THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

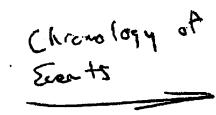
THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW BLACKVAULT COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

		**************************************			ረም ዘል _{ከማ}
	A CONTRACTOR OF THE PARTY OF TH				
~ · · · · · · · · · · · · · · · · · · ·	IA		BJ	C	Herman Control
		10-6	2	femile ess	
			Mec	23.5	
	(b)(6),(b)(7)(C)		(0)(6),(0)(7)	(C)	
	(0)(0)(0)(7)(0)				
	67		(b)(6),(b)(7)(C)	†. 7000000000000000000	
		,			
				5	
		and the second s			
					2.1
		(D)(6),(b)(7)(C)		
		,			
(b)(6)),(b)(7)(C)				
					507



(b)(6),(b)	(7)(C)				
From	(BOS) (mailt	(b)(6),(b)(7)(C)			
Sent: Wednes	day, January 05, 2011 11	:23 AM			
101	thorized Activity on the N	A SECTION AND ADDRESS OF THE PARTY OF THE PA			
(b)(5)	anoused vertaith ou tile in	11T network			<u> </u>
(0)(0)					
On 01/04/11 De	etective (b)(8),(b)(7)(C)/ α as Task Force received a	644			
Electronic Crime	ts Task Force received a	of the Cambridge Pol	ice Department and	a member of the New F	nelsod
· AMEMINET FOIL	THE THEFT OF AMERICAN AND A SECOND	. —		THE MISSESSEE COMMISSION OF THE PARTY OF THE	
suggested that t	the computer was being a control of Building 16, the Do	used to download to		IL CHI MILL SPANINGE and M	advisoration and the
Freineering Day	ent of Building 16, the Do Partment	rrance Building (77	Massachusette Aven	computer was found in	a wire closet
from the library	hat on 01/03/11 the fibra without authorization. L	ry had notified him t	that someone was di	ownloading large number	
				ling was first noticed by	rs or journals the library sa
Was enis	W trace the activity to a	manda.d	The state of the s	**************************************	A (94) /L\/0\ /L\/7\/0\
LUSAXODODIOO1	ve was connected to the 100E1601. The netbook	netbook. The netbo	ok was an Acer Asni	iter connected to the sw	itch. An
- / Smill to Will but	100 An 12/21/4A Feb.	The second of	nous of all West DELD		69E/10000428-00E0
Which are IP adds	rece holomelanda a am	magical phemist (O D	e using two ip addre	e	reported as
the default port i	or SSH (Secure Shell networks) traffic. Cambridge Police	Abus puntocon and a	that the netbook had	port 22 and 8092 open	(b)(8),(b)(7)(C)
	Manue Cambrida - a. o.	•	miss w Alfel		
TO THE STATE OF TH	rs Ariellasika (a.a.t. J	A 44 A	TO THE PERSON OF		-AL4
with the user "Ge	system was Ubuntu, a ty ne Host" logged in. The i	pe of Linux. The log	in screen showed a	ompiter name of feb.	ated that the
futile (b)(6),(b)(7)	ne Host" logged in. The I	login screen had a pa	issword. All efforts t	O bypass the loan scree	it-raptop"
PPLACE CEDILED IS A	MRM+MAIL_1 \~/\~/!\~/\~/\~		an out 344 (CN) W	DUNC MAM AN MARIA IS A .	4 .4
ALTON SOCIETIES				ivila, un ind menuse t	A
hopes of capturing	More sehwel	A	recen in idage till U	CLDOOK stimping in alaca	andak ak
ne istable asus	C.CAN Chross williams also		ONLY OF CHE LIE	(COOK TRIMINAL CCM .L.	فا اسم أمحد
M Anset As it file 70	USDOCT ratiums for the	Marie and a		I Discret a camera in the	s seebee eleans
View the lournake	The technical journals but are ilmited as to how	eing downloaded ha	ve a monetary value	· All MIT stackage have	t is removed
they graduate have	e to come a cubetantial make		MARCHINE OF STREET	TSIGE OF MIT including st	succió (O uriente afra-
\$200.00 to \$3,000.	e to pay a substantial sub 00. Total value of the do	ecription to access to	he files. The price fo	r downloading one file c	an vary from
• • • • • • • • • • • • • • • • • • • •	At FINE (NO	MINAGER SIES CONC	De in excess of \$50,	000.00.	7 11 4371

