Digital Forensic Final

Ali Kaba

Contents

Objectives

Technical Tools Information

Hardware Tools

Product Name	Forensic UltraDock V5
Model Number	31350-3209-0000
Unique ID	03-016341-C01
Firmware	f3.01.0004.000

Software Tools

FTK Imager	Used to view data
FTK Registry Viewer	Used to investigate registry files
WinMD5Free v1.20	Used to check MD5 checksum value of files
Microsoft Word	Used to write up this document
Prefetchviewer	Used to view items in the prefetch folder
Volatility	Used to analyses memory
Command Prompt	Used to run Volatility
Skitch	Used to take screenshots

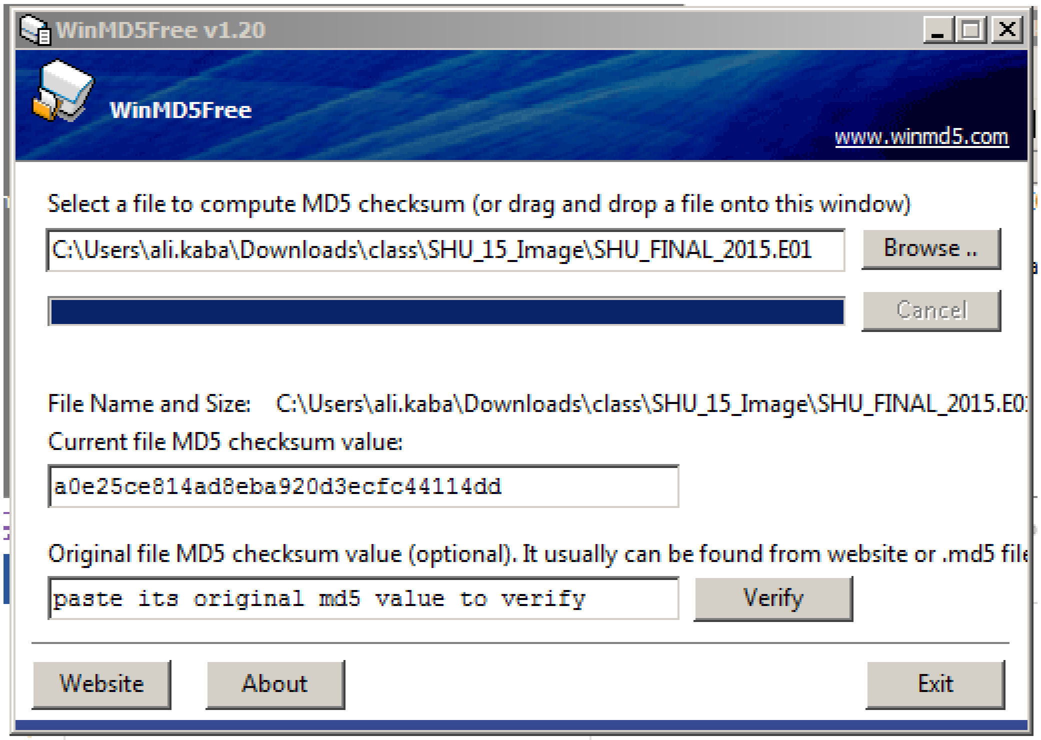
Hashing

Disk Drive

Product Manufacturer	Toshiba
Model Number	MK5065GSXF
Serial Number	33KPCX6WT
Firmware	GV108B
Disk Health	Normal
Start/Stops	12
Power Cycles	12
Bad Sectors	0
Disk Temp	~25 Celcius
Capacity (MB)	476940

Below is the hash routine for the “SHU_FINAL_2015.E01” file.

Original File Name	N/A
Original Directory	N/A
Original MD5 Pre-Hash	N/A
Master Copy File Name	SHU_FINAL_2015.E01
Master Copy Directory	C:\Users\ali.kaba\Downloads\class\SHU_15_Image\SHU_FINAL_2015.E01
Original MD5 Pre-Hash	N/A
Master Copy MD5 Pre-Hash	a0e25ce814ad8eba920d3ecfc44114dd
Working Copy File Name	SHU_FINAL_2015 - Copy.E01
Working Copy Directory	C:\Users\ali.kaba\Downloads\class\SHU_15_Image\SHU_FINAL_2015 - Copy.E01
Master Copy MD5 Pre-Hash	a0e25ce814ad8eba920d3ecfc44114dd
Working Copy MD5 Pre-Hash	a0e25ce814ad8eba920d3ecfc44114dd



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\SHU_15_Image\SHU_FINAL_2015.E01

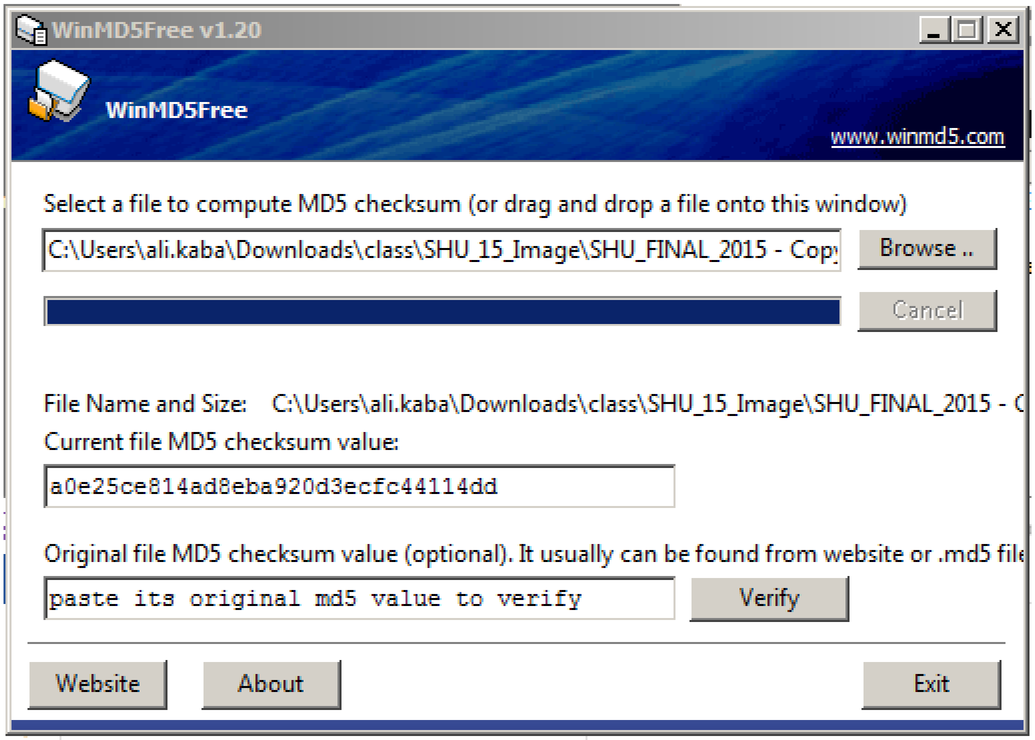
File Name and Size: C:\Users\ali.kaba\Downloads\class\SHU_15_Image\SHU_FINAL_2015.E0

Current file MD5 checksum value:

```
a0e25ce814ad8eba920d3ecfc44114dd
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\SHU_15_Image\SHU_FINAL_2015 - Copy

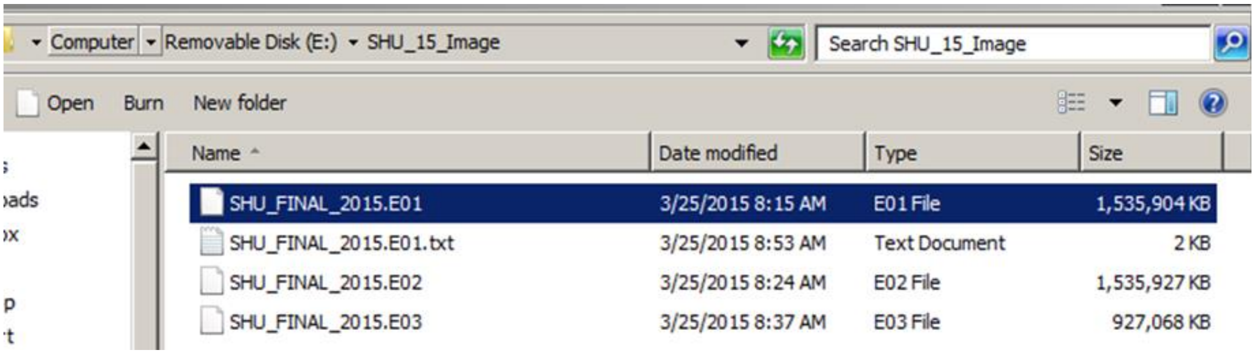
File Name and Size: C:\Users\ali.kaba\Downloads\class\SHU_15_Image\SHU_FINAL_2015 - C

Current file MD5 checksum value:

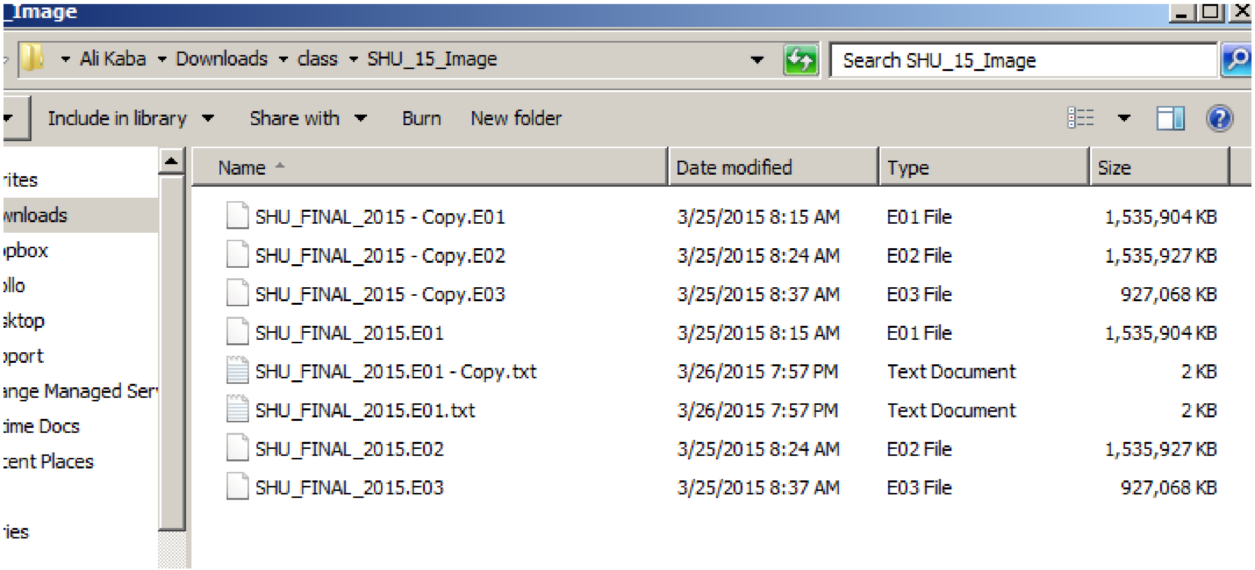
```
a0e25ce814ad8eba920d3ecfc44114dd
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify



Name	Date modified	Type	Size
SHU_FINAL_2015.E01	3/25/2015 8:15 AM	E01 File	1,535,904 KB
SHU_FINAL_2015.E01.txt	3/25/2015 8:53 AM	Text Document	2 KB
SHU_FINAL_2015.E02	3/25/2015 8:24 AM	E02 File	1,535,927 KB
SHU_FINAL_2015.E03	3/25/2015 8:37 AM	E03 File	927,068 KB

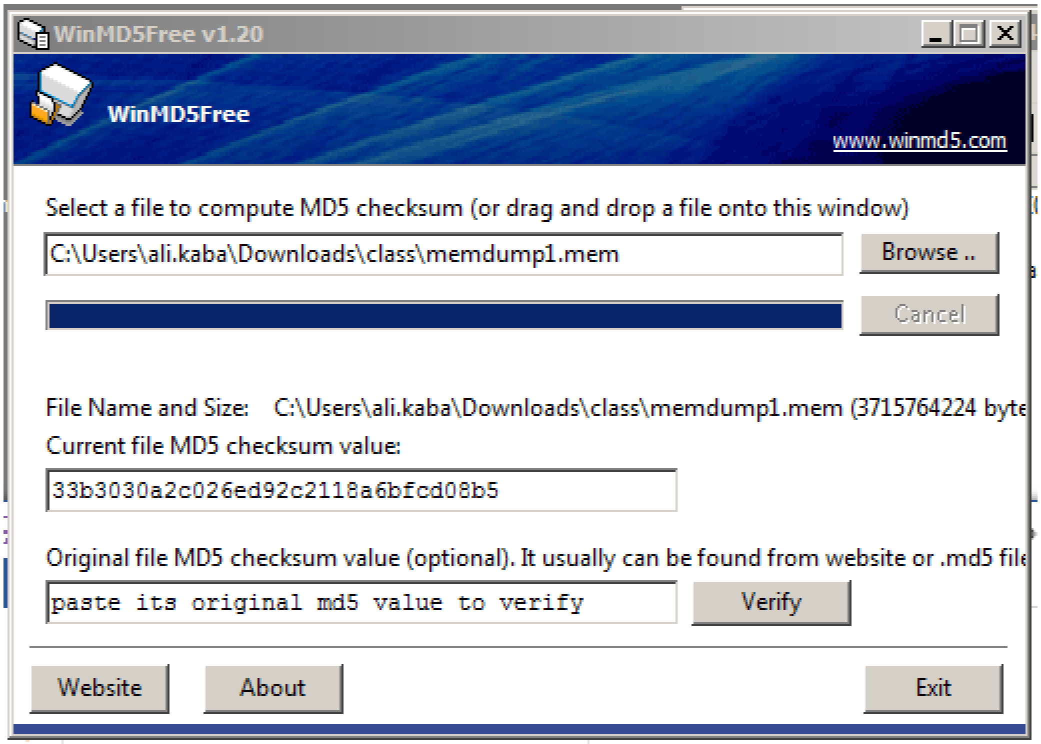


Name	Date modified	Type	Size
SHU_FINAL_2015 - Copy.E01	3/25/2015 8:15 AM	E01 File	1,535,904 KB
SHU_FINAL_2015 - Copy.E02	3/25/2015 8:24 AM	E02 File	1,535,927 KB
SHU_FINAL_2015 - Copy.E03	3/25/2015 8:37 AM	E03 File	927,068 KB
SHU_FINAL_2015.E01	3/25/2015 8:15 AM	E01 File	1,535,904 KB
SHU_FINAL_2015.E01 - Copy.txt	3/26/2015 7:57 PM	Text Document	2 KB
SHU_FINAL_2015.E01.txt	3/26/2015 7:57 PM	Text Document	2 KB
SHU_FINAL_2015.E02	3/25/2015 8:24 AM	E02 File	1,535,927 KB
SHU_FINAL_2015.E03	3/25/2015 8:37 AM	E03 File	927,068 KB

Memory

Below is the hash routine for the file name “memdump1.mem” file.

Original File Name	memdump1.mem
Original Directory	C:\Users\ali.kaba\Downloads\class\memdump1.mem
Original MD5 Pre-Hash	33b3030a2c026ed92c2118a6bfcd08b5
Master Copy File Name	memdump1.mem
Master Copy Directory	C:\Users\ali.kaba\Downloads\class\memdump1.mem
Original MD5 Pre-Hash	33b3030a2c026ed92c2118a6bfcd08b5
Master Copy MD5 Pre-Hash	33b3030a2c026ed92c2118a6bfcd08b5
Working Copy File Name	memdump1 - Copy.mem
Working Copy Directory	C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem
Master Copy MD5 Pre-Hash	33b3030a2c026ed92c2118a6bfcd08b5
Working Copy MD5 Pre-Hash	33b3030a2c026ed92c2118a6bfcd08b5



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\memdump1.mem

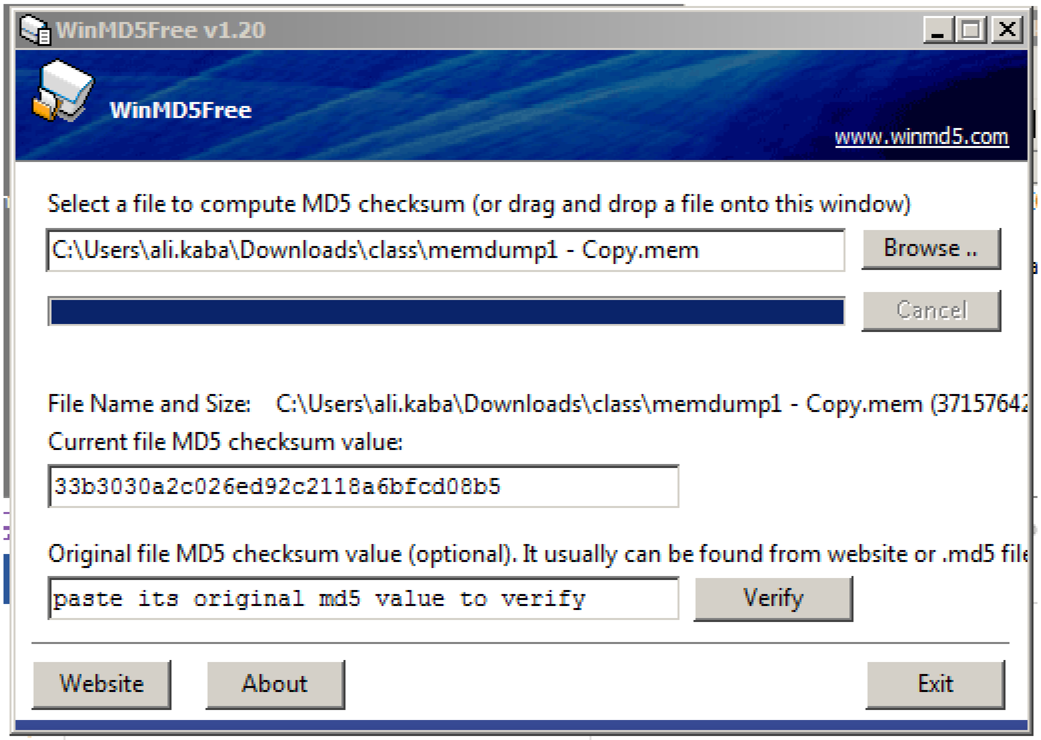
File Name and Size: C:\Users\ali.kaba\Downloads\class\memdump1.mem (3715764224 byte

Current file MD5 checksum value:

```
33b3030a2c026ed92c2118a6bfcd08b5
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem

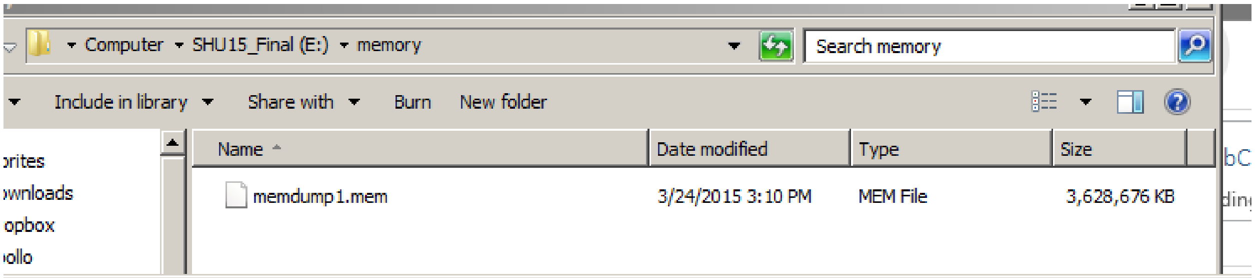
File Name and Size: C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem (37157642

Current file MD5 checksum value:

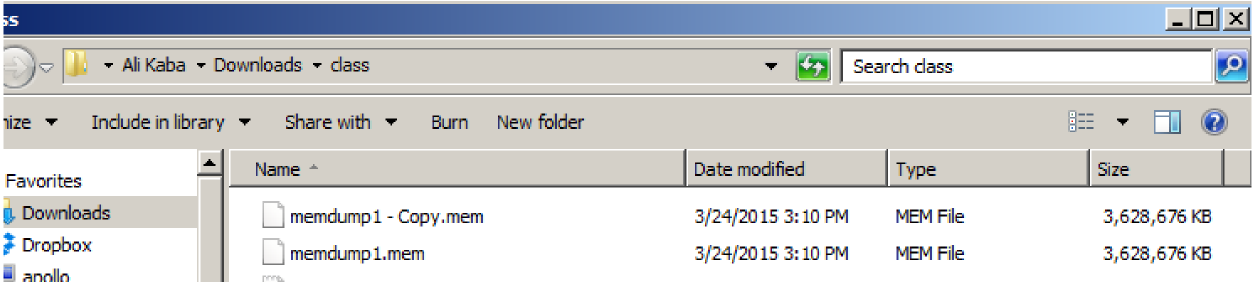
```
33b3030a2c026ed92c2118a6bfcd08b5
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify



Name	Date modified	Type	Size
memdump1.mem	3/24/2015 3:10 PM	MEM File	3,628,676 KB



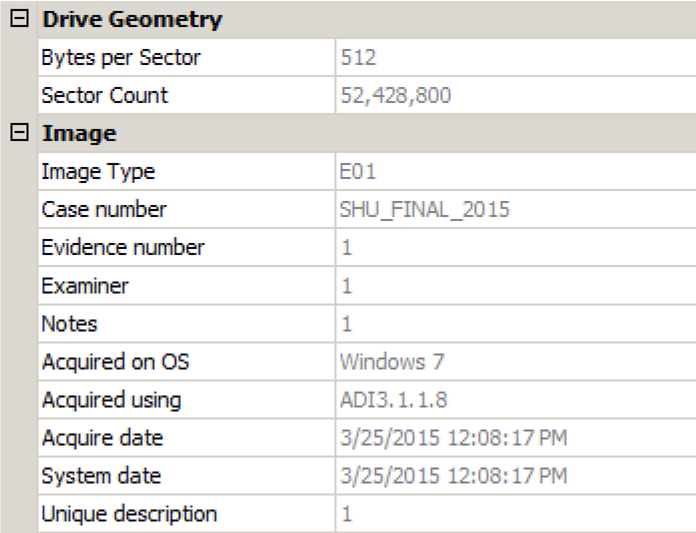
Name	Date modified	Type	Size
memdump1 - Copy.mem	3/24/2015 3:10 PM	MEM File	3,628,676 KB
memdump1.mem	3/24/2015 3:10 PM	MEM File	3,628,676 KB

Investigating: Disk Drive

The following are detail information about this disk drive image.

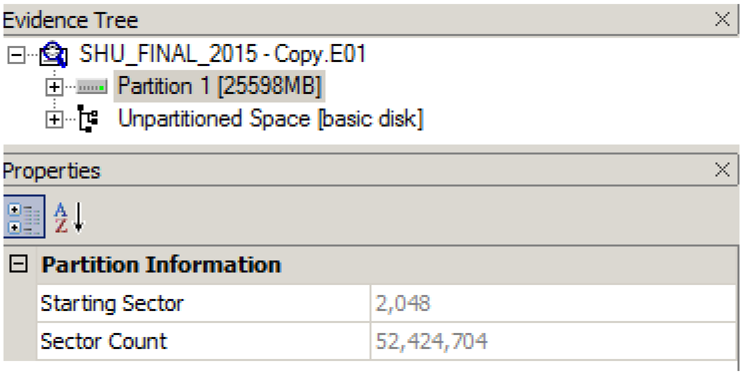
Volume Name	SHU_FINAL_2015
Bytes per Sector	512
Sector Count	52,428,800
Partition Name	Partition 1
Partition Size (MB)	25598
Partition Starting Sector	2,048
Partition Sector Count	52,424,704
Logical Drive Name	NONAME
Logical Drive Cluster Size	4,096
Logical Drive Cluster Count	6,553,087
Logical Drive Free Cluster Count	3,823,252
Logical Drive Volume Serial Number	BE1B-7BD2
Logical Drive File System Version	Windows XP (NTFS 3.1)
Logical Drive File System	NTFS

The case is SHU_FINAL_2015, it has 512 bytes per sectors and 52,428,800 sector count.



Drive Geometry	
Bytes per Sector	512
Sector Count	52,428,800
Image	
Image Type	E01
Case number	SHU_FINAL_2015
Evidence number	1
Examiner	1
Notes	1
Acquired on OS	Windows 7
Acquired using	ADI3.1.1.8
Acquire date	3/25/2015 12:08:17 PM
System date	3/25/2015 12:08:17 PM
Unique description	1

The partition 1 starting sector is 2,048 is 25598MB.



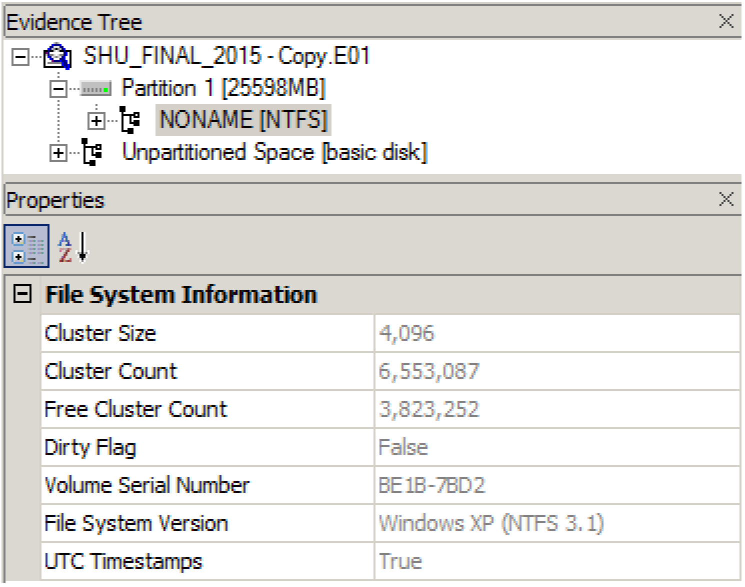
Evidence Tree

SHU_FINAL_2015 - Copy.E01
- Partition 1 [25598MB]
- Unpartitioned Space [basic disk]

Properties

Partition Information	
Starting Sector	2,048
Sector Count	52,424,704

The partition name is called NONAME and is a Windows NTFS 3.1 file system. Its cluster size is 4,096 and cluster count is 6,553,087. The Free cluster count is 3,823,253 and volume serial number is BE1B-7BD2



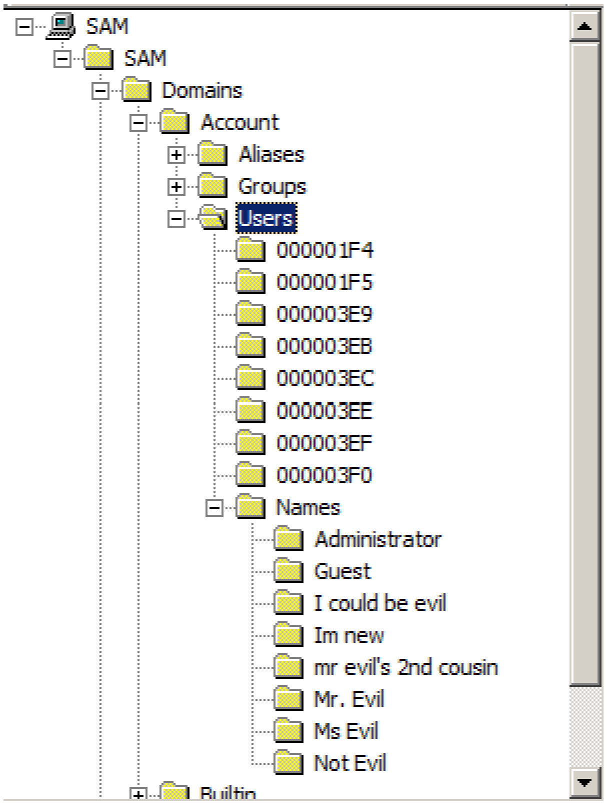
Evidence Tree

SHU_FINAL_2015 - Copy.E01
- Partition 1 [25598MB]
  - NONAME [NTFS]
- Unpartitioned Space [basic disk]

Properties

File System Information	
Cluster Size	4,096
Cluster Count	6,553,087
Free Cluster Count	3,823,252
Dirty Flag	False
Volume Serial Number	BE1B-7BD2
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

User accounts are found in SAM.

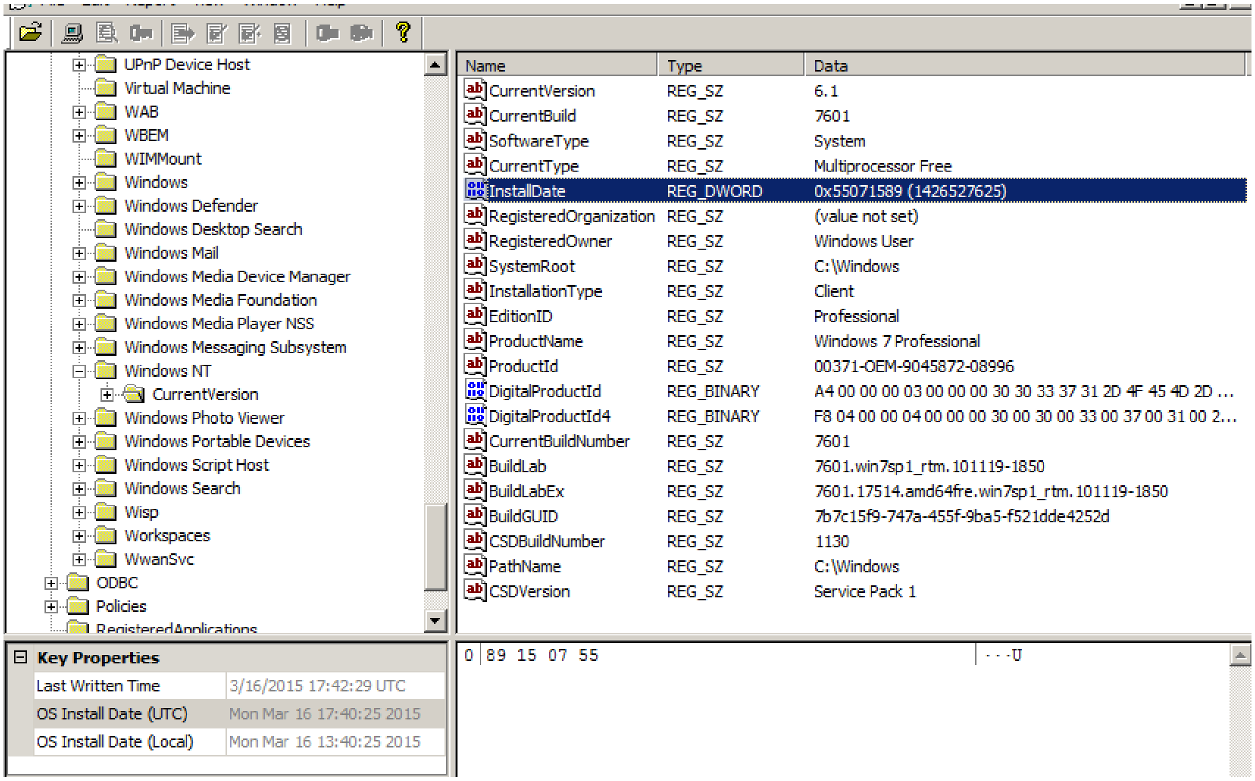


Based on the data provided below, an account was created and deleted before “Mr. Evil” and between “Mr. Evil” and “Not Evil” as well as between “I could be evil” and “Ms Evil”. Guest and Im New never logged on.

