

# **TALES FROM THE CRYPT!**

*No Keys? No Problem!*

*Hal Pomeranz*

*Deer Run Associates*

# THE HORROR!

Suspect use of TrueCrypt volumes!

**GASP!**

No way to access data!

**OH NO!**

What artifacts exist in unencrypted OS?

Not an academic question

May force production of documents that can be named with "reasonable particularity"

*US v Hubbell (2000), re Boucher (2009)*

# **WINDOWS AUTOPSY!**

Is TrueCrypt installed?

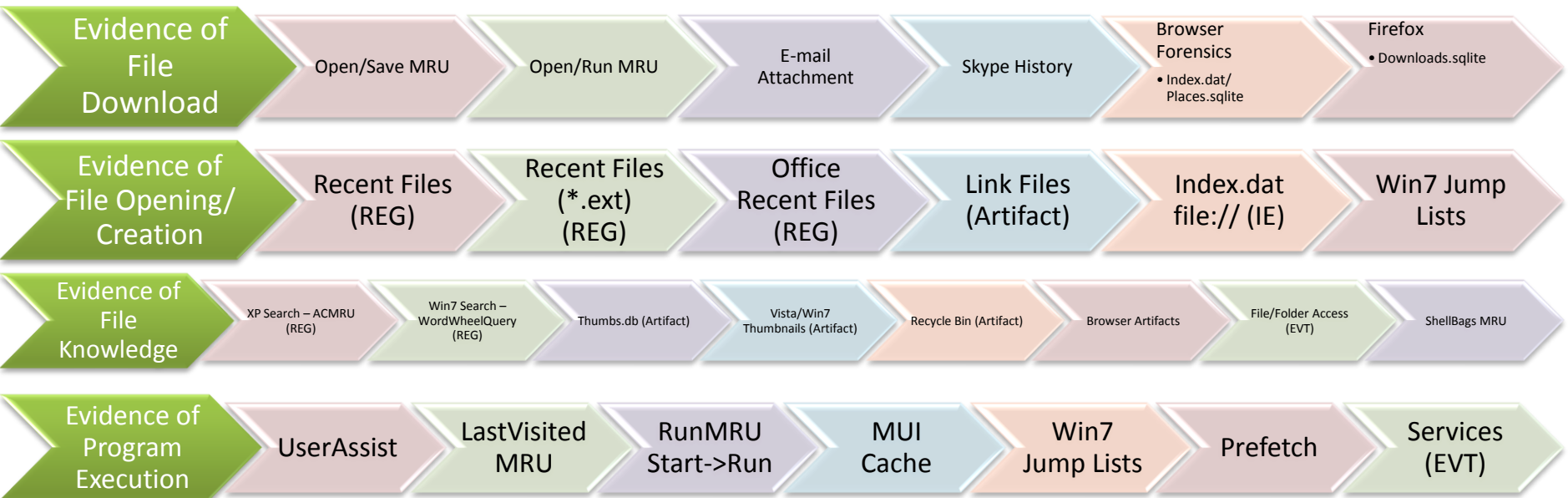
Who installed it?

Are TrueCrypt volumes present?

Were TrueCrypt volumes mounted?

What was in the volumes?

