Nulltack
Purple team bootcamp

WINDOWS FORENSICS

Event Logs & Registry Analysis

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed
Mohammed baqer

Contents

1. Introduction to Windows Forensics

Windows forensics is all about understanding the internal mechanics of how Windows operates as a system — its processes, its files, its records. If you want to do serious digital investigations, this is essential knowledge. It gives you the ability to extract meaningful evidence and build a solid picture of what happened on a machine.

1.1 Why Windows Forensics Matters

Think about it this way: if you have more information, you have a better investigation. That's the whole point. And Windows generates a huge amount of information about everything that happens on it you just need to know where to look and how to read it.

There are two primary sources of evidence we focus on in Windows forensics:

- **1.** Event Logs
- **2.** The Registry

2. Windows Event Logs

2.1 What Are Windows Event Logs?

Windows Event Logs are special files that record everything that happens on a Windows computer. Every action, every system activity, every error — it all gets written down. They are the system's memory.

There are two key reasons why these logs matter so much for investigations:

- They provide a timeline of system activity you can see exactly what happened, and when.
- They are essential for security investigations any unauthorized access, any breach, any suspicious behavior will show up in these logs.

Note : *Event logs are your timeline. They tell you what happened, in what order, and at exactly what time.*

2.2 The Three Main Categories of Event Logs

Windows Event Logs are divided into three main categories. Each one has a specific purpose and covers a different part of the system.

Category	What It Records	Examples
System Logs	Events generated by the operating system itself	System startup, shutdown, driver failures, service activity
Application Logs	Events from third-party applications installed on the machine	Microsoft Outlook, SQL Server — crashes, errors, activity logs
Security Logs	Security-related events — the most important category for forensics	Login attempts, file access, privilege escalation, account changes

2.3 Security Log — Key Examples

The Security Log in particular captures these types of events:

- Successful and failed login attempts
- File access and modification (object access auditing)
- Account management changes — creating, enabling, disabling, deleting accounts

2.4 Why You Must Configure Logging Properly

Here's a big problem that comes up in real investigations: logs aren't always turned on by default, or they're not configured to capture what you need. And this creates a massive blind spot.

Imagine an attacker gets into an account on your system. If logging wasn't enabled, there's nothing to investigate. The attacker walked in and out and left

no trace not because they were that good, but because the system wasn't recording anything. That's a very difficult situation to be in.

NOTE : *If logging is not configured properly, even a successful attack can be nearly impossible to reconstruct. Always verify that your audit policies are active before an incident happens.*

At the same time, more logs mean more disk space. So you need to balance security requirements with operational needs you want to log enough to catch what matters, without filling up your storage.

2.5 Event Log Structure : The Five W's

When you're looking at an individual event in the log, you always ask yourself the Five W's. This is the framework for reading and understanding any log entry:

Question	What It Means	Example
What?	What type of event occurred?	A login attempt (Event ID 4624 successful login or 4625 failed login)
When?	What time did it happen?	Timestamp recorded in the event
Where?	Which machine did it happen on?	The computer name recorded in the event
Who?	Which user account was involved?	Username, security ID (SID)
How?	How did the event occur?	Login type, process name, source IP

Note : *Every event log entry answers the Five W's. Build the habit of asking these five questions every time you open a log entry.*

2.6 The Four Event Types

Not all log entries are equal. Windows uses four levels to classify the severity or nature of each event:

Level	Name	What It Means
1	Error	Something failed — data loss or significant failure occurred
2	Warning	Not broken yet, but could indicate a future problem. Example: hard disk space running low not a crisis, but a warning sign.
3	Information	Normal operations being recorded. Example: an application or service started successfully.
4 / 5	Audit Success / Audit Failure	Found in the Security log. Success = action was allowed. Failure = action was denied or the attempt failed. Example: a failed login attempt records as an Audit Failure.

Note : *Audit Success and Audit Failure events in the Security log are incredibly useful. A pattern of Audit Failure events many failed logins in quick succession is a classic sign of a brute-force attack.*

