FORENSIC COMPANY, INC.
999 N SOMEPLACE AVE
SOMETOWN, CA 99999
(999) 999-9999

99999-F22A-CR1

Examination Report

Prepared by:
Andreas T. Spruill
Sr. Director of Risk Management

June 30, 2020

Table of Contents

EXAMINATION REPORT

1 INTRODUCTION

1.1 BACKGROUND

On 15 September 2010, Laura Grey, Senior Specialist, Records and Information Management, Great Company, Inc., contacted Forensic Company, Inc.(FCI) and requested computer forensic consulting services in conjunction with their internal matter identified as the "Donald Smith Investigation." FCI subsequently entered into a services agreement with Great Company, Inc., in which specific rates for services to be provided were agreed upon. On 7 December 2010, the services to be provided under this agreement were expanded via Change Request 1 (CR1). A copy of the Statement of Work Change Request is attached hereto as **Exhibit A**.

I am a full-time employee with FCI, currently supporting the Professional Services Division as a Computer Forensic Examiner. A copy of my Curriculum Vitae is attached hereto as **Exhibit B**. I submit this report to explain various tasks performed by FCI on behalf of Great Company, Inc, as requested under CR1. Services provided under the original agreement are fully documented in a previously submitted examination report dated 3 December 2010.

1.2 REQUEST

Ms. Grey requested that FCI conduct an examination of a single hard disk drive, preserved in the form of a DD image, to determine, to the extent possible, the following:

a. Information related to the presense of any data destruction utilities
b. Information related to any permanent destruction of the drive's contents
c. Information related to any content that may have been permanently destroyed

1.3 SUMMARY OF FINDINGS

Per the requested services, the following summary of findings is submitted:

A. On 09/11/2006, a user, logged in under the local administrator account, installed and configured for use by all users, the application "SecureClean 4," manufactured by White Canyon Software. White Canyon Software specializes in the manufacture and selling of applications designed to permanently destroy electronically stored information (ESI). According to the SecureClean User Manual "… SecureClean is designed to provide every user with the highest level of personal privacy protection by finding and overwriting old data, making it impossible to recover."

   At the time of installation, the application was configured to autorun upon start of the Windows Operating System and to purge the systems temporary work file upon shutdown.

B. On 09/11/2006, following the installation of the SecureClean 4 application, a user, logged in under the local administrator account, initiated the applications "Deep Clean" function against the device. This action permanently destroyed all deleted email, temporary internet files, and temporary Windows files, as well as the contents of the devices unallocated space, file slack and the MFT entries of deleted items.

On 10/15/2006 and 10/24/2006, a user, logged in under the "dsmith" account, initiated the applications "Quick Clean" function against the device. This action permanently destroyed all delected email, temporary internet files and temprorary Windows files.

On 11/08/2006, a user, logged in under the "dsmith" account, initiated the applications "Deep Clean" function against the device. This action permanently destroyed all items as previousily described.

C. Analysis of operating system components showed that it had recorded references to the existence of 545 user content files, for which there was no reference recorded by the file system's MFT.

2 FORENSIC EXAMINATION

2.1 TOOLS

The following tools and equipment were used to process the submitted items of evidence:

A. Computer Name: FCI3CHXWD1, FCI Asset Tag 200999, located in FCI's Los Angles Field Office laboratory. FCI3CHXWD1 is a Dell Precision 690 tower computer system running a FCI licensed copy of Microsoft Windows 7 Professional (x64).

B. EnCase Enterprise version 6.18.0.59, fully licensed to FCI, utilizing HASP dongle 105690596, and installed on FCI3CHXWD1.

C. Digital Forensic Examiner's Power Pack v1.1, 42 LLC (CA), fully licensed to FCI and installed on FCI3CHXWD1.

2.2 EVIDENCE

The following is a listing of submitted items of evidence:

Table 1 - Items of Evidence

Item	OE EIN	Description	Type	RD EIN	DDE EIN
1	100-000693	Seagate External USB Hard Disk Drive, Model 9KW2A4-502, Serial Number 999KJJM	H	N/A	100-000916

Type Codes: S-System | H-Hard Drive | F-Floppy disk | Z-Zip Disk | T-Tape | CD-CD | D-DVD | P-PDA | CP-Cell Phone | X-Other

2.2.1 ITEM OF EVIDENCE 1

On 19 November 2010, Item of Evidence 1 was provided to FCI by Ms. Grey via FedEx, Tracking Number 7941 2923 9999. Upon receipt, this item was assigned FCI internal Evidence Identification Number (EIN) 100-000693 and chain of custody documentation was initiated. This item of evidence contained a DD image file for a single hard disk drive (HDD). A copy of the DD image was then placed on another forensically prepared HDD marked as EIN 100-000916. A true and correct of copy of the chain of custody documentation for this item of evidence is attached hereto under **Exhibit C**.

Ms. Grey also provided via email an imaging audit printout of the DD image contained on Item of Evidence 1. A true and correct of the printout is attached hereto under **Exhibit D**.

