Levi Seibert

00086809

lseiber1@my.athens.edu

11/16/2020

Kali Linux's Usefulness for Computer Forensics

Kali Linux (formerly known as Backtrack) is a free, open source Linux operating system developed by Offensive Security for use in information security and penetration testing services (Shah, *10 Best Known Forensics Tools That Works on Linux*). The operating system has several pre-installed, free tools that are available for use by both computer amateurs and professionals in the fields of vulnerability analysis, password attacks, wireless attacks, sniffing & snooping, and significantly, forensics. The four main forensic tools that come installed on Kali Linux are Autopsy, Binwalk, Bulk_Extractor, and Hashdeep. Some of the other forensic tools already on Kali Linux include Guymager and tools used for file carving and PDF forensics. Additionally, there are several tools that are not designed for forensic investigations that still may prove useful in an examination. Besides having all these third-party tools freely available to its users, Kali Linux itself is an excellent tool for forensic investigations. The combination of the operating system and the plethora of preinstalled tools makes Kali Linux an excellent instrument for investigations and examinations.

For those who are unfamiliar with Kali Linux, the following paragraph may be helpful if one wants to try it out. I have created a Kali Linux (default mode) virtual machine set up in Oracle VM VirtualBox. Instructions to set up a similar Kali virtual machine can be found online and differ by machine and user preferences. It will be assumed that the user is using VirtualBox and has already created a machine with Kali Linux as the operating system. To get started using Kali for forensic related work, the user should select the aforementioned Kali Linux machine from the available machines in VirtulBox and select start. After the operating system loads up, a login screen will appear, asking for the user to enter the root password. After the user inputs the correct password, the computer will login in and the graphical desktop will appear. From there, the user can choose whether to open the terminal and use built-in Kali tools (the shortcut is in the taskbar on the side of the screen) or to choose one of the forensic tools from the list of applications (Sublist 11: Forensics; see **Figure 1**). The user can then use the following information for the given utility they wish employ for their forensic endeavors.

Kali Linux, like most Linux operating systems (and most operating systems in general), have several built-in forensic capabilities. Obviously, the tools that come with the operating system make the product a lot more sophisticated and involved but the stand-alone operating system does have several forensic capabilities built into it. For example, Kali has the ability to mount drives, hash files, and view file details. It also can be used to check network connectivity (ifconfig) and open ports. These actions, along with numerous others, are performed from the root terminal and can provide the examiner with pertinent information without making use of a third-party application. Examine **Figure 2** for an example of some of these terminal-based forensic tools. Another handy feature that Kali Linux possesses is the ability to boot the operating system in Forensics Mode, which will protect the internal hard drive from changes and will disable the auto-mounting of removable media, such as USB drives and CDs (g0tmi1k, *Kali Linux Forensics Mode: Kali Linux Documentation*). This would be very useful in an examination to ensure that the drive being analyzed is not edited during an examination. Regardless of how it is booted, there are plenty of options of ways to use the operating system for forensic efforts.

One of the main pre-installed forensic tools on Kali Linux is Autopsy. Autopsy is used to examine a drive or partition and is esteemed by professionals and amateurs alike. The tool can also be used to recover files as well as hash image files. The program is graphical and runs in a web browser, but it does not have "top-quality" graphics that users may be used to seeing. Despite the fact that it may not look as professional or classy as similar tools, it is still considered to be a go-to tool for many forensic examiners. One of the reasons this is true is that Autopsy outputs its results in real time, a feature that many similar tools lack (*Autopsy -- Digital Forensic Toolkit*).

Binwalk is one of the harder tools to comprehend from the Kali Linux forensic toolkit; however, it still offers plenty of uses that may aid an investigator in his/her examination. Binwalk is an extraction tool that is used to extract file systems that are embedded in firmware images. This open-source tool is especially known for its abilities to reverse engineer firmware images (*Binwalk: Firmware Extraction*).

Bulk_Extractor is a program that extracts forensically pertinent information, such as email addresses, websites visited, and credit card numbers from input data. This input data may take the form of disk images, files, or file directories. Bulk_Extractor operates on its files without parsing the file system or file system structure (*bulk-extractor*).