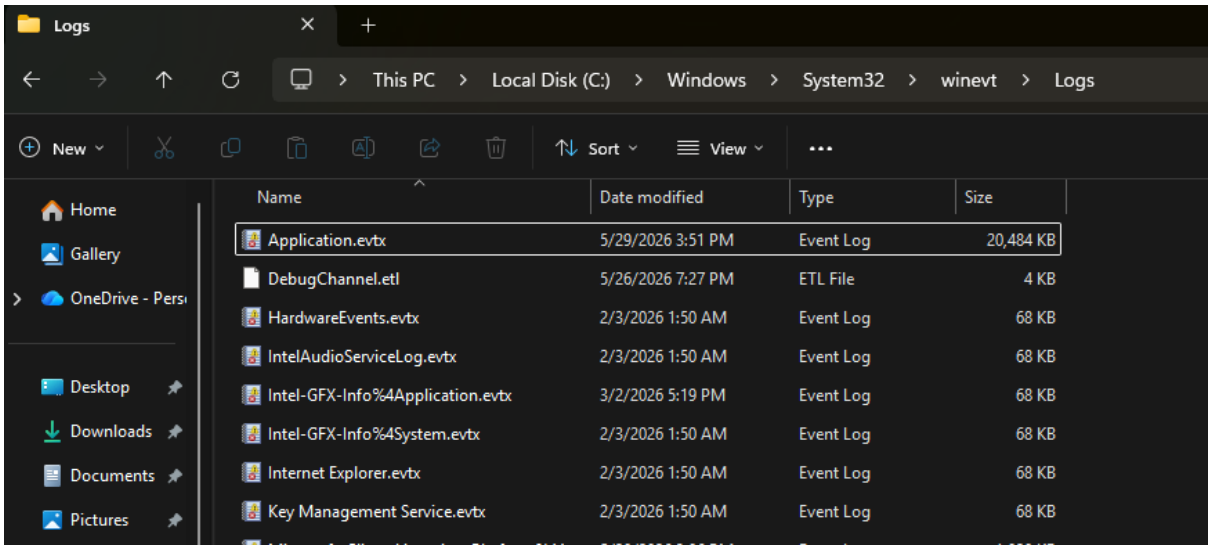
2.7 The Event Log File Format

Event log files use the **.evtx** extension and are **stored in binary format.** This means you cannot open them with Notepad or any plain-text editor they will appear as unreadable characters. You need a dedicated tool to read them.

2.8 Where Event Logs Are Stored

By default, Windows stores all event logs in a specific directory on the system:

```
C:\Windows\System32\winevt\Logs
```

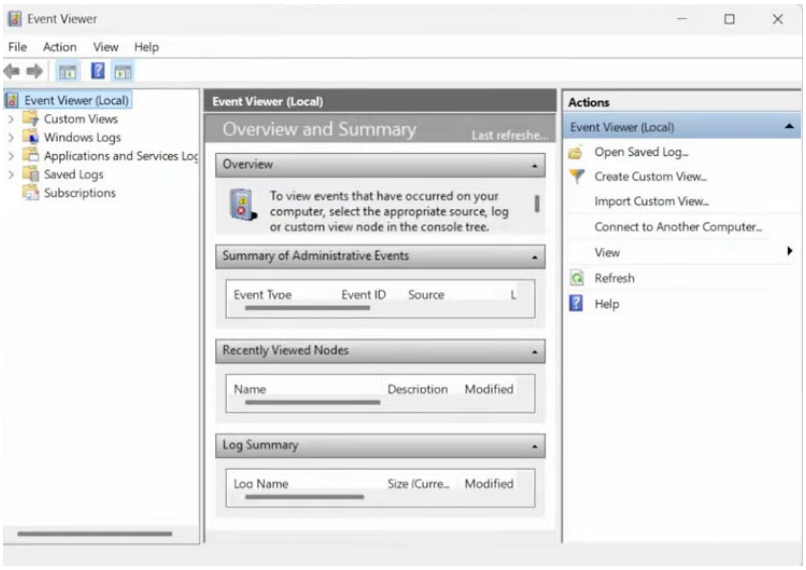


When you open this folder, you will see a collection of .evtx files — one for System, one for Security, one for Application, and more.

2.9 Tools for Viewing Event Logs

The easiest way to view event logs is through the built-in Windows Event Viewer. You can open it by running cmd :

```
eventvwr
```



Inside Event Viewer, you can:

- Browse System, Security, and Application logs
- Double-click any event to see its full details — process that created it, timestamp, Event ID, source, etc.
- Create custom views — filter by level, source, Event ID, or keyword
- Search by keyword such as 'Audit Failure'

2.10 Critical Security Event IDs to Know

These are the Event IDs you need to have memorized. In any Windows forensic investigation, you will be looking for these specific events:

Event ID	Meaning
4624	Successful Login — an account successfully logged on
4625	Failed Login Attempt — an account failed to log on
4634	Account Logoff
4647	User Initiated Logoff
4720	User Account Created
4722	Account Enabled
4723	Password Change Attempt
4724	Password Reset
4726	Account Deleted
4732	Member Added to Security Group
4733	Member Removed from Security Group
4688	New Process Created
4689	Process Exited
4656	Object Access Attempted (handle to an object requested)
6005	System Startup (Event Log service started)
6006	System Shutdown (Event Log service stopped)

3. The Windows Registry

3.1 What Is the Registry?

Think of the Windows Registry as the brain of the computer. It is the central place where Windows stores all of its configuration every setting, every preference, every piece of information about what's installed and how the system is set up.

