

Court File No. CV-14-507120

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

THE CATALYST CAPITAL GROUP INC.

Plaintiff

and

BRANDON MOYSE and WEST FACE CAPITAL INC.

Defendants

SUPPLEMENTARY AFFIDAVIT OF MARTIN MUSTERS
(sworn April 30, 2015)

I, MARTIN MUSTERS, of the City of Oakville, in the Regional Municipality of Halton, MAKE OATH AND SAY:

1. I am the Director of Forensics at Computer Forensics Inc. (“CFI”), a computer security consulting firm based in Oakville, Ontario. In this capacity, I am responsible for all aspects of CFI’s computer forensic services.

2. I previously swore affidavits in this proceeding on June 26, 2014 and on February 15, 2015. Since the swearing of my February 15, 2015 affidavit, I have reviewed the affidavits of Brandon Moyse (“Moyse”) and Kevin Lo (“Lo”) affirmed on April 2, 2015. This affidavit is sworn in reply to those affidavits.

“Cleaning” a Computer’s Registry does not Hide Web Browsing Activity

3. In his April 2 affidavit, Moyse states that he “cleaned” the registry of his computer before turning it over to be imaged for a forensic review in order to “fully” erase his World Wide Web activity.

4. This explanation makes no sense. A computer’s registry does not store information concerning a user’s Web browsing history. The most common data relating to a Web browser

application such as Google Chrome or Microsoft Internet Explorer that is stored in the registry are the application's settings, which likely include a pre-set start page when the application is first launched. Other settings include set preferences or extensions added to the application.

5. Thus, unless Moyses's start page for his Web browser was a pornographic site, he would have no reason to "clean" his registry if his only reason for doing so was to attempt to hide his Web browsing activity.

The Secure Delete History is Stored in the Registry and Can be Deleted

6. The Lo affidavit states that Moyses's computer registry did not contain a Secure Delete Log, which one would expect to find if someone had used Secure Delete. I cannot verify that information without reviewing the images of Moyses's computer myself. However, assuming this fact to be true, that fact is insufficient to support Lo's conclusion that the Secure Delete program was not used to delete any files or folders from Moyses's computer.

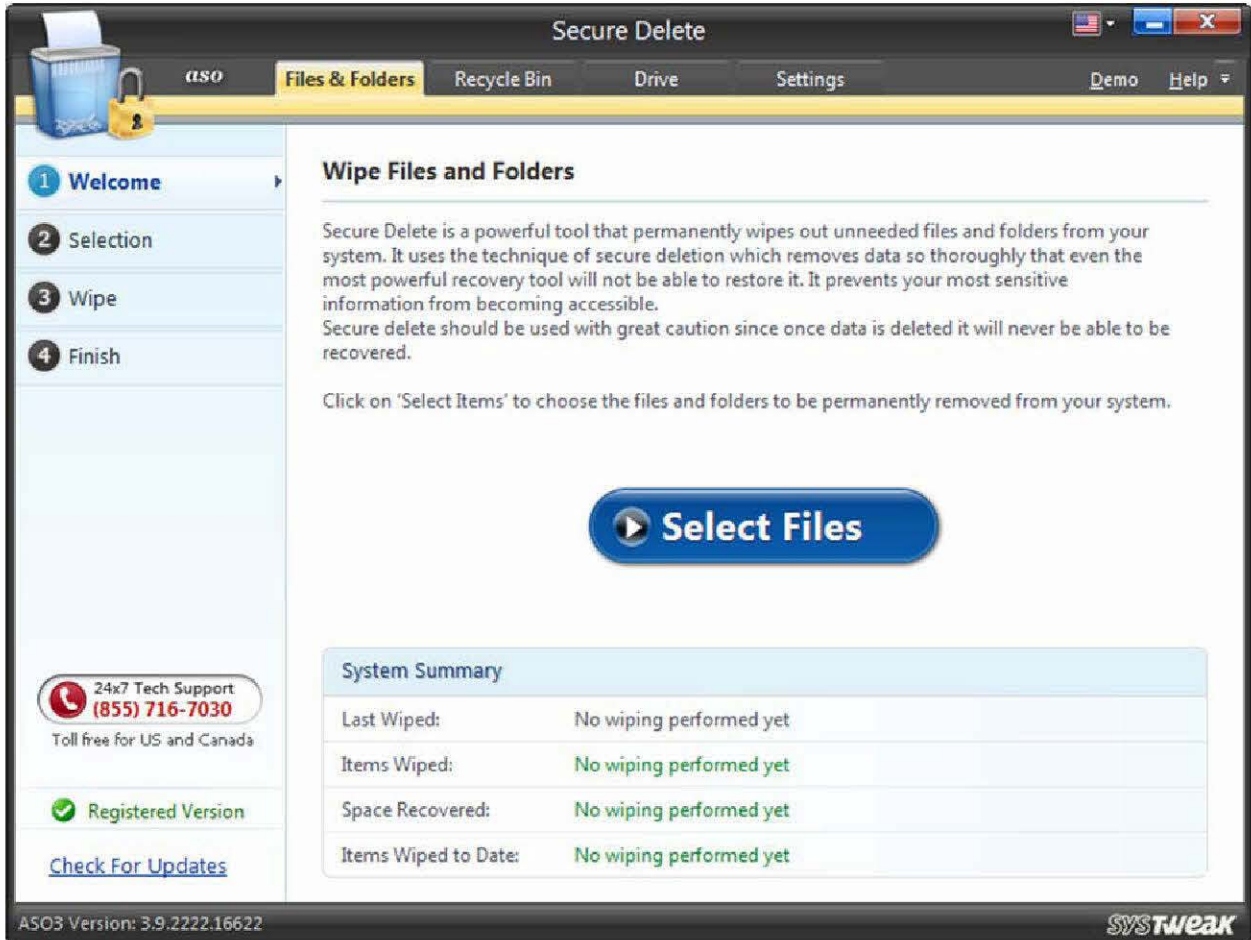
7. Lo's conclusion is based on the absence of a Secure Delete Log in the registry and a screenshot of the Secure Delete system summary for Moyses's computer.

