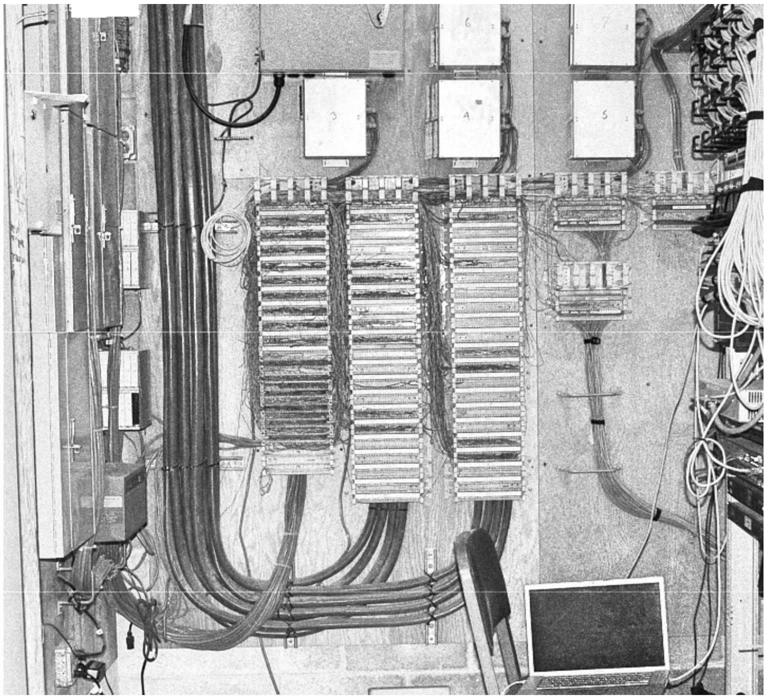
Towards a biography of Aaron Swartz : selected archives from the FBI File and *USA v. Swartz.*

Camille Akmut

January 17, 2020

Abstract

Legal and police documents; technological and sociological information.



Notes regarding the neutral documents of a neutral case

I. Neutrality of MIT, a fable revised (through archives)

One of the documents presented here, ”MOTION TO SUPPRESS ALL FRUITS OF INTERCEPTIONS AND DISCLOSURES OF ELECTRONIC COMMUNICATIONS” (followed by another, pertaining to a later period) sheds a new light on the purported ”neutrality” of MIT evoked in *Report to the president.*

In this document, we read :

> ”Mike Halsall, MIT Senior Network & Information Security Analyst, turned over to Secret Service S/A Michael Pickett” various information from the MIT network.

And, further, coming from the defense :

> ”MIT's disclosure to the Secret Service of DHCP logs, network flow data, and packet capture information in the absence of a subpoena or search warrant”.

MIT staff was overzealous, they simply could not wait to turn over information they were not lawfully asked to provide. – This is what we gather from these documents.

”*MIT called campus police to the scene, who, in turn, brought in the Cambridge Police and the Secret Service.*” we find yet elsewhere, in them.

> ”The ruse worked. Within an hour of their departure, the hacker returned.”

we read even further.

”*no one has sought a warrant*” the involved FBI agent about even wrote himself.

He could not believe his luck, that day. He was ready to confiscate the material 'at any moment'. Like a boy in a candy store, was his experience of MIT – to be vulgar.

Hal Abelson wrote the words ”neutral” and ”neutrality” a staggering 100 times, without even knowing it. And, so a 100 times we must call them back to both more care, and more courage.

II. More technical documents

”MOTION TO SUPPRESS” is the most important source of technical information besides the already highlighted Sep. 2012 superseding indictment[1];

as well as ”GOVERNMENT'S CONSOLIDATED RESPONSE TO DEFENDANT'S MOTIONS TO SUPPRESS” from Nov. 2012.

This one holds the enormous phrase :

[1] (Although we used the superseding indictment from 2012, there's a similar document from c. 2010, with small changes e.g. keepgrabbing2.py is capitalized)

”The Victims: JSTOR and MIT”

MIT is a billion dollar heavy university whose reputation is in substantial part based on ”hackers” (the term used in this one document to describe Aaron Swartz) that now found themselves defendants in lawsuits.

These ’victims”, their lawyers, their staff, or the courts, call research ”things of value” (superseding indictment), in these legal documents. and put a price on it. ”in excess of 5,000$” (ibid.), ”50,000$” (police report).

***

All of these documents, all in their own way, shed light on our modern information societies :

They shed light on the practices of not only surveillance agencies (i.e. LinkedIn pages) but also courts (”Twitter postings”, as the honorable Carmen Ortiz wrote in a message that must have been like a slap to the face of Aaron’s lawyer), and the methods used by various engineers in the monitoring of institutional networks.

Unchanged is the might of corporations whose financial interests, once touched, lead to an avalanche of legal papers, we went through all of them, so we know. Enough to bury and kill someone.

Historians and sociologists will read these documents with great care, interest — as will hopefully others. ”You poor take courage, your rich take care”.

Annex :

– 1 ”SWARTZ’s online profiles” (FBI file)
– 2 ”RESIDENTIAL ADDRESS” in Cambridge, MA and Brooklyn, NY (USA v. Swartz)
– 3 Seized electronic equipment (USA v. Swartz)[2]
– 4 Current employer (USA v. Swartz)
– 5 ”MOTION TO SUPPRESS” (USA v. Swartz)
– 6 ”GOVERNMENT’S CONSOLIDATED RESPONSE” (USA v. Swartz)
– 7 Logs
– 8 Photos
– 9 Police report
– 10 FBI e-mail

References
Aaron Swartz’s FBI File https://archive.org/details/AaronHSwartzFBIFile/
USA vs. Aaron Swartz https://archive.org/details/555334-1-11-cr-10260-nmg/

[2] (found in various other forms, places, but this is the most detailled one we could find)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/19/2009

AARON SWARTZ has a profile on the website LINKEDIN, at www.linkedin.com/in/aaronsw. SWARTZ is listed as a writer, hacker and activist based in the San Francisco Bay Area. SWARTZ's education includes Stanford University, Sociology, 2004. SWARTZ's experience includes the following:

Founder of watchdog.net
2008 - Present

Tech Lead at Open Library
2007 - Present

Co-founder of reddit
November 2005 - January 2007

Metadata Advisor at Creative Commons
2002 - 2004

Member of RDF Core Working Group
1999 - 2000

Member of W3C
1999 - 2000

The website watchdog.net: the good government site with teeth states that "We're trying to build a hub for politics on the Internet". This plan includes pulling all information about politics, votes, lobbying records, and campaign finance reports together under one unified interface. SWARTZ posted blogs on 07/30/2008, 06/16/2008, 05/07/2008, 04/21/2008, 04/16/2008, 04/14/2008.

