

Final Project Paper
Team Kappa
Keyloggers: Effective uses in Cyber Forensics & Hacking

IST 454
Spring 2011

James R. Crawford
Joshua Endter
Chris Javan
Ankit Jain
Joe Schneider
Glen Romonosky

Introduction:

Our project is **Keyloggers: Effective uses in Cyber Forensics & Hacking.**

We have chosen to focus on keyloggers because most students have very little experience with keyloggers. Many of the students who do have experience with keyloggers have not used them in the professional industry; thus, lacking the context of how and when they are used. It is also important for students to know which software keylogging programs are available, and most importantly how they are used.

Computer Forensics consists of the art of examining digital media to preserve, recover, and analyze the data in an effective manner. [1] Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keyloggers are especially effective in monitoring ongoing crimes. Keystroke loggers are available in software or hardware form, and are used to capture and compile a record of all typed keys. The information gathered from a keystroke logger can be saved on the system as a hidden file, or emailed to the hacker/forensic analyst. Generic keystroke loggers typically record the application name, time and date when the application was accessed, as well as all keystrokes associated with the application. Advanced keystroke loggers have many additional features. Our chosen keylogger has the following features [2, 18]:

- Monitors Keystrokes
- Monitors sent and received emails
- Logs events in a timeline
- Logs internet chat conversations

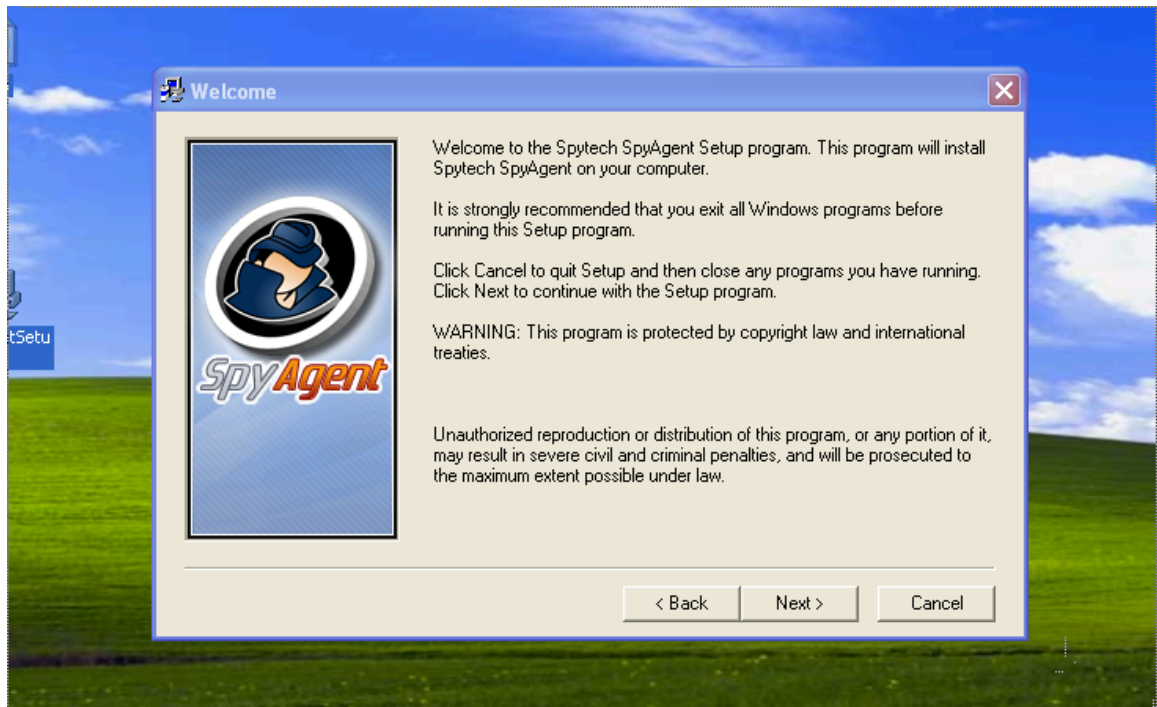
Captures screenshotsKeystroke loggers have the advantage of collecting information before it is encrypted; thus, making a forensic analyst's job easier. Through our research, we have selected the best keylogger: SpyTech SpyAgent. Our video conveys the implementation, use, and data analysis of the logger through a voice-overed tutorial [21].

Tutorial Walkthrough:

See next page.



Step 1: Go to website, download SpyAgent.