8. In fact, it is a relatively simple matter to "reset" Secure Delete to hide any trace of having run the program. A simple internet search on how to delete the remanent files of Advanced System Optimizer (the software program that contains the Secure Delete tool) from a computer's registry. This publicly available information walks a user through the steps necessary to open the registry, identify the Secure Delete files, and delete those files so as to remove all traces of the user having run Secure Delete to delete files without a trace.

9. I am not surprised that Lo did not find any evidence of a Secure Delete Log on Moyses's computer, because Moyses, who admitted to conducting research relating to the computer registry, could very easily have deleted the Secure Delete Log after he deleted folders or files from his computer.

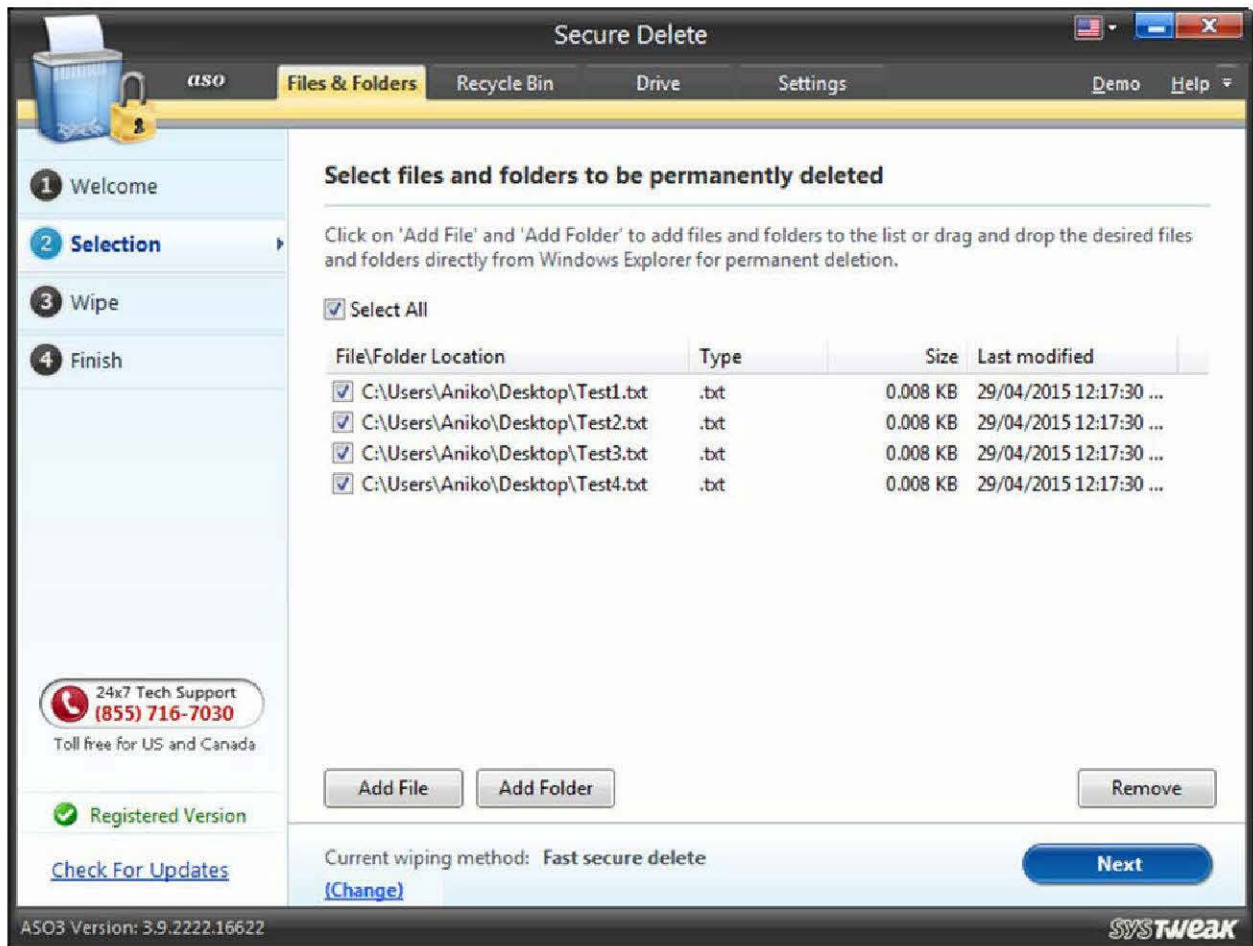
10. To demonstrate how easy it is to “reset” Secure Delete, I conducted a test on a computer on which I used Secure Delete to delete test files and then reset the Secure Delete system summary by deleting the Secure Delete Log from the computer’s registry.

