Computer Forensic Laboratory for the Polytechnic University of Puerto Rico

Carlos J. González Acevedo
Computer Engineering
Jeffrey Duffany, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Computer Forensic is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law, was define computer forensic. The legal and technical aspects of computer forensics will help you capture vital information if your network is compromised, will help you ensure the overall integrity and survivability of your network infrastructure and you prosecute the case if the intruder is caught. Security professionals need to consider their policy decisions and technical actions in the context of existing laws. This paper presents the design and implementation of an experimental Computer Security and Forensic Analysis (CSFA) laboratory and the tools associated with it for the University. The laboratory is envisioned to be a training facility for future computer security professionals.*

Key Terms *— Computer, Forensic, Software, Tools.*

BACKGROUND

Forensic evidence of all types must be collected by following rigorous and well-tested procedures in order to protect any such evidence from contamination or destruction, or from becoming subject to claim of tampering and improper handling, and to establish and preserve the chain of custody. Any failure to follow the strict procedures developed and agreed upon may result in some digital evidence being excluded or limited by the courts.

Some of the procedures in the digital forensic process are:

- Log all actions: this provides a record of all of actions taken at all stages of the investigation and serves a number of purposes.
- Record the scene: necessary to move the equipment slightly to give access to the rear of the equipment and the connections.
- Screen Information recording: if any files are open, they should be saved, preferably to an external device and action recorded.
- Cable and socket labeling: this helps with the reconstruction of the system if it is required.
- Checking for passwords: if any passwords are found, they should be recorded for use later in the process.

These phases are described in the following:

- Evidence collection: these are items that may contain digital data.
- Evidence Preservation: is the preservation of the items in a manner that is reliable, complete, accurate, and verifiable.
- Evidence Analysis: the examination of the individual elements of information.
- Evidence presentation: normally be supported by documentation.

Chain of custody is a legal term that refers to the ability to guarantee the identity and integrity of the article from the time it is collected through the time the results of the analysis are reported and subsequently disposed of.

Example #1: Mandiant Red Curtain

MANDIANT Red Curtain (MRC) is software for Incident Responders that analyzes executable files (for example, .exe, or .dll) to determine how suspicious they are based on a set of criteria. It examines multiple aspects of a file, looking at

things such as the entropy, compiler and packing signatures, the presence of digital signatures, and other characteristics to generate a threat "score". [7]

Example #2: TCP View

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. [12]

Example #3: Sigcheck

System administrators and security analysts often need to assess the validity of Windows system and application files loaded on a critical end-point or server device.

Example #4: Process Monitor

PROCESS MONITOR is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.[11]

Example #5: Memoryze Mandiant

MANDIANT Memoryze is free memory forensic software that helps incident responders find evil in live memory. Memoryze can acquire and/or analyze memory images, and on live systems, can include the paging file in its analysis.[8]

Example #6: Helios root Kit

Helios is an advanced malware detection system has been designed to detect, remove and innoculate against modern rootkits. [1]

Example #7: Case Notes

The purpose of CaseNotes is to provide a single lightweight application program to run on the Microsoft Windows platform to allow forensic analysts and examiners of any discipline to securely record their contemporaneous notes electronically.

METHODS

Multiple sources of data within an acquired image can contain valuable time-based information, including the contents of log file, Registry key and values, and the contents of the Recycle Bin. A number of free or low-cost tools are available that can more than adequately replace or even extend the functionality inherent to many of the commercial application bundles. There are time when it is important to use a commercial application for data analysis and presentation. Freely available tool provides a greater visibility into the data and provides answers much faster.

A number of widely used and accepted digital forensic imaging and analysis software suites are currently available. The software ranges in cost and capability, and in addition, you will normally need to arrange single task tools to carry out specific tasks. When you have decided on the software that best suits your requirements and have purchased and installed these products, you must also test them to make sure they work on the systems as you have configured them. It is essential you ensure that the software works in the manner advertised since the functionality of the software may become an issue in any disciplinary or judicial proceedings if it has not been tested.

