4-12-2006

Freeware Live Forensics tools evaluation and operation tips

Ricci Ieong
eWalker Consulting Ltd

DOI: 10.4225/75/57b1305ec7050
4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

Freeware Live Forensics tools evaluation and operation tips

Ricci IEONG,
Principal Consultant,
eWalker Consulting Ltd

Abstract

Highlighted by a digital forensics investigation specialists from FBI in DFRWS 2006, live forensics investigations already become one of the most important procedures in digital forensics investigations. Many digital forensics investigation product companies have already joint the battlefield in developing their only live forensics tools. However, similar to the development trend in traditional digital forensics, evaluation criteria for Live Digital Forensics could only be standardized after operating procedures being standardized. One way to standardize the Live Digital Forensics Investigation procedure is to define the investigation objectives around the core digital forensics principles. Through the use of FORZA framework, a more legal and investigation oriented live digital forensics investigation procedures have been outlined. Based on the FORZA based procedure, a set of operation best practices, operational tips and evaluation criteria was derived. Using the derived criteria, various free Live Forensics toolkits including Windows Forensics Toolchest (WFT), Incident Response Collection Report (IRCR), First Responders Evidence Disk (FRED) and Computer Online Forensic Evidence (COFEE) were evaluated and reported in this paper.

Keywords

Live Digital Forensics Investigation, FORZA framework, freeware live forensics tools

INTRODUCTION

In DFRWS 2006, FBI digital forensics investigator highlighted that due to increase in data storage size, internet centric cases and urgent investigation requirements, live forensics investigation becomes one of the most important area in digital forensics investigation. In order to support the live forensics investigation requirement, toolboxes have to be developed according to the required investigation procedure. Before the development in live forensics procedure, many freeware IT security, and incident response tools have already been developed. Most of them were used for extracting particular piece of information. In year 2000, some forensics investigators started to develop their investigation procedures for executing these sets of tools in order.

However, different toolkits have their own execution procedures. Most of them were developed based on developer's experience. So it would be extremely difficult to testify whether the collected live forensics evidence is forensically sound. Without a certification and attestation procedure, presenting live forensics investigation data into court would have to be testified case by case.

As highlighted in paper yet to be published [Ieong and Chau 2007], live forensics investigation can be summarized in the following live forensics investigation principles:

- Completeness of data – data that would be destroyed or affected after system shutdown should all be collected.
- Order of volatility – data should be collected in the order that would not be affecting other results.
- Time required and Importance of evidence – data should be collected within a reasonable time and depending on their importance.
- Repeatability – All data collected for testing should be available and performed actions should be as repeatable as possible.

- Integrity of evidence – data collected from live digital forensics investigation should be protected from being tampered.
- Accuracy of evidence – tools for collecting the data should be accurately recording the data
- Verifiability and Reasonableness – the actions performed should be verifiable in court and be reasonable to the case.
- Case dependencies – the actions performed in one particular live digital forensics investigation should be relevant and depending on the case.

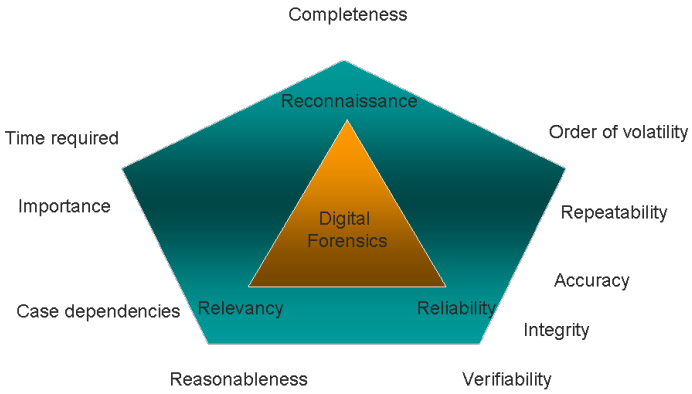

Figure 1: Mapping of Live Forensics Investigation requirement to 3R principles

Based on the proposed live digital forensics investigation procedure, a set of case-dependent dynamic evaluation criteria based on the live forensics investigation principles, best practices and operation tips was defined. The following section highlighted how the evaluation criteria could be applied for assessing the freeware toolkits.