SWARTZ has a profile on the website FACEBOOK. His networks include Stanford '08 and Boston, MA. The picture used in his profile was also used in an article about SWARTZ in THE NEW YORK TIMES.

SWARTZ's personal webpage, www.aaronsw.com, includes a section titled "Aaron Swartz: a lifetime of dubious accomplishments". In 2007, SWARTZ began working full-time as a

Investigation on 02/15/2009 at Manassas, VA

File # 288A-WF-238943 Date dictated

by SA [redacted]

b6
b7C
b7F

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-WF-238943

member of the Long-Term Planning Committee for the Human Race (LTPCHR).

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
OF AMERICA|	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant.	)	

DEFENDANT'S MOTION FOR LEAVE TO CHANGE RESIDENTIAL ADDRESS

Aaron Swartz moves this Court for leave to change his residential address to 76 Oxford St # 1, Cambridge, MA 02138-1809. Mr. Swartz has already reported this change to Pretrial Services Officer Gina Affsa. The residential change is necessary because his former landlord would not extend his lease on his Massachusetts Avenue apartment.

As reported at the arraignment, Mr. Swartz has begun working as independent contractor performing research for a New York City company. This work requires Mr. Swartz to spend variable days of the week in New York City. When he stays over night in New York, Mr. Swartz's address is 99 Graham Street, Apt. #1, Brooklyn, New York 11206.

Mr. Swartz reports in person weekly to the Pretrial Services office in Boston.

Respectfully submitted,

/s/Andrew Good
Andrew Good
BBO # 201240
Good & Cormier
83 Atlantic Avenue
Boston, MA 02110
Tel. 617-523-5933
agood@goodcormier.com

U.S. Department of Justice

Carmen M. Ortiz
United States Attorney
District of Massachusetts

Main Reception: (617) 748-3100

United States Courthouse, Suite 9200
1 Courthouse Way
Boston, Massachusetts 02210

August 12, 2011

Mr. Andrew Good
Good and Cormier
83 Atlantic Avenue
Boston, MA 02110

Re: United States v. Aaron Swartz
Criminal No. 11-CR-10260

Dear Counsel:

Pursuant to Fed. R. Crim. P. 16 and Rules 116.1(C) and 116.2 of the Local Rules of the United States District Court for the District of Massachusetts, the government provides the following automatic discovery in the above-referenced case:

A. Rule 16 Materials

1. Statements of Defendant under Rule 16 (a)(1)(A) & (a)(1)(B)

a. Written Statements

The defendant's booking sheet and fingerprint card from the Cambridge Police Department are contained on enclosed Disk 5.

There are numerous relevant statements not made to government agents drafted by Defendant Swartz before the date of his arrest contained in electronic media, such as Twitter postings, websites and e-mail. These are equally available to the defendant. Those that the government intends to use in its case-in-chief are available for your review, as described in paragraph A(3) below.

Subject thereto, there are no relevant written statements of Defendant Swartz made

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence
- Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 (Please note that because of the number of files contained on Samsung model HD154UI hard drive, serial number S1Y6J1C2800332, it has not been practicable to date to make a complete file list in an Excel readable format, unlike the other drives.)
- A fingerprint analysis report from the Cambridge Police Department with respect to the Acer Laptop and Western Digital hard drive recovered at MIT
- A supplemental fingerprint analysis report with respect to these items

While not required by the rules, intermediate as well as final forensic reports where available are enclosed for many of the recovered and seized pieces of equipment on Disks 6 and 1, respectively.

B. Search Materials under Local Rule 116.1(C)(1)(b)

Search warrants were executed on multiple pieces of electronic equipment and at multiple locations. Copies of the search warrants, applications, affidavits, and returns have already been provided to you, but are further found on Disk 3.

Four Samsung Model HD154UI hard drives were examined following their consensual and unconditional delivery to the United States Secret Service on June 7, 2011. As an additional precaution, a warrant, enclosed on Disk 3, was also obtained.

C. Electronic Surveillance under Local Rule 116.1(C)(1)(c)

No oral, wire, or electronic communications of the defendant as defined in 18 U.S.C. § 2510 were intercepted relating to the charges in the indictment.

D. Consensual Interceptions under Local Rule 116.1(C)(1)(d)

There were no interceptions (as the term "intercept" is defined in 18 U.S.C. § 2510(4)) of wire, oral, or electronic communications relating to the charges contained in the indictment, made with the consent of one of the parties to the communication in which the defendant was intercepted or which the government intends to offer as evidence in its case-in-chief.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA)
)
v.) Criminal No. 11-10260-NMG
)
AARON SWARTZ,)
)
Defendant)

ASSENTED TO MOTION FOR MODIFICATION OF CONDITIONS OF PRETRIAL RELEASE

Now comes the defendant Aaron Swartz who hereby requests that this Honorable Court modify his conditions of release. As reason therefore, defendant states:

1. That he was released on July 19, 2011 on conditions memorialized in Chief Magistrate Judge Judith G. Dein's ORDER Setting Conditions of Release (Doc. 6) that included that he maintain his current residence in Cambridge, Massachusetts with travel restricted to the continental United States and that he report as directed by Pretrial Services;
2. That he is currently reporting in person every other week to Pretrial Services;
3. That he has fully complied with all the conditions of pretrial release through the current date;
4. That he is currently employed by Avaaz Foundation in New York;
5. That his employment requires that he relocate to a new address, [redacted] [redacted] [redacted] Brooklyn, New York [redacted];
6. That this change of residence will not interfere with his communications with counsel, their working together in meaningful pretrial preparation, or his counsel's ability in any way to prepare for trial;

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
v.	)	No. 11-10260-NMG
AARON SWARTZ	)	

MOTION TO SUPPRESS ALL FRUITS OF INTERCEPTIONS AND DISCLOSURES OF ELECTRONIC COMMUNICATIONS AND OTHER INFORMATION BY MIT PERSONNEL IN VIOLATION OF THE FOURTH AMENDMENT AND THE STORED COMMUNICATIONS ACT AND INCORPORATED MEMORANDUM OF LAW (MOTION TO SUPPRESS NO. 1)

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case (1) the network flow data and DHCP logs collected by MIT personnel and disclosed to the government without a warrant or court order or subpoena, as well as all evidence derived therefrom, and (2) all evidence from the packet capture instituted by MIT personnel on the morning of January 4, 2011, and continuing, at the request of the government that MIT personnel continue to intercept electronic communications, through January 6, 2011, and subsequently turned over to the Secret Service, as well as all evidence derived therefrom.[1]

As reason therefor, defendant states:

[1] In a separate motion to suppress, Swartz contends that after law enforcement agents arrived on the scene on January 4, 2011, and recommended that MIT personnel continue the packet capture they had begun earlier that morning and began to direct the investigation, MIT personnel were acting as government agents, and their actions were therefore subject to the requirements of the Fourth Amendment. *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law. This motion is directed in part at the interceptions conducted by MIT personnel before they began acting as government agents, as well as MIT's turning over to the government material in which Swartz had a reasonable expectation of privacy, in the complete absence of judicial process compelling MIT to produce such evidence to the government at a time when law enforcement agents were directing MIT employees regarding how to further their criminal investigation of the defendant.

