



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 1 OF 16 PAGES

THIS FOLLOWING IS A PRELIMINARY REPORT OF AN ONGOING FORENSIC EXAMINATION. INFORMATION MAY BE SUPPLEMENTED AS THE EXAMINATION CONTINUES.

FACTS OF CASE

According to investigation reports, on June 23, 2006 at approximately 6:32 a.m, Special Agent Flint Waters used the Phex software to access the Gnutella network. Using search terms consistent with child pornography, SA Waters located 250 files from IP address 65.100.95.9.

On August 9, 2006, a movie file of suspected child pornography was available for download at IP address 71.36.254.55.

A subpoena to Qwest revealed both IP addresses were being used by subscriber Ned Solon at 839 South Melrose during the corresponding dates and times.

On September 18, 2006, SA Balliett obtained a search warrant for 839 South Melrose.

On September 22, 2006 at approximately 1:00 p.m., agents Balliett and Huff interviewed Ned Solon at his place of business. At 1:50 p.m., a search warrant of the residence at 839 South Melrose was conducted.

SA Huff conducted an on-scene preview of Solon's computer on September 21, 2006. However, the investigation report indicates that the search warrant did not take place until the following day. According to SA Huff, the computer revealed a time of 2:38 and a date of September 21, 2006.

Agents Huff and Balliett also previewed Solon's computer on September 22, 2006 and found nothing of evidentiary value.

On September 29, 2006, Huff's continued forensic analysis located 80 files within the Limewire Incomplete folder, many of which contained file names consistent with child pornography. Five of those files were all or partially viewable.

On January 18, 2007, an Indictment was filed charging Ned Solon as follows:

On or about September 20, 2006, in the District of Wyoming, the Defendant, Nathaniel Solon, did knowingly possess a Maxtor hard drive, serial number Y35609QE, containing digital images of child pornography; said digital images including but not limited to an image entitled "[PTHC] Porn_BB Sex_Not Yet 2yos Masturbation Aid_Baby Girl Spreads WIDE For Sex Relief-InfantsPrettyCuntIllegallyFellatedByUnderstandingPedoMErno!!_2.16.mpg" said image being produced using materials, including the Maxtor hard drive, that was mailed, or shipped, or transported in interstate or foreign commerce.

On October 26, 2007, the Prosecutor's Statement was filed with the Court making the following claims:

Examiners were able to recover a total of 8 viewable files from unallocated space on the Defendant's hard drive, 2 of which were duplicates. All of these files were downloaded on September 20, 2006 and subsequently deleted. It appeared from an examination of the Defendant's hard drive that he would download child pornography, view the downloaded files, access software used for copying material from a hard drive to a CD-Rom and then delete the child pornography from the hard drive.

TYPED EXAMINER'S NAME

TAMI L. LOEHR

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

 United States vs. Nathaniel Solon
 07-CR-32-B

PAGE 2 OF 16 PAGES

PURPOSE OF EXAMINATION

Determine if the evidence supports the charges that Ned Solon knowingly possessed digital images of child pornography specifically, the image identified in the Indictment.

EVIDENCE EXAMINED

Item No	Description	Notes
400	120gb Maxtor Hard Drive, S/N Y35609QE	Original evidence in the custody of ICE; forensic examination was conducted on EnCase evidence files provided by Randy Huff

EXAMINATION DETAILS

On March 12, 2008, I traveled to Cheyenne, Wyoming and met with Randy Huff and Nicole Balliett, special agents for the Department of Homeland Security, Bureau of Immigration and Customs Enforcement. I was provided with a forensic image of Item 400 on the Western Digital hard drive that I previously provided identified by serial number WMA8E4557190.

I connected the Western Digital hard drive to a Tableau Forensic SATA/IDE Bridge which was connected to my forensic laptop via USB. I reviewed the contents of the evidence drive which contained 60 EnCase evidence files titled Item 400.E01 through Item 400.E60. I created a new case on my forensic laptop using EnCase 6.8 and added the evidence files to the case.

I ran the Initialize Case feature of EnCase and noted Item 400 has a capacity of 114.5gb but only 14.4gb contained data in active space. The operating system is Windows XP which was installed on 10/21/04 at 10:30 a.m. and registered to Ned Solon. Other than the default accounts created by the Windows operating system, I noted one user account for "Ned Solon". The last logon was 9/21/06 at 2:33 p.m. and the last proper shutdown was 9/21/06 at 2:35 p.m. The time zone was set to Mountain Standard Time and I adjusted the time zone settings in EnCase accordingly.

Name: 400
 ActualDate: 09/23/06 10:36:34AM
 TargetDate: 09/23/06 10:37:04AM
 FilePath: E:\Item 400.E01
 Case Number: 2006-0337
 Evidence Number: 400
 Examiner Name: SA Huff
 Notes: Maxtor 120 GB HD
 Drive Type: DRIVEFIXED
 File Integrity: Verifying
 Acquisition Hash: 6BE5C7EBD7BF122A7DE2B43D736D34EE
 Verify Hash:
 EnCase Version: 3.22g
 System Version: Windows 2000
 Fastblocced: No
 Is Physical: Yes
 Compression: None
 Total Sectors: 240121728

Volume

File System: NTFS Drive Type: Fixed

TYPED EXAMINER'S NAME

TAMI L. LOEHRs

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 3 OF 16 PAGES

Sectors per cluster:	8	Bytes per sector:	512
Total Sectors:	240,091,362	Total Capacity:	122,926,776,320 bytes (114.5GB)
Total Clusters:	30,011,420	Unallocated:	107,481,567,232 bytes (100.1GB)
Free Clusters:	26,240,617	Allocated:	15,445,209,088 bytes (14.4GB)
Volume Name:		Volume Offset:	63
Id:	S-1-5-21-57989841-1482476501-1801674531		
Serial Number:	DC57-2DEC		
Full Serial Number:	14DC5753DC572DEC		
Driver Information:	NTFS 3.1		