ORDER OF LIVE FORENSICS INVESTIGATION FLOW

Live Forensics Investigation flow depends on the situation and cases to be investigated. It also depends on the case officer requirement. Without any specific requirement, a typical live forensics investigation flow can be depicted in the following diagram.

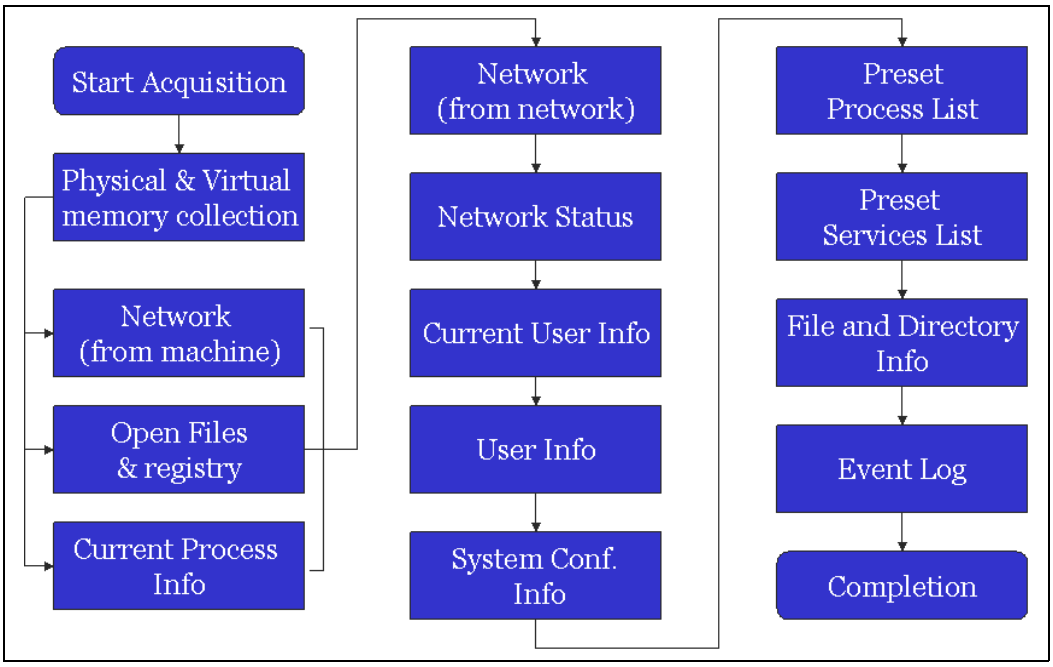

Figure 2: A reference order of data collection process in live forensics investigations

For individual cases and different situations, live forensics investigation requirement, execution flow could be derived based on Ieong's paper (Ieong and Chau, 2007) In his paper, a set of questions for deriving the requirement and investigation flow based on FORZA model was outlined.

In a ***typical online illegal web publishing situation***, the most important information to be verified and identified during the investigation is to identify the target machine is being used for illegal upload of identified matter together with the identity of the user, current user and any web related account information.

According to this requirement, the live forensics toolkits should be formulated to collect relevant data in the following order:

- Current network connections
- Open files and registry information
- Current connected network IP addresses
- Current network path, network broadband device configuration
- Current processes executing
- Current user name
- Opened web connection
- Machine uptime
- System configuration
- Browser history, cache, passwords
- USB and external devices used before

