

# CCF LAB 2

16.01.2017

Ali Abdulmadzhidov

06:12 - Found image of disk full of evidences.

07:12 - Firstly made some standart procedures.

```
> file primary-disk.dd
primary-disk.dd: x86 boot sector, code offset 0x52, OEM-ID "NTFS  ", sectors/cluster
8, reserved sectors 0, Media descriptor 0xf8, heads 255, hidden sectors 2048, dos < 4.0
BootSector (0x80)
> sha512sum /data/Evidence/primary-disk.dd
61d5573e1ac9e5aaf6da768e6967aa8fcf30907346877d6711ed2894f7d77d76586dc710da3f2516381d87e
7cc4f91b85af74453f985d5663954b6f861c92cef /data/Evidence/primary-disk.dd
> sha512sum /data/Evidence/primary-disk.dd
61d5573e1ac9e5aaf6da768e6967aa8fcf30907346877d6711ed2894f7d77d76586dc710da3f2516381d87e
7cc4f91b85af74453f985d5663954b6f861c92cef /data/Evidence/primary-disk.dd
> md5sum /data/Evidence/primary-disk.dd
2089ac80f6de29a64d53245c28239d385 /data/Evidence/primary-disk.dd
```

07:30 - Mounted image in readonly

```
> mount -o ro /data/Evidence/primary-disk.dd /media
```

07:45 - Started search for typical files \*.pdf, \*.jpg ...





# INTERPOL

CONNECTING POLICE FOR A SAFER WORLD



INTERPOL  
WORLDWIDE



MISSING  
PERSONS



WANTED  
PERSONS

[HOME](#)

[ABOUT INTERPOL](#)

[NEWS AND MEDIA](#)

[MEMBER COUNTRIES](#)

[INTERPOL EXPERTISE](#)

[CRIME AREAS](#)

[Back to Search result](#)



## LEGAL STATUS

Present family name : **BOURNE**  
Forename : **Jason**  
Sex : Male  
Date of birth : unknown  
Place of birth : unknown  
Language spoken : English, French, German,  
Russian, Dutch.  
Nationality : US

## OFFENCES

Categories of Offences : Espionage, Fraud, Thefts, Computer  
and information technology crimes,  
Counterfeiting/forgery  
Wanted by : FBI



## LEGAL STATUS

Present family name : **KREUTZ**  
Forename : **Marie Helena**  
Sex : Female  
Date of birth : unknown  
Place of birth : unknown  
Language spoken : English, German  
Nationality : DE

## OFFENCES

Categories of Offences : Espionage, Thefts  
Wanted by : Interpol

**IF YOU HAVE ANY INFORMATION PLEASE CONTACT**

Your national or local police  
[General Secretariat of INTERPOL](#)



## Alliance Securite, Maritime Division

---

### Explorer of the Seas



### Specifications

- Overall length: 225 Feet
- Beam: 29.5 Feet
- Draft: 11 Feet
- Displacement (fully loaded): 1,850 Tons (approx.)
- Main Engines/Propulsion: MAN (2x 2,775 bhp)
- Cruising Speed: 21 Knots
- Cruising Range: 12,000+ Miles
- Passenger Capacity: 25
- Crew: 18

Knowing that our user's name is "jb", we can suppose that he is Jason Born from USA, but he also has fake passwords. Also we have second subject - Marie Kreutz, from Germany.

In that folder we also have some keystore, but we don't know master password for now.

