

Lab 7: Registry Forensics with RegRipper Plug-ins

Registry là gì ?

- Windows registry là một cơ sở dữ liệu theo hình thức phân cấp, lưu trữ các cấu hình của hệ điều hành, ứng dụng, người dùng và thiết bị.
- Đó là một nguồn thông tin quý giá về hệ thống, các chương trình đã được cài đặt và thực thi, hoạt động của người dùng và các thiết bị kết nối.
- Những dấu vết trong registry cũng có thể tiết lộ sự hiện diện của phần mềm độc hại.
- Windows registry là một tập hợp các tệp dữ liệu nhị phân, còn được gọi là "hive".
- Các hive chính của registry là SAM, Security, Software và System.
- Chúng được lưu trữ tại đường dẫn C:\windows\system32\config.
- Ngoài ra, còn có các hive cụ thể của người dùng là NTUSER.DAT và USRCLASS.DAT.
- Chúng được lưu trữ trong user profile tương ứng.
- Hive SAM chứa các cài đặt, thiết lập của người dùng và các mật khẩu được mã hóa bằng các hàm băm.
- Hive Security chứa các cài đặt bảo mật của hệ thống.
- Hive Software lưu trữ cấu hình của cửa sổ và các chương trình.
- Hive System lưu trữ thông tin về hệ thống và các thiết bị được kết nối.
- Registry có hai thành phần cơ bản: key (khóa) và value (giá trị).
- Key là các containers có thể chứa các key hoặc value khác.
- Value được xác định bởi tên, loại và giá trị dữ liệu kết hợp.
- Key gốc quan trọng nhất là HKLY_LOCAL_MACHINE, trong đó các hive chính của registry được ánh xạ làm các subkey.

Regripper là gì ?


- RegRipper là một công cụ để trích xuất và phân tích dữ liệu từ hệ thống registry.
- Nó được viết bằng ngôn ngữ Perl.
- RegRipper thực thi các plugin để phân tích cú pháp đăng ký và trích xuất dữ liệu.

