

Study on Pagefile.sys in Windows System

Nisarg Trivedi

Institute of Forensic Science, Gujarat Forensic Sciences University, Gujarat, India

Abstract: Pagefile.sys is a file that is used by Microsoft Windows to store frames of memory that do not currently fit into physical memory. It means Windows uses a page file to store data that can't be held by your computer's random-access memory when it fills up. Analysis of the Pagefile.sys gives the information of which events were done on PC. Analysis of Pagefile.sys can give the sensitive information such as User Ids, Passwords, Hidden Processes, Download info, Search Activity of Browser etc. This Paper represents various approaches and tools used to capture and analyze data from Pagefile.sys.

Keywords: Physical Memory, Artifacts in Pagefile.sys, Sensitive information.

I. Introduction

Windows uses part of your hard drive space as "virtual memory" [7]. It loads what it needs to load into the much faster RAM (random access memory) memory, but creates a swap or page file on the hard drive that it uses to swap data in and out of RAM [7]. Pagefile.sys is located on the root of C: drive (or in where the Operating System is installed) and is named as pagefile.sys, but it is a hidden system file so you won't see it unless you have changed your file viewing settings to show hidden and system files [7]. Pagefile.sys is a windows system files, acts as swap file and was designed to improve performance [8].

Virtual memory allows Windows to open more windows and run more programs simultaneously while only keeping the one being actively used in RAM [7]. The "problem" lies in the fact that information remains in the page file. As you use different programs and perform different functions on your computer the page file may end up containing all sorts of potentially sensitive or confidential information [7]. Event Log Records, like other data, may be found within the Pagefile or within unallocated space [1].

II. Myth about Pagefile.sys

Disabling the Page File Improves Performance [3].

Some people will tell you that you should disable the page file to speed up your computer [3]. The thinking goes like this: the page file is slower than RAM, and if you have enough RAM, Windows will use the page file when it should be using RAM, slowing down your computer [3].

This isn't really true. People have tested this theory and found that, while Windows can run without a page file if you have a large amount of RAM, there's no performance benefit to disabling the page file [3]. However, disabling the page file can result in some bad things [3]. If programs start to use up all your available memory, they'll start crashing instead of being swapped out of the RAM into your page file [3]. This can also cause problems when running software that requires a large amount of memory, such as virtual machines [3]. Some programs may even refuse to run [3].

In summary, there's no good reason to disable the page file – you'll get some hard drive space back, but the potential system instability won't be worth it [3]. Note that Cleaning the pagefile.sys at system shutdown increases the performance of the system [6].

III. Management of Pagefile.sys

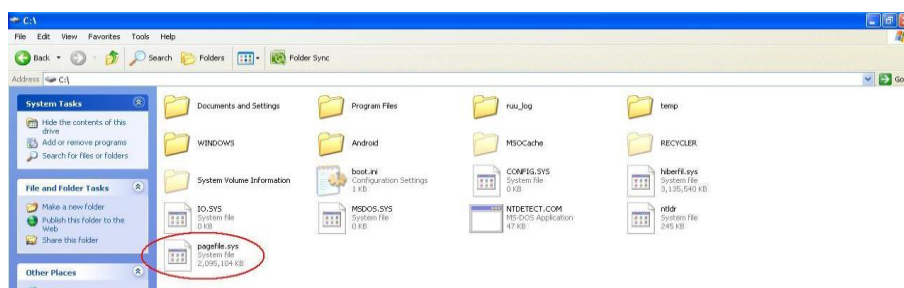


Figure 1: Location of Pagefile.sys in Computer System

The page file isn't use consistently, so some data may linger there for quite some time [2]. Above Figure shows the location of Pagefile in User's Computer System. By default it is generated and Located in same in which the Operating System is installed (You can also change its location). The above Pagefile size is approximately 2.00 GiB. The RAM of the above system is 3.00 GiB.