Account Name	Hex	Decimal	Logon Count	Last Log
Administrator	000001F4	500	6	11/21/2010 3:47:20 UTC
Guest	000001F5	501	0	Never
Mr. Evil	000003E9	1001	9	3/25/2015 12:04:49 UTC
Not Evil	000003EB	1003	2	3/24/2015 14:41:55 UTC
I could be evil	000003EC	1004	2	3/24/2015 14:42:39 UTC
Ms Evil	000003EE	1006	1	3/24/2015 14:41:16 UTC
mr evil’s 2nd cousin	000003EF	1007	2	3/24/2015 14:42:13 UTC
Im new	000003F0	1008	0	Never

Below list OS install date, version OS, registered name and Time zone.

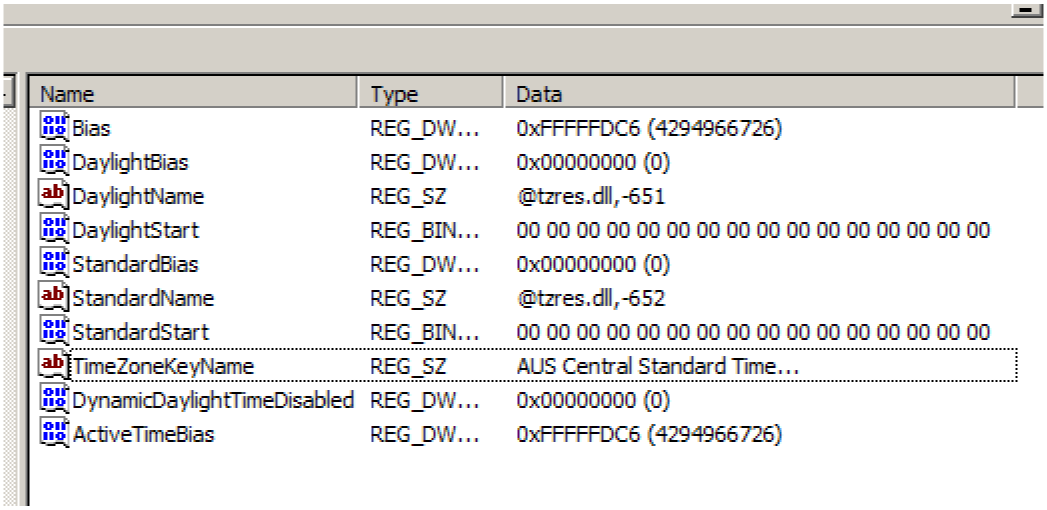
OS Install Date	OS Version	Registered Name	Time Zone
Mon Mar 16 17:40:25 2015 (UTC)	6.1	Windows User	AUS Central Standard Time



Name	Type	Data
CurrentVersion	REG_SZ	6.1
CurrentBuild	REG_SZ	7601
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x55071589 (1426527625)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	Windows User
SystemRoot	REG_SZ	C:\Windows
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Professional
ProductName	REG_SZ	Windows 7 Professional
ProductId	REG_SZ	00371-OEM-9045872-08996
DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 30 30 33 37 31 2D 4F 45 4D 2D ...
DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 00 30 00 30 00 33 00 37 00 31 00 2...
CurrentBuildNumber	REG_SZ	7601
BuildLab	REG_SZ	7601.win7sp1_rtm.101119-1850
BuildLabEx	REG_SZ	7601.17514.amd64fre.win7sp1_rtm.101119-1850
BuildGUID	REG_SZ	7b7c15f9-747a-455f-9ba5-f521dde4252d
CSDBuildNumber	REG_SZ	1130
PathName	REG_SZ	C:\Windows
CSDVersion	REG_SZ	Service Pack 1

Key Properties	
Last Written Time	3/16/2015 17:42:29 UTC
OS Install Date (UTC)	Mon Mar 16 17:40:25 2015
OS Install Date (Local)	Mon Mar 16 13:40:25 2015

```
0 89 15 07 55                    ...U
```

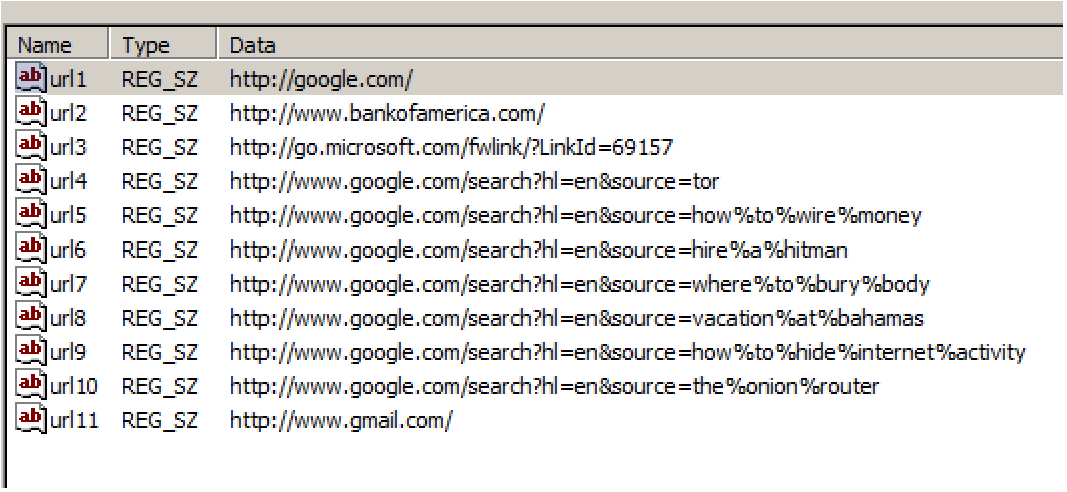


Name	Type	Data
Bias	REG_DW...	0xFFFFFDC6 (4294966726)
DaylightBias	REG_DW...	0x00000000 (0)
DaylightName	REG_SZ	@tzres.dll,-651
DaylightStart	REG_BIN...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
StandardBias	REG_DW...	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-652
StandardStart	REG_BIN...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	AUS Central Standard Time...
DynamicDaylightTimeDisabled	REG_DW...	0x00000000 (0)
ActiveTimeBias	REG_DW...	0xFFFFFDC6 (4294966726)

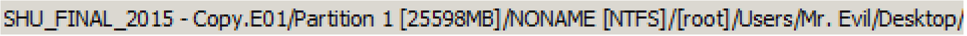
Mr. Evil URLs in chronological order:

URL	Query
http://google.com	N/A
http://www.bankofamerica.com	N/A
http://go.microsoft.com/fwlink/?LinkId=69157	N/A
http://google.com	tor
http://google.com	how to wire money
http://google.com	hire a hitman
http://google.com	where to bury body
http://google.com	vacation at Bahamas

http://google.com	How to hide internet activity
http://google.com	The onion router
http://gmail.com	N/A

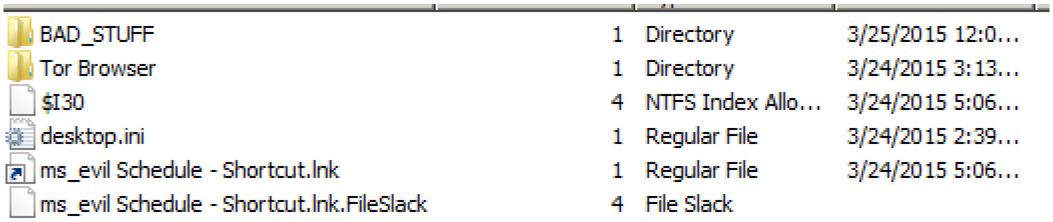


Name	Type	Data
url1	REG_SZ	http://google.com/
url2	REG_SZ	http://www.bankofamerica.com/
url3	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=69157
url4	REG_SZ	http://www.google.com/search?hl=en&source=tor
url5	REG_SZ	http://www.google.com/search?hl=en&source=how%to%wire%money
url6	REG_SZ	http://www.google.com/search?hl=en&source=hire%a%hitman
url7	REG_SZ	http://www.google.com/search?hl=en&source=where%to%bury%body
url8	REG_SZ	http://www.google.com/search?hl=en&source=vacation%at%bahamas
url9	REG_SZ	http://www.google.com/search?hl=en&source=how%to%hide%internet%activity
url10	REG_SZ	http://www.google.com/search?hl=en&source=the%onion%router
url11	REG_SZ	http://www.gmail.com/



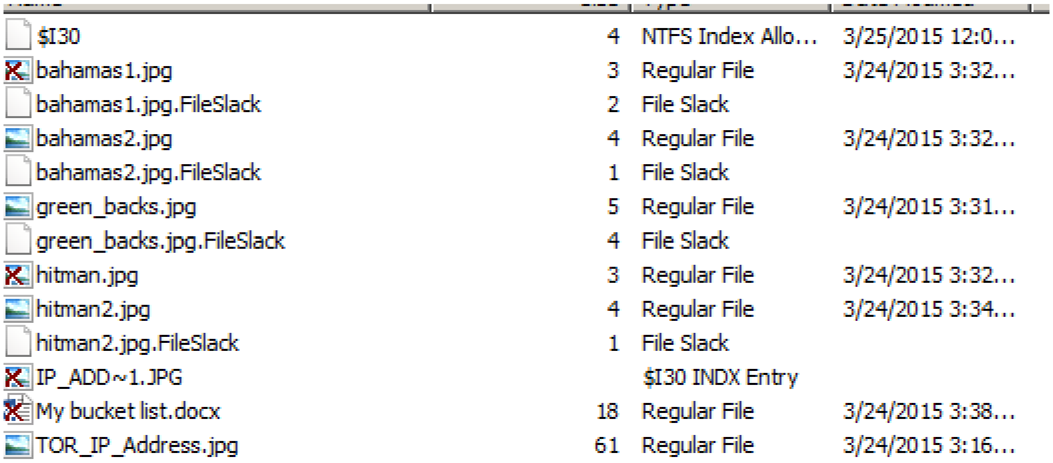
After navigating into SHU_FINAL_2015 - Copy.E01/Partition 1 [25598MB]/NONAME [NTFS]/[root]/Users/Mr. Evil/Desktop/

