

Novel First Responder Script as a Tool for Computer Forensics

Marjan Stoilkovski, Mitko Bogdanoski, Aleksandar Risteski

Abstract—The computer forensics as a branch of digital forensic pertaining to legal evidence found in computers and digital storage media. In order forensic acquisition to be more reliable it must be performed on computers that have been powered off. This type of forensics is known as 'traditional' or 'dead' forensic acquisition. However, this type of forensic cannot be used to collect and analyze the information which is not on the hard disk, or encrypted data. The disadvantages of the dead forensics can be overcome handling a live forensics acquisition process. There are many commercial and freeware tools which can be used to provide information based on live forensics acquisition. The problem with this tools is that in many cases the examiner cannot explain the script functionality and generated results and information. Because of this reason there is a increased need for developing and using script which can be easy explained and adapted to any analysis which should be made by the examiners. The paper presents a developed First Responder script which can be used to perform a live forensics analysis.

Keywords—computer forensics, script, response, examiners, analysis, Linux

I. Introduction

Nowadays, the security of information systems is crucial. There is almost no organization that does not take appropriate security measures on its own level in order to protect systems from external and internal attacks. To ensure an adequate level of security, the organizations have been establishing special CERT (Community Emergency Response Team) teams whose key objective is to increase information security in the organization. In case if there are no such teams established, this role is undertaken by system administrators, who must attend specialized training to perform those unique duties connected with cyber security.

Marjan Stoilkovski
Cybercrime Unit / Ministry of Interior
R. Macedonia
marjan_stoilkovski@moi.gov.mk

Mitko Bogdanoski
Military Academy "General Mihailo Apostolski" / University of Goce Delcev-
an associated member
R. Macedonia
mitko.bogdanoski@ugd.edu.mk

Aleksandar Risteski
Faculty of Electrical Engineering and Information Technologies / Ss Cyril
and Methodius University
R. Macedonia
acerist@feit.ukim.edu.mk

In order to increase the information security and users' awareness, all the users of the information systems in the organization should be trained about the secure usage of the systems, ethics in information system, and the way of reporting for any registered computer incident. The need for this training is because each of them can, intentionally or unintentionally, harm the security of the information systems, and consequently harm the security of the organization.

However, no matter how much the companies invest in information security and no matter how much the staff is trained, there will always be malicious users which driven by different motives will try to exploit vulnerabilities in hardware and software solutions in the company, as well as employees' negligence. Very often, the attackers in their intentions are supported by internal attacks made by employees in companies (insiders).

The goal of the companies is to stop attackers in the perimeter network, i.e. not to allow them to enter the internal network of the company / organization. The reason for this is that when the attacker enters in the internal network and systems the only thing left is to resist malicious users using computer forensics. However, very often the responsible for information security in the companies cannot catch the attackers at the perimeter network, so after registered intrusion into the system they must react immediately and analyze the intentions of the attackers. In order the analysis to be at the highest level the responsible for information security must be trained to make a detailed analysis of the attack and, if it is possible, to discover as many information about the attacker. Sure that, even the attacker is discovered, the intrusion must be reported and companies need to ask for assistance from the competent authorities to tackle cyber threats (law enforcement), and to initiate appropriate action against the attackers.

In whole this process of discovering the intentions of the attack, as well as detection of offenders, the computer forensics takes a main role. In the process of information gathering basic analysis will be performed using traditional forensics, but if there is the slightest chance, live forensics should be performed on the running computer systems. Using the live response the investigator can capture all the volatile data that will be lost as soon as the machine is powered down, such as the current configuration of the machine and the data in its RAM memory. It should be noted that, whether traditional or live forensics is performed, during the entire process of systems' analysis the investigators should avoid possible corruption of the original data.

The purpose of this paper is to provide basic concepts for live forensics and to explain its advantage when instead of automated software tools for computer forensics the investigators are using specially created scripts that are easy to

adapt as necessary, i.e. accordingly to the needs of the forensic examiners. For this purpose, the rest of the paper is organized as follows. Section 2 gives a brief overview of live computer forensics investigation process. Section 3 outlines the process of analysis of the RAM. In Section 4 the functionality and capabilities of the developed First Responder script is explained. Finally, the Section 5 concludes our work.

