

# Skout Collect

## Version 2.0.1

EVALUATION REPORT

September 2012





NIJ Electronic Crime Technology Center of Excellence  
550 Marshall St., Suite B  
Phillipsburg, NJ 08865  
[www.ECTCoE.org](http://www.ECTCoE.org)

## NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP  
Russell Yawn, CFCE  
Chester Hosmer  
Mark Davis, Ph.D.

Michael Terminelli, ACE  
Randy Becker, CFCE  
Jacob Fonseca

Victor Fay-Wolfe, Ph.D.  
Kristen McCooey, CCE; ACE  
Laurie Ann O'Leary

# Table of Contents

|  |           |
|--|-----------|
| <b>Introduction</b> .....  | <b>1</b>  |
| <b>Overview</b> .....  | <b>3</b>  |
| Product Information .....  | 3         |
| Special Features.....  | 3         |
| <b>Evaluation and Testing of Skout Collect</b> .....             | <b>5</b>  |
| Skout Configuration .....  | 5         |
| Test – VMware Collection.....                                    | 6         |
| Test – Laptop With Single Hard Drive .....                       | 9         |
| Test – Multiple Hard Drives (32-Bit OS).....                     | 9         |
| Test – Multiple Hard Drive-Raid Array-Windows 64-Bit.....        | 10        |
| Test – Macbook Air With Solid State Drive .....                  | 11        |
| Live Imaging Tests.....  | 11        |
| Test – Virtual Machine Live.....                                 | 11        |
| Test – Toshiba E205 Laptop Live Collection .....                 | 14        |
| Test – Live Test of Windows 7 Desktop With Multiple Drives ..... | 15        |
| <b>Conclusion</b> .....  | <b>17</b> |

**This report is current at the time of writing. Please be sure to check the vendor website for the latest version and updates. All software and trademarks are property of their respective companies and owners.**



# Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit <http://www.justnet.org>.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions.** Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed

process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.

- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.<sup>1</sup>

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

<sup>1</sup> National Institute of Justice High-Priority Criminal Justice Technology Needs, March 2009 NCJ 225375.



# Overview

## Product Information

Skout Collect from Skout Forensics is designed to image target computers with a portable external hard drive. An investigator purchases or configures a Skout Collect drive and sends it to the location of the target computer. The drive is then connected to the target system, automated collection software is executed via a boot CD or Windows executable and the drive is returned to the investigator for further analysis.

The process as described on the Skout Forensics website ([www.skoutforensics.com](http://www.skoutforensics.com)) is comprised of three main steps:

1. Purchase a Skout drive that is slightly larger than the evidence being collected.
  - Have it sent anywhere in the world.
  - Connect the Skout drive to the target system.
  - Available 1 TB, 750 GB, 500 GB, 320 GB; >1 TB is available upon request.
2. Once the Skout drive is connected to the target system:
  - Simply press “Enter” or click “OK” to start the collection process.
  - Data is saved to the encrypted Skout drive automatically.
  - The automated software is contained on a boot CD or windows executable.
  - Seamlessly images all internal hard disks and attached devices and images volatile memory using HBGary’s FDPPro.
3. The user will be alerted when the process has completed.
  - The evidence is secure and cannot be accessed without knowledge of the password.
  - Transport, store or analyze the resulting evidence contained on the Skout drives.
  - Use the drive for multiple collections until the Skout drive is filled.

Skout Collect is available in two different versions. “Skout Collect Drives” comes in varying sizes of collection hard drives and is designed to be used until the drive is full. The second product is an Enterprise solution that allows any drive to be configured as a Skout Collect drive with a pay-as-you-go structure in increments of 1 TB each. Skout Forensics also sells a number of accessories such as bootable thumb-drives, foam-lined cases and high-speed drive adapters that enable faster collection times of target computers. Current prices are available on the Skout Forensics website.

## Special Features

The following features of Skout Collect were taken from the product brochure available on the Skout Forensics website:

- Inherently maintains chain of custody through 256-bit secure encryption.
- Uses standard “dd” format, a widely acceptable forensic format that is cross-compatible with standard forensic software.
- Logs all processes performed.
- MD5 hash of source and images.
- HBGary’s FDPPro Memory Collection tool collects valuable volatile RAM automatically (<http://www.hbgary.com>).

- System info, make, model, serial number, size, etc. of the devices is logged.
- Automatically images each attached physical device (thumb drives, external hard drives, etc.).
- Neatly organizes cases by using time-stamped folders.
- Works on most systems including, but not limited to, Macintosh, Windows and Linux.
- Easily adds additional tools to the streamline process flow; ideal for network collections or Incident Response.



# Evaluation and Testing of Skout Collect

## Skout Configuration

Skout Enterprise is the program used to configure Skout drives for imaging. In order to prepare for the rest of the testing, the following steps were performed:

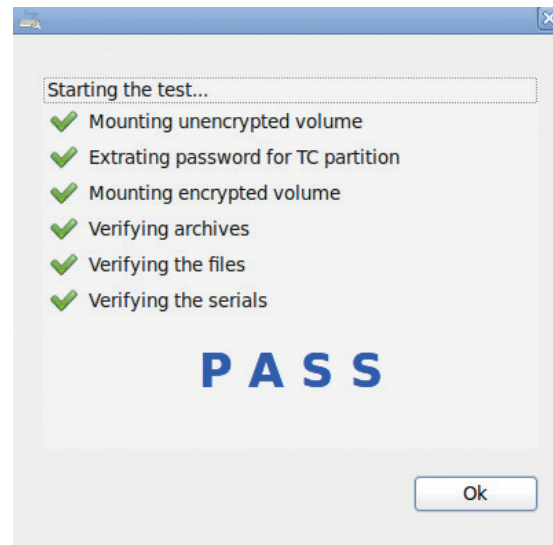
1. The Skout Collection and Skout Web Enterprise ISO files were downloaded from a FTP site provided by Skout Forensics. Documentation provided by Skout was also downloaded and reviewed.
2. Both ISOs were hashed using the MD5 algorithm to verify the downloaded files.
3. Each ISO was burned to a CD-R.

