Regripper

windows Registry Forensic Analysis tool

Introduction to the Windows Registry .

Introduction to RegRipper .

Analysis of Registry files with RegRipper .

Introduction to the Windows Registry

The Windows Registry is a hierarchical database that stores the configuration settings of the operating system, applications, users, and devices.

It serves as a valuable source of information about the system, including details about installed and executed programs, user activities, and connected devices.

Registry artifacts can provide critical insights, such as detecting the presence of malware.

Structure of the Windows Registry

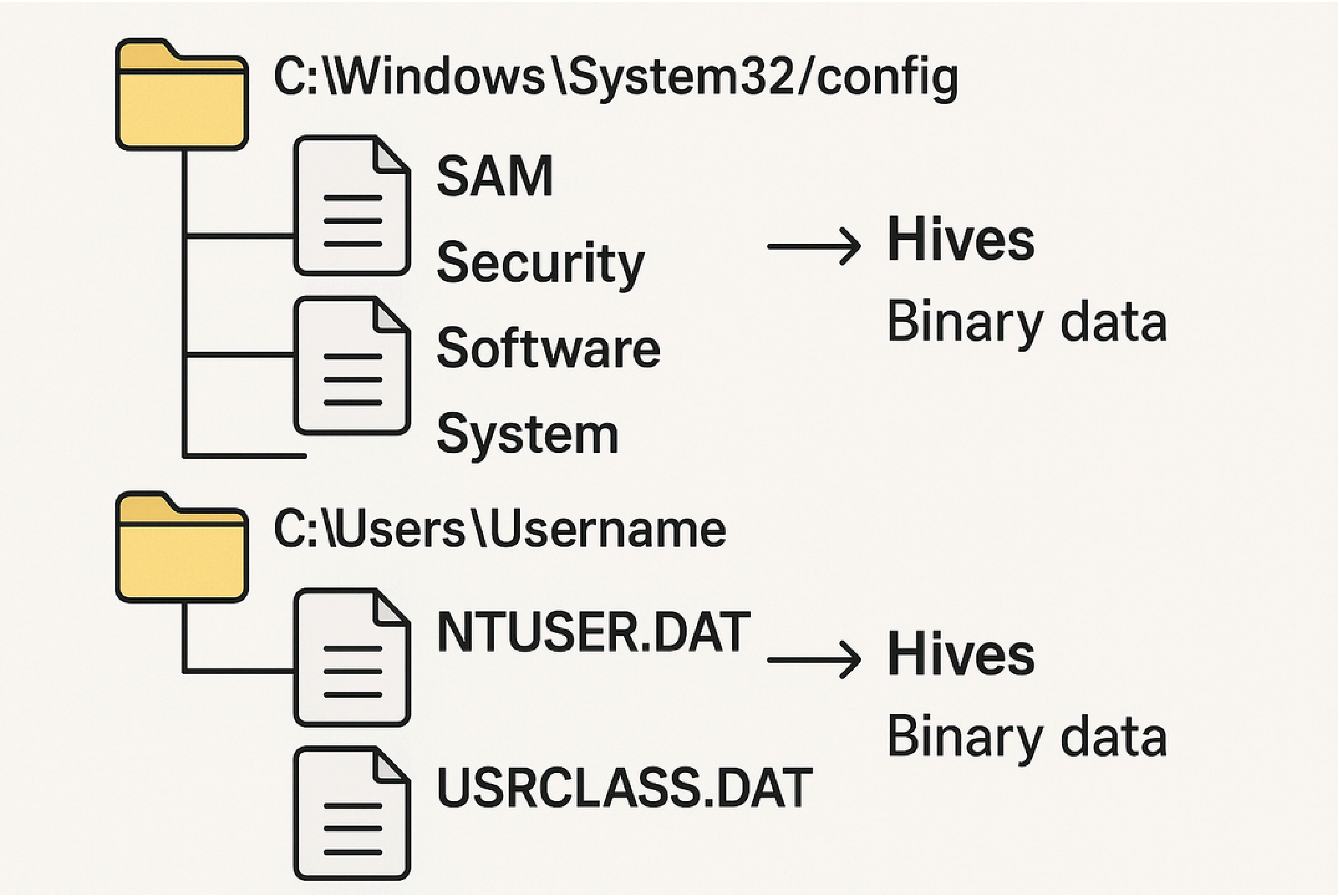
- The Windows Registry is composed of binary data files known as "hives."

