TA-2 Assignment

DOMS | Page No. 1
Date / /

Name:- Kishan Lal
Course:- M.sc Digital Forensics & Information Security
Er.No:- MSDFIS02
Sub:- Computer Forensics

* Write Sword-note about the following topics.

(1) Autopsy.

* What is Autopsy?

- "Autopsy is a digital forensics platform and graphical interface to the Sleuth kit and other digital forensics tools. it is used by law enforcement, military and corporate examiners to investigate what happend on a computer. you can even use it to recover photos from your camera's memory card" - official website.

Basically, the autopsy is a free open-source tool that supports a wide range of other digital forensics modules and tools.

The Autopsy is Computer Software that makes it simpler to deploy many of the open-source programs and plugins used in The Sleuth kit The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to find pertinent sections of data. The tool is largely maintained by Basis Technology

Corp. with the assistance of Programmers from the Community.

* Features

- Multi-user cases: Collaborate with fellow examiners on large cases.
- Timeline Analysis: Displays System events in a graphical interface to help identify activity.
- Keyword Search: Text Extraction and index Searched modules enable you to find files that mention specific terms and find regular expression Patterns.
- Web Artifacts: Extracts web activity from common browsers to help identify user activity.
- Registry Analysis: uses RegRipper to identify recently accessed documents and USB devices.
- LNK file analysis: Identifies Shortcuts and accessed documents.
- Email Analysis: Parses MBox format messages. Such as Thunderbird.
- EXIF: Extracts gps location and camera information from JPEG files.
- Media Playback and Thumbnail Viewer.
- Robust File System Analysis: Support for common file systems, including NTFS, FAT12, FAT16, FAT32, ExFAT, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, yaffs2
- Unicode Strings Extraction: Extracts strings from unallocated Space and unknown file types in many languages.

- File Type Detection: based on signatures and extension mismatch detection.
- Interesting File Modules will flag file and folders based on name and path.
- Android Support: Extracts data from SMS, Call logs, Contacts, Tango, Words with Friends, and more.

* How to install Autopsy

Autopsy comes pre installed in Kali Linux, Although it is highly recommend that one use the Autopsy in windows for better GUI experience.

Official website is https://www.autopsy.com/download/

you can download the autopsy for any architecture of windows 64-bit or 32-bit, also there is a .deb package that you can use to install in Linux.

* How to use Autopsy for digital investigations?

Now, we will see how we can use Autopsy for investigation a hard drive. for that, we will go through a popular Scenario most of us come across while Studying digital forensics, and that is the Scenario of Greg Schardt.

Let me tell you the Scenario in brief:

It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, Greg Schardt. Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of wireless Access Points where he would then ~~intercept~~ intercept internet traffic, attempting to get credit card numbers, usernames & Passwords, find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the Computer to the Suspect, Greg Schardt.

Step:1 Run Autopsy and Select New Case.

Step:2 Provide the case name and the directory to store the case files, click on Next.

Step:3 Add Case Number and Examiner's details, then click on Finish.

Step:4 Choose the required data source type, in this case Disk Image and click on Next.

Step:5 Give Path of the data Source and click on Next.

Step:6 Select the required modules and click on Next.

Step:7 After the data Source has been added, click on Finish

Step:8 You reach here once all the modules have been ingested, you can begin begin investigating but I recommend waiting until analysis and integrity check is complete.

(2) Write blocker

Write blocker is a tool designed to prevent any write access to the hard disk. Thus permitting read-only access to the data storage devices without compromising the integrity of the data. A write blocking if used correctly can guarantee the protection of the chain of custody. NIST has issued a set of general guidlines for write blocking requirements.

Write blockers are basically of two types:
(1) Hardware Write Blocker.
(2) Software Write Blocker.
Both types of write blockers are ment for the same purpose that is to prevent any writes to the storage devices. Let's discuss each type of write blocker.

* Hardware write Blocker

Hardware write blocker are used to intercept and block any modifying command from ever reaching the storage device.

- They offer monitering and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device.
- They provide built-in interfaces to a number of storage devices.

- Hardware write blockers can connect to other types of storage with adapters.
- Hardware devices that writes block also provide a visual indication of function through LEDs and switches. This makes them easy to use and makes functionality clear to users.

* Software write Blocker

Software write blocker are installed on a forensic workstation. According to NIST's specification of Software write Blocker, a Software write blocker tool operate by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface. They provide the ability to simultaneously write block on many disk devices as are connected to a computer without the need for multiple expensive hardware write blocking devices. Some of the features that are provided by different write blocking tools are:

- The user can control automatic write blocking policies for fixed and/or removable disks.
- The user can have write blocking tool remember each fixed device's blocked or un-blocked status for case of use on media repetedly used on a workstation/laptop.
- Some of the write blocking tools provide a GUI interface that allows the user the ability to block and unblock any disk or fresh device.

Date / /

(3) Sysinternals

Windows Sysinternals is a suite of more than 70 freeware utilities that was initially developed by Mark Russinovich and Bryce Cogswell that is used to monitor, manage and troubleshoot the Windows Operating System and which microsoft now owns and hosts on its TechNet site.

These utilities are executable files that do not require instruction to run. Administrators can access the utilities from TechNet — either as a single suite download or individually — or run them directly from the Sysinternals Live Services. Certain applications that have no troubleshooting features are not included in the Sysinternals suite download, such as Bluescreen, which emulates the blue screen of death and can be used as a screensaver.

* Sysinternals Categories

The Sysinternals site divides the utilities into six categories. file and disk, networking, Process, Security, System information and miscellaneous.

File and disk: This Section hosts utilities that monitor file usage and disk status. one of the more popular applications in this Section is Process monitor which displayes real-time activity in the file system registry, and processes.

Networking: This area features applications to troubleshoot and monitor connections on desktop and Server Systems. Two of the more popular tools in this section are TCPview which checks TCP and UDP endpoints and PsTools which is Set of command-line utilities that can help administrators monitor and manage remote systems.

Process: This Section holds utilities to monitor and troubleshoot running applications. A popular application here is Process Explorer, which monitors the files and directories that a particular process has open.

Security: This area features Security-based utilities including Autoruns, which shows the applications that start automatically when the system boots.

System Information: This category hosts applications that display general information about a workstation or Server.

Miscellaneous: Utilities in this Section do not fit in other categories and have limited diagnostic or troubleshooting capabilities one of the more popular downloads in this area is Bginfo, which creates a background image that shows key features of the System's Configuration such as the IP address and computer name.

(4) Splunk

Splunk is a software platform to search analyze and visualize the machine-generated data gathered from the websites, applications, sensors, devices etc. which make up your IT infrastructure and business.

Eg. you have a machine which is generating data continually and you want to analyze the machine state in real time, then how will you do it? Can you do it with the help of Splunk? yes! you can.

Real time processing is Splunk's biggest selling point because, we have seen storage devices get better and better over the years, we have seen processors become more efficient with better over the years, we have seen processors become more efficient every day, but not data movement. This technique has not improved and this is the bottleneck in most of the processes within organization.

If you already think Splunk is an awesome tool, then hear me out. when I say that this is just the tip of the iceberg. You can be rest assured that the reminder of this blog post will keep you glued to your seat if you have an intention to provide your business the best solution, be it for system monitoring or for data analysis.

The other benifits with implementing Splunk are:

- your input data can be in any format for e.g .csv or json or other formats
- you can configure Splunk to give Alerts/events notification at the onset of a machine state.
- you can accurately predict the resources needed for scaling up the infrastructure.
- you can create knowledge objects for operational intelligence.

This infographic below mentions some of the functions for Splunk can be used.