

Making Memories: Using Memory Analysis for Faster Response to User Investigations

Aaron Sparling, Portland Police Bureau
Jessica Hyde, Magnet Forensics / George
Mason

SANS DFIR

Making Memories



MANY KNOW TO USE
MEMORY FOR IR
INVESTIGATIONS



VALUE TO USE IN END USER
INVESTIGATIONS

What do you think of for user investigations



Drugs



CSAM



Money Laundering



Fraud



ID Theft



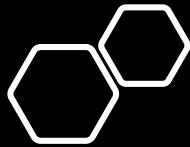
Weapons



Trafficking



Homicide / Assault

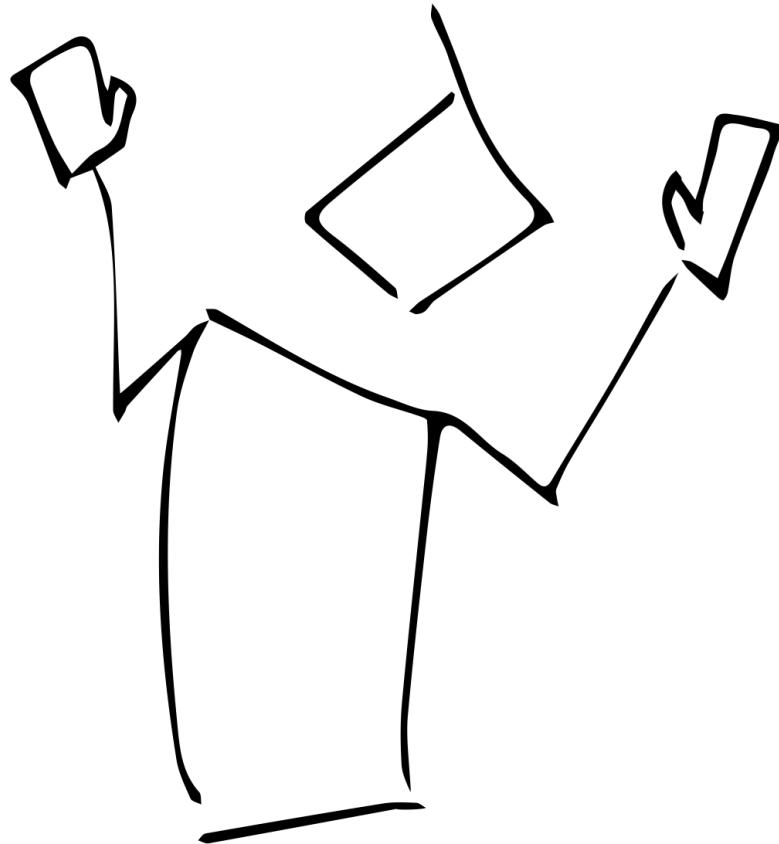


So you're an
Incident
Responder....
I know about
memory

But are you using memory on -

- HR violations / Usage Policy Violations
- IP theft
- Insider Trading
- Wrongful Termination
- Workplace Harassment
- Insider Threat

Why memory forensics



Numerous Artifacts reside in memory:

<i>Network artifacts</i>	<i>URL's</i>	<i>Passwords</i>	<i>Decrypted Data</i>
<i>Caches</i>	<i>Clipboard Data</i>	<i>Encryption Keys</i>	<i>Event Logs</i>
<i>IP Addresses</i>	<i>Chat</i>	<i>Internet artifacts/activity,</i>	<i>Prefetch</i>
<i>.lnk files</i>	<i>MFT</i>	<i>Registry</i>	<i>USB</i>
<i>Carved Audio</i>	<i>Carved Video</i>	<i>Carved Pictures</i>	<i>Google Searches</i>

Why Memory



Numerous Artifacts reside in memory



Memory Analysis can drive the investigation (pointers) - actionable intel



As memory increase in size, memory is becoming much more like a second file system (less to page out)



Fast - Image time - work while processing



Recent and Relevant data



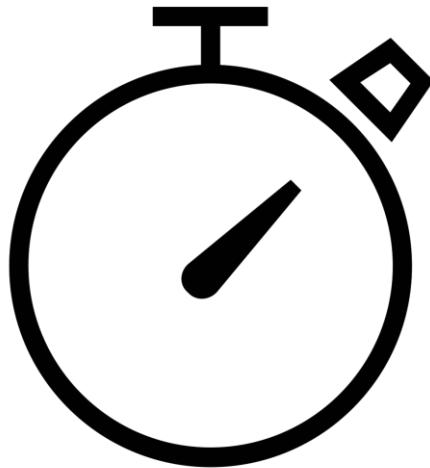
Can be performed on laptop (minimal hardware requirements)



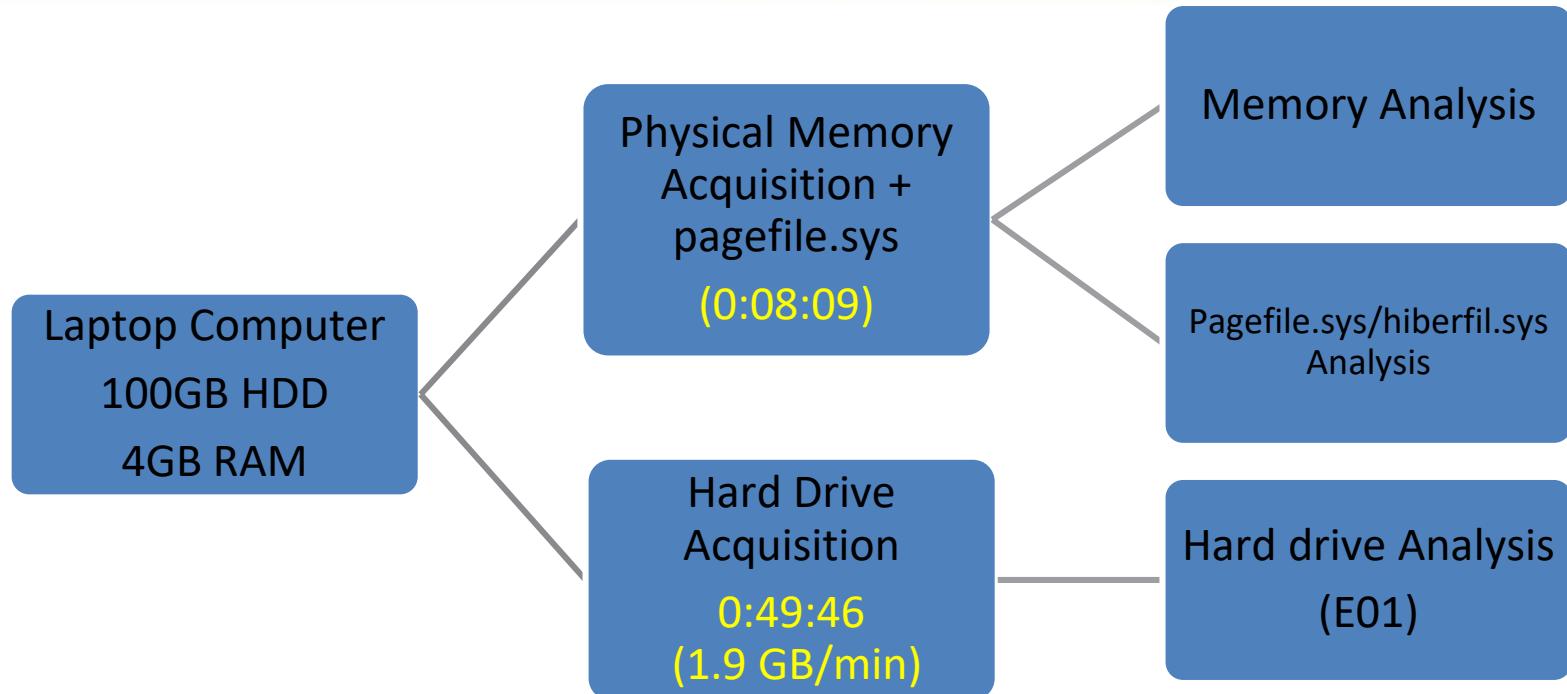
Validate against the image AFTER critical actions taken

Fast

- Actionable Intel
- Drive your investigation questions



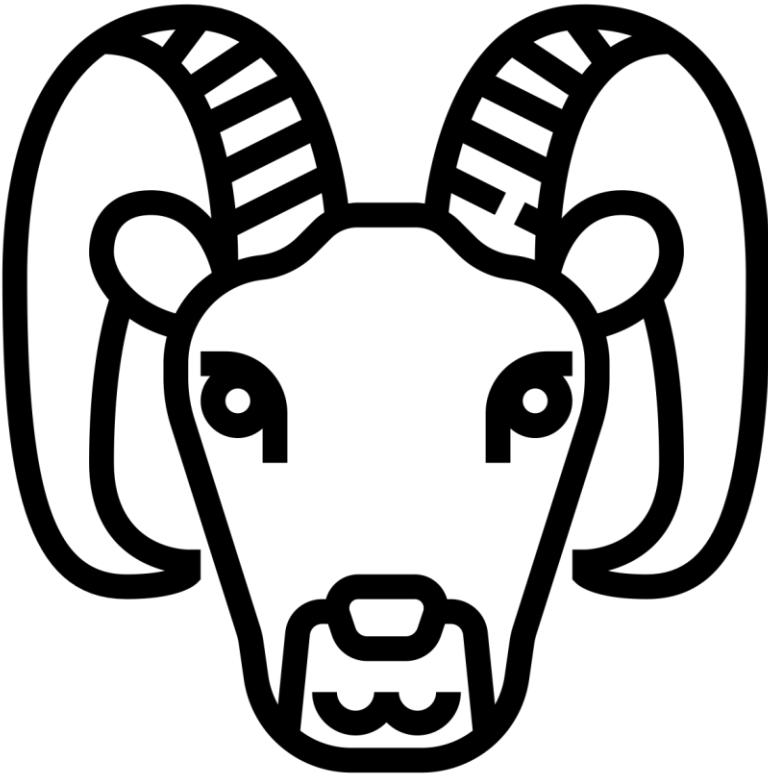
Memory vs Drive Acquisition



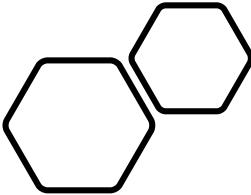


RAM

Collection



Money Maker Case Evidence

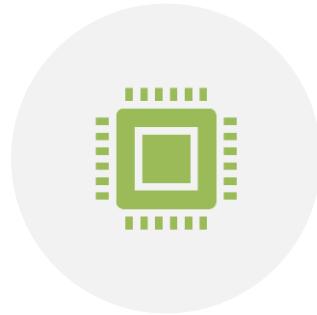


You have been tasked with investigating an individual who is suspected of identity theft and credit card fraud.

Money Maker Case Evidence



FORENSIC IMAGE (E01) DELL
LAPTOP COMPUTER

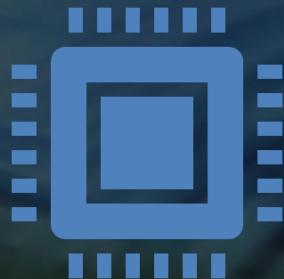


MEMORY DUMP
DELL LAPTOP (TAKEN ON
LOCATION)



FORENSIC IMAGE (E01) USB FLASH
DRIVE

Money Maker Case Task



Analyze raw memory dump and
memory-resident files from disk
(pagefile.sys and hiberfil.sys)



Profile users' activities, uncover data,
locate passwords, decrypt encrypted
volumes and locate indicators for further
filesystem analysis.

TRADITIONAL FORENSIC APPROACH / METHODOLOGY

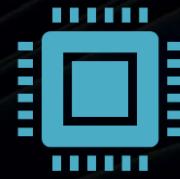


- Digital evidence items collected on location and delivered to the lab for analysis.
- Disk imaging and processing done in a controlled lab environment
- Process image
- Analyze contents

Think DFIRently!



Process Capture



RAM Capture



Analysis during
disk imaging

What if 8 min is too long?



