FORENSIC EXAMINATION REPORT

CASE NUMBER 007

Examiner	Divya Palani - 20870275
Case generated	Tuesday, October 24, 2017
Report generated	Friday, October 21, 2022

CASE OVERVIEW

CASE PROCESSING DETAILS

SCAN 1

Scanned by	**Jamey Tubbs**
Scan date	**Tuesday, October 24, 2017 9:54:43 AM**

EVIDENCE OVERVIEW

Evidence items	1
Combined results	236,985

J WATERS WIN 7 PC.E01 (236,985)

Evidence number	J Waters Win 7 PC.E01
Location	J Waters Win 7 PC.E01

Anti virus

Record 1

Tags	Anti virus
Item	avast! Free Antivirus
Type	Installed Programs
Artifact category	Operating System
Date and time	10/03/14 9:08:54 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SOFTWARE
Location	• Registry Key: Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Avast
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	Anti-forensic software
Item	Dropbox Decryptor version 1.2
Type	Installed Programs
Artifact category	Operating System
Date and time	12/03/14 8:28:15 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\Reg Back\SOFTWARE
Location	• Registry Key: Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0AE53A78-0B2A-4DE3-B007-F676E588CE50}_is1
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	Anti-forensic software
Item	TrueCrypt
Type	Installed Programs
Artifact category	Operating System
Date and time	10/03/14 9:15:40 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SOFTWARE
Location	• Registry Key: Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TrueCrypt
Evidence number	• J Waters Win 7 PC.E01

Record 3

Tags	Anti-forensic software
Item	Autopsy
Type	Installed Programs
Artifact category	Operating System
Date and time	12/03/14 8:12:04 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\Reg Back\SOFTWARE
Location	• Registry Key: Microsoft\Windows\CurrentVersion\Uninstall\{69e9f31a-5020-438f-b824-f44aa6b6c91a}
Evidence number	• J Waters Win 7 PC.E01

Record 4

Tags	Anti-forensic software
Item	Autopsy
Type	Installed Programs
Artifact category	Operating System
Date and time	12/03/14 8:12:04 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SOFTWARE
Location	• Registry Key: Microsoft\Windows\CurrentVersion\Uninstall\{69e9f31a-5020-438f-b824-f44aa6b6c91a}
Evidence number	• J Waters Win 7 PC.E01

Record 5

Tags	Anti-forensic software
Item	TrueCrypt
Type	Installed Programs
Artifact category	Operating System
Date and time	10/03/14 9:15:40 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\Reg Back\SOFTWARE
Location	• Registry Key: Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TrueCrypt
Evidence number	• J Waters Win 7 PC.E01

Record 6

Tags	Anti-forensic software
Item	Dropbox Decryptor version 1.2
Type	Installed Programs

Artifact category	Operating System
Date and time	12/03/14 8:28:15 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SOFTWARE
Location	• Registry Key: Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0AE53A78-0B2A-4DE3-B007-F676E588CE50}_is1
Evidence number	• J Waters Win 7 PC.E01

Boot softwares

Record 1

Tags	Boot softwares
Item	NTOSBOOT
Type	Windows Prefetch Files
Artifact category	Operating System
Date and time	23/07/13 12:54:46 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB) (Unallocated Clusters)
Location	• Physical Sector 475199000
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	Boot softwares
Item	NTOSBOOT
Type	Windows Prefetch Files
Artifact category	Operating System
Date and time	14/04/14 7:33:55 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\pagefile.sys
Location	• File Offset 5393764352
Evidence number	• J Waters Win 7 PC.E01