The DD image of the single HDD and its respective imaging audit printout were reviewed before any analysis was undertaken with the following information noted:

Acquisition MD5:	4fd7f8e444355e6d0866a4900bfb4348
Verification MD5:	4fd7f8e444355e6d0866a4900bfb4348
Total Size:	60,011,642,880 Bytes (55.9GB)
Total Sectors:	117,210,240
Disk Signature:	D7 9C D7 9C

Drive Partitions

Id	*Type*	*Start Sector*	*Total Sectors*	*Size*
de	Dell Utility	0	80,325	39.2MB
07	NTFS	80,325	117,113,850	55.8GB

2.3 ANALYSIS

2.3.1 WINDOWS REGISTRY

The Microsoft Windows Registry is a central hierarchical database used in Windows operating systems to store information that is necessary to configure the system for one or more users, applications and hardware devices.

A registry hive is a group of keys, subkeys, and values that has a set of supporting files that contain backups of its data. The supporting files for all hives except HKEY_CURRENT_USER are in the %SystemRoot%\System32\Config folder on Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. The supporting files for HKEY_CURRENT_USER are in the %SystemRoot%\Profiles\Username folder.

The Registry backup files from the DD Image on Item of Evidence 1 were parsed with the following data extracted from the listed Registry Keys.

2.3.1.1 ACTIVE CONTROL SET

Registry Key: System\Select\

Sub-Key	Value
Current	1

2.3.1.2 SYSTEM INFORMATION

Registry Key: System\ControlSet001\Control\ComputerName\ComputerName

Sub-Key	Value
Computer Name	FCLT8934

Registry Key: Software\Microsoft\Windows NT\CurrentVersion

Sub-Key	Value
ProductName	Microsoft Windows XP
CSDVersion	Service Pack 2
RegisteredOwner	Great Company, Inc.
RegisteredOrganization	Great Company, Inc.
InstallDate	09/16/2005 17:57:07

Registry Key: System\ControlSet001\Control\Windows\

Sub-Key	Value
LastShutdownTime	01/16/2007 16:28:41

Registry Key: System\ControlSet001\Control\Watchdog\Display

Sub-Key	Value
ShutdownCount	232

2.3.1.3 TIME ZONE INFORMATION

Registry Key: System\ControlSet001\Control\TimeZoneInformation

Sub-Key	Value
ActiveTimeBias	300 (-5 hours offset from GMT)
StandardBias	300 (-5 hours offset from GMT)
StandardName	Eastern Standard Time
DaylightBias	60 (1 hour offset from Standard Time)
DaylightName	Eastern Daylight Time
Bias	300 (-5 hours offset from GMT)

2.3.1.4 USER ACCOUNTS

Registry Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Sub-Key	Value
DefaultUserName	dsmith
AltDefaultUserName	dsmith

Registry Key: Software\Microsoft\Windows NT\CurrentVersion\ProfileList
Registry Key: S-1-5-21-2020637620-3599195085-359561344-500
Key Last Write: 09/14/05 16:48:25

Sub-Key	Value
ProfileImagePath	%SystemDrive%\Documents and Settings\Administrator

Registry Key: S-1-5-21-3826821714-972506294-598665437-500
Key Last Write: 01/16/07 15:05:29

Sub-Key	Value
ProfileImagePath	%SystemDrive%\Documents and Settings\Administrator.FCLT8892

Registry Key: S-1-5-21-790525478-854245398-839522115-1534
Key Last Write: 01/16/07 16:28:19

Sub-Key	Value
ProfileImagePath	%SystemDrive%\Documents and Settings\dsmith

Registry Key: SAM\SAM\Domains\Account\Users

Sub-Key	Value

Sub-Key	Value
Username	Administrator
UserComment	Built-in account for administering the computer/domain
Security Identifier	S-1-5-21-3826821714-972506294-598665437-500
Profile Path	%SystemDrive%\Documents and Settings\Administrator.FCLT8892
Last Login Date	01/16/2007 19:58:52
Pwd Reset Date:	09/14/2005 19:36:47
Pwd Fail Date	11/30/2006 21:05:12
Flags	Password does not expire / Normal user account

2.3.1.5 IDE HARDWARE DEVICES

Registry Key: System\ControlSet001\Enum\IDE

Sub-Key	Value
FriendlyName	Hitachi HTS541060G9AT00
DeviceDescription	Disk drive
Device	DiskHitachi_HTS541060G9AT00_____MB3OA61A
KeyLastWrite	08/24/05 12:51:13
Instance	5&2f26e1ec&0&0.0.0
KeyLastWrite	01/16/07 16:20:38

2.3.1.6 MOUNTED DEVICES

Registry Key: \system\MountedDevices\

Sub-Key	Value
\??\Volume{9dd6b1ba-26f9-11da-9487-806d6172696f}	d7 9c d7 9c
\DosDevices\C	d7 9c d7 9c