Consent can be revoked



Process Capture

<https://www.magnetforensics.com/magnet-process-capture/>



Acquisition in about 20 seconds



Parsing under 10 min



Still great data source

Inform the interview questions

User Attribution

Timelining

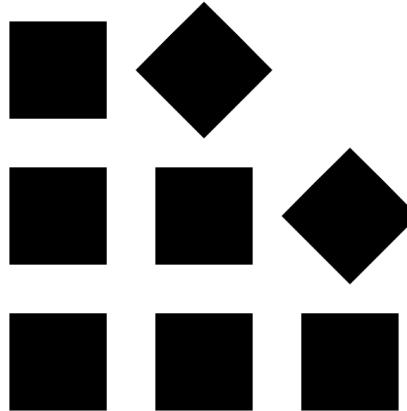
Passwords

Not my Pants

Use of encryption

External devices

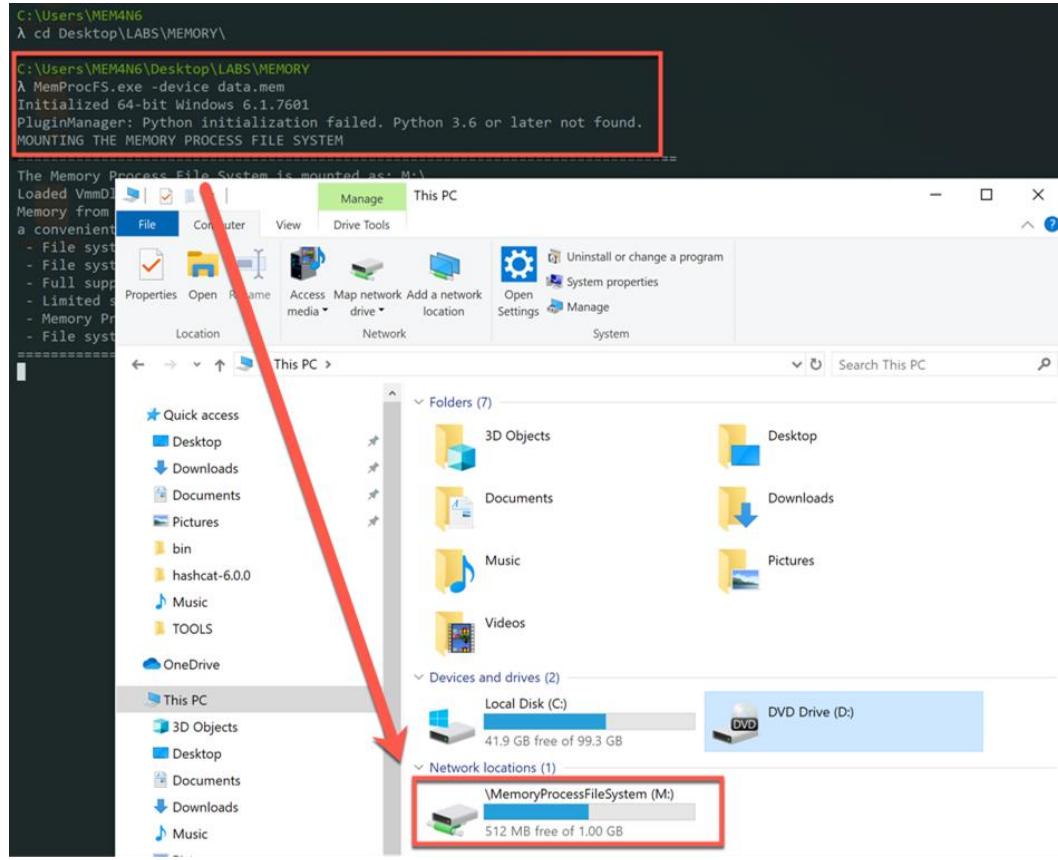
REGISTRY ANALYSIS



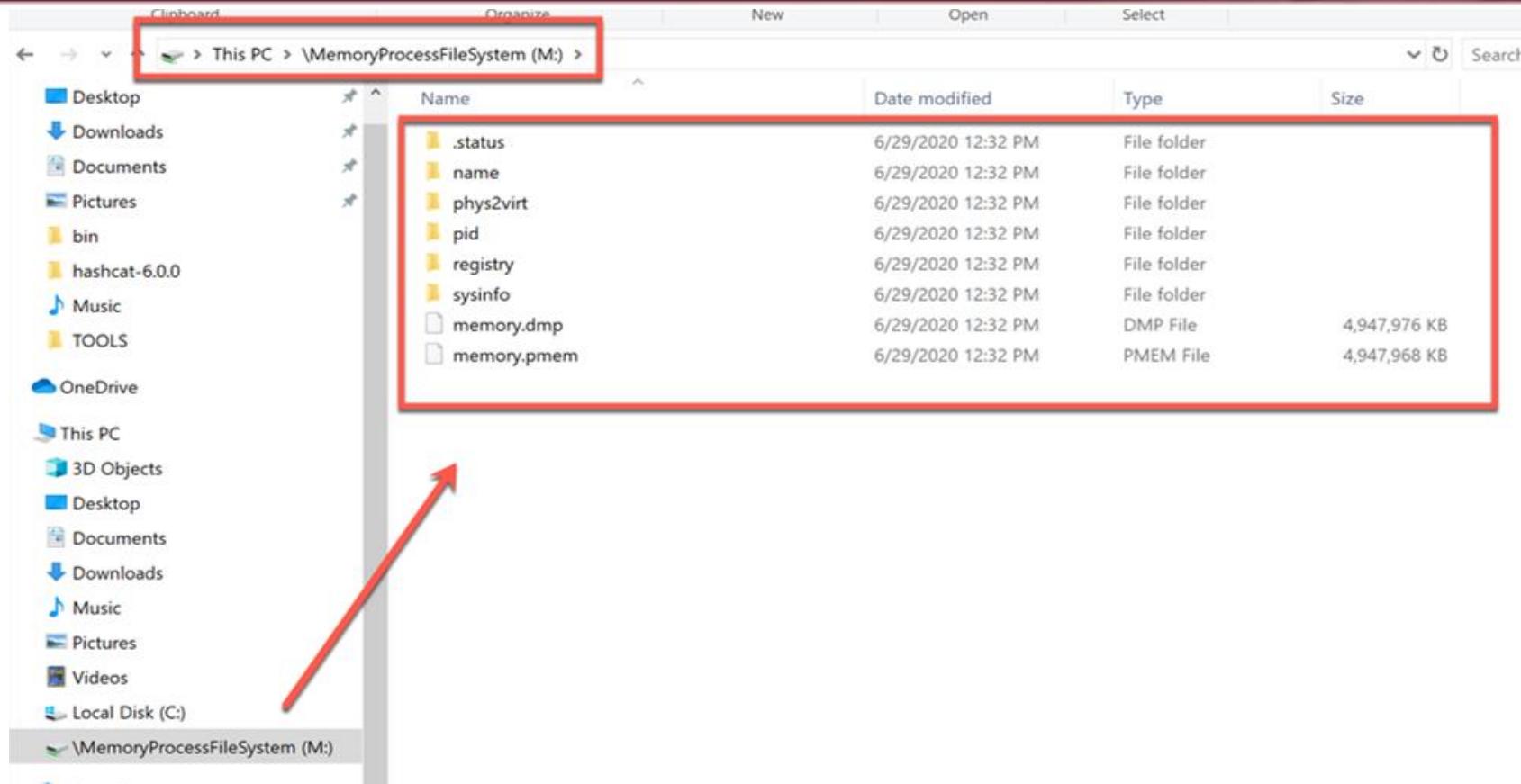
Locating Registry Hives in Memory

```
T:\MEM_IMAGES\MONEY_MAKER_PC\Carding_Case\MEM_DUMP
λ volatility -f data.lime --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual          Physical          Name
-----
0xfffff8a004d79010 0x000000009aa61010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a008778010 0x0000000093421010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a00ac35410 0x0000000033c2a410 \??\C:\Users\Jim Nassium\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a00ac39410 0x0000000046ed8410 \??\C:\Users\Jim Nassium\ntuser.dat
0xfffff8a00000e010 0x00000000a6c1d010 [no name]
0xfffff8a000023410 0x00000000a6c28410 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000059010 0x00000000a6b9f010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000219010 0x00000000a09ca010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000c72010 0x000000008e52f010 \REGISTRY\MACHINE\SECURITY
0xfffff8a000cd6010 0x000000008c7a6010 \SystemRoot\System32\Config\SAM
0xfffff8a000e83270 0x0000000085cf0270 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000f17010 0x000000008558b010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a002368410 0x0000000024d6f410 \??\C:\Windows\AppCompat\Programs\Amcache.hve
0xfffff8a002409010 0x000000011cb45010 \??\C:\System Volume Information\Syscache.hve
```

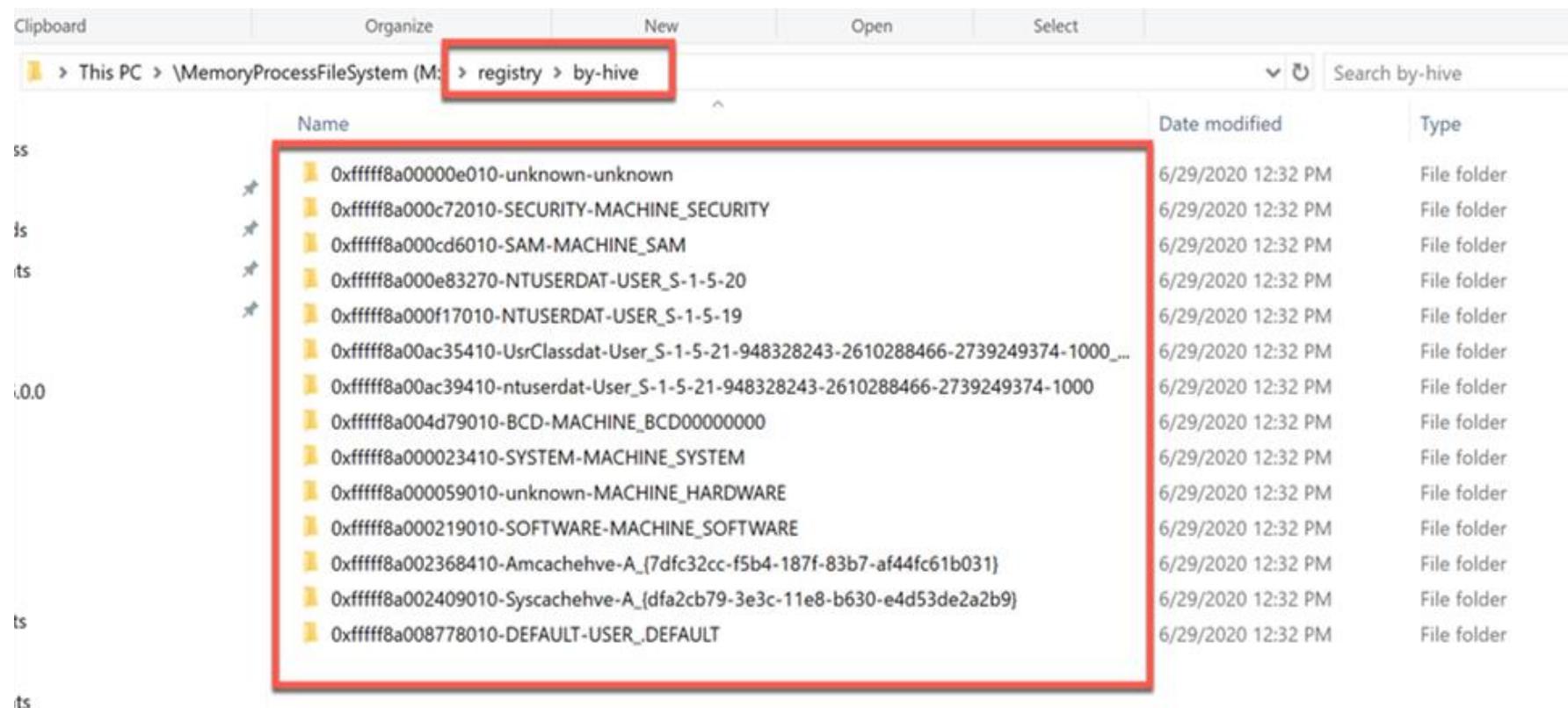
MemProcFS.exe



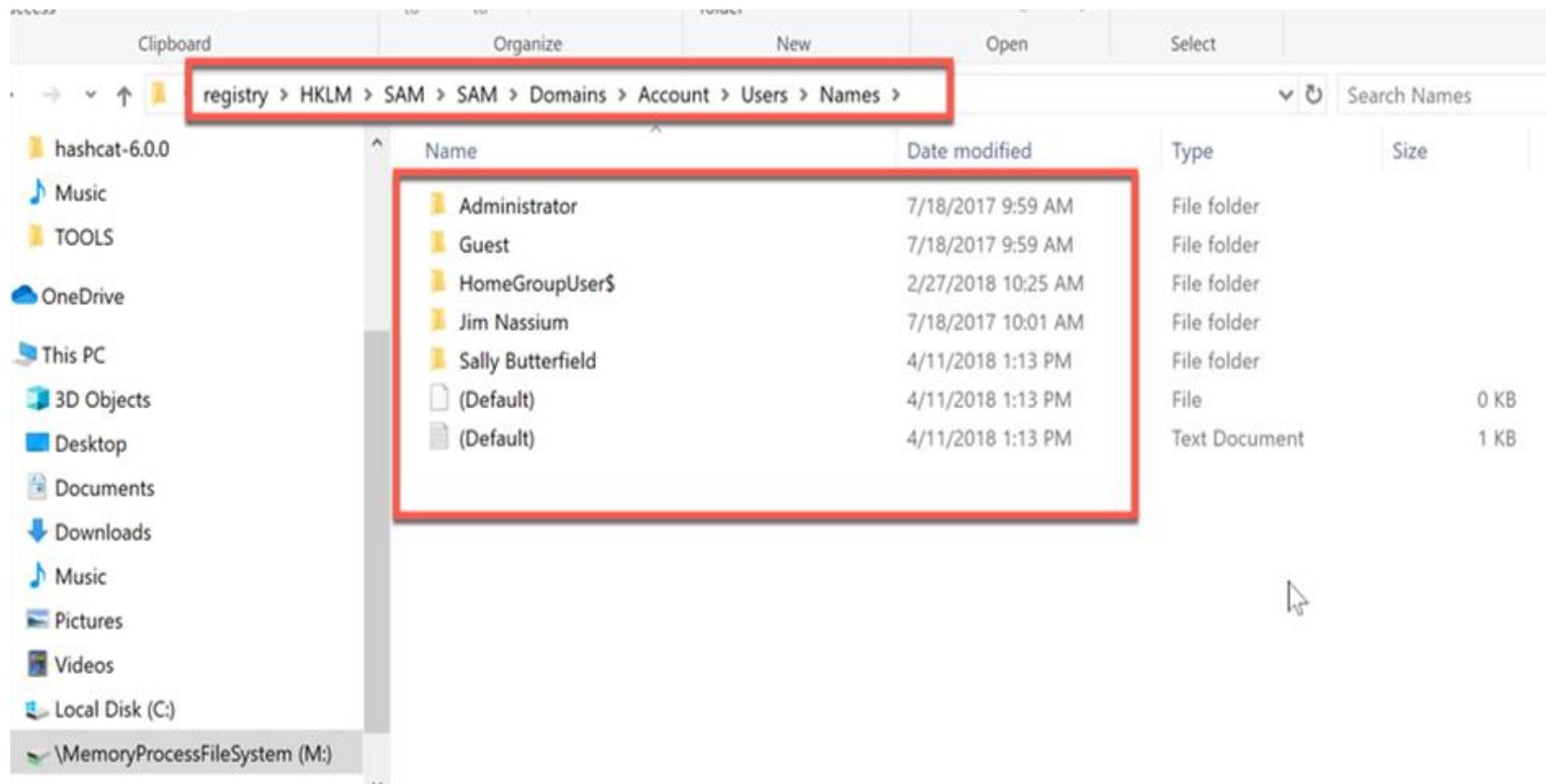
Mounted memory



Registry > by-hive



User Account Names



Locating the “CurrentControlSet”

```
T:\MEM_IMAGES\MONEY MAKER_PC\Carding_Case\MEM_DUMP
\ volatility -f data.lime --profile=Win7SP1x64 printkey -K "CurrentControlSet"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile
-----
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: CurrentControlSet (V)
Last updated: 2018-04-12 10:32:59 UTC+0000

Subkeys:
    desktop
Values:
REG_LINK      SymbolicLinkValue : (V) \Registry\Machine\System\ControlSet001
```

Enumerating USB devices from memory

cmd

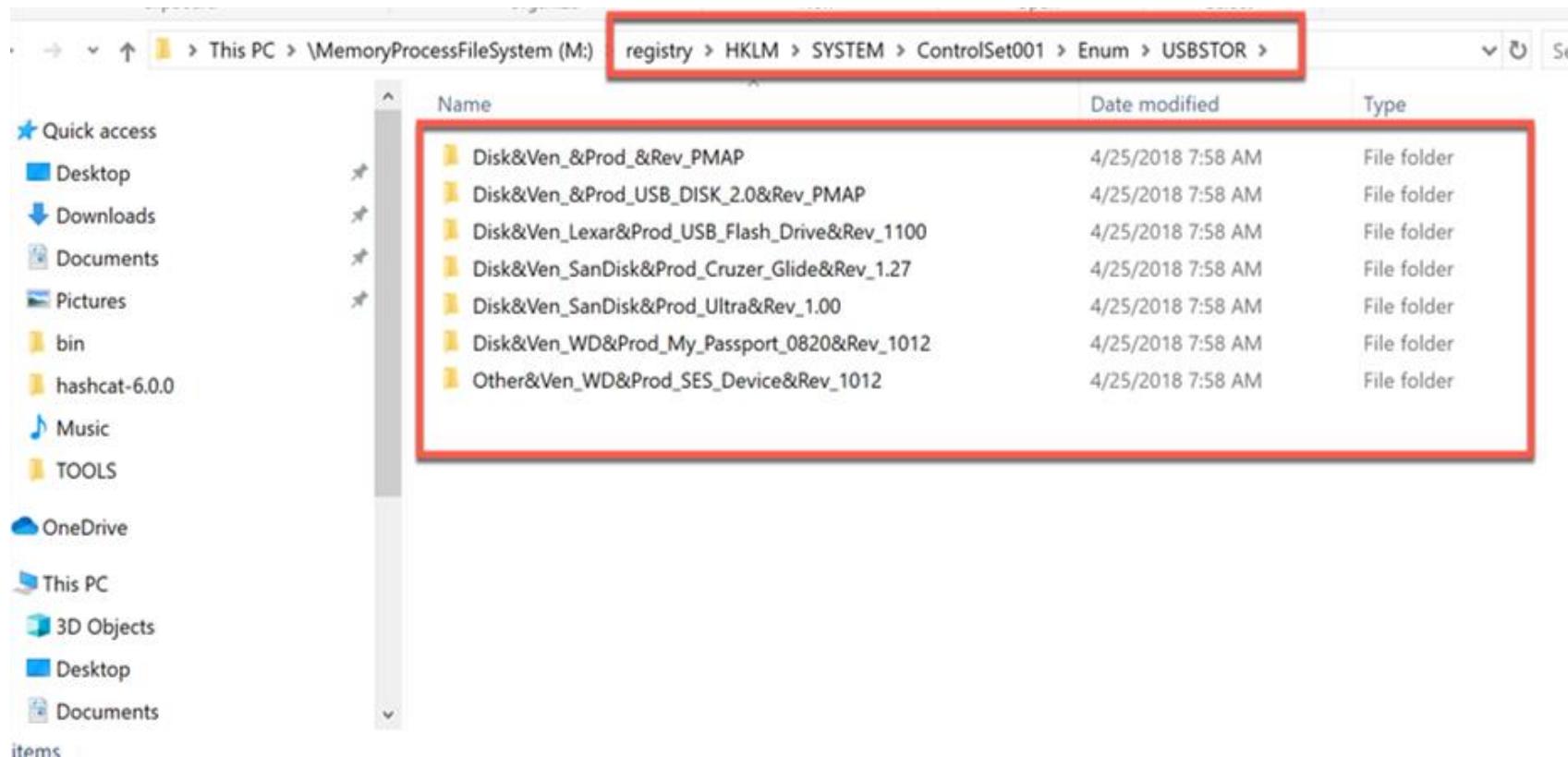
```
T:\MEM_IMAGES\MONEY MAKER PC\Carding_Case\MEM_DUMP
λ volatility -f data.lime --profile=Win7SP1x64 printkey -K "ControlSet001\Enum\USBSTOR"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

-----
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: USBSTOR (S)
Last updated: 2018-04-25 14:58:11 UTC+0000 ←

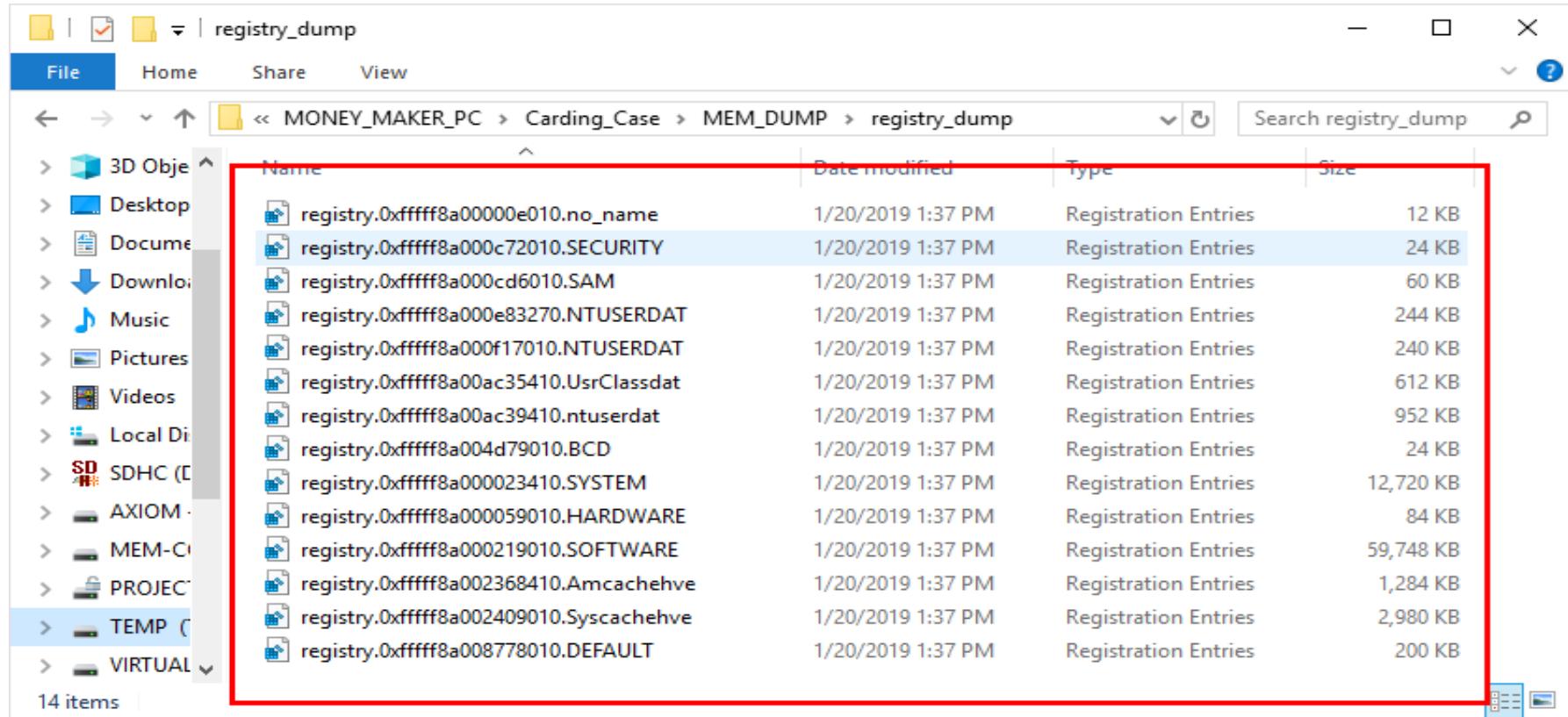
Subkeys:
(S) Disk&Ven_&Prod_&Rev_PMAP
(S) Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP
(S) Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100
(S) Disk&Ven_SanDisk&Prod_Cruzer_Glide&Rev_1.27
(S) Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00
(S) Disk&Ven_WD&Prod_My_Passport_0820&Rev_1012
(S) Other&Ven_WD&Prod_SES_Device&Rev_1012
```