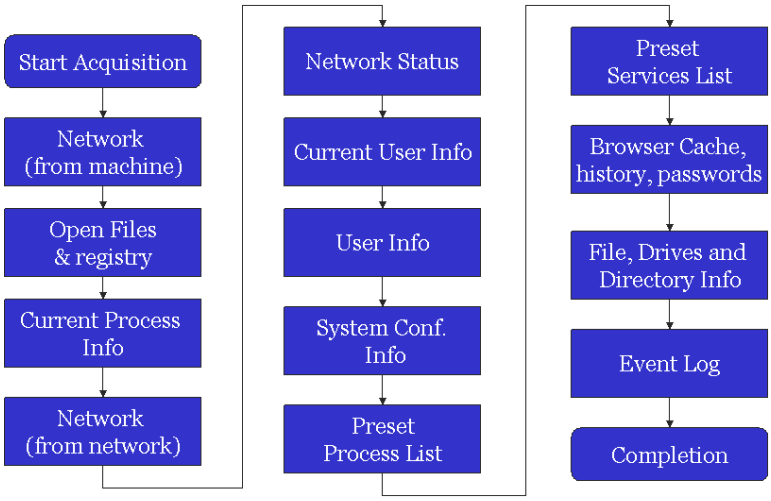

Figure 3: A reference order for typical online illegal web publishing situation

While in a ***typical web hacking situation***, incident handling and responses team would like to determine if the system was being compromised by virus or worm and whether additional Trojan or backdoor programs have been implanted to the system. More importantly, owner of the system may want to ensure that the system would not be easily compromised again and to fix the system as soon as possible.

Thus, the following requirement should be more applicable for collecting of live forensics information in a web hacking situation:

- Current Network port and network connection
- Open files and registry information
- Current processes executing
- Audit log files from the system
- Directory time stamp
- File list/file signature matching,
- Current user name and user account list,
- Program install date,
- Preset process,
- Service list,
- Bootup list
- System configuration

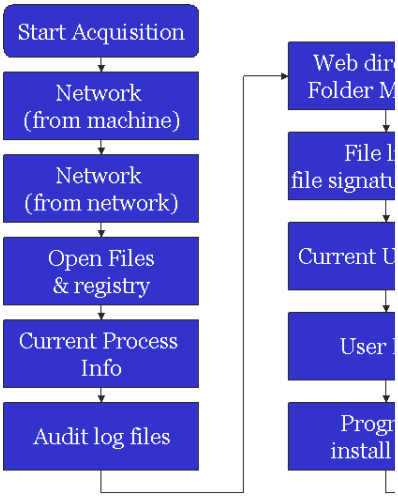

Figure 4: A reference order for typical web hacking situation

In a ***typical botnet situation***, the top priority in an investigation is to determine the source IP address of the botnet controller and owner. Network connection or controller IP address may only be shown in a short period of time, so the fast network information acquisition should be performed first. Besides, system owner may want to know the vulnerability of the system where the botnet penetrate into the system as well as to estimate the damages induced to the entire infrastructure.

While physical memory and virtual memory acquisition, even though is comparatively volatile, due to slow in acquisition, the acquisition procedure could be postponed to late stage.

With this requirement, the order of live forensics investigation should be reorder to the following:

- Current network port and network connection
- Sniff the current network connection
- Open files and registry information
- Current process executing
- Current network status
- Current user name and user account list
- File list/file signaturing matching
- System configuration
- Preset process, Service and bootup list
- Event Log
- Physical Memory and Virtual Memory

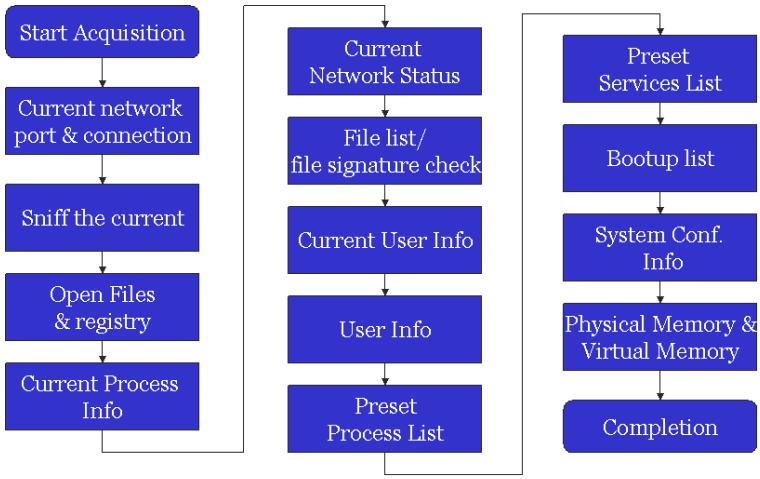

Figure 5: A reference order for typical botnet situation.

