ORIGINAL

(b)(6),(b)(7)(C) CID)

From: BOS
Sent: Friday, September 21, 2012 2:13 PM
To: CID
Cc: BOS; ISD
Subject: CT 775.510 Aaron Swartz (J-102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM:	BOSTON FIELD OFFICE	FILE:	J-102-775-60071-S
TO:	CRIMINAL INVESTIGATIVE DIVISION	X-REF:	N/A
INFO:	INVESTIGATIVE SUPPORT DIVISION	SEIZURE#:	N/A

SUBJECT: REPORT OF JUDICIAL ACTION

ACTUAL LOSS: TBD POTENTIAL LOSS: $2,000,000.00

CASE TITLE:	AARON SWARTZ
CASE TYPE:	775.510
SECONDARY TYPES:	848.191, 848.304, 848.930
CONTROLLING OFFICE:	BOSTON FIELD OFFICE
REPORT MADE BY:	SA (b)(6),(b)(7)(C)
DATE CASE OPENED:	01/07/11
PREVIOUS REPORT:	05/29/12 - REPORT OF JUDICIAL ACTION
REPORTING PERIOD:	05/30/12 - 09/21/12
STATUS:	CONTINUED

SYNOPSIS:

A superseding indictment was rendered charging Swartz with wire fraud, computer fraud, unlawfully obtaining information from a protected computer and recklessly damaging a protected computer.

In preparation for trial, members of JSTOR and the Massachusetts Institute of Technology were interviewed by the prosecution team.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to all previous reports in this case, the most recent of which is the Report Judicial Action written by SA (b)(6),(b)(7) on 05/29/12.

On 09/13/12, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) of the Cambridge, MA Police Department, Assistant U.S. Attorney (AUSA) Stephen Heymann and AUSA (b)(6),(b)(7)(C) interviewed several JSTOR employees in Ann Arbor, MI regarding the network intrusion. The prosecution team spoke with JSTOR legal counsel, (b)(6),(b)(7)(C) of Debevoise and Plimpton LLP, regarding the case. Additionally, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) of JSTOR were interviewed at 301 East Liberty Street in Ann Arbor, Michigan.

(2)

Sept 25 & 26 they (MIT) did not keep logs on DHCP.

Any Record MIT keeps that shows .6 .240 Linkage

Dec 2010 ARP Tables are 5 minutes in duration = No Historical Data kept.

Computers can use more than 1 IP address
Virtual Interface Can do it
Can do many IP Addresses.

Block MAC address on DHCP? ~~[illegible]~~
Prevents it from being assigned an IP or renew its lease
Leases last 1 Hour on the system
1/2 Hour into use it starts to try release then 1/4 then 5 minutes

End Call
2:10pm

R I F 50

IBM JSTOR

18m MIT

19m MIT

[redacted]

TED Challenges

Archive =
Box = Search
Looking at Screen = Search

Backgrounds - More

JSTOR - where then DS'

How JSTOR - Makes Money -

(#4) READ
& Know -

- Guest Limitations -

Sept 24th

13th
6:00pm
Train

8/30/12 [illegible] [illegible] & I

TO DO
- Get Geiger access to all evidence @ CERT -
- Check w/ (b)(6),(b)(7)(C) [redacted]

Sept 13 Ann Arbor Michigan
Sept 12th Fly Out

18th & 19th

Error messages
Does the message remain the same
Sept → Oct
Different Malfunctions
Different Language Examples

GJ = Stay Away -

MIT's laptop who set

Sept 25th → Sept 26th
throttled the system

Messages

1292?

Aug 28 ?

[redacted] (b)(6),(b)(7)(C)

[redacted] (b)(6),(b)(7)(C)

Def

Call

3 9mm

Middle Sept

1. 40

8/27/1

9 Mod ?

- 40

End of year

[redacted] (b)(6),(b)(7)(C)

509

-x IP

[illegible] (b)(6),(b)(7)(C) [redacted] is a [illegible]

3/24 [illegible]
4:10 pm
Friday

(b)(6),(b)(7)(C) [redacted]

Error Messages came

??? HTML →

Servers Can we show that he looked
at those Error messages

Chris [illegible] Will they be User Access
Hides
discovery HTML

CVS Pharmacy

Conference Call 1045am 8/27/12
Heymann - Garland - (b)(6),(b)(7)(C) [redacted] - Me
Supercede Swartz Indictment of Swartz

1 of 2 Things

(b)(5) [redacted]

Since indictment - Servers

(b)(5) [redacted]

(b)(6),(b)(7)(C) [redacted]

930 AM 30 Seconds

(b)(6),(b)(7)(C) [redacted]

CS Attorneys office

(b)(6),(b)(7)(C) [redacted]

275 1
1165 2 1 1
14^{30}

948 AM 8/23/11
Supercede in this Case

1st Question

Drive connected to ACER
on JAN 6th
80-90K PDF's
When were they created
What Dates they are
i.e. JAN 4th 5th or 6th

4 Drives Fro Action

The Drives that Sept 2 gave up.

~~Jan~~ Oct 24th
Sept 24th } Jan 4th
Sept 25, 26 ISTOM } 3 Blocks

511

(b)(6),(b)(7)(C)

8/5r

11/34am

2nd

Aug 20th

(b)(6),(b)(7)(C)

Massachusetts AG's office

Cyber Crime Division

Middlesex DA's office

Cyber Protection Program

(b)(6),(b)(7)(C)

Digital Evidence Investigator

to (b)(6),(b)(7)(C) t 101

9:18 AM 8/8/12

(b)(6),(b)(7)(C)

3-August-12 Email from (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

1254pm 8/9/12

(b)(6),(b)(7)(C)

Work to Vians

(b)(6),(b)(7)(C)

9:49 pm 8/14/12

(b)(6),(b)(7)(C)

London Reading 14th August

London Mobile (b)(6),(b)(7)(C)

(Feynman Case) (b)(6),(b)(7)(C) 7/5/12

1) ACER - Portions of CERT Report
Additional Files on ACER

2) Radius Logs
& Screen shots to Store in
CD's

- Keep Grabbing IE and Thumb Drive -

Did we turn over a copy of ACER?

Collect on Separate Disk. Files on
Acers & Thumbdrives

Bash history Files turned over
today -

RIF

[redacted] (b)(6),(b)(7)(C)

Quincy Chang. Didn't Sleep well lost MyUt

[redacted] (b)(6),(b)(7)(C)

iPhone was tracked?

[redacted] (b)(6),(b)(7)(C)

332 pm 6/18/12

[redacted] (b)(6),(b)(7)(C) — ??

[redacted] (b)(6),(b)(7)(C)

Included Emails

3 Emails

Thanks for your time

→ 4-6 weeks ←

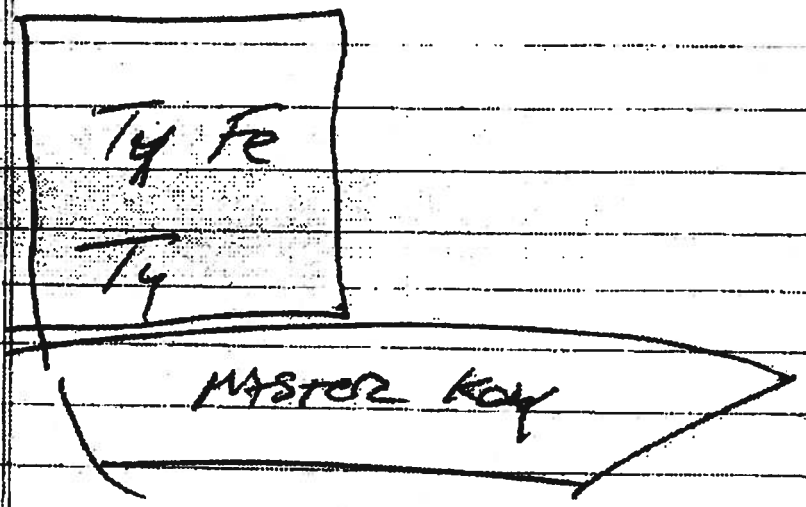
(b)(6),(b)(7)(C)

ordered Spring

(3) 4R January

(4) F6s

(b)(5)



Encrypted CD

Entrance to Unit

Fire

(b)(6),(b)(7)(C)

Thursday
Lunch @ US Attorneys

Fell In

(b)(6),(b)(7)(C) [redacted]

9:20 AM
Mar 22, 2012

(b)(6),(b)(7)(C) [redacted]

Jan 4, 2011

Separate Drive
network flaw (b)(6),(b)(7)(C) [redacted]

Dr...

(b)(6),(b)(7)(C) [redacted] Steele Hermann

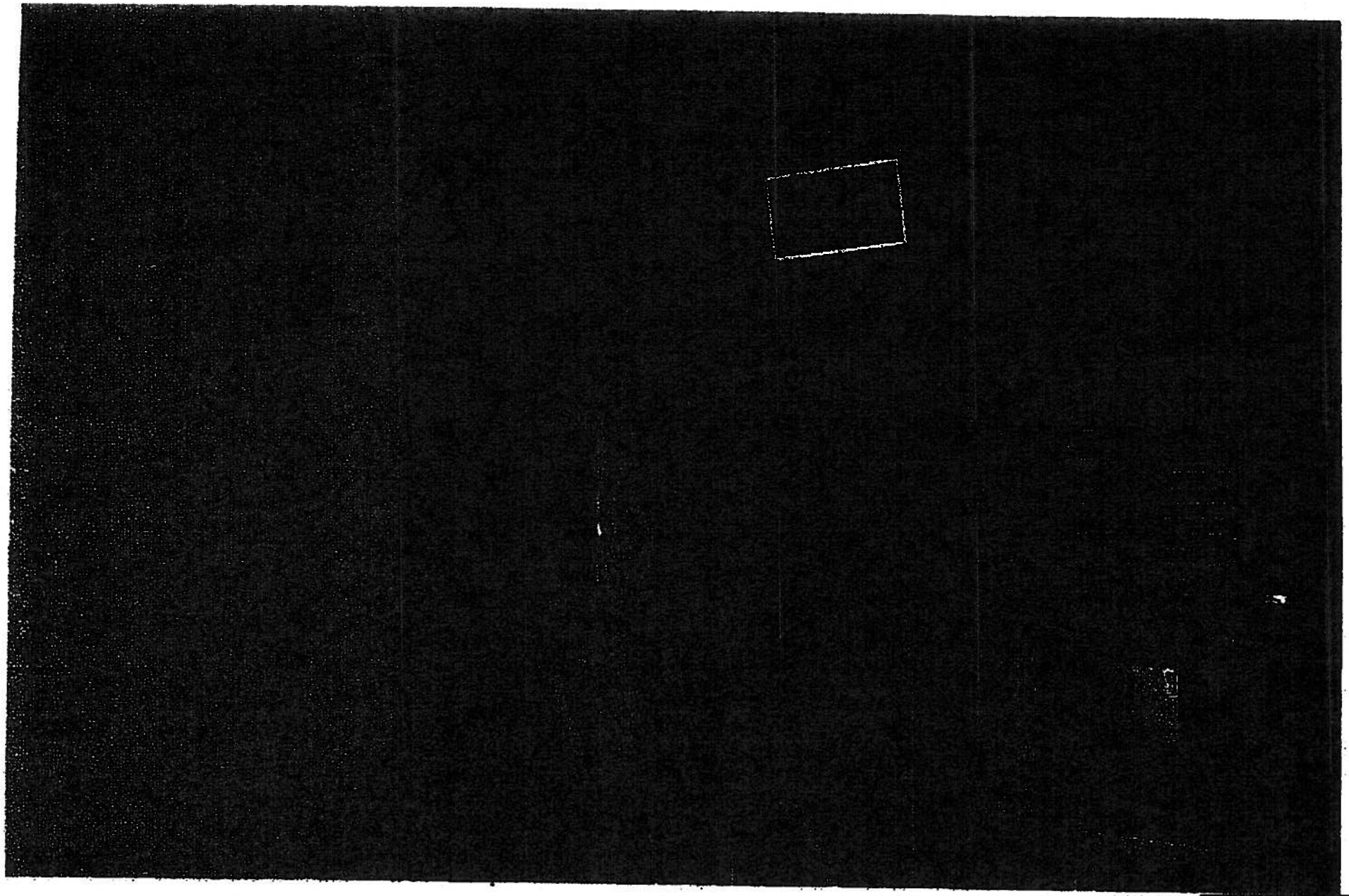
Called it on time

Post It.

Did Get It

RIF

RIF



RIF

[redacted]

~~Text [illegible]~~
~~the 12.~~
~~History of Streetcars~~
~~Cabbages Freakies~~
~~Amam Consequences of Urbanism~~
Urban Renewal ~~and Residential~~
Essential Wars. 39: no blacks
~~Working out while reading~~
123: revolutionary highways (!)
~~Jeff + hitting the~~
~~Chariot~~
124: permanent loss of counts
Ask (b)(6),(b)(7)(C) [redacted] abt the
Liberation quote

The Private City

Street car Suburbs

Nothing Gained From Cars
demographic inversion
Euclid v. Ohio
Chinese laundries
Mindfulness

Bourgeois utopias
SIO -

~~Crabgrass~~
~~Loeb HT384.U5~~
~~Human Consequences~~
~~WID HT151.B435~~ [illegible]
~~Urban Renewal~~
~~Loeb HT175.W986~~
~~Please, Please!~~
~~WID Econ 3330.141~~
~~Streetcars to suburbs~~
~~Loeb WID HE308.F65~~
missing WID 32044012053144
12q. for Ullbacreech also 220
animal for health care

(b)(6),(b)(7)(C)

430

(b)(6),(b)(7)(C)

10.15

(b)(6),(b)(7)(C)

Crabgrass

~~4 Critics of population~~

5 Problems of definition

7 foreign comparison

8 income rises by file mile

8f foreign elite lives in cities

19 Source of Ideal

20 " adapted to different needs

20 "most fundamental reality

Brittany's art

"don't know ... well
but you seem cool enough
... with you

...iderland
...IO HT351.584
...Spiral
~~...~~ NAC 1695 ...25
...geois Utopias
... HT351.F5 ...
... Consumer's Republic
...ID HC110.C6 C537

[redacted]

I was feeling pretty hungry, so I decided to treat myself to my favorite meal: the [illegible] egg sandwich at [illegible]. It couldn't have that many calories I figured. And besides I'd gained a little weight

I grabbed an [illegible] & a [illegible] and headed out

The [illegible] [illegible] [illegible] [illegible]

[redacted]

I got here a half hour
before because [illegible]
I decided to pass the time
at the library around
the corner, but it was
closed too.

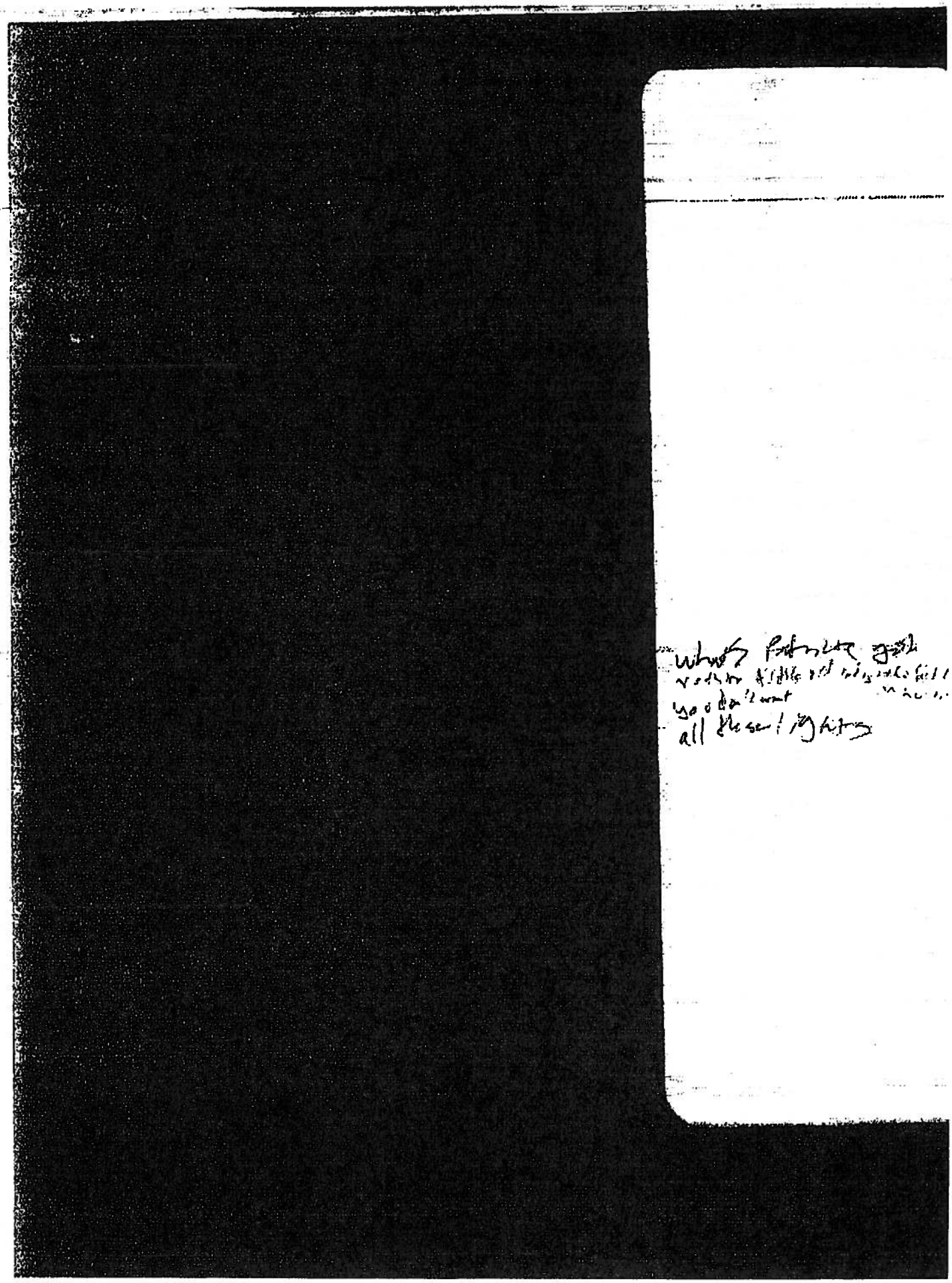
As I headed back from the
library, the chest pain
started again. After the
last time, I'd listened to
[illegible] for a while and the
mystery
it sounded funny, but

[redacted]

eventually decided it was nothing. But now the pain was back.

Some people are hypochondriacs. They think everything's a problem and call a doctor at the slightest provocation. I'm the opposite (a hyper-chondriac?) — I just don't want to bother anyone.

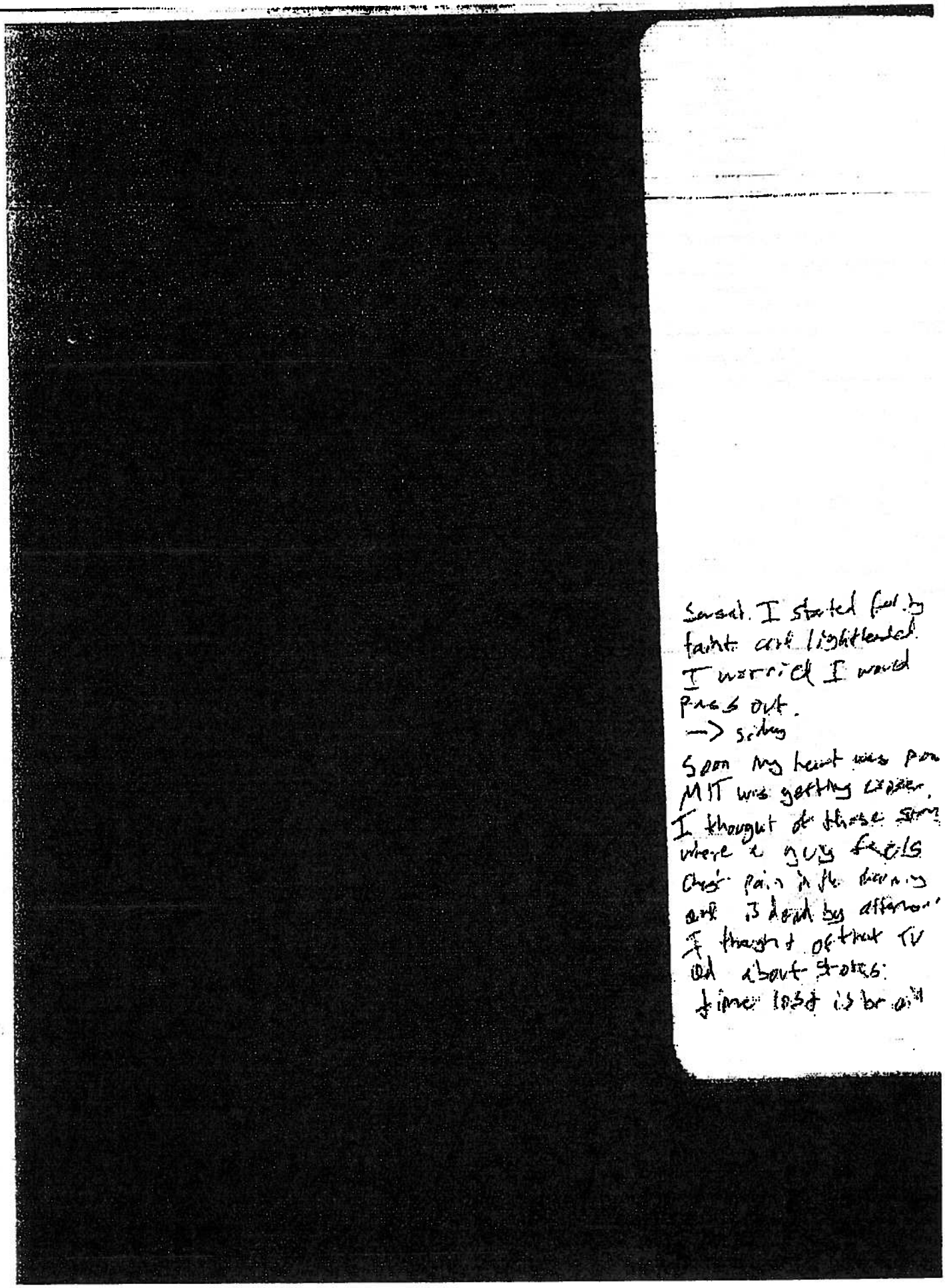
Still, I figured it



[redacted]

was with looking .nt
~~The Plan~~ I'd goog
for the symptoms of a
heart attack.

The library was closed o
Jessica doesn't have a com
uter, so I headed for t
Things kept getting worse. The
~~pain was pressure~~ in my chest
kept feeling tighter,
like I was being squeezed
from inside. I broke
out in a cold



Sweat. I started feel. dizzy faint and lightheaded. I worried I would pass out.
→ sitting
Soon my heart was pou MIT was getting louder. I thought of those stor where a guy feels chest pain in the morning and is dead by afternoo I thought of that TV ad about stroke: time lost is brain

[redacted]

[redacted] I started
running.

But just made things
worse, so I slopped
and tried to walk slowly.
But the buildings were
so close — I started running
again. I quickly slowed

Finally I found a doorway!

My vision was tight, like
the darkness was pressing in

I began typing:
"Signs of a" – it
autocompleted: "heart attack"

Chest pains, tightness in
particular – Check.
Lightheadedness – Check.
Shortness of breath – check.

"Do not wait," it said.
"Call 911 at the first signs"
I logged off

[redacted]

I began topics:
"Signs of a " — it
[illegible] completed. [illegible]

Chest pains, tightness in
particular — check.
Lightheadedness — check
Shortness of breath — check

"Do not wait," it said.
"Call 911 at the first sign."
I logged off

[redacted]

Sidney & I passed by a hotel. "Nice umbrella," shouted the doorman "want to trade?"

"Thanks," I said. I laughed. "People today," he said to the other doorman Asking him about heart attack symptoms. Didn't feel right [illegible] [illegible] [illegible]

Anyway, I love you and hate — How could

[redacted]

I have a heart attack?

end

There wasn't a phone in the computer lab. Or in the hallway. I ran across the street and into the student center [illegible]

The [illegible], there was a phone in the basement, right?

9-1-1, I dialed. I've never [illegible] dialed 911

[redacted]

intentionally before. Once when I was very little, I was playing with the phone – pushing buttons, listening to the tones they made. Eventually I heard a different sound. "Emergency Services" it said. Scared, I quickly hung up. The phone rang a minute later and soon my parents were yelling at me.

"Emergency Services"
it said. I did that thing
of the fire.

"Tell me exactly what you
saw." was the first question.
This seemed odd, but it
made a kind of sense.
What if something happened
to me and I couldn't answer
the other questions —
they'd have to come find me
no matter what kind of
emergency

[redacted]

"I'm in the basement of the student center at MIT," I said. My voice was faint and weak. I was surprised how bad I sounded — I could think clearly, why couldn't I speak clearly?

"~~Do you know~~ what's the address here?"

"I'm not sure,

[redacted]

but it's across the street from 77 Mass Ave --
"And you're in the basement level?"
"Yes"
"Now what's going on?"
"I think I'm having a heart attack" [illegible]
"OK, a Paramedic team is on the way. Is it open there?" counting going this seemed first.
"Yes, it's open"

[redacted]

"OK, just stay on the line, I'm going to ask you a few questions just so they know. Are you [illegible] chest pains
"Yes
"Shortness of breath?"
"Yes."
"How old are you?"
"27.
There was a pause.
"Any dizziness?"
"I feel lightheaded
"OK, I want you to

[redacted]

find the most comfortable position and stay there. Don't eat or drink anything, that could just make things worse. We're done now, but call me back right away if anything changes.

"OK."

"Alright."

There were some background noises on the line. I thought of a call center: cubicles, buttons pressed

Swivel chairs, paper.
I hung up

I tried sitting down but
that didn't feel right.
So I started standing up
I settled on
I waited.

And waited.

I heard footsteps coming
down the stairs and scurrying
up. But it was just a woman
"It's not here," she

[redacted]

called back.

I went back to crouching.

It felt like it had been a while. Maybe I should wait upstairs. I went over to the stairs, but they seemed daunting. I went back to the phone and crouched.

It had been so long since the pain started last time.

[redacted]

lost. Had I lost? Was I going to die?

I heard a voice coming down the stairs. "I wonder where he's at - Asbury Campus policeman appeared. This was not what I was hoping for. "And there he is!" He came over.

"What's going on?" Asked I started to explain

[redacted]

Soon a man in a reflective
vest was there.
"What's going on?" he
asked. I started over.
The people were multiplying.
~~[illegible]~~,
Two came from my left, carrying
a stretcher. The girl made
a joke I didn't hear.
This didn't seem like
the time for jokes

More were from the right
and soon I was surrounded.

They spoke in Swedish
I don't know, so
I'll just make up the
medical terms, since I
can't remember them.

"Get me a 1-5," the
woman said. "1-5," someone
replied. They attached
a pressure cuff, [redacted] and
EKG leads. "Can I get
an O2 sat when you
get a chance?" "I'm
working on it," someone replied, and I

got an oxygen monitor too. I think there was a stethoscope.

"Someone get him a chair." A swivel chair was wheeled out from behind the desk.

"Let me feel your pulse."

My heart was pounding, it felt like it would burst right through my chest.

"Yeah, it's a little fast."

[redacted]

They looked at notes and charts and conferred. Why weren't they doing anything?
"You asthmatic?" "No." "Bradycardic?"
~~"Ok" "Free 5"~~ "No." "[illegible]?"
"We're going to give you some oxygen, just temporarily." I was fitted with an oxygen mask.

They conferred some more.

"OK, why don't you

[redacted]

Get up here on the stretcher!"
E.d.t. -
"What hospital do yr want to go to?"
Huh? "I don't know" I said. The corpsman then asked my name and date of birth and if I was on med. caps. Had this ever happened before? Any family history? Drugs? Psychiatric/ Allergies?

[redacted]

"How are you feeling? Better?"

"A little."

"There are lots of hospitals around here. Cambridge, Mass General, Mt. Auburn, Beth Israel. It's really your pick."

"Beth Israel," I said.

"Is that where your doctor is?"

"Yeah."

[redacted]

They talked some more and soon the stretcher was rolled away. It felt like the opening to <u>Naked Gun</u>. We rolled thru hallways and up stairs and around people and past an ATM someone [illegible] was using.

"Can I get 200?" the woman asked.

"I don't think he liked my joke," she said.

"Hey, I could use a

asked for any more!"
"You should do," a
guy replied.

We rolled out the back
~~and down~~ to the loading
dock and down
a ramp. The ambulance
was waiting by the road.
They lifted me up and loaded
me in

"I'm (b)(6),(b)(7)(C)" the
woman said. "I'm sorry

[redacted]

to be with you in the back. You doing OK?" "Yeah, I'm starting to feel better."
"[illegible]"
There was more [illegible] and some chains.
They buckled me in.
"You ready to go?" "Yeah, we're ready," she said.
They closed the back and peeled off.

[redacted]

My vision was narrowed still, I mostly saw the little window in the back. He pulled ~~[illegible]~~ onto the street, over the bridge, then Boston. It was Naked Gun in reverse.

"Can you take aspirin?"
"Yeah"
"I'm going to give you 5 baby aspirin. I can't give you water

So just clear them. "
I did
[redacted]
They asked me to take off my shirt so they could place more EKG leads. I got an IV. "Is your throat what that is?" "Yes."

"Are you allergic to anything?"
"Peanuts and Penicillin."
"Well, we'll put away the peanuts."

I laughed.
"At least someone gets my jokes," he said.
"You need a sense of humor in this job, you know?"

She put a sheet over my chest.

Soon we were there. They opened

the door before, in the chair

[redacted]

Traffic walkie-talkies buzzed with a constant stream of incidents. 11 24 year old female with arm injury. 84 year old male. Motor vehicle collision with tree.

[redacted]

the door and rolled me out.

The shiny rear room

empties except for another stretcher that had been hitched in first and its attendant paramedic.

A woman emerged at the desk "Looks like you've got two," the paramedic said. "Yeah, things are hopping," she said, like a shop owner excited about a crowd.

She looks down the other

[redacted]

gory's info.

On TV, hospitals are busy places and everything happens in a rush, one thing right after another. This one was empty and my overwhelming impress of the whole thing was that it was slow. A wait to get there, a wait to decide what to do, a wait before getting on the [illegible], a wait

[redacted]

before starting the
truck and now
a wait here. Aside
from the first minutes
when the emergency
personnel swarmed
it here seemed like
anyone was in a rush.

Luckily I was feeling better
now.

Eventually they got to
me and I was [illegible]

[redacted]

[redacted]

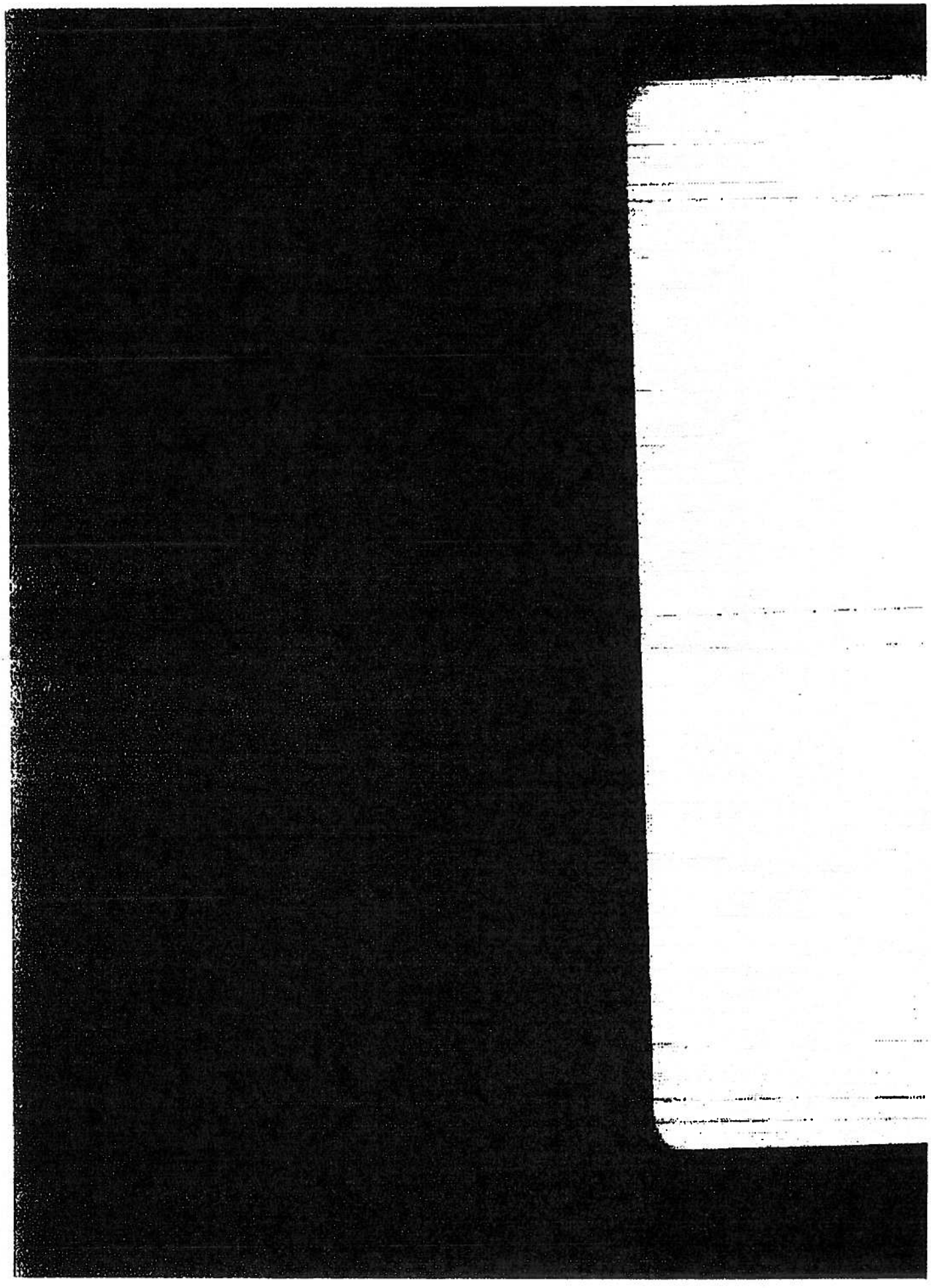
in the computer and moved onto a hospital cart. I was ~~taken for another EKG and then asked~~ where I was on the pain scale. I was taken for an EKG and returned. The paramedics began winding up their equipment and washing down the stretcher.

"Scott's probably already

[redacted]

there," the guy said.
"Yeah, but this one has
with a time! It's got
pre-first-trial," she sa
They said goodbye and
headed off.

"It's elevator," said
the girl. "Two want to
take him back."
"Ok, I'm gonna give it
to Ramirez. You think he ca
cover it?"
"What's he got?"



[redacted]

"Nothing. A little old lady who fell on her hip.

They wheeled me back.

Patrick came in to explain. "Uh, so," he rubbed his bike anxiously against the wall. "The EKG shows these elevations, they're like, uh, here, let me just show it to you, that'll be easier.

