

ISE 640 Lab Three Guidelines and Rubric
Creating a Baseline Using the Windows Forensic Toolchest

Overview: You will be completing several labs throughout this course. The purpose of these labs is twofold:

- The experience will provide you with valuable opportunities to “walk a mile” in the shoes of a forensic practitioner performing basic forensic tasks. Gaining this type of experience is necessary in managing and relating to the individuals and teams with whom you will interact with in the field.
- Practice the communication and writing skills you will need to employ in both pieces of your final project.

It is important to note that these activities are important to your final project but do not share the same scenario as your final project. They are practice opportunities that focus on a specific but smaller set of topics and skills. You will complete a lab “briefing” paper and submit it to your instructor for grading. A template of this brief is provided for you.

Scenario: Please be aware that the instructions given inside of Lab Three refer to a separate scenario, not the one that we will be addressing in class. Use our classroom scenario to focus your learning in the lab.

In the previous lab, Lab Two, you were given the following scenario: While working for ACME Construction Company, you have been tasked with an investigation of a Windows 8 hard drive. You have been told that your company suspects a high-level employee of a policy violation. It is believed that Drew Patrick wrongfully copied sensitive corporate documents containing valuable intellectual property (IP) to his personal computer. Further, there is reason to believe that he may have then provided the documents to a competitor. Due to the value of the IP, the investigation has moved from a simple incident response to a forensic investigation.

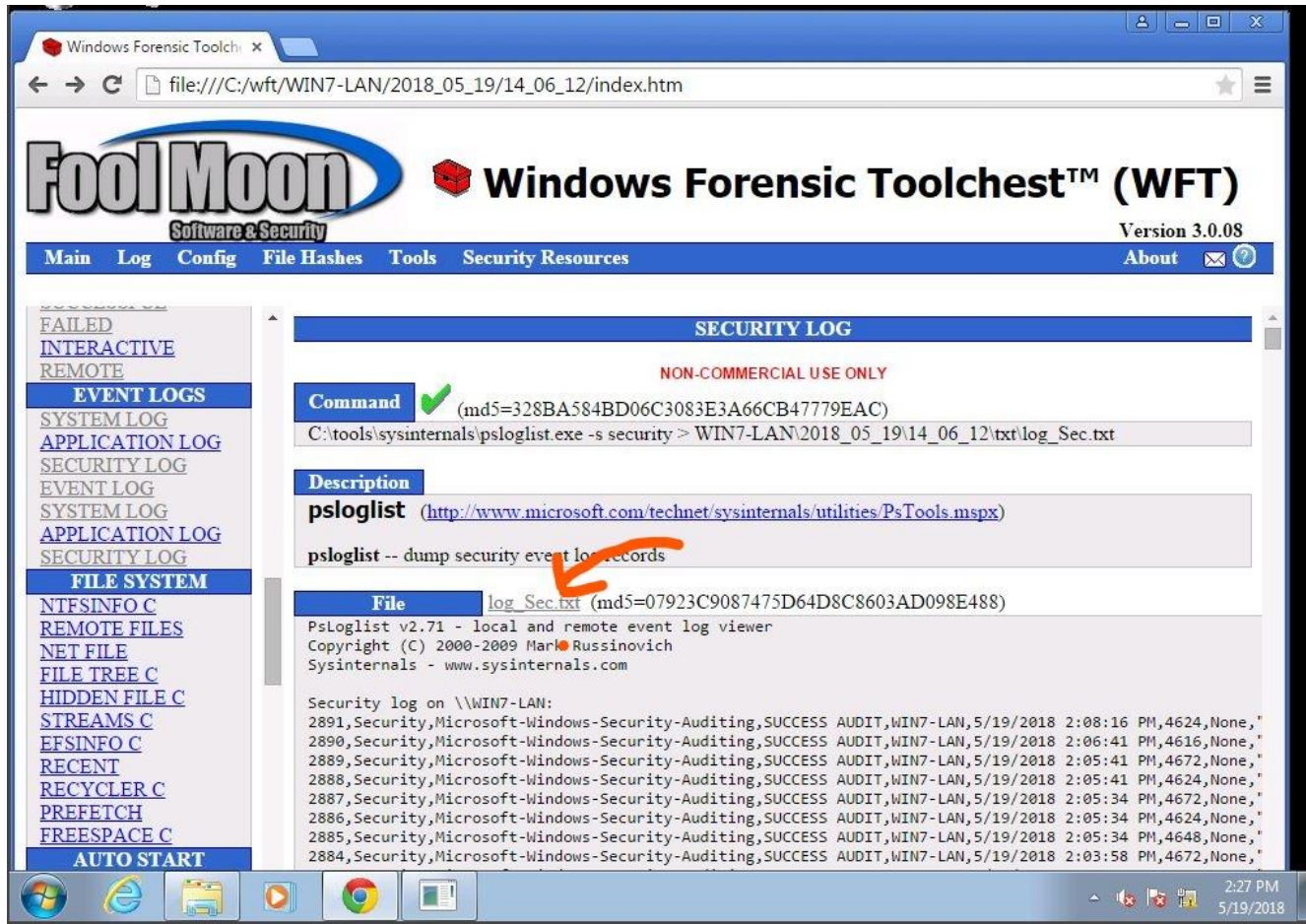
In Lab Two, you finished creating and verifying an image for use in the forensic lab. Lab Three will have you tasked with a different part of the investigation. Wily miscreants will often attempt to cover their tracks. One supposedly clever way of doing this is to create a separate login account and use that account to perform all their evil deeds. Any decent investigator will analyze all the accounts, their creation dates, privileges, and activities in an effort to rule out the idea of evidence being planted by another or any attempt to cover one's tracks.

