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!

Still digging and $\binom{(b)}{(b)}$ is going to pass along a screen shot of what he is seeing for Novembrush the activity was less impactful in November, but just these two months ballpark normal usage $\binom{(b)}{(c)}$ is also seeking out data prior and since for review.	ber and December. It a ~2 million + PDFs over	oppears as their
(D)(0). (D)(7)(
Fronti (b)(6),(b)(7)(C) Septs Friday, January 28, 2011 1:53 PM	***************************************	
To (b)(6),(b)(7)(C) Cc Subject: RE: MIT Update: It's worse than we know		
I will call in a moment.		
From Sant: Friday, January 28, 2011 1:43 PM	Manager and a street of the st	
Te (b)(6),(b)(7)(C)		
Subject: MIT Update: It's worse than we know Importance: High (b)(6),(b) HI (7)(C)		
Speaking with $(b)(6),(b)(7)$ just now about making ours we have $(7)(C)$ time as needs currently underway and discovering that the IP addresses associated with these specific additional days of mass downloading.	d for the MIT evaluation incidents have numer	
It would take some time to normalize against usual MIT usage, but at first glance, it is re what band I covered that the individual responsible has already acquired the entire it ASAP if you think it useful and I let know that I thought you might be calling him sho for clarification. In light of this information, it would seem that we need to try and under the identified incidents going forward. Certainly our tack here merits some re-evaluation the potential for additional measures of prevention as we move forward. Also copying in	STOR corpus. Glad to I ortly after receiving thi rstand the full picture o <u>both</u> concerning this	nave a call is message outside of i case and
(b)(d),(b)(7)(C)		
Thanks,		
(b)(6),(b)(7)(C)		
JSTOR Portico		
)(6),(b)(7)(C) theke,org		

me to be	
	Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Freeze	Preymant, Supmen (USAMA) CAMA CAMA CAMA CAMA CAMA CAMA CAMA
Sent	Monday, February 07, 2011 11:18 AM
Tes	(b)(6),(b)(7)(C) BOS); External (b)(6),(b) ambridgepolice.org
Subject:	FW: MIT Update: It's worse than we know
From (C) Sent: Friday, January To: Heymann, Stephe Subject: FW: MIT Up	
and this too.	*
(b)(6),(b)(7)	A STATE OF THE PROPERTY OF THE
From (C)	
Santa Priday, January	28. 2011 3:02 PM
To: (b)(6),(b)(7)(C)	
(b)(6),(b)	(7)(C)
Subject: RE: MIT Up	date: It's worse than we know
I do know from (b)(7) stable URLs. That is, g	initial analysis that the downloading was done systematically using sequential increases in our et stable URL 12345, get stable URL 12346, 12347, 12348 and so on.
This tells us a few thin towards types. Two, it the next one.	gs. One, that the previous activity was similar to the pattern (b) is seeing. That is, not targeted tends credence to an entire corpus grab approach. Don't care what it is I am getting, just get me
SV81	
b)(7)	
/ /5//8/7/5///6/	The state of the s
(b)(6),(b)(7)(C)	
Sont: Friday, January	28, 2011 2:50 PM
Te	
	(8),(b)(7)(C)
Subject: Ke: MIT Upo	late: It's worse than we know
11	be targeted towards research articles or any particular titles, collections, or disciplines. For the 2.8
	the breakdown by article type is:
Research articles - 1,38	15,569
Reviews - 938,063	
MISC - 459,457	
News - 62,127	
Editoriei – 9,472	
Those numbers more o	r less correlate to the corpus as a whole. I'd say the he was going after everything.
(b)(8),(b)(7)(C)	Pithaka.ore>
Onto: Fri. 28 Jan 2011	
Te (b)(0),(b)(7)(C)	hthela.org

Cc thake.org> 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),(b)(7)(C) and totals 17,865 for the 2 month period. Recognizing that some legitimate downloads may have occurred vrom the 3 filtered iP's, it would still be safe to say that about 2.8 million illegal downloading occurred prior to November and into January. I don't have those numbers yet. But looking at the graph you can see that some pretty aggressive downloading was taking piece the last week of Dec (over 100k.day). It seems likely this extended into January for some period of time. It wouldn't be much of a stretch to say that as much of a million or more additional downloads may have occurred that are not reflected on this chart. I expect to have January data available for review by Monday. I'll also start loading Oct and Sept numbers as well to complete the picture.
(b)(8), (b)(7)(
From (b)(6),(b)(7)(C) thaka.org> Date: F4, 28 Ian 2013 14:13:57-0500 Te(b)(6),(b)(7)(C) thaka.org> Subject: RE: MIT Update: It's worse than we know So, with September and October, what does the number look like? Still looking like the entire corpus? From (c) Sent: Friday, January 28, 2011 2-10 PM To (b)(6),(b)(7)(C) Subject: RE: MIT Update: It's worse than we know [D)(6),(b)(7) Still digging and (b) is going to pass along a screen shot of what he is seeing for November and December, it appears as though the activity was less impactful in November, but just these two months belipark "2 million + PDFs over their
normal usage (b) also seeking out data prior and since for review.
(e).
Prems Santa Friday, Jenusou 28, 2011 1453 PM Ten (b)(6),(b)(7)(C) Cos Santa Friday, Jenusou 28, 2011 1453 PM Ten (b)(6),(b)(7)(C) Santa Friday, Jenusou 28, 2011 1453 PM Ten (b)(6),(b)(7)(C)
t will call in a moment.
Frem (b)(6),(b)(7) Sentz Fifdey, January 28, 2011 1:43 PM To (b)(8),(b)(7)(C) Sussificit: Fir Update: It's worse than we know

OF THE RESIDENCE OF THE PROPERTY OF THE PROPER		
	(b)(d),(b)(7)(C)	
Prom:	V) = = = = = = = = = = = = = = = = = = =	cambridgepolice.org>
Sent	Wednesday, February 0	2, 2011 657 AM
Tec	Heymann, Staphen (US/ RE: MIT Update: It's wor	AMA)((b)(6),(b)(7)(C) BOS)
Subjects	ME MIT UPDATE TE WOT	es than we know
Got it		
Premi Heymann, Stephen (US	(b)(6),(b)(7)(C	usdol.gov]
Bents Wednesday, February 0		
Te:(b)(6).(b)(7)(C) (BOS);		
Subjects FW; MET Update: It's		
From: (b)(6),(b)(7) [melto	b)(8),(b)(7)(C)	
Sent: Friday, January 28, 201:	1 3:05 PM	
Ter Heymann, Stephen (USAM		
Subject: FW: MIT Update: Ith	s worse than we know	
4464 4		
and this too.		
(b)(6),(b)(7)		
From (C)		
Soutz Eddisy, January 28, 201 Tol(b)(6),(b)(7)(C)	L3:02 PM	
Cc (b)(6),(b)(TVC	
Subject: RE: MIT Update: It's		
(b)(d),		
	analysis that the download	ing was done systematically using sequential increases in our
		12346, 12347, 12348 and so on.
		(6)
This tells us a few things. Ona,	that the previous activity v	ras similar to the patiern(6), is seeing. That is, not targeted
towards types. Two, it lends or	edence to an entire corpus	grab approach. Don't care what it is I am getting, just get me
the next one.		100 100 1
(5)		
(6) (6), (b),77		
(b)(8),(b)(7)(C)		
Promis		
Sent: Friday, January 28, 2011	2:50 PM	
Tos (b)(b) (b)(7)(C)		
Cc (b)(6),(b)(7) Subject: Re: MIT Update: It's	(C)	
sombses we: wri obcars: its	MOISE CHIEF ME MICH	
This desen's appear to be terrest	ad towards research articles	or any particular titles, collections, or disciplines. For the 2.8
million in Nov and Dec, the brue		or milk hat transmit strikes american de americanent, i en ana em
Research articles - 1,385,569	waster of or other rates	•
Reviews - 938,063		
Misc - 459,457		
News - 62,127		
Editorial - 9.472		

