

**CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC),
THIRUVANANTHAPURAM, KERALA**

A PROJECT REPORT ON
“Windows system logs and Registry analysis”
SUBMITTED TOWARDS THE



PG-DCSF SEPTEMBER 2023

BY
Group Number - 09

Jai Veer Singh

PRN: 230360940016

Kakde Shreyas Pandhari

PRN: 230960940019

Dagadghate Purshottam Shivaji

PRN: 230360940010

Sharma Niles

PRN: 230360940047

Kale Vijay

PRN: 230360940020

Under The Guidance Of

Mr. Jayaram P.
Centre Co- Ordinator

Mr. Sreedeeep AL
Project Guide

ABSTRACT

Due to the increasing number of computers and easily available internet connection, the crimes involving computers are increasing rapidly. Keeping this in mind, the researchers always try to find new and effective ways to find the evidence that can be presented in the court of law to prove or disprove the case.

Windows event logs were not considered accountable proof before some of the cases that were solved with the help of Windows Event Logs. The purpose of this post is to analyze Windows Event Logs for Artifacts from the Forensic perspective. How windows event logs are stored, how they can be useful in a forensic investigation and what are the tools that are used to analyze the Windows event logs. This post also covers some of the vulnerabilities that need to be considered before analysis

Keywords:- Application event log , system event log, Security event log , Access data ftk imager

INTRODUCTION

In an event of a forensic investigation, Windows Event Logs serve as the primary source of evidence as the operating system logs every system activities. Windows Event Log analysis can help an investigator draw a timeline based on the logging information and the discovered artifacts. The information that needs to be logged depends upon the audit features that are turned on which means that the event logs can be turned off with the administrative privileges. From the forensic point of view, the Event Logs catch a lot of data.

- The Windows Event Logs are used in forensics to reconstruct a timeline of events.
- The main three components of event logs are:
 - Application
 - System
 - Security
- On Windows Operating System, Logs are saved in root location %System32%\winevt\Logs in a binary format.
- Offline event log file size can be set by the user
- When Maximum Log size is reached:
 - Oldest Events are Overwritten
 - Archive the Logs when full
- If do not wish to overwrite the events, clear logs manually

METHODOLOGY

Windows System Log files:-

Log files can contain a wealth of information and play a vital role when investigating possible intrusion cases
Not always turned on by default

Various types of logs files:-

- Windows Event logs
- Internet Information Services (IIS) logs
- Apache Web server Logs
- Syslogs
- FTP Logs
- Firewall/IDS Logs

Windows Event Logs:-

The purpose of this document is to break down Microsoft Windows event logs for artifacts that might be important to an investigator. How are specialists utilizing Windows event logs in forensic examinations? How do investigators approach the different sorts of breaches when gathering information from Windows event logs? What are the best procedures to ‘analyze Windows event logs?

The Windows event logs are records filling in as a placeholder of all events on a computer machine, Network or Servers. This incorporates logs on particular events on the system, an application or the operating system. The Windows Event Logs help in recreating the timeline of events in order to assist an investigation. The type of events that are recorded can be any occurrence that affects the system:

- An Incorrect Login Attempt,
- A Hack, Breach, System Settings Modification,
- An Application Failure,
- System Failure etc.

All these events are logged in the “%System32%/Winevt/Log”. All Windows events incorporate data on the event, for example, the date and time, source, fault type, and a Unique ID for the event type.

The event logs contain an abundance of data, which enables an administrator to investigate and manage the system.

The event Viewer utility on the Windows helps in analysis of the events on that machine. But for the forensic analysis, the investigator has to acquire the offline files of event logs which then will be analyzed by using third-party tools.

- Record events occurring on a windows system and are configurable
- Stored in a proprietary format; need to view events in windows event viewer or a third party tool such as event Log Explorer
- Windows vista and Windows 7 moved to a structured XML log- format which allows events to be logged more precisely for easier interpretation
- Each log entry is classified by type and contains header data and a description of the event
- The event header contains useful information such as:
 - Data and time
 - Logged on user
 - Computer name
 - An Event ID, which describes the event type
 - Source of the event; the application or services that logged the event
 - The type of the event, i.e error, warning, information , success audit and failure audit

There are three main types of logs:-

- 1) Application Event logs
- 2) System Event logs
- 3) Security Event logs

Windows 7 Event Logs

- 1) Windows 7 holds 136 different event logs
- 2) Some contain valuable information but many are not populated

Application Event Log:-

The Application Log records application related events that are installed in the system. This records the errors that occur in an application, informational events, and warnings from the software applications. Using the Application log we can troubleshoot any software problem that prevents it from either logging in or functioning properly.

- 1) Contains events logged by programs
- 2) Developers of the application determine if and what will be logged to the Application event log

System Event log:-

The System Log records events that are logged by the Operating System segments. These events are frequently pre-established by the working OS itself. System log files may contain data about hardware changes, device drivers, system changes, and all activities related to the machine. Because of increasing number of threats against networks and systems, the security logs variety has increased greatly.

- 1) Contains events logged by windows system components
- 2) Windows predetermines which events are populated in this log
- 3) Consider how the events shown below may indicate a malicious attack vector

Security Events Log:-

The Security Log contains Logon/Logoff activity and other activities related to windows security. These events are specified by the system's audit policy. The security log is the best and last option to detect and investigate attempted and/or successful unauthorized activity. Event logs can also be used to troubleshoot problems in the system.