09:10 - Scanned image for viruses. It is full of trojans and adware.

```

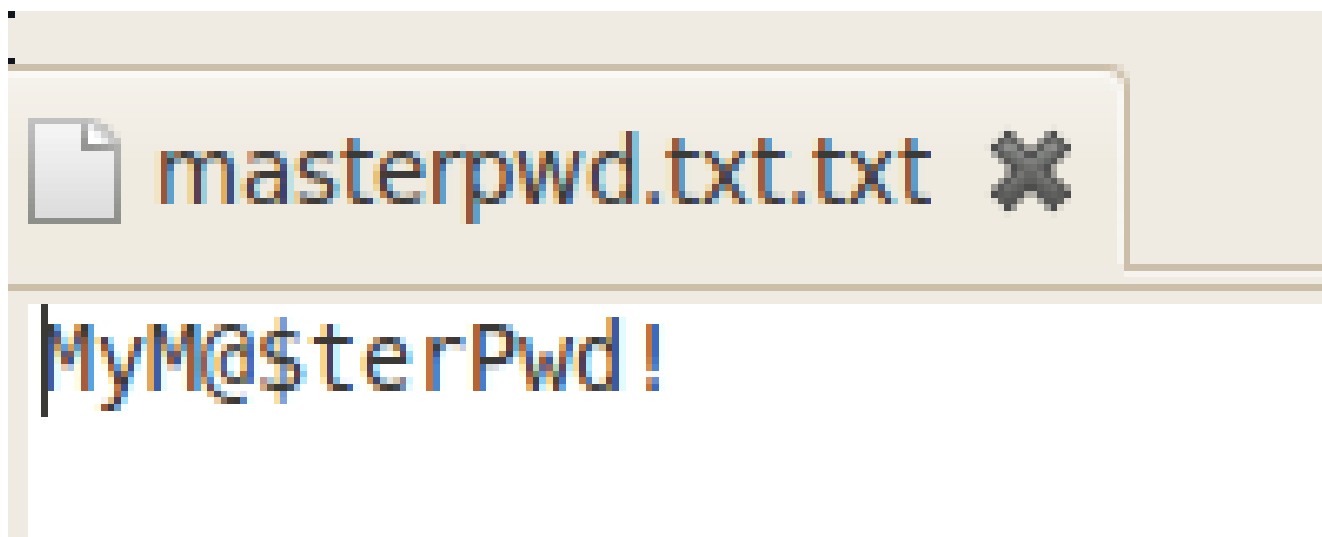
> clamscan -l /data/Evidence/clamscan.log -r -i /media

/media/Program Files/Adobe/Adobe Help Viewer/1.0/ahv.exe: Win.Trojan.Ramnit-7850 FOUND
/media/Program Files/Adobe/Reader 8.0/Reader/Acrofx32.dll: Win.Trojan.Ramnit-5459 FOUND
/media/Program Files/Adobe/Reader 8.0/Reader/adobe_eula.dll: Win.Trojan.Ramnit-5466
FOUND
/media/Program Files/Adobe/Reader 8.0/Reader/icucnv34.dll: Win.Trojan.Ramnit-7189 FOUND
/media/Program Files/BabylonToolbar/BabylonToolbar/1.5.3.17/BabylonToolbarApp.dll:
Win.Adware.BHO-7316 FOUND
/media/Program Files/BabylonToolbar/BabylonToolbar/1.5.3.17/BabylonToolbarEng.dll:
Win.Adware.BHO-7317 FOUND
/media/Program Files/BabylonToolbar/BabylonToolbar/1.5.3.17/BabylonToolbarsrv.exe:
Win.Adware.BHO-7318 FOUND
/media/Program Files/BabylonToolbar/BabylonToolbar/1.5.3.17/BabylonToolbarTlbr.dll:
Win.Adware.BHO-7319 FOUND
/media/Program Files/BabylonToolbar/BabylonToolbar/1.5.3.17/bh/BabylonToolbar.dll:
Win.Adware.BHO-7320 FOUND
/media/Program Files/Common Files/Adobe/Updater5/AdobeUpdater.exe: Win.Trojan.Agent-
1373820 FOUND
/media/Program Files/Java/jre6/bin/jpiexp.dll: Win.Trojan.Ramnit-7017 FOUND
/media/Users/jb/AppData/Local/Microsoft/Windows/Temporary Internet
Files/Content.IE5/6VI08I0R/toolbar[1].exe: Win.Trojan.Agent-973588 FOUND
/media/Users/jb/AppData/Local/Mozilla/Firefox/Profiles/oq7c6xx8.default/Cache/A3E3FCA7d
01: Win.Trojan.Downloader-60957 FOUND
/media/Users/jb/AppData/Local/Temp/2CD5E65E-BAB0-7891-8557-
08019CE30634/MyBabylonTB.exe: Win.Adware.BHO-7320 FOUND
/media/Users/jb/AppData/Local/Temp/BabylonToolbar/BabylonToolbar/1.5.3.17/BabylonToolba
r4ie.exe: Win.Adware.BHO-7320 FOUND
/media/Users/jb/AppData/LocalLow/Sun/Java/jre1.6.0_18/Data1.cab: Win.Trojan.Ramnit-7017
FOUND
/media/Users/mk/Desktop/UPS_INVOICE_TRNR_PLEASE_PRINT.DOC.exe: Win.Trojan.Generic-42
FOUND

----- SCAN SUMMARY -----
Known viruses: 4748140
Engine version: 0.97.5
Scanned directories: 2208
Scanned files: 14822
Infected files: 17
Total errors: 9
Data scanned: 2097.48 MB
Data read: 2894.78 MB (ratio 0.72:1)
Time: 497.601 sec (8 m 17 s)