In Windows XP and 2000, you can clean the file pagefile.sys to improve its overall performance. This can be done by creating or modifying the REG_DWORD value from 1 to 0 in the registry key ClearPageFileAtShutdown [6]. This is located here.

Right Click on MyComputer→Advance Option→ Settings button of Performance→Select Advance→Virtual Memory→Change

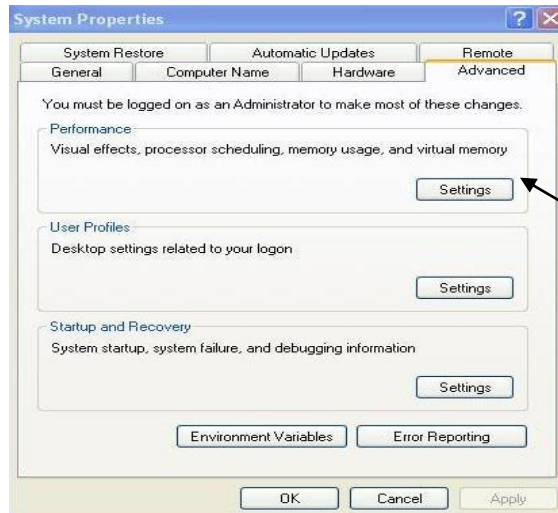


Figure 2: System Property

Click on the Setting Button.

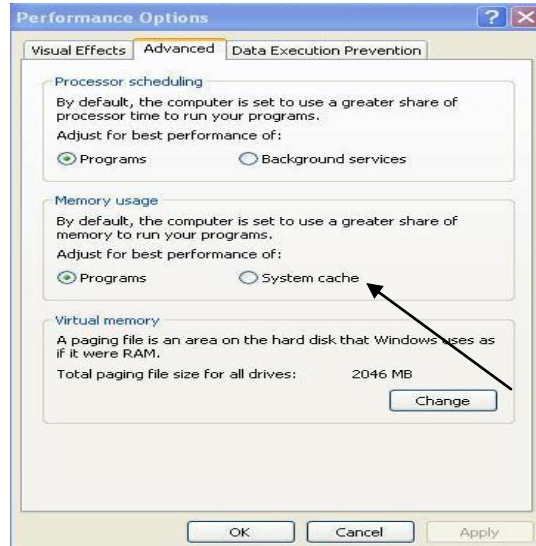


Figure 3: Performance Option

It must be noted that default size of virtual memory is 2046 MB, but with the help of change button, it can be varied as per requirement.

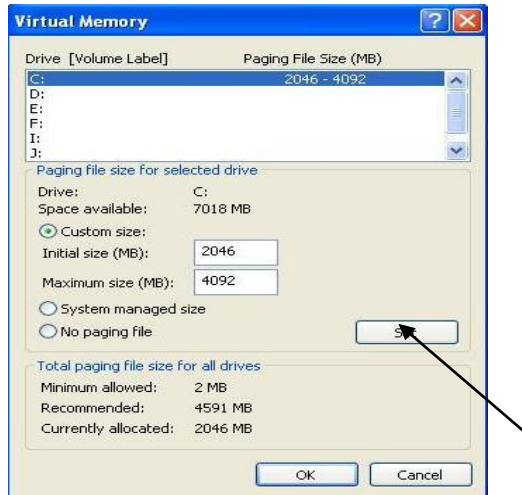


Figure 4: Virtual Memory

In above figure, it can be seen that Operating system is installed in C drive and hence default location of the pagefile.sys is also located in same.

Total paging file sizes for all drives are also mentioned which illustrate minimum allowed size, currently allocated as well as recommended size.

IV. Pagefile.sys Analysis

Below screenshot is taken by using LinuxReader software [4]. We can read pagefile.sys by using this software. Information which can be gathered is mentioned below. Pagefile could be read in LinuxReader software in Text/Binary/Hex/Unicode etc.