Values:

Navigating to USBSTOR



Registry Hives Dumped From Memory



The screenshot shows a Windows File Explorer window with the following details:

- File Explorer Title Bar:** registry_dump
- Menu Bar:** File, Home, Share, View
- Address Bar:** << MONEY MAKER_PC > Carding_Case > MEM_DUMP > registry_dump
- Search Bar:** Search registry_dump
- Left Sidebar:** Shows a tree view of local drives and network locations, including 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, Local Disk (C), SDHC (D), AXIOM (E), MEM-C (F), PROJECT (G), TEMP (H), and VIRTUAL (I).
- Main Content Area:** A list of registry hive files. A red box highlights this area.
- Table Headers:** Name, Date modified, Type, Size
- Table Data:** The following registry hives are listed:

Name	Date modified	Type	Size
registry.0xfffff8a00000e010.no_name	1/20/2019 1:37 PM	Registration Entries	12 KB
registry.0xfffff8a000c72010.SECURITY	1/20/2019 1:37 PM	Registration Entries	24 KB
registry.0xfffff8a000cd6010.SAM	1/20/2019 1:37 PM	Registration Entries	60 KB
registry.0xfffff8a000e83270.NTUSERDAT	1/20/2019 1:37 PM	Registration Entries	244 KB
registry.0xfffff8a000f17010.NTUSERDAT	1/20/2019 1:37 PM	Registration Entries	240 KB
registry.0xfffff8a00ac35410.UsrClassdat	1/20/2019 1:37 PM	Registration Entries	612 KB
registry.0xfffff8a00ac39410.ntuserdat	1/20/2019 1:37 PM	Registration Entries	952 KB
registry.0xfffff8a004d79010.BCD	1/20/2019 1:37 PM	Registration Entries	24 KB
registry.0xfffff8a000023410.SYSTEM	1/20/2019 1:37 PM	Registration Entries	12,720 KB
registry.0xfffff8a000059010.HARDWARE	1/20/2019 1:37 PM	Registration Entries	84 KB
registry.0xfffff8a000219010.SOFTWARE	1/20/2019 1:37 PM	Registration Entries	59,748 KB
registry.0xfffff8a002368410.Amcachehive	1/20/2019 1:37 PM	Registration Entries	1,284 KB
registry.0xfffff8a002409010.Syscachehive	1/20/2019 1:37 PM	Registration Entries	2,980 KB
registry.0xfffff8a008778010.DEFAULT	1/20/2019 1:37 PM	Registration Entries	200 KB

14 items

USB Detective

USB Detective v1.3.6 Community Edition (non-commercial use only)

File Tools View Report

Serial/UID Description

Select Files/Folders...

Case Information

Case Name: MoneyMaker Evidence Item: 001

Case Folder: C:\Users\IAICS-RAM\Desktop\LABS\Carding_Case\REGISTRY Browse...

File/Folder Locations

SYSTEM Hive(s): E:\MAGNET Webinar\MoneyMaker\registry_dump\Full_ File Folder

SOFTWARE Hive(s): E:\MAGNET Webinar\MoneyMaker\registry_dump\Full_ File Folder

NTUSER.DAT Hive(s): E:\MAGNET Webinar\MoneyMaker\registry_dump\Full_ File Folder

Setupapi Log(s): File Folder

Amcache Hive(s): File Folder

Event Log(s): Upgrade to professional to process event logs. File Folder

Process Artifacts

Cancel Clear

2019/02/22 4:16:55 PM: USB Detective

VSN Last User Select Amcache.hve...

Organize New folder

Name Date modified

Name	Date modified
registry.0xfffff8a0000e010.no_name	1/20/2019
Hitachi Travelstar 1C	1/20/2019
memory	1/20/2019
References	1/20/2019
USB	1/20/2019
OneDrive	1/20/2019
This PC	1/20/2019
3D Objects	1/20/2019
Desktop	1/20/2019
Documents	1/20/2019
Downloads	1/20/2019
Music	1/20/2019
Pictures	1/20/2019
Videos	1/20/2019
Local Disk (C)	1/20/2019
registry.0xfffff8a002368410.Amcachehive	1/20/2019
registry.0xfffff8a002409010.Syccachehive	1/20/2019
registry.0xfffff8a008778010.DEFAULT	1/20/2019

USB Detective

USB Detective v1.3.6 Community Edition (non-commercial use only) [MoneyMaker-001]

- □ X

File Tools View Report Help

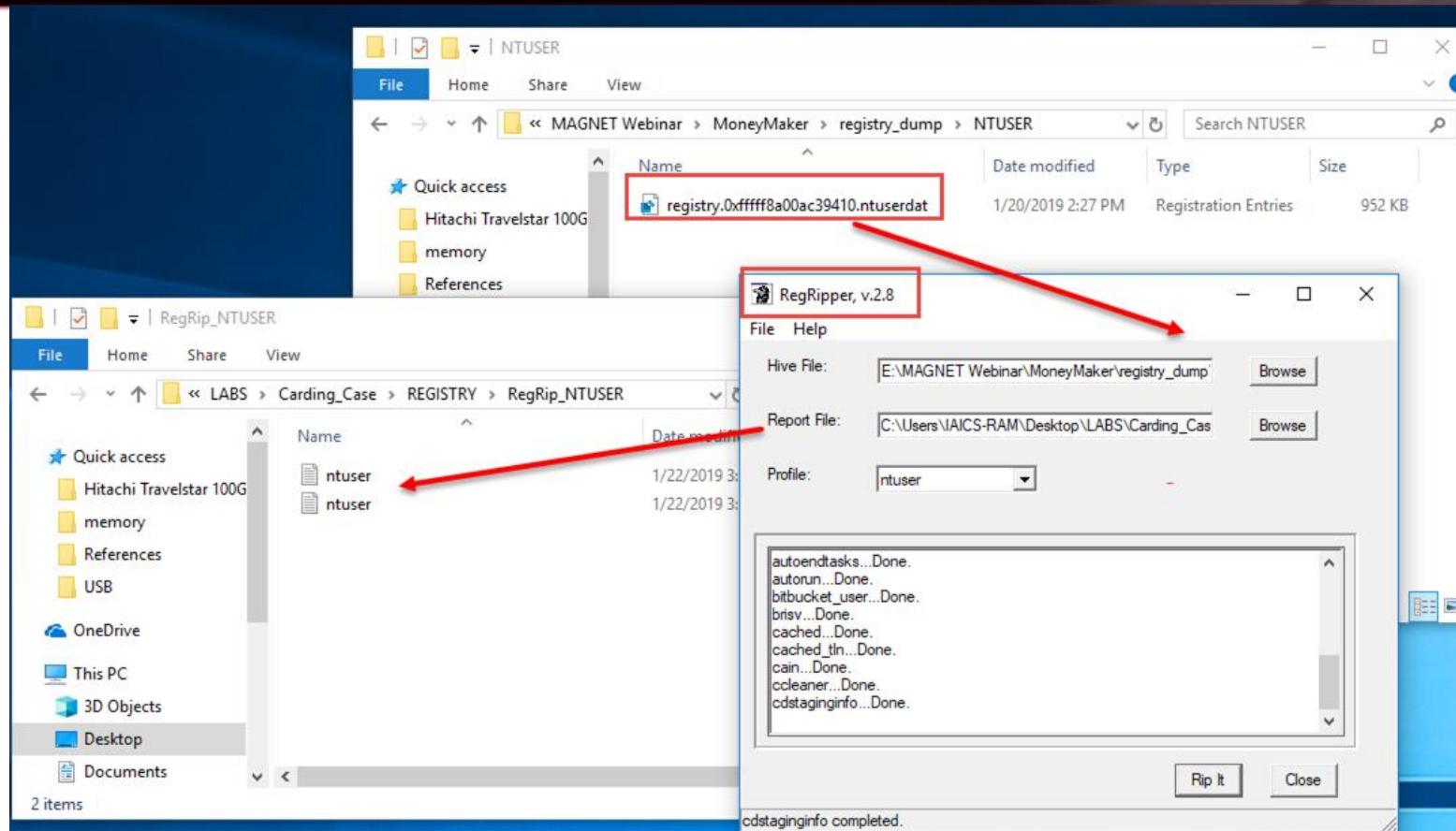
Serial/UID	Description	First Connected (PST/PDT)	Last Connected (PST/PDT)	Last Disconnected (PST/PDT)	Volume Name/Label	Drive Letter(s)	VSN	Last User
070B3C2F3929D638	USB Device	12/12/2017 2:02:26 PM	1/5/2018 7:21:16 PM		MEM COURSE		5A42EEDB, FE8E7C41	Full_Reg_Dump
AA45832GR3KC8D55	Lexar USB Flash Drive USB Device	10/10/2017 2:07:11 PM	10/10/2017 2:07:15 PM		Untitled		988AC1C7	Full_Reg_Dump
4C530599940704118061	SANDISK CRUZER GLIDE				Untitled		56C2330D	Full_Reg_Dump
4C531001560722101274	SANDISK CRUZER GLIDE				MEM		E45A5CE5	Full_Reg_Dump
4C531001370920112323	SANDISK ULTRA				NITRO-LABS	G:	F8082F7C	Full_Reg_Dump
07971D0894211D5F	USB DISK 2.0 USB Device				TAILS, VAULT	E:	B6A95767, E49C7980	Full_Reg_Dump

1/22/2019 4:19:59 PM: Processing Amcache hive (E:\MAGNET Webinar\MoneyMaker\registry_dump\Full_Reg_Dump\registry.0xfffff8a002368410.Amcachehive.reg).
1/22/2019 4:19:59 PM: Finished processing Amcache hive (E:\MAGNET Webinar\MoneyMaker\registry_dump\Full_Reg_Dump\registry.0xfffff8a002368410.Amcachehive.reg).
1/22/2019 4:19:59 PM: No event log(s) provided.
1/22/2019 4:19:59 PM: Performing additional correlation across provided artifacts.
1/22/2019 4:19:59 PM: Populating results grid and checking for duplicate timestamps.

Timestamp Consistency Levels

Not Calculated	Mid
Low	High

RegRipper



User Assist

```
1959 -----
1960 unreadmail v.20100218
1961 (NTUSER.DAT) Gets contents of Unreadmail key
1962
1963 Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
1964 -----
1965 -----
1966 UserAssist
1967 Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
1968 LastWrite Time Tue Jul 18 17:03:29 2017 (UTC)
1969
1970 {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
1971 Wed Apr 25 16:41:57 2018 Z
1972 (F38BF404-1D43-42F2-9305-67DE0B28FC23)\explorer.exe (19)
1973 Wed Apr 25 16:41:50 2018 Z
1974 (1AC14E77-02E7-4E5D-B744-2EB1AE5198B7)\cmd.exe (1)
1975 Tue Apr 24 20:36:21 2018 Z
1976 Chrome (6)
1977 Tue Apr 24 20:35:34 2018 Z
1978 (1AC14E77-02E7-4E5D-B744-2EB1AE5198B7)\notepad.exe (8)
1979 Tue Apr 24 20:35:13 2018 Z
1980 (6D809377-6AF0-444B-8957-A3773F02200E)\LibreOffice\program\scalc.exe (1)
1981 Tue Apr 24 20:18:34 2018 Z
1982 (7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E)\Gpg4win\bin\kleopatra.exe (3)
1983 Tue Apr 24 20:13:28 2018 Z
1984 (7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E)\GnuPG\bin\gpg-wks-client.exe (1)
1985 Tue Apr 24 20:13:17 2018 Z
1986 (7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E)\GnuPG\bin\gpgv.exe (1)
1987 Tue Apr 24 20:13:11 2018 Z
1988 (7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E)\GnuPG\bin\gpg.exe (2)
1989 Tue Apr 24 20:09:15 2018 Z
1990 (6D809377-6AF0-444B-8957-A3773F02200E)\LibreOffice\program\soffice.exe (2)
1991 Tue Apr 24 19:49:45 2018 Z
1992 IDRICK.VeraCrypt (2)
1993 Tue Apr 24 18:28:10 2018 Z
1994 C:\Users\Jim Nassium\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1OLROGBE\VeraCrypt Setup 1.22.exe (1)
1995 Tue Apr 24 18:23:00 2018 Z
1996 TrueCryptFoundation.TrueCrypt (2)
1997 Tue Apr 24 18:18:24 2018 Z
1998 C:\Users\Jim Nassium\Desktop\Tor Browser\Browser\firefox.exe (3)
1999 Tue Apr 24 18:05:40 2018 Z
2000 Microsoft.InternetExplorer.Default (2)
```

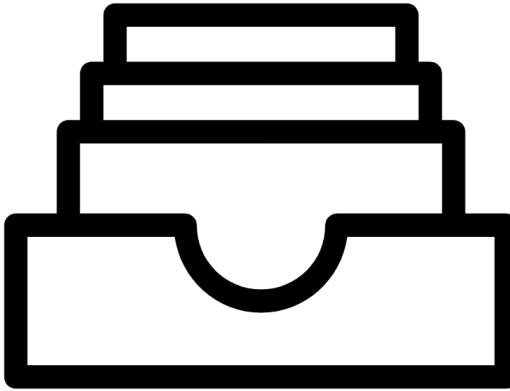
Recent Docs

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
LastWrite Time Tue Apr 24 20:35:34 2018 (UTC)
MRUListEx = 3,4,0,2,1
    3 = credit cards.txt
    4 = Stolen CC - Copy.txt
    0 = carding stuff.txt
    2 = image_info.txt
    1 = License Keys.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
LastWrite Time Tue Apr 24 20:35:13 2018 (UTC)
MRUListEx = 0
    0 = the goods.xlsx
```