	Haymann Stanban (USABAA) (b)(6),(b)(7)(C)	
From:	rieginaliti, Stepheli (Ozalivia)	OV>
Sent:	Wednesday, February 02, 2011 8:32 AM	
To:	(b)(6),(b)(7)(C) BO\$); External (b)(6),(b) pcambridgepoli	ce.org
Subject	FW: MIT Update: It's worse than we know	
	(4)	
(b)(6),(b)(7)(0	(C) (b)(G) (b)(7)(O) (b)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)	y ny ara-ara-dahampi ara-ara-ara-ara-dah 1997 yilyong-periodenan-ara-ara-
From:	mailto (b)(6),(b)(7)(C) pithaka.org]	
To: Heymann, Step	ary 28, 2011 3:05 PM	
	Update: It's worse than we know	
ampace en riti	opaste. It's worse uigh we know	
and this too.		
W DITH SHIP (DOI		
(b)(6),(b)(7)	THE RESERVE THE PROPERTY OF TH	A CONTRACTOR OF THE PARTY OF TH
From Control Tonor	 ary 28, 2011 3:02 PM	
To:	aiy 20, 2011 5.02 PM	
Cc	(b)(6),(b)(7)(C)	
	Update: It's worse than we know	
(b)(<u>·</u>	
(0)((0),	
I do know from(b)((7)(C linitial analysis that the downloading was done systematically using :	sequential increases in our
	$\overline{(7)(C)}$ initial analysis that the downloading was done systematically using 9 s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on.	sequential increases in our
	(7)(C initial analysis that the downloading was done systematically using so, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on.	sequential increases in our
stable URLs. That is	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on.	
stable URLs. That is This tells us a few ti	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern (6) , is see	eing. That is, not targeted
stable URLs. That is This tells us a few ti towards types. Two	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on.	eing. That is, not targeted
stable URLs. That is This tells us a few ti	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern (6) , is see	eing. That is, not targeted
stable URLs. That is This tells us a few ti towards types. Two the next one.	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern (6) , is see	eing. That is, not targeted
This tells us a few ti towards types. Two the next one.	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. (b) things. One, that the previous activity was similar to the pattern(6), (is see o, it lends credence to an entire corpus grab approach. Don't care what it	eing. That is, not targeted
This tells us a few to towards types. Two the next one. (b)(6), (b)(7)(6), (b)(7)(6), (b)(7)(7)(6)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. (b) things. One, that the previous activity was similar to the pattern(6), (is see o, it lends credence to an entire corpus grab approach. Don't care what it	eing. That is, not targeted
This tells us a few ti towards types. Two the next one. (b)(6), (b)(7)(6)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), (is see o, it lends credence to an entire corpus grab approach. Don't care what it	eing. That is, not targeted
This tells us a few to towards types. Two the next one. (b)(6). (b)(6),(b)(7)(6) From: Sent: Friday, Januar	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. (b) things. One, that the previous activity was similar to the pattern(6), (is see o, it lends credence to an entire corpus grab approach. Don't care what it	eing. That is, not targeted
This tells us a few to towards types. Two the next one. (b)(6), (b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seen, it lends credence to an entire corpus grab approach. Don't care what it	eing. That is, not targeted
stable URLs. That is This tells us a few to towards types. Two the next one. (b)(6), (b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seen, it lends credence to an entire corpus grab approach. Don't care what it objects are used to be a seen of the pattern of the	eing. That is, not targeted
stable URLs. That is This tells us a few to towards types. Two the next one. (b)(6), (b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seen, it lends credence to an entire corpus grab approach. Don't care what it	eing. That is, not targeted
This tells us a few towards types. Two the next one. (b)(6), (b)(6), (b)(6),(b)(7)(6) From: Sent: Friday, Janual To: Cc: (b) Subject: Re: MIT U	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), (is see to, it lends credence to an entire corpus grab approach. Don't care what it (C) ary 28, 2011 2:50 PM (C) Update: It's worse than we know	elng. That is, not targeted is I am getting, just get me
This tells us a few towards types. Two the next one. (b)(6). (b)(6),(b)(7)(6) From: Sent: Friday, January To: Cc: (b) Subject: Re: MIT L	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seen, it lends credence to an entire corpus grab approach. Don't care what it compared by the compared by t	elng. That is, not targeted is I am getting, just get me
stable URLs. That is This tells us a few to towards types. Two the next one. (b)(6). (b)(6),(b)(7)(7)(7)(6) From: (b)(6),(b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	elng. That is, not targeted is I am getting, just get me
This tells us a few towards types. Two the next one. (b)(6), (b)(7)(7)(7)(6), (b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	elng. That is, not targeted is I am getting, just get me
This tells us a few ti towards types. Two the next one. (b)(6), (b)(6),(b)(7)(6) From: Sent: Friday, Janual To: Cc: (b) Subject: Re: MIT U This doesn't appear million in Nov and Di Research articles – 1 Reviews – 938,063	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	elng. That is, not targeted is I am getting, just get me
This tells us a few towards types. Two the next one. (b)(6), (b)(7)(6) From: Sent: Friday, Januar To: Cc: (b) Subject: Re: MIT L This doesn't appear million in Nov and Do Research articles — 1 Reviews — 938,063 Misc — 459,457	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	elng. That is, not targeted is I am getting, just get me
This tells us a few towards types. Two the next one. (b)(6). (b)(6),(b)(7)(6) From: (b)(6),(b)(7)(6) From: Sent: Friday, January To: Cc: (b) Subject: Re: MIT L This doesn't appear in Million in Nov and Done in Nov	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	elng. That is, not targeted is I am getting, just get me
This tells us a few towards types. Two the next one. (b)(6), (b)(7)(6) From: Sent: Friday, Januar To: Cc: (b) Subject: Re: MIT L This doesn't appear million in Nov and Do Research articles — 1 Reviews — 938,063 Misc — 459,457	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	elng. That is, not targeted is I am getting, just get me
This tells us a few to towards types. Two the next one. (b)(6), (b)(7)(7)(7)(6), (b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URI. 12345, get stable URI. 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), is seed to, it lends credence to an entire corpus grab approach. Don't care what it objections are used to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is:	eing. That is, not targeted is I am getting, just get me or disciplines. For the 2.8
This tells us a few to towards types. Two the next one. (b)(6), (b)(7)(7)(7)(6), (b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6), (is see to be the corpus of the corpus of the corpus of the pattern (6), (is see to be the corpus of the corpus	eing. That is, not targeted is I am getting, just get me or disciplines. For the 2.8
This tells us a few towards types. Two the next one. (b)(6). (b)(6). (b)(6),(b)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)(7)	s, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on. things. One, that the previous activity was similar to the pattern(6),(is see o, it lends credence to an entire corpus grab approach. Don't care what it (C) ary 28, 2011 2:50 PM (b) (6),(b)(7)(C) Update: It's worse than we know to be targeted towards research articles or any particular titles, collections, collect, the breakdown by article type is: 1,385,569 re or less correlate to the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole. I'd say the he was going after every content of the corpus as a whole.	eing. That is, not targeted is I am getting, just get me or disciplines. For the 2.8

