

**SEARCH WARRANT**  
HP USB drive,  
marked 0045SMKBT1 85102

Case No. 11M-5063-JGD

AO 93 (Rev. 12/09) Search and Seizure Warrant

# UNITED STATES DISTRICT COURT

for the  
District of Massachusetts

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

HP USB drive, marked 0045SMKBT1 85102

)  
)  
) Case No. 11M-5863-JGD  
)  
)  
)

## 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 \_\_\_\_\_ District of Massachusetts  
*(identify the person or describe the property to be searched and give its location):*  
HP USB drive, marked 0045SMKBT1 85102 , as described in Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized):*  
evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. §1030(a)(5)(A) and 18 U.S.C. § 1343 (wire fraud,) as described in Attachment B

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 March 10, 2011  
*(not to exceed 14 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 Judith G. Dein  
*(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: 2/24/11 3:05  Judith G. Dein  
*Judge's signature*

City and state: Boston, Massachusetts Chief U.S. Magistrate Judge Judith G. Dein  
*Printed name and title*

USAO-000271

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

**Return**

Case No.: <b>11M-5063 JGD</b>	Date and time warrant executed: <b>2/25/2011 9:08 AM</b>	Copy of warrant and inventory left with: <b>KEVIN CAVANAUGH</b>
----------------------------------	---	--

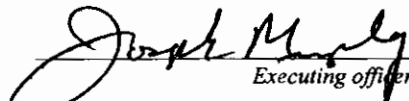
Inventory made in the presence of:  
**Property Technician Kevin Cavanaugh & Dep. Sup. Joseph Wilson**

Inventory of the property taken and name of any person(s) seized:  
  
**(1) HP USB Drive  
marked ~~00~~ 459 MKBT1 85102**

**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: **3/4/11**

  
 Executing officer's signature  
**Joseph Murphy Special Fed Dep US Marshal 1**  
 Printed name and title

**Attachment A**

HP USB drive, marked 0045SMKBT1 85102

11M-5063-JSD

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mit.edu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

- media;
  - 4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
  - 5. evidence of the times the computer equipment was used;
  - 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
  - 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### **DEFINITIONS**

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.



ATTACHMENT C

**PROCEDURES FOR SEIZING COMPUTERS AND RELATED DEVICES**

1. Seizing hardware and software

Agents are authorized to seize and remove from the premises the computer hardware, software, related documentation, and storage media, so that computer analysts can accurately retrieve the items authorized by this warrant in a laboratory or other controlled environment. The retrieval process does not need to be completed within 14 days after the date of the warrant or before the return of the written inventory required by Fed. R. Crim. P. 41(a).

2. Returning hardware and software

If, after inspecting a seized computer system, the agents and computer analysts determine that these items are no longer necessary to retrieve and preserve electronic evidence, the prosecutor determines that they need not be preserved as evidence, fruits or instrumentalities of a crime, and these items do not contain contraband, they should be returned within a reasonable time, upon written request.

If the computer system cannot be returned, agents should, upon written request, make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that are neither the fruits nor instrumentalities of crime nor contraband.

**APPLICATION FOR  
SEARCH WARRANT**  
HP USB drive,  
marked 0045SMKBT1 85102

**Case No. 11M-5063-JGD**

# UNITED STATES DISTRICT COURT

for the  
District of Massachusetts

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*  
HP USB drive, marked 0045SMKBT1 85102

Case No. 11M-5063-JED

## APPLICATION FOR A 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)*: HP USB drive, marked 0045SMKBT1 85102, as described in Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. §1030(a)(5)(A) and 18 U.S.C. § 1343 (wire fraud,) as described in Attachment B

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

- evidence of a crime;
- contraband, fruits of 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:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Sec. 1030(a)(2)	intentionally accessing a computer without authorization and obtaining information
18 U.S.C. Sec. 1030(a)(5)(A)	intentionally causing damage without authorization to a protected computer
18 U.S.C. Sec. 1343	wire fraud

The application is based on these facts:  
See attached Affidavit of Special Agent Michael S. Pickett

- 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.

