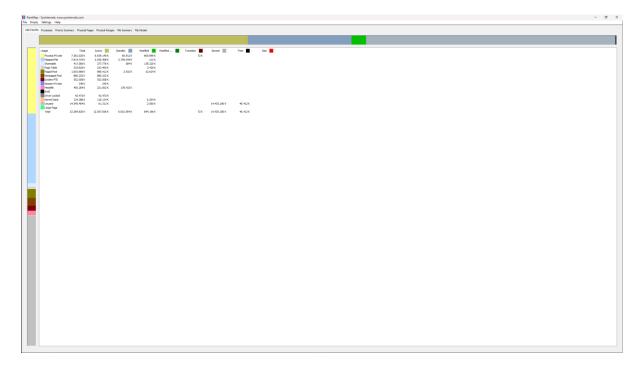
Atividade 3:

RAMMAP, como o próprio nome sugere é uma ferramenta que analisa o sistema, mais especificamente na área da memória e como o Windows organiza os processos baseado na memória física.



Atividade 4:

O Autoruns tem como objetivo mostrar quais programas estão configurados para serem executados durante a inicialização ou logon do sistema e quando você inicia vários aplicativos internos do Windows.

Everything 🚨 Logon 🔚 Explorer 🙋 Internet Explorer	Scheduled Tasks Q Services			🤌 Winlogon 📙 Win		rint Monitors 😽 LSA Providers	Network Providers 😬 VIMI	(OH
Logon HICU/SOFTWARE/Microsoft/Windows/CurrentVersion/Run				Sat Nov 9 14 14:58 2024				
HILLUISCH IWAKE Witchesoff (Windows) Lurrent Version (Kun	CCleaner	(Verified) Gen Digital Inc.	C\Program Files\CCleaner\CCleaneri4.ese	Toe Oct 15 11:03:10 2024				
■ © LACM	EA	(Verified) Electronic Arts, Inc.	C:\Program Files\Electronic Arts\EA Desktop\EA Desktop\EALauncher.e					
EpicGamesLauncher	EpicGamesLauncher		C/\Program Files (x86)\Epic Games\Launcher\Portaf\Binaries\Win64\Ep					
		(Verified) Microsoft Corporation	C/\Program Files (x86)\Microsoft\Edge\Application\vnsedge.exe					
© ← OneOrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\User\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Mon Nov 11 15:38:16:20				
Opera GX Browser Assistant Opera GX Stable	Opera GX Browser Assistant Opera GX Interpet Browser	(Verified) Opera Software AS (Verified) Opera Norway AS	Chibers\User\AppData\Local\Programs\Opera Gh\assistant\browser_a Chiber\User\AppData\Local\Programs\Opera Gh\opera.exe	Mon Feb 1 13:18:20:202 Thu Nov. 7 13:50:59:203				
S Special Chart	Riot Client	(Verified) Riot Gernes, Inc.	CAffet Same Affet Client Rict Client Services are	Thu Nov 7 21:19:52 2024				
Steam Steam		(Verified) Valve Corp.	C/\Program Files (x86)\Steam\steam.exe					
HKLMI.SOFTWARE\Microsoft@indows\CurrentVersion\Run				Tue Oct 29 13:01:43 2024				
■ B Edagent ■ Ø BdfgnApp	Bitdefender agent	(Verified) Bitdefender SRL (Verified) Bitdefender SRL	C/\Program Files\Bitdefender\Bitdefender Security Applibdagent.exe	Tue Oct 29 12:22:55 2024 Fri Oct 4 13:01:51 2024				
DidipnApp Ocusir iCUIS Software	Bitdefender Vpn App ICUE	(Verthed) Endefender SRL (Verthed) Corsair Memory, Inc.	C:\Program Files\Bitdefender\Bitdefender\PM\Bd/pn\lgp.exe C\Program Files\Corsain\Corsair\Cut5 Softwareh\Cut Launches.exe	Tue Oct 29 12/59/31 2024				
First Vanguard	Vanguard tray notification	(Verified) Riot Games, Inc.	C:\Program Files\Riot Venguerd\u00fcvgtray.exe	Thu Oct 24 29:18:26 2024				
₹ TakAudUService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor	C:\WWNDOWS\Syntem32\DriverStore\FileRepository\realhekservice.inf_a					
				Set May 7/02/25/14 2022				
■ T cmd exe	Processador de comandos do Windows	(Verified) Microsoft Windows	C/\WINDOWS\system32\cmd.exe	Thu Oct 24 19:12:34 2024				
HKLM/SOFTWARE\Alicrosoff\Active Setup\Installed Components Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\130.0.6723.117\Installer_	Set Oct 26 21:40:41 2024 Thu New 7:31:20:44 2024				
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C\Program Files (x80)\Microsoft\Edge\Application\130.02849.80\instal					
■ D n/a	Microsoft .NET IE SECURITY REGISTRATION							
HK1M;SOFTWARE\Wow6432Node\Microsoft\Windows\CumentVersion	Run			Thu Sep 12 12:03:20 2024	•			
Adobe CCXProcess Adobe Creative Cloud	CCXProcess	(Verified) Adobe Inc.	C/\Program Files (\n00)\Adobe\Adobe Creative Cloud Experience\CCIPr	Thu May 2 00:56:14 202				
Adobe Creative Cloud SuniavaUpdateSched	Creative Cloud Java Update Scheduler	(Verified) Adobe Inc. (Verified) Oracle America, Inc.	CAProgram Files Adobet Adobe Creative Cloud ACC Creative Cloud exe CAProgram Files (x86)/Common Files Uswal Java Updatel jusched.ese					
