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?

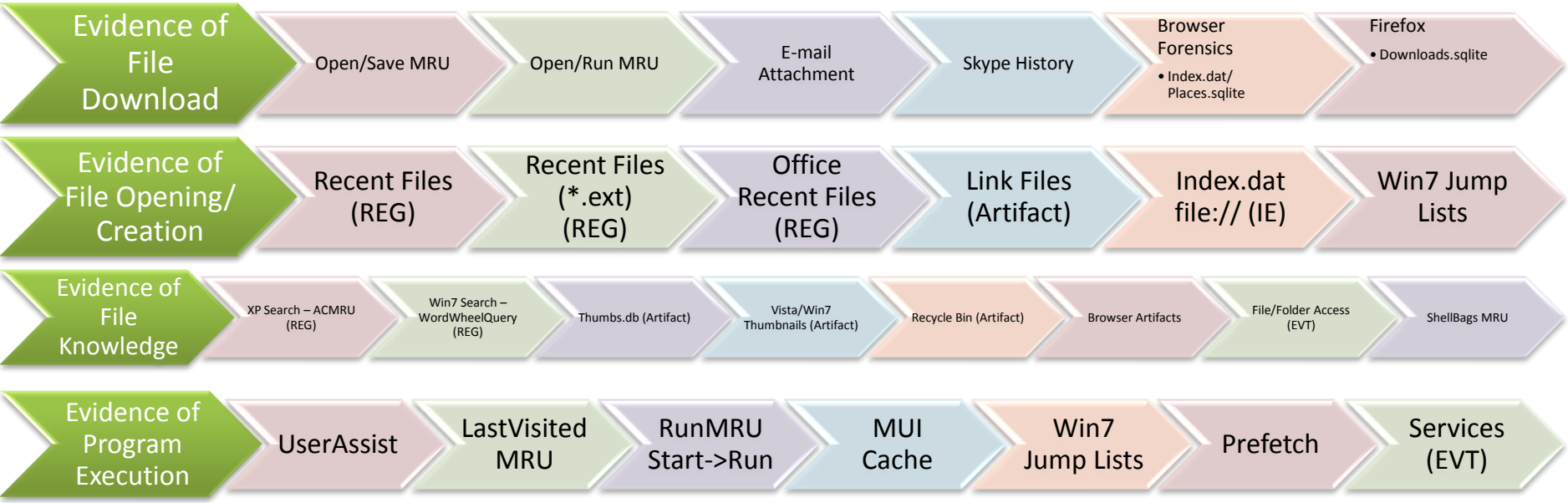
Who installed it?

Are TrueCrypt volumes present?

Were TrueCrypt volumes mounted?

What was in the volumes?

SECRETS OF THE FORENSICATORS!