After reviewing the Skout Enterprise Instructions PDF, it was determined that a computer with an Ethernet connection was needed. This was bypassed by configuring a VMware session to use the Skout ISO image as a CD drive and the computer's wireless connection as a bridged network adapter. The following steps were taken to prepare the two provided Skout drives:

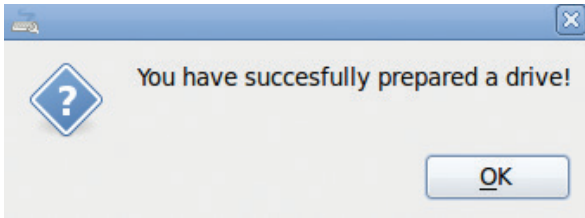
1. Booted the VMware session from the ISO file.
2. Connected the Skout drive to the computer and configured it to connect to the VMware session.
3. On the configuration menu, entered the key provided by Skout, clicked "all available space" and entered "password" twice for the password.



4. Clicked "Test Drive." Received the "Pass" message.



- Clicked “Prepare”; after about five minutes, received the completion message.



- The same procedure was used to prepare a second drive.

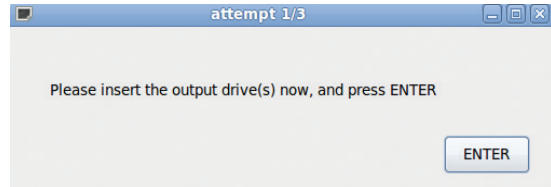
## Test – VMware Collection

The following test was performed primarily to collect screenshots of normal Skout Collect boot CD operation. This was performed on the same VMware virtual machine that was used to create the drives. The virtual hard disk is 12 GB in size and has Windows XP 32-bit installed.

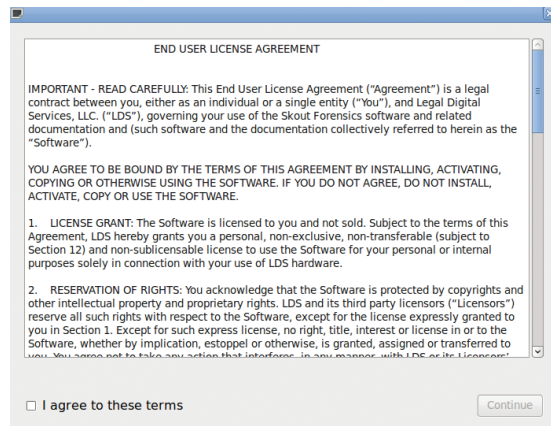
- The VMware session was configured to use a Backtrack 5 32-bit ISO as the CD drive. The VMware was started. Backtrack was started in forensics mode (no drives mounted) and the drive (/sda) was hashed using the “md5sum” program. Backtrack was shutdown.
- The VMware session was configured to use the Skout Collection ISO and the VMware session was started. A Skout splash screen was displayed during bootup.



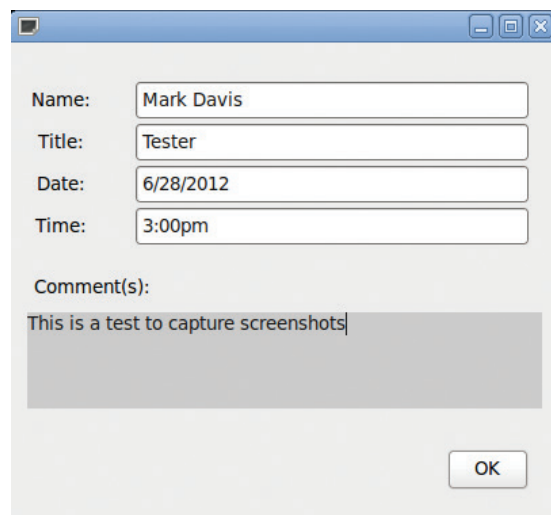
- When prompted, the Skout drive was connected to the computer and configured for use by the VMware session.



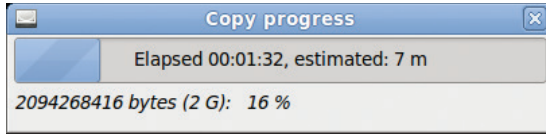
- The end-user license agreement (EULA) was accepted.



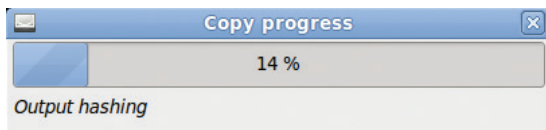
- The following window appeared and was completed as follows. “Ok” was clicked.



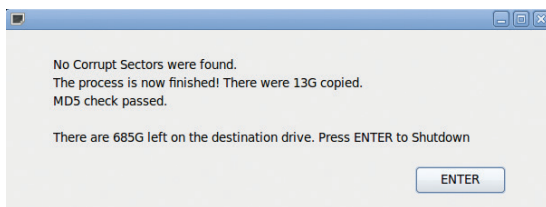
6. A copy progress window appeared indicating the progress and time remaining of the clone. (In this case, about eight minutes total).



7. After completion of copying, Skout Collect then displayed an “Output hashing” window.



8. A completion message was displayed. “Enter” was pressed and the VMware session shut down. No corrupt sectors were found.



