UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

---

UNITED STATES OF AMERICA,

v. Case No. 13-MJ-00449-WEC

DECRYPTION OF A SEIZED
DATA STORAGE SYSTEM,

Defendant.

---

## AFFIDAVIT OF ROBIN SHELLOW IN SUPPORT OF MOTION TO VACATE OR STAY THIS COURT'S ORDER OF MAY 21, 2013

---

STATE OF WISCONSIN )
) ss.
COUNTY OF MILWAUKEE )

I, Robin Shellow, being first duly sworn on oath depose and say:

1. I was retained by Jeffrey Feldman on January 25th, 2013.

2. During the execution of the search warrant Feldman advised the agents that he did not wish to speak to them without a lawyer, thus invoking his Fifth Amendment privilege himself which I later confirmed in my letter of January 28, 2013 to Assistant United States Attorney Jonathan Koenig. (Exhibit A.)

3. I did not know which Assistant United States Attorney, if any, was assigned to this matter so on or about January 28th, 2013, I contacted Assistant United States Attorney Jonathan Koenig to ascertain who the Assistant United States Attorney was assigned to this case and conveyed that I represent Jeffrey Feldman and that if a warrant was issued I would produce him immediately. On January 30, 2013, I received an email from Assistant United States Attorney Jonathan Koenig stating that he had

EXHIBIT
1

forwarded my letter of January 28, 2012 to Assistant United States Attorney Moreno-Taxman as she was assigned to this case. (Exhibits A & B, 1/28/13 Letter to AUSA Jonathan Koenig, 1/30/13 Email response from Jonathan Koenig, 2/4/13 Email correspondence between undersigned counsel and AUSA Moreno-Taxman.[1])

4. Based on my observation of Jeffrey Feldman and experience in this area, Jeffrey Feldman sought professional assistance on January 25, 2013, completed that professional assistance and returned to work at Rockwell Automation shortly thereafter. This information was provided to Assistant United States Attorney Koenig initially and subsequently to Assistant United States Karine Moreno-Taxman. (Exhibits A & B)

5. Sometime in February or March of 2013 when I appeared in either Case No. 2011-CR-7 or 12-CR-213, or at another time when I was in the Federal Building on non-Court related business, I encountered Assistant United States Attorney Moreno-Taxman in the hallway where she advised me that she was considering using the All Writs Act to compel decryption, but had not yet made any final decisions.

6. I reminded Assistant United States Attorney Moreno-Taxman that Feldman had sought professional assistance out of state and that he had either returned or would be returning shortly, so that if a warrant was issued, I would surrender him to the United States Marshals.

7. During that conversation, Assistant United States Attorney Moreno-Taxman asked whether my client would voluntarily decrypt the seized items, to which I replied "No". I also advised her that Feldman had invoked his Fifth Amendment privilege through me in a letter that was transmitted to her by Assistant United States

[1] Parts of the 2/4/13 email have been redacted as it contains discussion regarding another case not relevant to this instant matter.

Attorney Jonathan Koenig and that Feldman had also personally invoked his Fifth Amendment privilege during the execution of the search warrant.

8. During that conversation, Assistant United States Attorney Moreno-Taxman used words to the effect that, because Feldman worked in the technology industry the seized items had customized or expert-like encryption. I perceived this statement to be an entreaty for me to confirm her statement. I did not take the bait. Instead, I asked what evidence there was of such specialized encryption and was told she was not willing to disclose that information.

9. On April 19th, 2013 I was advised by Bruce Vilametti of the Milwaukee Journal-Sentinel of the Court's first Order. (Doc. 3).

10. For approximately two weeks following the Court's Order of April 19, 2013, The Shellow Group attempted to discern whether or not counsel could enter her appearance in this matter as it had not been charged. The Government knew I was Feldman's attorney, but to my knowledge the Court did not.

11. Finally, on the advice of my father, Attorney James Shellow, I entered by letter, my Notice of Appearance as an "interested person", something I had never heard of or done before.

12. Since acceptance of my Notice of Appearance I now receive automatic notices of filings in this matter.

13. In preparing to respond/object to the Court's Order of May 21st, 2013 (Doc. 6), I consulted a computer expert who I provided with the three affidavits in this case.

14. The computer consultant provided me with a preliminary opinion as to the accuracy, truthfulness, and completeness of the information contained in the three sworn affidavits to identify *Franks*-like problems. During that conversation I learned the following:

> A. In the world of Peer to Peer (P2P) Networks, when a file is requested to be downloaded, it can be, and many times is, downloaded from multiple sources (computers) in different locations and then reassembled at the client end. This is possible by identifying exactly the same file at different locations using the Sha1 values. This process of downloading pieces from different locations was developed in order to help balance the load on a particular P2P network. In the case of a P2P sting it is desirable to do a "Single Source Download" where the entire file is downloaded from the single target computer because it is possible that the target computer just has the file name and knowledge of what computer the file is on but not the file itself. The "enhanced" P2P software used by OCE 4583 was designed to specifically perform these single source downloads but, apparently, was only able to acquire the Sha1 hash values of the files and or downloads from multiple sources. (Doc. 1, pg. 5, ¶ 12)

B. There is no explanation of where the "dates listed" dates come from.

C. In reviewing paragraphs 10 and 12 of Doc. 1, the expert found that during this investigation OCE 4583 attempted, without success, to conduct single source downloads.

D. It is likely that the length and description of the contents of the two movie files in the Application for the initial search warrant referenced in ¶10, were obtained by OCE 4583 or NCMEC when retrieving copies of the files from their own databases using the Sha1 values and viewing the length and content of the copies, or downloading the files in a non-Single Source Download.

E. The manual does not state anything about locking or damaging the information if too many password guesses are made.

15. Many experts define encryption as the reconstitution or recreation of data as opposed to the unlocking of data.

16. I also spoke with Attorney Chet Kaufman, who litigated *In Re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011; United States v. John Doe,* Case Nos. 11-12268 and 11-15421.