Registry Key: \system\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Sub-Key	Value
Device	IDE#DiskHitachi_HTS541060G9AT00_____MB3OA61A
Instance	5&2f26e1ec&0&0.0.0
Volume ID	{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

2.3.1.7 SYSTEM CONFIGURATION

Registry Key: \system\ControlSet001\Control\Session Manager\Memory Management\
Key Last Write: 09/11/06 18:48:40

Sub-Key	Value
ClearPageFileAtShutdown	1 (Active)

2.3.1.8 USERASSIST VALUES

Registry Key: \dsmith\ntuser\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
Key Last Write: 01/16/07 16:27:50

Sub-Key	Value
C:\Program Files\WhiteCanyon\SecureClean 4\SCLauncher4.exe	Date: 11/08/2006 22:42:25; Count: 1
Clean My Computer.lnk	Date: 11/08/2006 22:42:25; Count: 1

2.3.1.9 SYSTEM ACTIVITY

Registry Key: \administrator.FCLT8892\NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MUICache
Key Last Write: 01/16/07 15:04:48

Sub-Key	Value
C:\Program Files\WhiteCanyon\SecureClean 4\scregmanager4.exe	SecureClean Registry Manager
C:\Program Files\WhiteCanyon\SecureClean 4\sctray4.exe	SecureClean Tray

Registry Key: \dsmith\NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MUICache
Key Last Write: 01/16/07 16:24:37

Sub-Key	Value
C:\Program Files\WhiteCanyon\SecureClean 4\scregmanager4.exe	SecureClean Registry Manager
C:\Program Files\WhiteCanyon\SecureClean 4\sctray4.exe	SecureClean Tray
C:\Program Files\WhiteCanyon\SecureClean 4\SCLauncher4.exe	SecureClean Component Launcher
C:\Program Files\WhiteCanyon\SecureClean 4\SCDragDrop4.exe	SecureClean Drag-N-Drop File Zapper

2.3.1.10 AUTORUN

Registry Key: \software\Microsoft\Windows\CurrentVersion\Run
Key Last Write: 01/16/07 15:15:09

Sub-Key	Value
SecureClean4Tray	C:\Program Files\WhiteCanyon\SecureClean 4\sctray4.exe
SecureClean4RegManager	C:\Program Files\WhiteCanyon\SecureClean 4\scregmanager4.exe

2.3.1.11 APPLICATIONS

Registry Key: \software\Microsoft\Windows\CurrentVersion\Uninstall\{83b13a64-d98a-48a2-8cbc-ec0ec5433b18}
Key Last Write: 09/11/06 18:45:43

Sub-Key	Value
DisplayName	SecureClean4
UninstallString	C:\Program Files\WhiteCanyon\SecureClean 4\scuninstall4.exe

Registry Key: \software\WhiteCanyon\SC4
Key Last Write: 09/11/06 18:45:44

Registry Key: \Administrator.FCLT8892\NTUSER.DAT\Software\WhiteCanyon\SC4
Key Last Write: 09/11/06 18:45:42

2.3.1.12 INTERNET ACTIVITY

Registry Key: \administrator.FCLT8892\NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs
Key Last Write: 09/11/06 20:30:50

Sub-Key	Value
http://www.optonline.net/	url1
http://www.whitecanyon.com/	url2
http://www.amazon.com/	url3

2.3.2 SYSTEM EVENT LOGS

The Windows XP Event Log Service records computer based application, security, and system events. The application log contains events logged by programs. Events that are written to the application log are determined by the developers of the software program. The security log records events such as valid and invalid logon attempts, as well as events related to resource use. Users must be logged on as Administrator or as a member of the Administrators group in order to turn on, use, and specify which events are recorded in the security log. The system log contains events logged by Windows XP system components. Windows XP predetermines the events that are logged by system components.[1]

The supporting files for these event logs are in the %SystemRoot%\System32\Config folder on Windows XP systems. The event logs from the DD Image on Item of Evidence 1 were parsed and the resulting data extracted to a Windows Excel Spreadsheet, a true and correct copy of which is attached hereto under **Exhibit E**.

The following information is provided regarding the parsed Event Logs:

Name	SysEvent.Evt
Last Accessed	01/16/07 16:28:21
File Created	03/14/05 07:45:58
Last Written	01/16/07 16:28:21
Entry Modified	01/16/07 16:28:21
File Identifier	180
Hash Value	9c3e29146e23d7f2a624c77d6775d96d
Full Path	\C\WINDOWS\system32\config\SysEvent.Evt

Name	SecEvent.Evt
Last Accessed	01/16/07 16:28:21
File Created	03/14/05 07:45:58
Last Written	01/16/07 16:28:21
Entry Modified	01/16/07 16:28:21
File Identifier	188
Hash Value	9c673170eebf09b870fc0e612eb1bcb5
Full Path	\C\WINDOWS\system32\config\SecEvent.Evt