- Records events such as logon attempts, policy changes and events related to resource use
- By default, Windows XP security log is turned off
- Starting with Windows 2003, logon events contained not only the NetBIOS name of the system which initiated the Logon , but also its IP
- Starting with Windows 2003, logon events contained not only the NetBIOS name of the system which initiated the Logon , but also its IP
- Successful logon events trigger Event IDs of 528 or 540 (successful logon) and 538 or 551 (logoff) in Windows XP
- Vistas and Windows 7 use Event ID 4624 for successful logons and 4634 for a system initiated logoff and 4647
- For a user initiated logoff
- There are numerous logon types which are of interest of the investigator:-

Logon Tyes	Title	Description
2	Interactive	Console Logon
3	Network	Network logon, such as via net user or network share
5	Services	Service logon
7	Unlock	The user unlocked the workstation
10	Remote Interactive	Logon using terminal services or the remote Desktop Protocol

Event Log Header:-

- 1) The size of the log files can be set by the user, but is 512 KB by default in windows XP
- 2) When a log reaches its size limit and new events need to be written older entries are purged and can also be cleared by a user
- 3) Deleted event log records can be carved out of unallocated space
 - Event log header is contained in the first 48 bytes of a valid Event log file and for each individual log entry
 - At offset 4 for 4 bytes, there is the "Magic number"

Other Important Event Logs

Some other windows event logs that should be monitored besides three main Event Logs:

- Directory Service Events — Domain controllers record any Active Directory changes.
- File Replication Service Events — For File Replication service events; Sysvol changes
- DNS Events — DNS servers record DNS specific events

Windows Event Log Vulnerabilities

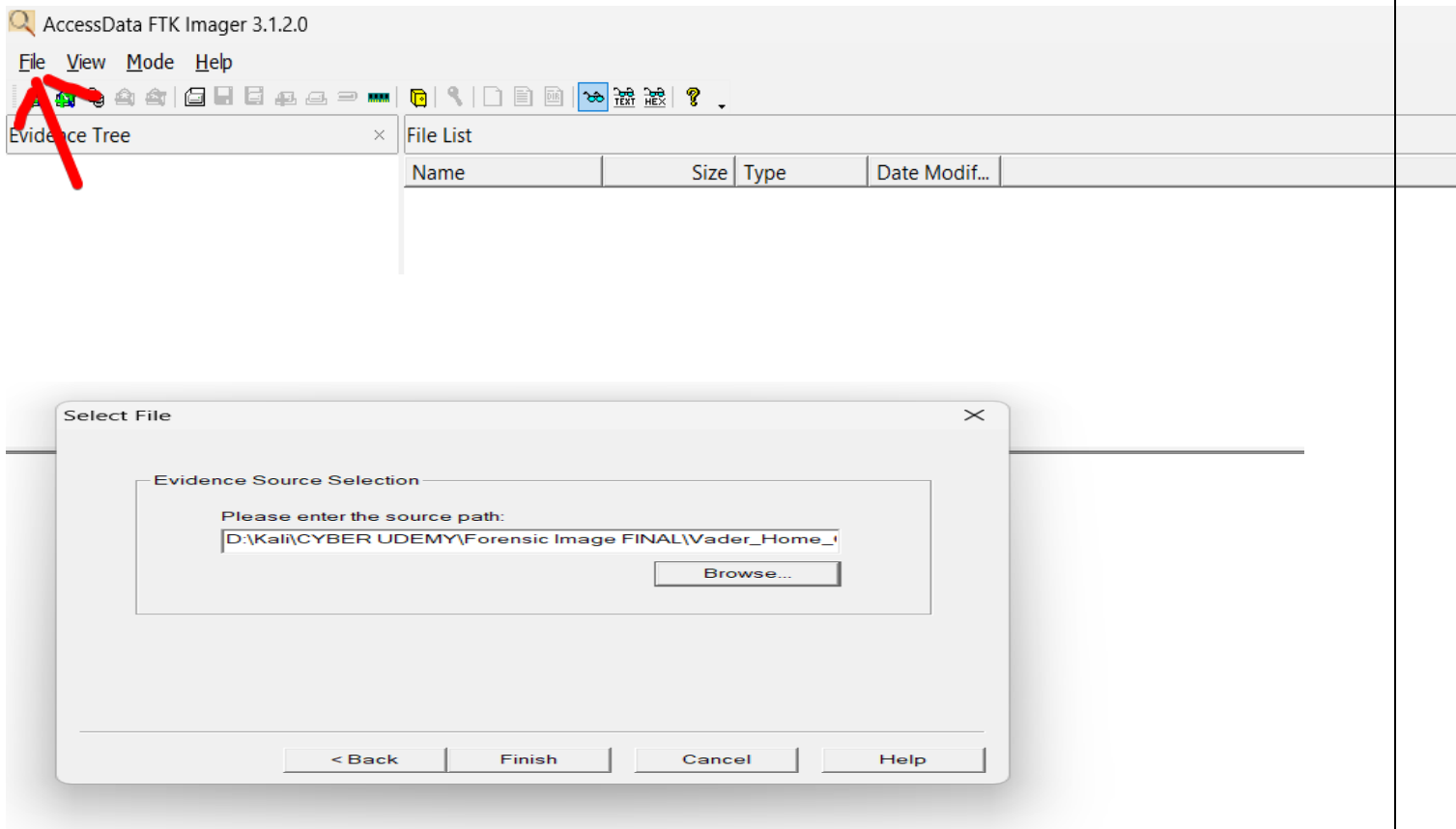
- It is possible to disable the event log service in Windows
- Important data can be modified such as Date and Time, Computer Name, and Usernames
- Event logs from one machine can be transplanted into another machine
- When the logs are generated, the time stamp uses internal host clock which can affect logs if it is inaccurate.