(6)(8),(6)(7)(C)	
Ce:	
suppose reg. up. 1 Openios: re 5 mense men see unow	
Attached are 2 screen shots depicting PDF download activity from MIT for November and December.	One showly all
described; and totals 2.654.624 for the 2 months. The other filters out describeds from the 3 IP's th	at look to be executed
downloads and totals 2,654,626 for the 2 months. The other filters out downloads from the 3 IP's the with the download obuses (b)(6),(b)(7)(C) and totals 17,665 for the 2 months.	period. Recognizing that
some legitimate downloads may have occurred from the 3 filtered IP's, it would still be safe to say th	at about 2.6 million illegal
downloads occurred during November and December. We know that some illegal downloading occu	
and into January. I don't have those numbers yet. But looking at the graph you can see that some pr	
downloading was taking place the last week of Dec (over 100h.day). It seems likely this extended int	
of time. It wouldn't be much of a stretch to any that as much of a million or more additional downloa	
that are not reflected on this chart. I aspect to have January data available for review by Monday. I	ll also start loading Oct
and Sept numbers as well to complete the picture.	
(D)(C).	
(5)(6),(b)(7)(C)	**
From Withaka.com	
Debat Fri. 28 Jan 2011 14:13:57 -0500 Te ((b)(8),(b)(7)(C)	
(b)(6).(b)(7)(C)	
Co Programme Programme Co	
Subject: NE: Mil' Update: It's worse than we know	
So, with September and October, what does the number look like? Still looking like the entire or	2
So, with September and October, what does the number fook like? Sub footing like the entire of	ripusr
(b)(d),(b)(7)(C)	
From 20 2011 2110 MM	
South Friday, January 28, 2011 2:10 PM	
Te (b)(0),(b)(7)(C)	
Subfact: RE: MIT Update: It's worse than we know	
(b)(6),(b)	
(7)(C)	
Still digging and in a going to pass along a screen shot of what he is seeing for November and	
though the activity was less impactful in November, but just these two months helipark "2 million."	m + PDPs over their
normal usage (b) a also seeking out data prior and since for review.	
63.16	
(b)(d),(b)(7)(C)	
Cross P	
Gents Priday, January 28, 2011 1:53 PM	
(b)(0),(b)(7)(C)	
Statelegia RE: MIT Update: It's worse than we know	
Comfidence sent sent observes non sented asset sen estant.	
t will call in a moment.	
(b)(b),(b)(7)	
Cont. Fillin, Jones 28, 2011 1:43 PM	2
	•
Ces (CACACACACACACACACACACACACACACACACACACA	
Subjects MIT Update: It's worse then we know	
Transaction see High	

HEGIN PGP SIGNATURE—— (0),(0)(7)(C)	

Prome	(b)(6),(b)(7)(C) Reambridgepolice.org>	
Sent:	Mednecdes January 26, 2011 8:34 PM	
To:	(b)(e),(b)(7)(C) BOS) (b)(e),(b)(7)	
Subject:	RE: Follow-up questions with (C)	
Any response from		
(b)(8),(b)(7)(0		
From: Wednesday.	(805) [mailto] usss.dhs.gov]	
70	1/5/01	
CC CONTRACTOR	(b)(6),(b)(7) Pup questions with (C)	
sanjuos RE: Folio	-th descrip with	
The state of the s	er 4pm on Thursday or 1pm on Friday is a good time to have a conference call.	
(b)(6),(b)(7)(C)		
U.S. Secret Service Boston Field Office		
New York		
(b)(6),(b)(7)(C)	(b)(6),(b) (7)(C)	
Prom: (b)(6),(b)(7)(0	" [mailtoiMIT.EDU]	
To (b)(6),(b)(7)(C)	(BOS); External (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C)	
Ce	(b)(6),(b)(7)	
	rup questions with (C)	
(6)	ly time I've got available on Wednesday is after 4:00pm, due to an all-day commitment	
Standing of Gow, it	ty time I ve got available on wednesday is after 4.00pm, due to an all-day commitment sounds like that might not work for Steve, but if it does, it works for me. Thursday is wide	
	only a hard-stop for me at 5:30pm. Friday also has me tied up 9am-3pm.	
7/5\/A\	- Property	
(b)(7)(for tomorro	w, does 3:00pm work for you to meet down in hold? Perchary comment last meeting. I'm	
thinking we can ju	st furnish you with one of the duplicate drives that's already got the data on it (or we can	
clone one of those). (D)(8). is located	
here: ((5)(6),(5)(7)(C)		
(B)(0).		
Hope all are well a	and alarman transm	
Hope an are wen e	int seeling warm	
Best,		
(b)(0),(b)(7)(
(b)(8),(b)(7)(C)		
N-M-M-M	A sections.	
II Security System	Analyst	
MIT	m an par 1700	
/b\/8\ /b\/7\/0\	2307	
(b)(6),(b)(7)(C)		

		(b)(8),(b)(7)(C)				- Carlotte	
From:				MIT.EDU>			
Sout		Monday, Januar	24, 2011	0:15 PM			
fe:	(b)(6),(b)(7)(C)	BOS): 6	THE THE ALL	tembridgep	olice.ora:	
			Pusdoj		Januari again		
Cet	1		7	(b)(8),(b)(7)			
Subject:	L	Re: Follow-up qu		(C)			
and and		Mer LONON-Mh di	matrician Mi		•		
starting at 9am; open all day, wi o)(6), o)(7) for tomo thinking we can	it sounds like th only a hard crow, does 3:0 just furnish y	got available on that might not w -stop for me at 5: Xpm work for yo ou with one of th	ork for Sta 30pm. Fr ou to meet	eve, but if it does iday also has me down in [6]	s, it works to tied up 9s: (b)(6), Per(b)(7)	for me. Thurs m-3pm. comment last i	day is wide meeting, I'm
cione one of the	98). (chichi, is k	ocated		,			
)(6),)(7)							
lope all are we	II and stavino	warm.					
Best, (6),(b)(7)		,					
8),(b)(7)(C)		Security Analys	et.				
T Security Syst	ems & Servic		**				
ALT							
	(b)(6),(b)(7)(C)					
OP Fingerprins	(b)(8),(b)(7)(C			1 12 11			
On Jan 24, 2011	, at 6:25 PM	5)(6),(b)(7)(C)	(BO	S) wrote:			
Vhen would be a	good time for	you to have a conf	erence cali	on Wednesday?		5.11.2	
iso, if it works fo	r you, i would veillance file. V	lice to drap by you When would be a g	r office son	natime tomorrow	to get a co	y of the packet	date ceptur
(6),(b)(7)(C)							
.S. Secret Service cutus Pield Office							
b)(6),(b)(7)(C)				a Total se			
rom: Heymann,	Conhes ARAS	(b)(e),(l	b)(7)(C)	undel av d		****	THE RESERVE TO SERVE THE PERSON NAMED IN COLUMN 1
remit reymem, lent: Monday, Ja	may 24, 2011	14) [MBBBD] 5:45 PM					