He showed me a printo[illegible]

[redacted]

Of one of those little heart graphs you see. "See, like, there's a clear example. Here and here, it's supposed to be the same. But it's not. It's slightly elevated. Now when it's elevated in just one place, it's a heart attack. But you, you're elevated all over." Oh.

"That's usually a sign of pericarditis which is like

[redacted]

Well, it's an inflammation of the sack around the heart. Like arthritis is an inflammation of the joints?"

Yeah.

"Usually we give you some anti-inflammatories."

"Is it chronic or does it go away?"

"Eh, it goes away, don't worry. I'm going to draw some blood. You're going to feel a little..."

I felt a prick. That wasn't so bad. Q "Mm. Q Ow, that hurt! Q "Here, need to move your arm." He moved it down and tried again — ow! that really hurt.

"Ok, your doctors are (b)(7)(C) and the attending is (b)(6),(b)(7)(C) the resident, he'll probably be your main doctor.

Later, (b)(6),(b)(7)(C) came in. "Well, you've got these ST elevations. What are

[redacted]

you do?" "I'm a [illegible]
"Ah, well you have
abnormal ST elevations

[redacted] (b)(6),(b)(7)(C)

"What's going on?"
"You want the full story?"
"Well, just give me the ab[illegible]
activities, I kind of have the
[illegible]" "He held up a P[illegible]

— [illegible]
"What's going on?"
I gave him the abnormal[illegible]

[redacted]

I've ordered a heart [illegible] and we're going to check your blood for heart markers. But this is weird, so I'm going to show it to my attending."

The attending came in. "What's going on?" I gave him the [illegible] story. I'd gotten fairly good at it. "Has this ever happened to you before?" "No." "Taken any drugs?"

[redacted]

No. Smoked. No. Drank
No. Anything strange? [illegible]
Under any stress? No
Nervous? Anxious? No.
"Well, it's probably just
stress. You're too young to
be having heart problems.
But with pericarditis
we want to be conservative."
So we're going to keep you
under observation
overnight and give you
a stress test in the morning.
You should be out by noon."

[redacted]

"Ok ... [illegible]. A [illegible] walked by. "Too much light in here." [illegible] switched some lights off and left. Another woman rolled in with a computer to verify my details, including my insurance. I wondered for the first time how much this was all going to cost. The vast expense of it all hadn't occurred to me before.

I got my chest X-ray and some lunch (Roast leg red sauce and meatballs with a side of carrots. And diet coke to drink! How odd)

(b)(6) (b)(7)(C) visited & I was ready to go to observation, which is supposed to be a more comfortable bed and a tiny TV. Another nurse took over. It was much busier although there was a

[redacted]

Verating TV. There wasn't much to.
Luckily I'd taken a book
to Tosa's. So I read.

The nurse just came back in.
~~[illegible]~~ "Just one more
question they forgot to
ask you: Do you feel
safe where you are?"
Huh? Do they think it's
Munchausen's?

In the bathroom a sign says
"You are not alone." Turns

[redacted]

But it's not a surveillance warning, just an offer for sexual abuse counseling. That's what [illegible] was about.

The hospital bed is more isolated than anything so far this month. Not only is there no clocks, there are no windows. There is no phone. No one can ask me if I want to call someone or if I needed to cancel plans or explain why I wouldn't

[redacted]

[redacted]

be at work tomorrow.
It doesn't bother me -
my whole plan for today
was to relax and read -
but how can anyone else
do it?

It is a tiny cell just
big enough for the bed. The
curtain is drawn and the
door is closed, there's no
sign of another human being.
Imagine waking up like this
you'd think you were

[redacted]

[redacted]

in solitary confinement. This is the life that drives men mad.

~~[illegible]~~ A O_2 monitor is on my finger, my EKG leads tether me to a machine; a blood pressure cuff inflates every couple minutes and IV needle digs into my arm. How am I supposed to sleep like this?

Another voice would be so comforting right now.

[redacted]

My worst nightmare came true
I finished my book. I
found a phone and a clock,
but I only knew two phone
numbers. This feels like a
logic puzzle. I called
the first # and had them log
into Facebook as me
and look up my girlfriend's
Sadly she's not still in town
but seemed distraught (could
I'm perfectly comfortable,
and willing to arrange a
delivery.

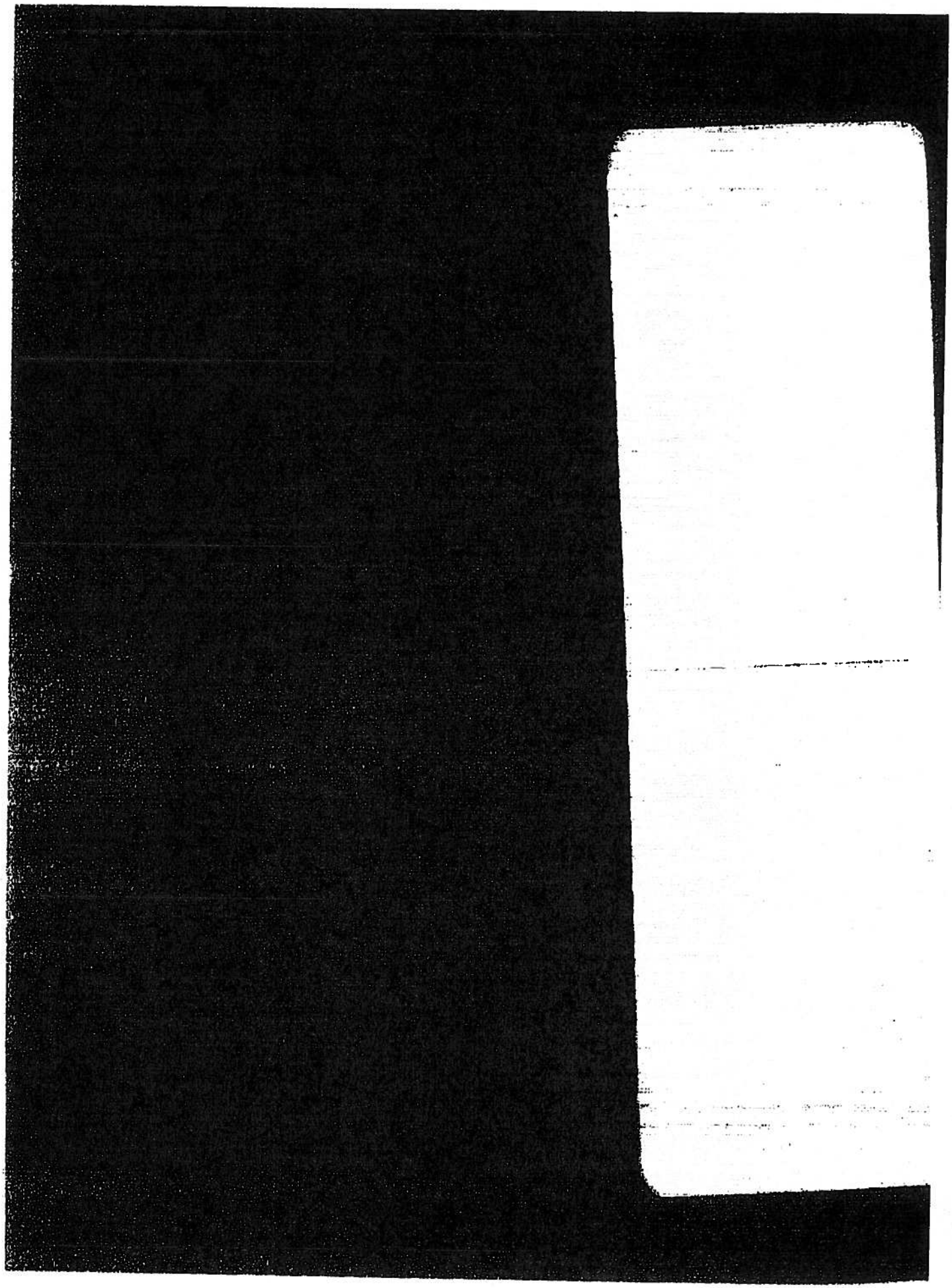
I really don't want to use

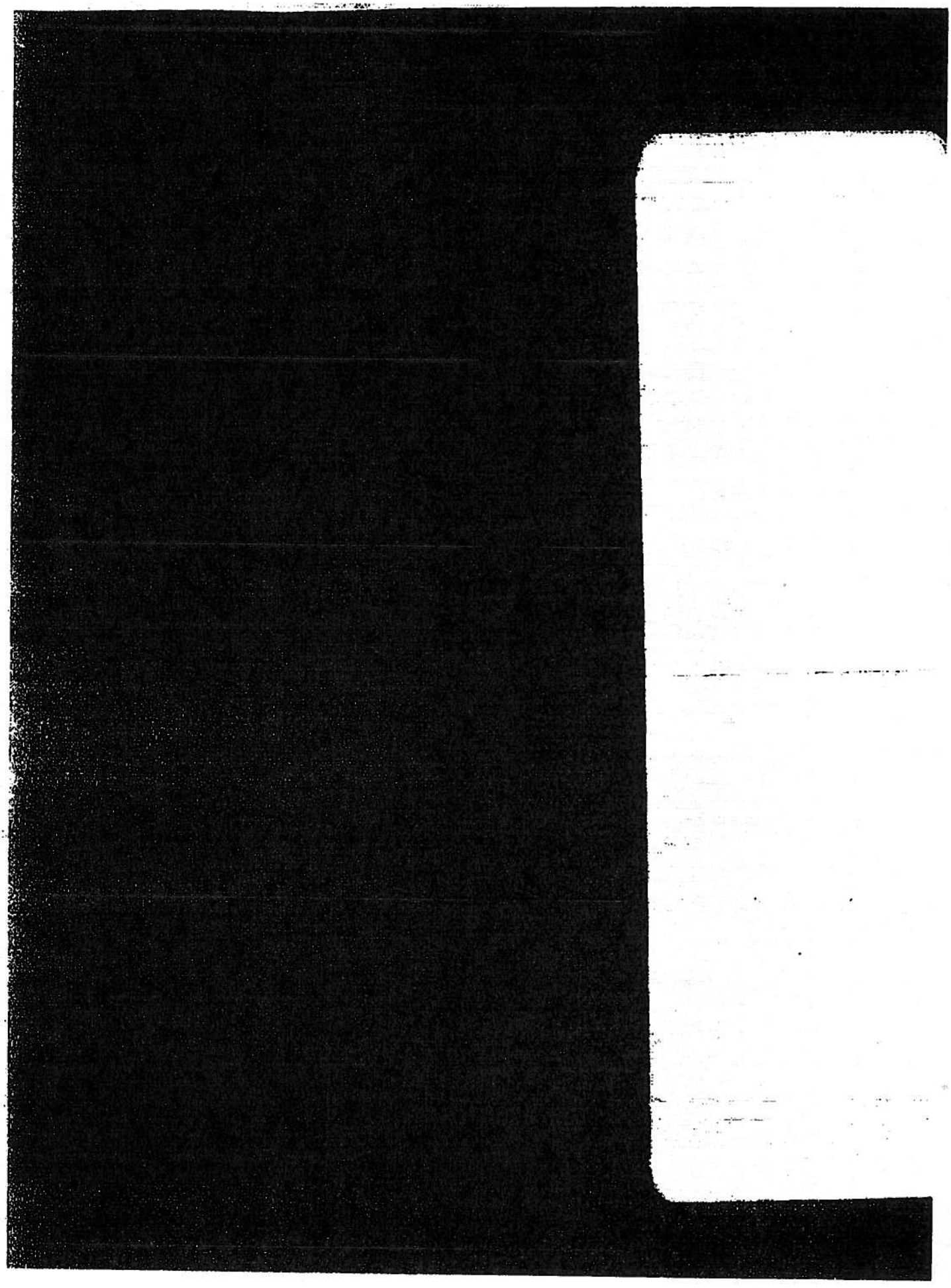
[redacted]

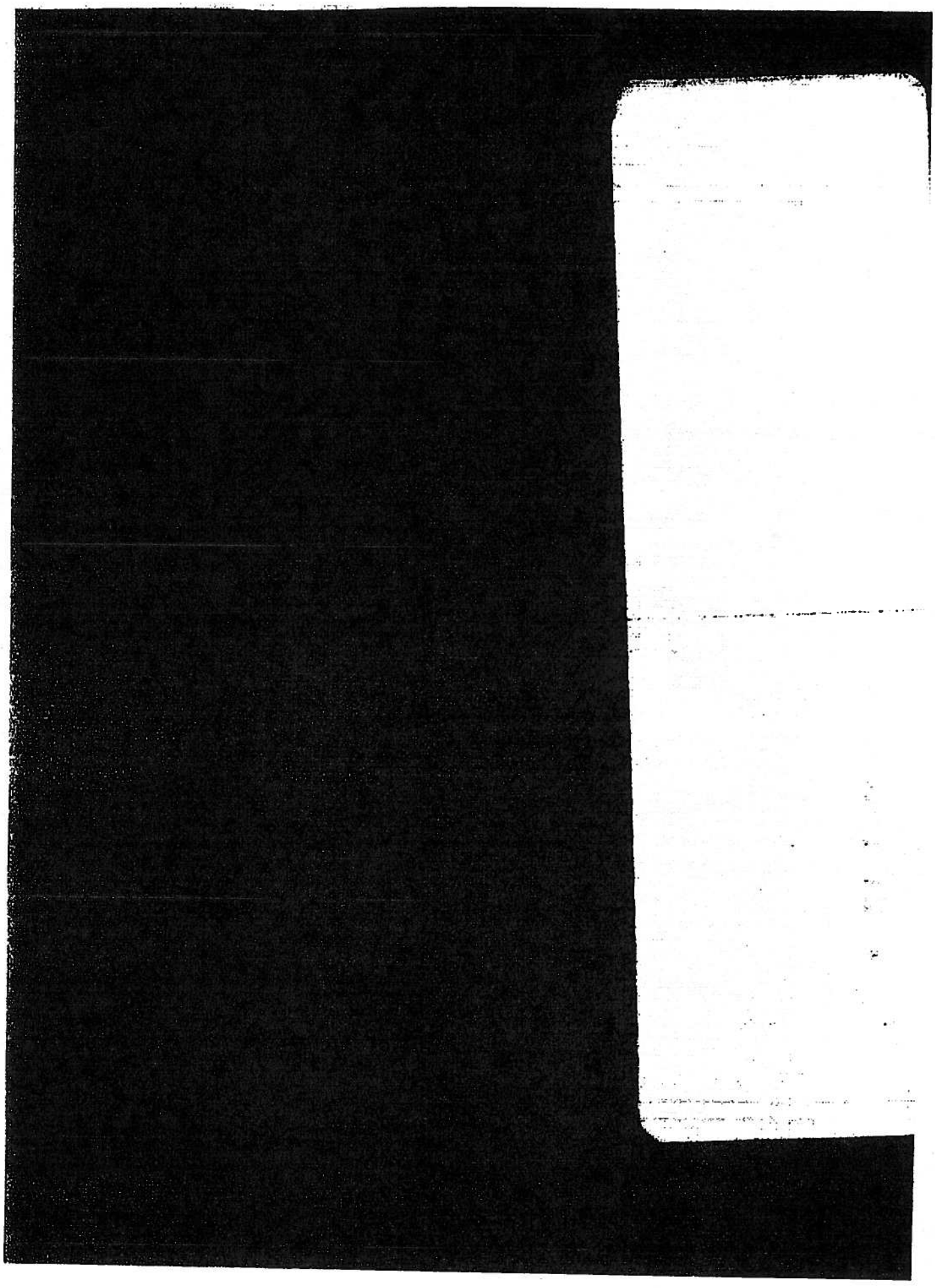
the phone, but the prospect of 17 hours chained in a cell w/o a book was too much to take.

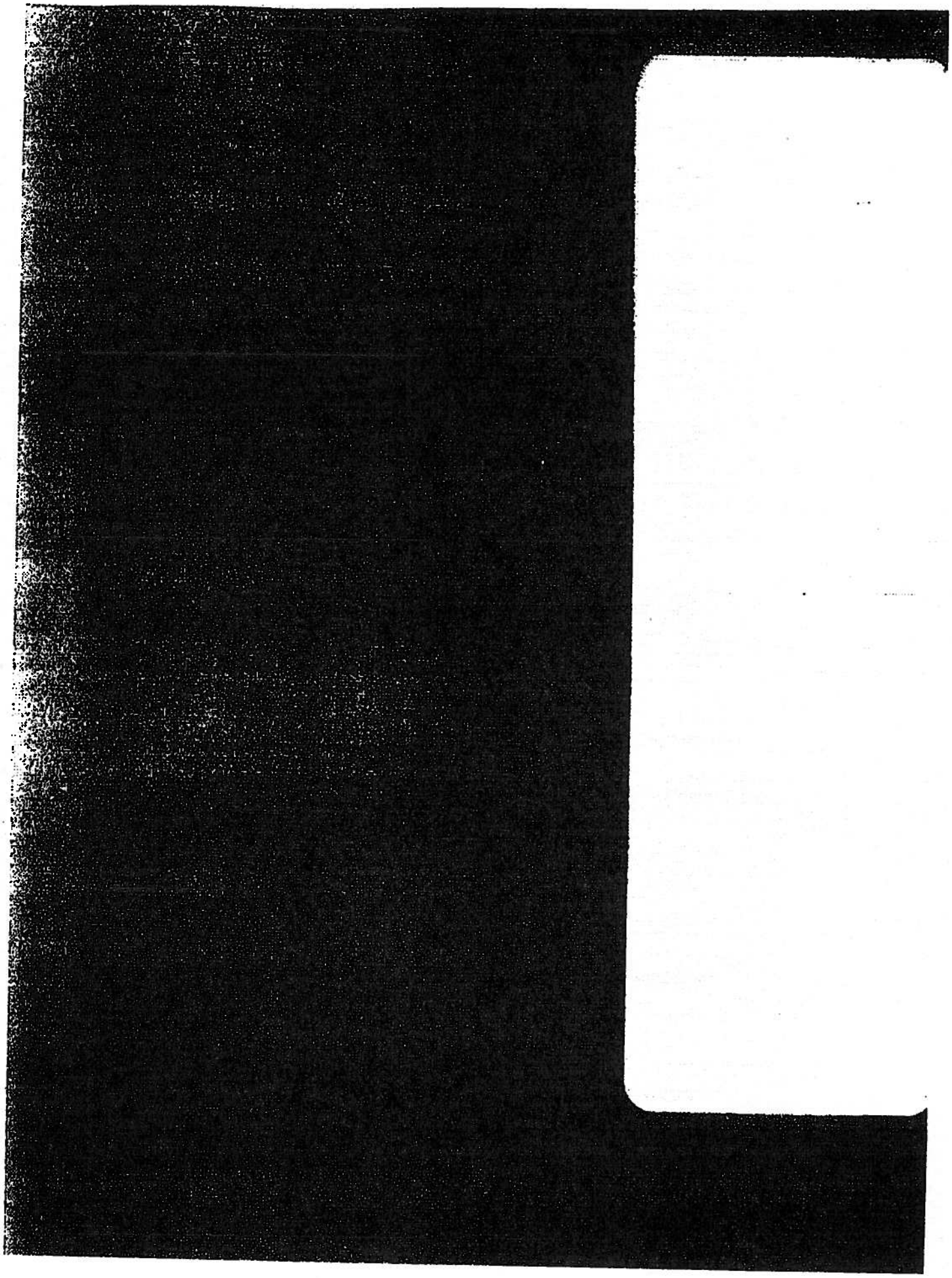
[redacted]

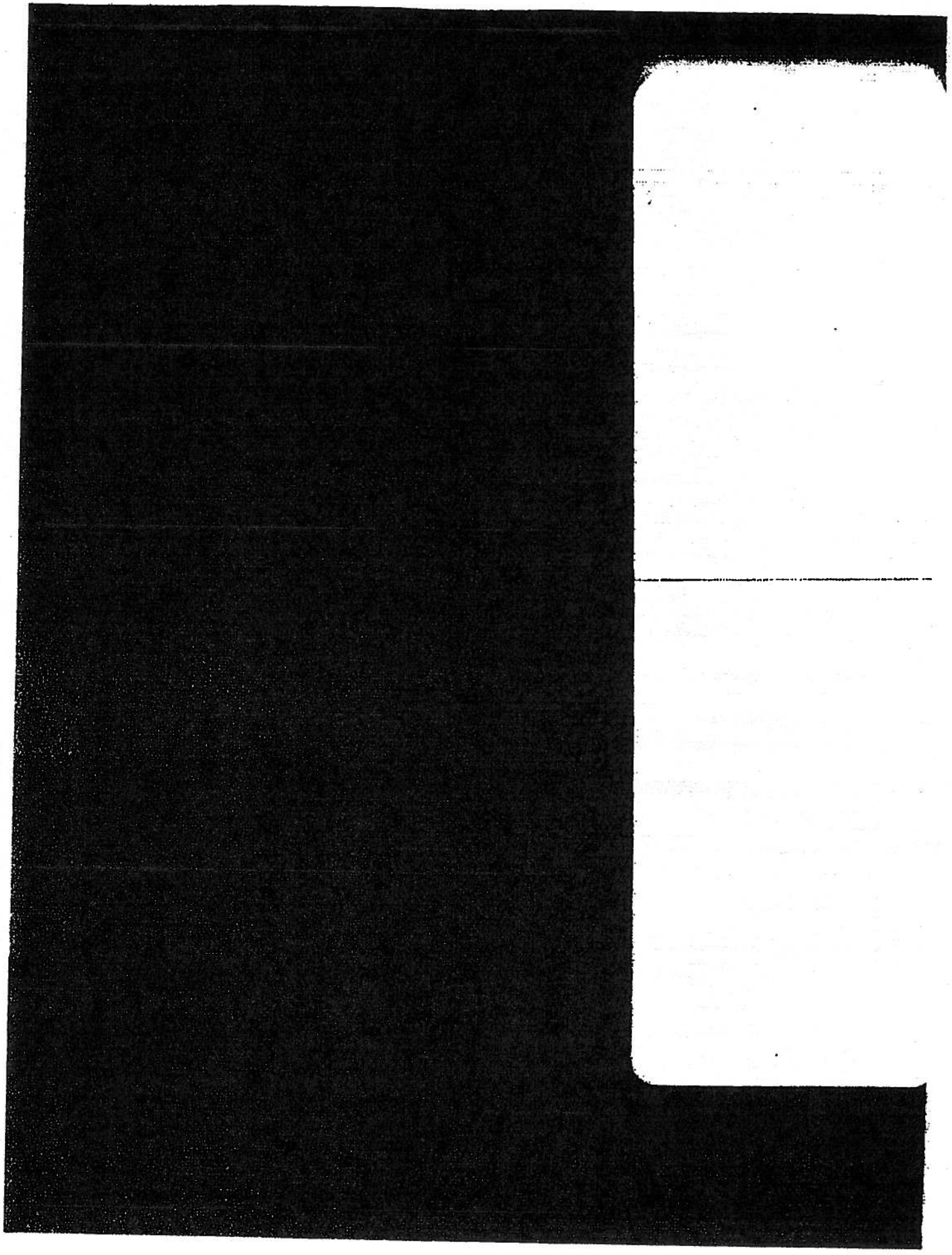
RIF



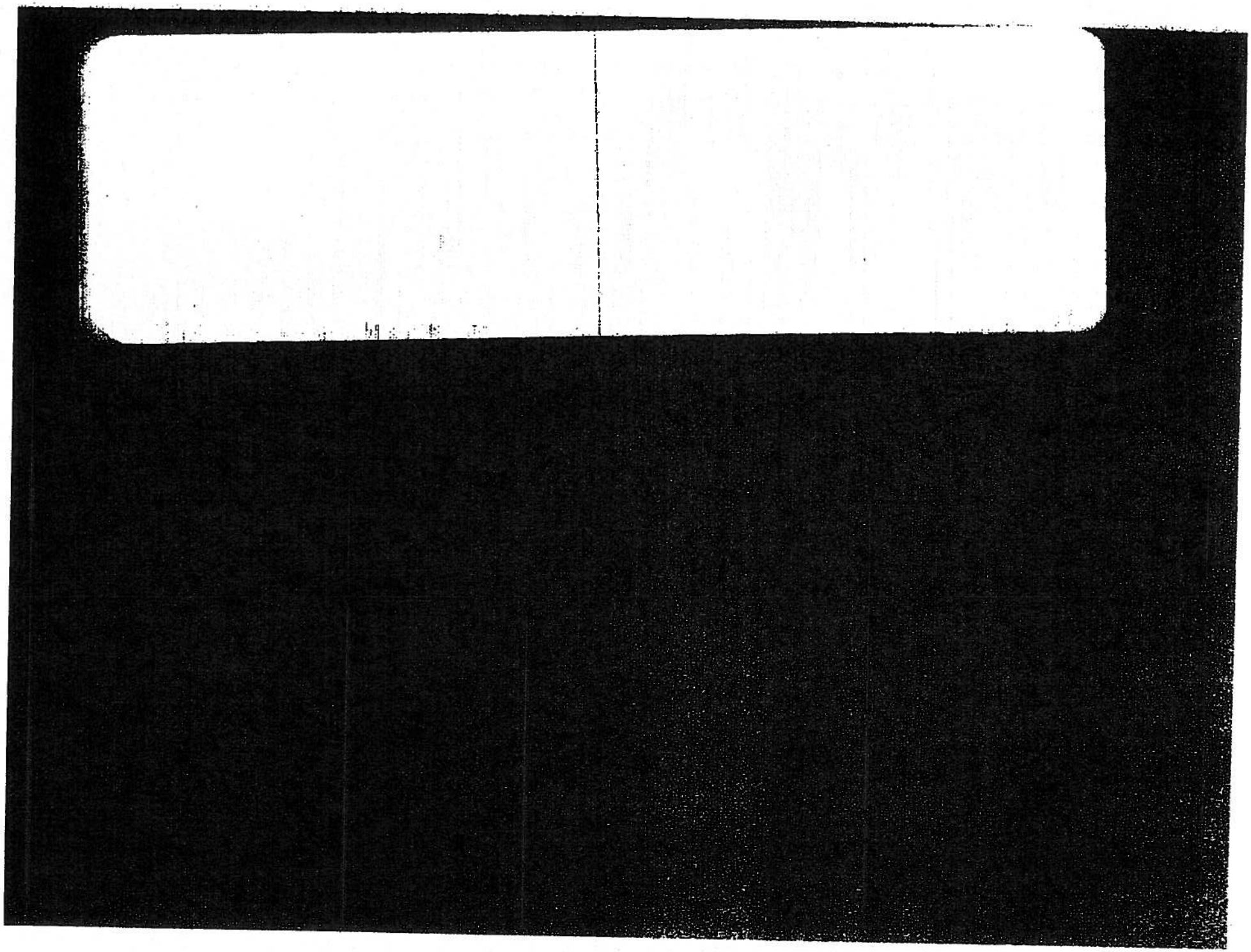


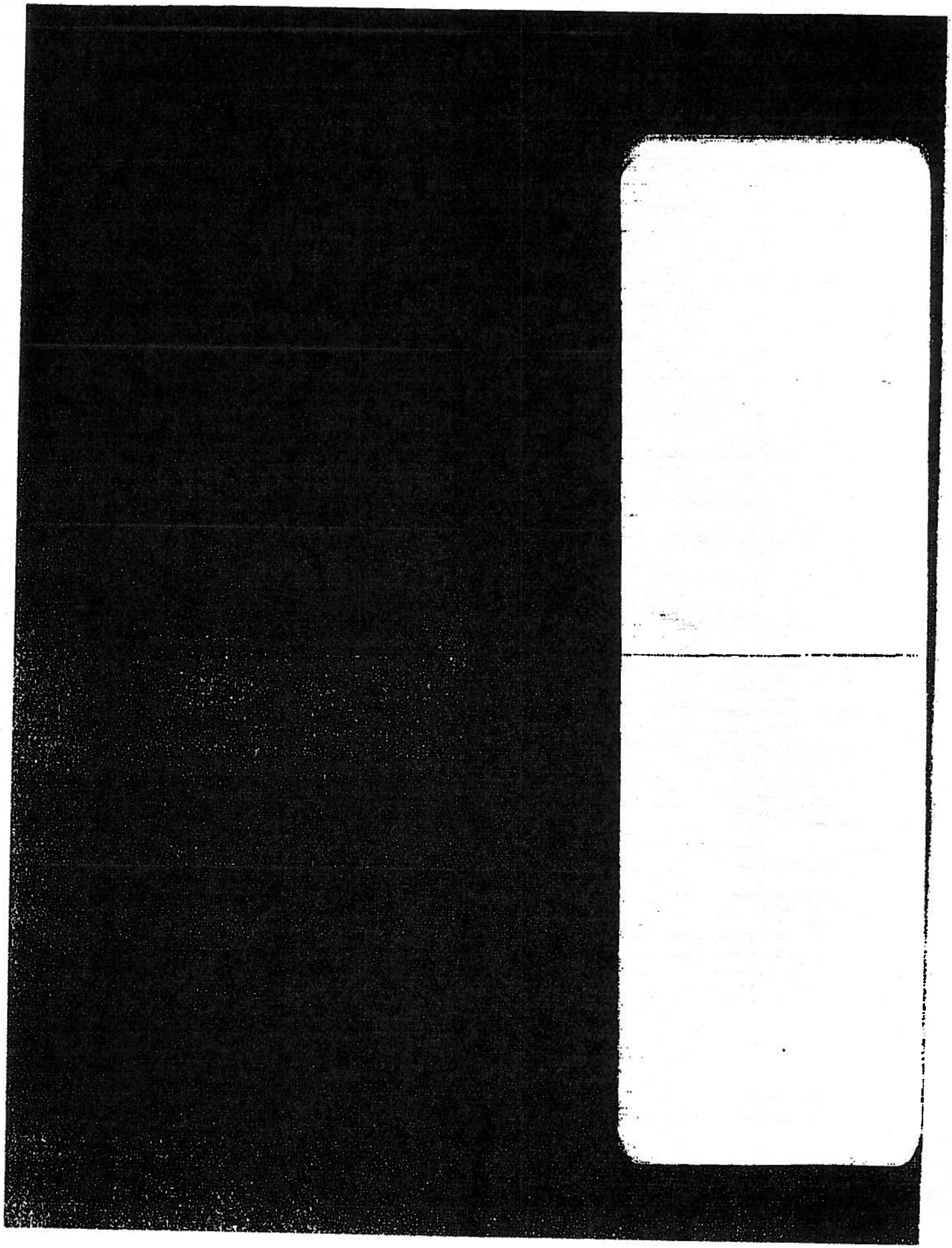


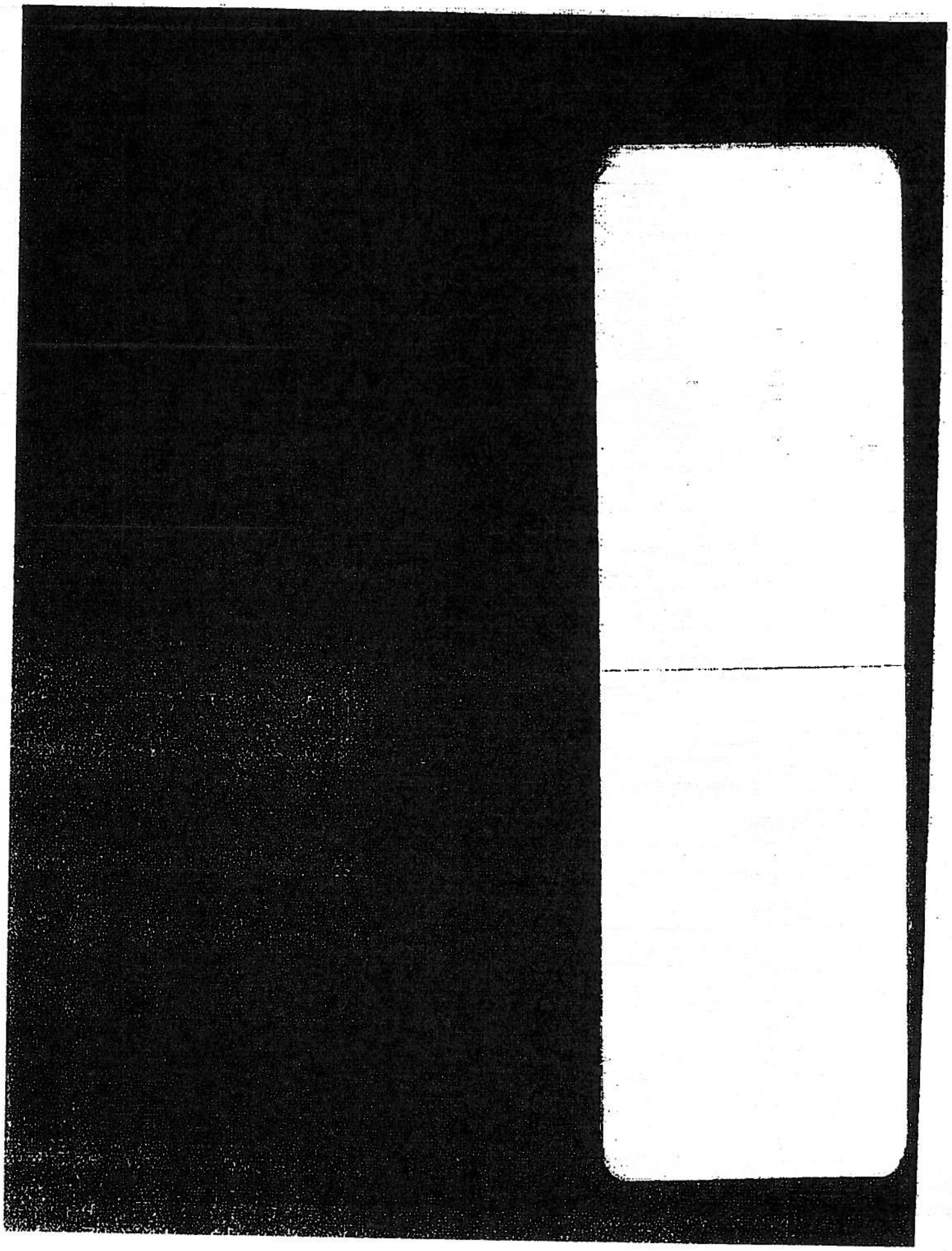




[redacted]







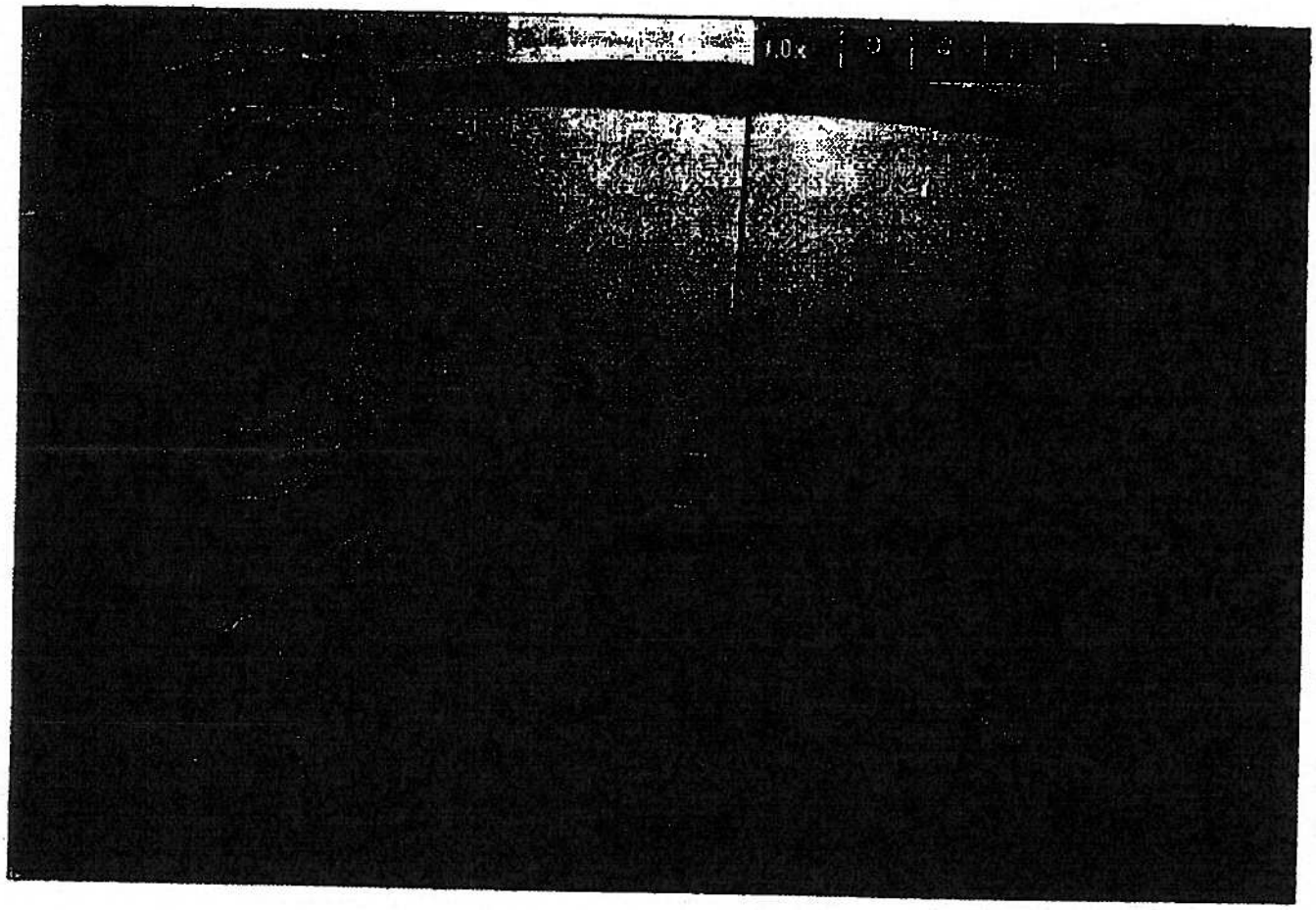
the plane, but the prospect of 17 hours cramped in a seat like a book was too much to take.