To modify the event log involves having access to the Security Event Log record and after that, the information contained inside can be altered. Consequently, if the Event Log records could be monitored for any duplicating, written work or erasing then one might say that it is possible to underline the possible attack on the integrity of its information. By using the Windows Registry, we can observe if the Event Logs had been changed or disabled. Based on these discoveries the system can be designed to be resilient or invulnerable. It will prohibit any physical access to the event logs and will likewise create a hash signature that will highlight if any changes have been made.

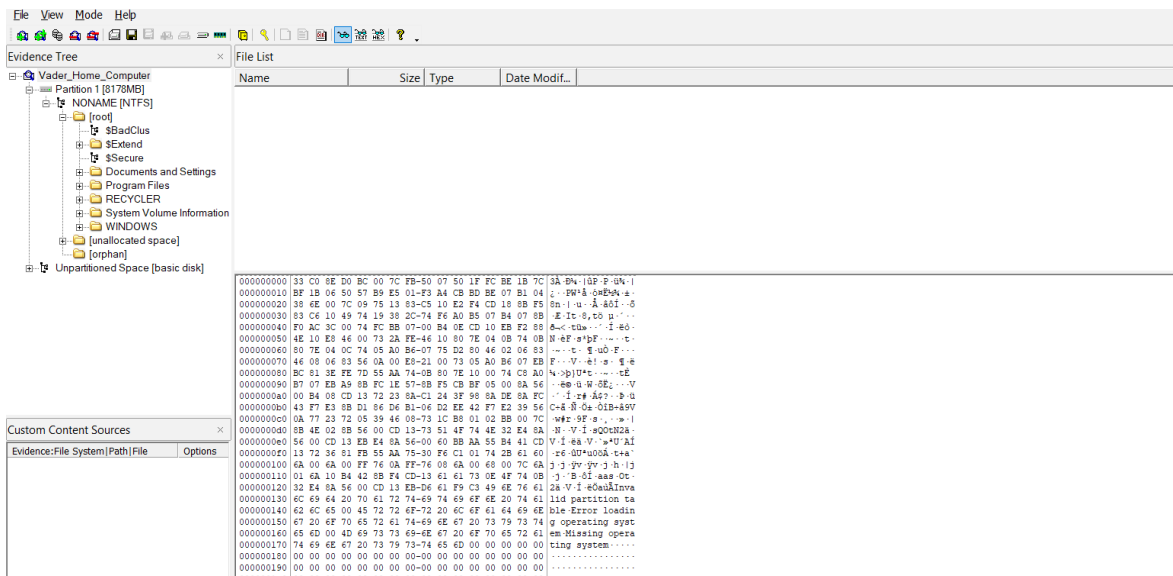
Solutions For Vulnerability

- Restrict the Physical Access to any Outsider
- Store Daily Backup of the System Logs
- Time Stamping vulnerability can be solved by using a single time-stamping device in a network which can increase the accuracy and integrity of the events.
- A Public Key Infrastructure server is used to authenticate the system users so that the fake events cannot be injected.

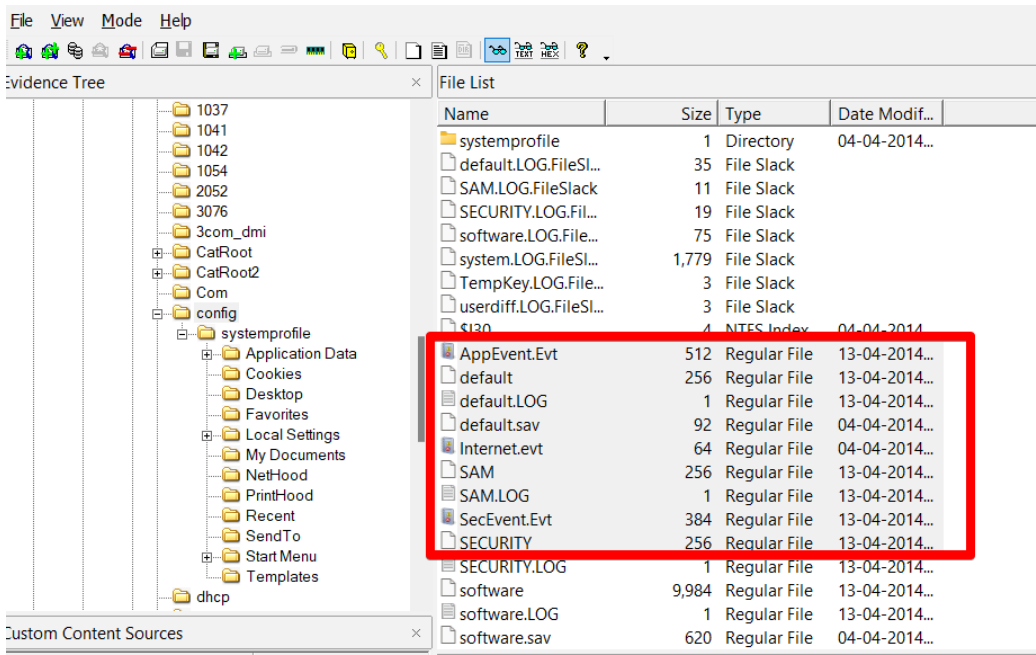
Step- 1:- Load Image files in the Access data FTK Imager