ownloading came from IP address (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) On 10/13/10, (C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a NAC address of 0017f22cb074 and computer name of "ghost-lapton", (b)(6),(b)(7)(C) disabled the host registrations identified as bogus. (b)(6),(b)(7)(C)
unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost420mailinator.com, a NAC address of 0017f22cb074 and computer name of "ghost-laptop". (DX6)(DX7) disabled
"Grace Host" with an email of ghost420mailinator.com, a NAC address of 0017f22cb074 and computer name of "ghost-laptor". (b)(6).(b)(7)(disabled
of Network Security and Support Services for MIT, notified (b)(8),(b)(7)(C)
and (D)(B)(D)(T)(C) , the Director of MIT Operations and Infrastructure,
that information indicated that the same unknown person appears to be
using MIT guest registration from a wired connection in building 16.
on 11/29/10, the MIT Network and Information Security Team was
notified by the MIT branch of the Institute of Electrical and
Electronic Engineers that journal spidering has occurred on their site and it was tracked to the Student Information Processing Board XVN
cluster, a group of computers that are shared and that anyone in the
MIT community can use to host a Virtual Machine.
on $01/03/11$, (C) received an email from (b)(6),(b)(7)(C) forwarded from
On 01/03/11, (C) received an email from forwarded from (b)(6)(b)(7)(C) informing him that that the excessive downloading of journals
had begun again.
(b)(6),(b)(7)(C)
On 01/04/11, (C) emailed of Network Operations, and (b)(8),(b)(7)(C) hit,edu) (b)(7)(C)
(b)(6),(b)(7)(C) for Network and Infrastructure Services for NIT, asking them
to further pinpoint the location of the computer downloading the
journals. At $0808,\frac{(b)(6),(b)}{(b)}$ located a computer hidden by a box connected to a switch in a wire closet in the basement of building
16. The computer was also connected to an external hard
drive. $(b)(8),(b)(7)$ established a packet capture of the same switch the
computer was found attached to. [(b)(6),(b)(7)]
also provided SA (C) with a copy of historical network flow
data concerning IP addresses (ONO) (ONO) and (ONO) (ONO) first 12/14/10 to
01/04/11 and DHCP log information for computers registered as ghost-
macbook and ghost-laptop. $\frac{(b)(6),(b)(7)}{(b)(6),(b)(7)}$
SA (C) contacted SA (C) (CID) at the CERT Coordination Center at
the Software <u>Engineering</u> Institute at Carnegie Mellon University. SA(D)(D)
provided $SA_{(0),(0),(0)}^{(0),(0),(0)}$ with instructions to upload the data to the CERT drop box.
On 01/06/11, at approximately 1232, video survaillance showed the
individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(8),(b)(7)(C) of the
MIT Police Department called(b)(6).(b)(7)(C) of the MIT Folice Department
and stated that he had located the suspect later identified as Swartz
riding his bicycle on Massachusetts Avenue near the intersection with Lee
Street in Cambridge, Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) 2339

	(b)(d),(b)(7)(C) MIT,EDU>	
Prome	Tuesday, January 13, 2011 11:44 AM	
Sont		
Tec	Heymann, Stephen (USAMA)	
Ces		gepolice.org
Subject	RE: Confirming Interviews on Friday	
Yes (6),(b is evel	lable. I should have made that clear in my earlier e-mail, but was focu	sed on identifying the right IS&T
(b)(6),(b)(7)(C)		
Office of the Co.		
Office of the Ger		
	nstitute of Technology	
	ts Avenue, Building (D)(0).(D)	
cambridge, MA tel: (b)(6),(b)(7)((C)	
fax: 617-258-02	67	
b)(6),(b) mit.edu		
20/20		
Prons: Heymann	be materials are intended only for the use of the intended recipient. Delivery of this reliable not compromise or weive such confidentiality, privilege, or exemption from discinstance $(b)(6),(b)(7)(C)$ 1. Stephen (USAMA) [mailto]	
Tex (b)(8),(b)(7)(6	11, 2011 10:06 AM (b)(b)(b)(7)(C) (BOS):	
		per EOUSA
Phone:	(b)(5),(b)(7)(C)	
Steve (b)(8),(b)(From (Bents Tuesday, To: Hermann, Steve) (c)(b)(6),(b)(7)(c)	[[melito](b)(7)([MIT.EDU] Jenuary T1, 2011 8:27 AM techen (USAMA)	
Subject: RE: Co	minming Interviews on Friday	

Steve -

Friday does work for us, although it might be easier to start at 12:00 (our conference room is booked from 9:30 to 12:00). Hopefully that's okay.