```
1524602213|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs - Downloads
1513116548|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.dmp - test1.dmp
1524601081|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gpg - key.gpg
1523478157|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.html - MSR605 Magnetic Credit Card Reader Writer Encoder Swipe Magstripe MSR206 _ eBay.html
1524602213|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg - scarfacanew.jpg
1515210532|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.SNAG - E9A778B4-E2FE-49A6-8FE5-275A5C03A6F6.SNAG
1524602134|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt - credit cards.txt
1524602113|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx - the goods.xlsx
1515374965|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip - QUICK_TRIAGE.zip
1524602213|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder - Downloads
-----
reveton v.20131010
```

MFT – Master File Table Analysis



Parsing MFT

```
T:\MEM_IMAGES\MONEY MAKER PC\Carding_Case\MEM_DUMP
\ volatility -f data.lime --profile=Win7SP1x64 mftparser --output-file=mft_parser.txt
Volatility Foundation Volatility Framework 2.6
Outputting to: mft_parser.txt
Scanning for MFT entries and building directory, this can take a while
```

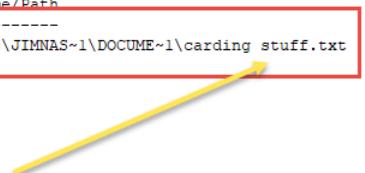
Locating resident data in MFT

```
mlwr-4n6@MLWR-DFIR:/mnt/t/MEM_IMAGES/MONEY MAKER PC/Carding Case/MEM_DUMP/mft$ grep -i password -r mft/
mft/file.0x10bc1ac00.data0.dmp:<td>Password:</td>
mft/file.0x10bc3000.data0.dmp:<TD>Password:</TD>
mft/file.0x10f344400.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Access2Base" library:readonly="false" library:passwordprotected="false">
mft/file.0x10f70c00.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Tools" library:readonly="true" library:passwordprotected="false">
mft/file.0x119a1800.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="ImportWizard" library:readonly="true" library:passwordprotected="false">
mft/file.0x119a1c00.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="ImportWizard" library:readonly="true" library:passwordprotected="false">
mft/file.0x11a654c00.data0.dmp:Password!=Mo58SvUt3Wz
mft/file.0x120f7b1000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Tools" library:readonly="true" library:passwordprotected="false">
mft/file.0x121015000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="FormWizard" library:readonly="true" library:passwordprotected="false">
mft/file.0x1210c000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Depot" library:readonly="true" library:passwordprotected="false">
mft/file.0x121715000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="ScriptBindingLibrary" library:readonly="false" library:passwordprotected="false">
mft/file.0x122064c00.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Standard" library:readonly="false" library:passwordprotected="false">
mft/file.0x12ceb400.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Template" library:readonly="true" library:passwordprotected="false">
mft/file.0x12ceb800.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Template" library:readonly="true" library:passwordprotected="false">
mft/file.0x354c00.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="ScriptBindingLibrary" library:readonly="false" library:passwordprotected="false">
mft/file.0x4354c00.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="FormWizard" library:readonly="true" library:passwordprotected="false">
mft/file.0x64838800.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Standard" library:readonly="false" library:passwordprotected="false"/>
mft/file.0x741a6c00.data0.dmp:<store my passwords (Password1)
mft/file.0x8120c000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Standard" library:readonly="false" library:passwordprotected="false"/>
mft/file.0x83900000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Euro" library:readonly="true" library:passwordprotected="false">
mft/file.0xa3900000.data0.dmp:<library:element library:name="DlgPassword"/>
mft/file.0xa3904000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Euro" library:readonly="true" library:passwordprotected="false">
mft/file.0xaeef54000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Tutorials" library:readonly="false" library:passwordprotected="false">
mft/file.0xaeef5c000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Tutorials" library:readonly="false" library:passwordprotected="false">
mft/file.0xc3fae000.data0.dmp:password:
mft/file.0xd5d90000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Gimmicks" library:readonly="false" library:passwordprotected="false">
mft/file.0xd5d98000.data0.dmp:<library:library xmlns:library="http://openoffice.org/2000/library" library:name="Gimmicks" library:readonly="false" library:passwordprotected="false">
mlwr-4n6@MLWR-DFIR:/mnt/t/MEM_IMAGES/MONEY MAKER PC/Carding Case/MEM_DUMP$ cd mft/
mlwr-4n6@MLWR-DFIR:/mnt/t/MEM_IMAGES/MONEY MAKER PC/Carding Case/MEM_DUMP/mft$ xxd file.0x741a6c00.data0.dmp ←
00000000: 4e6f 7465 733a 0d0a 0d0a 6e65 6565 2074
00000010: 6f28 6765 7420 6120 4d53 5220 3630 3520
00000020: 666f 7220 636c 6f6e 696e 6720 6361 7264
00000030: 73d0 0a6e 6565 6420 746f 2067 6574 2064
00000040: 756d 7073 2066 726f 6d20 6461 726b 2077
00000050: 6562 0d0a 0d0a 7374 6f72 6520 6d79 2070
00000060: 6173 7377 6f72 6473 2028 5061 7373 776f
00000070: 7264 3129
Notes....need t
o get a MSR
for cloning card
s...need to get d
umps from dark w
eb....store my p
asswords (Passwo
rd1)
```

MFT – Resident DATA

```
1893992 ****
1893993 MFT entry found at offset 0x741a6c00
1893994 Attribute: In Use & File
1893995 Record Number: 23515
1893996 Link count: 2
1893997
1893998
1893999 $STANDARD_INFORMATION
1894000 Creation Modified MFT Altered Access Date Type
1894001 -----
1894002 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 Archive
1894003
1894004 $FILE_NAME
1894005 Creation Modified MFT Altered Access Date Name/Path
1894006 -----
1894007 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 Users\JIMNAS~1\DOCUME~1\CARDIN~1.TXT
1894008
1894009 $FILE_NAME
1894010 Creation Modified MFT Altered Access Date Name/Path
1894011 -----
1894012 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 2017-12-12 22:08:32 UTC+0000 Users\JIMNAS~1\DOCUME~1\carding stuff.txt
1894013
1894014 $OBJECT_ID
1894015 Object ID: dd0a329e-87df-e711-89ac-e4d53de2a2b9
1894016 Birth Volume ID: 80000000-9000-0000-0000-180000000100
1894017 Birth Object ID: 74000000-1800-0000-4e6f-7465733a0d0a
1894018 Birth Domain ID: 0d0a6e65-6564-2074-6f20-676574206120
1894019
1894020 $DATA
1894021 0000000000: 4e 6f 74 65 73 3a 0d 0a 0d 0a 6e 65 65 64 20 74
1894022 0000000010: 6f 20 67 65 74 20 61 20 4d 53 52 20 36 30 35 20
1894023 0000000020: 66 6f 72 20 63 6c 6f 6e 69 6e 67 20 63 61 72 64
1894024 0000000030: 73 0d 0a 6e 65 65 64 20 74 6f 20 67 65 74 20 64
1894025 0000000040: 75 6d 70 73 20 66 72 6f 6d 20 64 61 72 6b 20 77
1894026 0000000050: 65 62 0d 0a 0d 0a 73 74 6f 72 65 20 6d 79 20 70
1894027 0000000060: 61 73 73 77 6f 72 64 73 20 28 50 61 73 73 77 6f
1894028 0000000070: 72 64 31 29
1894029
1894030 ****
```

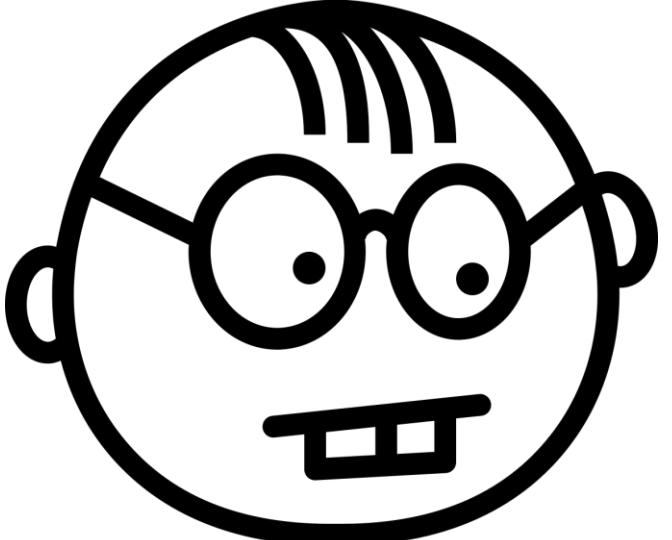
Notes:....need.t
o.get.a.MSR.605.
for.cloning.card
s..need.to.get.d
umps.from.dark.w
eb....store.my.p
asswords.(Passwo
rd1)



\$STD_INFO & \$FILE_NAME