```


10:10 - Surfing through directories to find something interesting. In /media/Users/jb/AppData/Local/Temp found password for keystore and opened it. Also there're some truecrypt container.






Title	▼	Username	URL	Password	Comments
Images in Filedrop.tc		*****		*****	
Shared Pwd with Pam for Documents		*****		*****	

10:15 - Password for truecrypt container is in ower password store. Excellent.

 **Images in Filedrop.tc**


 **New Entry**


Group:  Documents  Icon: 


Title:

Username:



URL:




Password:  

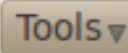
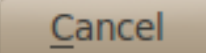
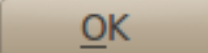
Repeat:  

Quality:  64 Bit

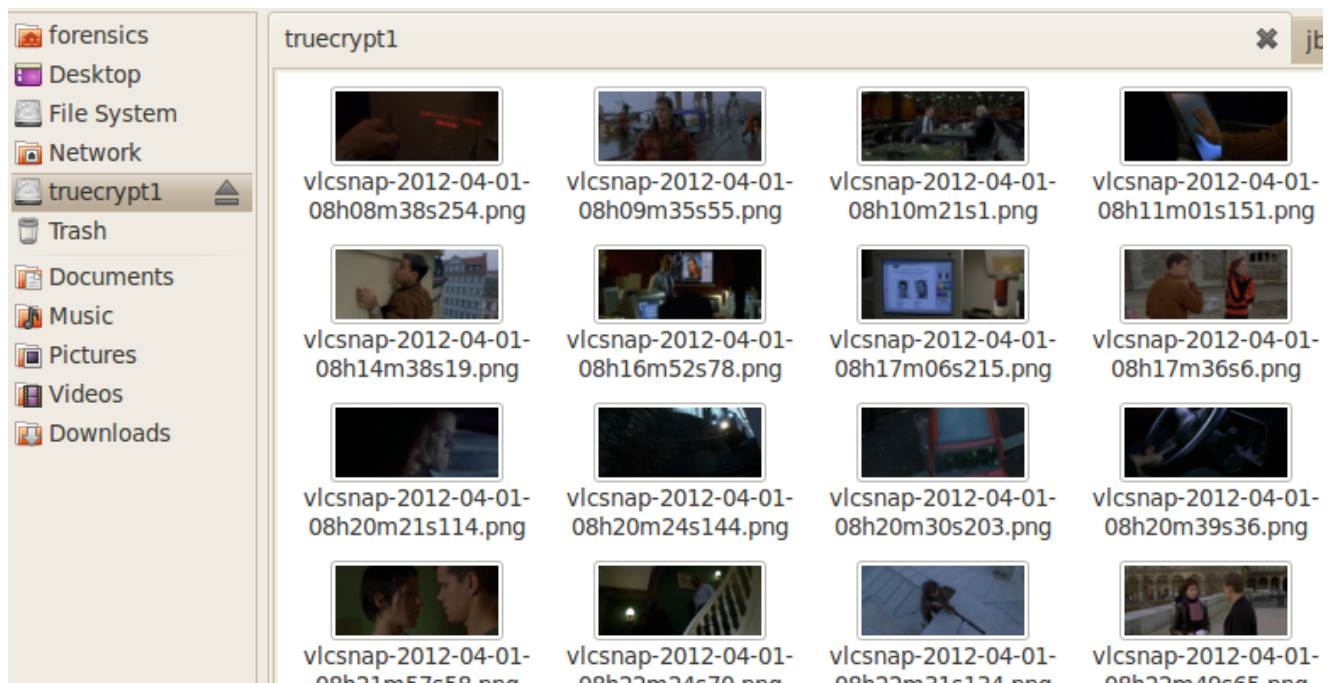
Comment:

Expires:    ☒ Never

Attachment:    

10:20 - In container we have snapshots from some video.



10:25 - Second password references us to commincation with some Pam. Try to find some mail data.

10:30 - In /media/Users/jb/AppData/Roaming/Thunderbird/Profiles/1w94q78u.default/Mail/gmx.ch/ we have local cache for sent and received mail.



From - Fri Mar 30 08:11:43 2012  
X-Account-Key: account1  
X-UIDL: 0lsVCp-1SespNle0L-00lo60  
X-Mozilla-Status: 0003  
X-Mozilla-Status2: 10000000  
X-Mozilla-Keys:  
Return-Path: <marie.kreutzer.8471@hotmail.com>  
Delivered-To: GMX delivery to jason.bourne.7354@gmx.ch  
Received: (qmail invoked by alias); 30 Mar 2012 06:09:06 -0000  
Received: from blu0-omc2-s2.blu0.hotmail.com (EHLO blu0-omc2-s2.blu0.hotmail.com) by mx0.gmx.net (mx066) with SMTP; 30 Mar 2012 08:09:06 +0200  
Received: from BLU0-SMTP113 ([65.55.111.73]) by blu0-omc2-s2.blu0.hotmail.com Thu, 29 Mar 2012 23:09:05 -0700  
X-Originating-IP: [46.253.187.58]  
X-Originating-Email: [marie.kreutzer.8471@hotmail.com]  
Message-ID: <BLU0-SMTP113E5C6DFCAD8F5B2985DAEA7490@phx.gbl>  
Received: from amnesia ([46.253.187.58]) by BLU0-SMTP113.phx.gbl over TLS secured; Thu, 29 Mar 2012 23:08:25 -0700  
From: Marie Kreutzer <marie.kreutzer.8471@hotmail.com>  
To: <jason.bourne.7354@gmx.ch>  
Subject: Look at what I've found  
Date: Fri, 30 Mar 2012 08:04:49 +0200  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
    boundary="-----\_NextPart\_000\_0004\_01CD0E4B.C7A7EE60"  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Windows Mail 6.0.6001.18000  
X-MimeOLE: Produced By Microsoft MimeOLE V6.0.6001.18000  
X-OriginalArrivalTime: 30 Mar 2012 06:08:26.0069 (UTC) FILETIME=[84FDB050:01CD0E4B.C7A7EE60]  
X-GMX-Antivirus: 0 (no virus found)  
X-GMX-Antispam: 0 (Mail was not recognized as spam);  
    Detail=5D7Q89H36p4L00VTXC6D4q0N+AH0PUCnGL2vq0gpaBYL16oitsMrgDt/NQNpSCZFSflc5  
    T+wmVvGhi6RhogBTswdYB2kk3o1a3dIYM6nGXo9ggIQ16vcX/E1T8lzMef54CFr7MdN4qchlN3K8  
    ImsDGoUBZdloilwFKP+MefGwMAcvFnW4l4pww==V1;  
  
-----\_NextPart\_000\_0004\_01CD0E4B.C7A7EE60  
Content-Type: multipart/alternative;  
    boundary="-----\_NextPart\_001\_0005\_01CD0E4B.C7AA5F60"  
  
-----\_NextPart\_001\_0005\_01CD0E4B.C7AA5F60  
Content-Type: text/plain; charset="iso-8859-1"  
Content-Transfer-Encoding: quoted-printable  
  
Hi Jason,  
  
We should hide!  
  
