Exploring Digital Forensics Tools in Cyborg Hawk Linux

© Nataliia P. Tmienova © Oleg E. Ilarionov © Nina M. Ilarionova
Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine
tmyenovox@gmail.com oilarionov@gmail.com ilarionovanm@gmail.com

Abstracts

Computer forensics (software and technical expertise) belongs to the category of engineering and technical expertise. It is an important element in a number of computer expertises, because it allows to build a holistic system of evidence comprehensively. The importance of computer forensics is explained by the increased role of the computers in the modern world. A huge number of offenses and crimes is committed precisely with the help of computer technologies. The computer forensics and expertise of computer equipment is especially relevant in criminal and civil cases. Expertise of computers, hardware, software, databases due to the continuous improvement of computer equipment and software is one of the most complex types of research.

The community of free software developers is constantly creating assemblies of utilities designed for software and technical expertise. The most popular is the KaliLinux collection, whereas Cyborg Hawk Linux is undeservedly ignored.

The purpose of our research is to describe the capabilities of the Cyborg Hawk Linux tools.

Keywords: computer forensics, software and technical expertise, forensic tools, open source tools, proprietary tools, penetration testing distributions.

1 Introduction

Development of information technologies, penetration of computer technology advancements into applied and scientific sphere and into everyday human life has its drawbacks, unfortunately. There are many intruders who use these achievements for mercenary, criminal purposes. In this regard, there is a need to transform special knowledge from the field of computer information into the field of forensic science to uncover and investigate crimes that relate to computer technologies. Computer forensic allows obtaining the most reliable information concerning computer crimes. This type of research is widely used in consideration of cases in civil and criminal legal proceedings and is one of the most relevant and demanded.

Computer forensics covers a broad range of activities associated with identifying, extracting, and considering evidences from digital media. It can be defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence [1] derived from volatile and non-volatile media storage [2]. Various hardware, software, and information objects are objects of computer forensics.

Computer forensics can be divided into the following types: hardware, software, network, and information forensics. The following methods are used in the process of computer forensics:

- ✓ method of software research;
- ✓ method of hardware research;
- ✓ method of information research.

Carrying out of software and technical expertise is necessary in cases when a crime or an offense was implemented with using computer facilities or information data, and when special knowledge in the field of computer technology is required to establish traces of crime and other forensically significant information. In particular, software and technical expertise provides the solution of the following expert tasks:

- ✓ identification of properties, qualities, status and features of the using of technical computer systems;
- ✓ establishing the development and using features of software products;
- ✓ establishing the facts of the equipment use during the documents creating or committing other actions related to the crime;
- ✓ access to information on attached devices;
- ✓ research information created by a user or a program for the implementation of information processes;
- ✓ establishing the features of the functioning of the computer facilities which implement network information technology.

Computer forensics is used to find out the digital evidence using different tools. It is quite difficult and complex process. Digital investigations take place in three main phases. In first phase, the investigator takes images of digital device and copies these images from the target device to some other device for in-depth analysis. In second phase, which is called analysis, the investigator identifies the digital evidence using different types of techniques such as recovering the deleted files, obtaining information of user accounts, identifying information about the attached devices like USB, CD/DVD drives, external hard disks and so on. The third phase is called reporting in which the investigator reconstructs the actual scenario based on the sequence of activities happened on the target system [3].

Digital forensic analysis is divided into two main categories. The first category is the static forensic analysis.

During this analysis, all the target devices that are required in the analysis are shutdown. The second category is live analysis. During this type of analysis, the system stays in the boot mode [4] to acquire pertinent information from the physical memory content.

Live analysis aims at gathering evidence from systems using different operations and techniques related to primary memory content. Live forensic is the most challenging kind of digital forensic investigations. To perform the live forensics, it is vital to understand the basic techniques and tools used in digital forensics. The investigator needs to acquire the complete image of a computer usage history as well as the current state through live forensic analysis tools. Though static analysis is kind of a developed part of digital forensics, but other techniques related to live analysis need to be developed to mitigate its weaknesses [3].

Classifications of computer forensics tools include open source, proprietary, hardware, software, special purpose and general purpose [5]. Each tool has its own advantages and disadvantages. The choice of forensics tools depends on the nature of the studying, the obtained results, the requirements for safety and economic efficiency of the tool.