COMMONLY USED LIVE FORENSICS FREEWARE TOOLKITS

By year 2000, a number of freeware tools have been developed for incident response and IT security review purpose. Many of them could be used in incident handling as well as digital forensics investigation work.

For instance, *fport* (freeware from Foundstone), one of the most frequently used tool, is used for collecting the current network port opened and the corresponding process ID. That enables investigator to immediately identify whether a malicious program has been executed and connected to the network.

Other useful IT security tools such as *listdlls* and *handle* (freeware from sysinternals) can also be applied for determining the dynamic linked library used by current process and identifying the opened files and registry used by current process have also been used in live forensics investigation process as well.

One drawbacks of using freeware tools was that user has to remember all the commands and parameters in order to execute them directly at the command prompt. Then investigators have to manually consolidate the raw text output to a case related report.

In order to make full use of the freeware tools, toolkits that execute them in order and along priority related to forensics principles would be required.

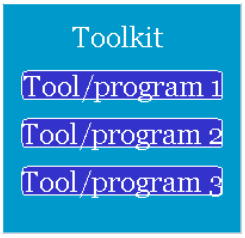

Figure 6: Relationships between Toolkit and tool/program

Incident Response Collection Report (IRCR)

IRCR is known to be the very first toolkits that developed for collecting live forensics information from the computer. In early year 2000, John McLeod [] originally wrote a script for collecting volatile information as well as performing incident response process in Perl. Without any ready-made, combined, all-in-one Windows Incident Response tools, John wrote the script for managing a selected list of incident response, security and forensics freeware tools.

After release of First Responders Evidence Disk (FRED) from Jesse Kornblum [], McLeod redesigned the scripts and rebuilt them in batch scripts. In that way, the scripts could be modified by forensics examiner depending on the execution requirement.

IRCR is a batch script in Microsoft DOS and Windows platform. It depends on a set of selected freeware programs. Investigators have to collect and provide the directory and links to all the programs before the scripts could be executed properly. Based on the scripts, IRCR collected command history, network connection, opened ports, current processes, registry startup information and even event logs from the target system.

First Responders Evidence Disk (FRED)

Shortly after McLeon developed IRCR, Jesse Kornblum wrote his First Responders Evidence Disk (FRED). Similar to IRCR, FRED is coded in batch scripts for managing a set of pre-selected freeware incident response and IT Security tools for collecting live and volatile forensics information.

Following the same school of thoughts on live forensics, FRED script initiates and executes the list of programs and stores the results to files with cryptographic checksum calculated after immediately after data collection. Investigator has to specify the location to store the output data. Investigator can also redirect the output to USB devices or remote network output directory depending on user specification.

Based on the selected 13 commands, FRED collected opened port number, current processes, current logged on users, network configuration, hidden streams, files in the C: and D: drives.

Windows Forensics Toolchest (WFT)

In year 2003, Monty McDougal presented a more comprehensive and sophisticated scheme for collecting volatile system information from a live system. He developed his toolchest following the generally acceptable principle in digital forensics based on (1) Maintain forensics integrity; (2) Require minimal user interaction; (3) Gather all pertinent information for later analysis.

WFT is designed, coded and compiled as executable program. Users cannot change the programming code or revise the order of execution. However, similar to IRCR and FRED, WFT relies on pre-existing freeware incident response and IT security programs for data acquisition. Through the WFT configuration files, list of freeware

tools cryptographic checksum and execution parameters, forensics investigation tools would be compared and analysed. Program with unmatched checksum would be highlighted.

In WFT, memory, file/directory timestamp, system information, port number, current process, user information, network configurations and all data collected in IRCR and FRED are also collected.

Not only including more incident handling and live forensics tools, WFT also includes a report generator for instant generation of HTML format report during the data acquisition process. The generated HTML output enables the investigator to navigator through the results in a user friendly way.

Modification of IRCR, FRED and WFT in Helix

The three Live Forensics toolkits described above are powerful toolkits for digital forensics investigators. However, investigators have to download and bring along all the set of forensics programs to be used by the toolkits. Without those programs, the toolkit would not be able to acquire forensics information. Besides, the programs directory and versions of the Operating System specific programs have to be specified and included in a program repository before execution which imposed extra operation effort to investigators.