17. Kaufman provided me with the names of potential forensic encryption experts, as well as an organization containing such experts, who meet *Daubert* standards

and where they can be contacted. Retention of an expert with specific qualifications and knowledge in the area of encryption will take time and most likely will require counsel to travel to California to retain such expert. Thus furthering support for this request for a stay should this Court not vacate its Order of May 21, 2013. (Doc. 6).

18. I have also conducted internet research and learned the following on my own:

A. There are thousands of software programs available commercially, that claim to have the capacity to decrypt the various drives seized. (Exhibit C).

B. None of the decryption affidavits suggest that there is any specialized encryption software contained on the seized drives, other than what is ordinarily found on any external hard drive sold at many retail locations, such as Best Buy, Wal-Mart, Office Depot, etc.

C. Western Digital, Maxtor, and Seagate all have master passwords which I found after conducting 4 hours of internet research.

D. The auto setting on e-Mule software requires user to select a box to disable obfuscation.

20. 15 external storage devices and one computer were seized pursuant to the search warrant. It is the Government's theory that Feldman has memorized 16 individual passwords.

21. In paragraph e of the Affidavit in Support of the Application Under the All Writs Act for Compelled Decryption, S.A. Banner failed to advise the Court that passwords can be as long as 36 characters and are often randomly assigned by the device itself, unless and until, they are changed by the user. (Doc. 1-1, pg 3, ¶e) It also fails to

show whether or not the manufacturers were contacted and/or subpoenaed to obtain the device's master password or to assist in decryption.

22. The Government's request to Order the decryption flies in the face of paragraph 20f of the Initial Application for Search Warrant, where the affiant asserts that the seized items must be removed from the residence, as it often takes weeks or months to analyze the drives. (Exhibit D, Doc. 1, 13-M-421)

23. In my own experience representing defendants in child pornography cases in this District, it is not unusual for seized hard drives to take in excess of a year to be analyzed by Federal authorities. Long delays in forensic computer analysis are well documented in every district due to the large number of cases and the relative dearth of qualified government analysts.

24. Feldman in this submission, prior to the deadline of June 4th, 2013, as set by this Court in its May 21, 2013 Order (Doc. 6), submits his invocation of his Fifth Amendment privilege to not incriminate himself as he does not wish to violate the Court Order. It is anticipated that if the current Order remains in effect the Government will seek sanctions that will include incarceration as a penalty for Feldman's invocation and/or re-invocation of his Fifth Amendment privilege.

25. The Government has created a Hobson's choice by forcing Feldman to make a choice between his Fifth Amendment privilege, or face months of incarceration, loss of his job, and discontinuation of his professional assistance, while the Government and Feldman litigate one of the most important constitutional issues of the wired era.[2]

[2] Additionally, if Feldman is convicted he will potentially face enhancements for obstruction of justice pursuant to the advisory sentencing guidelines.

26. This is fundamentally unfair, especially as it relates to Feldman, who has gone out of his way to ensure that the Government knows he will not flee or endanger the public as shown by the disclosure of his professional assistance. Feldman has been under no obligation to advise the Government of his whereabouts during this investigation, but has done so transparently and in good faith.

27. Feldman should not be required to violate the Court's Order in order to litigate that which this Court has labeled an "issue of first impression in the Seventh Circuit". (Doc. 3)

28. The Government is not prejudiced by a full and fair hearing on these issues as it can further its decryption efforts. It is absolutely unnecessary to incarcerate Feldman while this issue of first impression is litigated.

29. In order for Feldman to receive effective assistance of counsel, this matter must be carefully litigated and briefed at every stage. Such litigation requires extensive briefing, evidentiary hearings and expert testimony.

Dated this 31st day of May, 2013.

Respectfully Submitted,

Robin Shellow, #1006052
Counsel for Jeffrey Feldman

Subscribed and sworn to before me
This 31st day of May, 2013.

Notary Public, State of Wisconsin
My Commission Expires:

NOTARY PUBLIC
JEFFREY S.
[illegible]
STATE OF WISCONSIN

TSG

THE SHELLOW GROUP™

www.theshellowgroup.com

324 West Vine Street / Milwaukee, WI 53212
Phone 414.263.4488 / 1.888.SHELLOW / FAX: 414.263.4432

January 28, 2013

Mr. Jonathan Koenig,
Assistant United States Attorney
United States Attorney's Office
517 E. Wisconsin Avenue, Room 530
Milwaukee, Wisconsin 53202

Re: Jeffrey Feldman, Date of Birth 1/12/67

Dear Mr. Koenig:

I am sending you this notice of retainer as I have been unable to ascertain who in your office may be assigned to this case and because you and I have a working relationship and trust that you will be able to ensure that this notice finds its way to the correct person.

Please be advised that I represent Jeffrey Feldman concerning possible criminal charges stemming from the execution of a search warrant at 2051 S. 102nd St., Apt. E, West Allis, Wisconsin on January 24, 2013. Mr. Feldman is currently in treatment and intends to exercise his 5th and 6th Amendment Rights to remain silent and not to be questioned by law enforcement without or until his attorney is present.

Should a warrant be issued for his arrest please advise and I will make arrangements to surrender Mr. Feldman immediately.

Please contact me with any questions. My telephone numbers are: Office: 414-263-4488, Cell: 414-719-9947, Home: 262-285-4700.

Very truly yours,

THE SHELLOW GROUP

Robin Shellow
Attorney for Jeffrey Feldman

cc: United States Marshall's Office
Federal Bureau of Investigations -Milwaukee Div.
Chief of Police Charles Padgett, West Allis Police Dept.

ATTORNEY
ROBIN SHELLOW

Of Counsel:
URSZULA TEMPSKA

Outside Consultant:
R. BRONSON LEVIN, Ph.d
Psychologist

THE SHELLOW GROUP
is Trademark of the
The Shellow Group,
A Sole-Proprietorship

EXHIBIT
A

**Theresa Spalding**

**From:** Koenig, Jonathan H. (USAWIE) <Jonathan.H.Koenig@usdoj.gov>
**Sent:** January 30, 2013 9:53 AM
**To:** rshellow-execpc; Theresa Spalding
**Cc:** Moreno-Taxman, Karine (USAWIE)
**Subject:** Jeffrey Feldman

Robin –

I have forwarded your correspondence of January 28th to Karine Moreno Taxman.