```
change.log log.txt vol_plugins.txt vol_plugins_verbose.txt mft.txt

351068
351069 ****
351070 ****
351071 MFT entry found at offset 0x11bc1c00
351072 Attribute: In Use & File
351073 Record Number: 187831
351074 Link count: 1
351075
351076
351077 $STANDARD_INFORMATION ←
351078 Creation Modified MFT Altered Access Date Type
351079 -----
351080 2018-04-17 21:28:35 UTC+0000 2017-11-02 02:28:57 UTC+0000 2017-11-15 14:17:33 UTC+0000 2018-04-17 21:28:35 UTC+0000 Archive
351081
351082 $FILE_NAME ←
351083 Creation Modified MFT Altered Access Date Name/Path
351084 -----
351085 2018-04-17 21:28:35 UTC+0000 2018-04-17 21:28:35 UTC+0000 2018-04-17 21:28:35 UTC+0000 2018-04-17 21:28:35 UTC+0000 :
351086 E:\credit cards.txt
351087 $DATA
351088
351089 $OBJECT_ID
351090 Object ID: 40000000-0000-0000-0010-000000000000
351091 Birth Volume ID: 52090000-0000-0000-5209-000000000000
351092 Birth Object ID: 41017be5-ea0b-0000-ffff-ffff82794711
351093 Birth Domain ID: 00000000-0000-0000-000000000000
351094
351095 ****
351096 ****
351097 ****
```



User Artifacts

- User Processes
- Browser history
- Prefetch

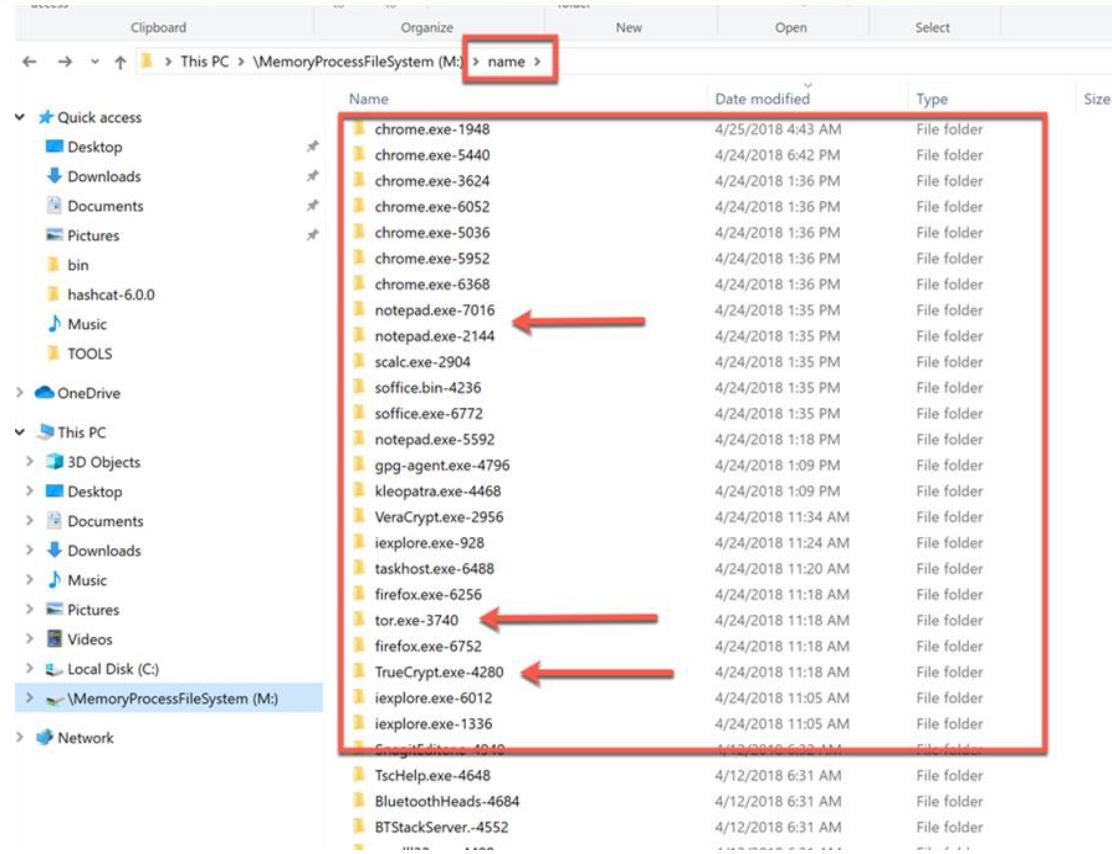
pslist

mem-4n6@nitro:~/Desktop/LABS/MEM-DUMPS/MoneyMaker\$ vol.py -f data.lime pslist

Volatility Foundation Volatility Framework 2.6

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa800390d870	System	4	0	136	675	-	0	2018-04-12 10:33:07 UTC+0000	
0xfffffa8005859920	smss.exe	0xfffffa8003b3cb10	iFrmewrk.exe	2988	3920	10	250	1	0 2018-04-12 13:30:41 UTC+0000
0xfffffa800679eb10	csrss.exe	0xfffffa80044a5b10	BTTray.exe	3968	3920	11	248	1	0 2018-04-12 13:30:41 UTC+0000
0xfffffa8006ecf790	wininit.exe	0xfffffa80044c0b10	Snagit32.exe	3044	3920	19	496	1	1 2018-04-12 13:30:41 UTC+0000
0xfffffa8006ed9060	csrss.exe	0xfffffa80044b92f0	StikyNot.exe	3992	3920	8	143	1	0 2018-04-12 13:30:41 UTC+0000
0xfffffa8006f4bb10	services.exe	0xfffffa80044b36f0	unsecapp.exe	2884	752	3	78	1	0 2018-04-12 13:30:41 UTC+0000
0xfffffa8006f292a0	lsass.exe	0xfffffa800459b900	SnagPriv.exe	2888	3044	5	81	1	1 2018-04-12 13:30:48 UTC+0000
0xfffffa8006f31b10	lsm.exe	0xfffffa800456cb10	svchost.exe	3900	580	12	382	0	0 2018-04-12 13:30:50 UTC+0000
0xfffffa8005b77b10	winlogon.exe	0xfffffa80046bbb10	rundll32.exe	4408	3968	1	58	1	1 2018-04-12 13:31:01 UTC+0000
0xfffffa800716eb10	svchost.exe	0xfffffa80046c5b10	BTStackServer.	4552	752	22	334	1	0 2018-04-12 13:31:06 UTC+0000
0xfffffa800718fb10	nvsvc.exe	0xfffffa80046f9060	BluetoothHeads	4684	4552	1	29	1	1 2018-04-12 13:31:08 UTC+0000
0xfffffa80071ae9c0	svchost.exe	0xfffffa80079f8b10	TscHelp.exe	4648	3044	1	58	1	1 2018-04-12 13:31:35 UTC+0000
0xfffffa8007242b10	svchost.exe	0xfffffa8008680b10	SnagitEditor.e	4940	3044	21	556	1	1 2018-04-12 13:32:11 UTC+0000
0xfffffa8007261b10	svchost.exe	0xfffffa80077ffb10	iexplore.exe	1336	3920	11	660	1	0 2018-04-24 18:05:40 UTC+0000
0xfffffa8007280b10	svchost.exe	0xfffffa8008440b10	Lexplorer.exe	6012	1336	19	819	1	1 2018-04-24 18:05:41 UTC+0000
0xfffffa80065f7b10	svchost.exe	0xfffffa8009e99060	TrueCrypt.exe	4280	3920	5	214	1	1 2018-04-24 18:18:22 UTC+0000
0xfffffa80067bf060	svchost.exe	0xfffffa800a327060	firefox.exe	6752	3920	51	617	1	1 2018-04-24 18:18:24 UTC+0000
0xfffffa8006838060	wlanext.exe	0xfffffa8009eb8060	tor.exe	3740	6752	3	77	1	1 2018-04-24 18:18:33 UTC+0000
0xfffffa8006833060	conhost.exe	0xfffffa8003ef9730	firefox.exe	6256	6752	24	318	1	1 2018-04-24 18:18:50 UTC+0000
0xfffffa8005c12060	spoolsv.exe	0xfffffa800a492060	taskhost.exe	6488	580	6	268	1	0 2018-04-24 18:20:06 UTC+0000
0xfffffa8005c09b10	svchost.exe	0xfffffa800492060	iexplore.exe	928	1336	16	535	1	1 2018-04-24 18:24:30 UTC+0000
0xfffffa8007512b10	svchost.exe	0xfffffa8008fd0430	VeraCrypt.exe	2956	3920	7	262	1	0 2018-04-24 18:34:21 UTC+0000
0xfffffa8007556220	btdwins.exe	0xfffffa8009975180	kleopatra.exe	4468	3920	8	395	1	1 2018-04-24 20:09:38 UTC+0000
0xfffffa800755a330	svchost.exe	0xfffffa80093c8060	gpg-agent.exe	4796	5616	3	95	1	1 2018-04-24 20:09:58 UTC+0000
0xfffffa8007567b10	EvtEng.exe	0xfffffa80099c7760	kleopatra.exe	3632	3920	0	-----	1	0 2018-04-24 20:10:25 UTC+0000
0xfffffa8007577b10	RegSrvc.exe	0xfffffa80099c7760	kleopatra.exe	2324	3920	0	-----	1	0 2018-04-24 20:15:38 UTC+0000
0xfffffa800761bb10	UploaderSrv	0xfffffa8009946b10	notepad.exe	2636	3920	0	-----	1	0 2018-04-24 20:18:34 UTC+0000
0xfffffa8006756060	ZeroConfigSe	0xfffffa8004619340	scalc.exe	5592	3920	1	62	1	0 2018-04-24 20:18:50 UTC+0000
0xfffffa8003a9f060	svchost.exe	0xfffffa80084f48c0	soffice.exe	2904	3920	1	16	1	0 2018-04-24 20:35:13 UTC+0000
0xfffffa80067b2330	WUDFHost.exe	0xfffffa8008fb060	soffice.bin	6772	2904	1	23	1	0 2018-04-24 20:35:13 UTC+0000
0xfffffa8007791b10	svchost.exe	0xfffffa8009836b10	notepad.exe	4236	6772	20	273	1	0 2018-04-24 20:35:13 UTC+0000
0xfffffa80077ab060	unsecapp.exe	0xfffffa800870cb10	notepad.exe	2144	3920	1	62	1	0 2018-04-24 20:35:30 UTC+0000
		0xfffffa800870cb10	notepad.exe	7016	3920	1	62	1	0 2018-04-24 20:35:34 UTC+0000
		0xfffffa800870cb10	chrome.exe	6368	3920	31	1070	1	0 2018-04-24 20:36:21 UTC+0000

Processes by Name

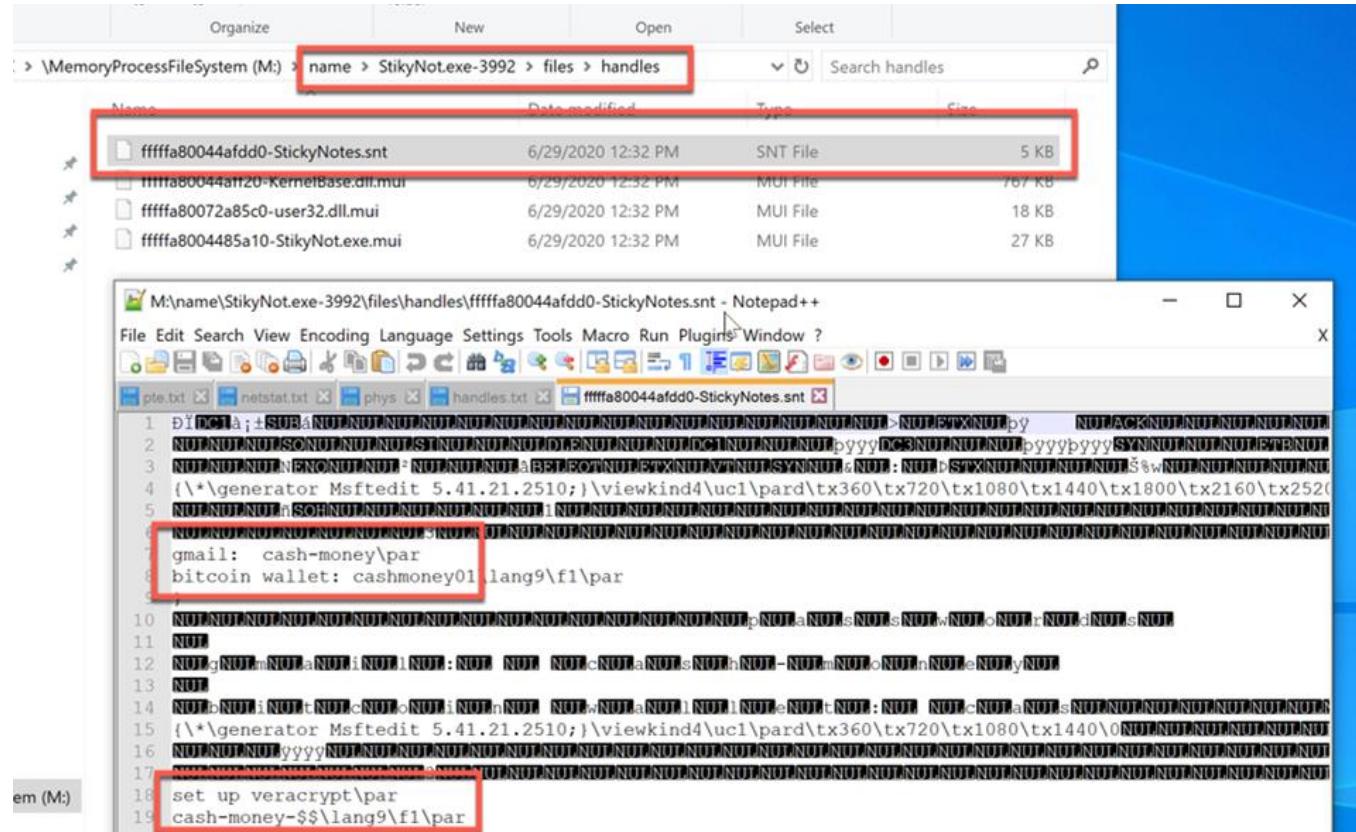


MemProcFS verbose tree

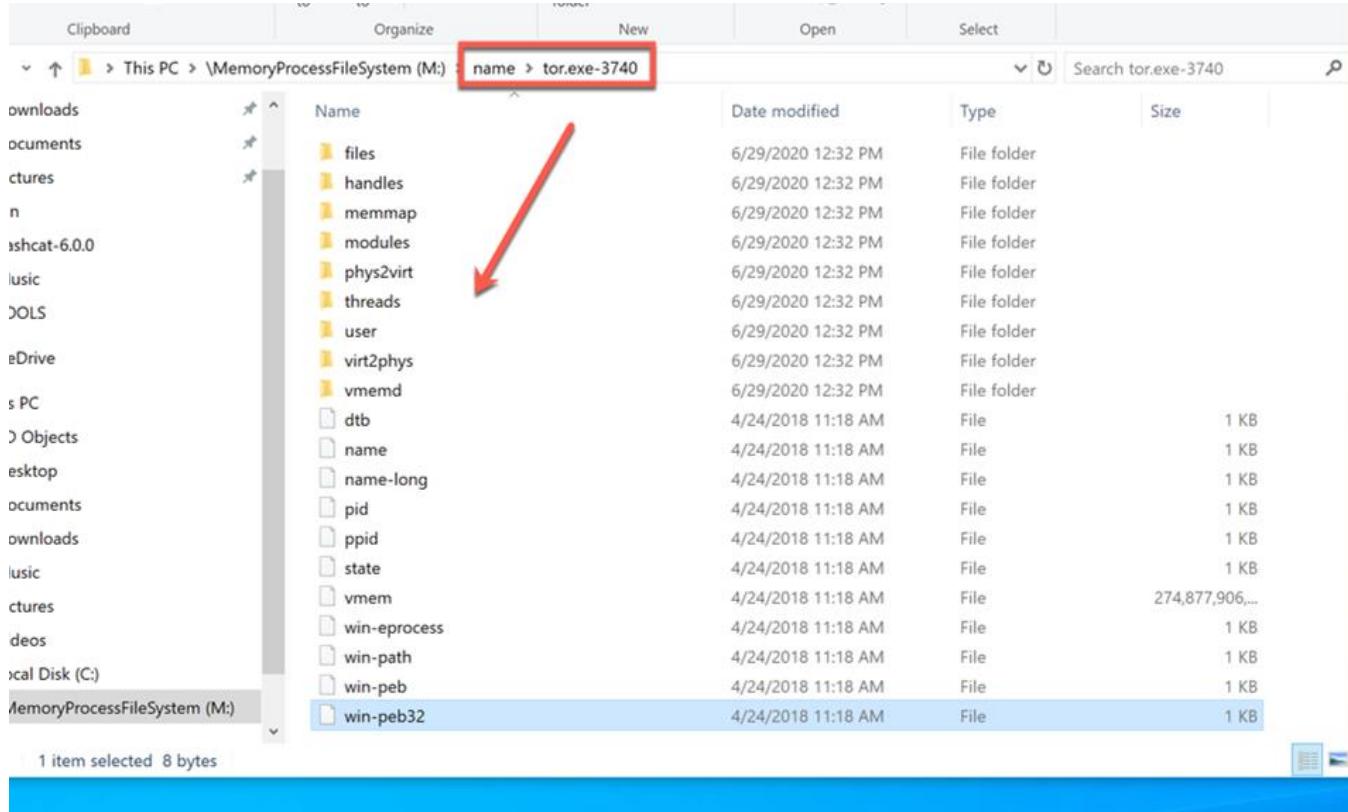
The screenshot shows a Windows File Explorer window with the path `\MemoryProcessFileSystem (M:) > sysinfo > proc` highlighted by a red box. Below the file list, a Notepad window is open with the title `tree-v - Notepad`. The Notepad content displays a verbose tree of processes:

Process	Pid	Parent	Flag	User	Path / Command Line
- System	4	0		SYSTEM	System
-- smss.exe	332	4		SYSTEM	<code>\Device\HarddiskVolume2\Windows\System32\smss.exe</code> <code>\SystemRoot\System32\smss.exe</code> <code>\SystemRoot\System32\smss.exe</code>
- csrss.exe	444	432		SYSTEM	<code>\Device\HarddiskVolume2\Windows\System32\csrss.exe</code> <code>C:\Windows\system32;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\TaskHost.exe</code>
-- conhost.exe	1280	444		SYSTEM	<code>\Device\HarddiskVolume2\Windows\System32\conhost.exe</code>
- wininit.exe	512	432		SYSTEM	<code>\Device\HarddiskVolume2\Windows\System32\wininit.exe</code>
-- services.exe	580	512		SYSTEM	<code>\Device\HarddiskVolume2\Windows\System32\services.exe</code> <code>C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows\.;C:\Windows\system32</code>
-- svchost.exe	124	580		LOCAL SERVICE	<code>\Device\HarddiskVolume2\Windows\System32\svchost.exe</code> <code>C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows\.;C:\Windows\system32</code>
-- svchost.exe	392	580		SYSTEM	<code>\Device\HarddiskVolume2\Windows\System32\svchost.exe</code> <code>C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows\.;C:\Windows\system32</code>

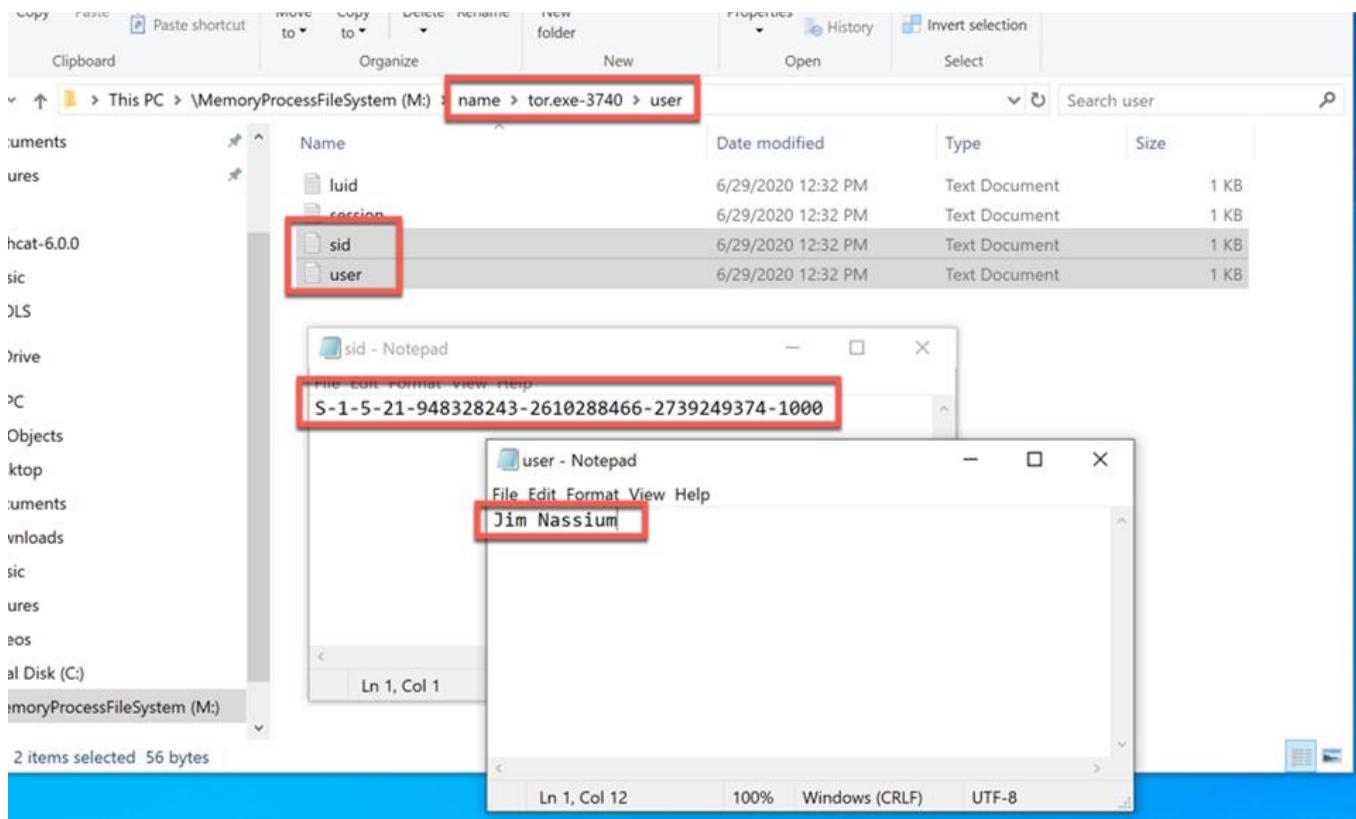
Process analysis



Executable process analysis



Executable process analysis



Analyzing user processes