II. Live Computer Forensics

The process of traditional (dead) forensics is simple, reliable and thorough. The main strength of the dead forensic is precisely defined process of acquisition. During the dead forensics acquisition process can be verified at any time. However, this type of forensic cannot be used to collect and analyze the information which is not on the hard disk. Also in today's world criminals and terrorists more often use encryption as a response to the advances in the computer forensics. The problem of encrypted files is that even the examiner has an exact copy of an encrypted file, the analysis is not possible because of seemingly random data. There are many tools for disk and file encryption that can be used, as for example ArchiCrypt Live or BestCrypt. Shutting down the computer can cost losing other valuable data, as for example some important network data (i.e. open ports), decryption file for encrypted files, which can be stored in the volatile memory.

In order to response to the disadvantages of the dead acquisition against disc encryption and loss of the data from the volatile memory the live forensics acquisition was developed. The volatile data can be recovered and safely stored only using live forensics. This type of forensics gives chance to the analysts to collect volatile evidence in a format which can be read by the humans, instead of binary format. Live response is vital because after shutting down the computer all the information (evidence) from the volatile memory, which can be crucial during the analysis, will be lost. Actually, live response offers the ability to peer into the runtime state of the system providing valuable context for an investigation that had been historically lost with “snatch and grab methods”. Live data forensics requires a higher level of specialism than the procedures in the search and seizure of dead boxes. The live forensics process is shown on Figure 4 [1].

In the most of the cases live response is conducted using response toolkits [1, 2, 3, 4, 5, 6]. The easiest way for live response is by usage of automated wrapped programs. These programs are generic system administration tools that are utilized with few changes to support digital utilization. Similar information can also be collected using existing commercial agent-based systems. More advance method for live forensic response is by using of specially created scripts that run a series of command-line programs and redirect the output to a forensic workstation or peripheral media. Creating of this scripts requires advance programming knowledge, but can be very useful and can be adapted depending of the evidences which should be analyzed.

However, it must be noted that a live analysis is very sensitive, especially on risk getting false information because the software could maliciously hide or falsify data. The other problem is that the analysts might not have appropriate level of access to the investigated system.

Also, the attacker might have modified the system in a way that prevents detection of attack and modifications. [7]

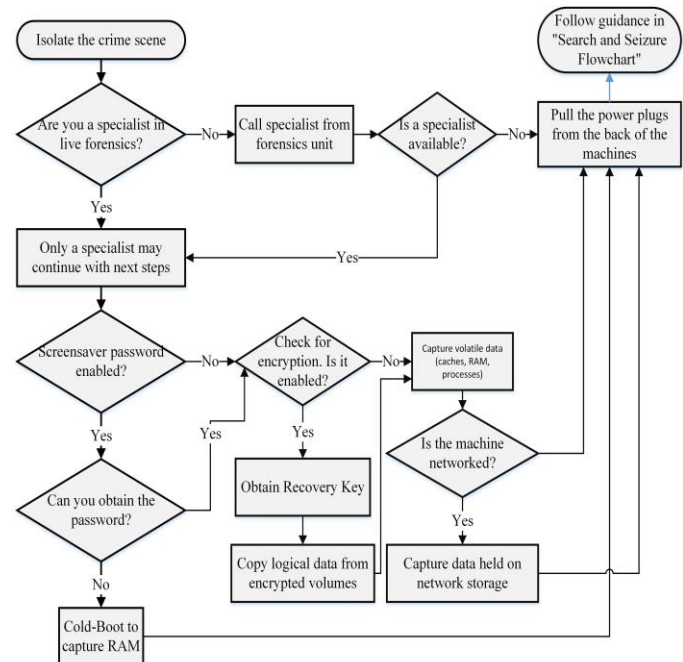


Figure 1. Live Data Forensics Flowchart

III. RAM Analysis

It is obvious that life data forensics requires a higher level of specialism than the procedures in the search and seizure of dead boxes. As the possibility of altering or even overwriting evidence during the investigation with live data forensics is very high it is more likely to be carried out by someone who is well educated and trained, as well as experienced.

There are many available freeware and commercial tools used in computer forensics or to obtain computer data and information from computer systems. This section lists some of the most used software tools by forensics investigators.

Some of the existing tools are multifunctional, which means that they can be used for many types of investigations and analysis, whereby the others are more focused, serving a fairly limited purposes. These software tools are focused on every specific type of digital evidence, deleted files, e-mails, network traffic, etc. During the software selection, a choice needs to be made between open source tools or a commercial products. Both of them have their advantages and disadvantages. Factors such as cost, functionality, capabilities, and support are some of the criteria that can be used to make this decision.