Bây giờ chúng ta sẽ tiến hành cài đặt Regripper thông qua đường link này nhé

Google Code Archive

Search this site

Projects Search About

Project  regripper

Source

Issues

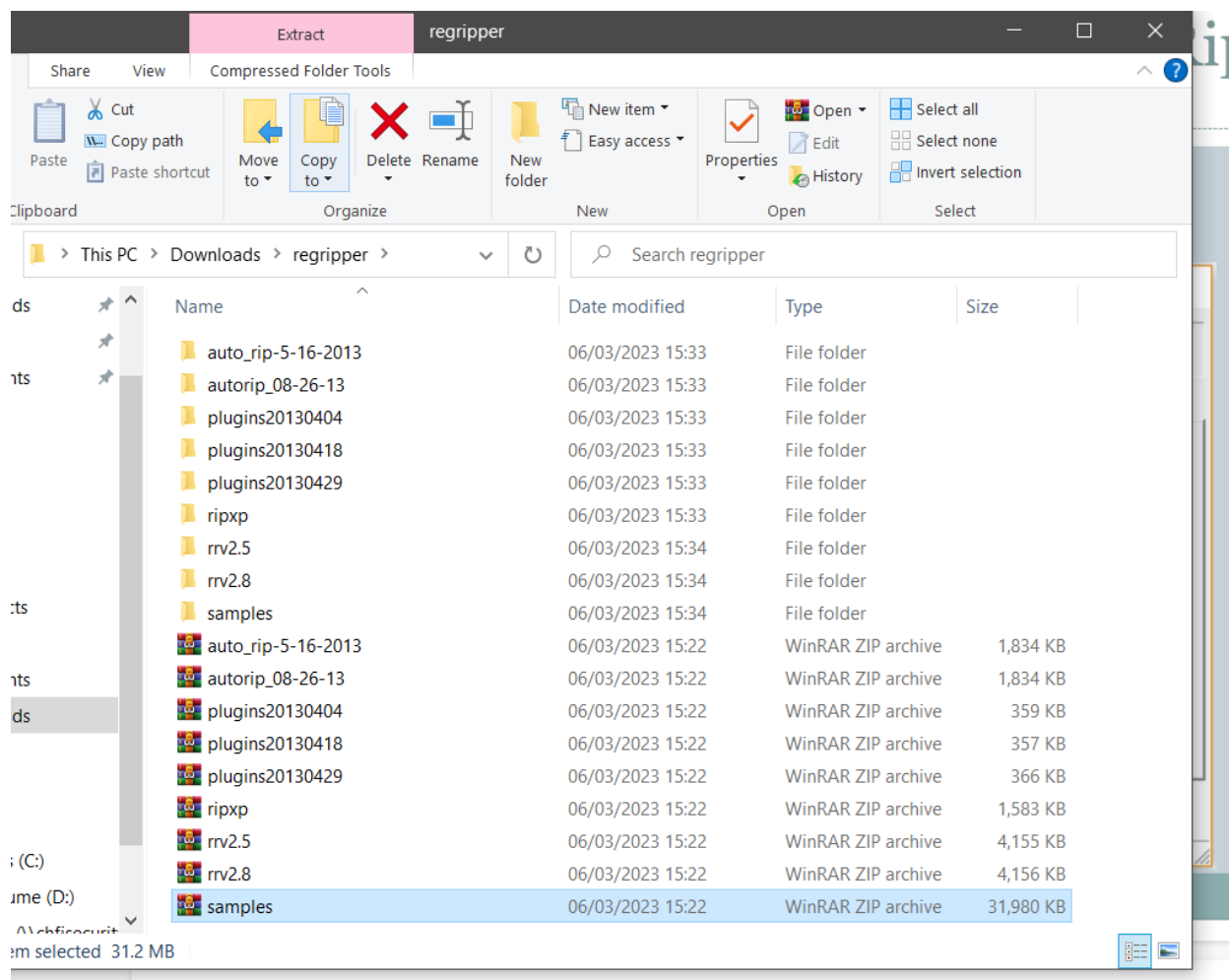
Wikis

Downloads

File	Summary + Labels	Uploaded	Size
autorip_08-26-13.zip	autorip_08-26-13.zip	Aug 26, 2013	1.79MB
ripxp.zip	RipXP	Jun 29, 2013	1.55MB
auto_rip-5-16-2013.zip	auto_rip, 16 May 2013 Deprecated	May 22, 2013	1.79MB
rv2.8.zip	RegRipper v2.8	Apr 30, 2013	4.06MB
plugins20130429.zip	Plugin updates, 29 April 2013	Apr 30, 2013	365.67KB
plugins20130418.zip	Plugin updates, 18 Apr 2013	Apr 19, 2013	356.36KB
plugins20130404.zip	RegRipper plugin archive	Apr 4, 2013	358.63KB
rv2.5.zip	RegRipper download	Apr 4, 2013	4.06MB
samples.zip	Sample hives	Oct 2, 2012	31.23MB

<https://code.google.com/archive/p/regripper/downloads>

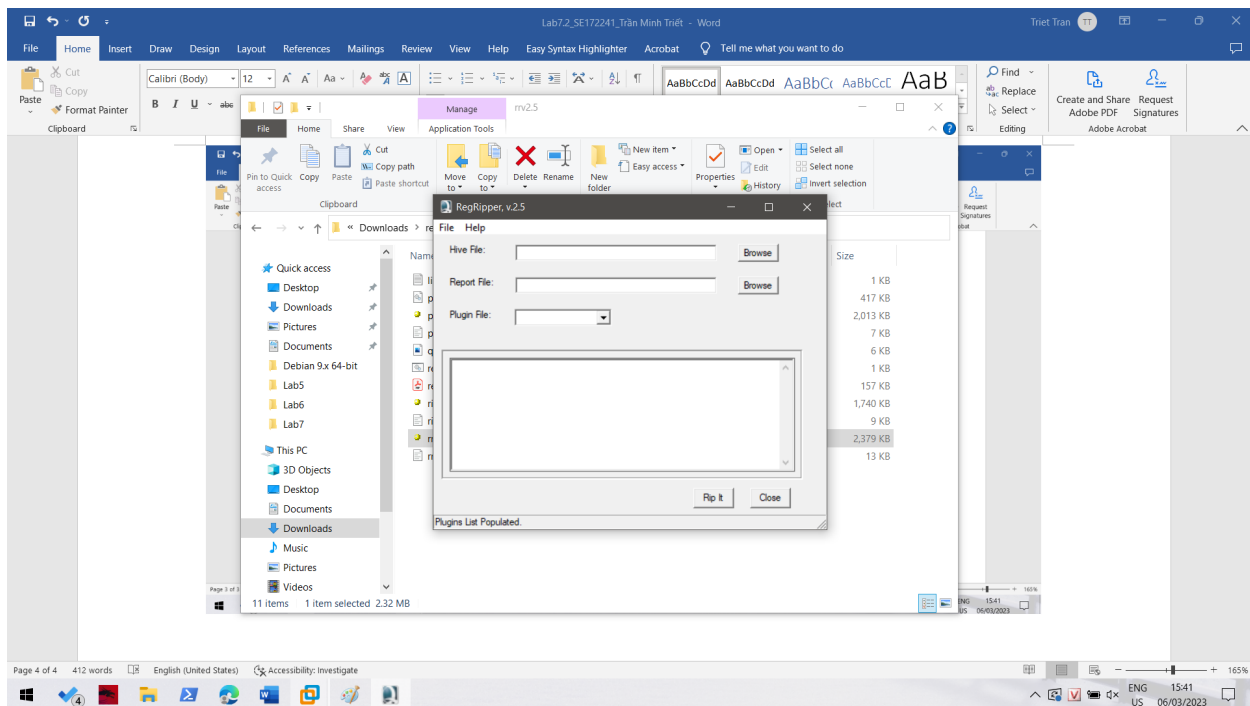
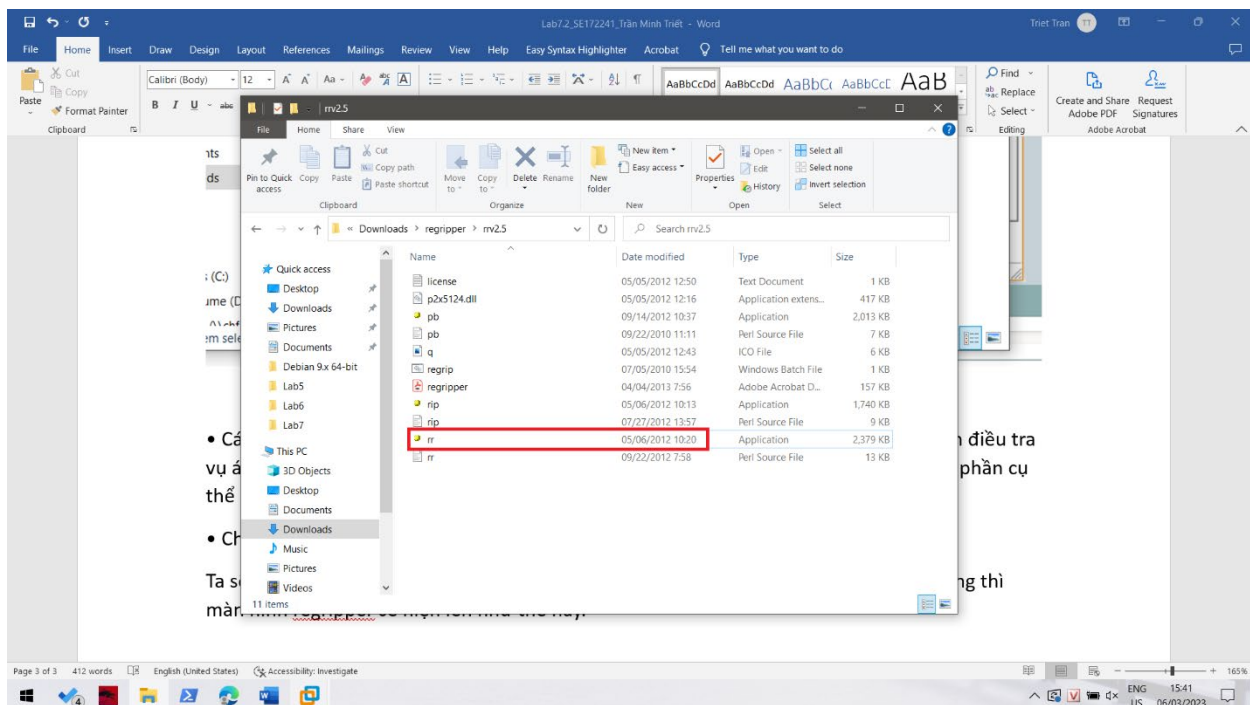
<https://code.google.com/archive/p/regripper/downloads>