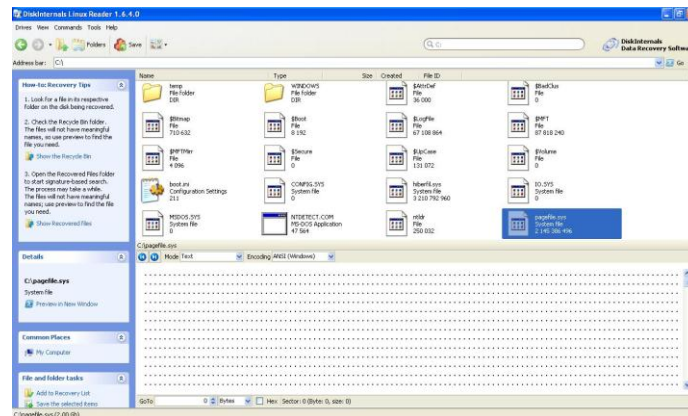


Figure 5: Open Pagefile.sys in Linux Reader Software

```

.....W...õ.....:\ALLUSERSPROFILE=C:\Documents and Settings\All Users.APPDATA=C:\
Documents and Settings\Trivedi's\Application Data.CLIENTNAME=Console.CommonProgramFiles=C:\Program Files\Common
Files.COMPUTERNAME=NISARG.ComSpec=C:\WINDOWS\system32\cmd.exe.FP_NO_HOST_CHECK=NO.HOMEDRIVE=C:.HOMEPATH=
Documents and Settings\Trivedi's.LOGONSERVER=\\NISARG.NUMBER_OF_PROCESSORS=2.OS=Windows_NT.Path=C:\WINDOWS\
system32;C:\WINDOWS;c:\windows\system32\wbem;c:\Program Files\Intel\Wireless\Bin\
.PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH.PROCESSOR_ARCHITECTURE=x86.PROCESSOR_IDENTIFIER=x86
Family 6 Model 15 Stepping 6, GenuineIntel.PROCESSOR_LEVEL=6.PROCESSOR_REVISION=0f06.ProgramFiles=C:\Program
Files.SESSIONNAME=Console.SystemDrive=C:.SystemRoot=C:\WINDOWS.TEMP=C:\DOCUME~1\TRIVED~1\LOCALS~1\Temp.TMP=C:\
DOCUME~1\TRIVED~1\LOCALS~1\Temp.USERDOMAIN=NISARG.USERNAME=Trivedi's.USERPROFILE=C:\Documents and Settings\
Trivedi's.windir=C:\
    
```

Figure 6: Information about Computer in LinuxReader Software

This screenshot gives information about our computer such as, Name of Computer, Number of Processor, Processor Architecture, Processor Level.



Figure 7: Information about Web History in LinuxReader Software

This screenshot describe web history visited through the web browser by user. It can be seen in figure that underlined areas describes links of the websites that have been visited by user through web browser. Other text in figure encrypted form, not readable by examiner. There is also some Useless stuff can be seen in the figure.

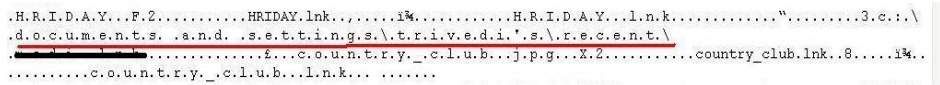


Figure 8: Information about Recent Data in LinuxReader Software

Recent document opened by user is underlined. From Pagefile.sys we can find the recent activity done by the User. Recently visited Folders and Files can be found by investigating Pagefile.sys . It will give all the information of User’s visited file or folder on the System.

HxD is a hex editor, disk editor, and memory editor for Windows. It can open files larger than 4 GiB and open and edit the raw contents of disk drives, as well as display and edit the memory used by running processes. It can calculate various checksums, compare files, or shred files.