- The primary registry hives include: SAM,Security ,Software ,System.

- These hives are stored in the directory: C:\Windows\system32\config

- Additionally, each user has their own registry hives: NTUSER.DAT and USRCLASS.DAT

- These user-specific hives are located within the respective user’s profile directory.



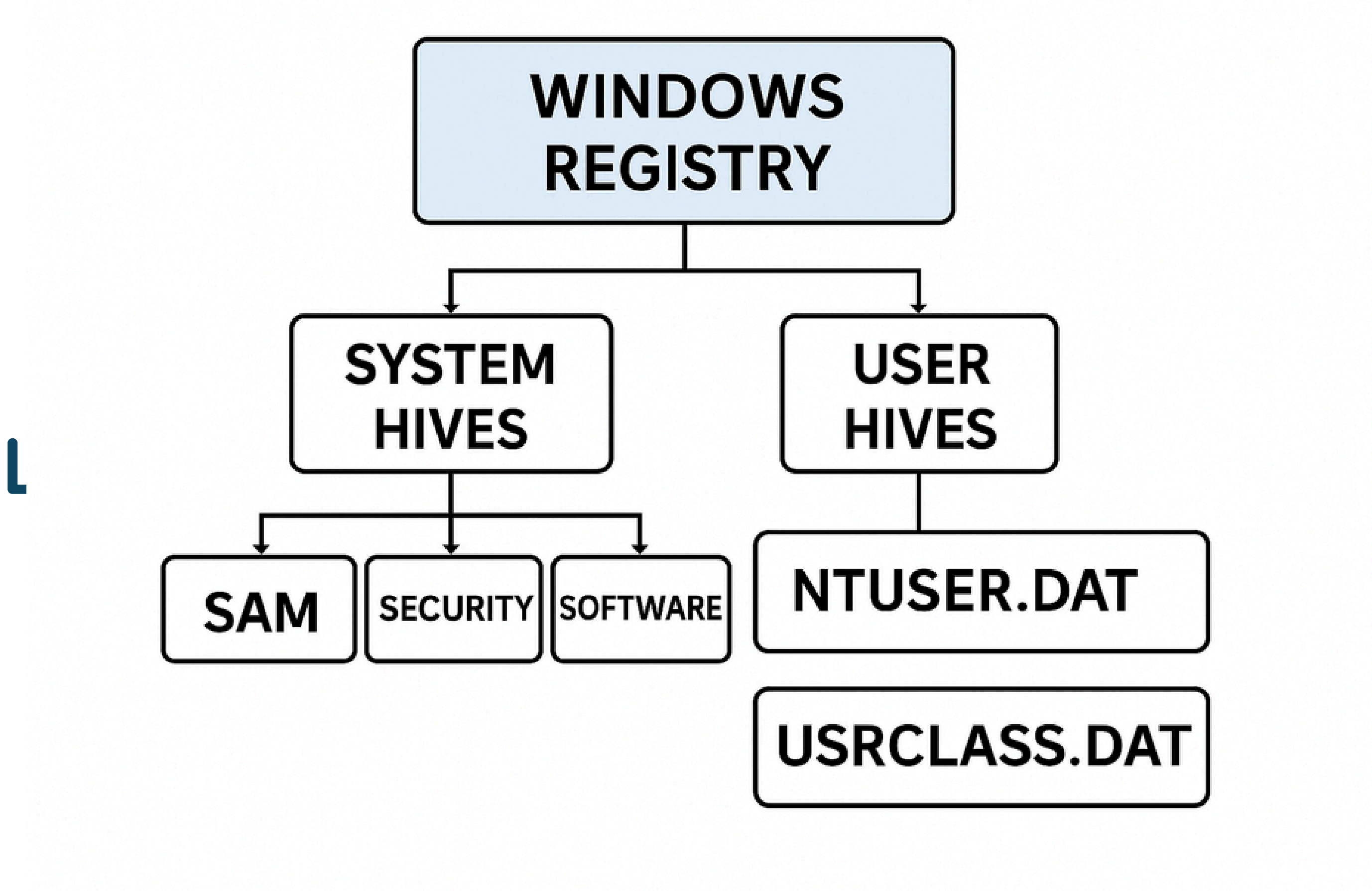
Structure of the Windows Registry

The Registry has two basic elements **: keys** and **values.**

Keys : are containers that can include other keys and/or values.

