**Lab #3 Learn Guymager-One of Kali Linux Digital Forensic Security Tools**

**Last Name: \_\_\_\_\_\_ First Name:** \_\_\_\_\_\_\_

**Objective:** Hand-On lab to carry out for students to understand how Kali Linux security tools work. The aim for this lab is to gain knowledge of using one of Kali Linux Digital Forensic Security Tools such as guymager. The second aim is to learn how to use a forensic imager tool(guymager) to digital investigate digital technologies such as thumb drive, phone and other more. The last aim of this hands-on lab is to learn why Kali Linux is a penetrating and security auditing by using digital forensic tools such as guymager and more. Guymager is a wide-open forensic disk imager tool for media acquisitions. Image acquisition is an important need for the process in digital forensic research. A forensic image/forensic copy is a bit by bit /sector by sector digital copy of a physical storage device such as thumb drive, cd rom and other types of storage devices which includes the physical device unallocated, free and slack spaces.

**Scenarios:** There are many scenarios in which can show an individual can use the guymager tool in order to obtain a digital forensic image of a physical device. Some examples of scenarios would be: A Suspect has been accused of traveling to Dubai for arms deals. The subject denies any involvement in arms, or any travel/interest in Dubai. A thumb drive was seized from the subject, which appears to be blank. A forensic image of the thumb drive has been created; A suspect has been accused of trying to obtain microbrewery equipment to manufacture anthrax. The subject was found to be in possession of a thumb drive, which appears to be blank. A forensic image of the thumb drive has been created (USB2.E01) and recovers any deleted data from the image and other more scenarios. During a criminal investigation, any digital evidence that is collected/preserved from the crime scene is collected from a forensic scientist or forensic investigator then evidence collected goes through different steps before being used as evidence in court of law. Firstly, normal physical copies are taken of digital evidence before the evidence is investigated hardcore. Secondly, a forensic image of the physical storage evidence is taken bit by bit/sector by sector by forensic investigator by different tools such as guymager and Access FTK Imager. After a forensic image is taken of the physical evidence, the forensic image is then used as different evidence in court proceedings in order to convict/ not convict somebody.

**Background:** Kali Linux is a multiplatform, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains many tools that are fixed on towards different information tasks such as Security Research, Computer Forensics and more. Linux was developed through rewriting of Backtrack by Mati Aharoni and Devon Keams of Offensive Security. Linux contains over six hundred different preinstalled penetration applications that can be discovered. Each program in Kali Linux has its own unique flexibility and case uses. Kali separates these useful utilities into the following categories: Information Gathering, Vulnerability Analysis, Wireless Attacks, Web Applications, Exploitation Tools, Stress Testing, Forensics Tools, Sniffing & Spoofing, Password Attacks, Maintaining Access, Reverse Engineering, Reporting Tools, and Hardware Hacking. Guymager follows under the forensics tools category.

Digital forensic tools are different types of hardware and software tools that can be used to aid in the recovery and preservation of digital evidence. Forensic tools are not only used to capture a disk image of devices but are used for automating much of the analysis process such as hidden/deleted files and directories, identify/recovering files and other more uses. Digital forensic tools are used to collect and persevere digital evidence in order to be used to support or refute hypothesis before courts. Some examples of digital forensic tools are SANS SIFT, ProDiscover Forensic, Volatility Framework and many more forensic tools. Guymager is a wide-open forensic disk imager tool for media acquisitions. Guymager is a pre-install tool found in kali linux. Image acquisition is an important need for the process in digital forensic research. A forensic image/forensic copy is a bit by bit /sector by sector digital copy of a physical storage device such as thumb drive, cd rom and other types of storage devices which includes the physical device unallocated, free and slack spaces. Guymager is used to clone digital materials in order to solve cybercrimes. Clone copies are used as evidence in court proceedings. Guymager is based on two tools called libewf and libguytools. This forensic tool had many different features such as an easy GUI user interface, makes full usage of multi-processor machines and generates flat (dd), EWF(E01), AFF images and supports disk cloning.

**Goals:**

Students will learn these different concepts and terms throughout the various stages of performing this hands-on lab about one of kali Linux security tool (Guymager) and help to complete the aim of this hands-on lab:

* Learn what Kali Linux is
* Learn what are the different tools that are found in Kali Linux
* Learn how to digital clone a physical storage device
* Learn about different forensic tools in Kali Linux
* Learn how to use a disk imager in a virtual machine such as Kali Linux
* Learn why digital forensic tools are used for and why they are important in court proceedings
* Learn to understand and analysis the results such as number of sectors, hash value and more after cloning a physical device
* Learn how to transfer files from a virtual machine to host computer

**Tools**

* Laptop/Desktop
* Kali Linux Virtual Machine

**Task**

**Skip Task #1 if Kali Linux virtual is installed on your device!**

**Task #1: Installing/Preparing/Starting Kali Linux Virtual Machine**

1. Install the VMware with default options from the website (<https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/15>\_0) if you are using a PC or VMware Fusion or Virtual Box if you are using MAC OS operating system.
2. In a search engine, go to <https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/> website where you will click the Kali Linux VMware 64 bit to get the current version of the computer application. Then unzip the download file.
3. Navigate to the Kali VM that was unzipped and start the virtual machine.
4. Log in to Kali with the username kali and password of Kali.

**Task #2: Running of the Guymager Program/Capturing a Forensic Image of the Physical Device**

1. In a new terminal window, type in this command to open the Guymager Forensic Tool in the kali Linux: **sudo guymager.**
2. The guymager forensic will now open in the Kali Linux.
3. Select a physical storage device/model that you as the individual want to create a digital image of.
4. Then right click on the device you want to image. A pop-menu will display where you will select “acquire image” to start the imaging of the device.
5. A pop menu showing the acquiring image will open. There you will click on Expert Format Witness file format.
6. Fill out the details like case number, evidence number, examiner, description and notes as you would like to fill them up.
7. To locate the image directory, type the location of the image directory or click on “” to search for the image directory.
8. Select your destination folder and then click on Choose.
9. Type the image file name without the extension. The extension will be entered the same itself.
10. Don’t include any special characters such as space, hash or other more. If a character is entered, an error message will be displayed.
11. After clicking on the button “OK”.
12. A pop-menu showing the state from ‘idle’ to ‘acquisition running’ and progress, and time remaining, average speed will be displayed.
13. The results of the cloning device will be displayed in Kali Linux. There were you take a screenshot of the results from the cloning of the physical device.
14. After the cloning of the device is finished, the image file of the device will be in the directory that was provided in the menu.
15. How many sectors are on the device?

|  |
| --- |
|  |
|  |

1. What is the MD5 hash of the device?

|  |
| --- |
|  |
|  |
|  |

1. How long did acquisition take?

|  |
| --- |
|  |
|  |

1. How many files were created after the cloning of the device?

|  |
| --- |
|  |
|  |
|  |

1. Submit a screenshot of the image results below this question e.