9. The VMware session was configured to use a Backtrack 5 32-bit ISO as the CD drive. The VMware was started. Backtrack was started in forensics mode (no drives mounted) and the drive (/sda) was hashed using the “md5sum” program. Backtrack was shutdown. The hash value matched the previously calculated hash value, indicating that no changes were made to the hard drive from using the Skout Collect CD.

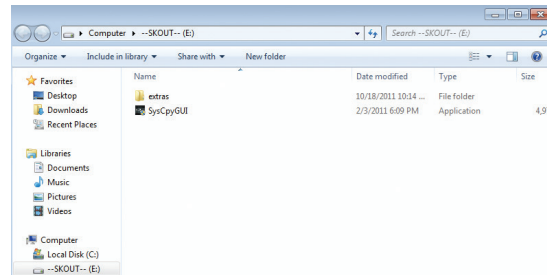
```
[*] UDEV mounts in Read Only mode
root@bt5-forensics:~# md5sum /dev/sda
b0a00734cda47bd63562ce1259c81ebe /dev/sda
root@bt5-forensics:~#
```

10. The VMware session was then booted to Windows XP. The size of the drive was recorded.

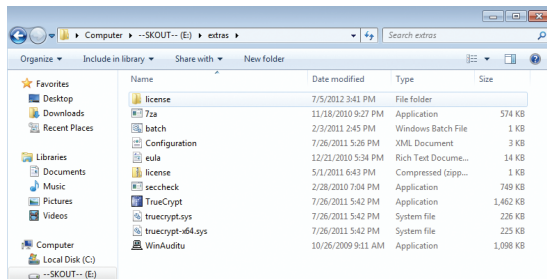
## Test Results

To examine the results of this test, the following steps were taken:

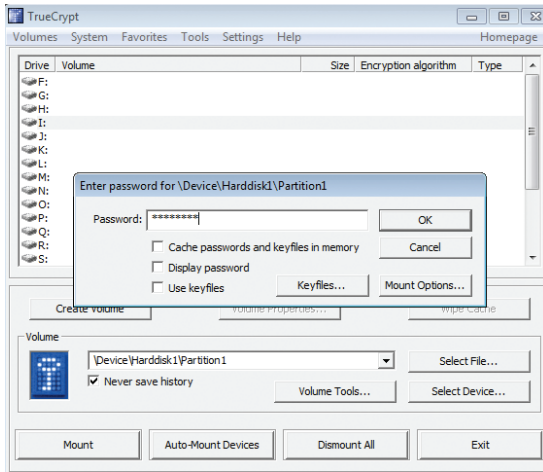
1. The Skout external drive was plugged into a Windows 7 machine.



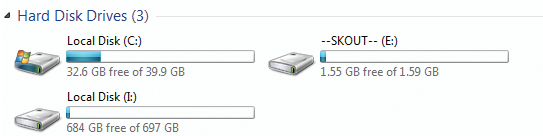
2. The “SKOUT” drive appeared and was browsed to. The “Extras” folder was clicked and the TrueCrypt program was displayed and double clicked.



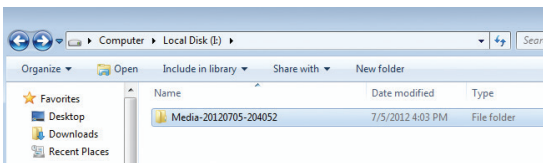
- TrueCrypt was used to mount the Skout drive, with the previously configured password.



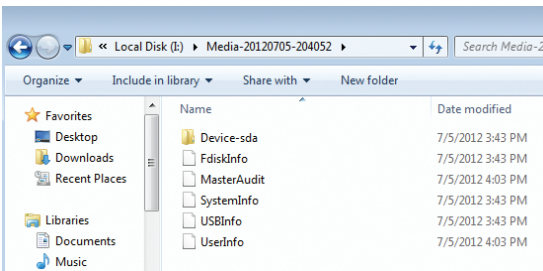
- A drive named "SKOUT" appeared in Windows Explorer.



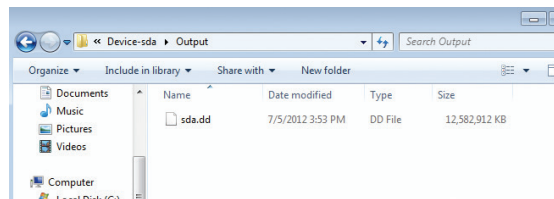
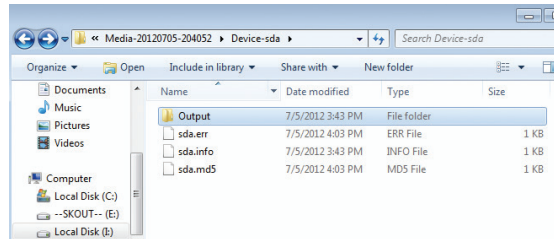
- The newly mounted drive was browsed to. A folder with a date and time stamp of the Skout acquisition was present.



- Several files were contained within the directory, including audit files, fdisk info and system info. Also included was a folder called "Device-sda."



- Within the device folder were three files, containing the drive info, MD5 checksum and general information about the drive. Also was a folder labeled "Output." Within the "Output" folder was the image of the drive, "sda.dd."