*Applicant's signature*

Secret Service Special Agent Michael S. Pickett

*Printed name and title*

Sworn to before me and signed in my presence

Date: 2/24/11



*Judge's signature*

City and state: Boston, Massachusetts

Chief U.S. Magistrate Judge Judith G. Dein

*Printed name and title*

11M-5063-JED

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael S. Pickett, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search an Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601 (“the ACER LAPTOP”), a 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675 (“the WESTERN DIGITAL HARD DRIVE”), and an HP USB drive, marked 0045SMKBT1 85102 (“the USB DRIVE”), as described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the United States Secret Service (“the Secret Service”), Department of Homeland Security, and have been since 2003. My current duties include the investigation of electronic crimes and forensic examination of computers and cellular telephones. As an agent, I have participated in numerous investigations involving computer and high technology related crimes, including computer intrusions, Internet fraud and credit card fraud. I also have received specialized training in the investigation of crimes involving unauthorized intrusions into computer networks. In connection with my official responsibilities, I am charged with investigating violations of 18 U.S.C. §§ 1030 and 1343.

3. As set forth herein, there is probable cause to believe that the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB DRIVE contain evidence, instrumentalities, and fruits of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud).

4. I make this affidavit based upon communications with witnesses and others with knowledge of the events, conversations with Secret Service agents, Cambridge Police, and MIT police, my review of records gathered in the course of the investigation described below and my

own observations and knowledge. Because this affidavit is intended to show only that there is probable cause for the requested warrants, it does not set forth all aspects of the investigation of which I or other Secret Service agents are aware.

### **TECHNICAL TERMS**

5. Based on my experience, I use the following technical terms to convey the following meanings for the purpose of this affidavit:

a. **IP address:** An Internet protocol address (or simply “IP address”) is a unique numeric address used by a computer on the Internet. An IP address looks like a series of four numbers, each in the range 0 - 255, separated by periods (e.g., 18.55.7.216). Every computer attached to the Internet must be assigned an IP address so the Internet traffic sent from and directed to that computer may be directed properly from the source to its destination. Most Internet service providers control a range of IP Addresses. The Massachusetts Institute of Technology (“MIT”) controls all IP Addresses which begin with the number 18. Some computers have static – that is, long term – IP addresses, while others have dynamic – that is flexibly assigned or frequently changed – IP addresses.

b. **MAC address:** A Media Access Control address is a unique identifier assigned to a network interface, in this case, a computer’s network interface card. The MAC address most often is assigned by the manufacturer of the network interface card. Although intended to be a permanent and globally unique identification, it is often possible to change the MAC address on hardware, an action often referred to as “MAC address spoofing.”

**PROBABLE CAUSE**

6. Based on the facts set forth below, there is probable cause to believe that Aaron Swartz:
- a. broke into a network interface closet at the Massachusetts Institute of Technology (“MIT”);
  - b. without authorization, accessed MIT’s computer network from a network switch within that closet;
  - c. fraudulently used the appearance of being a MIT student, faculty member or researcher to access JSTOR’s extensive electronic library; and
  - d. fraudulently took from that library over a million journal articles which JSTOR made available by paid subscription or individual purchase.

**JSTOR**

7. JSTOR, founded in 1995, is a United States-based, on-line system for archiving and providing access to academic journals. It provides full-text searchable digitized copies of over 1,000 academic journals, dating back for lengthy periods of time. JSTOR is an independent, self-sustaining, non-profit organization.

8. It can be extraordinarily expensive, in terms of both cost and space, for a research or university library to maintain a comprehensive collection of academic journals. By digitizing extensive, historical collections of journal titles, JSTOR enables libraries to out-source the storage of these journals, ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary searches of them.

9. JSTOR licenses all content under copyright from rights holders and gets permission from them both to digitize the content and make the content available online.<sup>1</sup>

10. In the vast majority of instances, JSTOR charges subscription fees to the libraries, universities and publishers who wish to have access to JSTOR’s digitized journals. In the

---

<sup>1</sup> Some materials available on JSTOR are not subject to copyright.

instance of a large research university, this annual subscription fee for the various collections of content offered by JSTOR can cost more than fifty thousand dollars. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes available some articles through its Publisher Sales Service, a program offered through participating JSTOR publishers in which journal articles are available for individual purchase. Publishers decide which articles can be purchased and set fees for their articles. JSTOR facilitates the purchase of articles from the archives on behalf of the participating publishers.