I came across two folders:

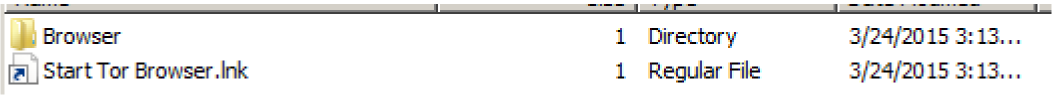


BAD_STUFF	1	Directory	3/25/2015 12:0…
Tor Browser	1	Directory	3/24/2015 3:13…
$I30	4	NTFS Index Allo…	3/24/2015 5:06…
desktop.ini	1	Regular File	3/24/2015 2:39…
ms_evil Schedule - Shortcut.lnk	1	Regular File	3/24/2015 5:06…
ms_evil Schedule - Shortcut.lnk.FileSlack	4	File Slack	

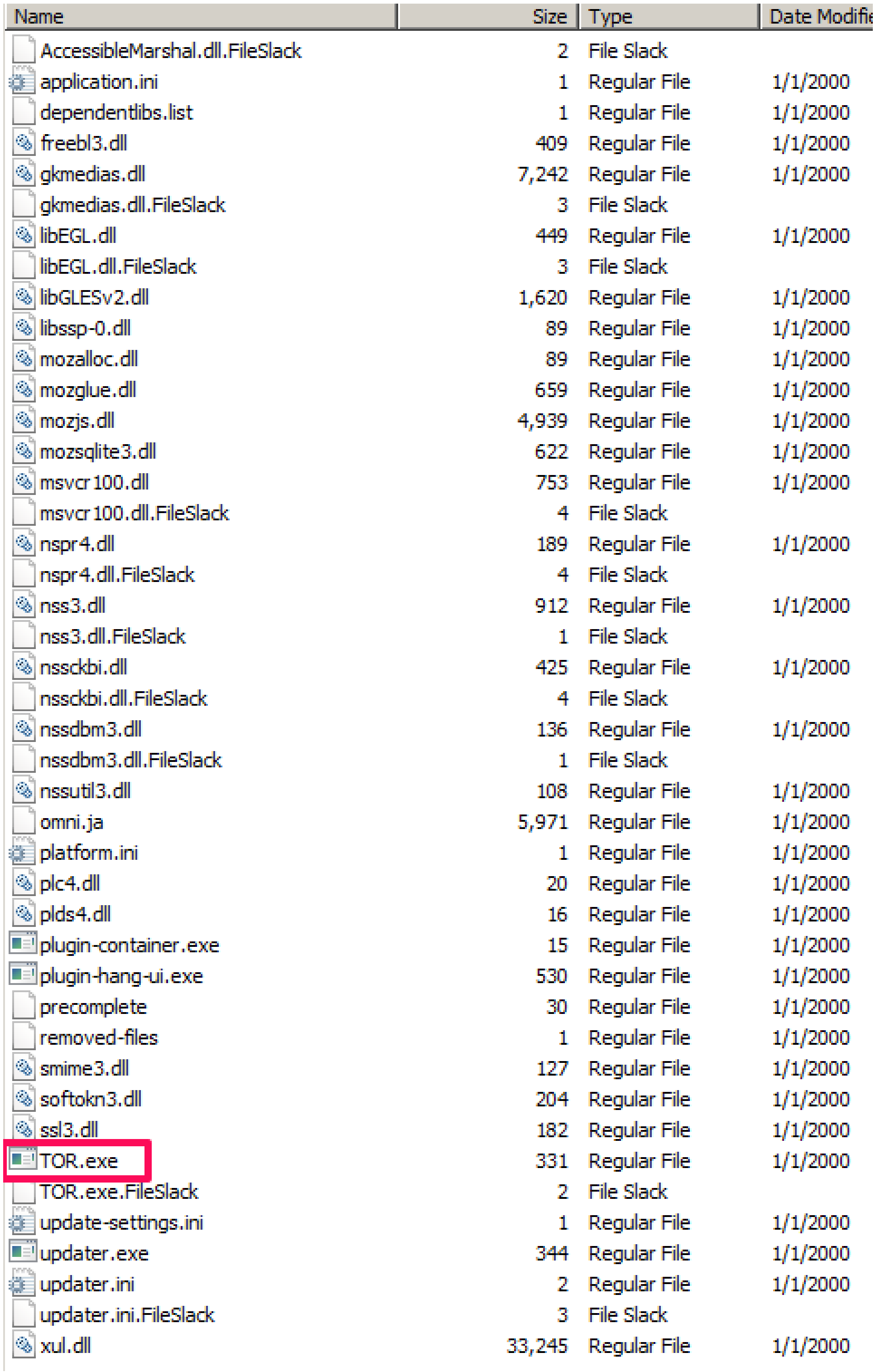
Tor was in fact downloaded onto the desktop and the BAD_STUFF folder has pictures related to the URLs:



$I30	4	NTFS Index Allo…	3/25/2015 12:0…
bahamas1.jpg	3	Regular File	3/24/2015 3:32…
bahamas1.jpg.FileSlack	2	File Slack	
bahamas2.jpg	4	Regular File	3/24/2015 3:32…
bahamas2.jpg.FileSlack	1	File Slack	
green_backs.jpg	5	Regular File	3/24/2015 3:31…
green_backs.jpg.FileSlack	4	File Slack	
hitman.jpg	3	Regular File	3/24/2015 3:32…
hitman2.jpg	4	Regular File	3/24/2015 3:34…
hitman2.jpg.FileSlack	1	File Slack	
IP_ADD~1.JPG		$I30 INDX Entry	
My bucket list.docx	18	Regular File	3/24/2015 3:38…
TOR_IP_Address.jpg	61	Regular File	3/24/2015 3:16…



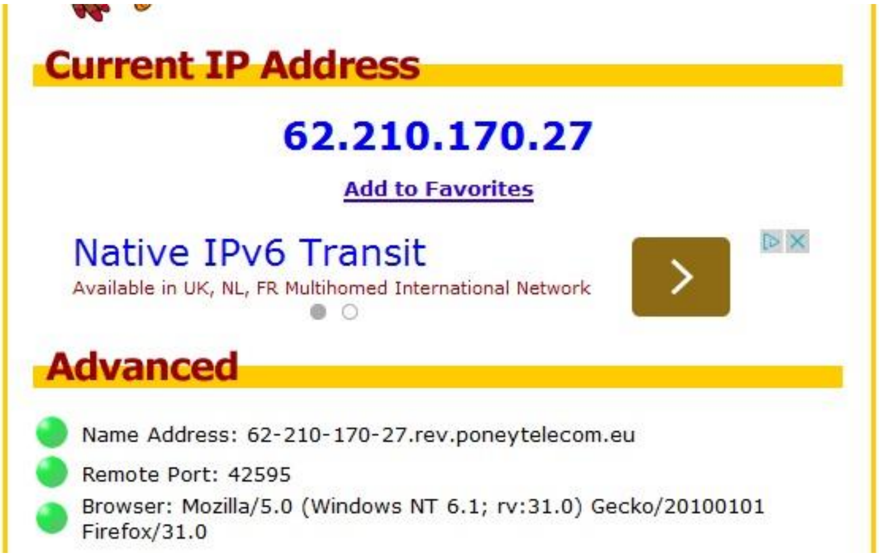
Browser	1	Directory	3/24/2015 3:13...
Start Tor Browser.lnk	1	Regular File	3/24/2015 3:13...



Name	Size	Type	Date Modifie
AccessibleMarshal.dll.FileSlack	2	File Slack	
application.ini	1	Regular File	1/1/2000
dependentlibs.list	1	Regular File	1/1/2000
freebl3.dll	409	Regular File	1/1/2000
gkmedias.dll	7,242	Regular File	1/1/2000
gkmedias.dll.FileSlack	3	File Slack	
libEGL.dll	449	Regular File	1/1/2000
libEGL.dll.FileSlack	3	File Slack	
libGLESv2.dll	1,620	Regular File	1/1/2000
libssp-0.dll	89	Regular File	1/1/2000
mozalloc.dll	89	Regular File	1/1/2000
mozglue.dll	659	Regular File	1/1/2000
mozjs.dll	4,939	Regular File	1/1/2000
mozsqlite3.dll	622	Regular File	1/1/2000
msvcr100.dll	753	Regular File	1/1/2000
msvcr100.dll.FileSlack	4	File Slack	
nspr4.dll	189	Regular File	1/1/2000
nspr4.dll.FileSlack	4	File Slack	
nss3.dll	912	Regular File	1/1/2000
nss3.dll.FileSlack	1	File Slack	
nssckbi.dll	425	Regular File	1/1/2000
nssckbi.dll.FileSlack	4	File Slack	
nssdbm3.dll	136	Regular File	1/1/2000
nssdbm3.dll.FileSlack	1	File Slack	
nssutil3.dll	108	Regular File	1/1/2000
omni.ja	5,971	Regular File	1/1/2000
platform.ini	1	Regular File	1/1/2000
plc4.dll	20	Regular File	1/1/2000
plds4.dll	16	Regular File	1/1/2000
plugin-container.exe	15	Regular File	1/1/2000
plugin-hang-ui.exe	530	Regular File	1/1/2000
precomplete	30	Regular File	1/1/2000
removed-files	1	Regular File	1/1/2000
smime3.dll	127	Regular File	1/1/2000
softokn3.dll	204	Regular File	1/1/2000
ssl3.dll	182	Regular File	1/1/2000
TOR.exe	331	Regular File	1/1/2000
TOR.exe.FileSlack	2	File Slack	
update-settings.ini	1	Regular File	1/1/2000
updater.exe	344	Regular File	1/1/2000
updater.ini	2	Regular File	1/1/2000
updater.ini.FileSlack	3	File Slack	
xul.dll	33,245	Regular File	1/1/2000

Tor is free software for enabling anonymous communication. The name is an acronym derived from the original software project name The Onion Router.[5] Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays[6] to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". –Wikipedia

Below is the TOR's IP address found in the BAD_STUFF folder located on the desktop of Mr. evil:



Current IP Address

62.210.170.27

Add to Favorites

Native IPv6 Transit
Available in UK, NL, FR Multihomed International Network

Advanced

- Name Address: 62-210-170-27.rev.poneytelecom.eu
- Remote Port: 42595
- Browser: Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0

What is a prefetch?