1. He had a reasonable expectation of privacy in the electronic communications flowing to and from his ACER netbook.[2]

2. The interception of network flow data to the netbook and the packet capture constituted interceptions of electronic communications within the meaning of Title III.

3. The interceptions conducted by MIT and its disclosure of the information gathered to the Secret Service violated 18 U.S.C. §2511(1), as no exceptions to the requirements of Title III apply to MIT's conduct. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed as violative of the Fourth Amendment.

4. The disclosure of DHCP logs by MIT personnel in the absence of a warrant issued upon a showing of probable cause or a court order pursuant to 18 U.S.C. §2703(d) violated the Fourth Amendment and/or the Stored Communications Act.

5. MIT's disclosure to the Secret Service of DHCP logs, network flow data, and packet capture information in the absence of a subpoena or search warrant violated 18 U.S.C. §§2702, 2703, as well as Swartz's rights under the Fourth Amendment such that suppression of the evidence, as well as all derivative fruits, in required.

THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.

LOCAL RULE 7.1(A)(2) STATEMENT

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

[2] All averments herein regarding Swartz's ownership and possession of the ACER netbook and the attached hard drive, and the communications flowing to and from them, are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

MEMORANDUM OF LAW

I. FACTUAL BACKGROUND.

On September 26, 2010, MIT received an email from Brian Larsen at JSTOR, an online archive of scholarly journal articles, informing it that there had been, that morning, an excessive downloading of journals. By the next day, the IP addresses from which the journals were being downloaded had been located (largely, if not exclusively, by JSTOR) and the user information for the guest registration of the computer being used had been identified; JSTOR then blocked access to these IP addresses. Timeline of events related to JSTOR downloading incident: 9/26/10 - 1/6/11, Exhibit 1 ("Timeline") at 1. On October 9, 2010, JSTOR again notified MIT that its access was being blocked because of excessive downloading. Timeline at 2. JSTOR quickly identified the IP address being used for the downloads, and MIT personnel thereafter discovered that access was being accomplished in Building 16 by a computer registered through its visitor guest registration process by the same guest whose computer was linked to the September incident.[3] Timeline at 2-3.

MIT and JSTOR conferred regarding methods to prevent excessive downloading. Timeline at 3-4. On December 26, 2010, there was another episode of excessive downloading, which MIT personnel did not learn of until on or about January 3, 2011. On the morning of January 4, 2011, at approximately 8:00 am, MIT personnel located the netbook being used for the downloads and decided to leave it in place and institute a packet capture of the network traffic to and from the netbook.[4] Timeline at 6. This was accomplished using the laptop of Dave Newman, MIT Senior

[3] MIT personnel first received notice of the October 9, 2010, incident when they returned following the Columbus Day holiday on October 12, 2010. Timeline at 2.

[4] A packet capture captures the entire communication, including subject matter and content, and to the extent it was diverting and copying communications in transit to and from the netbook, this constituted a classic interception of electronic communications in violation of *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*). *See* page 9, *infra.*

Network Engineer, which was connected to the netbook and intercepted the communications coming to and from it. *Id.* Later that day, beginning at 11:00 am, the Secret Service assumed control of the investigation.[5] Later on January 4, 2011, Mike Halsall, MIT Senior Network & Information Security Analyst, turned over to Secret Service S/A Michael Pickett "historical network flow data concerning 18.55.6.240 & 7.240 [the IP addresses associated with the earlier JSTOR downloads][6] dating from 12/14 until present and relevant DHCP log information[7] from prior occurrences of ghost-macbook and ghost-laptop [the two guest registrations at issue] JSTOR downloading incidents (from Sept. and Oct.)." Timeline at 7. The disclosure took place only after the MIT General Counsel's Office approved the disclosure of the information to law enforcement authorities even in the absence of a warrant or court order or subpoena – and at a time when MIT personnel were acting as government agents – and in contravention of MIT policy that such information, which exceeded that found in bank records or telephone toll records, would be disclosed only upon the receipt of lawful court orders or subpoenas, *i.e.*, process complying with the Stored Communications Act, 18 U.S.C. §2701 *et seq. See* Section IV, *infra.* In a separate email from Halsall to S/A Picket on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday,

[5] *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

[6] Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.

[7] "DHCP" stands for Dynamic Host Configuration Protocol. DHCP assists with the assignment of IP addresses to computers on networks. When a computer joins a network, the computer issues a DHCP request on the network, which asks a DHCP server on the network to provide an IP address to the requesting computer. Part of the information contained in this request is the MAC (Media Access Control) address which is a unique identifier of the network card contained in the computer requesting an IP address. It also includes the commands made by the computer in question. *See* page 7, *infra.*

possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2. No warrant or court order has been provided to counsel which would evidence the government's having, even post-interception, acquired the contents of the warrantless interceptions by seeking judicial authorization as required.

II. MIT'S ACTIONS VIOLATED TITLE III.

A. Swartz Had a Reasonable Expectation of Privacy in his Electronic Communications to and from his Netbook.[8]

Swartz had a subjective expectation of privacy in electronic communications to and from his netbook, and that expectation is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but "the mere act of accessing a network does not in itself extinguish privacy expectations." *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

> No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.
>
> No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .
>
> No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. In fact, in internal emails, JSTOR described MIT as "unique" in having an open campus. Exhibit 4. Unlike other institutions which require passwords to access their servers and require additional layers of authentication to access digital libraries such as JSTOR, MIT required neither

[8] Swartz incorporates by reference the discussion in Section II of his Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

a password, a formal affiliation with the school, or any form of identification for any visitor to become an authorized guest enjoying access to the MIT electronic communication service which was the equal of that afforded to MIT students and professors.

Swartz was validly signed on to the MIT network as a guest, as the MIT guest policy permitted him to be, as verified by an October 14, 2010, email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to Brian Larsen at JSTOR, informing him that "[o]ur investigations here point to the same *guest* that was involved in the 9/27 incident. We don't have enough information to follow the trail completely, but the signs suggest that the same *guest user* was responsible for this latest activity. . . . all of this excessive use was caused by a *guest visitor* at MIT," Exhibit 5 (emphasis added), and then by an October 18, 2010, email from Ms. Duranceau to Tim McGovern, MIT Manager of Network Security & Support Services:

> Tim and Mike:
> Would it be accurate for me to answer [JSTOR's] query this way:
>
> "*We offer guests access to the MIT network, and this practice will continue*. However, once we [in the future] institute our additional authorization layer for JSTOR, *this route will be closed to guests*. So we will have closed the pathway used."
> * * * *
> Mike, I will be asking JSTOR about your mod_rewrite idea once I check in with Rich Wenger in the Libraries and once JSTOR has shifted more clearly into implementing the new method rather than still working on resolving the excessive use issue.