At 1526 on 01/04/11 this individual came back and appears to be replacing the external drive:

Hus 2 IP or Sie kac MAC Possible Untuel interferce. July 16 Ser fuller 9/29 JSTBR 10/12 Meet 24 11/23 exissue doubloiding 3 Tutorial IP 5 Publicul, Acces Switch sectionity to Statel 195ing at 20900 /14/11 Suspect Auron Sunta take into custily Saw Ping from China Parus H Swartz DOB 8 NOV 1986 Different MAC Addresses have been used Passport 029801374 Jayport 14 Ry 12,70 host

work a Afriduit	1/19/11 Conf Cell
<u>β SSV</u> (8),(b)(7)(C)	Hey man talked to (DX6).(DX7)(C) yesterd 1/18/11 obot direct contact / MIT
5),(b)(7)(c) Solution So	De at (b)(6),(b)(7)(C) an taffic at SSH came I had exalled
(b)(6),(b)(7)(C) [all (b)(6),(b)(7)(C)	(b)(6),(b)(7)(c) = BOP SSW = Acure +
Call Lel or Hur (bX6),(bX7XC)	(b)(6),(b)(7)(C)

```
D15Doc10 (FW MIT undate It's worse than we know).txt

Heymann, Stephen (USAMA) (b)(8),(b)(7)(C)(Busdoj.gov)

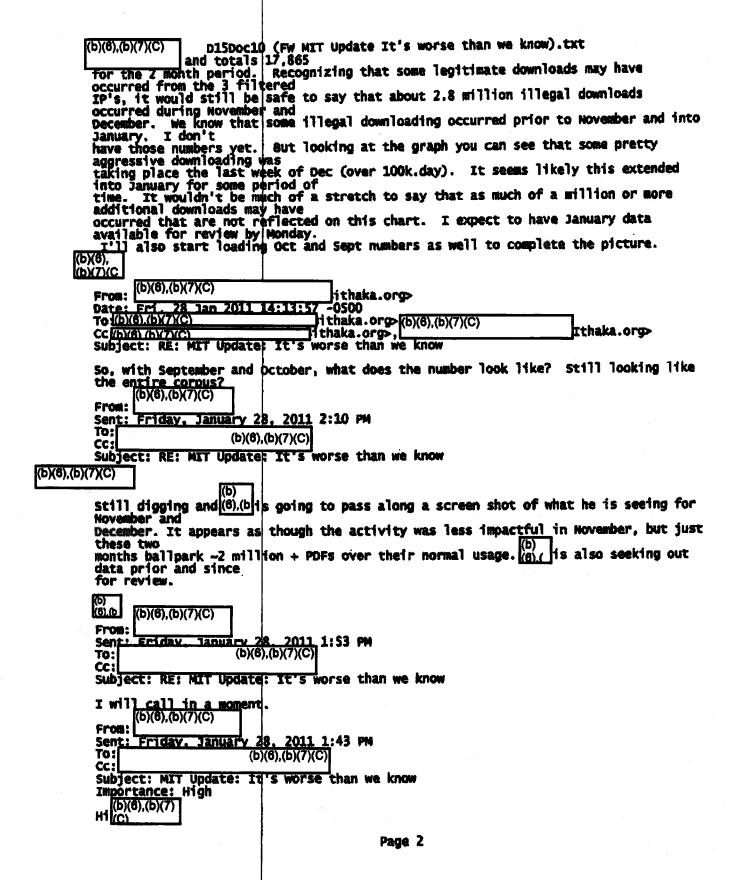
Wednesdav, February 02, 2011 8:32 AM

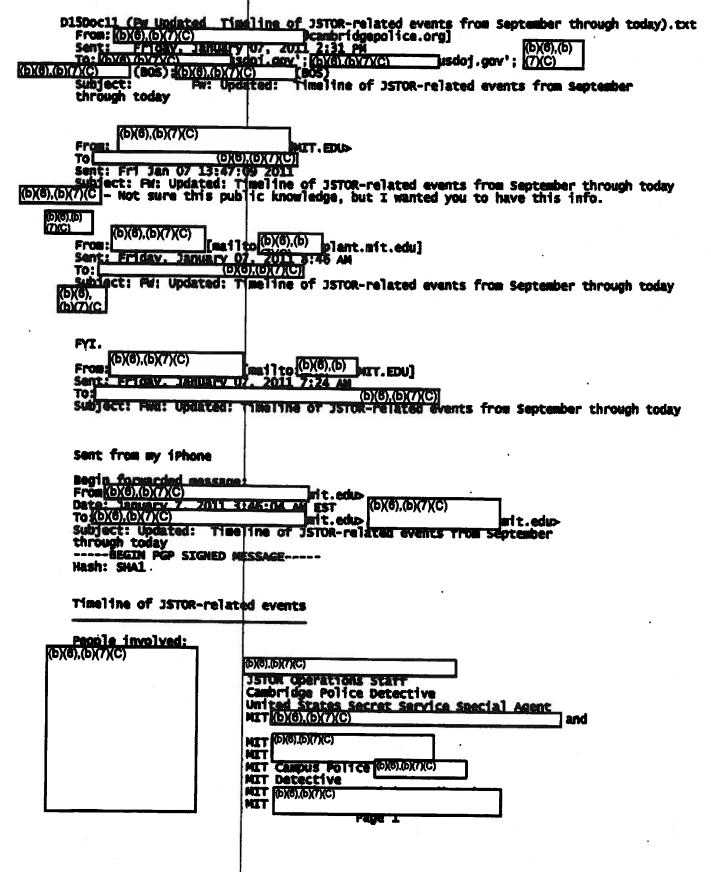
(BOS); External(b)(8),(b)(7)(Cambridgepolice.org)

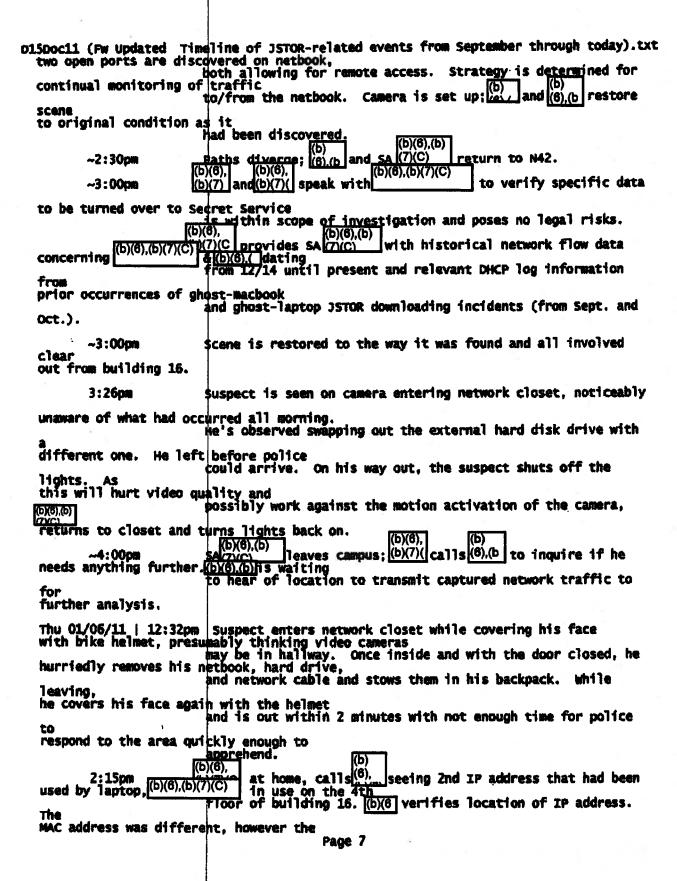
FW: MIT Update: It's worse than we know
From:
Sent: Wednesd
To: (b)(6),(b)(7)(C)
Subject:
From: (b)(8),(b)(7)(C) [mai to (b)(8),(b)(7)(C) ithaka.or Sent: Friday, January 28, 2011 3:05 PM To: Heymann, Stephen (USAMA) Subject: FW: MIT Update It's worse than we know
From: (b)(8),(b)(7)(C)
                                                                        ithaka.org]
... and this too.
From: (b)(6),(b)(7)(C)
Sent: Friday.
To: (b)(6),(b)(7)(C)
                                               2011 3:02 PM
                          January 21
Subject: RE: MIT Update It's worse than we know I do know from (7)(C) initial analysis that the
                                           initial analysis that the downloading was done
systematically using sequential increases in our stable URLs. That is, get stable URL 12345, get stable URL 12346,
12347, 12348 and so
This tells us a few things. One, that the previous activity was similar to the pattern(b)(6) is seeing. That is, not targeted towards types. Two, it lends credence to an entire corpus grab
approach. Don't care what it is I am getting, just get me the next one.
           (b)(6) (b)(7)(C)
From:
                                               2011 2:50 PM
Sent:
           Friday, January 28
To:
Cc:
                     (b)(6),(b)(7)(C)
 Subject: Re: MIT Update: It's worse than we know
This doesn't appear to be targeted towards research articles or any particular titles, collections, or disciplines.

For the 2.8 million in Nov and Dec, the breakdown by article type is:

Research articles - 1,385,569
 Reviews - 938,063
Misc - 459,457
News - 62,127
Editorial - 9,472
 Those numbers more or less correlate to the corpus as a whole. I'd say the he was
 going after everything.
From: (b)(6),(b)(7)(C)
Data: Eri 28 Jan 2011 14:28:43 -0500
To:((b)(6),(b)(7)(C)
Cc((b)(6),(b)(7)(C)
Subject: Fthaks one
                                                                              (b)(6),(b)(7)(C)
                                                                                                                                ithaka.oro
 Subject: Re: MIT Update: It's worse than we know
 Attached are 2 screen shots depicting PDF download activity from MIT for November
and December. One show's all downloads and totals 2,854,824 for the 2 months. The other filters out downloads from the 3 IP's that look to be associated with the download abuse (b)(6),(t)
                                                                                                                                           (b)(6),(b)(7)(C)
                                                                       Page 1
```