### The Fraudulent Downloads

11. MIT offers short-term service on its computer network to registered campus guests. On September 24, 2010, an individual registered on the network using the pseudonym “Gary Host” and providing the throwaway e-mail address, [ghost@mailinator.com](mailto:ghost@mailinator.com).<sup>2</sup> As part of the registration process, his computer identified the MAC address of its network interface as 00235a735ffb and its client name<sup>3</sup> as “ghost laptop”.

12. On September 25, 2010, shortly after midnight, the “ghost laptop” was assigned IP address 18.55.6.215. Later that day, JSTOR experienced an extraordinary volume of automated requests and downloads from its digitized journal collections to that IP address. The downloads continued into the evening, when JSTOR blocked access to its network from 18.55.6.215.

13. The next morning, JSTOR began to experience rapid and voluminous downloads from IP address 18.55.6.216. Accesses from this address continued until the middle of the day, when JSTOR blocked this IP address as well. That day, JSTOR turned to blocking a much

---

<sup>2</sup> Mailinator is a free disposable e-mail address service that allows a user to create a new e-mail address on the fly. Mailinator will accept mail for any mail address within the mailinator.com domain, and allows anyone to read it without having to create an account or enter a password. All mail sent to mailinator.com is automatically deleted after several hours whether read or not. It is intended to provide users with an anonymous and temporary e-mail address. See <http://mailinator.com/faq.jsp> (Mailinator FAQs), last visited on February 1, 2011.

<sup>3</sup> A computer’s name helps to identify it on a network and can be chosen by a user.

broader range of IP address, temporarily denying service to legitimate JSTOR users at MIT.

14. MIT controls the assignment of all IP addresses in which the first block is "18." It has assigned the second block in the IP address for use by specific buildings on campus. In this instance, "18.55" defines connections made to the MIT network from within Building 16 on campus.

15. On September 27, 2010, MIT deactivated the guest registration for the "ghost laptop" by barring the MAC address 00235a735ffb from being assigned a new IP address.

16. On October 2, 2010, "Gary Host," again using a computer with the client name "ghost laptop," registered as a guest and obtained an IP address from the MIT network. He appears to have bypassed the affirmative bar which MIT had placed to his usage of the network by spoofing the MAC Address of the "ghost laptop," changing the last byte of the MAC address from 00235a735ffb to 00235a735ffc (changing the final "b" to "c"). The "ghost laptop" was assigned IP address 18.55.7.48.

17. On October 8, 2010, the perpetrator, using the same naming conventions as he had for "ghost laptop," obtained a guest registration simultaneously for a second computer on the MIT network. "Grace Host" registered the computer client "ghost macbook," providing the e-mail address [ghost42@mailinator.com](mailto:ghost42@mailinator.com).<sup>4</sup> The MIT network assigned the "ghost macbook" IP address 18.55.5.100, locating the "ghost macbook's" network connection somewhere within Building 16.

18. Extraordinary downloading of JSTOR's digitized copies of journals began just before 3:00 p.m. on October 9, 2010, from IP address 18.55.5.100 (assigned to the "ghost macbook") and continued until approximately 7:00 p.m. In parallel, extraordinary downloading from JSTOR's collections to IP address 18.55.7.48 (assigned to the "ghost laptop") began at approximately 6:30 p.m. and continued as well until approximately 7:00 p.m. that night.

---

<sup>4</sup> The MAC address of the "ghost macbook," 0017f22cb074," is within the range coded by Apple into hardware it manufactures.



19. During the months of November and December, 2010, over two million illegal downloads were made from JSTOR to two IP addresses assigned to Building 16 at MIT; 18.55.6.240 and 18.55.7.240. Of these, approximately half were research articles, with the remainder being reviews, news, editorials, and miscellaneous things. This is more than one hundred times the number of downloads by all the legitimate MIT JSTOR users combined during the same period.

20. JSTOR did not spot this phase of illegal downloading until Christmas time. MIT's network logs reflect that the computer assigned IP address 18.55.6.240 had not registered as a guest on the MIT computer network on this occasion. An analysis on January 4, 2011, however, reflected that both IP addresses 18.55.6.240 and 18.55.7.240 were assigned to a computer with the MAC address 004ce5a0c756. Using network tools available to MIT on this occasion, the computer was tracked back to a specialized network wiring closet in the basement of Building 16 at MIT.