Exhibit 6 (emphasis added). Thus, MIT had an open-access network that permitted anyone to access it by signing in as a visitor/guest, and anyone signed in to the MIT network was permitted to access JSTOR without further identification or authorization. The name and email address used to sign in as a visitor were fundamentally irrelevant to MIT, as it did not use it in any way to identify the visitor or even to ascertain whether it was a "bona fide identity," nor did guests to the MIT network receive notice that they were prohibited from using static IP addresses, changing IP addresses, or changing MAC addresses when accessing the MIT network on successive occasions. Neither MIT nor JSTOR initiated the additional authorization protocol prior to the seizure of the netbook and Swartz's arrest on January 6, 2011.

That MIT regarded Swartz as a guest user is also confirmed by several other MIT communications during the fall of 2010. On September 29, 2010, Ellen Duranceau informed Brian Larsen at JSTOR that "the origin of the activity was *a guest visiting MIT*." Exhibit 7 (emphasis added). JSTOR is available to "[u]sers [who] come to MIT to establish a guest account on the network, and "do not have to have MIT affiliation to use the content." Summary of Key Points by Ellen Duranceau, Exhibit 8. *See* Email from Ellen Duranceau to Ann Wolpert, October 15, 2010, Exhibit 9 ("we cannot identify the *guest* involved in these incidents" (emphasis added)); Email from Ellen Duranceau to Brian Larsen, October 15, 2010, Exhibit 10 ("[o]ur records and logs . . . do not allow us to definitively identify the *guest*" (emphasis added); Email from Ellen Duranceau to Rich Wenger, October 18, 2010, Exhibit 11 ("it appears that the individual used MIT's wireless network guest account process").

In addition, MIT's written policy on DHCP logs created a reasonable expectation of privacy in *that* information, providing that they would be deleted after 30 days, IS&T Policies:DHCP Usage Logs Policy, available at http://ist.mit.edu/about/policies/dhcp-usage-logs (last visited September 24, 2012), and that they would be disclosed *only* in response to a court order or subpoena:

> When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:
>
> - The date and time of the request
> - The MAC address of the requesting device or computer
> - The IP address provided
> - The specific DHCP command that was issued
> - Other technical information related to the request
>
> In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

> The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.
>
> * * * *
>
> *MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.*

Id. (emphasis added).

Moreover, on many occasions, the MIT RADIUS log server provided further evidence documenting MIT's authorization of Swartz's access to the MIT network:

> **Remote Authentication Dial In User Service** (**RADIUS**) is a networking protocol that provides centralized Authentication, *Authorization*, and Accounting (AAA) management for computers to connect and use a network service. . . . Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. . . . The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server. RADIUS serves three functions:
>
> - to authenticate users or devices before granting them access to a network,
> - *to authorize those users or devices for certain network services* and
> - to account for usage of those services.

http://en.wikipedia.org/wiki/RADIUS (last visited September 23, 2012)(emphasis added). Swartz, accordingly, maintained a reasonable expectation of privacy in the communications to and from his netbook and that expectation was objectively reasonable.

B. MIT's Actions in Intercepting Communications to and from Swartz's Netbook and Disclosure of the Intercepted Communications Violated Title III.

18 U.S.C. §2511(1) prohibits:

> **(a)** intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> * * * *
>
> **(c)** intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the

> information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> **(d)** intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . .

18 U.S.C. §2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . ." Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." "Contents" is in turn defined as "*any* information concerning the substance, purport or meaning" of the communication. §2510(8)(emphasis added).

The packet capture, which targeted the content of data being sent to or from the netbook that was discovered in Building 16's data room, revealed the contents of electronic communications of all electronic communications intercepted. *See* Email from Dave Newman, MIT Senior Network Engineer, to S/A Pickett, January 5, 2011, Exhibit 12 ("I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads"). Use of the packet capture constituted the interception of electronic communications of the defendant and others, including, but not limited to, those with whom he was communicating within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid Title III order authorizing the interceptions of the electronic communications, of which none were sought or issued here.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal No. 11-10260-NMG**
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

GOVERNMENT'S CONSOLIDATED RESPONSE TO DEFENDANT'S MOTIONS TO SUPPRESS

The Court should deny Defendant Aaron Swartz's five motions to suppress (Dkt. Nos 59-63), which attack the manner in which the Government collected the vast majority of electronic and physical evidence in this case.

I. INTRODUCTION

A. The Victims: JSTOR and MIT

A research or university library can find the cost and space to maintain a comprehensive collection of academic journals extraordinarily expensive. Founded in 1995, JSTOR is an independent, self-sustaining, non-profit organization that provides research and university libraries access to numerous academic journals without the normal costs of a paper-based collection. To do so, JSTOR digitizes articles and distributes them over an online system that it built, which enables libraries to outsource the journals' storage, ensures their preservation, and enables them to be searched extensively by authorized users.

JSTOR pays copyright-holders for permission to digitize the copyright-holders' articles and make them available online.[1] To pay its expenses, JSTOR normally charges subscription

[1] Some materials available on JSTOR are not subject to copyright.

generally and at Swartz specifically; and (f) elude detection and identification.

II. THE FACTS

Late during the night of September 24, 2010, an individual registered his computer on MIT's campus and obtained a guest account on MIT's computer network. The individual did not provide his true identity at this or any subsequent time, and neither MIT personnel nor law enforcement officers knew the individual's name until his arrest months later. The individual registered his computer by specifying his name as "Gary Host," a pseudonym, and his e-mail address as ghost@mailinator.com, a disposable e-mail address by virtue of its requiring no initial e-mail registration and keeping no records of e-mail access.[3] Before assigning the computer an IP address, MIT's network automatically collected the computer's owner-created name — "ghost laptop" — and the unique identifying number associated with the computer's Internet networking hardware, known as the computer's Media Access Control or "MAC" address. These are standard login and communication procedures.

MIT's DHCP[4] computer server then used a standard Internet protocol to assign the individual an IP address (18.55.6.215) for use while on the network. The network kept records of the computer's registration information, its IP address, and its MAC address. These records are standard computer-networking records, and did not include any computer commands that the individual typed in or ran, or any data that the computer downloaded. (Exs. 6, 7).

[3] Mailinator advertised itself as a free e-mail service that would accept mail for any e-mail address directed to mailinator.com without need for a prior registration or account; would automatically delete all e-mail after several hours, whether read or not; and would keep no logs (records) of e-mail access.