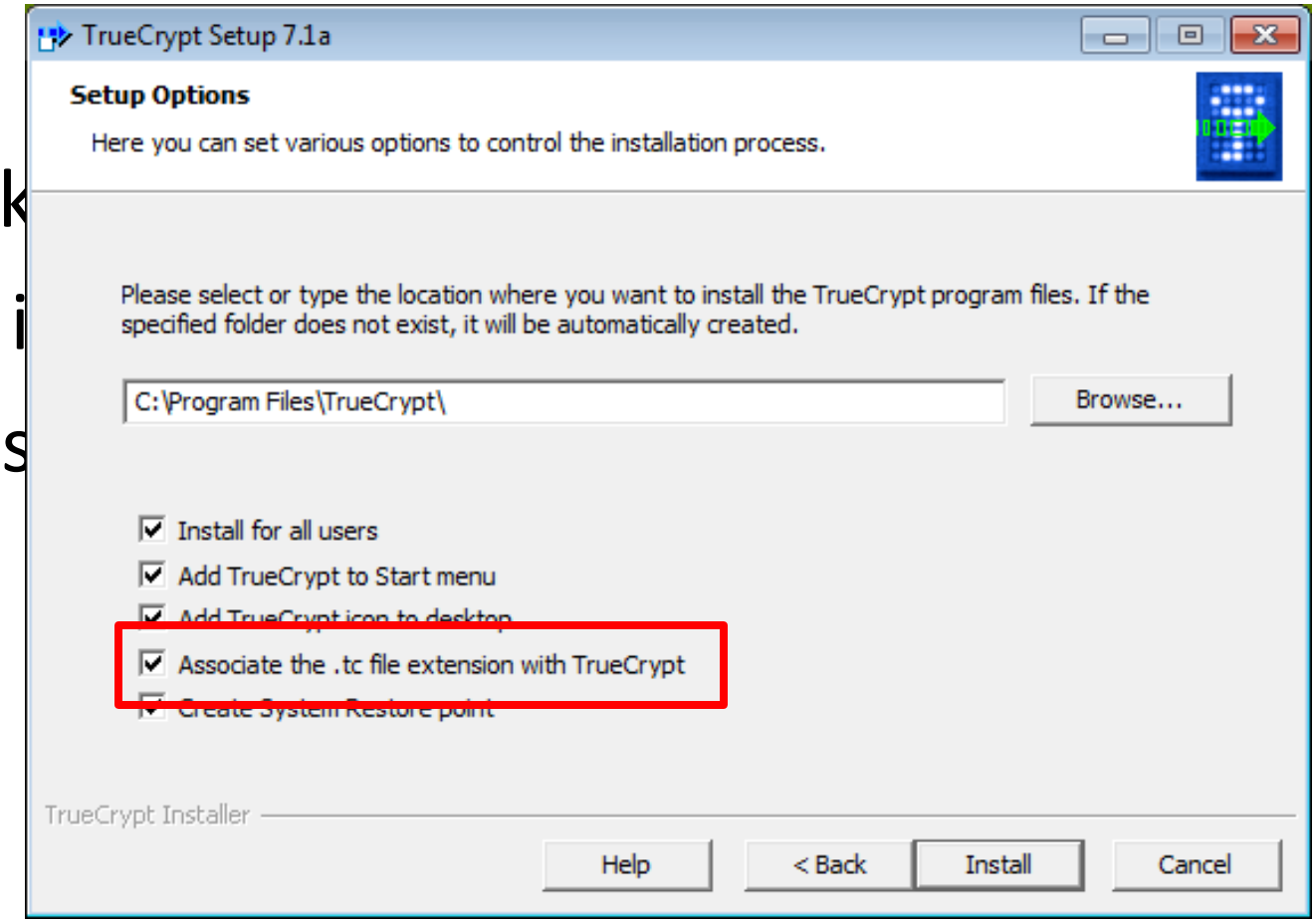


IS IT INSIDE THE HOUSE?!?