In order to reduce the operation effort and user interaction with the target machine during the live forensics investigation, Helix, a live forensics CD-ROM was created. FRED, IRCR and WFT are included in the Helix as standard forensics toolkits. List of freeware tools that the three scripts required have also been stored into the CD-ROM. The links and directory of the required programs were also built to ensure that the FRED, IRCR and WFT can execute the corresponding files without any extract programming or operation effort. Investigator can simply select the options in the GUI with minimal user interaction.

Computer Online Forensic Evidence Extractor (COFEE)

In year 2006, inspired by WFT, Ricci Ieong started the development of Computer Online Forensic Evidence Extractor (COFEE) (Ieong 2006) COFEE uses batch script to manage a list of existing incident response tools and IT security tools volatile data forensics acquisition system similar to WFT, IRCR and FRED. But all the scripts, programs were stored on USB storage device before data acquisition.

Instead of requesting users to key in the output directory, COFEE automatically redirect the output to the inserted USB storage device. With the automatic OS version detection and storage assignment scheme, Operating System dependent program will be automatically selected after the version detection. Investigator only needs to insert the USB storage devices to the target machine and click one to two buttons in order to start the data acquisition process.

Another difference between COFEE with other live forensics toolkits is separation of the data acquisition procedures with the data examination procedures. In WFT, the report generation processes are executed immediately after the data acquisition process on the target machine. However, performing report generation on target machine may also alter the memory content in the target machine. As report generation does not necessarily be executed on target machine, therefore, only data acquisition programs, in COFEE, would be executed on target machines. All program selection, data examination and analysis processes would be performed on investigator machine.

Besides, more forensics programs are supported by COFEE such as screen capture and password capture tools.

EVALUATION CRITERIA OF LIVE DIGITAL FORENSICS TOOLKITS

Without a unique procedure for Live Forensics Investigation, evaluation of live forensics investigation tools should be situation dependent. Based on each situation, the live forensics investigation tool should be evaluated against the digital forensics principle and the Live Forensics best practices.

A yet to be published paper [Ienog and Chau 2007], highlighted the use of FORZA framework [Ieong 2006] to outline the best practices in live forensics investigation.

Without any standard procedures for live forensics investigation, static evaluation criteria could not be applied to live digital forensics investigation. Instead, the project team derived the following set of evaluation criteria based on these best practices.

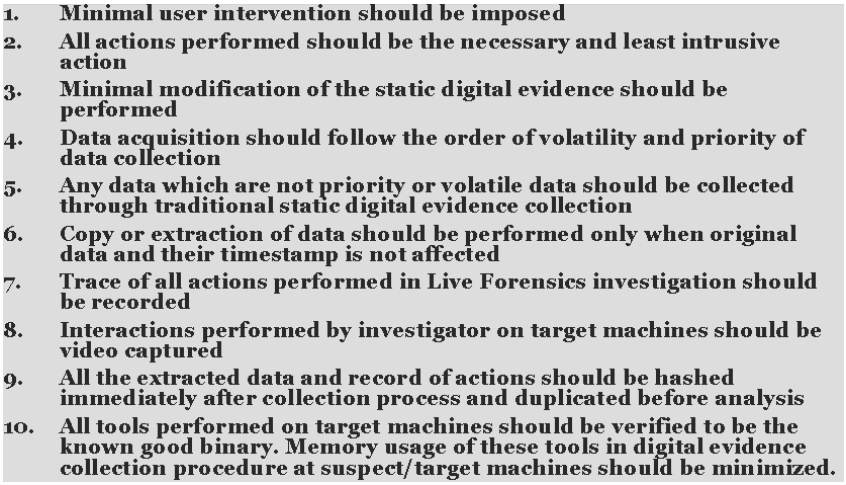

Figure 7: Highlight of Live Forensics Best Practices

Customizable and order of volatility

Firstly, without any investigation requirement specified, data should be acquired according to the order of volatility. Because highly volatile data could be tampered or affected throughout the investigation, if it is collected after some execution, part of the collected data may be altered during the investigation process and the data would be less acceptable to court.

With case officer or chief investigator requirement, Live Forensics Investigation execution order could be modified according to the specified requirement. It may not be necessary that all the volatile information has to be collected during the volatile data collection. It should be relevant and necessary for the investigation.