From: (b)(6),(b)(7)(C) Contacts @ JSTOR.txt
Sent: Tuesday, January 25, 2011 4:32 PM
To:
Cc:
Subject: Contacts @ JSTOR (b)(6),(b)(7)(C)

Hi (b)(6),(b)(7)(C)

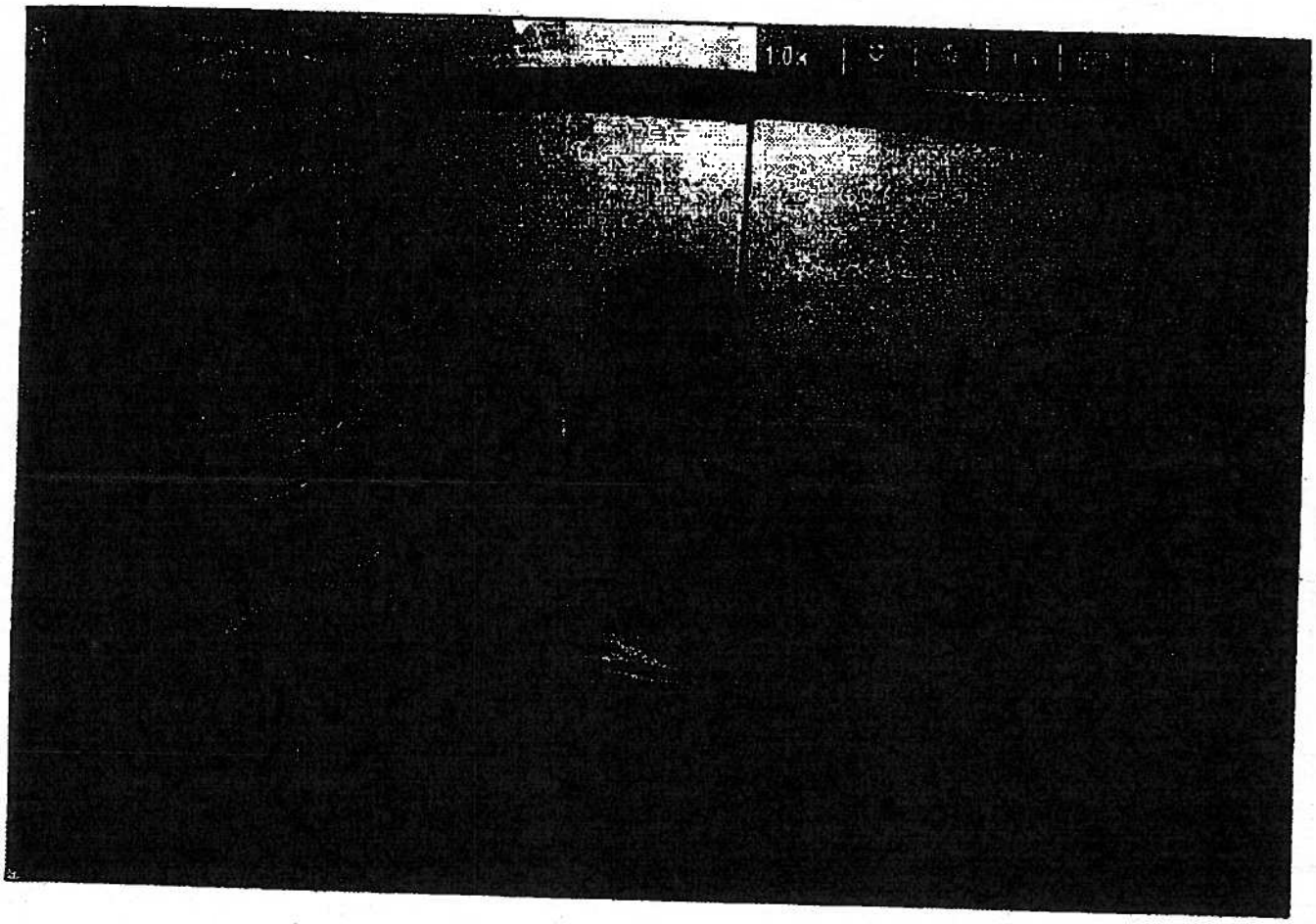
Please find the information requested below.

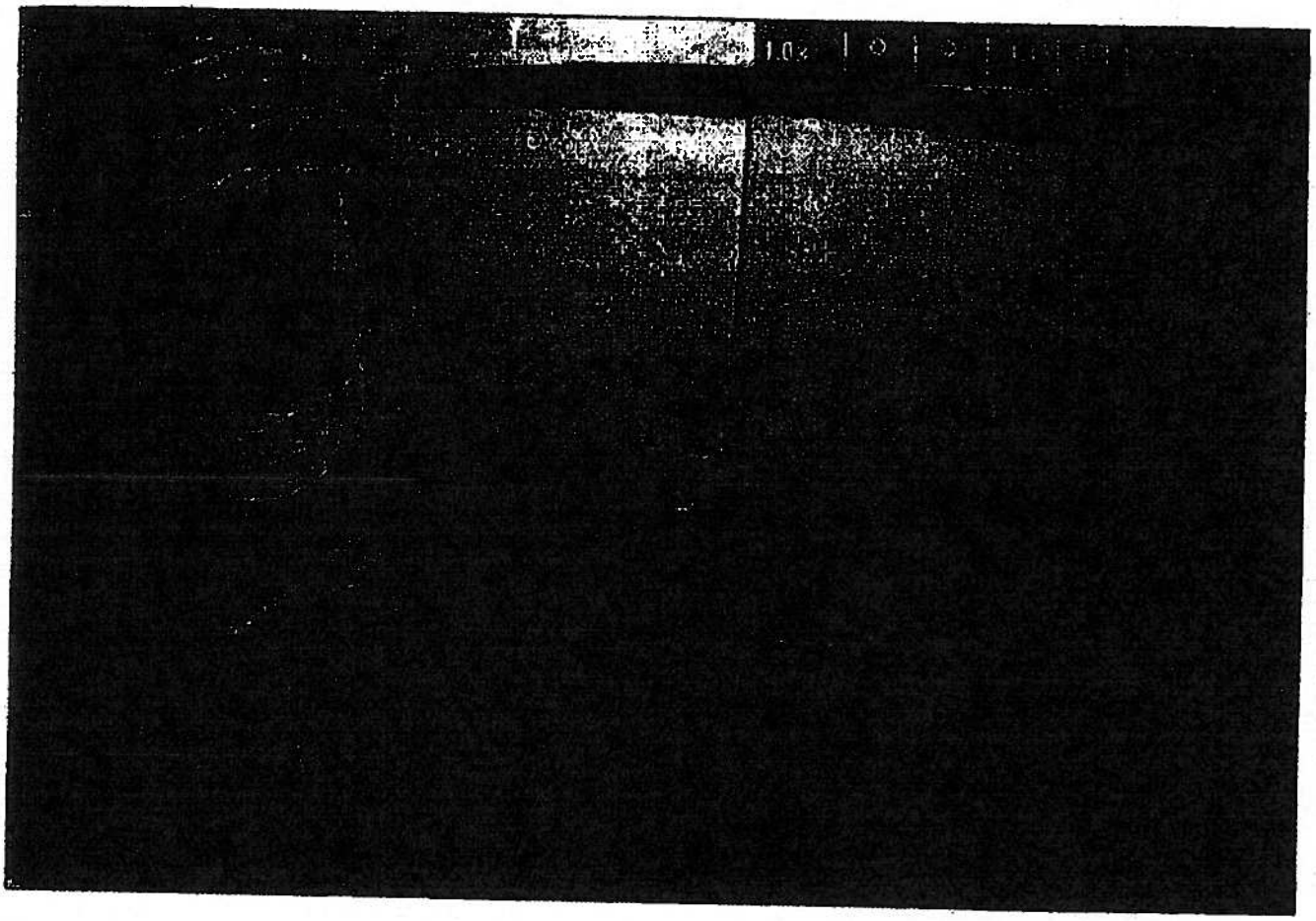
(b)(6),(b)(7)(C)

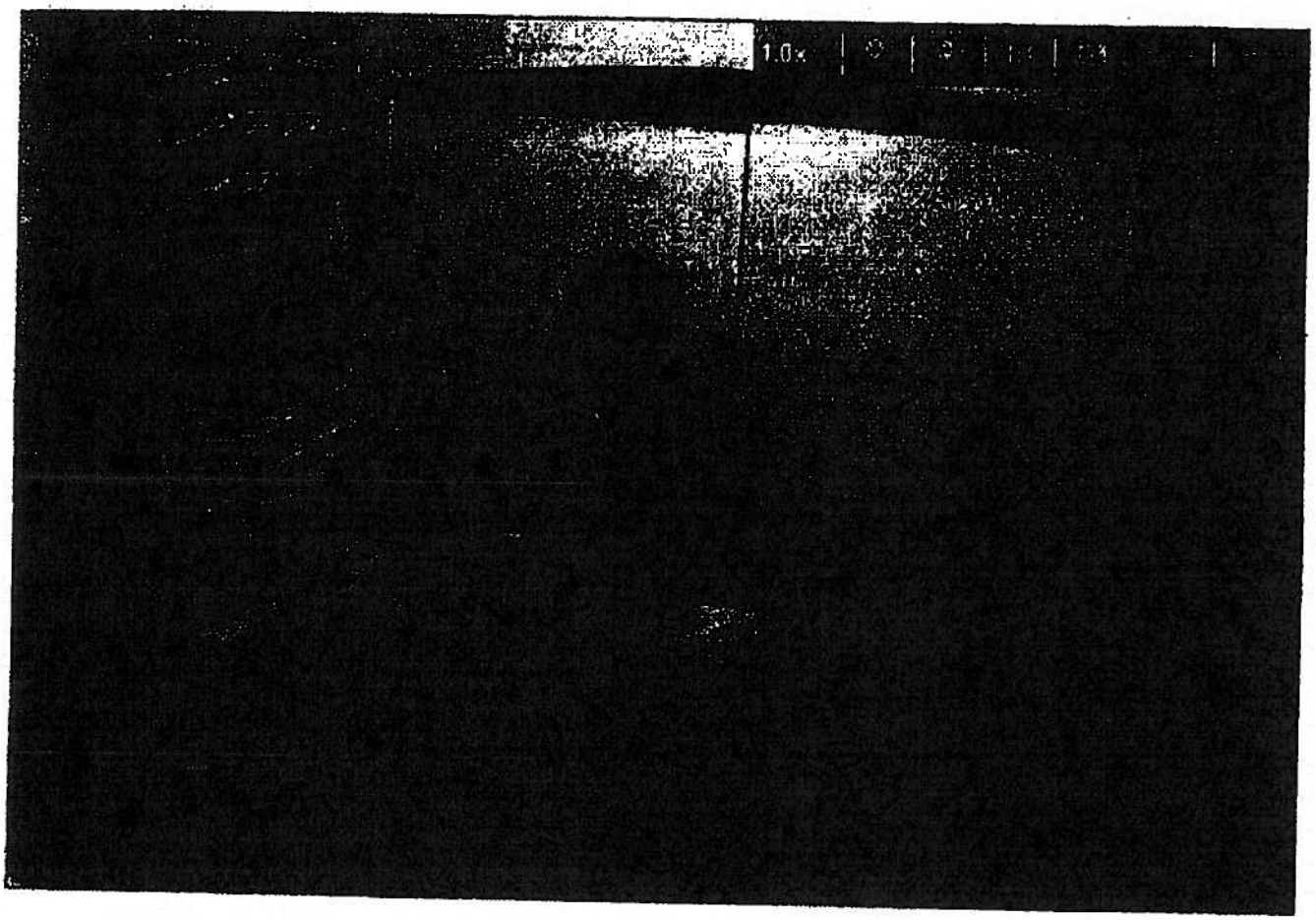


RIF

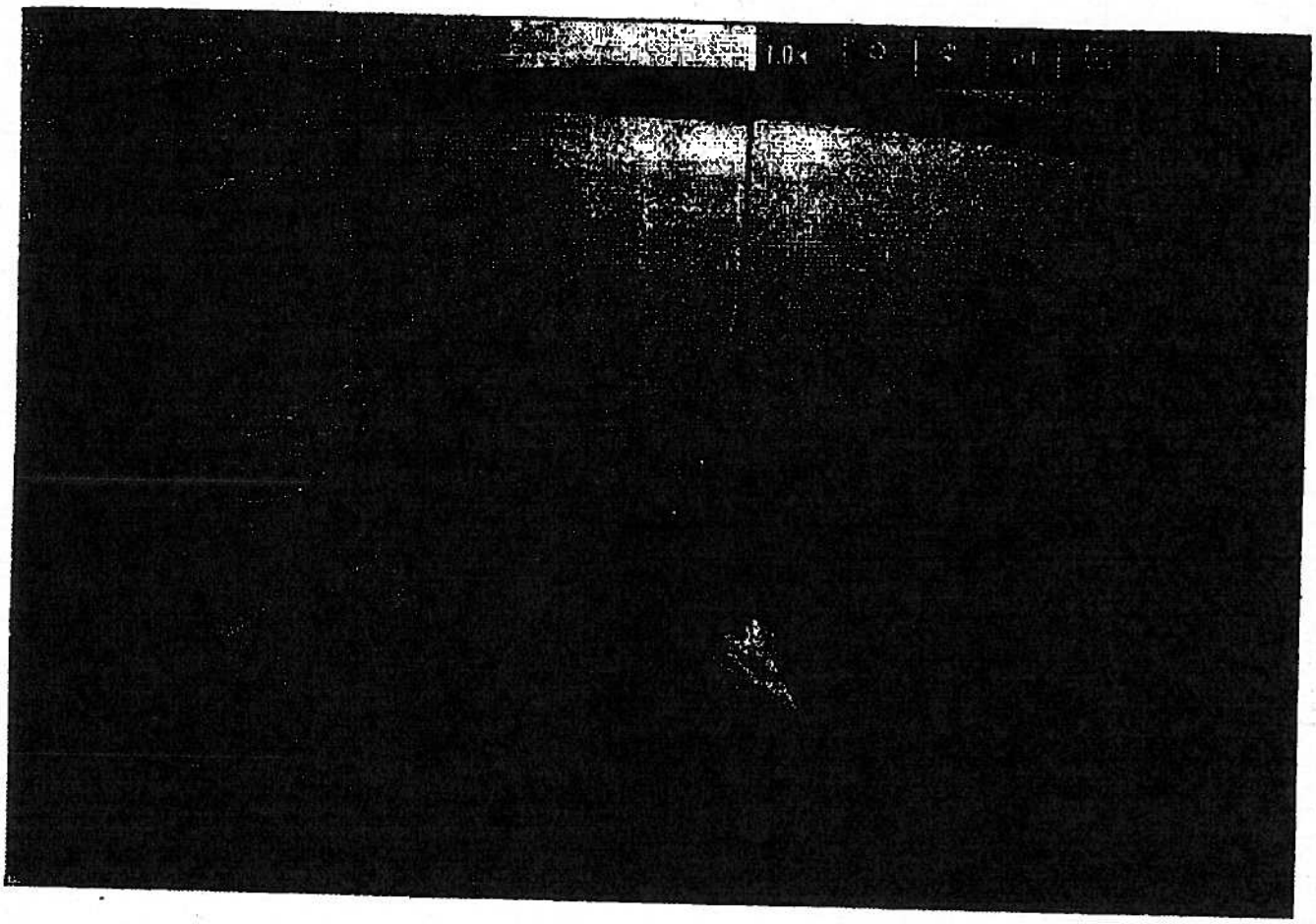
595

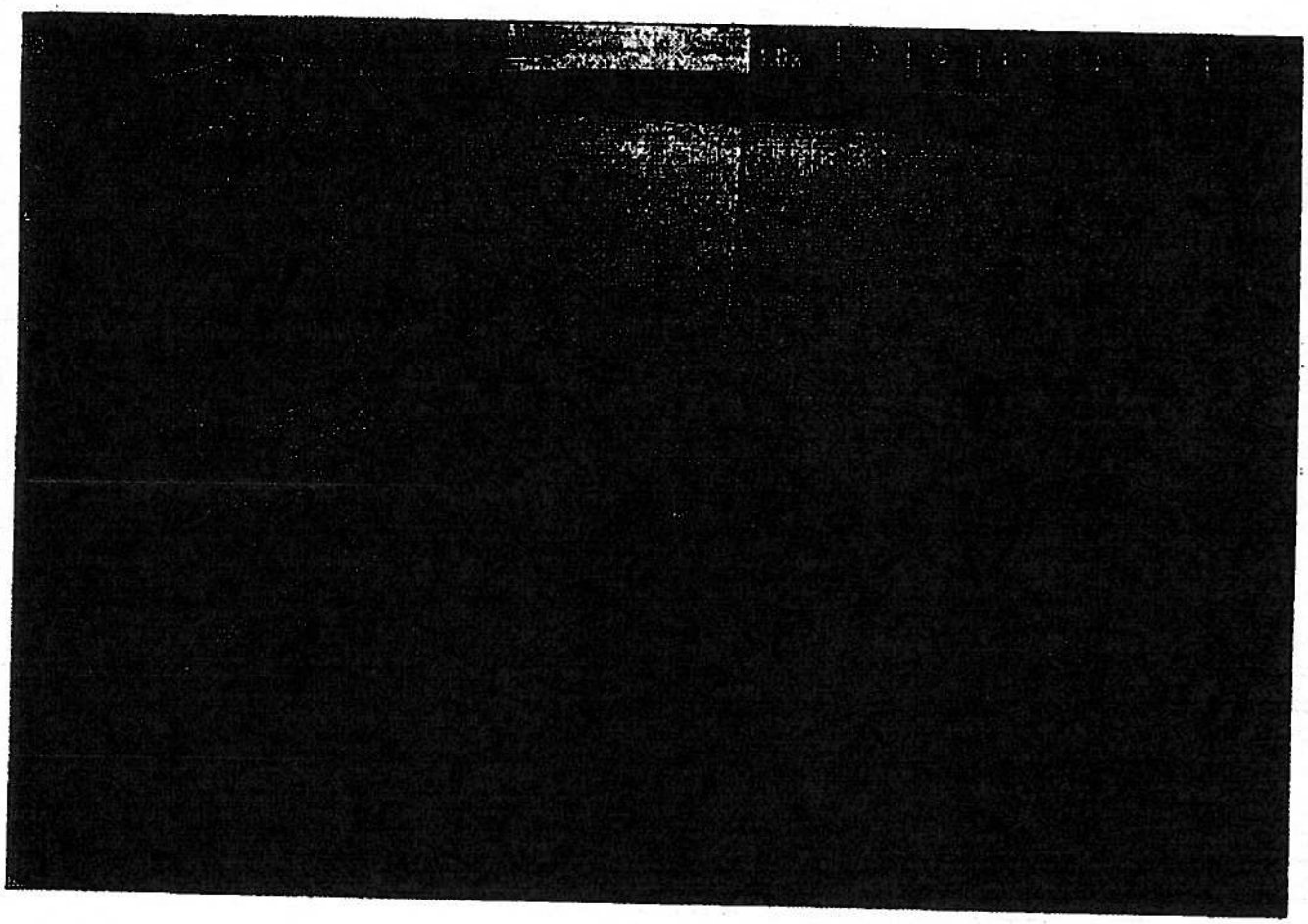


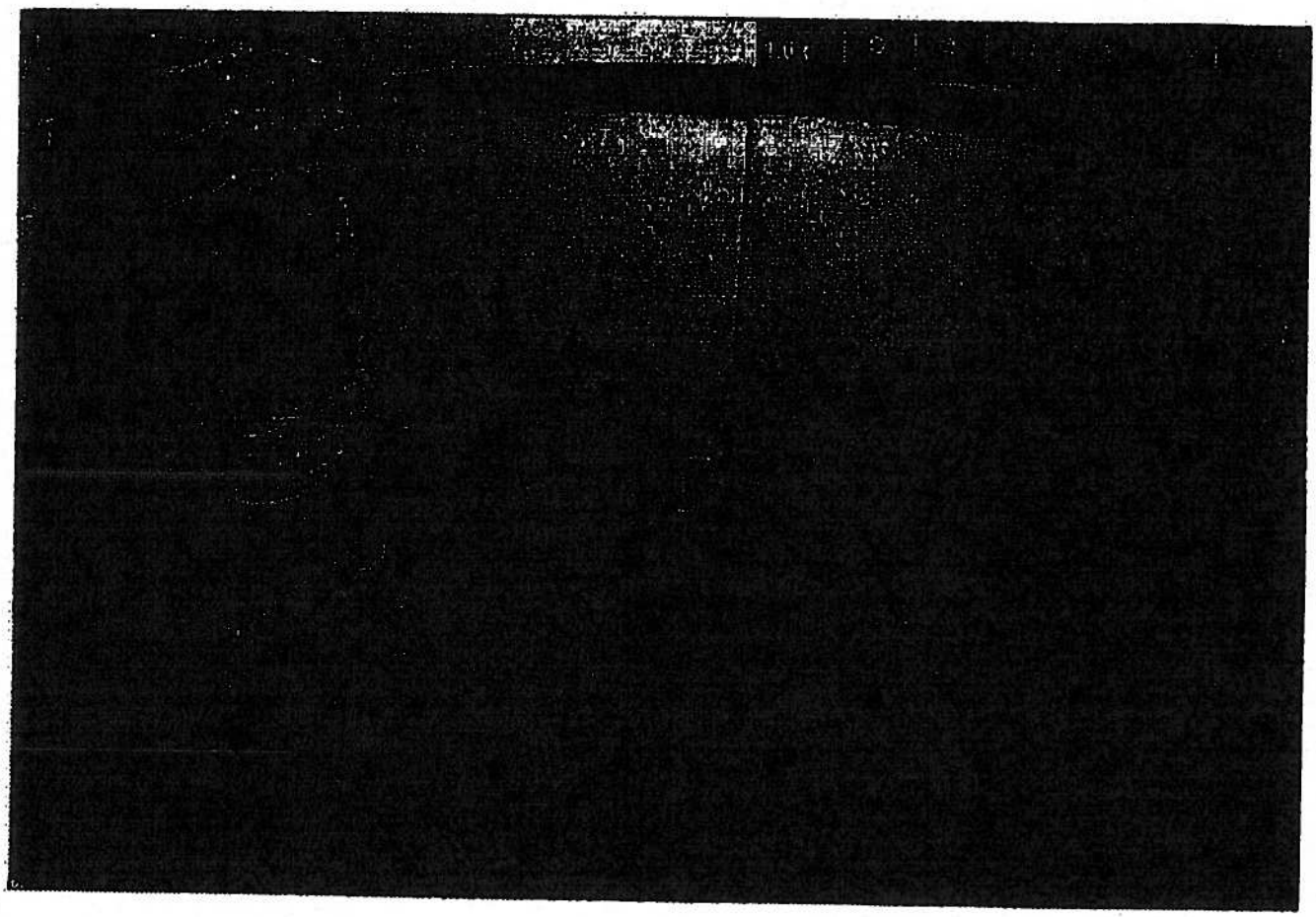




RIF







(b)(6),(b)(7)(C)

- 04JAN2011 – MIT discovers a laptop connected to the MIT network in a telecommunications wire closet in the basement of building. MIT police contact the Cambridge Department. Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force notifies the Task Force and SA (b)(6),(b)(7)(C) respond to MIT. A camera is set up in the wire closet. MIT Police observe a suspect return to the closet, replace the hard drive attached to the laptop and then leave the closet.

MIT informs SA (b)(6), (b)(7) of the timeline that lead to the discovery of the laptop:

  - 24SEP2010 - Aaron Swartz registers a laptop on MIT's network. MIT's network recognizes the laptop's MAC address as 00235a735ffb.
  - 25SEP2010 – Swartz's laptop is assigned IP address 18.55.6.215. JSTOR experiences an extraordinary volume of automated requests and downloads from its digitized journal collections to that IP address. JSTOR blocks access to its network from 18.55.6.215.
  - 26SEP2010 - JSTOR suffers rapid and voluminous downloads from IP address (b)(6),(b)(7)(C) JSTOR blocks a much broader range of IP address, temporarily denying service to legitimate users at MIT.
  - 27SEP2010 - MIT bars the MAC address .00235a735ffb from being assigned a new IP address.
  - 02OCT2010 – Swartz spoofs his MAC address as 00235a735ffc and is able to register as a guest on the MIT network.
  - 08OCT2010 – MIT network assigns the Swartz' laptop IP address (b)(6),(b)(7)(C)
  - 09OCT2010 - Downloading of journals from IP address (b)(6),(b)(7 begin.
  - NOV to DEC 2010 – Over 2 Million illegal downloads from JSTOR.
  - 24SEP2010 - Aaron Swartz registers a laptop on MIT's network. MIT's network recognizes the laptop's MAC address as 00235a735ffb.
  - 25SEP2010 – Swartz's laptop is assigned IP address 18.55.6.215. JSTOR experiences an extraordinary volume of automated requests and downloads from its digitized journal collections to that IP address. JSTOR blocks access to its network from 18.55.6.215.
  - 26SEP2010 - JSTOR suffers rapid and voluminous downloads from IP address 18.55.6.216. JSTOR blocks a much broader range of IP address, temporarily denying service to legitimate users at MIT.
  - 27SEP2010 - MIT bares the MAC address 00235a735ffb from being assigned a new IP address.
  - 02OCT2010 – Swartz spoofs his MAC address as 00235a735ffc and is able to register as a guest on the MIT network.
  - 08OCT2010 – MIT network assigns the Swartz' laptop IP address (b)(6),(b)(7)(C)
  - 09OCT2010 - Downloading of journals from IP address (b)(6),(b)(7) begin.
  - NOV to DEC 2010 – Over 2 Million illegal downloads from JSTOR.

- 06JAN2011 – MIT Police observe the same suspect return to the closet, retrieve the laptop and hard drive and leave the closet. MIT Police observe the suspect near the University and the suspect is arrested for breaking and entering. During booking the suspect is identified as Aaron Swartz. Inside the backpack Swartz was wearing is a USB flash drive. MIT locates Swartz's laptop connected to MIT's

network in another building. The laptop and hard drive are collected by SA (b)(6), (b)(7)(C) and turned over to Cambridge Police for processing.

- 24FEB2011 – A Search Warrant is issued for SA (b)(6), (b)(7)(C) to examine Swartz's Laptop, the attached Hard Drive and the USB Flash Drive. The MAC address assigned by the manufacturer to the Ethernet interface card in Swartz's laptop is the same as the MAC address recognized by MIT's network the first time Swartz's laptop registered in September, 2010. On Swartz's Laptop was a software application "keepgrabbing.py" designed to download .PDF files. The USB Drive found in Swartz's backpack contained a nearly identical file. The Western Digital Hard Drive, which was recovered with the laptop, had Aaron Swartz's fingerprint on it. The drive contained a folder named "pdfs" which contained an estimated over 97,000 .PDF files. A spot check of approximately a dozen of those files reflected that each was a digitized journal article from the journal storage service. A logging file on the Acer Laptop, known as the .bash_history file, showed the steps Swartz's took to bypass MIT's and JSTOR's security

THE FACTS – AARON SWARTZ INVESTIGATION

BACKGROUND

September 24, 2010

Late during the night of September 24, 2010, an unidentified 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. 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 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.

September 25, 2010

The day after registering the "ghost laptop," the unidentified 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 18.55.6.215 to 18.55.6.216. 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.

September 27, 2010

When JSTOR notified MIT of the problems, MIT banned the "ghost laptop" from using its network as well. 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.

October 2, 2010

Less than a week after JSTOR and MIT had barred the individual's ghost laptop from communicating with their networks, the unidentified 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.

October 8, 2010

The unidentified 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."

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 that could be blocked. Consequently, JSTOR blocked access by and to every computer using an MIT IP address campus-wide for approximately three days, again depriving legitimate MIT users from accessing JSTOR's services. 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 unidentified 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. During 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 detected, 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.

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. The wiring closet is protected by a pair of locked steel doors. 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.

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

LAW ENFORCEMENT IS NOTIFIED

January 4, 2011

MIT personnel call the MIT Police to the scene, who, in turn, call a USSS New England Electronic Crimes fulltime Task Force Officer directly. The TFO is a Detective from Cambridge Police. Three members of the task force respond to the scene, a USSS Special Agent, a Boston Police Detective who is a fulltime TFO and the Cambridge Police TFO who received the call. A Cambridge Police Crime Scene Unit was summoned to the scene for processing. Over the course of the morning and early afternoon of January 4th, MIT and law enforcement officers collaboratively 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;

(b)(3):Rule 6E

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 more than likely 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.

Within an hour of their departure, the unidentified hacker returned. After entering the wiring closet and shutting the doors behind him, 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. This activity was captured by the video camera that was installed inside the wiring closet.

Agents notified the US Attorney's Office for the District of Massachusetts the facts of the investigation.

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. 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. As he left, he again hid his face with his bicycle helmet. This activity was also captured by the camera installed within the wiring closet. 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.

Shortly after 2:00pm on January 6, 2011, MIT Police Captain (b)(6),(b)(7)(C) 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 (b)(6), (b)(7)(C) 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 subsequently 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. 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.

February 9, 2011

The Secret Service applied for and subsequently obtained a federal warrant for Aaron Swartz's apartment, located at 950 Massachusetts Avenue in Cambridge.

February 11, 2011

Agents and a Task Force Officer executed the federal search warrant on Swartz's residence.

Immediately after the residence search warrant was completed a second search warrant was applied for and issued for Swartz's worksite. That search warrant was executed on Swartz's work address, 124 Mount Auburn Street in Cambridge, The Safra Center for Ethics at Harvard Law School.

February 24, 2011

The Secret Service obtained a search warrant to seize and search the laptop, the hard drive in the enclosure and the USB storage device that was being secured within the Cambridge Police Evidence Unit.

February 25, 2011

The evidence is transferred from the Cambridge Police to the USSS Boston Field Office pursuant to the search warrant.

May 16, 2011

Swartz was served in hand, at his residence with a forfeiture warrant for property of JSTOR in his possession and refused to comply with the Court's warrant.

June 7, 2011

USSS BFO Agent responds to Swartz's current defense counsel's office, Goode and Cormier 83 Atlantic Ave Boston, MA. At that location USSS took custody of (4) four HDD's containing 8,989,635 articles (PDF's) that had been downloaded from the JSTOR website through MIT's network by Swartz.

July 14, 2011

Federal Grand Jury indicts Aaron Swartz for Wire Fraud, Computer Fraud and data theft.

July 19, 2011

Aaron Swartz is arrested and arraigned at the Moakley Federal Court House in Boston, Massachusetts.

September 12, 2012

Aaron Swartz is indicted with a superseding indictment unpacking the offenses.

Rough Chronological Sketch

9/24/10
"Gary Host" obtains DHCP lease
lists e-mail address as ghost@mailinator.com
client name: "ghost laptop"
MAC address 00:23:5a:73:5f:fb
IP at registration (b)(6),(b)(7)(C)

9/25/10
DHCP ack for 18.55.6.215
client name: "ghost laptop"
MAC address 00:23:5a:73:5f:fb
abusive downloads to JSTOR from 18.55.6.215

9/26/10
abusive downloads to JSTOR from (b)(6),(b)(7)(C)

9/27/10
MIT deactivates "ghost laptop" registration;
blocks MAC address 00:23:5a:73:5f:fb

10/2/10
Swartz changes last byte of MAC address
"Gary Host", as a result, able to obtain new guest DHCP lease
lists e-mail address as ghost@mailinator.com
client name: "ghost laptop"
MAC address 00:23:5a:73:5f:fc
given IP address (b)(6),(b)(7)(C)

10/8/10
"Grace Host" obtains DHCP lease
lists e-mail addres as ghost42@mailinator.com
client name: "ghost macbook"
MAC address 00:17:F2:2c:b0:74
assigned IP (b)(6),(b)(7)(C)

10/9/10
Abusive downloading from JSTOR to IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

November 2010-January 2011
Abusive downloading from JSTOR to IP addresses: (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

1/4/11
MAC address 00:4c:e5:a7:56 is registered to both (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

On 01/14/11 [redacted] Detective [redacted] Captain [redacted] AUSA Heymann and [redacted] counsel for MIT met at the MIT office of General Counsel with [redacted] Information Service and Technology [redacted] analyst for MIT [redacted] informed the group that an examination of the DHCP logs during the time in September when JSTOR was reporting the excessive downloads show a computer registered as "ghost-laptop" with a MAC address of 00:23:5a:73:sf:fb and an email address of ghost@mailinator.com.

