

ATERFACTOS: WRR Y REGRIPPER

RegRipper
<http://github.com/keydet89>

ERIC SERRANO MARIN

ANÁLISIS FORENSE INFORMÁTICO IES MARTINEZ MONTAÑES

Contenido

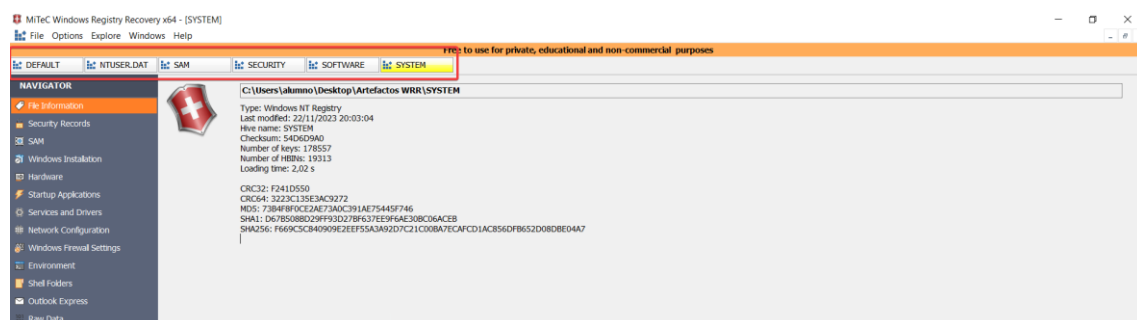
Realice un documento con explicaciones para realizar las siguientes tareas:

| | |
|---|----|
| | 2 |
| 1. Mediante Windows Registry Recovery muestre los datos más relevantes de: NTUSER.DAT, DEFAULT, SECURITY, SOFTWARE, SYSTEM y SAM (exportados con FTK Imager de c:\Windows\System32\Config). Explicación básica de la utilidad del archivo y datos más relevantes. | 2 |
| NTUSER.DAT.DAT | 3 |
| SAM | 4 |
| SECURITY..... | 5 |
| SOFTWARE. | 6 |
| SYSTEM | 8 |
| 2. Mediante regripper consola consiga la siguiente información de su sistema:..... | 11 |
| ➤ Zona horaria del equipo | 11 |
| ➤ Última vez que se ha apagado el sistema operativo | 11 |
| ➤ ¿Qué IP tiene?..... | 11 |
| ➤ Qué arquitectura tiene su equipo (x64, x86, AMD64, ...)..... | 11 |
| ➤ Nombre del equipo físico y en red | 12 |
| ➤ Versión de su sistema operativo, fecha y hora de su instalación... | 12 |
| ➤ ¿Cuál es el último usuario logueado?..... | 12 |
| ➤ ¿Qué sistema operativo utiliza? | 13 |
| ➤ ¿Qué versión de java python utiliza?..... | 13 |
| ➤ Añada la información de 2 plugins más que considere interesantes | 13 |
| ➤ Busque en Internet nuevos plugins para RegRipper, descárguelos y pruebe al menos 2 de estos plugins. | 15 |

Realice un documento con explicaciones para realizar las siguientes tareas:

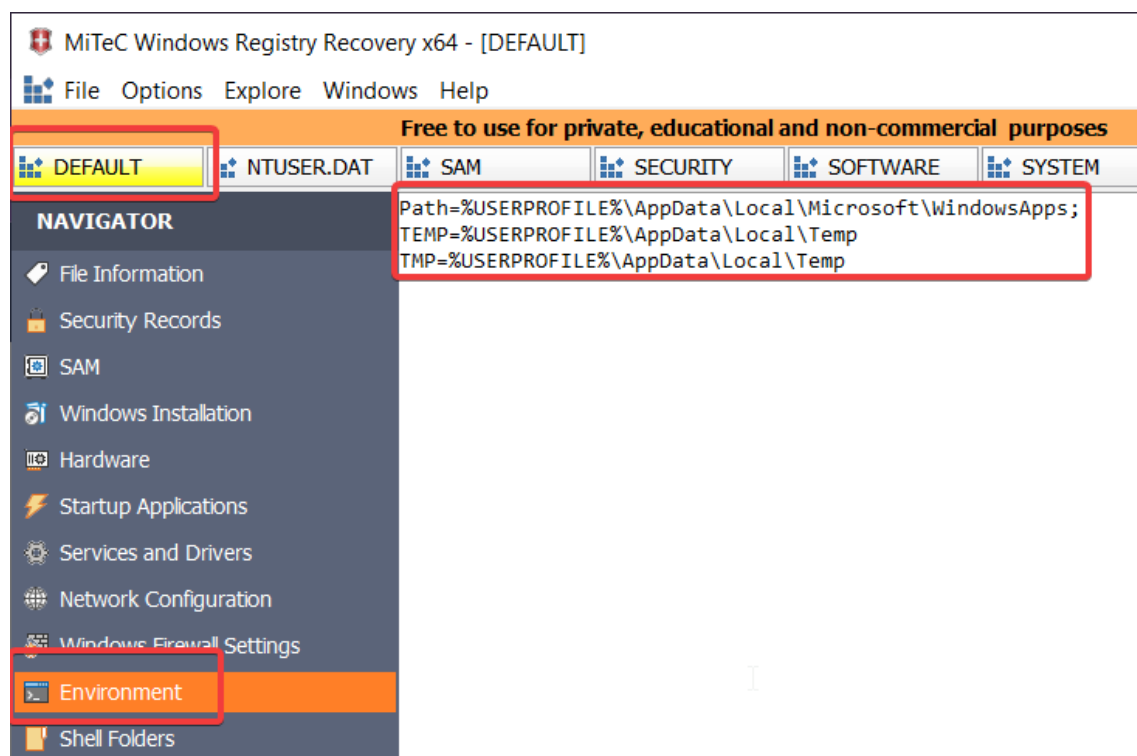
1. Mediante Windows Registry Recovery muestre los datos más relevantes de: NTUSER.DAT, DEFAULT, SECURITY, SOFTWARE, SYSTEM y SAM (exportados con FTK Imager de c:\Windows\System32\Config). Explicación básica de la utilidad del archivo y datos más relevantes.

Ya tenemos todos los archivos.