11. In my test, I began by opening the Secure Delete tool, as shown in the following screenshot:

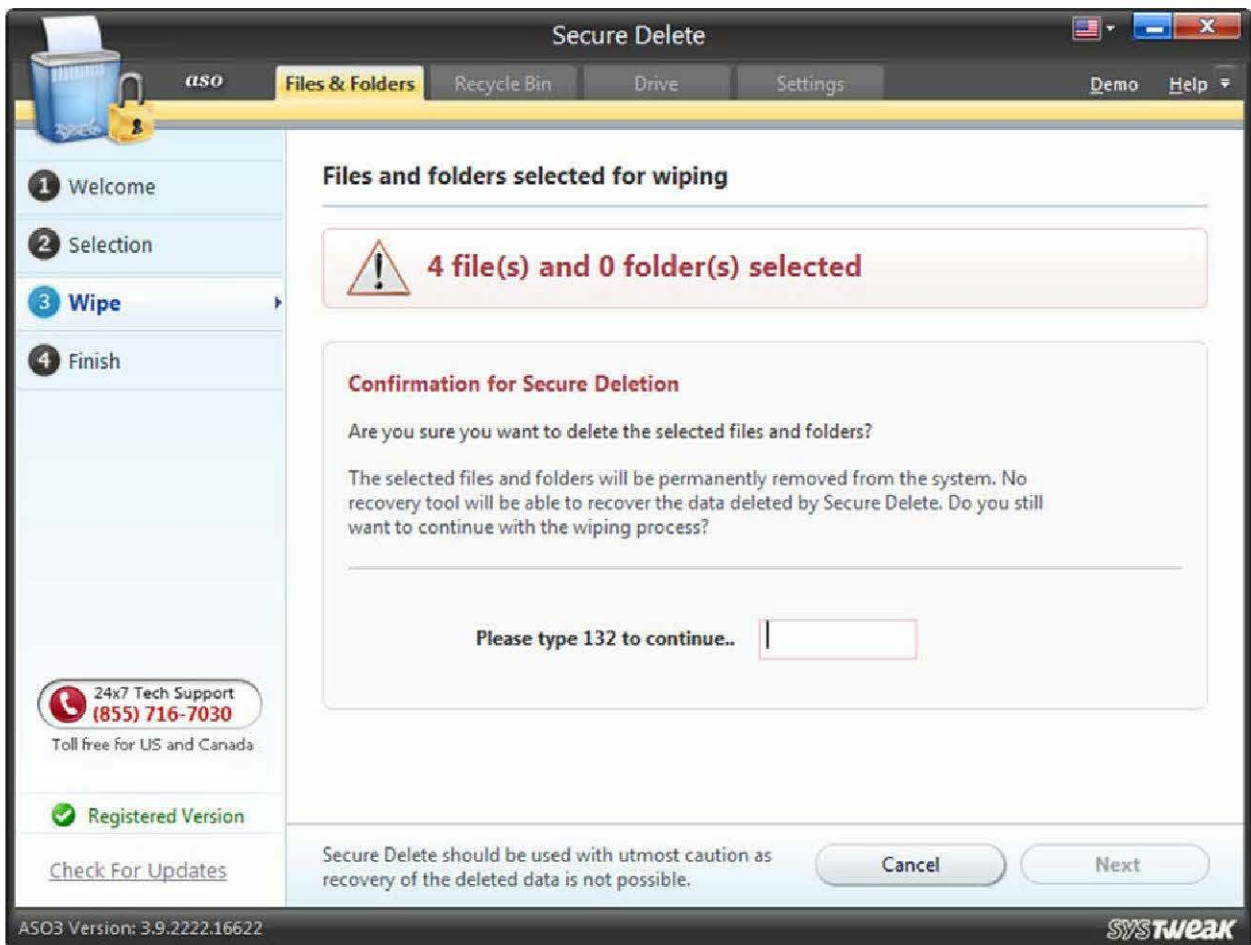


12. This screenshot shows what the Secure Delete system summary