Name	AppEvent.Evt
Last Accessed	01/16/07 16:28:21
File Created	03/14/05 07:45:58
Last Written	01/16/07 16:28:21
Entry Modified	01/16/07 16:28:21
File Identifier	187
Hash Value	a5d37f11c928b7534409bb7eb84892b6
Full Path	\C\WINDOWS\system32\config\AppEvent.Evt

[1] http://support.microsoft.com/kb/308427

2.3.3 PREFETCH

The Microsoft Windows XP operating system uses a process called "prefetching" to improve system performance. Prefetching occurs during system startup (boot prefetching) and during application execution (application prefetching). The boot prefetching process monitors references to all files and folders during the first two minutes of the boot process, the first minute after all Windows services starts, and the first 30 seconds after the start of a user's account. Application prefetching monitors the first 10 seconds after an application process starts. Once the data is processed, it is written to a file and stored in the %SystemRoot%\Windows\Prefetch folder.

The Prefetch files from the DD Image on Item of Evidence 1 were parsed and the resulting data outputted to a text file, a true and correct copy of the full output is attached hereto under **Exhibit F**.

The following data was extracted from the listed prefetch files:

File: SCTRAY4.EXE-0FA6F8E9.pf
Last Run: 01/16/07 01:22:50PM
Times Executed: 2
Selected Processes:
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCTRAY4.EXE

File: SCREGMANAGER4.EXE-34CA7F7A.pf
Last Run: 01/16/07 01:22:47PM
Times Executed: 1
Selected Processes:
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCREGMANAGER4.EXE

File: EXPLORER.EXE-02121B1A.pf
Last Run: 01/16/07 01:22:35PM
Times Executed: 55
Selected Processes:
\DEVICE\HARDDISKVOLUME2\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\SECURECLEAN FILE ZAPPER.LNK
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCDRAGDROP4.EXE
\DEVICE\HARDDISKVOLUME2\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\SCAN MY COMPUTER.LNK
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCLAUNCHER4.EXE
\DEVICE\HARDDISKVOLUME2\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\CLEAN MY COMPUTER.LNK
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCTRAY4.EXE

File: NTOSBOOT-B00DFAAD.pf
Last Run: 01/16/07 01:20:39PM
Time Executed: 107
Selected Processes:
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCTRAY4.EXE
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCWATCH4.EXE
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCREGMANAGER4.EXE
\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCDRAGDROP4.EXE
\DEVICE\HARDDISKVOLUME2\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\SCAN MY COMPUTER.LNK

\DEVICE\HARDDISKVOLUME2\PROGRAM FILES\WHITECANYON\SECURECLEAN 4\SCLAUNCHER4.EXE
\DEVICE\HARDDISKVOLUME2\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\CLEAN MY COMPUTER.LNK

2.3.4 LINK FILES

Link files, also known as shortcuts, have the file extension .lnk. Link files refer to, or link to, target files. These target files can be applications, directories, documents, or data files. They can also be non-file-system objects such as printers or various computer management consoles. Link files are created by the operating system upon installation, by applications with which they are installed or when a user accesses a file. Link files can also be created directly by a user.[2]

The Link files from the DD Image on Item of Evidence 1 were parsed and the resulting data outputted to a Microsoft Excel spreadsheet, a true and correct copy of the full output is attached hereto under **Exhibit G**.

The following notable data was extracted from the identified Link files:

Name	Clean My Computer.lnk
Last Accessed	01/16/07 16:12:37
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 19:20:22
File Identifier	52666
Hash Value	bc523ad7f10bf151e2e49d882f7c1193
Full Path	\C\Documents and Settings\All Users\Start Menu\Programs\WhiteCanyon\SecureClean 4\Clean My Computer.lnk

Target File

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCLauncher4.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:39PM
Last Written Date:	11/10/05 08:13:48AM
Last Accessed Date:	09/11/06 06:45:39PM

Name	Scan My Computer.lnk
Last Accessed	01/16/07 16:12:37
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 19:20:22
File Identifier	52670
Hash Value	70ac1c0a54605f853760717da08f2d89
Full Path	\C\Documents and Settings\All Users\Start Menu\Programs\WhiteCanyon\SecureClean 4\Scan My Computer.lnk

Target File

[2] EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition, Steve Bunting, December 2007

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCLauncher4.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:39PM
Last Written Date:	11/10/05 08:13:48AM
Last Accessed Date:	09/11/06 06:45:39PM

Name	Clean My Computer.lnk
Last Accessed	01/16/07 16:12:18
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 18:59:47
File Identifier	52667
Hash Value	2efc7baff403647c2894a83b2046e052
Full Path	\C\Documents and Settings\All Users\Desktop\Clean My Computer.lnk

Target File

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCLauncher4.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:39PM
Last Written Date:	11/10/05 08:13:48AM
Last Accessed Date:	09/11/06 06:45:39PM

Name	Scan My Computer.lnk
Last Accessed	01/16/07 16:12:17
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 18:59:47
File Identifier	52671
Hash Value	8231e588cfbe85bb9005a486ba173e6a
Full Path	\C\Documents and Settings\All Users\Desktop\Scan My Computer.lnk