# SECRETS OF THE FORENSICATORS!



# IS IT INSIDE THE HOUSE?!?

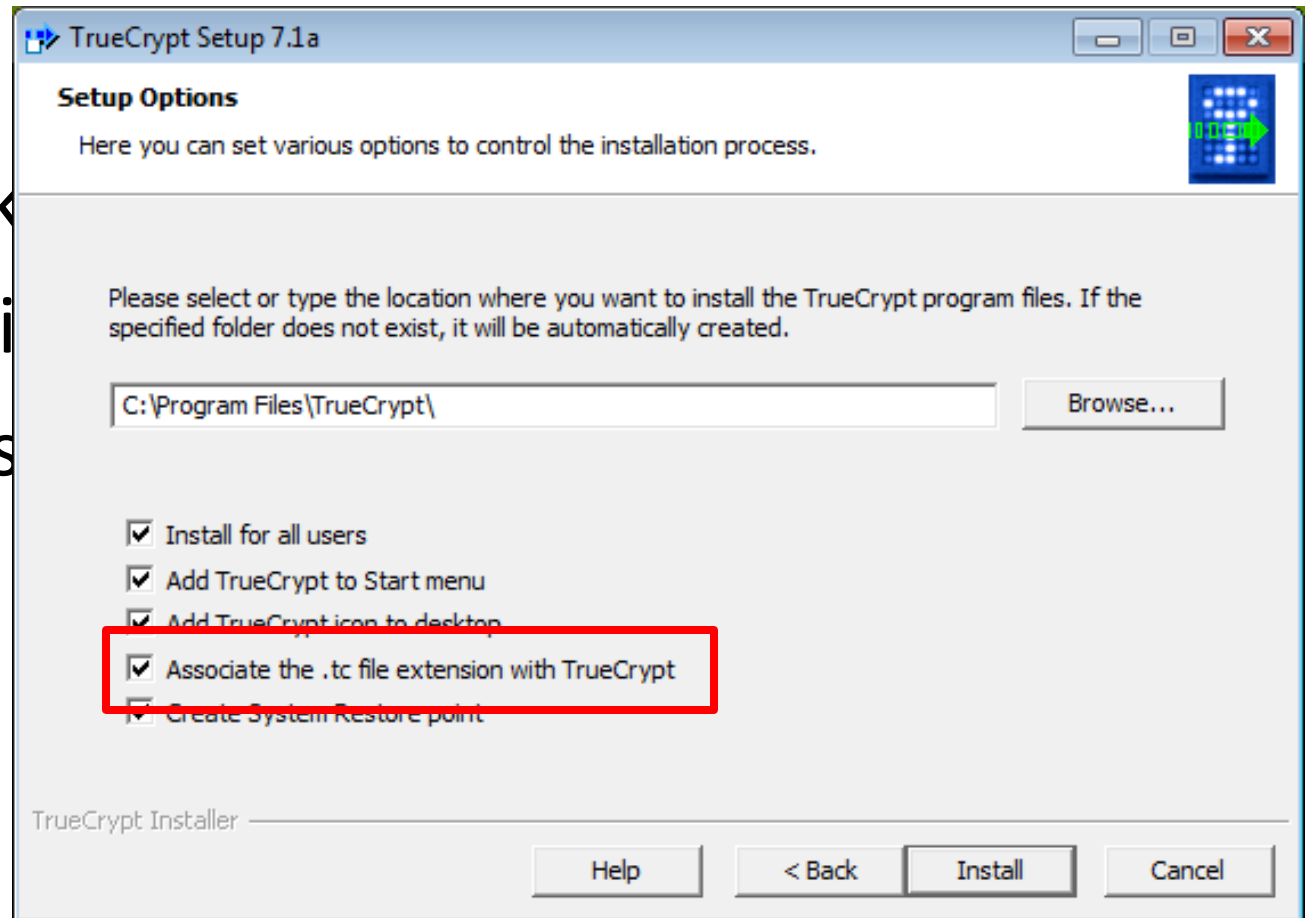
TrueCrypt installation directories

Registry –

Uninstall k

Normally i

Associates



# WHERE DID IT COME FROM?!?

NetAnalysis v1.52 - Forensic Internet History Analysis - [NetAnalysis-TrueCrypt]

File Filter Searching Tools Bookmarks Reports Audit View Column Help

GMT Standard Time [UTC +0000]

Last Visited [Local]	Hits	User	URL
<input type="checkbox"/> 2012-06-24 15:36:08 Sun	1	Hal Pomeranz	http://www.truecrypt.org/dl
<input type="checkbox"/>	-		http://www.truecrypt.org/df4edd72d
<input type="checkbox"/> 2012-06-24 07:36:32 Sun	1	Hal Pomeranz	http://www.truecrypt.org/download/transient/e9a09a5e3c/TrueCrypt%20Setup%207.1a.exe
<input type="checkbox"/> 2012-06-24 15:36:32 Sun	2	Hal Pomeranz	http://www.truecrypt.org/download/transient/e9a09a5e3c/TrueCrypt%20Setup%207.1a.exe
<input type="checkbox"/> 2012-06-24 07:36:32 Sun	1	Hal Pomeranz	http://www.truecrypt.org/download/transient/e9a09a5e3c/TrueCrypt%20Setup%207.1a.exe
<input type="checkbox"/> 2012-06-24 15:36:32 Sun	2	Hal Pomeranz	http://www.truecrypt.org/download/transient/e9a09a5e3c/TrueCrypt%20Setup%207.1a.exe
<input type="checkbox"/> 2012-06-24 07:35:57 Sun	1	Hal Pomeranz	http://www.truecrypt.org/downloads
<input type="checkbox"/> 2012-06-24 15:39:38 Sun	9	Hal Pomeranz	http://www.truecrypt.org/downloads
<input type="checkbox"/> 2012-06-24 07:35:57 Sun	1	Hal Pomeranz	http://www.truecrypt.org/downloads
<input type="checkbox"/> 2012-06-24 15:35:57 Sun	2	Hal Pomeranz	http://www.truecrypt.org/downloads
<input type="checkbox"/> 2012-06-24 15:35:57 Sun	1	hal pomeranz	http://www.writeblocked.org/media/system/css/system.css
<input type="checkbox"/> 2012-06-24 15:35:57 Sun	1	hal pomeranz	http://www.writeblocked.org/media/system/images/livemarks.png