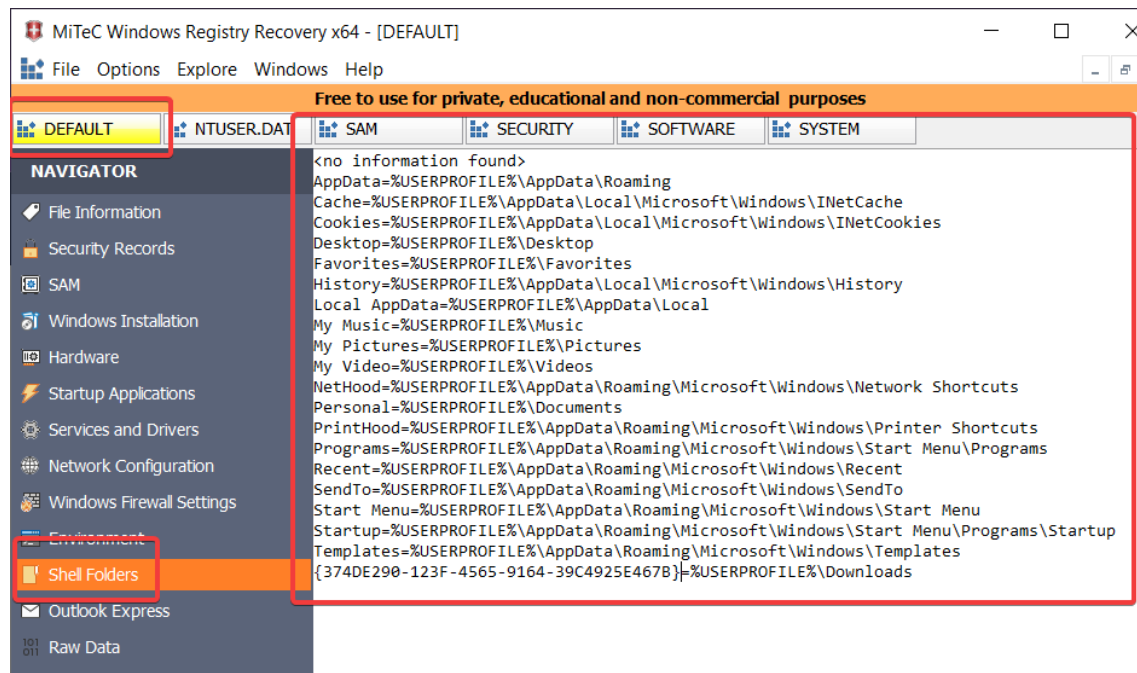


DEFAULT:

Variables de entorno de mi usuario Windows:



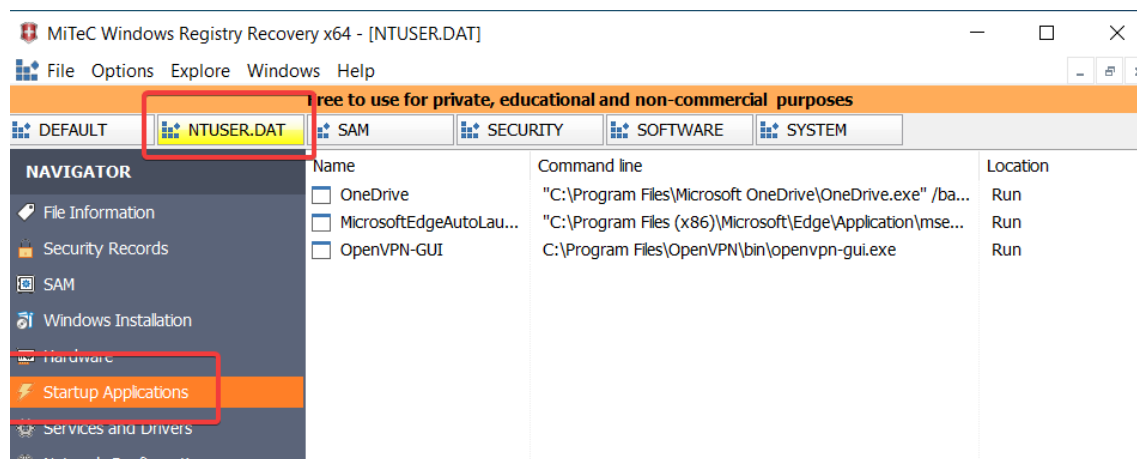
Carpetas predeterminadas y configuraciones de directorios especiales en el Registro de Windows.



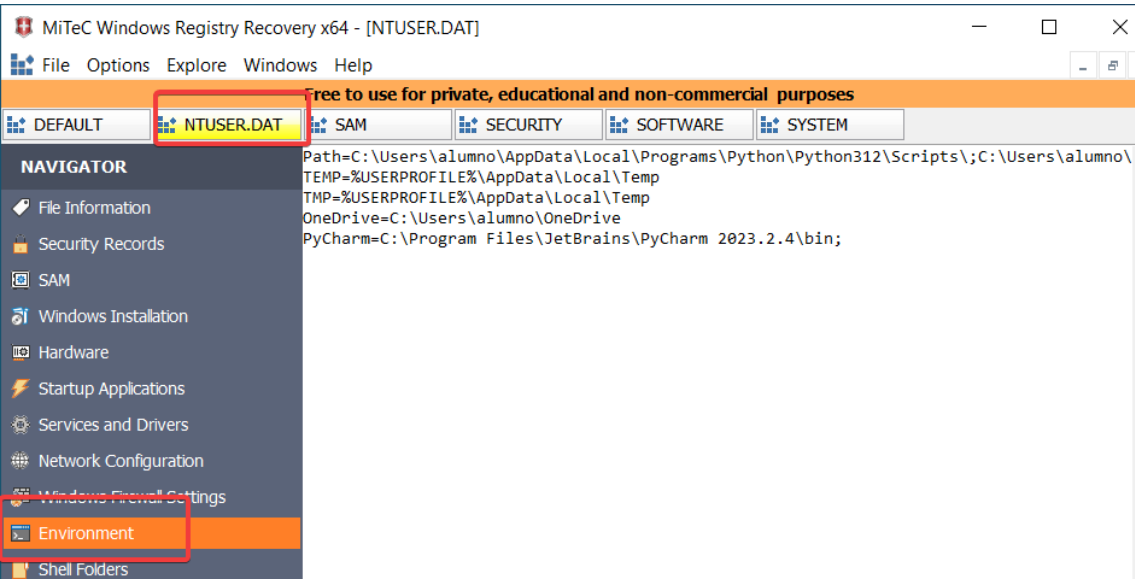
NTUSER.DAT

Configuraciones de registro, perfiles de usuario, Accesos y permisos..