Target File

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCLauncher4.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:39PM
Last Written Date:	11/10/05 08:13:48AM
Last Accessed Date:	09/11/06 06:45:39PM

Name	SecureClean File Zapper.lnk
Last Accessed	01/16/07 16:12:17
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 18:59:47
File Identifier	52663
Hash Value	769b42fc17b40ef2b9eaa3511efcb4a2

Full Path	\C\Documents and Settings\All Users\Desktop\SecureClean File Zapper.lnk

Target File

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCDragDrop4.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:39PM
Last Written Date:	11/09/05 10:52:42AM
Last Accessed Date:	09/11/06 06:45:39PM

Name	Uninstall SecureClean.lnk
Last Accessed	01/16/07 16:12:37
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 19:20:22
File Identifier	52672
Hash Value	bf903916a668b79a1994c8e3d16e0c0d
Full Path	\C\Documents and Settings\All Users\Start Menu\Programs\WhiteCanyon\SecureClean 4\Uninstall SecureClean.lnk

Target File

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCUninstall4.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:40PM
Last Written Date:	11/09/05 10:03:18AM
Last Accessed Date:	09/11/06 06:45:40PM

Name	LiveUpdate.lnk
Last Accessed	01/16/07 16:12:37
File Created	09/11/06 18:45:42
Last Written	09/11/06 18:45:42
Entry Modified	09/11/06 19:20:22
File Identifier	52673
Hash Value	ec5fff5c2d73100695dce66433043e13
Full Path	\C\Documents and Settings\All Users\Start Menu\Programs\WhiteCanyon\SecureClean 4\LiveUpdate.lnk

Target File

Symbolic Link	C:\Program Files\WhiteCanyon\SecureClean 4\SCLiveUpdate.exe
Working directory	C:\Program Files\WhiteCanyon\SecureClean 4
Created Date:	09/11/06 06:45:39PM
Last Written Date:	11/09/05 12:58:34PM
Last Accessed Date:	09/11/06 06:45:39PM

The Link files from the DD Image on Item of Evidence 1 were further parsed to identify all target files by long file name. The resulting list of target files was compared to a complete listing of file names from Item of Evidence 1.

This comparison of file names resulted in 158 files not matched, a true and correct copy of the resulting output is attached hereto under **Exhibit H**.

Table 2 – Summary of Unmatched Files by Extension

File Extension	Count
csv	1
doc	58
log	1
pdf	1
ppt	2
txt	1
xls	42
zip	38
Total	**144**

2.3.5 RECYCLE BIN

When a user deletes a file or folder in the Windows XP operating system, it is placed in the Recycle Bin folder structure. Items are temporarily stored in this folder structure until they are permanently deleted by the user. Users can move items to the Recycle Bin by either dragging them to the Recycle Bin desktop icon or by selecting the items and pressing the Delete key. Users may also right-click an item and select "Delete" from the pop-up menu.

In order to recover deleted items stored in the Recycle Bin, the system maintains a log file of all item currently stored therein. This file is named INFO2. When an item is added to an empty Recycle Bin this file is created and then update as files are added or individually restored. When the Recycle Bin is emptied (all files deleted) this INFO2 file is also deleted.

The supporting file structure for the Recycle Bin functionality is located at %SystemRoot%\Recycler\%User SID% on Windows XP systems. The Recycle Bin contents and INFO2 files on the DD Image on Item of Evidence 1 were parsed and the following data extracted:

Table 3 - Listing of Recycle Bin Contents

Deleted File Name	Deleted Date	Index #
C:\Documents and Settings\dsmith\Desktop\36854 Eval Xxxxxx 22NOV.doc	12/2/2006 13:06	17
C:\Documents and Settings\dsmith\Desktop\36855 Eval Xxxxxx 22NOV-Date Change.doc	12/2/2006 13:07	18
C:\Documents and Settings\dsmith\Desktop\36649 Eval Xxxxxx 26SEP.doc	12/2/2006 13:07	19
C:\Documents and Settings\dsmith\Desktop\35969 Eval Xxxxxx 22JUN.doc	12/2/2006 13:07	20
C:\Documents and Settings\dsmith\Desktop\36748 Eval Xxxxxx	12/2/2006 13:07	21