Love,  
Marie

-----\_NextPart\_001\_0005\_01CD0E4B.C7AA5F60  
Content-Type: text/html; charset="iso-8859-1"

From - Fri Mar 30 18:43:56 2012  
X-Account-Key: account1  
X-UIDL: 01Fu3P-1S90Dalk9p-004gQm  
X-Mozilla-Status: 0003  
X-Mozilla-Status2: 10000000  
X-Mozilla-Keys:  
Return-Path: <pamela.landy.1749@hushmail.com>  
Delivered-To: GMX delivery to jason.bourne.7354@gmx.ch  
Received: (qmail invoked by alias); 30 Mar 2012 16:43:09 -0000  
Received: from smtp11.hushmail.com (EHLO smtp11.hushmail.com) [65.39.178.133]  
by mx0.gmx.net (mx060) with SMTP; 30 Mar 2012 18:43:09 +0200  
Received: from smtp11.hushmail.com (localhost.localdomain [127.0.0.1])  
by smtp11.hushmail.com (Postfix) with SMTP id 131FE1CBDEA  
for <jason.bourne.7354@gmx.ch>; Fri, 30 Mar 2012 16:42:59 +0000 (UTC)  
Received: from smtp.hushmail.com (w4.hushmail.com [65.39.178.50])  
by smtp11.hushmail.com (Postfix) with ESMTP  
for <jason.bourne.7354@gmx.ch>; Fri, 30 Mar 2012 16:42:53 +0000 (UTC)  
Received: by smtp.hushmail.com (Postfix, from userid 99)  
id 924F910E2DB; Fri, 30 Mar 2012 16:42:51 +0000 (UTC)  
MIME-Version: 1.0  
Date: Fri, 30 Mar 2012 18:42:48 +0200  
To: jason.bourne.7354@gmx.ch  
Subject: Your identity  
From: pamela.landy.1749@hushmail.com  
Content-Type: multipart/mixed;  
boundary="=\_f80736b668848097f0addb78faa79677"  
Message-Id: <20120330164251.924F910E2DB@smtp.hushmail.com>  
X-GMX-Antivirus: 0 (no virus found)  
X-GMX-Antispam: 0 (BackTrace mail analyze);  
Detail=5D7Q89H36p4L00VTXC6D4q0N+AH0PUCnGL2vq0gpaBYL16oitsMrgDt/NQNpSCZFFjD0y  
97xb7Zpf+wwZnd5ZXNcvLDXR3Wg3wRjdQbwEMh8=V1;

--=\_f80736b668848097f0addb78faa79677  
Content-Type: multipart/alternative;  
boundary="=\_d4cce86eca035748a5e79305c8164af0"

--=\_d4cce86eca035748a5e79305c8164af0  
Content-Transfer-Encoding: 7bit  
Content-Type: text/plain; charset="UTF-8"

Hi Jason,  
See attached. You know the password.  
Best,  
Pam

--=\_d4cce86eca035748a5e79305c8164af0  
Content-Transfer-Encoding: quoted-printable  
Content-Type: text/html; charset="UTF-8"

<span style=3D"font-family: Arial; font-size: 13px;">Hi Jason,<br>See attached. You know the password.<br>Best,<br>Pam<br></span>