For a forensic investigator, the registry is like talking to a detective who has been watching the machine from the inside. It can tell you:

- What programs were installed on the system
- What hardware was ever connected to the machine
- Who used this machine
- How everything was configured

Note : *The Registry is the best source of truth on a Windows system. It knows everything about what the machine has done and how it was set up.*

3.2 The Three Building Blocks of the Registry

The Registry is made up of three components that work together in a hierarchy think of it like a physical filing cabinet:

Component	Analogy	What It Is
Hive	The cabinet itself	The largest top-level division of the registry. Each hive is a separate file on disk.
Key	Folders inside the cabinet	Containers inside a hive that organize data. Keys can contain other keys (called subkeys).
Value	Documents inside the folders	The actual data stored inside a key. Each value has a name and a data entry — this is where the real information lives.

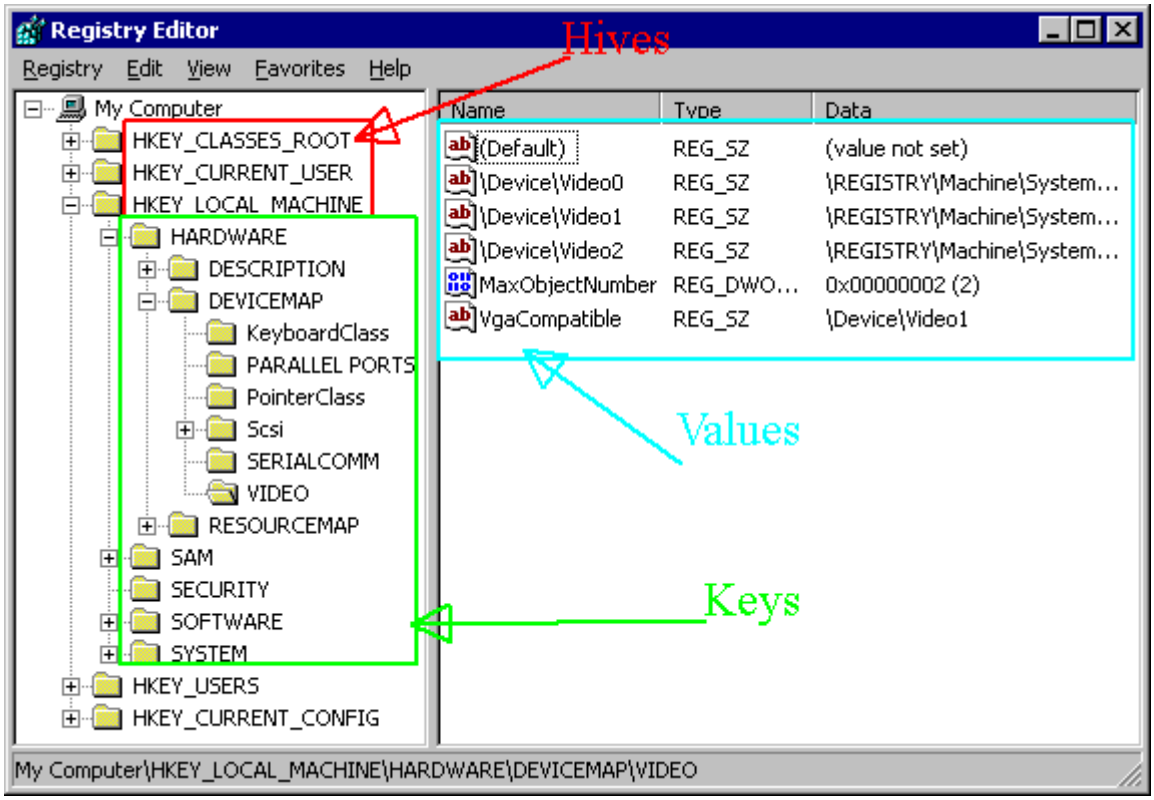
So the hierarchy goes: Hive → Keys → Subkeys → Values. That's the structure you navigate when you open the registry.

3.3 The Root Keys (Hives)

When you open the Registry Editor, the very first things you see are the root keys these are the top-level hives. They are sometimes called 'root keys' because everything else branches out from them.