Deleted File Name	Deleted Date	Index #
27OCT.doc		
C:\Documents and Settings\dsmith\Desktop\36749 Eval Xxxxxx 24OCT.doc	12/2/2006 13:07	22
C:\Documents and Settings\dsmith\Desktop\36630 Eval Xxxxxx.doc	12/2/2006 13:07	23
C:\Documents and Settings\dsmith\Desktop\36467 Eval Xxxxxx 07SEP.doc	12/2/2006 13:07	24
C:\Documents and Settings\dsmith\Desktop\36746 Eval Xxxxxx 25OCT.doc	12/2/2006 13:07	25
C:\Documents and Settings\dsmith\Desktop\36583 Eval Xxxxxx.doc	12/2/2006 13:07	26
C:\Documents and Settings\dsmith\Desktop\36650 Eval Xxxxxx 28SEP.doc	12/2/2006 13:07	27
C:\Documents and Settings\dsmith\Desktop\36806 Eval xxxxxxxx 17NOV.doc	12/2/2006 13:07	28
C:\Documents and Settings\dsmith\Desktop\36742 Eval Xxxxxx 26OCT.doc	12/2/2006 13:07	29
C:\Documents and Settings\dsmith\Desktop\36115 Eval Xxxxxx 20JUL.doc	12/2/2006 13:07	30
C:\Documents and Settings\dsmith\Desktop\Dr xxxx's CV.doc	12/2/2006 13:08	31
C:\Documents and Settings\dsmith\Desktop\xxxxxxxxxx.doc	12/2/2006 13:09	32
C:\Documents and Settings\dsmith\Desktop\2007 OE Outside CA Form.doc	12/2/2006 13:10	33
C:\Documents and Settings\dsmith\Desktop\Copy of Routing Schedule xxxxxxxxx.xls	12/3/2006 6:42	34
C:\Documents and Settings\dsmith\Local Settings\Application Data\Microsoft\Outlook\GreatOutlookv10.log	1/16/2007 13:15	35
C:\Documents and Settings\All Users\Desktop\Offline Client.lnk	1/16/2007 13:16	36

2.3.6 MASTER FILE TABLE

The master file table (MFT) is a database in which information about every file and directory on an NT File System (NTFS) volume is stored. There is at least one record for every file and directory on the NTFS logical volume. Each record contains attributes that tell the operating system (OS) how to deal with the file or directory associated with the record. Detailed information about a file or directory such as the type, size, date/time of creation, date/time of most recent modification and author identity is either stored in MFT entries or in space external to the MFT but described by the MFT entries.

The MFT for the NTFS partition from the DD Image on Item of Evidence 1 was parsed and the resulting data extracted to a Windows Excel Spreadsheet, a true and correct copy of which is attached hereto under **Exhibit I**.

The MFT contains 10,040 record entries for deleted items, whose filenames are recorded as SC008433.T~P and continuing sequentially to SC018472.T~P. The standard attributes and filename attributes date/time for which are all set to the same value, starting at 11/08/06 22:52:40 and continuing to 11/08/06 22:52:47, respectively.

2.3.7 INDX BUFFER

Folder entries within the MFT contain an index of the file entries stored within that folder or, if the MFT cannot hold the entire folders entries, an index buffer is allocated outside the MFT to hold these index entries.

All recoverable INDX buffers on the DD Image on Item of Evidence 1 were parsed and the resulting data extracted to a Windows Excel Spreadsheet, a true and correct copy of which is attached hereto under **Exhibit J**.

The resulting data set was further parsed to identify all unique file entries by file path and file name. The resulting list of 1,811 files was compared to a complete listing of file path and file names from Item of Evidence 1 with none of the items being located, a true and correct copy of the resulting output is attached hereto under **Exhibit K**.

The following table is shows the number of user content files by file type within the 1,811 entries:

Table 4 – Summary of User Content Files by Extension

File Extension	Count
bmp	2
doc	26
gif	141
htm	58
JPG	9
LNK	34
png	4
TXT	45
URL	1
XLS	1
ZIP	3
Total	**324**

2.3.8 REGISTRY SHELL BAG

All versions of the Microsoft Windows operating system since XP stores data within each users registry file regarding the arrangement of folders and files in Explorer views, as well as to monitor recently used and frequently used applications in the Start-Menu.[3] The registry keys that support this functionality are:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\BagMRU
- HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags
- HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\BagMRU
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

[3] http://www.42llc.net/index.php?option=com_myblog&show=Shell-BAG-Format.html&Itemid=39

The user registry files, along with those copies stored in the restore point folder structure, on the DD Image on Item of Evidence 1 were parsed to identify references to file and folder items with the resulting data extracted to a Windows Excel Spreadsheet, a true and correct copy of which is attached hereto under **Exhibit L**.

The resulting data set was further parsed to identify all file entries by file name. The resulting list of 71 files was compared to a complete listing of file names from Item of Evidence 1 with 63 items not located, a true and correct copy of the resulting output is attached hereto under **Exhibit M**.