From - Fri Mar 30 08:20:08 2012  
X-Mozilla-Status: 0001  
X-Mozilla-Status2: 00800000  
X-Mozilla-Keys:  
Message-ID: <4F755098.9090405@gmx.ch>  
Date: Fri, 30 Mar 2012 08:20:08 +0200  
From: Jason Bourne <jason.bourne.7354@gmx.ch>  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.28) Gecko/20120306 Thunderbird/3.1.20  
MIME-Version: 1.0  
To: Marie Kreutzer <marie.kreutzer.8471@hotmail.com>  
Subject: Re: Look at what I've found  
References: <BLU0-SMTP113E5C6DFCAD8F5B2985DAEA7490@phx.gbl>  
In-Reply-To: <BLU0-SMTP113E5C6DFCAD8F5B2985DAEA7490@phx.gbl>  
Content-Type: multipart/alternative;  
boundary="-----070008070303070703010503"

This is a multi-part message in MIME format.  
-----070008070303070703010503  
Content-Type: text/plain; charset=ISO-8859-1; format=flowed  
Content-Transfer-Encoding: 7bit

That's really bad news. Could you investigate how to get to Naples, IT?  
Miss you,  
Jason

On 3/30/2012 8:04 AM, Marie Kreutzer wrote:  
> Hi Jason,  
> We should hide!  
> Love,  
> Marie

From - Fri Mar 30 18:45:46 2012  
X-Mozilla-Status: 0001  
X-Mozilla-Status2: 00800000  
X-Mozilla-Keys:  
Message-ID: <4F75E328.5030808@gmx.ch>  
Date: Fri, 30 Mar 2012 18:45:28 +0200  
From: Jason Bourne <jason.bourne.7354@gmx.ch>  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.28) Gecko/20120306 Thunderbird/3.1.20  
MIME-Version: 1.0  
To: pamela.landy.1749@hushmail.com  
Subject: Re: Your identity  
References: <20120330164251.924F910E2DB@smtp.hushmail.com>  
In-Reply-To: <20120330164251.924F910E2DB@smtp.hushmail.com>  
Content-Type: multipart/alternative;  
boundary="-----020409040500070102040806"

This is a multi-part message in MIME format.  
-----020409040500070102040806  
Content-Type: text/plain; charset=UTF-8; format=flowed  
Content-Transfer-Encoding: 7bit

Get some rest, Pam.  
You look tired...

On 3/30/2012 6:42 PM, pamela.landy.1749@hushmail.com wrote:  
> Hi Jason,  
> See attached. You know the password.  
> Best,  
> Pam

They want to go to Naples? Also there're are 2 attachments in base64, that can be easily decoded.

This one we've already seen.



# INTERPOL

CONNECTING POLICE FOR A SAFER WORLD



INTERPOL  
WORLDWIDE



MISSING  
PERSONS



WANTED  
PERSONS

[HOME](#)

[ABOUT INTERPOL](#)

[NEWS AND MEDIA](#)

[MEMBER COUNTRIES](#)

[INTERPOL EXPERTISE](#)

[CRIME AREAS](#)

[Back to Search result](#)



## LEGAL STATUS

Present family name : **BOURNE**  
Forename : **Jason**  
Sex : Male  
Date of birth : unknown  
Place of birth : unknown  
Language spoken : English, French, German,  
Russian, Dutch.  
Nationality : US

## OFFENCES

Categories of Offences : Espionage, Fraud, Thefts, Computer  
and information technology crimes,  
Counterfeiting/forgery  
Wanted by : FBI



## LEGAL STATUS

Present family name : **KREUTZ**  
Forename : **Marie Helena**  
Sex : Female  
Date of birth : unknown  
Place of birth : unknown  
Language spoken : English, German  
Nationality : DE

## OFFENCES

Categories of Offences : Espionage, Thefts  
Wanted by : Interpol

## IF YOU HAVE ANY INFORMATION PLEASE CONTACT

Your national or local police  
[General Secretariat of INTERPOL](#)



# INTERPOL

CONNECTING POLICE FOR A SAFER WORLD



INTERPOL  
WORLDWIDE



MISSING  
PERSONS



WANTED  
PERSONS

[HOME](#)

[ABOUT INTERPOL](#)

[NEWS AND MEDIA](#)

