key).

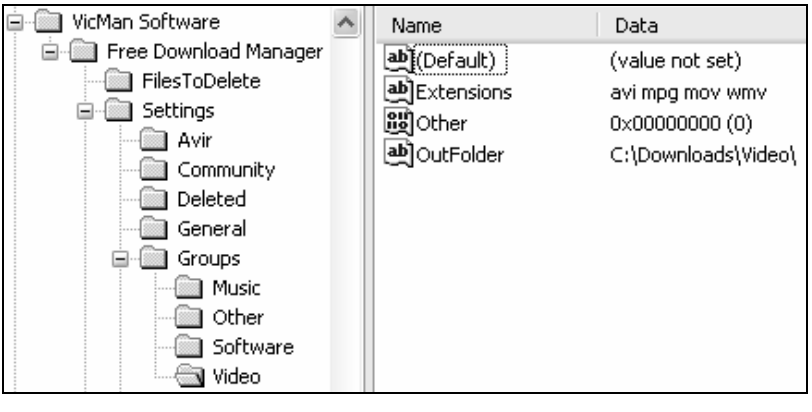


Fig. 2. Groups of FDM in Windows registry

After establishing a system connection to a proxy server, the user requests a service, such as, a file, connection, web page, or other resource. The proxy server evaluates the user request according to its filtering rules. For example, it may filter traffic by IP address or protocol. FDM provides a facility to download files using HTTP, HTTPS, FTP, BitTorrent and Metalink protocols. The Windows registry '*Network'* key contains login credentials of FTP, HTTP and HTTPS, maximum number of

segments of a single file to speed up the download, minimum size of each segment, and Internet access type (which describes whether user is specifying proxy settings manually or importing from Microsoft Internet Explorer). Table 1 lists all the possible values of the *'InternetAccess-Type'* key value.

Table 1. Value data of InternetAccessType key value

Value Data	Description
Value '0'	User is not using any proxy
Value '1'	Importing proxy settings from Microsoft IE
Value '2'	User is specifying proxy setting manually

When a user configures proxy settings manually, these settings are recorded under the '*Network'* key as shown in Figure 3.

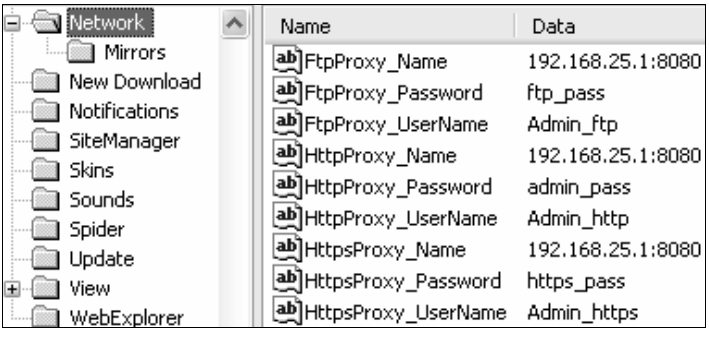


Fig. 3. Network key and related key values

Figure 3 illustrates the proxy address, port address, username and password for FTP, HTTP and HTTPS protocols. Proxy address and port number are concatenated under the *'xxxxProxy_Name'* key value where *'xxxx'* can be any protocol specified by the proxy. The login credentials given by users are stored in plaintext format and therefore vulnerable to attack. If an attacker gains access to the system on which FDM is installed with proxy setting configured by the user/administrator, he can get login credentials with ease and possibly further exploit the network. In this scenario, two cases are to be considered. First, if the attacker is an employee and gains access to a user account, he could gain additional permissions not accessible and he might be able to download files which are normally restricted or blocked. Secondly, if an attacker gains access to an administrator account, he would able to release restrictions, choke the network, block web services, bypass proxies, violate or modify security policy, as well as launch Denial-Of-Service attacks, create backdoors for future attacks, etc.

It is important to be aware of the registry branches which contain sub-keys related to FDM if it is installed on a suspected system. These sub-keys refer to the context menu when right-clicking on webpage irrespective of whether an internet connection

is enabled or disabled. The following key shows the integration of FDM with default web browser Internet Explorer.