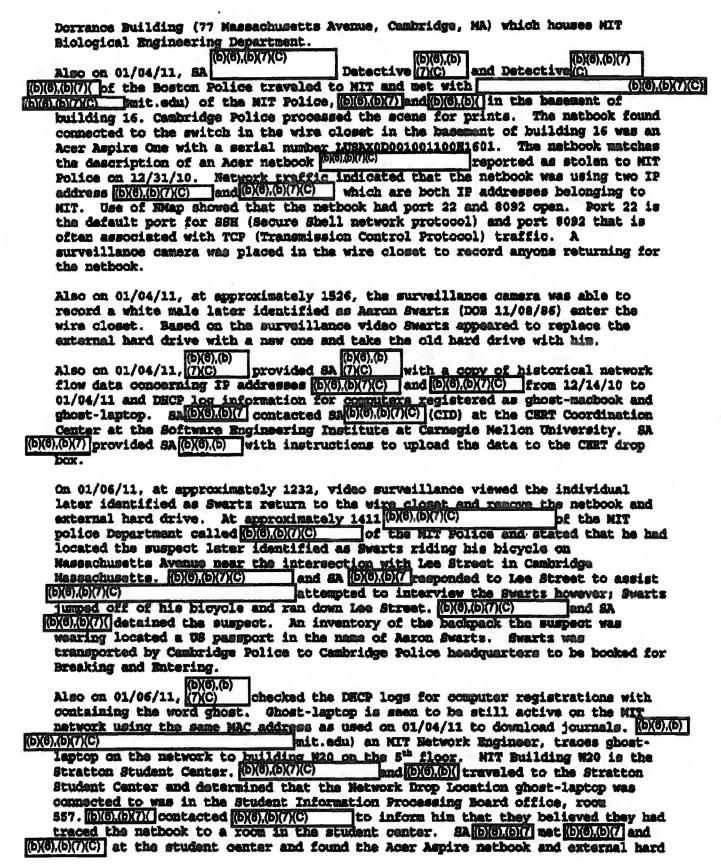
i have been in contact with the folks in IS&T and then came up with a slightly different list of names of people you'd probably want to speak with. They suggested (D(6),(D)(7)(C) and (D)(6),(D)(7) (they've advised me that (D)(6), (D)(7) (they've	7
We can hold the meeting in the Office of General Counsel conference room, located in room [D[6],D](]To get here, well through the main entrance of 77 Messachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a local corridor directly in front of you (known as the Infinite Corridor). Follow the Infinite Corridor until you enter another large open lobby, known as Lobby 10 (you will see a large set of doors on the right that look out onto a large quad fact the Back Bay, called Killian Court). When you're in Lobby 10, there will be two elevators on your left (to further confust things, you may see a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the elevators to the third floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General Counsel. Follow the hallway until you see another sign for the entrance to the Office of the General Counsel.	
I'm in meetings the bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details tomorrow.	
Office of the General Counce! Massachusetts institute of Technology 77 Massachusetts Average, Building [D(8),(D)(7)] Cambridge, MA 02139 tol: [(D)(6),(b)(7)(C) fax: 617-258-0267 (b)(6),(b)(7)(C) This message and any attached documents contain information which may be confidential, subject to privilege, or exempt from disclosure under applicable law. These materials are intended only for the use of the intended recipient. Bullyary of this message to any person other than the intended recipient shall not compromise or waive such confidentiality, privilege, or examplion from disclosure as to this communication. Process Hoyelmans, Stephen (USAMA) [presite] Smalt Monday, Innuance 10, 2011 4:30 PM Trad(D)(6),(D)(7)(C)	
Con BOS); BO	
(0)(8),(0)(7) (C) If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate	
(6)(6),(6)(7)(C) and(6)(6),(6)(7)(C) joining me. Tentatively, we would like to speak with the following five people in the order listed (as well as anyone else you may think useful or appropriate).	
физиритист ——————————————————————————————————	

(b)(6),(b)(7)(C)			*	
	titute of Technology Avenue, Building (C) (C)			
Promit Heymann, Same Plander, Ju Tes (b)(6),(b)(7)(C)	Staphen (USANA) [mailto]	e of the intended recisions. I	Delivery of this message to any person ption from disciousre as to this commi	other than the
the order listed (t work from your end, let's di BIDD(7(C) Joining me. Tents as well as anyone else you m	stively, we would like t	to speak with the following f	I anticipate ive people in
((((((((((((((((((((((((((((((((((((per EOUSA	
(b)(s),(b)(1)(c)				İ

Thank you, Steve

<u>*</u>	(b)(6),(b)(7)(C)	
From:		IT.EDU>
Sent	Tuesday, January 11,	
Tox	Hermann, Stachen (USAMA)
Cc	(b)(6),(b)(7)(C)	OS); External (b)(6).(b) cambridgepolice.org
Subject	RE: Confirming Inter-	riews on Friday
Stave		
Friday does work fo 11:00). Hopefully t		start at 11:00 (our conference room is booked from 9:30 to
probably want to sp would likely be able	peak with. They suggested (b)(6),(b) to provide the same information to me that he probably can't provide a	ame up with a slightly different list of names of people you'd $(7)(C)$ and $(b)(6),(b)(7)$ they've advised me that $(b)(6)$, they've advised me that $(b)(6)$, they $(b)(6),(b)(7)$ and $(b)(6),(b)(7)$ and provide). Also $(b)(6)$, they've advised me that $(b)(6),(b)(7)$ and information beyond what you could get from $(b)(6),(b)(7)$ everyone, i'm sure we can make it work, but i just want to be a
-	lent as possible. Let me know your	
through the main e corridor directly in large open lobby, it the Back Bay, called things, you may see elevators to the thi	ntrance of 77 Massachusetta Avenu front of you (known as the infinite of nown as Lobby 10 (you will use a law I Killan Court). When you're in Lob a a sign that says "Lobby 13" with an rd floor. When you exit the elevato	usel conference room, located in room ((*)(*)(*)(*)(*)) To get here, was a vice will enter a large lobby (known as Lobby 7) and see a locarridor). Follow the infinite Corridor until you enter another rge set of doors on the right that look out onto a large quad factby 10, there will be two elevators on your left (to further confunctions) and the point). Take either of the arrow, but you're in Lobby 10 at that point). Take either of the rs, immediately turn left and you will see a sign for the Office of another sign for the entrance to the Office of the General
tomorrow.	bulk of today, so I will be somewha	it inaccessible, but we can coordinate any additional datalis
b)(6), b)(7)(C)		
b)(7)(C)	7	
(8),(b)(7)(C)	Il Councel	
(6),(5)(7)(C) Office of the General		
o)(7)(C) (8),(b)(7)(C) Office of the General Massachusatts Insti	tute of Technology	
(6),(b)(7)(C) Office of the General Messachusatts Insti	tute of Technology venue, Building (0)(8),(6)(7)	
(6),(b)(7)(C) Office of the General Massachusatts Institute	tute of Technology venue, Building (0)(8),(6)(7)	
b)(7)(C) (6),(b)(7)(C) Office of the General Massechusetts Insti 77 Massechusetts A Cambridge, MA 02:	tute of Technology venue, Building (0)(8),(6)(7)	
Office of the General Messachusetts Acambridge, MA 02: tel: fax: 617-258-0267	tute of Technology venue, Building (0)(8),(6)(7)	
b)(7)(C) Office of the General Massechusetts Insti 77 Messechusetts A Cambridge, MA (2) tel: fex: 617-258-0267 This message and any at applicable law. These mintended recipient shall	tute of Technology (venue, Building (0)(8),(b)(7) 139 (b)(8),(b)(7)(C) tacked documents contain information with startels are intended only for the use of the not compromise or waive such confidential	ich mey be confidential, subject to privilege, or exampt from disclasure under a intended recipient. Delivery of this measure to any person other than the iter, privilege, or exemption from disclosure as to this communication.
Office of the General Massachusatts Insti 77 Massachusatts Insti 77 Massachusatts A Cambridge, MA (22 tel: fax: 617-258-0267 5),(b)(7) mit.edu This message and any at applicable law. These at intended recipient shall	tute of Technology versus, Building (D(8),D)(7) 139 (b)(8),(b)(7)(C) stacked documents contain information while starteds are intended only for the use of the	s intended recipient. Delivery of this measure to any person other than the Rey, privilege, or exemption from disclosure as to this communication.