- Các plugin là các tập lệnh Perl được đóng góp bởi cộng đồng forensic. Trong quá trình điều tra vụ án pháp y của bạn, thường xuyên sử dụng RegRipper để trích xuất thông tin từ một phần cụ thể của registry.

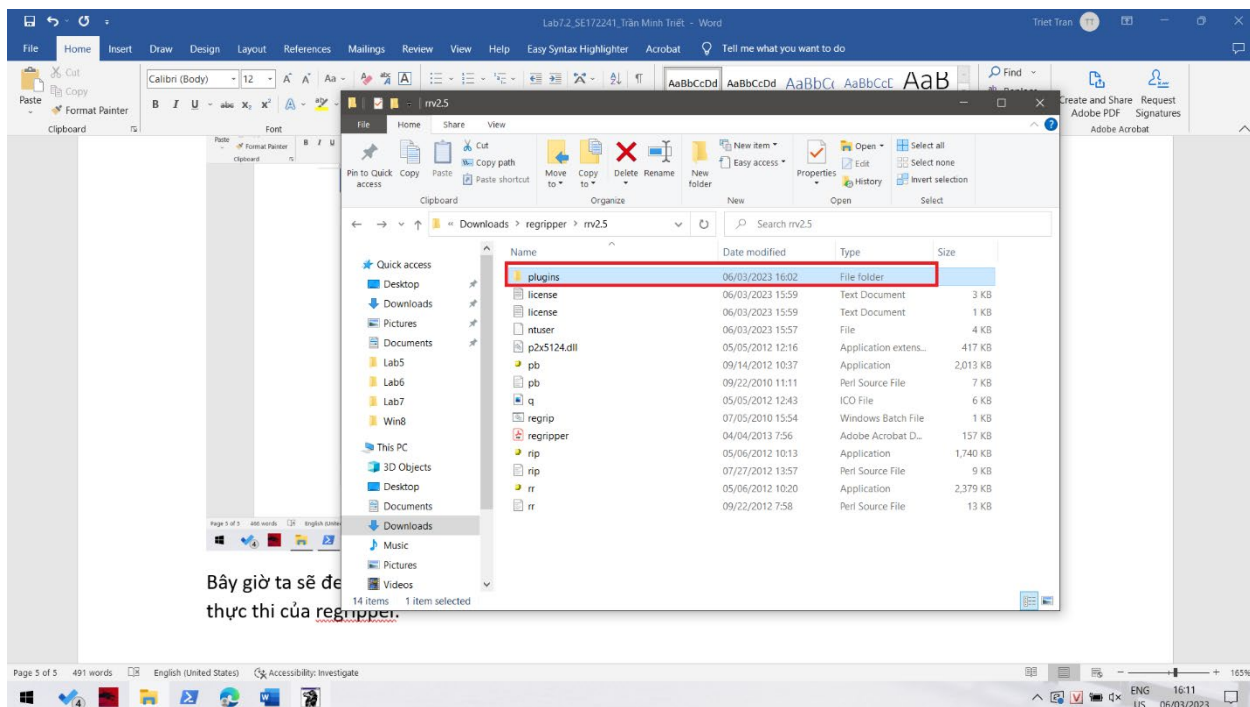
- Chúng ta sẽ sử dụng các plugin có sẵn.