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ MenuExt

When an application is installed in Windows operating systems, registry maintains its un-installation path under *'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Uninstall'* key. The registry contains FDM un-install information under *'Free Download Manager_is1'* sub-key. Key values *'UninstallString'*, *'InstallLocation'* and *'Inno Setup: User'* contain the un-install path, installed location, and the installer Login ID. Having the Login ID of the installer makes a stronger case if the suspected user has installed it.

3 Log Files Analysis

This section describes an in-depth analysis of the log/history files created by FDM. FDM maintains a history in multiple files for each user in the default location *'C:\Documents and Settings\User Profile\Application Data\Free Download Manager'*. The user has to delete the history of downloaded files manually. A summary of the forensic artefacts collected from all FDM log files is available in Table 2. A discussion of the details of each log file follows.

Table 2. Log Files and their artefacts

Log Files \ Artefacts	File Name	Group Name	Destination Path	URL address	Proxy Settings	Date & Time	Username &Password
dlmgrsi.sav			Y				
downloads.del.sav	Y	Y	Y	Y	Y	Y	Y
downloads.his.sav	Y		Y	Y	Y	Y	Y
downloads.sav	Y	Y	Y	Y	Y	Y	Y
history.sav			Y	Y		Y	
sites.sav		Y		Y			Y
spider.sav		Y	Y	Y			Y

FDM maintains a record of the last ten downloaded files in *'dlmgrsi.sav'*. This file stores download directory paths of all the downloaded files in chronological order. The download directory path of each file is separated from other files with 4 bytes of separator. This is a forensically significant file because it contains the download directory paths of the last ten downloaded files, even if these files are deleted from both *'All Groups'* and *'History'* folders as discussed in the previous section. When a user downloads the eleventh file, the download path of first file will be deleted and the download location of last file will be appended at the end of file. This shows that 'dlmgrsi.sav' uses a queue, a First-In-First-Out (FIFO) data structure, to store data to the length of ten. FDM does not permit the user to increase the queue length.

However, if the developers of FDM increase the storage capacity of the queue, it would be very beneficial for forensic investigators.

The *'Downloads.his.sav*' file contains file name, complete URL address, download path, username, password, as well as download start and stop time. Figure 4 illustrates the file name *'whoistd.zip'*. After a separator, it shows the complete download directory path. The next bytes hold the URL address *'http://apple:orange @www.nirsoft.net/utils/ whoistd.zip'*. The URL address also contains the username and password of the user, e.g. *'apple:orange'*, if required to download the file. The following 8 bytes [7E 49 C5 01 C0 02 3A 38] provide the start date and time (when the user supplies the URL for downloading). This pair of 4 bytes are swapped [C0 02 3A 38 7E 49 C5 01] to convert it into a 64-bit little-endian hexadecimal value. The next 8 bytes repeat the download start time and the subsequent 8 bytes contains download finish time. By default, FDM only stores completely downloaded file history, however, it also provides the option to maintain the history of in-progress, stopped, and schedule files. When a user deletes the history, FDM also clear the contents of this file after exiting the application.

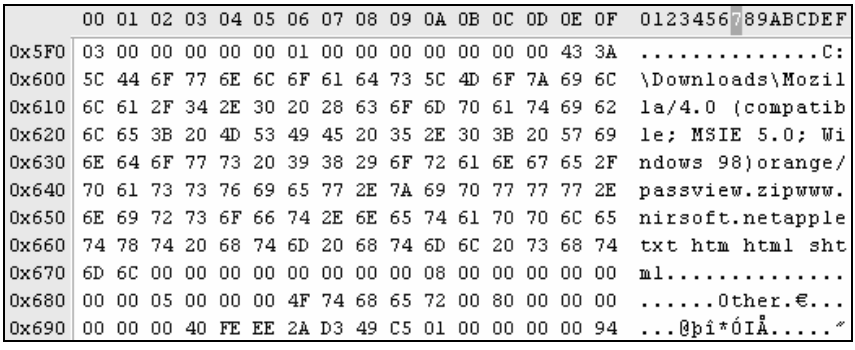
	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0x240	00	00	00	0B	00	00	00	77	68	6F	69	73	74	64	2E	7A	.......whoistd.z
0x250	69	70	21	00	00	00	44	3A	5C	46	6F	72	65	6E	73	69	ip!...D:\Forensi
0x260	63	20	54	6F	6F	6C	73	73	73	73	73	5C	77	68	6F	69	c Toolsssss\whoi
0x270	73	74	64	2E	7A	69	70	35	00	00	00	68	74	74	70	3A	std.zip5...http:
0x280	2F	2F	61	70	70	6C	65	3A	6F	72	61	6E	67	65	40	77	//apple:orange@w
0x290	77	77	2E	6E	69	72	73	6F	66	74	2E	6E	65	74	2F	75	ww.nirsoft.net/u
0x2A0	74	69	6C	73	2F	77	68	6F	69	73	74	64	2E	7A	69	70	tils/whoistd.zip
0x2B0	00	00	00	00	00	38	F5	34	7E	49	C5	01	C0	02	3A	38	.....8õ4~IÅ.À.:8
0x2C0	7E	49	C5	01	C0	02	3A	38	7E	49	C5	01	EA	A1	00	00	~IÅ.À.:8~IÅ.ê¡..
0x2D0	00	00	00	00	13	00	00	00	41	6E	61	6C	79	73	69	6E	........Analysin