Record 3

Tags	Boot softwares
Item	NTOSBOOT
Type	Windows Prefetch Files
Artifact category	Operating System
Date and time	10/03/14 8:10:44 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\Prefetch\NTOSBOOT-B 00DFAAD.pf
Location	• File Offset 0
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	Downloaded files
Item	https://www.dmt-nexus.me/Files/Books/General/Cannabis%20Grow%20Bible.pdf
Type	Chrome Downloads
Artifact category	Web Related
Date and time	12/03/14 8:18:03 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: downloads(id: 22) • Table: downloads_url_chains(rowid: 33)
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	Downloaded files
Item	http://downloads.sourceforge.net/project/autopsy/autopsy/3.0.9/autopsy-3.0.9-64bit.msi?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fautopsy%2Ffiles%2Fautopsy%2F3.0.9%2F&ts=1394643501&use_mirror=hivelocity
Type	Chrome Downloads
Artifact category	Web Related
Date and time	12/03/14 7:58:23 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: downloads(id: 20) • Table: downloads_url_chains(rowid: 30)
Evidence number	• J Waters Win 7 PC.E01

Record 3

Tags	Downloaded files
Item	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCUQFjAA&url=https%3A%2F%2Fwww.dmt-nexus.me%2FFiles%2FBooks%2FGeneral%2FCannabis%2520Grow%2520Bible.pdf&ei=qpYgU5niBNTOkQf8xoCIBA&usg=AFQjCNEgLROJN1tHDpDk_Sj33fQE6Yn24g
Type	Chrome Downloads
Artifact category	Web Related
Date and time	12/03/14 8:17:44 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: downloads(id: 21) • Table: downloads_url_chains(rowid: 32)
Evidence number	• J Waters Win 7 PC.E01

Record 4

Tags	Downloaded files
Item	http://files5.freedownloads.us.com/dl?bc=969089
Type	Chrome Downloads
Artifact category	Web Related
Date and time	11/03/14 11:24:09 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: downloads(id: 16) • Table: downloads_url_chains(rowid: 23)
Evidence number	• J Waters Win 7 PC.E01

Record 5

Tags	Downloaded files
Item	http://downloads.sourceforge.net/project/sqlitebrowser/sqlitebrowser/2.0%20beta1/sqlitebrowser_200_b1_win.zip?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fsqlitebrowser%2F&ts=1394643064&use_mirror=softlayer-ams
Type	Chrome Downloads
Artifact category	Web Related
Date and time	12/03/14 7:51:07 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History

Location	• Table: downloads(id: 18) • Table: downloads_url_chains(rowid: 26)
Evidence number	• J Waters Win 7 PC.E01

Record 6

Tags	Downloaded files
Item	http://www.handshake.de/user/chmaas/delphi/download/xvi32.zip
Type	Chrome Downloads
Artifact category	Web Related
Date and time	12/03/14 7:39:23 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: downloads(id: 17) • Table: downloads_url_chains(rowid: 25)
Evidence number	• J Waters Win 7 PC.E01

Record 7

Tags	Downloaded files
Item	http://downloads.sourceforge.net/project/autopsy/autopsy/3.0.9/autopsy-3.0.9-64bit.msi.asc ?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fautopsy%2Ffiles%2Fautopsy%2F3.0.9%2F&ts=1394643380&use_mirror=tcpdiag
Type	Chrome Downloads
Artifact category	Web Related
Date and time	12/03/14 7:56:23 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: downloads(id: 19) • Table: downloads_url_chains(rowid: 28)
Evidence number	• J Waters Win 7 PC.E01

Encrption

Record 1

Tags	Encrption
Item	compexperts_bench
Type	Network Profiles
Artifact category	Operating System
Date and time	2014-03-06 14:31:51
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SOFTWARE • J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\{3589C9DA-C0C2-4659-B0E8-5C0D4F4D43ED}\{EAB18FCF-CBE1-4513-B98A-299DBFC20B65}.xml
Location	• Registry Key: Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{A7480119-B06D-4EC6-ABE0-E7FB16FD6EF3} • Registry Key: Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080000000F0000F04E964B991CD3503FACCFDC89991DAC858839D473FF241757616EA1B3201A3728 • n/a
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	Microsoft license
Item	LICENSE.txt
Type	Text Documents
Artifact category	Documents
Date and time	20/09/13 9:12:52 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Program Files (x86)\OpenOffice 4\share\readme\LICENSE.txt
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Product key