Ta sẽ sử dụng folder rrv2.5. Chọn nhấn vào file thực thi tên “rr” file application cuối cùng thì màn hình regripper sẽ hiện lên như thế này.

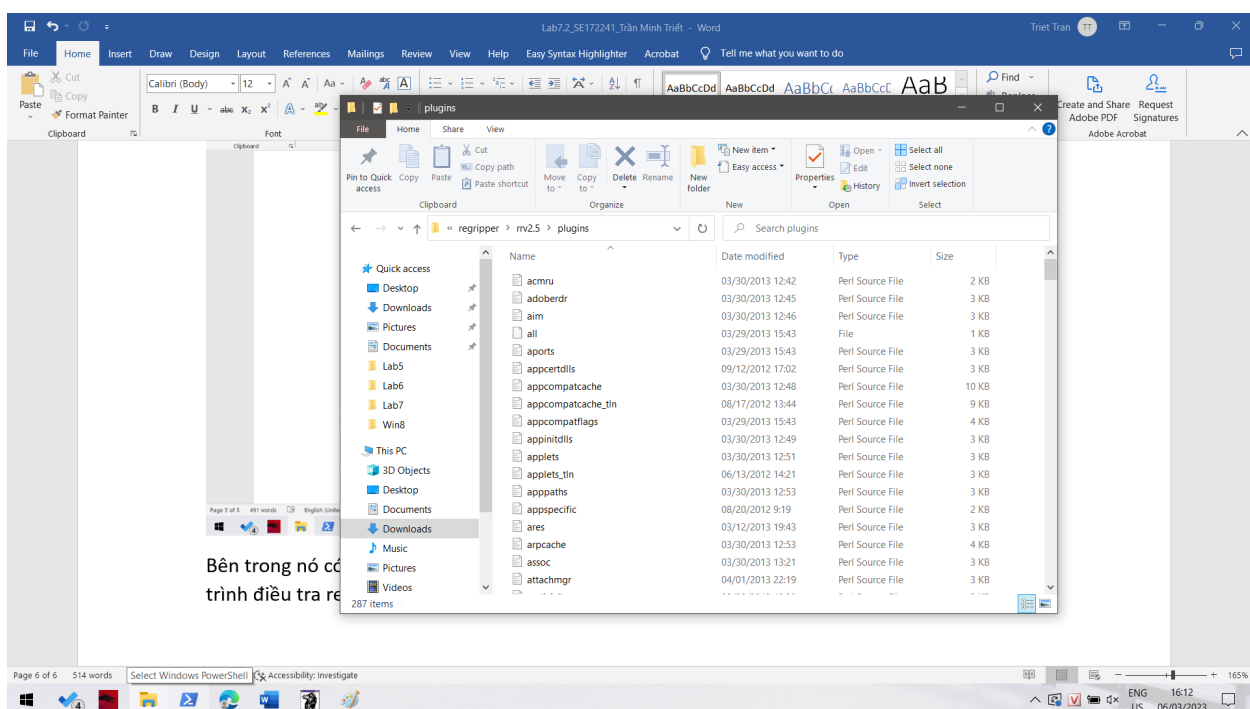


Tuy nhiên regripper là một công cụ chạy dựa trên plugin mà bây giờ tool của chúng ta chưa được import plugin nào nên ta phải đi import chúng cho nó.