HKI MISOFTWARE\Wisew6432Node\Microsoft\Active Setup\installed Co	moonents	(ventes) Oracle America, inc.	C. (Program Plate (100) Common Plate Gard Sales Gardinesses	Sat Oct 26 21:40:41 2024				
■ D n/a	Microsoft NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C/\Windows\System32\mscories.dll	Set May 7 (2:20:30 2022				
HKCU/Software/Classes\"\ShellEx\ContextMerxuHandlers				Mon Nov 11 15:38:24 202				
● Filefynctx HKCU/Software\Classes\Directory\ShellEr\ContextMers\Handles	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	Chilbert User AppData Local Microsoft One Drivet 24.211.1020.0001 Url.	Mon Nov 11 15:38:13:23 Mon Nov 11 15:38:24:20				
- FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\User\User\AppData\Local\Microsoft\OneDrive\24.211.1020.0001/Fit					
HKCU/Software\Classes\Directory\Background\Shellis\ContextMenuH	endlers			Mon Nov 11 15:38:24:25				
■ FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	Children Libert App Data Local Microsoft One Drivet 24.211.1020.000 T.F.L.					
HKLM/Software\Classes*\ShellEx\ContextMersuHandlers 017-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C/Program Files/7-Zip/7-sip.dll	Tue Oct 29 12:26:37 2024 Tue Am 20 05:00:00 2023				
■ M Accht	Core Sunc	(Not verned) igor Paviov (NetFied) Adobe Inc.	C\Program Files (x80)/Common Files\Adobe\CoreSyncSitension\Core					
■ TWeRAR	WinRAR shell extension	(Verified) win.rar GmbH	C//Program Files/WinRAR/rarext.dll	Tue Aug 109/26/37 2021				
🗷 🗓 Bdihlfat	EdShellEstensions Module	(Verified) Bittdefender SRL	C:\Program Files\Bitdefender\Bitdefender Security App\bdshallest.dll					
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				Tue Oct 29 12:26:37 2024				
BdSMSt	BdShellExtensions Module	(Verified) Bitdefender SRL	C\Program File\Bitdefende\Bitdefender Security App\bdshellest.dll	Wed Feb 21 09:38:18 202 Tue Oct 29 12:26:37 2024				
■ DB 7-Ze	7-Zip Shell Extension	(Not Verified) loor Paylov	CAProgram Filet 7-Zig17-do.dtl	Tue Ain 20 05:00:00 2023				
S Belletie	EdShellExtensions Module	(Verified) Bitdefender SRL		Wed Feb 21 09:38:18:202				
HKLM\Software\Classes\Directory\ShellEx\DragDrogHandless				Sun Oct 122:22:17:2023				
2 03 7-Zφ	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zig\7-sip.dll	Tue Am 20 05:00:00 2023				
HKLM:Software\Classes\Directory\Background\ShellDr\ContextMenuli NiColDesktooContext	NVIDIA Display Shell Extension	(Verified) NV/DIA Corporation	C\WINDOWS\Sixtem32\DriverStore\FieRepositors\nvmd.inf amdif4	Tue Oct 29 12:26:37 2024 Sat Sep 28 18:02:02 2024				
■ NvCpDestopContext ■ BdShEst	RVIDIA Display Shell Extension BdShellExtensions Module	(Verified) NVIDIA Corporation (Verified) Bitdefender SRL	C:\WinDOWS\Gystems2\Dinverstore\netkepository\numdurf_amdb4 C:\Program Files\Bitdefender\Bitdefender\Security\Applibdshellert.dll					
HOLM/Software/Classes/Folder/Shellfs/ContextMenuHandlers		(vernes) superender and	C. Program real succession in success of programme and a	Tue Oct 29 12:26:37 2024				
2	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C/\Program Files\7-Zip\7-sip.dll	Tue Jun 20 05:00:00 2023				
AccEnt								
■ ∰WinBAR ■ BdShEat	WinRAR shell extension EdShellEstensions Module	(Verified) win.zer GmbH (Verified) Bibbefender SRI,	C:\Program Files\WinRAR:sarest.dll C:\Program Files\Biddefender\Bibdefender Security Applibidshellest.dll	Tue Aug 106:26:37:2021 Wed Feb 21 09:38:18:202				
HELLAN, Self-worst, Classes), Folder', ShellEv', Draw Drook Handlers	Edonesistensions module	(verned) sindefender sixs.	Charlogram Historia de ender o monte ender security appropriete data	Sun Oct 1 23/03/58 2021	04			
WindAR	WinRAR shell extension	(Verified) winzer GmbH	C:\Program File\WinRAR\sarext.dll	Tue Aug 1 06:26:37 2021	3			
HKLM/Software/Classes\Folder/ShellEx\ColumnHandlers				Sun Oct 122:22:17:2023				
LibreOffice Column Handler								
HKLM\Software\Microsoft\Windows\CumentVersion\Explorer\Shellicon								