The five root keys you'll see are:

- HKEY_LOCAL_MACHINE (HKLM) — machine-wide configuration: hardware, installed software, system settings
- HKEY_CURRENT_USER (HKCU) — settings for the currently logged-in user
- HKEY_USERS — settings for all user profiles on the machine
- HKEY_CLASSES_ROOT — file type associations and COM objects
- HKEY_CURRENT_CONFIG — current hardware profile information



3.4 The Most Important Hives for Forensics

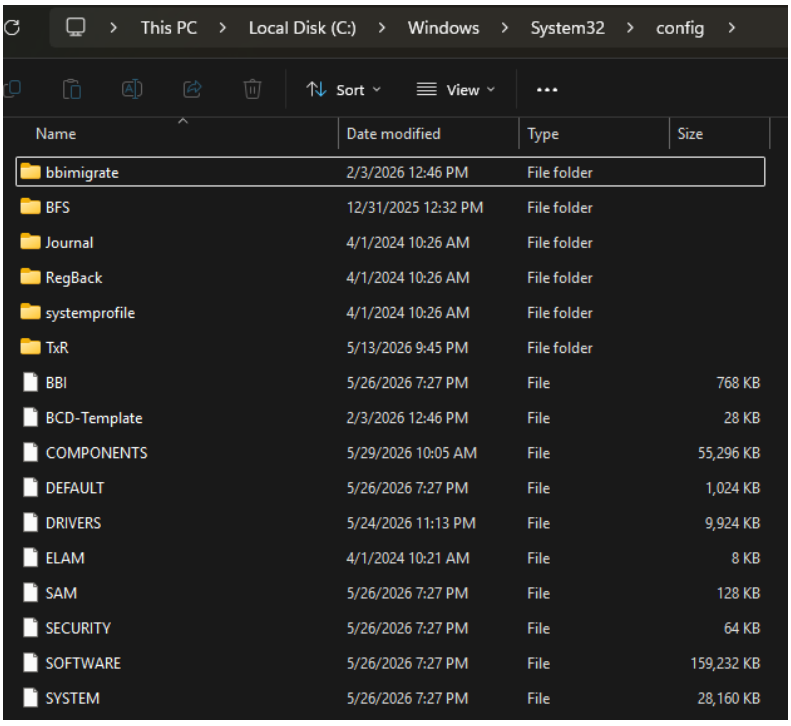
While all hives contain useful data, these are the ones you'll care about most during an investigation:

Hive	Why It Matters Forensically
SAM	Security Account Manager stores user accounts and password hashes. Critical for identifying who had accounts on the machine.
SECURITY	Security policies and audit settings — tells you how the system was configured for logging and access control.
SOFTWARE	All installed applications their configurations and settings live here.
SYSTEM	Hardware and drivers what devices were connected to the machine, system configuration.

3.5 Where Registry Files Live on Disk

The registry hive files are stored on disk at this path:

```
C:\Windows\System32\config
```



Inside that folder you will find files named SAM, SECURITY, SOFTWARE, and SYSTEM these are the actual binary files that make up the registry hives.

3.6 Transaction Log Files — The Registry's Safety Net

Here is something important to understand: Windows does not write changes to the registry hive files immediately. Instead, it uses a temporary holding area first.

When a change happens, Windows saves it to special temporary log files first you'll see these named:

```
SOFTWARE.LOG1
SOFTWARE.LOG2
```

These changes are only committed to the main hive file when the system properly shuts down or after a period of inactivity. This is a safety mechanism if the computer crashes, the registry doesn't get corrupted.

Note : *If a machine was abruptly powered off or crashed, some recent registry changes may only exist in the .LOG1 or .LOG2 transaction log files not in the main hive file. Always check these log files during an investigation.*

3.7 Dirty Hives and Forensic Investigation

- A "dirty hive" occurs when a computer shuts down improperly (e.g., power loss), leaving the main hive file incomplete
- Dirty hives are missing recent changes that were waiting in transaction logs
- Critical rule for investigators: When investigating a dirty hive, you must use the transaction logs
- Without transaction logs, the most recent minutes or hours of evidence may be lost - often the most important evidence

3.8 Forensic Tools and Cleaning Process

- Registry Explorer is the recommended tool as it can detect dirty hives and help clean them by merging the logs
- The cleaning process involves pointing the tool to the correct transaction log files
- After selecting the log file, the complete hive can be saved
- Registry Explorer is the top choice for forensic investigation - it can find deleted keys and handle cleaning operations
- Regripper is another tool used to extract important forensic data from hives