

Professional Forensic Services, LLC
Report of Examination
DATE: November 10, 2023

To: Tim Rote

[REDACTED]
[REDACTED]

Tualatin, OR 97062

RE: Case No 2773

Request: This is a request to process a 122GB Maxtor hard drive and search for evidence of child pornography files.

Specimens:

- 122GB Maxtor IDE hard drive, Serial Number G60C0B6E

Processes:

- Created forensic E01 image of the 122GB Maxtor IDE hard drive, Serial Number G60C0B6E, utilizing FTK Imager v4.7.1.2 and archived to a 128GB SanDisk flash drive labeled DE1.
- Processed the forensic image utilizing Magnet Axiom v7.6.0.37501.
- Conducted search queries, extracted files and created Axium Portable Case.
- Created Final Report.

Summary:

On November 1, 2023, I received the Specimen 122GB Maxtor IDE hard drive from client. Using a Tableau Forensic Writeblocker, I created a forensic E01 image of the Specimen hard drive and archived it to a 128GB SanDisk flash drive labeled DE1. The image was MD5 hash verified. The image was successfully processed with Magnet Axium to include carving for deleted files.

A total of 59,480 image files and 324 video files were extracted. I viewed each of these files and found no child pornography images or videos. Adult pornography video files were found on the drive.

File time stamps from the Specimen hard drive show that files were last created, accessed and or modified on November 12, 2003.

Evidence of possible child pornography was found through LNK and Prefetch files that were carved from unallocated space. LNK files are shortcut files that link to an application or file and can be generated when a user opens a local or remote file or document. Windows creates Prefetch files when an application is first run. These files can show the file names that are opened by a program such as Windows Media Player. The file names associated with these LNK and Prefetch files were indicative of child pornography. Fig 1 depicts two of the recovered LNK files:

ARTIFACT INFORMATION		DETAILS	
Linked Path	D:\x\COPY of __INCOMPLETE__Katherine-young 13 year old pre-teen lolita bounces on a much older mans love muscle(incest rape teen hardcore sex xxx)(1)7cea89335a1f6732d5ff83ab7896c9d20c69f000.mpg	Linked Path	D:\shared_INCOMPLETE__Gay Porn - (Str8 Marine Sex) DYPC 16702 - Older marine fucks his youngeac34daf0e6e700043f10bfacbf4c4d00457004.mpg
Target File Created Date/Time	3/31/2003 9:12:04 PM	Target File Created Date/Time	3/31/2003 7:12:08 PM
Target File Last Modified Date/Time	3/28/2003 6:25:11 PM	Target File Last Modified Date/Time	3/31/2003 8:38:36 PM
Target File Last Accessed Date/Time	4/15/2003 8:31:33 PM	Target File Last Accessed Date/Time	3/31/2003 9:10:10 PM
Target Attributes	FILE_ATTRIBUTE_ARCHIVE	Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Drive Type	DRIVE_FIXED	Drive Type	DRIVE_FIXED
Volume Serial Number	70AE6E52	Volume Serial Number	70AE6E52
Volume Name	d	Volume Name	d
Show Command	SW_SHOWNORMAL	Show Command	SW_SHOWNORMAL
Net Bios Name	nwt-1	Net Bios Name	nwt-1
MAC Address	00:E0:18:72:93:A0	MAC Address	00:E0:18:72:93:A0
Target File Size (Bytes)	71183760	Target File Size (Bytes)	1831920
Artifact type	LNK Files	Artifact type	LNK Files
Item ID	140	Item ID	8812

Fig 1: LNK files

As can be seen in Fig 1, both of these files are linked to a volume labeled D: with a Volume Serial Number of 70AE6E52. I am unable to determine any other identifying information for “Volume D” other than it was used to store various files and folders, including the ones seen in Fig 1. It should be noted that the “INCOMPLETE” files are commonly seen in peer-to-peer file sharing software programs and are video files that are in the process of being downloaded. Although the files are not fully downloaded, they can in some instances be played. Evidence of WINMX was found installed on the Specimen hard drive. WINMX is a peer-to-peer file sharing program. The program was last run on May 7, 2003 at 4:27PM.