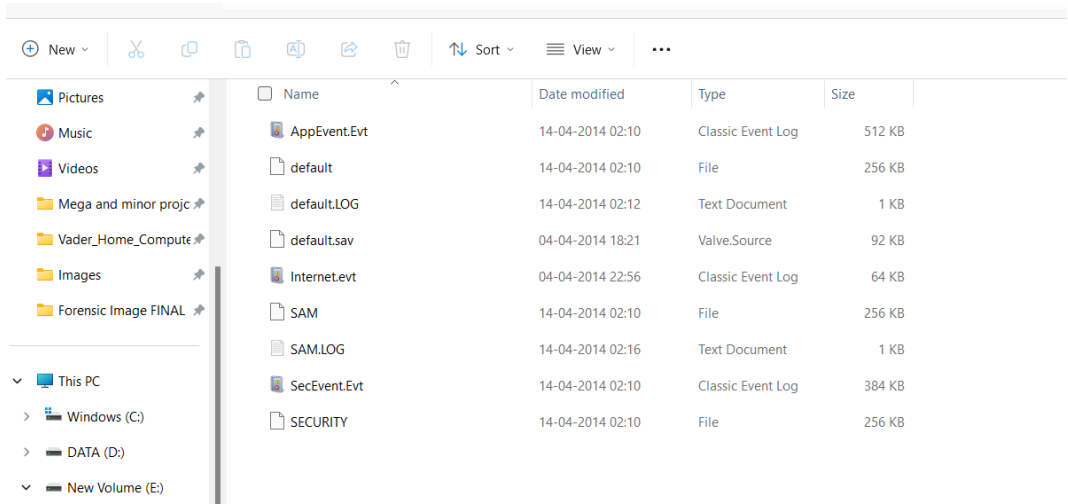
Step – II After loading the Image we see the interface of the app something like this



Step 3:- Export event log files from the path Root → Windows → System32 → Config → App event, Security event, Internet event



Extracted this Files in our Folder :-



Step -4 :- Open the Event files in the software name Event Log explorer

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	14-04-2014	02:50:41	576	Security	Privilege Use	NT AUTHORITY\NETWORK	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:50:41	528	Security	Logon/Logoff	NT AUTHORITY\NETWORK	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:50:41	576	Security	Privilege Use	NT AUTHORITY\NETWORK	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:50:41	528	Security	Logon/Logoff	NT AUTHORITY\NETWORK	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:30:47	520	Security	System Event	SYSTEM	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:27:45	538	Security	Logon/Logoff	NT AUTHORITY\ANONYMOUS	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:27:45	540	Security	Logon/Logoff	NT AUTHORITY\ANONYMOUS	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:27:45	538	Security	Logon/Logoff	NT AUTHORITY\ANONYMOUS	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:27:45	540	Security	Logon/Logoff	NT AUTHORITY\ANONYMOUS	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:20	538	Security	Logon/Logoff	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:13	515	Security	System Event	SYSTEM	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	576	Security	Privilege Use	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	528	Security	Logon/Logoff	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	680	Security	Account Logon	SYSTEM	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	538	Security	Logon/Logoff	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	576	Security	Privilege Use	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	528	Security	Logon/Logoff	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:16:08	680	Security	Account Logon	SYSTEM	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:15:53	551	Security	Logon/Logoff	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:15:25	538	Security	Logon/Logoff	NT AUTHORITY\ANONYMOUS	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:15:24	540	Security	Logon/Logoff	NT AUTHORITY\ANONYMOUS	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:12:12	576	Security	Privilege Use	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84
Audit Success	14-04-2014	02:12:12	528	Security	Logon/Logoff	IS-1-5-21-1715567821-3	DARTH-2F3D6FB84

So here we can get the detail information about Date , Time which user login and log off at what time

Q1) When was a user profile Tiny tim was created?

Ans:- So we need to filter result by adding text in description tiny _tim

Filter

Apply filter to:

☒ Active event log view (File: E:\Mega and minor project\Minor project Final\EVENT LOGS\A

☐ Event log view(s) on your choice

Event types:

☒ Information ☒ Warning ☒ Error ☒ Audit Success ☒ Audit Failure

Source: ☐ Exclude

Category: ☐ Exclude

User: ☐ Exclude

Computer: ☐ Exclude

Event ID(s): ☐ Exclude

Enter ID numbers and/or ID ranges, separated by commas (e.g. 1,100,250-450)