www.digital-detective.co.uk | Cache | S:\AppData\Local\Microsoft\Windows\...\index.dat | FO: 47104 | URL Records: 6915

# WHO DID THIS TO US?!?

Registry Decoder - Digital Forensics Solutions

File Reporting

File View Search Plugins Path Analysis Timeline **User Assist**

Results for running User Assist against Z:\TrueCrypt Testing\registry-hives\WTUSER.DAT

	User Assist Value	SessionID	Run Count	Last Run Date
177	C:\Users\Hal Pomeranz\Downloads\TrueCrypt Setup 7.1a.exe		1	2012/06/24 07:42:39 UTC
178	TrueCryptFoundation.trueCrypt		5	2012/06/24 08:22:03 UTC
179	C:\Users\Hal Pomeranz\Downloads\PidginPortable_2.10.4.paf.exe		1	2012/06/24 08:30:39 UTC
180	C:\Users\Hal Pomeranz\Downloads\Firefox Setup 13.0.1.exe		1	2012/06/24 08:31:35 UTC
181	X:\PidginPortable\PidginPortable.exe		2	2012/06/24 08:52:10 UTC
182	X:\PidginPortable\App\Pidgin\pidgin-portable.exe		0	
183	X:\Firefox\firefox.exe		5	2012/06/24 08:49:56 UTC
184	E6C59D5826C5DF		0	
185	Microsoft.AutoGenerated.{9BD3D1D4-4FDF-4047-715A-CDD90A5D7EC5}		3	2012/06/24 09:12:15 UTC
186	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\TrueCrypt\TrueCrypt.exe		1	2012/06/24 08:55:43 UTC