AUSA Jonathan H. Koenig
Appellate Division Chief
U.S. Attorney's Office for the
Eastern District of Wisconsin
517 E. Wisconsin Ave. – Ste. 530
Milwaukee, Wisconsin 53202
T 414-297-4399  F 414-297-1738
jonathan.h.koenig@usdoj.gov

EXHIBIT
B

## Theresa Spalding

**From:** Moreno-Taxman, Karine (USAWIE) <Karine.Moreno-Taxman@usdoj.gov>
**Sent:** February 04, 2013 5:12 PM
**To:** Theresa Spalding
**Subject:** RE: [redacted]

I am out the rest of this week. Maybe Robin and I can talk next week.

**From:** Theresa Spalding [mailto:theresa@theshellowgroup.com]
**Sent:** Monday, February 04, 2013 3:42 PM
**To:** Moreno-Taxman, Karine (USAWIE)
**Subject:** [redacted]

Karine,

After we hung up I gave Robin your message regarding [redacted] and wouldn't you know it she has questions!

1. Can we tell [redacted] about the 5th via a legal call with him?
2. Do you want to meet with her or work with prior to the 5th?
3. I believe Mr. Koenig forwarded a notice of Retainer letter from Robin regarding a Jeffrey Feldman to you for us. Robin just asked that she would like to speak to you about Mr. Feldman prior to any formal charges being filed or a warrant being issued for his arrest and just to remind you that he is currently in treatment so if a warrant for his arrest is issued please contact us and we will arrange to have him produced immediately.

Thank you.

Theresa Spalding
Paralegal
**THE SHELLOW GROUP**
324 West Vine Street
Milwaukee, Wisconsin 53212
Tel: 414-263-4488
Fax: 414-263-4432
Website: www.theshellowgroup.com

The information contained in this email message is intended only for the personal and confidential use of the designated recipient(s) noted above. This message may be attorney-client communication and, as such, is privileged and confidential. If the reader of this message is not the intended recipient, you are notified that you have received this message in error and that any review, dissemination, distribution or copying of this message or the taking of any action in reliance on its contents is strictly prohibited. If you have received this communication in error, please notify us immediately. Thank you.

forensic password decryption

Web More Search tools

About 299,000 results (0.21 seconds)

[Decryption & Password Cracking Software - AccessData]
www.accessdata.com/products/digital-forensics/decryption ▾
AccessData provides state of the art **decryption** and **password** cracking software solutions for law enforcement, federal agencies and corporations.

[Password Recovery & Decryption - Decipher Forensics]
www.decipher**forensics**.com/services/**decryption** ▾
If you have forgotten a **password**, Decipher **Forensics** can help. We are capable of **decrypting** and accessing the protected document or recovering the missing ...

[Password Recovery/Decryption - Computer Forensics Services by ...]
www.cloudninediscovery.com › Services › Computer Forensics ▾
CloudNine Discovery can **decrypt** and recover **password** protected documents and files using very sophisticated technology. We can **decrypt** files created by ...

[Toolkit - Password recovery, forensic, forensics, system and security ...]
www.elcomsoft.com/iphone-**forensic**-toolkit.html ▾
Ltd. offers the complete toolkit for performing **forensic** analysis of encrypted user ... The toolkit includes Elcomsoft Phone **Password** Breaker, the tool to **decrypt** ...

[PDF] [Accelerated Password Decryption Joint Product ... - Tableau, LLC]
www.tableau.com/pdf/PR-TACC_Tableau_AD_Joint_Announcement.pdf ▾
support WinRAR, PGP and other advanced **decryption** techniques. SYSTEM REQUIREMENTS. Accelerated **password decryption** is enabled on **forensic** ...

[Paraben Forensic Software - Passware Kit Forensic]
www.paraben.com/passware-kit.html ▾
**Forensic Password** Recovery Software for over 200+ file types. Paraben's **Decryption** Collection is now Passware Kit **Forensic** by Passware, Inc. This advanced ...

[Scene of the Cybercrime: Computer Forensics Handbook ...]
my.safaribooksonline.com/book/networking/**forensic**...**password**.../312
312 Chapter 6 · Understanding Network Intrusions and Attacks **Password Decryption** Software Most **password**-cracking programs don't actually **decrypt** anything ...

[IncrediMail Password Decryptor - www.SecurityXploded.com]
securityxploded.com/incredimail-**password-decryptor**.php ▾
May 30, 2011 – This makes it useful tool for Penetration Testers and **Forensic** Investigators. IncrediMail **Password** Decryptor works on most of the Windows ...

[PDF] [Password Recovery Kit Forensic 12.3 - Passware]
www.lost**password**.com/pdf/PasswareKit**Forensic**_datasheet.pdf ▾
**Password** Recovery Kit **Forensic** 12.3. All-in-one **password** recovery and encrypted evidence discovery solution. Find.**Decrypt**.Open. Key Benefits. Recovers ...

[ElcomSoft Breaks iPhone Encryption, Offers Forensic Access to File ...]
blog.crack**password**.com/.../elcomsoft-breaks-iphone-encryption-offers-f... ▾
May 23, 2011 – Protected iPhone backups can be broken into with Elcomsoft Phone **Password** Breaker; once **decrypted**, information stored in these backups ...

1 2 3 4 5 6 7 8 9 10 Next

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

EXHIBIT
C

+You Images Maps Play YouTube News Gmail Drive Calendar More

forensic password decryption

Web More Search tools

Page 2 of about 299,000 results (0.21 seconds)

Passware **Password** Recovery Kit **Forensic**
www.lostpassword.com › Forensic Solutions
Passware **Password** Recovery Kit **Forensic** – Reduces time spent on recovering ... to these items using the fastest **decryption** and **password** recovery algorithms.