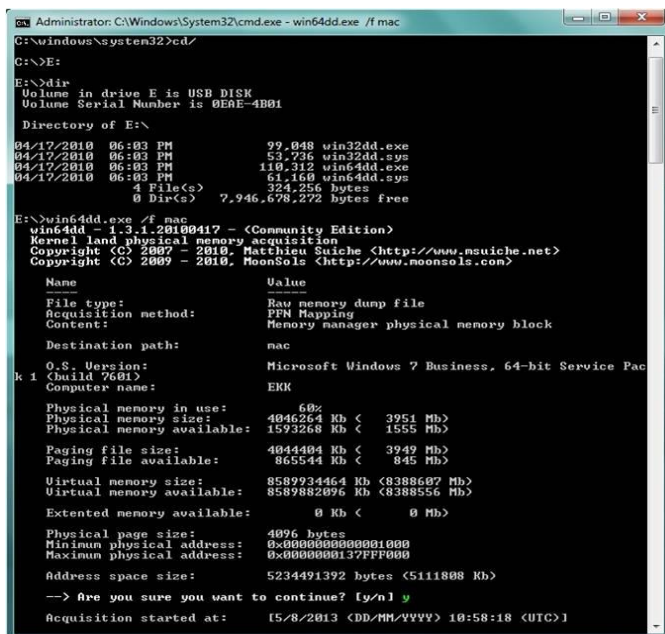
The main purpose why we decide to perform live data forensic are: encryption, malwares, remote storage, cloud

computing etc. The digital evidences and information that could be obtain with live data forensic in general are the volatile data as the data from RAM (Random-Access Memory), system processes, network activities. Moreover, the live data forensic tool could also analyze the dump of the disks and the images.

There are many available free tools for Live data forensics. Most of them are Linux based live CD's as Caine, Deft, Helix, Microsoft COFEE (Computer Online Forensics Evidence Extractor is Microsoft tool for live forensic for Law Enforcement Agencies-LEA) etc. The Linux based live CD's for live forensic use the same Linux base tools and commands.

The most performed action in the live forensics is acquisition of the RAM. There are many free available tools and live CD's which can be used to complete this task. The following example shows how **win32dd/win64dd** can be used for making a dump of the RAM memory (Figure 5).

win32dd.exe is a free kernel land tool to acquire physical memory, Executable can run as a command line tool, user prompt or from a configuration file. The **Win64dd.exe** can be run from a USB drive that is plugged into the target machine. The tool collects RAM and places the collected information into an .E01 file. There is a 32-bit version as well as a 64-bit version.



```

Administrator: C:\Windows\System32\cmd.exe - win64dd.exe /f mac
C:\Windows\system32>cd /
C:\>E:
E:\>dir
Volume in drive E is USB DISK
Volume Serial Number is 0EAE-4B01

Directory of E:\

04/17/2010  06:03 PM                99,848  win32dd.exe
04/17/2010  06:03 PM                53,736  win32dd.sys
04/17/2010  06:03 PM               110,312  win64dd.exe
04/17/2010  06:03 PM                61,168  win64dd.sys
                4 File(s)
                0 Dir(s)
                7,946,678,272 bytes free

E:\>win64dd.exe /f mac
win64dd - 1.3.1.20100417 - <Community Edition>
Kernel land physical memory acquisition
Copyright (C) 2007 - 2010, Matjeu Saiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Name
-----
File type:          Raw memory dump file
Acquisition method: PFM Mapping
Content:            Memory manager physical memory block

Destination path:  mac

O.S. Version:      Microsoft Windows 7 Business, 64-bit Service Pack 1
Build:             (build 7601)
Computer name:     ERK

Physical memory in use: 60%
Physical memory size: 4046264 Kb < 3951 Mb>
Physical memory available: 1593268 Kb < 1555 Mb>

Paging file size:   4044404 Kb < 3949 Mb>
Paging file available: 865544 Kb < 845 Mb>

Virtual memory size: 8589934464 Kb < 8388607 Mb>
Virtual memory available: 8589882096 Kb < 8388556 Mb>

Extended memory available: 0 Kb < 0 Mb>

Physical page size: 4096 bytes
Minimum physical address: 0x0000000000000000
Maximum physical address: 0x00000000137FFF0000
Address space size: 5234491392 bytes <511808 Kb>

-> Are you sure you want to continue? [y/n] y
Acquisition started at: 15/8/2013 (DD/MM/YYYY) 10:58:18 (UTC)
  
```

Figure 2. Using of win32dd/win64dd for making a dump of the RAM memory

After the RAM acquisition a file (mac 4GB) is created on the destination path that is defined when win64dd.exe from CMD (run as administrator) is executed (Figure 3).

