

REPORT.20120112104700074/DEMO CHILD EXPLOITATION

TRIAGE REPORT

TAGS SUMMARY

Tag	Tag Name	Number of Entries Tagged	Percentage of Total Entries Tagged
	Clear Tag	(14)	16.66%
1	1 - Exploitation Pictures	(5)	5.95%
2	2 - Incriminating Searches	(7)	8.33%
3	3 - Supporting Evidence	(22)	26.190%
4	4 - Anti-Forensics	(16)	19.04%
5	5 - User Info	(6)	7.14%
6	6 - Tag 6		
7	7 - Tag 7		
8	8 - Tag 8		
9	9 - Scan Set Up Notes	(14)	16.66%
10	10 - 10 - Tag 10		

*Summary of all items tagged by the officer.
Tags are user-definable.*

REPORT INFORMATION

Information collected at the beginning of the scan

Report Information

Tag	Report Info	Value
9 - Scan Set Up Notes	Date/Time	2012-01-12T10:45:41
9 - Scan Set Up Notes	System Date/Time	2012-01-12T10:47:00
9 - Scan Set Up Notes	Precise Time Zone	Europe/London;United Kingdom Time;GMT+00:00

Some brief notes about the scan, more details are available but these have been selected by the officer as relevant, showing the SearchPak and CapturePaks used.

SEARCH PROFILE

Scan settings details

Selected SearchPaks

Tag	Name
9 - Scan Set Up Notes	ADF Solutions Inc-Anti-Forensics - Keyword Search - Encryption Tools
9 - Scan Set Up Notes	ADF Solutions Inc-Anti-Forensics - Keyword Search - Wipers and other tools
9 - Scan Set Up Notes	ADF Solutions Inc-IPOC Keyword Search - File Content under1mb size - PART 1
9 - Scan Set Up Notes	ADF Solutions Inc-IPOC Keyword Search - Filename Only - PART 2
9 - Scan Set Up Notes	ADF Solutions Inc-IPOC Visual Search
9 - Scan Set Up Notes	ADF Solutions Inc-Windows Artefacts - Link Files

Selected CapturePaks

Tag	Name
9 - Scan Set Up Notes	Installed Applications
9 - Scan Set Up Notes	Internet Browsing History
9 - Scan Set Up Notes	Internet Search History
9 - Scan Set Up Notes	USB Device History
9 - Scan Set Up Notes	User Profiling

INSTALLED APPLICATIONS

This CapturePak collects the list of installed applications on a Windows or Linux target system.

Installed Application List

Tag	Name	Publisher	Installation Location	Installation Date	Registry Path
4 - Anti-	CCleaner	Piriform	C:\Program	2012-01-	Drive1/Partition0/Windows/System32/config/SOFTWARE

A full list of installed applications has been captured by the scan but these have been tagged by the officer as they are Anti-Forensics.

Forensics			Files\CCleaner	10T16:02:41+00:00	
4 - Anti-Forensics	TrueCrypt	TrueCrypt Foundation		2012-01-10T16:22:53+00:00	Drive1/Partition0/Windows/System32/config/SOFTWARE
4 - Anti-Forensics	Eraser 6.0.9.2343	The Eraser Project		2012-01-10T16:21:08+00:00	Drive1/Partition0/Windows/System32/config/SOFTWARE

INTERNET BROWSING HISTORY

This CapturePak collects the list of all the cached URLs from Web browsers installed on Windows target system. Supported Web browsers are MS Explorer, Mozilla/Firefox, and Google Chrome.

A small number of relevant items have been tagged, some registry entries and some history of the suspect accessing illegal pictures.