**Decryption** Service - Passware
www.lostpassword.com › Support
Passware provides an in-house **password** recovery and **decryption** service for more than 200 file types. We use Passware Kit **Forensic** – the very same software ...

Hard Disk **Decryption** - Passware
www.lostpassword.com › Support
Passware Kit Enterprise and Passware Kit **Forensic decrypt** hard disks ... case, Passware Kit assigns brute-force attacks to recover the original **password** for the ...

**Decryption** Tools/ **Password** Breaking, **Decryption** ... - IndiaMART
www.indiamart.com › Computer › Computer Hardware & System
Some of the products sold by the company are **Decryption** Tools/ **Password** Breaking, **Decryption** Tools/ **Password** Breaking Tools, Hard Drive **Forensics**, Hard ...

rack-a-tacc **password decryption** - Digital Intelligence
www.digitalintelligence.com/products/rack-a-tacc/
**Forensic** Computers, Training, Hardware, and Software Solutions for the Computer **Forensics** ... Rack-A-TACC Rack Mounted **Password Decryption** Device ...

Passware Kit **Forensic** Decrypts TrueCrypt Hard Disks in Minutes ...
www.prnewswire.com/.../passware-kit-**forensic**-**decrypts**-truecrypt-hard-...
Passware Kit **Forensic** Decrypts TrueCrypt Hard Disks in Minutes. ... March 30 / PRNewswire/ -- Passware Inc., a provider of **password** recovery, **decryption**, and ...

Passware **Password** Recovery Kit **Forensic** Free Download - Softpedia
www.softpedia.com › Windows › Security › Decrypting & Decoding
1 vote - $995.00 - Windows - Security
Download Passware **Password** Recovery Kit **Forensic** - Complete **password** recovery and e-discovery solution.

Surviving Encryption - SUMURI
sumuri.com/index.php/.../passware-certification-and-**forensic**-training
What is PALADIN **Forensic** Software? ... will learn how to apply **decryption** and **password** recovery techniques in different scenarios, to include, encrypted files, ...

The Best Damn Cybercrime and Digital **Forensics** Book Period - Page...
books.google.com/books?isbn=0080556086
Jack Wiles, Anthony Reyes - 2011 - Computers
Paraben's **Decryption** Collection Enterprise is an advanced **password** recovery suite with support for Windows Vista and Server 2003, EFS, SQL, and Lotus ...

EnCase Computer **Forensics** -- The Official EnCE: EnCase Certified ....
books.google.com/books?isbn=1118058984
Steve Bunting - 2012 - Computers
Windows 2000 EFS can be **decrypted** automatically without input or **password** cracking, since EDS can gather all the information locally needed for automatic ...

**Previous** 1 **2** 3 4 5 6 7 8 9 10 **Next**

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

forensic password decryption

Web More Search tools

Page 3 of about 299,000 results (0.15 seconds)

**Decrypting** the Dropbox filecache.dbx file – new ... - Magnet **Forensics**
www.magnetforensics.com › Press & Events › Blog
Mar 1, 2013 – Support will be added to IEF Standard for **decrypting** this file on a dead box (or **forensic** image) in the near future, but for now we wanted to ...

[PDF] **Decryption & Password** Cracking Software - Cryptome
cryptome.org/2012/01/0006.pdf
Triage. Live Response. **Decryption** and **Password** Cracking. Software http:// accessdata.com/products/computer-**forensics**/**decryption**. 1/3/2012 6:47 PM ...

**Password** recovery - OSForensics
www.osforensics.com › Discover
**forensics** tool ... **Password** recovery & **Decryption** ... the login usename, the site's **password**, the browser used to access the site & the Window's user name.

[PDF] AccessData **Forensic** BootCamp - JESC
www.jesc.co.za/downloads/.../4%20syllabus.applied_**decryption**.en_us.p...
Applied **Decryption**. Distributed Network Attack. **Password**. Recovery Toolkit. **Forensic** Toolkit, Registry. Viewer , and FTK Imager. Advanced • Three-day ...

Paraben **Decryption** Collection Enterprise - H11 Digital **Forensics** ...
w.h11-digital-**forensics**.com/paraben-**forensics**-**decryption**-collection-ent...
Paraben **Forensics**: **Decryption** Collection Enterprise. Paraben **Forensics** can help you break **password** protected files for dozens of programs. Recover more ...

**Decryption** Tools / **Password** Recovery Software - CYINT ...
www.cyint.in/products_**decryption**tools.htm
Products : **Decryption** Tools/ **Password** Breaking Tools. PASSWARE KIT **FORENSICS** ... Use the File menu to save the **decrypted** document into a new file.

[PDF] Passware **Password** Recovery Kit **Forensic** v.10.5 - Arina Electro...
arina.ch/website/arina_pdf/passware-**forensic**.pdf
and released a complete encrypted evidence discovery solution for computer **forensics**. All **password** recovery and **decryption** algorithms that Passware has ...

**Forensic Decrypt** - SlideShare
www.slideshare.net/**forensic**legends/**forensic**-**decrypt**
Mar 28, 2013 – Before Elcomsoft **Forensic** Disk Decryptor, only Elcomsoft Distributed **Password** Recovery couldhandle encrypted disks", says Yuri Konenkov, ...

Passware - mh-SERVICE
www.mh-service.de › ... › Forensic Software › Password Recovery
Passware Kit **Forensic** introduces a new attacks editor, which sets up the **password** recovery process in the most precise way to provide the quickest **decryption** ...

Passware Contributes to Mac **Forensics** by **Decrypting** FileVault ...
www.redorbit.com › News › Technology
Feb 1, 2012 – Passware Contributes to Mac **Forensics** by **Decrypting** FileVault; Warns ... a provider of **password** recovery, **decryption**, and electronic evidence ...

**Previous** 1 2 3 4 5 6 7 8 9 10 **Next**

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

+You Images Maps Play YouTube News Gmail Drive Calendar More

password decryption software 3.1.0.8 free download

Web More Search tools

About 26,300 results (0.31 seconds)

**password decryption software 3.1.0.8 download free - Softonic**
en.softonic.com › Security software › Password › Revealers
**password decryption software 3.1.0.8 download free** - FacebookPasswordDecryptor 2.5: Recover stored Facebook account passwords, and much more ...