Values are identified by a **name**, a **type**, and the **associated data value**.

The most important root key is **HKEY_LOCAL_MACHINE (HKL** where the main registry hives are mapped as subkeys.



Windows Registry Hives and Their Functions

The Windows Registry is organized into several key hives, each serving a distinct purpose:

SAM (Security Accounts Manager):

The SAM hives contains the users‘ settings and hached passwords

Security:

stores the system security settings

Software:

stores the Windows and the programs configuration

System:

contains the information about the system and the connected devices

Introduction to RegRipper

RegRipper

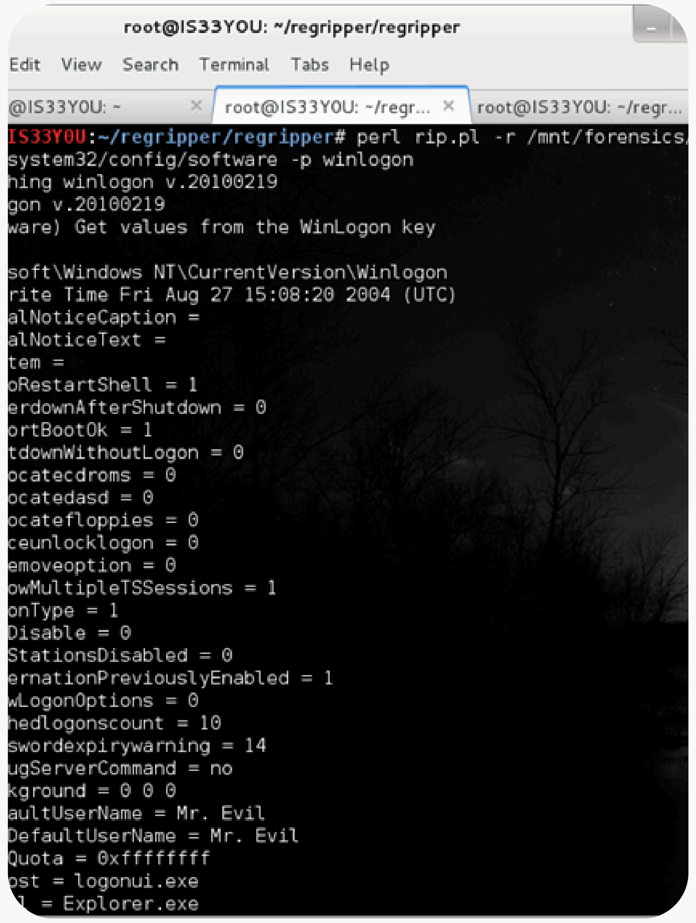
www.RegRipper.wordpress.com

RegRipper : is an open-source tool designed to extract, and analyze data from the Windows registry , It is written in Perl and developped by Harlan Carvey..

RegRipper executes plugins to parse the Registry and extract specific data There are hundreds of plugins available that are being updated and new plugins added.

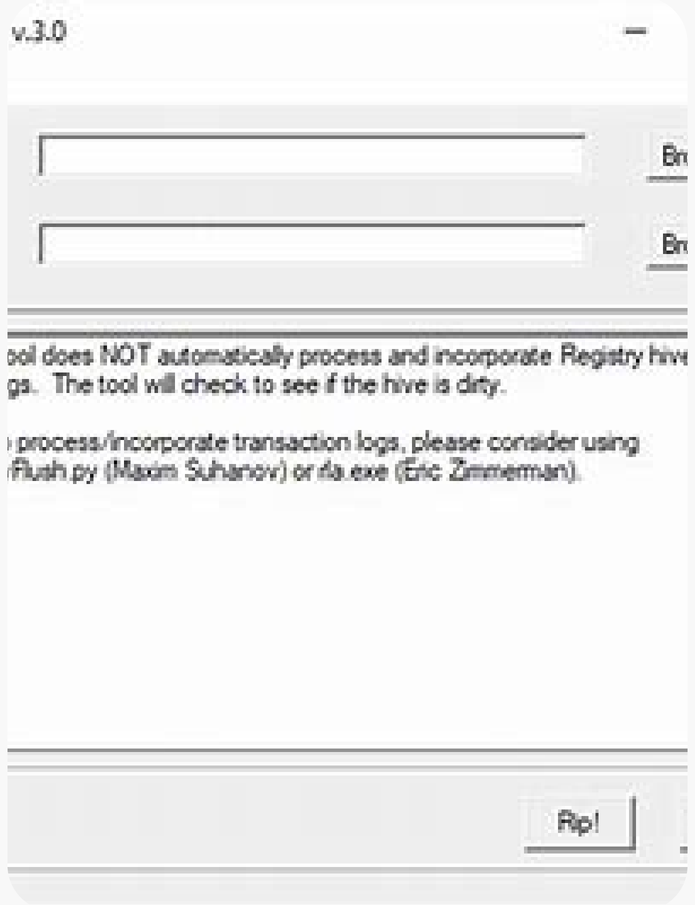
- For example:
    - usbdevices: Lists USB devices connected.
    - userassist: Shows programs recently run by users.
    - services: Lists installed Windows services.