Fig. 4. History of download locations of all downloaded files

The *'Downloads.sav*' file holds all download file entries in *'All Groups'*. These file entries store the files currently downloaded, in-progress, stopped, or scheduled by users. When a user deletes a suspected file from *'All Groups'*, the corresponding contents will be removed from *'Download.sav'* after exiting the application. *'Downloads.sav'* contains file name, download directory path, URL address, username and password (if required to download a file), protocol used to download, proxy address, port address, group name, and download completion time.

Figure 5 shows the file download path *'C:\Downloads\'*, password '*orange'*, file name *'passview.zip'*, website address *'www.nirsoft.net*', username *'apple'*, group name *'Other'* and download completion time *'[40 FE EE 2A D3 49 C5 01]'*. The hexadecimal value of time is already in little-endian format so it does not need to swap the pair of 32- bits. The date and time of downloading the file is *'Mon, 25 April 2005 20:12:55 UTC'*. This shows that user has manually changed the date and time of the suspected system to mislead investigators.

The *'History.sav'* file maintains a log in the form of segments; each segment is separated from other segments with a separator 'FDM History N''. The first segment



	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0x5F0	03	00	00	00	00	00	01	00	00	00	00	00	00	00	43	3A	..............C:
0x600	5C	44	6F	77	6E	6C	6F	61	64	73	5C	4D	6F	7A	69	6C	\Downloads\Mozil
0x610	6C	61	2F	34	2E	30	20	28	63	6F	6D	70	61	74	69	62	la/4.0 (compatib
0x620	6C	65	3B	20	4D	53	49	45	20	35	2E	30	3B	20	57	69	le; MSIE 5.0; Wi
0x630	6E	64	6F	77	73	20	39	38	29	6F	72	61	6E	67	65	2F	ndows 98)orange/
0x640	70	61	73	73	76	69	65	77	2E	7A	69	70	77	77	77	2E	passview.zipwww.
0x650	6E	69	72	73	6F	66	74	2E	6E	65	74	61	70	70	6C	65	nirsoft.netapple
0x660	74	78	74	20	68	74	6D	20	68	74	6D	6C	20	73	68	74	txt htm html sht
0x670	6D	6C	00	00	00	00	00	00	00	00	08	00	00	00	00	00	ml..............
0x680	00	00	05	00	00	00	4F	74	68	65	72	00	80	00	00	00	......Other.€...
0x690	00	00	00	40	FE	EE	2A	D3	49	C5	01	00	00	00	00	94	...@þî*ÓIÅ.....”

Fig. 5. History of download files

contains URL addresses of all downloaded files. In some cases, it also stores download completion time of completely downloaded files prior to the listing of the file URL address. However, login credentials to access the downloaded files are not stored. The second segment contains the *'Site Explorer*' history (websites visited by the user). In some cases, it also holds the access time of each webpage visited in little-endian format. The third segment contains the history of all download directories used by the user to download files.

FDM maintains password-protected websites under the *'Site Manager'* tab as shown in Figure 1. If a user manually deletes entries of websites listed under the '*Site Manager'* tab, it will also erase the contents of that website from a *'Sites.sav'* log file after the user exits FDM. The *'Sites.sav'* log file contains the website address, login credentials, and download group name of each password-protected website. To figure out details of a crime, investigators routinely require login credentials of visited websites used to download the illicit material. Login credentials allow investigators to map the retrieved information with user activity.