Example #1: Mandiant Red Curtain

A tool to manually scan folders or files for suspicious criteria, such as entropy/randomness, binary packing, compiler signatures, digital signatures, and other characteristics that generate an overall threat score. MRC includes an analysis engine and a data presentation layer. The engine reads in the file to be analyzed, using the data within the file to calculate the Shannon Entropy across a series of overlapping windows of file segments. This data is then fed to the presentation layer, which organizes it for display to the user.

Example #2: TCP View

When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP

addresses to their domain name versions. By default, TCPView updates every second, but you can use the Options|Refresh Rate menu item to change the rate. You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting File|Close Connections, or by right-clicking on a connection and choosing Close Connections from the resulting context menu.

Example #3: Sigcheck

Verify that images are digitally signed and dump version information with this simple command-line utility. SigCheck is a free downloadable command-line utility from Sysinternals.

Example #4: Process Monitor

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters
- Reliable capture of process details, including image path, command line, user and session ID
- Process tree tool shows relationship of all processes referenced in a trace

Example #5: Memoryze Mandiant

Image the full range of system memory (not reliant on API calls).

- Image a process' entire address space to disk.
- Image a specified driver or all drivers loaded in memory to disk.
- Enumerate all running processes (including those hidden by rootkits).
- Identify all drivers loaded in memory, including those hidden by rootkits.

Example #6: Helios root Kit

Helios has four basic modes of operation:

- On‐demand scanning -This is a one button check of the systems health
- Background scanning –Helios will continuously poll the system status to determine whether there are any discrepancies.
- Application protection - Helios performs an integrity check of each and every application
- that starts on the system and checks to see that certain vital functions.
- Innoculation - If configured in alert mode, Helios will inform the user whenever a file access / driver load / physical memory operation is performed and allows the user to allow or deny the event. [4]

Helios attempts to actively monitor and prevent rootkits from infecting your system. It reveals – information about not only the infection, but also how Helios determined the infection's existence.

Example #7: Case Notes

Main features are:

- Secure "write-once, read-many" style of case note data capture.
- Full audit trail of case note data entry.
- Tamper evident storage of data using internal MD5 hashes.
- No use of heavy database technologies.
- Use of AES 512bit encryption (optional) to further secure data in sensitive cases. [10]

ANALYZING PROJECT

The best way to get started is to dive right in. When correlating and analyzing volatile data, it helps to have an idea of what are you're looking for. One of the biggest issues that some information technology administrators and responders face when an in incident occurs is tracking down the source of the incident based on the information they have available. This set of tools will not only provide a comprehensive view of the state of the system at a snapshot in time, but also collect data that may help direct analysis and follow-on investigative efforts. This is why is so important of having a process, a list of steps and tools that you can follow, and if something needs to be added or modified, you can do so easily. Knowing the tools and their use is the best way to improve your success on finding suspected process and activities on a compromised system. [9]

Example #1: Mandiant Red Curtain

Start MRC via the shortcut installed on your Desktop or via the Start menu. By default the shortcut to MRC is installed in Start → All Programs → Mandiant Red Curtain :

- Scan your c:\windows\system32 directory by selecting File → New → Scan a Folder. You will then be presented with a dialog box to select a Folder for scanning. Navigate to c:\windows\system32 and click OK. An important note: When MRC conducts file scans, it opens each file and reads its contents. That means that the last accessed date for each file will be modified as it's examined by MRC.
- A progress bar will be displayed that shows you which files are being scanned. When the scan is complete, MRC should look something like Figure 1 below: "MRC User Interface After Scanning c:\windows\system32".
- You can save your results by using the File → Save As... menu item. [5]

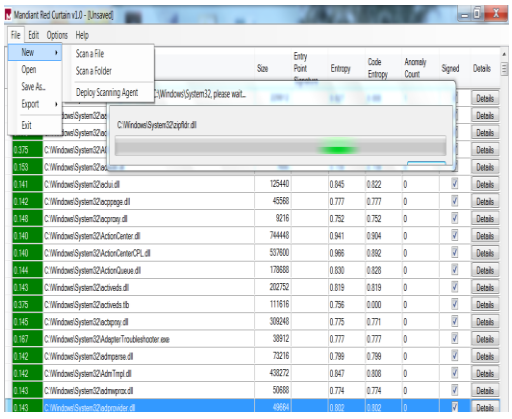

Figure 1
Red Curtain

Example #2: TCP View

Open TCPView with the RUN command. The screen will look something like Figure 2.