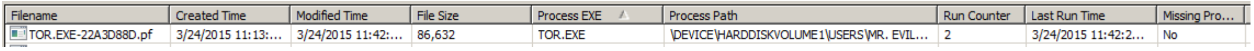
Each time you turn on your computer, Windows keeps track of the way your computer starts and which programs you commonly open. Windows saves this information as a number of small files in the prefetch folder. The next time you turn on your computer, Windows refers to these files to help speed the start process.

The prefetch folder is a subfolder of the Windows system folder. The prefetch folder is self-maintaining, and there's no need to delete it or empty its contents. If you empty the folder, Windows and your programs will take longer to open the next time you turn on your computer. -Windows

After navigating into this directory:

SHU_FINAL_2015 - Copy.E01/Partition 1 [25598MB]/NONAME [NTFS]/[root]/Windows/Prefetch/

I used Winprefetchview to find that TOR was infact launched as showed below:

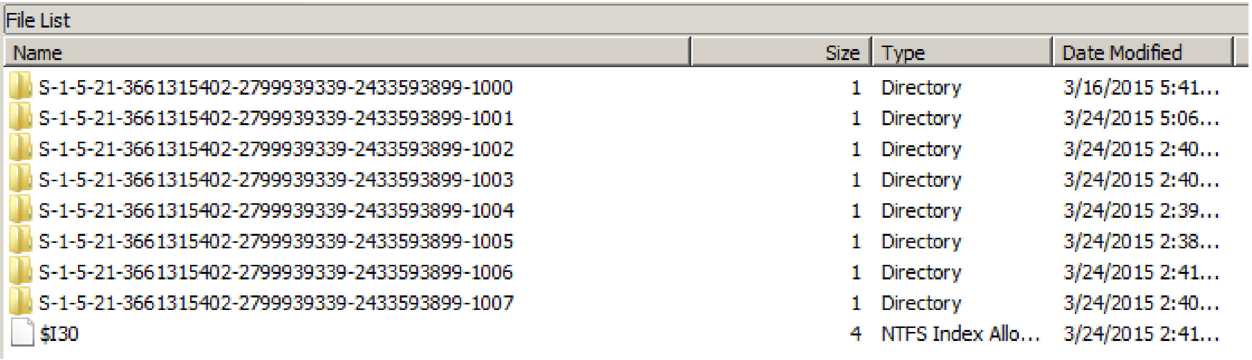


Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pro...
TOR.EXE-22A3D88D.pf	3/24/2015 11:13:...	3/24/2015 11:42:...	86,632	TOR.EXE	\DEVICE\HARDDISKVOLUME1\USERS\MR. EVIL...	2	3/24/2015 11:42:2...	No

After navigating into the Recyle.Bin folder, I was able to see SID related to active accounts as well as deleted accounts:

Account Name	Hex	Decimal	Recycle Folder
Administrator	000001F4	500	Never

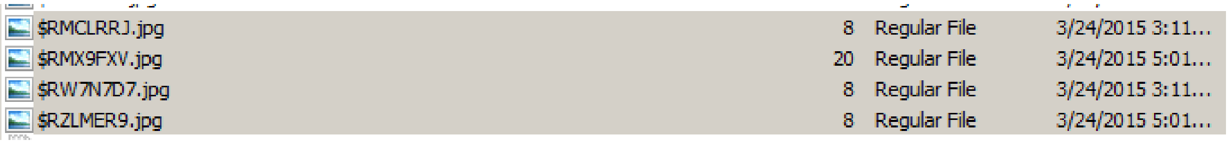
Guest	000001F5	501	Never
Mr. Evil	000003E9	1001	Yes
Not Evil	000003EB	1003	Yes
I could be evil	000003EC	1004	Yes
Ms Evil	000003EE	1006	Yes
mr evil's 2nd cousin	000003EF	1007	Yes
Im new	000003F0	1008	Never



File List

Name	Size	Type	Date Modified
S-1-5-21-3661315402-2799939339-2433593899-1000	1	Directory	3/16/2015 5:41...
S-1-5-21-3661315402-2799939339-2433593899-1001	1	Directory	3/24/2015 5:06...
S-1-5-21-3661315402-2799939339-2433593899-1002	1	Directory	3/24/2015 2:40...
S-1-5-21-3661315402-2799939339-2433593899-1003	1	Directory	3/24/2015 2:40...
S-1-5-21-3661315402-2799939339-2433593899-1004	1	Directory	3/24/2015 2:39...
S-1-5-21-3661315402-2799939339-2433593899-1005	1	Directory	3/24/2015 2:38...
S-1-5-21-3661315402-2799939339-2433593899-1006	1	Directory	3/24/2015 2:41...
S-1-5-21-3661315402-2799939339-2433593899-1007	1	Directory	3/24/2015 2:40...
$I30	4	NTFS Index Allo...	3/24/2015 2:41...

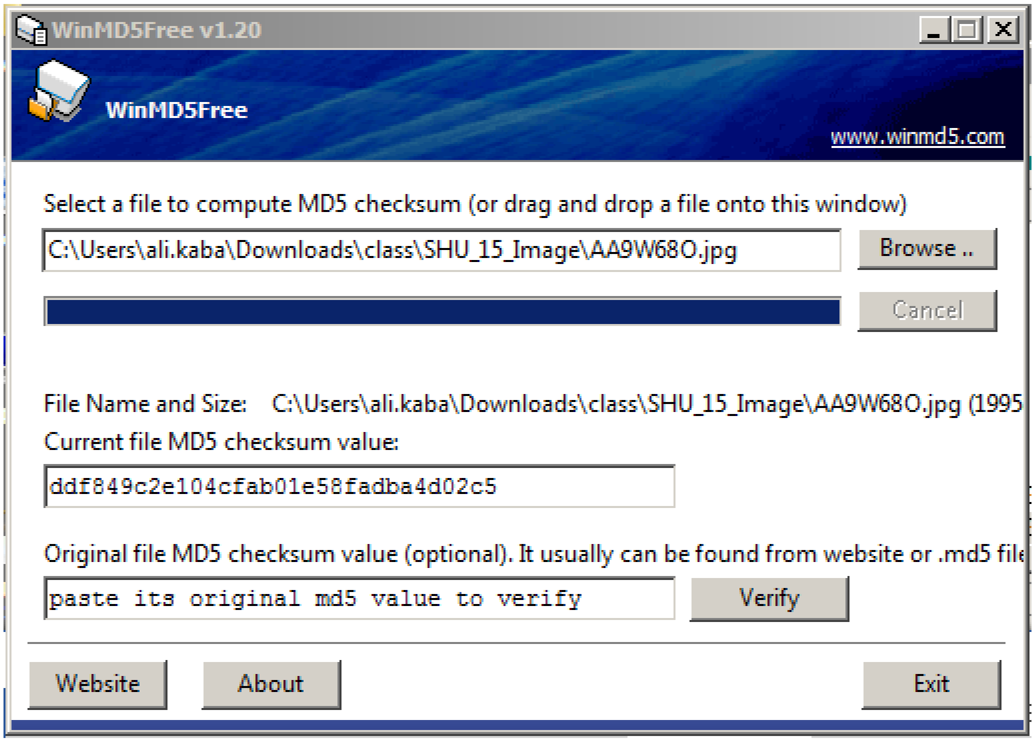
I navigated into the ….1004 folder (Mr. Evil) and found four pictures:



$RMCLRRJ.jpg	8	Regular File	3/24/2015 3:11...
$RMX9FXV.jpg	20	Regular File	3/24/2015 5:01...
$RW7N7D7.jpg	8	Regular File	3/24/2015 3:11...
$RZLMER9.jpg	8	Regular File	3/24/2015 5:01...

Name	File Name	Path
$RMCLRRJ.jpg	BBivonY.jpg	C:\Users\Mr. Evil\Desktop\junk\BBivonY.jpg
$RMX9FXV.jpg	AA9W68O.jpg	C:\Users\Mr. Evil\Desktop\junk\AA9W68O.jpg
$RW7N7D7.jpg	BBivLkU.jpg	C:\Users\Mr. Evil\Desktop\junk\BBivLkU.jpg
$RZLMER9.jpg	BBi062O.jpg	C:\Users\Mr. Evil\Desktop\junk\BBi062O.jpg

File Name	Hash
BBivonY.jpg	ddf849c2e104cfab01e58fadba4d02c5
AA9W68O.jpg	60a3cb07d788b3434f8da8c0d93e8e4a
extra_picture.jpg	347519a4ab087e6940b4e07eaa30207c