Time required

Similar to the previous requirement, only necessary data should be acquired. In some situation, live forensics investigation have to be performed within a short period of time, or some information has to be collected for investigator to make an urgent decision, then less relevant live forensics investigations may not have to be conducted.

Completeness

The longer time spent on data acquisition, the more data the tools could collect. However, time required and the order of volatility of data would be affecting the possibility of collecting all data from the target machine. Thus in the evaluation process, only relative completeness could be evaluated.

Accuracy and integrity

To ensure the data acquired is reliable and fair to both parties, data collected should be accurate with high integrity. Integrity verification of the live forensics data is different from traditional digital forensics investigation. In traditional digital forensics investigation, cryptographic checksum can be generated on collected data or hard disk any time when required. However, in live forensics investigation, the original state and data of the live environment would be destroyed after system shutdown. So data acquired during live forensics acquisition can only be verified against collected information instead of original data. Accuracy of the tools for collecting information becomes the important evaluation element.

Redundancy

In order to ensure that collected data can be provided to other parties for evaluation and counter-checking process, sets of live captured data should be preserved and duplicated before any data analysis and examination.

Preservation of memory

Both execution of live forensics investigation program and storage of data acquired before transferring to external data storage would be affecting or even tampering the memory of the target machine. Therefore the best live forensics tools should have least tamper to the memory.

Preservation of network status

As most of the live forensics data is related to network status and connection information, the live forensics tools should be measured against affect on network and changes induced to the network status.

Ease of use and review

After taking care of the functions and features of live forensics investigation, the live forensics investigation tools should be easy to use. Fewer the options to be chosen and fewer the input required, the lower the error induced in live forensics investigation. Therefore, live forensics investigation tools should have less user interaction at the target machine.

Record of actions

Finally, all the actions performed have to be recorded even in automatic investigation process. Program activities details, time, and parameters of the actions performed during the data acquisition process would be affecting the acceptability of the actions performed.

TESTING RESULTS AND ISSUES IN LIVE FORENSICS TOOLKITS

In this test, the project team performed live forensics data acquisition tests using the four selected toolkits on both desktop computer and notebook computer. The project team mainly focused on the time required, execution error, and results collected. Afterwards, scripts, generated logs and the memory status were evaluated before and after the program execution.

Using the evaluation framework proposed before, the project team concluded the findings in the following subsections. Overall ratings of the tools were summarized in the following table (shown in Table 1).

Order of execution

Test Method

Review of the execution methods, programs execution order and test results of each toolkit.

Test Results

Based on the listed live forensics investigation flow, it was observed that the four live forensics investigation toolboxes were not completely organized in the order of volatility. Most of their order of execution was arranged in the order of functionality. For instance, in WFT, even though memory has been extracted first, some less volatile data acquisition functions were executed before some more volatile data acquisition functions. More volatile (e.g. opened network ports information) was being collected after less volatile (e.g. services and drivers information).

Customizable

Test Method

Review of the execution methods, programs execution order, testing scripts and test results of each toolkit.

Test Results

Regarding to the current order of execution for tested tools, the four toolboxes were not especially tuned for particular investigation requirement. For FRED, IRCR and COFEE, as the execution scripts were coded using batch scripts, the order of execution can be rearranged by modifying the code. But WFT is written in executable program, so users cannot change the order of execution directly.

Besides, the order of scripts in COFEE was listed in a plain text file. Therefore, users can rearrange the program execution order without knowing batch script programming.

Time required

Test Method

Review of the program execution time and test results of each toolkit.

Test Results

Among all the data acquisition process, most toolkits could be completed in a short period of time. Usually, the slowest data acquisition steps are the memory acquisition process and the drive & directory browsing process. Without those two processes, data acquisition could be completed within 10 minutes.

FRED only required less than one minute for the complete data acquisition process. IRCR required around 3 – 5 minutes for execution which included checking of the hidden streams in the directory. While WFT and COFEE both collected system configuration, and memory, it took around 15 – 30 minutes to completely acquire the information on a P4 1.66GHz machine with 1.25G RAM.