- The recorded hash of the drive as recorded by Skout Collect was compared to the hash report by backtrack, and they matched.

```

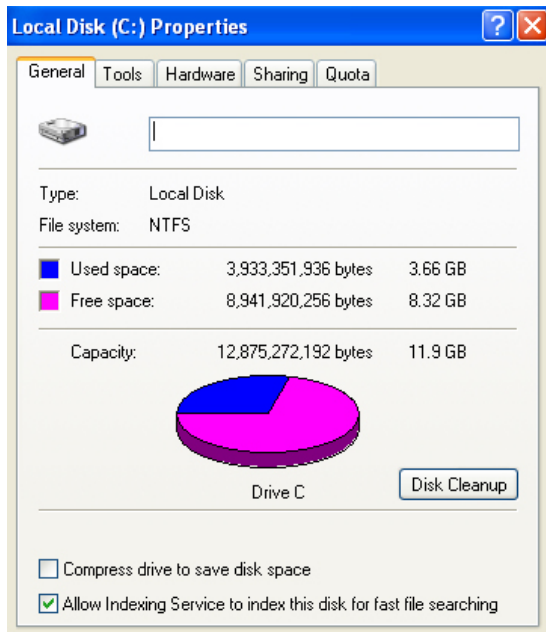
dc3dd 7.0.0 started at 2012-07-08 13:24:53 +0000
compiled options:
command line: /usr/local/bin/dc3dd if=/dev/sda
hoF=/mnt/sdb/Media-20120708-132247/Device-sda/Output/sda.dd
hash-md5 log=/mnt/sdb/Media-20120708-132247/Device-sda/sda.err
hlog=/mnt/sdb/Media-20120708-132247/Device-sda/sda.md5
device size: 25165824 sectors (probed)
sector size: 512 bytes (probed)
12884901888 bytes (12 G) copied (100%), 1218.77 s, 10 M/s
output hashing (100%)

input results for device '/dev/sda':
25165824 sectors in
0 bad sectors replaced by zeros
b0a00734cda47bd63562ce1259c81ebe (md5)

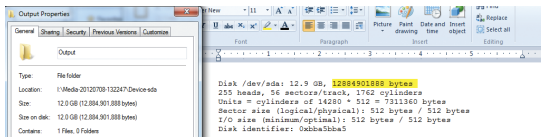
output results for file '/mnt/sdb/Media-20120708-132247/Device-sda/Output/sda.dd':
25165824 sectors out
[ok] b0a00734cda47bd63562ce1259c81ebe (md5)

dc3dd completed at 2012-07-08 13:45:12 +0000
    
```

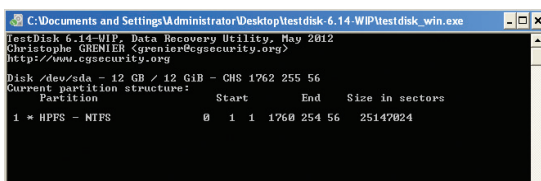
- The sda.dd file was located. FTK Imager was used to mount the sda.dd file as a local disk. This disk's properties were examined and it was found to be the same size in bytes as the original, verifying that the disk image was complete.



10. The fdisk info was examined to determine the physical size of the disk. This information matched the size of the sda.dd file, indicating the entire disk was imaged.



11. Another program, TestDisk, was used inside of the running virtual machine to determine the physical properties of the disk; again this matched the output recorded by Skout Collect.



```
input results for device '/dev/sda':
25165824 sectors in
0 bad sectors replaced by zeros
b0a00734cda47bd63562ce1259c81ebe (md5)

output results for file '/mnt/sdb/Media-20120708-132247/Device-
sda/Output/sda.dd':
25165824 sectors out
[ok] b0a00734cda47bd63562ce1259c81ebe (md5)
```

In this test the tools performed exactly as expected. Further tests will not include all the screenshots and details since it would be redundant. Results and observation will be reported.

## Test – Laptop With Single Hard Drive

This test was performed on a Toshiba branded laptop, Model: Satellite E205, with 4 GB of RAM and a 500 GB hard drive. To perform this test, the following steps were performed:

1. It was verified that the internal CD/DVD drive would boot before the internal hard drive.
2. The computer was powered on and the Skout Collect CD inserted into the drive. It appeared that the CD tried to boot; however, nothing was displayed on the screen.
3. This process was repeated with a freshly burned Skout Collect CD. After several attempts, it was determined that Skout Collect would not boot this computer.
4. The Backtrack 5 DVD was used to boot this computer to ensure proper operation of the computer. Backtrack booted properly. However, when the “startx” command was entered, the screen went black, much like the Skout Collect boot CD behaved. Upon further examination, it was determined that this was a video driver issue and not directly related to the Skout Collect program. The vendor has been notified of this issue and expects to have a solution in the new version to be released in August 2012.

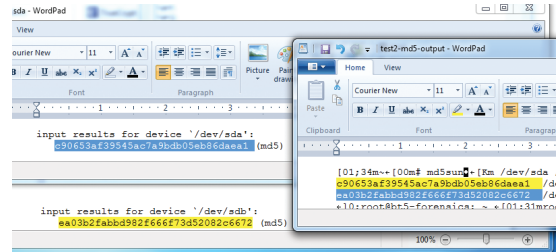
## Test – Multiple Hard Drives (32-Bit OS)

This test was performed on a custom home-built computer with two drives attached to the SATA inputs on the motherboard. There is no RAID configuration. The installed operating system is Windows 7 32-bit. The following steps were performed:



1. The computer was powered on. The “Del” key was pressed repeatedly to enter the computer’s BIOS configuration. It was verified that the CD/DVD drive was configured to boot first. The Skout Collect CD was inserted into the drive and the computer was restarted.
2. Once booted, a window appeared that stated “Please insert the output drive(s) now, and press ENTER.” The Skout drive was connected to a front-mounted USB port and enter was pressed.
3. The error message, “No valid external hard drive was detected, please connect a valid SKOUT Drive and try again,” was received. The drive was then connected to a rear-mounted (directly on the motherboard) USB port and enter was clicked. It was later determined that this was an issue with this particular computer’s USB ports and not an issue with Skout.
4. The EULA appeared and was accepted. The screen asking for case information was displayed and “Test: 2 Internal Drives” was entered for the name. All other fields were left blank. “Ok” was clicked.
5. The copy progress status bar appeared and indicated that Skout Collect would finish in about one hour and 35 minutes. Once completed, an output hashing status bar was displayed. Once the hashing status bar completed, another copy progress window was shown, with an estimated time of two hours and 32 minutes. Once again, a hashing status bar appeared. Both times the hashing progress windows took about as much time for copying as the progress bar did.
6. After completion, a window was displayed indicating that no corrupt sectors were found and 383 GB were copied.
7. The computer was booted with Backtrack 5 and the hash value of the two drives was calculated and recorded with the script command.