URL List

Tag	URL	User Name	Date of the Visit	Source Location
3 - Supporting Evidence	C:\Users\Dick Hensian\Pictures\preteen girls	Dick Hensian		Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	C:\Users\Dick Hensian\Pictures\Underage boys	Dick Hensian		Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Pictures/preteen%20girls/preteen2AE6Bd01.jpg	Dick Hensian	2012-01-12T10:27:10+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat
3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Pictures/Underage%20boys/lsmag4DA6Ad01.jpg	Dick Hensian	2012-01-12T10:26:45+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat
3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Pictures/Underage%20boys/lsmag04D76d01.jpg	Dick Hensian	2012-01-12T10:26:41+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat
3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Pictures/Underage%20boys/lsmag8A1BCd01.jpg	Dick Hensian	2012-01-12T10:26:50+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat
3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Pictures/preteen%20girls/lsmodel224B8d01.jpg	Dick Hensian	2012-01-12T10:27:05+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat

3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Pictures/preteen%20girls/preteen3C239d01.jpg	Dick Hensian	2012-01-12T10:27:15+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat
3 - Supporting Evidence	:2012011220120113: Dick Hensian@file:///C:/Users/Dick%20Hensian/Documents/Incest%20Stories.rtf	Dick Hensian	2012-01-12T10:28:38+00:00	Drive1/Partition0/Users/Dick Hensian/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012011220120113/index.dat

INTERNET SEARCH HISTORY

This CapturePak collects the search terms typed in Web browsers on Windows target systems. Supported Web browsers are MS Explorer, Mozilla/Firefox, and Google Chrome. The supported search engines are Google, Yahoo!, MSN/Bing, Facebook, Twitter, and MySpace.

Internet search terms used in Firefox tagged as Anti-Forensics and Incriminating Searches.

Search history content

Tag	Search Query	User Name	Date of the Search	Search Engine	Web Browser	Source Location
4 - Anti-Forensics	anonymous surfing	Dick Hensian	2012-01-12T10:31:18+00:00	Google	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-Forensics	ccleaner	Dick Hensian	2012-01-10T16:01:28+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-Forensics	encyption tools	Dick Hensian	2012-01-10T16:21:52+00:00	Google	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-Forensics	file deletion software	Dick Hensian	2012-01-10T15:54:44+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	free legal child model sites	Dick Hensian	2012-01-12T10:32:54+00:00	Google	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	free lsmodels sites	Dick Hensian	2012-01-12T10:32:35+00:00	Google	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-Forensics	free privacy cleaner software	Dick Hensian	2012-01-10T16:01:16+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-Forensics	hide your IP address	Dick Hensian	2012-01-10T15:55:36+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-	how to surf	Dick	2012-01-	Bing	Mozilla	Drive1/Partition0/Users/Dick

Forensics	anonymously	Hensian	10T15:55:16+00:00		Firefox	Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
4 - Anti-Forensics	how to wipe your internet history	Dick Hensian	2012-01-10T15:52:34+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	incest stories	Dick Hensian	2012-01-10T16:18:00+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	lolita pics	Dick Hensian	2012-01-10T16:18:52+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	lolita porn	Dick Hensian	2012-01-12T10:30:17+00:00	Google	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	preteen kids	Dick Hensian	2012-01-10T16:17:36+00:00	Bing	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite
2 - Incriminating Searches	preteen porn	Dick Hensian	2012-01-12T10:30:08+00:00	Google	Mozilla Firefox	Drive1/Partition0/Users/Dick Hensian/AppData/Roaming/Mozilla/Firefox/Profiles/7k5uv9p.default/places.sqlite

USB DEVICE HISTORY

This CapturePak collects the history of all the USB devices plugged into the target computer.

All USB devices that have been connected to the computer are listed – useful during a scene search.

USB Device List

Device Name	Serial Number	Last Mount	GUID	Volume Label	Registry Path
Kingston DT R500 USB Device	001A92053F1CBB31F1020078	2012-01-10T16:23:27+00:00	{4d36e967-e325-11ce-bfc1-08002be10318}	MY_USB	Drive1/Partition0/Windows/System32/config/SYSTEM
Hitachi HTS545050 B9A300 USB Device	100919B40017		{4d36e967-e325-11ce-bfc1-08002be10318}	BACKUP	Drive1/Partition0/Windows/System32/config/SYSTEM

CBM Flash Disk USB Device	2811050097F2FC05		{4d36e967-e325-11ce-bfc1-08002be10318}	PHOTOS (E:)	Drive1/Partition0/Windows/System32/config/SYSTEM
usb2.0 flashdisk USB Device	CCCB1009101852250139746803	2012-01-10T17:25:17+00:00	{4d36e967-e325-11ce-bfc1-08002be10318}	E:\	Drive1/Partition0/Windows/System32/config/SYSTEM

USER PROFILING

This CapturePak collects general the information about users detected on a Windows target system.