Brian Career [6] reports that open source tools are as effective and reliable as proprietary tools. Manson and his team [7] compared one open source tool and two commercial tools. They found that all three tools produced the same results with different degree of difficulty.

2 Description of the most popular tools designed for carrying out software and technical expertise

The community of free software developers is constantly creating assemblies of utilities designed for software and technical expertise. A comprehensive review of the top twenty open source free computer forensics investigation tools can be found in [8]. For a list of proprietary computer forensics tools see [9] and [10].

The most popular assemblies of utilities intended for carrying out software and technical expertise are:

- Kali Linux [11] – Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services.
- CAINE [12] (Computer Aided Investigative Environment) – CAINE is the Linux distro created for digital forensics. It offers an environment to integrate existing software tools as software modules in a user friendly manner. This tool is open source.
- DEFT [13] (Digital Evidence & Forensic Toolkit) – The Linux distribution DEFT is made up of a GNU / Linux and DART (Digital Advanced Response Toolkit), suite dedicated to digital forensics and intelligence activities.
- PHLAK [14] (Professional Hacker's Linux Assault Kit) – PHLAK is a modular LiveCD Linux distribution with a focus on pen-testing, forensics, and network analysis. It includes two lightweight GUIs (XFCE4 and Fluxbox) and loads of tools, including crackers, sniffers, MITM utilities, and data recovery and duplication utilities.
- Cyborg Hawk Linux [15] – Cyborg Hawk Linux is a Ubuntu based Linux Hacking Distro also known as a Pentesting Linux Distro it is developed and designed for ethical hackers and penetration testers. Cyborg Hawk Distro can be used for network security and assessment and also for digital forensics. It also has various tools suited to the testing of Mobile Security and Wireless infrastructure.
- BackTrack 5 R3[16]–BackTrack is intended for all audiences from the most savvy security professionals to early newcomers to the information security field. BackTrack promotes a quick and easy way to find and update the largest database of security tools collection to-date.
- Parrot Security OS [17] – Parrot Security OS is a cloud friendly operating system designed for Pentesting, Computer Forensic, Reverse engineering, Hacking, Cloud pentesting, privacy/anonimity and cryptography. Based on Debian and developed by Frozenbox network.
- BackBox Linux[18]–BackBox is a Linux distribution based on Ubuntu. It has been developed to perform penetration tests and security assessments. Designed to be fast, easy to use and provide a minimal yet complete desktop environment, thanks to its own software repositories, always being updated to the latest stable version of the most used and best known ethical hacking tools.

The using of assembly, rather than individual software tools, can improve reliability, safety and performance.

The most popular compilation is the KaliLinux, which contains about 300 utilities, whereas Cyborg Hawk Linux [15], which contains more than 800 tools, is undeservedly ignored.

The purpose of our research is to describe the capabilities of the Cyborg Hawk Linux tools.

3 Our Virtual Machine Platform

Cyborg Hawk is a Linux based operating system that comes with a rich repository of security and forensics tools. The computer forensics tools are grouped into several categories. We use the forensics tools within the Cyborg Hawk.

VMware Workstation is a hypervisor that runs on 64-bit computers [19]. It enables us to set up multiple virtual machines and network them together. Each virtual machine can execute on different distribution of Linux operating system. VMware Workstation is proprietary software but we used the trail version for free. Below are the steps for setting up the platform for our experiment.

1. Install VMware Workstation on a machine;
2. Create a virtual machine on the VMware workstation;
3. Install Cyborg Hawk Linux on the virtual machine;
4. Launch Cyborg Hawk Linux from the virtual machine;
5. From the list, select forensics and then select a tool.

4 Description of the Cyborg Hawk Linux tools

The Cyborg Hawk Linux disk image was investigated on a VMware Workstation virtual machine running on a 64-bit computer.

There are 15 classes in the Cyborg Hawk Linux software analysis toolkit, each of which is divided into categories and subcategories that contain different number of utilities (table 1).