8. The Skout drive was plugged into the Windows 7, and the TrueCrypt was accessed as per the previous test. The hash values recorded by Backtrack and Skout were compared and found to match.



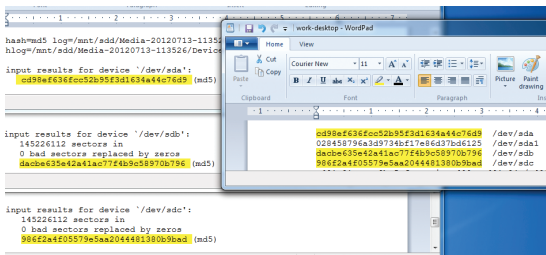
9. The computer was booted to its native OS, Windows 7 32-bit, TestDisk was executed, and the drive information was found to match the Skout Collect captured info. Both drive images were mounted read-only using FTK Imager, and the size comparison was the same. Furthermore, both drives could be browsed with Windows Explorer and contained all of the expected data.

## Test – Multiple Hard Disks-Raid Array-Windows 64-Bit

The following test was performed on a custom-built computer with three hard drives running a 64-bit version of Windows 7. One of the drives is the operating system drive and is connected to the computer via IDE cable. The other two drives are configured using a SATA RAID controller. For this test, the following steps were performed:

1. The computer was booted with the Backtrack 5 DVD. The hash values of all the drives were recorded using the “Script” and “md5sum” command.
2. The computer was then powered off.
3. The computer was booted using the Skout Collect CD. When prompted, the Skout external hard drive was connected. The EULA was agreed to. The form was completed with “work-desktop” as the case name. The progress bar appeared. This computer was allowed to run overnight.

- The next morning Skout collect had completed. The drive was removed and the system powered down.
- The Skout drive was connected to a Windows 7 computer and the TrueCrypt volume was mounted using the previously configured password as in the previous tests. The hash values of the Skout output for all three drives was compared to the Backtrack result and it was observed that they matched.



- The hard drive parameters and size of the drives were also found to match.
- The IDE drive image could be mounted and viewed with FTK Imager. However, the RAID drives would have to be reconstructed using appropriate tools. There is every expectation that these drives imaged correctly since the MD5 hash values and drive parameters matched.

## Test – Macbook Air With Solid State Drive

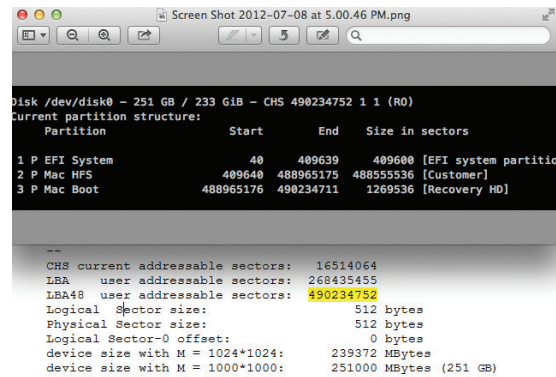
This test was to determine if Skout Collect would function correctly on a Macbook Air equipped with a solid state 256 GB drive.

The following steps were performed:

- An Apple branded Superdrive (external CD/DVD drive) was connected to the USB port of the Macbook Air.
- The Macbook Air was powered on, with the alt/option key held down. A Backtrack 5 CD/DVD was inserted into the Superdrive. Once the bootup

selected screen appeared, the CD/DVD drive was selected. Backtrack was booted and the Macbook Air's internal storage hashed. The Macbook Air was then shut down.

- The Macbook Air was powered on holding the alt/option key. The Skout Collect CD was inserted into the Superdrive. Once Skout booted, the screen was very fuzzy and difficult to read. The EULA was agreed to and "Macbook-Air-Test" was entered for the case. The progress bar appeared but was not readable due to the graphical errors. The vendor expects a fix to be released in August 2012.
- The test completed screen was displayed and the computer was powered down. The Skout drive was plugged into the Windows 7 computer and the TrueCrypt volume mounted. The hashes, drive vs. image sizes and addressable space vs. hard disk parameters all matched.



## Live Imaging Tests

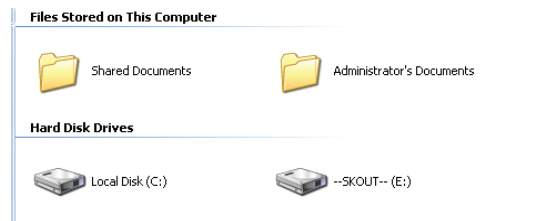
In preparation for the live tests, the Skout Enterprise CD was booted. Within the drive preparation process, it is possible to "reclaim" space that has not been used, adding it back to the purchased licensed space from Skout Forensics. As a test, one drive was manually formatted before attempting this. It was not possible to reclaim the unused space on this drive. It is always recommended that Skout drives be prepared and formatted only with the Skout Enterprise program. Both drives were then prepared using all available space.

It is important for an investigator to understand that collecting data from a live system will impact the target system. Any action, even as simple as plugging a USB drive into a computer, will cause the underlying operation system to access system files, potentially overwriting information and changing date and time stamps. Ideally, these actions will not affect user-generated data, such as documents, picture files or e-mail. This impact is typically minimal and an investigator will have to weigh the pros and cons to an investigation. Furthermore, it is also worth noting that operating systems are constantly doing things behind the scenes and may access or update files at any time.