Detective [redacted] noted that all of the suspicious computer registrations on 09/24/10, 10/01/10, 10/08/10 and 12/24/10 occurred on Friday nights. Captain [redacted] confirmed that foot traffic in the tunnel of building 16 would be light during those times.

[redacted] stated that on 10/01/10 the an attempt was made to register with the same MAC address as used on 09/24/10; However, [redacted] had blocked that MAC address from registering. [redacted] stated that on 10/02/10 another attempt was made to register on the network with a MAC address of 00:23:5a:73:sf:fc but still for "ghost-laptop."

[redacted] also stated that at one point on 10/09/11, "ghost-laptop" was registered with a MAC address of 00:23:5a:73:5f:fc and "ghost-macbook" was registered with a MAC address of 00:17:f2:2c:b0:74 at the same time.

[redacted] also stated that after 12/19/11, the attempts to register on the MIT network for "ghost-laptop" and "ghost-macbook" changed from attempts to gain an IP address dynamically assigned through the MIT guest registration process to assigning themselves static IP addresses on the MIT network. This behavior continued until after Swartz was observed on 01/06/11 moving the laptop from Building 16 to and the machine was registered on the network from the Stratton Student Center.

[redacted] also stated that on 01/06/11 at approximately 1251 the computer connected to an IP address registered to Amazon's Elastic Compute Cloud (EC2) service.

[redacted] noted that5 up to 12/19/10, Swartz obtained IP addresses by using the guest registration to be assigned an IP address through DHCP. From 12/19/10 to 01/06/11, Swartz would assign himself a static IP address. [redacted] theorized that once Swartz understood the subnet mask of the network Building 16 was on it would have been easy to assign himself an IP address that was not being used; However when he moved the laptop to the Stratton Student Center on 01/06/11, he connected to a new switch and went back to obtaining an IP address through DHCP.

Prior to this incident, JSTOR granted access to anyone using a IP address from the MIT network. MIT has a class A network and owns all of the IP addresses beginning with 18.

[redacted] recalled that on 01/03/11 [redacted] sent him an email telling him that JSTOR informed her that they had detected abuse from IP address [redacted] On 01/04/11, [redacted] traced the IP address [redacted] in the ARP table to MAC address 00dc.e5a0.c756. MAC address C04c.e5a0.c756 was also assigned IP address [redacted] on the ARP table. [redacted] stated that IP address [redacted] was logged with zero seconds talking on the network. [redacted] theorized that Swartz established IP address [redacted] to

communicate with the computer incase the MIT network shut down IP address (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) stated that IP address (b)(6),(b)(7)(C) was an IP address registered to JSTOR that appeared in the logs.

(b)(6),(b)(7)(C) stated that early in the morning of 01/04/11 he noticed in the ARP table that the IP address reported for abuse by JSTOR was active on the switch Gi 8/16 that he knew was in Building 16. The switch is also listed in the logs M16-004t-sw-entry.mit.edu. 004T refers to the room number 4T, the wire closet where the Acer Aspire one netbook with serial number LUSAX0D001001100E1601 was found. (b)(6),(b)(7) recalled that at approximately 0200 he sent an email to (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) with the switch the computer committing the abuse was attached to and asked them to find it.

(b)(6),(b)(7)(C) confirmed that the closet was generally kept locked.

(b)(6),(b)(7)(C) stated that at first Swartz used guest registration to obtain an IP address but that static IP address were used later. (b)(6),(b)(confirmed that someone with guest registration has full access in and out of the network. (b)(6),(b)(7)(C) stated that MIT border routers do block the Microsoft ports.

(b)(6),(b)(7)(C) stated all three registrations Swartz used were variation of ghost with the computer name either being ghost-macbook or ghost-laptop and the name used for guest registration being either Gene, Gary or Grace.

(b)(6),(b)(7)(C) stated that based on the logs he reviewed that Swartz must have spoofed his MAC address at least once. The MAC address used in January (00:4c:e5:a0:c7:56) had an invalid Organizationally Unique Identifier (OUI).

(b)(6),(b)(7)(C) stated that the emails Swartz used for guest registration used a service called mailinator. Mailinator is a service that gives spoofed emails the appearance of legitimate emails.

The packet capture from 01/04/11 identified two open ports on the Acer Aspire one found in 04T. The ports that were open were 22 and 8092. (b)(6),(b)(7)(C) identified that the service CherryPy was running. CherryPy is a web application framework using the python programming language.

(b)(6),(b)(7)(C) estimated that as of 1/14/11, MIT had spent 160 man-hours investigating the abuse by Swartz.

Nokia cell phone with power cord
T-Mobile HTC G2 cell phone with power cord
Twelve (12) magnetic media tapes in a FedEx box
Metallic Blue iPod
White iPod with white carrying case
White iPod with Serial Number 8A6330856UX8A
White iTalk
Black 16GB thumb-drive
"Office Depot" DVD-R with handwritten label "Bibliographic data which mysteriously appeared one day as the sun was shining"
Pocket notebook with blue and white hexagon and rectangle design cover
Pure Drive model 761 external hard drive quick start guide with CD
Disc utility internal hard drive upgrade kit
Seagate SATA 3.5" Barracuda internal hard drive installation guide
Scientific Atlantic modem
Apple multi adapter with serial number 6F9395M7ZU6
Apple multi adapter with serial number 6F7281NNU4S
Black notebook journal
Wireless-G 2.4 GHz broadband router linksys with serial number CDFG1G609626
MacBook install disk one and two in paper sleeve
MacBook user guide in cardboard case
Apple care service letter
Genius Bar work confirmation
Digital Media compact flash
Fifty-four miscellaneous compact disks
Two hard drive enclosures
T-Mobile sidekick
Sony Micro Vault
Harvard University earning statement
Earning statement addressed to Aaron Swartz
Master's Thesis M-876 Lind, William Edmund, Thomas McDonald: "A study of an Engineer Administrator & his Influence of Public Roads in the US 1919-1953"

ISSN	Journal	Articles Downloaded	Total Articles	% Downloaded
00071447	The British Medical Journal	83,412	431,510	19.33%
00368075	Science	24,577	201,093	12.22%
00946214	Public Health Reports (1896-1970)	11,472	45,503	25.21%
09588434	The Musical Times and Singing Class Circular	8,216	20,012	41.06%
0002936X	The American Journal of Nursing	6,963	46,854	14.86%
00278424	Proceedings of the National Academy of Sciences of the Unit	6,891	104,949	6.57%
00292397	The North American Review	5,722	22,686	25.22%
00274666	The Musical Times	5,450	49,069	11.11%
00182613	Historische Zeitschrift	5,345	45,692	11.70%
0009840X	The Classical Review	5,243	30,832	17.01%
00028762	The American Historical Review	5,236	61,141	8.56%
15471357	The Virginia Law Register	4,360	11,265	38.70%
00068071	Botanical Gazette	4,298	13,455	31.94%
00030147	The American Naturalist	4,169	19,407	21.48%
00262234	Michigan Law Review	3,921	19,577	20.03%
00167398	The Geographical Journal	3,867	28,677	13.48%
00027162	Annals of the American Academy of Political and Social Scier	3,842	42,099	9.13%
00029890	The American Mathematical Monthly	3,642	38,724	9.41%
00440094	The Yale Law Journal	3,577	17,760	20.14%
00130133	The Economic Journal	3,482	19,258	18.08%
09510788	The Burlington Magazine for Connoisseurs	3,345	14,132	23.67%
00138266	The English Historical Review	3,309	38,676	8.56%
0017811X	Harvard Law Review	3,169	22,417	14.14%
00048038	The Auk	3,005	24,714	12.16%
00366773	The School Review	2,713	10,824	25.06%
00101958	Columbia Law Review	2,625	15,423	17.02%
00973157	Proceedings of the Academy of Natural Sciences of Philadelp	2,511	7,543	33.29%
00029114	American Journal of Archaeology	2,329	11,920	19.54%
00027294	American Anthropologist	2,322	27,913	8.32%
01903578	The Biblical World	2,252	5,546	40.61%
00223808	The Journal of Political Economy	2,246	13,658	16.44%
00129658	Ecology	2,226	18,350	12.13%
03701662	Proceedings of the Royal Society of London	2,225	5,549	40.10%

00029122	American Journal of Botany	2,176	14,266	15.25%
00105422	The Condor	2,083	10,570	19.71%
01496611	Modern Language Notes	2,042	13,048	15.65%
00409618	Bulletin of the Torrey Botanical Club	2,007	11,094	18.09%
00029602	The American Journal of Sociology	1,911	24,140	7.92%
00141704	Ethics	1,889	5,965	31.67%
00138274	The English Journal	1,867	23,313	8.01%
02607085	Philosophical Transactions (1683-1775)	1,850	4,392	42.12%
2041997X	Provincial Medical and Surgical Journal (1844-1852)	1,832	4,278	42.82%
01905929	Bulletin of the American Geographical Society	1,827	4,523	40.39%
0035869X	Journal of the Royal Asiatic Society of Great Britain and Irela	1,797	13,101	13.72%
00211753	Isis	1,762	17,633	9.99%
00964018	The Science News-Letter	1,742	50,313	3.46%
00916765	Environmental Health Perspectives	1,718	13,358	12.86%
00426601	Virginia Law Review	1,716	11,407	15.04%
01609335	The Journal of Philosophy, Psychology and Scientific Method:	1,709	4,098	41.70%
21506256	The Decorator and Furnisher	1,708	4,089	41.77%
0003049X	Proceedings of the American Philosophical Society	1,682	7,696	21.86%
00098353	The Classical Journal	1,664	12,210	13.63%
00322032	Poetry	1,648	37,776	4.36%
00323195	Political Science Quarterly	1,586	15,911	9.97%
15503283	The American Journal of Theology	1,555	3,683	42.22%
00216682	The Jewish Quarterly Review	1,532	6,162	24.86%
00318108	The Philosophical Review	1,503	11,662	12.89%
15583813	The American Law Register (1852-1891)	1,482	3,788	39.12%
00081221	California Law Review	1,457	8,181	17.81%
02610523	Philosophical Transactions of the Royal Society of London	1,421	3,278	43.35%
20419996	Association Medical Journal	1,353	3,277	41.29%
01999818	Proceedings of the American Academy of Arts and Sciences	1,334	4,424	30.15%
00274380	Notes	1,328	15,794	8.41%
00029947	Transactions of the American Mathematical Society	1,322	16,690	7.92%
00218723	The Journal of American History	1,300	25,992	5.00%
00029300	The American Journal of International Law	1,297	20,638	6.28%
00063444	Biometrika	1,267	7,347	17.25%
00264423	Mind	1,267	10,422	12.16%
00384038	Southern Economic Journal	1,259	10,166	12.38%

00028282	The American Economic Review	1,256	25,161	4.99%
00030279	Journal of the American Oriental Society	1,242	16,264	7.64%
00030023	Transactions of the American Microscopical Society	1,239	5,985	20.70%
00180777	Hermes	1,233	6,974	17.68%
0015587X	Folklore	1,231	8,702	14.15%
0022166X	The Journal of Human Resources	1,201	2,286	52.54%
00029556	The American Journal of Psychology	1,191	13,275	8.97%
00221376	The Journal of Geology	1,148	10,871	10.56%
09528385	Journal of the Royal Statistical Society	1,139	4,950	23.01%
00251496	Man	1,133	19,184	5.91%
1940641X	The Classical Weekly	1,125	9,162	12.28%
00267074	Mnemosyne	1,066	10,316	10.33%
00030554	The American Political Science Review	1,055	25,079	4.21%
00029475	The American Journal of Philology	1,041	9,491	10.97%
00963771	The Scientific Monthly	1,030	10,277	10.02%
1526422X	International Journal of Ethics	1,014	3,536	28.68%
00255572	The Mathematical Gazette	1,001	20,506	4.88%
00219525	The Journal of Cell Biology	996	21,620	4.61%
00220515	Journal of Economic Literature	987	12,985	7.60%
00043249	Art Journal	971	4,463	21.76%
00435597	The William and Mary Quarterly	969	11,105	8.73%
00063568	BioScience	962	13,545	7.10%
09595295	The Journal of the Anthropological Institute of Great Britain i	960	2,261	42.46%
00373052	The Sewanee Review	960	12,857	7.47%
00267937	The Modern Language Review	952	28,654	3.32%
00218715	The Journal of American Folklore	931	10,008	9.30%
0161391X	The Mississippi Valley Historical Review	923	9,576	9.64%
00426636	The Virginia Magazine of History and Biography	912	8,854	10.30%
19440227	American Art News	899	2,135	42.11%
0030851X	Pacific Affairs	894	14,386	6.21%
0033362X	The Public Opinion Quarterly	886	5,923	14.96%
00384909	The Southwestern Naturalist	879	5,031	17.47%
00224367	The Journal of Risk and Insurance	872	3,646	23.92%
00377732	Social Forces	870	13,766	6.32%
0022409X	Journal of Range Management	865	7,949	10.88%
00335770	The Quarterly Review of Biology	862	30,745	2.80%

00220205	The Journal of Criminal Law, Criminology, and Police Science	861	3,335	25.82%
00376752	The Slavic and East European Journal	860	7,968	10.79%
00943061	Contemporary Sociology	858	21,772	3.94%
00314587	The Pennsylvania Magazine of History and Biography	855	9,439	9.06%
00251909	Management Science	843	8,539	9.87%
00825433	T'oung Pao	838	4,421	18.95%
00029939	Proceedings of the American Mathematical Society	838	26,696	3.14%
00131954	Educational Studies in Mathematics	837	1,967	42.55%
00076287	The Burlington Magazine	837	23,328	3.59%
00261521	The Metropolitan Museum of Art Bulletin	836	7,077	11.81%
00376779	Slavic Review	833	13,873	6.00%
01497952	German Studies Review	831	6,376	13.03%
00029831	American Literature	827	10,204	8.10%
00911798	The Annals of Probability	826	3,913	21.11%
09962743	Revue d'histoire moderne et contemporaine (1899-1914)	824	1,961	42.02%
0018702X	The Hudson Review	820	7,530	10.89%
03170861	Canadian Public Policy / Analyse de Politiques	819	3,672	22.30%
01882503	Revista Mexicana de Sociología	817	4,826	16.93%
0024094X	Leonardo	815	7,745	10.52%
00424935	Vetus Testamentum	813	5,869	13.85%
00369241	The Scottish Historical Review	812	5,947	13.65%
00352969	Revue française de sociologie	811	4,776	16.98%
00318248	Philosophy of Science	811	5,400	15.02%
00205850	International Affairs (Royal Institute of International Affairs	808	28,435	2.84%
00368423	Science News	808	44,934	1.80%
0022216X	Journal of Latin American Studies	806	4,308	18.71%
0003097X	Bulletin of the American Schools of Oriental Research	805	3,848	20.92%
00284866	The New England Quarterly	804	8,609	9.34%
00337587	Radiation Research	802	12,297	6.52%
00220507	The Journal of Economic History	800	12,214	6.55%
00380431	Sociometry	794	1,813	43.79%
00754269	The Journal of Hellenic Studies	793	10,079	7.87%
00925853	American Journal of Political Science	789	2,242	35.19%
00917648	Wildlife Society Bulletin	786	4,323	18.18%
00222445	Journal of Marriage and Family	786	6,135	12.81%
08857059	Marriage and Family Living	782	2,598	30.10%

R I F

08854173	Journal of the American Institute of Criminal Law and Crimin	781	2,303	33.91%
00262803	Micropaleontology	779	2,447	31.83%
00178160	The Harvard Theological Review	768	3,599	21.34%
00167428	Geographical Review	767	9,667	7.93%
00487511	Reviews in American History	762	3,891	19.58%
03664457	Bulletin of Miscellaneous Information (Royal Gardens, Kew)	760	2,974	25.55%
02847310	Ekonomisk Tidskrift	750	2,531	29.63%
09595341	Journal of the Statistical Society of London	736	1,800	40.89%
0009837X	Classical Philology	718	9,944	7.22%
08831351	PALAIOS	713	1,908	37.37%
0041977X	Bulletin of the School of Oriental and African Studies, Univer	703	14,521	4.84%
0266626X	Proceedings of the Royal Geographical Society and Monthly I	692	1,624	42.61%
00093920	Child Development	692	8,362	8.28%
00435643	The Wilson Bulletin	688	11,479	5.99%
20419961	Provincial Medical Journal and Retrospect of the Medical Scie	683	1,570	43.50%
00308129	PMLA	680	9,575	7.10%
03684016	Journal of the Royal African Society	671	3,499	19.18%
00238791	Latin American Research Review	669	2,452	27.28%
00221899	The Journal of Infectious Diseases	666	27,144	2.45%
00218456	Journal of Accounting Research	657	2,212	29.70%
00720127	The Galpin Society Journal	654	2,000	32.70%
0006341X	Biometrics	648	9,570	6.77%
15436322	College Art Journal	647	1,905	33.96%
00274321	Music Educators Journal	644	14,288	4.51%
00340553	Reading Research Quarterly	642	1,689	38.01%
19480938	Monatshefte für deutsche Sprache und Pädagogik	634	1,586	39.97%
15489000	The Journal of Land & Public Utility Economics	631	1,923	32.81%
00335533	The Quarterly Journal of Economics	623	6,361	9.79%
09501207	Proceedings of the Royal Society of London. Series A, Contai	619	3,855	16.06%
07499833	University of Pennsylvania Law Review and American Law Re	609	3,742	16.27%
00344338	Renaissance Quarterly	600	9,481	6.33%
00181560	Higher Education	592	3,441	17.20%
00018678	Advances in Applied Probability	589	3,137	18.78%
02666235	Journal of the Royal Geographical Society of London	583	1,371	42.52%
21503176	The Crayon	567	1,386	40.91%
0095182X	American Indian Quarterly	567	3,017	18.79%

RIF

00031615	The Americas	562	6,743	8.33%
00029327	American Journal of Mathematics	561	6,836	8.21%
00222879	Journal of Money, Credit and Banking	546	3,285	16.62%
00287199	Journal of the New York Entomological Society	543	5,111	10.62%
0043373X	Western Folklore	543	5,210	10.42%
03655695	Abstracts of the Papers Printed in the Philosophical Transacti	540	1,332	40.54%
00213020	Italica	539	5,939	9.08%
0018246X	The Historical Journal	531	3,648	14.56%
00218553	Journal of African Law	526	1,604	32.79%
00125962	The Drama Review: TDR	525	1,510	34.77%
00730548	Harvard Journal of Asiatic Studies	525	2,159	24.32%
15225437	Publications of the American Statistical Association	517	1,234	41.90%
0003486X	The Annals of Mathematics	514	5,946	8.64%
00220477	Journal of Ecology	510	8,256	6.18%
19356595	Bulletin of the Art Institute of Chicago (1907-1951)	504	3,787	13.31%
00130095	Economic Geography	503	4,965	10.13%
0028646X	New Phytologist	497	15,069	3.30%
03636941	The Journal of English and Germanic Philology	494	13,065	3.78%
01903187	International Family Planning Perspectives	482	1,843	26.15%
0034673X	Review of Religious Research	477	3,290	14.50%
15360407	Journal of the American Geographical Society of New York	476	1,017	46.80%
1478615X	Proceedings of the Royal Geographical Society of London	475	1,189	39.95%
00221465	Journal of Health and Social Behavior	462	2,004	23.05%
0016111X	The French Review	462	24,625	1.88%
19327080	Brush and Pencil	459	1,222	37.56%
09088857	Journal of Avian Biology	458	1,309	34.99%
20419953	Provincial Medical and Surgical Journal (1840-1842)	454	1,155	39.31%
00063185	Biological Bulletin	454	8,567	5.30%
15455858	The Elementary School Teacher	451	1,227	36.76%
2152243X	The Art Journal (1875-1887)	447	1,007	44.39%
00072745	The Bryologist	439	8,013	5.48%
1946195X	The American Art Journal (1866-1867)	436	1,002	43.51%
15583562	The American Law Register (1898-1907)	433	1,057	40.96%
00030031	American Midland Naturalist	431	8,792	4.90%
1047840X	Psychological Inquiry	429	1,335	32.13%
01630350	Latin American Music Review / Revista de Música Latinoame	423	758	55.80%

00764981	Proceedings of the Massachusetts Historical Society	418	1,986	21.05%
02664666	Econometric Theory	409	2,022	20.23%
14795973	Journal of the Society of Comparative Legislation	407	980	41.53%
01905937	The Old and New Testament Student	405	943	42.95%
10620516	The American Journal of Semitic Languages and Literatures	404	1,762	22.93%
09628436	Philosophical Transactions: Biological Sciences	402	4,484	8.97%
03063127	Social Studies of Science	400	1,920	20.83%
21505977	The Lotus Magazine	398	911	43.69%
09501193	Proceedings of the Royal Society of London. Series B, Contai	396	1,830	21.64%
00147354	Family Planning Perspectives	394	3,191	12.35%
00151386	Film Quarterly	394	4,952	7.96%
00290564	Nineteenth-Century Fiction	393	2,048	19.19%
01411926	British Educational Research Journal	386	2,251	17.15%
00308684	The Pacific Historical Review	382	10,559	3.62%
09349138	Amtliche Berichte aus den Königlichen Kunstsammlungen	381	949	40.15%
00268232	Modern Philology	380	7,626	4.98%
00192287	Journal of the Illinois State Historical Society (1908-1984)	379	5,210	7.27%
00324728	Population Studies	374	4,058	9.22%
1948092X	Pädagogische Monatshefte / Pedagogical Monthly	369	848	43.51%
03702316	Philosophical Transactions (1665-1678)	369	919	40.15%
00135984	The Elementary School Journal	367	9,434	3.89%
01905945	The Old Testament Student	361	931	38.78%
15405079	The American Journal of Archaeology and of the History of th	360	743	48.45%
00282480	Negro American Literature Forum	356	403	88.34%
00219398	The Journal of Business	353	3,599	9.81%
00223395	The Journal of Parasitology	352	17,193	2.05%
20420013	The Scottish Antiquary, or, Northern Notes and Queries	351	787	44.60%
15583538	The American Law Register and Review	350	813	43.05%
00220655	Journal of Educational Measurement	349	2,018	17.29%
10505164	The Annals of Applied Probability	339	1,391	24.37%
00247413	Luso-Brazilian Review	339	1,799	18.84%
00224642	The Journal of Southern History	337	14,654	2.30%
14315955	Jahrbuch der Königlich Preussischen Kunstsammlungen	334	809	41.29%
00182680	History of Education Quarterly	333	3,936	8.46%
00220027	The Journal of Conflict Resolution	331	2,587	12.79%
07417918	The Analyst	327	836	39.11%

00098388	The Classical Quarterly	327	5,131	6.37%
14738104	International Affairs (Royal Institute of International Affairs	326	3,829	8.51%
01937758	IRB: Ethics and Human Research	323	1,227	26.32%
00914169	The Journal of Criminal Law and Criminology (1973-)	322	2,288	14.07%
00243590	Limnology and Oceanography	319	9,527	3.35%
00030139	Journal of the American Musicological Society	315	3,016	10.44%
08990344	Museum of Fine Arts Bulletin	311	955	32.57%
21512752	The Art World	308	755	40.79%
03075133	The Journal of Egyptian Archaeology	304	4,399	6.91%
21531706	The Quarterly of the Oregon Historical Society	300	796	37.69%
00804401	Transactions of the Royal Historical Society	299	1,666	17.95%
1364503X	Philosophical Transactions: Mathematical, Physical and Engi	296	3,326	8.90%
15487237	Proceedings of the Academy of Political Science in the City o	292	1,010	28.91%
01452258	African Economic History	291	894	32.55%
00659746	Transactions of the American Philosophical Society	291	2,162	13.46%
00182710	History of Religions	290	1,941	14.94%
10520368	The Journal of Mycology	288	813	35.42%
01487825	The South Carolina Historical and Genealogical Magazine	286	1,682	17.00%
00182176	Hispanic Review	286	6,342	4.51%
05432499	Medical Anthropology Newsletter	284	883	32.16%
02581485	Notizblatt des Königl. botanischen Gartens und Museums zu	277	1,443	19.20%
00255718	Mathematics of Computation	277	7,813	3.55%
01612492	Callaloo	274	5,518	4.97%
0013189X	Educational Researcher	268	4,231	6.33%
00219231	Journal of Biblical Literature	264	10,073	2.62%
08913609	Bulletin of the Pennsylvania Museum	261	1,386	18.83%
00221724	The Journal of Hygiene	261	4,767	5.48%
00360341	Russian Review	257	9,237	2.78%
09588442	Proceedings of the Musical Association	254	698	36.39%
00228443	Transactions of the Kansas Academy of Science (1903-)	250	4,622	5.41%
21517576	The New York Latin Leaflet	249	550	45.27%
00043125	Art Education	248	5,381	4.61%
00088080	The Catholic Historical Review	247	16,870	1.46%
00218790	Journal of Animal Ecology	241	6,853	3.52%
16120124	Sammelbände der Internationalen Musikgesellschaft	240	550	43.64%
21505837	The Illustrated Magazine of Art	238	647	36.79%

01675249	Law and Philosophy	238	877	27.14%
00667374	Proceedings of the Aristotelian Society	238	1,956	12.17%
00098841	The Bulletin of the Cleveland Museum of Art	235	4,563	5.15%
03050068	Comparative Education	233	2,477	9.41%
19489323	Cosmopolitan Art Journal	231	534	43.26%
00224189	The Journal of Religion	229	13,265	1.73%
00387134	Speculum	229	18,055	1.27%
20419988	London Journal of Medicine	228	556	41.01%
21512760	Fine Arts Journal	227	578	39.27%
00237639	Land Economics	227	3,925	5.78%
00275514	Mycologia	222	11,393	1.95%
10635157	Systematic Biology	221	1,470	15.03%
10497544	American Slavic and East European Review	220	1,540	14.29%
19457863	The North-American Review and Miscellaneous Journal	219	480	45.63%
19480202	The Collector and Art Critic	219	644	34.01%
14795949	Journal of Comparative Legislation and International Law	218	2,441	8.93%
00754358	The Journal of Roman Studies	218	6,884	3.17%
00458511	Copeia	218	13,942	1.56%
08834237	Statistical Science	213	1,744	12.21%
00987921	Population and Development Review	211	4,332	4.87%
00220671	The Journal of Educational Research	211	9,800	2.15%
08979049	Records of the Columbia Historical Society, Washington, D.C	210	1,246	16.85%
00143820	Evolution	208	9,164	2.27%
00171298	Glotta	206	2,556	8.06%
10497498	Publications of the American Economic Association	205	579	35.41%
00436534	The Wisconsin Magazine of History	205	7,296	2.81%
10791760	Mershon International Studies Review	203	272	74.63%
19330545	Transactions of the Annual Meetings of the Kansas Academy	203	437	46.45%
10601805	Proceedings of the American Society of Microscopists	201	392	51.28%
00028320	Transactions of the American Entomological Society (1890-)	200	1,977	10.12%
03073114	The Journal of the Royal Anthropological Institute of Great B	199	1,431	13.91%
08831610	Bulletin of the American Association of University Professors	199	3,851	5.17%
00221082	The Journal of Finance	199	8,736	2.28%
00682454	The Annual of the British School at Athens	197	1,950	10.10%
00267902	The Modern Language Journal	196	18,754	1.05%
00129682	Econometrica	194	8,418	2.30%

0022362X	The Journal of Philosophy	192	15,224	1.26%
03650855	Abstracts of the Papers Communicated to the Royal Society ·	189	434	43.55%
00410020	The Town Planning Review	189	5,846	3.23%
00222801	The Journal of Modern History	187	14,237	1.31%
00274631	The Musical Quarterly	186	5,131	3.63%
00168831	The German Quarterly	186	10,301	1.81%
00224812	The Journal of Symbolic Logic	183	12,079	1.52%
00659711	Transactions and Proceedings of the American Philological As	182	1,626	11.19%
00401706	Technometrics	181	6,674	2.71%
10683380	The Journal of Race Development	180	445	40.45%
02643952	Philosophical Transactions of the Royal Society of London. Se	179	615	29.11%
15361489	(null)	178	387	45.99%
00804630	Proceedings of the Royal Society of London. Series A, Mathel	178	11,804	1.51%
0030364X	Operations Research	177	6,728	2.63%
10500960	The Micropaleontologist	176	301	58.47%
00218251	Journal for Research in Mathematics Education	176	1,858	9.47%
07319487	Learning Disability Quarterly	175	1,397	12.53%
00966134	Memoirs of the American Academy of Arts and Sciences	174	428	40.65%
00181498	The High School Journal	174	7,135	2.44%
00028444	American Fern Journal	173	4,369	3.96%
00346535	The Review of Economics and Statistics	171	6,887	2.48%
00389765	Stanford Law Review	170	4,109	4.14%
10553177	Novon	169	2,032	8.32%
00930334	The Hastings Center Report	169	5,017	3.37%
01976664	Family Relations	166	2,957	5.61%
00324701	Population Index	166	12,111	1.37%
01621459	Journal of the American Statistical Association	166	17,909	0.93%
00267961	The Modern Law Review	163	9,113	1.79%
01602810	Hebraica	162	468	34.62%
09213260	Tijdschrift der Vereeniging voor Noord-Nederlands Muziekge:	160	567	28.22%
00104159	Comparative Politics	159	1,516	10.49%
00182133	Hispania	157	17,439	0.90%
15592472	Music Supervisors' Journal	152	2,362	6.44%
14784017	Transactions and Papers (Institute of British Geographers)	150	311	48.23%
15455890	The Course of Study	150	330	45.45%
19483325	The Quarterly of the Texas State Historical Association	149	475	31.37%

03615413	History in Africa	149	903	16.50%
03617882	The International Journal of African Historical Studies	144	6,355	2.27%
00222992	The Journal of Negro History	141	4,679	3.01%
00208833	International Studies Quarterly	140	1,608	8.71%
00130117	The Economic History Review	139	11,923	1.17%
00161071	French Historical Studies	131	1,498	8.74%
00221546	The Journal of Higher Education	131	9,319	1.41%
17442524	The Folk-Lore Journal	130	377	34.48%
0038478X	The Southwestern Historical Quarterly	130	8,014	1.62%
00730688	Harvard Studies in Classical Philology	129	1,316	9.80%
13680382	Anthropological Review	127	324	39.20%
21518890	The American Art Review	127	332	38.25%
02763605	Black Music Research Journal	126	460	27.39%
00182168	The Hispanic American Historical Review	123	14,692	0.84%
13560131	Journal of the Anthropological Society of London	122	245	49.80%
00218901	Journal of Applied Ecology	122	5,652	2.16%
19480709	The Art Union	121	294	41.16%
03624056	International Family Planning Digest	120	137	87.59%
03076776	RAIN	120	1,070	11.21%
15455904	The Elementary School Teacher and Course of Study	117	203	57.64%
00432539	Die Welt des Islams	117	2,859	4.09%
00028312	American Educational Research Journal	114	2,321	4.91%
00905364	The Annals of Statistics	114	4,970	2.29%
00219002	Journal of Applied Probability	113	4,887	2.31%
02643960	Philosophical Transactions of the Royal Society of London. Si	112	432	25.93%
00239186	Law and Contemporary Problems	112	3,459	3.24%
15225445	Quarterly Publications of the American Statistical Associatior	111	204	54.41%
00266493	Annals of the Missouri Botanical Garden	110	3,337	3.30%
15350940	Slavonic and East European Review. American Series	108	118	91.53%
04353676	Geografiska Annaler. Series A, Physical Geography	106	1,450	7.31%
03770567	Journal of the Folk-Song Society	105	398	26.38%
00218529	The Journal of Aesthetics and Art Criticism	105	7,229	1.45%
08953309	The Journal of Economic Perspectives	103	1,627	6.33%
15360393	Journal of the American Geographical and Statistical Society	102	196	52.04%
21514879	The Artist: An Illustrated Monthly Record of Arts, Crafts and	100	304	32.89%
08862192	Anuario Interamericano de Investigacion Musical	97	122	79.51%

00393665	Studies in Family Planning	97	3,403	2.85%
01905953	The Hebrew Student	96	237	40.51%
02714442	Transactions of the American Philological Association (1869-	96	243	39.51%
15208605	Proceedings of the American Political Science Association	95	266	35.71%
00104086	Comparative Education Review	95	3,746	2.54%
08933243	Missouri Botanical Garden Annual Report	94	229	41.05%
00104175	Comparative Studies in Society and History	94	2,497	3.76%
08939454	The Review of Financial Studies	92	1,275	7.22%
00393738	Studies in Philology	92	3,347	2.75%
13680366	Transactions of the Ethnological Society of London	91	216	42.13%
01486179	Black American Literature Forum	91	962	9.46%
00274224	Music & Letters	90	14,371	0.63%
19481594	Annual Reports of the Dante Society	89	230	38.70%
00380407	Sociology of Education	89	1,484	6.00%
00208183	International Organization	89	4,154	2.14%
21511284	The Illustrated Wood Worker	88	189	46.56%
02643820	Philosophical Transactions of the Royal Society of London. A	87	176	49.43%
01906348	Minnesota History Bulletin	87	356	24.44%
00390526	Journal of the Royal Statistical Society. Series D (The Statist	85	3,606	2.36%
05644429	Anuario	83	83	100.00%
00222372	Journal of Mammalogy	83	11,892	0.70%
21514348	The Monthly Illustrator	79	151	52.32%
21526907	The Collector	77	244	31.56%
00397946	Syria	77	5,900	1.31%
07346018	Representations	74	905	8.18%
10698337	Journal of the Society of Biblical Literature and Exegesis	73	164	44.51%
01488937	The Journal of International Relations	73	198	36.87%
00220256	Journal of Cuneiform Studies	72	1,180	6.10%
00664162	Annual Review of Ecology and Systematics	69	757	9.11%
00219371	The Journal of British Studies	69	2,542	2.71%
17441994	The Folk-Lore Record	68	150	45.33%
08861145	Transactions of the American Entomological Society (1867-1	68	152	44.74%
03642968	The Journal of Germanic Philology	68	211	32.23%
00317217	The Phi Delta Kappan	68	17,637	0.39%
00207071	International Journal of American Linguistics	67	3,567	1.88%
21511276	The Connoisseur	66	156	42.31%

