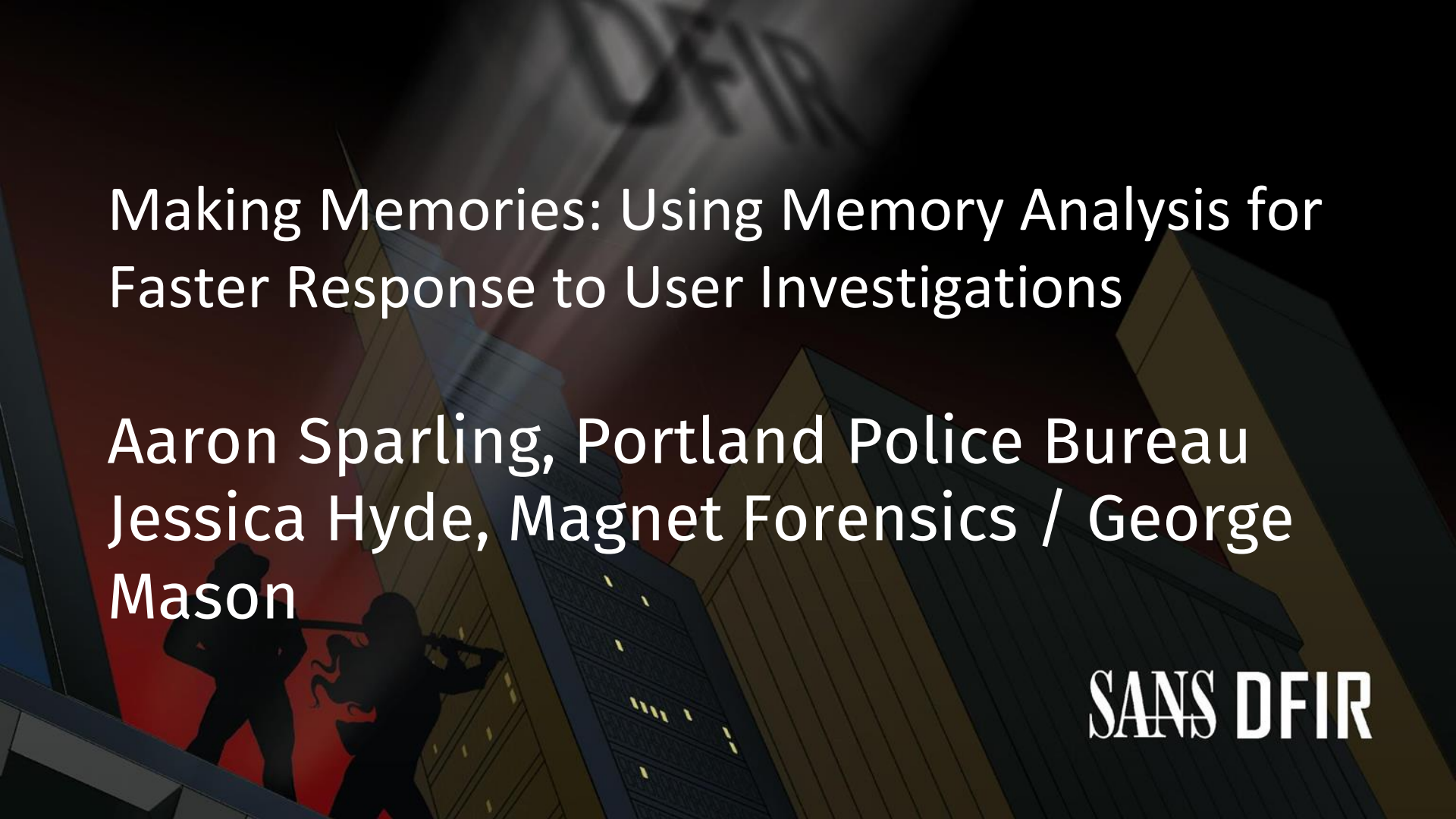


Making Memories: Using Memory Analysis for Faster Response to User Investigations

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

SANS DFIR

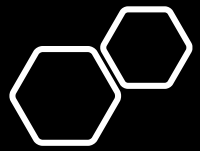
Making Memories

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

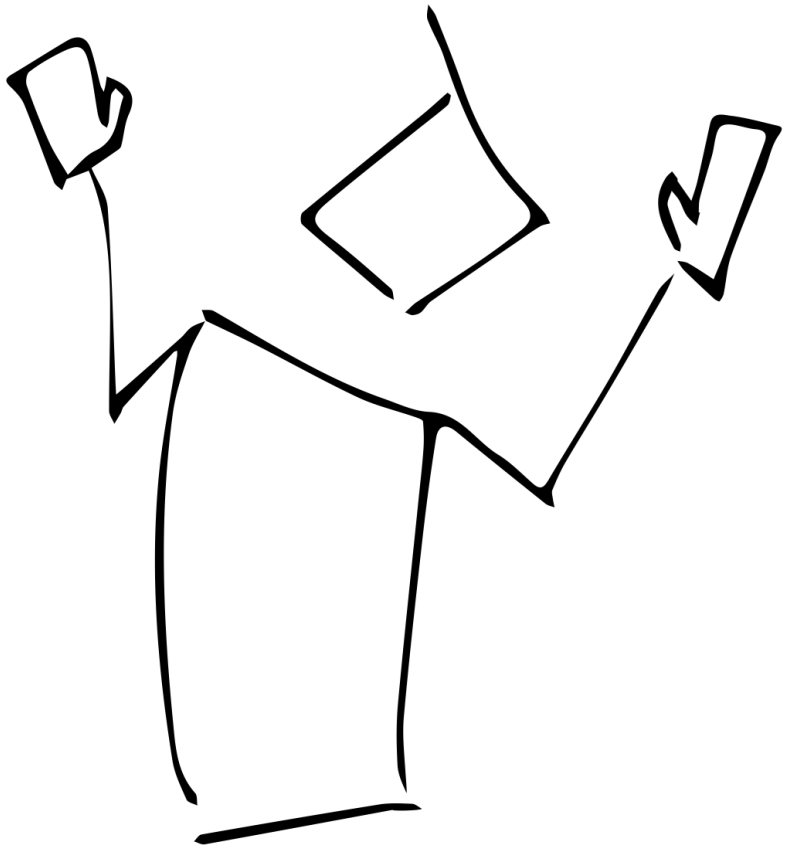


So you're an Incident Responder…. I know about memory

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:

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

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

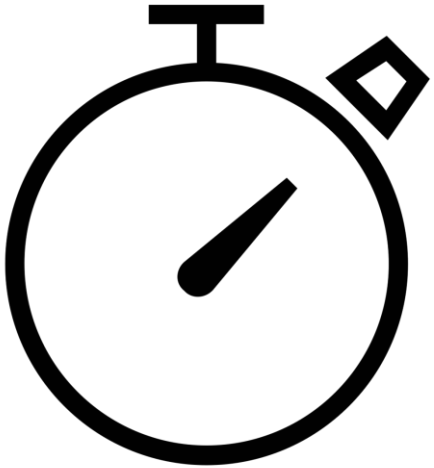
Recent and Relevant data

Can be performed on laptop (minimal hardware requirements)

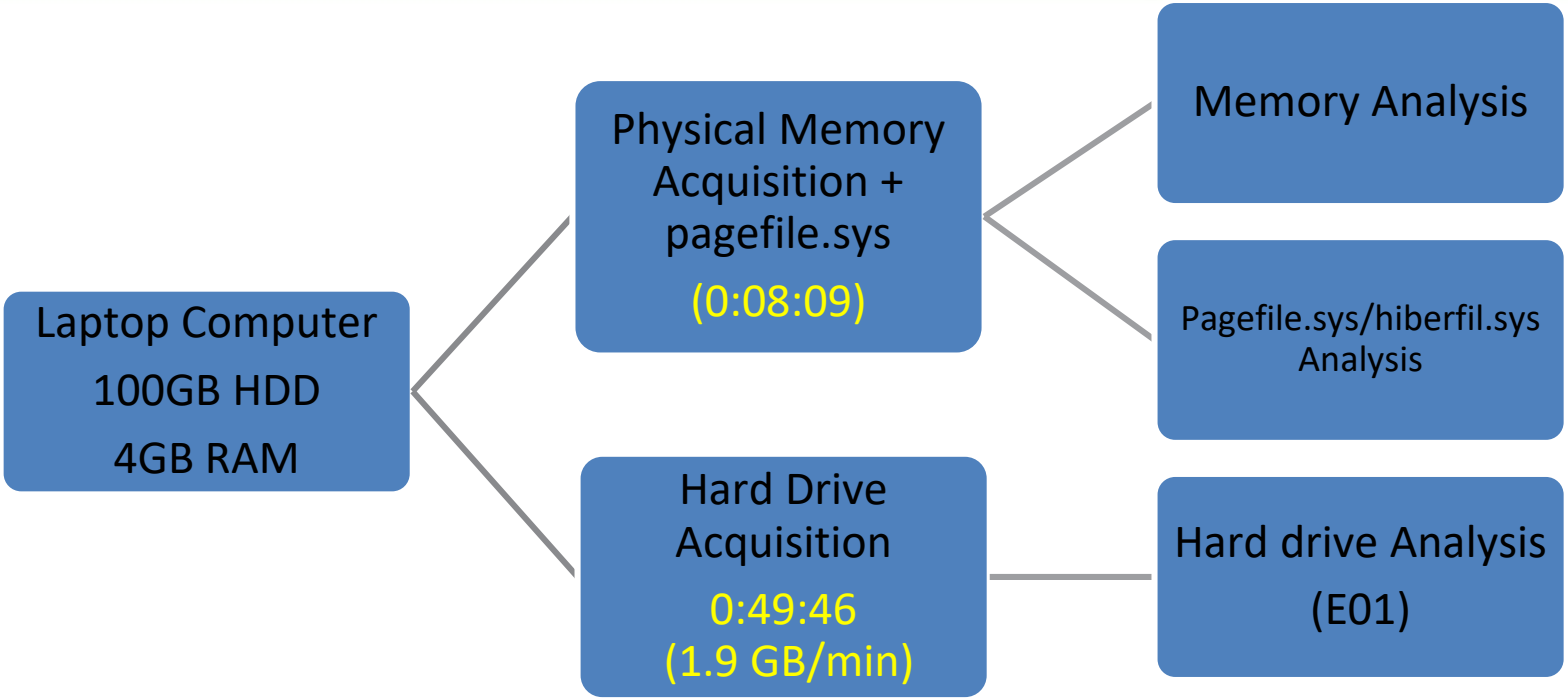
Validate against the image AFTER critical actions taken

Fast

- Actionable Intel
- Drive your investigation questions

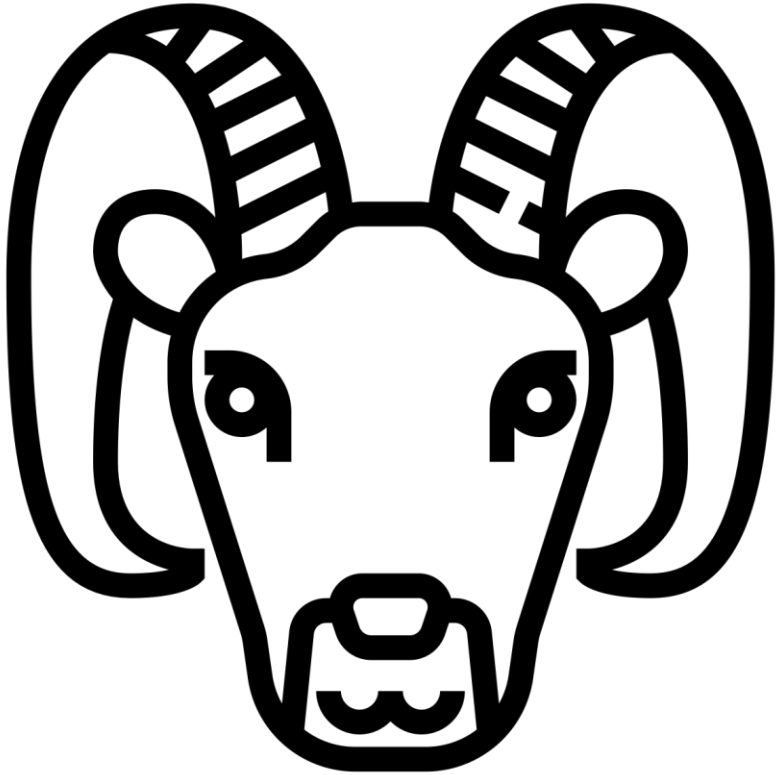


Memory vs Drive Acquisition



RAM

Collection

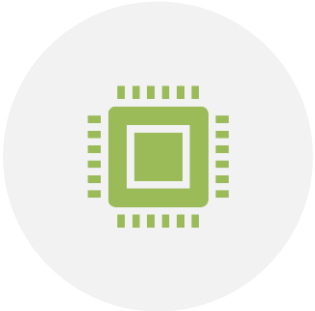


Money Maker Case Evidence

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

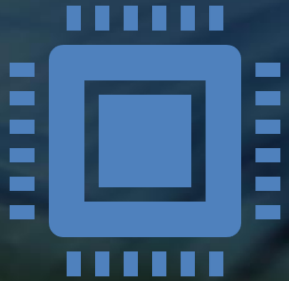


MEMORY DUMP

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)

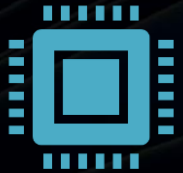
Profile users' activities, uncover data, locate passwords, decrypt encrypted volumes and locate indicators for further filesystem analysis.

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

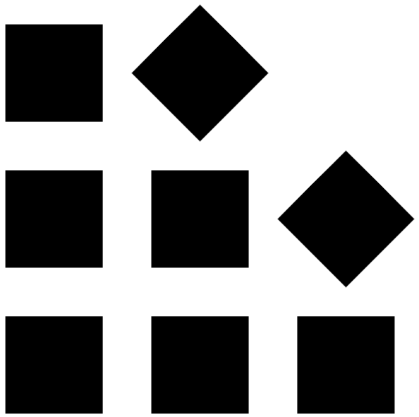
Parsing under 10 min

Still great data source

Inform the interview questions

- User Attribution
- Timelining
- Passwords
- Not my Pants
- Use of encryption
- External devices