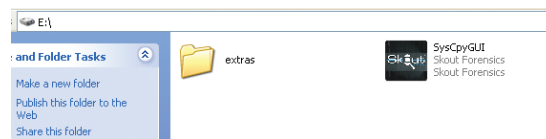
## Test – Virtual Machine Live

This test was performed to determine the effectiveness of Skout on a live system. This test is being performed on a VMware session to generate screenshots and to easily perform an analysis of the memory impact of the live collection of Skout. For the testing of the live imaging system, the following steps were performed:

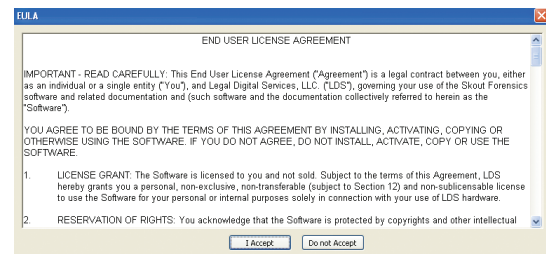
1. The virtual machine was booted with the Skout Collect ISO file. Skout was used to create an image of the drive as performed in previous tests with a name of “Baseline.” This will serve as the baseline for the file system change analysis.
2. The native operating system, Windows XP SP3 32-bit, was booted in the virtual machine. The machine was shut down. The virtual machine was then booted with the Skout Collect ISO file, and an image was created as in previous tests with the name of “Base-Start-Stop.” This image will be compared to the baseline to eliminate any file system changes that occur from just booting and shutting down the operating system.
3. The Virtual Machine was then booted using the native operating system. The Skout external drive was connected to the computer and connected to the Virtual Machine. Windows then installed a driver for this drive and mounted the Skout drive as drive letter “E:.”



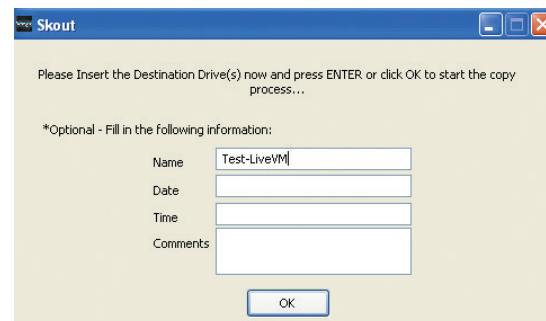
4. Within the drive, a folder and a program “SysC-PYGUI” were present. “SysCPYGUI” was double-clicked.



5. The EULA was displayed and agreed to.

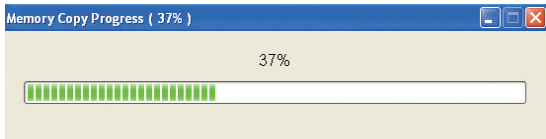


6. The following screen was displayed. This was similar to the case information from the Boot CD tests. “Test-LiveVM” was entered for the name and “Ok” was clicked.

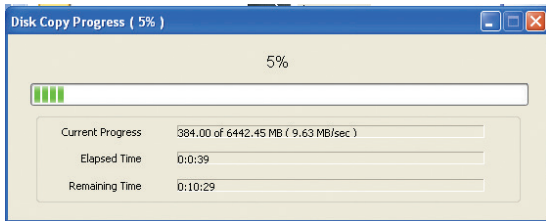


7. A status bar indicating the progress of the memory collected was displayed.

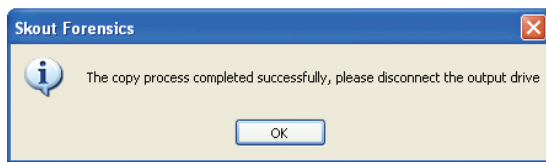




- Once the memory was collected, a progress bar indicating the status of the disk copying progress was displayed.



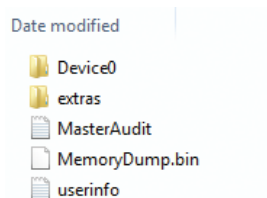
- Once the drive collection process was completed, a window appeared instructing the user to disconnect the Skout drive. The Skout drive was disconnected.



### Test Results

The Skout drive was connected to the Windows 7 VMware session for analysis of the collected data. The Skout drive was mounted using TrueCrypt as in the previous tests.

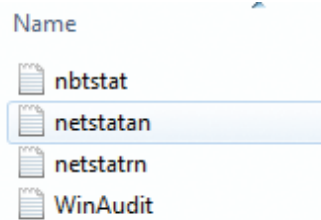
Several folders and files were noticed in the collection folder.



The “MasterAudit” file contains details of the system and the steps performed by Skout Collect. The “MemoryDump.bin” file is the contents of the memory

of the system at time of collection. The “Userinfo” file contains the manually entered details of the case during collection.

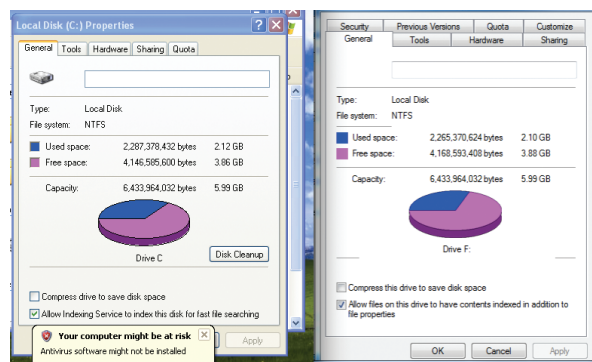
The “Extras” folder contains information such as active network connections and an audit of the Windows system, including installed software, at the time of collection.