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\SHU_15_Image\AA9W68O.jpg

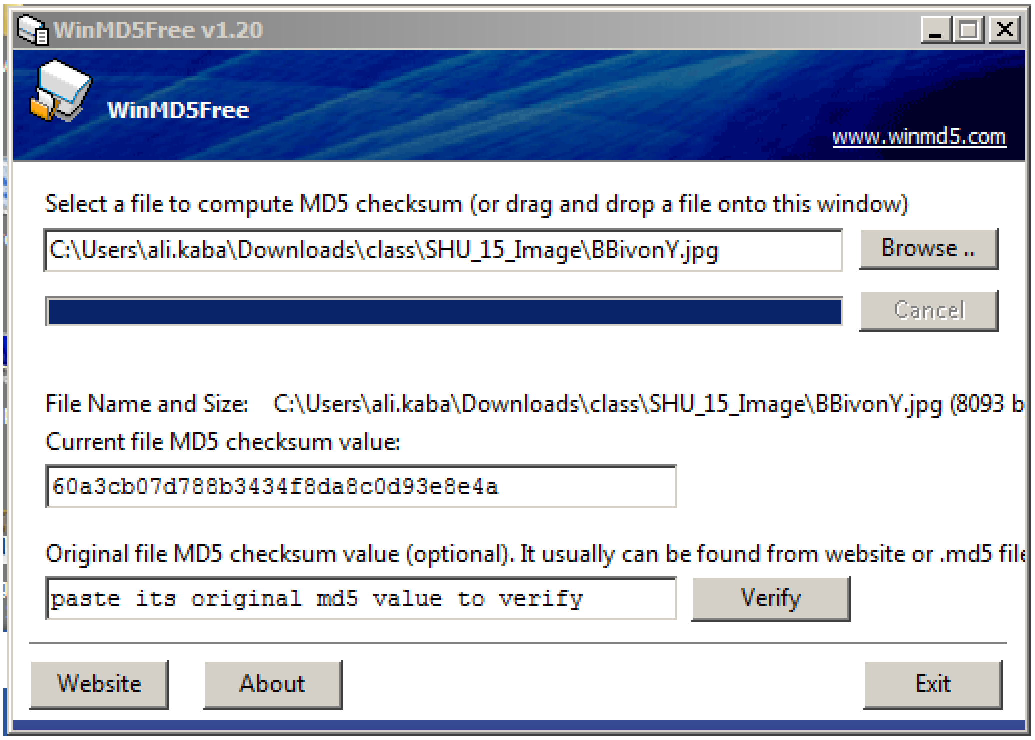
File Name and Size: C:\Users\ali.kaba\Downloads\class\SHU_15_Image\AA9W68O.jpg (1995

Current file MD5 checksum value:

```
ddf849c2e104cfab01e58fadba4d02c5
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\SHU_15_Image\BBivonY.jpg

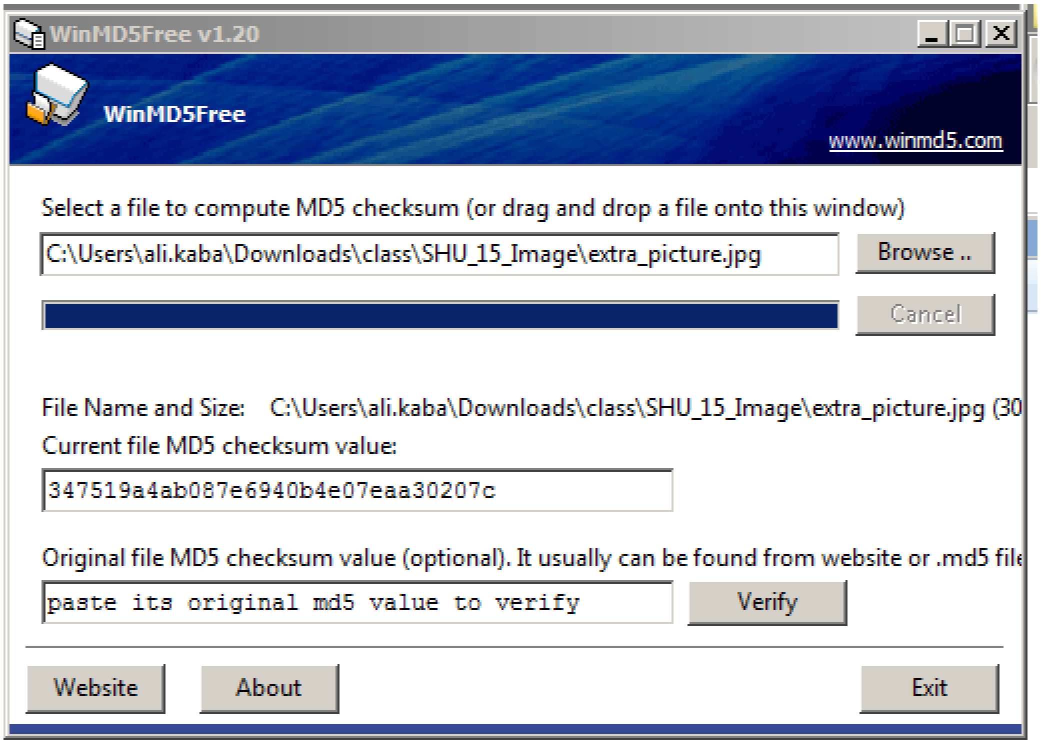
File Name and Size: C:\Users\ali.kaba\Downloads\class\SHU_15_Image\BBivonY.jpg (8093 b

Current file MD5 checksum value:

```
60a3cb07d788b3434f8da8c0d93e8e4a
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\SHU_15_Image\extra_picture.jpg

File Name and Size: C:\Users\ali.kaba\Downloads\class\SHU_15_Image\extra_picture.jpg (30

Current file MD5 checksum value:

347519a4ab087e6940b4e07eaa30207c

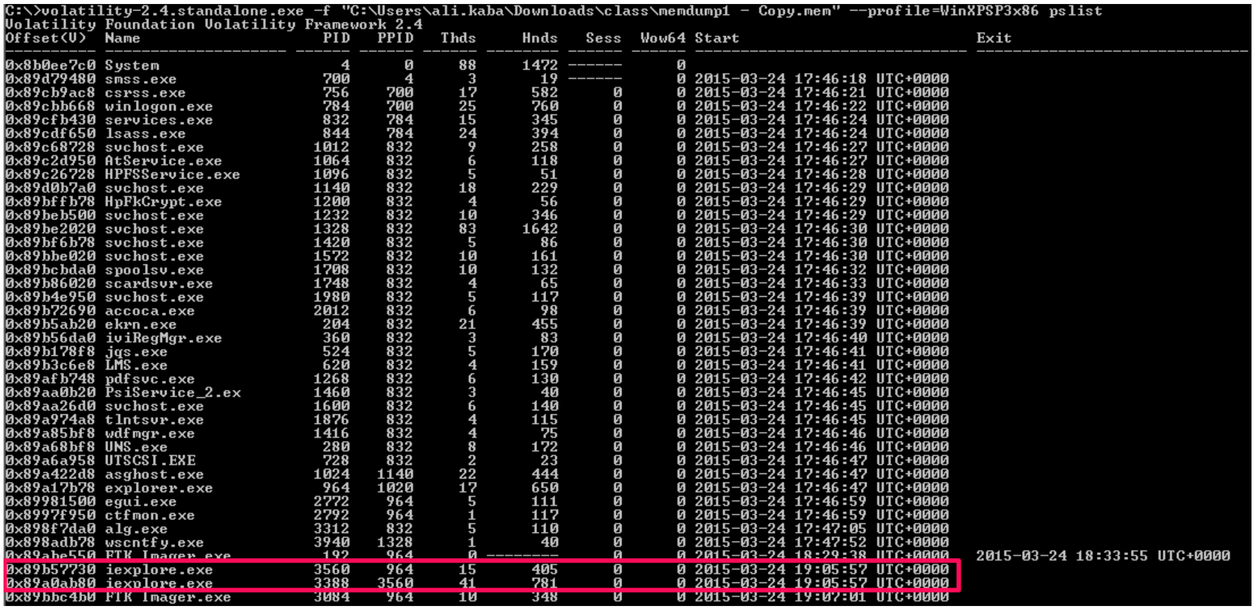
Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify

Investigating: Memory

I ran the below line to see what processes were running:

```
volatility-2.4.standalone.exe -f "C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem" --profile=WinXPSP3x86 pslist
```



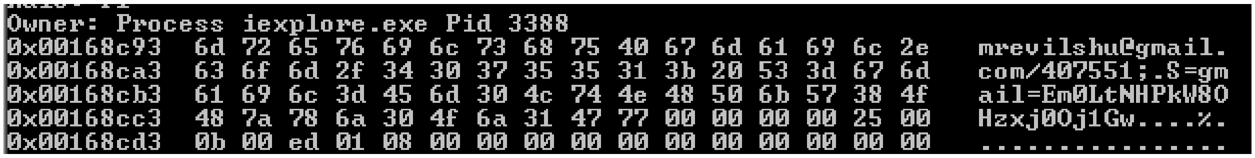
```
C:\>volatility-2.4.standalone.exe -f "C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem" --profile=WinXPSP3x86 pslist
Volatility Foundation Volatility Framework 2.4
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8b0ee7c0 System                    4      0     88     1472 ------      0
0x89d79480 smss.exe                700      4      3       19 ------      0 2015-03-24 17:46:18 UTC+0000
0x89cb9ac8 csrss.exe               756    700     17      582      0      0 2015-03-24 17:46:21 UTC+0000
0x89cbb668 winlogon.exe            784    700     25      760      0      0 2015-03-24 17:46:22 UTC+0000
0x89cfb430 services.exe            832    784     15      345      0      0 2015-03-24 17:46:24 UTC+0000
0x89cdf650 lsass.exe               844    784     24      394      0      0 2015-03-24 17:46:24 UTC+0000
0x89c68728 svchost.exe            1012    832      9      258      0      0 2015-03-24 17:46:27 UTC+0000
0x89c2d950 AtService.exe          1064    832      6      118      0      0 2015-03-24 17:46:27 UTC+0000
0x89c26728 HPFSService.exe        1096    832      5       51      0      0 2015-03-24 17:46:28 UTC+0000
0x89d0b7a0 svchost.exe            1140    832     18      229      0      0 2015-03-24 17:46:29 UTC+0000
0x89bffb78 HpFkCrypt.exe          1200    832      4       56      0      0 2015-03-24 17:46:29 UTC+0000
0x89beb500 svchost.exe            1232    832     10      346      0      0 2015-03-24 17:46:29 UTC+0000
0x89be2020 svchost.exe            1328    832     83     1642      0      0 2015-03-24 17:46:30 UTC+0000
0x89bf6b78 svchost.exe            1420    832      5       86      0      0 2015-03-24 17:46:30 UTC+0000
0x89bbe020 svchost.exe            1572    832     10      161      0      0 2015-03-24 17:46:30 UTC+0000
0x89bcbda0 spoolsv.exe            1708    832     10      132      0      0 2015-03-24 17:46:32 UTC+0000
0x89b86020 scardsvr.exe           1748    832      4       65      0      0 2015-03-24 17:46:33 UTC+0000
0x89b4e950 svchost.exe            1980    832      5      117      0      0 2015-03-24 17:46:39 UTC+0000
0x89b72690 accoca.exe             2012    832      6       98      0      0 2015-03-24 17:46:39 UTC+0000
0x89b5ab20 ekrn.exe                204    832     21      455      0      0 2015-03-24 17:46:39 UTC+0000
0x89b56da0 iviRegMgr.exe           360    832      3       83      0      0 2015-03-24 17:46:40 UTC+0000
0x89b178f8 jqs.exe                 524    832      5      170      0      0 2015-03-24 17:46:41 UTC+0000
0x89b3c6e8 LMS.exe                 620    832      4      159      0      0 2015-03-24 17:46:41 UTC+0000
0x89afb748 pdfsvc.exe             1268    832      6      130      0      0 2015-03-24 17:46:42 UTC+0000
0x89aa0b20 PsiService_2.ex        1460    832      3       40      0      0 2015-03-24 17:46:45 UTC+0000
0x89aa26d0 svchost.exe            1600    832      6      140      0      0 2015-03-24 17:46:45 UTC+0000
0x89a974a8 tlntsvr.exe            1876    832      4      115      0      0 2015-03-24 17:46:45 UTC+0000
0x89a85bf8 wdfmgr.exe             1416    832      4       75      0      0 2015-03-24 17:46:46 UTC+0000
0x89a68bf8 UNS.exe                 280    832      8      172      0      0 2015-03-24 17:46:46 UTC+0000
0x89a6a958 UTSCSI.EXE              728    832      2       23      0      0 2015-03-24 17:46:47 UTC+0000
0x89a422d8 asghost.exe            1024   1140     22      444      0      0 2015-03-24 17:46:47 UTC+0000
0x89a17b78 explorer.exe            964   1020     17      650      0      0 2015-03-24 17:46:47 UTC+0000
0x89981500 egui.exe               2772    964      5      111      0      0 2015-03-24 17:46:59 UTC+0000
0x8997f950 ctfmon.exe             2792    964      1      117      0      0 2015-03-24 17:46:59 UTC+0000
0x898f7da0 alg.exe                3312    832      5      110      0      0 2015-03-24 17:47:05 UTC+0000
0x898adb78 wscntfy.exe            3940   1328      1       40      0      0 2015-03-24 17:47:52 UTC+0000
0x89abe550 FTK Imager.exe          192    964      0 --------      0      0 2015-03-24 18:29:38 UTC+0000   2015-03-24 18:33:55 UTC+0000
0x89b57730 iexplore.exe           3560    964     15      405      0      0 2015-03-24 19:05:57 UTC+0000
0x89a0ab80 iexplore.exe           3388   3560     41      781      0      0 2015-03-24 19:05:57 UTC+0000
0x89bbc4b0 FTK Imager.exe         3084    964     10      348      0      0 2015-03-24 19:07:01 UTC+0000
```