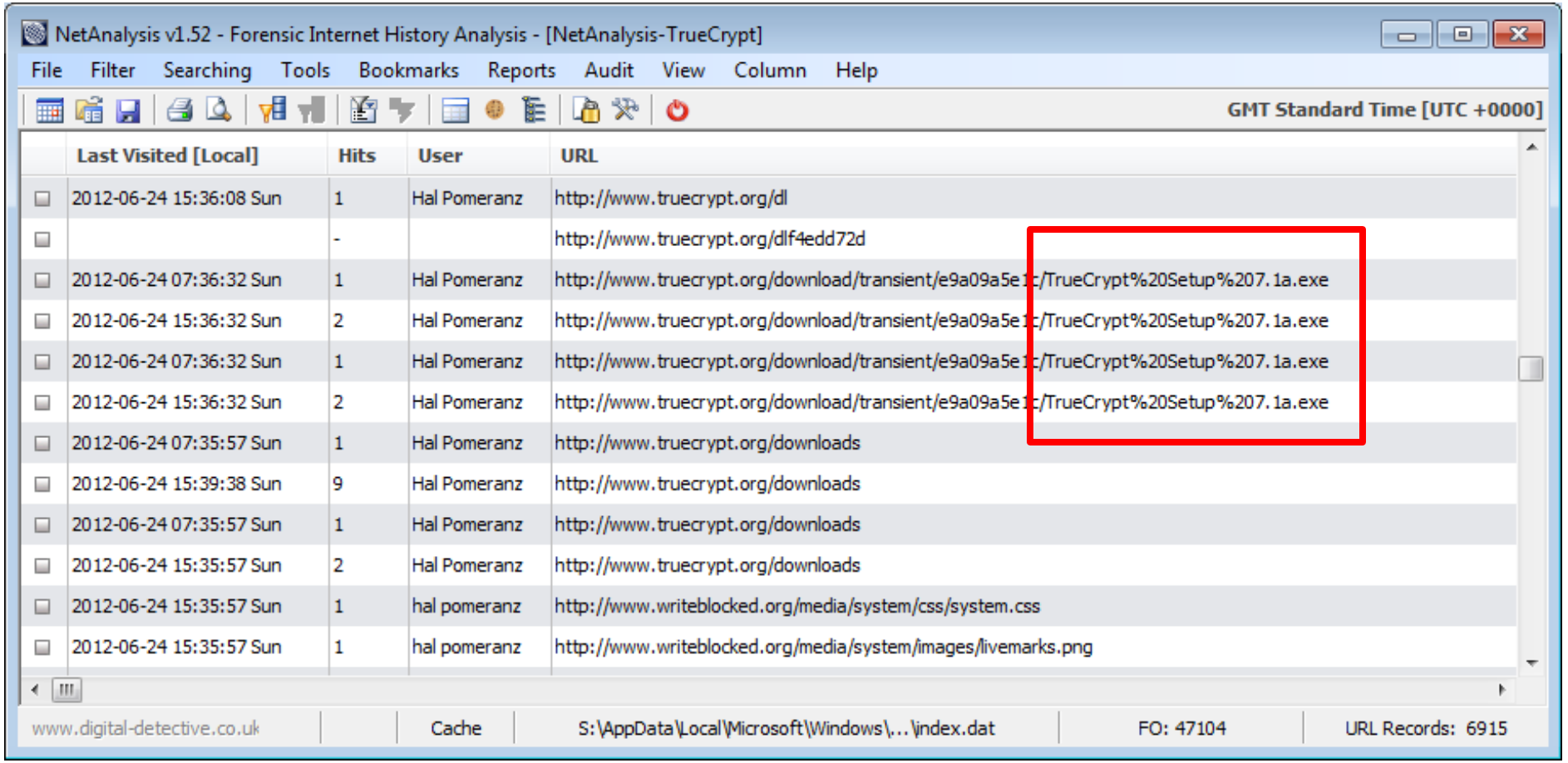
TrueCrypt installation directories

Registry –

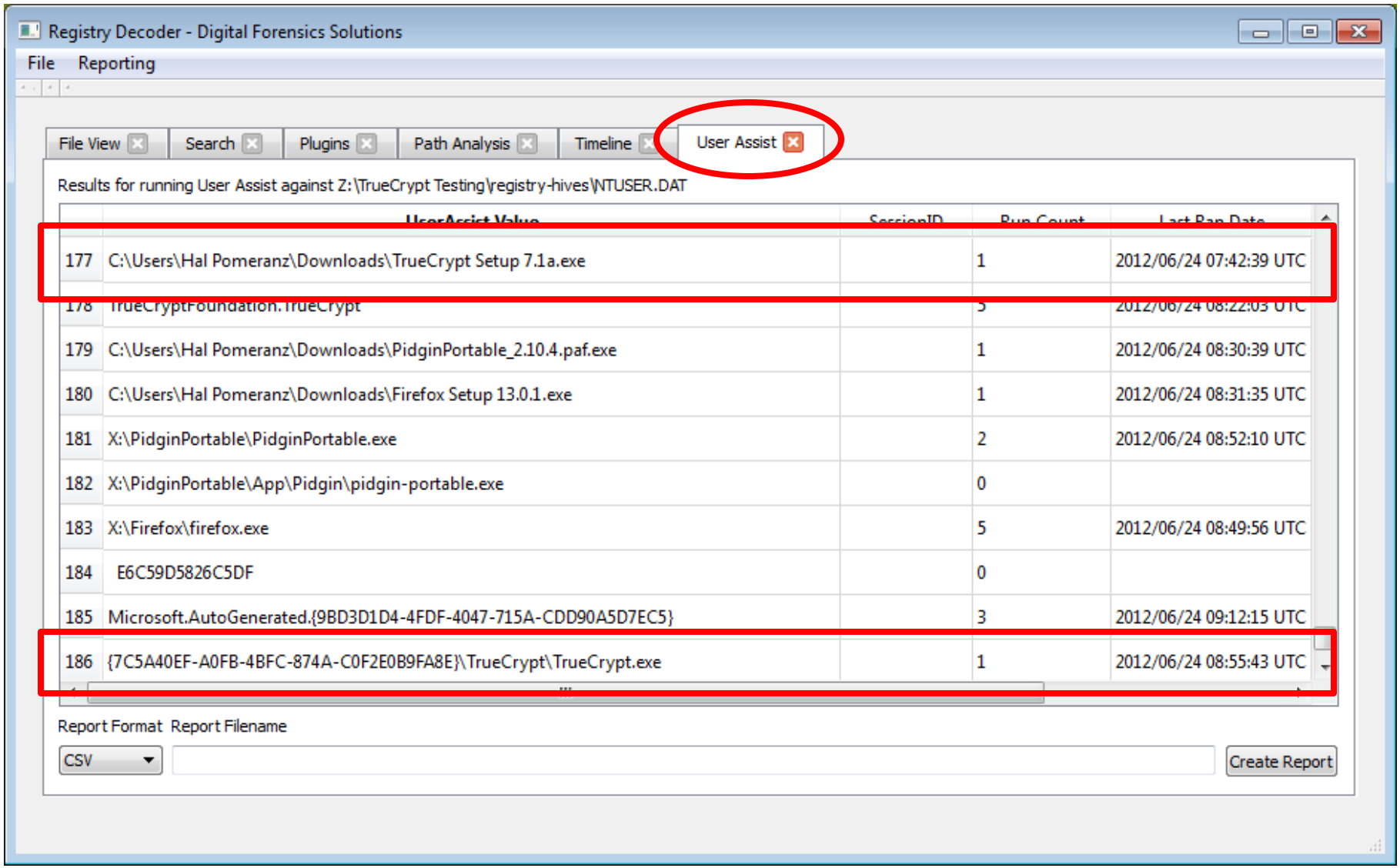
- Uninstall k
- Normally i
- Associates



WHERE DID IT COME FROM?!?