[MEMBER COUNTRIES](#)

[INTERPOL EXPERTISE](#)

[CRIME AREAS](#)

[Back to Search result](#)



## LEGAL STATUS

Present family name : **BOURNE**  
Forename : **Jason**  
Sex : Male  
Date of birth : unknown  
Place of birth : unknown  
Language spoken : English, French, German,  
Russian, Dutch.  
Nationality : US

## OFFENCES

Categories of Offences : Espionage, Fraud, Thefts, Computer  
and information technology crimes,  
Counterfeiting/forgery  
Wanted by : FBI



## LEGAL STATUS

Present family name : **KREUTZ**  
Forename : **Marie Helena**  
Sex : Female  
Date of birth : unknown  
Place of birth : unknown  
Language spoken : English, German  
Nationality : DE


## OFFENCES


Categories of Offences : Espionage, Thefts  
Wanted by : Interpol




**IF YOU HAVE ANY INFORMATION PLEASE CONTACT**

Your national or local police  
[General Secretariat of INTERPOL](#)

But here is something new. treadstone.zip archive. It is crypted. But we remember, that we have password for communicatoin with Pam.

 **Shared Pwd with Pam for Documents**


 **New Entry**


Group:  Documents  Icon: 

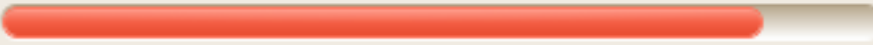
Title:

Username:



URL:




Password:  

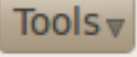
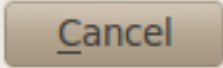
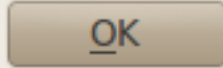
Repeat:  

Quality:  112 Bit

Comment:

Expires:    ☒ Never

Attachment:    

It absolutely fits here. In pdf we have some more data about JB. His real name is Wasiliy Popov and he is from Saint Petersburg. Also he is CIA agent.



**TOP SECRET**

**Project: Treadstone**



**Applicant: POPOV, Wassili**



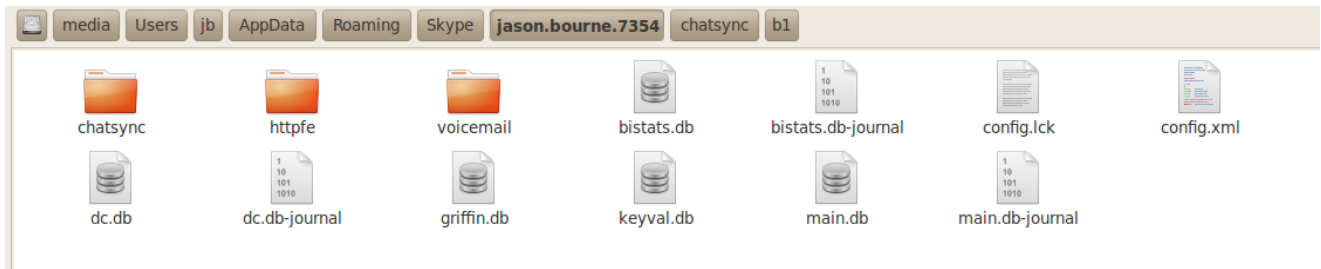
**Surname:** POPOV  
**Name:** Wassili  
**Date of Birth:** 4/1/1972  
**Place of Birth:** Saint Petersburg  
**Nationality:** Russian  
**Gender:** Male  
**Current Whereabouts:** Unknown

**Used Aliases:**

- BOURNE, Jason (US)
- WEBB, David (US)
- KANE, John Michael (UK)
- DE PIENTO, Gilberto (FR)



11:01 - Digging deeper into cache files leads me to skype caches. Got some usernames and message parts.



```
Hi Jason. Still awake?  
Hk+Y,  
VL}/l  
azm!  
Dup. Still some work to do....
```

```
>M.b  
marie.kreutzer.8471  
jason.bourne.7354  
marie.kreutzer.8471
```

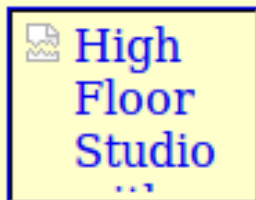
11:30 - At last go to browser's cache.