FDM provides the ability to download a complete website from a web server using *'HTTP Spider'*. The *'Spider.sav'* file contains entries of all downloaded web pages from a specified website. When a user removes a website from '*HTTP Spider*', all entries of that website are also erased from this log file.

'Downloads.del.sav' holds the contents of the *'Recycle Bin*'. The *'Recycle Bin*' of FDM contains incomplete (in-progress, stopped and scheduled files) and deleted download files. It holds the file name, download directory path, URL address, download start time, group name used to save a file, proxy server address, port, username, and password (if required to download the file). Investigators must know that the FDM '*History*' only contains completely download files and the *'Recycle Bin'* contains the incomplete and deleted files.

4 Forensic Examination of RAM and Swap Files

A number of FDM "footprints" appear in RAM in addition to log files and the Windows registry. These can provide links of multiple internet activity record files (cookies, temporary files and internet temporary files) used during the download process.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00801400	31	39	32	2E	31	36	38	2E	32	35	2E	31	3A	38	30	38	192.168.25.1:808
00801410	30	00	00	00	00	00	00	00	03	00	04	00	4B	01	0E	01	0.....K...
00801420	70	61	73	73	5F	68	74	74	70	00	00	00	00	00	00	00	pass_http.....
00801430	03	00	03	00	4E	01	0D	01	41	64	6D	69	6E	5F	68	74	....N...Admin_ht
00801440	74	70	00	00	00	00	00	00	02	00	03	00	41	01	0F	01	tp.....A...

Fig. 6. Proxy settings in RAM

Table 3. Instances of forensic artefacts within RAM

Artefacts	Instances in RAM
Download directory path	6-8 times
URL Address	2-3 times
Login credentials	2-3 times
Proxy login credentials	10-12 times
Site names / address	2-3 times

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
03F1ECF0	0B	03	64	00	6C	00	6D	00	67	00	72	00	73	00	69	00	..d.l.m.g.r.s.i.
03F1ED00	2E	00	73	00	61	00	76	00	40	00	00	00	28	00	00	00	..s.a.v.@...(...
03F1ED10	00	00	00	00	00	00	04	00	10	00	00	00	18	00	00	00	.....
03F1ED20	0E	12	9D	66	80	B5	D9	11	84	3D	00	05	5D	4D	4C	09	..f.µÙ..=..]ML.
03F1ED30	80	00	00	00	D8	00	00	00	00	00	18	00	00	00	01	00	....Ø.....
03F1ED40	BC	00	00	00	18	00	00	00	09	00	00	00	05	00	00	00	¼.....
03F1ED50	1D	00	00	00	44	3A	5C	48	61	63	6B	65	72	73	20	43	....D:\Hackers C
03F1ED60	6F	72	6E	65	72	5C	52	65	67	56	69	65	77	2E	7A	69	orner\RegView.zi
03F1ED70	70	1A	00	00	00	44	3A	5C	48	61	63	6B	65	72	73	20	p....D:\Hackers
03F1ED80	43	6F	72	6E	65	72	5C	77	6F	72	64	2E	7A	69	70	29	Corner\word.zip)
03F1ED90	00	00	00	44	3A	5C	46	6F	72	65	6E	73	69	63	20	54	...D:\Forensic T
03F1EDA0	6F	6F	6C	73	73	73	73	73	5C	41	6E	61	6C	79	73	69	oolssssss\Analysi
03F1EDB0	6E	67	20	65	6D	61	69	6C	2E	64	6F	63	21	00	00	00	ng email.doc!...
03F1EDC0	44	3A	5C	46	6F	72	65	6E	73	69	63	20	54	6F	6F	6C	D:\Forensic Tool
03F1EDD0	73	73	73	73	73	5C	77	68	6F	69	73	74	64	2E	7A	69	sssss\whoistd.zi
03F1EDE0	70	1F	00	00	00	44	3A	5C	48	61	63	6B	65	72	73	20	p....D:\Hackers
03F1EDF0	43	6F	72	6E	65	72	5C	73	64	61	72	74	69	63	6C	65	Corner\sdarticle
03F1EE00	2E	70	64	66	00	00	00	00	FF	FF	FF	FF	82	79	47	11	.pdf....ÿÿÿÿ.yG.