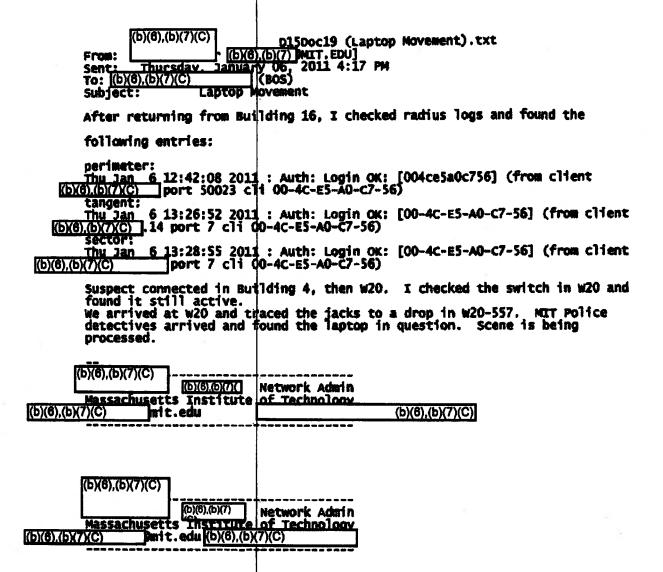






D15Doc11 (Pw Updated Timeline of JSTOR-related events from September through today).t	ĸŧ
3:42pm (b)(6),(b) (7)(C) calls Det $(7)(C)$ to request police presence prior to	
group entering the SIPB offices to check the room for the netbook.	
4:00pm Det. $\frac{(b)(6),(b)}{(7)(C)}$ and SA $\frac{(b)(6),(b)}{(7)(C)}$ arrive outside w20 room 557. The	
students present are asked by Det. (b)(6),(b) if they saw anyone drop off a silver laptop computer; they all	
respond they'd only been there and had seen no computer. The room is searched by all (b)(7)	
locates the laptop, nearly placed under a table in a corner abutting a filing cabinet. The netbook	
is plugged in to a network jack about 6 feet away and is sitting on an external hard drive, attached, the	
way it had been when in building 16. (b)(6),(b) 54(7)(C) dons gloves and proceeds to examine the netbook.	
appeared to be in a halfway shutdown state and all attempts to access a terminal on the machine	
were unsuccessful. It was determined that there was no feasible way to do live forensics on the computer in	
attempt to capture a snapshot of current $(b)(6),(b)(7)(C)$ placed a call to the Cambridge police	
netbook. to inquire about getting another fingerprint exam for the	
4:45pm The group returns to w92 and meets with (6) , to debrief. 5:30pm $(b)(6),(b)(7)(C)$ $(b)(6),(b)(7)(C)$ office to join a	
conference call with (b)(6),(b)(7)(C) (to brief them on the technical details of the	
sequence of events which enabled the group to locate the netbook. The call was concluded ~6:00.	
A rough approximation of MIT's staff's time spent on incident since September: 160 hours in aggregate.	
(b)(6),(b)(7)(C)	
IT Security Systems & Services, IS&T	
6),(b)(7)(C)	
PGP public key ID: 9E62D0E6 http://pgp.mit.edu BEGIN PGP SIGNATURE Version: GnuPG v1.4.8 (b)(6),(b)(7)(C)	
(b)(8),(b)(7)(C)	
Page 9	

D15Doc11 (Fw Updated Timeline of JSTOR-related events from September through today).txt [6](8),(6)(7)(C)



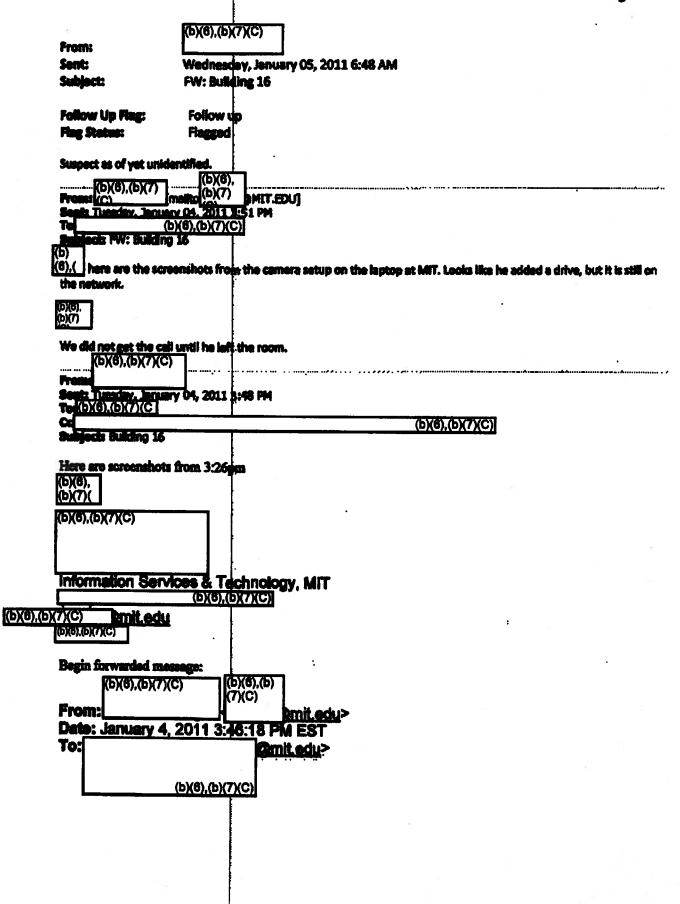
disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it. /doi.org/10.1007/j.co

The proper statement of the Secret Service. If you have captured the secret service. If you have captured the secret service." | Additional common captured the secret service. If you have captured the secret service." | Additional captured the secret service. If you have capture

