Aluno : Lucas do Carmo Braz RA: 12418293

Atividade 1-A

Atividade 1-A - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

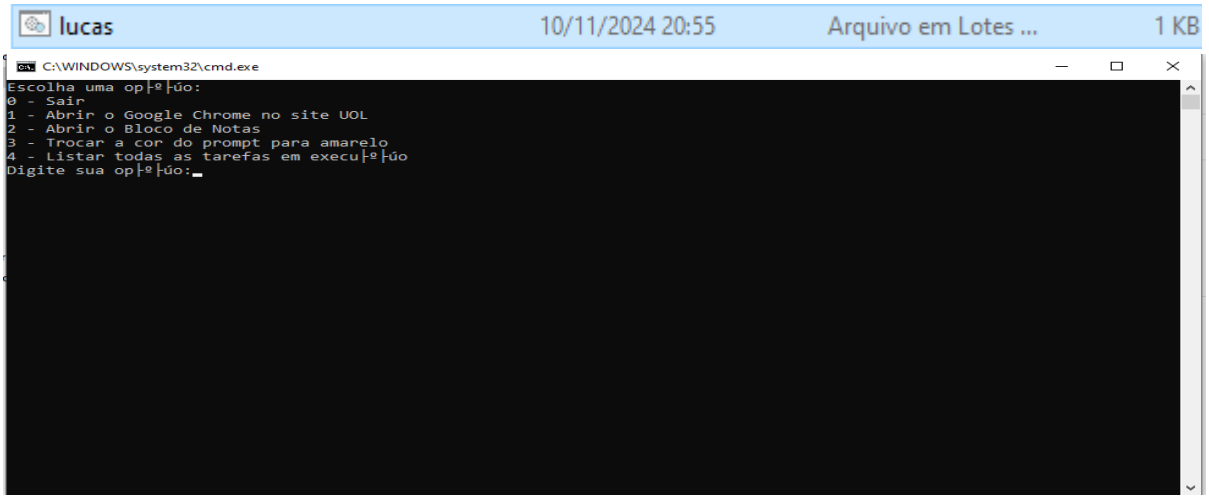
```
1-A
@echo off                    :: Desativa a exibição dos comandos enquanto são executados
cls                          :: Limpa a tela do prompt de comando
:menu                        :: Define o rótulo "menu" para criar um ponto de retorno
cls                          :: Limpa a tela novamente
color 2                      :: Define a cor do texto do prompt como verde

echo           Programando como um raiz!!!        :: Exibe uma mensagem no prompt
echo ==========================================  :: Exibe uma linha de separação para o menu
echo "*1 - Mostre os arquivos que está na pasta*"  :: Exibe a opção 1 do menu
echo "*2 - Mostre as informações do sistema onde estou*" :: Exibe a opção 2 do menu
echo "*3 - Sair*"                                :: Exibe a opção 3 do menu
echo ==========================================  :: Exibe outra linha de separação

set /p opcao= Escolha uma opcao:                 :: Solicita ao usuário que escolha uma opção e armazena o valor na variável "opcao"
echo --------------------------------            :: Exibe uma linha de separação
if %opcao% equ 1 goto opcao1                     :: Se a opção for 1, redireciona para o rótulo ":opcao1"
if %opcao% equ 2 goto opcao2                     :: Se a opção for 2, redireciona para o rótulo ":opcao2"
if %opcao% equ 3 goto opcao3                     :: Se a opção for 3, redireciona para o rótulo ":opcao3"
if %opcao% GEQ 4 goto opcao4                     :: Se a opção for maior ou igual a 4, redireciona para o rótulo ":opcao4"

:opcao1                                         :: Define o rótulo ":opcao1"
cls                                             :: Limpa a tela
dir                                             :: Lista os arquivos e pastas do diretório atual
echo -----------                                 :: Exibe uma linha de separação
echo "*arquivos lidos*"                         :: Exibe uma mensagem de confirmação
echo -----------                                 :: Exibe uma linha de separação
pause                                           :: Pausa a execução até o usuário pressionar uma tecla
goto menu                                       :: Retorna ao menu principal

:opcao2                                         :: Define o rótulo ":opcao2"
cls                                             :: Limpa a tela
dir                                             :: Lista os arquivos e pastas do diretório atual novamente
echo -----------                                 :: Exibe uma linha de separação
echo "*este é se sistema*"                      :: Exibe uma mensagem de confirmação
echo -----------                                 :: Exibe uma linha de separação
pause                                           :: Pausa a execução até o usuário pressionar uma tecla
goto menu                                       :: Retorna ao menu principal

:opcao3                                         :: Define o rótulo ":opcao3"
cls                                             :: Limpa a tela
exit                                            :: Sai do script e retorna ao prompt de comando

:opcao4                                         :: Define o rótulo ":opcao4"
cls                                             :: Limpa a tela
echo "*Opção Inválida*"                         :: Exibe uma mensagem de erro
echo "*Opção Inválida*"                         :: Exibe a mensagem novamente
pause                                           :: Pausa a execução até o usuário pressionar uma tecla
goto menu                                       :: Retorna ao menu principal
```