Step 2: Click on executable and follow instructions



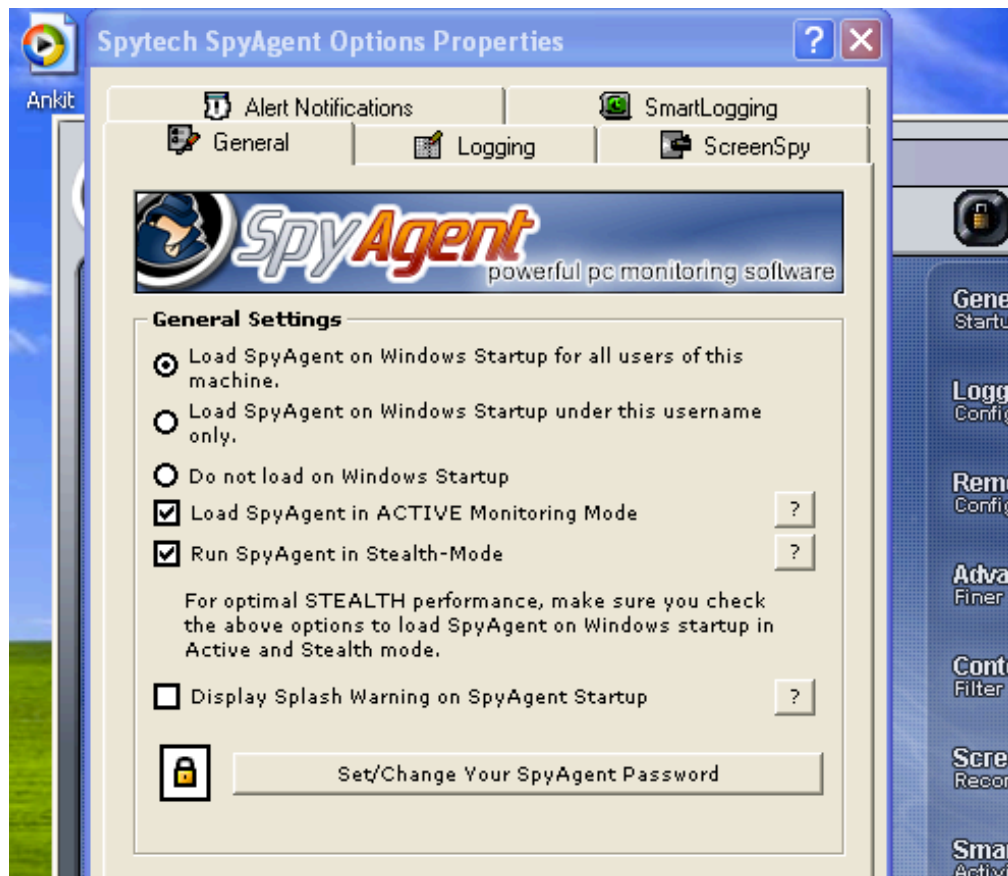
Note: Can choose to run in either Administrator or stealth mode

Note: The hot key combination for running SpyAgent is
CONTROL+SHIFT+ALT+M

Note: You can select in installation the time delay it takes for SpyAgent to open after Windows loads.



Step 2.5: Click "Program Options" at the bottom



Click the “Load SpyAgent on Windows Startup for all users of this machine” radio button.

Click “OK” or choose to monitor a specific user

Click “Run SpyAgent in stealth mode” radio button.



Click “Setup/Change Your SpyAgent Password” button at bottom, then enter your information and then click OK.

Click OK to accept Spytech SpyAgent Options Properties



Step 3: Click “Remote Log Delivery” in right-hand column

Step 4: Click “Send all Logs Via E-mail” radio button.

Step 5: In the “Send Mail too” text box, write desired e-mail

Step 6: Choose time interval for which you wish to receive the monitoring logs.