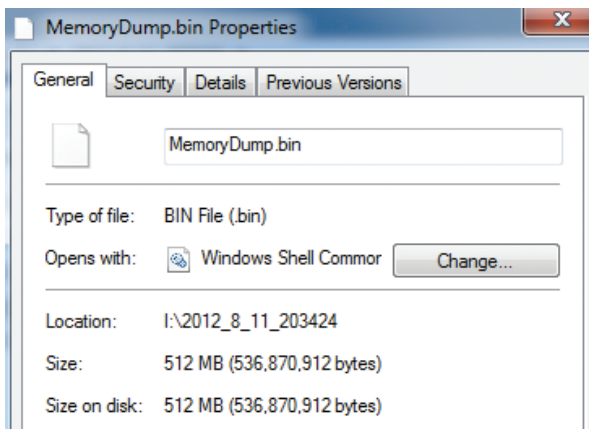
The “Device0” folder contains the image of the hard drive.

| Size       | Date modified |
|------------|---------------|
| Device.000 | 2,000,000 KB  |
| Device.001 | 2,000,000 KB  |
| Device.002 | 2,000,000 KB  |
| Device.003 | 291,456 KB    |
| Device0    | 1 KB          |

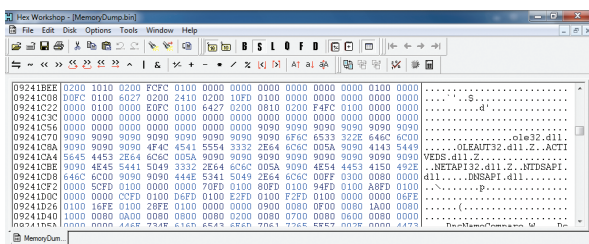
The image files were then mounted as a local drive using FTK Imager. Shown below is a screenshot of the virtual machine’s drive that was imaged vs. the properties of the mounted imaged drive. Notice in particular that both drive sizes are identical. Also, browsing the mounted image showed all data that was expected to be present.



The memory dump file's properties were viewed. The virtual machine was configured to use 512 MB of RAM. Since 1 MB is actually representative of 1,048,576 bytes, it can be seen here that the memory image is the expected 536,870,912 bytes.



Using a hex editor to browse the memory file revealed the names of many running processes.



The Skout drive was then plugged into a forensic workstation. The drive image was processed using FTK. All files that had an accessed, modified or created time after Skout was started were bookmarked. From the analysis, six files were created.

| File Name             | Full Path   |
|-----------------------|---|
| TP PS Driver 18BD...  | VMWare\Part_1\NDNAME-NTFS\WINDOWS\system32\spool\drivers\w32x86\31TP PS Driver 18BD068C9... |
| SYSCPYGUI.EXE...      | VMWare\Part_1\NDNAME-NTFS\WINDOWS\Prefetch\SYSCPYGUI.EXE-1074EE60.pf                        |
| ZZA.EXE-09F6315E...   | VMWare\Part_1\NDNAME-NTFS\WINDOWS\Prefetch\ZZA.EXE-09F6315E.pf                              |
| TRUECRYPT.EXE...      | VMWare\Part_1\NDNAME-NTFS\WINDOWS\Prefetch\TRUECRYPT.EXE-0418D58A.pf                        |
| MEMORY.EXE-00...      | VMWare\Part_1\NDNAME-NTFS\WINDOWS\Prefetch\MEMORY.EXE-00595A1F.pf                           |
| PerfMon_Perfdata_8... | VMWare\Part_1\NDNAME-NTFS\WINDOWS\Temp\PerfMon_Perfdata_804.dat                             |

Five of the files created relate to Windows performance caching, primarily the Prefetch system. The sixth file was found to be related to VMware print drivers.

Furthermore, 164 were modified (Including the six that were created). Upon analysis it was concluded that these were all system files, such as the Windows memory paging files, registry changes and system restore files. Also, 80 additional files were accessed during this process, including the Windows registry, page files and driver files. No user data was found to be modified, changed or added during this process. This is a relatively small impact on the system considering the power of Skout.

The original baseline drive images were also analyzed and similar file system activity was discovered, indicating that Skout Collect's impact was minimal.

## Test – Toshiba E205 Laptop Live Collection

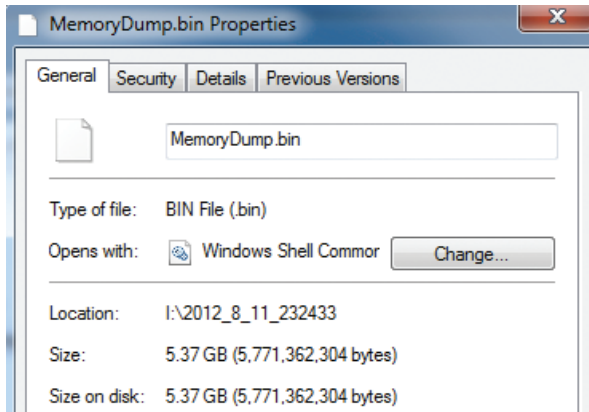
This test was performed on the Toshiba laptop that was previously tested using the boot CD. The following steps were performed:

1. The Toshiba laptop was booted into Windows 7. The Notepad application was opened and the following sentence was typed: "this is a test."
2. The Skout drive was connected to a USB port.
3. "SpyCPYGUI" was double clicked. The screens were clicked though as in the previous test.
4. The Skout drive was disconnected.