[4] DHCP is the acronym for Dynamic Host Configuration Protocol.

On September 25, 2010, the day after registering the “ghost laptop,” the individual used the “ghost laptop” to systematically access and rapidly download an extraordinary volume of articles from JSTOR by using a software program that sidestepped JSTOR’s computerized limits on the volume of each user’s downloads. The downloads and requests for downloads were so numerous, rapid, and massive that they impaired the performance of JSTOR’s computers.

As JSTOR, and then MIT, became aware of these downloads and problems, both attempted to block the individual’s computer from further communications. On the evening of September 25, 2010, after suffering hundreds of thousands of downloads from the ghost laptop, JSTOR temporarily ended the downloads by blocking network access from the computer at IP address 18.55.6.215.

The next day, however, the ghost laptop’s user obtained a new IP address from MIT’s network, changing the last digit in its IP address by one from 18.55.6.21***5*** to 18.55.6.21***6***. This defeated JSTOR’s IP address block, enabling the ghost laptop to resume furiously downloading articles from JSTOR. This downloading continued until the middle of September 26, when JSTOR spotted it and blocked communication from IP address 18.55.6.216 as well.

The September 25 and 26 downloads had impaired JSTOR’s computers and misappropriated significant portions of its archive. Because the download requests had originated from two MIT IP addresses that had begun with 18.55.6 — that is, 18.55.6.215 and 18.55.6.216 — JSTOR began blocking a broader range of MIT IP addresses on September 26. The new block prevented MIT researchers assigned MIT IP addresses 18.55.6.0 through 18.55.6.255 (as many as 253 computers) from performing research through JSTOR’s archive for three to four days.

Moreover, when JSTOR notified MIT of the problems, MIT, too, banned the "ghost laptop" from using its network. To do this, MIT terminated the ghost laptop's guest registration on September 27, 2010, and prohibited the computer, as identified by its hardware MAC address, from being assigned a new IP address again through the guest registration process.

On October 2, 2010, less than a week after JSTOR and MIT had barred the individual's ghost laptop from communicating with their networks, the individual obtained yet another guest connection for the ghost laptop on MIT's network. Having recognized that MIT or JSTOR had blocked his ghost laptop by recognizing its MAC address, the individual now manipulated the ghost laptop's MAC address to mislead MIT into believing that he was a new and different guest registrant.[5]

Six days later, the individual connected a second computer to MIT's network and created another guest account using pseudonyms similar to those he had used with the "ghost laptop": he registered the new computer under the name "Grace Host", a temporary email address of ghost42@mailinator.com, and a computer client name of "ghost macbook."

On October 9, 2010, the individual activated the ghost laptop and the ghost macbook to download JSTOR's articles once again. The downloads came so fast and numerous that the individual again significantly impaired the operation of some of JSTOR's computers.

Once again, MIT could not identify who was controlling these computers or where they were physically located, and JSTOR could not isolate the interloper to a consistent IP address

[5] A computer's MAC address is initially assigned by an equipment manufacturer, but can be misrepresented electronically by a knowledgeable user. The user altered the ghost laptop's MAC address to appear as 00:23:5a:73:5f:f***c*** rather than the prior MAC address of 00:23:5a:73:5f:f***b***.

that could be blocked. Consequently, JSTOR blocked access by *every* computer using an MIT IP address campus-wide for approximately three days, again depriving legitimate MIT users from accessing JSTOR's services. And MIT blocked computers using the ghost laptop's and the ghost macbook's MAC addresses as well.

Nevertheless, between the end of October and January 6, 2011, the hacker obtained at least three new IP addresses and assigned his computer two new MAC addresses. He also moderated the speed of the downloads, which made them less noticeable to JSTOR. The exfiltration of JSTOR's collection was nonetheless extreme: over this period, the individual downloaded well over a million of JSTOR's articles.

Because the hacker had modified the speed of his downloads, JSTOR did not notice his latest downloads until around Christmas, 2010. Once noticed, however, JSTOR provided MIT with the hacker's latest IP address. Now that MIT's network security personnel had a more robust set of network tools, they could consult network traffic routing records and trace the IP address back to a concrete physical location on campus.

So on January 4, 2011, an MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16. Building 16's street-level doors have no-trespassing signs posted on them. (Ex. 8). The wiring closet is protected by a pair of locked steel doors. (Ex. 9). The closet is generally locked, but at that time its lock could be forced by a quick jerk of its double doors. When MIT personnel entered the closet, they found a cardboard box with a wire leading from it to a computer network switch. (Ex. 10).[6]

[6] MIT personnel removed the box from the laptop at first, and then MIT personnel or law enforcement officers replaced the box on one or more occasions. The second photograph was taken after the box was replaced, not when it was initially found.

Hidden under the box was the ghost laptop, an Acer-brand laptop, connected to a separate hard drive for excess storage. (Ex. 11). The network cable connected the laptop to the network switch, thus giving the laptop Internet access. (Ex. 12). The laptop's direct connection to the network switch was unusual because MIT does not connect computers directly to those switches.

MIT called campus police to the scene, who, in turn, brought in the Cambridge Police and the Secret Service. Over the course of the morning and early afternoon of January 4th, MIT and law enforcement officers collaboratively[7] took several steps to identify the perpetrator and learn what he was up to:

(1) Cambridge Police crime scene specialists fingerprinted the laptop's interior and exterior and the external hard drive and its enclosure;

(2) MIT placed and operated a video camera inside the closet, which, as discussed below, later recorded the hacker (subsequently identified as Aaron Swartz) entering the wiring closet and performing tasks within it;

(3) The Secret Service opened the laptop and sought to make a copy of its volatile memory (RAM), which would automatically be destroyed when the laptop's power was turned off, but the effort resulted in their seeing only the laptop's user sign-in screen;

(4) MIT connected a second laptop to the network switch in order to record the laptop's communications, a type of recording often referred to as a "packet capture;" the Secret Service subsequently concurred with the packet capture, none of which was turned over to officers until MIT was issued a subpoena after Swartz's arrest;[8]

(5) Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to

[7] From the time of law enforcement's arrival on January 4, 2011, through the suspect's arrest and identification on January 6, 2011, the effort by MIT and law enforcement to identify the individual was both consensual and collaborative.

[8] This second laptop is seen on a chair in Ex. 10.

> the ghost laptop and ghost macbook between September 24, 2010 and January 6, 2011, some of which records were provided consensually, the remainder of which were provided pursuant to a subpoena to MIT.[9]

By mid-day on January 4th, MIT and law enforcement personnel had completed their initial crime scene investigation. Experience told them that merely removing the hacker's computer equipment would just result in his renewing his efforts elsewhere. So, rather than take the hacker's equipment away, MIT and law enforcement instead restored the closet to its initial appearance upon discovery, and monitored who entered it and handled the laptop. In this way, the hacker would not necessarily know that his criminal tools had been discovered, his identity might be uncovered, and he could be stopped.

