

UNITED STATES DISTRICT COURT

for the
Eastern District of Kentucky

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 5:13-MJ-5116-REW

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Kentucky
(identify the person or describe the property to be searched and give its location):

The premises at [REDACTED] Winchester, KY 40391. (See Attachment A, B.)

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
See Attachment B, which is attached and made a part hereof.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

April 29 2013

(not to exceed 10 days)

☒ in the daytime 6:00 a.m. to 10 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

R.E. Wier, US Mag Judge
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

4/15/2013
@ 5:15pm

Judge's signature

City and state:

Lexington, Kentucky

Hon. Robert E. Wier, United States Magistrate Judge

Printed name and title

Return

Case No.: 13-MJ-5116-REW	Date and time warrant executed: 4-16-13 / 10:10	Copy of warrant and inventory left with: D. Lastetter
-----------------------------	--	--

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

See Attached.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

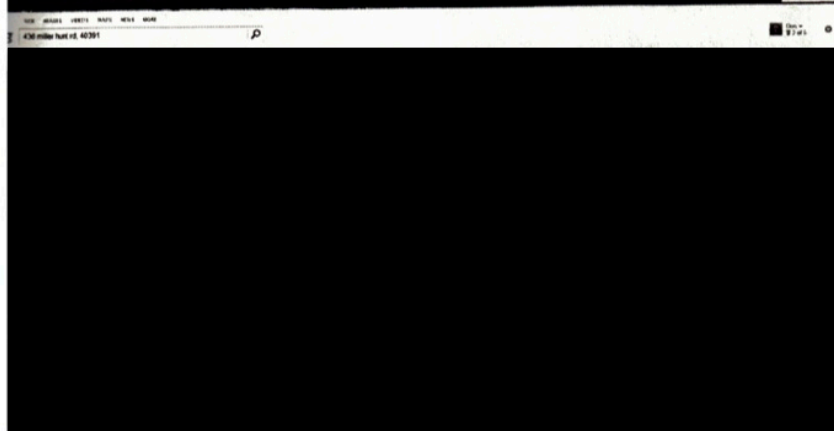
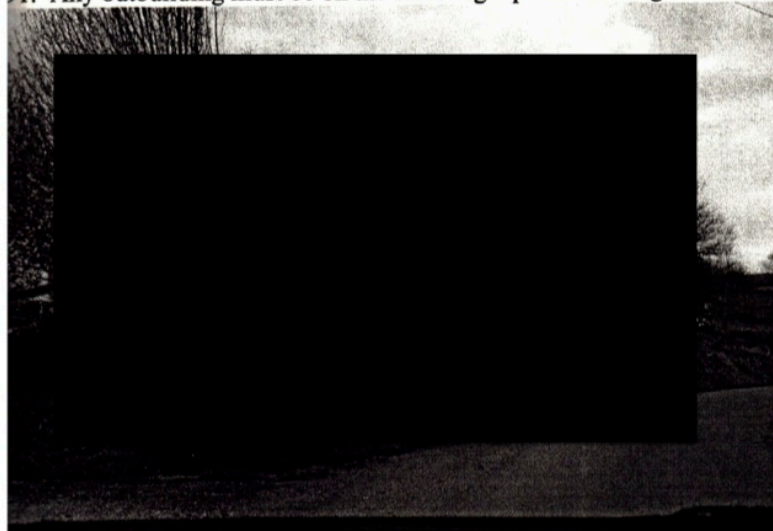
Printed name and title

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

residence and outbuildings on the premises, to wit [REDACTED] Winchester, KY

91. Any outbuilding must be on the same legal parcel bearing the address stated.





ATTACHMENT B

Property to be seized

The Court by this warrant allows any proper law enforcement officer to search the Premises identified on Attachment A and seize any of the following evidence. The evidence may be in any form, and the Court permits off-site review of any electronic storage media as provided in Rule 41(e)(2)(B). The warrant's temporal scope, as to records and information, extends to responsive evidence dated, arising, or coming into existence during the period between August 2012 and the present. In this attachment, "the subject matter addressed by this Warrant" means the hacking activity identified in para 1.a.-1.c. herein, as described fully in the relevant affidavit.