WHO DID THIS TO US?!?

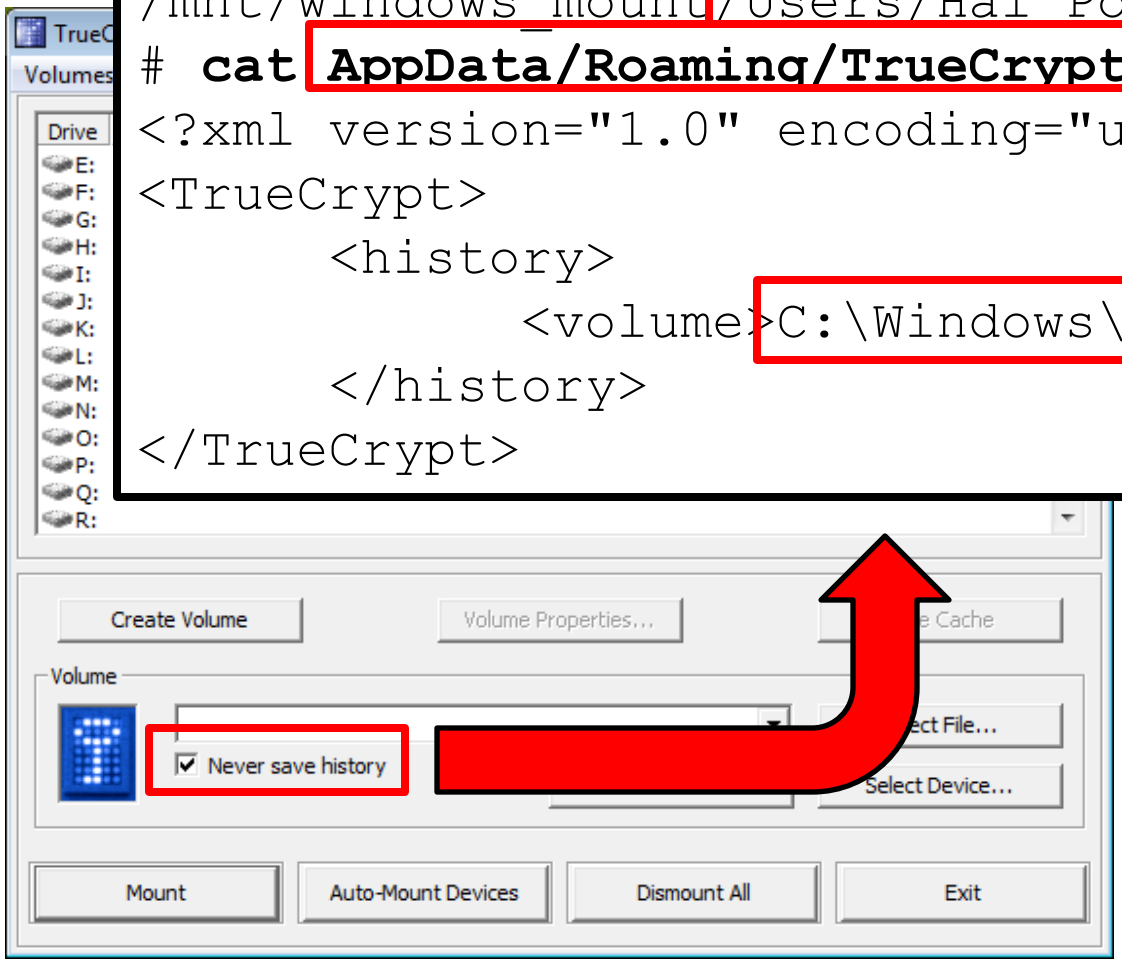


Searching for an Enigma!