Fig. 7. Content of Dlmgrsi.sav in RAM

WinHex [12] is available for forensic examination of RAM in Windows operating systems and was used in this case to investigate FDM instances in RAM. Artefacts located within RAM and swap files can give a very clear indication of URL addresses, download directory paths, login credentials, install location, path of log files, group name and their supported extensions. Figure 6 illustrates that RAM also contains proxy settings, including: proxy address, port number, and login credentials for HTTP protocol. The artefacts found in RAM can be used to support and strengthen evidence found in the Windows registry as described in section 2.

In addition to large number of files found in unallocated clusters, a large number of references to the victim's Login-ID were also located within swap files, including URL address of downloaded files. Data found in RAM fragments is scattered and have no particular order meaning recreation of download activity is difficult. Table 3 describes the number of times the artefacts (e.g. Download directory path, URL

address, login credentials required to download file, proxy settings, and websites) occur in the RAM.

Search keywords can aid discovery of FDM-specific information in the RAM and swap files. During examination, different helpful search words were explored for the investigator, such as, the default directory location of log files *'C:\ Documents and Settings'*, cookies related to downloaded files *'Cookie:'*, visited URL addresses *'Visited:'*, specific protocol search *'http://'*, web pages visited *'www.'*, IP addresses of proxy servers *'xxx.xxx.xxx.xxx'*. The keyword search for password and groups does not provide enough information to the forensic investigator. Analysis also revealed that the *'Dlmgrsi.sav'* file contents as discussed in section 3 are found twice in the RAM as shown in Figure 7.

5 Conclusion

Analysis of FDM revealed that all artefacts of FDM download activities are grouped together under a single path both in the Windows registry and directory structure. The Windows registry contains configuration and user settings under the *'HKEY_USERS\SID\ Software\VicMan Software \Free Download Manager'* registry key. In addition, FDM stores log files of each user at a default location: *'C:\Documents and Settings\User Profile\Application Data\Free Download Manager'*. The potential evidence that resides in the log files and registry is a significant forensic resource. However, it should be recognized that attackers can also exploit this information, thus making it a single point-of-failure. An anti-forensic tool could also be developed to delete the forensic artefacts from the registry and log files. Digital forensic investigators can find the '*Dlmgrsi.sav*' and '*History.sav*' log files extremely useful even if a user has removed traces of all downloaded files from *'All Groups'* and *'History'*. By linking registry entries and log files information, it creates a clearer picture of suspected download activity.

References

1. Download Manager (2004), http://en.wikipedia.org/wiki/Download_manager
2. Comparison of download managers (2004), http://en.wikipedia.org/wiki/Comparison_of_download_managers
3. Honeycutt, J.: Microsoft Windows Registry Guide, 2nd edn., pp. 570–578. Microsoft Press (2005)
4. Wong, L.W.: Forensic Analysis of the Windows Registry, Forensic Focus (2007), http://www.forensicfocus.com/index.php?name=Content&pid=73&page=1
5. Description of the Microsoft Windows Registry, Help and Support, Microsoft Corp (2007), http://support.microsoft.com/kb/256986/
6. Registry Quick Find Chart, AccessData Corp (2006), http://www.accessdata.com/support/white%5Fpap
7. Vivienne, M., Theodore, T., Iain, S.: The Windows Registry as a forensic artefact: Illustrating evidence collection for Internet usage. Digital Investigation 3(3), 166–173 (2006)

8. Derrick, J.F.: A Forensic Analysis of the Windows Registry (2007), http://www.eptuners.com/forensics/contents/A_Forensic_Examination_of_the_Windows_Registry_DETAILED.pdf
9. Registrar Registry Manager 6.02 (Lite Edition), http://resplendence.com/download/rrtri.exe
10. Registry Viewer 2.0, http://www.mitec.cz/Downloads/RegView.zip
11. Carvey, H.: The Windows Registry as a forensic resource. Digital Investigation 2(3), 201–205 (2005), http://www.sciencedirect.com/science/article/B7CW4-4GX1J3B-1/2/6f94db2adc419ceacce8e3-66614ad34f
12. WinHex 15.3, http://www.x-ways.net/winhex.zip