Windows Forensic Toolchest (WFT) is often used on Windows computers to quickly and easily gather many details concerning the operating system and related functions. An investigator can use WFT to run a scripted set of commands that will allow them to easily identify many properties such as logins (successful or failed), network shares, groups and accounts, and many others. Proper documentation of these settings and characteristics will help to weaken the “it was not me” argument.

In your lab, be sure to document the following for your final project:

1. Internet protocol (IP) address of the computer at the time of the examination (IPCONFIG)
2. List of user accounts on the suspect machine (NET USER)

3. List of users who have logged on locally (LOGINS – ALL)
4. The shared directories on the network, which may aid in passing data outside of the company-controlled environment (NET SHARE)
5. The security logs and their details will be used in the log analysis lab. You can take a quick look at them here so you know what to expect during the following lab. (EVENT LOGS – SECURITY LOG)



Opening the log_Sec.txt file should look something like this:

Windows Forensic Toolchest™ (WFT) Version 3.0.08

Main Log Config File Hashes Tools Security Resources About

EVENT LOGS

- SYSTEM LOG
- APPLICATION LOG
- SECURITY LOG
- EVENT LOG
- SYSTEM LOG
- APPLICATION LOG
- SECURITY LOG

FILE SYSTEM

- NTFSINFO C
- REMOTE FILES
- NET FILE
- FILE TREE C
- HIDDEN FILE C
- STREAMS C
- EFSINFO C
- RECENT
- RECYCLER C
- PREFETCH
- FREESPACE C

AUTO START

- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI
- STARTUP.FOLDE

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

Security log on \\WIN7-LAN:
2891,Security,Microsoft-Windows-Security-Auditing,SUCCESS AUDIT,WIN7-LAN,5/19/2018 2:08:16 PM,4624,None,"An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1e6d22 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: WIN7-LAN Source Network Address: 127.0.0.1 Source Port: 51206 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 128 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. "
2890,Security,Microsoft-Windows-Security-Auditing,SUCCESS AUDIT,WIN7-LAN,5/19/2018 2:06:41 PM,4616,None,"The system time was changed. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Process Information: Process ID: 0x3d4 Name: C:\Windows\System32\svchost.exe Previous Time: 2018-05-19T18:06:41.571625000Z New Time: 2018-05-19T18:06:41.571000000Z This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer. "
2892,Security,Microsoft-Windows-Security-Auditing,SUCCESS AUDIT,WIN7-LAN,5/19/2018 2:05:41 PM,4618,None,"Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1e6d22 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: WIN7-LAN Source Network Address: 127.0.0.1 Source Port: 51206 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 128 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. "

It is not critical that you understand the content of this log at this time. This will be used in another lab.

- You may also want to document the drive hash values created by WFT.
- For those who want to look a little deeper, the Processes – PS displays a list of all the running processes at the time WFT was run, and NETWORKING NETSTAT – AN displays active network connections that may be of interest in an investigation.

Prompt: In your report, be sure to address the following critical elements:

1. Provide a brief **summary** of the lab. What did you do in the lab? How did it work? What did you look for/find?
2. Briefly describe the **specific practices or resources** that were most important in supporting the investigation and maintaining evidentiary integrity in this lab. For example:
 - a) Chain of custody practices
 - b) Digital forensic tools
 - c) Incident response tactics
3. Briefly describe best practices or resources necessary in terms of **next steps** in this lab scenario.
4. Include **screenshots** that support items 2 and 3 in your briefing.
5. Ensure your entire briefing is appropriate to your **internal audience**, employing brevity and consumable language (in this lab, your audience will be your teammates/company attorneys/executive team).

Rubric

| Critical Elements | Proficient (100%) | Needs Improvement (75%) | Not Evident (0%) | Value |
|--|--|--|--|-------|
| Lab Summary | Provides brief summary of the lab | Provides brief summary of the lab, but summary is cursory or contains inaccuracies | Does not provide lab name and brief summary of the lab | 19 |
| Specific Practices or Resources | Briefly describes specific practices or resources that were most important in supporting the investigation and maintaining evidentiary integrity in this lab | Describes specific practices or resources that were most important in supporting the investigation and maintaining evidentiary integrity in this lab, but rationale is illogical, inaccurate, or lacks necessary details | Does not describe specific practices or resources | 19 |
| Next Steps | Briefly describes best practices or resources necessary in terms of next steps in this scenario | Briefly describes best practices or resources necessary in terms of next steps in this scenario, but rationale is illogical, inaccurate, or lacks necessary details | Does not describe best practices or resources | 19 |
| Screenshots | Includes screenshots that directly support practices and necessary resources | Includes screenshots, but does not include all necessary screenshots required or those provided do not directly support practices and necessary resources | Does not include screenshots | 19 |
| Internal Audience | Appropriate to internal audience, employing brevity and consumable language | Submission is appropriate to internal audience but does not employ brevity or consumable language | Submission is not appropriate to internal audience | 19 |

Southern New Hampshire University

| Critical Elements | Proficient (100%) | Needs Improvement (75%) | Not Evident (0%) | Value |
|---------------------------------|---|---|---|-------------|
| Articulation of Response | Submission has no major errors related to citations, grammar, spelling, or organization | Submission has some errors related to citations, grammar, spelling, or organization that negatively impact readability and articulation of main ideas | Submission has critical errors related to citations, grammar, spelling, or organization that prevent understanding of ideas | 5 |
| | | | Total | 100% |