OS Info

Product Name:	Microsoft Windows XP
Current Version:	5.1
Registered Owner:	Ned Solon
Registered Organization:	
System Root:	C:\WINDOWS
Current Build Number:	2600
Path Name:	C:\WINDOWS
Product ID:	76487-OEM-0053312-11946
Last Service Pack:	Service Pack 2
Product Key:	
VersionNumber:	
Source Path:	D:\V386
Install Date:	10/21/04 10:30:10AM
Last Shutdown Time:	09/21/06 02:35:29PM

Account Info

User name:	Ned Solon
Full Name:	Ned Solon
Type of User:	Local User
Account Description:	
Primary Group Number:	513
Security Identifier:	S-1-5-21-57989841-1482476501-1801674531-1004
User belongs to group:	Users Administrators
Logon Script:	
Profile Path:	C:\Documents and Settings\Ned Solon
Last Logon:	09/21/06 02:33:06PM
Last Password Change:	08/07/06 10:35:23PM
Last Incorrect Password Logon:	

TimeZone info

Current control set is 002
 Default control set is 002
 Failed control set is 001
 LastKnownGood control set is 003
 Standard time bias is -7:00 hours offset from GMT.
 StandardName: Mountain Standard Time
 Standard time is set to change the Standard bias by 0 minutes.
 Standard time is set to change on Sunday of the 5th week of October, at 02:00 hours.
 DaylightName: Mountain Daylight Time
 Daylight savings is set to change the Standard bias by 60 minutes.
 Daylight savings time is set to change on Sunday of the 1st week of April, at 02:00 hours.
 Active time bias is -6:00 hours offset from GMT.
 The current time setting is -6:00 hours offset from GMT.
 The offset must be either added or subtracted from GMT depending on the time zone location

TYPED EXAMINER'S NAME

TAMI L. LOEHR

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 4 OF 16 PAGES

In addition, I created a new case using Forensic Tool Kit (FTK) version 1.70 on my forensic laptop and added the EnCase evidence files. I unchecked all defaults with the exception of SHA1 hash, File Listing Database and data carve for .bmp, .jpg and .gif and left the processes to run overnight.

Using EnCase, I sorted all files by last access date and noted the last access date and time of 9/21/06 at 2:35 p.m. which is consistent with the search warrant. No files were accessed after the evidence was seized.

I bookmarked the Folder Structure for Item 400 and reviewed installed software applications. I noted the following software applications that might contain information of evidentiary interest:

- Ahead Nero
- Avast Antivirus
- HighMat / Windows XP CD Writing
- Limewire
- Real Player
- Roxio
- Windows Media Player

I reviewed the folder structure for common default folders used by individuals to store data such as My Documents and user-defined folders that might be of evidentiary interest. I noted multiple user-defined folders within the My Documents\My Music folder including Kim, Kim's video, Phoebe, Abbie and multiple picture folders. I also reviewed the Desktop inasmuch as it is common for users to store personal data in this location for easy access. The desktop had four shortcut files including Grand Theft Auto, RiskII, Weather Channel and Limewire. I found nothing of evidentiary value in the naming or contents of any of the common default and user-defined folders.

I reviewed all images using the Gallery view in EnCase and noted 21,031 image files including Windows images and clipart, cached images from Internet browsing, family photos and some adult pornography. I did not find any image files of evidentiary value.

I used FTK to carve images out of unallocated space. FTK reported 60,691 carved images with the total number of images in allocated and unallocated space to be 74,622. Using the Graphics Tab, I reviewed all 74,622 images that included Windows default images and clipart, images from locally installed and on-line games, images cached as a result of Internet browsing, personal photographs and some adult pornography. I did not find any image files of evidentiary value.

I ran the File Mounter to mount compound files such as the thumbs.db. The thumbs.db is a hidden file used in Microsoft Windows that stores a cache for the Window's Explorer's thumbnail view. Thumbs.db is saved in each directory that contains multimedia files. The contents of the thumbs.db files revealed nothing of evidentiary value.

I ran the Recover Folders feature of EnCase and recovered 286 entries but EnCase crashed when I tried to view the recovered folders and they were lost. I attempted to run the process again with similar results. I was unable to complete the Recover Folders process.

I exported registry files including System, SAM, Software, Security and the NTUSER.DAT for user account Ned Solon. Using Registry Viewer, I reviewed the registry files for information of evidentiary value, details to follow.

TYPED EXAMINER'S NAME
TAMI L. LOEHR

ORGANIZATION
LAW2000, INC.

SIGNATURE

DATE
3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 5 OF 16 PAGES

I exported all index.dat files for user account Ned Solon and reviewed them with Net Analysis but I found nothing of evidentiary value. In addition, I reviewed the Internet favorites from the Internet Explorer web browser. The Internet favorites included 3 adult pornography websites including Freegonzo.com but nothing of evidentiary value.

Using FTK, I located 566 emails and I reviewed them all but found nothing of evidentiary value. The Outlook application was opened and Ned Solon's email checked on 5/7/06 at 10:39 a.m, 7/3/06 at 11:49 a.m., 8/30/06 at 6:56 p.m., 9/8/06 at 11:52 p.m., and 9/13/06 at 7:05 pm.

I searched for instant messaging and chat files including MSN, Yahoo, AOL, Google but found nothing of evidentiary value.

Using EnCase, I ran a search for the following keywords, each of which is a phrase contained within the file names that SA Waters claims was available for download at IP address 65.100.95.9, and reviewed the search results.