Step 7: Select “Send Keystroke Logs” radio button

Step 8: Select “Send Windows Log” radio button

Step 9: Select “Send Connections Log” radio button

Step 10: Select “Send Actions and Events Log” radio button

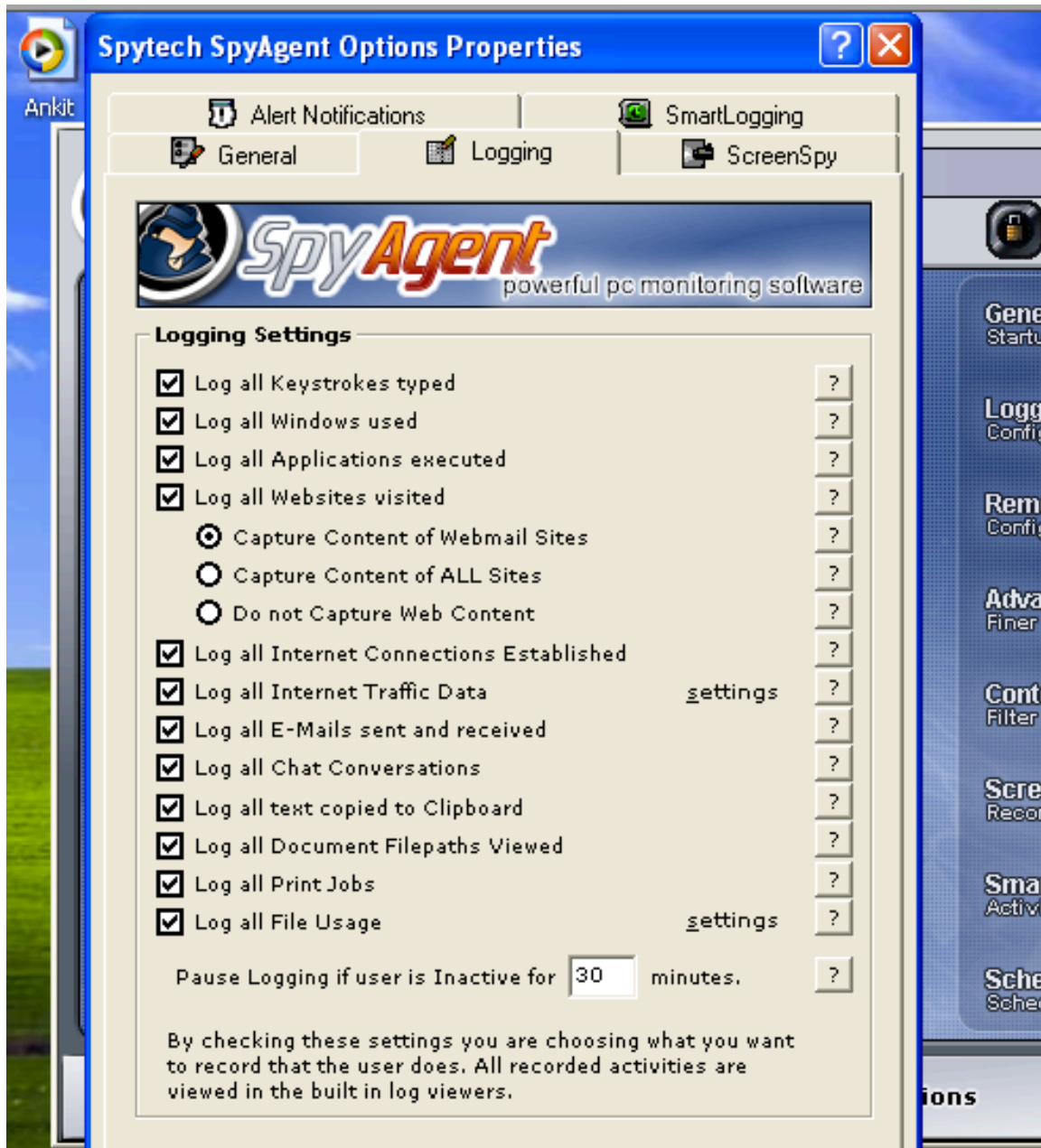
Step 11: Select “Send Snapshot of Current Desktop Log” radio button

Step 12: Select “Send Websites Log” radio button

Step 13: Select “Send Applications Log” radio button

Step 14: Select “Send Documents/Print Log” radio button

Step 15: Click OK



Step 16: Click the “Logging” feature button on the right-hand side.

Step 16.5: Click all radio boxes.

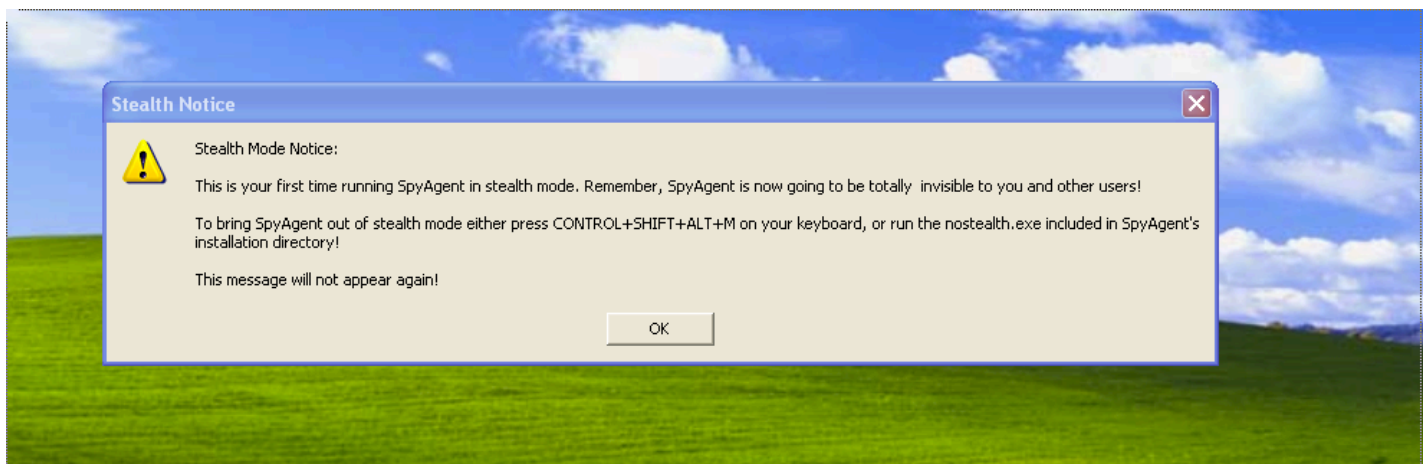
Click OK



Step 17: Click the “ScreenSpy” button on the right-hand side.