Hashdeep is a great tool for calculating the hashes of files. The program is command-line based but it is very easy to use and comprehend. The command “hashdeep -h” lists all of the options available with the tool and templates for how to use the options. For example, if a user wanted to find the MD5 hash of a file called “textfile1”, the user could type the following into the terminal: “hashdeep -c MD5 textfile” (Assuming the user is in the proper directory). The tool would then print out a statement with the size of the file, the MD5 hash, and the file location (see **Figure 3**). There are many other options available for this tool such as write the hash to a file, choose a different hash algorithm (such as SHA1, SHA256), operate in piecewise mode, operate in recursive mode, and compute estimated time remaining for the hash. It is worth pointing out that Kali Linux does offer a native way of calculating hashes by using the terminal command “md5sum”, “sha1sum”, or a similar command followed by the filename. While this simple capability is existent, Hashdeep provides much more options and features.

Guymager is an especially important tool to take note of since it is a forensic imager for media acquisitions. Guymager has a nice, clean-looking graphical interface (see **Figure 4**) and is quite simple to use. The user selects which drive they want to acquire an image for and inputs some case information and the desired destination of where the image file should be stored. Once the user has made his/her options, the tool starts its imaging process. While the device is being imaged, Guymager displays the percentage of completion and the estimated remaining time let for the imaging (*Guymager*).

Besides Autopsy, Binwalk, Bulk_Extractor, Hashdeep, and Guymager, Kali Linux has several other tools that may prove useful for a forensic investigation. There are file carving and PDF forensic tools available on Kali, but they will not be discussed today. Although the Kali Linux operating system was designed to assist penetration testers (“hackers”) in their services, there are also several pre-installed tools that may prove useful to the forensic investigator. This makes sense if one realizes that forensic investigators have similar goals to hackers. Both of these roles try to get into private computers to gather information. The purposes behind and methods used by the roles of hacker and forensic investigator obviously differ drastically, but there is some overlap in that hackers may use forensics and forensic investigators may use hacking. Therefore, it is reasonable that Kali Linux would include products that suit the needs of both of these occupations. These pre-installed tools include Wireshark (for analyzing network activity), Nmap/Zenmap (for analyzing open ports on the network), John the Ripper (for password cracking), and many more. Additionally, there are other applications, such as FOREMOST, which can recover deleted data from a drive (*FOREMOST -- Recover Permanently Deleted Files Easily in Kali Linux*), that are also freely available if the user chooses to download and install them.

It is easy to see that Kali Linux is a very handy tool in the toolkit of any forensic investigator. Its numerous capabilities are surpassed by few in the realm of forensic software. Tools such as Autopsy, Binwalk, Bulk_Extractor, Hashdeep, Guymager, Wireshark, and Nmap make Kali a go-to product for professionals and amateurs alike. Unfortunately, Kali does not provide all the tools its expensive competitors, such as Paraben's Electronic Evidence Examiner or Guidance Software's EnCase offer. However, considering the fact that Kali Linux is open-source and freely available to the public, it will remain a favorite tool in the toolbelt of many forensic professionals and amateurs for the foreseeable future.