**Free Password Decryption Software 3.1.0.8 download**
www.afreecodec.com › ... › Password Decryption Software 3.1.0.8
**Free download Password Decryption Software**, **download free Password Decryption Software 3.1.0.8**, **Free Password Decryption Software download.**

**Password Decryption Software 3.1.0.8 download free - Extract ...**
www.filecluster.com › Security › Password Managers
Nov 11, 2006 – **Download Password Decryption Software 3.1.0.8 Free** in **Password** Managers. **Password Decryption Software** - Extract **password** unmask ...

**Password Decryption Software 3.1.0.8 free download**
**password-decryption-software.download**.hdtlp.com/?**download**
**Password Decryption Software 3.1.0.8** [ **Download** ]. **Software** restore forgotten user login **password** reveal asterisks "*" character ...

**Password Decryption Software 3.1.0.8 Free Download - Extract ...**
www.**download**3000.com/**download-password-decryption-software**-cou...
**Password Decryption Software 3.1.0.8 download free**. Extract **password** unmask asterisks character.

**Download Password Decryption Software Freeware ... - Download32**
www.**download**32.com/**password-decryption-software**-i33003.html
**Password Decryption Software** information page, **free download** and review at Download32. ... **Download** Links of **Password Decryption Software 3.1.0.8**: ...

**Password decryption software Free Download**
**password**.brothersoft.com › **password**
60+ items – **Password decryption software Free Download**,**Password** ...

**Password Decryption Software 3.1.0.8 Free Download, Password ...**
pcwin.com/Utilities/**Password_Decryption_Software**/index.htm
Jul 12, 2007 – PCWin **free download** center makes no representations as to the content of **Password Decryption Software** version/build **3.1.0.8** is accurate, ...

**Download Recover Gmail Password 3.1.0.8 Password decryption ...**
www.10kdownloads.com › ... › Security & Privacy › Password Managers
Feb 6, 2012 – Recover Gmail **Password 3.1.0.8 Password decryption software** decrypts the encrypted ... 10k **downloads**. ... **Free** PDF Unlocker 1.0.4 ...

**Password Decryption Software 3.1.0.8 - Freeware**
www.all-freeware.com/details/42234/**password-decryption-software**.html
Jan 12, 2009 – **Password Decryption Software 3.1.0.8 free download**, review. Data doctor hidden password unmask utility decode any typed key board ...

1 2 3 4 5 6 7 8 9 10 **Next**

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

password decryption software 3.1.0.8 free download

Web More Search tools

Page 2 of about 26,300 results (0.26 seconds)

**Retrieve Forgotten Yahoo Password free download, download 3.1.0.8**
retrieve-forgotten-yahoo-password.softpile.com/106947/
**Download** Retrieve Forgotten Yahoo **Password 3.1.0.8** for **free**. ... **Password decryption software** decrypts the encrypted characters which are covered under ...

**password decryption software FREE Download | 94 files: Passwo...**
www.worldoffiles.net/link-f-p/**password-decryption-software**
You search: **password decryption software** - 94 files were found for **download free**. **Download** file **Password Decryption Software 3.1.0.8**.zip 76,40 Kb or file ...

**Windows Password Recovery Software 3.1.0.8 Free Download, Fre...**
www.**download**atoz.com/.../Windows%20**Password**%20Recovery%20Softw...
Windows **Password** Recovery **Software 3.1.0.8** - Windows Login Recovery ... Ap PDF **Password** Recovery ( pdf **decrypt** ) An application that can be used to ...

**Best Freeware Rediffmail Password Recovery Software Free ...**
www.**software**geek.com/rediffmail-**password**...**software**/**free**ware/p2.html
Rediffmail **Password** Recovery **Software** Freeware **Downloads** by NirSoft ... **Password Decryption Software 3.1.0.8** Data doctor hidden **password** unmask utility ...

**Encrypting and Decrypting software downloads - Download.hr**
www.download.hr › Security
Encrypting and **Decrypting free software download**. ... Create **password** protected DVD/CD/USB Stick to send it via postal mail, for backups and for travel Editor's ...

**Cain & Abel Free Download - Password Decryptors - Softpedia**
www.softpedia.com › Windows › Security › Decrypting & Decoding
676 votes - Free - Windows - Security
Jun 15, 2012 – **Download** Cain & Abel - This utility helps you **decrypt** or recover your lost or ... Part of the **Password** Decryptors **download** hub (+2 others) ...

**Recover Gmail Password 3.1.0.8**
gets.co/**software**/Recover_Gmail_**Password**_1075.html
May 8, 2011 – of Recover Gmail **Password**: **Password decryption software** decrypts the ... you can **free download** Recover Gmail **Password 3.1.0.8** now.

**password decryption software free download, password partner f...**
free.indir.biz › Home Page › Search › password partner 6181
Results 1 - 20 – **password decryption software free download, password** partner **free download, free download, free download Password Decryption Software free** ...

**Asterisk Password Recovery Free download ... - Softducks.com**
www.softducks.com › Security › Password Managers
Jul 25, 2009 – **Free download** Asterisk **Password** Recovery **3.1.0.8**, **Software** ... **Password decryption software** decrypts the encrypted characters which are ...

**Recover Gmail Password 3.1.0.8 - Free download software ...**
www.downchecker.com › Security › Password Managers
May 24, 2011 – **Download free** Recover Gmail **Password** version **3.1.0.8 software** 5064, Recover gmail **password** reveal stored yahoo msn rediffmail asterisk **** **password**. ... **Password decryption software** decrypts the encrypted characters ...