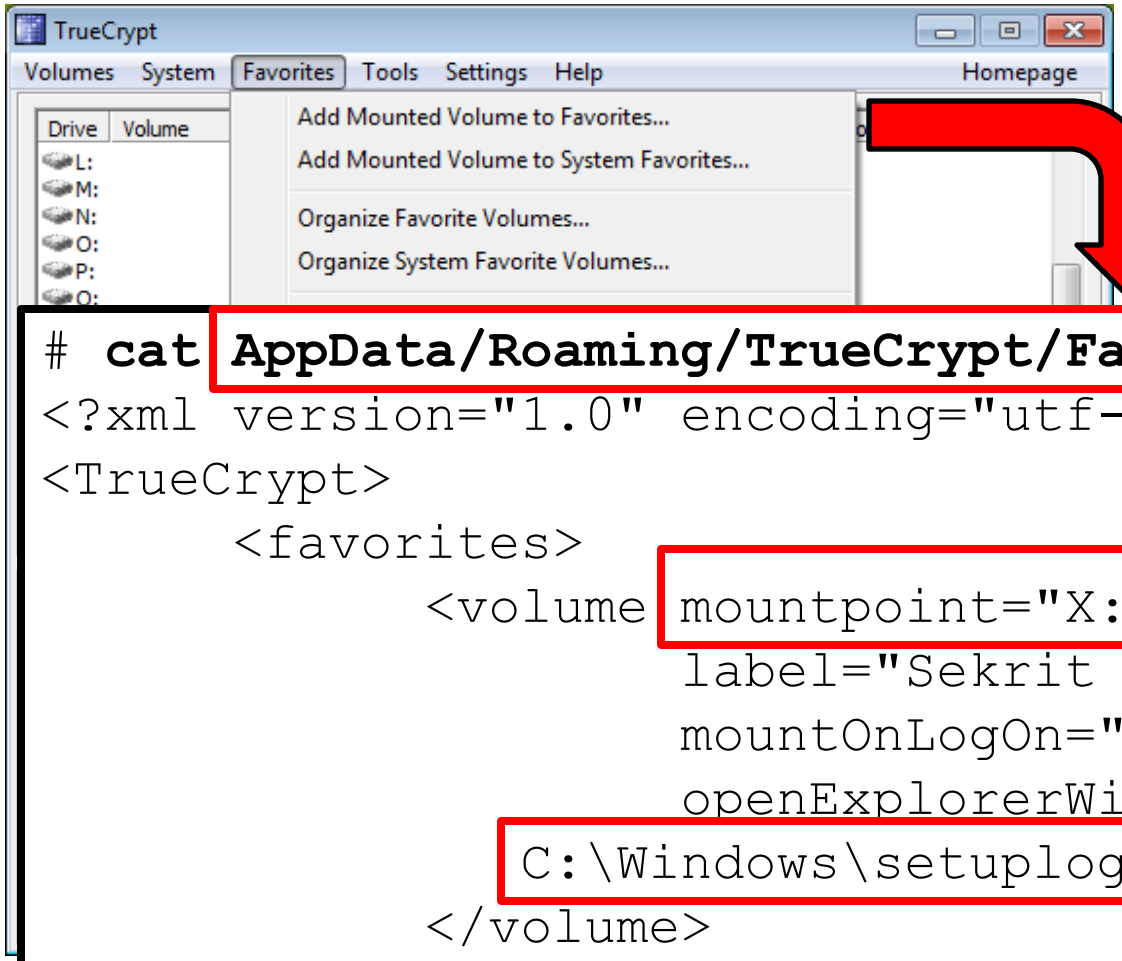
```
# tchunt -d /mnt/windows_mount
Suspect_File:     /mnt/windows_mount/Windows/setuplog.tc
#
# rip.pl -f system -r /mnt/…System32/SYSTEM >system.txt
# less system.txt
…
MountedDevices
LastWrite time = Sun Jun 24 16:15:17 2012Z
…
Device: TrueCryptVolumeX
        \??\Volume{1586675a-b25e-11e1-aebd-000c2976f352}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



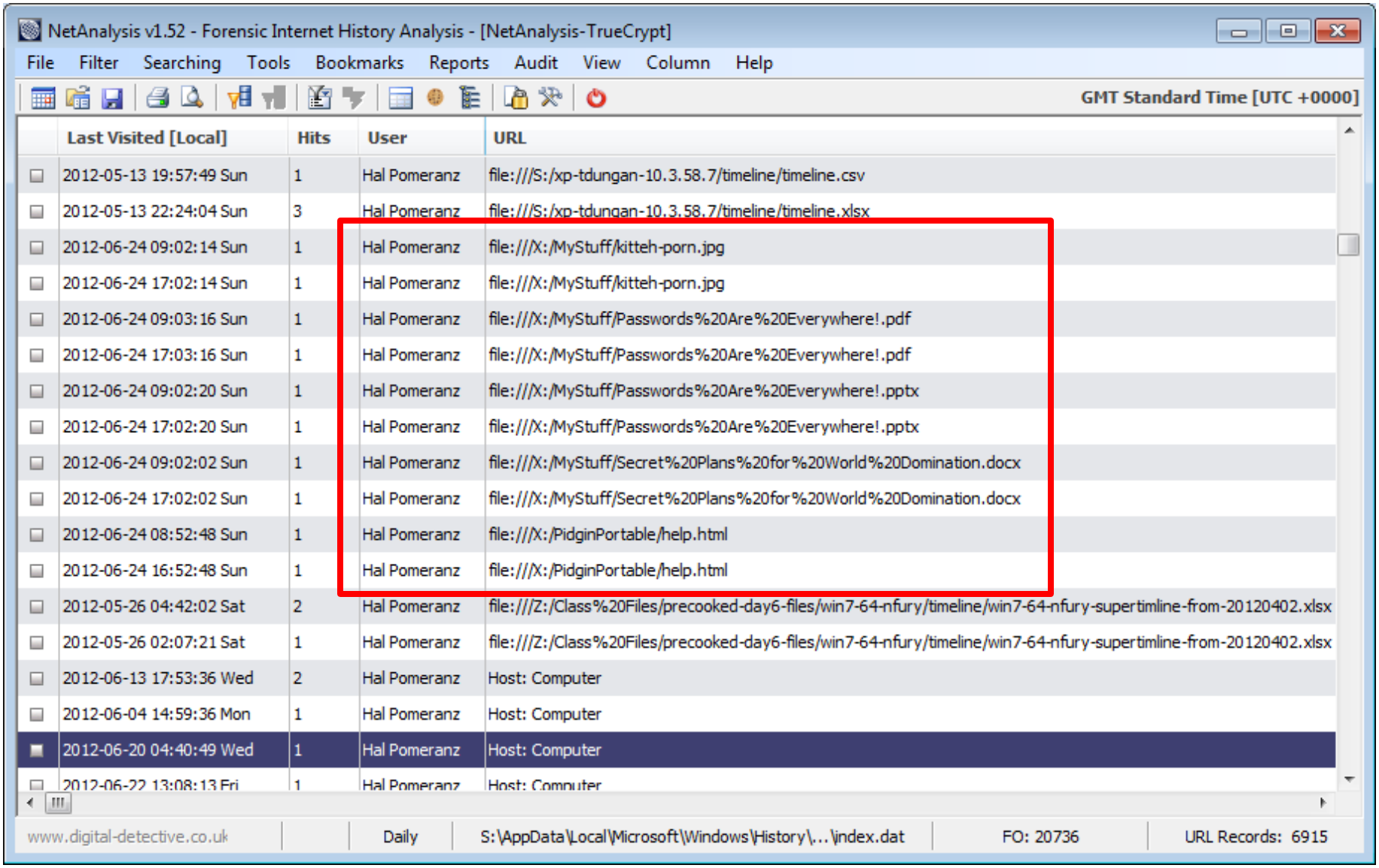