Fig 2 depicts the Prefetch file for Windows Media Player:

MATCHING RESULTS (2 of 153)				MPLAYER2.EXE
Application Name	Last Run Date/...	Application Path		Maxtor_122GB.E01
MPLAYER2.EXE	5/7/2003 2:33:30 PM	\DEVICE\HARDDISK\VOLUME1\PROGRAM FILES\WINDOWS MEDIA...	34	PREVIEW FIND \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\RASADHLP.DLL \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\DNSAPI.DLL \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\WINRNR.DLL \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\WLDAP32.DLL \DEVICE\HARDDISK\VOLUME2_XGAY PORN - (STR8 MARINE SEX) DYPC 16702 - OLDER MARINE FUCKS HIS YOUNGE MPG \DEVICE\HARDDISK\VOLUME2_XKATHERINE-YOUNG 13 YEAR OLD PRE-TEEN LOLITA BOUNCES ON A MUCH OLDER MANS LOVE MUSCLE(INCEST RAPE TEEN HARDCORE SEX XXX)(1) MPG \DEVICE\HARDDISK\VOLUME2_XCUTE GAY BOY GETS FUCKED IN THE ASS HARD BY OLDER MAN MPG \DEVICE\HARDDISK\VOLUME2_XOLDER SISTERS GET LESBIEN WITH LITTLE SISTER MPG \DEVICE\HARDDISK\VOLUME1\PROGRAM FILES\WINMX\WINMX.EXE
MPLAYER2.EXE	4/21/2003 8:45:01 PM	\DEVICE\HARDDISK\VOLUME1\PROGRAM FILES\WINDOWS MEDIA...	33	

Fig 2: Prefetch Files

As can be seen in Fig 2 both of the files associated with the LNK files were played in Windows Media Player on the Maxtor hard drive in April and May 2003.

I was also provided with a report titled “Sample Forensics Reports Child Porn.pdf” that contained a number of files with names indicative of child pornography. Fig 3 depicts these types of files from the Sample Forensics Reports Child Porn.pdf:

21) Maxtor HDD\C\Unallocated Clusters

D:\shared__INCOMPLETE__ Young teen fucks 2 guys gets full cum facial lolita rape young sex whore dick pussy anal teenscum hardcore_69_orgy_from_7cea89335a1f6732d5ff83ab7896c9d20c69f000.mpg

22) Maxtor HDD\C\Unallocated Clusters

D:\shared\COPY of __INCOMPLETE__ Teen 16 Year Young Cute Lolita (perfect Tits) Girl Gets Fucked With Cock In Pussy And Sucks French Cumshot (blowjob) Ass779c3f7325ebe62795fc5fe0e4446b1100bb9e00.avi

23) Maxtor HDD\C\Unallocated Clusters

D:\shared\Teen 16 Year Young Cute Lolita (perfect Tits) Girl Gets Fucked With Cock In Pussy And Sucks French Cumshot (blowjob) Ass.avi

34) Maxtor HDD\C\Unallocated Clusters

D:\shared\Gay Sex Video - Anal - Hardhats (Falcon) - Older Muscle Guy Fucks Young Twink - 57 sec.mpeg

36) Maxtor HDD\C\Unallocated Clusters

D:\shared__INCOMPLETE__(Gay Teens - St245#1_001) Older teen kisses, sucks and fucks hairless brother [22m]0d40ba2ea52cff48e19ef2eb3db792a412420042.mpg

37) Maxtor HDD\C\Unallocated Clusters

#E361 An unsigned or incorrectly signed file "C:\DOCUME-1\Max\LOCALS-1\Temp\ICD1.tmp\msaudio.inf" will be installed (Policy=Ignore). Error 0x800b0100: No signature was present in the subject.
[2003/04/01 19:36:39 3048.1]
#-198 Command line processed: "C:\Program Files\Windows Media Player\mplayer2.exe"
"D:\shared__INCOMPLETE__(Gay Teens - St245#1_001) Older teen kisses, sucks and fucks hairless brother [22m]0d40ba2ea52cff48e19ef2eb3db792a412420042.mpg"
#E361 An unsigned or incorrectly signed file "c:\docume-1\max\locals-1\temp\icd1.tmp\msaudio.inf" will be installed (Policy=Ignore). Error 1168:

38) Maxtor HDD\C\Unallocated Clusters

C:\DOCUME-1\Max\LOCALS-1\Temp\ICD1.tmp\msadds32.ax" will be installed (Policy=Ignore). Error 1168: Element not found.
[2003/04/01 19:36:41 3048.1]
#-198 Command line processed: "C:\Program Files\Windows Media Player\mplayer2.exe"
"D:\shared__INCOMPLETE__(Gay Teens - St245#1_001) Older teen kisses, sucks and fucks hairless brother [22m]0d40ba2ea52cff48e19ef2eb3db792a412420042.mpg"
#-024 Copying file "C:\DOCUME-1\Max\LOCALS-1\Temp\ICD1.tmp\msaudio.inf" to "C:\WINDOWS\Downloaded Program Files\msaudio.inf".

Fig 3: Sample Forensics Reports Child Porn.pdf:

All of the files seen in Fig 3 with names indicative of possible child pornography were LNK files carved from unallocated space and were linked to the D: volume.

All of the images and videos that were recovered were fully viewable by me. I was not able to recover any of the videos found with names indicative of possible child pornography. This is likely due to the files being stored on the volume labeled D: and only being played, not saved, to the Maxtor hard drive.

Respectfully Submitted



Joel Brillhart
Professional Forensic Services, LLC