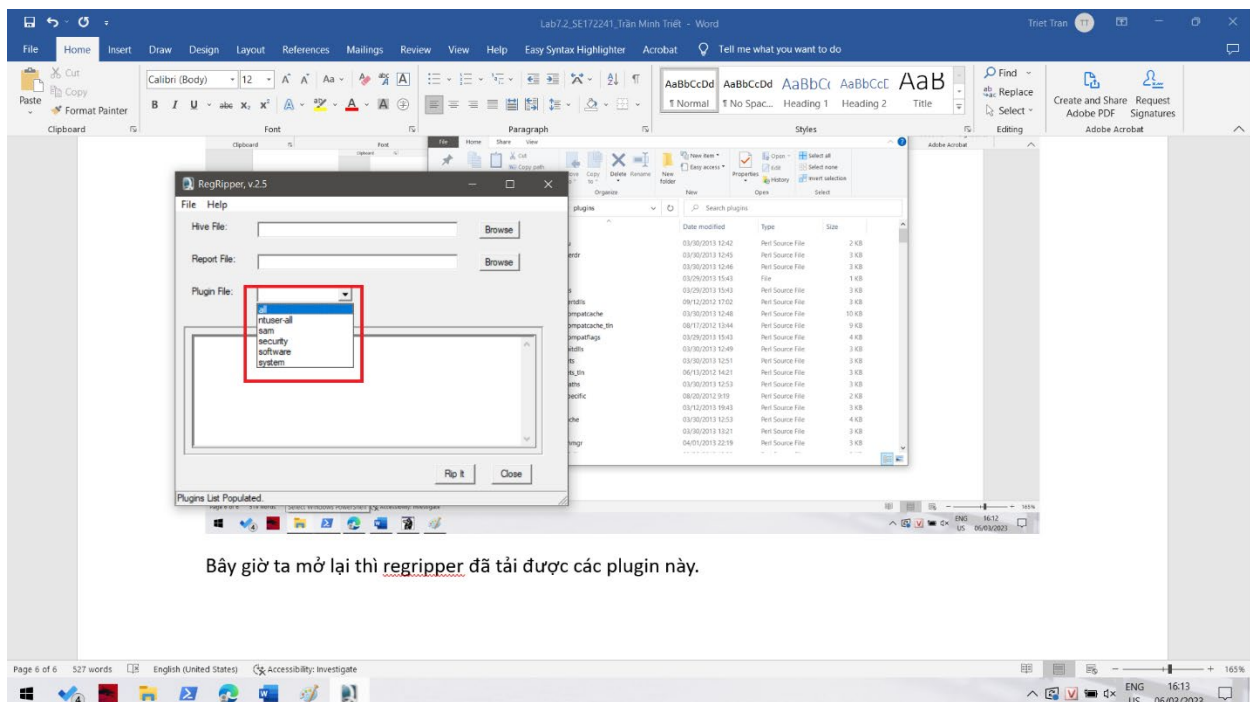
Ta sẽ bấm vào file exe đầu tiên trong folder này để xem thông tin của mỗi plugin cũng như save chúng lại.



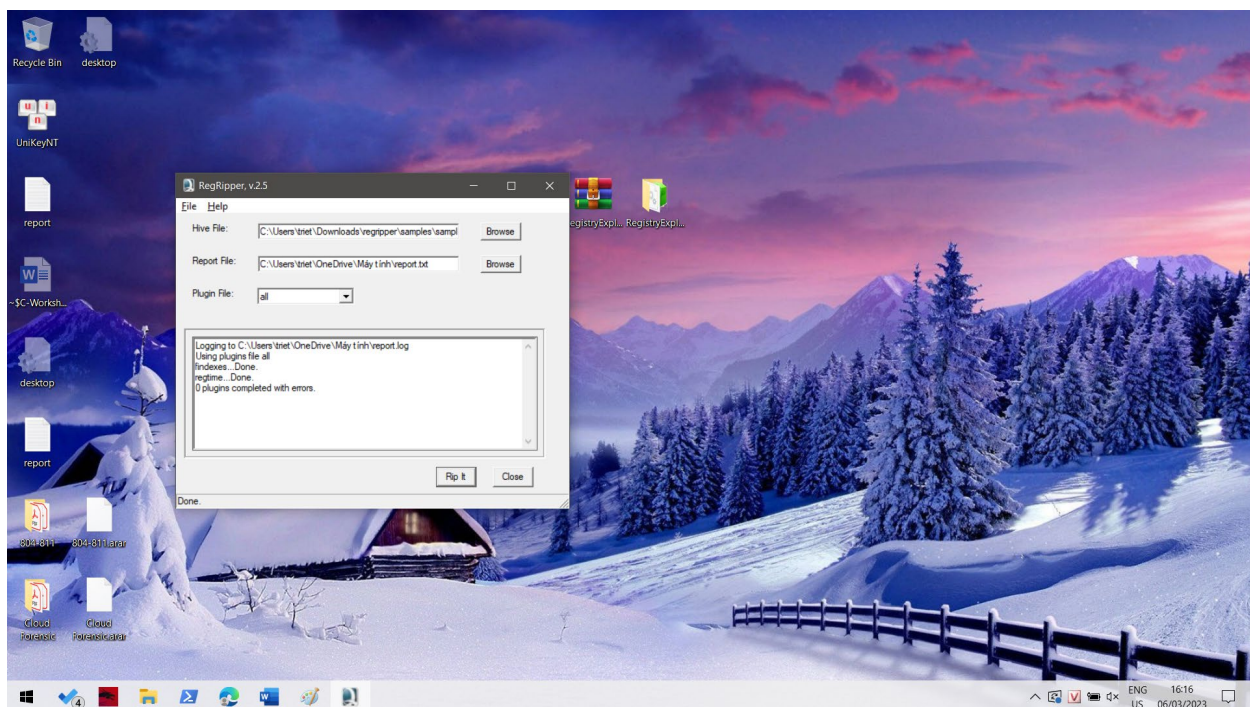
Bên trong nó có chứa rất nhiều plugin khác nhau được viết bằng perl nhằm phục vụ cho quá trình điều tra registry.



