

Microsoft Windows Computer Forensics at Kansas State University

Author: Harvard Townsend, University IT Security Officer

Date last modified: February 20, 2008

Initial questions to ask

- *What kind of data does the computer store?*
 - If it stores confidential data, we have to be particularly thorough in the investigation and follow <procedures very carefully.
 - There may be cases where it is appropriate to run a tool like Cornell's Spider or UTexas-Austin's SENF (Sensitive Number Finder) to find all instances of confidential data.
- *Should I image the disk drive(s)?*
 - Imaging is important to preserve original evidence, esp. if it is a criminal investigation or it might end up in litigation, since forensics activities typically alter potential evidence like file access times. Ideally, you should immediately make a duplicate image of the original drive and do forensics on the duplicate. This may require installing the drive with the duplicated copy in the suspect computer and booting from the duplicate, so make sure that the drive used to make the duplicate has the same interface as the original (IDE, SATA, etc.). Label the original and store it in a locked, secure location.
 - If the computer stores confidential data, image the hard drive(s) and preserve the original since it may require forensics analysis to determine if the confidential data was compromised. If it is caught quick enough, network flow data can also be used to help determine if confidential data was accessed. CTS only keeps about 2 weeks of flow data.
 - The Technology Service Center in East Stadium (<http://www.k-state.edu/cts/tsc/>) has devices for making copies of hard drives - both software imaging and hard drive duplicating.
 - Imaging may not be necessary for all incidents.
 - Imaging is a challenge with a RAID configuration or disk storage on a SAN.
- *Should I turn the computer off, or unplug the network cable, or disable the wireless interface?*
 - Turning the computer off may destroy memory-resident evidence, so don't turn it off until you know it's safe to do so.
 - Unplug the network cable or disable the wireless network interface, then contact the University IT Security Officer to discuss next steps.
- *How quickly can I repair the computer and get it back into production?*
 - This may be particularly important if it is a production server providing critical services.
 - If the compromised system must be preserved for forensics analysis and/or evidence preservation, you may have to restore the service and data onto a different computer from backup media that was created before the compromise. You will also have to address the vulnerability that was exploited before putting the service back online. For example, this may involve applying a security patch.
 - Discuss this with the University IT Security Officer
- *What is required to recover from the compromise?*
 - Compromises that allow remote control of a computer such that arbitrary commands can be executed will require reformatting the hard drive and reinstalling the operating system and all applications from scratch or from backup media created before the compromise. This is the only way to guarantee that all malware has been removed.
 - The vulnerability that resulted in the compromise must also be addressed before the computer can be put back into production on the network. All security patches for the OS and applications must be applied.

- The University IT Security Officer decides when a particular type of compromise requires a reformat/reinstall.

General principles

- Contact the University IT Security Officer immediately if you suspect a security incident
- Inform your supervisor and department head
- Involve law enforcement if you suspect criminal activity; contact the K-State Police first
- The Office of the University Attorney may need to be notified as well; the University IT Security Officer can assist you with that.
- If you will be accessing someone else's files or e-mail, K-State policy normally requires written permission from the Vice Provost for IT Services (see <http://www.k-state.edu/policies/ppm/3455.html>)
- Document everything you do during the investigation, especially if it is a criminal investigation, internal personnel investigation, or student code of conduct violation
- Label evidence and store it in a secure location
- Beware of forensics activities that might alter evidence
- Do not start repairing the computer until cleared to do so by the University IT Security Officer

Preserving Evidence

- The problem with electronic evidence is that nearly all forensics techniques are destructive in some way. For example, when you view a file to see if it contains relevant evidence, the file access time is updated.
- It is best to “freeze” the hard drive(s) in their current state, make an image copy, and do forensics on the copy. Can re-image the copy from the original to restore pristine state for further analysis.
- This may not be necessary if it is not a legal or internal personnel investigation
- If you need to try to recover deleted files or file fragments, do a bit-by-bit copy of the entire hard drive, which copies every bit on the disk, not just the allocated blocks. This is sometimes called a “mirror copy.” Otherwise, copying just the actual data may be adequate (sometimes called a “smart sector copy”).
- “Chain of custody” (also called “chain of evidence”) tracks the history of the evidence from the moment it is seized to the time it is submitted to the court. In criminal cases, you must document the chain of custody to prove that what you are showing in court is exactly what you collected.
 - Normally, it is adequate to simply document the whereabouts of the evidence and who handled it at all times, keeping the evidence locked up when not in use, and being prepared to testify to that effect in court.
 - In sensitive criminal cases, it is best to digitally sign evidence files
 - You may also want the police to accompany you when performing forensics, or contract with a third party to perform the forensics analysis
 - Don't leave the evidence unattended where someone else could get access
 - Is helpful to have the police store the evidence
- Photograph the computer in its original location, and in the shop when you're ready to start your forensics analysis (front, back, sides). This is helpful for the chain of custody record
- Best practice is to have an “evidence bag” to transport and store things like tapes, USB thumb drives, CDs, etc. Store electronic devices in anti-static bags.
- Evidence may be in memory, not on disk, which is destroyed when you turn off the computer. Are techniques to dump an image of the memory before turning off the computer.
- If it is necessary to login to a computer and run an application as part of the investigation, replace the original hard drive with a copy and boot from the copy.