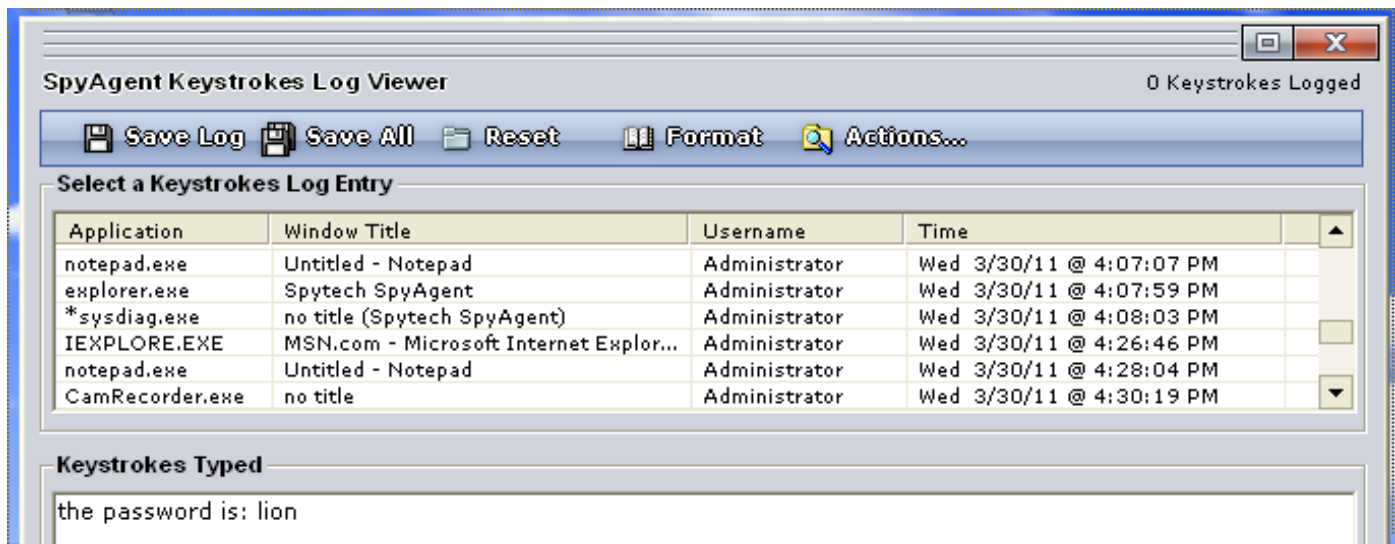
Step 17.5 Select the “Use ScreenSpy Logging” radio box. Choose where you would like to save your screenshots. For this demo, we will be using the default setting. Click OK.

Step 18: Click “Start Monitoring” in the lower left-hand corner. Enter your password



Step 19: Use the hotkey mentioned above

Step 21: Click OK

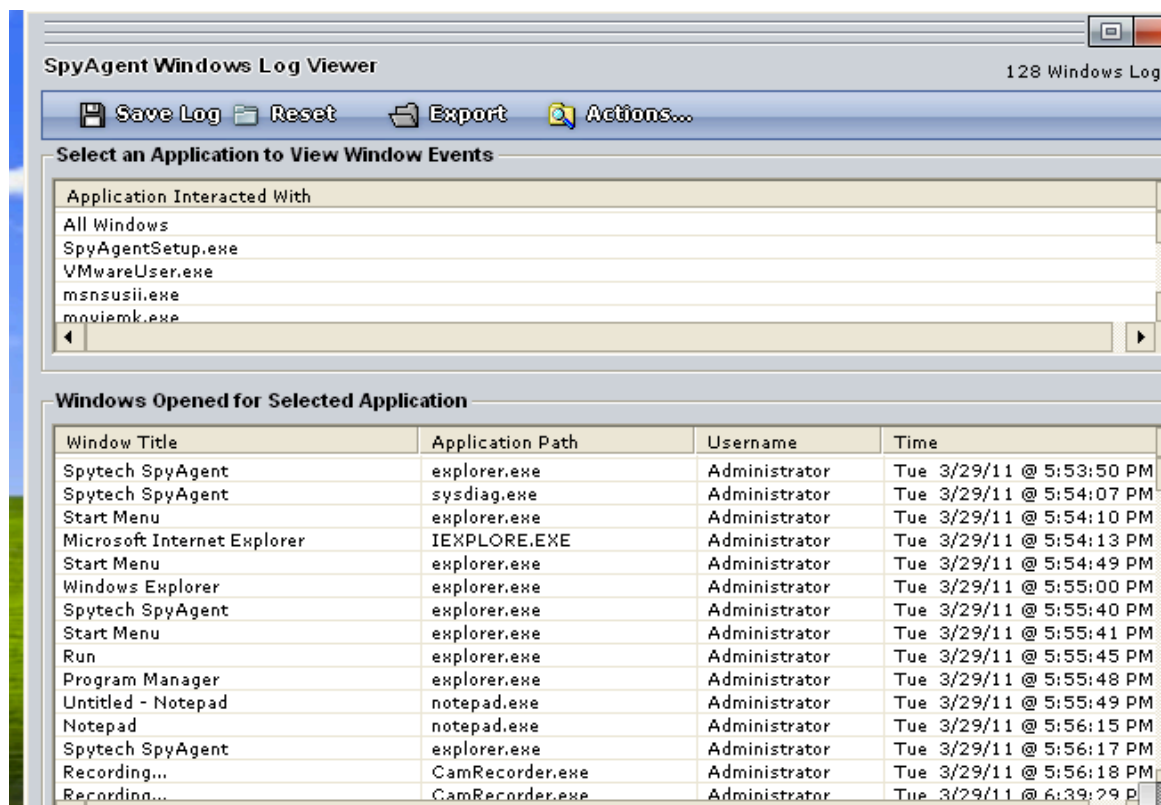


Step 22: Click “Keystrokes Typed” in the General user Activities window pane.