However, during the test, it was observed that transfer rate of the output storage greatly affected the time required in the acquisition process. This observation will be discussed in later section of this paper.

Completeness

Test Method

Comparison of the program execution order, test results against execution order of live digital forensics flow.

Test Results

Among the four tested toolkits, it was observed that FRED, IRCR did not acquire all necessary data for the 3 situations listed in previous section. IRCR did not extract the physical memory, current opened files and resources opened by existing process. FRED did not collect physical memory and system configurations.

Accuracy, Integrity and Redundancy

Test Method

Extraction and review of the cryptographic checksum execution procedures from the test results and execution log records.

Test Results

All toolkits have included the cryptographic checksum execution throughout the execution of process. In FRED and IRCR, md5 checksum were generated after completion of the tools execution. COFEE generated sha1 and md5 checksum immediately after each raw text result generation.

WFT not only generated md5 checksum immediately after each raw text result generation, but also verified the checksum of all programs before each program execution. That helps in ensuring the chain of evidence.

In live forensics investigation, redundancy of data cannot be preserved and repeated. However, as the captured data is in raw data format, investigators can work on the duplicated copy of the raw data instead of directly manipulating the original data.

Preservation of memory

Test Method

Review of the memory, file access and list of dlls being used before and after the execution of the toolkits based on three sets of consecutive test results performed.

Test Results

Based on the collected results, no trend in memory usage increment or decrement was identified. It also confirmed that no trace of memory has been occupied and left behind by the executed freeware programs. However, as thorough memory analysis of each freeware program has not been conducted, further memory analysis should be conducted on individual freeware programs in order to certify these testing results.

Preservation of network status

Test Method

Review of the network connections, network status using netstat and fport before and after the execution of the toolkits.

Test Results

Based on the collected results, network status of the target machine were not affected or modified in standalone testing mode.

However, if the output were re-directed to a remote network connection, then the network connection and status would be affected. In order words, in Helix, when output of FRED or IRCR was being redirected through netcat to neighboring network address, new network connections were found.

Ease of use and review

Test Method

Review of the user interface, command execution scheme of the toolkits.

Test Results

FRED, IRCR and WFT were command line only tools. Execution parameters, tools directory and output directory were specified manually by the user. With Helix Live CD, toolkits were modified. Thus, FRED and WFT were executed after specifying the output directory in the Helix GUI. Whereas users were requested to specify the output IP address for redirecting IRCR output results to.

COFEE was written as command line toolkits, but it could be executed in GUI mode or in command line mode. For GUI mode operations, users were requested to click the start button, then tools executed in the pre-defined order.

Results from IRCR and FRED were displayed in plain text format while COFEE and WFT were kept in both plain text and HTML format.

Record of actions

Test Method

Review of the action log records and testing results of the toolkits.

Test Results

FRED and IRCR collected all the results in one single file with timestamp on the command executed. COFEE and WFT kept separate execution logs during the operations. Therefore, all schemes preserved the record of actions performed in the live investigation.

(H/M/L) [1]	FRED	IRCR	WFT	COFEE
Order of volatility	Low	Low	Low	Low
Customizable	Medium	Medium	Low	High
Time required	High	High	Medium	Medium

[1] The best result is ranked as high, the worst result is ranked as low.

Completeness	Low	Medium	High	High
Accuracy and integrity	Medium	Medium	High	Medium
Redundancy	Medium	Medium	Medium	Medium
Preservation of memory	High	Medium	Low	Medium
Preservation of network status	Medium	Medium	Medium	Medium
Ease of use and review	Low	Low	High	High
Record of actions	Medium	Medium	Medium	Medium

Table 1: Summary of Live Forensics Toolkits comparison results

OTHER SIDE ISSUES IDENTIFIED

In addition to the main track testing, the project team observed three additional side issues. They could be formulated as some operation tips in live forensics operations.

Hash/checksum and last access time

During the tests, it was observed that the cryptographic hashing functions, md5sum.exe, fciv.exe (Microsoft), sha1.exe modified the last access time of the file being hash. Only the md5.exe hashing function preserved the timestamp of the file through the input redirect functions in the Windows platform.