Hits	First Searched	Last Searched	Search Text
56	03/13/08 09:03:16AM	03/13/08 01:40:54PM	LS-IsLand03
0	03/13/08 09:03:16AM	03/13/08 01:40:54PM	pedo gamine enfant fille
149	03/13/08 09:03:16AM	03/13/08 01:40:54PM	9yo_nude_preteen_girlreelkiddymov
1	03/13/08 09:03:16AM	03/13/08 01:40:54PM	lsbar-001a-015
10	03/13/08 09:03:16AM	03/13/08 01:40:54PM	(2min7sec)
3	03/13/08 09:03:16AM	03/13/08 01:40:54PM	domina lolitas
1	03/13/08 09:03:16AM	03/13/08 01:40:54PM	preston r@ygold
0	03/13/08 09:03:16AM	03/13/08 01:40:54PM	3 pics...12 yr
378	03/13/08 09:03:16AM	03/13/08 01:40:54PM	10yr boy doggyfuck
0	03/13/08 09:03:16AM	03/13/08 01:40:54PM	dee & desi 13
5	03/13/08 09:03:16AM	03/13/08 01:40:54PM	ddoggnprn.mpg
1	03/13/08 09:03:16AM	03/13/08 01:40:54PM	underwear pan.jpg
831	03/13/08 09:03:16AM	03/13/08 01:40:54PM	bilder nudist

LS-IsLand03: although there were 56 hits in unallocated space on Item 400, none of the file names found begin with "kdquality 099" as identified on the search warrant affidavit by SA Waters and therefore, are not the same file he refers to.

pedo gamine enfant fille: the search results for this keyword resulted in no hits.

9yo_nude_preteen_girlreelkiddymov: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file.

lsbar-001a-015: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file.

TYPED EXAMINER'S NAME
TAMI L. LOEHR

ORGANIZATION
LAW2000, INC.

SIGNATURE

DATE
3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 6 OF 16 PAGES

(2min7sec): the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file.

domina lolitas: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music and My Documents\Incomplete. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file. Additionally, because the file existed in the Incomplete folder at one time, Limewire may have completed the download and placed the file into the My Music folder without anyone's knowledge.

preston r@ygold: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file.

3 pics...12 yr: the search results for this keyword resulted in no hits.

10yr boy doggyfuck: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music. In addition, a .lnk file was found in the Recent folder created on 6/22/06 at 9:26 p.m. indicating that this file was opened on this date and date. However, there is no indication when the file was created or deleted or the nature of the content of the file.

dee & desi 13: the search results for this keyword resulted in no hits.

ddoggprn.mpg: although there were 5 hits in unallocated space on Item 400, none of the file names found were an exact match for the file name identified on the search warrant affidavit by SA Waters. The file names that are similar were found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\Incomplete indicating that the files were never completely downloaded onto Item 400. In addition, there is no indication when the files were created or deleted, whether the files were ever accessed, or the nature of the content of the files.

underwear pan.jpg: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file.

bilder nudist: the entire file name identified on the search warrant affidavit containing these keywords was found in unallocated space on Item 400 having once resided in C:\Documents and Settings\Ned Solon\My Documents\My Music and My Documents\Incomplete. However, there is no indication when the file was created or deleted, whether the file was ever accessed, or the nature of the content of the file. Additionally, because the file existed in the Incomplete folder at one time, Limewire may have completed the download and placed the file into the My Music folder without anyone's knowledge.

TYPED EXAMINER'S NAME

TAMI L. LOEHR

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 7 OF 16 PAGES

I ran additional searches for other keywords found within the file names that SA Waters says were available for download but resulted in no hits above. The second search revealed no matches to the file names that SA Waters indicates were available for viewing on 8/9/06 at IP address 71.36.254.55.

Hits	First Searched	Last Searched	Search Text
560	03/14/08 08:06:31AM	03/14/08 08:06:31AM	ssap preteen panties
12	03/14/08 08:06:31AM	03/14/08 08:06:31AM	kindergarden preteen.mpg
0	03/14/08 08:06:31AM	03/14/08 08:06:31AM	collinette dodue lolita

In addition, I ran a search for the SHA value H4VIBLSKAZ477WRTKH7IURE6NXEDCUTI that SA Waters indicates was available for viewing on 8/9/06 at IP address 71.36.254.55. I found the SHA value in unallocated space which identifies the file name as "Pedo - Vicky Compilation (Pthc) 10yo Kiddy Reality Child Get's What She Wants - All Kinds Of Fuck Fun With No Delusions)(14m58s).mpg!" urn:sha1:H4VIBLSKAZ477WRTKH7IURE6NXEDCUTI. However, there is no indication when the file was created or deleted or if the file was ever viewed.

I reviewed each of the software applications that may contain evidentiary value as follows:

LIMEWIRE

Limewire is a free peer-to-peer file sharing software application that uses the Gnutella network to locate and share files with other users on the Gnutella network. I reviewed all data associated with the Limewire application and noted that the software was installed on February 24, 2006 at 3:41 p.m. According to the Limewire.props file, the following locations were selected as the default for saving and searching files:

```
DIRECTORY_FOR_SAVING_FILES=C:\\Documents and Settings\\Ned Solon\\My Documents\\My Music
DIRECTORIES_TO_SEARCH_FOR_FILES=C:\\Documents and Settings\\Ned Solon\\My Documents\\My Music;C
:\\Program Files\\LimeWire\\Jessies;C:\\Documents and Settings\\Ned Solon\\Shared
```

When a file is downloaded using the Limewire application, the completed file is placed into the shared folder identified by the Limewire.props file, which is the My Music folder on Item 400. I reviewed the My Music folder under Ned Solon's user account and found several subfolders including Abbie, Kim, Kim's Videos, Ned, New Folder, etc. Abbie's folder contains music files and album art, mostly children's songs. Kim's folder contains music files and album art; Kim's video folder contains music videos, Ned's folder contains music files and album art, the New Folder contains 3 videos – Tommy Lee and Pamela Anderson and the Paris Hilton sex tape both adult videos created on the hard drive on 9/17/06 at around 5:30 p.m. One other video file called pumpedpussy1.wmv was created on 8/31/06 at 5:57 a.m. but I was unable to play the file to determine the content. I found nothing of evidentiary value in the My Music folder.