receives an email from $(b)(6),(b)(7)(C)$ the MIT $(b)(6),(b)(7)(C)$
(b)(6),(b)(7)(C) regarding excessive downloading from two IP addresses
(b)(8),(b)(7)(C) and 18.55.6.215. JSTOR restores MIT access but blocks access to the
identified IP addresses. (b)(6),(b)(7)(C) mit.edu), (b)(5),(b)(7)(C)
(by8)(by7)(c)
Host used email address chostemailinator.com, a MAC address of 00235a735ffb and
computer name "ghost-macbook" register on the network on 09/24/10. (b)(6),(b)(7)(C)
disabled the computer registration.
(6)(8) (6)(7)(0)
On 10/09/10 at approximately 1115. (b)(6),(b)(7)(C) from JSTOR Operations Staff
emails (b)(6),(b)(7)(C) the MIT(b)(6),(b)(7)(C) to inform her that MIT's access
to JSTOR had been cut off again due to excessive downloading.
on 10/12/10, the MIT Network and Information Security Team received an email from
(b)(8),(b)(7)(C) stating that JSTOR had told her the excessive downloading came from IP
address (b)(6),(b)(7)(C)
On 10/13/10, (b)(6),(b) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grade Host" with an email
OR 10/13/10, MACO TERESCORE OCCUPRENCE OF EXCESSIVE UNAUCDOFIZED
of chost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of
"ghost-laptop", (0)(0),(b) disabled the host registrations identified as
bogus. (b)(3),(b)(7)(C) Manager of (b)(6),(b)(7)(C) for MIT
notifie $(b)(6),(b)(7)(C)$ and $(b)(6),(b)(7)(C)$ the $(b)(6),(b)(7)(C)$ MIT Operations and
Infrastructure that information indicates that the same unknown person appears to
be using MIT guest registration from a wired connection in building 16.
On 11/29/10, the MIT Network and Information Security Team is notified by the MIT
branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information
Processing Board XVM cluster, a group of computers that are shared and that
anyone in the MIT community can host a Virtual Machine on.
On 11/30/10, the Virtual Machine downloading journals from JSTOR is taken
offline.
(b)(6),(b)(7)(C)
On 01/03/11 at approximately 1440, (0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(
forwarded from (b)(b),(b)(informing him that that the excessive downloading or journals had begun again.
((b)(6),(b)(7)(C) ((b)(6),(b)(7)(C)
On 01/04/11 at approximately 0249 (b)(6),(b)(7) possile the MIT
(b)(6),(b)(7)(C) and $(b)(6),(b)(7)(C)$ mit.edu) a $(b)(6),(b)(7)(C)$
for Network and Infrastructure Services for MIT asking them to further pinpoint
the location of the computer downloading the journals. At 0808 (D)(0),(D)(locates a
computer hidden by a box connected to a switch in a wire closet in the basement
of building 16. The computer is also connected to an external hard
drive. $(b)(\theta),(b)($ establish a packet capture of the same switch the computer is
found attached to.
On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a
On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from
On $01/04/11$, Detective $(b)(6),(b)(7)(C)$ of the Cambridge Police Department and a member of the New Bogland Electronic Crimes Tank Force received a call from $(b)(6),(b)(7)(C)$ MIT. EDU) of the Massachusetts Institute of
On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New Rogland Electronic Crimes Task Force received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a
On $01/04/11$, Detective $(b)(6),(b)(7)(C)$ of the Cambridge Police Department and a member of the New Bogland Electronic Crimes Tank Force received a call from $(b)(6),(b)(7)(C)$ MIT. EDU) of the Massachusetts Institute of



(b) (b)(8),(b)(7)(C) (b)(8),(b)
Thu 9/30/10 pm (6). emails and (7)(C) to provide the facts of the even
mentions that ((b)(6),
(b)(6), and(b)(7) had spoken regarding possible solution utilizing authentication
that's
already available from the Libraries for JSTOR access; some logistics to work ou
(b)(6),
Sat 10/9/10 11:15pm (b)(7) emails (c) informing her MIT's JSTOR access has been cut off
again due to extreme
downloading.
(b) (b)
Mon 10/11/10 7:44pm (6),(b emails (6); to strategize on preventing these types of abuses and
raises issue of JSTOR
sending in IP abuse information in timely manner vs. blocking all of MIT's access
suggests
additional measures of blocking due to lack of IP info as VPN-based abuses of
resources have been
exploited in the past.
(b)
Tue 10/12/10 6:36am Security team receives email from (6),(b regarding most recent JSTOR
abuse; no IP address
information yet to act on.
Tue 10/12/10 4:02pm Security team receives email from (6).(b) with logs and IP address
information provided by JSTOR. (b)(6),(b)(7)(C)
JSTOR access restored. Abuse coming from address
(b) (b) (b) (b) (c) (d)
Wed 10/13/10 6:34am (b)(7)(sends email to (8),() and (b)(7) regarding more info on further
bogus registration information.
Will press JSTOR to have brief technical conversation with JSTOR's
folks. Suggests if our
proxy solution already in place for other resources is utilized, it's possible that
JSTOR can
automatically push people through it who attempt to access JSTOR directly so a
large behavior
change doesn't inconvenience MIT community accessing JSTOR and there would
be authentication
to the resource.
Hart and deather assemble for the day of the Arms TV at
Host registration committing download now shows Grace Host (shost42@mailinator.com).
Constant diversity
We see Com Vest essistand on OPT while MAC address 00025-22500 (about
We saw Gary Host registered on 9/27 using MAC address 00235a735ffb (ghost-macbook).
We saw Grace Host registered on 10/9 using MAC address 0017f22cb074 (ghost-laptop).
We saw MAC addresses change, something that a person does typically to avoid
being banned or
tracked on network.
We saw ghost-macbook change to 00235a735ffc after being banned.

	lecurity Systems & Services, IS&T	
MI		
),(b)(7)(C	<u>. </u>	
.,,,,	(b)(6),(b)(7) public key ID(C) BEGIN PGP SIGNATURE—	
PG	public key ID (C) htm://new.mit	
कालाव	N/NC)	
1		
1		
1		
1		
	END POP SIGNATURE	

To compare the compared to the		
	(b)(3):Rule 6E	per EOUSA
Thanks (b)(6),(b)(7)(C) Prom (5)(6),(b)(7)(C) Sept: Thursday, Jenuary 06, 2011 2:09 PM Te(b)(6),(b)(7)(C) Subject: Re: Packet Capture	,(b)(7)(C)	
How could I get a copy of the network traffic? (b)(6),(b)(7)(C) Sent from Blackberry		
Prem(b)(6),(b)(7)(C) MIT.EDU> Te((b)(6),(b)(7)(C) MR.edu>((b)(6) Best: Wed Jan 05 17:01:53 2011 Bulbject: Packet Capture	mit.edu>).(b)(7)(C) mit.edu>	
Thank you (b)(6),(b)(7)(C) Network & Infrastructure Information Services and Technology (IS&T) Massachusetts Institute of Technology Room(b)(0),(b)(7)(C) Cambridge, MA G2139	(b)(3):Fude 6E Services	per EOUSA
(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 disseminated without the permission of the Secret Service. If you have

PGP Fingssprint (b)(6),(b)(7)(C)	
BEGIN PGP SEGNATURE	
MAN BAN GYAN A MUMA	

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 disconnected 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 sandar immediately and delets it.