Report Format Report Filename

CSV

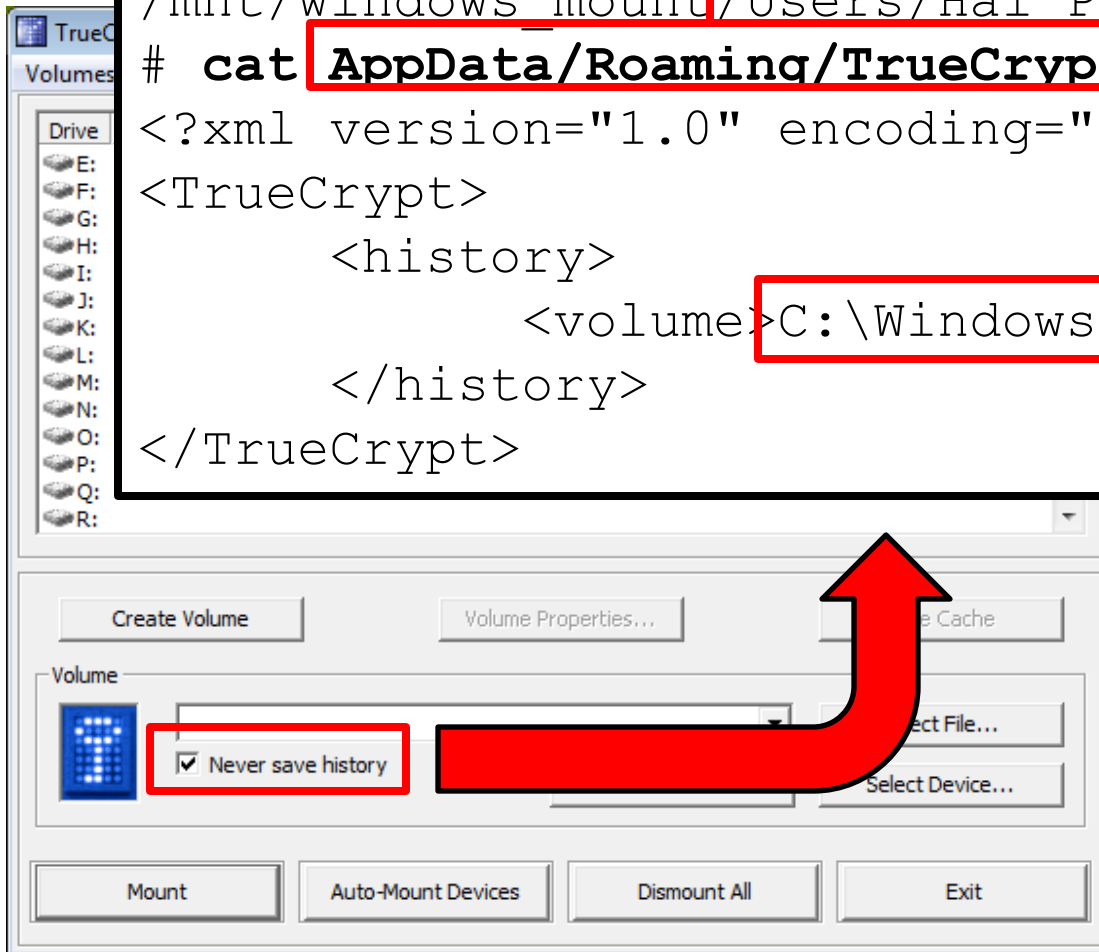
# SEARCHING FOR AN ENIGMA!

```
# tchunt -d /mnt/windows_mount
Suspect_File:      /mnt/windows_mount/Windows/setuplog.tc
#
# rip.pl -f system -r /mnt/...System32/SYSTEM >system.txt
# less system.txt
...
MountedDevices
LastWrite time = Sun Jun 24 16:15:17 2012Z
...
Device: TrueCryptVolumeX
      \??\Volume{1586675a-b25e-11e1-aebd-000c2976f352}
      \DosDevices\X:
...
```

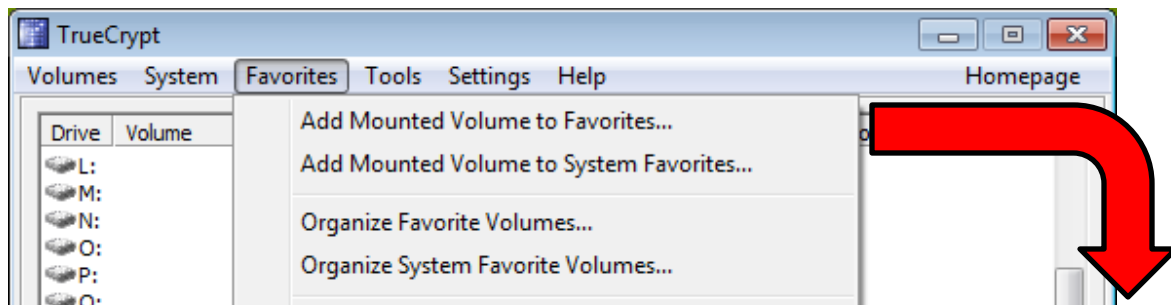


# HISTORY OF ABUSE!

```
# pwd
/mnt/windows_mount/Users/Hal Pomeranz
# cat AppData/Roaming/TrueCrypt/History.xml
<?xml version="1.0" encoding="utf-8"?>
<TrueCrypt>
  <history>
    <volume>C:\Windows\setuplog.tc</volume>
  </history>
</TrueCrypt>
```



# PLAYING FAVORITES!



```
# cat AppData/Roaming/TrueCrypt/Favorite\ Volumes.xml
<?xml version="1.0" encoding="utf-8"?>
<TrueCrypt>
  <favorites>
    <volume mountpoint="X:\"
            label="Sekrit Stash"
            mountOnLogOn="1"
            openExplorerWindow="1">
      C:\Windows\setuplog.tc
    </volume>
  </favorites>
</TrueCrypt>
```

# **BUT WHAT'S INSIDE?!?**

Could be files!

Could be programs!