Open new applications or Web sites and see what happens. You will see that the TCP View screen changes. You will see yellow and red tabs identifying new process and remote address opening. Try opening any Web site and verify the process been open and pay special attention to all the remote addresses that a simple page will open.

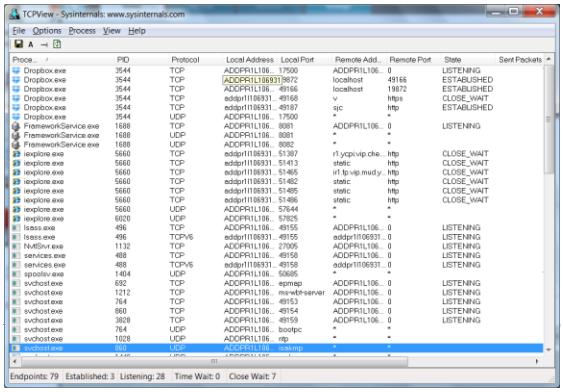

Figure 2
TCP View

Example #3: Sigcheck

Usage: sigcheck.exe [-a][-h][-i][-e][-n][[-s]|[-v]|[-m]][-q][-r][-u][-c catalog file] <file or directory>. See Table 1 for description. [13]

Table 1
Sigcheck options

-a Show extended version information

-c Look for signature in the specified catalog file

-e Scan executable images only (regardless of their extension).

-h Show file hashes

-i Show image signers

-m Dump manifest

-n Only show file version number

-q Quiet (no banner)

-r Check for certificate revocation

-s Recurse subdirectories

-u Show unsigned files only

-v Csv output

Example #4: Process Monitor

When you launch Process Monitor it immediately starts monitoring three classes of operation: file system, Registry and process.

- File System: Process Monitor displays file system activity for all Windows file systems, including local storage and remote file systems.
- Registry: Process Monitor logs all Registry operations and displays Registry paths using

conventional abbreviations for Registry root keys

- Process: In its process/thread monitoring subsystem Process Monitor tracks all process and thread creation and exit operations as well as DLL and device driver load operations.

The Network Process Monitor uses Event Tracing for Windows (ETW) to trace and record TCP and UDP activity. Profiling access monitor scans of all the active threads in the system and generates a profiling even for each one that records the kernel and user CPU time consumed

Example #5: Memoryze Mandiant

In order to visualize Memoryze's output, use Audit Viewer. Audit Viewer is an open source tool that allows users to examine the results of Memoryze's analysis. Audit Viewer allows the incident responder or forensic analyst to quickly view complex XML output in an easily readable format. Using familiar grouping of data and search capabilities, Audit Viewer makes memory analysis quicker and more intuitive.

Example #6: Helios Root Kit

Helios does not require installation. Double-click the executable and let's begin. As the GUI opens, click "Toggle Background Scan" and "Advanced Detection" on the left-hand menu to enable the Background Scan and Advanced options in the Scan Status window. For our tests, App Protection does not need to be enabled. The correctly configured GUI is shown Figure 3.

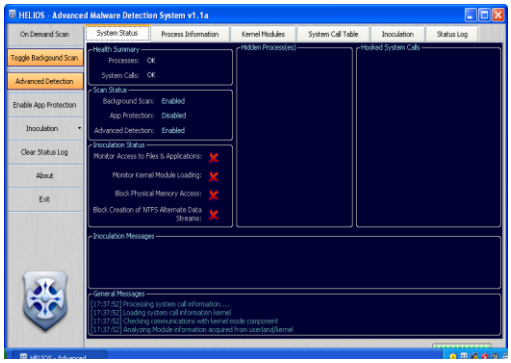

Figure 3
Helios Root Kit

Example #7: Case Notes 3.0

Case Notes Example. See Figure 4 below:

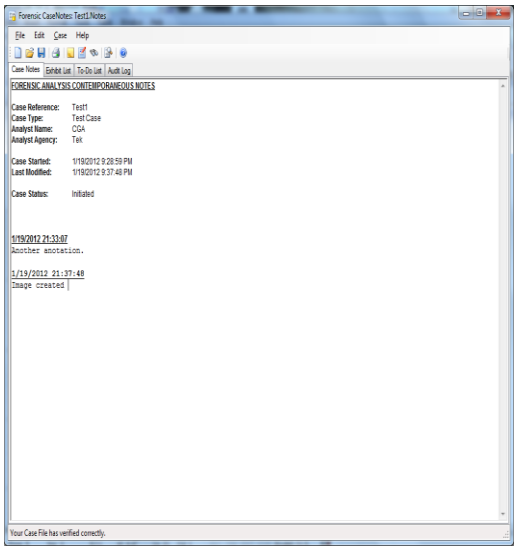

Figure 4
Case Notes

RESULTS

When you use tools such as those discussed on this paper, you are getting a snapshot of the state of a system at a point of time. For example, you may see something unusual in the Task Manager Graphical user interface (GUI) or in the output of the process monitor procmon.exe (such as an unusual executable image file path or command line). For an investigator who is familiar with Windows Systems and what a default or "normal" processes look like from this perspective, these indicators may be fairly obvious and may jump out immediately. What constitutes a "normal" or legitimate process can depend on a lot of different factors, so you need to have a process for examining your available data and determining the source of the source of the issue you're investigating. [3]

Example #1: Mandiant Red Curtain

The Red Curtain application main screen represented on Figure 5.

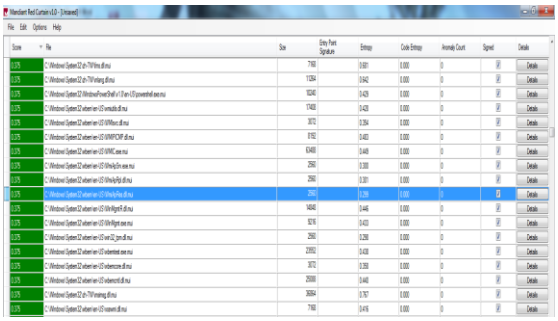

Figure 5
Red Curtain Display

Example #2: TCP View

One probable answer is to look for suspicious ports that are listening for connections. How can we do this? There are two windows tools, TCPView and Active Ports, that do exactly that.

- Click on Tcpview.exe. Take note of the processes running, the protocols they use, the local and remote addresses, and the state.
- Now run the Netcat listener by opening a command prompt and typing:

  nc –l –p 7777 –e cmd.exe
- Look back to TCPView. You should see a new process "nc.exe:xxxx". The local address should be xp:7777 and the state should be listening.

Example #3: Sigcheck

One way to use the tool is to check for unsigned files in your WindowsSystem32 directories with this command:

sigcheck -u -e c:windowssystem32.

You should investigate the purpose of any files that are not signed. SigCheck provides information not readily available through abilities provided via the operating system. Particularly useful are hash value and internal name values. Hash values can be fed into online services to check for known malicious files. [2]

Example #4: Process Monitor

Sample Scenario:

Let's assume you're unable to write to the HOSTS file successfully in Windows 7/Vista, and want to know what's happening under the hood.

Running Process Monitor & Configuring Filters:

- Download Process Monitor from Windows Sysinternals site.
- Extract the zip file contents to a folder of your choice.
- Run the Process Monitor application.
- Include the processes that you want to track the activity on.
- For this example, you want to include Notepad.exe in the Filters. See Figure 6.

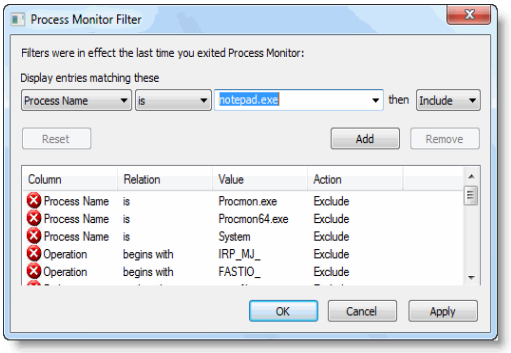

Figure 6
Process Monitor Filter

You can add multiple entries as well, in case if you want to track few more processes along with Notepad.exe. To keep this example simpler, let's only track Notepad.exe. [14]

You'll now see the Process Monitor main window which shows the list of registry and file accesses by processes, as and whey they occur.