Startup applications:



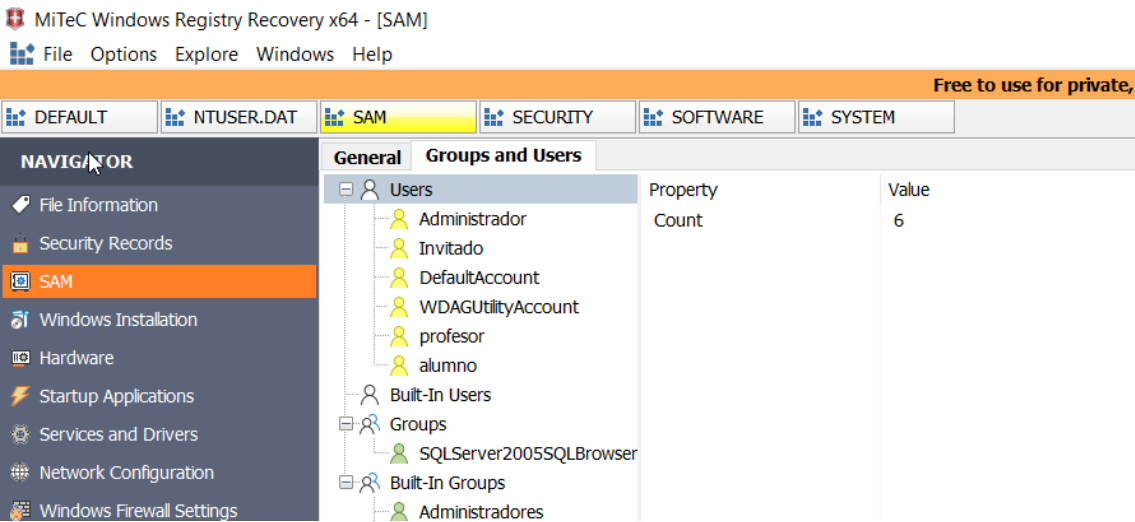
Variables de entorno:



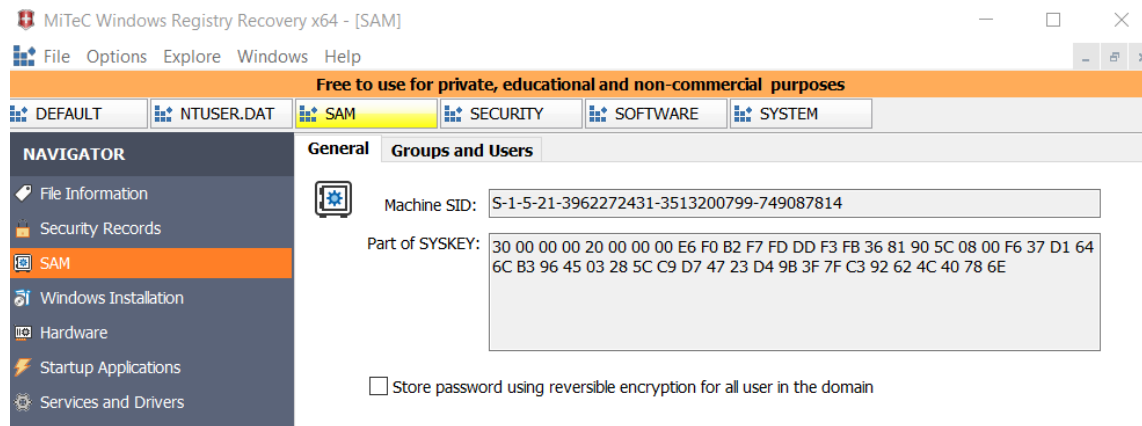
SAM

Almacena información relacionada con las cuentas de usuario y las políticas de seguridad.

Podemos ver todos los usuarios del sistema:

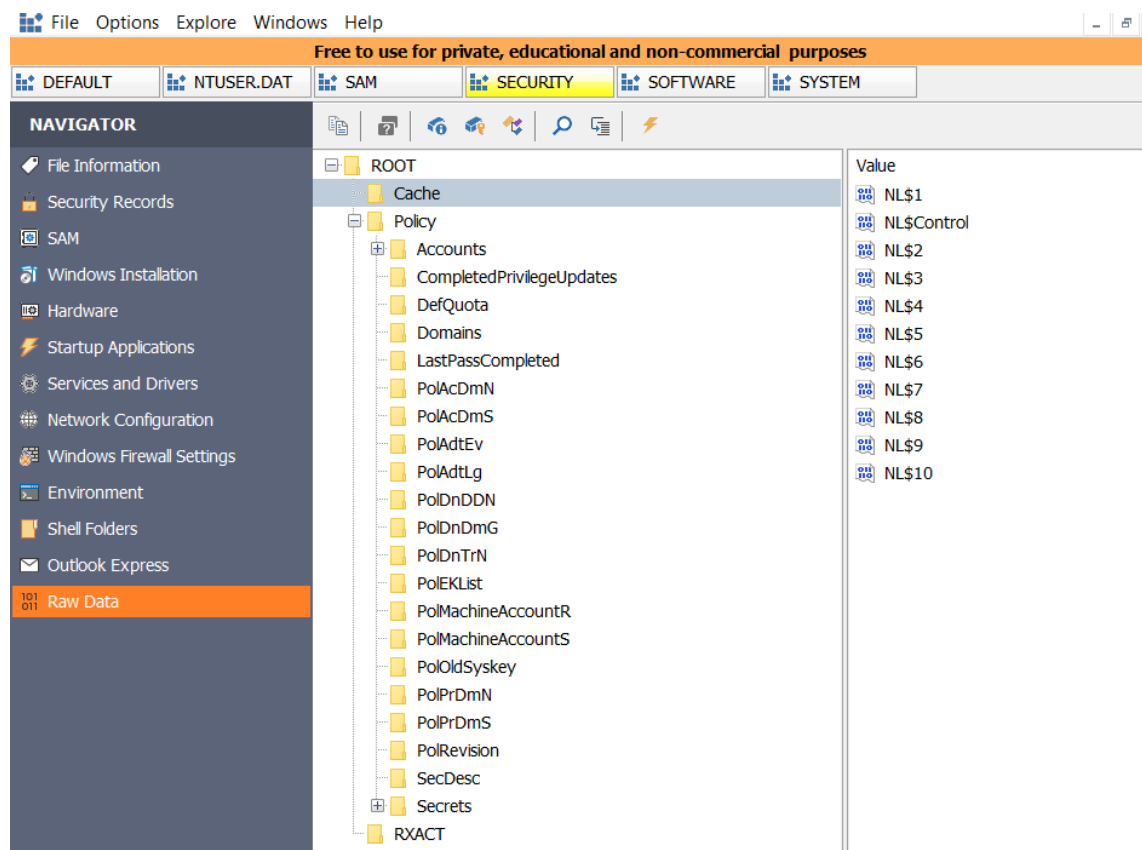


SID es un identificador de seguridad y SYSKEY se utiliza para cifrar la información almacenada en el archivo SAM, incluyendo las contraseñas de los usuarios:



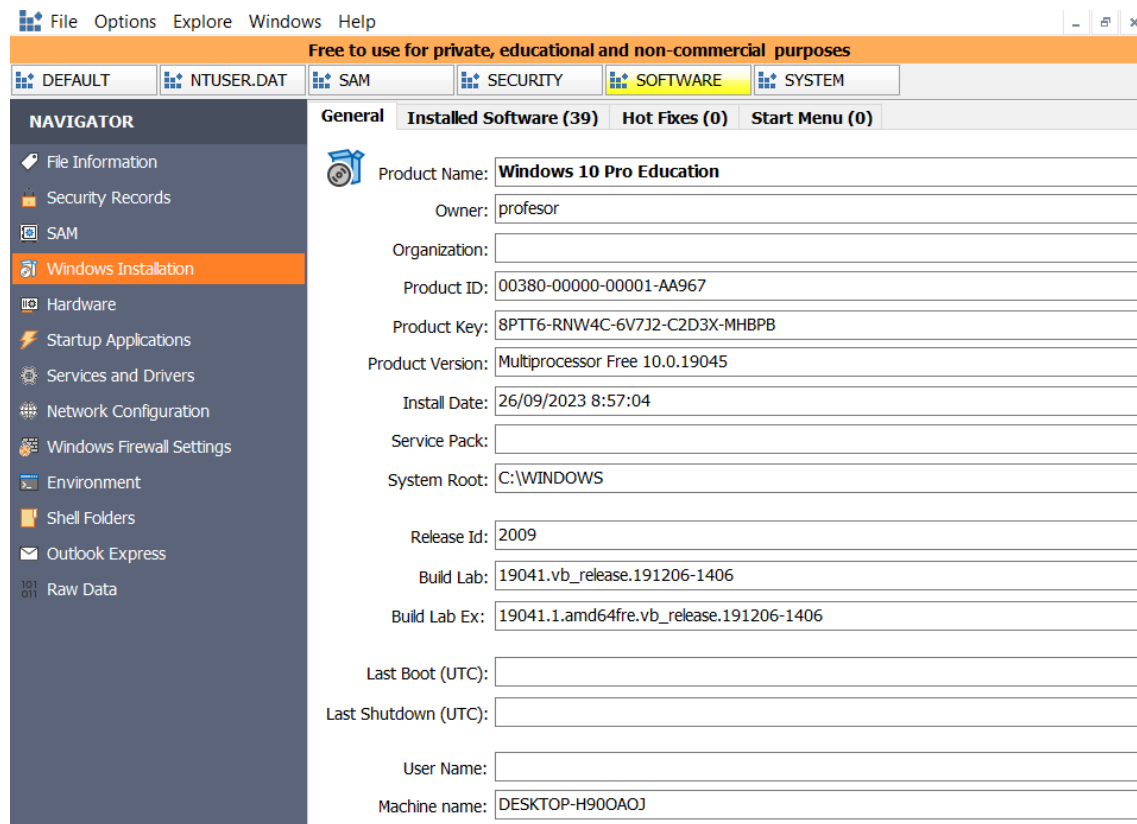
SECURITY

Raw Data.



SOFTWARE.

Nombre del sistema operativo, owner, install date, versión del sistema operativo, id del producto..



The screenshot shows the Windows System Information window. The 'SOFTWARE' tab is selected in the top navigation bar. The 'General' sub-tab is active, displaying various system information fields. The 'NAVIGATOR' pane on the left lists various system categories, with 'Windows Installation' highlighted. The main content area shows the following details:

| Field | Value |
|---------------------|---|
| Product Name | Windows 10 Pro Education |
| Owner | profesor |
| Organization | |
| Product ID | 00380-00000-00001-AA967 |
| Product Key | 8PTT6-RNW4C-6V7J2-C2D3X-MHBPB |
| Product Version | Multiprocessor Free 10.0.19045 |
| Install Date | 26/09/2023 8:57:04 |
| Service Pack | |
| System Root | C:\WINDOWS |
| Release Id | 2009 |
| Build Lab | 19041.vb_release.191206-1406 |
| Build Lab Ex | 19041.1.amd64fre.vb_release.191206-1406 |
| Last Boot (UTC) | |
| Last Shutdown (UTC) | |
| User Name | |
| Machine name | DESKTOP-H90OAOJ |

Software Instalado.

| Free to use for private, educational and non-commercial purposes | | | | | | |
|--|--|-------------------------|------------------|----------------|------------------|--|
| File Options Explore Windows Help | | | | | | |
| DEFAULT NTUSER.DAT SAM SECURITY SOFTWARE SYSTEM | | | | | | |
| NAVIGATOR | General | Installed Software (39) | Hot Fixes (0) | Start Menu (0) | | |
| | Name | Version | Company | Datetime | Uninstall | |
| File Information | AccessData FTK Imager | 4.7.1.2 | AccessData | 20231018 | MsiExec.exe /X{ | |
| Security Records | Autopsy | 4.21.0 | The Sleuth Kit | 20231115 | MsiExec.exe /I{ | |
| SAM | Bulk Extractor 1.6.0-dev | 1.6.0-dev | Naval Postg... | | C:\Program File | |
| Windows Installation | Cisco Packet Tracer 8.2.1 64Bit | 8.2.1.118 | Cisco Syste... | 20231016 | "C:\Program File | |
| Hardware | Explorador de SQL Server 2022 | 16.0.10... | Microsoft C... | 20231107 | MsiExec.exe /X{ | |
| Startup Applications | Git | 2.42.0.2 | The Git Dev... | 20231030 | "C:\Program File | |
| Services and Drivers | Google Chrome | 119.0.6... | Google LLC | 20231120 | "C:\Program File | |
| Network Configuration | HxD Hex Editor 2.5 | 2.5 | Maël Hörz | 20231122 | "C:\Program File | |
| Windows Firewall Settings | Java 8 Update 391 | 8.0.391... | Oracle Corp... | 20231108 | MsiExec.exe /I{ | |
| Environment | Microsoft Edge | 119.0.2... | Microsoft C... | 20231120 | "C:\Program File | |
| Shell Folders | Microsoft Edge Update | 1.3.181.5 | | | | |
| Outlook Express | Microsoft ODBC Driver 17 for SQL Server | 17.4.1.1 | Microsoft C... | 20231107 | MsiExec.exe /I{ | |
| Raw Data | Microsoft Office Profesional Plus 2019 - es... | 16.0.16... | Microsoft C... | | "C:\Program File | |
| | Microsoft OLE DB Driver for SQL Server | 18.2.4.0 | Microsoft C... | 20231107 | "C:\Program File | |
| | Microsoft OneDrive | 23.226... | Microsoft C... | | "C:\Program File | |
| | Microsoft SQL Server 2022 (64 bits) | | Microsoft C... | | "C:\Program File | |
| | Microsoft Update Health Tools | 3.74.0.0 | Microsoft C... | 20231113 | MsiExec.exe /X{ | |
| | Microsoft Visual C++ 2015-2022 Redistrib... | 14.36.3... | Microsoft C... | | "C:\ProgramDal | |
| | Microsoft Visual C++ 2015-2022 Redistrib... | 14.36.3... | Microsoft C... | | "C:\ProgramDal | |
| | Microsoft Visual Studio Installer | 3.7.218... | Microsoft C... | 20231106 | "C:\Program File | |
| | Microsoft VSS Writer para SQL Server 2022 | 16.0.10... | Microsoft C... | 20231107 | MsiExec.exe /I{ | |
| | Notepad++ (64-bit x64) | 8.5.8 | Notepad++... | | "C:\Program File | |
| | Npcap | 1.71 | Nmap Project | | "C:\Program File | |
| | OpenVPN 2.6.6-1001 amd64 | 2.6.601 | OpenVPN, I... | 20231031 | MsiExec.exe /X{ | |
| | Oracle VM VirtualBox 7.0.12 | 7.0.12 | Oracle and/... | 20231031 | MsiExec.exe /I{ | |
| | Programa de instalación de Microsoft SQL ... | 16.0.10... | Microsoft C... | 20231107 | MsiExec.exe /X{ | |
| | PyCharm 2023.2.4 | 232.10... | JetBrains s.r... | | C:\Program Files | |
| | Python Launcher | 3.12.15... | Python Soft... | 20231009 | MsiExec.exe /X{ | |
| | ShareX | 15.0.0 | ShareX Team | 20231009 | "C:\Program File | |
| | Vagrant | 2.3.7 | HashiCorp | 20231009 | MsiExec.exe /X{ | |
| | VirtViewer 11.0-256 (64-bit) | 11.0.256 | Virt Viewer P... | 20231004 | MsiExec.exe /X{ | |
| | Visual Studio Build Tools 2022 | 17.7.6 | Microsoft C... | 20231106 | "C:\Program File | |
| | vs_CoreEditorFonts | 17.7.40... | Microsoft C... | 20231106 | MsiExec.exe /I{ | |
| | WebView2 Runtime de Microsoft Edge | 119.0.2... | Microsoft C... | 20231120 | "C:\Program File | |
| | Windows SDK AddOn | 10.1.0.0 | Microsoft C... | 20231106 | MsiExec.exe /I{ | |
| | Windows Software Development Kit - Win... | 10.1.22... | Microsoft C... | | "C:\ProgramDal | |
| | WinRAR 6.24 (64-bit) | 6.24.0 | win.rar GmbH | | C:\Program Files | |
| | WinSCP 6.1.2 | 6.1.2 | Martin Prikryl | 20231108 | "C:\Program File | |
| | Wireshark 4.0.10 64-bit | 4.0.10 | The Wiresh... | | "C:\Program File | |