# SECRET FILES!

NetAnalysis v1.52 - Forensic Internet History Analysis - [NetAnalysis-TrueCrypt]

File Filter Searching Tools Bookmarks Reports Audit View Column Help

GMT Standard Time [UTC +0000]

	Last Visited [Local]	Hits	User	URL
<input type="checkbox"/>	2012-05-13 19:57:49 Sun	1	Hal Pomeranz	file:///S:/xp-tdungan-10.3.58.7/timeline/timeline.csv
<input type="checkbox"/>	2012-05-13 22:24:04 Sun	3	Hal Pomeranz	file:///S:/xp-tdungan-10.3.58.7/timeline/timeline.xlsx
<input type="checkbox"/>	2012-06-24 09:02:14 Sun	1	Hal Pomeranz	file:///X:/MyStuff/kitteh-porn.jpg
<input type="checkbox"/>	2012-06-24 17:02:14 Sun	1	Hal Pomeranz	file:///X:/MyStuff/kitteh-porn.jpg
<input type="checkbox"/>	2012-06-24 09:03:16 Sun	1	Hal Pomeranz	file:///X:/MyStuff/Passwords%20Are%20Everywhere!.pdf
<input type="checkbox"/>	2012-06-24 17:03:16 Sun	1	Hal Pomeranz	file:///X:/MyStuff/Passwords%20Are%20Everywhere!.pdf
<input type="checkbox"/>	2012-06-24 09:02:20 Sun	1	Hal Pomeranz	file:///X:/MyStuff/Passwords%20Are%20Everywhere!.pptx
<input type="checkbox"/>	2012-06-24 17:02:20 Sun	1	Hal Pomeranz	file:///X:/MyStuff/Passwords%20Are%20Everywhere!.pptx
<input type="checkbox"/>	2012-06-24 09:02:02 Sun	1	Hal Pomeranz	file:///X:/MyStuff/Secret%20Plans%20for%20World%20Domination.docx
<input type="checkbox"/>	2012-06-24 17:02:02 Sun	1	Hal Pomeranz	file:///X:/MyStuff/Secret%20Plans%20for%20World%20Domination.docx
<input type="checkbox"/>	2012-06-24 08:52:48 Sun	1	Hal Pomeranz	file:///X:/PidginPortable/help.html
<input type="checkbox"/>	2012-06-24 16:52:48 Sun	1	Hal Pomeranz	file:///X:/PidginPortable/help.html
<input type="checkbox"/>	2012-05-26 04:42:02 Sat	2	Hal Pomeranz	file:///Z:/Class%20Files/precooked-day6-files/win7-64-nfury/timeline/win7-64-nfury-supertimeline-from-20120402.xlsx
<input type="checkbox"/>	2012-05-26 02:07:21 Sat	1	Hal Pomeranz	file:///Z:/Class%20Files/precooked-day6-files/win7-64-nfury/timeline/win7-64-nfury-supertimeline-from-20120402.xlsx
<input type="checkbox"/>	2012-06-13 17:53:36 Wed	2	Hal Pomeranz	Host: Computer
<input type="checkbox"/>	2012-06-04 14:59:36 Mon	1	Hal Pomeranz	Host: Computer
<input checked="" type="checkbox"/>	2012-06-20 04:40:49 Wed	1	Hal Pomeranz	Host: Computer
<input type="checkbox"/>	2012-06-22 13:08:13 Fri	1	Hal Pomeranz	Host: Computer