Step 23: Select the “Save Log” button at the top left of the page.

Step 24: Name the file “Keystrokes” and save it on the desktop

Step 25: Close the window



Step 26: Click the “Windows Viewed” button in the General user Activities window pane.

Step 27: Select the “Save Log” button at the top left of the page.

Step 28: Name the file “WindowsLog” and save it on the desktop

SpyAgent Applications Log Viewer				66 Applications Logged
<div> <div>Save Log</div> <div>Reset</div> <div>Execute</div> <div>Export</div> <div>Actions...</div> </div>				
Application Ran	Username	Start Time	End Time	
C:\WINDOWS\system32\notepad.exe	Administrator	Tue 3/29/11 @ 5:55:49 PM	Tue 3/29/11	
C:\WINDOWS\Explorer.EXE	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\VMware\VMware Tools\VM...	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\VMware\VMware Tools\VM...	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\WINDOWS\system32\wscntfy.exe	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\VMware\VMware Tools\TPA...	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\WINDOWS\system32\wuauclt.exe	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Fraps\fraps.exe	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\TechSmith\Camtasia Studio...	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\TechSmith\Camtasia Studio...	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\Spytech Software\Spytech ...	Administrator	Tue 3/29/11 @ 5:53:50 PM	Tue 3/29/11	
C:\Program Files\Spytech Software\Spytech ...	Administrator	Tue 3/29/11 @ 5:53:51 PM	Tue 3/29/11	
C:\Program Files\Internet Explorer\iexplore.e...	Administrator	Tue 3/29/11 @ 5:54:14 PM	Tue 3/29/11	
C:\WINDOWS\system32\notepad.exe	Administrator	Tue 3/29/11 @ 6:41:11 PM	Tue 3/29/11	
C:\Program Files\Internet Explorer\iexplore.e...	Administrator	Tue 3/29/11 @ 6:40:01 PM	Tue 3/29/11	
C:\WINDOWS\Explorer.EXE	Administrator	Tue 3/29/11 @ 6:39:29 PM	Tue 3/29/11	
C:\Program Files\VMware\VMware Tools\VM...	Administrator	Tue 3/29/11 @ 6:39:29 PM	Tue 3/29/11	
C:\Program Files\VMware\VMware Tools\VM...	Administrator	Tue 3/29/11 @ 6:39:29 PM	Tue 3/29/11	
C:\WINDOWS\system32\wscntfy.exe	Administrator	Tue 3/29/11 @ 6:39:29 PM	Tue 3/29/11	
C:\Program Files\VMware\VMware Tools\TPA...	Administrator	Tue 3/29/11 @ 6:39:29 PM	Tue 3/29/11	
C:\WINDOWS\system32\wuauclt.exe	Administrator	Tue 3/29/11 @ 6:39:29 PM	Tue 3/29/11	

Step 29: Click the “Programs Executed” button in the General user Activities window pane. Select the “View Applications Log” choice.

Step 30: Select the “Save Log” button at the top left of the page.

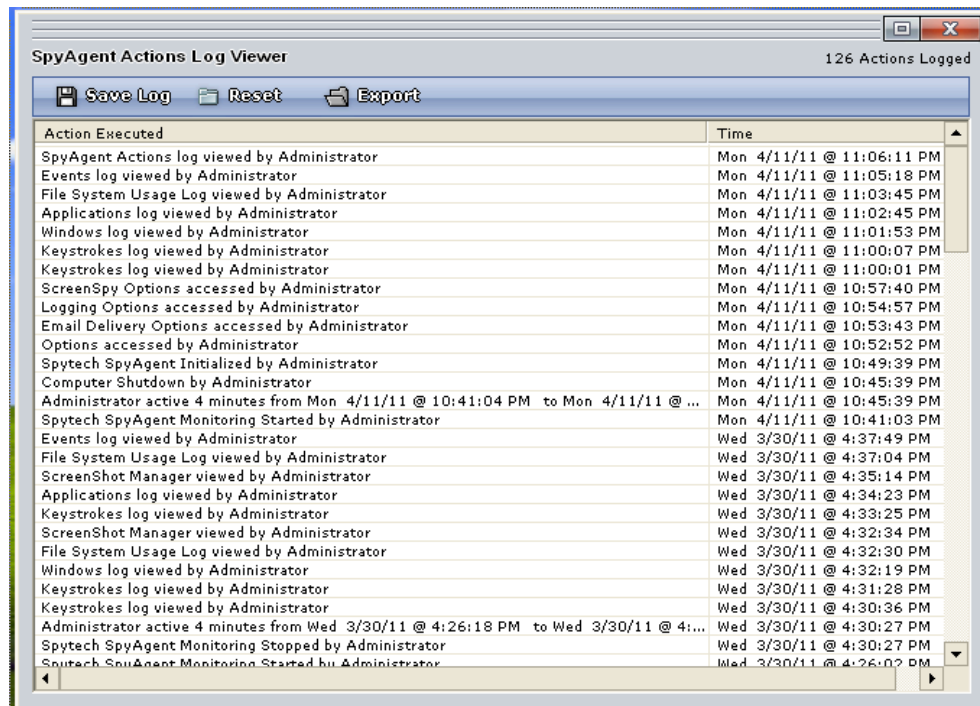
Step 31: Name the file “ProgramsExecuted” and save it on the desktop

Step 32: In order to receive the snapshots, create a folder called “Snapshots” on your desktop. Go to “My Computer” and then local disk C, documents and settings, all users, application data, and then AgentSS

Step33: Drag the images from the folder into the snapshots folder that was recently created on your desktop (this will allow for easy extraction when we move to analyzing the data)

Step 38: Select the “Save Log” button at the top left of the page.