También podemos ver las aplicaciones que se inician por defecto al encender el pc.

| Free to use for private, educational and non-commercial purposes | | | |
|--|--|--|----------------------|
| File Options Explore Windows Help | | | |
| DEFAULT NTUSER.DAT SAM SECURITY SOFTWARE SYSTEM | | | |
| NAVIGATOR | Name | Command line | Location |
| File Information | <input type="checkbox"/> SecurityHealth | %windir%\system32\SecurityHealthSystray.exe | Run |
| Security Records | <input type="checkbox"/> RtkAudUService | "C:\WINDOWS\System32\DriverStore\FileRepository\re... | Run |
| SAM | <input type="checkbox"/> IETToEdge BHO | C:\Program Files (x86)\Microsoft\Edge\Application\119.0... | BrowserHelperObjects |
| Windows Installation | <input type="checkbox"/> Skype for Business Bro... | C:\Program Files (x86)\Microsoft Office\root\VFS\Progra... | BrowserHelperObjects |
| Hardware | <input type="checkbox"/> UserInit | explorer.exe | WinLogon |
| Startup Applications | | | |
| Services and Drivers | | | |
| Network Configuration | | | |
| Windows Firewall Settings | | | |
| Environment | | | |
| Shell Folders | | | |
| Outlook Express | | | |
| Raw Data | | | |

SYSTEM

Last Boot y Last Shuwwdown

File Options Explore Windows Help

Free to use for private, educational and non-commercial purposes

DEFAULT NTUSER.DAT SAM SECURITY SOFTWARE **SYSTEM**

NAVIGATOR

- File Information
- Security Records
- SAM
- Windows Installation**
- Hardware
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express
- Raw Data

General Installed Software (0) Hot Fixes (0) Start Menu (0)

Product Name:

Owner:

Organization:

Product ID:

Product Key:

Product Version:

Install Date:

Service Pack:

System Root:

Release Id:

Build Lab: 19041.vb_release.191206-1406

Build Lab Ex: 19041.1.amd64fre.vb_release.191206-1406

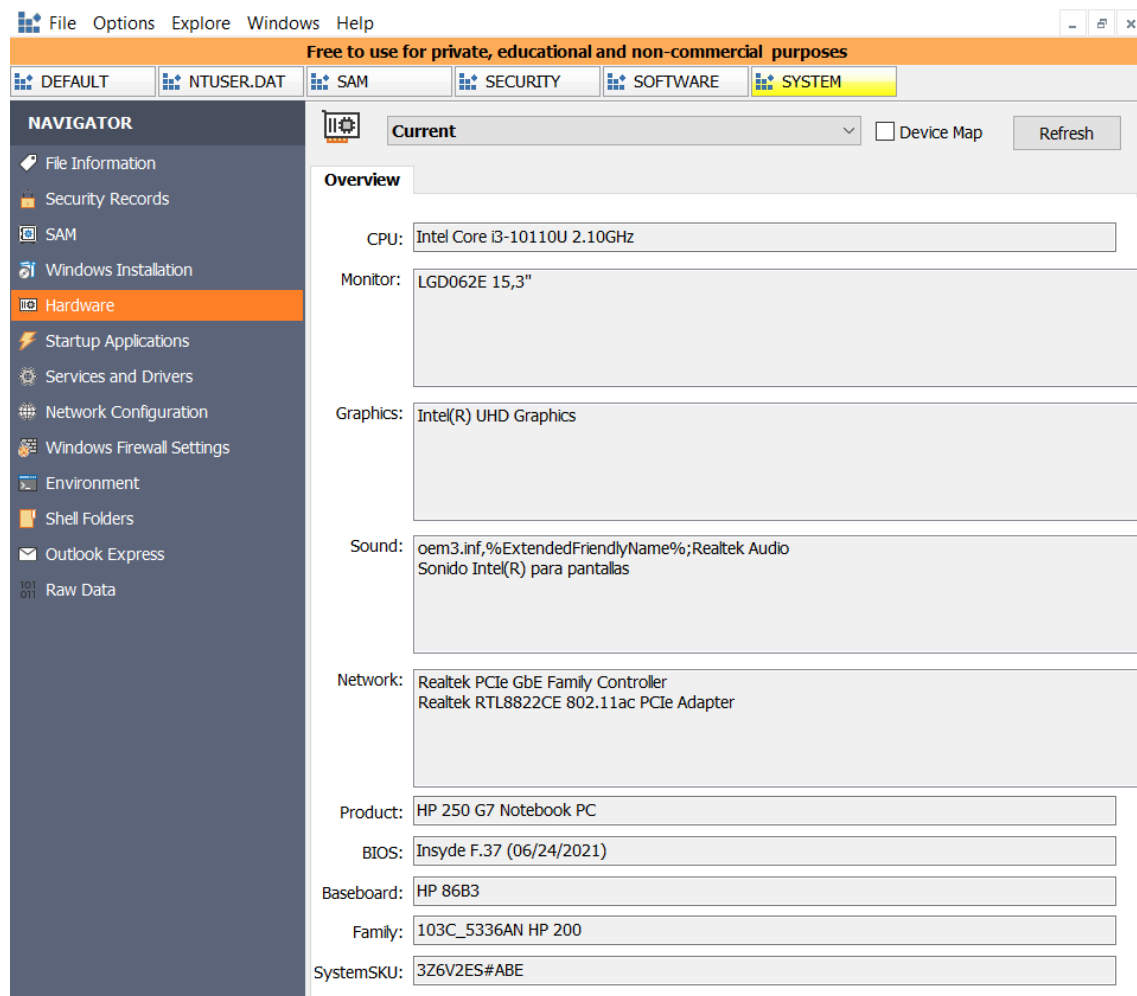
Last Boot (UTC): 22/11/2023 19:00:20

Last Shutdown (UTC): 22/11/2023 19:03:03

User Name:

Machine name: DESKTOP-H900AOJ

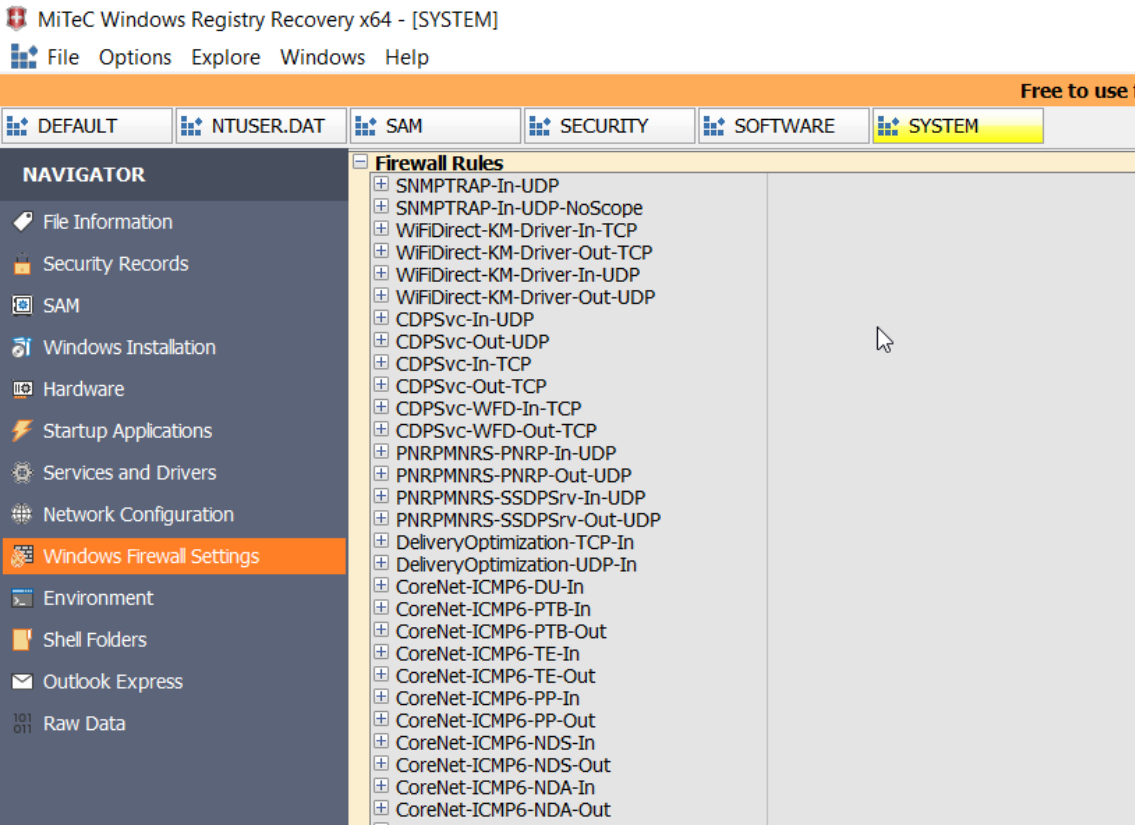
Hardware del equipo:



Drivers y servicios:

[illegible]

Configuración de Windows Firewall:



2. Mediante regripper consiga la siguiente información de su sistema:

➤ Zona horaria del equipo

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.3693]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p timezone
Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2023-10-30 14:57:03Z
DaylightName -> @tzres.dll,-301
StandardName -> @tzres.dll,-302
Bias -> -60 (-1 hours)
ActiveTimeBias -> -60 (-1 hours)
TimeZoneKeyName-> Romance Standard Time

C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>
```

➤ Última vez que se ha apagado el sistema operativo

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p shutdown
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2023-11-22 19:03:03Z
ShutdownTime : 2023-11-22 19:03:03Z

C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>
```

➤ ¿Qué IP tiene?

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p ips
Launching ips v.20200518
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress          Domain
172.22.241.172      Hint: gubia
172.22.251.90       Hint:
192.168.56.1
10.10.14.182        Hint:
```

➤ Qué arquitectura tiene su equipo (x64, x86, AMD64, ...)

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p processor_architecture
Launching processor_architecture v.20140505
processor_architecture v.20140505
(System) Get from the processor architecture from the System's environment key

PROCESSOR_ARCHITECTURE = AMD64
PROCESSOR_IDENTIFIER = Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
PROCESSOR_REVISION = 8e0c

C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>
```

➤ Nombre del equipo físico y en red

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master\plugins\hostname.pl not found.
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName      = DESKTOP-H900A0J
TCP/IP Hostname    = DESKTOP-H900A0J
```

➤ Versión de su sistema operativo, fecha y hora de su instalación

```
Software\Microsoft\Windows\CurrentVersion\ApplicationAssociationToasts not found.
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

Microsoft\Windows NT\CurrentVersion not found.
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>
```

No me aparece, así que voy a poner este comando, aunque sea de SOFTWARE.