If a file is canceled by the user or unable to complete the download process, Limewire automatically creates a folder titled "Incomplete" under the same directory as the shared folder and places the incomplete file in this location. The file name is amended by Limewire with a prefix of "T-#####" (wherein # is a number between 1 and 9) indicating that the file is incomplete.

Although files can not be viewed in Limewire until they are downloaded, a user may preview a file in Limewire once the download process has begun. A preview may or may not function, depending on how much of the file has been downloaded at the time the preview is selected. If the preview functions properly, the user will only see the portion of the file that has completed downloading at the time of the preview. For example, a 5 minute video is selected for

TYPED EXAMINER'S NAME

TAMI L. LOEHR

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 8 OF 16 PAGES

download. Let's assume the file takes 10 minutes to complete the download and 3 seconds into the download process the user selects preview. The user will only see the portion of the file that has downloaded in that 3 seconds. In this case, the file would likely not play because the file does not have enough content to function.

Using Limewire Pro 4.10.9 on my forensics computer, I ran a search for Gwen Stefani, selected several music videos and began the download process. During various stages of the download process I attempted to preview the files. Windows Media Player was launched, as this is my Windows default player, and tried to play the files but I received errors and the files would not play. Although, I was unable to preview any of the files, the preview files were created in the Incomplete folder and the file names were included in the Recent Files list for the Windows Media Player. I then canceled all three files from the download process. [Click here](#) to view screen shots of this process.

I reviewed Item 400 for Incomplete folders and located three of them. Two of the Incomplete folders contained nothing of evidentiary value. The Incomplete folder located at C:\Documents and Settings\Ned Solon\My Documents contained remnants of 80 files. 9 files were of no evidentiary value and included Limewire system files, video games and music files. 21 files have a logical size of 0 which means they are empty files that were never actually downloaded to the hard drive. Of the files that have a logical size greater than zero, 26 of those files are "Preview" video files and 24 files are incomplete video files identified with the "T-#####" prefix. All 50 files have file names indicative of child pornography. However, when I attempted to play all 50 files, 24 files would not play at all so I was unable to determine if the content matched the description of the file name. 12 of the files did not contain child pornography as the file name indicated and most of those 12 files were clearly adult videos. 9 files played but contained blank video, some of which played sound. I was able to play 5 files that contained obvious child pornography which I have identified below, numbered 1-T through 5-T and highlighted in yellow. In addition, a Preview file for each of the five files was found in the Incomplete folder and I numbered those 1-P through 5-P.

No.	Name
1-P	Preview-T-29810688-A PRETEEN- Part 1. 12 Or 13 Year Old Girl Pleasuring Her Pretty Young Young Cunt- Masturbation- preteen sex pedo lolita @ygold.mpg
1-T	T-29810688-A PRETEEN- Part 1. 12 Or 13 Year Old Girl Pleasuring Her Pretty Young Young Cunt- Masturbation- preteen sex pedo lolita @ygold.mpg
2-P	Preview-T-23805952-PTH[C] Porn_BB Sex_Not Yet 2yos Masturbation Aid_Baby Girl Spreads WIDE For Sex Relief-Infants Pretty Cunt Illegally Fellated By Understanding Pedo Mom !!_2.16.mpg
2-T	T-23805952-PTH[C] Porn_BB Sex_Not Yet 2yos Masturbation Aid_Baby Girl Spreads WIDE For Sex Relief-Infants Pretty Cunt Illegally Fellated By Understanding Pedo Mom !!_2.16.mpg
3-P	Preview-T-133785604-[R@ygold style] - R3T3 - many girls from 12yo to 14yo having sex experiences kiddie pedo boy lolita R@ygold underage.mpg
3-T	T-133785604-[R@ygold style] - R3T3 - many girls from 12yo to 14yo having sex experiences kiddie pedo boy lolita R@ygold underage.mpg
4-P	Preview-T-13970280-pthc - vicky english schoolgirl_VERY good underage, xxx, porn, lolita, pedo, incest, preteen.mpg
4-T	T-13970280-pthc - vicky english schoolgirl_VERY good underage, xxx, porn, lolita, pedo, incest, preteen.mpg
5-P	Preview-T-59107332-Babysivid-Samples 3yo gets it every way imaginable (pthc pedo babyfuck)5m46s.mpg
5-T	T-59107332-Babysivid-Samples 3yo gets it every way imaginable (pthc pedo babyfuck)5m46s.mpg

TYPED EXAMINER'S NAME
TAMI L. LOEHRSORGANIZATION
LAW2000, INC.

SIGNATURE

DATE
3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER
United States vs. Nathaniel Solon
07-CR-32-B

PAGE 9 OF 16 PAGES

1-T – This file started downloading at 9:18:44 p.m., was canceled at 9:51:27 p.m. and deleted 21 minutes later at 10:10:17 p.m.

1-P - At 9:19 p.m., approximately one minute into the download, the Preview option in Limewire was selected for 1-T. However, the file that I was able to play during the forensic exam had no video and played only the sound of a door closing. Therefore, there is no evidence that the content of 1-T was ever viewed before the download was canceled and the incomplete file deleted.