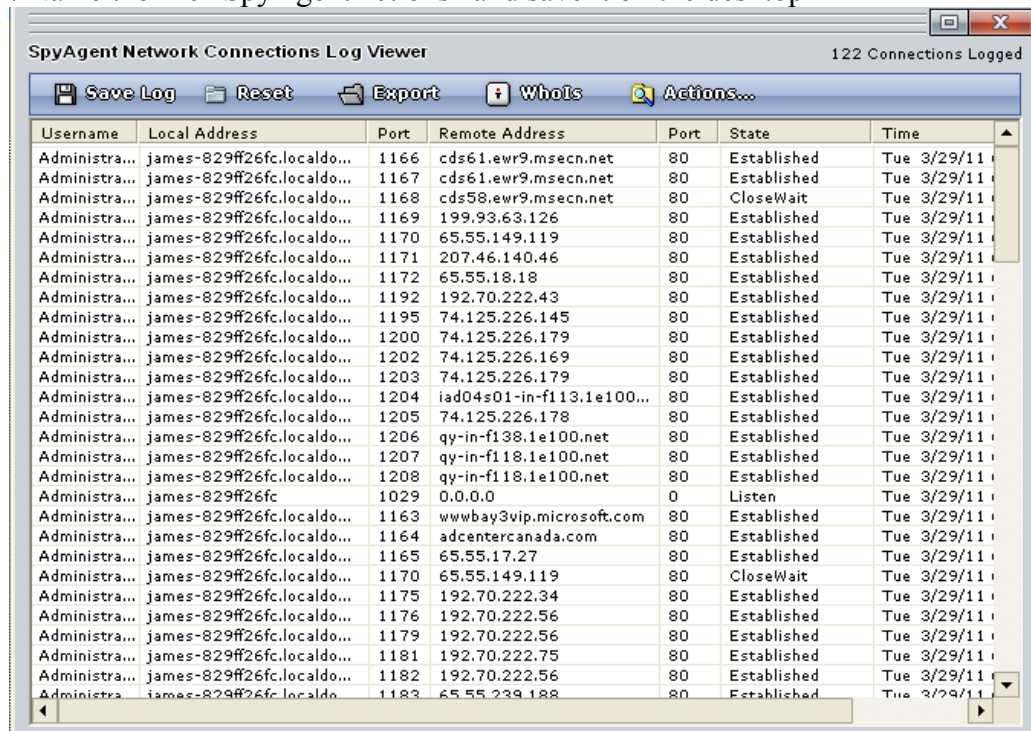
Step 39: Name the file “EventsTimeline” and save it on the desktop



Step 40: Click the “SpyAgent Actions” button in the General user Activities window pane.

Step 41: Select the “Save Log” button at the top left of the page.

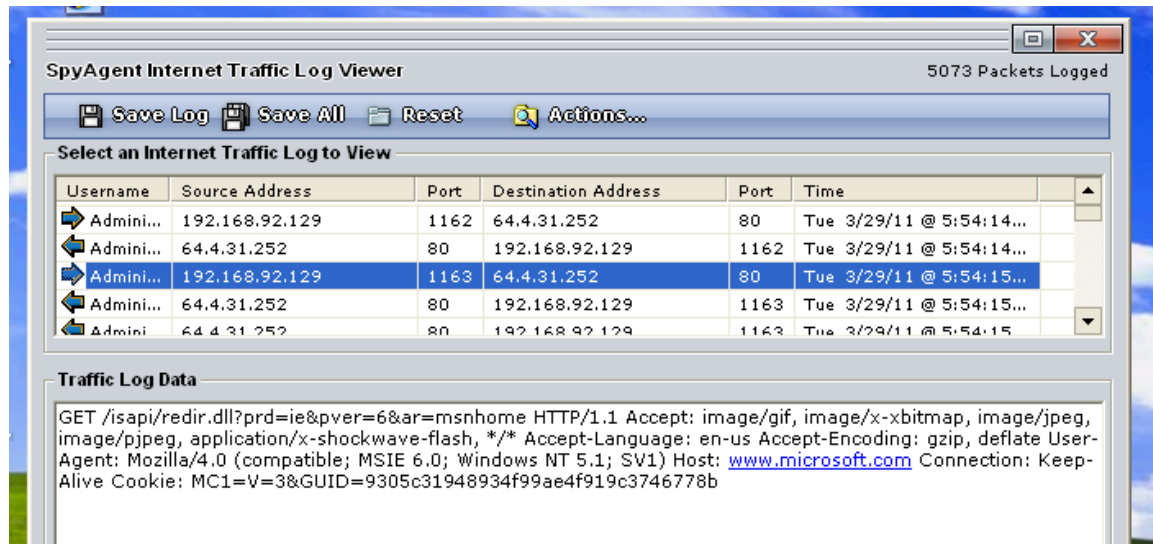
Step 42: Name the file “SpyAgentActions” and save it on the desktop



Step 43: Click the “Internet Activities” button in the Internet Activities window pane.