Several utilities have been selected in each category. For each of them we investigated its purpose, sequence and results of work on our virtual machine. One of the conclusions of the studying is that many utilities perform several functions and thus they belong to different classes and categories in the collection. Therefore, the number of original programs is much smaller than were stated by the developers of the assembly. In addition, a significant limitation in using of the assembly is that it is only designed to work with 64-bit processors.

5 Forensics Tools Experiment

There are several categories of computer forensic tools in the disk image of Cyborg Hawk Linux v1. Some categories have several tools. In the following subsections we will study the tools for Forensics.

5.1 Acquisition

Twenty one tools of this category are divided into 10 groups.

Let's consider the basic packages of tools.

AFF Package (*affcat, affconvert*) orthe Advanced Forensics Format (AFF).AFF was created as an open and extensible file format for storing disk images and associated metadata. The goal was to create a disk imaging format that would not block users into their proprietary format, which can limit its analysis. The open standard allows researchers use their preferred tools for solving crimes, collecting information and resolving security incidents quickly and efficiently. The format was implemented in AFFLIB which was distributed with an open source license.

Img package(*img_cat, img_stat*) outputs the contents of an image file. Image files that are not raw will have embedded data and metadata. *Img_cat* will output only the data. This allows you to convert an embedded format to raw or to calculate the MD5 hash of the data by piping the output to the appropriate tool.

Img package displays the contents of the image file. Image files that are not raw will have built-in data and metadata. Img_cat will return only data. This allows converting the built-in format to raw or calculating the MD5 hash of the data by submitting the output to the appropriate tool.

TSK KIT(*tsk_comparedir, tsk_gettimes, tsk_loaddb, tsk_recover*)– compare the contents of a directory with the contents of an image or local device.Sleuth Kit (TSK) allows exploring the compromised file system of a computer. TSK is a collection of UNIX command-line tools that can analyze NTFS, FAT, FFS, EXT2FS, and EXT3FS file systems. TASK reads and processes the file system structures independently, so the file system of the operating system does not need support.

5.2 Cryptography

There are 4 tools in this category (*Luks-Ops, TrueCrack, TrueCrypt, Tcpcryptd*).

TrueCrypt is a program for installing and maintaining a drive immediately. Immediate encryption means that the data is automatically encrypted or decrypted immediately before downloading or saving it without user intervention. Any data stored on the encrypted volume can be read (decrypted) without using the correct password or the correct encryption key. The *TrueCrypt* volume before decryption is nothing more than a series of random numbers.

5.3 Data recovery

The tools of this category are divided into four groups (*Carving Tools, Password Forensics, PDF Forensics, Ram Forensics*).

Carving Tools contains 20 programs that specialize in recovering files, missing disk partitions, etc.

Password Forensics contains 3 programs (*chntpw, md5deep, rahash2*), which allow to delete passwords to Windows, calculate and compare MD5 hash-functions and checksums. The main set of tools for password security is in the category of the fourth class (table 1).

Table 1. Classes and tools category in Cyborg Hawk Linux

Class	Category	Number of tools
1. Information Gathering	Network investigation	68
	Proxy	3
	VPN analysis	3
	Web inventory	63
2.Vulnerability assessment	Network	14
	Web application	68
3. Exploitation Toolkit	BeEFframework	1
	Database	5
	Network	23
	Social Engineering	2
	Web offense	19
4. Privelege Escalation	Password attacks	66
	Listening to channels (sniffing)	29
	Substitution (spoofing)	31
5. Maintaining Access		25
6. Reporting	Evidence handling	7
	Radio seize	2
	Software documentation	2
7. Reverse engineering	Debuggers	4
	Disassembly	6
	Exploit development tools	4
	Tools for modeling (RE Tools)	15
8. Stress tests	DOS	21
	Fuzzer	22
	Wlan stress testing	2
9. Forensics	Acquisition	21
	Cryptography	4
	Data recovery	42
	Digital anti-forensics	1
	Digital forensics	14
	Forensics evaluation tools	40
	Forensics suite	5
	Network investigation	2
	Secure wipe	4
	Steganography	8
10. Wireless Toolkit	Bluetooth	25
	Miscellaneous tools	8
	Radio/radar monitoring	10
	WiFi	36
11. RFID / NFC tools	Network	43
12. Hardware Hacking		4
13. VOIP Analysis		24
14. Mobile Security	Development Tools	3
	Device Forensics	9
	Penetration testing	9
	Reverse Engineering	20
	Wireless analyzers	6
15. Malware Analysis	Anti malware	2
	Malware lab	6

PDF Forensics: This tool will parse a PDF document to identify the fundamental elements used in the analyzed file. It will not render a PDF document.