2-T – This file started downloading at 9:25:22 p.m., was canceled 37 seconds later at 9:25:59 p.m. and deleted approximately 44 minutes later at 10:10:17 p.m.

2-P – At 9:25:48 p.m., 26 seconds into the download, the Preview option in Limewire was selected for 2-T. However, I was unable to play the file during my forensic exam. Therefore, there is no evidence that the content of 2-T was ever viewed before the download was canceled and deleted.

3-T – This file started downloading at 9:28:01 p.m., was canceled at 9:45:55 p.m. and deleted approximately 15 minutes later at 10:10:17 p.m.

3-P – At 9:28:28 p.m., 27 seconds into the download, the Preview option in Limewire was selected for 3-T. However, I was unable to play the file during my forensic exam. Therefore, there is no evidence that the content of 3-T was ever viewed before the download was canceled and deleted.

4-T – This file started downloading at 9:56:58 p.m., was canceled at 10:01:13 p.m. and deleted approximately 9 minutes later at 10:10:17 p.m.

4-P – At 9:57:21, 23 seconds into the download, the Preview option in Limewire was selected for 4-T. However, I was unable to play the file during my forensic exam. Therefore, there is no evidence that the content of 4-T was ever viewed before the download was canceled and deleted.

5-T – This file started downloading at 9:58:07, was canceled at 10:10:06 p.m. and deleted 11 seconds later at 10:10:17 p.m.

5-P – At 9:59:08; approximately 1 minute into the download, the Preview option in Limewire was selected for 5-T. However, the file size is zero which means the file never had any content and could not be played. Therefore, there is no evidence that the content of 5-T was ever viewed before the download was canceled and deleted.

For a detailed listing of these files including dates and times, [click here](#).

AHEAD NERO

Ahead Nero is a software application that is typically bundled with CD burner hardware and allows users to create, edit and organize multimedia files including the ability to burn files to CD-Rom. I reviewed the [Ahead Nero Registry](#) entries, files and data associated with the Nero software and noted that the version was 6.3.1.4 and was installed on 10/21/04. I reviewed the [NeroHistory.log](#) file which is created automatically by Nero and contains information regarding the software and the history of its use including CD-Rom's burned using the application. This log file was last written to on August 3, 2006 at 10:16 p.m. and the last CD-Rom was burned this date at 10:15:51. A review of the entire log files shows several music CDs burned between February 25 and August 3, 2006. There is no evidence that anything of a pornographic nature was burned to CD-RomM using the Nero software.

TYPED EXAMINER'S NAME TAMI L. LOEHRS		ORGANIZATION LAW2000, INC.	
SIGNATURE	DATE 3/24/2008	EXHIBIT	



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 10 OF 16 PAGES

HIGHMAT / WINDOWS XP

HighMat (High-performance Media Access Technology) is an add-on to the Windows XP CD writing software that allows the user to create disks in a format universally accepted in most DVD players. To facilitate CD recording using the Windows XP software, Windows XP uses a staging area to store the data for recording, which is located in the following hidden folder:

Drive_letter:\Documents and Settings\username\Local Settings\Application Data\Microsoft\CD Burning

I reviewed the CD Burning folder but found no evidence that any CD-Rom's were ever burned using this software.

REAL PLAYER

Real Player is a cross platform media player that can play various multimedia formats including music and video files. Later versions of Real Player included the ability to burn multimedia files to CD-Rom. I reviewed the Real Player Registry entries, files and data associated with the Real Player application and noted that Real Player was installed on 10/29/04. Real Player maintains a history of multimedia files opened using the application and stores this information in the History.log file. When a user attempts to open a file using the Real Player, a .lnk file is created in the history file. However, this is not conclusive evidence that a file was actually viewed inasmuch as an incomplete and non-functional file will create a .lnk file in the Real Player History.log file whether or not the file actually opened. A review of the History.log file revealed several .lnk files with names indicative of child pornography created in August and September, 2006. According to the log file, 2 files were opened on September 20, 2006 at 9:23 p.m. and 9:38 p.m. However, neither of these files was one of the five files that contain child pornography numbered 1-T through 5-T above.

In order to burn files to CD-Rom using the Real Player application, those files must be added to My Library within the Real Player software. I reviewed all files associated with the Real Player software and found no evidence that any of the suspect child pornography files were ever added to My Library or were ever burned to CD-Rom. Additionally, the CDBurning.log file was last written to on August 8, 2006 and contained no data.

ROXIO

Roxio is a software application that is typically bundled with CD burner hardware and allows users to create, edit and organize multimedia files including the ability to burn files to CD-Rom. I reviewed the Roxio Registry entries, files and data associated with the Roxio application and noted that it was installed on 10/29/05. I did not find any evidence that this application was ever used.

WINDOWS MEDIA PLAYER

Windows Media Player is a cross platform media player that comes bundled with the Windows operating system and can play various multimedia formats including music and video files. Later versions of Windows Media Player included the ability to burn multimedia files to CD-Rom. I reviewed the Windows Media Player Registry entries, files and data associated with the Windows Media Player application and noted that it was installed on 10/21/04. Like Real Player, Windows Media Player maintains a history of multimedia files opened using the application and stores this information in the registry. When a user attempts to open a file using the Windows Media Player, the file name is stored in the registry key "RecentFileList". However, this is not conclusive evidence that a file was actually viewed inasmuch as an incomplete and non-functional file will create an entry in the RecentFileList whether or not the file actually opened. A review of the RecentFileList in the registry revealed several files with names indicative of child pornography including files 4-P and 5-P. However, 5-P could not have been viewed in the Windows Media Player because it has a file size of zero.