From the Options menu, click Select Columns, place a checkmark near Sequence Number and click OK. See Figure 7.

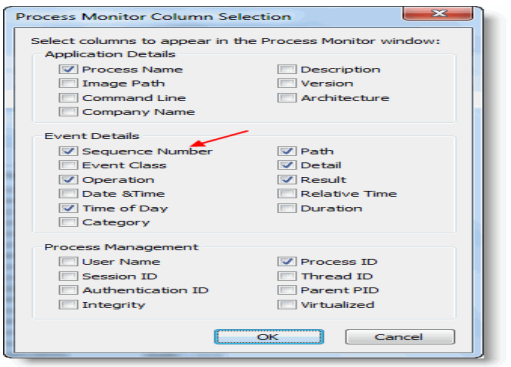

Figure 7
Process Monitor Filter

Capturing Events:

To configure the process of capturing an event, follow the next steps:

- Open Notepad.
- Switch to Process Monitor window.
- Enable the "Capture" mode (if it's not already ON). You can see the status of the "Capture" mode via the Process Monitor toolbar. See Figure 8.

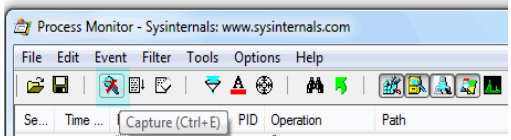

Figure 8
Process Monitor Toolbar

- The highlighted button above is the "Capture" button, which is current disabled. You need to click that button (or use CTRL + E key sequence) to enable capturing of events.
- Cleanup the existing events list using CTRL + X key sequence (Important) and start afresh list.
- Now switch to Notepad and try to reproduce the problem. To reproduce the problem (for this sample scenario), try writing to HOSTS file:
  (C:\Windows\System32\Drivers\Etc\HOSTS)
  and saving it. Windows offers to save the file (by showing the Save As dialog) with a different name, or in a different location. So what happens under the hood when you save to HOSTS file? Process Monitor shows that exactly. See Figure 9.

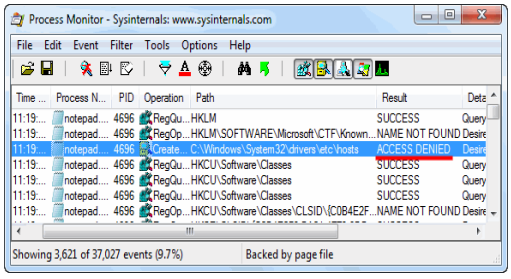

Figure 9
Process Monitor Results

- Important Note: Don't take much time to reproduce the problem after enabling capturing. Similarly turn off capturing as soon as you finish reproducing the problem. This is to prevent Process Monitor from recording other unneeded data (which makes analysis part more difficult). You need to do all that as quickly as you can.

The log file above tells us that Notepad encountered an ACCESS DENIED error when writing to the HOSTS file. The solution would be to check the permissions for HOSTS file; In Windows 7 and Windows Vista, you simply run Notepad as elevated (right-click and choose "Run as Administrator") to be able to write to HOSTS file successfully.

Saving the Output:

To save the output for future references do the following steps:

- In the Process Monitor window, select the File menu and click Save
- Select Native Process Monitor Format (PML), mention the output file name and Path, save the file. See Figure 10.

Example #5: Memoryze Mandiant

Memoryze has two main functional categories. The first is analysis, and the second is acquisition. Under analysis, processes, drivers and kernel structures can be searched for and investigated. Under acquisition, the user can acquire the entire address space of a process, the binary representing the driver in memory, or the entire memory of the host. Audit Viewer breaks the types of tasks down into two different configuration screens. The first screen the user will see is the analysis style tasks. See Figure 11.

The user should check each task they want to configure and execute such as process enumeration, driver enumeration, or hook detection. Configuration of each task follows after the user has selected all the tasks they desire.

The second set of tasks is acquisition related. See Figure 12.

Once the user has finished selecting which analysis and/or acquisition tasks s/he wishes to

perform, the user will see a review panel. See Figure 13.