**Previous** 1 2 3 4 5 6 7 8 **Next**

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

+You Images Maps Play YouTube News Gmail Drive Calendar More

password decryption software 3.1.0.8 free download

Web More Search tools

Page 4 of about 26,300 results (0.34 seconds)

[Flashfxp Downloads - FlashFXP Password Decryption (den fete ...](www.fileheap.com/software/flashfxp.html)
www.fileheap.com/software/flashfxp.html
FlashFXP **Password Decryption** 1.0 **download** by den fete gjengen This little puppy ... FlashfxpPasswordDecryptor is the **FREE software** to instantly recover FTP login .... **Password Decryption Software 3.1.0.8 download** by **Password** Recovery ...

**Free Download Password Decryption Software**, Get Lastest ...
tipdownload.com/Password-Decryption-Software_27097/
Get the **Password Decryption Software** 2.1.0.8 **free downloads**, reviews & **free** trial. You are not ... **Password Decryption Software 3.1.0.8** added on: 11-11-2006 ...

**Password Decryption Software 3.1.0.8 - Software Free Downloads**
www.everysoftware.org › Security › Password Managers
Nov 13, 2008 – Download **Password Decryption Software 3.1.0.8**, **Free Download** the Freeware Password Decryption Software at Everysoftware.org, License ...

**Password Decryption Software download** 1MB - Recovery **softwar**...
www.dodownload.com › ... › Password & Sign-On Managers
Jul 9, 2012 – **Password Decryption Software** :: Unmask utility retrieve **password** of windows application, browsers, ... Recovery **software** is easy to use, **free** of cost, user friendly **password** reveal utility that extract ... Other versions : **3.1.0.8** ...

**password decryption software** - Seo Keyword - Website-Tools.net
website-tools.net/google-keyword/word/**password+decryption+software**
**Password Decryption Software 3.1.0.8** - FileCluster. www.filecluster.com/**downloads/Password-Decryption-Software**.html www.filecluster.com. 2012-05-03 14:01:37 ... **Password Decryption Software FREE** Microsoft Access **Password** .

**Password Decryption Software 3.1.0.8 - Free Download Software**
www.fepoi.com/**download/password-decryption-software**-3108-preview-...
**Password Decryption Software 3.1.0.8** Utilities **Software** restore forgotten user login **password** reveal asterisks "****" character.

SoftLow.com - **Password Decryption Software 3.1.0.8 Free Downlo**...
www.softlow.com › Windows › Utilities › Backup
Softlow.com - **Download Free** Backup Utilities for Windows: **Password Decryption Software** - Extract **password** unmask asterisks character - retrieve, windows, ...

**password decryption software 3.1.0.8 free download**
ratdownload.com/fc/**password-decryption-software-3.1.0.8-free-download**
**password decryption software 3.1.0.8 free download**. Download CPTec Backup 1.0.8 Fluff 'em Up 1.0.8.

free download,**Password Decryption Software 3.1.0.8 free download**
www.popscreen.com/...=/-**free-downloadPassword-Decryption-Software**-31...
**Free download Password Decryption Software** and **download free Password Decryption Software 3.1.0.8** from afreeCodec.com.

**Free Download Password Decryption Software 3.1.0.8** - Extract ...
www.**freedownload**utilities.com/.../**password-decryption-software**.html
**Password Decryption Software** - **Software** restore forgotten user login **password** reveal asterisks "****" character.

**Previous** 1 2 3 4 5 **Next**

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms About Google password decryption software 3.1.0.8 free download

Web More Search tools

Page 5 of 43 results (0.14 seconds)

**Password Decryption Software 3.1.0.8 free download. Software ...**
password-decryption-software.winbyte.net/
**Password Decryption Software 3.1.0.8 free download.** Software restore forgotten user login password reveal asterisks **** character.

Vnc **decrypt password** vbscript websites - vnc.**software**.informer.com ...
craftkeys.com/vnc/vnc-decrypt-password-vbscript/
Look at most relevant Vnc **decrypt password** vbscript websites out of 1.23 ... Freewares and Sharewares Fast and **Free software Downloads** - EduTwist. ... LastBit Access **password** Recovery 15.0.9219. **password Decryption Software 3.1.0.8.**

**password decryption software 3.1.0.8 free download**
www.webstatsdomain.com/.../password+decryption+software+3.1.0.8+fr...
Jan 15, 2013 – **Password decryption software 3.1.0.8 free download** - check this search query .

*In order to showyou the most relevant results, we have omitted some entries very similar to the 43 already displayed.*
*If you like, you can repeat the search with the omitted results included.*

**Previous** 1 2 3 4 **5**

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

# United States District Court

## EASTERN DISTRICT OF WISCONSIN

*In the Matter of the Search of*

2051 South 102nd Street, Apartment E, West Allis - A two-story, six unit townhouse complex with six brown garage doors facing the south side of the unit. The building roof has brown asphalt shingles and the building has brown trim. The upper story has tan colored siding and the lower level is covered in brown colored brick. The black numerals "2051" are on a tan sign with brown trim which is attached to the front of the building which is closest to the street and faces east. The individual units have a black letter with tan trim affixed to each door. The letter "E" is affixed to the residential brown front door. The aforementioned townhouse is contained within the "BW," Biwer's Woods Condominium Complex and a sign bearing this complex name is south of the building.

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER: 13-M-421

## APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

2051 South 102nd Street, Apartment E, West Allis - A two-story, six unit townhouse complex with six brown garage doors facing the south side of the unit. The building roof has brown asphalt shingles and the building has brown trim. The upper story has tan colored siding and the lower level is covered in brown colored brick. The black numerals "2051" are on a tan sign with brown trim which is attached to the front of the building which is closest to the street and faces east. The individual units have a black letter with tan trim affixed to each door. The letter "E" is affixed to the residential brown front door. The aforementioned townhouse is contained within the "BW," Biwer's Woods Condominium Complex and a sign bearing this complex name is south of the building.

located in the Eastern District of Wisconsin there is now concealed *(identify the person or describe the property to be seized)*: **Please see Attachment A, which is hereby incorporated by reference.**

The basis for the search warrant under Fed. R. Crim. P. 41(c) is which is (check one or more):

□ evidence of a crime;
□ contraband, fruits of a crime, or other items illegally possessed;
□ property designed for use, intended for use, or used in committing a crime;
□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:
Title 18, United States Code (USC) 2252A, entitled "Certain activities relating to material constituting or containing child pornography.