```
# cat AppData/Roaming/TrueCrypt/Favorite\ Volumes.xml
<?xml version="1.0" encoding="utf-8"?>
<TrueCrypt>
      <favorites>
            <volume mountpoint="X:\"
                  label="Sekrit Stash"
                  mountOnLogOn="1"
                  openExplorerWindow="1">
               C:\Windows\setuplog.tc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

BUT WHAT'S INSIDE?!?

Could be files!

Could be programs!

SECRET FILES!



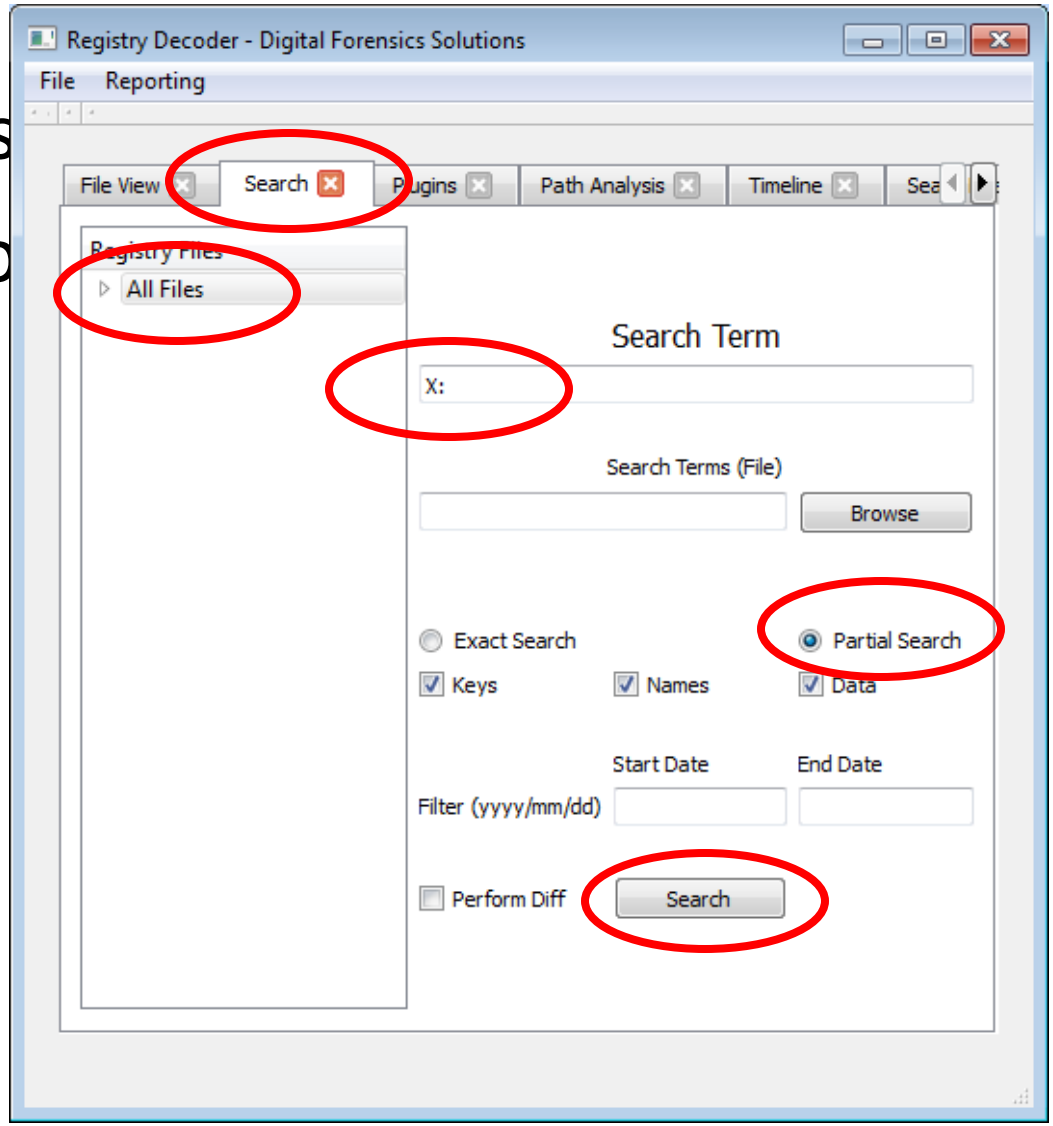
MISSING LNKS!

```
# 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
…
```