Preces		(b)(e),(b)(7)((C)	MET.EDU>	Anna N Sala Par		•
Sent		Friday, Janu	uary 07, 2011 1				
To:	(b)(6),	b)(7)(C)				120	
Ces	(b)(6),(b)(7		(BCS)			10.00	
Exhject			ive from suspe	ct			
BEGIN PGI Hash; SHA1	P SIGNED MESS	MGE			762		
swapped out	o check in regard by the suspect of a lot of the JSTO	n Tuesday; may	y/msy not be a				
I'm super impi time for you s	ressed with all ti ill.	ne good work ti	hat went into t	his coming tog	ether. Hopeful	ly it works like t	his most of the
Sest, (6),(b)(*			
)(8),(b)(7)(C)							•
		Security Analys	st IT Security 9	ystems & Servi	ces MIT	ē.	
PGP Fingerpri	nt: (b)(8),(b)(7)(0)					
	P SIGNATURE-						
(D)(8),(D)(7)(C)							
					i		
					ļ		
					ì		
4					•		

		(b)(d),(b)(7)(C)				
Prom:			MET.EDU>			
Sout			y 06, 2011 4:17 PM			
To:	(D)(8),(b		BOS)			
Subject:		Laptop Movemen	nt			
After returning t	from Building 16,	i checked radius i	ogs and found the			
following entries	£					
perimeter:	¥					
			ie0e756) (from clien	ıt .		
(b)(6),(b)(7) port	50023 cli 00-4C-l	E5-A0-C7-56)				
tongent:		Lamin OV. 100 4C.1	E5-A0-C7-56] (from	(b)(6),(b)(7)	L 7 -11 00 40 F	
sector:	SSA ZULL : AUNIK	man or loodes	c340-C7-30j (IIOM	Caent	port / al un-ac-e	3-MU-C/-30)
The ten 613:29	:5% 2011 : Auth:	Login Off: IDD-4C-I	E5-A0-C7-S6] (from	clamb(b)(6),(b)(7)	bort 7 di 00-4C-E	SALCZAS
1140 Pull 0 23,24				analist A	July 100 102	A LIN-01, 20)
We arrived at W	CONTRACTOR OF THE CONTRACTOR OF THE PARTY OF	e jecks to a drop is	ked the switch in W n W20-557. MIT Po			e laptop in
→						
INCURS NEW POPUL						
(D)(B),(D)(7)(C)		k Admin				
(b)(6),(b) mit.e	nstitute of Techn	CIORY				
(n)(n)(n) suntre		•				
	(b)(6),(b)	(7)(C)		•		
27						
(D)(B)(D)(T)(C)	Notared	k Admin				
	nstitute of Techn	7				
mite						
o)(6),(b)(7)						
(C)	(b)(6),(b)	(7)(C)				

> All e-mail to/from this eccount 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. <12-32-40.jpg><12-32-40.jpg><12-34-03-2.jpg><12-34-03-2.jpg><12-34-03-2.jpg><12-34-03-1.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-17.jpg><12-32-1

BEGIN PGP SIGNATURE	
(D)(0),(D)(7)(C)	
FAID BOR SIGNATI IDE	

(b)(8),(b)(7)(C)	ANT FOU IS	
Te(b)(8),(b)(7)(C)	MIT.EDU>	mft.edu>
Cd(b)(6),(b)(7)(C)	[mlt.edu>{(b)(6),(b)(7)(C)	
Sent: Wed Jan 05 17: Subject: Pecket Captu	11:53 2011	

Hi there.

I have collected about 70G of network treffic so far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

	nk you (b)(7)(C)
	Network & Infrastructure Services
	mation Services and Technology (IS&T)
	sechusetts institute of Technology n(D)(0).D)(7)(C)
	bridge, MA 02139
	(b)(7)(C)
(b)(8), (b)(7) (C)	mit.edu

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, discloss, 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.

Procee		(b)(6),(b)(7)(C)	MET.EDU>		
Sout:		Thursday, January (
Tes	(b)(8),(b)		BOS)		
Subject:	(UNO)(U)	RE: Packet Capture	100		
Hi there,					
I've setup a web format. The UR		machine containing th	e files so you can do	wnload them. Th	ey are in a standard topdur
(b)(3):Rule 6E				. *	
We've got plent	y of bandwidth	over here, however, i	downloading this n	nuch data is a prol	blem for you I could put the
ON & SALA DITME	and build freu	n down to your office.	Let me know.		
Thanks	(b)(8),(b)(7)(· 51		•	
	V=10-10-10-10	المراج			
(b)(6),(b)		(b)(6),(b)(7)(6) (i) [mailto	ousse.dhs.gov)		The second secon
Sont Thursday	January 06, 2	011 2:09 PM	yuss-uiis-yu•j		
Tel Sugned Ver V	(b)(6),(b	(/(C)			
How could I get	a copy of the n	atwork traffic?			
(b)(6),(b)(7)(C)	1				
Sent from Black	berry				
(b)(6),(b)(7)(C)				
Promi To (b)(6),(b)(7)(MIT.EDID> b)(6),(b)(7)(C)	Imitadu>	•	
Cc (b)(8),(b)(7)(C		mit.edu>(b)(8),(b)(7)(C	mitedu>		
Subject: Packet	15 17:01:53 20: Capture	11			
Hi there,	•				
i have collected	shout 70G of n	stwork traffic so far wi	th about 98% of whi	ich is the ISTOR jo	urnal downloads. I've don
wondering what	the next step i	rris sud i dou case su	Antid mer meume	s a commune and	control channel. I was jus
Thank you					
(6),(b)(7)(C)	Notice &	Infrastructure Services			
Information Serv	ices and Techni	ology (IS&T)			
Massachusatts ir Room (5)(8),(5)(7)	stitute of Tech	nology			
Cambridge, MA (

(b)(8),(b)(7)(C)	
U.S. Secret Service	
Boston Field Office (D)(G).(D)(7)(C))	
(b)(6),(b)(7) (b)(6),(b)	1/ 00///// 00/ 00
Premic(C) mailte(7)(C) MIT.EDU) Seint: Thursday, January 06, 2011 9:37 AM ((b)(6),(b)	
Reg(b)(6),(b)(7)(C) (ROS): Extremal (7)(C) cambridge on location	
(b)(6),(b)(7)(C)	
All,	
I am going to suggest that we take the leptop and hard drive offine today. I think the amount of network traff	
 captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able some people there for a short time in an attempt to ID. 	to put
I am following up a couple of possible ID's this morning and will get back to you on my success (or not).	
The open questions will be if we decide to take it offline, is this something I can do with instruction or will I re	red help?
Also, do we want to have the new drive printed?	•
(b)(7)(
(b)(6),(b)(7)(C)	
Santa Wadnesday, January 05, 2011 5:02 PM	
Tes (b)(6),(b)(7)(C) luses the anal(b)(6),(b)(7)(C)	
Subjects Packet Capture	
Hi there.	
I have collected about 709 of network traffic so far with about 98% of which is the JSTOR journal downloads.	
some initial checking of the capture and I don't see anything that identifies a command and control channel. wondering what the next step is.	i was just
statement and state and see	
Thank you	
(b)(6),(b)(7)(C)	
Network & Infrastructure Services	
Information Services and Technology (IS&T) Messachungts institute of Technology	
Room (D)(8),(D)(7)	
(b)(8),(b)(7)(C)	
(b)(6),(b)(7) mit.edu	