Record 1

Tags	Product key
Item	Windows 7 Professional
Type	Operating System Information
Artifact category	Operating System
Date and time	10/03/14 8:03:47 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SOFTWARE • J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\SYSTEM
Location	• Registry Key: Microsoft\Windows NT\CurrentVersion • Registry Key: ControlSet001\Control\Windows • Registry Key: ControlSet001\services\Tcpip\Parameters • Registry Key: ControlSet001\Control\ComputerName\ComputerName • Registry Key: ControlSet001\Control\FileSystem
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	Product key
Item	Windows 7 Professional
Type	Operating System Information
Artifact category	Operating System
Date and time	10/03/14 8:03:47 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\RegBack\SOFTWARE • J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Windows\System32\config\RegBack\SYSTEM
Location	• Registry Key: Microsoft\Windows NT\CurrentVersion • Registry Key: ControlSet001\Control\Windows • Registry Key: ControlSet001\services\Tcpip\Parameters • Registry Key: ControlSet001\Control\ComputerName\ComputerName • Registry Key: ControlSet001\Control\FileSystem
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:50:53 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Exports.lnk
Location	• File Offset 0
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:42:28 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Location	• File Offset 40960
Evidence number	• J Waters Win 7 PC.E01

Record 3

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports\Internet.pdf
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:51:12 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62085416
Evidence number	• J Waters Win 7 PC.E01

Record 4

Tags	Removable drive
Item	F:\2014-001-RAM.dmp
Type	LNK Files
Artifact category	Operating System
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62057904
Evidence number	• J Waters Win 7 PC.E01

Record 5

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:42:28 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62056904
Evidence number	• J Waters Win 7 PC.E01

Record 6

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports\2014-001 - 2014-03-18_07-59-39\index.html
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 3:00:28 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\index.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 7

Tags	Removable drive
Item	F:\Bauer Hash\Bauer Hash.txt
Type	LNK Files
Artifact category	Operating System
Date and time	17/03/14 8:49:05 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b9cdc69c1c24e2b.automaticDestinations-ms
Location	• File Offset 4992
Evidence number	• J Waters Win 7 PC.E01

Record 8

Tags	Removable drive
Item	D:\UFED_Logical_Analyzer_3.8.6.zip
Type	LNK Files
Artifact category	Operating System
Date and time	28/10/13 1:08:55 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB) (Unallocated Clusters)
Location	• Physical Sector 258748574
Evidence number	• J Waters Win 7 PC.E01

Record 9

Tags	Removable drive
Item	F:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 7:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Location	• File Offset 37824
Evidence number	• J Waters Win 7 PC.E01

Record 10

Tags	Removable drive
Item	G:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 7:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Location	• File Offset 6272
Evidence number	• J Waters Win 7 PC.E01

Record 11

Tags	Removable drive
Item	F:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 7:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62077352
Evidence number	• J Waters Win 7 PC.E01

Record 12

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports\Internet.pdf
Type	LNK Files
Artifact category	Operating System

Removable drive

Date and time	18/03/14 2:51:12 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\ff103e2cc310d0d.automaticDestinations-ms
Location	• File Offset 2048
Evidence number	• J Waters Win 7 PC.E01

Record 13

Tags	Removable drive
Item	G:\License Keys for IEF Class.docx
Type	LNK Files
Artifact category	Operating System
Date and time	13/03/14 10:22:18 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\License Keys for IEF Class.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 14

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:42:28 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\2014-001 - Mar 18 2014 074228.lnk
Location	• File Offset 0
Evidence number	• J Waters Win 7 PC.E01

Record 15

Tags	Removable drive
Item	F:\Bauer Hash
Type	LNK Files
Artifact category	Operating System
Date and time	17/03/14 7:24:51 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Location	• File Offset 44736
Evidence number	• J Waters Win 7 PC.E01

Record 16

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:50:53 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62073120
Evidence number	• J Waters Win 7 PC.E01

Record 17

Tags	Removable drive
Item	G:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 7:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 64373168
Evidence number	• J Waters Win 7 PC.E01