Ram Forensics: *volafox* and *volatility* are the tools for working with memory dumps of RAM. Supports memory dumps from all major operating systems.

5.4 Digital anti-forensics

Chkrootkit is the only tool in this category. *Chkrootkit* is a scanner that monitors the presence of rootkits on the local system by some search attributes. The program has several modules to search for rootkits and other unsafe objects. As expected, rootkits in our virtual machine were not detected.

5.5 Digital forensics

There are14 tools in this category (*autopsy, binwalk, bulk_extractor, chkrootkit, dc3dd, dcfldd, extundelete, foremost, fsstat, galleta, tsk_comparedir, tsk_gettimes, tsk_loaddb, tsk_recover*).

5.6 Forensics evaluation tools

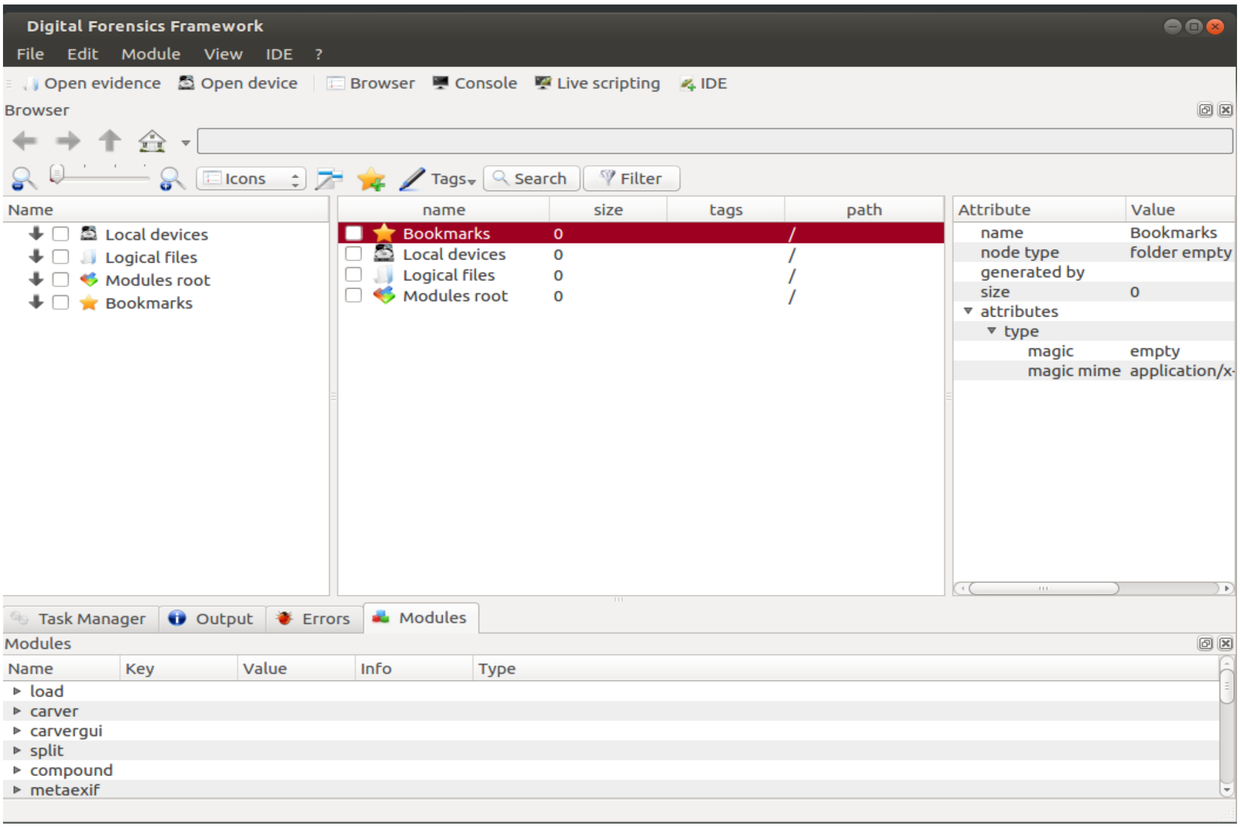
There are40 tools in this category (*affcompare, affcopy, affcrypto, affdiskprint, affinfo, affsign, affstats, affuse, affverify, affxml, autopsy, binwalk, blkcalc, blkcat, blkstat, bulk_extractor, cuckoo, ffind, fls, foremost, galleta, hfind, icat-sleuthkit, ifind, ils-sleuthkit, istat, jcat, mactime-sleuthkit, missidentify, mmcat, pdgmail, readpst, reglookup, reglookup-timeline, reglookup-recover, SIGFIND, sorter, srch-strings, tsk_recover, vinetto*).