21. There, MIT personnel found, and subsequently showed to law enforcement personnel, the ACER LAPTOP and an external Samsung hard drive, both of which had been concealed under a cardboard box. The laptop had been connected directly into MIT's computer network and the perpetrator had assigned to himself the IP addresses 18.55.6.240 and 18.55.7.240.

22. On January 4, 2011, MIT placed a video camera in the wiring closet. Later that day, the perpetrator, subsequently identified as Aaron Swartz, was videotaped entering the wiring closet. While there, he appeared to replace the external hard drive attached to the laptop.

23. Swartz, who is neither a student nor an employee of MIT, was recorded again entering the wiring closet on January 6, 2011. Before law enforcement officers could get there, he had removed his computer equipment from the closet and left.

24. Later, during the afternoon of January 6, 2011, the laptop removed from the network wiring closet (identified by its MAC address 004ce5a0c756) was plugged into a network

jack in Building W20. There, it was once again registered through MIT's guest services. When it was, the computer identified itself as "ghost laptop," the same identification provided during the illegal downloads in September and October. The ACER LAPTOP and the WESTERN DIGITAL HARD DRIVE were located and recovered by MIT personnel and law enforcement, without the previously observed external hard drive.

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground<sup>5</sup> and fled. The backpack in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

26. In the backpack was the USB DRIVE. From my training and experience and information provided to me by other agents, USB drives are frequently used to store software applications, data and records, including .pdf formatted records such as those that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers or hard drives, such as between those connected in the wiring closet to MIT's network and ones available to Swartz outside.<sup>6</sup>

27. On February 9, 2011, the Court issued warrants to search Swartz's residence at 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 ("the PREMISES"), the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB

---

<sup>5</sup> I mistakenly stated in my February 9<sup>th</sup> Affidavit that Swartz dropped his backpack to the ground before fleeing from police. He kept it with him when he fled.

<sup>6</sup> As reflected in paragraphs 17 and 18, above, there were two laptops used in the October 9, 2010, illegal downloads from JSTOR. One identified itself to MIT's network as "ghost laptop." The second identified itself to the MIT's network as "ghost macbook" and provided a MAC address within the range coded by Apple into hardware it manufactures. The "ghost macbook" used in the fraud and thefts has not been recovered yet.

DRIVE. The warrant to search the PREMISES was executed on February 11, 2011. The warrants to search the ACER LAPTOP, the WESTERN DIGITAL DRIVE, and the USB DRIVE were not executed prior to their expiration on February 22, 2011. At the time the warrant was issued for these pieces of electronic equipment, they were secured within the Identification Unit Laboratory of the Cambridge Police Department. Throughout the period of February 9, 2011, to the present, they remained within secure areas at Cambridge Police Headquarters, first in the Identification Unit Laboratory, then in the Evidence/Property Unit.

28. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after 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, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This 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. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

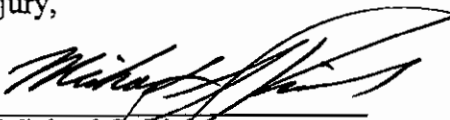
d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

**CONCLUSION**

29. Based on the information described above, I have probable cause to believe that Aaron Swartz has violated 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud).

30. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE and the USB DRIVE.

Sworn to under the pains and penalties of perjury,

  
Michael S. Pickett  
Special Agent  
United States Secret Service

Subscribed and sworn to before me on February 24, 2011

  
CHIEF UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601

2.0 terabyte Western Digital hard drive, serial number WMAZA1626675

HP USB drive, marked 0045SMKBT1 85102

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mit.edu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

- media;
- 4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
- 5. evidence of the times the computer equipment was used;
- 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
- 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### **DEFINITIONS**

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,



communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

**Attachment A**

HP USB drive, marked 0045SMKBT1 85102

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mit.edu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

- media;
  - 4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
  - 5. evidence of the times the computer equipment was used;
  - 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
  - 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### **DEFINITIONS**

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.