Images

Figure 1

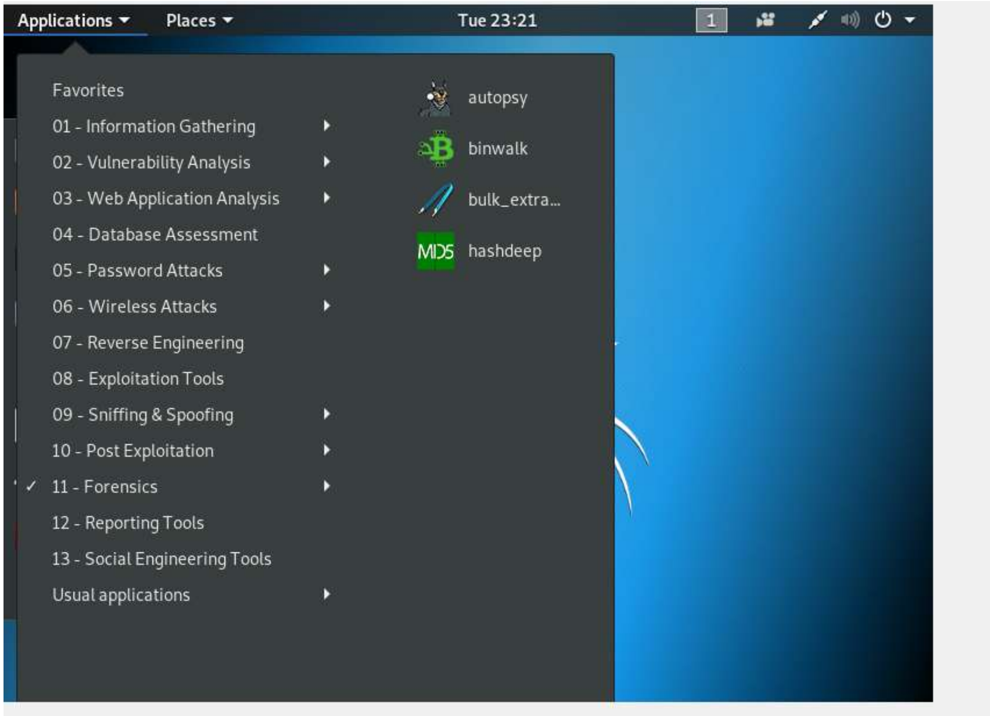