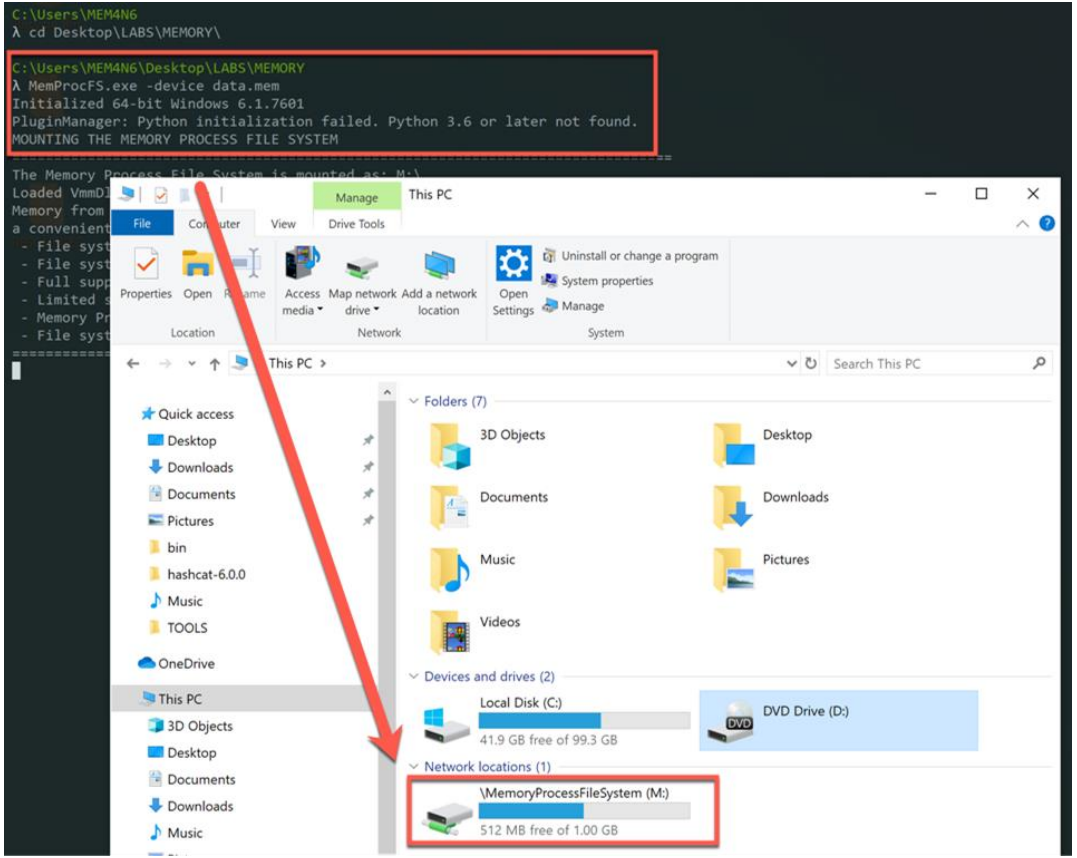
REGISTRY ANALYSIS



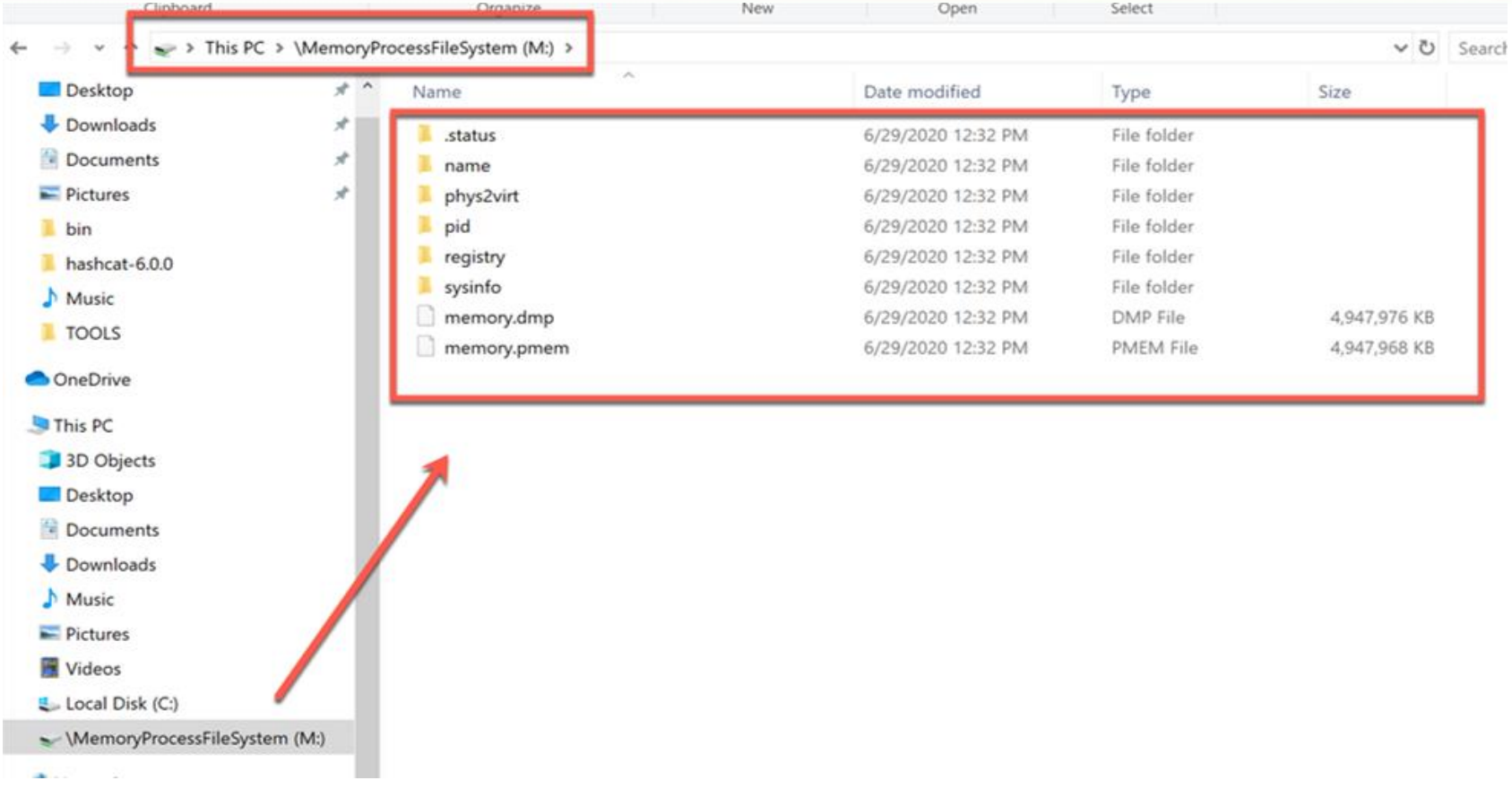
Locating Registry Hives in Memory

```
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
```

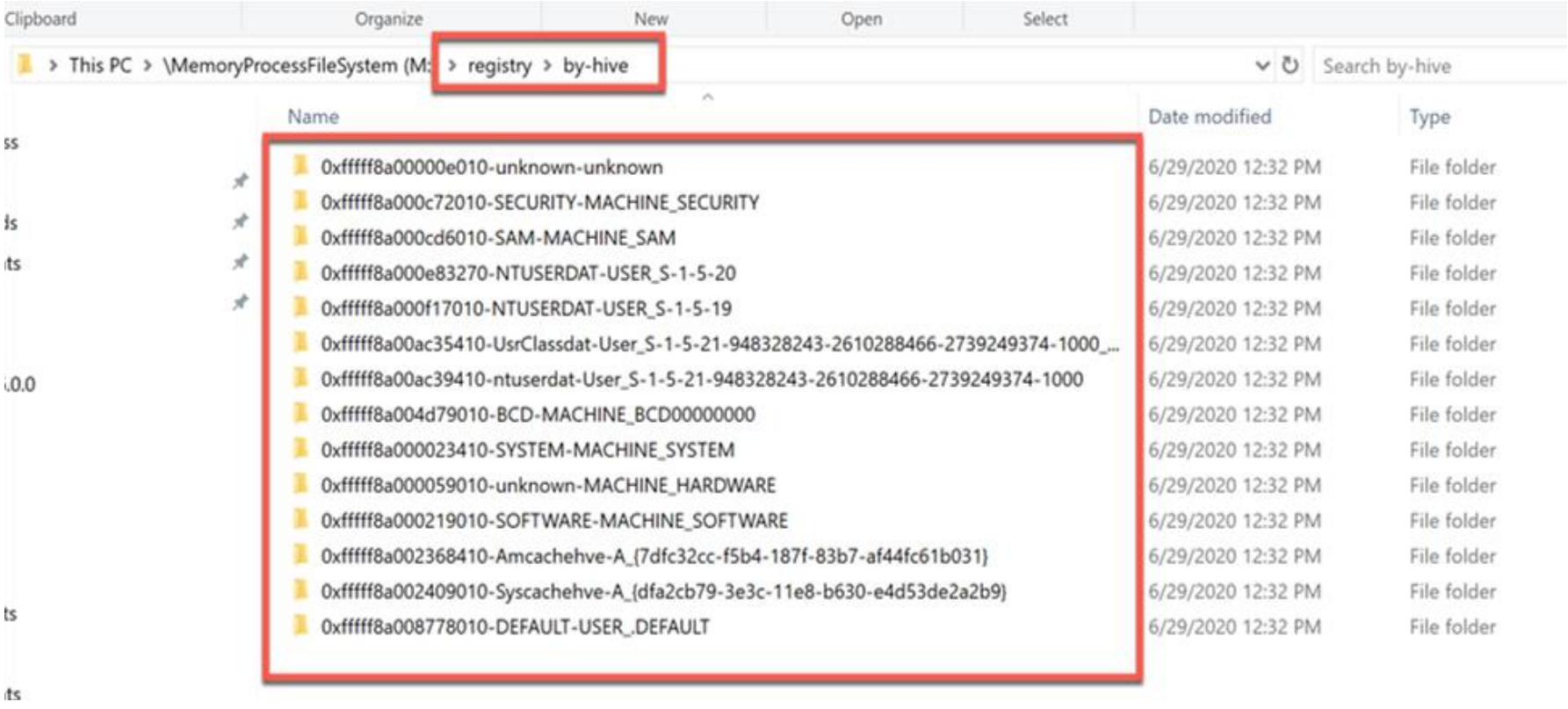
MemProcFS.exe



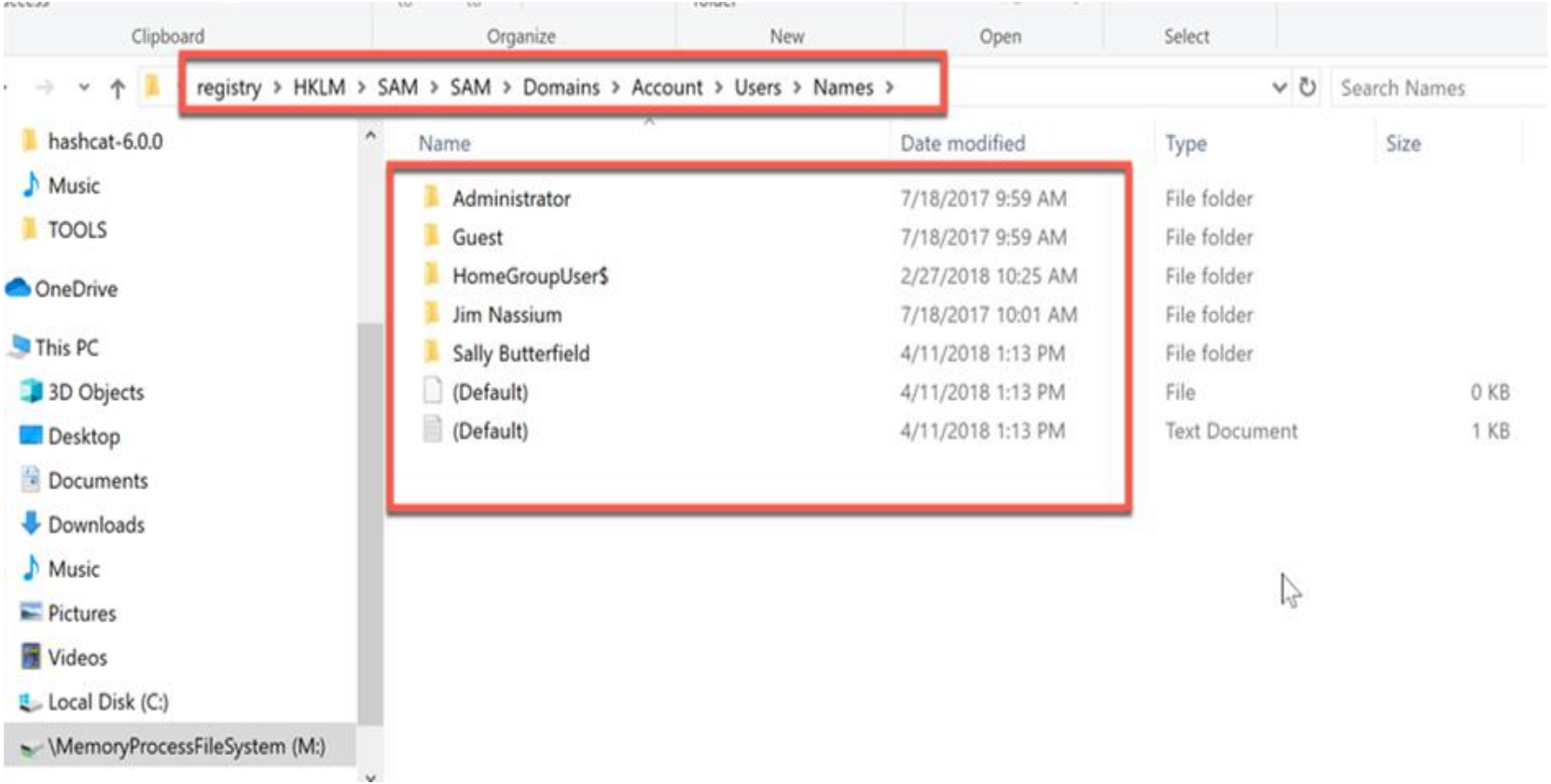
Mounted memory



Registry > by-hive



User Account Names



Locating the “CurrentControlSet”

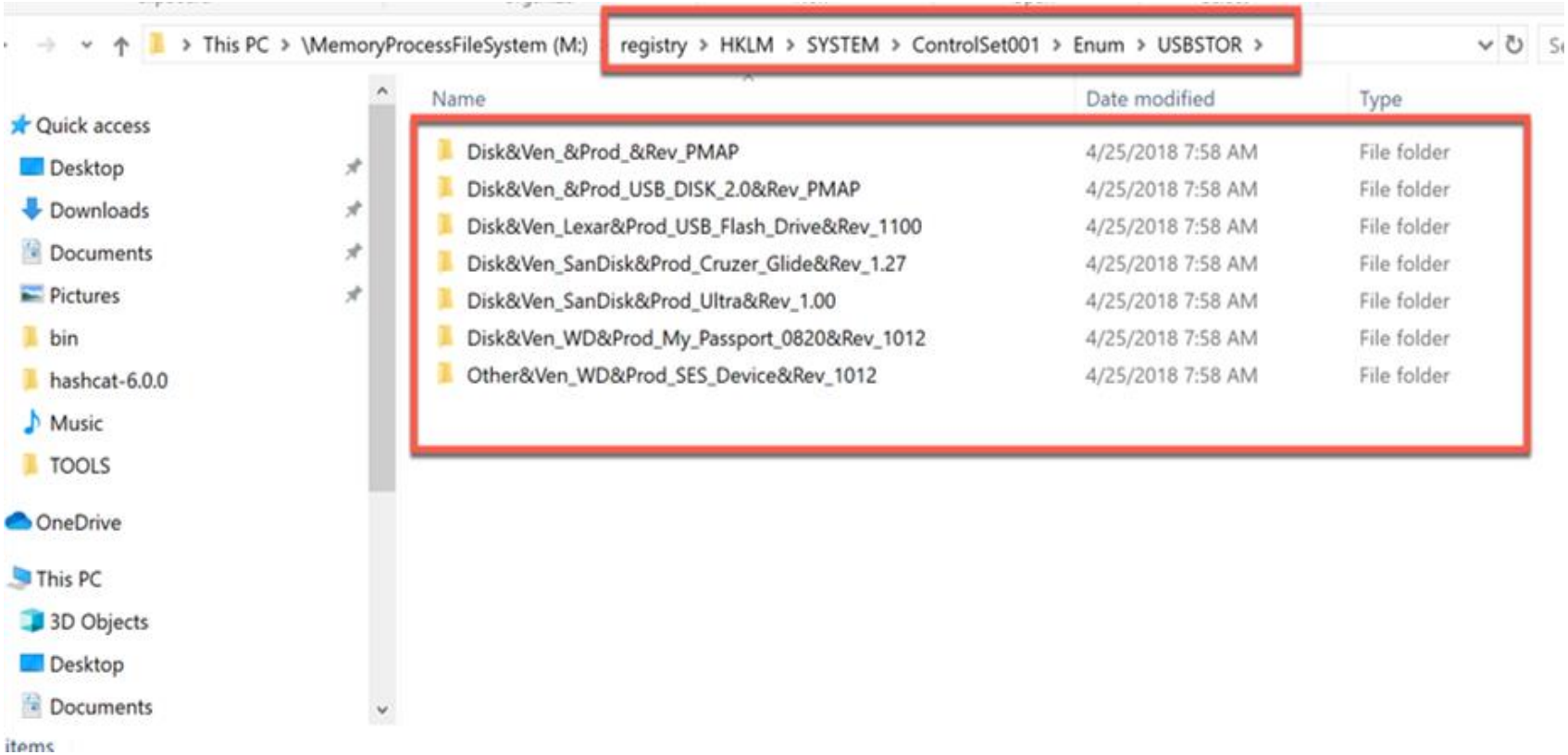
```
T:\MEM_IMAGES\MONEY_MAKER_PC\Carding_Case\MEM_DUMP
λ volatility -f data.lime --profile=Win7SP1x64 printkey -K "CurrentControlSet"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: CurrentControlSet (V)
Last updated: 2018-04-12 10:32:59 UTC+0000

Subkeys:

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

Enumerating USB devices from Memory

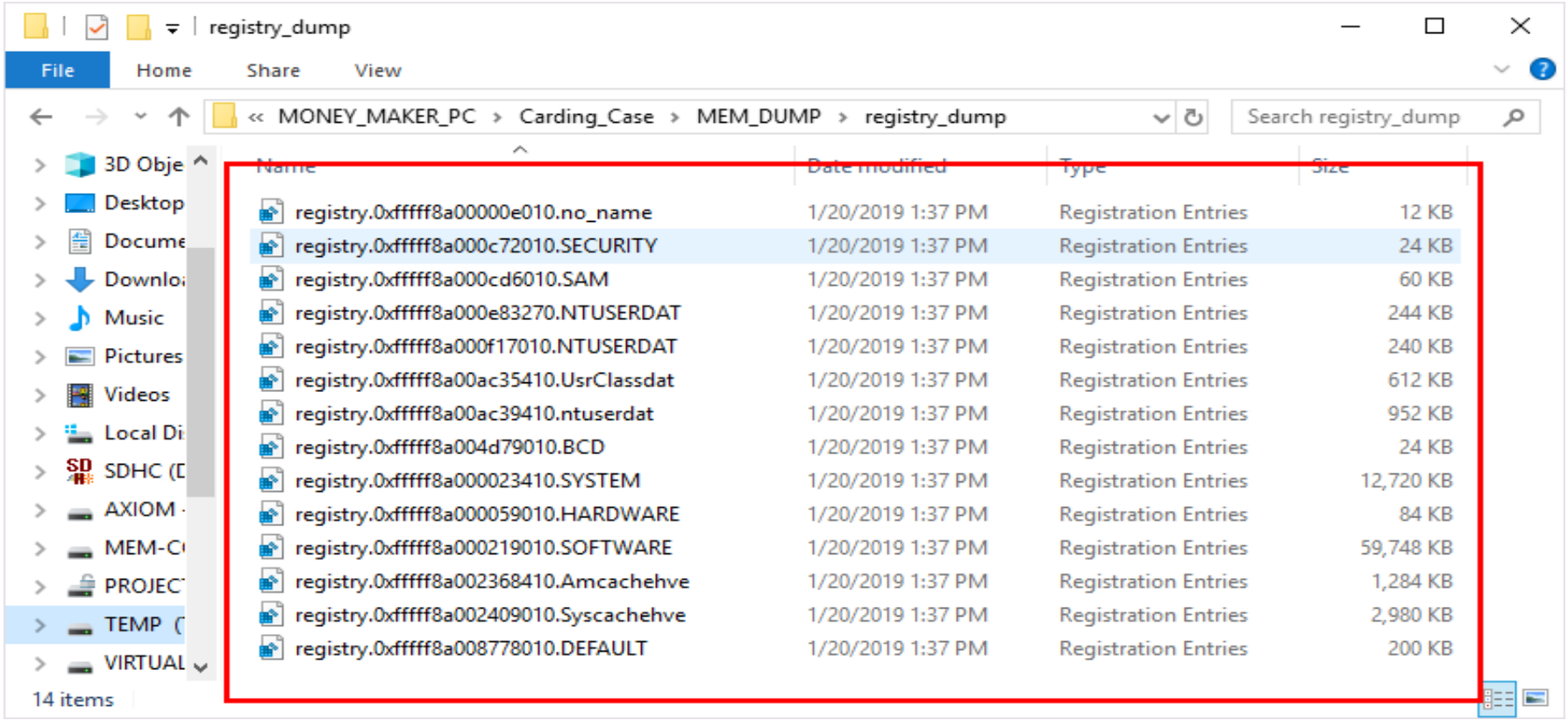
cmd