User account details showing how often and when last logged on.

User Accounts

Tag	User Name	Is Password Protected	Password Hash(LM/NTLM)	Home Directory Path	Last login Date	Number of logons	Source Location
5 - User Info	Administrator	Yes	78CF502EFEC65B390C4AEE1D6B09EAB2		2009-04-11T13:37:28+00:00	13	Drive1/Partition0/Windows/System32/config/SAM
5 - User Info	Dick Hensian	No		/Users/Dick Hensian	2012-01-12T10:22:12+00:00	9	Drive1/Partition0/Windows/System32/config/SAM
5 - User Info	Guest	No				0	Drive1/Partition0/Windows/System32/config/SAM
5 - User Info	Harry Hoodunnett	No		/Users/Harry Hoodunnett	2012-01-10T16:26:28+00:00	1	Drive1/Partition0/Windows/System32/config/SAM
5 - User Info	Tom Attoe	No		/Users/Tom Attoe	2012-01-10T16:23:25+00:00	1	Drive1/Partition0/Windows/System32/config/SAM
5 - User Info	User Herra	No				0	Drive1/Partition0/Windows/System32/config/SAM

Recently Accessed Documents

Tag	User Name	Document Name	Document Extension	Source Location
3 - Supporting Evidence	Dick Hensian	lsmag04D76d01	jpg	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	Dick Hensian	lsmag4DA6Ad01	jpg	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	Dick Hensian	lsmag8A1BCd01	jpg	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	Dick Hensian	lsmodel224B8d01	jpg	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	Dick Hensian	preteen2AE6Bd01	jpg	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	Dick Hensian	preteen3C239d01	jpg	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
3 - Supporting Evidence	Dick Hensian	Incest Stories	rtf	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT

Indicative file names tagged in Registry MRU for recent documents and Anti-Forensics applications being used.

Most Used Applications

Tag	User Name	Application Name	Access Date	Source Location
4 - Anti-Forensics	Dick Hensian	C:\Program Files\CCleaner\CCleaner.exe	2012-01-12T10:29:36+00:00	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT
4 - Anti-Forensics	Dick Hensian	C:\Program Files\TrueCrypt\TrueCrypt.exe	2012-01-12T10:29:47+00:00	Drive1/Partition0/Users/Dick Hensian/NTUSER.DAT

SEARCHPAKS MATCHES

This report contains a detailed log of all the files that matched with the deployed SearchPaks

Matches

The files below are tagged hits from the different SearchPaks. Note the Drive No. showing two drives, in this case a USB drive was attached to the computer and scanned at the same time. The drive details are identified at the end of the report.

Tag	Text Match	File Name	Ext	Drive No.	Creation Date	Path	SearchPak Name	Logical Size
4 - Anti-Forensics	TRUECRYPT EXE 33CC2C25	TRUECRYPT.EXE-33CC2C25	pf	1	2012-01-12T10:29:57	/Windows/Prefetch	Anti-Forensics - Keyword Search - Encryption Tools	19496