The application is based on these facts:

□ Continued on the attached sheet.
□ Delayed notice of ____ days (give exact ending date if more than 30 days:_________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Signature of Affiant

Sworn to before me, and subscribed in my presence

January 22nd 2013 at 9:30 AM
Date and time issued

at Milwaukee, Wisconsin
City and State

WILLIAM E. CALLAHAN, JR.
US MAGISTRATE JUDGE
Name & Title of Judicial Officer

William E Callahan
Signature of Judicial Officer

EXHIBIT D

## AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Brett E. Banner, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed with the FBI since November 1999 and I am currently assigned to the Milwaukee Division Child Exploitation Task Force (CETF). I am charged with conducting investigations of violations of Federal Law including the receipt, possession, distribution, and production of child pornography; coercion and enticement of a minor to engage in sexual contact; and, the sexual exploitation and sexual abuse of minors. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with law enforcement partners in local, state and federal law enforcement agencies. Prior to my assignment with Milwaukee I was assigned to the Detroit Division where I was the administrator for the Mid-Michigan Area Computer Crimes Task Force from June 2004 to September 2009. This task force primarily investigated crimes against children investigative matters. I have also been employed in the State of Wisconsin as a certified law enforcement officer from 1993 to 1999.
2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. This affidavit is being submitted in support of an Application for a Search Warrant for the residence located at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin, for evidence of violations of Title 18, United States Code (USC) 2252A, entitled "Certain activities relating to material constituting or containing child pornography."
4. Based upon the information summarized in this affidavit, I have reason to believe that evidence of such violations may be present at the residence located at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin (hereinafter, "PREMISES.")
5. The information supplied in this affidavit is based upon my investigation and information provided and investigation conducted by other law enforcement personnel in this matter to date. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact related to or otherwise the product of this investigation.

## DEFINITION OF TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:
   a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

d. Globally Unique Identifier (GUID)/User Hash: A GUID/User Hash is a special type of identifier used in software applications to provide a unique reference number.

e. Peer-to-Peer Network (P2P): A P2P network allows users to trade digital files through a worldwide network formed by linking computers together via special software. Typically, users perform a keyword search to locate files, and the files can then be downloaded from any users I possession of those files. Users cannot send or receive files without consent.

f. Hash Algorithm: Files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value (i.e. MD5, SHA-1, and eD2Ḱ MD4) is computed for each file being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. The slightest alteration of any file will results in a completely different hash value. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

g. Computer Ports: In computer networking, the term port can refer to either a physical or virtual connection point. Physical network ports allow connecting cables between computers, routers, modems and other peripheral devices. Virtual ports are part of TCP/IP networking. These ports allow software applications to share hardware resources without interfering with each other. Computers and routers automatically manage network traffic traveling via their virtual ports. Network firewalls additionally provide some control over the follow of traffic on each virtual port for security purposes. A port number is part of the addressing information used to identify the senders and receivers of messages. Port numbers are most commonly used with TCP/IP connections. Home network routers and computer software work with ports and sometimes allow you to configure port number settings. These port numbers allow different applications on the same computer to share network resources simultaneously. Port numbers are also associated with network addresses. For example, in TCP/IP networking, both TCP and UDP utilize their own set of ports that work together with IP addresses. Port numbers work like telephone extensions. Just as a business telephone switchboard can use a main phone number and assign each employee an extension number (like x100, x101, etc), so a computer has a main address and a set of port numbers to handle incoming and outgoing connections. In both TCP and UDP, port numbers start at 1 and go up to 65535. Numbers in the lower ranges are dedicated to common Internet protocols (like 21 for FTP and 80 for HTTP).

**PROBABLE CAUSE**

7. Between June 10, 2012 and July 24, 2012, an FBI Online Covert law enforcement agent (hereinafter "OCE 4583"), while connected to the Internet in an online undercover capacity, conducted numerous online investigations to identify those individuals possessing and sharing child pornography using the eDonkey2000 (eD2K) and Kademlia (KAD) peer-to-peer (P2P) networks. OCE 4583 utilized a P2P file sharing program, which scans both networks simultaneously and has been enhanced to ensure that downloads occur only from a single selected source.
8. During those investigations, OCE 4583 searched for suspected child pornography files and identified IP address 65.30.43.173 on the KAD network which had suspected child pornography files available for distribution. Specifically, IP address 65.30.43.173 responded to OCE 4583's queries for the following suspected child pornography Sha1 hash values (also utilized by the KAD network) as outlined below:
**CE7F199CABB9EB9163DA449C9893A2CCB62E67CD**
**AB4083A26CD2B8AD6488D9703936237AC30CA81E**
**4CAA0FA25A7004B830DB8DB9E8147381EE5E58BB**
**1AAB9FCBE0E6C54C6F2D0247971CF13420FCE271**
**A1D31200C10B2EAC35B87BD398F2C9B4B877C81C**
**724F75AF37E078ABFFF5530B0649E6030257D867**
**4A67D0742E2F7620E2B1F43B0A6F15E4FF97CC0E**
**4C5B96A15FA6C71152A7203FCA48EB6B9501933F**
**1DCF638AFDCCCD3DB92BF972E0080DB45465B790**
**F6F9E7087D2C7F8956525C62F93C4824C1D98CA0**
**F953EE2B704C1693CB536CB8AF236447AF0FC4AF**
**8C6DC6E487BF108F355841295B4B99C45537F566**
**2E6FE63B4F0A1D4149932F9BD87E1BE2A69AFDB4**
**826D541B81AA6394B4E67A5DE24F4FD290092F83**
**6088F39E04FFCCD5D2E46686CFCA94FBFEABE12F**
**1984A0ABB418E93527FC049C31429A29C0F4B2AD**
**92E99CE8AA61B07D73C405CA30F88AC0B02E3DD4**
9. During the dates listed, the Maxmind.com database reports that IP address 65.30.43.173 was registered to Time Warner/Road Runner. Further, the website reported that the aforementioned IP address was assigned to an address in Milwaukee, Wisconsin.