R I F

00305693	Ornis Scandinavica	66	1,068	6.18%
20420005	Northern Notes & Queries	65	131	49.62%
00045608	Annals of the Association of American Geographers	65	5,514	1.18%
19473850	The Junior High Clearing House (1920-1921)	61	126	48.41%
1945516X	Transactions of the American Entomological Society and Pro	61	145	42.07%
00059315	Berliner Museen	60	1,194	5.03%
00039292	Archiv für Musikwissenschaft	60	1,843	3.26%
19480717	Bradley, His Book	58	112	51.79%
15325059	American Economic Association Quarterly	58	123	47.15%
19494637	Mycological Bulletin	58	151	38.41%
01623737	Educational Evaluation and Policy Analysis	58	1,271	4.56%
10602682	Proceedings of the American Microscopical Society	57	99	57.58%
00440078	Yale French Studies	57	1,964	2.90%
02643839	Philosophical Transactions of the Royal Society of London. B	56	143	39.16%
02707993	Woman's Art Journal	56	1,387	4.04%
10711031	Journal of Farm Economics	56	7,680	0.73%
15554023	Educational Research Bulletin	55	5,076	1.08%
21511705	The Quarterly Illustrator	54	116	46.55%
13561898	Bulletin of the School of Oriental Studies, University of Lond	54	1,742	3.10%
15219488	International Studies Review	53	937	5.66%
00031224	American Sociological Review	53	13,905	0.38%
15350959	Slavonic Year-Book. American Series	51	54	94.44%
19330537	Transactions of the Kansas Academy of Science (1872-1880)	51	134	38.06%
16513215	Geografiska Annaler	51	1,053	4.84%
00361445	SIAM Review	51	6,946	0.73%
21502609	The New Path	50	126	39.68%
01956744	American Journal of Education	50	1,301	3.84%
00081973	The Cambridge Law Journal	50	7,856	0.64%
15264211	Trollopian	49	85	57.65%
15386341	Perspectives on Sexual and Reproductive Health	48	679	7.07%
03746313	Bulletin du Jardin botanique de l'État a Bruxelles	48	977	4.91%
00804606	Biographical Memoirs of Fellows of the Royal Society	48	1,396	3.44%
21511268	The Soil	46	122	37.70%
21505969	Art & Life	43	178	24.16%
19386753	The Ornithologists' and Oologists' Semi-Annual	42	92	45.65%
00346543	Review of Educational Research	42	3,692	1.14%

00682462	Papers of the British School at Rome	41	813	5.04%
01622749	International Family Planning Perspectives and Digest	40	57	70.18%
00351601	Revue de Musicologie	40	5,063	0.79%
15414132	Transactions of the Anthropological Society of Washington	39	78	50.00%
13680358	Journal of the Ethnological Society of London (1848-1856)	38	75	50.67%
15531031	Bulletin of the Cooper Ornithological Club	38	97	39.18%
21503184	The Art Review	38	108	35.19%
03061078	Early Music	38	5,340	0.71%
00154040	The Florida Entomologist	38	5,593	0.68%
09919228	Bulletin de la Société française de musicologie	37	145	25.52%
14717816	The Slavonic Review	37	621	5.96%
02625245	Music Analysis	37	688	5.38%
19304013	The Florida Buggist	36	82	43.90%
00352764	Revue économique	36	6,942	0.52%
14791234	Transactions of the Grotius Society	35	645	5.43%
00433810	The Western Historical Quarterly	35	6,284	0.56%
09504737	Transactions of the Royal Asiatic Society of Great Britain anc	34	131	25.95%
13680374	The Journal of the Ethnological Society of London (1869-187	33	100	33.00%
03421201	Mitteilungen des Kunsthistorischen Institutes in Florenz	33	1,182	2.79%
21528578	National Academy Notes including the Complete Catalogue o	32	95	33.68%
10942076	Near Eastern Archaeology	31	588	5.27%
00130427	Economica	31	8,603	0.36%
08981051	Zoological Bulletin	30	75	40.00%
15393682	Transactions and Proceedings of the Modern Language Assoc	29	61	47.54%
00912131	Ethos	29	1,136	2.55%
21526141	Transactions of the American Art-Union	28	56	50.00%
0934618X	Jahrbuch der Preuszischen Kunstsammlungen	28	194	14.43%
00219347	Journal of Black Studies	28	2,055	1.36%
00273716	The Murrelet	27	2,812	0.96%
14791226	Problems of the War	26	47	55.32%
08848971	Sociological Forum	26	1,270	2.05%
15381420	Living	25	113	22.12%
03050270	Journal of Biogeography	25	4,225	0.59%
10547193		24	40	60.00%
02708647	PSA: Proceedings of the Biennial Meeting of the Philosophy c	24	954	2.52%
15321282	Journal of Social Forces	23	772	2.98%

02716844	Midland Naturalist	22	31	70.97%
2150315X	The Art Critic	22	40	55.00%
10798986	The Bulletin of Symbolic Logic	22	911	2.41%
09345795	Amtliche Berichte aus den Preuszischen Kunstsammlungen	21	32	65.63%
15294560	Botanical Bulletin	20	49	40.82%
00043079	The Art Bulletin	20	6,390	0.31%
15719529	Bouwsteenen	19	39	48.72%
00157120	Foreign Affairs	19	16,484	0.12%
2152615X	Transactions of the Apollo Association for the Promotion of tl	17	29	58.62%
03606333	African Economic History Review	17	35	48.57%
15592464	Music Supervisors' Bulletin	17	38	44.74%
03616258	Publications of the Florida Historical Society	17	63	26.98%
14784009	Transactions (Institute of British Geographers)	16	17	94.12%
21503192	The Art News	16	32	50.00%
03627861	Annual Report (Fogg Art Museum)	15	228	6.58%
1466822X	Global Ecology and Biogeography	15	931	1.61%
13669516	Diversity and Distributions	15	987	1.52%
01605682	The Journal of the Operational Research Society	15	7,748	0.19%
Pamphlets	(null)	15	25,922	0.06%
02767732	Bulletin of the American School of Oriental Research in Jerus	14	20	70.00%
19400969	Supplementary Papers of the American School of Classical S	13	19	68.42%
07314086	Conflict Resolution	13	27	48.15%
09641998	Journal of the Royal Statistical Society. Series A (Statistics i	13	1,858	0.70%
1547626X	Criminal Science Monographs	12	21	57.14%
00472506	Journal of International Business Studies	12	2,359	0.51%
1938677X	The Semi-Annual (Agassiz Association. Department of the W	11	14	78.57%
19440995	National News Letter of Phi Delta Kappa	11	55	20.00%
00656801	Memoirs of the American Academy in Rome	11	364	3.02%
00393541	Studies in Art Education	11	1,905	0.58%
15393674	Transactions of the Modern Language Association of America	10	19	52.63%
03768899	The English Folk-Dance Society's Journal	10	20	50.00%
15393666	Modern Language Association of America. Proceedings	10	34	29.41%
1939053X	Notes (Fogg Art Museum)	10	66	15.15%
00202754	Transactions of the Institute of British Geographers	10	2,485	0.40%
19494629	Ohio Mycological Bulletin	9	14	64.29%
19386788	The Wilson Quarterly (1892)	9	27	33.33%

RIF

00129623	Bulletin of the Ecological Society of America	9	2,767	0.33%
19440383	Bulletin of the New England Art Union	8	12	66.67%
2151772X	American Art Illustrated	8	27	29.63%
21503168	The Knight Errant	8	49	16.33%
08852731	Journal of Criminal Law and Criminology (1931-1951)	8	4,204	0.19%
00301299	Oikos	8	8,155	0.10%
2152856X	Illustrated Art Notes upon the Annual Exhibition of the Natio	7	21	33.33%
00662348	L'Année épigraphique	7	1,498	0.47%
21528551	American Academy Notes	6	9	66.67%
13560123	Journal of Anthropology	6	48	12.50%
00113204	Current Anthropology	6	6,659	0.09%
19332505	The Annual of the American School of Oriental Research in J	5	17	29.41%
14737981	Journal of the British Institute of International Affairs	5	277	1.81%
15256979	The University Journal of Business	4	291	1.37%
03097013	Proceedings of the Aristotelian Society, Supplementary Volu	4	722	0.55%
00405841	Theory into Practice	4	2,859	0.14%
00071005	British Journal of Educational Studies	4	4,744	0.08%
1356014X	Transactions of the Anthropological Society of London	3	9	33.33%
19386796	The Journal of the Wilson Ornithological Chapter of the Agas	3	9	33.33%
13558145	Cell Stress & Chaperones	3	772	0.39%
01418211	European Journal of Education	3	1,523	0.20%
00019720	Africa: Journal of the International African Institute	3	7,476	0.04%
08950571	The Bulletin of the College Art Association	2	4	50.00%
02728192	The Bulletin of the College Art Association of America	2	42	4.76%

On September 24, 2010, Aaron Swartz registered a universities network as a guest using the pseudonym "Gary Host" and provided the throwaway e-mail address, ghost@mailinator.com. As part of the registration process, his computer identified the MAC address of its network interface as 00235a735ffb and its client name3 as "ghost laptop". On September 25, 2010, shortly after midnight, the "ghost laptop" was assigned IP address 18.55.6.215. Later that day, a journal storage server experienced an extraordinary volume of automated requests and downloads from its digitized journal collections to that IP address. The downloads continued into the evening, when the journal storage network blocked access to its network from 18.55.6.215.

The next morning, the journal storage server began to experience rapid and voluminous downloads from IP address (b)(6),(b)(7) Accesses from this address continued until the middle of the day, when the journal storage network blocked this IP address as well. That day, the journal storage network turned to blocking a much broader range of IP address, temporarily denying service to legitimate users at the university.

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

On September 27, 2010, the university deactivated the guest registration for the "ghost laptop" by barring the MAC address 00235a735ffb from being assigned a new IP address. On October 2, 2010, "Gary Host," again using a computer with the client name "ghost laptop," registered as a guest and obtained an IP address from the network. Swartz bypassed the affirmative bar which the university had placed to his usage of the network by spoofing the MAC Address of the "ghost laptop," changing the last byte of the MAC address from 00235a735ffb to 00235a735ffc (changing the final "b" to "c"). The "ghost laptop" was assigned IP address (b)(6),(b)(7)(C)

On October 8, 2010, Swartz using the same naming conventions as he had for "ghost laptop," obtained a guest registration simultaneously for a second computer on the network. "Grace Host" registered the computer client "ghost macbook," providing the email address ghost42@mailinator.com. The network assigned the "ghost macbook" IP address (b)(6),(b)(7)(C) locating the "ghost macbook's" network connection somewhere within Building 16.

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

During the months of November and December, 2010, over two million illegal downloads were made from the journal storage network to two IP addresses assigned to Building 16 at the university: (b)(6),(b)(7) and (b)(6),(b)(7) Of these downloads, approximately half were research articles, with the remainder being reviews, news, editorials, and miscellaneous things. This is

more than one hundred times the number of downloads by all the legitimate users combined during the same period.

Network logs reflect that the computer assigned IP address (b)(6),(b)(7)(C) had not registered as a guest on the computer network. An analysis on January 4, 2011, however, reflected that both IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) were assigned to a computer with the MAC address 004ce5a0c756. Using network tools available on this occasion, the computer was tracked back to a specialized network wiring closet in the basement of Building 16. An Acer laptop and a Samsung hard drive in an external enclosure were found in the wiring closet. Both had been concealed under a cardboard box. The laptop had been connected directly into the computer network and the Swartz had assigned to himself the IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

On January 4, 2011, the university contacted the New England Electronic Crime Task Force (NET) to request assistance with the investigation. USSS SA (b)(6),(b)(7)(C) Cambridge Detective (b)(6),(b)(7)(C) and Boston Detective (b)(6),(b)(7)(C) from the NET Task Force responded to the university. A video camera was placed in the wiring closet. Later that day, Aaron Swartz was videotaped entering the network wiring closet. While there, he replaced the hard drive in the external enclosure attached to the laptop.

On January 6, 2011, Swartz, who is neither a student nor an employee of the university, was recorded again entering the specialized network wiring closet in the basement of Building 16 and removing the laptop and external hard drive enclosure. Later that same day the same laptop, identified by its MAC address 004ce5a0c756, was plugged into a network jack in Building W20. There, it was once again registered through the university's guest services. When it was, the computer identified itself as "ghost laptop," the same identification provided during the illegal downloads in September and October. The Acer laptop and a different Western Digital hard drive in an external enclosure were located and recovered, without the hard drive that was originally observed in the external hard drive enclosure.

A police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near the university, approximately half an hour after the "ghost laptop" had been connected in Building W20. Aaron Swartz was arrested by SA (b)(6),(b)(7)(C) and local police for breaking and entering. The backpack in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet. In the backpack was a HP USB drive.

On February 24, 2011, the Court issued warrants to search the Acer Laptop, Western Digital Hard Drive and the HP USB Drive. The MAC address assigned by the manufacturer to the ethernet interface card on the seized Acer laptop is 00:23:5a:73:5f:fb, the same as the "ghost laptop" which connected to the network in September, 2010. On the Acer Laptop was a software application "keepgrabbing.py" designed to download .pdf files. The application would download the .pdf files to a directory named "pdfs". The USB Drive found in Swartz's backpack contained a file "keepgrabbing2.py", with a script very similar to that contained in the Acer laptop. The Western Digital Hard Drive, which was recovered with the Acer laptop, had Aaron Swartz's fingerprint on it. The drive contained a folder named "pdfs" which contained an estimated over

97,000 .pdf files. A spot check of approximately a dozen of those files reflected that each was a digitized journal article from the journal storage service. A logging file on the Acer Laptop, known as the .bash_history file, showed an attempt to submit a computer or user name "Grace Host" and e-mail address ghost42@mailinator.com to the registration form at 10.72.0.47:444/bin/dynreg. This network address was associated with guest registration on the network before the laptop's seizure in January, 2011.

On July 19, 2011, Swartz was arrested by SA (b)(6),(b)(7)(C) of the Boston Field Office and Detective (b)(6),(b)(7)(C) of the Cambridge Police Department on the authority of an Arrest Warrant issued on July 14, 2011 by the United States District Court for the District of Massachusetts. Swartz was booked at the John Joseph Moakley United States Courthouse at One Courthouse Way, Boston Massachusetts.

Hard drive in external 97k

332 3,421,292

326 2,726,544

329 1,739,461

331 1,005,388

~~9,999,685~~

8,989,685

RIF

UNITED STATES GOVERNMENT

Memorandum of interview

DATE AND TIME: September 18th, 2012

U.S. Secret Service

LOCATION: 77 Massachusetts Avenue, Cambridge, MA

Case # 102-775-60071-S

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE:
SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 18th, 2012, (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) tated that (b)(6),(b)(7)(C) called him and told him that he found a computer in the building 16 telecom room. (b)(6),(b) recalled that there was a cable from the switch to a cardboard box. (b)(6), said that when he lifted up the box he could see a computer under the box. (b)(6),(b)(7)(C) stated that the computer had power connected and an external drive enclosure connected.

(b)(6),(b)(7)(C) recalled that after he arrived at the telecom room in the basement of building 16 (b)(6),(b)(7)(C) (b)(6),(b)(7) and (b)(6),(b)(7)(C) rived. (b)(6), recalled that (b)(6),(b)(7)(C) setup the packet capture. (b)(6),(b)(7)(C) said he did not receive any instructions from law enforcement to set up the packet capture. recalled that (b)(6),(b)(7) arrived and installed the camera in the telecom room in the basement of building 16.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Thursday, October 11, 2012 3:38 PM
To: (b)(6),(b)(7)(C)
Subject: (b)(6),(b)(7)(C) MOI
Attachments: (b)(6),(b)(7)(C) MOI 9-18-12.docx

On September 18th, 2012, (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann; AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) stated that (b)(6),(b)(7)(C) called him and told him that he found a computer in the building 16 telecom room. (b)(6), recalled that there was a cable from the switch to a cardboard box. (b)(6), said that when he lifted up the box he could see a computer under the box. (b)(6),(b)(7)(C) stated that the computer had power connected and an external drive enclosure connected.

(b)(6),(b)(7)(C) recalled that after he arrived at the telecom room in the basement of building 16 (b)(6),(b)(7)(C) (b)(6),(b)(7)(and (b)(6),(b)(7) arrived. (b)(6), recalled that (b)(6),(b)(7)(C) setup the packet capture. (b)(6), said he did not receive any instructions from law enforcement to set up the packet capture. (b)(6), recalled that (b)(6),(b)(7)(C) arrived and installed the camera in the telecom room in the basement of building 16.

(b)(6),(b)(7)(C)
USSS Boston
(b)(6),(b)(7)(C)

UNITED STATES GOVERNMENT

Memorandum of interview

U.S. Secret Service

Case # 102-775-60071-S

DATE AND TIME: September 18th, 2012

LOCATION: 77 Massachusetts Avenue, Cambridge, MA

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE:
SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 18th, 2012 (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) recalled that he received an incident notice from the library notifying him of robotic downloads. (b)(6),(b)(7) stated that (b)(6),(b)(7)(C) from the library will notify the IT security team if there is an incident. (b)(6),(b)(7) stated that (b)(6),(b)(7) was not able to determine who the downloader was so she asked IT security for help. (b)(6),(b)(7)(stated that they had trouble determining who the downloaded was (b)(6),(b)(7) stated that when they realized that the downloaded was changing his MAC address it was a sophisticated attack.

(b)(6),(b)(7)(C) recalled that (b)(6),(b)(7)(C) told him that (b)(6),(b)(7)(C) discovered a computer in the basement connected to the network. (b)(6),(b)(7) stated that when he arrived in the basement the telecommunications closet was opened. (b)(6),(b)(7)(said that he felt that at the time it was obvious to him that someone had broken into the closet and connected a computer. (b)(6),(b)(7) also stated that it was obvious to him that the computer connected to the switch was responsible for the downloading from JSTOR.

UNITED STATES GOVERNMENT

Memorandum of interview

U.S. Secret Service

Case # 102-775-60071-S

DATE AND TIME: September 18th, 2012

LOCATION: 77 Massachusetts Avenue, Cambridge, MA

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE:
SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 18th, 2012, (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) recalled that (b)(6),(b)(7)(C) called him to install a camera on 01/04/11. (b)(6),(b) stated that he installed a camera at eye level at the back wall of the telecom room in the basement of building 16. (b)(6), stated that the camera was connected to the Cisco video management service, the same as the other video surveillance cameras he had set up. (b)(6), stated that no one was assigned to monitor the video feed. (b)(6), stated that the cameras were motion activated. (b)(6), stated that the MIT police had access to the video monitoring system. (b)(6), stated that no alert was set up to notify anyone if motion was detected in the telecom closet in the basement of building 16. (b)(6), did not consider the camera he installed in the telecom room to be hidden.

(b)(6), (b)(7) recalled that he went back to his office and when he checked the footage he saw Swartz in the telecom room. (b)(6), said that he then called (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Friday, November 09, 2012 5:47 PM
To: 'Heymann, Stephen (USAMA)'; (b)(6),(b)(7)(C) (USAMA)
Subject: Draft MOI
Attachments: (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-18-12.docx; (b)(6),(b)(7)(C) MOI 9-13-12.docx; (b)(6),(b)(7)(C) MOI 9-13-12.docx; (b)(6),(b)(7)(C) MOI 9-13-12.docx

Please review the attached Draft MOI.

(b)(6),(b)(7)(C)

USSS Boston

(b)(6),(b)(7)(C)

UNITED STATES GOVERNMENT

Memorandum of interview

DATE AND TIME: September 13th, 2012

U.S. Secret Service

LOCATION: 301 East Liberty Street, Ann Arbor, MI

Case # 102-775-60071-S

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE: SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 13th, 2012, (b)(6),(b)(7)(C) was interviewed at the JSTOR office at 301 East Liberty Street, Ann Arbor, MI, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) stated that he was the (b)(6),(b)(7)(C) and he was involved with data evaluation and the analysis of user data. (b)(6),(b)(7)(C) stated that he was able to analyze the activity between JSTOR and Swartz and determine that Swartz used a script rather than a web browser to download PDFs from JSTOR.

(b)(6),(b)(7)(C) stated that the average PDF request is between 300 to 500. (b)(6),(b)(7)(C) stated that on 11/8/10 there were 50,000 PDF requests, on 12/11/10 there were 150,000 PDF requests on 12/13/10 there were 2000,000 PDF requests and on 12/27/10 there were 150,000 PDF requests.

(b)(6),(b)(7)(C) stated that prior to the end of 2010 JSTOR ability to track trends were only detailed enough to observe overall activity and JSTOR could not go back to observe the activity of individual IP addresses until the end of 2010.

(b)(6),(b)(7)(C) stated that it is reasonable to assume that the spikes in download activity would cause degradation in performance.

(b)(6),(b)(7)(C) also stated that his data shows downloads on 01/06/11 from and IP address that is associated with building W20 or the Stratton Student Center on the MIT campus.

UNITED STATES GOVERNMENT

Memorandum of interview

DATE AND TIME: September 18th, 2012

U.S. Secret Service

LOCATION: 77 Massachusetts Avenue, Cambridge, MA

Case # 102-775-60071-S

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE: SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 18th, 2012, (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of her statements:

(b)(6),(b)(7)(C) told us that previous incidents she remembered involved several thousand downloads and she could not remember any other incident that involved millions of downloads. (b)(6),(b)(7)(C) told us that JSTOR is very heavily used by MIT. (b)(6),(b)(7)(C) told us that October is an intense time of use of JSTOR at MIT.

UNITED STATES GOVERNMENT

Memorandum of interview

U.S. Secret Service

Case # 102-775-60071-S

DATE AND TIME: September 18th, 2012

LOCATION: 77 Massachusetts Avenue, Cambridge, MA

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE: SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 18th, 2012, (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) told us he remembered (b)(6),(b)(7)(C) from IS and T called him and told him about an incident with a computer that was found connected to the network. (b)(6),(b)(7)(C) told us that he then called Detective (b)(6),(b)(7)(C) told us that remembered that when he got on scene at the telecommunications closet in the basement of building 16 (b)(6),(b)(7)(C) was already there.

(b)(6),(b)(7)(C) told us that he had access to view the video feed from the camera that was set up in the telecommunications closet in the basement of building 16.

UNITED STATES GOVERNMENT

Memorandum of interview

U.S. Secret Service

Case # 102-775-60071-S

DATE AND TIME: September 18th, 2012

LOCATION: 77 Massachusetts Avenue, Cambridge, MA

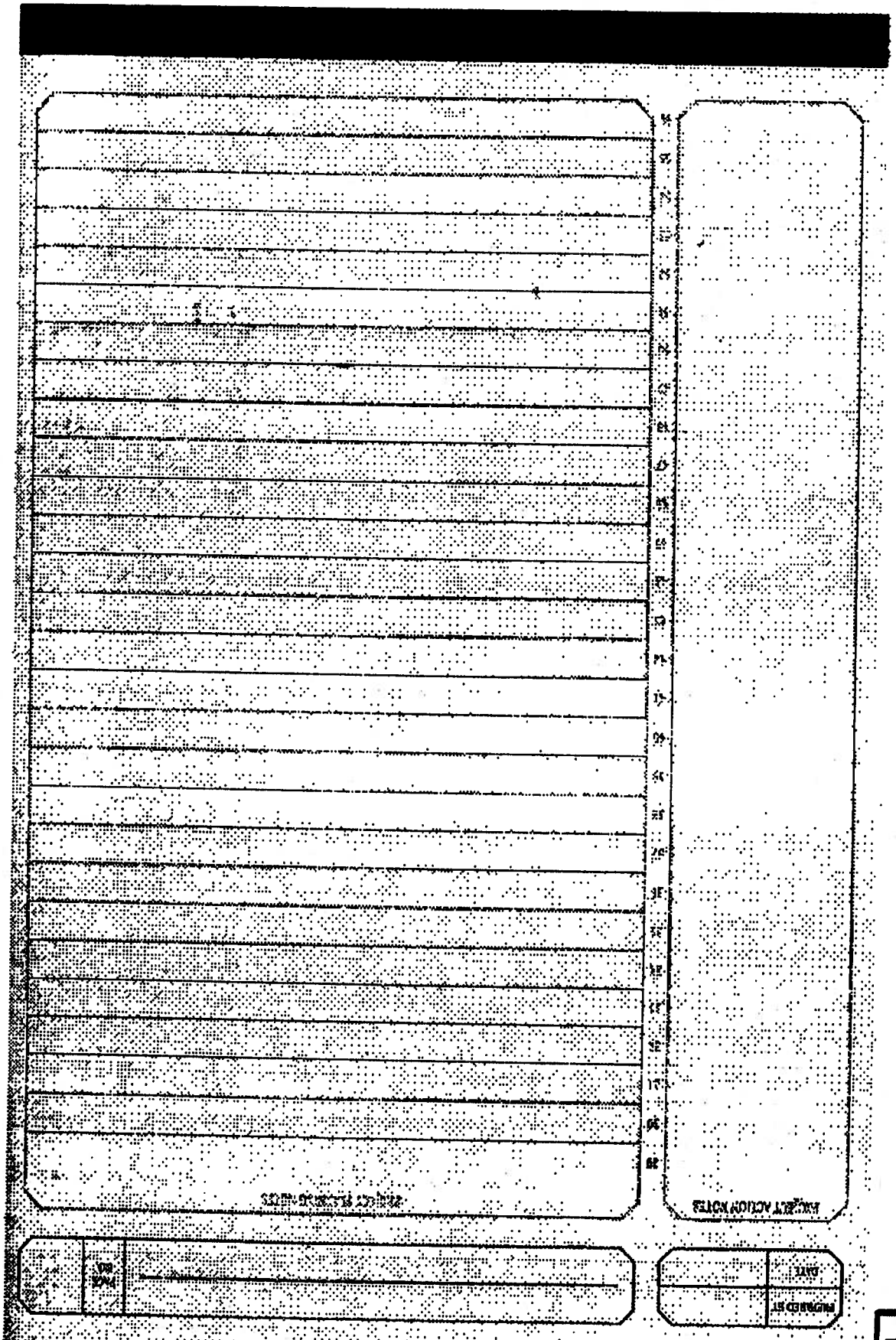
SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE: SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

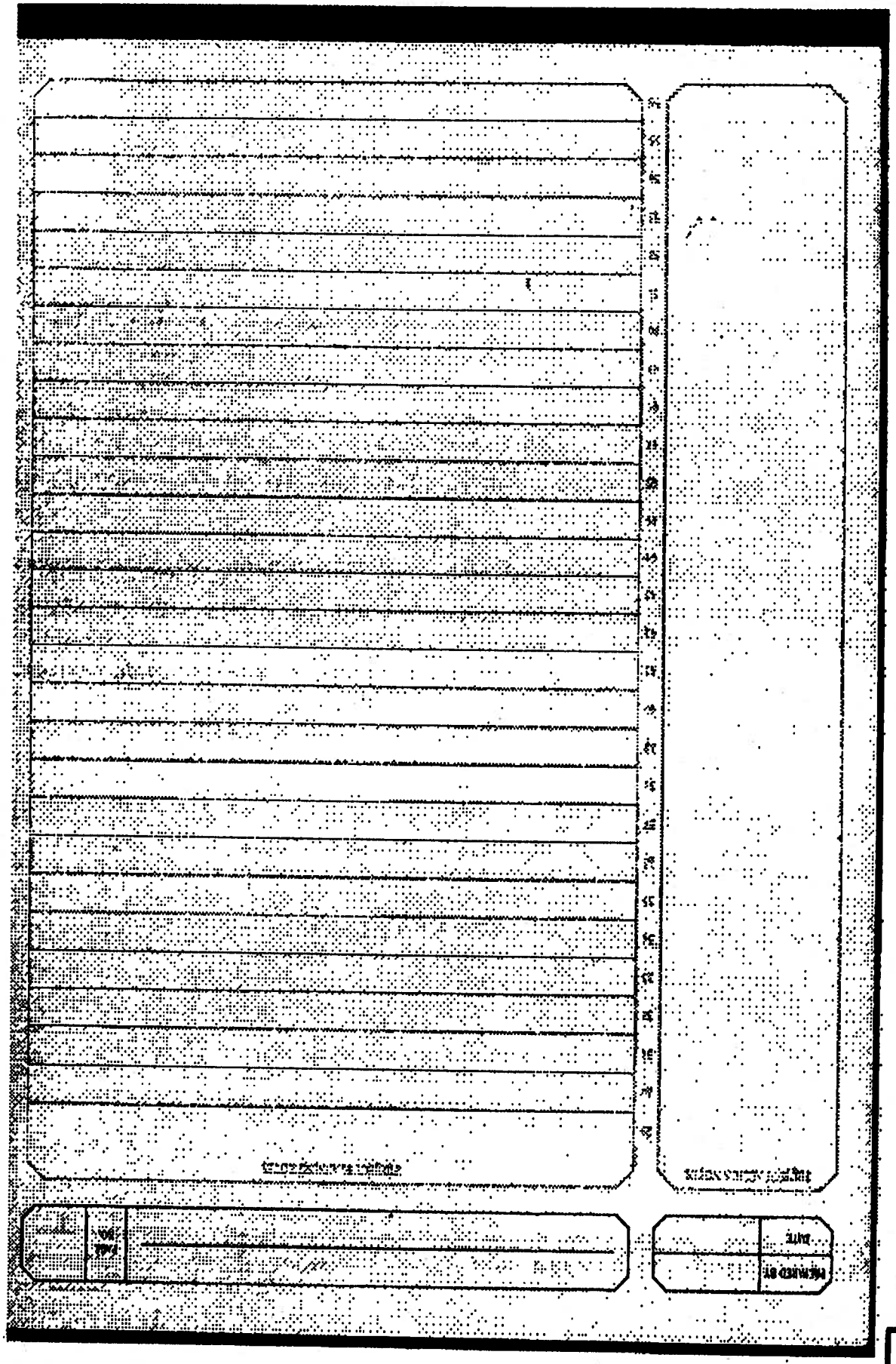
On September 18th, 2012, (b)(6),(b)(7)(C) was interviewed at the MIT General Counsels Office at 77 Massachusetts Avenue in Cambridge, Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) The following is a summary of his statements:

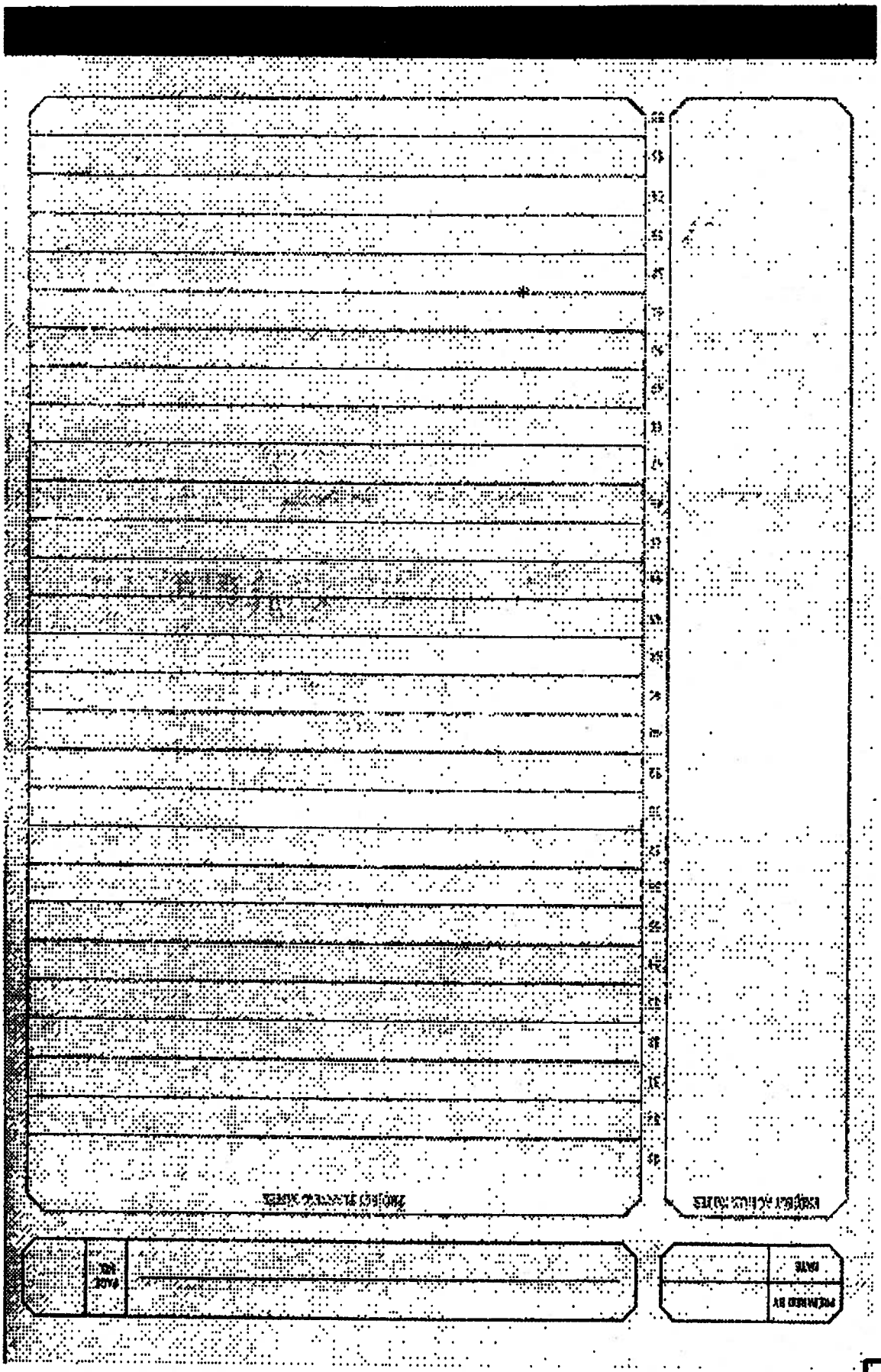
(b)(6),(b)(7)(C) told us that he remembered (b)(6),(b)(7)(C) telling him that (b)(6),(b)(7)(C) wanted them to go to the telecommunications closet in the basement of building 16 to investigate a network issue. (b)(6),(b)(7)(C) told us that when he arrived that the telecommunications closet that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) were already there (b)(6),(b)(7)(C) told us that he remembered the computer being hooked up the switch.

(b)(6),(b)(7)(C) told us that when the computer after the computer was removed from building 16 the MAC address was traced to building W20 (b)(6),(b)(7)(C) told us that he went to telecommunications room of building W20 to trace where the computer was (b)(6),(b)(7)(C) told us that the computer was found under a desk.