TYPED EXAMINER'S NAME

TAMI L. LOEHR

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER
United States vs. Nathaniel Solon
07-CR-32-B

PAGE 11 OF 16 PAGES

In order to burn files to CD-Rom using the Windows Media Player application, those files must be added to the Library within the Windows Media Player software. I reviewed all files associated with the Windows Media Player software and found no evidence that any of the suspect child pornography files were ever added to the Library or were ever burned to CD-Rom.

AVAST ANTIVIRUS

Avast Antivirus is a software application that provides detection and removal of unwanted intrusions including viruses, Trojans, worms and other malware. When malware is detected on the system, the software maintains a log of the activity. A review of the antivirus warning log revealed the following entries:

Warning.log

```

8/7/2006 10:10:46 PM 1155010246 SYSTEM 908 Sign of "Win32:Zlob-IV [Trj]" has been found in
"C:\DOCUME~1\NEDSOL~1\LOCALS~1\Temp\tmp1DE.tmp\[Upack]" file.
08/07/2006 10:10:54 PM 1155010254 SYSTEM 908 Sign of "Win32:Renos-H [Adw]" has been found in
"C:\WINDOWS\system32\wviummc.dll" file.
8/7/2006 10:12:01 PM 1155010321 SYSTEM 908 Sign of "Win32:Downloader-gen [Trj]" has been found in
"http://85.255.113.214/1/gdnUS2218.exe" file.
8/7/2006 10:12:13 PM 1155010333 SYSTEM 908 Sign of "Win32:Downloader-gen [Trj]" has been found in
"http://85.255.113.214/1/gdnUS2218.exe" file.
8/10/2006 9:14:37 PM 1155266077 SYSTEM 1504 Sign of "Win32:lstbar-AU [Trj]" has been found in
"http://windowsmedia.licenseupdates.com/license/regular_plugin.exe[UPX]" file.
9/10/2006 7:36:16 PM 1157938576 Ned Solon 1400 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\GTA San Andreas.zip\Setup.exe" file.
9/17/2006 8:14:13 AM 1158502453 Ned Solon 1328 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\EA Sports Madden 2006.zip\Setup.exe" file.
09/17/2006 8:16:50 AM 1158502610 Ned Solon 1328 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\Madden 2006.zip\Setup.exe" file.
09/17/2006 9:52:13 AM 1158508333 Ned Solon 1328 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\Grand Theft Auto - San Andreas.zip\Setup.exe" file.
09/17/2006 11:34:10 AM 1158514450 Ned Solon 1328 Sign of "Win32:VB-IE [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\The Ultimate Fighter S04E05 SDTV XviD-2SD [eztv].zip\Setup.exe" file.
09/17/2006 11:34:43 AM 1158514483 Ned Solon 1328 Sign of "Win32:VB-IE [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\The Ultimate Fighter S04E02 SDTV XviD-2SD [eztv].zip\Setup.exe" file.
09/17/2006 12:58:53 PM 1158519533 Ned Solon 1328 Sign of "Win32:VB-IE [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\Madden NFL 2004 .zip\Setup.exe" file.
9/17/2006 1:53:38 PM 1158522818 Ned Solon 1100 Sign of "Win32:Adware-gen. [Adw]" has been found in
"C:\WINDOWS\system32\shell32.exe" file.
9/17/2006 1:54:17 PM 1158522857 Ned Solon 1100 Sign of "Win32:Adware-gen. [Adw]" has been found in
"C:\WINDOWS\system32\shell32.exe" file.
9/20/2006 7:55:14 PM 1158803714 SYSTEM 1484 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\GTA San Andres FTP Fast Speed.zip\Setup.exe" file.
09/20/2006 8:05:29 PM 1158804329 SYSTEM 1484 Sign of "Win32:Crypt [Trj]" has been found in "C:\Documents and Settings\Ned
Solon\My Documents\My Music\San Andreas GTA.zip\setup.exe" file.
09/20/2006 8:06:25 PM 1158804385 SYSTEM 1484 Sign of "Win32:Trojano-G [Trj]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\Incomplete\T-233472-GTA San Andreas ISO.exe" file.
09/20/2006 8:08:24 PM 1158804504 SYSTEM 1484 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\EA Sports Madden 2006.zip\Setup.exe" file.
09/20/2006 8:09:00 PM 1158804540 SYSTEM 1484 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\Madden 06.zip\Setup.exe" file.
09/20/2006 8:10:25 PM 1158804625 SYSTEM 1484 Sign of "Win32:Vibpack [Wrm]" has been found in "C:\Documents and
Settings\Ned Solon\My Documents\My Music\Madden 06.zip\Setupt.exe" file.
9/21/2006 2:07:38 AM 1158826058 SYSTEM 1484 Function setifaceUpdatePackages() has failed. Return code is 0xC0000142,
dwRes is C0000142.
9/21/2006 2:07:40 AM 1158826060 SYSTEM 1484 An error has occured while attempting to update. Please check the logs.

```

TYPED EXAMINER'S NAME TAMI L. LOEHRS		ORGANIZATION LAW2000, INC.	
SIGNATURE		DATE 3/24/2008	EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER
United States vs. Nathaniel Solon
07-CR-32-B

PAGE 12 OF 16 PAGES

According to the log, Item 400 was infected with multiple viruses, adware and Trojans during the months of August and September. While viruses and adware are considered unwanted intrusions, the Trojans are of the most concern because of their ability to allow your computer to be controlled by outside sources. A Trojan is described as a piece of software which appears to perform a certain action but in fact performs a very different function. One of the most common functions of a Trojan is to circumvent the computer's security to allow unauthorized access by outside hackers. Additionally, the activity is often difficult to identify because the Trojan often deletes any evidence of its intrusion. Although I was unable to get specific definitions for some of the viruses and Trojans identified in the Warning log, one of the Trojans was defined as follows:

Win32:Zlob-IV [Trj] - The Zlob Trojan is a bakdoor trojan horse that can provide hackers with remote access to your computer. Once installed, Zlob will automatically load on every Windows startup and will attempt to hide its activity by injecting code into explorer.exe. Zlob also has the ability to execute programs and take control of your system.