Text in description: ☐ RegExp ☐ Exclude

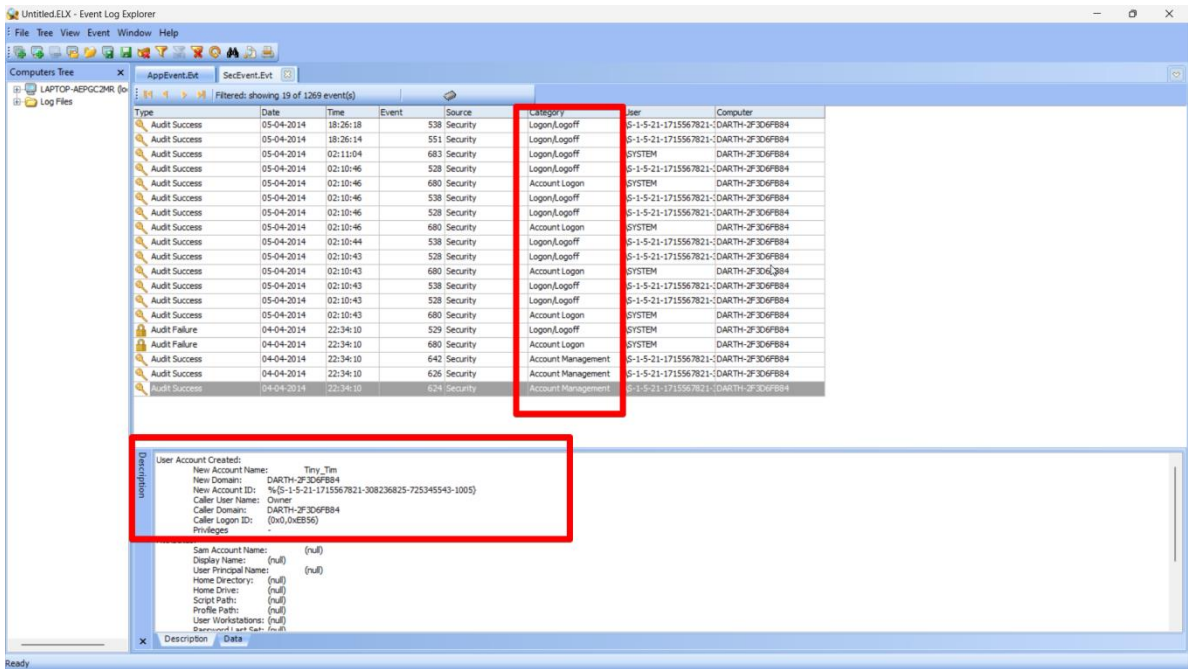
☐ Date ☐ Time ☐ Separately

From: 30-12-1899 00:00:00 To: 30-12-1899 00:00:00 ☐ Exclude

Display event for the last 0 days 0 hours ☐ Exclude

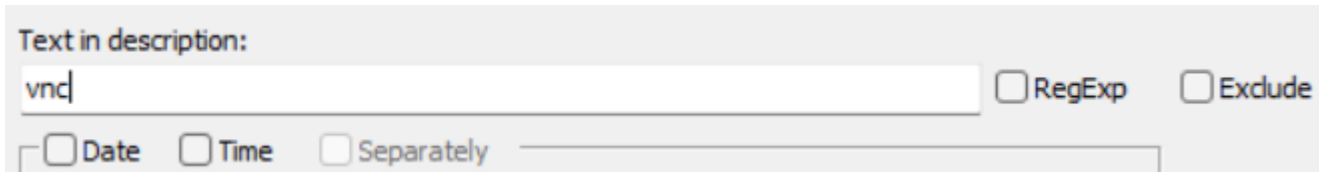
Clear Load... Save... OK Cancel

Then we get Filter result in which login/logoff result we get and at the end we get at what time at what date user Tiny_Tim created (i.e. Date :- 4-4-2014 Time:- 22:34:10)

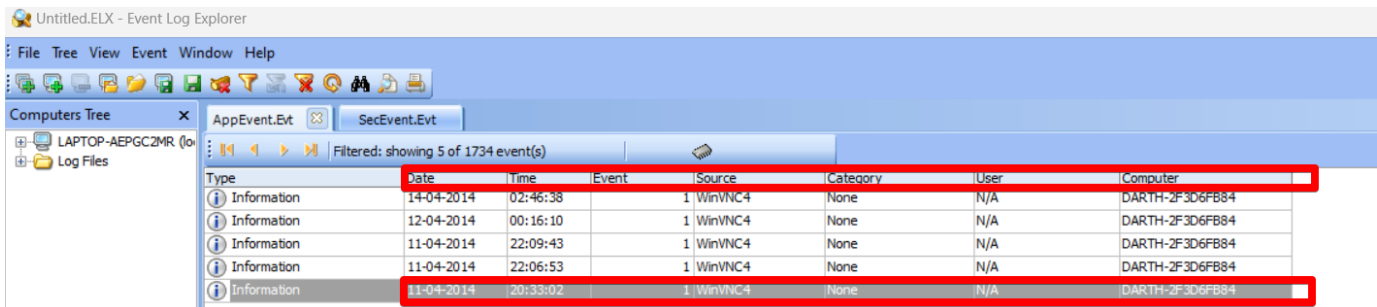


- Q2) Examine the AppEvent.Evt log and answer the following questions:
- Does the application event log provide any further indications of how VNC was used in this attack and where the source
 - of the attack may have come from?

Ans:- By filtering VNC in filter we get data



By filtering the data we get full data about VNC about source and from where attack may come from



Type	Date	Time	Event	Source	Category	User	Computer
Information	14-04-2014	02:46:38	1	WinVNC4	None	N/A	DARTH-2F3D6FB84
Information	12-04-2014	00:16:10	1	WinVNC4	None	N/A	DARTH-2F3D6FB84
Information	11-04-2014	22:09:43	1	WinVNC4	None	N/A	DARTH-2F3D6FB84
Information	11-04-2014	22:06:53	1	WinVNC4	None	N/A	DARTH-2F3D6FB84
Information	11-04-2014	20:33:02	1	WinVNC4	None	N/A	DARTH-2F3D6FB84

Windows Registry Analysis

In early versions of Windows, specific system files used to stored information in directories consisting information about default or user customized application, security or software settings. Later, user settings and other relevant information were systematically encapsulated to a structured format known as the Windows Registry. We can summaries windows registry in a few simple facts:

- Registries are Robust
- Helps individual software communicate better
- Stores data in a hierarchical structure to keep things organized
- Serves as an archive for collecting and storing configuration settings.
- Supports multiple users (User-specific data)
- System Components are stored in main folders called HIVE
- The information is Time Stamped

This document further introduces about Windows Registries and how they are Important from the forensics point of view and how they can help in getting evidence to prove or disprove the case. The document also describes where these registries are stored in the system directory and what are the most important registry keys that can be helpful. Each key is described with its location in the Registry Hive.