Procedures

These are in no particular order. The order you would follow depends on the nature of the investigation.

- a. *Check for confidential data* (SSNs or credit card numbers, for example)
 - Asking the user important, but inadequate as the sole source of information about the type of data on the computer
 - Cornell's Spider (<http://www.cit.cornell.edu/security/tools/>)
 - U. of Texas-Austin's Sensitive Number Finder (SENF - <https://source.its.utexas.edu/groups/its-iso/projects/senf/wiki/>)
 - These tools will modify file access times, so you may need to run them on a copy of the disk
- b. *Look for recently created/modified/accessed files*
 - Can restrict search to specific types of files or date ranges if you know what you're looking for
 - File times in Windows not 100% reliable, but can provide some clues
 - Depends on the file system type (NTFS records in UTC format so unaffected by time zone or DST; FAT file system based on local time of the computer)
 - Some updates to create/modify/access times may be delayed by the OS
 - Creation time is when it was first copied to that file system location
 - Many applications affect the file access time, like backup software
 - They can be modified by external programs to falsify the information
 - Be cognizant of time zone differences if trying to correlate file times to an event
 - Also check "My Recent Documents" (Windows XP) or "Recent items" (Windows Vista)
 - Is a set of shortcuts to recently changed documents
 - XP: "Documents" in Start Menu or in C:\Documents and Settings\username\Recent, or "My Recent Documents" in C:\Documents and Settings\username
 - Vista: Recent items" in Start Menu or C:\Users\username\Searches\Recent Documents or C:\Users\username\Recently Changed
- c. *Recover deleted files and file fragments*
 - Check the Recycle Bin
 - RestorerPro 2000 (\$\$)
 - Eraser and CCleaner are forensics enemies (and may indicate an attempt to hide info)
- d. *Check document metadata*
 - Author: in Microsoft Office documents/spreadsheets can be useful (Point to the file, click right mouse button, select Properties, then Details; in Office 2003: File->Properties->Summary; Office 2007: Office Button in upper left corner->Prepare->Properties)
 - Author defaults to the username logged into the computer where the file was first created; it is not changed by normal modifications to the document content, but can be changed manually.
- e. *Look for previous versions of a file* (Windows Vista only)
 - Windows Vista has shadow copying enabled by default
 - Point to a file, click right mouse button, choose "Properties", then "Previous Versions"
- f. *Use Google to research suspected malware or the symptoms* exhibited by the computer
 - May indicate file names to look for that the malware installs
 - Also registry keys, process names, open network ports to look for
- g. *Getting access without the account password*
 - Remove hard drive and mount it on a Linux system
 - Password removal software (runs Linux, accesses Windows file system, modifies the registry file)
 - Password cracking software like John the Ripper (<http://www.openwall.com/john/>). Note that Trend Micro OfficeScan deletes this program since it's considered a security threat.

- h. *Look for open ports and associated services that are unusual*
 - In a command window: netstat –an
 - netstat –nao includes process ID of listening process
 - netstat –b lists the EXE associated with the open port
 - Fport (<http://www.foundstone.com/us/resources/proddesc/fport.htm>) – freeware tool that gives more information than netstat
 - Nmap (<http://insecure.org/nmap/>) – versatile free scanning tool
 - Tcpview (<http://www.microsoft.com/technet/sysinternals/Utilities/TcpView.mspix>) is like a netstat GUI, but it also shows the remote address connected to that service.
 - DON'T SCAN OTHER COMPUTERS without permission
 - Port number assignments available at <http://www.iana.org/assignments/port-numbers>
- i. *Look at file shares*
 - In command window: net view [\\127.0.0.1](http://127.0.0.1)
 - Open file shares a common vector for infection, or exposure of sensitive data
- j. *Check for vulnerabilities which may indicate how the system was compromised*
 - Nessus (www.nessus.org) – very good freeware tool
 - Microsoft Baseline Security Analyzer (<http://www.microsoft.com/technet/security/tools/mbsahome.mspix>)
- k. *Look for unusual accounts*
 - Start->Run-> lusrmgr.msc
 - Select Users, look for any new, suspicious accounts
 - Select Groups, then Administrators. Look for accounts that should not have Administrator privileges
- l. *Check for accounts without a password, or with a weak password*
 - “John the Ripper” will quickly find weak passwords ((<http://www.openwall.com/john/>)). Note that Trend Micro OfficeScan deletes this program since it’s considered a security threat.
 - Start->Control Panel->User Accounts; does it say “Create a Password,” which means it doesn’t have one, or “Change my Password” which means it does.
- m. *Look for unusual processes*
 - Task Manager (Ctrl-Alt-Del -> Task Manager, or Start->Run->taskmgr)
 - Process Explorer from sysinternals (<http://www.microsoft.com/technet/sysinternals/Utilities/ProcessExplorer.mspix>)
 - Use Google to search for a process name to determine its function or if it is malicious
- n. *Check Scheduled Tasks to see if any have been added*
 - XP: Start->Programs->Accessories->System Tools->Scheduled Tasks
 - Vista: Start->Programs->Accessories->System Tools->Task Scheduler
 - Also check scheduled tasks log file (pull down the Advanced menu in the “Scheduled Tasks” window, and select “View Log”.
 - The log file is a text file: C:\WINDOWS\SchedLgU.txt
 - Windows commands “at” and “schtasks” (“at” tasks slightly different, don’t always show up in the list of tasks in the “Scheduled Tasks” window or the “schtasks” command.
- o. *Check the registry for programs that automatically start at boot time*
 - Run regedit.exe in a Windows command window, and search for (info courtesy of <http://www.absolutestartup.com/help/Winstart.htm>):
 - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** – these programs automatically start when any user is logged in. It is used for all users on this computer