```
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:
```

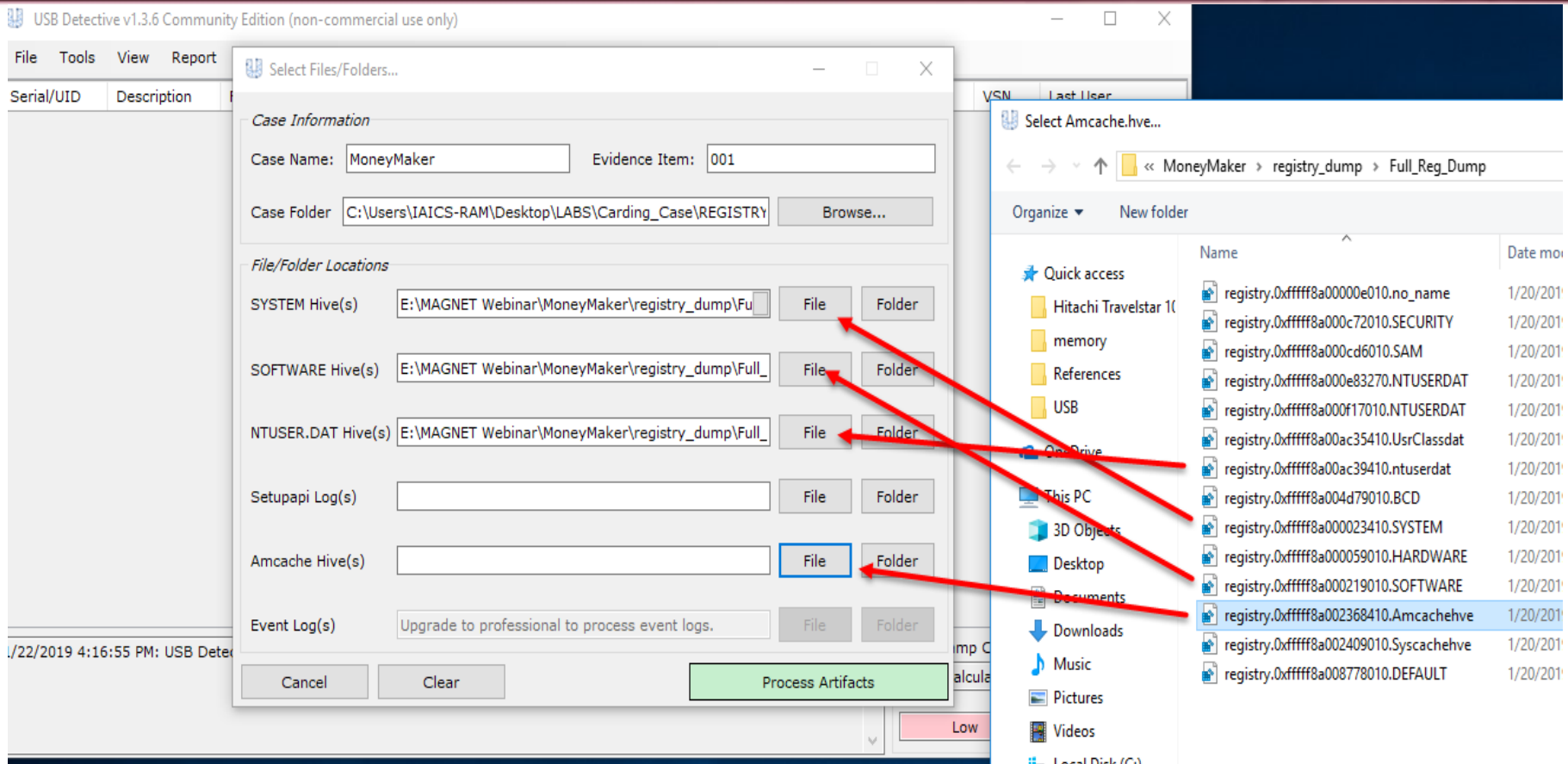
Navigating to USBSTOR



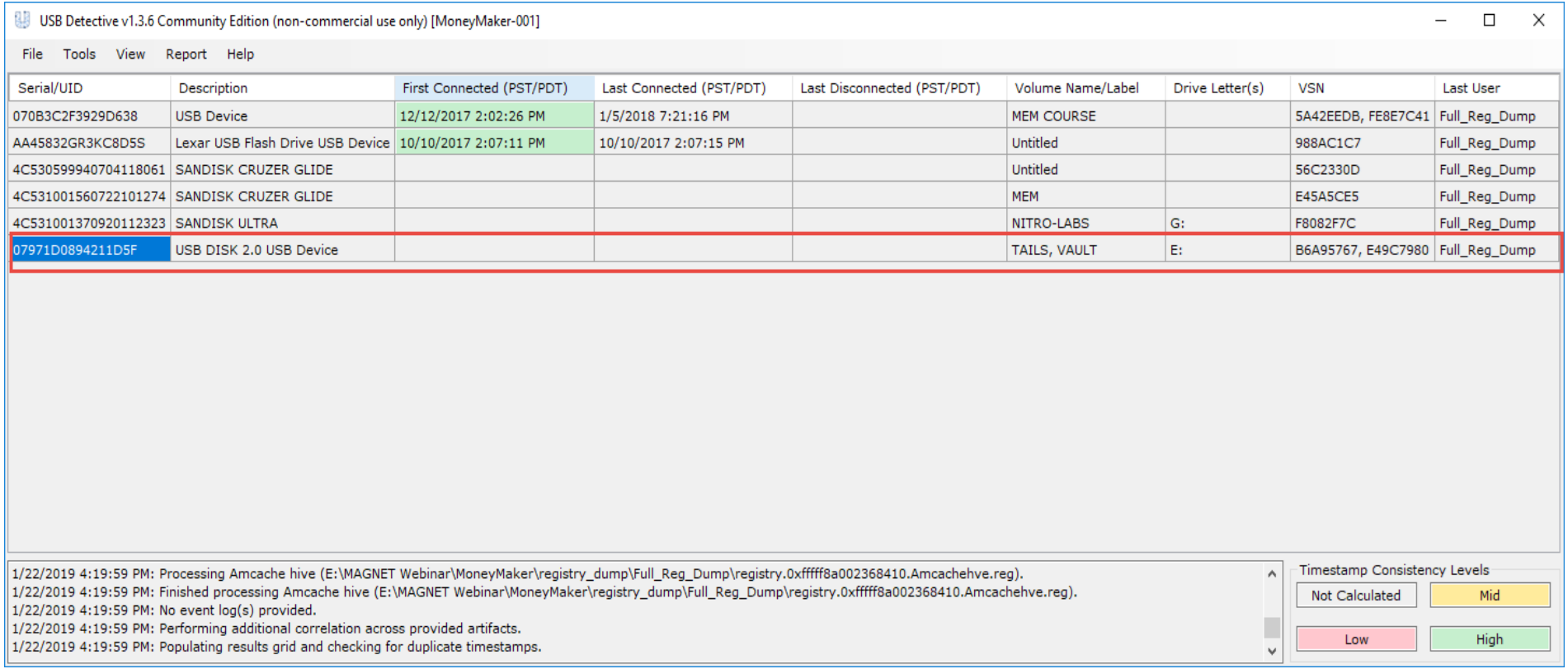
Registry Hives Dumped From Memory



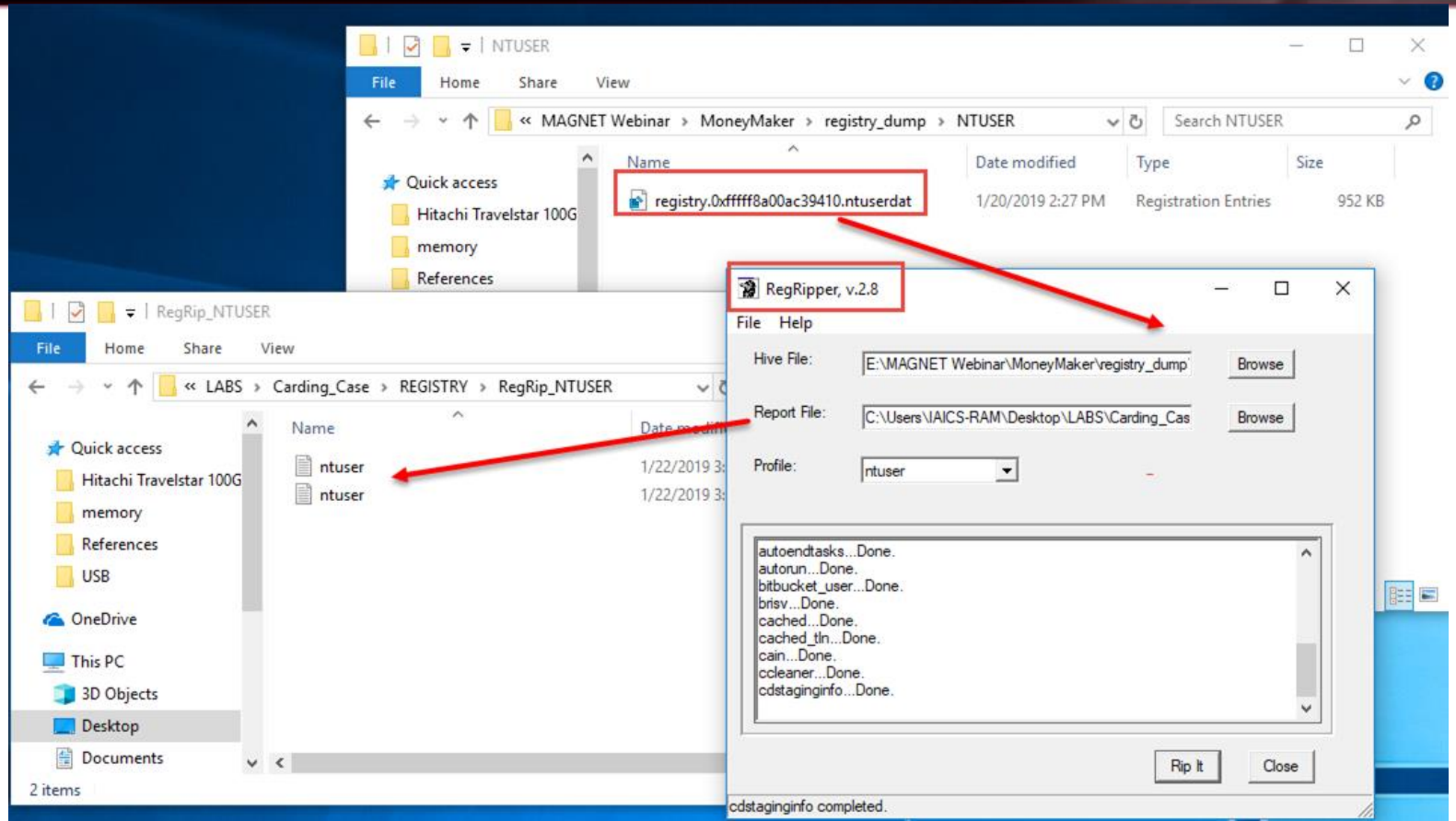
USB Detective



USB Detective



RegRipper


NTUSER
File
Home
Share
View
« MAGNET Webinar › MoneyMaker › registry_dump › NTUSER
Search NTUSER
Quick access
Hitachi Travelstar 100G
memory
References
Name
Date modified
Type
Size
registry.0xfffff8a00ac39410.ntuserdat
1/20/2019 2:27 PM
Registration Entries
952 KB
RegRip_NTUSER
« LABS › Carding_Case › REGISTRY › RegRip_NTUSER
USB
OneDrive
This PC
3D Objects
Desktop
Documents
ntuser
ntuser
2 items
RegRipper, v.2.8
File
Help
Hive File:
E:\MAGNET Webinar\MoneyMaker\registry_dump
Browse
Report File:
C:\Users\IAICS-RAM\Desktop\LABS\Carding_Cas
Browse
Profile:
ntuser
autoendtasks...Done.
autorun...Done.
bitbucket_user...Done.
brisv...Done.
cached...Done.
cached_tln...Done.
cain...Done.
ccleaner...Done.
cdstaginginfo...Done.
Rip It
Close
cdstaginginfo completed.

User Assist

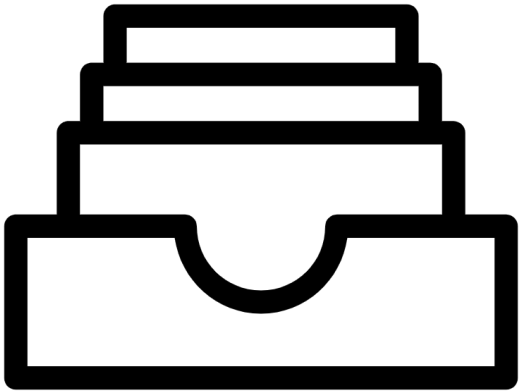
```
1959  ----------------------------------------
1960  unreadmail v.20100218
1961  (NTUSER.DAT) Gets contents of Unreadmail key
1962
1963  Software\Microsoft\Windows\CurrentVersion\UnreadMail not found.
1964  ----------------------------------------
1965  ----------------------------------------
1966  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    IDRIX.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
1513116948|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 Stripe Swipe Magstripe MSR206 _ eBay.html
1524602213|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg - scarfacenew.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
```

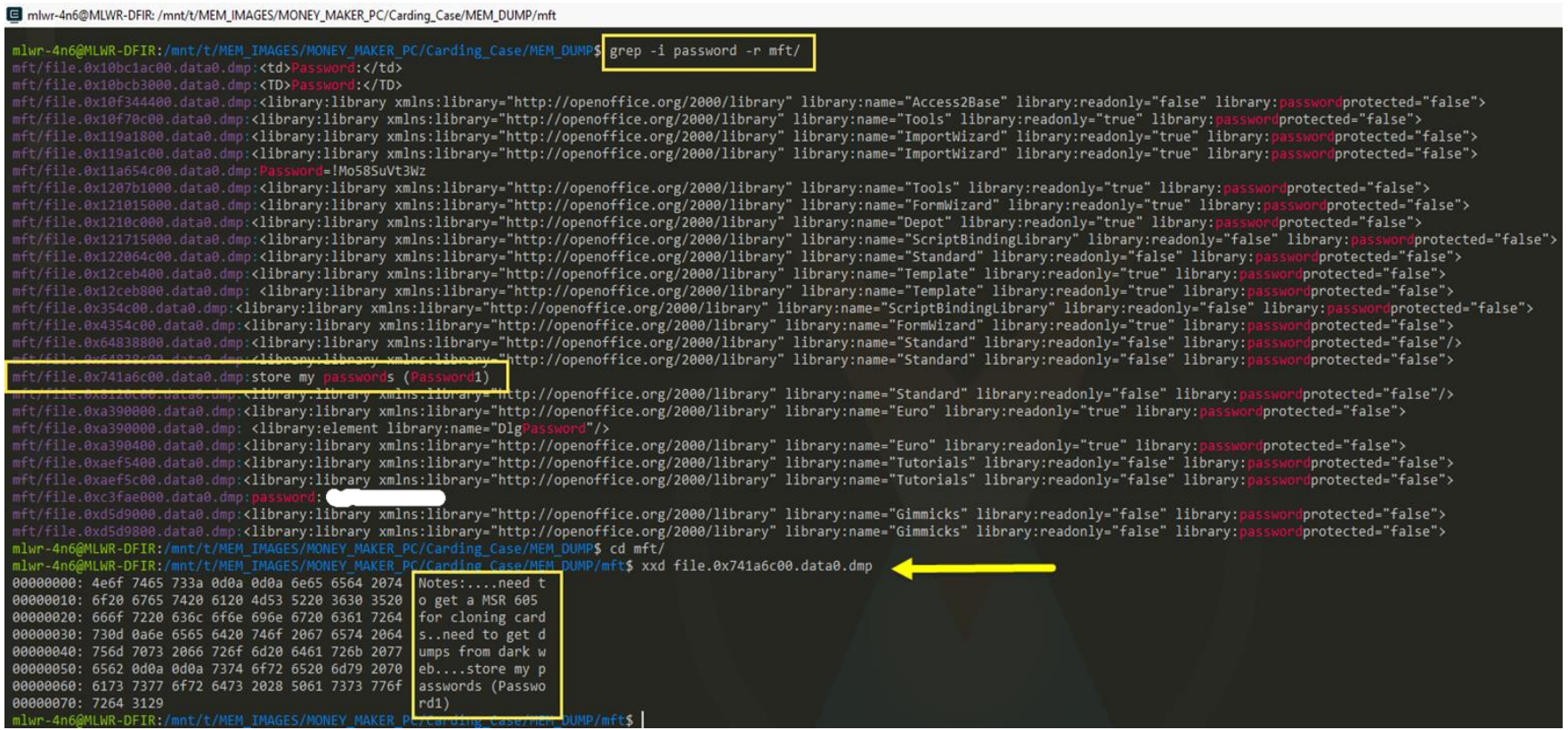
MFT – Master File Table Analysis



Parsing MFT