About Windows REGISTRY

The Registry is a various levelled or we can say a hierarchical database that stores low-level settings and other information for the Microsoft Windows Operating System and for applications that pick to utilize the registry. From the point of installation of operating system, registries are used. Kernel, Device Driver settings to the Hardware and User Interface all settings are stored in the windows registry.

When Programs and Applications are installed in the system their configurations and default values are stored in the registry although there are some applications which do not utilize windows registry. For example, .NET framework applications use XML files for configuration, Portable applications usually keep their configuration data within files in the directory/folder where the application executable resides.

Importance of Registry in Windows Forensics

For a Forensic analyst, the Registry is a treasure box of information. It is the database that contains the default settings, user, and system defined settings in windows computer. Registry serves as repository, monitoring, observing and recording the activities performed by the user in the computer. The Data is stored in the main folders in a Tree like structure which is called Hive and its subfolders are called KEYS and SUBKEYS where each component's configuration is stored called VALUES. Some Important aspects of Windows Registry are:

1. Windows Registry can be considered as a gold mine of forensic evidence.
2. We can create new registries manually or we can modify the ones that already exist.
3. Original files that contain registry values are stored in the system directory itself.
4. Registry files are system protected and can not be accessed by any user unless administration access is provided.
5. For the investigation purpose, the forensic investigator analyzes registry files via tools such as Registry Viewer, Regshot, Registry Browser etc..
6. Trojans and Malware information can be found in the registries.

Main Registry Hives

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE/SAM
- HKEY_LOCAL_MACHINE/SOFTWARE
- HKEY_LOCAL_MACHINE/SECURITY
- HKEY_LOCAL_MACHINE/SYSTEM
- HKEY_USERS
- HKEY_CURRENT_CONFIG

While acquiring registry files from the system we need to use an Imaging tool which can obtain system protected files because then only we can access and analyze them with the help of registry viewer. We can not obtain these files directly from the system because they are currently being used by the system to access registry editor.

The HKEY_CURRENT_USER data file is stored in a file called NTUSER.DAT located at “%SystemRoot%\Users\<UserName>”.

Other Important files that are monitored in HKEY_LOCAL_MACHINE are SAM, SOFTWARE, SECURITY, SYSTEM which are located at “%SystemRoot%\Windows\System32\config” along with some other files that are also important from the forensic perspective. These files do not have any file extension which makes it harder to access by users. Hierarchical central database storing configuration for application hardware devices and users made up of keys and Values found in five logical hives

Registry File Descriptions:-

SAM (Security Accounts manager)

- Only applicable to local or domain administrators
- Contains user name, SID and encrypted password hash for all users in a domain

SECURITY

- Contains the security permission for administrators. Used by the system to enforce security policy
- Limited usefulness for forensics

SOFTWARE

- Contains Windows Operating system setup, mounted
- Devices hardware settings and services

NTUSER.DAT

- Settings specific to individual users. Tracks user activity and preferences
- Stored in the root of the users profile and moves between system with roaming profiles

Registry Analysis –USBTOR

- The USBSTOR key contains information on USB external devices plugged into the system
- Device Class ID :- identifies the make model brand of the device
- Unique Instance ID :- identifies specific devices, even if they have the same Device class ID.
- Friendly Name:- Easily identifiable device name
- ParentPrefixID:- Windows uses this to refer to the specific device in the registry and log files. (Mounted Devices, Setupapi.log, etc...)
- The Mounted Devices key can be used to map a specific USB device back to a drive letter

- This can give additional meaning to evidential link files.
- Uses the Parent PrefixID
- Uses device issues are complex. It will require a lot of practice and research prior to using this technique in a real Trial

NTUSER.DAT –User Assist and ROT13

- Contains a list of programs executed on the system, including filename, run count and last execution timestamps
- Located in a users NTUSER.DAT file in the key
- The registry keys are encoded with ROT13:
- ROT 13 is a basic substitution Caesarian cipher where each letter is replaced with the letter 13 spaces farther down the Alphabet
- Designed to hide contents from the most basics of glances and supplies no cryptographic security

NTUSER.DAT –UserAssist Decoded

- The decoded ROT13 User Assist key shows the following important information
- RUNPATH refers to the absolute path within a file system
- RUNPIDL refers to a pointer to an object in this case they usually refer to shortcuts or Link files

NTUSER.DAT – MUI Cache

- ✓ Shows software which has been executed on a system
- ✓ Located in the following path in a users NTUSER.DAT file: software\Microsoft\Windows\ShellNoRoam\MUIcache
- ✓ Does not contain timestamp information but does have descriptive comments
- ✓ There exists little documentation from Microsoft detailing how, when and why this key gets populated but seems to be Created by the shell (i.e Explorer.exe) when an application is executed