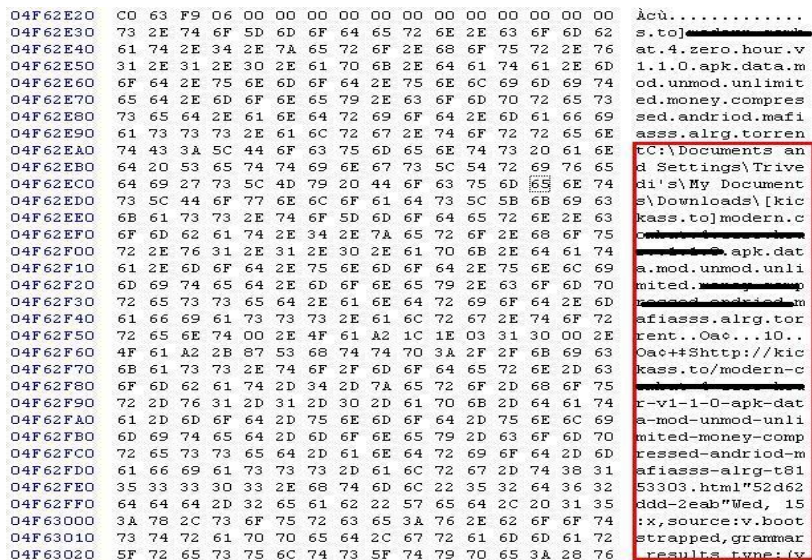
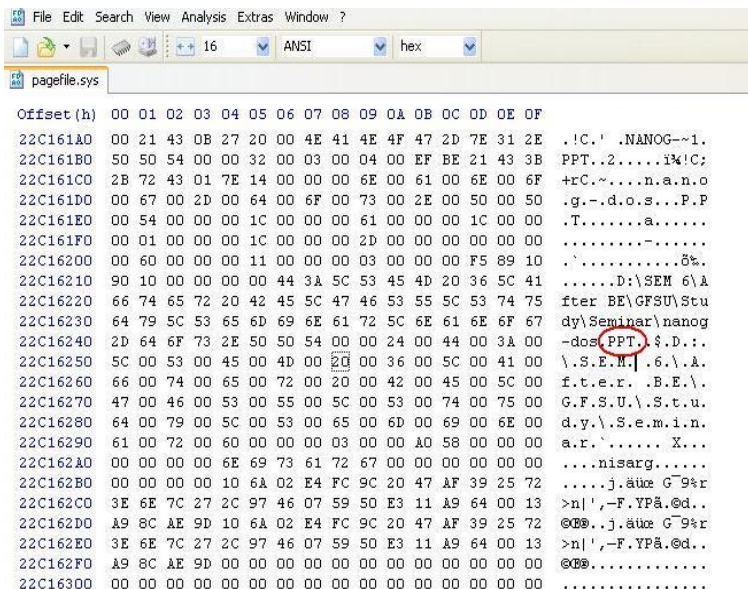


Figure 9: Downloaded Data Information using HxD Software

This screenshot is taken by using HxD Software ^[5]. Downloaded items and its file location with its full path can be seen in the screenshot. Here the downloaded .apk file stored in Downloads Folder located in My Documents of C: drive. All the downloaded data link can be retrieved in Pagefile.sys.