Table 5 - Shell BAG Files by Extension

File Extension	Count
ZIP	63

2.3.9 DISK USAGE

A byte level scan of the storage area allocated to the pagefile.sys[4] file showed that 99.70% of its content was the "00" hexadecimal value. The following is provided regarding the pagefile.sys file:

Name	pagefile.sys
Last Accessed	01/16/07 16:20:54
File Created	03/14/05 07:41:51
Last Written	01/16/07 16:20:54
Entry Modified	01/16/07 16:20:54
Physical Size	1,598,029,824
File Identifier	77012
Hash Value	853e37eb8ab4edae8cc22d64e0814475
Full Path	\C\pagefile.sys

A byte level scan of the content stored in the devices unallocated storage area[5] showed that 91.98% of this space was the "00" hexadecimal value. The following is provided regarding the unallocated clusters:

Name	Unallocated Clusters
Physical Size	44,663,226,368

2.3.10 VIRUS / MALWARE SCAN

The DD image on Item of Evidence 1 was mounted as a virtual physical device. The content of the mounted device was scanned using McAfee Virus Scan Enterprise+, version 8.7.0i, Scan Engine 5400.1158, DAT Version 6203.0000.

[4] Pagefile.sys – A file used to temporarily store code and data for programs that are currently running. This information is [normally] left in the file after the programs are terminated, and may be retrieved using forensic techniques. Also referred to as a swap file. *(The Sedona Conference Glossary: E-Discovery & Information Management, 2nd ed., December 2007.)*

[5] Unallocated Space - The area of computer media, such as a hard drive, that does not contain normally accessible data. Unallocated space is usually the result of a file being deleted. When a file is deleted, it is not actually erased, but is simply no longer accessible through normal means. The space that it occupied becomes unallocated space, i.e., space on the the drive that can be reused to store new information. Until protions of the unallocated space are used for new data storage, in most instances, the old data remains and can be retrieved using forensic techiniques. *(The Sedona Conference Glossary: E-Discovery & Information Management, 2nd ed., December 2007.)*

The scan did not return any relevant results. A true and correct copy of the scan log is attached hereto under **Exhibit N**.

2.4 FINDINGS

2.4.1 PRESENCE OF WIPING APPLICATIONS

The results of the analysis conducted under section 2.3.1.12 shows that sometime on or prior to 20:30 on 09/11/06, a user, who was logged into the computer user account "Administrator.FCLT8892" (the Local Administrator Account), Security ID: S-1-5-21-3826821714-972506294-598665437-500, typed into the Internet Explorer address field the web site address "www.whitecanyon.com." A review of the Security Event log extracted under section 2.3.2, shows that on 09/11/2006, the local administrator account was logged into the system from 15:13 to 15:28 and again from 17:32 to 19:30.

The website address "www.whitecanyon.com" is the web site for White Canyon Software whose marketing motto is "The World Leader in Data Deletion Technology" and who manufacturers a suite of data destruction tools.

The combined results of the analysis conducted under sections 2.3.1.11, 2.3.4 and 2.3.6 shows that on 09/11/2006 at 18:45, a user, who was logged into the local administrator account, installed an application called "SecureClean 4" (SC4) for use by all active user accounts.

A review of the folder and file structure extracted under section 2.3.6, shows that there exists a folder structure identified as follows:

Name	SecureClean 4
Description	Folder
Last Accessed	01/16/07 16:12:09
File Created	09/11/06 18:45:39
Last Written	09/11/06 20:18:49
Entry Modified	09/11/06 20:18:49
File Identifier	52622
Hash Value	9824d70880b281457019597aa1709b5e
Full Path	\C\Program Files\WhiteCanyon\SecureClean 4

The combined results of the analysis conducted under sections 2.3.1.7, 2.3.1.10 and 2.3.3 shows that the SC4 application was configured to autorun upon start of the Windows Operating System and that the system was configured to purge the systems pagefile upon shutdown.

SC4 is manufactured by White Canyon Software and can be purchased and downloaded from their website. According to the SC4 User Manual "… SecureClean is designed to provide every user with the highest level of personal privacy protection by finding and overwriting old data, making it impossible to recover." A true and correct copy of the SC4 User Manual is attached hereto under **Exhibit O**.[6]

By default, SecureClean is set to clean deleted email, temporary internet files, temporary Windows files, and drive free space. SC4 provides two levels of "cleaning;" Quick Clean and Deep Clean. Of the two, Deep Clean will permanently destroy the contents of the hard drives unallocated space, file slack and the MFT entries for deleted items.

[6] http://support.whitecanyon.com/index.php?_m=downloads&_a=downloadfile&downloaditemid=1

Cleaning can be intiated in five different ways. First is by a user accessing the SC4 Windows Tray Icon or the Start Menu program icon and manually selecting what actions to carry out. Second, from within the standard Windows Explorer, a user selecting a target drive and choosing Quick or Deep Clean. Third, setup a cleaning schedule whereby the system will automatically execute the desired cleaning action based given date/time parameters. Fourth, if so configured, at user logoff. Fifth, if so configured, at system shutdown.