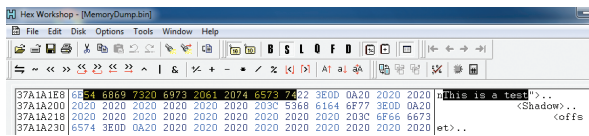
## Results

The Skout drive was then connected to another computer. The file size of the drive image matched what was expected. The memorydump.bin file was much larger than the expected 3,904 MB (4,093,640,704 bytes) reported by the laptop's operating system. This is a result of Skout using HBGary as the memory collection engine. In short, the user addressable space of memory includes all hardware on the computer's bus. A more detailed explanation of this can be found at:

<http://www.hbgary.com/winddexe-almost-there-but-not-quite->



Hex Workshop was used to open the memory image and “This is a test” was search for and found. Note: The notepad entry was never saved to a disk.



Review of the files that had been accessed, created or modified revealed similar results to the previous test and no user data was created, altered or accessed.

## Test – Live Test of Windows 7 Desktop With Multiple Drives

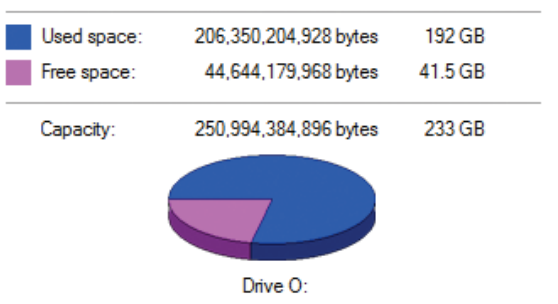
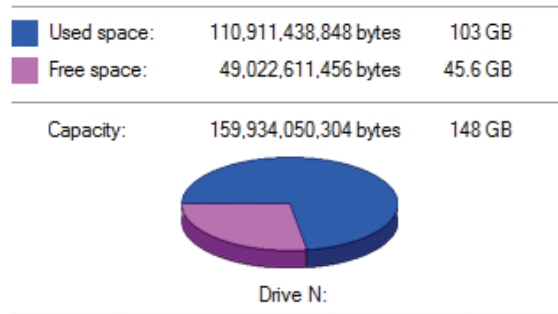
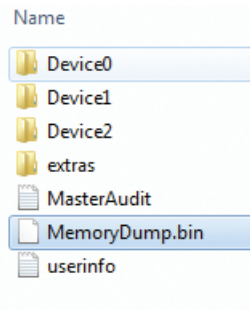
This test was performed on the same custom-built desktop (Windows 7 32-bit) as previously imaged with the Skout Collect CD. For this test, the following steps were performed:

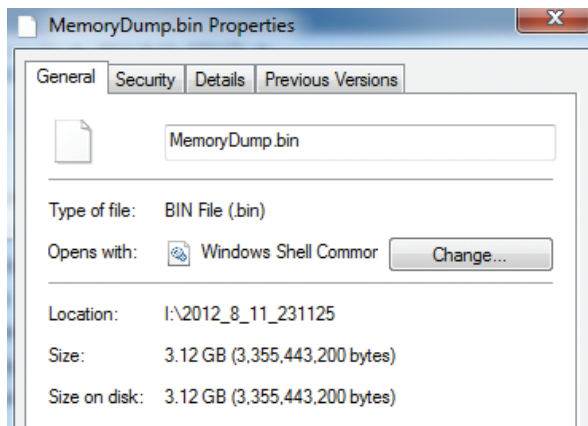
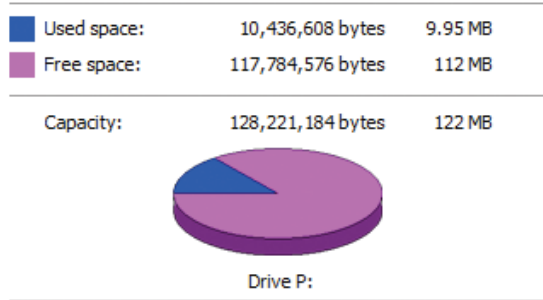
1. The test computer was booted normally into Windows 7.
2. A 128 MB USB drive was plugged into the front facing USB port of the computer.
3. The Skout collection drive was connected to a rear USB port of the computer

4. “SysCPYGUI.exe” was double clicked and the collection process was completed as in the first live test.

## Results

The Skout drive was then connected to another computer. The TrueCrypt partition was accessed as before. All drive images were mounted.





The file size of the drive images and the RAM image matched what was expected, including the attached external USB thumb drive.

Review of the files that had been accessed, created or modified revealed similar results to the previous test and no user data was created, altered or accessed.

## Conclusion

Skout Collect and Skout Enterprise performed as advertised in most instances. During the Skout Collect CD test, only the Toshiba laptop was not able to be imaged, due to a graphics driver issue. There was also a graphical issue with the MacBook Air that could be worked around. The vendor has been informed of these graphical issues and expects to have a fix released in August of 2012. All other tests performed as expected.

Skout Collect is an extremely simple to use program. Usually all that is needed to perform an acquisition is for a user to plug the Skout drive into the computer, boot from a CD if using the boot method, agree to the EULA, and enter some basic descriptive case information. Once those steps are completed, the software performs admirably imaging RAM (if using the live system) and any attached drives, minus the Skout collect drive. Given Skout's ease of use, a minimally trained user would find Skout Collect simple to operate.

Using TrueCrypt to secure the data, the Skout drives could be shipped and transported anywhere in the world with confidence that evidence is secure.

The speed of collection was surprisingly fast given that Skout uses the USB 2.0 standard. The 500 GB Toshiba laptop only took about 10 hours to fully image.

In addition, the VMware sessions were processed perfectly. Normally these VMware sessions are just used to capture screenshots of normal operation and some anomalies are expected. However, in these tests, no errors caused by the use of virtual machines were detected. This was a nonadvertised use of Skout Collect and a pleasant surprise.

In every instance that data was collected, the data collected matched what was expected. Skout Collect performed exceptionally well overall.