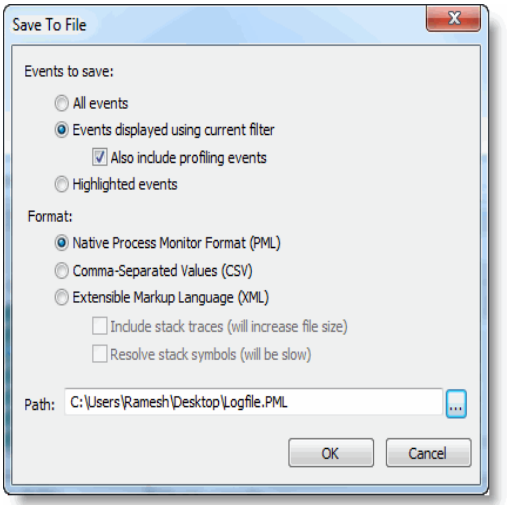

Figure 10
Saving Files Results

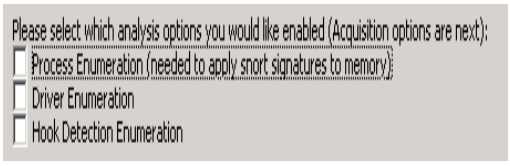

Figure 11
Analysis Style Selection

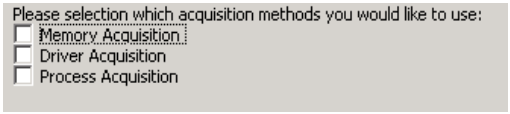

Figure 12
Acquisition Method Selection

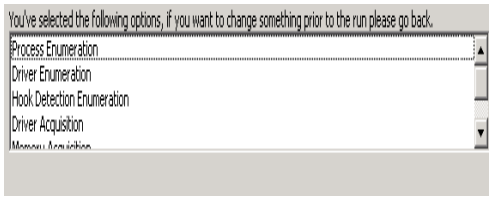

Figure 13
Review panel

This shows the user what tasks they have selected to be configured. Deeper configuration is to follow this initial setup. If the user wants to change any of their selections, they can simply go back and uncheck the tasks they chose previously.

Example #6: Helios root Kit

Questions for Helios root Evaluation.

Q1: Has Helios detected the hidden malwareHQ folder? And if so, where?

Q2: Has Helios detected the hidden malware process? And if so, where does Helios report this? Provide print screens of all relevant data.

Q3: Should security professionals be concerned about a rootkit detector that does not identify hidden folders? Why or why not?

Q4: Go to the Process Information tab in Helios. Notice the option to Kill the malware service. Does killing the service prevent it from starting again on reboot?

Example #7: Case Notes

New case screen. See Figure 14.

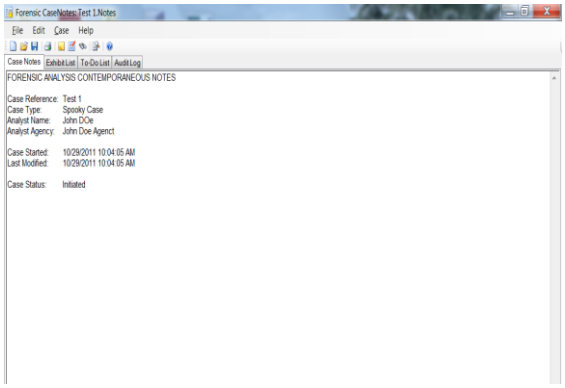

Figure 14
New Case

Audit Log. See Figure 15.

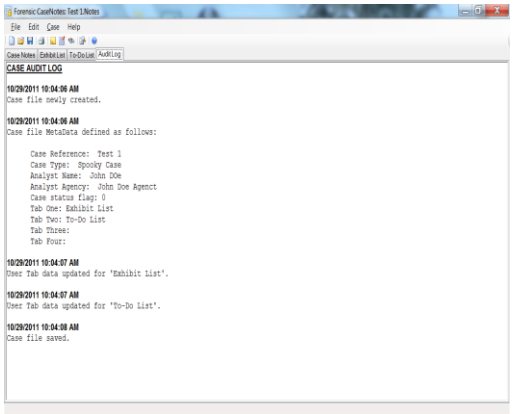

Figure 15
Log File

All notations are identified by date and hour and kept on the log files. See Figure 16.