Record 18

Tags	Removable drive
Item	E:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 4:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB) (Unallocated Clusters)
Location	• Physical Sector 258610790
Evidence number	• J Waters Win 7 PC.E01

Record 19

Tags	Removable drive
Item	F:\
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 4:06:09 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData \Roaming\Microsoft\Windows\Recent\IEF Frontline (F).lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 20

Tags	Removable drive
Item	G:\License Keys for IEF Class.docx
Type	LNK Files
Artifact category	Operating System
Date and time	10/03/14 9:48:20 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 64379328
Evidence number	• J Waters Win 7 PC.E01

Record 21

Tags	Removable drive
Item	F:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 7:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData \Roaming\Microsoft\Windows\Recent\USB DISK (F).lnk
Location	• File Offset 0
Evidence number	• J Waters Win 7 PC.E01

Record 22

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports\Internet.pdf
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 3:02:06 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData \Roaming\Microsoft\Windows\Recent\Internet.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 23

Tags	Removable drive
Item	F:\2 Guns (2013) DVDRip XviD-MAXSPEED www.torentz.3xforum.ro.mp4
Type	LNK Files
Artifact category	Operating System
Date and time	14/03/14 7:06:27 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData \Roaming\Microsoft\Windows\Recent\2 Guns (2013) DVDRip XviD-MAXSPEED www.torentz.3xforum.ro.lnk
Location	• n/a

Evidence number	• J Waters Win 7 PC.E01

Record 24

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports\2014-001 - 2014-03-18_07-59-39\index.html
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 3:00:03 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5d696d521de238c3.automaticDestinations-ms
Location	• File Offset 7040
Evidence number	• J Waters Win 7 PC.E01

Record 25

Tags	Removable drive
Item	F:\2 Guns (2013) DVDRip XviD-MAXSPEED www.torentz.3xforum.ro.mp4
Type	LNK Files
Artifact category	Operating System
Date and time	02/12/13 7:14:27 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62054912
Evidence number	• J Waters Win 7 PC.E01

Record 26

Tags	Removable drive
Item	F:\Case2012-123.001.txt
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 5:25:59 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\$MFT
Location	• File Offset 62065072
Evidence number	• J Waters Win 7 PC.E01

Record 27

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Case Information.txt
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:52:43 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Case Information.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 28

Tags	Removable drive
Item	18/03/14 2:50:53 PM
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:50:53 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Location	• File Offset 42624
Evidence number	• J Waters Win 7 PC.E01

Record 29

Tags	Removable drive
Item	G:\
Type	LNK Files
Artifact category	Operating System

Date and time	13/03/14 10:22:19 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\IEF Frontline (G).lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 30

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Exports\2014-001 - 2014-03-18_07-59-39
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 3:00:28 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\2014-001 - 2014-03-18_07-59-39.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 31

Tags	Removable drive
Item	F:\Case2012-123.001.txt
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 5:25:59 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Case2012-123.001.lnk
Location	• File Offset 0
Evidence number	• J Waters Win 7 PC.E01

Record 32

Tags	Removable drive
Item	G:\
Type	LNK Files
Artifact category	Operating System
Date and time	01/01/80 7:00:00 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Location	• File Offset 6272
Evidence number	• J Waters Win 7 PC.E01

Record 33

Tags	Removable drive
Item	F:\2014-001 - Mar 18 2014 074228\Case Information.txt
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 2:42:30 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b9cdc69c1c24e2b.automaticDestinations-ms
Location	• File Offset 3072
Evidence number	• J Waters Win 7 PC.E01

Record 34

Tags	Removable drive
Item	F:\2014-001-RAM.dmp
Type	LNK Files
Artifact category	Operating System
Date and time	18/03/14 4:06:09 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\2014-001-RAM.dmp.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Removable drive