4 - Anti-Forensics	CCLEANER EXE CC440C DB	CCLEANER.EXE-CC440CDB	pf	1	2012-01-10T16:02:54	/Windows/Prefetch	Anti-Forensics - Keyword Search - Wipers and other tools	29200
1 - Exploitation Pictures	preteen girls Ismodel156D8d01.jpg	Ismodel156D8d01	jpg	2	2012-01-12T10:36:25	/preteen girls	IPOC Keyword Search - File Content under1mb size - PART 1	3483
1 - Exploitation Pictures	Users Dick Hensian Pictures For Sorting underage 262d01.jpg	76 underage 262d01	jpg	1	2011-09-12T18:58:25	/Users/Dick Hensian/Pictures/For Sorting	IPOC Keyword Search - File Content under1mb size - PART 1	24551
1 - Exploitation Pictures	preteen girls preteen0D8D3d01.jpg	preteen0D8D3d01	jpg	2	2012-01-12T10:36:25	/preteen girls	IPOC Keyword Search - Filename Only - PART 2	4848
1 - Exploitation Pictures	Users Dick Hensian Pictures For Sorting underage 262d01.jpg	76 underage 262d01	jpg	1	2011-09-12T18:58:25	/Users/Dick Hensian/Pictures/For Sorting	IPOC Keyword Search - Filename Only - PART 2	24551
3 -		Ismodel156D8d01	jpg	2	2012-01-	/preteen girls	IPOC Visual Search	3483

Supporting Evidence					12T10:36:25			
3 - Supporting Evidence		preteen0EB1Fd01	jpg	2	2012-01-12T10:36:25	/preteen girls	IPOC Visual Search	4558
3 - Supporting Evidence		preteen girls	lnk	1	2012-01-12T10:27:05	/Users/Dick Hensian/AppData/Roaming/Microsoft/Windows/Recent	Windows Artefacts - Link Files	491
3 - Supporting Evidence		Incest Stories	lnk	1	2012-01-12T10:28:38	/Users/Dick Hensian/AppData/Roaming/Microsoft/Windows/Recent	Windows Artefacts - Link Files	587

In the table above original files can be included as links in the report and where appropriate thumbnails of pictures can be included.

SEARCHPAKS SCAN SUMMARY

This report summarizes the number of matches found on the suspect computer during the SearchPaks scan

Scan Duration

Amount of time the scan ran for

Duration	Scan Completed
0h 21m 11s	Yes

Summary showing details of devices scanned and hits per SearchPak

Files Scanned per Drive

Total number of files scanned per partitions

Drive Make	Drive Model	Drive Serial Number	Drive Number	Partition Number	Allocated Files Scanned	Files from Containers Scanned	File Slacks Scanned	Deleted Files Scanned	Unreferenced Files	Mount Command
------------	-------------	---------------------	--------------	------------------	-------------------------	-------------------------------	---------------------	-----------------------	--------------------	---------------

Scanned										
WDC	WDC WD3200BEKT- 75KA9T0	WD- WXX1A60K6953	1	0	67502	979	0	0	0	/dev/sda
Hitachi	Hitachi HTS545050B9A300	100919B40017	2	0	76	1	0	0	0	/dev/sdb

Matches per SearchPak

Matches found per SearchPak

SearchPak Name	Matches	Highest Relevancy Score	Number of Files Copied	Contact Name	Contact Agency	Contact Email	Contact Phone
IPOC Visual Search	1367	20	1367	Mr. ADF Support	ADF Solutions Inc (Private)	support@adfsolutions.com	+1 (301) 312 6578 UK 0115 9522727
Anti-Forensics - Keyword Search - Encryption Tools	14	100	0	Mr. ADF Support	ADF Solutions Inc (Private)	support@adfsolutions.com	+1 (301) 312 6578 UK 0115 9522727
Anti-Forensics - Keyword Search - Wipers and other tools	15	100	0	Mr. ADF Support	ADF Solutions Inc (Private)	support@adfsolutions.com	+1 (301) 312 6578 UK 0115 9522727
IPOC Keyword Search - File Content under 1mb size - PART 1	237	100	237	Mr. ADF Support	ADF Solutions Inc (Private)	support@adfsolutions.com	+1 (301) 312 6578 UK 0115 9522727
IPOC Keyword Search - Filename Only - PART 2	201	100	201	Mr. ADF Support	ADF Solutions Inc (Private)	support@adfsolutions.com	+1 (301) 312 6578 UK 0115 9522727
Windows Artefacts - Link Files	15	100	15	Mr. ADF Support	ADF Solutions Inc (Private)	support@adfsolutions.com	+1 (301) 312 6578 UK 0115 9522727