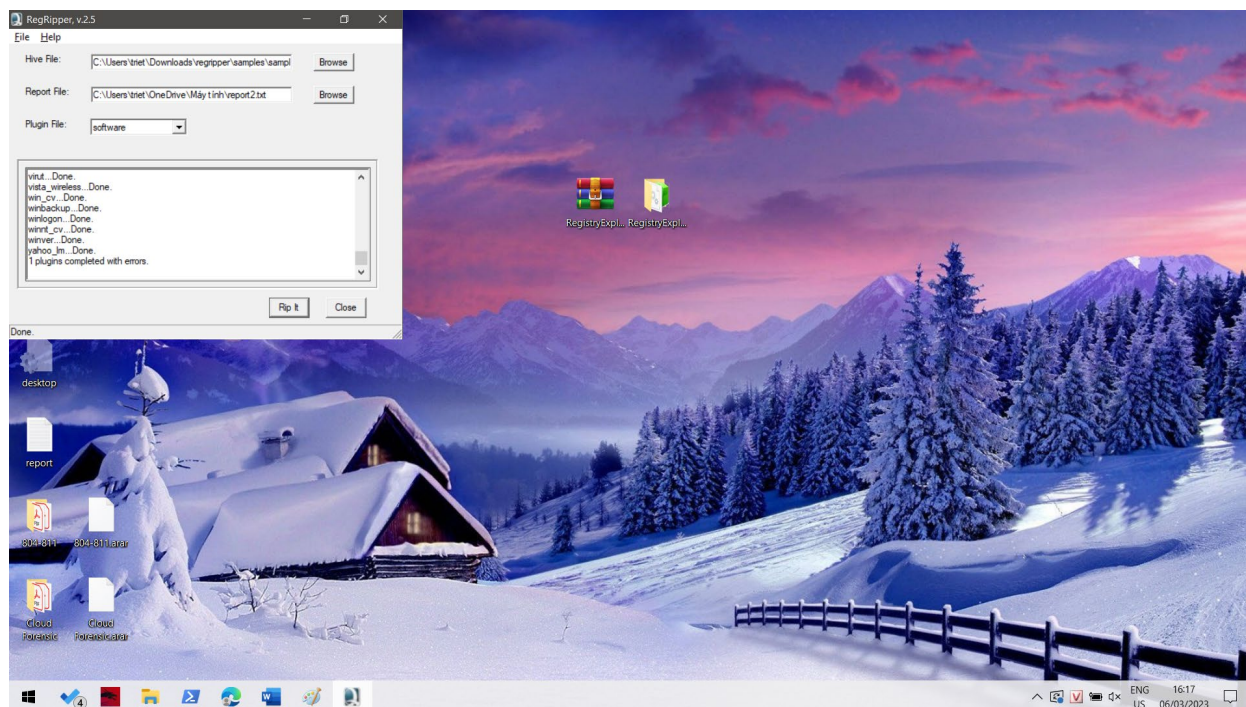
Bây giờ ta mở lại thì regripper đã tải được các plugin này.



Ta chọn 1 plugin, load file registry sample vào và chỉ đường dẫn tới file report để regripper tạo ra báo cáo cho quá trình phân tích registry.