```
T:\MEM_IMAGES\MONEY_MAKER_PC\Carding_Case\MEM_DUMP
λ 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



MFT – Resident DATA

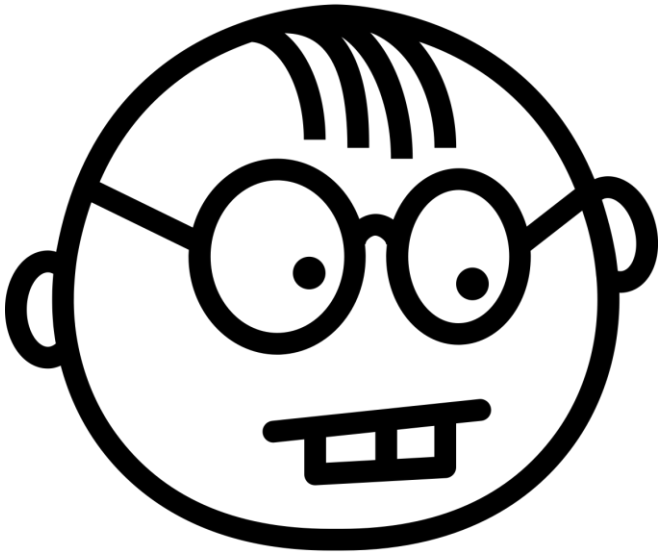
```
1893992 ***************************************************************************
1893993 MFT entry found at offset 0x741a6c00
1893994 Attribute: In Use & File
1893995 Record Number: 23515
1893996 Link count: 2
1893997
1893998
1893999 $STANDARD_INFORMATION
1894000 Creation                    Modified                    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   Notes:....need.t
1894022 0000000010: 6f 20 67 65 74 20 61 20 4d 53 52 20 36 30 35 20   o.get.a.MSR.605.
1894023 0000000020: 66 6f 72 20 63 6c 6f 6e 69 6e 67 20 63 61 72 64   for.cloning.card
1894024 0000000030: 73 0d 0a 6e 65 65 64 20 74 6f 20 67 65 74 20 64   s..need.to.get.d
1894025 0000000040: 75 6d 70 73 20 66 72 6f 6d 20 64 61 72 6b 20 77   umps.from.dark.w
1894026 0000000050: 65 62 0d 0a 0d 0a 73 74 6f 72 65 20 6d 79 20 70   eb....store.my.p
1894027 0000000060: 61 73 73 77 6f 72 64 73 20 28 50 61 73 73 77 6f   asswords.(Passwo
1894028 0000000070: 72 64 31 29                                       rd1)
1894029
1894030 ***************************************************************************
```

$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   E:\credit cards.txt
351086
351087  $DATA
351088
351089
351090  $OBJECT_ID
351091  Object ID: 40000000-0000-0000-0010-000000000000
351092  Birth Volume ID: 52090000-0000-0000-5209-000000000000
351093  Birth Object ID: 41017be5-ea0b-0000-ffff-ffff82794711
351094  Birth Domain ID: 00000000-0000-0000-0000-000000000000
351095
351096  ********************************************************************************
351097  ********************************************************************************
```

Normal text file | length : 176,828,482 lines : 2,879,171 Ln : 351,085 Col : 152 Sel : 5 | 1 | Windows (CR LF) | UTF-8 | INS



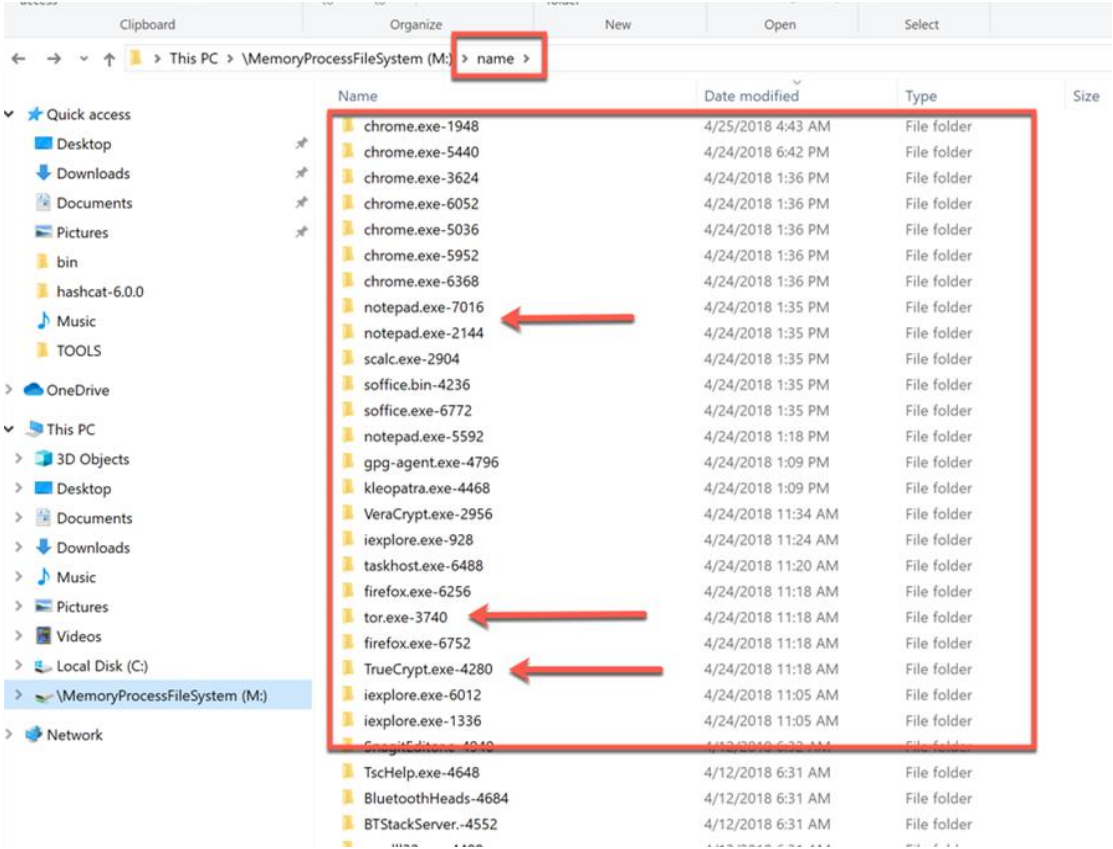
User Artifacts

- User Processes
- Browser history
- Prefetch

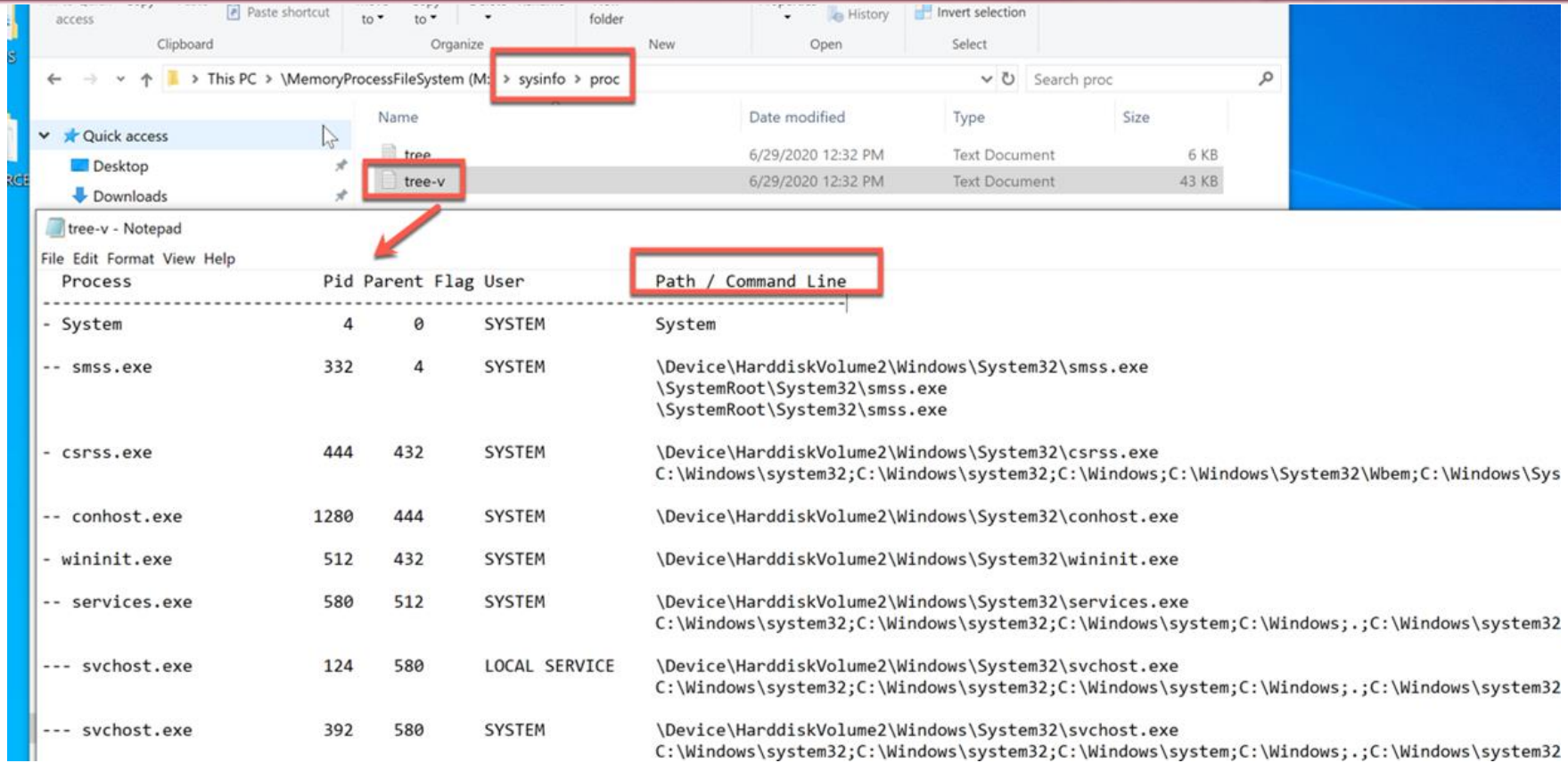
pslist