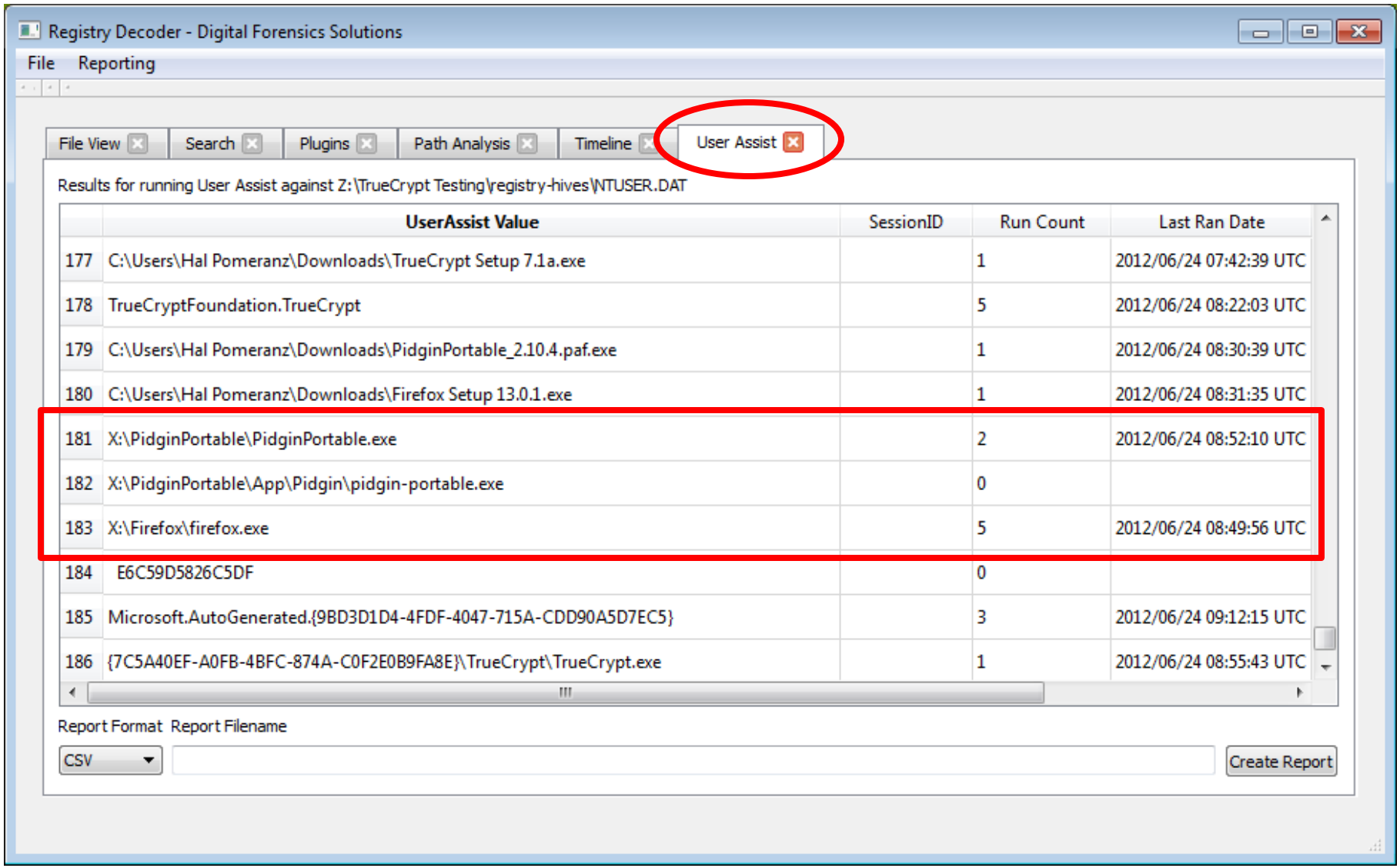
REGISTERED OFFENDERS!