```
File Edit View Search Terminal Help  
mem-4n6@nitro:~/Desktop/LABS/MEM-DUMPS/MoneyMaker$ vol.py -f data.lime firefoxhistory > firefoxHX.txt  
Volatility Foundation Volatility Framework 2.6  
mem-4n6@nitro:~/Desktop/LABS/MEM-DUMPS/MoneyMaker$ ll  
total 4150192  
drwxrwxrwx 3 mem-4n6 mem-4n6 4096 Mar 29 13:42 /  
drwxr-xr-x 9 mem-4n6 mem-4n6 4096 Feb 23 17:35 ../  
-rwxrwxrwx 1 mem-4n6 mem-4n6 4249772192 Apr 25 2018 data.lime*  
drwxr-xr-x 2 mem-4n6 mem-4n6 4096 Mar 27 16:54 dumpfiles/  
-rw-r--r-- 1 mem-4n6 mem-4n6 1692 Mar 29 13:44 firefoxHX.txt  
mem-4n6@nitro:~/Desktop/LABS/MEM-DUMPS/MoneyMaker$
```

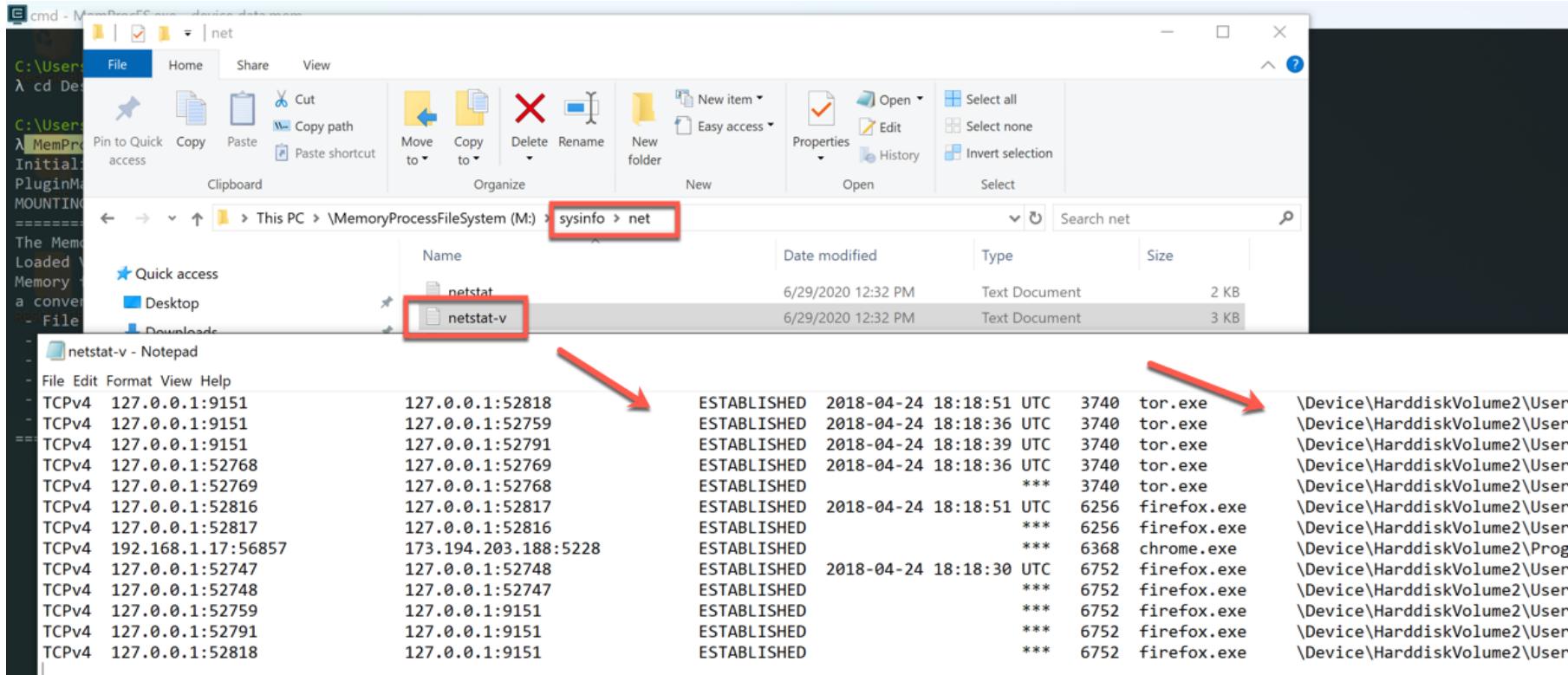
firefoxHX.txt - SciTE

ID	URL	Title
4	ACKplace:type=6&sort=14&maxResults=	
3	ACKplace:sort=8&maxResults=	
2	ENOhttps://blog.torproject.or	
1	ENOhttps://www.torproject.or	

Chrome search terms

Row ID	Keyword ID	URL ID	Lowercase	Entered Text
25	2	84	scarface	scarface
24	2	83	scarface	scarface
23	2	82	scar face	scar face
22	2	79	create private key wingpg	create private key wingpg
21	2	77	create private key gpg	create private key gpg
20	2	76	create private key	create private key
19	2	72	gmail	gmail
18	2	65	office libre download	office libre download
17	2	60	emule	emule
16	2	59	ip2p	ip2p
15	2	58	p2p	p2p
14	2	54	pgp for windows	pgp for windows
13	2	52	carding forums	carding forums
12	2	49	printing id cards forums	printing id cards forums
11	2	43	printing id cards	printing id cards
10	2	36	free bitcoin wallet	free bitcoin wallet
9	2	32	how to get bitcoins	how to get bitcoins
8	2	31	bitcoin	bitcoin
7	2	30	bitcoin	bitcoin
4	2	11	truecrypt download	truecrypt download
3	2	8	tor	tor
2	2	7	how to clone stolen credit cards	how to clone stolen credit cards
6	7	27	msr 605	msr 605
5	2	25	ebay	ebay
24	2	84	scarface	scarface
23	2	83	scarface	scarface
22	2	82	scar face	scar face
21	2	79	create private key wingpg	create private key wingpg
20	2	77	create private key gpg	create private key gpg
19	2	76	create private key	create private key
18	2	72	gmail	gmail
17	2	65	office libre download	office libre download
16	2	60	emule	emule

Netstat verbose - connections



prefetch

```
mem-4n6@nitro:~/Desktop/LABS/MEM-DUMPS/MoneyMaker$ vol.py -f data.lime prefetchparser
```

Prefetch file	Execution Time	Times	Size
SPPSVC.EXE-B0F8131B.PF	2018-04-25 11:54:44 UTC+0000	18	78240
CONHOST.EXE-1F3E9D7E.PF	2018-04-25 16:44:20 UTC+0000	198	18662
CHROME.EXE-D999B1BA.PF	2018-04-25 14:15:01 UTC+0000	47	42242
WUAUCLT.EXE-70318591.PF	2018-04-25 15:49:56 UTC+0000	36	75552
CMD.EXE-4A81B364.PF	2018-04-25 16:41:50 UTC+0000	1	9614
VSSVC.EXE-B8AFC319.PF	2018-04-25 10:00:14 UTC+0000	39	35090
GPGME-W32SPAWN.EXE-6E6D6464.PF	2018-04-25 16:17:29 UTC+0000	52	11486
GPG.EXE-6065ABF5.PF	2018-04-25 16:17:29 UTC+0000	34	21786
BDEUISRV.EXE-4D0648DC.PF	2018-04-25 16:41:18 UTC+0000	1	25244
FIREFOX.EXE-A90CFF.PF	2018-04-24 18:18:24 UTC+0000	10	249792
TASKHOST.EXE-7238F31D.PF	2018-04-25 16:05:19 UTC+0000	92	52560
DRVINST.EXE-4CB4314A.PF	2018-04-24 18:17:02 UTC+0000	36	55490
GPGME-W32SPAWN.EXE-6E6D6464.PF	2018-04-25 16:17:29 UTC+0000	52	11486
CONSENT.EXE-531BD9EA.PF	2018-04-25 16:41:48 UTC+0000	38	270124
AUDIODG.EXE-BDFD3029.PF	2018-04-25 16:41:11 UTC+0000	41	27662
GPG.EXE-6065ABF5.PF	2018-04-25 16:17:29 UTC+0000	34	21786
CONSENT.EXE-531BD9EA.PF	2018-04-25 16:41:48 UTC+0000	38	270124
TASKHOST.EXE-7238F31D.PF	2018-04-25 16:05:19 UTC+0000	92	52560
FIREFOX.EXE-A90CFF.PF	2018-04-24 18:18:24 UTC+0000	10	249792
AUDIODG.EXE-BDFD3029.PF	2018-04-25 16:41:11 UTC+0000	41	27662

Password Cracking

Access USER credentials



User LM & NTLM password hashes



cmd

```
T:\MEM_IMAGES\MONEY MAKER PC\Carding Case\MEM_DUMP
\ volatility -f data.lime --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jim Nassium:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6202d74bed778d6217cd01e62ac22521:::
Sally Butterfield:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
T:\MEM_IMAGES\MONEY MAKER PC\Carding Case\MEM_DUMP
```

hashdump plugin

The screenshot shows a Windows command prompt window and a Notepad++ application window.

In the command prompt (cmd), the user is executing the following command:

```
T:\MEM_IMAGES\MONEY MAKER_PC\Carding_Case\MEM_DUMP
λ volatility -f data.lime --profile=Win7SP1x64 hashdump > hashdump.txt
```

The command is highlighted with a red box.

After running the command, the directory listing shows the generated file:

```
T:\MEM_IMAGES\MONEY MAKER_PC\Carding_Case\MEM_DUMP
λ ls
data.lime      MoneyMaker-PC
hashdump.txt    PAGE_BRUTE-2018-08-07-09-22-51-RESULTS
MTC           registry_dump
                           surge.exe
                           timeliner.body
                           timeliner.csv
```

The file "hashdump.txt" is also highlighted with a red box.

The Notepad++ window displays the contents of the "hashdump.txt" file:

```
hashdump.txt
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
3 Jim Nassium:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
4 HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6202d74bed//8d6217cd01e62ac22521:::
5 Sally Butterfield:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
6
```

The lines for "Jim Nassium", "HomeGroupUser\$", and "Sally Butterfield" are highlighted with red boxes.

At the bottom of the Notepad++ window, status information is displayed:

```
Normal text file | length : 438 | lines : 6 | Ln : 1 | Col : 1 | Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS | . . .
```

Using NTLM hash to get password

The screenshot shows the CrackStation online password cracking interface. On the left, there's a banner for 'CrackStation' and a sidebar with 'CrackStation' and 'Password Hashing Services'. A red box highlights the URL 'https://crackstation.net' in the browser bar. In the center, a Notepad++ window displays a 'hashdump.txt' file containing a list of hashes. A red box highlights the third entry: 'Jim Nassium:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::'. Below the Notepad window, a text input field says 'Enter up to 20 non-salted hashes, one per line.' with '64f12cddaa88057e06a81b54e73b949b' entered. A reCAPTCHA box is present. At the bottom, a table shows the cracked hash: 'Hash' (64f12cddaa88057e06a81b54e73b949b), 'Type' (NTLM), and 'Result' (Password1). A red arrow points from the 'Result' column to the cracked password.

D CrackStation - Online Password H X + T:\MEM_IMAGES\MONEY_MAKER_PC\Carding_Case\MEM_DUMP\hashdump.txt - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

https://crackstation.net

Apps YouTube TV VirusTotal

hashdump.txt

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0:::

Jim Nassium:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::

HomeGroupUser\$:1002:aad3b435b51404eeaad3b435b51404ee:6202d74bed778d6217cd01e62ac22521:::

Sally Butterfield:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0

Normal text file length : 438 lines : 6 Ln : 3 Col : 83 Sel : 32 | 1 Windows (CR LF) UTF-8 INS

Enter up to 20 non-salted hashes, one per line.

64f12cddaa88057e06a81b54e73b949b

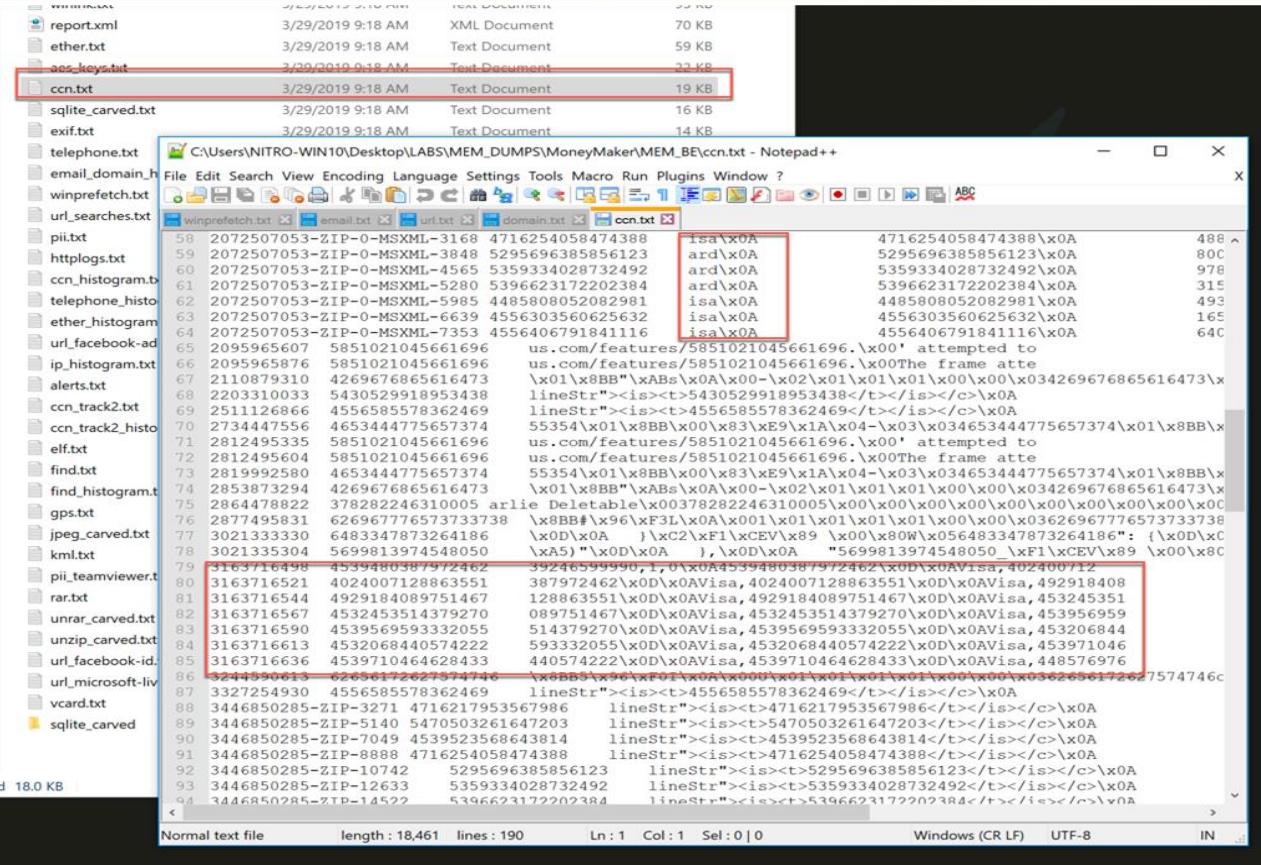
I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
64f12cddaa88057e06a81b54e73b949b	NTLM	Password1

bulk_extractor



The screenshot shows a file explorer window on the left and a Notepad++ window on the right. The file explorer lists several files, with 'ccn.txt' highlighted by a red box. The Notepad++ window displays the contents of 'ccn.txt', which is a text document with approximately 18,461 lines. The text content includes various log entries and system information, such as file paths and frame attributes. A second red box highlights a specific section of the text starting with 'isa\x0A'. The status bar at the bottom of the Notepad++ window indicates 'Normal text file', 'length : 18,461', 'lines : 190', 'Ln : 1', 'Col : 1', 'Sel : 0 | 0', 'Windows (CR LF)', 'UTF-8', and 'IN'.

hashdump + bulk_extractor + wordlist

The image shows two terminal windows side-by-side. The left window is titled 'cmd - bash' and contains the following command-line session:

```
PDX-FORENSICS@PPB-DFIR ~> /m/t/H/FINAL
$ ls
BE filescan malfind memdump.dmp procdump vaddump
PDX-FORENSICS@PPB-DFIR ~> /m/t/H/FINAL
$ vol.py -f memdump.dmp --profile=Win7SP1x86 hashdump
Volatility Foundation Volatility Framework 2.0
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Sue Smith:1000:aad3b435b51404eeaad3b435b51404ee:c39f2deb3d2ec06a62cd887fb391dee0:::
GhostUser:1001:aad3b435b51404eeaad3b435b51404ee:0efc7e09eff754a87835da9b55e9232f:::
PDX-FORENSICS@PPB-DFIR ~> /m/t/H/FINAL
$ |
```

The right window is titled 'cmd - bulk_extractor.exe -o - -e wordlist "T:\HTCIA 2018\FINAL\memdump.dmp"' and contains the following output:

```
T:\HTCIA 2018\FINAL\DC
bulk_extractor.exe -o - -e wordlist "T:\HTCIA 2018\FINAL\memdump.dmp"
bulk_extractor version: 1.5.5
Hostname: PPB-DFIR
Input file: T:\HTCIA 2018\FINAL\memdump.dmp
Output directory: .
Disk Size: 3210735616
Threads: 8
Attempt to open T:\HTCIA 2018\FINAL\memdump.dmp
9:39:08 Offset 67MB (2.09%) Done in 0:00:10 at 09:39:18
9:39:15 Offset 150MB (4.70%) Done in 0:02:56 at 09:42:12
9:39:18 Offset 234MB (7.32%) Done in 0:02:39 at 09:41:59
9:39:26 Offset 318MB (9.93%) Done in 0:02:51 at 09:42:17
9:39:35 Offset 402MB (12.54%) Done in 0:03:12 at 09:42:47
9:39:36 Offset 486MB (15.15%) Done in 0:02:47 at 09:42:24
9:39:45 Offset 570MB (17.77%) Done in 0:02:57 at 09:42:43
9:39:54 Offset 654MB (20.38%) Done in 0:03:06 at 09:43:01
9:40:11 Offset 738MB (22.99%) Done in 0:03:32 at 09:43:43
9:40:20 Offset 822MB (25.60%) Done in 0:03:33 at 09:43:54
9:40:30 Offset 905MB (28.22%) Done in 0:03:31 at 09:44:01
9:40:39 Offset 989MB (30.83%) Done in 0:03:25 at 09:44:04
9:40:45 Offset 1073MB (33.44%) Done in 0:03:16 at 09:44:02
9:40:53 Offset 1157MB (36.05%) Done in 0:03:09 at 09:44:03
9:41:00 Offset 1241MB (38.67%) Done in 0:02:58 at 09:43:58
9:41:07 Offset 1325MB (41.28%) Done in 0:02:51 at 09:43:59
9:41:15 Offset 1409MB (43.89%) Done in 0:02:45 at 09:44:02
9:41:23 Offset 1493MB (46.51%) Done in 0:02:36 at 09:44:00
9:41:28 Offset 1577MB (49.12%) Done in 0:02:27 at 09:43:57
9:41:36 Offset 1660MB (51.73%) Done in 0:02:18 at 09:43:54
9:41:41 Offset 1744MB (54.34%) Done in 0:02:09 at 09:43:50
9:41:46 Offset 1828MB (56.96%) Done in 0:02:01 at 09:43:49
9:41:51 Offset 1912MB (59.57%) Done in 0:01:52 at 09:43:45
9:41:56 Offset 1996MB (62.18%) Done in 0:01:42 at 09:43:39
9:42:01 Offset 2080MB (64.79%) Done in 0:01:34 at 09:43:35
9:42:05 Offset 2164MB (67.41%) Done in 0:01:27 at 09:43:35
9:42:10 Offset 2248MB (70.02%) Done in 0:01:18 at 09:43:30
9:42:16 Offset 2332MB (72.63%) Done in 0:01:11 at 09:43:28
9:42:21 Offset 2415MB (75.25%) Done in 0:01:03 at 09:43:24
```

Bulk extractor + wordlist

Share View

> This PC > TEMP (T:) > HTCIA 2018 > FINAL > BE

Name	Date modified	Type	Size
aes_keys	8/3/2018 9:39 AM	Text Document	0 KB
alerts	8/3/2018 9:39 AM	Text Document	0 KB
ccn	8/3/2018 9:39 AM	Text Document	0 KB
ccn_track2	8/3/2018 9:39 AM	Text Document	0 KB
domain	8/3/2018 9:39 AM	Text Document	0 KB
elf	8/3/2018 9:39 AM	Text Document	0 KB
email	8/3/2018 9:39 AM	Text Document	0 KB
ether	8/3/2018 9:39 AM	Text Document	0 KB
exif	8/3/2018 9:39 AM	Text Document	0 KB
find	8/3/2018 9:39 AM	Text Document	0 KB
gps	8/3/2018 9:39 AM	Text Document	0 KB
httplogs	8/3/2018 9:39 AM	Text Document	0 KB
ip	8/3/2018 9:39 AM	Text Document	0 KB
jpeg_carved	8/3/2018 9:39 AM	Text Document	0 KB
json	8/3/2018 9:39 AM	Text Document	0 KB
kml	8/3/2018 9:39 AM	Text Document	0 KB
pii	8/3/2018 9:39 AM	Text Document	0 KB
rar	8/3/2018 9:39 AM	Text Document	0 KB
report	8/3/2018 9:39 AM	XML Document	0 KB
rfc822	8/3/2018 9:39 AM	Text Document	0 KB
sqlite_carved	8/3/2018 9:39 AM	Text Document	0 KB
telephone	8/3/2018 9:39 AM	Text Document	0 KB
unrar_carved	8/3/2018 9:39 AM	Text Document	0 KB
unzip_carved	8/3/2018 9:39 AM	Text Document	0 KB
url	8/3/2018 9:39 AM	Text Document	0 KB
vcard	8/3/2018 9:39 AM	Text Document	0 KB
windirs	8/3/2018 9:39 AM	Text Document	0 KB

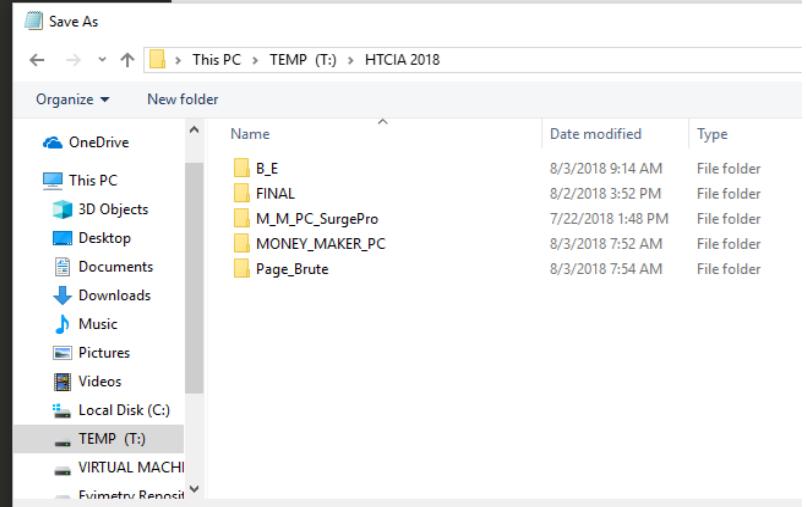
T:\HTCIA 2018\FINAL\BE
λ bulk_extractor.exe -o.\ -e wordlist "T:\HTCIA 2018\FINAL\memdump.dmp"
bulk_extractor version: 1.5.5
Hostname: PPB-DFIR
Input file: T:\HTCIA 2018\FINAL\memdump.dmp
Output directory: .\
Disk Size: 3210735616
Threads: 8
Attempt to open T:\HTCIA 2018\FINAL\memdump.dmp
9:39:08 Offset 67MB (2.09%) Done in 0:00:10 at 09:39:18

hashdump

```
cmd - bash
bash Home Share View
PDX-FORENSICS@PPB-DFIR -> ./m/t/H/M/C/M/M/2/memory
$ vol.py -f data.lime imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug    : Determining profile based on KDBG search...
INFO : volatility.debug    : Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : LimeAddressSpace (Unnamed AS)
AS Layer3 : FileAddressSpace (/mnt/t/HTCIA_2018/MONEY_MAKER_PC/Carding_Case/MEM_DUMP/MoneyMaker-PC/20180425094441/memory/data.lime)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002bfe110L
Number of Processors : 4
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffffff80002bffd00L
KPCR for CPU 1 : 0xfffffff8800310f000L
KPCR for CPU 2 : 0xfffffff88003180000L
KPCR for CPU 3 : 0xfffffff880031f1000L
KUSER_SHARED_DATA : 0xfffffff78000000000L
Image date and time : 2018-04-25 16:44:42 UTC+0000
Image local date and time : 2018-04-25 09:44:42 -0700
PDX-FORENSICS@PPB-DFIR -> ./m/t/H/M/C/M/M/2/memory
$ export VOLATILITY_PROFILE=Win7SP1x64
PDX-FORENSICS@PPB-DFIR -> ./m/t/H/M/C/M/M/2/memory
$ vol.py -f data.lime hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jim Nassium:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6202d74bed778d6217c01e62ac22521:::
Sally Butterfield:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PDX-FORENSICS@PPB-DFIR -> ./m/t/H/M/C/M/M/2/memory
$
```

```
unrar_carved
unzip_carved
url
vcard
windirs
```

```
Untitled - Notepad
File Edit Format View Help
64f12cddaa88057e06a81b54e73b949b
31d6cfe0d16ae931b73c59d7e0c089c0
```



wordlist

```
T:\HTCIA_2018\FINAL\BE
λ ls -la
total 93436
drw-rw-rw- 2 DFIR-PDX 0      8192 2018-08-03 09:43 .
drw-rw-rw- 7 DFIR-PDX 0      4096 2018-08-03 09:43 ..
-rw-rw-rw- 1 DFIR-PDX 0      462 2018-08-03 09:42 aes_keys.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 alerts.txt
-rw-rw-rw- 1 DFIR-PDX 0    13276 2018-08-03 09:43 ccn.txt
-rw-rw-rw- 1 DFIR-PDX 0    3710 2018-08-03 09:43 ccn_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 ccn_track2.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:43 ccn_track2_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0   921532 2018-08-03 09:43 domain.txt
-rw-rw-rw- 1 DFIR-PDX 0   12480 2018-08-03 09:43 domain_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 elf.txt
-rw-rw-rw- 1 DFIR-PDX 0   41747 2018-08-03 09:43 email.txt
-rw-rw-rw- 1 DFIR-PDX 0   1189 2018-08-03 09:43 email_domain_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0   7192 2018-08-03 09:43 email_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0   9758 2018-08-03 09:43 ether.txt
-rw-rw-rw- 1 DFIR-PDX 0   287 2018-08-03 09:43 ether_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0   2249 2018-08-03 09:43 exif.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 find.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:43 findhistogram.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 gps.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 httplogs.txt
-rw-rw-rw- 1 DFIR-PDX 0  22847 2018-08-03 09:43 ip.txt
-rw-rw-rw- 1 DFIR-PDX 0   212 2018-08-03 09:43 ip_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 jpeg_carved.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 json.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 kml.txt
-rw-rw-rw- 1 DFIR-PDX 0  72275 2018-08-03 09:43 packets.pcap
-rw-rw-rw- 1 DFIR-PDX 0  98931 2018-08-03 09:43 pii.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:43 pii_teamviewer.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 rar.txt
-rw-rw-rw- 1 DFIR-PDX 0  46436 2018-08-03 09:43 report.xml
-rw-rw-rw- 1 DFIR-PDX 0   5176 2018-08-03 09:43 rfc822.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 sqlite_carved.txt
-rw-rw-rw- 1 DFIR-PDX 0   357 2018-08-03 09:41 telephone.txt
-rw-rw-rw- 1 DFIR-PDX 0   212 2018-08-03 09:43 telephone_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 unrar_carved.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 unzip_carved.txt
-rw-rw-rw- 1 DFIR-PDX 0  5591632 2018-08-03 09:43 url.txt
-rw-rw-rw- 1 DFIR-PDX 0   207 2018-08-03 09:43 url_facebook-address.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:43 url_facebook-id.txt
-rw-rw-rw- 1 DFIR-PDX 0  147938 2018-08-03 09:43 url_histogram.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:43 url_microsoft-live.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:43 url_searches.txt
-rw-rw-rw- 1 DFIR-PDX 0   9524 2018-08-03 09:43 url_services.txt
-rw-rw-rw- 1 DFIR-PDX 0      0 2018-08-03 09:39 vcard.txt
-rw-rw-rw- 1 DFIR-PDX 0  27858002 2018-08-03 09:43 windirs.txt
-rw-rw-rw- 1 DFIR-PDX 0   123468 2018-08-03 09:43 winlnk.txt
-rw-rw-rw- 1 DFIR-PDX 0   6952413 2018-08-03 09:43 winpe.txt
-rw-rw-rw- 1 DFIR-PDX 0   16100 2018-08-03 09:43 winprefetch.txt
-rw-rw-rw- 1 DFIR-PDX 0  45656494 2018-08-03 09:43 wordlist.txt
-rw-rw-rw- 1 DFIR-PDX 0  7973386 2018-08-03 09:43 wordlist_split_000.txt
```



hashcat

cmd

C:\Forensic Tools\hashcat-4.0.1

λ ls

charsets	example400.cmd	extra	hashcat.potfile	OpenCL
docs	example400.hash	hashcat.dictstat2	hashcat32.bin	rules
example.dict	example400.sh	hashcat.exe	hashcat32.exe	show.log
example0.cmd	example500.cmd	hashcat.hcstat2	hashcat64.bin	
example0.hash	example500.hash	hashcat.hctune	kernels	
example0.sh	example500.sh	hashcat.log	masks	

C:\Forensic Tools\hashcat-4.0.1

λ |

hashcat + NTLM.TXT + wordlist_split

```
C:\Forensic Tools\hashcat-4.0.1  
λ hashcat.exe -m 1000 -a 0 "T:\HTCIA 2018\NTLM hash.txt" "T:\HTCIA 2018\wordlist_split_000.txt"
```

hashcat

```
C:\Forensic Tools\hashcat-4.0.1
\ hashcat.exe -m 1000 -a 0 "T:\HTCIA 2018\FINAL\NTLM hash.txt" "T:\HTCIA 2018\FINAL\wordlist_split_000.txt"
hashcat (v4.0.1) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
  This may cause "CL_OUT_OF_RESOURCES" or related errors.
  desktop
  To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: Intel's OpenCL runtime (GPU only) is currently broken.
  We are waiting for updated OpenCL drivers from Intel.
  You can use -force to override, but do not report related errors.
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL Platform #1: NVIDIA Corporation
=====
* Device #1: Quadro M1000M, 512/2048 MB allocatable, 4MCU

OpenCL Platform #2: Intel(R) Corporation
=====
* Device #2: Intel(R) HD Graphics 530, skipped.
* Device #3: Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz, skipped.

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

Password length minimum: 0
Password length maximum: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastical reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger disabled.

Dictionary cache built:
* Filename...: T:\HTCIA 2018\FINAL\wordlist_split_000.txt ←
* Passwords.: 768812
* Bytes....: 7973386
* Keyspace...: 768812
* Runtime...: 0 secs

0efc7e09eff754a87835da9b55e9232f:GhostUser
c39f2beb3d2ec06a62cb887fb391dee0:Password2