The ruse worked. Within an hour of their departure, the hacker returned. After entering the wiring closet and shutting the doors behind him, (Ex. 13), the hacker replaced the hard drive connected to the laptop with a new one he took from his backpack, and then concealed his equipment once again underneath the cardboard box.

Two days later, on January 6, 2011, the hacker returned to the wiring closet yet again. This time, worried about being identified, the hacker covered his face with his bicycle helmet as he entered the closet. (Ex. 14). Once inside and with the door closed, the hacker disconnected the laptop and placed it, the external hard drive, and the network cable in his backpack. (Ex. 15). As he left, he again hid his face with his bicycle helmet. (Ex. 16).

By January 6, 2011, the hacker had downloaded a major portion of the 6 to 7 million articles then contained in JSTOR's digitized database.

[9] As discussed below, both the law and MIT's policies and procedures allowed MIT to turn these records over consensually, but it also could, and at points did, insist upon a subpoena.

A little after 2:00 that afternoon, MIT Police Captain Albert Pierce, who had been involved in the investigation, was heading down Massachusetts Avenue within a mile of MIT when he spotted a bicycler who looked like the hacker caught on the wiring closet video. Captain Pierce identified himself as a police officer. After a brief exchange, the individual dropped his bike to the ground and ran away. The individual was chased, apprehended, arrested, and identified as Aaron Swartz. During a search incident to arrest, Cambridge police found a USB storage drive in Swartz's backpack, which they seized and stored as evidence.

Approximately an hour later, MIT technical staff used computer routing and addressing records to locate Swartz's ghost laptop and hard drive in the Student Information Processing Board's office in MIT's student center. Law enforcement found the equipment on the floor under a desk. (Ex. 17). The equipment was subsequently seized and stored as evidence by Cambridge Police.

Aaron Swartz was charged by the Commonwealth in a criminal complaint alleging breaking and entering into MIT's property with intent to commit a felony, and was subsequently indicted by a Massachusetts grand jury for the same charge along with stealing JSTOR's electronically processed or stored data, and accessing a computer system without authorization.

While the Commonwealth pursued state charges, the U.S. Attorney's Office began a separate investigation on January 5, 2011. On February 9, 2011, the Secret Service obtained a warrant to search Swartz's apartment, followed by a warrant to search his office on February 11, 2011. Both were executed on February 11th. Also on February 9, 2011, the Secret Service obtained warrants to seize from the Cambridge Police and then search the laptop, the hard drive, and the USB storage device. These warrants were returned unexecuted and new warrants were

Activity in MITnet computer registration database

Fields:

```
mac, status, account, bcontact, tcontact, ace_type, ace, visit_name, visit_email, visit_phone, visit_sponsor, visit_course, visit_class, visit_total, visit_expires, comment, created_dt, created_tm, created_by, modified_dt, modified_tm, modified_by
```

Registration on Sept. 24:

```
INSERT INTO host_less  VALUES ('00235a735ffb',0,'visitor',NULL,NULL,0,0,'Gary Host','ghost@mailinator.com','','',NULL,NULL,5,'29-Sep-2010','','24-Sep-2010','22:46:19',0,'30-Sep-2010','12:57:46',182635)₩g
```

Registration on Oct. 2:

```
INSERT INTO host_less  VALUES ('00235a735ffc',0,'visitor',NULL,NULL,0,0,'Gary Host','ghost42@mailinator.com','','',NULL,NULL,10,'13-Oct-2010','','02-Oct-2010','10:20:37',0,'13-Oct-2010','05:54:22',182635)₩g
```

Registration on Oct. 8:

```
INSERT INTO host_less  VALUES ('0017f22cb074',0,'visitor',NULL,NULL,0,0,'Grace Host','ghost42@mailinator.com','','',NULL,NULL,5,'13-Oct-2010','','08-Oct-2010','22:13:26',0,'14-Oct-2010','10:45:57',182635)₩g
```

Registration on Oct. 22:

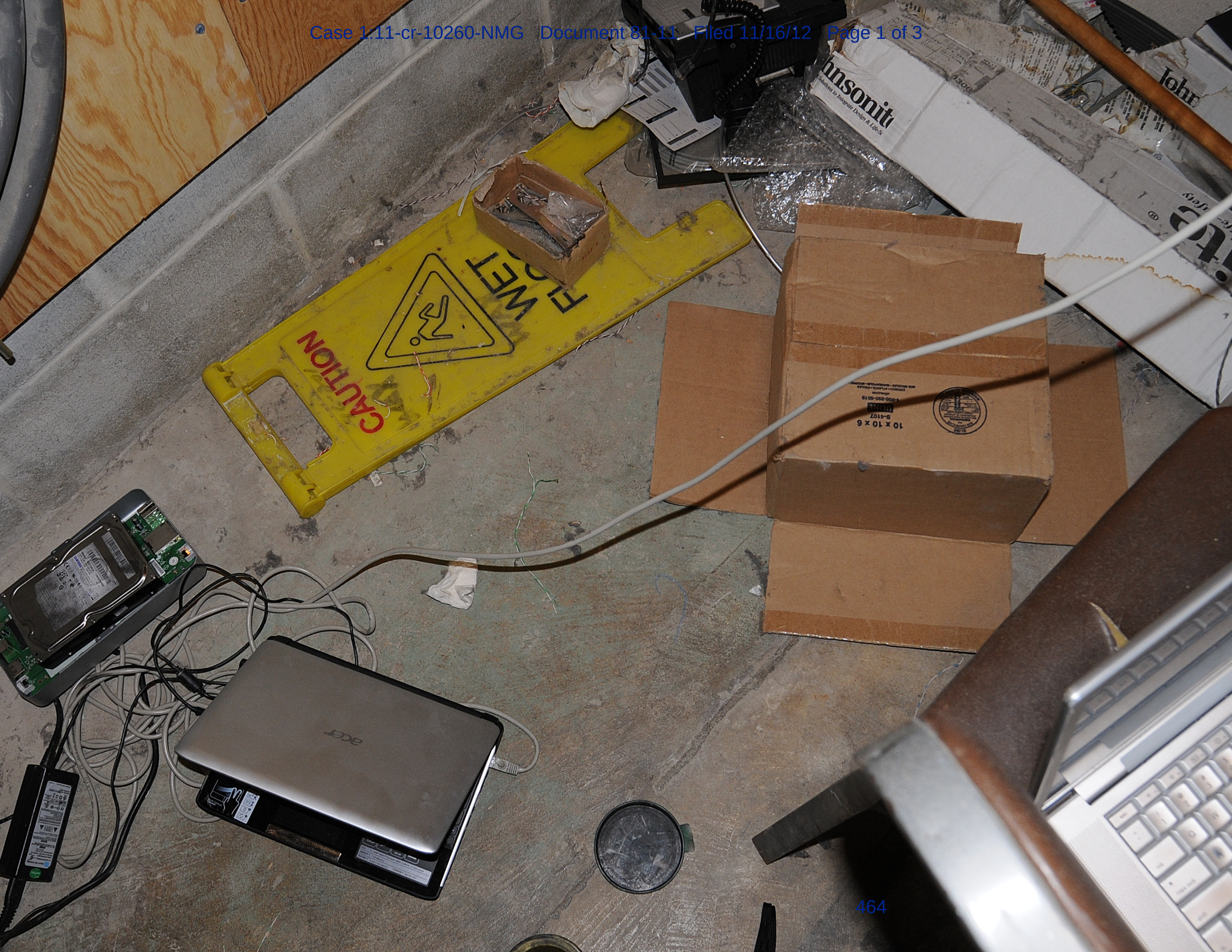
```
INSERT INTO host_less  VALUES ('004ce5a0c755',1,'visitor',NULL,NULL,NULL,NULL,'Grace Host','ghost42@mailinator.com','','',NULL,NULL,10,'11-Nov-2010','','22-Oct-2010','21:39:30',0,'06-Nov-2010','22:12:19',0)₩g
```