Usage Modes


root@IS33YOU: ~/regripper/regripper
Edit View Search Terminal Tabs Help
@IS33YOU: ~
root@IS33YOU: ~/regr...
root@IS33YOU: ~/regr...

```
IS33YOU:~/regripper/regripper# perl rip.pl -r /mnt/forensics/
system32/config/software -p winlogon
hing winlogon v.20100219
gon v.20100219
ware) Get values from the WinLogon key

soft\Windows NT\CurrentVersion\Winlogon
rite Time Fri Aug 27 15:08:20 2004 (UTC)
alNoticeCaption =
alNoticeText =
tem =
oRestartShell = 1
erdownAfterShutdown = 0
ortBootOk = 1
tdownWithoutLogon = 0
ocatecdroms = 0
ocatedasd = 0
ocatefloppies = 0
ceunlocklogon = 0
emoveoption = 0
owMultipleTSSessions = 1
onType = 1
Disable = 0
StationsDisabled = 0
ernationPreviouslyEnabled = 1
wLogonOptions = 0
hedlogonscount = 10
swordexpirywarning = 14
ugServerCommand = no
kground = 0 0 0
aultUserName = Mr. Evil
DefaultUserName = Mr. Evil
Quota = 0xffffffff
ost = logonui.exe
l = Explorer.exe
```



ool does NOT automatically process and incorporate Registry hive
gs. The tool will check to see if the hive is dirty.

process/incorporate transaction logs, please consider using
Flush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

1. **RegRipper (CLI version):** Command-line interface to run plugins on registry hives.

1. **RRGUI:** A simple graphical interface for selecting hives and plugins.

Use Cases

Digital Forensics Investigations

- RegRipper helps examiners reconstruct user and system activity during an investigation.

✅ **Key Plugins :**

- **UserAssist** : track programs executed by users.
- **MRUList** : see recently accessed files.
- **ShellBags** : reconstruct folder views and access.
- **USBSTOR** : list connected USB devices.

🧩 **Why it's useful:** Reveals user behavior, access patterns, and possible insider threats.

Use Cases

Malware Analysis

- RegRipper helps identify persistence mechanisms and malware footprints left in the Registry

✅ **Key Plugins :**

- **Run / RunOnce :** programs set to run at startup.
- **Services :** new or suspicious services.
- **AppInit_DLLs :** Image File Execution Options – stealthy persistence tricks.
- **ShimCache / AmCache :**track executed binaries.

🧩 **Why it's useful:** Identifies how malware installs, hides, and survives reboots.

Use Cases

Incident Response

- Quick registry analysis for live or post-incident response helps understand attack vectors or lateral movement.

✅ **Key Plugins :**

- **NetworkList / DHCP :** network connections and IP history..
- **FirewallRules :** firewall config and exceptions.
- **UserAccounts / SAM** :accounts created or modified.
- **LSA Secrets (from SECURITY hive) :** possible credential theft.

🧩 **Why it's useful:** Helps responders identify attackers' tracks and system exposure.

Use Cases

System Auditing / Baselining

- Understand system configuration, installed software, and scheduled tasks for security audits.

✅ **Key Plugins :**

- **Installed Programs (Uninstall key) :** lists software.
- **Scheduled Tasks / Services :** background processes and auto-start entries.
- **TimeZone / ControlSet info** : system settings and last boot.

🧩 **Why it's useful:** Assists in creating secure baselines and spotting anomalies in system setup

Conclusion

By automating the complex task of registry analysis, RegRipper improves both speed and precision, revealing evidence that might otherwise go unnoticed. Whether used in cybersecurity investigations

Thank you