Step 44: Select the “Save Log” button at the top left of the page.

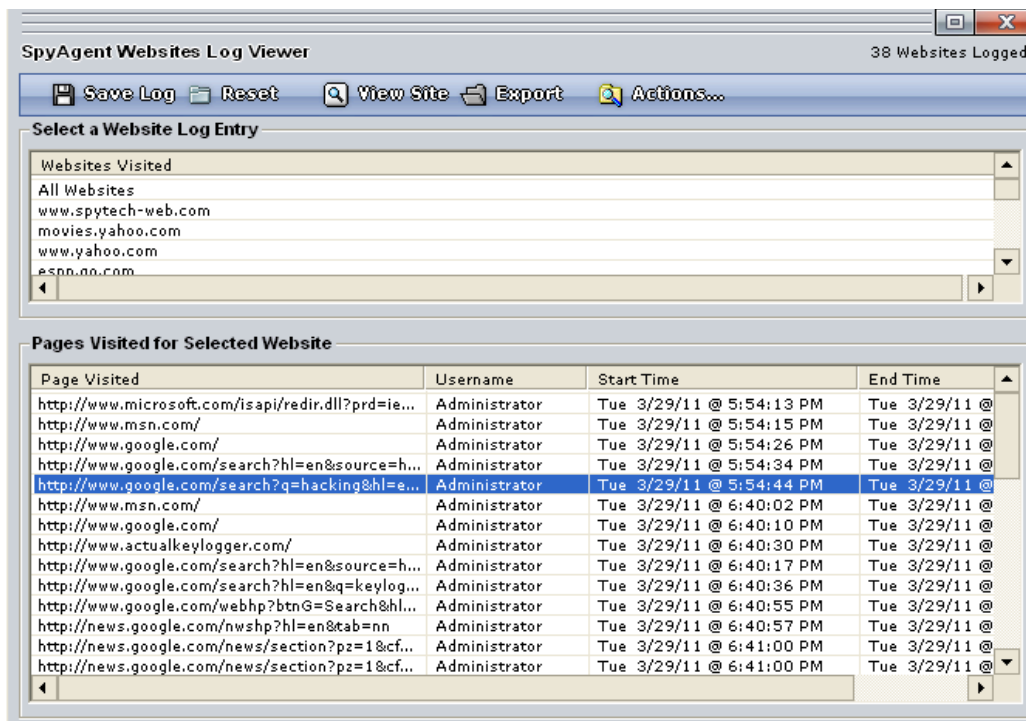
Step 45: Name the file “Internet Activities” and save it on the desktop



Step 46: Click the “Internet Activities” button in the Internet Activities window pane.
Select Internet Traffic Log choice.

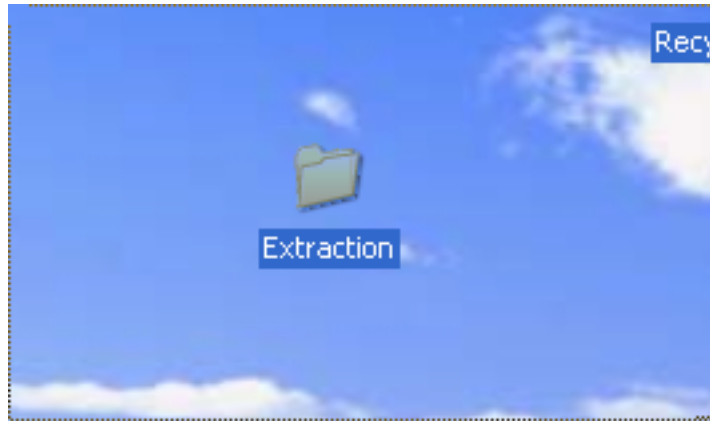
Step 47: Select the “Save Log” button at the top left of the page.

Step 48: Name the file “InternetTraffic” and save it on the desktop as an HTML file.



Step 49: Click the “Websites Visited” button in the Internet Activities window pane.

Step 50: Select the "Save Log" button at the top left of the page.
Step 51: Name the file "Websites" and save it on the desktop
Step 52: Click the "Internet Activities" button in the Internet Activities window pane.
Select Internet Connections Log choice
Step 53: Select the "Save Log" button at the top left of the page.
Step 54: Name the file "InternetConnections" and save it on the desktop



Step 55: On your desktop, create a file called "Extraction"
Step 56: Place all files created from previous steps into the "Extraction" folder
Step 57: Insert the USB jump-drive into the computer.
Step 58: Insert the "Extraction" folder onto the USB jump-drive
Step 59: Delete the "Extraction" folder from the desktop to cover your tracks
Step 60: End

References:

- [1] Michael G. Noblett; Mark M. Pollitt, Lawrence A. Presley (October 2000).
"Recovering and examining computer forensic evidence".
<http://bartholomewmorgan.com/resources/RecoveringComputerEvidence.doc>.
Retrieved 26 July 2010.
- [2] EC-Council. "System Hacking: Part III, Executing Applications." *Ethical Hacking & Countermeasures*. EC-Council, 2009. 859-928. Print. Courseware Guide V6.1 Volume 2.
- [3] "SC-KeyLog PRO - The Ultimate Keylogger for Monitoring Local and Remote Computers in Stealth." Welcome to Soft-Central.net. 2002. Web. 06 Feb. 2011.
<<http://www.soft-central.net/keylogger/pro.php>>.
- [4] "Revealer Keylogger Free Edition." Logixoft. 2009. Web. 06 Feb. 2011.
<<http://www.revealerkeylogger.com/>>.
- [5] "Handy-Keylogger.com - Invisible PC Monitoring Key Logger. Remote Software Spy Key Logger." Stealth Keylogger Download, Get Undetectable Key Logger Now.

2010. Web. 06 Feb. 2011. <<http://www.handy-keylogger.com/more-information.html>>.

[6] "Ardamax Keylogger - Invisible Keylogger with Remote Installation Feature." Invisible Keylogger, Application Launcher and Mouse Utility Download. 2011. Web. 06 Feb. 2011. <<http://www.ardamax.com/keylogger/>>.

[7] "Keystroke Recorder - All in One Key Logger for Computer Monitoring, Keystroke Logging, Mouse Recording, Keylogging." Keylogger Software - Download Powered Keylogger, Advanced Keylogger | Keyloggers. 2011. Web. 06 Feb. 2011. <<http://www.mykeylogger.com/keystroke-logger/powered-keylogger/>>.

[8] "Elite Keylogger Spy Software - Invisible Remote Keylogger Download. Capture Windows XP, 2000 Logon Password!" Elite Remote Keylogger Download, Get Best Remote Key Logger Now. Web. 06 Feb. 2011. <<http://www.elite-keylogger.com/elite-keylogger-spy-software.html>>.

[9] "Quick-Keylogger.com - More Information - Keystroke Recorder." Free Keylogger Download. Get Simple to Use Key Logger Now. Web. 06 Feb. 2011. <<http://www.quick-keylogger.com/more-information.html>>.

[10] Spy Keylogger - Stealth Keyboard Logger, Key Logger, Keylogger Software. Web. 06 Feb. 2011. <<http://www.spy-key-logger.com/>>.

[11] "Keylogger Download - Free Keylogger - "Perfect Keylogger" - Invisible Windows 7/Vista/XP Key Logger. Download the Best Parental Spy Software. Stealth Key Logger for Parents, Spouses and Their Kids!" BlazingTools.com - Perfect Keylogger Monitoring Software. Key Logging and Chat Recording Spy Software for Parents and Spouses! Web. 06 Feb. 2011. <<http://www.blazingtools.com/bpk.html>>.

[12] Comparison, Side. Invisible Keylogger - 2010 Keylogger Software Reviews & Download. Web. 06 Feb. 2011. <<http://www.invisiblekeylogger.com/>>.

[13] Keylogger - Actual Spy Software, Logs All Keystrokes. Keylogger Download. Web. 06 Feb. 2011. <<http://www.actualspy.com/>>.

[14] KeyLogger, Download KeyLogger, KeyStroke Logger, Parental Control Software. Web. 06 Feb. 2011. <<http://www.spytector.com/>>.

[15] "KeyLogger.com Invisible KeyLogger Stealth for Windows Vista/XP/2000." KeyLogger.com, Hardware and Software Key Logger, Undetectable Keylogger for Keystroke Recording. Web. 06 Feb. 2011. <<http://amecisco.com/iks2000.htm>>.

[16] "Ghost Key Logger Lite - a Free Keylogger That Invisibly Captures All Keystrokes to a Logfile. Download the Free Keylogger Yourself!" Sureshot Software -

Home. Web. 06 Feb. 2011.

<<http://www.sureshotsoftware.com/keyloggerlite/index.html>>.

[17] Remote Spy Software - RemoteSpy. Web. 06 Feb. 2011.

<<http://www.remotespy.com/>>.

[18] Spytech Spy Software - Computer Monitoring Software - Internet Recording.

Web. 06 Feb. 2011. <<http://www.spytech-web.com/spyagent-features.shtml>>.

[19] "Download Spy Software for Free!" Spy Software - 007 Local/Remote

Computer Spy Program and Monitoring Software. Web. 06 Feb. 2011.

<http://www.e-spy-software.com/spy_software.htm>.

[20] "ExploreAnywhere Spy Software - Spy Buddy." ExploreAnywhere Spy Software

- Computer Internet Monitoring Spy Software. Web. 06 Feb. 2011.

<<http://www.exploreanywhere.com/sb-features.php>>.

[21] "Keylogger & Spy Software Articles & Reviews, How to Identify a High Quality Keylogger? Dangers Children Face in the Internet, and the Solutions to These Dangers. Protect Your Family!" Keylogger Download Keylogger, Download Free Trial Keylogger. Keylogger Download, All In One Key Logger - Invisible (stealth) Best Keylogger. Download Spy Software & Vista/Win7 Keylogger, Key Logging Software! 2010. Web. 06 Feb.

2011.<http://www.relytec.com/keylogger_articles.htm>.