In mozilla's cache we have some interesting images of map (Paris, Berlin, Naples, New York) and driver's site screenshot. Let's start from drivers. Looking on them we can suppose that suspect has Lenovo IdeaPad notebook.

**Driver Name :** Synaptics Pointing Device Driver  
**Family :** IdeaPad S9,IdeaPad S10  
**File Size :** 26.2 MB  
**Driver Version :** 13.2.4.12  
**File Format :** exe  
**Release Date :** 2009-11-03  
**Applicable OS :** Windows 7 32bit,Windows 7 64bit  
**Manufacturer :** Synaptics  
**Last modified date :** 2009-11-03

Also suspect tried to find some place to stay in several cities. New York mosly.

### [Your Apt Listing Here!](#)



#### ***Off Market***

25 Tudor City Place Apt 2008  
Studio, [Roof Terrace](#)  
*\$1700. per month Utilities Included*



5 Tudor City Place Apt 834  
River View, [Fitness Center](#)  
*\$1700. per month includes utilities*



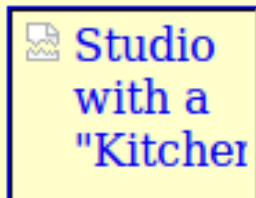
#### ***Rented***

**One Bedroom** 45 Tudor City  
Place 2010  
Mint Unfurnished, Hi Floor Views,  
*\$2500. per month utilities incl.*[Roof Terrace](#)



### **Rented**

5 Tudor City Place 731 December  
1st  
River View, Fitness Center, AC  
\$2400. per month includes utilities



### **Rented Sept 2011**

45 Tudor City Place Apt 503  
Roof Terrace, Kitchen  
\$1650. per month includes utilities



### **Rented Sept 2011**

5 Tudor City Place Apt 930  
River View, Fitness Center, AC  
\$1700. per month includes utilities

Here we have list of visited sites from Mozilla and IE.

TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME	DIRECTORY	H
HTTP HEADERS						
URL	Visited: jlb@http://media.instdn.com/xmlcdn/emulecom/en/index.html					0
3/30/2012 17:54:00		03/30/2012 17:54:00				
URL	Visited: jlb@https://apps.skype.com/friendfinder/?action=search					03/30/20
12 00:03:44		03/30/2012 00:03:44				
URL	Visited: jlb@http://info.babylon.com/setup/setup.html?no_policy=1&lang=10					
3/30/2012 17:54:28		03/30/2012 17:54:28				
URL	Visited: jlb@file:///C:/Users/jlb/Documents/mypasswd.kdb					03/31/2012 09:59
:49		03/31/2012 09:59:49				
URL	Visited: jlb@http://www.metainstaller.com/emule/template.php					03/30/20
12 17:53:59		03/30/2012 17:53:59				
URL	Visited: jlb@file:///E:/KeePassX-0.4.3-win32.zip					03/29/2012 23:17:49
3/29/2012 23:17:49						
URL	Visited: jlb@file:///E:/Jungfrau.joch.jpg					04/01/2012 10:06:22
12 10:06:22						
URL	Visited: jlb@file:///C:/Users/jlb/Documents/wanted.png					03/30/2012 08:12
:36		03/30/2012 08:12:36				
URL	Visited: jlb@file:///C:/Users/jlb/Desktop/pass_uk_kane.pdf					03/30/20
12 11:33:38		03/30/2012 11:33:38				
URL	Visited: jlb@file:///F:/vlcsnap-2012-04-01-08h08m38s254.png					04/01/20
12 08:55:45		04/01/2012 08:55:45				
URL	Visited: jlb@https://channel.skype.com/facebook/channel/?uiversion=5.0.0.156&language=en					03/30/2012 07:43:41
03/30/2012 07:43:41						