AFF Packagewas considered in 5.1.

Libewf package(*ewfacquire, ewfacquirestream, ewfexport, ewfinfo, ewfverify*)writes data of data carriers from devices and files into EWF files.*Ewfacquire* can be used to create disk images in the EWF format. It includes several message digests including MD5 and SHA1. To create an image of */dev/sdb1* and logging data to */root/Desktop/log.txt*, we obtained the image by issuing this command on CyborgLinux*ewfacquire -d sha1 -l /root/Desktop/log.txt /dev/sdb1.*

5.7 Forensics suite

There are 5 tools in this category (*autopsy, capstone, dff, dff-gui, dumpzilla*). DFF (Digital Forensics Framework) is used to collect, preserve and identify digital evidence. We need to load pre-prepared file with a forensic image into DFF and analyze the data file by one of the built-in modules (figure 1).



Name
Local devices
Logical files
Modules root
Bookmarks

name	size	tags	path
Bookmarks	0		/
Local devices	0		/
Logical files	0		/
Modules root	0		/

Attribute	Value
name	Bookmarks
node type	folder empty
generated by	
size	0
▾ attributes	
▾ type	
magic	empty
magic mime	application/x-

Modules

Name	Key	Value	Info	Type
▸ load				
▸ carver				
▸ carvergui				
▸ split				
▸ compound				
▸ metaexif				

Figure 1. DFF analysis of evidence

5.8 Network investigation

There are 2 tools in this category (*p0f, xplico*).

P0f is a passive operating systems fingerprinting tool. All the host has to do is connect to the same network or be contacted by another host on the network. The packets generated through these transactions gives p0f enough data to guess the system. In our experiment, by issuing the command *p0f -f /etc/p0f -i eth0*, we were able to read fingerprints from */etc/p0f* and listen on eth0 via libpcap application.

Xplico is a Network Forensic Analysis Tool (NFAT) that is capable of extracting application data from packet capture files. It is best suited for offline analysis of PCAP files but it can also analyze live traffic. Xplico can extract email, HTTP, VoIP, FTP, and other data directly from the PCAP files. It is able to recognize the protocols with a technique named Port Independent Protocol Identification (PIPI).

5.9 Secure wipe

The tools in this category include 4 tools (*sdmem, sfill, srm, sswap*).

5.10 Steganography

8 tools of this category are divided into 2 groups.

Steg Toolkit(*stegbreak, stegcompare, stegdetect, stegdeimage, steghide*) isused for the embedding system and the password when the attack succeeded for an image.

Snowdrop is intended to bring (relatively) invisible and modification-proof watermarking to a new realm of "source material" – written word and computer source codes. The information is not being embedded in the least significant portions of some binary output, as it would be with a traditional low-level steganography, but into the source itself.

Vinetto extracts the thumbnails and associated metadata from the Thumbs.db files.

Outguess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources. The nature of the data source is irrelevant to the core of outguess. The program relies on data specific handlers that will extract redundant bits and write them back after modification. Currently only the PPM, PNM, and JPEG image formats are supported, although outguess could use any kind of data, as long as a handler were provided.