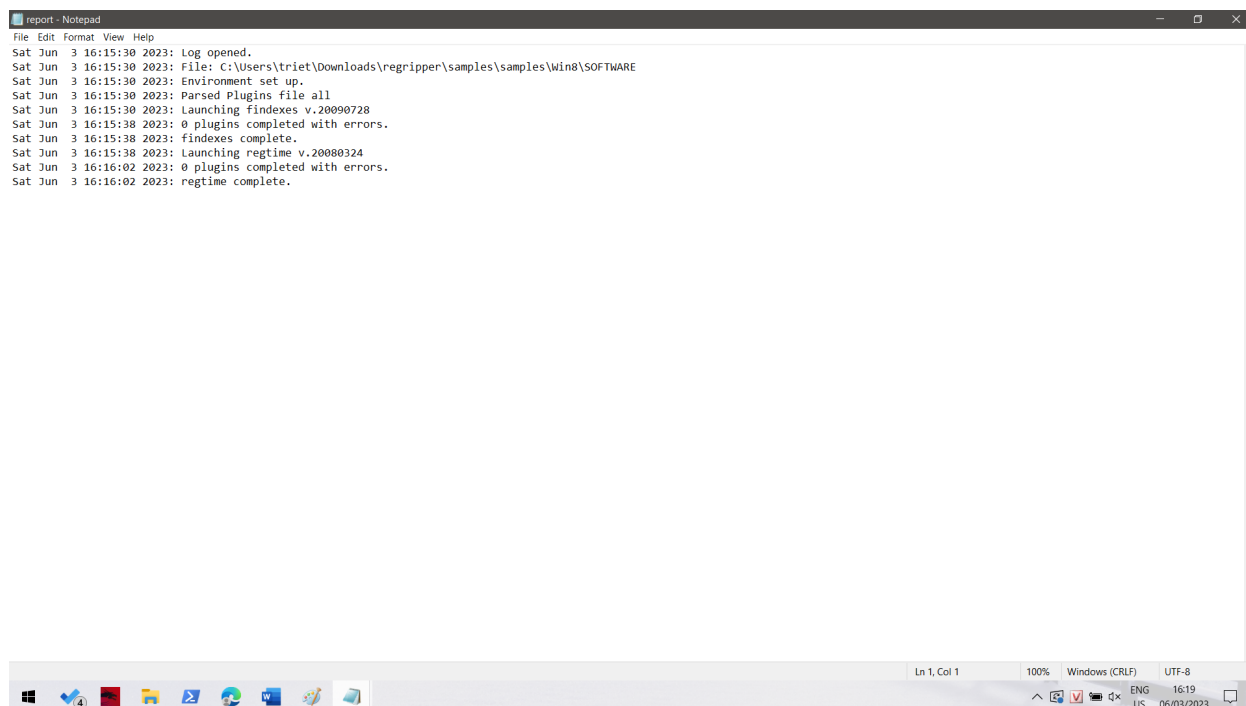


Ở bước này em sử dụng tất cả plugin để phân tích nên màn hình output có hơi ngắn gọn nhưng nó phân tích đầy đủ.



Còn đây là output khi ta chỉ load 1 plugins.

Sau khi quá trình phân tích hoàn tất thì regripper sẽ tạo ra cho ta 2 file: 1 file report.txt và report.log.



File report.log thì ghi nhận lại quá trình regripper phân tích registry có lỗi gì không, có plugin nào xử lý lỗi không kèm theo các thông tin chi tiết khác như timestamp và message.