looks like before the program has been run.

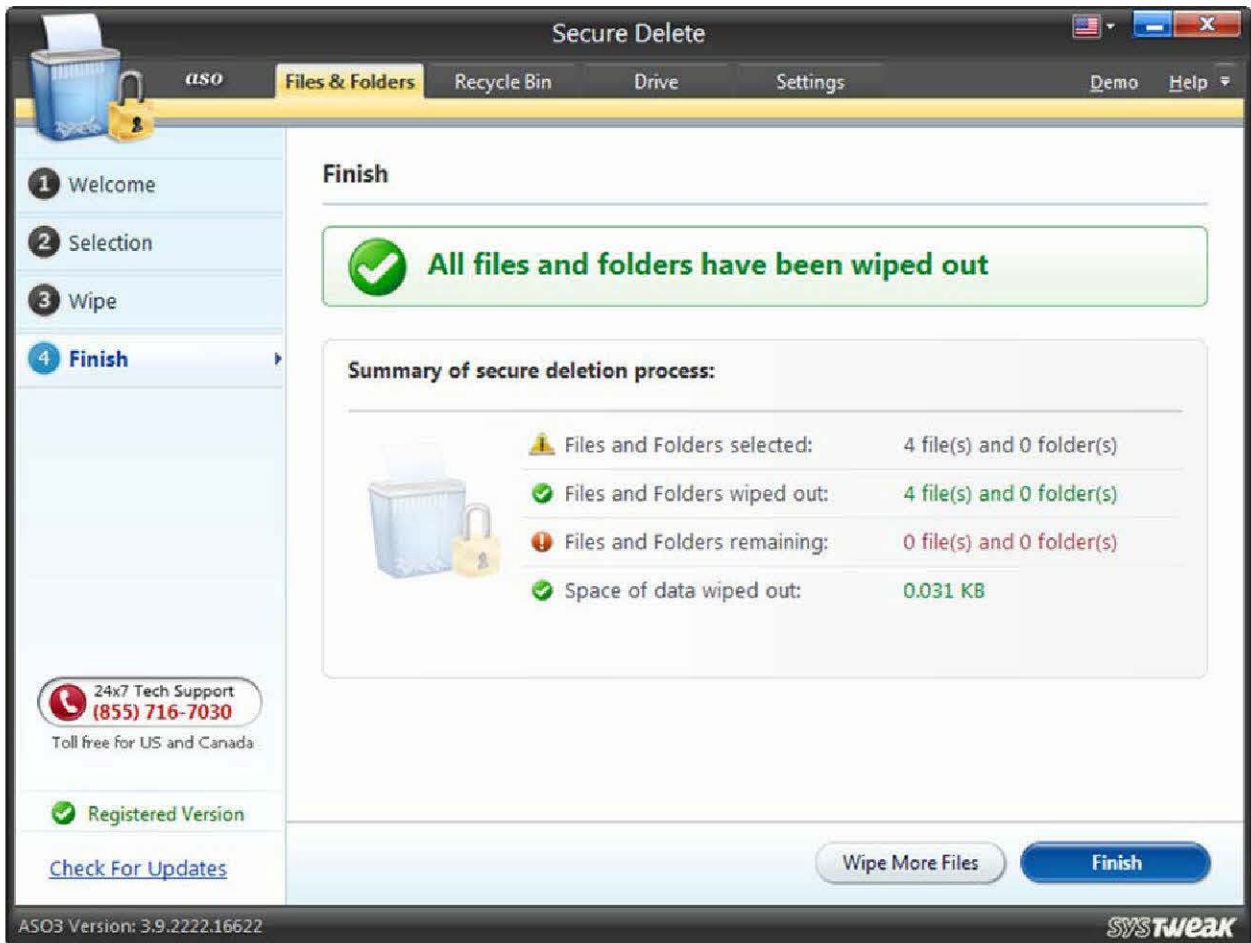
13. Next, I added four documents to the list of documents that I wanted to delete using the Secure Delete tool:



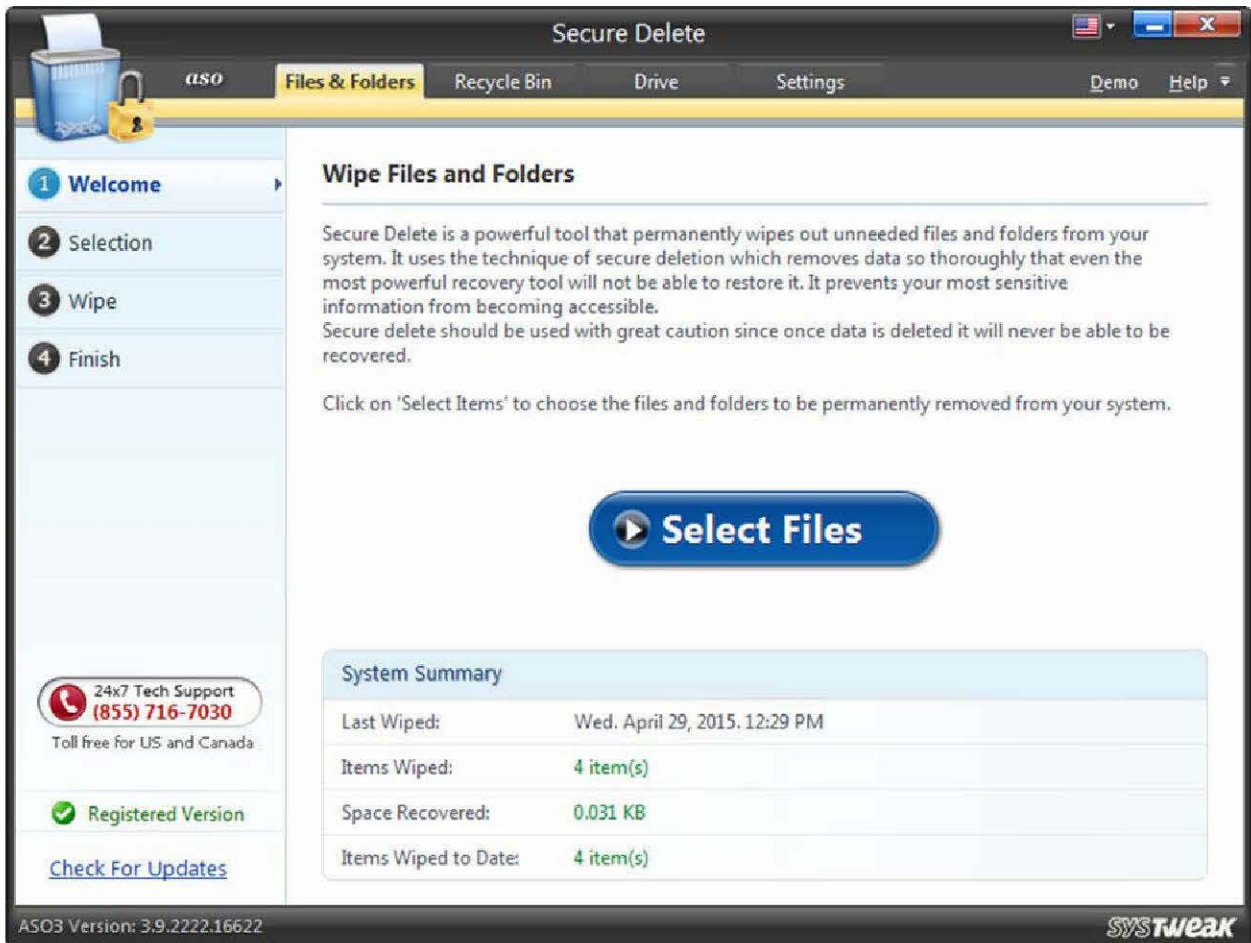
14. After clicking on the “Next” button in the bottom-right corner, the program asked me to confirm that I wanted to permanently delete the files:



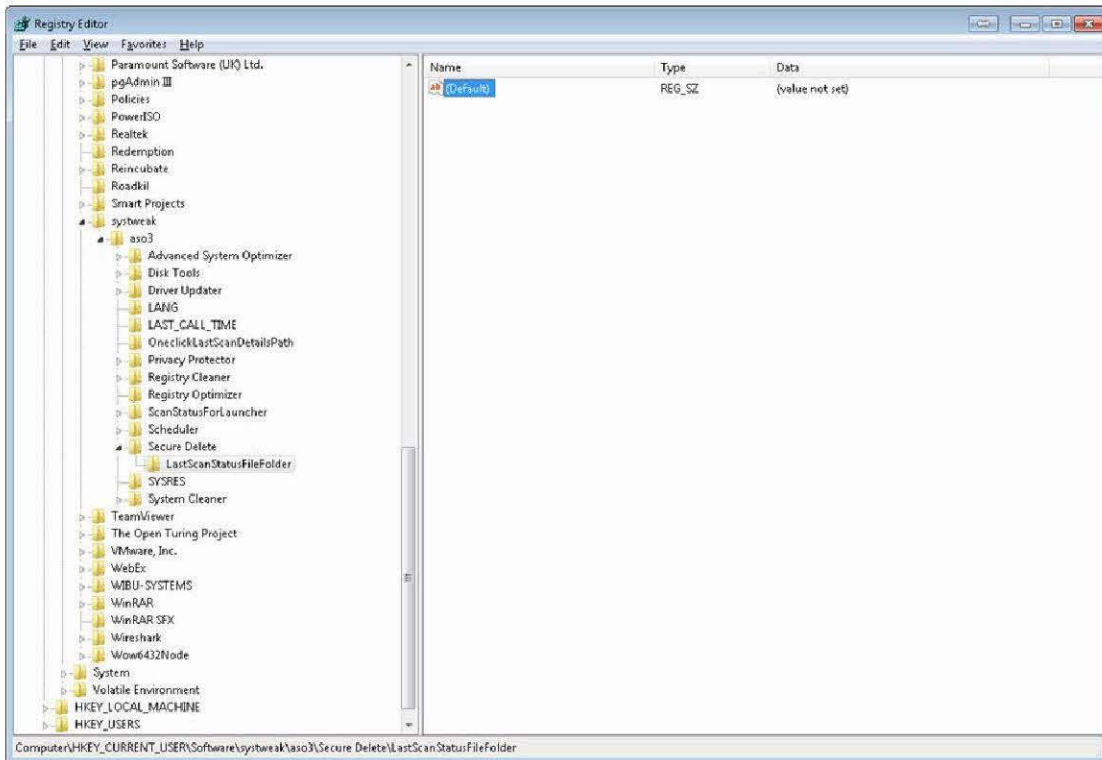
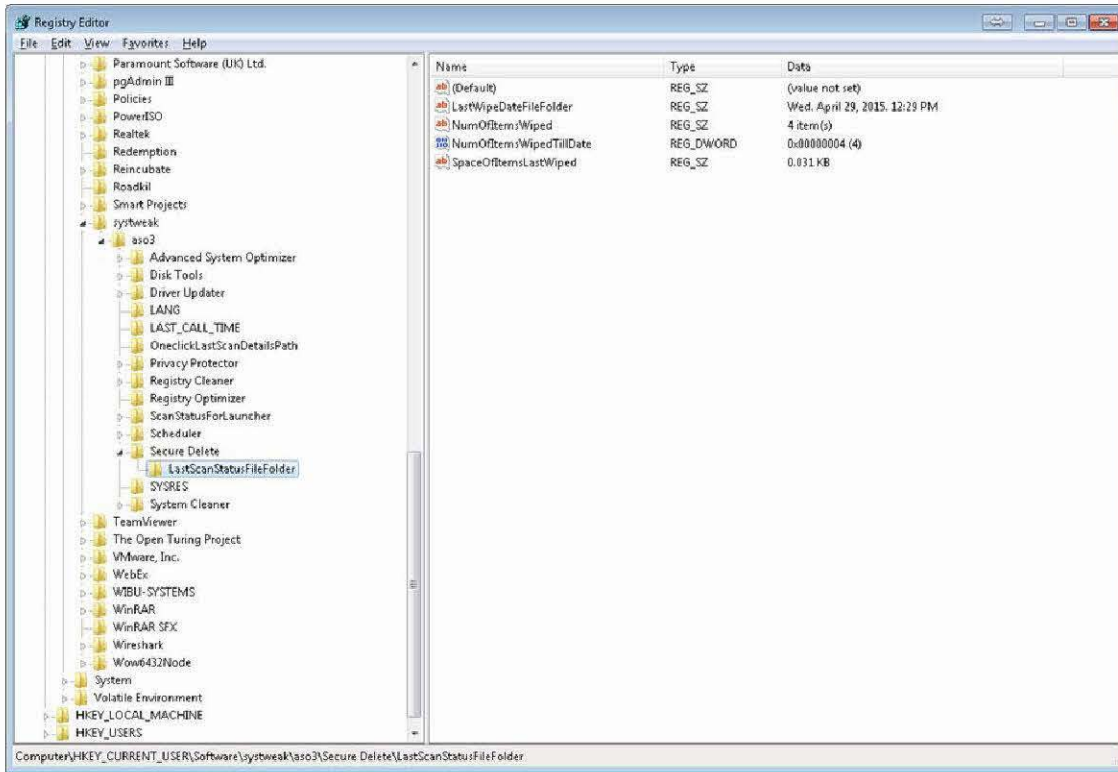
15. The user has to type “132” into the dialogue box and click “Next” to permanently delete the files. After doing so, the confirms the user’s activity:



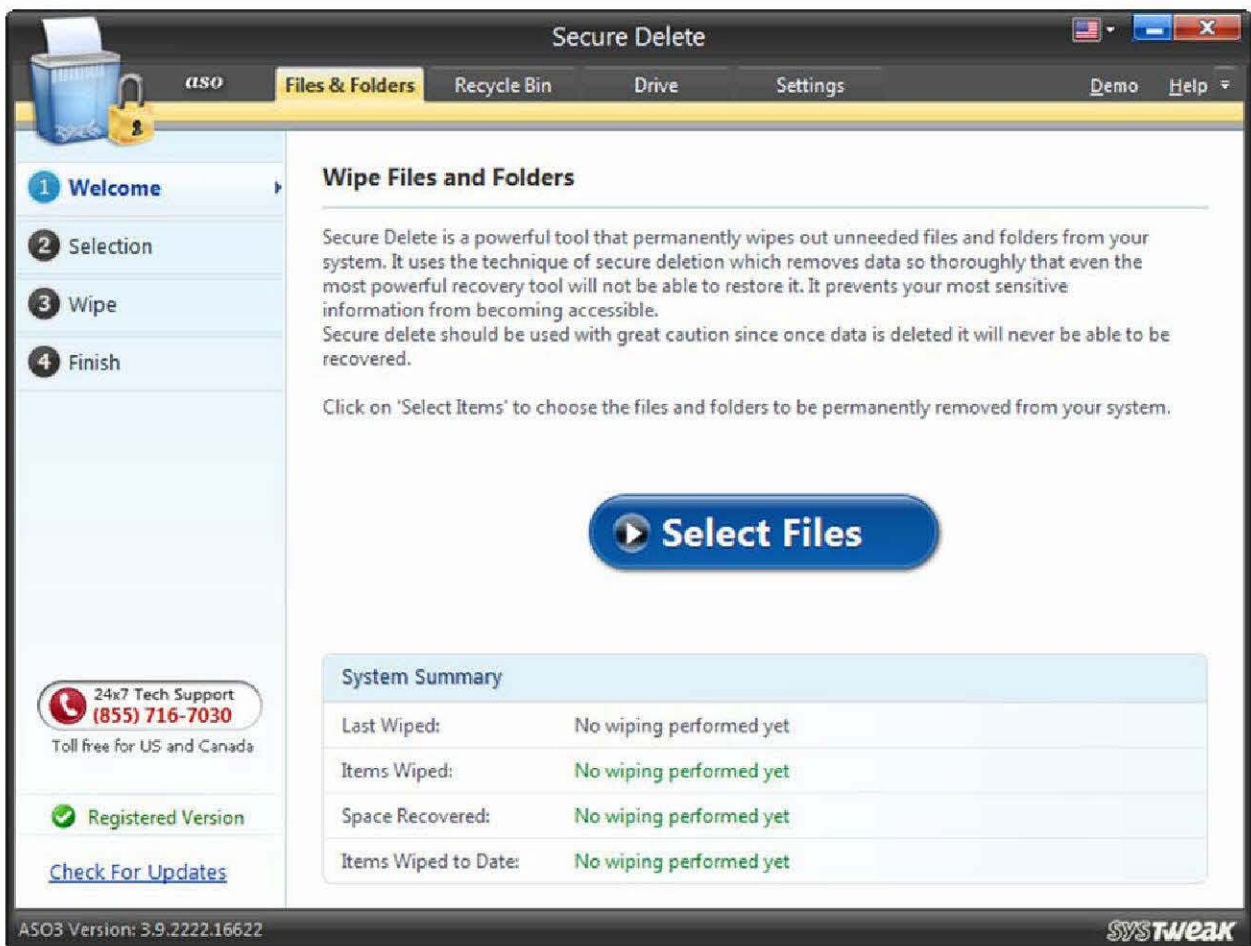
16. Clicking on “Finish” brings the user back to the start page, this time with the system summary updated to reflect the recent deletion activity:



17. As shown above, the system summary recorded the fact that I had deleted four files from the test computer. In order to “reset” this summary, I opened the Registry Editor, selected the Secure Delete folder, and deleted its contents, as shown in the following two screenshots:



18. After deleting the Secure Delete registry information, the program's system summary reset itself to appear as if no wiping activity had been performed:



19. Thus, the fact that Lo did not find any evidence of wiping activity does not mean that no such activity took place. Moreover, because deletions to the registry leave no trace, it is impossible to determine whether the absence of wiping history in the Secure Delete system summary means that Moyses did not use the software to permanently delete files or folders or whether he used the software and then removed the evidence of his having done so by deleting the Secure Delete files from his registry.

20. In my experience as a computer forensic IT investigator, the most likely conclusion to draw from Moyses's conduct of June and July 2014 is that he did in fact use Secure Delete to permanently delete files from his computer on July 20, 2014. I base this conclusion on the following facts:

- (a) Prior to July 20, 2014, Moyse exhibited a pattern of conduct that is consistent with taking confidential information from his former employer, as set out in my June 26, 2014 affidavit and my evidence given during my cross-examination held August 1, 2014;
- (b) Moyse's admitted conduct of investigating how to "clean" his registry displays a level of IT sophistication that exceeds that of the ordinary user;
- (c) Moyse wiped the Blackberry smartphone that had been issued to him by Catalyst prior to returning it to Catalyst, thereby permanently destroying evidence of his phone and data usage at a time when he knew litigation would likely result from his conduct; and
- (d) The running of the Secure Delete program the night before Moyse was scheduled to deliver his computer to a forensic expert is too coincidental to be an innocent "mistake".

21. Based on the foregoing, while it is impossible to know for sure, it is my opinion that Moyse most likely did use the Secure Delete program on July 20, 2014 to delete files from his computer so as to prevent those files from being recovered by a forensic analysis of his computer by an independent supervising solicitor.

SWORN BEFORE ME at the City of
Toronto, in the Province of Ontario on
April 30, 2015



Commissioner for Taking
Affidavits, etc.

Andrew Winton



MARTIN MUSTERS

THE CATALYST CAPITAL GROUP INC.
Plaintiff

-and- BRANDON MOYSE et al.
Defendants

Court File No. CV-14-507120

**ONTARIO
SUPERIOR COURT OF JUSTICE**

PROCEEDING COMMENCED AT
TORONTO

**SUPPLEMENTARY MOTION RECORD
(MOTION RETURNABLE JUNE 11, 2015)**

LAX O'SULLIVAN SCOTT LISUS LLP

Counsel

Suite 2750, 145 King Street West

Toronto, Ontario M5H 1J8

Rocco DiPucchio LSUC#: 38185I

rdipucchio@counsel-toronto.com

Tel: (416) 598-2268

Andrew Winton LSUC#: 54473I

awinton@counsel-toronto.com

Tel: (416) 644-5342

Fax: (416) 598-3730

Lawyers for the Plaintiff

CAT000051/11

726