Session.....: hashcat
Status.....: Cracked
Hash.Type...: NTLM
```

IMAGE MOUNTING

Analysis of
Mounted
Encrypted
E01(USB)



Mounted USB – FS not recognized

AccessData FTK Imager 3.4.3.3

File View Mode Help

Evidence Tree File List

Mount Image To Drive

Add Image

Image File: T:\HTCIA 2018\MONEY_MAKER_PC\Carding_Case\DISK_IMAGES\USB\USB DISK 2.0.e01

Mount Type: Physical & Logical

Drive Letter: Next Available (E:)

Mount Method: File System / Read Only

Write Cache Folder: T:\HTCIA 2018\MONEY_MAKER_PC\Carding_Case\DISK_IMAGES\USB

Mount

Mapped Image List

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive3	Block Device/Read ...	Image	T:\HTCIA 2018\MONEY_MAKER_PC\Carding_Case\DISK_IMAGES\USB\USB DISK 2.0.e01
D:	File System/Read Only	Partition 1 [1908...]	T:\HTCIA 2018\MONEY_MAKER_PC\Carding_Case\DISK_IMAGES\USB\USB DISK 2.0.e01

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

File Computer View Drive Tools This PC

Quick access

OneDrive

This PC

3D Objects

Desktop

Documents

Downloads

Music

Pictures

Videos

Music

Pictures

Videos

Local Disk (C:)

Unrecognized file system (D:)

iCloud Photos

TEMP (T:)

VIRTUAL MACHINES (V:)

Evimetry Repository (W:)

CASE FILES (X:)

Evimetry Repository (W:)

Network

14 items 1 item selected

Local Disk (C:) 230 GB free of 475 GB

TEMP (T:) 309 GB free of 479 GB

VIRTUAL MACHINES (V:) 483 GB free of 953 GB

CASE FILES (X:) 421 GB free of 474 GB

Unrecognized file system (D:) 0 bytes free of 1.86 GB

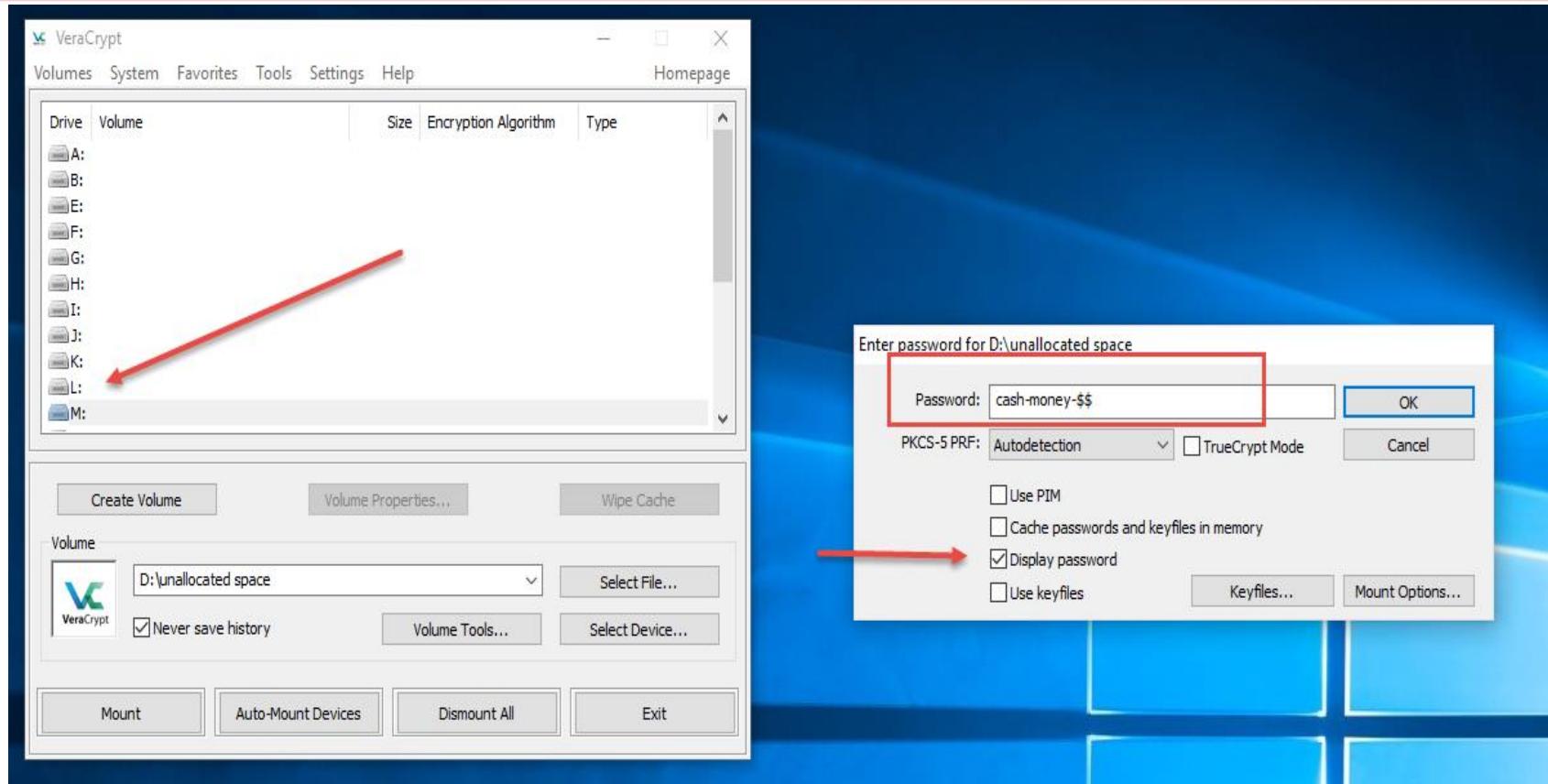
Evimetry Repository (W:) 0 bytes free of 0 bytes AFF4FS

Custom VeraCrypt plugin

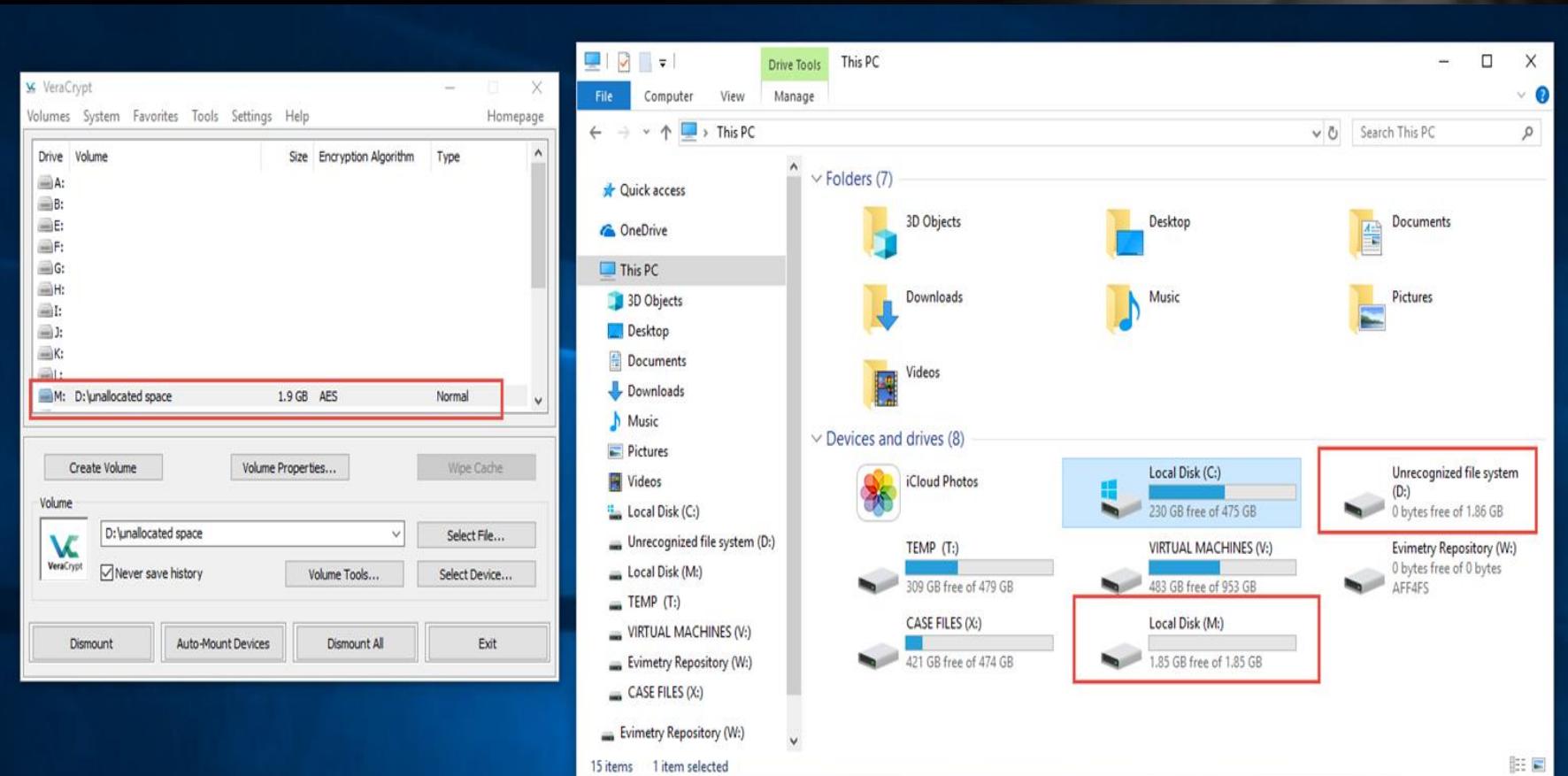
```
T:\HTCIA_2018\MONEY_MAKER_PC\Carding_Case\MEM_DUMP
T:\HTCIA_2018\MONEY_MAKER_PC\Carding_Case\MEM_DUMP
\ volatility --plugins=C:\Users\DFIR-PDX\Documents\VeraCrypt -f data.lime --profile=Win7SP1x64 veracryptsummary
Volatility Foundation Volatility Framework 2.6

Password          cash-money-$$ at offset 0xfffffff8800db30b44
Process           VeraCrypt.exe at 0xfffffa8008fd0430 pid 2956
Service           veracrypt state SERVICE_RUNNING
Kernel Module    veracrypt.sys at 0xfffffff8800da68000 - 0xfffffff8800db36000
Symbolic Link    Volume{dfa2cca3-3e3c-11e8-b630-e4d53de2a2b9} -> \Device\VeracryptVolume5 mounted 2018-04-24 19:51:26 UTC+0000
File Object      \Device\VeracryptVolume5\ at 0x129362d40
File Object      \Device\VeracryptVolume5\ at 0x12a6c85d0
File Object      \Device\VeracryptVolume5\ at 0x12a81df20
File Object      \Device\VeracryptVolume5\the goods.xlsx at 0x12a90df20
File Object      \Device\VeracryptVolume5\ at 0x12d2bd6e0
Driver           \Driver\veracrypt at 0x12d33f150 range 0xfffffff8800da68000 - 0xfffffff8800db36000
Device           VeraCryptVolume5 at 0xfffffa8009547080 type FILE_DEVICE_DISK
Container        Path: <HIDDEN>
Device           VeraCrypt at 0xfffffa800582ed30 type FILE_DEVICE_UNKNOWN
```

Mounting + VeraCrypt + password



Mounted USB – FS recognized!



We found it!

The screenshot shows a Windows desktop environment with several windows open:

- VeraCrypt**: A file manager window showing drives A:I. A red box highlights the "credit cards - Notepad" file.
- Local Disk (M:)**: An Explorer window showing files on the Local Disk (M:). A red box highlights the "credit cards", "Stolen CC - Copy", and "the goods" files.
- credit cards - Notepad**: A text file containing the text: "this is were I will store all my stolen credit cards!"
- the goods - Excel**: An Excel spreadsheet with data. A red box highlights the entire sheet.
- IssuingNetwork,CardNumber**: A text file listing card numbers and their details.

The Excel spreadsheet (**the goods - Excel**) contains the following data:

Gender	MiddleName	Surname	StreetAdd	City	StateFull	ZipCode	Country	EmailAddi	Username	Password	BrowserU	Telephon	Telephon	Birthday	Age	CCType	CCNumbe	CVV2	CCExpires	Nationalit	UPS	Occupatio	Com
male	M	Adams	648 Kenne	Westboro	Massachu	01581	US	GeorgeMj	Spleace	eeThaip	Mozilla/5.7	774-276	71	1/8/1966	52	Visa	471621795	736	1/2021	012-07-92	12 216	470 Arc	cutter Opti
female	E	Brown	630 Viking	Adamsvill	Ohio	43701	US	MadelynE	Facatte	ahk5Ooto	Mozilla/5.7	470-796	6-1	12/10/193	82	MasterCar	54705032	465	6/2023	286-30-67	12 4A1	16	C(heical Cou
female	G	Cook	3096 Mod	Saint Mar	Idaho	83861	US	ChristieG	Kedis1945	EeThe40c	Mozilla/5.	208-245	6-1	8/17/1945	72	Visa	4359235	674	8/2022	519-57-67	12 4Y7	649	Foot doct Met
female	R	Meredith	2493 Lone Mobile	Alabama		36607	US	AngelaRM	Meaire199	Vaizai9Ae	Mozilla/5.	251-473	8-1	11/25/199	21	Visa	471625405	488	4/2020	419-62-39	12 78	7V7	Choke set Whi
female	T	Hann	363 Paul V	Kenner	Louisiana	70065	US	MaryThan	Spitiied	EadObidigt	Mozilla/5.	504-469	3-1	3/3/1996	22	MasterCar	52956963	800	10/2021	439-22-91	12 106	702	Pharmacy Fort
male	C	Gulley	471 Geral	New York	New York	10007	US	RaymondL	lifertake	euy0Wee	Mozilla/5.	646-357	2-1	6/15/1956	61	MasterCar	53593340	978	5/2023	084-72-57	12 6W6	64	Geophysic Sha
female	P	Leclair	4367 Hartl	Appleton	Wisconsin	54914	US	LauraPlec	Frooking1	ap2hZoh1	Mozilla/5.	920-358	7-1	7/19/1977	40	MasterCar	53966231	315	12/2020	387-88-67	12 009	11V	Tile instal Dah
male	A	Penn	2590 Jeffre	Norfolk	Virginia	23510	US	CurtisAPe	Beetim	thuveeF6	Mozilla/5.	757-746	3-1	8/15/1982	35	Visa	448580805	493	3/2022	695-03-78	12 397	Y80	Home apc Lico
female	M	Kernan	3806 Post	Atlanta	Georgia	30309	US	BettyMKe	Sainle	OoKAAlo2	Mozilla/5.	404-236	4-1	7/2/1997	20	Visa	45563035	165	5/2020	669-16-92	12 A39	0A	Loan colle Roa
male	L	Henry	2757 Roge	Cincinnati	Ohio	45202	US	DiegoLei	Straboy	ekiejeUi	Mozilla/5.	513-555	4-1	12/31/198	32	Visa	455640675	640	10/2021	292-38-08	12 374	048	Detective Cup
female	A	Parr	1673 Chan Homestea	Pennsylvan		15120	US	Consuelo	Shatareat	ceTh9ahb	Mozilla/5.	412-462	5-1	6/5/1968	49	MasterCar	51657533	109	2/2020	183-74-53	12 9A3	87	Forrest an Mor
female	S	Whitney	3293 Sheri Salina	Kansas		67401	US	CriseildaS	Raine1978	gaerchilD	Mozilla/5.	785-823	2-1	3/21/1978	40	MasterCar	535494598	165	1/2020	515-58-39	12 F27	A05	Taper Desi
female	J	Rivera	4921 Kova	Framingh	Massachu	01702	US	MicheleJR	Pround	tahl1Co2	Mozilla/5.	508-555	2-1	5/4/1990	27	Visa	455676446	138	4/2021	024-60-08	12 E35	956	Forest fire Giar
female	F	Heffner	2735 Harry	Charlotte	North Car	28202	US	LynetteFH	Bleaked3	ieH2niada	Mozilla/5.	704-772	1-1	2/2/1933	85	MasterCar	517696773	720	1/2020	243-94-07	12 719	7A	Employm Mu
female	F	Holmes	2538 Have Three Riv	Michigan		49093	US	CarolineFi	Drete1935	ghGawoo	Mozilla/5.	517-617	2-1	2/14/1993	79	Visa	471634276	315	2/2023	372-88-99	12 082	131	Transport: Gam
male	B	Aguilar	1037 Bedf	Stamford	Connecticut	06901	US	SeanBagu	InC1989	gatato	Mozilla/5.	203-964	0-1	4/15/1989	29	MasterCar	552697048	101	9/2020	045-96-82	12 9W9	55	Financial Tken
male	M	Arrington	1818 Kessi	Conway	South Carr	29528	US	BenitoMA	Paill1965	ahh5yeeP	Mozilla/5.	843-349	5-1	9/2/1965	52	Visa	24854730	371	5/2019	655-03-55	12 E61	W2	Announce Shol
female	P	Fox	3387 Black	Winchest	Kentucky	40391	US	ClaudiaPF	Havesiont	ahuOpPe	Mozilla/5.	859-473	9-1	7/31/1981	36	MasterCar	53145724	665	4/2023	404-50-74	12 964	8483	Construct Kids
female	A	Phillips	4296 Gami	Houston	Texas	77586	US	CynthiaAF	Wherrien	Awa9uTu	Mozilla/5.	281-909	7-1	8/19/1948	69	Visa	471693911	232	4/2020	454-52-30	12 209	932	Food serv Plan
male	L	Bell	2922 Stroc	Atlanta	Georgia	30303	US	ScottBell	Frompard	iecohch	Mozilla/5.	404-880	7-1	4/10/1998	20	MasterCar	52065733	756	6/2021	667-22-39	12 269	7A	Diessel me Twir
male	V	Wegener	4705 India	Moanalua	Hawaii	96819	US	MarvinW	Forle1983	aiu9aCei	Mozilla/5.	808-645	7-1	4/29/1983	34	Visa	471644086	420	3/2020	751-05-09	12 8Y6	692	Communi W. E

Keeping up with memory?

Take a class!

- Malware and Memory Forensics Training (Volatility)
[https://www.memoryanalysis.net/
memory-forensics-training](https://www.memoryanalysis.net/memory-forensics-training)
- SANS FOR526: Advanced Memory Forensics & Threat Detection
[https://www.sans.org/course/
memory-forensics-in-depth](https://www.sans.org/course/memory-forensics-in-depth)
- Magnet Forensics AX250: Advanced Forensics
[https://www.magnetforensics.co
m/digital-forensics-
training/magnet-axiom-advanced-
computer-forensics/](https://www.magnetforensics.com/digital-forensics-training/magnet-axiom-advanced-computer-forensics/)

Aaron Sparling	@OSINTlabworks
Alissa Torres	@sibertor
Andrew Case	@attrc
Jamie Levy	@gleeda
Michael Ligh (MHL)	@iMHLv2
Richard Davis	@davisrichardg
Volatility	@volatility

The Twitter logo, consisting of the word "Twitter" in its signature white sans-serif font, centered on a dark blue background.



Making Memories

Workflow Guide

<https://bit.ly/3fbGkVh>

Questions ?

AARON SPARLING

JESSICA HYDE

@OSINTLabworks

@B1N2H3X