NTUSER.DAT –MRU LISTS

- ❖ Many applications retain a most Recently used (MRU) list detailing the files that have recently been opened by that Application
- ❖ A users Recent folder is a well known directory which contains documents files and directories recently opened
- ❖ The RecentDocs key is found in the users NTUSER.DAT file in :
HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\RECENTDOCS
- ❖ The keys are stored as numbers with the names of the files stored in the data section in Unicode
- ❖ The MRUListEx value contains the order the files were accesse
- ❖ The RecentDocs key has subkeys present which break out the Recent documents via file extension
- ❖ The most recently accessed file appears firsts in the list

NTUSER.DAT – Open Save MRU

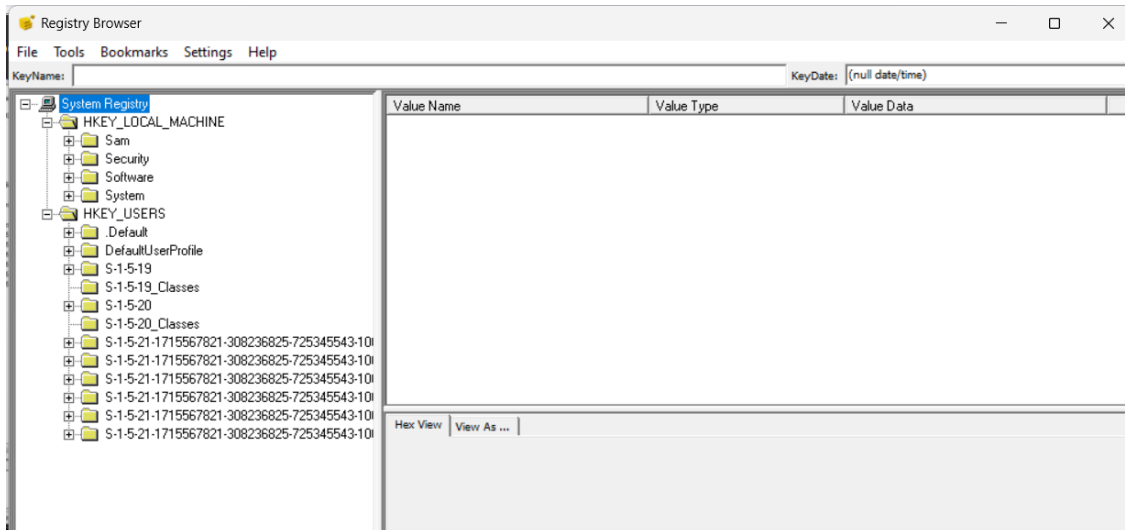
- Maintains a list of files recently opened or saved by the user
 - Organized by extension
 - Forensics parsing tools extract times and dates as well

NTUSER.DAT – TypedURLs

- Traditional definition : URLs that the user physically typed into the browser URL bar Max 25 entries
- Use Caution(if this is your only evidence)
- AutoComplete will populate this key
- Malware does exist that fills auto-populate functions
- Consider the Julie Amero case

POC:-

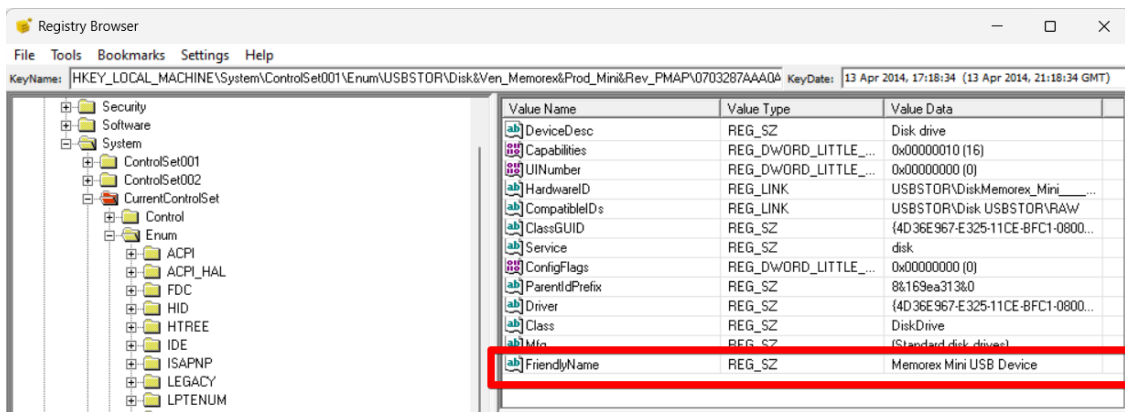
Step –I:- Load the image file in the Registry Browser app



Step-II :- Within the registry, navigate to HKLM\System\CurrentControlSet\Enum\USBSTOR

a. What is the Friendly name of the “Disk&Ven_Memorex&Prod_Mini&Rev_PMAP” thumb drive that was attached to this system?