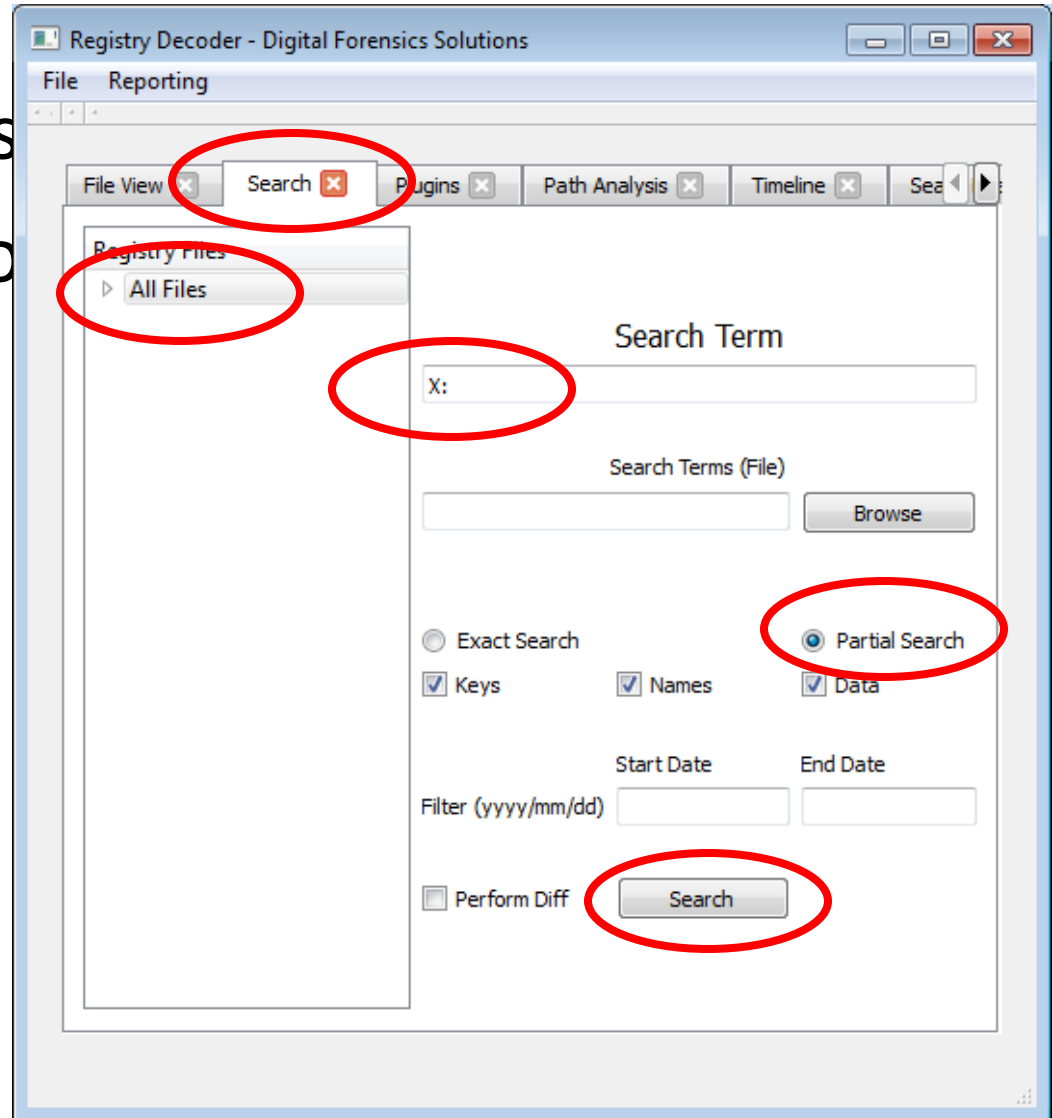
www.digital-detective.co.uk      Daily      S:\AppData\Local\Microsoft\Windows\History\... \index.dat      FO: 20736      URL Records: 6915

# MISSING LNKS!

```
# pwd
/mnt/windows_mount/Users/Hal Pomeranz
# cd AppData/Roaming/Microsoft/
# for i in */Recent/*; do
    echo ===== $i
    lnkinfo "$i" | grep -F X:\\
done
...
===== Windows/Recent/MyStuff.lnk
    Local path          : X:\MyStuff
===== Windows/Recent/Passwords...!.pptx.lnk
    Local path          : X:\MyStuff\Passwords...!.pptx
    Working directory  : X:\MyStuff
===== Windows/Recent/PidginPortable.lnk
    Local path          : X:\PidginPortable
...
```

# REGISTERED OFFENDERS!

Confirm LNK findings  
Drive letter search to



# EXECUTIONS!

Registry Decoder - Digital Forensics Solutions

File Reporting

File View Search Plugins Path Analysis Timeline **User Assist**

Results for running User Assist against Z:\TrueCrypt Testing\registry-hives\NTUSER.DAT