```
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
0xfffffa800679eb10 csrss.exe
0xfffffa8006ecf790 wininit.exe
0xfffffa8006ed9060 csrss.exe
0xfffffa8006f4bb10 services.exe
0xfffffa8006f292a0 lsass.exe
0xfffffa8006f31b10 lsm.exe
0xfffffa8005b77b10 winlogon.exe
0xfffffa800716eb10 svchost.exe
0xfffffa800718fb10 nvvsvc.exe
0xfffffa80071ae9c0 svchost.exe
0xfffffa8007242b10 svchost.exe
0xfffffa8007261b10 svchost.exe
0xfffffa8007280b10 svchost.exe
0xfffffa80065f7b10 svchost.exe
0xfffffa80067bf060 svchost.exe
0xfffffa8006838060 wlanext.exe
0xfffffa8006833060 conhost.exe
0xfffffa8005c12060 spoolsv.exe
0xfffffa8005c09b10 svchost.exe
0xfffffa8007512b10 svchost.exe
0xfffffa8007556220 btwdins.exe
0xfffffa800755a330 svchost.exe
0xfffffa8007567b10 EvtEng.exe
0xfffffa8007577b10 RegSrvc.exe
0xfffffa800761bb10 UploaderServ
0xfffffa8006756060 ZeroConfigSe
0xfffffa8003a9f060 svchost.exe
0xfffffa80067b2330 WUDFHost.exe
0xfffffa8007791b10 svchost.exe
0xfffffa80077ab060 unsecapp.exe
0xfffffa8003b3cb10 iFrmewrk.exe          2988   3920     10      250      1      0 2018-04-12 13:30:41 UTC+0000
0xfffffa80044a5b10 BTTray.exe            3968   3920     11      248      1      0 2018-04-12 13:30:41 UTC+0000
0xfffffa80044c0b10 Snagit32.exe          3044   3920     19      496      1      1 2018-04-12 13:30:41 UTC+0000
0xfffffa80044b92f0 StikyNot.exe          3992   3920      8      143      1      0 2018-04-12 13:30:41 UTC+0000
0xfffffa80044b36f0 unsecapp.exe          2884    752      3       78      1      0 2018-04-12 13:30:41 UTC+0000
0xfffffa800459b900 SnagPriv.exe          2888   3044      5       81      1      1 2018-04-12 13:30:48 UTC+0000
0xfffffa800456cb10 svchost.exe           3900    580     12      382      0      0 2018-04-12 13:30:50 UTC+0000
0xfffffa80046bbb10 rundll32.exe          4408   3968      1       58      1      1 2018-04-12 13:31:01 UTC+0000
0xfffffa80046c5b10 BTStackServer.        4552    752     22      334      1      0 2018-04-12 13:31:06 UTC+0000
0xfffffa80046f9060 BluetoothHeads        4684   4552      1       29      1      1 2018-04-12 13:31:08 UTC+0000
0xfffffa80079f8b10 TscHelp.exe           4648   3044      1       58      1      1 2018-04-12 13:31:35 UTC+0000
0xfffffa8008680b10 SnagitEditor.e        4940   3044     21      556      1      1 2018-04-12 13:32:11 UTC+0000
0xfffffa80077fbb10 iexplore.exe          1336   3920     11      660      1      0 2018-04-24 18:05:40 UTC+0000
0xfffffa8008440b10 iexplore.exe          6012   1336     19      819      1      1 2018-04-24 18:05:41 UTC+0000
0xfffffa8009e99060 TrueCrypt.exe         4280   3920      5      214      1      1 2018-04-24 18:18:22 UTC+0000
0xfffffa800a327060 firefox.exe           6752   3920     51      617      1      1 2018-04-24 18:18:24 UTC+0000
0xfffffa8009eb8060 tor.exe               3740   6752      3       77      1      1 2018-04-24 18:18:33 UTC+0000
0xfffffa8003ef9730 firefox.exe           6256   6752     24      318      1      1 2018-04-24 18:18:50 UTC+0000
0xfffffa8009840b10 taskhost.exe          6488    580      6      268      1      0 2018-04-24 18:20:06 UTC+0000
0xfffffa800a492060 iexplore.exe           928   1336     16      535      1      1 2018-04-24 18:24:30 UTC+0000
0xfffffa8008fd0430 VeraCrypt.exe         2956   3920      7      262      1      0 2018-04-24 18:34:21 UTC+0000
0xfffffa8004053150 kleopatra.exe         4468   3920      8      395      1      1 2018-04-24 20:09:38 UTC+0000
0xfffffa8009975180 gpg-agent.exe         4796   5616      3       95      1      1 2018-04-24 20:09:58 UTC+0000
0xfffffa80093c8060 kleopatra.exe         3632   3920      0 --------      1      0 2018-04-24 20:10:25 UTC+0000   2018-04-24 20:10:30 UTC+0000
0xfffffa80099c7760 kleopatra.exe         2324   3920      0 --------      1      0 2018-04-24 20:15:38 UTC+0000   2018-04-24 20:15:39 UTC+0000
0xfffffa8008a48060 kleopatra.exe         2636   3920      0 --------      1      0 2018-04-24 20:18:34 UTC+0000   2018-04-24 20:18:34 UTC+0000
0xfffffa8009946b10 notepad.exe           5592   3920      1       62      1      0 2018-04-24 20:18:50 UTC+0000
0xfffffa8004619340 scalc.exe             2904   3920      1       16      1      0 2018-04-24 20:35:13 UTC+0000
0xfffffa80084f48c0 soffice.exe           6772   2904      1       23      1      0 2018-04-24 20:35:13 UTC+0000
0xfffffa8008fbc060 soffice.bin           4236   6772     20      273      1      0 2018-04-24 20:35:13 UTC+0000
0xfffffa8009836b10 notepad.exe           2144   3920      1       62      1      0 2018-04-24 20:35:30 UTC+0000
0xfffffa800a78d060 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
```

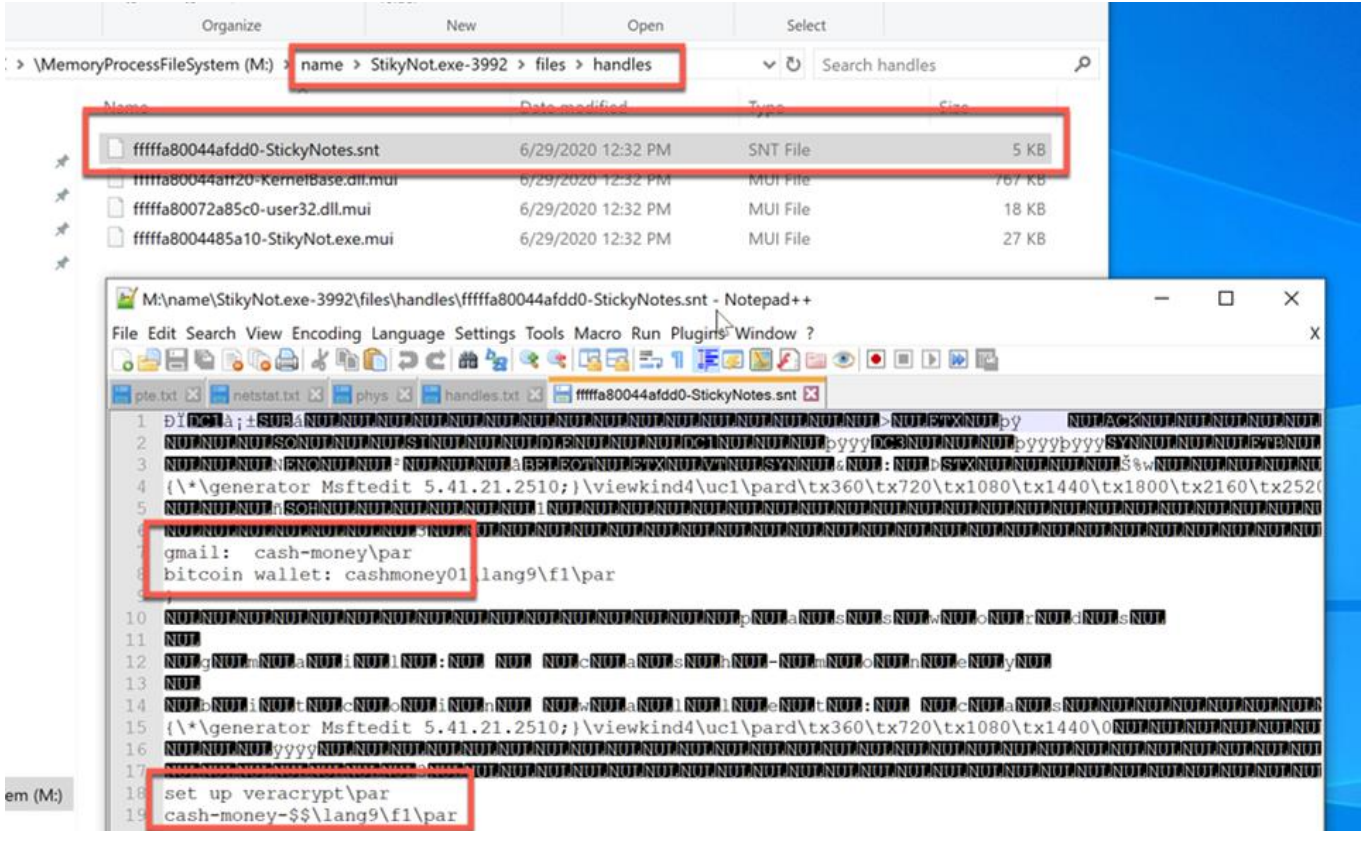
Processes by Name



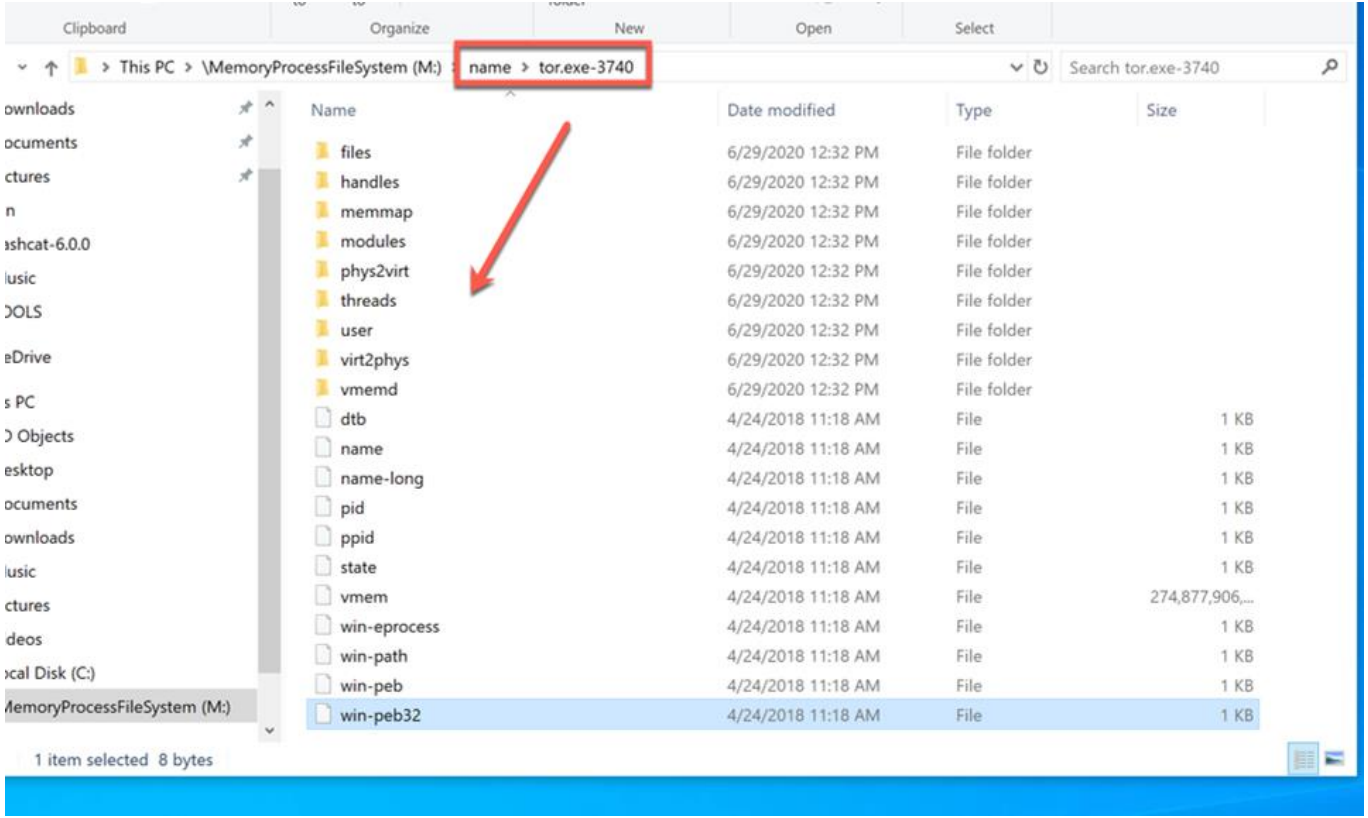
MemProcFS verbose tree



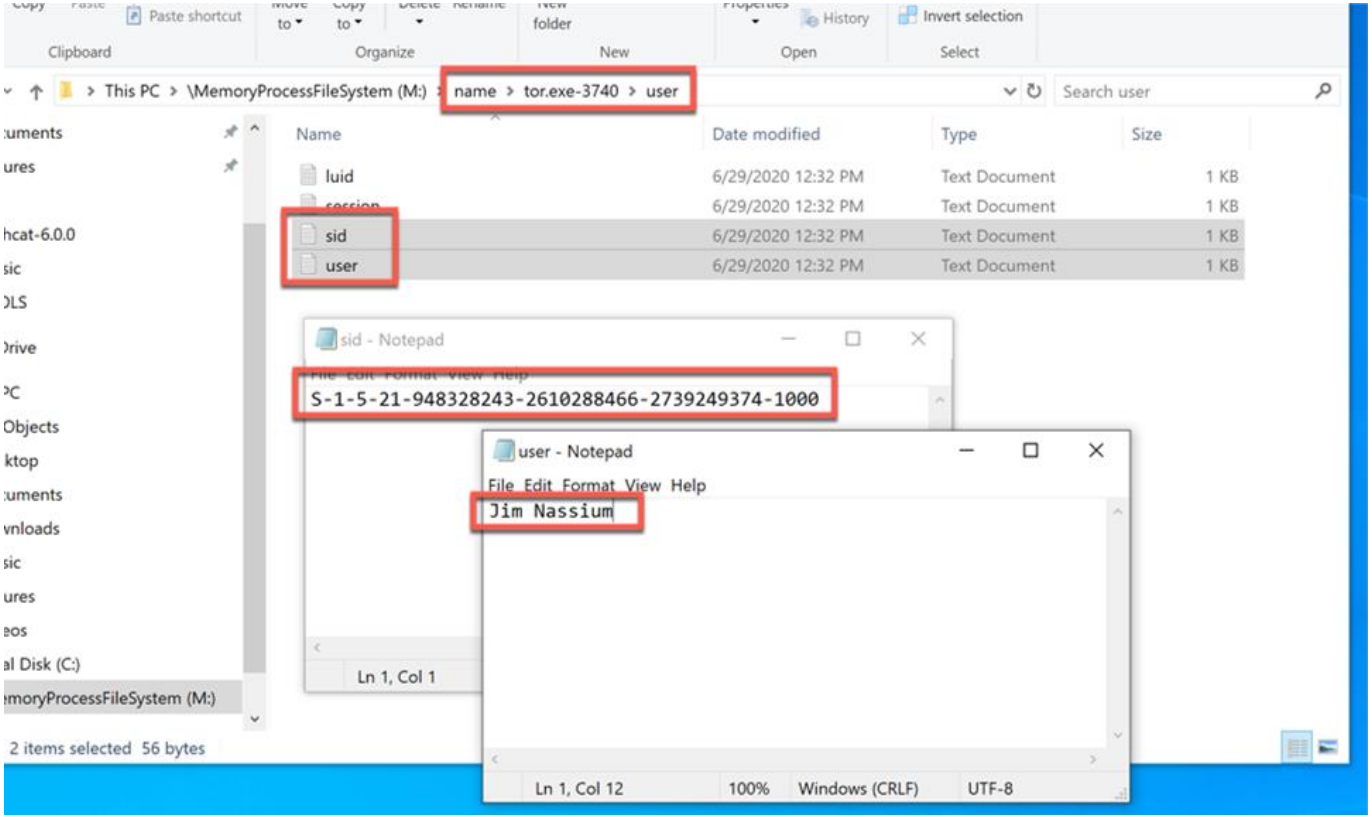
Process analysis



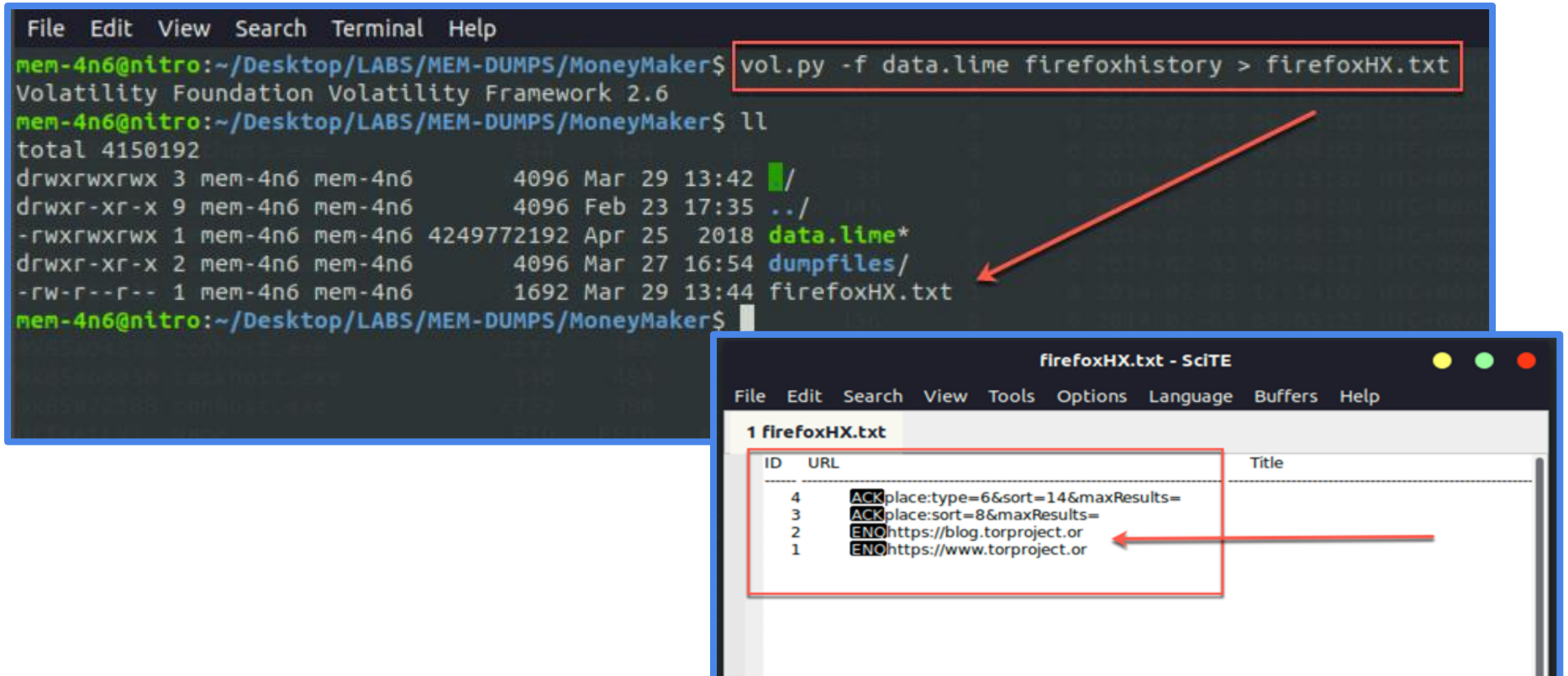
Executable process analysis



Executable process analysis



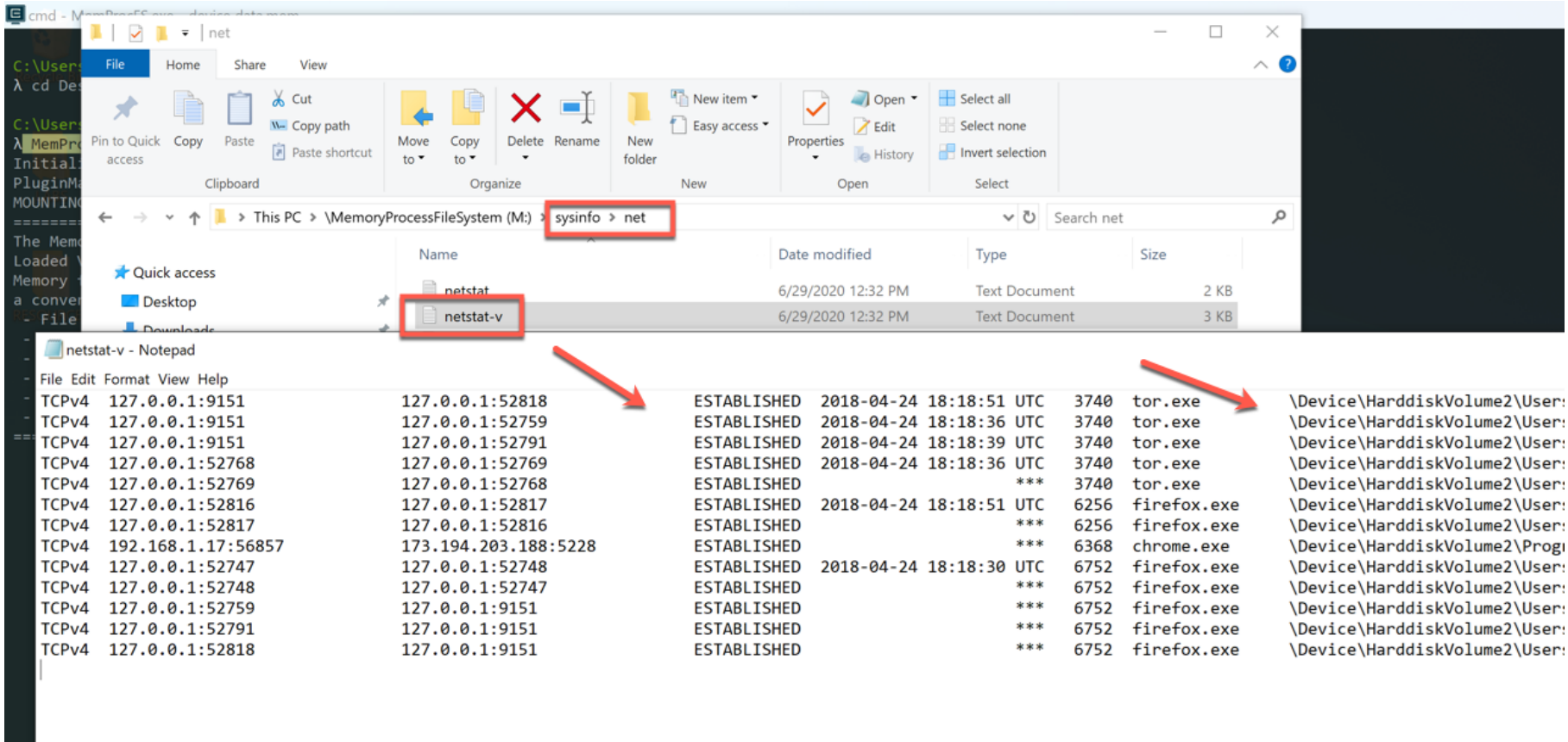
Analyzing user processes



Chrome search terms