In other words, generation of cryptographic checksum may affect the last access time of the target file. Therefore, cryptographic checksum should only be performed on files where timestamps are not a critical to the investigation.

USB Storage Speed

In all test cases, it was observed that the time required in data acquisition not only depends on the CPU speed of the machine, memory of the machine, but also depends on the USB storage transfer speed. USB storage transfer speed is affected by USB version transfer speed, storage memory buffer and the storage devices write speed. Based on the speed tests performed, it was found that USB 2.0 transfer data almost 40 times faster than USB 1.1. If the target computer is using USB 1.1, the entire operation would be slow down by as much as 40 times.

Under USB 2.0, hard disk was found to be the fastest storage solution. The read and write speed are around 1 to 1.5 times than remote network drive. With faster rpm rate of the hard disk and more memory, the USB storage device can acquire data faster.

In USB 2.0 hard disk, the read and write speed were almost the same, but in USB 2.0 thumb drive, the read rate was almost 2 to 3 times faster than the write rate of the device.

	USB 2.0 Thumb Drive	USB 2.0 Hard disk	Remote Network drive (100M Ethernet)
Read time	12 – 17 MB/s	10 – 12 MB/s (4200 rpm) 20 – 28 MB/s (5400 rpm)	10 – 12.5MB/s
Write time	6 – 10 MB/s	6 – 11 MB/s (4200 rpm) 20 – 22 MB/s (5400 rpm)	4 – 12.5MB/s

Table 2: Table of USB 2.0 and network devices speed tests.

Although USB 2.0 hard disk storage is found to be faster than remote network drive, it is highly affected by the CPU utilization of the target machine. It was found that the USB write speed would be reduced if the CPU is utilization rate increases.

Administrative vs. Non-administrative rights

When performing live forensics investigation, it is assumed that the tools would be executed using administrative privilege. Without administrative rights, tools that required registry information execution, user account listing, system configuration, and even memory dump could not be executed.

In general, most of the useful information can only be collected with administrative rights and privilege account.

Antivirus effect on live forensics tools

Other than administrative rights issue, anti-virus tools also induces execution problem to live forensics investigation. Some of the live Forensics investigation freeware tools were considered as virus by anti-virus tools. For example, most password collection programs such as pwdump, and even the network connection tools, netcat were being classified as virus. Some anti-virus tools not only stop the program from being executed, but also quarantine the files from the tools repository.

CONCLUSION:

Live forensics investigation is considered to be an important step that accompanied traditional digital forensics investigation for creating a full picture in forensics investigation. Using the FORZA model, Ieong proposed a live forensics framework, the order of investigation execution and a set of best practices for live digital forensics investigation.

Based on that framework, the project team further derived the order of live forensics investigation for online illegal upload, web defacement and botnet investigation based on their nature and possible information that the case owner would like to collect.

Then the project team further extended the research work by introducing a set of live forensics evaluation criteria – *Customizable and order of volatility, Time required, Completeness, Accuracy and integrity, Redundancy, Preservation of memory, Preservation of network status, Ease of use and review, Record of actions*. Through this set of criteria, a set of tests on a desktop PC using 4 different freeware live forensics toolkits were performed.

However, because live digital forensics investigation is affected by accuracy of results extracted and physical memory being modified throughout the course of investigation, the project team considered that more experiments should be performed on all the toolkits to cover these aspect.

REFERENCES:

1. Ieong R. S. C. (2006), "COFEE Design Specification", *eWalker internal document,* 2006
2. Ieong R. S. C. (2006), "FORZA – Digital forensics investigation framework that incorporate legal issues", *Digital Forensics Research Workshop (DFRWS)*, 2006
3. Ieong R. S. C. and Chau H. C. (2007), "Deriving case specific live forensics investigation procedures from FORZA", *ACM SAC 2007, Korea*
4. John McLeod, "IRCR v2" URL , http://tools.phantombyte.com/
5. Jesse Kornblum, "Preservation of Fragile Digital Evidence by First Responders", *Digital Forensics Research Workshop (DFRWS)*, 2002
6. Kenneally, E.E. & Brown C.L.T. (2005). "Risk sensitive digital evidence collection", *Digital Investigation 2005*; 2(2), pp101 – 119

COPYRIGHT