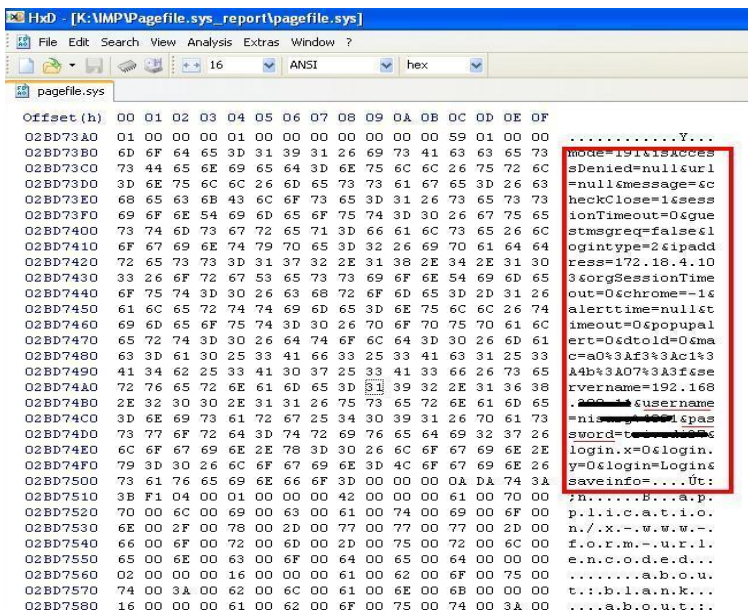


```

File Edit Search View Analysis Extras Window ?
16 ANSI hex
pagefile.sys
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
22C161A0 00 21 43 08 27 20 00 4E 41 4E 4F 47 2D 7E 31 2E  .!C.' .NANOG--1.
22C161B0 50 50 54 00 00 32 00 03 00 04 00 EF BE 21 43 3B  PPT.,2.....i%!C;
22C161C0 2B 72 43 01 7E 14 00 00 00 6E 00 61 00 6E 00 6F  +rC~....n.a.n.o
22C161D0 00 67 00 2D 00 64 00 6F 00 73 00 2E 00 50 00 50  .g~.d.o.s...P.P
22C161E0 00 54 00 00 00 1C 00 00 00 61 00 00 00 1C 00 00  .T.....a.....
22C161F0 00 01 00 00 00 1C 00 00 00 2D 00 00 00 00 00 00  .....-.....
22C16200 00 60 00 00 00 11 00 00 00 03 00 00 00 F5 89 10  .'. .......&%.
22C16210 90 10 00 00 00 00 44 3A 5C 53 45 4D 20 36 5C 41  .....D:\SEM 6\A
22C16220 66 74 65 72 20 42 45 5C 47 46 53 55 5C 53 74 75  fter BE\GFSU\Stu
22C16230 64 79 5C 53 65 6D 69 6E 61 72 5C 6E 61 6E 6F 67  dy\Seminar\nahog
22C16240 2D 64 6F 73 2E 50 50 54 00 00 24 00 44 00 3A 00  -dos(PPT$.D:..
22C16250 5C 00 53 00 45 00 4D 00 20 00 36 00 5C 00 41 00  \.S.E.H.|.6.\.A.
22C16260 66 00 74 00 65 00 72 00 20 00 42 00 45 00 5C 00  f.t.e.e.r. .B.E.\.
22C16270 47 00 46 00 53 00 55 00 5C 00 53 00 74 00 75 00  G.F.S.U.\.S.t.u.
22C16280 64 00 79 00 5C 00 53 00 65 00 6D 00 69 00 6E 00  d.y.\.S.e.m.i.n.
22C16290 61 00 72 00 60 00 00 00 03 00 00 A0 58 00 00 00  a.r.'. .... X...
22C162A0 00 00 00 00 6E 69 73 61 72 67 00 00 00 00 00 00  ....nisarg.....
22C162B0 00 00 00 00 10 6A 02 E4 FC 9C 20 47 AF 39 25 72  ....j.äüç G-9%r
22C162C0 3E 6E 7C 27 2C 97 46 07 59 50 E3 11 A9 64 00 13  >n|',-F.YPä.@d..
22C162D0 A9 8C AE 9D 10 6A 02 E4 FC 9C 20 47 AF 39 25 72  @@@.j.äüç G-9%r
22C162E0 3E 6E 7C 27 2C 97 46 07 59 50 E3 11 A9 64 00 13  >n|',-F.YPä.@d..
22C162F0 A9 8C AE 9D 00 00 00 00 00 00 00 00 00 00 00  @@@.....
22C16300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```

Figure 10: Extension Information using HxD Software

In above figure, it can be seen that we locate a specific file through its extension by entering in a search dialogue box. For example, in above figure “.ppt” has been entered as search criteria and all the files of this extension are achieved. U can also enter “crime” “terrorist” “gun” “hack” etc. (words may be varies through case by case) to check whether there is any file or information related to crime is exist there or not.