2.4.2 USE OF WIPING APPLICATIONS

The SC4 application maintains a log of cleaning actions.[7] A review of the folder and file structure extracted under section 2.3.6, shows that under the White Canyon Program Folder there exists a log file, a true and correct copy of which is attached hereto as **Exhibit P**. This log file is fully identified as follows:

Name	SCCleaningLog.txt
Last Accessed	01/07/07 22:27:14
File Created	09/11/06 20:18:49
Last Written	11/09/06 00:09:40
Entry Modified	11/09/06 00:09:40
Logical Size	1,379
File Identifier	48
Hash Value	1656d58a8410bd43a7ac4d25ccd98454
Full Path	\C\Program Files\WhiteCanyon\SecureClean 4\

A review of the log file entries shows that it recorded six cleaning operations having occurred, four Quick Cleans and two Deep Cleans:

1. The first recorded event was a Deep Clean initiated on 09/11/2006 at 18:49 and completing on 09/11/2006 at 20:18. A review of the Security Event log extracted under section 2.3.2, shows that the local administrator account was the only logged account at the time this action was initiated.
2. The second recorded event was a Quick Clean initiated on 10/15/2006 at 13:53 and completing on 10/15/2006 at 13:59. A review of the Security Event log extracted under section 2.3.2, shows that the computer user account "dsmith," Security ID: S-1-5-21-790525478-854245398-839522115-1534, was the only logged account at the time this action was initiated.
3. The third recorded event was a Quick Clean initiated on 10/15/2006 at 14:39 and completing on 10/15/2006 at 14:40. A review of the Security Event log extracted under section 2.3.2, shows that the "dsmith" account was the only logged account at the time this action was initiated.
4. The fourth recorded event was a Quick Clean initiated on 10/15/2006 at 14:41 and completing on 10/15/2006 at 14:42. A review of the Security Event log extracted under section 2.3.2, shows that the "dsmith" account was the only logged account at the time this action was initiated.
5. The fifth recorded event was a Quick Clean initiated on 10/29/2006 at 10:49 and completing on 10/29/2006 at 10:56. A review of the Security Event log extracted under section 2.3.2, shows that the "dsmith" account was the only logged account at the time this action was initiated.
6. The last recorded event was a Deep Clean initiated on 11/08/2006 at 22:43 and completing on 11/09/2006 at 00:09. A review of the Security Event log extracted under section 2.3.2, shows that the "dsmith" account was the only logged account at the time this action was initiated.

[7] SecureClean User Manual, pp 20-21.

The results of the analysis conducted under section 2.3.1.8 shows that a user, logged under the "dsmith" account, accessed the link file "Clean My Computer.lnk" on 11/08/2006 at 22:42, which in turn executed the "SCLauncher4.exe file."

The results of the analysis conducted under section 2.3.6 shows that the MFT contains 10,040 record entries for deleted items, whose filenames are recorded as SC008433.T~P and continuing sequentially to SC018472.T~P. The standard attributes and filename attributes date/time for which are all set to the same value, starting at 11/08/06 22:52:40 and continuing to 11/08/06 22:52:47, respectively.

The results of the analysis conducted under section 2.3.9 shows that a byte level scan of the storage area allocated to the pagefile showed that 99.70% of its content was the "00" hexadecimal value. Further, this analysis also showed that a byte level scan of the content stored in the devices unallocated storage area showed that 91.98% of this space was the "00" hexadecimal value.

2.4.3 IDENTIFICATION OF LOST CONTENT

The combined results of the analysis conducted under sections 2.3.4, 2.3.5, 2.3.7, and 2.3.8 shows that the operating system had recorded references to the existence of multiple files, for which there was no reference recorded by the file system's MFT. A summary of these files by reference area is as follows:

Table 6 - Lost Content Summary

Area of Reference	Count	Exhibit
Link Files	144	Exhibit H
INDX Buffer	324	Exhibit K
Registry ShellBAG	63	Exhibit M
Total	**531**	

3 CONCLUSION

At this time, no further examination is planned in regards to this matter. If requests for further examination are submitted in the future, the results will be documented on supplemental reports.

4 LISTING OF EXHIBITS

Table 7 - Listing of Exhibits

A	Statement of Work Change Request between Great Company and Forensic Company
B	Curriculum Vitae of Andreas T. Spruill
C	Chain of Custody documentation
D	Imaging audit printout of the DD image contained on Item of Evidence 1
E	Event logs from the DD Image on Item of Evidence 1
F	Parsed results of the Prefetch files from the DD Image on Item of Evidence 1
G	Parsed results of the Link files from the DD Image on Item of Evidence 1
H	Listing of Unmatched files parsed from the Link files from the DD Image on Item of Evidence 1
I	Parsed listing of the MFT for the NTFS partition from the DD Image on Item of Evidence 1
J	Listing of all recoverable INDX buffer entries on the DD Image on Item of Evidence 1
K	Listing of Unmatched files from the recoverable INDX buffers on the DD Image on Item of Evidence 1
L	Listing of file and folder entries stored in registry ShellBAG keys on the DD Image on Item of Evidence 1
M	Listing of Unmatched files from registry ShellBAG keys on the DD Image of Evidence 1
N	Virus / Malware Scan Log of Item of Evidence 1
O	SecureClean 4 User Manual
P	SecureClean 4 Activity Log file

Digital Signatures	
Prepared by:	**Reviewed by:**