Stegdetectwill look for signatures of several well-known steganography embedding programs in order to alert the user that text may be embedded in the image file, such as jpeg. To see if there is steganography embedded message in our *n.jpg* file in a USB drive, we launched *Stegdetect*by using this command:*stegdetect -t /media/cyborg/B4FE-5315/n.jpg.*

The result of executing the utility is shown below:*stegdetect -t /media/cyborg/B4FE-5315/n.jpg: negative,* where*negative* indicates no message embedded in the *n.jpg* file.

5 Conclusions

In this paper we have demonstrated the application of various computer forensics tools on Cyborg Hawk Linux. We showed the syntax for using the tools and the result of executing the tools on our virtual machine. As it was demonstrated the tools produce consistent results according to their specifications. However, similar results can be obtained by using physical machines. Our results will help the computer forensics investigators on selecting appropriate tool for a specific purpose. It also helps penetration testers to check for signs of vulnerabilities on their system. We showed that Cyborg Hawk Linux is a good choice for forensics investigators for several reasons. These include that the tools are free, easy to use, do not need configuration, and produce consistent results.

References

1. O.L. Carroll, S.K. Brannon, and T. Song, "Computer forensics: Digital forensic analysis methodology",*Comp. Forensic*, vol. 56, no. 1, pp. 1-8, Jan.2008.
2. M. Meyers and M. Rogers, "Computer forensics: The need for standardization and certification",*Int. J. Digit. Evidence*, vol. 3, no. 2, pp.1-11, Sep.2004.
3. S. Rahman and M. N. A. Khan, "Review of live forensic analysis techniques",*Int. J. of Hybrid Inf. Technology*,vol.8, no.2, pp.379-388, 2015
4. S. Yadav, "Analysis of digital forensic and investigation",*VSRD-IJCSIT*, vol. 1, no. 3, pp. 171-178, 2011
5. A.Ghafarian, H. Seno, and S. Amin. "Exploring digital forensics tools in Backtrack 5.0 r3".*Proceedings of International Conference on Security and Management - SAM'14*, 2014.
6. B. Carrier "Open source digital forensics tools: The legal argument". *AtStake*. Oct. 2002. [Online]. Available: http://dl.packetstormsecurity.net/papers/IDS/atstake_opensource_forensics.pdf[Accessed Oct. 27, 2017]
7. D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, and J. Treichelt. "Is the open way a better way? Digital forensics using open source tools". *System Sciences. HICSS 2007. 40th Annual Hawaii International Conference on Science*, pp 266-270. [Online]. Available: https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550266b.pdf[Accessed Oct. 27, 2017]
8. A.Z. Tabona"Top 20 free digital forensics investigation tools for sysadmins".[Online]. 2002.Available :http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/ [Accessed Oct. 27, 2017]
9. Wikipedia, "List of digital forensics tools". [Online]. Available :http://en.wikipedia.org/wiki/List_of_digital_forensics_tools [Accessed Oct. 27, 2017]
10. Mares and Company,"Alphabetical list of links to manufacturers, suppliers, and products".[Online]. Available http://www.dmares.com/maresware/linksto_forensic_tools.htm [Accessed Oct. 27, 2017]

11. KaliLinux[Online]. Available: https://www.kali.org/[Accessed Oct. 27, 2017]
12. CAINE (Computer Aided INvestigative Environment) [Online]. Available: http://www.caine-live.net/[Accessed Oct. 27, 2017]
13. DEFT (Digital Evidence & Forensics Toolkit) [Online]. Available:http://www.deftlinux.net/[Accessed Oct. 27, 2017]
14. PHLAK [Online]. Available:https://sourceforge.net/projects/phlakproject/[Accessed Oct. 27, 2017]
15. Cyborg Hawk Linux [Online]. Available:http://cyborg.ztrela.com/[Accessed Oct. 27, 2017]
16. BackTrack[Online]. Available:http://www.backtrack-linux.org/[Accessed Oct. 27, 2017]
17. Parrot Security OS [Online]. Available:https://www.parrotsec.org/[Accessed Oct. 27, 2017]
18. BackBox Linux [Online]. Available:https://backbox.org/[Accessed Oct. 27, 2017]
19. VMware [Online]. Available: http://www.vmware.com[Accessed Oct. 27, 2017]