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 louned to you and should not be further disseminated without the permission of the Secret Service. If you have

-	(b)(8),(b)(7)(C)
From: Sent:	Thursday, January 96, 2011 2:11 PM
To:	(b)(6),(b)(7)(C) BOS(b)(6),(b)(7)(C) Externs!
,	(b)(8),(b)(7)(C) cambridgepolice.org
Cc	(b)(6),(b)(7)(C)
Subject:	RE: When to pull laptop
the video archive.	(b) we saw the port go down at 12:32pm today. I'm going to look at Did someone take this down intentionally?
(b)(6), (b)(7)(C)	1
(b)(6),(b)(7)(- Network Massachusetts 77 Massachusetts 77 Massachusett Cambridge. MA Phone: Email (b)(6),(Institute of Technology ts Ave, Room (b)(6)(b)(7)(C) (b)(6),(b)(7)(C)
Promi	(BOS) [maitousss.dhs.gov]
like to keep the su	or you to pull the laptop and external? I am in my Boston office now. I could be there in 15. I would refilence camera running because I think he will come back when he notices the laptop is offline. Is we could dust for prints again before we pull the laptop since we know he came back?
	(b)(6),(b) (C) (

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

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

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

(b)(6), (b)(7)	
(b)(6),(b)(7)(C) Froms South: Wednesday, Jenuary 05, 2011 5:02 PM Te((b)(6),(b)(7)(C) (b)(6),(b)(7)(C)] Co Subject: Packet Capture	
Hi there, I have collected about 70G of network traffic so far with about 98% of whic some initial checking of the capture and I don't see anything that identifies wondering what the next step is. Thank you	
(b)(6),(b)(7)(C) - Network & Infrastructure Services	
Information Services and Technology (IS&T) Massachusetts Institute of Technology Room (D)(8),(b)(7)(C) Cambridge, MA 02189)(6),(b)(7)(C)	
b)(6),(b)mit.edu	

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.

Series Se	(b)(6),(b)(7)(C)
From:	cambridgepolice.org>
Sent:	Thursday, January 06, 2011 11:20 AM
To:	(b)(6),(b)(7)(C) MIT.FDU'
Cc:	(b)(6),(b)(7) (b)(6),(b)(7)(C) BOS)
Subject:	Re: MIT - Bld 16
(b)	(b)
(6) (that is certain)	y your call and sounds good (6), will be responding either way.
(-7/1)	(D)
(b)(6),(b)(7)	C
From	MIT.EDU>
$T_0(b)(6),(b)(7)(C)$	
CC: (b)(6),(b)(7)	
Sent: Thu Jan 06	11:17:02 2011
Subject: RE: MIT	- Bid 16
(b)(6),	,
(b)(7)(- We can bag,	tag and deliver if that works. I am thinking that if we are leaving the camera up, we should be in and
out rather quickly	incase the suspect ventures by. I would imagine $(b)(6)$, could process it in her lab.
(b)(6).	*
	C) (b)(6),(b)
(b)(6),(b)(7)	mailta(7)(C) cambridgepolice.org]
	anuary 06, 2011 11:13 AM
To: (b)(8),(b)(7)(C)	(b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)	usss.dhs.gov'; pcomcast.net';
	dhs.gov'
Subject: Fw: MIT	- Bld 16
(b)(6),(b)(7)(C)	
The thread helow	nas the status of the investigation to date.
The Bliede Octob	(b)(6),(b)(7)
As I am on a day o	ff today I would request that CPD Crime Scene personnel hook up with SA(C) and process
	hard drive for prints that the suspect left the other day after we cleared the scene.
As you'll notice fro	n the thread, the operation is being shut down and we will continue the investigation just not with the
computer nooked	up and downloading data.
(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)
	(h)(6)
(b)(6), and (b) can	you call $(b)(6),(b)(7)(C)$ and hook up with her and $(b)(7)$
Respectfully Subm	itted,
(b)(6), (b)(7)(
(b)(7)(
(J-1/6) (J-1/3	(6) (6)(7)(6)
(b)(6),(b)(7	
(b)(6),(b)(7)(C)	17.1/01/1.1
cc (b)(6),(b)(7)(C)	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
(b)(6),(b)(7)(C BOS(b)(6)	
Sent: Thu Jan 06	
Subject: RE: MIT	

The open quantions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed? (b)(0), (b)(7) (b)(6),(b)(7)(C) "(h)(h)(h)(r)(c) de Padus Captura Hi there. I have collected about 705 of network treffic to far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is. Thank you (b)(d),(b)(7)(C) Metwork & Infrastructure Services Information Services and Technology (IS&T) Massachusetts Institute of Technology Room (0)(0).(0)(7) Combridge, MA 02159 (D)(J)(D)(7)(C) (b)(0),(b) mit.edu

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 samitive, 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.

From:		(b)(6),(b)(7)(C)	MIT.EDU>				
Sent:	No.	Wednesday, January 05					
Ta:	(b)(8),(b)(7)(C) (BOS),(b)(7)(C)			
Ce	(b)(8),(b)(7)((C)					
Subject:		Packet Capture					•
Hi there, I have collected a	bout 70G of nets	work traffic so far with (shout 98% of u	hich is the	ISTOR iourn	ral downloads	. I've dons
	ing of the captu	re and I don't see enyth					
some initial checi	ing of the captu						
some initial check wondering what t Thank you	ing of the captu he next step is.						
some initial check wondering what (Thank you (6),(b)(7)(C)	ing of the captur he next step is. Network & inf	re and I don't see enyth Frastructure Services					
some initial check wondering what t Thank you	ing of the captur he next step is. Network & Info	re and I don't see enyth frastructure Services ogy (IS&T)					
some initial check wondering what i Thank you (6),(b)(7)(C) Information Servi	ing of the captur he next step is. Network & Info	re and I don't see enyth frastructure Services ogy (IS&T)					
some initial check wondering what i Thank you (6),(b)(7)(C) Information Servi Massachuse(ts in	ing of the captur he next step is. Network & inf ces and Technol ititute of Technol	re and I don't see enyth frastructure Services ogy (IS&T)					
some initial check wondering what 1 Thank you (6),(b)(7)(C) Information Servi Massachusetts in Room (0)(0),(0)(7)	ing of the captur he next step is. Network & inf tes and Technol titute of Technol	re and I don't see enyth frastructure Services ogy (IS&T)					