While looking at the processes I came across two iexplorer.exe processes but we will focus on the closest to the bottom. There were no cmd.exe process running.

	PID	PPID
iexplorer.exe	3560	964
iexplorer.exe	3388	3560
cmd.exe	N/A	N/A

Now I ran the following line to find out what email address was logged:

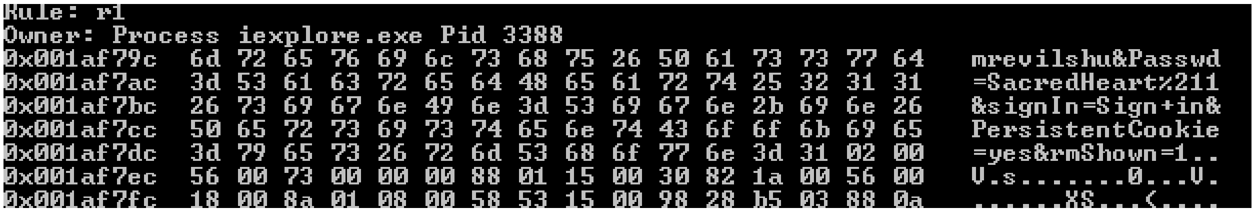
volatility-2.4.standalone.exe -f "C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem" --profile=WinXPSP3x86 yarascan –Y "@gmail" –p 3388 –R 9



```
Rule: r1
Owner: Process iexplore.exe Pid 3388
0x00168c93  6d 72 65 76 69 6c 73 68 75 40 67 6d 61 69 6c 2e   mrevilshu@gmail.
0x00168ca3  63 6f 6d 2f 34 30 37 35 35 31 3b 20 53 3d 67 6d   com/407551;.S=gm
0x00168cb3  61 69 6c 3d 45 6d 30 4c 74 4e 48 50 6b 57 38 4f   ail=Em0LtNHPkW8O
0x00168cc3  48 7a 78 6a 30 4f 6a 31 47 77 00 00 00 00 25 00   Hzxj0Oj1Gw....%.
0x00168cd3  0b 00 ed 01 08 00 00 00 00 00 00 00 00 00 00 00   ................
```

Email: mrevilshu@gmail.com

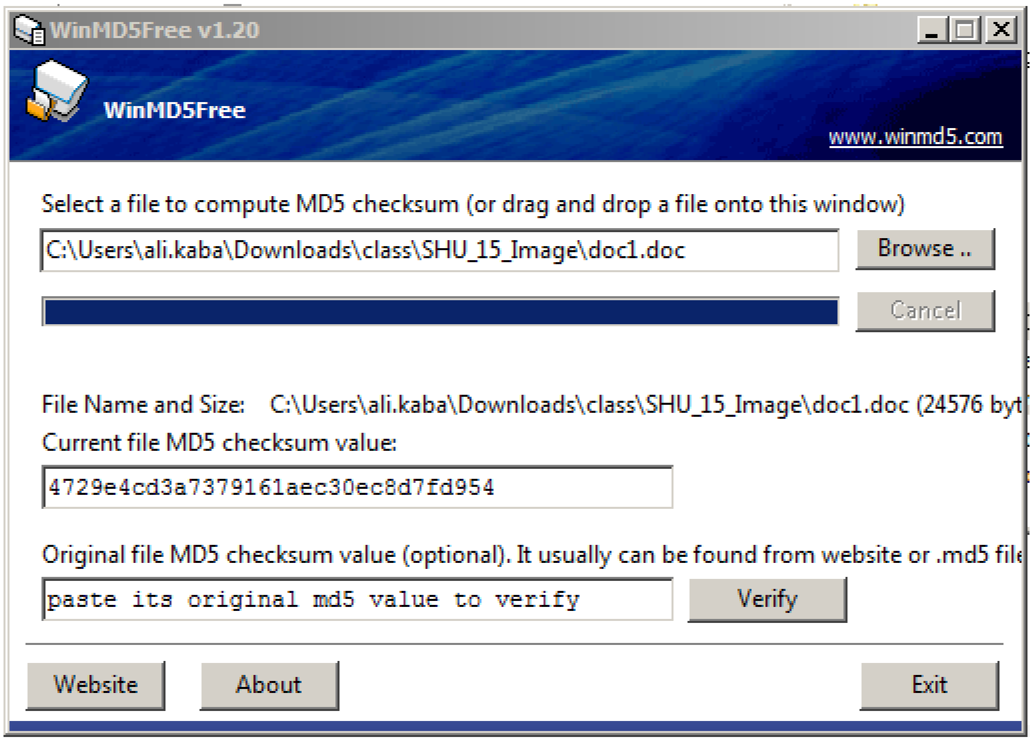
volatility-2.4.standalone.exe -f "C:\Users\ali.kaba\Downloads\class\memdump1 - Copy.mem" --profile=WinXPSP3x86 yarascan –Y "Passwd" –p 3388 –R 9



```
Rule: r1
Owner: Process iexplore.exe Pid 3388
0x001af79c  6d 72 65 76 69 6c 73 68 75 26 50 61 73 73 77 64   mrevilshu&Passwd
0x001af7ac  3d 53 61 63 72 65 64 48 65 61 72 74 25 32 31 31   =SacredHeart%211
0x001af7bc  26 73 69 67 6e 49 6e 3d 53 69 67 6e 2b 69 6e 26   &signIn=Sign+in&
0x001af7cc  50 65 72 73 69 73 74 65 6e 74 43 6f 6f 6b 69 65   PersistentCookie
0x001af7dc  3d 79 65 73 26 72 6d 53 68 6f 77 6e 3d 31 02 00   =yes&rmShown=1..
0x001af7ec  56 00 73 00 00 00 88 01 15 00 30 82 1a 00 56 00   V.s.......0...V.
0x001af7fc  18 00 8a 01 08 00 58 53 15 00 98 28 b5 03 88 0a   ......XS...(....
```

Password: SacredHeart!1

Document name is Doc1.doc and hash is: 4729e4cd3a7379161aec30ec8d7fd954



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\ali.kaba\Downloads\class\SHU_15_Image\doc1.doc

File Name and Size: C:\Users\ali.kaba\Downloads\class\SHU_15_Image\doc1.doc (24576 byt

Current file MD5 checksum value:

```
4729e4cd3a7379161aec30ec8d7fd954
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 fil

```
paste its original md5 value to verify
```

Document's content is as followed:

My bucket list

After I find a hitman to kill my wife, I have to find a location to bury the body

I have to wire the money to the hitman

Then I have to cash in the wifes life insurance and then I'll be on my trip to :)

There will be no traces of my activity!!!!!! Onions make me cry

Bank of America account number is 643435766-22421

The link file located on the desktop targets the following file: E:\ms_evil Schedule.txt

Conclusion

Based off the finding, this is a pretty cut and dry situation. We confiscated Mr. Evil's Hard Drive and capture his computer's memory.

In the hard drive, we reviewed the Windows Registry Security Accounts Managed (SAM), Software, System and NTuser.dat. The Windows Registry contains everything and all settings in regards to the windows machine it is installed in. In the SAM hive, we discovered 6 accounts and one of those accounts of Mr. Evil's. In the Software's hive, we were able to find where Mr. Evil went online in the TypeURL keys.

In that directory, Mr. Evil went to google.com and later on went to bankofamerica.com. After that he searched "tor" than "how to wire money" than "hire a hitman" than "where to bury body" than "vacation at bahamas" than "how to hide internet activity" than "the onion router" than went into gmail.com in that order of links that are relevant.

We also discovered two distinct folders on his desktop "BAD_STUFF" and "Tor Browser". The second folder showed that TOR was infact installed as well as being launched according to the windows/prefetch folder. The first folder had several pictures related to the Bahamas, hitman and TOR's ip address, a bucket list text file that showed to be deleted and other incriminating files.

The bucket list file was recovered but was password protected so we navigated into the captured memory using Volatility and found the password. After opening up the document it listed Mr. Evil's plan.

I believe evidence collected this machine shows more than enough to prosecute Mr. Evil for his evil doings.