Name	Date modified	Type	Size
mac	8/5/2013 1:17 PM	File	4,193,280 KB
win32dd.exe	4/17/2010 6:03 PM	Application	97 KB
win32dd.sys	4/17/2010 6:03 PM	System file	53 KB
win64dd.exe	4/17/2010 6:03 PM	Application	108 KB
win64dd.sys	4/17/2010 6:03 PM	System file	60 KB

Figure 3. Created file after the process of RAM acquisition

Search action through this file can be executed and also analysis of its complete content can be done. From the analysis we could expect to find the encryption passwords, unsaved documents or part of the documents, internet activities, mail messages and other information.

iv. First Responder Script

As we already mentioned, usage of the commercial forensics software can be more effective in the process of computer forensics and obtaining digital evidences, because they are professional made, easy to use with a GUI and have much functionalities. Also the usage of the freeware well known forensic software sometimes can really improve the work of the forensic examiner, and can help in the process of collection of evidence. The practical inconvenient comes when the examiner need to explain how he get the information and when he should explain to the not technical person the complete process of computer forensics. The problem also comes when he need to explain the work of the used software in order to obtain the digital evidence.

Building and developing the scripts for the concrete purpose and case, for many examiners is difficult because it need a time for building and testing, but also there are many different cases that make difficult to predict what scripts and software they will need. That is one of the reason why they usually use the commercial or some well know free forensic toolkit.

In this paper we are presenting a novel developed tool for first responders used for obtaining digital evidence on the scene. The script is bin/bash Linux based program that integrate some commands and tools from Linux.

```

MAIN_WORK () {
    echo "*****"
    >/tmp/mac.txt
    echo "***** FIRST RESPONDER *****"
    >>/tmp/mac.txt
    echo "*****"
    >>/tmp/mac.txt
    echo "
    REPUBLIC OF MACEDONIA
    "
    >>/tmp/mac.txt
    echo "
    MITKO BOGDANOVSKI
    "
    >>/tmp/mac.txt
    echo "
    MARJAN STOLIKOVSKI
    "
    >>/tmp/mac.txt
    echo "
    ALEKSANDAR RISTESKI
    "
    >>/tmp/mac.txt
    echo " " >>/tmp/mac.txt
    echo " " >>/tmp/mac.txt
    echo " "
  }
  
```

The Script is menu driven multi-functional software prepared to meet the basics needs of the first responders in order to collect digital evidence and information (Figure 4).

```

echo "***** WHAT_IS_IT *****"
echo "++ echo "++"
echo "++ FIRST RESPONDER is a bash script whit multiple functions as: ++"
echo "++"
echo "++ - LIST ALL DEVICES CONNECTED ON THE SYSTEM AND CHOSE A ++"
echo "++ DEVICES FOR MAKEING AN IMAGE, CARRY OUT THE PROCESS AND ++"
echo "++ VERIFYING THE IMAGE WITH COMPERING THE HASH VALUE FROM ++"
echo "++ THE ORIGINAL DEVICE AND FROM THE IMAGE ++"
echo "++ - COPY LIVE FILES OR DIRECTORY FROM THE SYSTEM TO EXTERNAL ++"
echo "++ DEVICE ++"
echo "++ - SEARCH BY KEY WORD OR STRING, AND COPY THE MATCH FILES ++"
echo "++ TO A CHOISEN DIRECTORY ++"
echo "++ - SEARCH THE FILES BY EXTENSION AND COPY THEM IN A CHOISEN ++"
echo "++ DIRECTORY FOR ANALYSES ++"
echo "++ - DATA CARVING (carvin the .jpg files from image) ++"
echo "++"
echo "++ The script is going to show all process information on the ++"
echo "++ terminal, but also for those information can be created ++"
echo "++ report_file (e.g. mac.txt) as shown in. main_work function. ++"
echo "++"
  
```



```

FN=$(cat $OUTDIR/macsearch.txt | awk -F ":" '{print
$1}' | sed 's/*//')
cp $INDIR/$FN $OUTDIR 2>/dev/null
cd $OUTDIR
ls -l
echo "The search is finished, all the files are in you
directory"
fi

```

The third available option in the script gives a possibility for any file or directory to be copied from one destination to another if the first responder decides to copy any file.

```

if [ "$MACHINE" -eq 3 ]
then
echo "Enter the source dir/file"
read SOURCE
ls -l $SOURCE
echo " "
echo " "
echo "Enter the file or dir that you would like to copy"
read SOURCENAME
echo " "
echo " "
df -h
echo " "
echo "Enter the destination dir/file"
echo " "
read TARGET
[ ! -d "$TARGET" ] && mkdir -p $TARGET
echo " "
cp /$SOURCE/$SOURCENAME $TARGET
echo "successful copied" $SOURCENAME "to" $TARGET
fi