CONCLUSIONS

I did not find any still images containing suspect child pornography in allocated or unallocated space on Item 400.

I did not find any multimedia files containing suspect child pornography in allocated space.

I did not find any user-defined files or folders in allocated space indicative of accessing, viewing or saving child pornography.

I did not find any emails, chat logs, instant messages or other communications in allocated or unallocated space regarding pornography, children or otherwise.

I found five video files on Item 400 in unallocated space that contain suspect child pornography. All five files were created on 9/20/2006 between 9:18pm and 10:10 p.m. in the Incomplete folder created by Limewire. Based on their location in the Incomplete folder, the download of these files was either cancelled by the user or failed to download in their entirety for some other reason. All five files were deleted on 9/20/06 at 10:10 p.m., shortly after their failure to download. Although each of the five files have corresponding preview files, there is no evidence that any of the previews actually played and therefore, no evidence that the content was ever viewed.

There is no conclusive evidence that any of the five files containing suspect child pornography were ever viewed, saved or copied to another location including storage media such as CD-Rom's. In fact, I found no evidence that any pornography was ever burned to CD-Rom's. Additionally, it does not meet the common sense approach that a user would burn an incomplete file to a CD-Rom since incomplete files play only a portion of the intended content or none at all.

With respect to the file specifically listed in the Indictment, the download of this file was canceled 37 seconds into the download process. The preview of this file was never played because the created and last written times are identical. Additionally, I was unable to play the preview file during my exam. There is no evidence that this file was ever viewed, saved, copied or otherwise knowingly possessed prior to the file being deleted.

TYPED EXAMINER'S NAME TAMI L. LOEHR		ORGANIZATION LAW2000, INC.	
SIGNATURE		DATE 3/24/2008	EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER
United States vs. Nathaniel Solon
07-CR-32-B

PAGE 13 OF 16 PAGES

There is no evidence that four of the files SA Waters claims were available at IP address 65.100.95.9 ever existed on Item 400. The remaining file names appear in unallocated space but there is no evidence to determine when the files were created, when they were deleted or if they were ever viewed.

There is conclusive evidence that individuals other than Ned Solon used the computer including, but not limited to, Kim, Phoebe, Jessie, Savannah and Kody. In fact, Savannah was using Ned Solon's email address to email many different individuals and the only evidence that it was not Ned Solon sending the email is when Savannah specifically stated in the email that it was her at the keyboard.

There is conclusive evidence that Item 400 was compromised with Trojans that have the ability to allow unauthorized access to the system by outside sources. However, at this point in my forensics exam, I have been unable to determine to what extent these Trojans compromised the system, if any.

FORENSIC TOOLS USED

Hardware

Forensic Computer – Dell Latitude D30
2.2ghz Intel Core Duo processor
4gb RAM
Windows XP Professional
Tableu IDE/SATA Write Blocker

Software

FTK Version 1.7.0 build 07.01.09
EnCase Version 6.8
Registry Viewer Version 1.4a
Mount Image Pro Version 2
Net Analysis Version 1.37

DISCLOSURE REVIEWED

1. Indictment dated 01/18/07
2. CD-Rom's dated 3/23/07 titled Ned Solon File List CD (1 and 2 of 2)
3. CD-Rom titled Log Files, US v. Solon, US Exhibits
4. CD-Rom dated 03/12/08 titled Solon Files
5. Printed log files (Government's Exhibit 24)
6. Printed log files (pages 1-32)
7. Application and Affidavit for Search Warrant; Search Warrant
8. Report of Investigation (Bates 500001-500012)
9. Interviews of Ned Solon

TYPED EXAMINER'S NAME TAMI L. LOEHRS	ORGANIZATION LAW2000, INC.	
SIGNATURE	DATE 3/24/2008	EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 14 OF 16 PAGES

10. Prosecutor's Statement dated 10/26/07

THIS REPORT CONTAINS HYPERLINKS TO SUPPORTING DOCUMENTATION INCLUDED ON THE ATTACHED CD-ROM.

GLOSSARY OF COMPUTER TERMS

The following are common computer terms that may be used in this report:

ALLOCATED SPACE: Allocated, or used, space is the area of a hard disk that holds files that are recognized by the operating system. This recognition is accomplished via a file allocation table of some type. Different types of operating systems use different types of allocation tables to keep track of files.

COMPUTER EVIDENCE: Computer evidence is unique when compared with other forms of "documentary evidence." Unlike paper documentation, computer evidence is fragile, and a copy of a document stored in a computer file is identical to the original. Thus, the legal "best evidence" rules change when it comes to the processing of computer evidence.

COMPUTER FORENSICS: Computer Forensics deals with the preservation, identification, extraction, interpretation and documentation of computer evidence. Like any other forensic science, computer forensics involves the use of sophisticated technology, tools and procedures that must be followed to guarantee the accuracy of the results. Typically, computer forensic tools exist in the form of computer software and hardware write-blocking devices. Computer forensic examiners guarantee the accuracy of evidence processing results through the use of time tested procedures, and through the use of validated software tools from independent developers.