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce** – The programs here start only once when any user is logged in and will be removed after the Windows boot process would have finished.
 - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx** – The programs here start only once when any user is logged in and will be removed after the Windows boot process would have finished. Also the RunOnceEx registry key does not create a separate processes. The RunOnceEx registry key also support a dependency list of DLLs that remain loaded while either all the sections or some of the sections are being processed.
 - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices** – these programs automatically start when the system is loading before the user logs in. It is used for service applications - antivirus, drivers etc. In Windows NT/2000/XP it could be canceled by admin to use other service startup sections. Read more at [services startup](#)
 - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce** – these programs automatically start only once when the system is loading as service application and items are deleted after the Windows boot process have finished.
 - Others listed at <http://www.absolutestartup.com/help/Winstart.htm>
- p. *Check browser cookies and cache*
- Check IE and Firefox, or any other browsers you find installed on the computer
 - There are commercial and freeware tools that simplify examining browser data
 - Internet Explorer:
 - Cookies are in c:\Documents and Settings\username\Cookies; each cookie is a separate file with the filename reflecting the website for which the cookie was set. View the folder in “Details” format to see file name and modify/create/access times.
 - History is in c:\Documents and Settings\username\Local Settings\History
 - Cache is in c:\Documents and Settings\username\Local Settings\Temporary Internet Files\
 - In Windows Vista, the Cache is in C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files\
 - With IE7, you can start the browser, pull down the Tools menu, select “Internet Options”, then the “General” tab. In the “Browsing history” section, select Settings to see the current location for the cache. To view the cache content, select “View Files”. This will list the cookies and the cache content in a normal Windows Explorer window where you can sort them by name, Internet address, date last accessed, do a search, etc.
 - Firefox
 - Files of interest are kept in the folder C:\Documents and Settings\username\Application Data\Mozilla\Firefox\Profiles\4u815odq.default (the last folder name in this path is unique to each installation). In Vista, they’re in C:\Users\username\AppData\Local\Mozilla...
 - Cookies are in a single text file named “cookies”
 - History is in the same folder in file named “history” – can view with WindowsVI, but it’s in “Mork” format ([http://en.wikipedia.org/wiki/Mork_\(file_format\)](http://en.wikipedia.org/wiki/Mork_(file_format))) so it’s not very intelligible when viewed with a text editor.
 - By default, Firefox only keeps history for 9 days
 - Bookmarks are in an HTML file named “bookmarks.html” in the same location. Load it into a browser to view
 - Cache is in a folder of that name; seems to only keep a few days of pages
 - You can view cache from within Firefox by entering “about:cache” as the URL
 - Stored passwords are in the same location, file signon.txt

- q. *Check Windows Event Logs*
 - On XP, are stored in c:\windows\system32\config
 - SecEvent.Evt = security event log
 - SysEvent.Evt = system event log
 - AppEvent.Evt = application event log
 - Event Log Viewer is in control panel, Administrative Tools, Event Viewer. Can launch from the command line with “eventvwr.exe”.
 - From the File menu in the Event Viewer, you can open a different log file to look at event logs from a different disk drive (like a boot drive moved from a compromised computer)
- r. *Check application or database logs* for access information, esp. if it is a server
 - Web server logs
 - Microsoft SQL Servers logs
 - Trend Micro logs
 - Any other major applications on that system
- s. *Check firewall logs*
 - Trend Micro OfficeScan firewall logs
 - Windows Firewall logs:
Control Panel->Windows Firewall->Advanced->Security Logging->Settings
- t. *Run an anti-virus scan*
 - Update pattern/definition files first
 - Beware that OfficeScan will by default quarantine or delete the malware it finds, potentially altering or destroying evidence; is very difficult to recover a quarantined file in Trend Micro.
 - Check antivirus event logs and quarantine folder
- u. *Look for rootkits*
 - By design, rootkits are difficult to detect
 - “Rootkit Revealer” from www.sysinternals.com can detect some rootkits; beware of false positives since some software, like anti-virus tools or personal firewalls intentionally hide items (try to hide them from attackers, for example)