```
mem-4n6@nitro:~/Desktop/LABS/MEM-DUMPS/MoneyMaker$ vol.py -f data.lime chromesearchterms
Volatility Foundation Volatility Framework 2.6
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
Volatility Foundation Volatility Framework 2.6
Scanning for Prefetch files, this can take a while.............
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
λ 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

cmd

```
T:\MEM_IMAGES\MONEY_MAKER_PC\Carding_Case\MEM_DUMP
λ volatility -f data.lime --profile=Win7SP1x64 hashdump > hashdump.txt
Volatility Foundation Volatility Framework 2.6

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

T:\MEM_IMAGES\MONEY_MAKER_PC\Carding_Case\MEM_DUMP\hashdump.txt - Notepad++

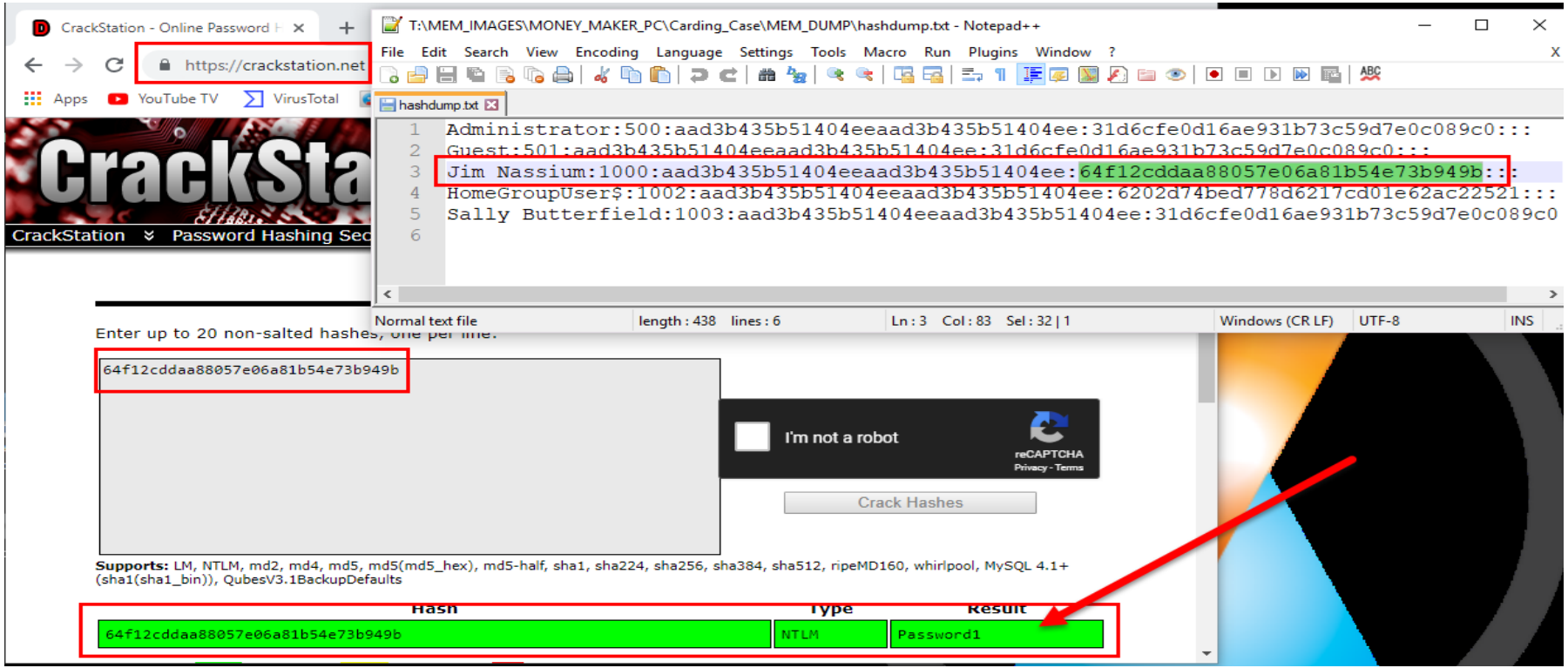
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? X

hashdump.txt

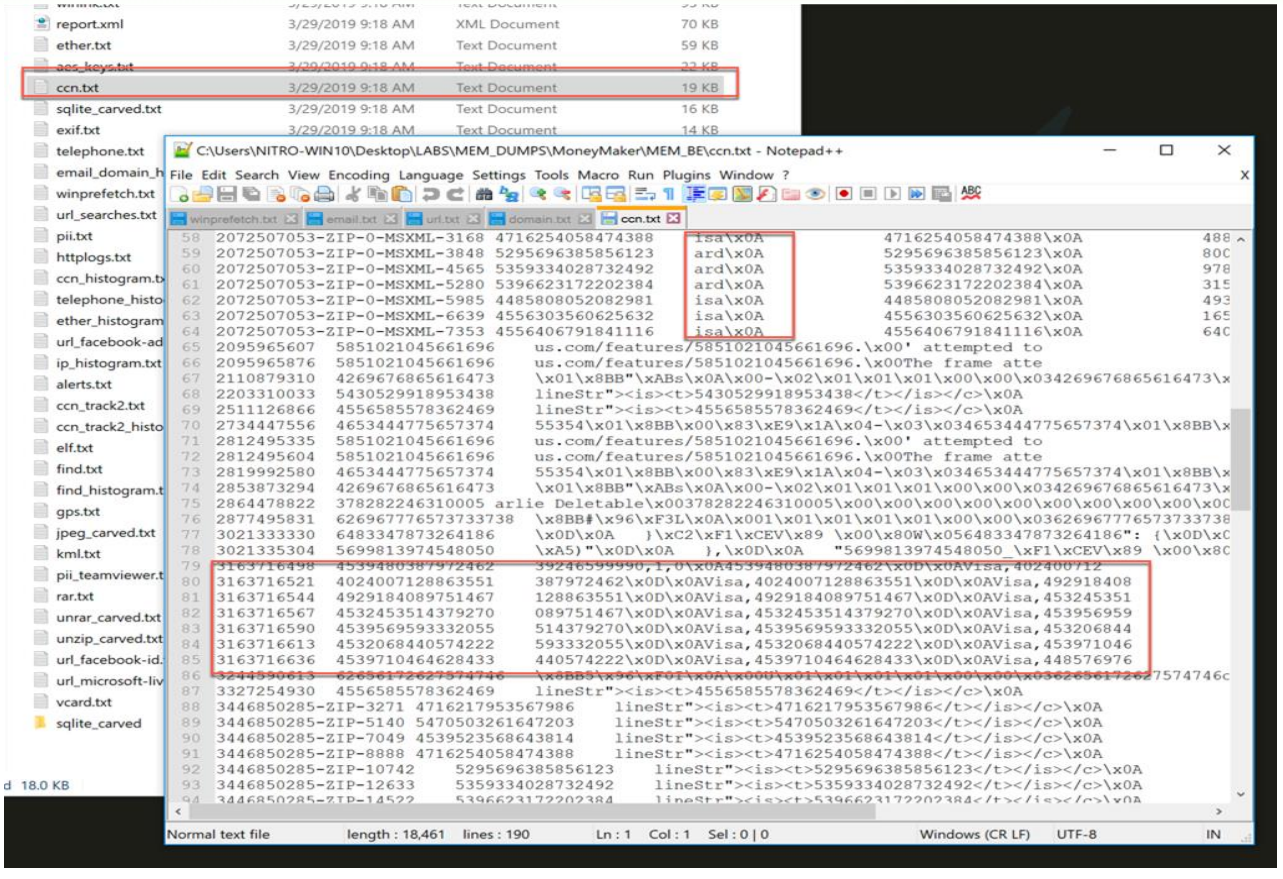
```
1  Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
2  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
3  Jim Nassium:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
4  HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6202d74bed778d6217cd01e62ac22521:::
5  Sally Butterfield:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
6
```

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

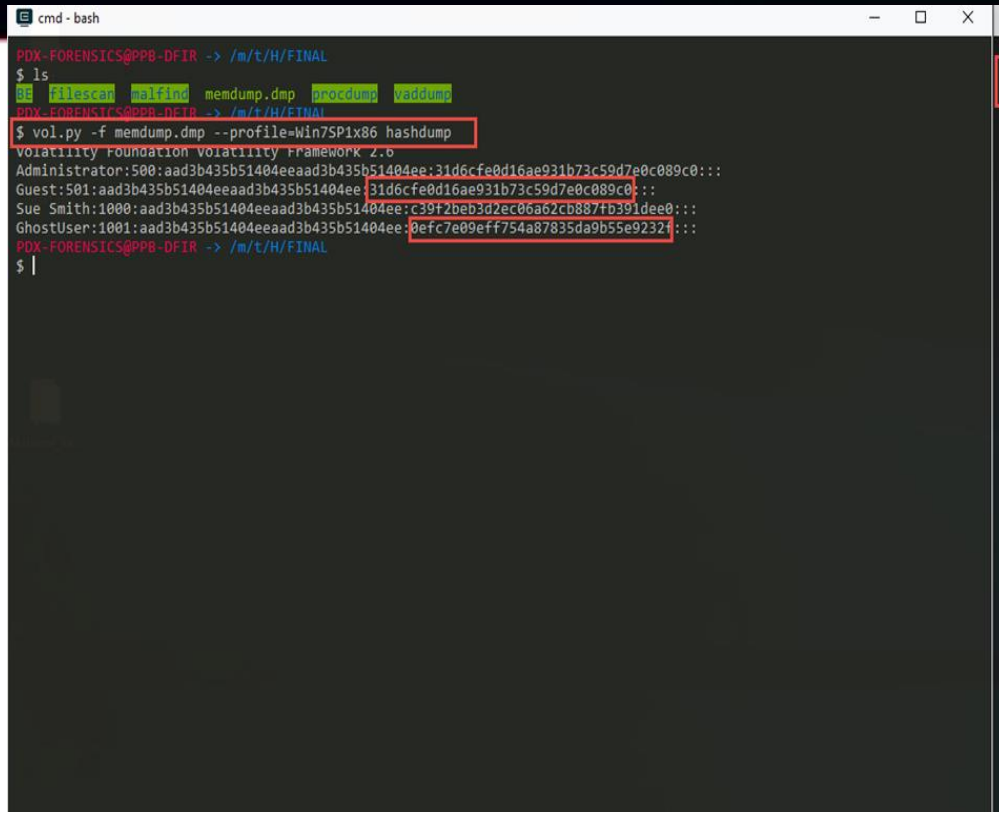
Using NTLM hash to get password

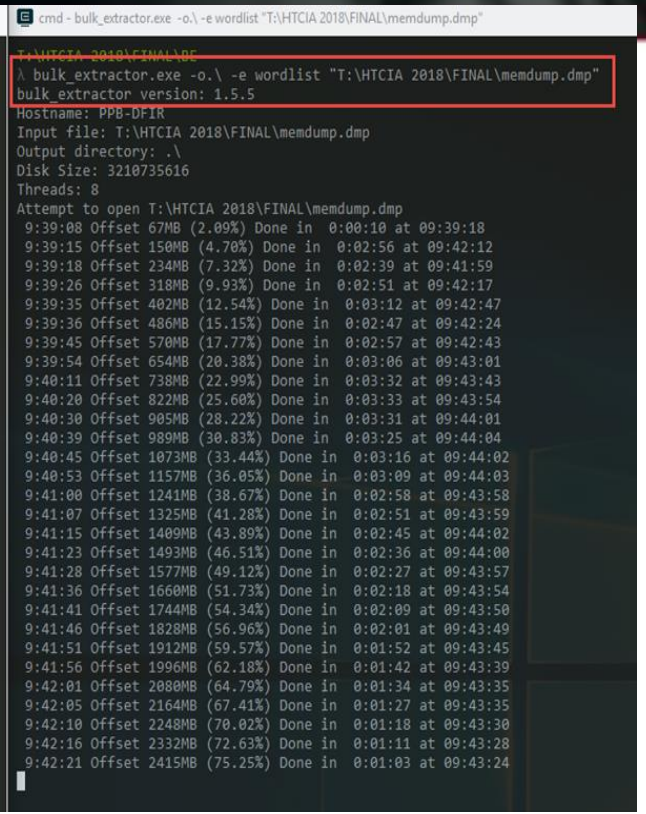


bulk_extractor

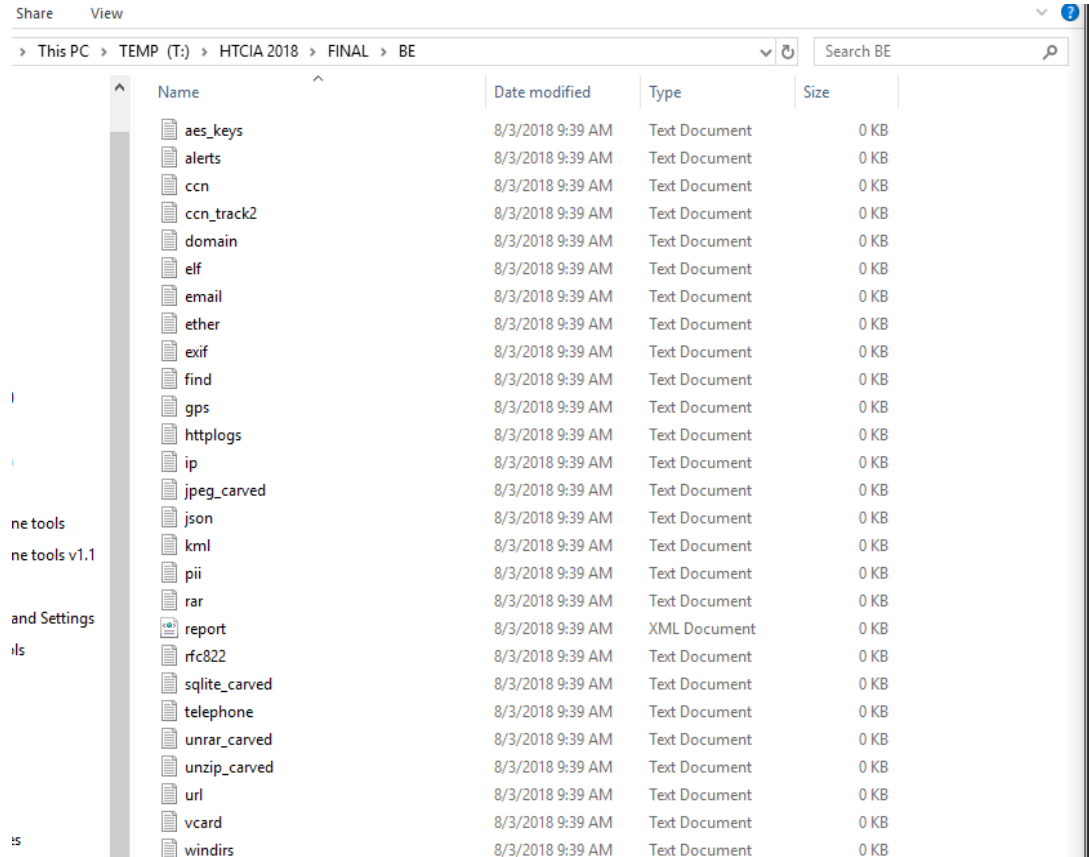


hashdump + bulk_extractor + wordlist



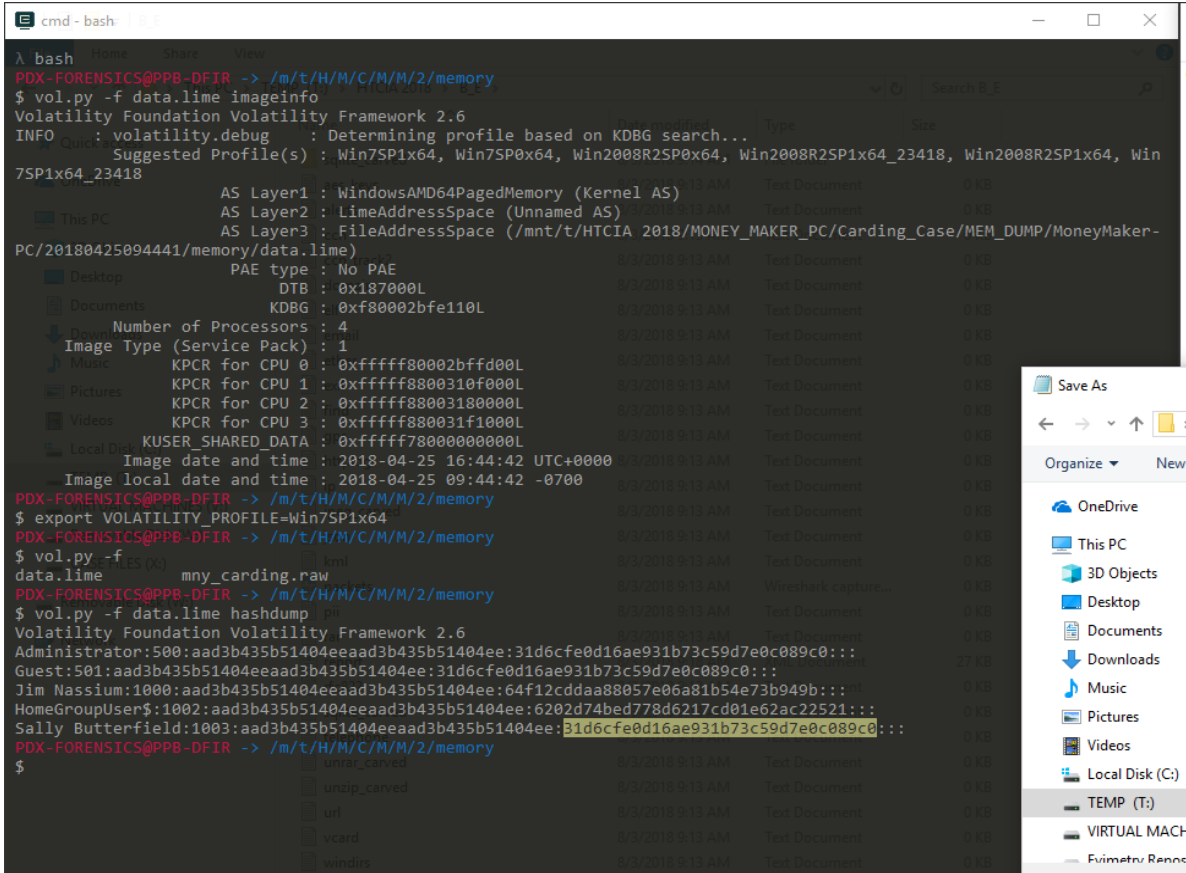


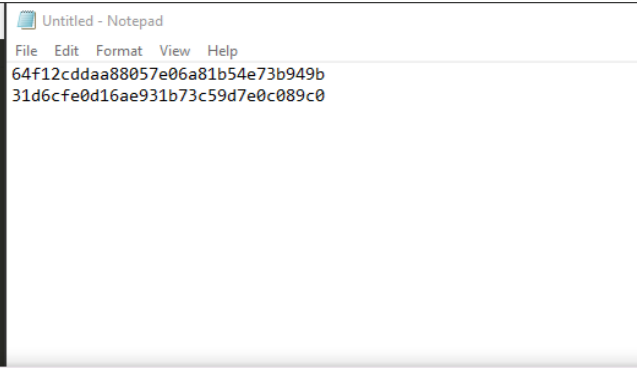
Bulk extractor + wordlist

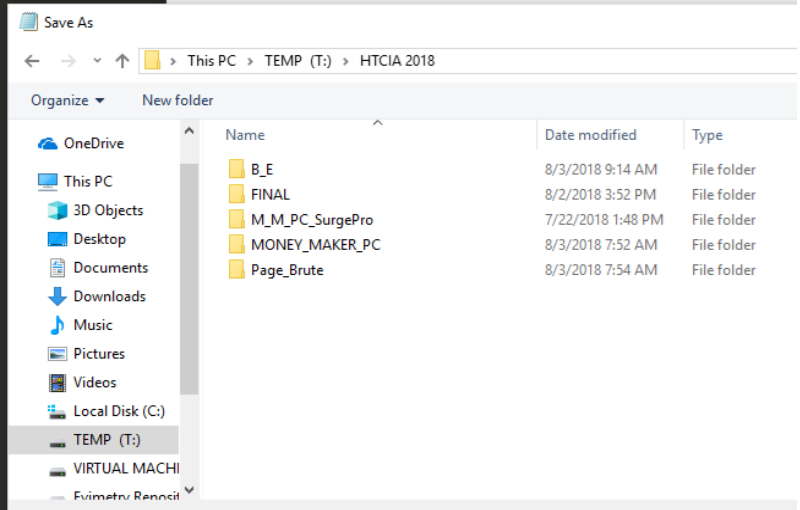