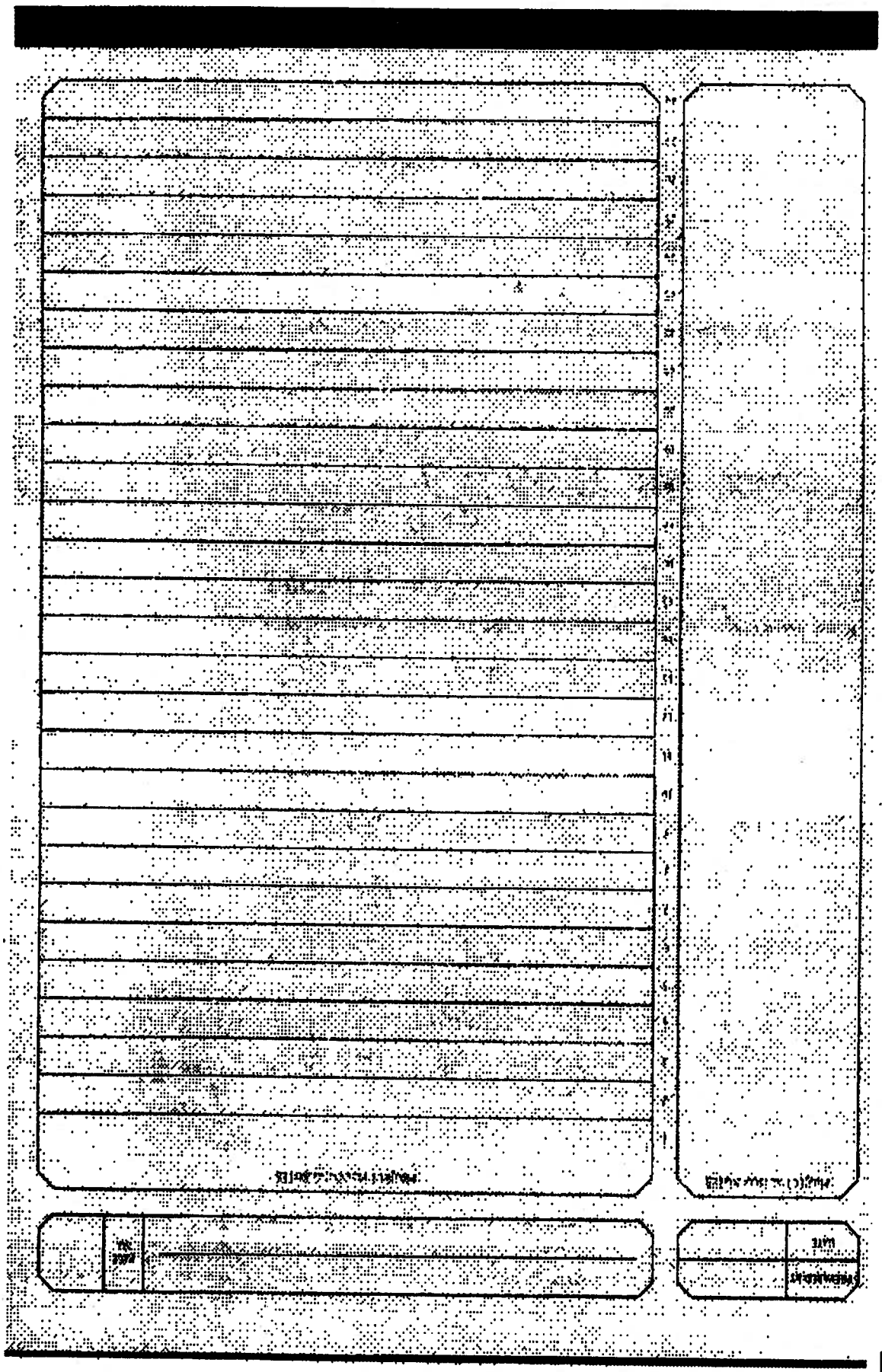


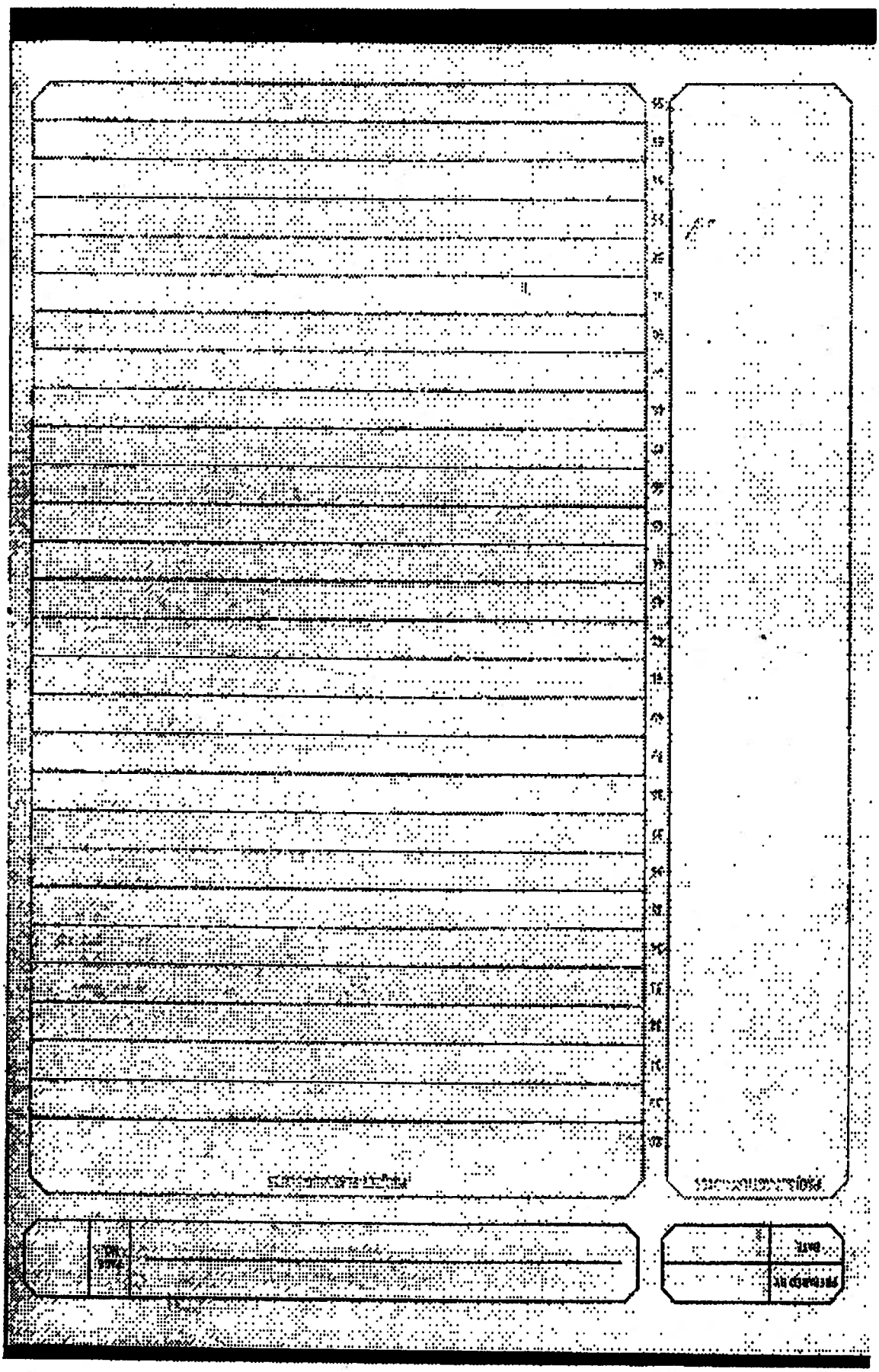
RIF



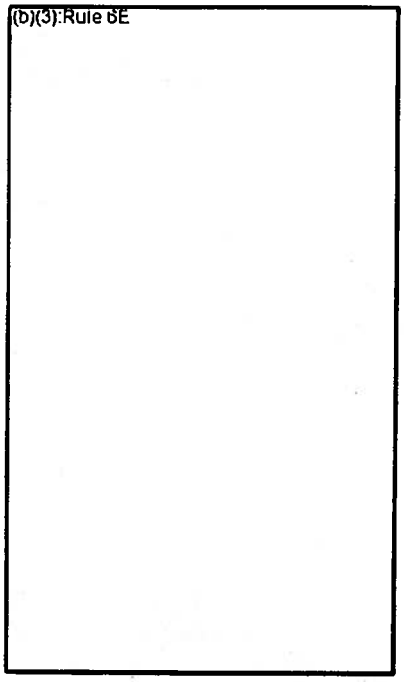


RIF





RIF


(b)(3):Rule 6E

1/4/2012

(b)(6),(b)(7)(C)

CERT Forensics Team

Process for creating image of Samsung332 disk for discovery in JSTOR-Swartz case

1) A forensically acquired image of the original disk was validated using its associated MD5 and SHA1 checksums to ensure that it remained a complete and true copy of the original drive.

(b)(7)(E)

2) The image was cloned to create a single "dd-format" file that represented a bit-for-bit duplicate of the contents of the original drive. The accuracy and integrity of this copy was also validated by calculating its cryptographic checksums.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Note: Although the metadata of the original disk image was demonstrated to be preserved, the disk image would differ in the following ways:

(b)(7)(E)

Linode
329 East Jimmie Leeds Road
Suite A
Galloway, NJ 08205
(615) 250-4945

Dear Custodian of Records:

Our agency is conducting an ongoing criminal investigation that involves one or more account holders. As part of that investigation, we are requesting that information related to www.aaronsw.com be preserved pending the issuance of formal legal process. More specifically, we are requesting that you preserve all subscriber information and/or account contents or group information related to the customer or subscribers. Additionally we are asking that all private messages, correspondence and bulletin board postings from above named users be preserved. We are also asking that all web content be preserved .

At this time we are expecting to obtain formal legal process in the next 90 days. We acknowledge that if we do not serve legal process upon you in the next 90 days, and do not request a 90 day extension, the preserved information may no longer be available.

Point of contact for this request is SA (b)(6), (b)(7)(C) at (617) 565-5640 or (b)(6),(b)(7)(C)

Respectfully

(b)(6),(b)(7)(C)

Special Agent
United States Secret Service
10 Causeway Street.
Suite 447
Boston, MA. 02222

On 01/14/11 SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) Captain (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) counsel for MIT met at the MIT office of General Counsel with (b)(6),(b)(7)(C) for scholarly publishing and licensing (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) stated that since 1997 MIT had bought many collections from JSTOR. Buying a collection from JSTOR costs a onetime archive capitol fee and subscription maintenance fee.

(b)(6),(b)(7)(C) estimated that MIT has spent at least $435,000.00 including a $50,000.00 a year maintenance fee.

(b)(6),(b)(7)(C) stated MIT's relationship with JSTOR was a partnership model and fees were based on the number of PhD programs the college had.

(b)(6),(b)(7)(C) stated that MIT had purchased 8 collections from JSTOR so far.

(b)(6),(b)(7)(C) stated that there is now a gateway for MIT to access electronic resources to JSTOR but that MIT access to JSTOR used to be based on an IP filter. (b)(6),(b)(7)(C) stated that for an MIT student to access JSTOR from off campus they always had to go through a gateway.

(b)(6),(b)(7)(C) stated that prior to the establishment of the gateway due to Swartz's abuse, a student on the MIT network could gain direct access to JSTOR (b)(6),(b)(7)(C) stated that as far as she was aware, only MIT used to have a system where anyone on the network could access JSTOR.

(b)(6),(b)(7)(C) stated that the only other occurrence of JSTOR reporting abuse to her was early in their relationship back in 1997 or 1998.

(b)(6),(b)(7)(C) stated that when JSTOR first reported abuse from the MIT network in 2010 they initially blocked access by the entire MIT network but with each subsequent incident JSTOR refined the IP addresses blocked. On the third incident JSTOR blocked the class C subnet the abuse came from.

(b)(6),(b)(7)(C) stated that her primary point of contact with JSTOR was (b)(6),(b)(7)(C).

(b)(6),(b)(7)(C) stated that MIT was on the JSTOR participants list that is listed on the JSTOR public website.

(b)(6),(b)(7)(C) stated that she believed students from Harvard need a PIN to access JSTOR.

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) Captain (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) counsel for MIT met at the MIT office of General Counsel with (b)(6),(b)(7)(C) analyst for MIT Information Service and Technology (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) informed the group that an examination of the DHCP logs during the time in September when JSTOR was reporting the excessive downloads show a computer registered as "ghost-laptop" with a MAC address of 00:23:5a:73:sf:fb and an email address of ghost@mailinator.com.

Detective (b)(6),(b)(7)(C) noted that all of the suspicious computer registrations on 09/24/10, 10/01/10, 10/08/10 and 12/24/10 occurred on Friday nights. Captain (b)(6),(b)(7)(C) confirmed that foot traffic in the tunnel of building 16 would be light during those times.

(b)(6),(b)(7)(C) stated that on 10/01/10 the an attempt was made to register with the same MAC address as used on 09/24/10; However, (b)(6),(b) had blocked that MAC address from registering. (b)(6),(b)(7 stated that on 10/02/10 another attempt was made to register on the network with a MAC address of 00:23:5a:73:sf:fc but still for "ghost-laptop."

(b)(6),(b)(7)(C) also stated that at one point on 10/09/11, "ghost-laptop" was registered with a MAC address of 00:23:5a:73:5f:fc and "ghost-macbook" was registered with a MAC address of 00:17:f2:2c:b0:74 at the same time.

(b)(6),(b)(7)(C) also stated that after 12/19/11, the attempts to register on the MIT network for "ghost-laptop" and "ghost-macbook" changed from attempts to gain an IP address dynamically assigned through the MIT guest registration process to assigning themselves static IP addresses on the MIT network. This behavior continued until after Swartz was observed on 01/06/11 moving the laptop from Building 16 to and the machine was registered on the network from the Stratton Student Center.

(b)(6),(b)(7)(C) also stated that on 01/06/11 at approximately 1251 the computer connected to an IP address registered to Amazon's Elastic Compute Cloud (EC2) service.

(b)(6),(b)(7)(C) noted that5 up to 12/19/10, Swartz obtained IP addresses by using the guest registration to be assigned an IP address through DHCP. From 12/19/10 to 01/06/11, Swartz would assign himself a static IP address. (b)(6),(b)(7)(C) theorized that once Swartz understood the subnet mask of the network Building 16 was on it would have been easy to assign himself an IP address that was not being used; However when he moved the laptop to the Stratton Student Center on 01/06/11, he connected to a new switch and went back to obtaining an IP address through DHCP.

Prior to this incident, JSTOR granted access to anyone using a IP address from the MIT network. MIT has a class A network and owns all of the IP addresses beginning with 18.

(b)(6),(b)(7)(C) recalled that on 01/03/11 (b)(6),(b)(7)(C) sent him an email telling him that JSTOR informed her that they had detected abuse from IP address 18.55.06.240. On 01/04/11, (b)(6),(b) traced the IP address (b)(6),(b)(7)(C) in the ARP table to MAC address 004c.e5a0.c756. MAC address 004c.e5a0.c756 was also assigned IP address (b)(6),(b)(7)(C) on the ARP table. (b)(6),(b)(stated that IP address (b)(6),(b)(7)(C) was logged with zero seconds talking on the network. (b)(6),(b)(7)(C) theorized that Swartz established IP address to (b)(6),(b)(7)(C)

communicate with the computer incase the MIT network shut down IP address (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) stated that IP address (b)(6),(b)(7)(C) was an IP address registered to JSTOR that appeared in the logs.

(b)(6),(b)(7)(C) stated that early in the morning of 01/04/11 he noticed in the ARP table that the IP address reported for abuse by JSTOR was active on the switch Gi 8/16 that he knew was in Building 16. The switch is also listed in the logs M16-004t-sw-entry.mit.edu. 004T refers to the room number 4T, the wire closet where the Acer Aspire one netbook with serial number LUSAX0D001001100R1601 was found. (b)(6),(b)(7)(recalled that at approximately 0200 he sent an email to (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) with the switch the computer committing the abuse was attached to and asked them to find it.

(b)(6),(b)(7)(C) confirmed that the closet was generally kept locked.

(b)(6),(b)(7)(C) stated that at first Swartz used guest registration to obtain an IP address but that static IP address were used later. (b)(6),(b)(7)(confirmed that someone with guest registration has full access in and out of the network.

(b)(6),(b)(7)(C) stated that MIT border routers do block the Microsoft ports.

(b)(6),(b)(7)(C) stated all three registrations Swartz used were variation of ghost with the computer name either being ghost-macbook or ghost-laptop and the name used for guest registration being either Gene, Gary or Grace.

(b)(6),(b)(7)(C) stated that based on the logs he reviewed that Swartz must have spoofed his MAC address at least once. The MAC address used in January (001c.e5a0.c756) had an invalid Organizationally Unique Identifier (OUI).

(b)(6),(b)(7)(C) stated that the emails Swartz used for guest registration used a service called mailinator. Mailinator is a service that gives spoofed emails the appearance of legitimate emails.

The packet capture from 01/04/11 identified two open ports on the Acer Aspire one found in 04T. The ports that were open were 22 and 8092. (b)(6),(b)(7)(C) identified that the service CherryPy was running. CherryPy is a web application framework using the python programming language.

(b)(6),(b)(7)(C) estimated that as of 1/14/11, MIT had spent 160 man-hours investigating the abuse by Swartz.

Items to be Returned:
Metallic Blue iPod
White iPod with white carrying case
White iPod with Serial Number 8A6330856UX8A
White iTalk
Black 16GB thumb-drive
Pocket notebook with blue and white hexagon and rectangle design cover
Pure Drive model 761 external hard drive quick start guide with CD
Disc utility internal hard drive upgrade kit
Seagate SATA 3.5" Barracuda internal hard drive installation guide
Scientific Atlantic modem
Black notebook journal
Wireless-G 2.4 GHz broadband router linksys with serial number CDFG1G609626
Miscellaneous compact disks
Earning statement addressed to Aaron Swartz
Master's Thesis M-876 Lind, William Edmund, Thomas McDonald: "A study of an Engineer Administrator & his Influence of Public Roads in the US 1919-1953"

Items to be viewed and handled:
Twelve (12) magnetic media tapes in a FedEx box
Apple multi adapter with serial number 6F9395M7ZU6
Apple multi adapter with serial number 6F7281NNU4S
MacBook install disk one and two in paper sleeve
MacBook user guide in cardboard case
Apple care service letter
Genius Bar work confirmation
Two hard drive enclosures
Harvard University earning statement

Items to be viewed but not handled:
Nokia cell phone with power cord
T-Mobile HTC G2 cell phone with power cord
"Office Depot" DVD-R with handwritten label "Bibliographic data which mysteriously appeared one day as the sun was shining"
CD with hacking tools on it
T-Mobile sidekick
Sony Micro Vault

1/4/11 MIT Intrusion

[redacted] (b)(6),(b)(7)(C)

Building 16
Biology library

1/13/11 10 AM note from [illegible]
notified 900GB of PDF
download
JSTOR ~~MIT~~ Bio Research Journ[illegible]

activity started 12/26/10

(b)(6),(b)(7)(C) [redacted]

September [redacted] (b)(6),(b)(7)(C) share ... JSTOR

(b)(6),(b)(7)(C) [redacted]

~~take Sep~~ noticed large amount
of downloads

Arrives on [illegible] [illegible]

659

(b)(6),(b)(7)(C)

12/27/81

(b)(6),(b)(7)(C)

WIT° 920 779214

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

927839801

During Booking ask to call to woman home (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

099

Call (b)(6),(b)(7)(C) for (b)(6),(b)(7)(C) #

Call (b)(6),(b)(7)(C) @ USTBR

To preserve all Records

Check (b)(6),(b)(7)(C)
if Posted

Prepare Subpoena Request

Read Blog
Look for name (b)(6),(b)(7)(C)

2 All logs of downloads to
WIT Calling 2 day before
+ 2 days after excessive
download likes

What was downloaded
times dates of downloads

Also get WIT Records
for downloads

Copy of Stolen theft report
to AUSA

Get Report on Track on laptop
Booking Room Video/Audio/phone call

who is ADA assigned
when is next appearance

who has he worked w/ in
the Open Library

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Aaron Swartz
Harvard University
(b)(6),(b)(7)(C)

Zipcode
(609) 593-7103
329 East Jimmie Leeds Rd
Suite A
Galloway NJ 08205
PAX (615) 250 4/9/45

199

Conference 1/14/11 ≈ 1100
MIT Office of General Counsel
(b)(6),(b)(7)(C) Det (b)(6),(b)(7)(C) MIT Pol.
(b)(6),(b)(7)(C) MIT PD
Counsel MIT
Det Cambridge
AUSA Heymann

conference call w/ JSTOR
JSTOR stated it looked to them
that multiple computers were
conducting download
computer would open browser
download document → close browser

MIT network class A
JSTOR access authorized through
IP span

(b)(6),(b)(7)(C) —
Says MIT has stop it
Harassment & abuse area to
report abuse
(b)(6),(b)(7)(C) reports abuse
of JSTOR Acess excessive download

logs show: DHCP logs show
~~OCT~~ SEP
~~Sep~~ Incident Brief
Valid OUI for use of
Ethernet Card of MAC Book

OCT Sep [redacted] (b)(6),(b)(7)(C) reviews logs
but does not save

OCT DHCP log shows ghost-macbook
MAC 00:17:f2:2c:b0:74
valid MAC for Macbook

Visitor Registration valid for 2 weeks

in Sep [redacted] (b)(6),(b)(7)(C) looked at MAC
address checked Host
when was registered as
Gary Host Ghost-laptop
ghost@mailinator

[redacted] (b)(6),(b)(7)(C) reports MIT shut down
by JSTOR for excessive downloads

when tracked to building 16

662

in September guest Registration disabled

no Sep logs preserved

OCT 8 ≈ 2200 = Friday

ghost-Macbook DHCP client ID
Host name
ghost-Macbook only in OCT
different MAC address

Sep MAC 00:23:5a:73:5f:fb ⇐
ghost-laptop not valid OUI

occurrence all Friday nights
Sep 24 OCT ~~2~~ 1 + 8 DEC 24
SEP 24 OCT 1 OCT 8 DEC 24

OCT 1 machine attempts to register ⇐
old MAC blocked
OCT 2 ~ 10:20 changes MAC
from 00:23:5a:73:5f:fb
to 00:23:5a:73:5f:fc
still ghost-laptop

OCT 1 - ~~oct~~ Thursday OCT 1
~~12:55 - 7:48~~

Oct 09 (b)(6),(b)(7)(C) , thanks
Blocks JSTOR access

Oct 8 ≈ 22:18 out of Guest
Registration

00:17:f2:2c:50:74 valid OUT
ghost-macbook

Oct 9 Two machines registration
ghost-macbook + ghost-laptop

00:23:5a:73:5f:fc = ghost-laptop
00:17:f2:2c:50:74 = ghost-macbook

JSTOR shut down access oct 9

Swartz Counsel (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) good cormier.com

! why not ~~the~~ wifi
plugging into switch gives better
bandwidth + faster download

DEC 19 ~~no longer requesting~~
~~Guest access~~

DEC 19 no longer assigned IP
through DHCP
~~a~~ uses static IP
self assigned static IP

(b)(6),(b)(7)(C) = China

(b)(6),(b)(7)(C) connects to (b)(6),(b)(7)(C)
a Port 22

Check Slash dot article

(b)(6),(b)(7)(C) Chinanet-SW
China Telecom

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) requests to

Dec 24

(b)(6),(b)(7)(C) Aussie HQ

Canberra Australia

(b)(6),(b)(7)(C) Amazon.com

(b)(6),(b)(7)(C) Amazon

Flow Jan 6 ≈ 1251

(b)(6),(b)(7)(C)

Jan 6 ≈ 1251 connects to
Amazon IP Address

after 1230
Jan 6 goes back to DHCP
to register again
Different building does not
Know IP Address

699

A laptop was reported stolen
from Bldg 2 some time after 2100 12/29

stolen Dec 29 to Dec 31

Amazon Elastic Compute Cloud = EC2
aws.amazon

Prior JSTOR Access
Used to be all of MIT 18.*.*
~~access was~~ Used to have access to
JSTOR

1/3/11 (b)(6),(b)(7)(C) to
(b)(6),(b)(7)(C) email
(b)(6),(b)(7)(C)

JSTOR notifies above of (b)(6),(b)(7)(C)

1/4/11 (b)(6),(b)(7)(C) traces IP to
Router by IP Address in ARP table
ARP table shows 00:1c.e5a0.c756

Same MAC in table has (b)(6),(b)(7)(C)
0 seconds talking on network

possible IP set up in case (b)(6),(b)(7)(C)
was shut down

(b)(6),(b)(7)(C) [redacted] = JSTOR

ARP Table shows Switch
G: 8/16 = Building 16
M16-004T-sw-entry.mit.edu = switch

M16-004T 004T is Room
Room in Building 16 is 4T

1/4/11 02
(b)(6),(b)(7)(C) [redacted] sends emails (b)(6),(b)(7)(C) [redacted] →
(b)(6),(b)(7)(C) [redacted] with location of switch

Mechanism of connecting to JSTOR.
script

Closet was locked
not know how access
key possible
the double doors
top of second door not locked

MIT Registration
Guest access used 1st
static IP ~~manual~~ used later

Guest Registration has full access
in/out of network
Border routers block Microsoft Ports

all 3 registration variations of Ghost
ghost-macbook ghost-laptop
Gene Grg Grace

Firstly on 2200 hit much test traffic

MAC address spoofed at least once

JAN MAC no valid OUI
Acer Aspire should have Marvel

004c.e5a0.c756

00-23-5A Compal Information

To prevent Identification
spoof MAC Address
use of ~~mail~~ mailinator

Two open ports SSH + CherryPy

Cherry Py framework
where commands can be sent
web: [illegible]

160 hours spent of MIT
IS&T on issue

(b)(6),(b)(7)(C)

1520 (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) Starts Packet Capture
~ 0820 - 0830 1/7/11

(b)(5)

999

Available Evidence

- Building 16 Surveillance
- Network Capture
- Photos of surveillance
- radius-logs

Acer Aspire & external
were deliberately hidden under
box

(b)(5)

(b)(5)

(1) Set up Conf call w/ JSTOR
Network personal

(b)(5)

Aaron Swartz uses address on
Mass Ave on for incorporation

(2) Identify Associates

(3) Postal Where delivering Mail

Aaron Swartz images
look for (b)(6),(b)(7)(C)

look for (b)(6),(b)(7)(C) in twitter

667

(b)(6),(b)(7)(C)

x 1630

(b)(6),(b)(7)(C)

Scholarly Publishing + Licensing

(b)(6),(b)(7)(C)

JSTOR since 97 bought
many collections one time fee
+ subscription maintenance
1435 K ~~one fee~~ total
$ 50 k a year Maintenance

Archive Capital fee = one time fee
Maintenance fee = subscription

Partnership Model
fee based on # of programs

purchased 8 collections so far

Gateway to electronic Resources
MIT access is IP filter

from off campus must come
through Gateway

A student on the MIT Network can go direct to JSTOR

MIT Net rules of use

Policies + Procedures

only one other occurrence
early in relationship w/
JSTOR 96, 97, 98

1st Report shut down whole
MIT class A

~~other 2~~ 2nd shut down class B

3rd shut down class C

correspondence w/ (b)(6),(b)(7)(C)

MIT on participants list

Harvard need PIN to access JSTOR

Cambridge Crime Scene

(b)(6),(b)(7)(C)

Wired Magazine

UPS Store Cambridge
950 Mass Ave

1/18/11 Conf w/ Heymann
Contact JSTOR
for POC

SW Affidavit
- Residence
- computer
- External Storage
- Thumb Drive
- Cell Phone

Question Room mate

who did he call

Twitter
Amazon EC2

Important:

ONLINE REPORT

Data is entered poorly, processed incorrectly and generally not free from defect. Any data supplied by this system must be independently verified.

This is NOT a CONSUMER REPORTING REPORT and does not constitute a "consumer report" under the Fair Credit Reporting Act ("FCRA"). This report may not be used to determine the eligibility for credit, insurance, employment or any other purpose regulated under the FCRA.

This system may be used only in accordance with your Subscriber Agreement, the Gramm-Leach-Bliley Act ("GLB"), the Driver's Privacy Protection Act ("DPPA") and all other applicable laws. User agrees to having knowledge of all applicable laws pertaining to the usage of data. User accepts all responsibility civilly and criminally for any use of this system.

Violations of these restrictions or misuse of this system will cause your access to be terminated and will cause an immediate investigation.

Comprehensive Report

Comprehensive Report
Date: 01/06/2011
Reference ID: SAR-RT BOS

Report Legend
- Confirmed Address
- Deceased Person
- View Address Map
- View Social Network(s)

Shared Address
- 1st Degree of Separation
- 2nd Degree of Separation
- 3rd Degree of Separation
- 4th Degree of Separation
- 5th Degree of Separation

Subject Information

(Best Information for Subject)

Name: AARON H SWARTZ (12/10/2004 to 09/01/2010)
Date of Birth: 11/08/1986. Born 24 Years Ago
SSN (b)(6),(b) 0493 issued in ILLINOIS between 1991-1992

Other Names Associated with Subject
None found

Other DOBs Associated with Subject
None found

Other Phones Associated with Subject:
(b)(6),(b)(7)(C) (Land Line)

Indicators

Bankruptcy: No
Property: No
Corporate Affiliations: No

Email Addresses Associated with Subject
aaronsw@wff.continue.com
aswartz@upclink.com

Comprehensive Report Summary

Bankruptcies: None found
Phones Plus: 7 found
Driver's License: None found
Address(es) found: 4 found
Motor Vehicles Registered: None found
Possible Criminal Records: None found

Address History (4 Found)

(b)(6),(b)(7)(C) (12/10/2004 to 01/06/2011)
1 Current Private Phone
Subject's Phone
(b)(6),(b)(7)(C)
Owners:
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) (07/2007 to 07/15/2010)
Address contains: 24 apartments
4 Current Private Phones
Current Private Phones at address
NOT PUBLISHED (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) (03/15/2007 to 04/10/2007)

(b)(6),(b)(7)(C) (04/21/2006 to 04/21/2006)
Address contains: 3 apartments
2 Current Private Phones
Current Private Phones at address
(b)(6),(b)(7)(C)
Owner:
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

Cities History (3 Found)

HIGHLAND PARK, IL (LAKE COUNTY) (12/10/2004 to 10/2010)
SAN FRANCISCO, CA (SAN FRANCISCO COUNTY) (03/15/2007 to 07/15/2010)
SOMERVILLE, MA (MIDDLESEX COUNTY) (04/21/2006 to 04/21/2006)

Counties History (3 Found)

LAKE, IL (12/10/2004 to 10/2010)

SAN FRANCISCO, CA (03/15/2007 to 07/15/2010)
MIDDLESEX, MA (04/21/2005 to 04/21/2006)

Possible Relatives - Summary (6 Found)

(b)(6),(b)(7)(C)

D (b)(6),(b)(7)(C)

D

(b)(6),(b)(7)(C)

D WILLIAM M SWARTZ 09/18/1912 Age: 98 died at (75)

(b)(6),(b)(7)(C)

Possible Relatives - Details (6 Found)

View Person Record [Back to Summary]

Names:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Addresses:
✔ S (b)(6),(b)(7)(C) (09/01/2000 to Present)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) (03/01/2010 to 09/01/2010)
(b)(6),(b)(7)(C) (07/01/1997 to 07/02/2005)
(b)(6),(b)(7)(C) (10/01/1986 to 08/13/1997)
(b)(6),(b)(7)(C) (09/27/1992 to 05/25/1993)
(b)(6),(b)(7)(C) (07/01/1989 to 06/01/1991)
(b)(6),(b)(7)(C) (01/01/1986 to 06/01/1991)
(b)(6),(b)(7)(C) (10/01/1985 to 06/01/1991)
(b)(6),(b)(7)(C) (02/01/1985 to 04/01/1986)
(b)(6),(b)(7)(C) (03/01/1985 to 03/01/1986)

(b)(6),(b)(7)(C)

Possible Relatives:

View Person Record [Back to Summary]

Name:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C) -4127 issued in ILLINOIS in 1934-1951

Date of Birth:
07/29/1924, 86 years old

Date of Death:

D 10/28/2007, Passed away at 83 years old

Other Phones:
(b)(6),(b)(7)(C)

Addresses:
S (b)(6),(b)(7)(C) 10/01/2010)
(b)(6),(b)(7)(C) 03/16/2005)
(b)(6),(b)(7)(C) 10/01/1976 to 10/04/2003)
(b)(6),(b)(7)(C) (06/01/1974 to 06/01/1974)
(b)(6),(b)(7)(C)

Possible Relatives:

View Person Record [Back to Summary]

Names:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Other Phones:
(b)(6),(b)(7)(C)

(847) 987-6220

Email Address:
(b)(6),(b)(7)(C)

Addresses:
(b)(6),(b)(7)(C)

S (b)(6),(b)(7)(C)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Name:
(b)(6),(b)(7)(C)

SSNs:
(b)(6),(b)(7)(C)

Addresses:
S (b)(6),(b)(7)(C)
S
S
S

View Person Record | Back to Summary |

Name:
(b)(6),(b)(7)(C)
SSN:
(b)(6),(b)(7)(C)
Date of Birth:
(b)(6),(b)(7)(C)
Date of Death:
D (b)(6),(b)(7)(C)
Addresses:
S (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

View Person Record | Back to Summary |

Name:
(b)(6),(b)(7)(C)
SSN:
(b)(6),(b)(7)(C)
Date of Birth:
(b)(6),(b)(7)(C)
Other Phone:
(847) 432-5775

Addresses:
(b)(6),(b)(7)(C)

View Person Record | Back to Summary |

Name:

(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Email Addresses:
(b)(6),(b)(7)(C)

Addresses:
✔ 5 (b)(6),(b)(7)(C)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Names:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Email Address:
(b)(6),(b)(7)(C)

Addresses:
✔ 5 (b)(6),(b)(7)(C)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary].