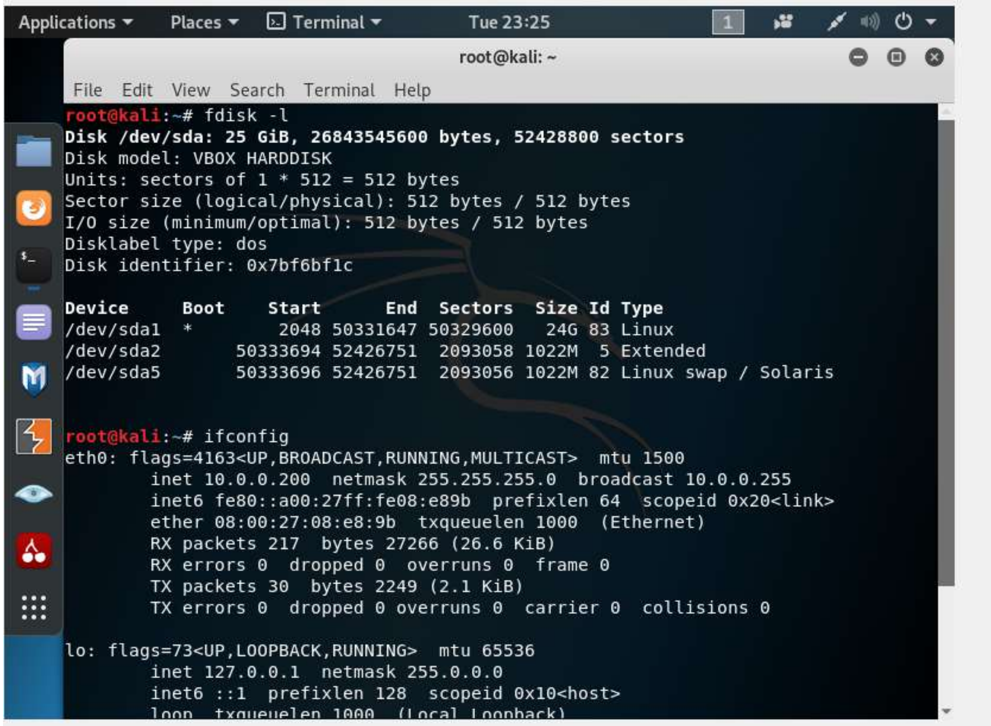
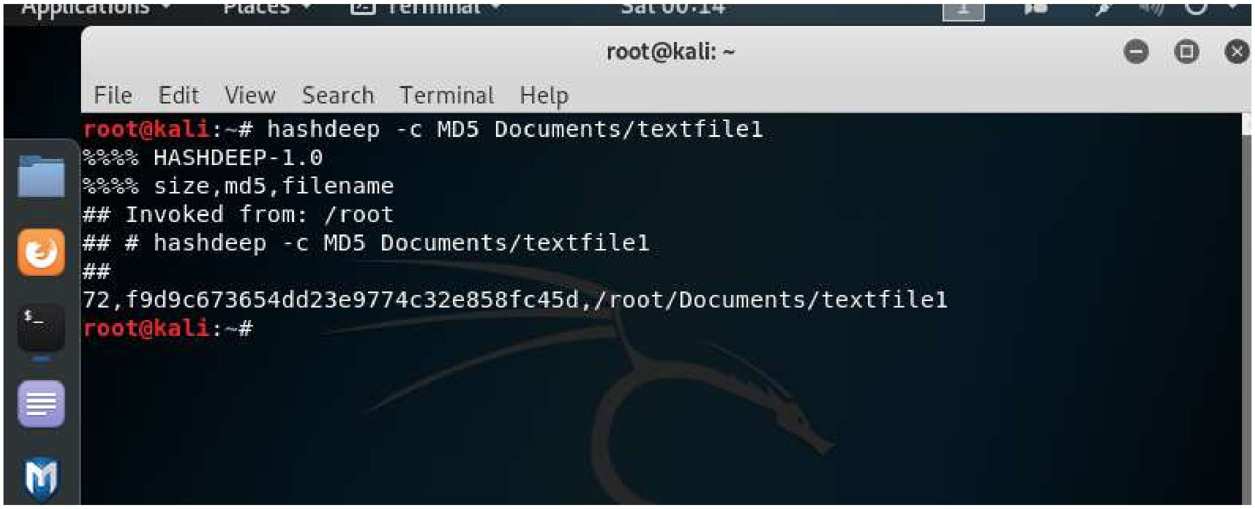