```

The fourth option from the script actually is data carving. With this script the first responder could find, copy and analyze all the images (jpg) on the image file.

```

if [ "$MACHINE" -eq 4 ]
then
echo "Enter the path where is the image"
read PAT
ls $PAT
echo " "
echo -n "Please enter the name of the image to carve from: "
read IMAGENAME
STARTLINE=`xxd $IMAGENAME | grep ffd8`
echo "Possible start of JPEG found here:"
echo $STARTLINE
OFFSET=`echo $STARTLINE | awk -F: '{print $1}' | tr a-f A-F`
DECOFFSET=`echo "ibase=16;$OFFSET" | bc`
echo -n "Please enter how many bytes from the start of the
line ffd8 appears at: "
read BYTES
START=`echo "$DECOFFSET+$BYTES" | bc`
echo "Possible end of JPEG found here:"
ENDLINE=`xxd -s $START image_carve.raw | grep ffd9`
echo $ENDLINE
OFFSET=`echo $ENDLINE | awk -F: '{print $1}' | tr a-f A-F`
DECOFFSET=`echo "ibase=16;$OFFSET" | bc`
echo -n "Please enter how many bytes from the start of the
line ffd9 ends at: "
read BYTES
END=`echo "$DECOFFSET+$BYTES" | bc`
SIZE=`echo "$END-$START" | bc`
echo -n "Please enter the name of the JPEG file extracted: "
read JPEGNAME
dd if=$IMAGENAME of=$JPEGNAME skip=$START bs=1 count=$SIZE
fi

```

The fifth option in the script for the first responder is extension analyses. The user could filter all the "files with the same "suspect" extension and the copy it in particular folder for extended analyses.

```

if [ "$MACHINE" -eq 5 ]
then
echo "Enter the file extension"
echo "If the needed extension is specified in the script,
live this filed blank"
read EXTENSIONS
echo " "
echo "Enter the source dir/file"
read SOURCEDIR
ls $SOURCEDIR
echo " "
echo " "
df -h | grep "/dev"
echo " "
echo "Enter the destination dir/file"
read TARGETDIR

```

```

echo " "
#cp $(find $SOURCEDIR -type f | grep -iE '\.($EXTENSIONS)$')
$TARGETDIR
cp $(find $SOURCEDIR -type f | grep -iE
'\.(jpg|tif|bmp|psd|pdd|gif|pdf)$') $TARGETDIR
echo " "
echo "the suspect files are in the TARGET directory, for
conntents analyse process"
fi

```

For completing all functionalities, a log file (mac.txt) will be created that records every step and any activity on the target computer using the script.

The developed script contains five main functions, and provides an easy to use functions allowed by the easy accessible integrated menu. This script is open to upgrade and improve with additional functionality that can contribute for more effective work of the first responders.

v. Conclusion

The aim of this paper is to show the importance of the life computer forensics during the computer incidents analysis. In order to show the importance of the life forensics the paper firstly shows the flowchart for the live data forensics, describing all the steps which should be taken by the examiners during the analysis. Then the paper gives an explanation of the process of RAM analysis. At the end the paper presents the new developed First Responder script for live forensics which is bin/bash Linux based program that integrate some commands and tools from Linux. The developed script is menu driven multi-functional software prepared to meet the basics needs of the first responders in order to collect digital evidence and information. It actually contains five main functions, and provides an easy to use functions allowed by the easy accessible integrated menu. It is open platform which can be easy upgraded and improved with additional functionality that can contribute for more effective work of the first responders.

References

- [1] Council of Europe, Electronic evidence guide, "A basic guide for police officers, prosecutors and judges," Version 1.0, EU/COE Joint Project on Regional Cooperation against Cybercrime March 2013
- [2] C. Waits, J. A. Akinyele, R. Nolan, L. Rogers, "Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis," August 2008
- [3] K. Mandia, C Prorise and M, Pepe, " Incident Response and Computer Forensics," McGraw-Hill Osborne Media, 2nd edition, 2003
- [4] M. McDougal, "Windows Forensic Toolchest," January 2007
- [5] J. Moeller, "Windows Vista Forensic Jumpstart Part I and Part II," January 2007, DoD Cyber Cryme Conference 2007
- [6] J. Kornblum, "Preservation of Fragile Digital Evidence by First Responders," In Proceedings of 2002 Digital Forensic Research Workshop (DFRWS), 2002
- [7] S. Mrdovic, A. Huseinovic, E. Zajko, "Combining Static and Live Digital Forensic Analysis in Virtual Environment," 22nd International Symposium on Information, Communication and Automation Technologies (2009).