```

HxD [K:\NMP\Pagefile.sys_report\pagefile.sys]
File Edit Search View Analysis Extras Window ?
16 ANSI hex
pagefile.sys
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
02BD73A0 01 00 00 00 01 00 00 00 00 00 00 00 00 00 59 01 00 00  .....Y...
02BD73B0 6D 6F 64 65 3D 31 39 31 26 69 73 41 63 63 65 73  mode=191111Access
02BD73C0 73 44 65 6E 69 65 64 3D 6E 75 6C 6C 26 75 72 6C  sDenied=null&url
02BD73D0 3D 6E 75 6C 6C 26 6D 65 73 73 61 67 65 3D 26 63  =null&message=6c
02BD73E0 68 65 63 6B 43 6C 6F 73 65 3D 31 26 73 65 73 73  heckClose=1&sess
02BD73F0 69 6F 6E 54 69 6D 65 6F 75 74 3D 30 26 67 75 65  ionTimeout=0&gve
02BD7400 73 74 6D 73 67 72 65 71 3D 66 61 6C 73 65 26 6C  stmsgreq=false&l
02BD7410 6F 67 69 6E 74 79 70 65 3D 32 26 69 70 61 64 64  ogintype=2&ipadd
02BD7420 72 65 73 73 3D 31 37 32 2E 31 38 2E 34 2E 31 30  ress=172.18.4.10
02BD7430 33 26 6F 72 67 53 65 73 73 69 6F 6E 54 69 6D 65  3&orgSessionTime
02BD7440 6F 75 74 3D 30 26 63 68 72 6F 6D 65 3D 2D 31 26  out=0&chrome=1&
02BD7450 61 6C 65 72 74 74 69 6D 65 3D 6E 75 6C 6C 26 74  alerttime=null&t
02BD7460 69 6D 65 6F 75 74 3D 30 26 70 6F 70 75 70 61 6C  imeout=0&popupal
02BD7470 65 72 74 3D 30 26 64 74 6F 6C 64 3D 30 26 6D 61  ert=0&dtold=0&ma
02BD7480 63 4D 61 30 25 33 41 66 33 25 33 41 63 31 25 33  c=a0%3Af3%3Ac1%3
02BD7490 41 34 62 25 33 41 30 37 25 33 41 33 66 26 73 65  A4b%3A07%3A3f&e
02BD74A0 72 76 65 72 6E 61 6D 65 3D 31 39 32 2E 31 36 38  rvername=192.168
02BD74B0 2E 32 30 30 2E 31 31 26 75 73 65 72 6E 61 6D 65  .!@#$%^&*()~|.-:;
02BD74C0 3D 6E 69 73 61 72 67 25 34 30 39 31 26 70 61 73  =nisarg%1@#$%^&*
02BD74D0 73 77 6F 72 64 3D 74 72 69 76 65 64 69 32 37 26  sword=t%1@#$%^&*
02BD74E0 6C 6F 67 69 6E 2E 78 3D 30 26 6C 6F 67 69 6E 2E  login.x=0&login.
02BD74F0 79 3D 30 26 6C 6F 67 69 6E 3D 4C 6F 67 69 6E 2E  y=0&login=Login&
02BD7500 73 61 76 65 69 6E 66 6F 3D 00 00 0A D4 74 3A  saveinfo=...Ü:
02BD7510 3B F1 04 00 01 00 00 00 42 00 00 00 61 00 70 00  ?h.....B...ä.p.
02BD7520 70 00 6C 00 69 00 63 00 61 00 74 00 69 00 6F 00  p.l.i.c.a.t.t.i.o.
02BD7530 6E 00 2F 00 78 00 2D 00 77 00 77 00 77 00 2D 00  n./x.-.w.w.w.-.
02BD7540 66 00 6F 00 72 00 6D 00 2D 00 75 00 72 00 6C 00  f.o.r.m.-.u.r.l.