1. All records relating to violations of Title 18 U.S.C. § 1030(a)(2)(C) (Computer Crime); Title 18 U.S.C. § 1028A(Aggravated Identity Theft); 18 U.S.C. § 1028(a)(7) and (f) (Identity Theft, Attempt and Conspiracy); and Title 18 U.S.C. § 371 (Conspiracy), those violations involving records located at [REDACTED] Winchester, KY 43091 ("the PREMISES") and connected to user name Deric Lostutter beginning on or about August, 2012, including:
 - a. Records and information relating to a conspiracy to gain unauthorized access to rollredroll.com, bigredmanowar@comcast.net and any other websites, email, Facebook or other social media accounts of "John Doe" the administrator of rollredroll.com;
 - b. Records and information relating to the unauthorized access of rollredroll.com, bigredmanowar@comcast.net and any other websites, email, Facebook or other social media accounts of "John Doe" the administrator of rollredroll.com;
 - c. Records and information relating to any unauthorized access to any known or unknown victims whose information was obtained through any of John Doe's compromised accounts;
 - d. Records and information relating to the e-mail account bigredmanowar@comcast.net any and all accounts used to communicate with the online "hacker" groups KnightSec and/or Anonymous or any accounts used to facilitate illegal computer activity regarding the subject matter addressed by this Warrant, to wit the hacking event regarding para. 1.a.-1.c.
 - e. Records and information relating to the identity or location of the perpetrators of the criminal violations above or to the identity or location of additional co-conspirators or witnesses;
 - f. Records and information, concerning the subject matter addressed by this Warrant, relating to all communications with the Internet Protocol addresses assigned to the PREMISES including 184.43.20.206, 184.43.21.58, 184.43.48.69, 184.43.55.95, 184.43.20.166, and 184.43.38.211 and to IP address 70.174.58.83, 184.43.21.58;
 - g. Records and information relating to malicious software;
 - h. Guy Fawkes Masks.
 - i. Records and information relating to communications with or instructions from members of KnightSec, Anonymous, or any other group engaged in computer intrusions as to the subject matter addressed by this Warrant;

- j. Cellular telephones and/or smart phones, and information and records thereon including text messages, contacts, emails, URLs, applications and geolocation information relating to communications or meetings between conspirators, or connected with social engineering to obtain information to facilitate the violations that are the subject matter addressed by this Warrant, and billing records for such devices;
 - k. Records relating to the ownership, occupancy or use of the PREMISES;
2. As specified in this paragraph, computers or storage medium used as a means to commit the violations of Title 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(b)(ii) (Computer Crimes); Title 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1028(a)(7) and (f) (Identity Theft, Attempt and Conspiracy); and Title 18 U.S.C. § 371 (Conspiracy) described above. That is, law enforcement may seize any computers or electronic media that were or for which there is a reasonable basis to believe have been used as a means to commit or participate in the offenses listed in this paragraph, which is the subject matter addressed by this Warrant. Specifically, any electronic device or storage media within the possession, custody, control, or ownership of Deric Lostutter (or the person reasonably believed to be that identity) at warrant execution may be seized and searched hereunder.
3. For any computer storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- 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. records of or information about Internet Protocol addresses used by the COMPUTER relevant to the subject matter addressed by the Warrant;
 - j. records of or information about the COMPUTER's Internet activity, as relevant to the subject matter addressed by the Warrant, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

- pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.
 5. Definitions:
 - a. As used above, the terms "records" and "information" includes all forms of creation or storage, 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); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
 - b. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
 - c. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DEPARTMENT OF JUSTICE FEDERAL
BUREAU OF INVESTIGATION

Receipt for Property Received/Returned/Released/Seized

File # 288A-LS-2628098

On (date) 4/16/2013

item(s) listed below were:

- ☐ Received From
☐ Returned To
☐ Released To
☒ Seized

(Name)

(Street Address)

(City)

Winchester, Kentucky 40391

Description of Item(s):

1 - Small external hard drive S/N NA0DSK0K, CD labeled 2012 projects (NS shadow, CD labeled back track)

2 - Several CDs containing photos and other misc cds, notes of music and artists

3 - X Box 360 with power cord S/N 0633907o3008- X-Box
S/N PQ21P580968032 - power cord

4 - Three (3) thumbdrives (pink, white, gray)

5 - One (1) Sony cd (unlabeled)

6 - Two criminal justice CDs, private investigation applicant instructions, Affordable Used Car receipt, AT&T receipts for phone/internet, pay pal document, car bill of sale, credit report, ethernet report, and other misc docs

7 - HTC phone, Model ADR6400L, S/N HT11WS002037 (display cracked)

8 - Alienware laptop, 00188-03W-249-492, Service Tag S/N 1JX3BW1

9 - Inspiron Laptop 1545, Model No. PP41L, Service Tag S/N F8L10K1

10 - HTC phone, S/N HT2BPW300832

Received By

(signature)

Received From

(signature)

Deric Losuta
Deric Losuta