```
T:\HTCIA 2018\FINAL\BE
λ bulk_extractor.exe -o.\ -e wordlist "T:\HTCIA 2018\FINAL\memdump.dmp"
bulk_extractor version: 1.5.5
Hostname: PPB-DFIR
Input file: T:\HTCIA 2018\FINAL\memdump.dmp
Output directory: .\
Disk Size: 3210735616
Threads: 8
Attempt to open T:\HTCIA 2018\FINAL\memdump.dmp
 9:39:08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

hashdump


cmd - bash
λ bash
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...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, 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 : 0xfffff80002bffd00L
KPCR for CPU 1 : 0xfffff8800310f000L
KPCR for CPU 2 : 0xfffff88003180000L
KPCR for CPU 3 : 0xfffff880031f1000L
KUSER_SHARED_DATA : 0xfffff78000000000L
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 mny_carding.raw
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:6202d74bed778d6217cd01e62ac22521:::
Sally Butterfield:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PDX-FORENSICS@PPB-DFIR -> /m/t/H/M/C/M/M/2/memory
$


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


Save As
This PC › TEMP (T:) › HTCIA 2018
Organize
New folder
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
TEMP (T:)
VIRTUAL MACHI
Name
Date modified
Type
B_E 8/3/2018 9:14 AM File folder
FINAL 8/2/2018 3:52 PM File folder
M_M_PC_SurgePro 7/22/2018 1:48 PM File folder
MONEY_MAKER_PC 8/3/2018 7:52 AM File folder
Page_Brute 8/3/2018 7:54 AM File folder

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 find_histogram.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

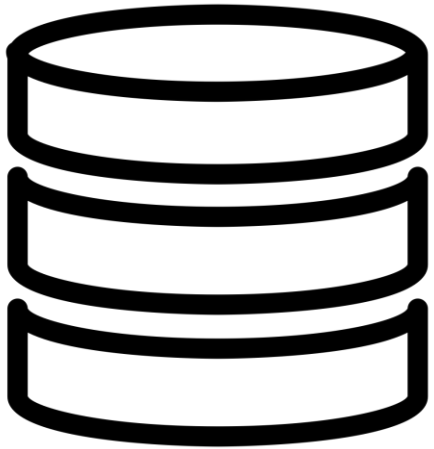
```
C:\Forensic Tools\hashcat-4.0.1
λ hashcat.exe -m 1000 -a 0 "T:\HTCIA 2018\NTLM hash.txt" "T:\HTCIA 2018\wordlist_split_000.txt"
```