02BD7550 65 00 6E 00 63 00 6F 00 64 00 65 00 64 00 00 00  e.n.c.o.d.e.d...
02BD7560 02 00 00 00 16 00 00 00 61 00 62 00 6F 00 75 00  .....a.b.o.u.
02BD7570 74 00 3A 00 62 00 6C 00 61 00 6E 00 68 00 00 00  t:.b.l.a.n.k...
02BD7580 16 00 00 00 61 00 62 00 6F 00 75 00 74 00 3A 00  ....a.b.o.u.t...
  
```

Figure 11: Username and Password using HxD Software

Using this tool we can find lots of sensitive information. I have found the login in to some account which shows the username and password. Like this e-mail addresses could also found.

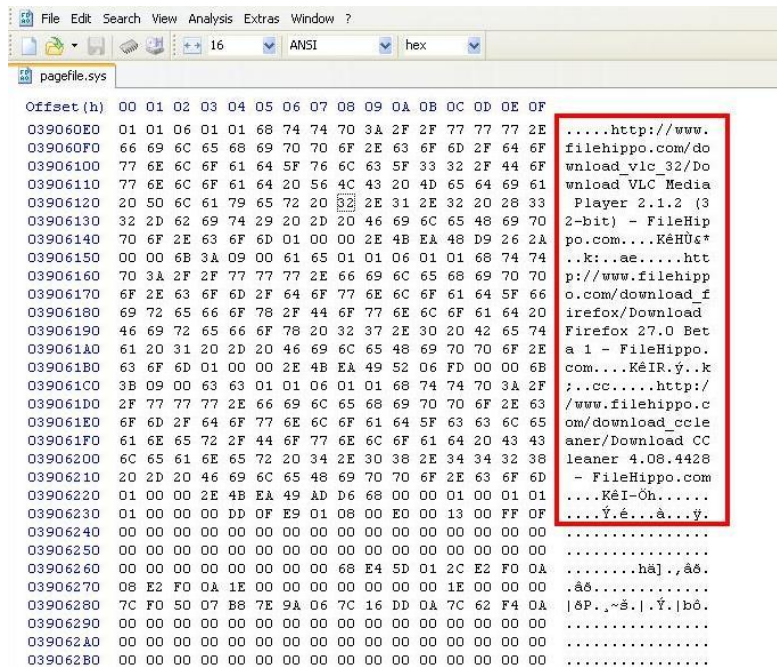


Figure 12: Downloaded Software Information using HxD Software

Above figure shows the download of software from the web link. Software with its version which is downloaded in the system can be found. Like this we can find.

These all are the information which we can get through different tools. The tools which are used for the analysing the Pagefile.sys have their different approach. The above tools are the graphical tools, there are some other tools which also do the Pagefile.sys analysis.

IV. Conclusion

There are so many tools and techniques are available for Pagefile.sys analysis. They all have different methods and different approaches. It is very good to find out the sensitive information from the Pagefile.sys. This is helpful for solving the many crimes related to computer. The data which is stored in the Pagefile.sys are changes repeatedly. Pagefile.sys is also useful for investigation purpose for obtaining information. The tools which are used for analysis have to be developing more powerful with coming years.

References

- [1] Harly Carvey, "Windows Forensic Analysis Toolkit"
- [2] John Sammons, "The Basics of Digital Forensic"
- [3] <http://www.howtogeek.com/126430/htg-explains-what-is-the-windows-page-file-and-should-you-disable-it/>
- [4] Linux Reader Software http://www.freewarefiles.com/DiskInternals-Linux-Reader_program_21787.html
- [5] HxD Software <http://mh-nexus.de/en/hxd/>
- [6] <http://en.kioskea.net/faq/719-pagefile-sys-file>
- [7] <http://netsecurity.about.com/od/windowsxp/qt/aa071004.htm>
- [8] <http://www.neuber.com/taskmanager/process/pagefile.sys.html>