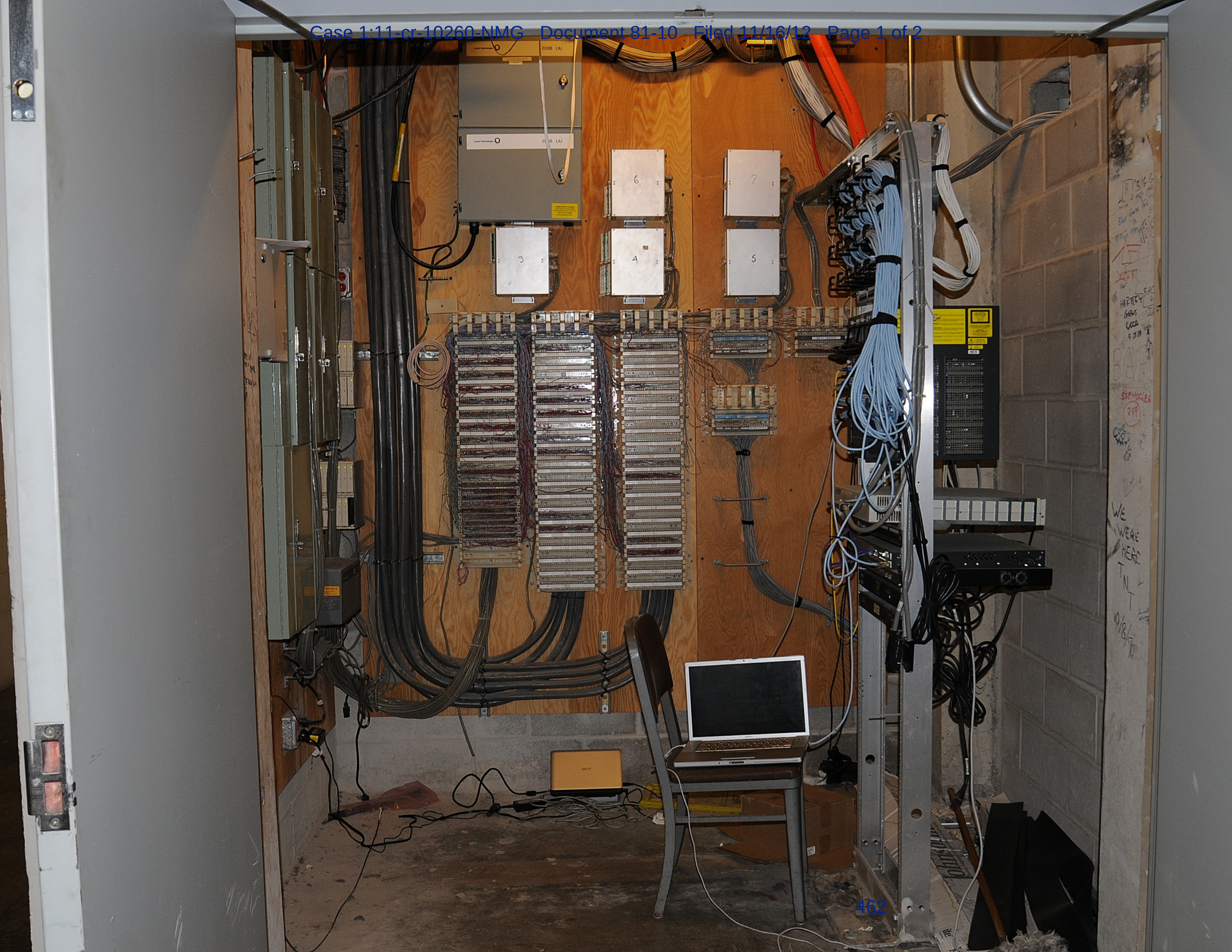
Registration on Nov. 28:

```
INSERT INTO host_less  VALUES ('004ce5a0c756',1,'visitor',NULL,NULL,NULL,NULL,'Grace Host','ghost42@mailinator.com','','',NULL,NULL,2,'07-Jan-2011','','28-Nov-2010','18:29:19',0,'06-Jan-2011','12:44:43',0)₩g
```

Activity in DHCP logs corresponding to computer registration database

```
ghost.txt:dhcplogger/dhcp-20100925.gz:Sep 24 22:45:35 installer dhcpd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20100930.gz:Sep 29 01:31:29 installer dhcpd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20100930.gz:Sep 29 01:39:52 installer dhcpd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101001.gz:Sep 30 18:11:25 installer dhcpd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:20:07 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:20:50 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:20:54 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:26:44 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:27:06 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:27:52 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:28:45 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:29:29 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101003.gz:Oct  2 10:30:29 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101008.gz:Oct  7 01:49:06 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101009.gz:Oct  8 22:12:09 installer dhcpd: DHCPOFFER on 18.2.55.166 to 00:17:f2:2c:b0:74 (ghost-macbook) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101009.gz:Oct  8 22:15:06 installer dhcpd: DHCPOFFER on 18.2.55.166 to 00:17:f2:2c:b0:74 (ghost-macbook) via 18.55.0.1
ghost.txt:dhcplogger/dhcp-20101009.gz:Oct  8 22:58:57 installer dhcpd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1
ghost-laptop_dhcp_01062011.txt:dhcp-20110107.gz:Jan  6 12:42:49 installer dhcpd: DHCPOFFER on 18.2.53.219 to 00:4c:e5:a0:c7:56 (ghost-laptop) via 18.53.0.1
```