Name:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Email Address:
(b)(6),(b)(7)(C)

Addresses:
✔ 5 (b)(6),(b)(7)(C) (08/24/2008 to Present)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Name:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Addresses:
✔ (b)(6),(b)(7)(C)

Current landline phones at address:
(b)(6),(b)(7)(C)

✔ 5

(b)(6),(b)(7)(C)

Current landline phones at address:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Name:

(b)(6),(b)(7)(C)

SSN:

(b)(6),(b)(7)(C)

Dates of Birth:

(b)(6),(b)(7)(C)

Date of Death:

(b)(6),(b)(7)(C)

Addresses:

(b)(6),(b)(7)(C)

Current landline phones at address:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Current landline phones at address:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Possible Relatives:

View Person Record [Back to Summary]

Name:

(b)(6),(b)(7)(C)

SSN:

(b)(6),(b)(7)(C)

Dates of Birth:

(b)(6),(b)(7)(C)

Other Phone:

(b)(6),(b)(7)(C)

Addresses:

(b)(6),(b)(7)(C)

Current landline phones at address:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Name:

(b)(6),(b)(7)(C)

SSN:

(b)(6),(b)(7)(C)

Addresses:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Possible Associates - Summary (6 Found)

(b)(6),(b)(7)(C)

Possible Associates - Details (6 Found)

View Person Record [Back to Summary]

Name:

(b)(6),(b)(7)(C)

SSN:

(b)(6),(b)(7)(C)

Date of Birth:

(b)(6),(b)(7)(C)

Email Address:

(b)(6),(b)(7)(C)

Addresses:

(b)(6),(b)(7)(C)

Current landline phones at address:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Names:

(b)(6),(b)(7)(C)

SSN:

(b)(6),(b)(7)(C)

Date of Birth:

(b)(6),(b)(7)(C)

Other Phones:

(b)(6),(b)(7)(C)

Email Address:

(b)(6),(b)(7)(C)

Addresses:

(b)(6),(b)(7)(C)

Current landline phones at address:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Names:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Other Phone:
(b)(6),(b)(7)(C)

Email Address:
(b)(6),(b)(7)(C)

Addresses:
(b)(6) (b)(7)(C)

S (b)(6) (b)(7)(C)
(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Names:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Other Phones:
(b)(6),(b)(7)(C)

Addresses:

(b)(6),(b)(7)(C)

S (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

View Person Record [Back to Summary]

Name:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Date of Birth:
(b)(6),(b)(7)(C)

Addresses:
(b)(6),(b)(7)(C)

S (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Current landline phones at address:
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6) (b)(7)(C)

View Person Record [Back to Summary]

Name:
(b)(6),(b)(7)(C)

SSN:
(b)(6),(b)(7)(C)

Addresses:
S (b)(6) (b)(7)(C)
(b)(6),(b)(7)(C)

Neighbors (9 Found)

Neighbors for (b)(6) (b)(7)(C)
(b)(6) (b)(7)(C)
1 Current Private Phone

Current Private Phone at address
(b)(6),(b)(7)(C)

Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Date Of Death:

D 03/26/1992, Passed away at 84 years old

Resident Name: [View Person]

(b)(6),(b)(7)(C)

Resident Names: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

Resident Names: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

2 Current Private Phones

Current Private Phones at address

(b)(6),(b)(7)(C)

Resident Name: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

Resident Name: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

Resident Name: [View Person]

(b)(6),(b)(7)(C)

Resident Names: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

Resident Name: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

1 Current Private Phone

Current Private Phone at address

(b)(6),(b)(7)(C)

Resident Name: [View Person]

(b)(6),(b)(7)(C)

Date Of Birth:

(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Neighbors for (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Neighbors for (b)(6),(b)(7)(C)
(b)(6),(b)(
1 Current Private Phone

Current Private Phone at address
(b)(6),(b)(7)(C)

Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Date Of Death:
09/03/2007, Passed away at 82 years old
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Date Of Death:
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
1 Current Private Phone

Current Private Phone at address
(b)(6),(b)(7)(C)

Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Name: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)
Resident Names: [View Person]
(b)(6),(b)(7)(C)

Date Of Birth:
(b)(6),(b)(7)(C)

Neighbors' Phones (19 Found)

Neighbors' Phones for (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)

MCS

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)

[View Person Record]

Neighbors' Phones for (b)(6),(b)(7)(C)

(b)(6),(b)(7)

(b)(6),(b)(7)(C)

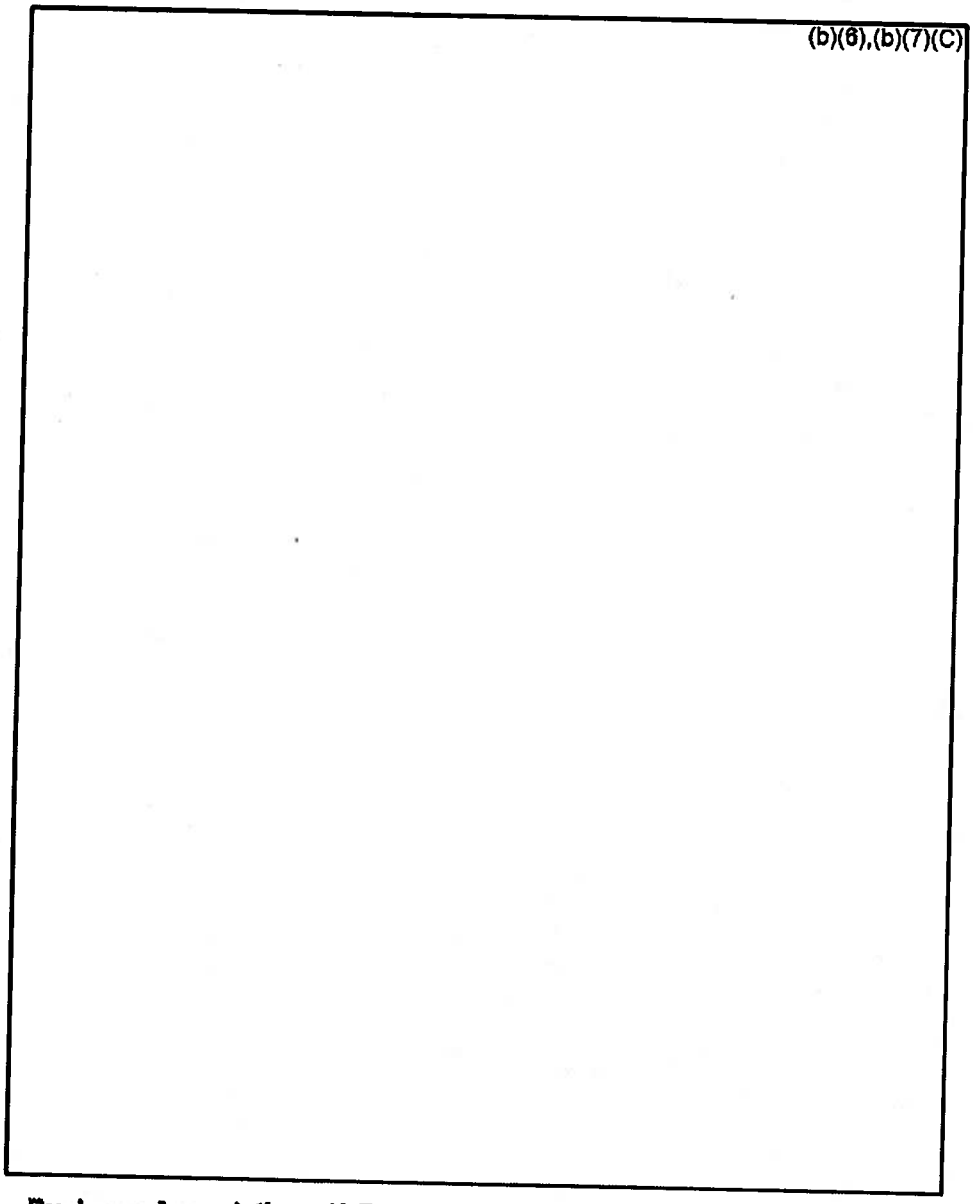
[View Person Record]

Neighbors' Phones for (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

[View Person Record]

(b)(6),(b)(7)(C)



Business Associations (1 Found)

Business Details
AARON SWARTZ (Primary)
Link Number (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Current Other Phone at address

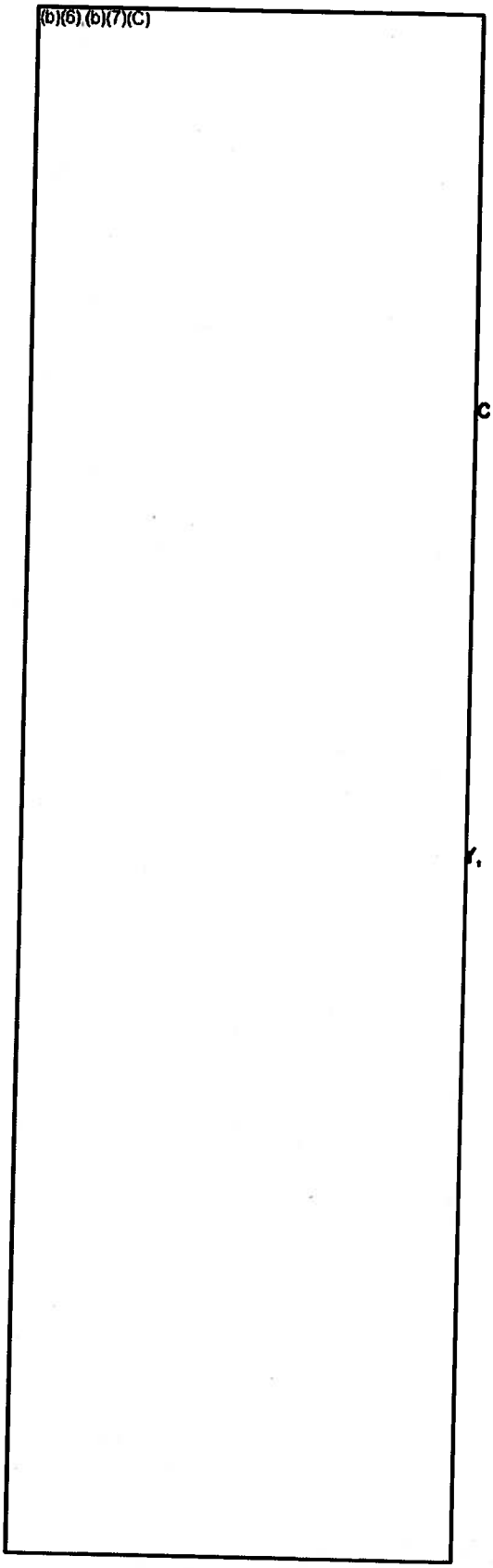
(b)(6),(b)(7)(C)

Index

AARON H SWARTZ, 2
AARON SWARTZ, 21

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)


(b)(6),(b)(7)(C)

D15Doc6 (Contacts @ JSTOR).txt

From: [redacted] thaka.org]
Sent: Tuesday, January 25, 2011 4:32 PM
To: [redacted] (BOS)
Cc: 'Stephen.Heyman[redacted]
Subject: Contacts @ JSTOR

Hi [redacted]

Please find the information requested below…

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) User Services
[redacted]@ithaka.org

[redacted]

(b)(6),(b)(7)(C) Office of General Counsel
[redacted] ithaka.org

[redacted] Public Systems

(b)(6),(b)(7)(C) Public Systems

D15Doc9 (FW MIT abuse).txt

From: Heymann, Stephen (USAMA) [Stephen.Heymann@usdoj.gov]
Sent: Wednesday, February 02, 2011 8:29 AM
To: External (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: FW: MIT abuse
Attachments: MIT NovDec all IP's.png; MIT NovDec excluding abuse IP's.png

From: (b)(6),(b)(7)(C) [mailto: (b)(6),(b)(7)(C) thaka.org]
Sent: Friday, January 28, 2011 2:58 PM
To: Heymann, Stephen (USAMA)
Subject: MIT abuse

FYI

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:29 PM
To:
Cc: (b)(6),(b)(7)(C)
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) (b)(6),(b)(7)(C) and totals 17,865
for the 2 month period. Recognizing that some legitimate downloads may have occurred from the 3 filtered
IP's, it would still be safe to say that about 2.8 million illegal downloads occurred during November and
December. We know that some 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 place 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)(6),(b)(7)(C)

Speaking with (b)(6),(b)(7)(C) just now about making sure we have (b)(6),(b)(7) time as needed for the MIT evaluation currently underway and discovering that the IP addresses associated with these specific incidents have numerous additional days of mass downloading.

It would take some time to normalize against usual MIT usage, but at first glance, it is reasonably safe to assume from what (b)(and I covered that the individual responsible has already acquired the entire JSTOR corpus. Glad to have a call ASAP if you think it useful and I let (b)(6), know that I thought you might be calling him shortly after receiving this message for clarification. In light of this information, it would seem that we need to try and understand the full picture outside of the identified incidents going forward. Certainly our tack here merits some re-evaluation, both concerning this case and the potential for additional measures of prevention as we move forward. Also copying in (b)(6),(b)(7)(C) at this juncture.

(b)(6),(b)(7)(C)

Thanks,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) @ithaka.org

D15Doc11 (FW Updated Timeline of JSTOR-related events from September through today).txt

(b)(6),(b)(7)(C)

MIT (b)(6),(b)(7)(C) Operations & Infrastructure
MIT
MIT (b)(6),(b)(7)(C)
MIT
MIT Voice/Data Installation (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C)
MIT IT (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C) Network Security & Support Services
MIT (b)(6),(b)(7)(C) Network & Information Security (b)(6),(b)(7)(C)

Sun 9/26/10 | 12:31pm (b)(6),(b)(7)(receives email from (b)(6),(b)(7)(at JSTOR stating that at 8am excessive downloading of journals started and that all of MIT's access to JSTOR has been blocked.

Mon 9/27/10 | 10:28am Security team receives email from (b)(6),(b)(7) regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) & 18.55.6.215 and needs help identifying the user of those addresses. (b)

Mon 9/27/10 | pm follows up with (b)(6),(b)(7)(that we're looking into identifying user.

Mon 9/27/10 | pm JSTOR restores MIT's access having changed their blocking to just 18.55.6.*; user information discovered reveals bogus guest network registration named

Gary
Host (ghost@mailinator.com)

with host registration occurring on Fri 9/24/10.

Mon 9/27/10 | pm Computer registration for bogus host disabled.

Tue 9/28/10 | am (b)(6),(b)(7)(C emails (b)(6),(b)(7)(C to speak to issues regarding the bogus registration info as well as the IP blocking approach and thinks a call with JSTOR might be fruitful in determining JSTOR's future courses of action around blocking, as a) blocking is usually a temporary solution and b) this problem would most likely reoccur because IP addresses are easily changed.

Thu 9/30/10 | pm (b)(6),(b)(7)(emails (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) to provide the facts of the event; mentions that (b)(6),(b)(7)(and (b)(6), had spoken regarding possible solution utilizing authentication that's already available from the Libraries for JSTOR access; some logistics to work out.

Sat 10/9/10 | 11:15pm (b)(6),(b)(7)(C emails (b) informing her MIT's JSTOR access has been cut off again due to extreme downloading.

Mon 10/11/10 | 7:44pm (b)(6),(b)(7)(emails (b)(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

D15Doc11 (Fw Updated Timeline of JSTOR-related events from September through today).txt

additional measures of blocking due to lack of IP info as VPN-based abuses of resources have been exploited in the past.

Tue 10/12/10 | 6:36am | Security team receives email from (b)(6),(b)(7)(regarding most recent JSTOR abuse; no IP address information yet to act on.

Tue 10/12/10 | 4:02pm | Security team receives email from (b)(6),(b)(7)(with logs and IP address information provided by JSTOR.

(b)(6),(b)(7)(C) | JSTOR access restored. Abuse coming from address

Wed 10/13/10 | 6:34am | (b)(6),(b)(7)(sends email to (b)(6), and (b)(6),(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.

Host registration committing download now shows Grace Host (ghost420mailinator.com).

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.

It becomes clear that this is willful and intentional abuse for possible purpose of spidering JSTOR without being identified. All bogus host registrations are disabled.

Wed 10/13/10 | 3:12pm | (b)(6),(b)(7)(emails (b)(6),(b)(7)(and (b)(6),(b)(7)(with the information that it appears to be the same unknown person using our guest registration capability from a wired connection in building 16.

Wed 10/13/10 | 3:42pm | (b)(6),(b)(7) responds to (b)(6),(b and Security team that she will pursue the Libraries moving to the proxy/econtrol system for accessing JSTOR.

Wed 10/13/10 | 10:41pm | (b)(6),(b)(7)(sends email to (b)(6), and (b)(6),(b)(7) that the offending machine is no longer seen on the network.

Thu 10/14/10 | 10:47am | (b)(6), emails (b)(6),(b)(7)(to inquire as to whether JSTOR is still seeing continued excessive downloading. Voices support for the Libraries to move to econtrol/proxy

D15Doc11 (Pw Updated Timeline of JSTOR-related events from September through today).txt

system
for MIT's access to JSTOR.

Thu 10/14/10 | 5:05pm (b)(6),(b)(7)(C) emails (b)(6),(and (b)(6),(b)(7) to let us know of JSTOR's wanting some sort of indication that we've identified the user or any expectation of being able to identify in the future.

Thu 10/14/10 | 9:09pm (b)(6),(b)(7) responds to (b)(6),(b)(7)(C) email with reasons for difficulties of identifying random guest user making attempts to thwart detection when using our wired network.

Thu 10/14/10 | 11:26pm (b)(6),(b)(7)(C) asks (b)(6),(for any updates to share with (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C).

Thu 10/14/10 | 11:33pm (b)(6),(emails facts of case to date to (b)(6),(b around extreme robotic activity of JSTOR at MIT.

Fri 10/15/10 | 1:31am (b)(6),(b)(7)(emails (b)(6),(b)(7) and (b)(6),(to keep eye out for the host so their physical location can be determined if they show up again.

Fri 10/15/10 | 11:26am (b)(6),(b)(7)(forwards email from JSTOR to MIT Security team; JSTOR would like assurances that we could monitor for this type of behavior. (b)(6),(b)(7)(responds to JSTOR that it is not technically feasible for us to do that kind of monitoring. I point out that JSTOR has many more capabilities than we do to facilitate that kind of monitoring.

(b)(6),(b)(7)(C Meanwhile, there are emails between (b)(6),(b)(7)(C) and that speak to risk management and protection, both technically and practically, of our own assets and resources against this type of threat.

Fri 10/22/10 | 4:48pm (b)(6),(b)(7)(C from JSTOR sets up conference for 10/26 with (b)(6),(b)(7)(from JSTOR, (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

Tue 10/26/10 | 2:00pm Conference call with JSTOR; next moves to econtrol/proxy system for authentication to JSTOR was discussed. (b)(6),(b) sends email with update and next steps: JSTOR will make landing page to smooth access for users who try to access JSTOR directly from MIT's network rather than using proxy. Libraries would then go ahead and communicate with users (drafts were already ready). Proxy server configuration changes would be made. JSTOR would be contacted and would change the list of permitted IPs to only MIT's proxy servers.

Mon 11/29/10 | 6:47pm Security team receives notice from IEEE that journal spidering is occurring on their site. It is tracked to the SIPB XVM cluster, a group of computers that are

D15Doc11 (FW Updated Timeline of JSTOR-related events from September through today).txt
shared and that anyone in the
MIT community can host a Virtual Machine on.

Tue 11/30/10 | 2:40am The user running the Virtual Machine on SIPB's cluster is
notified; his Virtual Machine had been
compromised and scripts placed on it that were downloading
journals from JSTOR, IEEE and APS.
The machines were taken offline. (b)(6), (b)(7)(C) from (b)(6), (b)(7)(

Mon 01/03/11 | 10:49am (b)(6), (b)(7)(receives email forwarded via
JSTOR regarding an incident on 12/26 at 9pm
of (b)(6),(b)(7)(C) excessively downloading JSTOR journals again;
surprising, as under impression that
authentication had been set up and proxy was being used.
Discovers that hold-up has been
JSTOR's difficulties with setting up landing page to make it
easier
for our users.

Tue 01/04/11 | 1:34am (b) (6), pings (b) (6),(b regarding incident; (b)(6), (b)(7)(had starting to
look into incident at that time. Can
find zero information regarding this IP address, not even
bogus
guest registration data as found
before. Started email reply to (b)(6), (b)(7)(then started examining
older
emails - all former abuses had
come from 18.55. With recent network infrastructure access
and
tools given to Security team to
enable self-sufficient discovery/protection of network and
users,
more investigation into the
(b)(6),(b)(7)(C) address and its possible physical location was
pursued.

The user was now not using any of the typical methods to
access
MIT-net to avoid all usual
methods of being disabled, including assigning himself an
additional IP address (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) which had been doing the
so communication wouldn't be interrupted if we disabled
downloading.

Tue 01/04/11 | 2:49am (b)(6), (b)(7)(sends email to (b) (6), and (b)(6), (b)(7) containing findings to
see if they could further pinpoint
location in building 16.

Tue 01/04/11 | 3:24am (b) (6),(b sends email to (b)(6), (b)(7)(with update, concurs that move
to econtrol/proxy system is prudent,
and that further information should be known with (b)(6), (b)(7) and
(b)(6),(b)
(7)(C)
help.

Tue 01/04/11 | 3:42am (b)(6), (b)(7) (C) emails (b)(6), (b)(7) and (b) (6), with copy of email to (b)(6), (b)(7)
and copy of email to (b)(6), and (b)(6),(b)(7)(C)

Tue 01/04/11 | 8:08am (b)(6), (b)(7)(C) emails (b)(6), (b)(7)(with news that he's found the
offending computer; an Acer netbook hidden
under a box in the network closet in the basement of building
16.
Under the netbook is

D15Doc11 (Fw Updated Timeline of JSTOR-related events from September through today).txt

an external hard drive.

(b)(6),(b)(7)(C) arrives to assist Dave. Traffic to/from the netbook is captured on (b)(6),(b) laptop. The only traffic destined for the netbook is a single ping from Chinese address space.

9:44am (b)(6),(b)(7)(and (b)(6),(b)(7)(talk via phone. (b)(6),(b) calls (b)(6),(b)(7)(C) to advise and for counsel around legality of possibly having MIT police seize laptop.

(b)(6),(b)(7)(is notified by (b)(6),(b)(7)(C) and notifies MIT police.

10:30am (b)(6),(b)(7)(C) and (b)(6),(b)(7)(join (b)(6),(b) and (b)(6),(b)(7) in building 16, along with two MIT uniformed officers who are guarding scene. We are told that Det. (b)(6),(b)(7)(C) has notified Cambridge police who are en route.

~11:00am Det. (b)(6),(b)(7)(C) arrives with additional uniformed officers, Det. (b)(6),(b)(7)(C) Crime Scene Investigators and USSS Agent (b)(6),(b)(7)(C) and (b)(6),(b)(7) detail events. (b)(6),(b)(7)(C) handles computer forensics for the Secret Service.

CSI folks fume for prints and photograph the scene. Prints are found and lifted from netbook. Scene is released for further investigation.

(b)(6),(b)(7)(C) arrives with an IP-based video camera for surveillance after it's decided, at the recommendation of (b)(6),(b)(7)(C) that the netbook be left in place to continue to monitor traffic to/from it. At that time, it is observed that the netbook is still reaching out to JSTOR and downloading journals.

It was also observed that connections were now being made to the computer from an IP address in China. (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) arrive to assist.

~12:30pm (b)(6),(b) and (b)(6),(b)(7)(stop by General Counsel's office to advise MIT's counsel of law enforcement's presence on campus and discuss what data is in-scope to provide them for the investigation that OI has stewardship over. (b)(5),(b)(6),(b)(7)(C)

(b)(5),(b)(6),(b)(7)(C)

~1:30pm (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) continue to observe netbook;

suspect had been observed in the past changing his MAC address.
It is plausible, given the circumstance, that the laptop was moved up there when it had been removed from
the basement.

2:22pm (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) drive to building 16 to attempt to recover the netbook.
(b)(6),(b)(7)(C) calls (b)(6),(b)(7)(C) on the way to inform him and for police
presence while the attempt is made to locate the netbook. (b)(6), informs them that he and SA (b)(6),(b)(7)(C) had just
apprehended the suspect near Central Square attempting to flee. Detective (b)(6),(b)(7)(C) joins us with a uniformed
officer.

~2:40pm (b)(6), (b)(7) is called and joins us quickly in 16 to aid in tracing the
punched-down wires in the TR to the possible location of the netbook. The netbook could not be located on the
4th floor; instead, a Dell laptop in an office belonging to students is identified as having leased the
(b)(6),(b)(7)(C) address, by happenstance, after the suspect's netbook stopped using it.

~3:15pm The group returns to W92. The netbook had been using a statically assigned IP address, however, because
it moved, it was possible that it had been reconfigured to use
DHCP services for network access. (b)(6), (b)(7)(C) checks today's DHCP logs for "ghost", part of the laptop's name that had
been used over the past months.
ghost-laptop is seen in the logs, with the same MAC address that
had been used on Tuesday. (b) (6), (b)(7)(C) verifies that the netbook is still active on the network. (b) (6), finds the
netbook seems to be on the network in building W20 on the 5th floor. The log shows:

Jan 6 12:48:31 wall-street dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)

Jan 6 13:27:01 installer dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)

At 12:42 the netbook was re-registered on the network in building
4, 8 minutes after being picked up from building 16. 39 minutes later, at 1:26, it was plugged into a
network jack in building W20.

3:20pm (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) arrive at W20. The network closet is examined and jack location determined. (b)(6),(b)(7)(C)
determine the network drop location is in the SIPB

D15Doc16 (Guerrilla Open Access Manifesto).txt

From: Heymann, Stephen (USAMA)[(b)(6),(b)(7)(C) sdoj.gov]
Sent: Friday, April 15, 2011 12:30 PM
To: [(b)(6),(b)(7)(C) (BOS); External-[(b)(6),(b)(7) cambridgepolice.org
Subject: Guerrilla Open Access Manifesto

...The Open Access Movement has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

"I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal – there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.

Those with access to these resources – students, librarians, scientists – you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not – indeed, morally, you cannot – keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral – it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed....

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks....

http://www.earlham.edu/~peters/fos/2008/09/guerilla-oa.html

D15Doc24 (Numbers of Interest).txt

From: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)cambridgepolice.org]
Sent: Tuesday, February 22, 2011 11:07 AM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov); (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (BOS)
Subject: Numbers of Interest

Hi Steve,

Below are the numbers we would like to have subpoenaed for ownership records.

AT&T numbers: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

Verizon: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

T-Mobile: (b)(6),(b)(7)(C)

Bandwith.com (competitive local exchange carrier / internet telephony) (b)(6),(b)(7) (b)(6),(b)(7)(C)

Bandwidth (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

As a result of my conversation with T-Mobile last Friday I was able to glean the following facts.

Internet Addressing: Destination IP and Phone Number IP are generic IP addresses which state that the operator of the phone went out to the Internet. There is no other information available or stored by T-Mobile when an individual accesses the Internet. I asked 18 ways from Sunday for a way to get more information from three different T-Mobile representatives including a tech analyst.

Call Forwarding: When an abbreviation e.g. "SNFC MT - EV, CA" is listed in the Destination Column this indicates that the cell phone operator has placed his phone on "call forward" mode and the number listed under "Phone Number" column is the number the operator punched into the phone directing incoming calls to be forwarded to that number. In the majority of these instances, Swartz has forwarded his calls to (b)(6),(b)(7)(C)

Country Code: 356: Initially upon asking questions all three representatives stated that this was a call from Malta. When pressed that this was not reasonable or logical no explanation was given. In one instance the tech analyst stated that he would do further research and call me back. He never called back and his voicemail now indicates that he is away. After doing some Internet research it would not be outlandish to believe that a person calling Swartz might be spoofing their number.

Conference Calling: The two conference calls placed during the month are calls Swartz initiated. He dialed the two numbers listed in the Phone Number column.

Hope this helps in clarification.

(b)(6),(b)(7)(C)

D15Dec25)Re 1-6-11 at 1232).txt

From: (b)(6),(b)(7)(C) [(b)(6),(b)(7)(C)@MIT.EDU]
Sent: Thursday, January 06, 2011 4:13 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: 1-6-11 at 1232

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

(b)(6),(b)(7)(C) skyfire /var/log/dhcplogger $ grep ghost dhcp
Jan 6 12:42:49 installer dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) 1 Jan 6 12:42:49 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 12:42:49 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 12:44:32 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:44:32 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:45:22 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:45:22 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:46:22 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:46:22 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:48:31 wall-street dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 12:48:31 wall-street dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) (18.69.0.33) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(Jan 6 12:48:31 wall-street dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(Jan 6 12:48:31 installer dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(Jan 6 12:48:32 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via 18.53.0.1 Jan 6 12:50:56 wall-street dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 12:50:56 wall-street dhcpd: DHCPACK on 18.53.6.12 to 00:4c:e5:a0:c7:56 (ghost-laptop) via 18.53.0.1 Jan 6 13:27:01 installer dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 13:27:01 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 13:27:01 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 13:27:02 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 13:27:02 wall-street dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)

On Jan 6, 2011, at 1:47 PM, (b)(6),(b)(7)(C) (BOS) wrote:

>
> (b)(6),(b)(7)(C)
>
>
> Sent from blackberry.
>
> From: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) gmail.com>
> To: (b)(6),(b)(7)(C) (BOS)
> Sent: Thu Jan 06 13:39:27 2011
> Subject: 1-6-11 at 1232
>
>
>
> 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

[redacted]D15boc27 (Re Jan 8 email to [redacted]).txt
From: [redacted][MIT.EDU]
Sent: Monday, February 07, 2011 3:55 PM
To: [redacted](BOS)
Subject: Re: Jan 8 email to [redacted]

I trust this is the one you're looking for?

On Jan 8, 2011, at 6:04 PM, [redacted] wrote:

I was wondering what Swartz had been doing on his brief layover in building 4 on his way to sipb. While gathering up all the stuff for [redacted] the network traffic that happened actually didn't happen in sipb but in 4... including 30 seconds and a couple of KB to Amazon EC2... very possible that's where all this stuff was headed - thought you might find it interesting. Anyway, besides a few other things, I'm pretty much tapping out and spent and gonna go chill for the rest of the weekend. Hope yours is good.

[redacted]skylynx ~ $ for i in `cat [redacted]building_4_flows.txt | awk '{ print $4 $7 }' | sed 's[redacted]/g' | sort -u | grep -v SrcIP`; do echo $i $$ whois $i | egrep -i "OrgName|NetName"; done

[redacted]
NetName: APNIC-113 (China)
[redacted]
OrgName: Asia Pacific Network Information Centre
[redacted]
NetName: AMAZON-EC2-5
OrgName: Amazon.com, Inc.
[redacted]
NetName: MIT (PRINTING-GREEN.MIT.EDU)
OrgName: Massachusetts Institute of Technology
[redacted]
NetName: MIT (DNS)
OrgName: Massachusetts Institute of Technology
[redacted]
NetName: MIT (DNS)
OrgName: Massachusetts Institute of Technology
[redacted]
NetName: MIT (DHCP)
OrgName: Massachusetts Institute of Technology
[redacted]
NetName: MIT (DNS)
OrgName: Massachusetts Institute of Technology
[redacted]
NetName: AMAZON-EC2-6
OrgName: Amazon.com, Inc.
[redacted] (Korea)
NetName: MAGPI-BLK-1 (JSTOR)
OrgName: MAGPI c/o University of Pennsylvania
[redacted]
NetName: AMAZON-EC2-8
OrgName: Amazon.com, Inc.
[redacted]
NetName: MOZNET-1
OrgName: Mozilla Corporation
[redacted]
NetName: CDNET-USA-2 (odd 3 second connection to

D15Doc27 (Re Jan 8 email to (b)(6),(b)(7)(C) .txt

port 80)
OrgName: CDNetworks Inc.
93.184.215.73
netname: EDGECAST-NETBLK-03 (some IP outside
Wichita)

On Feb 7, 2011, at 2:40 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Could you forward me the email you sent to (b)(6),(b)(7)(C) on January 8 at 6PM about the IP addresses
associated with building 4?

b15Doc28 (Re Name of MIT Contact).txt

From: (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, January 04, 2011 6:06 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Name of MIT Contact

(b)(6),(b)(7)(C) at MIT PD do you need his info?

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
To: (b)(6),(b)(7)(C)
Sent: Tue Jan 04 17:27:32 2011
Subject: Name of MIT Contact
Who was the first person to contact you from MIT

(b)(6),(b)(7)(C)

Sent from Blackberry

D15Doc29 (RE Packet traffic tofrom the Acer Laptop).txt

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 02, 2011 11:56 AM
To: (b)(6),(b)(7)(C) (CID)
Cc: Externa (b)(6),(b)(7)(cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: Packet traffic to/from the Acer Laptop

(b)(6),

(b)(5)

Steve

From: (b)(6),(b)(7)(C) (CID) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, February 02, 2011 10:55 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (USAMA)
Cc (b)(6),(b)(7)(cambridgepolice.org
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity.
Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)(C)

CERT - (b)(6),(b)(7)(C)
4500 Fifth Avenue
Pittsburgh, PA 15213
TEL (b)(6),(b)(7)(C)
We are eager to help in any way that we are able.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

(b)(6),(b)(7)(C)
From: (BOS)
To: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) usdoj.gov>
Cc: (b)(6),(b)(7)(C) (CID); Externa (b)(6),(b)(7 cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop
I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe the
flow data has enough detail to show remote connections into the laptop but the packet capture
should if the connection was active while the capture was running. I will check with CERT (b)(7)(E)

(b)(7)(E)
(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5)

D15Doc30 (Re Sorry--Important Clarification).txt

From: (b)(6),(b)(7)(C) [MIT.EDU]
Sent: Tuesday, February 08, 2011 8:56 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Sorry--Importance: High

Morning Steve - replies inline - and don't hesitate to let me know if you have additional questions:

On Feb 8, 2011, at 6:39 AM, Heymann, Stephen (USAMA) wrote:

(b)(6),
>(b)(7)(

Refer

D15Doc47 (Unauthorized activity on Massachusetts Institute of Technology network).txt
From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 6:46 PM
To: (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)
Cc: (b)(6),(b)(7)(C) (WFO); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) (REN)
Subject: Unauthorized activity on Massachusetts Institute of Technology network
Attachments: DSC01776.JPG; DSC01786.JPG; DSC01784.JPG

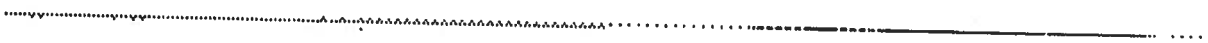
FYI

Unauthorized activity on Massachusetts Institute of Technology network
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 the (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) MIT.EDU) of Massachusetts Institute of Technology Police 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 technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department. (b)(6), (b)(6),(b)(7)(C) @mit.edu), an Information and Network Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11, (b)(6),(b)(7)(C) was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) @mit.edu) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are IP address 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 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile. (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing. (b)(6),(b)(7)(C) provided SA (b)(6),(b)(7)(C) with a copy of flow traffic on the network. The flow traffic is currently being

D15Doc47 (Unauthorized activity on Massachusetts Institute of Technology network).txt
uploaded to the CERT
dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more
network traffic to show if a suspect was controlling the netbook through a SSH channel and if the
network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in
the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to
notify MIT if the netbook is removed from the network. The technical journals being downloaded
have a monetary value. All MIT students have access to view the journals but are limited as to how
much they can download and anyone outside of MIT including students after they graduate have to
pay a substantial subscription to access the files. The price for downloading one file can vary from
$200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)



From: (b)(6),(b)(7)(C)
Sent: Thursday, January 20, 2011 4:56 PM
To: (b)(6),(b)(7)(C) Ames, Paul
Cc: (b)(6),(b)(7)(C)
Subject: MIT Hack Investigation Status

Sir(s),

This is a status draft of where we are regarding the Aaron Swartz investigation.

Several interviews have been completed and the MOI's (Memorandum of Interview) are in rough draft form. I have started the affidavit for the different search warrants which we will probably execute by the end of next week or the beginning of the following week.

We are taking our time with this investigation and crossing all the T's etc....

Case continuing, more to follow.

R/S
(b)(6),
(b)(7)(

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM:	BOSTON FIELD OFFICE	FILE:	102-775-60071-S
TO:	CRIMINAL INVESTIGATIVE DIVISION	X-REF:	N/A
INFO:	INVESTIGATIVE SUPPORT DIVISION	SEIZURE#:	N/A

SUBJECT: OPENING REPORT

CASE TITLE:	AARON SWARTZ
CASE TYPE:	775.510 - UNAUTHORIZED ACCESS UNIVERSITIES
SECONDARY TYPES:	848.191, 848,304, 848.930
CONTROLLING OFFICE:	BOSTON FIELD OFFICE
REPORT MADE BY:	SA (b)(6),(b)(7)(C)
DATE CASE OPENED:	01/07/11
PREVIOUS REPORT:	N/A
REPORTING PERIOD:	01/04/11 - 01/21/11
STATUS:	CONTINUED

SYNOPSIS:

On 01/04/11, MIT contacted the New England Electronic Crime Task Force to request assistance investigating a computer that was found connected to the MIT network in a locked closet without authorization. Further investigation showed that Aaron Swartz intruded into the MIT network without authorization by breaking into the locked closet containing networking components for MIT networks, connecting a computer to the MIT network and downloading documents from JSTOR. Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force for breaking and entering. An investigation of Swartz unauthorized intrusion into the MIT network and the theft of documents from JSTOR is continuing in the Boston district.

computer name "ghost-macbook" registered on the network on 09/24/10. (b)(6),(b)(7)(C) disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR Operations Staff emailed (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)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address (b)(6),(b)(7)(C)

On 10/13/10, (b)(6),(b)(7)(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 MAC address of 0017f22cb074 and computer name of "ghost-laptop". (b)(6),(b)(7)(disabled the host registrations identified as bogus. (b)(6),(b)(7)(C) Network Security and Support Services for MIT, notified (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) 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 XVM 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, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(7)(C) informing him that that the excessive downloading of journals had begun again.