Record 35

Tags	Removable drive
Item	D:\UFED_Physical_Analyzer_3.9.zip
Type	LNK Files
Artifact category	Operating System
Date and time	23/12/13 7:33:32 AM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB) (Unallocated Clusters)
Location	• Physical Sector 258611824
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	Roofie initiating chat
Item	#jackwaters2124/$roofiesanchez;5a94409f5a4ff8e6
Type	Skype Chat Messages
Artifact category	Chat
Date and time	13/03/14 4:37:07 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData \Roaming\Skype\jackwaters2124\main.db-journal
Location	• File Offset 90599
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	Roofie initiating chat
Item	#jackwaters2124/$roofiesanchez;aae459075cd489b
Type	Skype Chat Messages
Artifact category	Chat
Date and time	14/04/14 4:51:25 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Administrator\AppData \Roaming\Skype\jackwaters2124\main.db
Location	• Table: messages(rowid: 450) • Table: participants(rowid: 427) • Table: participants(rowid: 428)
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	User manual
Item	C:\Program Files (x86)\Internet Evidence Finder v6\Documentation\IEFv6UserManual.htm
Type	LNK Files
Artifact category	Operating System
Date and time	10/03/14 9:21:25 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\ProgramData\Microsoft\Windows\Start Menu\Programs\Internet Evidence Finder v6\Internet Evidence Finder v6.3 User Manual.lnk
Location	• n/a
Evidence number	• J Waters Win 7 PC.E01

Record 1

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 4:09:23 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Cache\data_2
Location	• File Offset 426015
Evidence number	• J Waters Win 7 PC.E01

Record 2

Tags	User searching for browser
Item	tor browser
Type	Google Searches
Artifact category	Refined Results
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Favicons
Location	• Table: favicons(id: 3) • Table: icon_mapping(id: 47) • Table: favicon_bitmaps(id: 3)
Evidence number	• J Waters Win 7 PC.E01

Record 3

Tags	User searching for browser
Item	tor browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 8:18:46 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: urls(id: 128)
Evidence number	• J Waters Win 7 PC.E01

Record 4

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:24 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: visits(id: 80) • Table: urls(id: 78)
Evidence number	• J Waters Win 7 PC.E01

Record 5

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: keyword_search_terms(rowid: 1) • Table: urls(id: 77)
Evidence number	• J Waters Win 7 PC.E01

Record 6

Tags	User searching for browser
Item	tor browser
Type	Google Searches
Artifact category	Refined Results

Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: keyword_search_terms(rowid: 8) • Table: urls(id: 128)
Evidence number	• J Waters Win 7 PC.E01

Record 7

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:21 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: urls(id: 77)
Evidence number	• J Waters Win 7 PC.E01

Record 8

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:24 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: urls(id: 78)
Evidence number	• J Waters Win 7 PC.E01

Record 9

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Favicons
Location	• Table: favicons(id: 3) • Table: icon_mapping(id: 6) • Table: favicon_bitmaps(id: 3)
Evidence number	• J Waters Win 7 PC.E01

Record 10

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:21 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: visits(id: 79) • Table: urls(id: 77)
Evidence number	• J Waters Win 7 PC.E01

Record 11

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:21 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Cache\data_1 • J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Cache\data_2

Location	• File Offset 62976 • File Offset 401408
Evidence number	• J Waters Win 7 PC.E01

Record 12

Tags	User searching for browser
Item	tor browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 8:18:46 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\History
Location	• Table: visits(id: 157) • Table: urls(id: 128)
Evidence number	• J Waters Win 7 PC.E01

Record 13

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:24 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Cache\data_1
Location	• File Offset 63488 • File Offset 65536
Evidence number	• J Waters Win 7 PC.E01

Record 14

Tags	User searching for browser
Item	safari browser
Type	Google Searches
Artifact category	Refined Results
Date and time	10/03/14 7:09:21 PM
Source	• J Waters Win 7 PC.E01 - Entire Disk (Microsoft NTFS, 243.8 GB)\Users\Default\AppData\Local \Google\Chrome\User Data\Default\Cache\data_1
Location	• File Offset 61440 • File Offset 62464
Evidence number	• J Waters Win 7 PC.E01