Page 2

From: (b)(6),(b)(7)(C)
Sent: Wednesday, February 02, 2011 3:13 PM To: (bX6) (bX7)(C) (80S)
CC: External (b)(6) (b)(7 cambridgepolice.org Subject: Re: grade host and ghost macbook registration email
BEGIN PGP SIGNED MESSAGE Hash: SHAl
Host Lookup
visitor registration name: Gary Host email: ghost420mailinator.com phone:
days remaining: 4 last expiration date: 13-oct-2010 MAC address: 00235a735ffc status: inactive comment:
please include (b)(6),(b)(7) (b)(6),(b)(7) (c) (d)(6),(b)(7) (e)(7) (e)(
- From the DHCP logs:
dhcplogger/dhcp-20101009.gz:Oct 8 23:02:05 installer_dhcnd: DHCPACK on 18.55.7.48 to 00:23:5a:73:5f:fc (ghost-laptop) via (b)(8),(b)(7)(dhcmlogger/dhcp-20101009.gz:Oct 8 23:13:49 installer dhcpd: DHCPACK on (b)(8),(b)(7)(C) to 00:17:f2:2c:b0:74 (ghost-macbook) via eth0
On Feb 2, 2011, at 1:04 PM, (b)(8),(b)(7)(C) (BOS) wrote:
> Do remember what email was used on 10/08/10 when ghost macbook and Grace
Host was registered? > (b)(6),(b)(7)(C) >
> U.S. Secret Service > Boston Field Office > (b)(6),(b)(7)(C)
*
> All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that
is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further
is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Version: GnuPG v1.4.8 (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
END PGP SIGNATURE

Page 1



which is the JSTOR journal downlos that identifies a command and con
which is the JSTOR journal downlos that identifies a command and com
which is the ISTOR journal downloo that identifies a command and com
which is the JSTOR journal downlos that identifies a command and com
which is the LSTOR journal downlos that identifies a command and com
which is the ISTOR journal downlos that identifies a command and com
which is the JSTOR journal downloa that identifies a command and com
which is the JSTOR journal downlos that identifies a command and com
which is the JSTOR journal downloa that identifies a command and con
that identifies a command and com
,

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

Case continued in Boston. DETAILS OF INVESTIGATION: (b)(6),(b)(7)(C) of the Cambridge Police Department and On 01/04/11, Detective a member of the New England Electronic Crimes Task Force, received a call MIT.EDU) of the Massachusetts Institute from (b)(6),(b)(7)(C) of Technology Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet of the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department. Detective (b)(6),(b) and Detective (C) (b)(6),(b)(7)(C) Also on 01/04/11, SA (b)(6)(b)(7)(C) of the Boston Police Department, traveled to MIT and met with(b)(6)(b)(7)(C) (b)(6)(b)(7)(C) mit.edu) of the MIT Police (b)(6)(b)(7) and (b)(6)(b)(1) in the (b)(6),(b)(7)(C) basement of building 16. Criminalist (b)(8),(b)(7)(C) and (b)(8),(b)(7)(C)Cambridge Police processed the scene for prints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAX0D001001100E1601. Hetwork traffic indicated that the netbook was using two IP addresses and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook. Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male later identified as Aaron Swartz (DOB 11/08/86) enter the wire closet. Based on the surveillance video, Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him. (b)(8),(b) (b)(6),(b) (7)(C) was able to provide SA(7)(C)Further on 01/04/11, with the following timeline:
[(b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) On 09/26/10. received an email from (6)(8) (6)(7)(C) the JSTOR (6)(6)(6)(0)(7)(C) stating that at 0800 excessive downloading of journals had been detected from MIT and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT. On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C)the MIT (6)(6),(6)(7)(C) Scholarly Publishing and Licensing, regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(8),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu),(b)(6),(b)(7)(C) Analyst, discovered network registration for "Gary Host" with email address ghost@maillinator.com, a MAC address of 00235a735ffb and

Information Services and Technology (IS&T)
Messachusetts Institute of Technology

Room (6)(8),(6)(7)

Cambridge, MA 02139

(b)(6),(b)(7)(C) (b)(8),(b)(7)(C) **mit.**,

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.