```
Microsoft\Windows NT\CurrentVersion not found.
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName        Windows 10 Pro Education
ReleaseID           2009
BuildLab            19041.vb_release.191206-1406
BuildLabEx          19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID Enterprise
RegisteredOwner    profesor
UBR                 3693
InstallDate         2023-09-26 08:57:04Z
InstallTime         2023-09-26 08:57:04Z
UBR                 3693
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>
```

➤ ¿Cuál es el último usuario logueado?

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SOFTWARE -p lastloggedon
Launching lastloggedon v.20200517
lastloggedon v.20200517
(Software) Gets LastLoggedOn* values from LogonUI key

LastLoggedOn
Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastWrite: 2023-11-22 19:04:20Z

LastLoggedOnUser    = .\alumno
LastLoggedOnSAMUser = .\alumno
LastLoggedOnUserSID = S-1-5-21-3962272431-3513200799-749087814-1002
```

➤ ¿Qué sistema operativo utiliza?

```

Microsoft Windows [! (current version not found.)]
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName                Windows 10 Pro Education
ReleaseID                  2009
BuildLab                   19041.vb_release.191206-1406
BuildLabEx                 19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID       Enterprise
RegisteredOwner            profesor
UBR                        3693
InstallDate                2023-09-26 08:57:04Z
InstallTime                2023-09-26 08:57:04Z
UBR                        3693

C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>

```

➤ ¿Qué versión de java python utiliza?

```

C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master\plugins\install.pl not found.
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SOFTWARE -p installer
Launching installer v.20200517
Launching installer v.20200517
(Software) Determines product install information

Installer
Microsoft\Windows\CurrentVersion\Installer\UserData

User SID: S-1-5-18
Key       : 00006109C80000000000000000F01FEC
LastWrite: 2023-11-20 15:07:07Z
20231108 - Office 16 Click-to-Run Extensibility Component 16.0.16924.20124 (Microsoft Corporation)

Key       : E776FAE68EE422A4791819135C92D862
LastWrite: 2023-10-30 15:34:08Z
20231009 - Python 3.12.0 Tcl/Tk Support (64-bit) 3.12.150.0 (Python Software Foundation)

```

➤ Añada la información de 2 plugins más que considere interesantes

Ejecución de archivos: **appcompattcache**

```

LastLoggedOnUserSID = S-1-5-21-3962272431-3513200799-749887814-1002
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r SYSTEM -p appcompattcache
Launching appcompattcache v.20220921
appcompattcache v.20220921
(System) Parse files from System hive AppCompatCache

ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: 2023-11-22 19:03:03Z
Signature: 0x34
00000009 000f00690c880000 000a000047ba0000 8664 Microsoft.SkypeApp kzf8qxf38zg5c
00000009 07e72b5c2afa0000 000a0000585d0000 8664 Microsoft.Windows.Photos 8wekyb3d8bbwe
C:\Users\alumno\AppData\Local\Temp\{2113E6F-C0C2-4042-8502-A4D5CBA1C02E}\cr\VC_redist.arm64.exe 2023-11-06 18:43:11
C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{EDFB724B-579E-4515-B5A8-C9E3A3CB71E5}\MicrosoftEdge_X64_117.0.2045.60_117.0.2045.47.exe 2023-10-09 14:00:53
C:\Program Files\Microsoft OneDrive\23.199.0924.0001\OneDriveUpdaterService.exe 2023-10-16 13:57:46
C:\WINDOWS\system32\ARP.EXE 2019-12-07 09:09:34
C:\WINDOWS\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_642dd10f697d62b0\X64\HPDCSetup.exe 2023-09-25 02:33:21
0000000b 002c4a6101a70000 000a000047ba0000 8664 Microsoft.MicrosoftEdge 8wekyb3d8bbwe
C:\WINDOWS\System32\DriverStore\FileRepository\dal.inf_amd64_0b214be229a13e84\jhi_service.exe 2020-04-27 01:08:58
C:\Program Files\Wireshark\dumpcap.exe 2023-10-04 23:02:18
0000000b 4a61004400e30000 000a00004a610df2 8664 Microsoft.LanguageExperiencePackes-ES 8wekyb3d8bbwe
C:\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_2.38.28001.0_x64_8wekyb3d8bbwe\Application 2023-10-02 14:42:28
C:\Users\alumno\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe 2023-10-03 17:36:53
C:\WINDOWS\system32\ApplicationFrameHost.exe 2022-10-16 19:00:15
00000009 000b08ff00050000 000a000055f00000 8664 Microsoft.WindowsMaps 8wekyb3d8bbwe
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Ngen.exe 2022-08-29 18:44:28
C:\WINDOWS\System32\wehsvc.exe 2019-12-07 09:09:47

```

RECENTDOCS (NTUSER.DAT)

He probado recentocs aunque sea de ntuser.dat porque me intrigaba.