	UserAssist Value	SessionID	Run Count	Last Ran Date
177	C:\Users\Hal Pomeranz\Downloads\TrueCrypt Setup 7.1a.exe		1	2012/06/24 07:42:39 UTC
178	TrueCryptFoundation.TrueCrypt		5	2012/06/24 08:22:03 UTC
179	C:\Users\Hal Pomeranz\Downloads\PidginPortable_2.10.4.paf.exe		1	2012/06/24 08:30:39 UTC
180	C:\Users\Hal Pomeranz\Downloads\Firefox Setup 13.0.1.exe		1	2012/06/24 08:31:35 UTC
181	X:\PidginPortable\PidginPortable.exe		2	2012/06/24 08:52:10 UTC
182	X:\PidginPortable\App\Pidgin\pidgin-portable.exe		0	
183	X:\Firefox\firefox.exe		5	2012/06/24 08:49:56 UTC
184	E6C59D5826C5DF		0	
185	Microsoft.AutoGenerated.{9BD3D1D4-4FDF-4047-715A-CDD90A5D7EC5}		3	2012/06/24 09:12:15 UTC
186	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\TrueCrypt\TrueCrypt.exe		1	2012/06/24 08:55:43 UTC

Report Format Report Filename

CSV

# PREFETCHED IN STONE!

```
# cd /mnt/windows_mount/Windows/Prefetch
# pf -v FIREFOX.EXE-133F59BF.pf | grep TRUECRYPTVOLUMEX
...
036 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX\FIREFOX.EXE
...
086 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX PROFILE\PREFS.JS
088 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX PROFILE\EXT...INI
090 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX PROFILE\PERM...
091 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX PROFILE\SESSION...
097 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX PROFILE\LOCAL...
126 : \DEVICE\TRUECRYPTVOLUMEX\FIREFOX PROFILE\SEARCH...
```



# **BRUTE FORCE AND TREACHERY!**

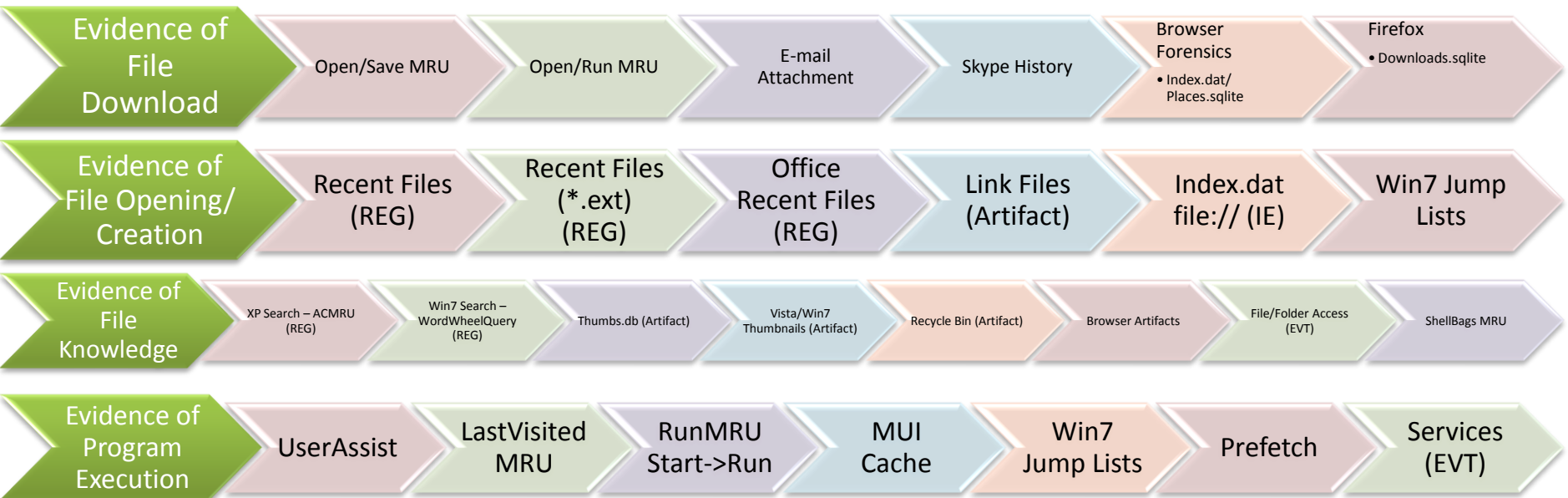
Got memory? (or hiberfil.sys)

Passware – <http://www.lostpassword.com/>

Got (lots of) time?

Truecrack – <http://code.google.com/p/truecrack/>

# DON'T GIVE UP!



# **YOU SURVIVED!**

Any final questions?

Thanks for listening!

Please fill out your evals!

Hal Pomeranz

hal@deer-run.com

Deer Run Associates

@hal\_pomeranz

<http://www.deer-run.com/~hal/>