CONCLUSION

Live system contain a lot of data that we can used to enhance our understanding of an incident, we just need to collect that data before we remove power from the system so that we can acquire an image of the hard drive. Provide you with enough information such that based on your needs and the conditions of the situation you're facing, you can not only employ your own "best practice", but when then situation change, employ and justify the used of better practice.

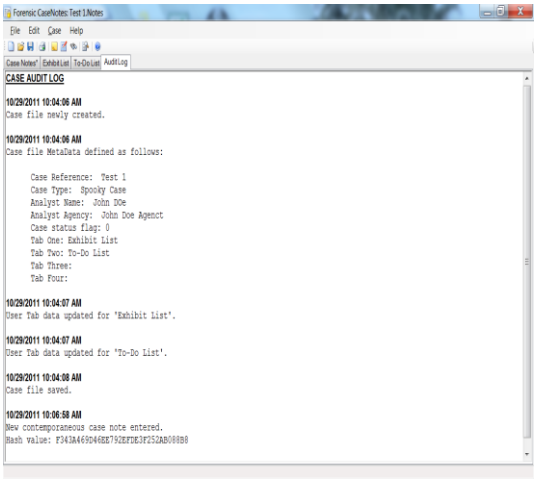

Figure 16
Log File

We can also automate some of the data correlations, further reducing the overall amount of data and reducing the numbers of mistake that may be made. Some basic concepts can be common across investigation, and knowing where to look for corroborating information can be an important key. With a stronger understanding of these areas, investigators will be better equipped to address issues of rootkits during both live-response and postmortem investigations.

The main role of a digital forensic laboratory is to be cost-effective and achieve its potential. A number of steps must be taken before it begins operation. Be derived from the rationale used for the business case and will outline the customer base that will be supported by the laboratory, as well as the role of both management and those individuals responsibilities.

RECOMMENDATIONS

Laboratory Utilization: The use of the laboratory could increase by performing, not only university laboratory use, but renting the facilities and expertise for outside investigations. That will not only increment the cost effectiveness of the laboratory, but also will create employment opportunities and experience.

Staff Considerations-Staff levels and roles [6]:

- Laboratory Manager: will be responsible for all aspects of running the laboratory, include all issues to the staff, such as recruitment, training, mentoring, counseling, ethical guidance, rewards and retention.
- Reception Officer: effectively the "front man" and recognized as the "point-of-contact".
- Triage Officer: responsible for deciding whether tasks are accepted into the laboratory, allocating the priority in which cases are to be dealt with.
- Imaging Officer: responsible for creating the copy (image) of the seize media and ensuring that the images are created in a forensically sound manner.
- Analyst: responsible for the analysis of the available material and ensuring that any finding form that can be reproduced by anyone. Will attempt to find useful information or evidence, current investigations and discover investigations or other incidents.

REFERENCES

[1] www.antirootkit.com/software/Helios.htm

[2] www.brighthub.com/computing/enterprise-security/articles/13389.aspx#ixzz1c0bKtOl6

[3] Carvey-Harlan, (2009), "Windows Forensic Analysis", Syngress publishers, second edition.

[4] www.helios.miel-labs.com/downloads/whitepaper.pdf

[5] www.holisticinfosec.org/toolsmith/docs/december2007.pdf

[6] Jones A. & Valli C. (2009), "Building a Digital Forensic Laboratory", Syngress Publishers.

[7] www.mandiant.com/mrc

[8] www.mandiant.com/products/free_software/memoryze/

[9] Philipp A., Cowen D. & Davis C., (2010), “Hacking Exposed”, Mc Graw-Hill Companies, second edition.

[10] www.qccis.com/forensic-tools

[11] www.technet.microsoft.com/en-us/sysinternals/bb896645

[12] www.technet.microsoft.com/en-us/sysinternals/bb897437

[13] www.technet.microsoft.com/en-us/sysinternals/bb897441

[14] Retrieved from: www.winhelponline.com/blog/process-monitor-track-events-generate-log-file/