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
Create Report

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!

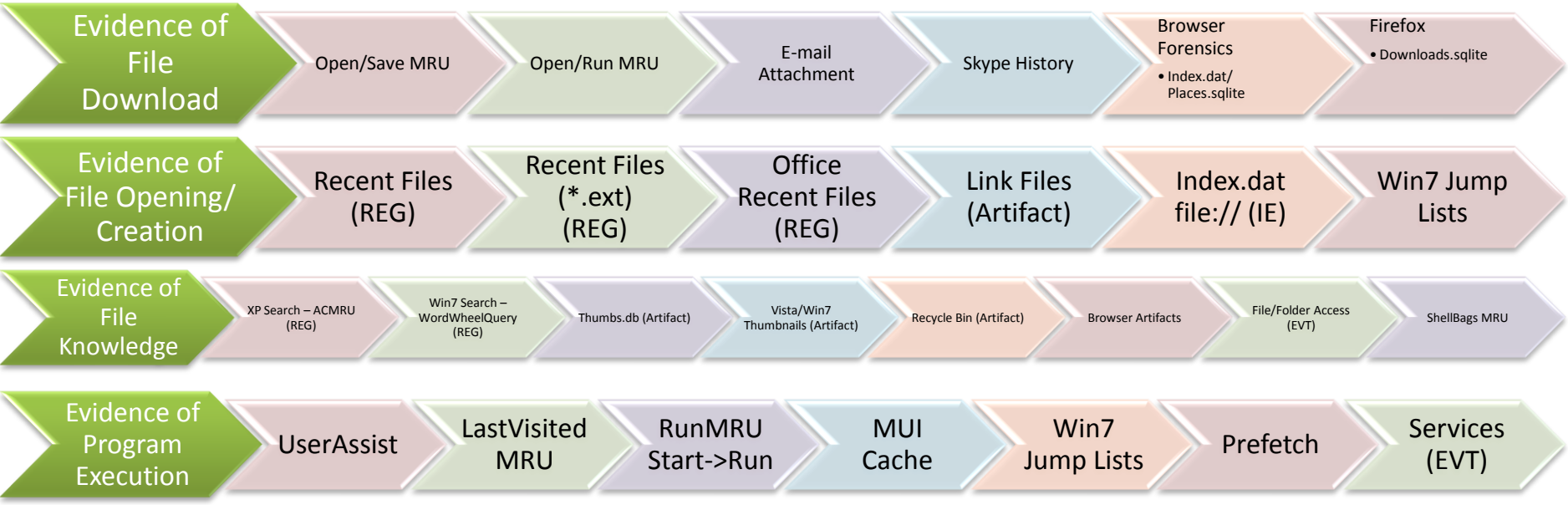
Got memory? (or hiberfil.sys)

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

Got (lots of) time?

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

DON'T GIVE UP!


Evidence of File Download
Open/Save MRU
Open/Run MRU
E-mail Attachment
Skype History
Browser Forensics
• Index.dat/ Places.sqlite
Firefox
• Downloads.sqlite
Evidence of File Opening/ Creation
Recent Files (REG)
Recent Files (*.ext) (REG)
Office Recent Files (REG)
Link Files (Artifact)
Index.dat file:// (IE)
Win7 Jump Lists
Evidence of File Knowledge
XP Search – ACMRU (REG)
Win7 Search – WordWheelQuery (REG)
Thumbs.db (Artifact)
Vista/Win7 Thumbnails (Artifact)
Recycle Bin (Artifact)
Browser Artifacts
File/Folder Access (EVT)
ShellBags MRU
Evidence of Program Execution
UserAssist
LastVisited MRU
RunMRU Start->Run
MUI Cache
Win7 Jump Lists
Prefetch
Services (EVT)

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/