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

To: Tim Rote
[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 Axiom 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 Axiom 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:

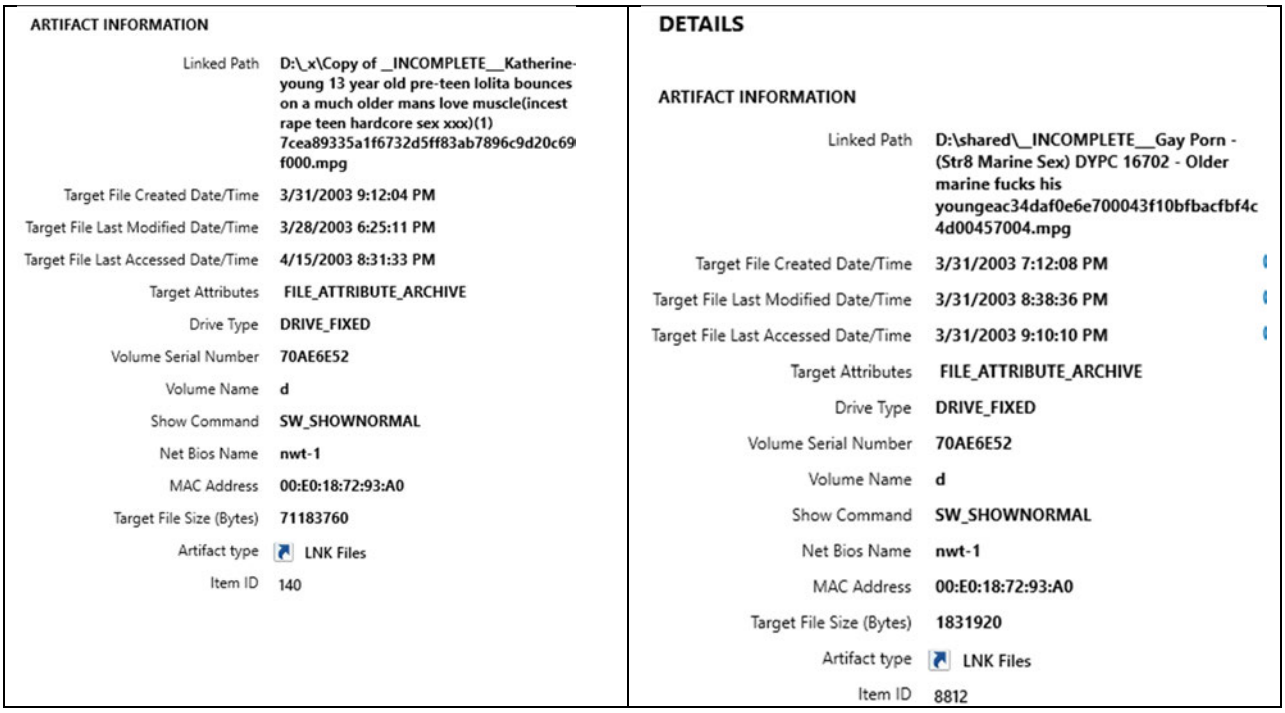

Fig 1: LNK files

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:

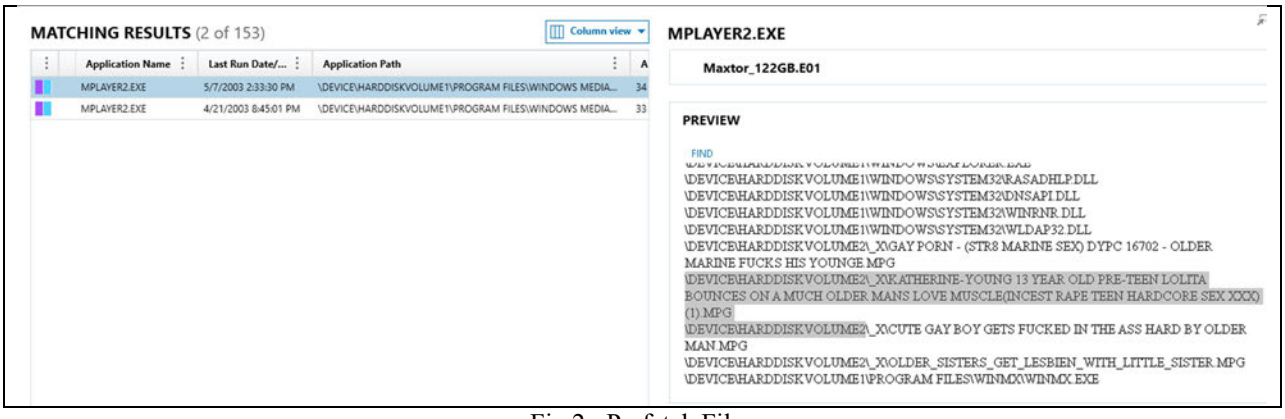

Fig 2: Prefetch Files

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