10. On September 6, 2012, the aforementioned suspected child pornography hashes were submitted to the National Center for Missing & Exploited Children (NCMEC) for preliminary identification. NCMEC advised that the following Sha1 hash values matched known child victims.
4CAA0FA25A7004B830DB8DB9E8147381EE5E58BB
724F75AF37E078ABFFF5530B0649E6030257D867
4A67D0742E2F7620E2B1F43B0A6F15E4FF97CC0E
1DCF638AFDCCCD3DB92BF972E0080DB45465B790
1984A0ABB418E93527FC049C31429A29C0F4B2AD

- **4A67D0742E2F7620E2B1F43B0A6F15E4FF97CC0E**

- **724F75AF37E078ABFFF5530B0649E6030257D867**

11. The remaining hashes were identified as "Recognized," which meant they had been previously submitted to NCMEC as suspected child pornography by law enforcement.
12. While conducting this investigation, OCE 4583 attempted without success to conduct single source downloads of the suspected child pornography files from IP address 65.30.43.173. OCE 4583 noted that IP address 65.30.43.173 had been given a "low ID" designation on the KAD network. A "high ID" means the ports chosen within the P2P software program are open and freely accessible, whereas a "low ID" means these ports are blocked and cannot be reached. In most instances a client is assigned a "low ID" because they are behind a firewall or router without port forwarding enabled. It should be noted that being assigned a "low ID" will not prevent the P2P software user from downloading or trading files; however, to date OCE 4583 has not been able to conduct single source downloads from users who have been assigned a "low ID." Even though OCE 4583 has not had success conducting a single source downloads with "low ID" clients, OCE 4583 has had success with "low ID" clients responding to OCE 4583's request for suspected child pornography files, as shown above.
13. On September 7, 2012, Time Warner Cable responded to subpoenas requesting Road runner subscriber information regarding IP address 65.30.43.173 on the date and times that child pornography was observed, as described above. Time Warner Cable provided the following subscriber information for said IP address: Jeffrey Feldman, 2051 S. 102nd Street, Apt. E, West

Allis, Wisconsin, telephone number 414-732-8163, length of Road Runner service 02/26/2008-present.

14. On September 13, 2012, Special Agent Jason Pleming, Special Agent Brett Banner and Task Force Officer Brant Ungerer went to the address of 2051 S. 102nd Street, Apt. E, West Allis, Wisconsin, Wisconsin, to conduct surveillance and determine if there was a wireless connection that could be associated with this residence. A check of the available wireless connections when parked in front of the residence revealed that there were several secured wireless connection points that did not have an SSID (Service Set Identifier – a naming convention for wireless networks which requires that all wireless devices on a wireless network employ the same SSID in order to communicate with each other) that could be associated with the residence. There were no unsecured wireless connection points found at this location, indicating that the suspect's wireless connection is secured, if the suspect is utilizing wireless internet.
15. On December 6, 2012, Special Agent Banner viewed a law enforcement commercial data base and learned that Jeffrey W. Feldman, date of birth 01/XX/196X, Social Security Account Number XXX-XX-7372, has lived at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin, since 1997. The data base also lists Feldman's telephone number as 414-732-8163.
16. Records of the State of Wisconsin reflect that Jeffrey W. Feldman has vehicles registered to him at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin 53227.

## COMPUTERS, ELECTTRONIC STORAGE, AND FORENSIC ANALYSIS

17. This application seeks permission to search for records that might be found at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin 53227 (hereinafter, "PREMISES"), in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
18. Probable cause. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:
    a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
    b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or a "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

19. Forensic evidence. This application seeks permission to locate not only computer files that might serve as direct evidence of the crime described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, which as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

20. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-

suite, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including to not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

22. Because it is possible that several people share the PREMISES as a residence, it is possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that is the possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

**Statement of Probable Cause in Support of Application**

23. Based on the facts as I have stated in this affidavit, there is probable cause to believe that evidence of violations of Section 2252A of Title 18 of the United States Code is located at the residence of 2051 South 102nd Street, Apartment E, West Allis, Wisconsin 53227. "Attachment A" to this affidavit is a list of items that would be the subjects of search and seizure at this location.

24. The residence at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin 53227, is more particularly described as follows: a two-story, six unit townhouse complex with six brown garage doors facing the south side of the unit. The building roof has brown asphalt shingles and the building has brown trim. The upper story has tan colored siding and the lower level is covered in brown colored brick. The black numerals "2051" are on a tan sign with brown trim which is attached to the front of the building which is closest to the street and faces east. The individual units have a black letter with tan trim affixed to each door. The letter "E" is affixed to the residential brown front door. The aforementioned townhouse is contained within the "BW," Biwer's Woods Condominium Complex and a sign bearing this complex name is south of the building.

ATTACHMENT A

1. All records relating to violations of Title 18, United States Code, Sections 2252A, including:
    a. Records containing child pornography or pertaining to the distribution, receipt or possession of child pornography;
    b. Records evidencing occupancy or ownership of the premises described above, including but not limited to utility and telephone bills, mail envelopes, or addressed correspondence;
    c. Cellular telephones, telephone and address books, and other notes and papers insofar as they memorialize, include, or confirm computer screen names, contact information, or images related to the sexual exploitation of children, in violation of Title 18, United States Code, Section 2252A;
    d. Any and all records of any form or other items or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence, including but not limited to sales receipts, invoices, bills for Internet access, and handwritten notes.
2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:
    a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. Evidence of the lack of such malicious software;
    d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
    e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
    f. Evidence of the times the COMPUTER was used;
    g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
    h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
    i. Contextual information necessary to understand the evidence described in this attachment;

j. Records and things evidencing the user of the Internet Protocol address 65.30.43.173, including;

k. Routers, modems, and network equipment used to connect computers to the Internet;

l. Records of Internet Protocol addresses used;

m. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet or P2P search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).