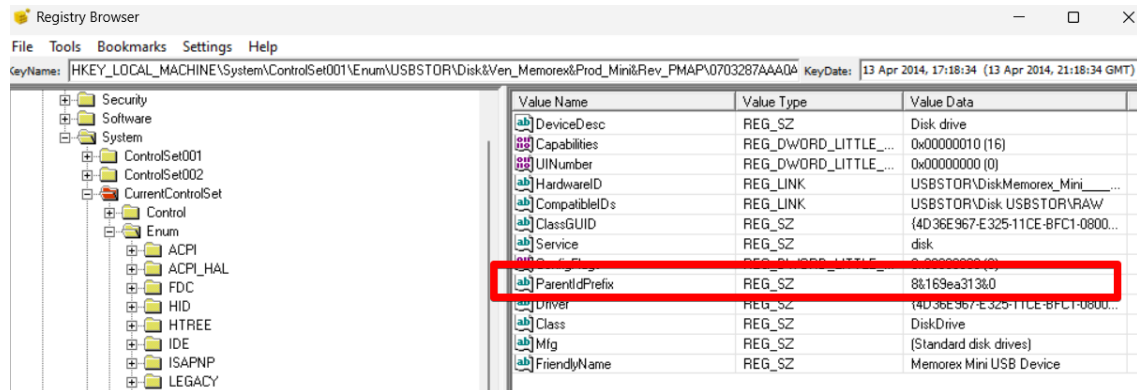
Ans:- The Friendly name is :- Memorex Mini USB Device



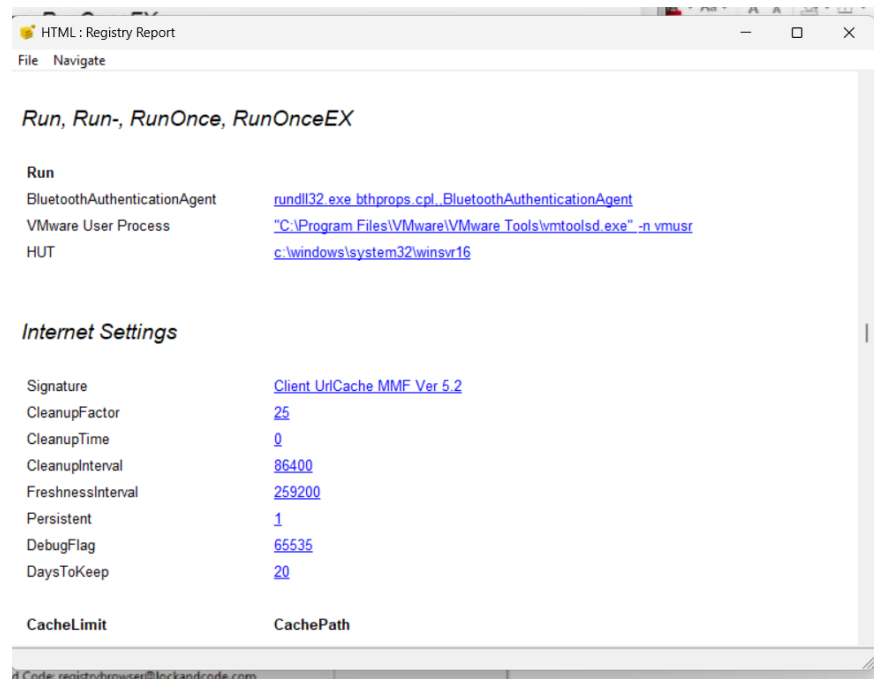
Step III:-

b) What is the Parent Prefix ID for this device?

Ans:-



Step -IV :- To Generate Registry report follow following steps Tools → Generate Report → Run, Run-, Run once , Run one Ex



Conclusion

Windows Event Logs are very essential from the Digital Forensic perspective because they store each and every event that happens in the Operating System. When a system is compromised by an unauthenticated user, it takes several steps and procedures to get access to the system. These steps can be used to trace back to the suspect. The incident response team is responsible for capturing the important artifacts for further analysis. Event logs are stored in offline physical files in the system root directory.

The Event Logs are categorized into different categories such as application, system, and security with different levels of severity. Other events such as network events are also logged in their separate files in the system. These files can be obtained manually or by using other utility tools.

Windows Registry is a significant forensic resource which provides a comprehensive picture of the case. With the techniques that are described in this document, an investigator can precisely acquire the registries from the compromised system. We have demonstrated the format of registry and the data it can uncover. If a single key is unreadable then its subkeys below that tree are also inaccessible to read. There are various tools that are used to read and analyze. In addition to that, we also have the option to parse the registry tree via the command line by using regedit.exe.

Windows Registry is essential and the exploration on it still continues. Regardless of whether we have known each key, subkey, and the value of Windows Registry, despite everything we need to consider how to utilize them in genuine cases. In the second part of this document, the important keys and subkeys are explained by their location and the data it contains to help the forensic investigation

REFERENCES

- [1]. www.cyberforensics.in
- [2]. <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical-0>
- [3]. Download 11-carve-fat.zip (Digital Forensic ToolTesting) (sourceforge.net)
- [4]. Digital Corpora: corpora/scenarios/2009-m57-patents/drives-redacted/
- [5]. Esra'a Alshammary, Ali Hadi, "Reviewing and Evaluating Existing File Carving Techniques for JPEGFiles".IEEE, 2016.
- [6]. G. G. Richard and V. Roussev, "Scalpel: A frugal, high performance file carver".
5th Annual Digital Forensic Research Workshop, 2005.
- [7]. "A Survey on Multimedia File Carving", (IJCSSES)Vol.6, No.6, December 2015.
- [8]. Gareth Palmieri, Shahrzad Zargari, "Using Open Source Forensic Carving tools on split dd and EWF files.", Sheffield Hallam University Research Archive,2017
- [9]. Nurhayati, Nurul Fikri, "The Analysis of File Carving Process Using Photorec and Foremost.", 2017
- [10]. S. L. Garfinkel, "Digital media triage with bulk data analysis and bulk-extractor," *Comput. Secur.*, vol. 32, pp. 56–72, 2013.