FILE SLACK: Files are created in varying lengths depending on their contents. Windows based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or more clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called "file slack". File slack potentially contains randomly selected bytes of data from computer memory. This happens because Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. This randomly selected data from memory is called "RAM slack" because it comes from the memory of the computer. RAM slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in RAM slack can come from work sessions that occurred in the past. It should be noted that the newer versions of the Windows operating system zero out (write all zeros to) the RAM slack when a file is created. RAM slack pertains only to the last sector of a file. If there are additional, unused sectors between the last sector of the file and the end of the cluster, this is called "drive slack." Unlike RAM slack, which comes from memory, drive slack is made up of the data that was stored on the storage device prior to the file in question. Such data could contain remnants of previously deleted files.

GB: A Gigabyte (GB) is a unit of computer memory or storage capacity equal to 1,073,741,824, or roughly one billion, bytes or characters. One gigabyte of storage space is the equivalent of 500,000 double-spaced pages of text. Hard disks capable of storing one-hundred gigabytes of data are now commonplace in desktop computers. Such storage devices could contain the equivalent of 50 million pages of data.

TYPED EXAMINER'S NAME

TAMI L. LOEHRS

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT



EXAMINATION REPORT

CASE NAME / NUMBER
United States vs. Nathaniel Solon
07-CR-32-B

PAGE 15 OF 16 PAGES

INSTANT MESSAGING (IM) : IM is a text-based computer conversation over the Internet between two or more people who must be online at the same time, and who must be using the same instant messaging system. Current, popular IM systems are AOL's Instant Messenger (AIM), AOL's ICQ, Microsoft's MSN Messenger and Yahoo! Messenger.

JPG/JPEG: Joint Photographic Experts Group (JPEG or shortened to JPG) is a compressed format for storing bitmap images, and is one of the most common image formats used on the Internet. Other common image formats include ART, BMP, GIF(F), and TIF(F).

KB: A kilobyte (KB) is a unit of computer memory or storage capacity equal to 1,024 bytes or characters.

MB: A megabyte (MB) is a unit of computer memory or storage capacity equal to 1,048,576, or roughly one million, bytes or characters.

METADATA: Metadata can be described simply as "data about data", or as a hidden level of information embedded in a file and maintained by the application that created the file. For example, Microsoft Word documents contain metadata showing the author of the file, the author's company, the number of file revisions, total editing time, and its own set of created, accessed and written dates. Most digital cameras save images with metadata embedded in the file showing the make and model of the camera, the date and time the photograph was taken, and the values of many of the camera's settings, such as exposure, flash, focal length, etc.

OPERATING SYSTEM (OS): An OS is set of software programs used by a computer to manage its own resources, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral device~ such as disk drives and printers. Examples of operating systems are Windows 98, Windows XP, Mac OSX, Linux, and Unix. The OS is the core of the computer's operation, and application programs such as word processors run on top of it.

PAGEFILE.SYS: The page file is a special file used by windows for holding temporary data which is swapped in and out of physical memory in order to provide a larger virtual memory set. In a Microsoft Windows NT, Windows 2000 and Windows XP environment, the file name is pagefile.sys and it is created during setup in the Root of the boot drive as a hidden file. It will not show up on an Explorer file listing unless you toggle off the "Hide system Files" option.

PARALLEL ATA (PATA): For many years, Parallel ATA was the most common disk drive interface. Serial ATA has now become the preferred disk drive interface due to its faster speed, smaller connector, and longer cable length. When Parallel ATA was first introduced, it was an important advancement because it provided controller electronics on the drive itself, eliminating the need for a separate adaptor card. It was easy to configure and was relatively inexpensive compared to its traditional rival, SCSI. PATA uses 40-pin ribbon cables with a maximum length of 18 inches and a maximum transfer rate of 133 MB/second.

PEER-TO-PEER (P2P) : P2P allows a sharing and delivery of user specified files among groups of people who are logged on to a file-sharing network. Napster was the first mainstream P2P software that enabled large scale file sharing. P2P networks are used to share multimedia files, such as music and movies. Typically, users place files they want to share with others in a "shared" folder on their computer. To access a P2P network you need to download, install and run a P2P tool (P2P client software). *The P2P software allows users to search for the types and names of files they are interested in downloading. Examples of current, popular P2P software are Kazaa and Grokster (FastTrack network), Limewire and BearShare (Gnutella network), eDonkey and Overnet (eDonkey/Overnet network), and BitTorrent (BitTorrent network).

TYPED EXAMINER'S NAME TAMI L. LOEHRS		ORGANIZATION LAW2000, INC.	
SIGNATURE	DATE 3/24/2008	EXHIBIT	



EXAMINATION REPORT

CASE NAME / NUMBER

United States vs. Nathaniel Solon
07-CR-32-B

PAGE 16 OF 16 PAGES

RAM: RAM, or Random Access Memory, is a type of memory that can be written to and read from in a nonlinear (random) manner. When a computer program or application is opened, it is transferred from the hard drive to RAM where it is more readily accessible. RAM enhances system performance because it can process requests from the CPU much more quickly than the hard drive. The kind of RAM used in main memory on most computers is Dynamic RAM (DRAM). DRAM stores data as electronic signals that must be constantly refreshed to keep them from dissipating. The data held in PAM is lost when the computer is turned off.

UNALLOCATED SPACE/CLUSTERS: Unallocated space is the area of a hard disk that is not currently occupied by saved files, but is free to have data written to it. Unallocated file space can contain the entire or partial content of deleted files, deleted folders, and temporary files that were transparently created and deleted by computer applications and the operating system. With manual or automated methods, it is often possible to "unerase" deleted files and view the original content so long as the data area of the file has not been overwritten by other data, such as from a newer file.

URL: Uniform Resource Locator (URL) is the address of a resource on the Internet. World Wide Web URLs begin with <http://>

TYPED EXAMINER'S NAME

TAMI L. LOEHR

ORGANIZATION

LAW2000, INC.

SIGNATURE

DATE

3/24/2008

EXHIBIT