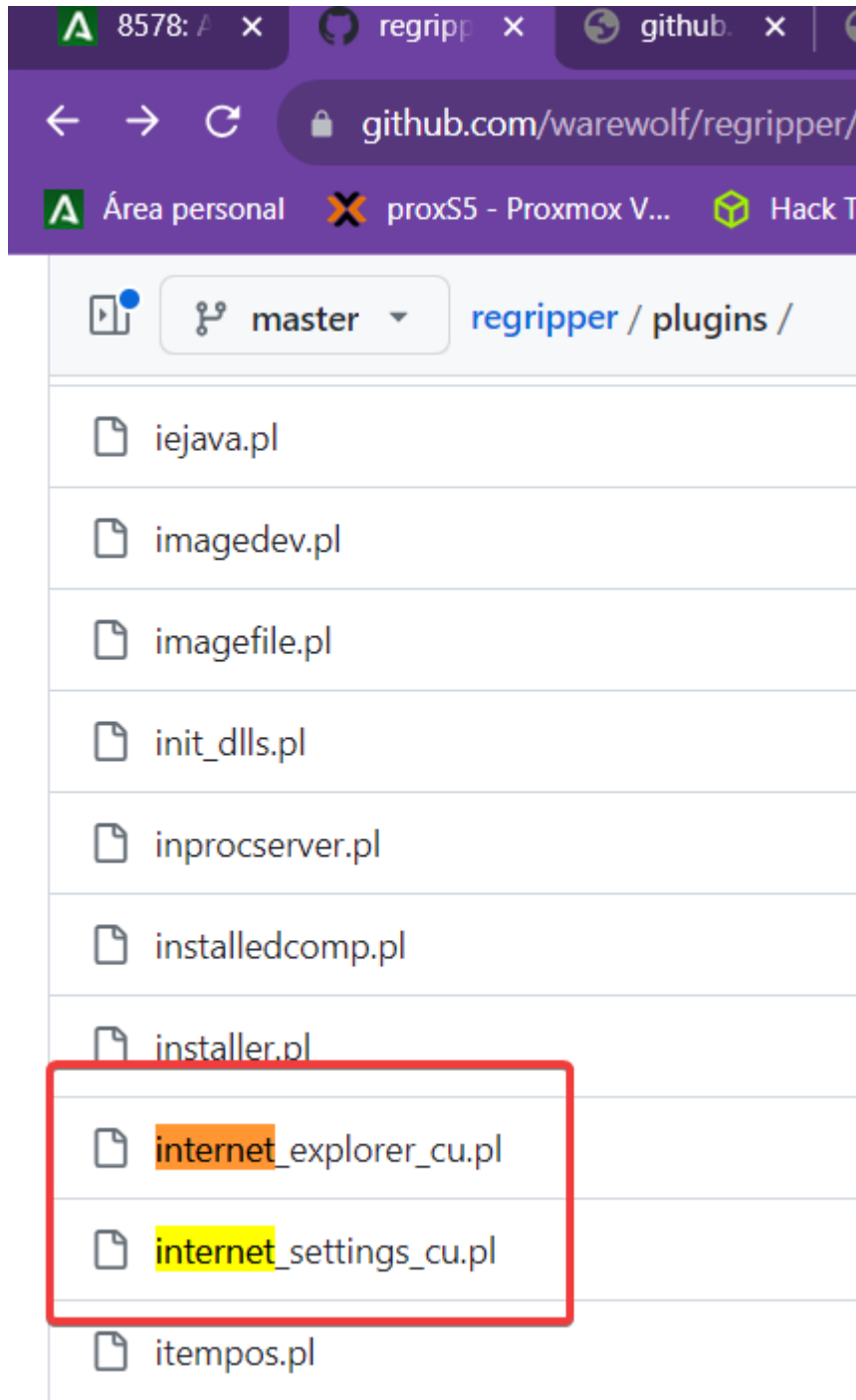
```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r NTUSER.DAT -p recentdocs
Launching recentdocs v.20200427
recentdocs v.20200427
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2023-11-22 18:46:49Z
82 = dsadsadsadsadsa.docx
30 = Reto recuperaci|n de archivos.docx
141 = Reto recuperaci|n de archivos_EricSerranoMar|n.pdf
10 = Archivo2.xlsx
140 = prueba.xlsx
139 = Archivos a recuperar
66 = Libro1.xlsx
59 = Downloads
84 = Archivo2.docx
137 = sjklahdkjsadas.xml
135 = Archivo2.xml
138 = lsjals.xml
136 = Archivo22.not
0 = Downloads
134 = Archivo1.png
132 = Archivo1.jpg
133 = Archivo1.not
25 = Pr|ctica Pareja 1.4 Auditor|ja del plan de prevenci|n y concienciaci|n - Hojas de c|ilculo de Google.pdf
4 = Descargas
131 = Pr|ctica Pareja 1.4 Auditor|ja del plan de prevenci|n y concienciaci|n.xlsx
85 = Pr|ctica Pareja 1.1 Plan de concienciaci|n_EricSerranoMar|n.pdf-20231122T151144Z-001
19 = Pr|ctica Pareja 1.1 Plan de concienciaci|n_EricSerranoMar|n.pdf
5 = drive-download-20231121T173336Z-001
7 = Tr|ptico Contrase|as Seguras.pdf
129 = Presentaci|n.pdf
130 = Poster2 Phishing.pdf
```

- **Busque en Internet nuevos plugins para RegRipper, descárguelos y pruebe al menos 2 de estos plugins.**

Voy a usar estos:

Solo hay que descargarlos y los metemos en la carpeta de plugins.



Internet_explorar_cu

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r NTUSER.DAT -p internet_explorer_cu
Launching internet_explorer_cu v.20120528
internet_explorer_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Explorer

Software\Microsoft\Internet Explorer
LastWrite Time Thu Oct 5 16:15:28 2023 (UTC)
  Download Directory = ''

Software\Microsoft\Internet Explorer\AutoComplete not found.
Software\Microsoft\Internet Explorer\AutoComplete not found.

Software\Microsoft\Internet Explorer\DOMStorage not found.
Software\Microsoft\Internet Explorer\DOMStorage not found.

Software\Microsoft\Internet Explorer\IETld
LastWrite Time Tue Sep 26 09:15:36 2023 (UTC)
  Internet Explorer version = 0.0.0.0

Software\Microsoft\Internet Explorer\Main
LastWrite Time Tue Oct 31 15:13:41 2023 (UTC)
Use of uninitialized value $list in pattern match (m//) at PERL2EXE_STORAGE/utf8_heavy.pl line 399.
  Anchor Underline           = yes
  Cache_Update_Frequency     = yes
  Disable_Script_Debugger     = yes
  DisableFirstRunCustomize    = 1
  DisableScriptDebuggerIE     = yes
  Display_Inline_Images       = yes
  Do404Search                 = 1 [0x01000000]
  Enable_Browser_Extensions   = yes
  ImageStoreRandomFolder      = 2ju4yz6
  Local_Page                  = %11%\blank.htm
  Play_Animations              = yes
  Play_Background_Sounds      = yes
  Save_Session_History_On_Exit = no
  Search_Page                  = http://go.microsoft.com/fwlink/?LinkId=54896
  Show_FullURL                 = no
  Show_StatusBar               = yes
  Show_ToolBar                 = yes
```

Internet_setting_cu

```
C:\Users\alumno\Desktop\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r NTUSER.DAT -p internet_settings_cu
Launching internet_settings_cu v.20120528
internet_settings_cu v.20120528
(NTUSER.DAT) Get HKCU information on Internet Settings

Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Wed Nov 22 19:04:28 2023 (UTC)
Use of uninitialized value $list in pattern match (m//) at PERL2EXE_STORAGE/utf8_heavy.pl line 399.
  CertificateRevocation      = true [1]
  DisableCachingOfSSLPages   = false [0]
  EnableNegotiate             = true [1]
  IE5_UA_Backup_Flag         = 5.0
  LockDatabase                = |áPV|é|Ü
  MigrateProxy                = true [1]
  PrivacyAdvanced             = true [1]
  ProxyEnable                 = false [0]
```

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012023103020231106
LastWrite Time Mon Nov 6 15:01:19 2023 (UTC)
CacheLimit           = 1 KB
CacheOptions         = 0xB
CachePath            = C:\Users\alumno\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012023103020231106
CachePrefix          = :2023103020231106:
CacheRelativePath    = Microsoft\Windows\History\History.IE5\MSHist012023103020231106
CacheRepair          = 0x0

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012023110620231113
LastWrite Time Mon Nov 13 15:01:15 2023 (UTC)
CacheLimit           = 1 KB
CacheOptions         = 0xB
CachePath            = C:\Users\alumno\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012023110620231113
CachePrefix          = :2023110620231113:
CacheRelativePath    = Microsoft\Windows\History\History.IE5\MSHist012023110620231113
CacheRepair          = 0x0

Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012023111320231120
LastWrite Time Mon Nov 20 15:05:08 2023 (UTC)
CacheLimit           = 1 KB
CacheOptions         = 0xB
CachePath            = C:\Users\alumno\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012023111320231120
CachePrefix          = :2023111320231120:
CacheRelativePath    = Microsoft\Windows\History\History.IE5\MSHist012023111320231120
CacheRepair          = 0x0
```