On 01/04/11, (b)(6),(b)(7)(C) emailed (b)(6),(b)(7)(C) Network Operations, and (b)(6),(b)(7)(C) mit.edu) a Network Engineer for Network and Infrastructure Services for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0800, (b)(6),(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)(6),(b)(7)(C) established a packet capture of the same switch the computer was found attached to.

(b)(6),(b)(7)(C) also provided SA (b)(6),(b)(7)(C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop.

SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b)(7)(C) provided SA (b)(6),(b)(7)(C) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance showed the individual later identified as Swartz return to the wire closet and remove the netbook

and external hard drive. At approximately 1411 (b)(6),(b)(7)(C) of the MIT Police Department called (b)(6),(b)(7)(C) of the MIT Police 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) responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview Swartz. However, Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7 detained the suspect. An inventory of the backpack the suspect was wearing contained a US passport in the name of Aaron Swartz that was later identified as the suspect. Swartz was transported by Cambridge Police to Cambridge Police headquarters to be booked for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) checked the DHCP logs for computer registrations with containing the word ghost. Ghost-laptop was identified as still being active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(7)(C) mit.edu) an MIT (b)(6),(b)(7)(C) traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b) traveled to the Stratton Student Center and determined that the network drop location ghost-laptop connected to was the Student Information Processing Board office, room 557. (b)(6),(b)(7) contacted (b)(6),(b)(7) (b)(6),(b)(7)(C) to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b)(7 met (b)(6),(b) and (b)(6),(b)(at the student center and found the Acer Aspire netbook and external hard drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves SA (b)(6),(b)(examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Also on 01/06/11, SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters SA (b)(6),(b)(7)(C) met (b)(6),(b)(7)(C) goodcormier.com). (b)(6),(b)(7)(C) informed SA (b)(6),(b)(that he represented Swartz and that his client would not make a statement. Swartz was not cooperative with investigators. Swartz initially refused to provide his name, date of birth and other biographical information.

On 01/10/11, SA (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and AUSA Heymann met at the MIT office of General Counsel with (b)(6),(b)(7)(C) counsel for MIT. The details of that meeting will be contained in a memorandum of interview to be made a part of this case folder.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was arrested by MIT Police Department for violation of Massachusetts General Law Chapter 266 section 18, Breaking and Entering in the daytime for felony.

On 01/06/11, SA (b)(6),(b)(7)(C) called AUSA Steven Heymann to inform him of the investigation of Aaron Swartz.

On 01/07/11, Aaron Swartz was arraigned in Cambridge District court for violation of MGL C266 S18, breaking and entering and his case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

AARON H SWARTZ - DEFENDENT - ARRESTED (STATE)

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	
FBI:	675304KD0
SID:	MA10556559
HT:	5'- 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Pending
1599A:	Pending
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	
ADDRESS:	
EMAIL:	
DATABASE CHECKS:	01/07/11

EXAMS CONDUCTED:

ECSAP: Pending
Poly: N/A
FSD: N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI:	01/07/11
NCIC/NLETS:	01/07/11
CCS/CFT:	01/07/11
LOCAL LE:	01/07/11

Results of database searches have been reported under "Details of Investigation".

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation and judicial action.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: W dnesday, January 05, 2011 6:45 AM
To: (b)(6),(b)(7)(C) Ames, Paul
Cc: (b)(6),(b)(7)(C)
Subject: Ne work Intrusion Summary

Follow Up Flag: Foll w up
Flag Status: Fla ged

Sir,

Notification - we (b)(6),(b)(7)(C) SSS (b)(6),(b)(7)(C) Boston PD and I) were called out to MIT for an assist. The information contained in JSTOR which was the target is valued somewhere in the six figures. A suspect was captured on camera later in the day but at this time he was not identified not apprehended. Investigation continuing.

R/S
(b)(6),(b)(7)(C)

To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Summary

Unauthorized activity on Massa husetts Institute of Technology network

On 01/04/11 I, (b)(6),(b)(7)(C) eceived a call from the (b)(6),(b)(7)(C) @MIT.EDU) of Massachusetts Institute of Technology Police t at an unauthorized computer had been found in a wire closet on MIT grounds; additionally Network Traffic su ested that the computer was being used to download technical journals. The computer was found in a wire c oset of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which contains MIT Bi logical Engineering Department. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu (b)(6),(b)(7)(C) Analyst for MIT stated that on 01/03/11 the library had notified him that someone as downloading large numbers of journals from the library without authorization. Large amounts unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another in ident of excessive downloading. From 01/03/11 to 01/04/11 (b)(6),(b)(7)(was able to trace the activity to a pa icular switch in the wire closet. When (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu) went to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was con ected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1 01. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) reported as stole to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7) and (b)(6),(b)(7) hich are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . P rt 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TC (Transmission Control Protocol) traffic. Cambridge ID Unit techs (b)(6), and (b)(6),(b)(7)(C) processed the scen for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Li ux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile. (b)(6),(b)(7)(C) started a wireshark p cket capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing (b)(6),(b)(7) provided us with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox (Carnegie Mellon University). MIT decided to leave the netbook

running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network.

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Th rsday, January 06, 2011 3:19 PM
To: (b)(6),(b)(7)(C) Ames, Paul; (b)(6),(b)(7)(C)
Cc:
Subject: (b)(6),(b)(7)(C) Re MIT - Bld 16

We have a Aaron Swartz DOB NOV 86 in custody now matching the description of the suspect in the video surveillance breaking in to the w re closet. He is currently being booked at MIT PD HQ for B and E.

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mbridgePolice.Org> (b)(6),(b)(7)(C)
To: Externa (b)(6),(b)(7)(C) cambrid epolice.org; Ames, Paul ambridgePolice.Org> (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) @CambridgePolice.Or >
Cc: (b)(6),(b)(7)(C) mit.edu (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) cambridgepolice.org; comcast.net comcast.net> (BOS)
Sent: Thu Jan 06 13:32:32 201 (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
Subject: RE: MIT - Bld 16

FYI: (b)(6),(b)(7)(C) Agent and I spoke today He was notified by (b)(6),(b)(7)(C) that the perpetrator was caught on tape again and removed the laptop so our ervices were not needed at this time.

Respectfully,
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Thursday, January 06, 20 1 11:13 AM
To: Ames, Paul
Cc: (b)(6),(b)(7)(C) mit.edu'; (b)(6),(b)(7)(C) usss.dhs.gov'; (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) comcast.net (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Fw: MIT - Bld 16

Deputy Superintendent Ames,

The thread below has the statue f the investigation to date.

As I am on a day off today I wou request that CPD Crime Scene personnel hook up with SA (b)(6),(b)(7)(C) and process the newest external har drive for prints that the suspect left the other day after we cleared the scene.

As you'll notice from the thread, he operation is being shut down and we will continue the investigation just not with the computer hooked up an downloading data.

(b)(6),(b)(7)(C) cell phone numbe is (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6) can you call (b)(6),(b)(7)(C) and hook up with her and (b)(6),(b)(7)(C)

Respectfully Submitted,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

From: (BOS) usss.dhs.gov> (b)(6),(b)(7)(C)
To: (b)(6),(b)(7)(C) @MIT.EDU> (b)(6),(b)(7)(C) mit.edu>
Cc: (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu>;
(b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Thu Jan 06 10:00:07 2011
Subject: RE: MIT - Bid 16

I agree with taking the laptop offline today and imaging it. (b)(5)

(b)(5)

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) (b)(6),

From: (C) [mailto (b)(7)(C) @MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External- (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bid 16

All,

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).

(b)(5)

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Packet Capture

Hi there,
I have collected about 70G of network traffic 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.

Thank you

(b)(6),(b)(7)(C)
Network & Infrastructure Services

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

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

DEFENDANT AARON SWARTZ'S SUMMARY OF EXPERT TESTIMONY

Pursuant to Federal Rule of Criminal Procedure 16(b)(1)(C), Defendant Aaron Swartz submits the following summary of expert testimony that may be introduced at trial pursuant to Federal Rules of Evidence 702, 703, and 704.

Alexander C. Stamos

Alexander C. Stamos is a Co-Founder of iSEC Partners, Inc. ("iSEC") headquartered in San Francisco, California with offices in Seattle and New York. iSEC Partners was purchased by NCC Group plc in 2010, and currently Mr. Stamos serves as a Vice President at iSEC as well as the Chief Technology Officer of Artemis Internet, another division of NCC Group. Mr. Stamos is an expert in network access and network security, including the design of secure systems, secure software engineering, and how to respond to breaches of network security. He has been offered as an expert witness in a number of federal and state courts to provide testimony regarding network access and network security. His experience relevant to this assignment includes the past eight years as a Partner at iSEC, two years as the Senior Security Architect at @stake, Inc. a year as a Security Engineer at Loudcloud, Inc., and multiple publications and presentation on the topic of network security. His current resume is attached hereto as Exhibit A.

714134.02

R I F

Particularly in the past eight years at iSEC, Mr. Stamos has defined the services offered by iSEC, and performed as the technical lead on projects for numerous consulting clients, including security testing of the Android and ChromeOS operating systems on behalf of Google, testing of Windows and other products for Microsoft, incident response during the "Aurora" attacks for Autodesk and other victims, system design and testing for McKesson, testing of mobile applications for JP Morgan Chase, and incident response for Davidson & Co, LinkedIn and Charles Schwab. Those consulting projects have involved the design of client computer networks and other enterprise management systems, implementation of security measures on those networks, reviews of those networks' designs and security protocols (including penetration tests), and forensic analysis of computer media generally. He is familiar with various degrees of security that could be applied to a given computer network, depending on the client's needs and means, from relatively minimal security that might be used by a small business or library to maximum security that might be used by a government agency. Likewise, he is familiar with the ways in which a user may gain access to computer networks that have implemented various security measures, from access authorized by a network's design to unauthorized access gained through subverting the network's security measures. He is also familiar with the records created by activity, including access, on a computer network and on individual computers, including a computer's IP address, kernel logs, disk and file metadata, shell history, and similar logging information maintained on and retained by a computer network's servers and other equipment.

At trial of this matter, Mr. Stamos may offer the following opinions:

- At the time of the alleged conduct at issue in this case—September 2010 through January 2011 (the "Relevant Period")—the computer network at the Massachusetts Institute of Technology ("MIT") allowed any person physically present on the MIT campus to gain access either to the MIT wired network (by plugging his or her computer into an Ethernet port connected to the MIT network) or the MIT wireless network (by simply being present within range of that network with a wireless-enabled computer).

- To access the MIT wired network during the Relevant Period, a user did not need to possess or enter an official MIT-issued user identification or password. Instead, the MIT wired network asked a prospective user to enter only a name and an email address. Upon providing that name and email address, anyone on the MIT campus was granted full access to the MIT network.
- Access to the MIT wired network during the Relevant Period did not depend on whether a prospective user entered his or her actual name or a permanent email address associated with that actual name. MIT did not take any steps to check, either at the time of initial access to the network or thereafter, whether a user had entered his or her actual name or a permanent email address associated with that name. Because of MIT's policy of open access, MIT had no practical way of connecting a name given by a user on its network to any person physically present on its campus.
- A user could also use the MIT wired network during the Relevant Period without submitting a name and email address, simply by assigning himself or herself a static IP address. Once a user assigned himself or herself a static IP address, this would allow the user to bypass the portal requesting his or her identifying information. It is not technically challenging for a computer user to determine an appropriate IP address for a given network. Although there were many technologies available to monitor or prevent this practice during late 2010 and early 2011, MIT did not use any of them.
- Access to the MIT wireless network during the Relevant Period did not even prompt the user for any identifying information. In other words, whereas access to the MIT wired network required entry of a name and email address, access to the wireless network did not; that network was available to anyone with a wireless-enabled computer who selected the MIT wireless network from their menu of potential network choices. The name and email prompt required for

access to the MIT wired network easily could have been required for access to the wireless network as well, but MIT chose not to do so.

- Access to the MIT network through the equipment in Room 004 of Building 16 on the MIT campus was no different from access to that network at numerous other access points on the MIT campus. Specifically, a user accessing the MIT network through the equipment in Room 004 was not required to enter any less information, or bypass any security features, compared to a user accessing the network from other access points on campus. As discussed above, a user accessing the MIT wired network from an Ethernet port on the MIT campus did not need to provide his or her name and email address to access the network. Such a user could simply self-assign an IP address and access the network immediately, without providing any identifying information.
- Once a user had gained access to the MIT network during the Relevant Period, as any person physically present on MIT's campus was permitted to do, that user would have full access to the JSTOR database available through the MIT network. Access to the JSTOR database was simple, requiring an MIT network user only to navigate to JSTOR's website (www.jstor.org). Once a user navigated to the JSTOR website, that website did not require entry of a name, user ID, email address, password, or any other identifying information. Neither MIT nor JSTOR required any such information to be submitted in order for an authorized MIT network user to access JSTOR, although it would have been technologically simple for MIT or JSTOR to limit access to specifically identified or authorized individuals. Neither did the JSTOR website display any terms of service or require the user to acknowledge or accept any limitations on use of the JSTOR website or database, even by clicking through a simple dialog box. An MIT network user's level of access to JSTOR during the Relevant Period was the same regardless of whether the user had gained access to the MIT network and the

JSTOR database through a physical or a wireless connection. JSTOR had agreed with MIT, in a written contract between the two entities, to permit any user allowed to access the MIT network to have access to the full JSTOR database on these terms.

- As a technologically sophisticated institution, MIT's policy of open network access cannot have been accidental. MIT made the deliberate choice to design its computer network, and create a network access policy, to permit any person physically present on the MIT campus to access its computer network. MIT's witnesses and documents have confirmed that, as a general matter, both during the Relevant Period and today, MIT's strong preference is to provide as open and free access as possible to its network and all the educational and research databases it licenses. To the extent a content provider such as JSTOR prefers to limit access, including by limiting access to only officially affiliated members of the MIT community (*i.e.*, students, faculty, and staff), MIT's library staff, which is responsible for negotiating the terms of licenses with content providers, will initially resist that request and attempt to persuade the provider to permit broader access, including to guests using the MIT networks.
- Had MIT wanted to implement a different, and stricter, security standard for its network, it easily could have done so, and would have had many options to choose from. MIT could have chosen a relatively modest security protocol permitting access only to users with a MIT-issued username and password, or it could have chosen a stricter protocol requiring a greater level of user verification. Numerous similar educational institutions have faced this same choice regarding the appropriate level of network security. There exists a well-developed industry that is well-positioned to advise such institutions on network security choices and then to implement whatever security protocol the institution chooses. As a

sophisticated consumer (and developer) of technology products and services of all types, MIT would have had access to and understood these options.

- During the Relevant Period, MIT had the ability to restrict access to any database available on its network, including JSTOR, through a system known as "econtrol." The econtrol system had been developed by MIT before the Relevant Period for reasons unrelated to the issues in this case. MIT could have used econtrol to require a prospective user of the JSTOR database to enter identifying information and/or to limit access to certain categories of prospective users. After the first incidents of downloading from JSTOR at issue in this case in September and October 2010, MIT suggested to JSTOR that it implement econtrol to restrict access to the JSTOR database, but JSTOR declined that offer, informing MIT that JSTOR would design its own system for restricting access to its database, and that, in the meantime, MIT should not make any changes affecting access to the JSTOR database through the MIT network. Had econtrol been implemented when MIT initially offered to implement it, the downloading from JSTOR at issue in this case in January 2011 would not have occurred. It would have been simple for MIT or JSTOR to restrict access to the JSTOR database from the MIT network at any time, whether using econtrol or some other protocol.
- As of today, it is no longer possible for any user of the MIT network to access the JSTOR database. It is still possible for any person physically present on the MIT campus to gain access to any MIT network. In the case of the MIT wireless network, anyone on the MIT campus can log on without providing any identifying information. In the case of the MIT wired network, anyone on the MIT campus can log on, either by providing a name and email address (which MIT does not verify) or by self-assigning an available IP address and providing no identifying information. But as of today, once a user has accessed an MIT network, if that user navigates to the JSTOR webpage, they are no longer able to access the

JSTOR database without providing proof of their affiliation with an institution that licenses the JSTOR database. For an MIT-affiliated user (*i.e.*, a student, faculty member, or staff member), access to JSTOR requires selecting MIT from a menu of institutions, and then entering a username and password. It would have been simple for MIT and/or JSTOR to have restricted access in this fashion during the Relevant Period, had MIT and JSTOR chosen to do so.

- A computer's IP address is not a fixed identifier of a specific computer or a particular computer user. Generally, a computer is assigned an IP address upon requesting and obtaining access to a particular computer network. The IP address is assigned by systems designated for this purpose on the network that is accessed. A computer that accesses multiple networks, from different locations, as portable laptop computers often do, may be assigned multiple different IP addresses within a short period of time, depending on the networks being accessed. It is trivially easy for a computer user to change his or her IP address. All major computer operating systems permit the user to enter a particular IP address and attempt to access a network using that address. Changing one's IP address is a common trouble-shooting technique for a computer user who, despite being authorized to access a particular network, may be having difficulty doing so due to technical problems. It is also common for corporate and educational networks to require the user to manually assign themselves IP addresses on some parts of the network. MIT's network supports the use of static IPs in most locations on campus.
- Similarly, a computer's MAC address is not a fixed identifier of a specific computer or a particular computer user. Although a computer is initially assigned a MAC address, all major computer operating systems enable users to change their MAC address, generally with tools included with the operating system. There are also software products on the market that specifically enable users to change their MAC address. Many individuals concerned with their personal

privacy regularly change their MAC address to prevent companies from tracking their activity across multiple networks, and free and commercial products are available to make these changes easier for novice users.

- (b)(6),(b)(7)(C) whom the Government designated as a potential testifying expert on November 20, 2012, submitted a report discussing several issues, including a discussion of a program known as "curl." (b)(6), (b)(7)(Report at 4. The "curl" program is a standard feature present on the Ubuntu Linux operating system. Ubuntu is currently the most popular operating system based on Linux. In other words, a Linux user would not need to separately write or download a "curl" program to use that functionality, which should be present on the operating system already.
- In his report, Mr. (b)(6), (b)(7) also discusses two programs called "keepgrabbing.py" and "serveblocks.py," which were allegedly present on a laptop analyzed by Mr. (b)(6),(b)(7)(C) Report at 5-10. A review of the code making up these programs reveals that these are extremely simple programs that could have been written by a typical high-school computer programming student. These programs utilized standard mechanisms for requesting files to be downloaded from external websites, in the same manner as a web browser such as Internet Explorer or Safari. These tools did not utilize any mechanisms to grant the user any greater or different level of access to the remote systems, including those belonging to JSTOR. In other words, these tools only downloaded files that were normally made available to any user who had already accessed the MIT network and the JSTOR database.
- Mr. (b)(6), (b)(7)(also discusses the "Bash history" of the laptop at issue. (b)(6), (b)(7) Report at 14-15. Bash is a command interpreter installed on operating systems, such as Linux, that permits a computer user to enter commands directed to the operating system. The Bash history is .txt file containing a temporary, partial history of

commands recently entered by the user. Although the number of recent commands retained in the Bash history is adjustable by the user, the Bash history typically contains only the most recent commands entered by the user. Accordingly, a Bash history is not a permanent record of all commands entered into the Bash command interpreter over the life of the computer at issue. Because it is a .txt file, the Bash history can be modified or deleted by a user at any time. Advanced users of Unix-like operating systems often automatically or manually clear their Bash history to only keep text relevant to their most recent activities.

Mr. Stamos's opinions will be based on his education and work experience, as disclosed above and in Exhibit A; on the documents produced by the Government in this case (in particular the MIT emails and documents discussing MIT's systems and its investigation of the incidents at issue in the case); on his personal survey of the current ability of a guest user of the MIT networks to access those networks and the JSTOR database as of December 2012; and on in-person interviews with MIT (b)(6),(b)(7)(C) and MIT network (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) both conducted on December 11, 2012.

Mr. Stamos's expert analysis is still ongoing. Swartz has diligently pursued additional information about the MIT network and the JSTOR database, and access to that network and database during the relevant time period in 2010 and 2011. Most of that information is not yet in Swartz's possession and has not been available for review and consideration by Mr. Stamos. Accordingly, Swartz reserves the right to have Mr. Stamos supplement the above summary of potential testimony upon receiving further information regarding MIT and JSTOR. Swartz will make any supplemental disclosure as soon as reasonably possible. Swartz agrees that, if he submits a supplemental summary of expert testimony, the Government should be permitted to supplement any rebuttal disclosure in response to Mr. Stamos within a reasonable time period.

Swartz has not yet finalized the format of any charts or demonstrative aids that Mr. Stamos may use at trial. To the extent required, he will supplement this disclosure to provide summary information concerning such charts and aids once they have been finalized and pursuant to any governing disclosure deadlines.

In addition to the above affirmative opinions, Mr. Stamos may offer expert testimony in rebuttal to the expert testimony offered by the Government's designated expert (b)(6),(b)(7)(C) and to testimony offered by other Government witnesses.

Dated: December 12, 2012

Elliot R. Peters (admitted *pro hac vice*)
Daniel Purcell (admitted *pro hac vice*)
Keker & Van Nest LLP
633 Battery Street
San Francisco, CA 94111
Tel.: (415) 391-5400
Fax: (415) 397-7188
Email: (b)(6),(b)(7)(C)

Michael J. Pineault
Clements & Pineault, LLP
24 Federal Street
Boston, MA 02110
Tel.: (857) 445-0135
Fax: (857) 366-5404
Email: (b)(6),(b)(7)(C)

Attorneys for Defendant AARON SWARTZ

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest LLP, 633 Battery Street, San Francisco, CA 94111-1809.

On December 12, 2012, I served the foregoing parties with the following document(s):

DEFENDANT AARON SWARTZ'S SUMMARY OF EXPERT TESTIMONY

Carmen M. Ortiz, U.S. Attorney
Stephen Heymann, AUSA
(b)(6),(b)(7)(C) AUSA
(b)(6),(b)(7)(C)
United States Federal Courthouse
1 Courthouse Way, Suite 9200
Boston, MA 02110
(b)(6),(b)(7)(C)
Tel.: (617) 748-3100
Fax: (617) 748-3974

☑ by regular **UNITED STATES MAIL** by placing Original in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest LLP for collection and processing of correspondence for mailing. According to that practice, items are deposited with the United States Postal Service at San Francisco, California on that same day with postage thereon fully prepaid. I am aware that, on motion of the party served, service is presumed invalid if the postal cancellation date or the postage meter date is more than one day after the date of deposit for mailing stated in this affidavit.

☑ by **E-MAIL VIA PDF FILE**, by transmitting on this date via e-mail a true and correct copy scanned into an electronic file in Adobe "pdf" format. The transmission was reported as complete and without error.

Executed on December 12, 2012, at San Francisco, California.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

(b)(6),(b)(7)(C)

Alexander C. Stamos

(b)(6),(b)(7)(C)

Phone
E-mail

(b)(6),(b)(7)(C)

WORK EXPERIENCE

Artemis Internet, Inc. — San Francisco, California
CTO — January 2012 – Current

Artemis is a subsidiary of NCC Group plc and a sister company to iSEC Partners, formed to develop innovative solutions to problems faced by security-sensitive enterprises. As CTO, Alex is the most senior executive at the Artemis subsidiary and is responsible for creating new products and growing this burgeoning business.

- Conceived of and developed the core concept of the .secure top-level-domain.
- Lead the effort to apply for .secure and navigate the ICANN process
- Developed and filed three utility and two provisional patents on core .secure technologies
- Currently building a team to execute the .secure vision

iSEC Partners, Inc. — San Francisco, California
Founder, Partner, Vice President — October 2004 – Current

Co-Founder and Partner specializing in incident response, secure system design and secure software engineering practices. During the early days of the company, was integral in the creation of the company's professional services organization and led internal operations. As the company grew, Alex headed a well-recognized research and evangelism effort while continuing to lead teams on some of iSEC's most challenging projects.

- Built a self-funded 5-person venture into a 40 person firm
- Sold to NCC Group plc for $25M in October 2010
- Concurrent responsibilities in finance, marketing, operations, and technical delivery
- Successfully managed and mentored 7 direct and 24 indirect reports, ranging from recent college graduates to experienced security experts
- Executed iSEC's media relations strategy through interviews, papers and high-profile speaking engagements
- Head of entire Professional Services organization. Successes include:
  - Defined iSEC's initial suite of services
  - Created project delivery and management model
  - Led professional services to excel in all customer satisfaction metrics, including an 80% return revenue rate and dozens of Fortune-500 clients
- Performed as technical lead on numerous consulting projects, including:
  - Design and security reviews of critical enterprise management systems
  - Was lead technical resource on numerous reviews of high profile web applications ranging from innovative startups to established Top-5 banks
  - Led several penetration tests and design reviews of a major commercial operating system
  - Managed a multi-company project to provide security assurance to a major mobile device platform
  - Successfully reverse engineered a widely deployed DRM framework
  - Several critical cryptographic and system security reviews of high-availability financial systems
- Forensics, incident response and expert witness work includes:
  - Rapid incident response and system forensics on a high-profile financial industry intrusion, leading to successful international law-enforcement action
  - Investigation into a remote business intrusion leading to a quick settlement for the victim in a civil lawsuit
  - Workstation and smartphone forensics to investigate internal financial employee misconduct
  - Defensive investigation of patent claims leading to a successful outcome for the respondant
  - Management of data protection and destruction for a high-profile data privacy incident
- Performed original application research and presented at leading conferences, becoming a recognized leader in web and mobile application security
- Created and delivered several acclaimed software security curricula to academic and corporate audiences

@stake, Inc. San Francisco, California
Senior Security Architect/Managing Security Architect September 2002 – September 2004

As a Managing Security Architect at @stake, Alex was responsible for every part of the consulting engagement lifecycle; from sales and project development to delivery and documentation. Performed as a technical lead or contributor on dozens of varied projects, ranging from low-level reverse engineering assignments to high-level network re-designs.

- Discovered several major vulnerabilities during a comprehensive penetration test and code review of a major web server platform
- Served as technical leader on a complex, six person, enterprise-wide network and host assessment
- Performed security assessments of 802.11 equipment using penetration testing and code review, once finding new cryptographic issues in a standards-track protocol
- Completed a solo re-architecture of a major software vendor's ASP network, resulting in greatly improved uptime, security, and manageability

Loudcloud, Inc. Sunnyvale, California
Security Engineer/Senior Security Engineer June 2001 – September 2002

At Loudcloud, was responsible for providing best-of-breed security solutions to Fortune 500, foreign government, and U.S. government customers. Was involved at every step of the security process: architecture, consultation, implementation, auditing, monitoring, incident response, and forensics. Alex also had personal responsibility for managing customer communication, sales support, patch levels, and for building Loudcloud's global security-monitoring infrastructure.

- Designed and implemented a new global Network IDS infrastructure, allowing Loudcloud to provide real-time intrusion detection and alerting across six global datacenters, with a minimum of day-to-day human interaction and maintenance
- Designed and engineered Loudcloud's Security Monitoring System, saving the company seven-figures in outsourcing costs
- From April 2002 on owned primary responsibility for customer and sales support for Loudcloud Security team
- Acted as lead responder to various security incidents, including DDoS attacks, worm infections, and penetrations of production servers

EDUCATION

University of California, Berkeley July 1997 – May 2001
B.S. in Electrical Engineering and Computer Science

- Chancellor, National Merit and Alumni Scholar
- Undergraduate research experience in clustered systems and software security
- Graduate courses in Computer Networking, Security and Cryptography
- Held undergraduate research positions in CS Department and at E.O. Lawrence Berkeley National Laboratory

SELECTED PRESENTATIONS AND PUBLICATIONS

"Vulnerabilities 2.0 in Web 2.0: Next Generation Web Apps from a Hacker's Perspective"
Presented at:

- Black Hat USA 2006
- Web 2.0 Expo 2007
- ACM Reflections/Projections Conference
- Black Hat Japan 2006
- ToorCon 8

"Rich Internet Applications: Blurring the Line Between Desktop and Web Security"
Presented at:

- Black Hat USA 2008
- Web 2.0 Expo Europe
- Defcon 16

"Mobile Web Security"
Presented at:

- California CISO Lecture Series
- ISSA Silicon Valley
- Web 2.0 Expo SF 2009
- *Submitted to* Web 2.0 Expo NY 2009

"Cloud Computing Security: Fuzzy Systems Provide Fuzzy Assurances"
Presented at:

- BlackHat USA 2009
- ISACA Los Angeles and Orange County
- ISACA Silicon Valley Conference
- ISSA-LA Annual Meeting

"Cybercrime Today and Tomorrow's Threats"
Presented at:

- Web 2.0 Expo 2009
- O'Reilly Emerging Technology (ETech) Conference 2009

"Breaking Forensics Software: Weaknesses in Critical Evidence Collection"
Presented at:

- Black Hat USA 2007
- FBI Regional Computer Forensics Laboratory
- High Tech Crimes Investigation Association
- Defcon 15

"Code Scanning Tools: Success and Failure in the Field"
Presented at:

- ISACA Silicon Valley Annual Conference
- USENIX WOOT '08 Bump Session

"Cross Domain Request Forgery and Web Crimes"
Presented at:

- FBI Infraguard - SF Bay Winter Conference

"Attacking Web Services"
Presented at:

- CanSecWest/core06
- Black Hat USA 2005
- Software Security Summit
- InfoWorld SOA Executive Forum
- OWASP App Sec DC 2005

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

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

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

HP USB drive, marked 0045SMKBT1 85102

Case No. 11M-5063-JGD

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Massachusetts
(identify the person or describe the property to be searched and give its location):
HP USB drive, marked 0045SMKBT1 85102 , as described in Attachment A

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

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

YOU ARE COMMANDED to execute this warrant on or before March 10, 2011
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

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

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

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

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

Date and time issued: 2/24/11 3:05 pm

Judge's signature

City and state: Boston, Massachusetts

Chief U.S. Magistrate Judge Judith G. Dein
Printed name and title

R/F

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

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

Certification

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

Date: _____

_____
Executing officer's signature

_____
Printed name and title

RIF

1:14-5063-JGD

Attachment A

HP USB drive, marked 0045SMKBT1 85102

RIF

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds $5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:

A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:

1. JSTOR
2. Massachusetts Institute of Technology
3. Jstor.org
4. Mit.edu
5. IP addresses in the class A domain 18.

B. Records and tangible objects pertaining to the following topics:

1. JSTOR
2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
3. Records and data stored on JSTOR
4. Records and data originating on JSTOR
5. Means of access to JSTOR
6. Computer software capable of making repeated requests for data and records from JSTOR
7. Computer software capable of making repeated downloads of records and data from JSTOR

RIF

media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of the times the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

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

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

RIF

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

D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

1114-5065-160

ATTACHMENT C

PROCEDURES FOR SEIZING COMPUTERS AND RELATED DEVICES

1. Seizing hardware and software

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

2. Returning hardware and software

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

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

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

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

Case No. 11M-5063-JGD

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
HP USB drive, marked 0045SMKBT1 85102, as described in Attachment A

located in the _____ District of Massachusetts, there is now concealed *(identify the person or describe the property to be seized)*:
evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. §1030(a)(5)(A) and 18 U.S.C. § 1343 (wire fraud,) as described in Attachment B

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

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

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

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

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Secret Service Special Agent Michael S. Pickett
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/24/11

Judge's signature

City and state: Boston, Massachusetts

Chief U.S. Magistrate Judge Judith G. Dein
Printed name and title

RIF

11M-5063-JGD

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

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

INTRODUCTION AND AGENT BACKGROUND

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

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

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

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

RIF

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

TECHNICAL TERMS

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

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

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

RIF
762

PROBABLE CAUSE

6. Based on the facts set forth below, there is probable cause to believe that Aaron Swartz:

a. broke into a network interface closet at the Massachusetts Institute of Technology ("MIT");

b. without authorization, accessed MIT's computer network from a network switch within that closet;

c. fraudulently used the appearance of being a MIT student, faculty member or researcher to access JSTOR's extensive electronic library; and

d. fraudulently took from that library over a million journal articles which JSTOR made available by paid subscription or individual purchase.

JSTOR

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

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

9. JSTOR licenses all content under copyright from rights holders and gets permission from them both to digitize the content and make the content available online.[1]

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

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

RIF

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

The Fraudulent Downloads

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

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

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

---

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

[3] A computer's name helps to identify it on a network and can be chosen by a user.

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

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

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

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

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

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

---

[4] The MAC address of the "ghost macbook," 0017f22cb074," is within the range coded by Apple into hardware it manufactures.

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

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

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

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

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

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

RIF

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

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

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

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

---

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

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

RIF

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

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

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual

memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

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

CONCLUSION

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

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

Sworn to under the pains and penalties of perjury,

Michael S. Pickett
Special Agent
United States Secret Service

Subscribed and sworn to before me on February 24, 2011

CHIEF UNITED STATES MAGISTRATE JUDGE

RIF

ATTACHMENT A

PREMISES TO BE SEARCHED

Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601

2.0 terabyte Western Digital hard drive, serial number WMAZA1626675

HP USB drive, marked 0045SMKBT1 85102

RIF

770

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds $5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:

A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:

1. JSTOR
2. Massachusetts Institute of Technology
3. Jstor.org
4. Mit.edu
5. IP addresses in the class A domain 18.

B. Records and tangible objects pertaining to the following topics:

1. JSTOR
2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
3. Records and data stored on JSTOR
4. Records and data originating on JSTOR
5. Means of access to JSTOR
6. Computer software capable of making repeated requests for data and records from JSTOR
7. Computer software capable of making repeated downloads of records and data from JSTOR

RIF

8. MIT's computer network

9. MIT's physical plant

10. Remote electronic storage locations

11. MAC addresses

C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;

D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;

E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100B1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and

F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow remote access and control of the computer equipment

3. evidence of the attachment of other computer hardware or storage

RIF

772

media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of the times the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

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

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

RIF

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

D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

Attachment A

HP USB drive, marked 0045SMKBT1 85102

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds $5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:

A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:

1. JSTOR
2. Massachusetts Institute of Technology
3. Jstor.org
4. Mit.edu
5. IP addresses in the class A domain 18.

B. Records and tangible objects pertaining to the following topics:

1. JSTOR
2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
3. Records and data stored on JSTOR
4. Records and data originating on JSTOR
5. Means of access to JSTOR
6. Computer software capable of making repeated requests for data and records from JSTOR
7. Computer software capable of making repeated downloads of records and data from JSTOR

RIF

8. MIT's computer network

9. MIT's physical plant

10. Remote electronic storage locations

11. MAC addresses

C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;

D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;

E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and

F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow remote access and control of the computer equipment

3. evidence of the attachment of other computer hardware or storage

RIF

media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of the times the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

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

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

RIF

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

D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RIF