Figure 2



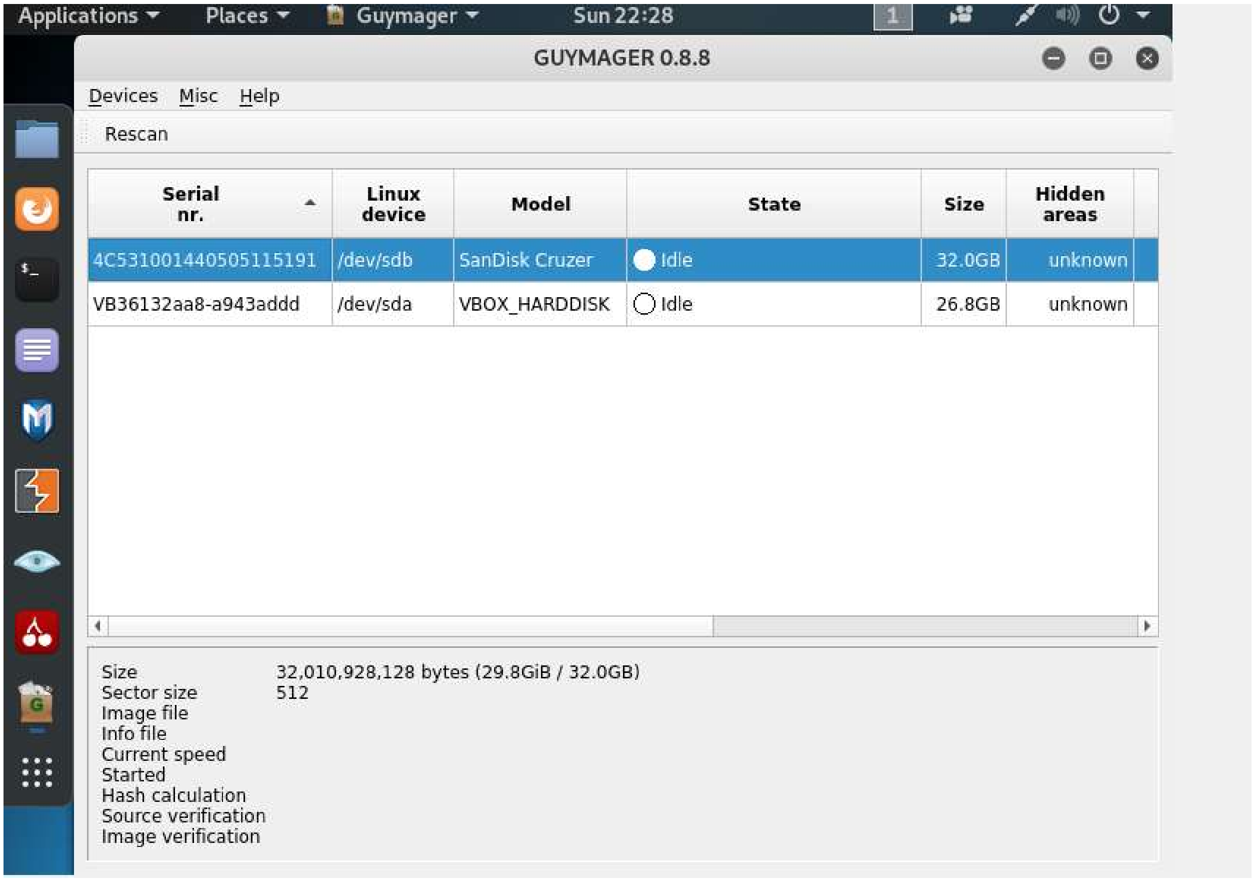
```
root@kali:~# fdisk -l
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x7bf6bf1c

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 50331647 50329600   24G 83 Linux
/dev/sda2       50333694 52426751  2093058 1022M  5 Extended
/dev/sda5       50333696 52426751  2093056 1022M 82 Linux swap / Solaris


root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.200  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fe08:e89b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:08:e8:9b  txqueuelen 1000  (Ethernet)
        RX packets 217  bytes 27266 (26.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 2249 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
```

Figure 3



```
root@kali:~# hashdeep -c MD5 Documents/textfile1
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /root
## # hashdeep -c MD5 Documents/textfile1
##
72,f9d9c673654dd23e9774c32e858fc45d,/root/Documents/textfile1
root@kali:~#
```

Figure 4



Serial nr.	Linux device	Model	State	Size	Hidden areas
4C531001440505115191	/dev/sdb	SanDisk Cruzer	● Idle	32.0GB	unknown
VB36132aa8-a943addd	/dev/sda	VBOX_HARDDISK	○ Idle	26.8GB	unknown

```
Size                 32,010,928,128 bytes (29.8GiB / 32.0GB)
Sector size          512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
```

Sources

"Autopsy -- Digital Forensic Toolkit." *Best Kali Linux Tutorials*, KaliLinux.in, www.kalilinux.in/2020/04/autopsy-kali-linux-2020.html.

"Binwalk: Firmware Extraction." *ReFirm Labs*, ReFirm Labs, 1 Apr. 2020, www.refirmlabs.com/binwalk/.

"Bulk-Extractor." *Penetration Testing Tools*, Kali Tools, tools.kali.org/forensics/bulk-extractor.

"FOREMOST -- Recover Permanently Deleted Files Easily in Kali Linux." *Best Kali Linux Tutorials*, KaliLinux.in, www.kalilinux.in/2019/09/foremost-kali-linux-recover-deleted-files.html.

g0tmi1k. "Kali Linux Forensics Mode: Kali Linux Documentation." *Kali Linux Forensics Mode | Kali Linux Documentation*, 25 Nov. 2019, www.kali.org/docs/general-use/kali-linux-forensics-mode/.

"Guymager." *Penetration Testing Tools*, Kali Tools, tools.kali.org/forensics/guymager.

Shah. *10 Best Known Forensics Tools That Works on Linux*. 1 Sept. 2020, linoxide.com/linux-how-to/forensics-tools-linux/.