CAUTION
WET FL
hnsonit
Solutions to Integrate Design & Life-S
Johr
ULINE
10 x 10 x 6
S-4107
1-800-295-5510
acer


200B LIU
200B LIU
6
7
3
4
5
WE
WERE
HERE
T N T
10/8/10

M.I.T. POLICE
301 VASSAR ST CAMBRIDGE, MA

INCIDENT # / REPORT #	OFFICER	RANK	REVIEW STATUS
11000351 / 1	JPERAULT	DETECTIVE	APPROVED by JPERAULT

INCIDENT #11000351 DATA

As Of 01/06/2011 16:19:21

BASIC INFORMATION

CASE TITLE	LOCATION	APT/UNIT	CITY, STATE
B&E	21 AMES ST		CAMBRIDGE, MA

DATE/TIME REPORTED	DATE/TIME OCCURRED
01/06/2011 14:20:45	On or after 01/04/2011 15:26

INCIDENT TYPE/OFFENSE
B&E DAYTIME FOR FELONY c266 S18

PERSONS

ROLE	NAME	SEX	RACE	AGE	DOB	PHONE
VICTIM	MIT,					(HOME)
	ADDRESS: [redacted] CAMBRIDGE, MA					(CELL)

OFFENDERS

STATUS	NAME	SEX	RACE	AGE	DOB	PHONE
DEFENDANT	SWARTZ, AARON H	MALE	UNKNOWN	24	[redacted]	(HOME)
	ADDRESS: , IL					(CELL)

[NO VEHICLES]

PROPERTY

CLASS	DESCRIPTION	MAKE	MODEL	SERIAL #	VALUE

OFFICER REPORT: 11000351 - 1 / JPERAULT (DETECTIVE)

DATE/TIME OF REPORT	TYPE OF REPORT	REVIEW STATUS
01/06/2011 14:20:45	INCIDENT	APPROVED

NARRATIVE

On January 4, 2010 at approximately 10:30 hours I responded to MIT building 16, room 004T for a report of a past break. This room is a telephone closet and networking closet; it's access is controlled by MIT's IS&T Department. David Newman of MIT IS&T explained to me that someone had entered the restricted room and connected a laptop and external hard drive directly to a networking switch. The laptop and external hard drive were being hidden under a cardboard box. Newman further explained that they were able to determine that this laptop was illegally downloading scientific periodicals from JStor, a subscription based database that houses academic periodicals.

Cambridge Police Detective Joseph Murphy, Special Agent Michael Pickett from the United States Secret Service and Boston Police Officer Tim Laham responded to building 16 room 004T. Cambridge Police's Crime Scene Services also responded and processed the laptop and external hard drive for latent prints. It was determined that the laptop would be left in place and IS&T would monitor the network traffic in an attempt to identify the suspect. A camera was also installed by MIT's IS&T Department to monitor the area.

On January 4, 2010 at approximately 15:26 hours a white male, dark or black shoulder length wavy hair, wearing a dark coat, gray backpack, jeans with a white bicycle helmet enters the room. It appears as thought the suspect takes a hard drive out of his back pack and bends over the laptop and external hard drive. He exits the room moments later.

On January 5, 2010 MIT's IS&T Department informed me that approximately 70 gigabytes of data had been downloaded, 98% of which was from JStor. SA Mike Pickett had informed me that MIT's IS&T had put an approximate value on the dowloaded information at $50,000.

On January 6, 2010 at approximately 12:32 hours a white male, dark or black shoulder length wavy hair, wearing a dark coat, gray backpack, jeans with a white bicycle helmet enters the room, I was monitoring the video feed at the MIT Police Department at this time. It appears as thought the suspect packed up the laptop and hard drive and exited the room. MIT Police units responsed to the area and searched for the suspect. A check of the room determined that the laptop and hard drive had been removed.

On January 6, 2010 at approximately 14:11 hours Captain Albert Pierce of the MIT Police Department called me and stated he had located the suspect riding his bike on Massachusetts Ave at Lee Street. Special Agent Pickett and I responded to the Lee Street to assist Captain Pierce. The suspect jumped off his bike when encountered by Captain Pierce and ran down Lee Street. Captain Pierce and Special Agent Pickett were able to apprehend the suspect at 24 Lee Street. He was handcuffed by SA Pickett.

The suspect encountered by Captain Pierce and apprehended on Lee Street is the same person seen on video entering the restricted telephone closet in building 16 on January 4th at 15:26 hours and on January 6th at 14:11 hours.

He was arrested for two counts of Breaking and Entering in the daytime with the intent to commit a felony, Chapter 266 Section 18.

From: MICHAEL PICKETT (BOS) <Michael.Pickett@usss.dhs.gov>
Sent: Friday, January 7, 2011 3:25 PM (GMT)
To: Heymann, Stephen (USAMA) <Stephen.Heymann@usdoj.gov>
Subject: RE: Swartz Case

The laptop and external hard drive have been logged into evidence with MIT police. Cambridge Police will take the laptop and hard drive to process them for prints this morning. I am prepared to take custody of the laptop anytime after it has been processed for prints or whenever you feel is appropriate. As far as I know no one has sought a warrant for the examination of the computer, the cell phone that was on his person or the 8gb flash drive that was in his backpack. FYI the laptop and external hard drive were not on his person when he was arrested. They were traced by the laptop MAC address on the network, in a computer room in the MIT student center.

Mike Halsall has already provided me with a copy of the flow traffic. David Newman has made the packet capture available for download. I will download it today.

I will ask Mike Halsall for a copy of the surveillance.

Jay A Perault is the Captain from MIT Police that has been working with me during this investigation and was present during the arrest of Aaron Swartz.

Michael S. Pickett
U.S. Secret Service
Boston Field Office

(the following is not part of the archives)

```
λ>  (\x -> "curl" ++ " -O" ++ " www.jstor.org/pdfs/" ++ x ++ ".pdf") "landau_siegel"
"curl -O www.jstor.org/pdfs/landau_siegel.pdf"
```

I forgot to answer the most basic or obvious question regarding keepgrabbing.py, so I'll do it here.

- Why was the program called 'keepgrabbing'?

Well, because that's what it did. It just kept downloading without interruptions.

That's because of the "while 1:" statement.

e.g.

```
while 1:
  print "keepgrabbing"
```

output :

```
keepgrabbing
keepgrabbing
keepgrabbing
keepgrabbing
keepgrabbing
keepgrabbing
keepgrabbing
...
```

The only way to interrupt it would have been through a command-line interrupt (^C) / KeyboardInterrupt.

At least that's my (current) understanding of it. - It's still preferable to no explanation at all.

(If this had been a novel or any other work of art, it would have ~~perhaps~~ probably been more evident that such questions ought to be answered…)