Còn file report.txt mới chính là file kết quả phân tích chính của chúng ta.

```
report - Notepad
File Edit Format View Help
fileexts v.20090728
(All) Scans a hive file looking for binary value data that contains MZ

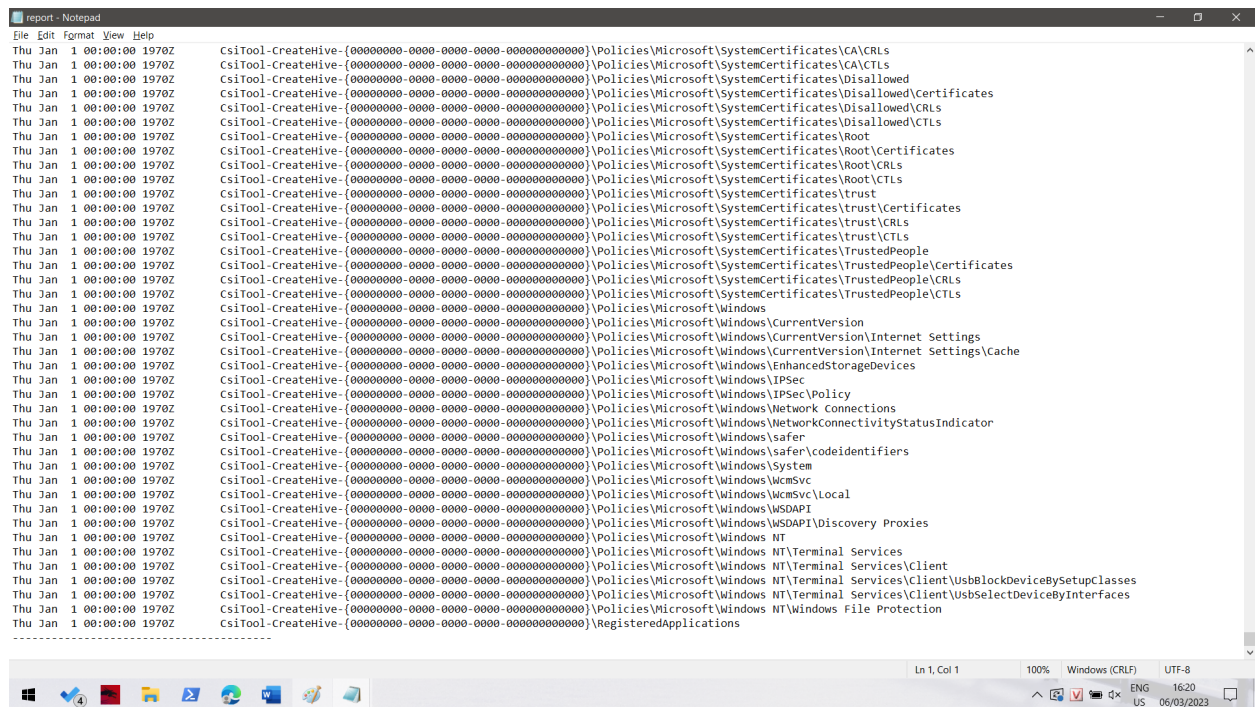
Key: Microsoft\SystemCertificates\Disallowed\Certificates\471C949A8143DB5AD5CDF1C972864A2504FA23C9 LastWrite time: Thu Jan 1 00:00:00 1970
Value: Blob Length: 1751 bytes

Key: Microsoft\SystemCertificates\AuthRoot\AutoUpdate LastWrite time: Thu Jan 1 00:00:00 1970
Value: EncodedCTL Length: 108452 bytes

Number of values w/ binary data types: 11290
Number of values w/ MZ in binary data: 2
-----
regtime v.20080324
(All) Dumps entire hive - all keys sorted by LastWrite time

Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\ATI Technologies
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\ATI Technologies\Install
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\ATI Technologies\Install\South Bridge
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\ATI Technologies\Install\South Bridge\ATI_AHCI_RAID
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList\Excel.exe
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList\Explore.exe
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList\MSPaint.exe
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList\notepad.exe
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList\Winword.exe
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\OpenWithList\Wordpad.exe
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\shell
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\shell\removeproperties
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\shell\removeproperties\DropTarget
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\shell\
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers\BriefcaseMenu
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers\Open With
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers\Open With EncryptionMenu
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers\Sharing
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers\{90AA3A4E-1CBA-4233-8BB8-535773D48449}
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\ContextMenuHandlers\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\PropertySheetHandlers
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\PropertySheetHandlers\BriefcasePage
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes*\ShellEx\PropertySheetHandlers\CryptoSignMenu
```

```
report - Notepad
File Edit Format View Help
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\application
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\appref-ms
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\aps
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\aps\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\arc
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\arj
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\art
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\art\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asa
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asc
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asc\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ascx
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ascx\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASF
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASF\OpenWithProgIds
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASF\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASF\ShellEx
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASF\ShellEx\{8B2E617C-0920-11D1-9A0B-00C04FC2D6C1}
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASF\ShellEx\{e357fccd-a995-4576-b01f-234630154e96}
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asm
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asm\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asmx
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asp
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\asp\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\aspx
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\aspx\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASX
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASX\OpenWithProgIds
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\ASX\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\AU
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\AU\OpenWithProgIds
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\AU\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\avi
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\avi\OpenWithProgIds
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\avi\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\avi\ShellEx
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\avi\ShellEx\{8B2E617C-0920-11D1-9A0B-00C04FC2D6C1}
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\avi\ShellEx\{e357fccd-a995-4576-b01f-234630154e96}
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\bas
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\bas\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\bat
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\bat\PersistentHandler
Thu Jan 1 00:00:00 1970Z      CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Classes\bc
```



```
report - Notepad
File Edit Format View Help
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\CA\CRLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\CA\CTLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Disallowed
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Disallowed\Certificates
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Disallowed\CRLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Disallowed\CTLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Root
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Root\Certificates
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Root\CRLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\Root\CTLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\trust
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\trust\Certificates
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\trust\CRLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\trust\CTLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\TrustedPeople
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\TrustedPeople\Certificates
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\TrustedPeople\CRLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\SystemCertificates\TrustedPeople\CTLs
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\CurrentVersion
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Cache
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\EnhancedStorageDevices
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\IPSec
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\IPSec\Policy
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\Network Connections
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\NetworkConnectivityStatusIndicator
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\safer
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\safer\codeidentifiers
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\System
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\WcmSvc
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\WcmSvc\Local
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\WSDAPI
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows\WSDAPI\Discovery Proxies
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows NT
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows NT\Terminal Services
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows NT\Terminal Services\Client
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbBlockDeviceBySetupClasses
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\Policies\Microsoft\Windows NT\Windows File Protection
Thu Jan 1 00:00:00 1970Z CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}\RegisteredApplications
```

Rất nhiều thông tin được cung cấp từ timestamp đến tên của hive đến nội dung bên trong của hive đó như key và value.

Đây chỉ là một số ít plugin có sẵn trong công cụ RegRipper được sử dụng trong phân tích Windows registry. Sự tuyệt vời của công cụ này nằm ở tính linh hoạt và khả năng mở rộng của nó.

Tội phạm máy tính gây ra những mối đe dọa vô lý đối với xã hội hiện đại, vì máy tính hiện diện khắp nơi. Các tội phạm này có thể là gian lận, xâm nhập, tấn công gây không khả dụng, vi phạm bản quyền, v.v. Các nhà điều tra pháp y máy tính tìm kiếm các bằng chứng bổ nhiệm và bằng chứng trừu tượng từ hệ thống máy tính của một nghi phạm. Khi họ gặp phải một máy tính chạy Windows, Windows registry chứng tỏ là một nguồn thông tin quan trọng trong quá trình điều tra.

Vậy là ta đã hoàn thành bài sử dụng công cụ regripper này để phân tích registry rồi.