hashcat

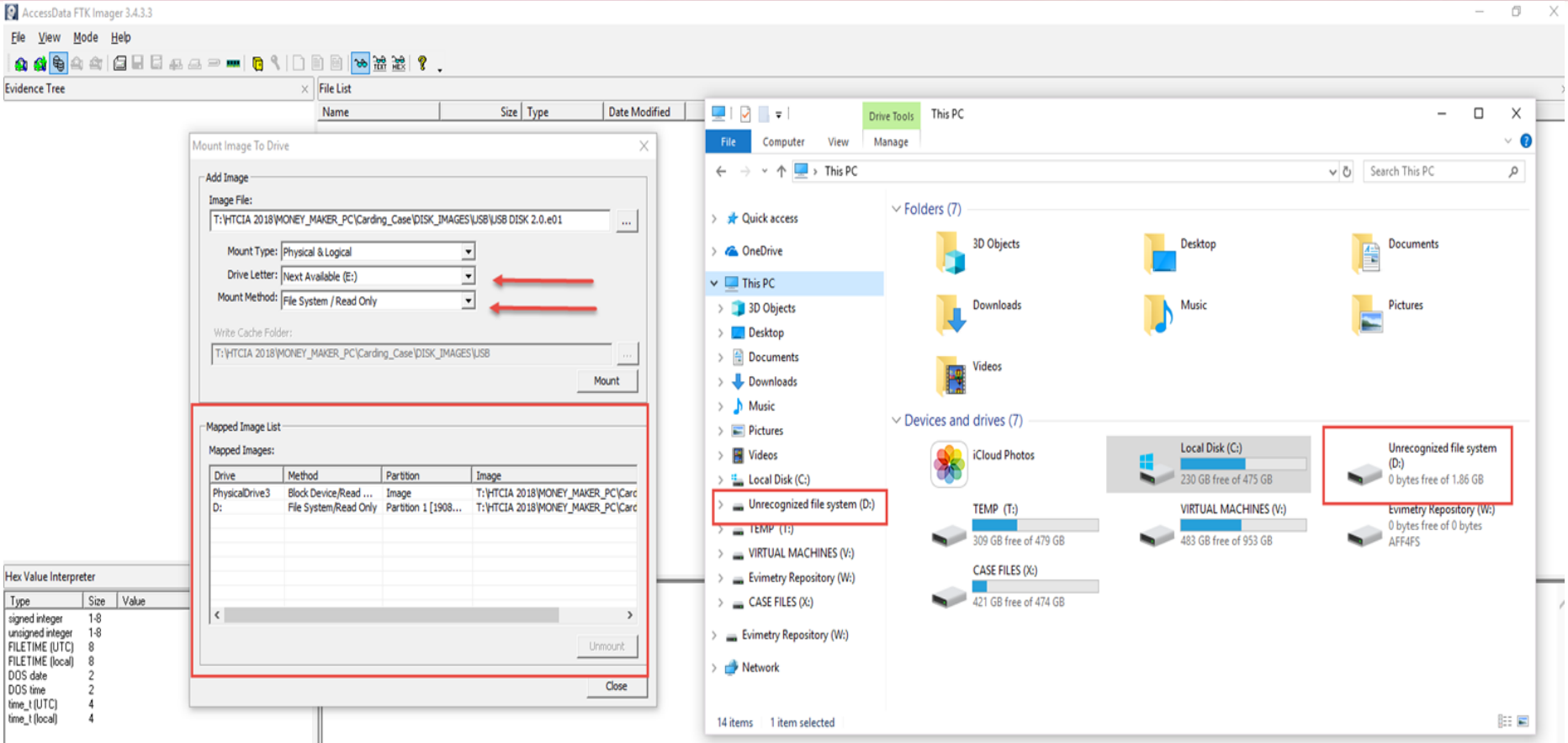
```
C:\Forensic Tools\hashcat-4.0.1
λ hashcat.exe -m 1000 -a 0 "T:\HTCIA 2018\FINAL\NTLM hash.txt" "T:\HTCIA 2018\FINAL\wordlist_split_000.txt"
hashcat (v4.0.1) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             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

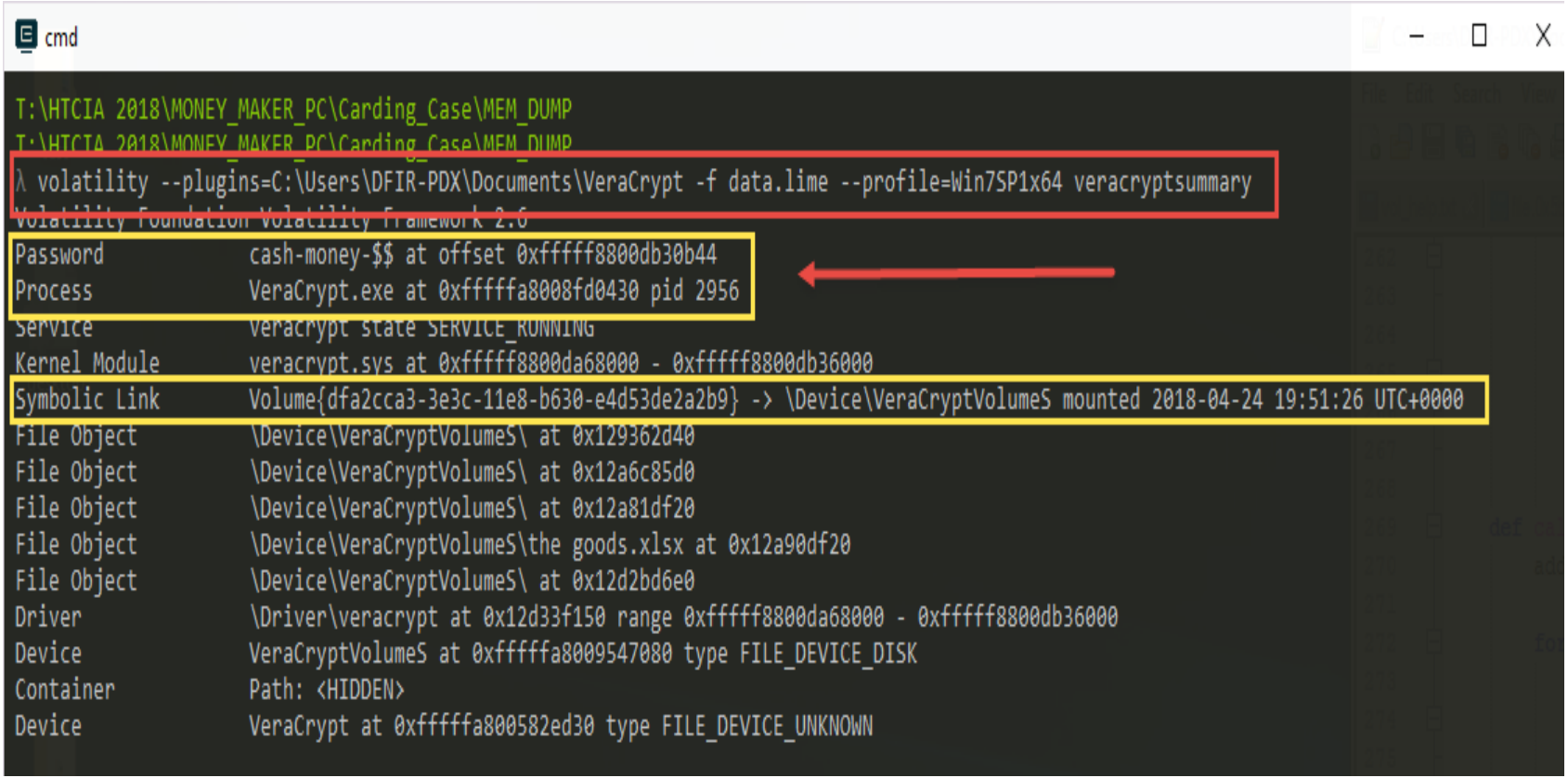
Analysis of Mounted Encrypted E01(USB)



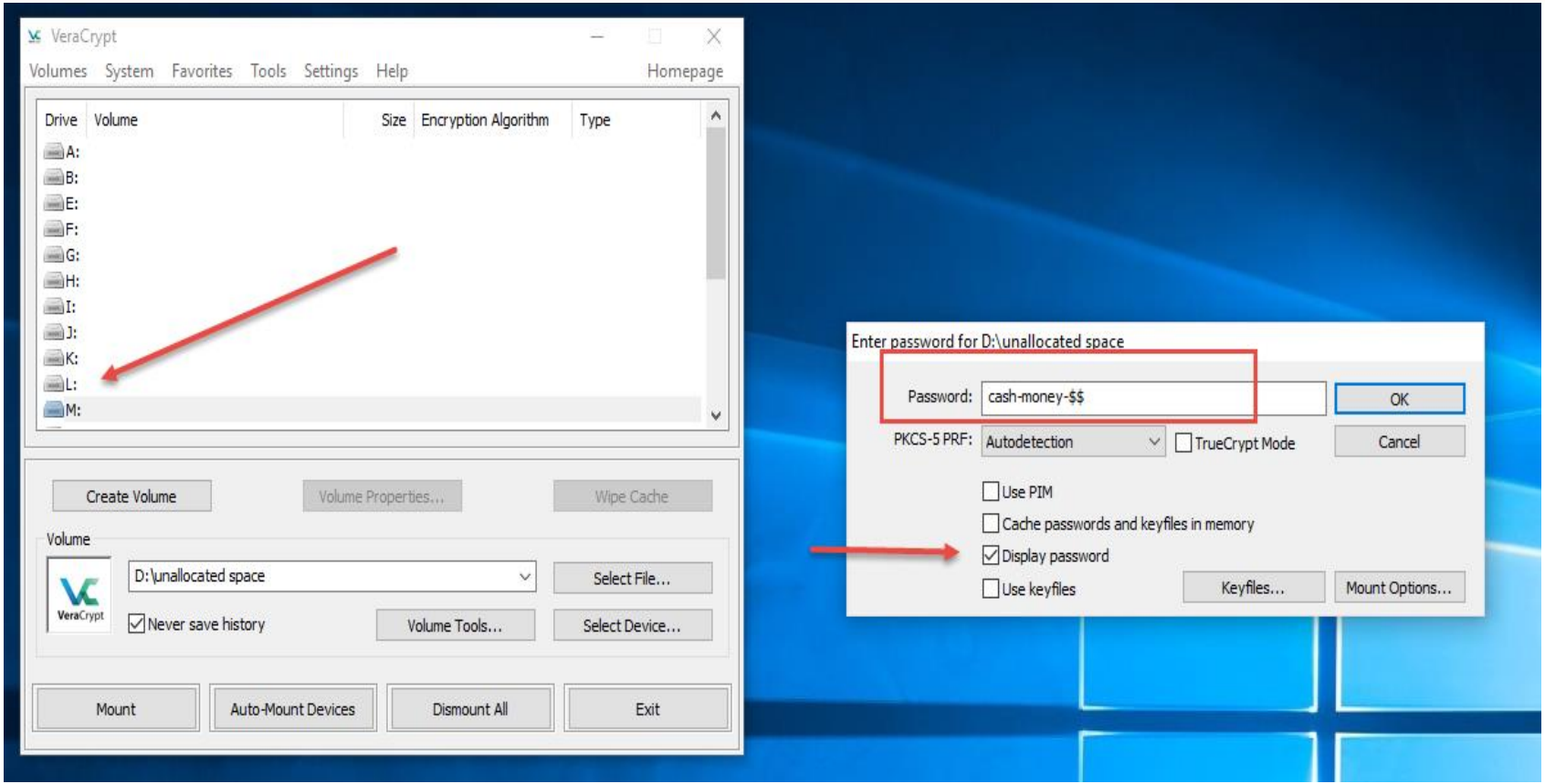
Mounted USB – FS not recognized



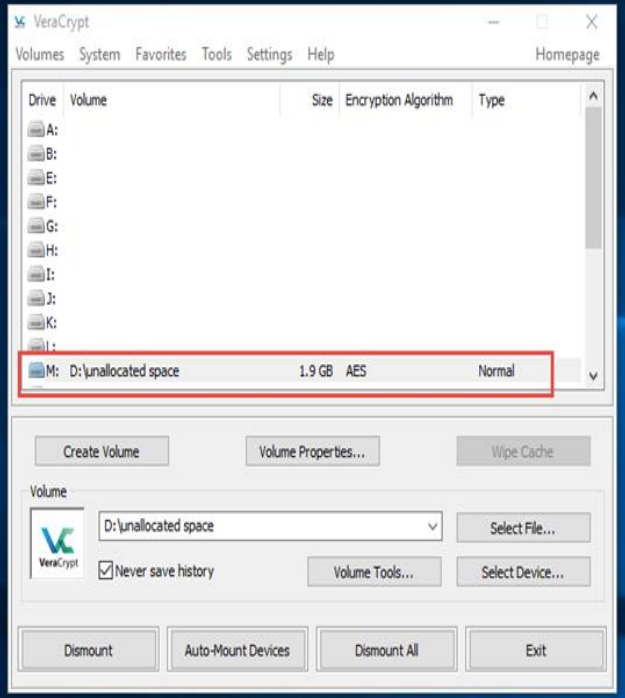
Custom VeraCrypt plugin

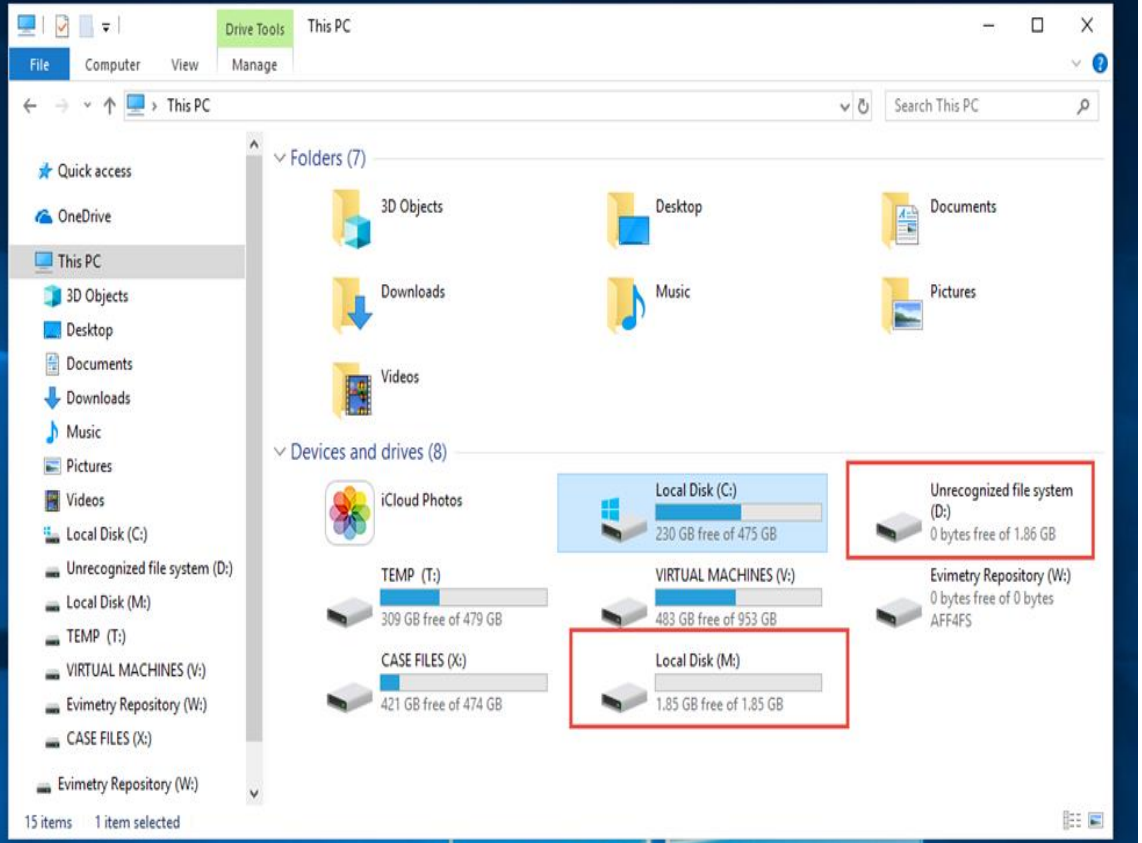


Mounting + VeraCrypt + password

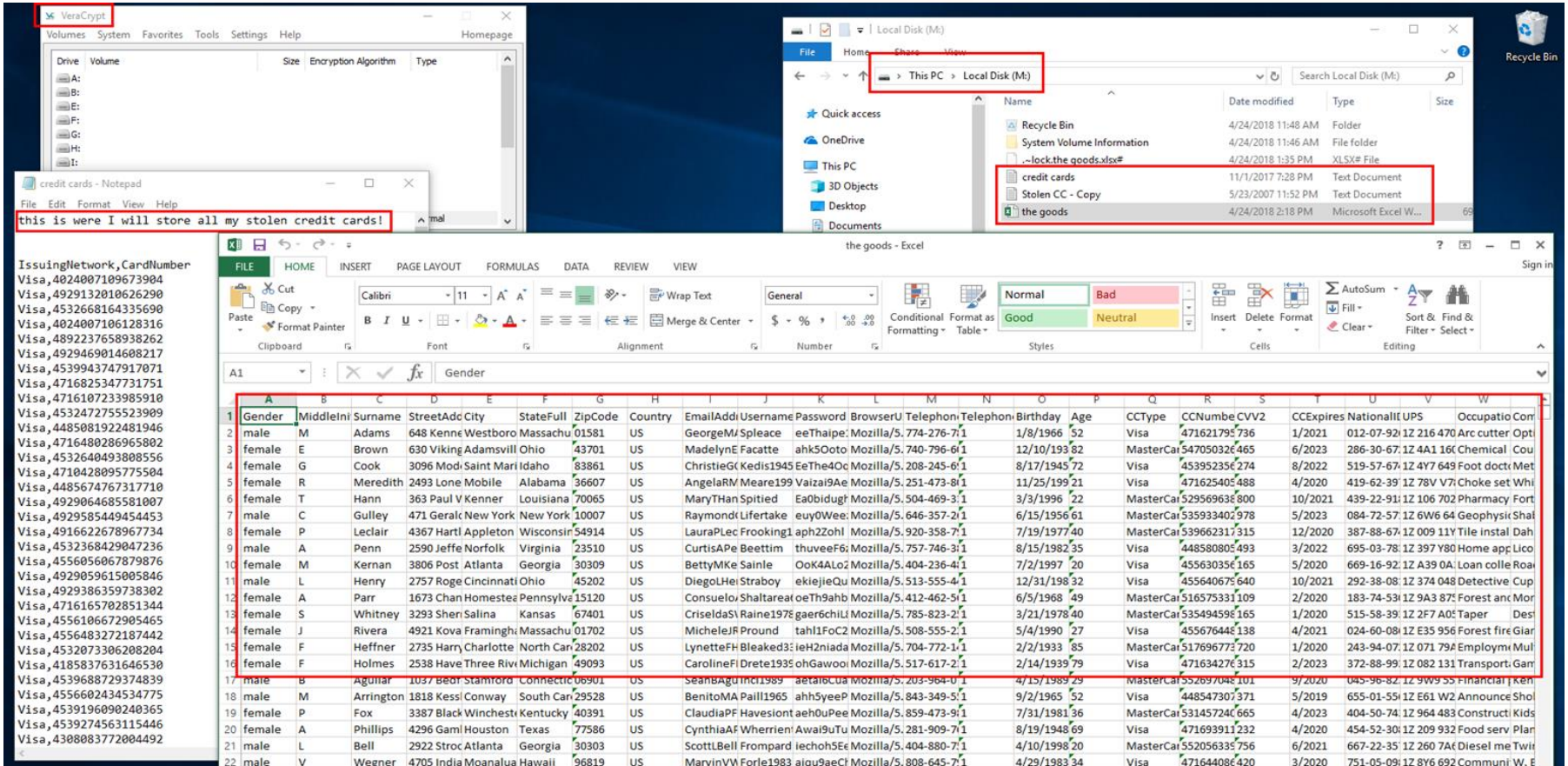


Mounted USB – FS recognized!





We found it!


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
credit cards - Notepad
File Edit Format View Help
this is were I will store all my stolen credit cards!
Local Disk (M:)
File Home Share View
This PC › Local Disk (M:)
Search Local Disk (M:)
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Name Date modified Type Size
Recycle Bin 4/24/2018 11:48 AM Folder
System Volume Information 4/24/2018 11:46 AM File folder
~lock.the goods.xlsx# 4/24/2018 1:35 PM XLSX# File
credit cards 11/1/2017 7:28 PM Text Document
Stolen CC - Copy 5/23/2007 11:52 PM Text Document
the goods 4/24/2018 2:18 PM Microsoft Excel W...
Recycle Bin
IssuingNetwork,CardNumber
Visa,4024007109673904
Visa,4929132010626290
Visa,4532668164335690
Visa,4024007106128316
Visa,4892237658938262
Visa,4929469014608217
Visa,4539943747917071
Visa,4716825347731751
Visa,4716107233985910
Visa,4532472755523909
Visa,4485081922481946
Visa,4716480286965802
Visa,4532640493808556
Visa,4710428095775504
Visa,4485674767317710
Visa,4929064685581007
Visa,4929585449454453
Visa,4916622678967734
Visa,4532368429047236
Visa,4556056067879876
Visa,4929059615005846
Visa,4929386359738302
Visa,4716165702851344
Visa,4556106672905465
Visa,4556483272187442
Visa,4532073306208204
Visa,4185837631646530
Visa,4539688729374839
Visa,4556602434534775
Visa,4539196090240365
Visa,4539274563115446
Visa,4308083772004492
the goods - Excel
FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW
Sign in
Paste Cut Copy Format Painter
Calibri 11
Wrap Text Merge & Center
General
Conditional Formatting Format as Table
Normal Bad Good Neutral
Insert Delete Format
AutoSum Fill Clear
Sort & Filter Find & Select
Clipboard Font Alignment Number Styles Cells Editing
A1 Gender
Gender MiddleIni Surname StreetAdd City StateFull ZipCode Country EmailAddi Username Password BrowserU Telephon Telephon Birthday Age CCType CCNumbe CVV2 CCExpires NationalI UPS Occupatio
male M Adams 648 Kenne Westboro Massachu 01581 US GeorgeM/ Spleace eeThaipe Mozilla/5. 774-276-7 1 1/8/1966 52 Visa 471621795 736 1/2021 012-07-92 1Z 216 470 Arc cutter
female E Brown 630 Viking Adamsvill Ohio 43701 US MadelynE Facatte ahk5Ooto Mozilla/5. 740-796-6 1 12/10/193 82 MasterCar 54705032 465 6/2023 286-30-67 1Z 4A1 16 Chemical
female G Cook 3096 Mod Saint Mari Idaho 83861 US ChristieG(Kedis1945 EeThe4Oc Mozilla/5. 208-245-6 1 8/17/1945 72 Visa 45395235 274 8/2022 519-57-67 1Z 4Y7 649 Foot doct
female R Meredith 2493 Lone Mobile Alabama 36607 US AngelaRM Meare199 Vaizai9Ae Mozilla/5. 251-473-8 1 11/25/199 21 Visa 471625405 488 4/2020 419-62-39 1Z 78V V7 Choke set
female T Hann 363 Paul V Kenner Louisiana 70065 US MaryTHan Spitied Ea0bidugh Mozilla/5. 504-469-3 1 3/3/1996 22 MasterCar 52956963 800 10/2021 439-22-91 1Z 106 702 Pharmacy
male C Gulley 471 Geral New York New York 10007 US Raymond Lifertake euy0Wee Mozilla/5. 646-357-2 1 6/15/1956 61 MasterCar 535933402 978 5/2023 084-72-57 1Z 6W6 64 Geophysi
female P Leclair 4367 Hartl Appleton Wisconsin 54914 US LauraPLec Frooking1 aph2Zohl Mozilla/5. 920-358-7 1 7/19/1977 40 MasterCar 539662317 315 12/2020 387-88-67 1Z 009 11Y Tile instal
male A Penn 2590 Jeffe Norfolk Virginia 23510 US CurtisAPe Beettim thuveeF6 Mozilla/5. 757-746-3 1 8/15/1982 35 Visa 448580805 493 3/2022 695-03-78 1Z 397 Y80 Home apr
female M Kernan 3806 Post Atlanta Georgia 30309 US BettyMKe Sainle OoK4ALo Mozilla/5. 404-236-4 1 7/2/1997 20 Visa 455630356 165 5/2020 669-16-92 1Z A39 0A Loan colle
male L Henry 2757 Roge Cincinnati Ohio 45202 US DiegoLHe Straboy ekiejieQu Mozilla/5. 513-555-4 1 12/31/198 32 Visa 455640675 640 10/2021 292-38-08 1Z 374 048 Detective
female A Parr 1673 Chan Homestea Pennsylva 15120 US Consuelo Shaltareat oeTh9ahb Mozilla/5. 412-462-5 1 6/5/1968 49 MasterCar 516575331 109 2/2020 183-74-53 1Z 9A3 87 Forest an
female S Whitney 3293 Sher Salina Kansas 67401 US CriseldaS Raine1978 gaer6chiL Mozilla/5. 785-823-2 1 3/21/1978 40 MasterCar 535494596 165 1/2020 515-58-39 1Z 2F7 A0 Taper
female J Rivera 4921 Kova Framingh Massachu 01702 US MicheleJF Pround tahl1FoC2 Mozilla/5. 508-555-2 1 5/4/1990 27 Visa 455676446 138 4/2021 024-60-08 1Z E35 956 Forest fire
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 1Z 071 79 Employm
female F Holmes 2538 Have Three Riv Michigan 49093 US CarolineFl Drete1935 ohGawooi Mozilla/5. 517-617-2 1 2/14/1939 79 Visa 47163427 315 2/2023 372-88-99 1Z 082 131 Transport
male B Aguilar 1037 Beds Stamford Connectic 06901 US SeanBAgu Inch1989 aetai6Cua Mozilla/5. 203-964-0 1 4/15/1989 29 MasterCar 552697045 101 9/2020 045-96-82 1Z 9W9 55 Financial
male M Arrington 1818 Kess Conway South Car 29528 US BenitoMA Paill1965 ahh5yeeP Mozilla/5. 843-349-5 1 9/2/1965 52 Visa 448547307 371 5/2019 655-01-55 1Z E61 W2 Announce
female P Fox 3387 Black Winchest Kentucky 40391 US ClaudiaPF Havesiont aeh0uPee Mozilla/5. 859-473-9 1 7/31/1981 36 MasterCar 531457246 665 4/2023 404-50-74 1Z 964 483 Construct
female A Phillips 4296 Gam Houston Texas 77586 US CynthiaAF Wherrien Awai9uTu Mozilla/5. 281-909-7 1 8/19/1948 69 Visa 471693911 232 4/2020 454-52-30 1Z 209 932 Food serv
male L Bell 2922 Stroc Atlanta Georgia 30303 US ScottLBell Frompard iechoh5Ee Mozilla/5. 404-880-7 1 4/10/1998 20 MasterCar 552056335 756 6/2021 667-22-35 1Z 260 7A Diesel me
female V Wegner 4705 India Moanalua Hawaii 96819 US MarvinVW Forle1983 ajgu9aeC Mozilla/5. 808-645-7 1 4/29/1983 34 Visa 471644086 420 3/2020 751-05-09 1Z 8Y6 692 Communi

Keeping up with memory?

Take a class!

- Malware and Memory Forensics Training (Volatility) https://www.memoryanalysis.net/memory-forensics-training
- SANS FOR526: Advanced Memory Forensics & Threat Detection https://www.sans.org/course/memory-forensics-in-depth
- Magnet Forensics AX250: Advanced 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

Twitter

Making Memories

Workflow Guide
https://bit.ly/3fbGkVh

Questions ?

AARON SPARLING **@OSINTLabworks**
JESSICA HYDE **@B1N2H3X**