Atividade 1-B

lucas - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

```
@echo off
cls
:menu
cls
echo Escolha uma opção:
echo 0 - Sair
echo 1 - Abrir o Google Chrome no site UOL
echo 2 - Abrir o Bloco de Notas
echo 3 - Trocar a cor do prompt para amarelo
echo 4 - Listar todas as tarefas em execução
set /p opcao=Digite sua opção:

if %opcao% equ 0 goto sair
if %opcao% equ 1 goto abrirChrome
if %opcao% equ 2 goto abrirBlocoDeNotas
if %opcao% equ 3 goto trocarCor
if %opcao% equ 4 goto listarTarefas
goto opcaoInvalida

:sair
cls
exit

:abrirChrome
start chrome https://www.uol.com.br
goto menu

:abrirBlocoDeNotas
start notepad
goto menu

:trocarCor
color 6
goto menu

:listarTarefas
tasklist
pause
goto menu

:opcaoInvalida
echo Opção Inválida
pause
goto menu
```



Atividade 2- A

Nome do Log: **System**

Fonte: **Microsoft-Windows-Kernel-Power**

Data: **25/08/2020 20:26:44**

Identificação do Evento: **41**

Categoria da Tarefa: **(63)**

Nível: **Crítico**

Palavras-chave: **(70368744177664),(2)**

Usuário: **SISTEMA**

Computador: **DESKTOP-RS2L8OU**

Descrição:

O sistema foi reiniciado sem um desligamento correto primeiro. Esse erro pode ser causado quando o sistema para de responder, trava ou fica sem energia inesperadamente.

Atividade 2-B

Nome do Log: System
Fonte: Microsoft-Windows-UserModePowerService
Data: 16/11/2017 19:26:45
Identificação do Evento: 12
Nível: Informações
Usuário: SISTEMA

Computador: HOME
Processo: C:\Program Files\AVAST Software\Avast\AvastSvc.exe

Atividade 2-C

Tipo de Evento: Error
Mensagem de Erro: Não foi possível abrir o objeto de desempenho do serviço do Servidor. Os primeiros quatro bytes (DWORD) da seção de dados contêm o código do status.
Detalhes Adicionais:

Nome do Log: Application
Fonte: Microsoft-Windows-PerfNet
Data: 10/11/2024 19:57:21
Identificação do Evento:2004
Categoria da Tarefa:Nenhum
Nível: Erro
Palavras-chave:
Usuário: DESKTOP-8OAVM52\lucas
Computador: DESKTOP-8OAVM52
Descrição:
Não foi possível abrir o objeto de desempenho do serviço do Servidor. Os primeiros quatro bytes (DWORD) da seção de dados contém o código do status.
XML de Evento:

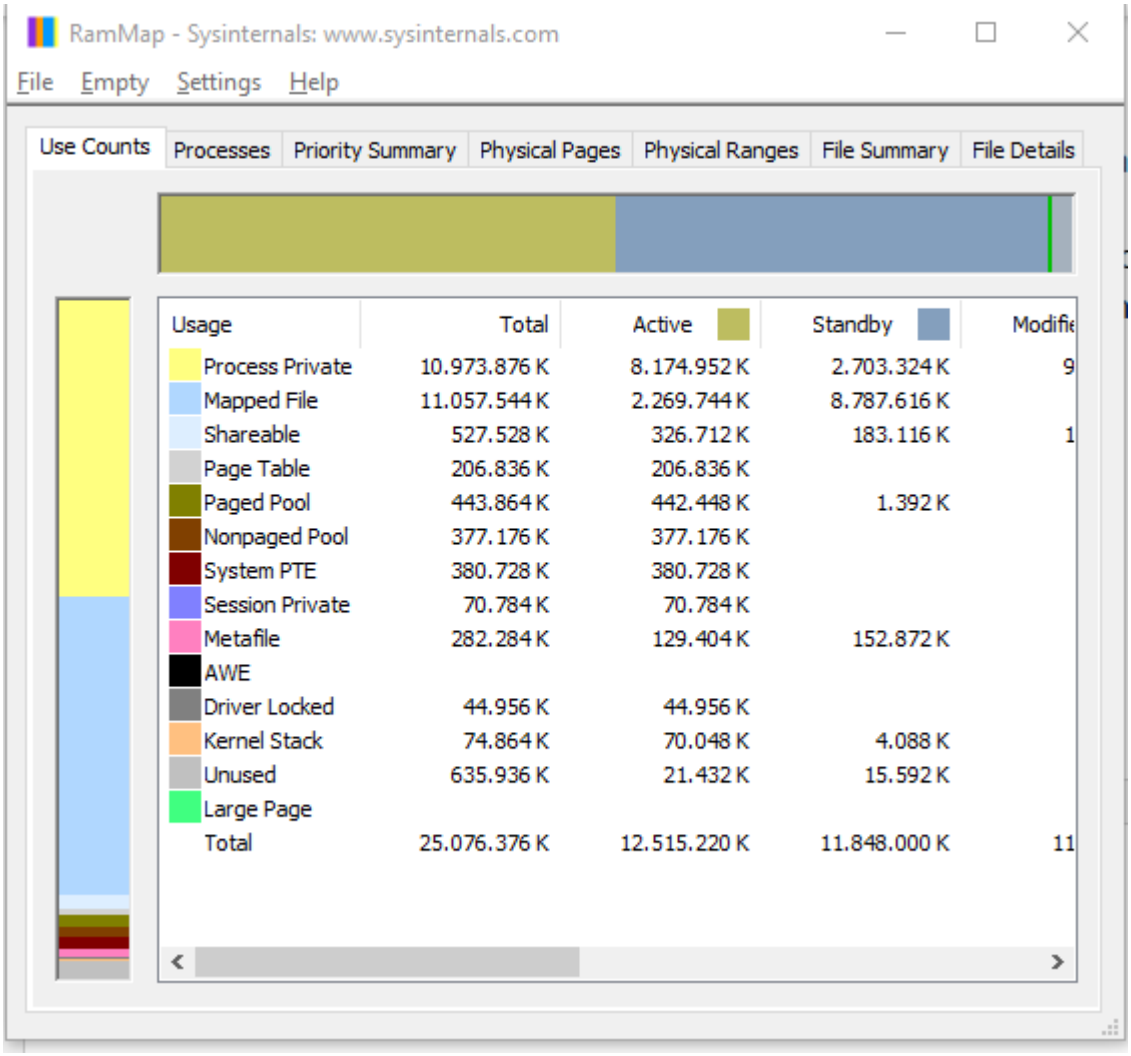
```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
 <System>
  <Provider Name="Microsoft-Windows-PerfNet" Guid="{cab2b8a5-49b9-4eec-b1b0-fac21da05a3b}" />
  <EventID>2004</EventID>
  <Version>1</Version>
  <Level>2</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2024-11-10T22:57:21.6282661Z" />
  <EventRecordID>19856</EventRecordID>
  <Correlation />
  <Execution ProcessID="14532" ThreadID="16856" />
  <Channel>Application</Channel>
  <Computer>DESKTOP-8OAVM52</Computer>
  <Security UserID="S-1-5-21-595621832-1785238944-2711119992-1001" />
 </System>
 <EventData>
  <Data Name="NTSTATUS">3221225506</Data>
 </EventData>
</Event>
```

Atividade 3

A -O **RAMMap v1.52** é uma ferramenta avançada para análise detalhada do uso da memória RAM no Windows. Ela permite visualizar como a memória está

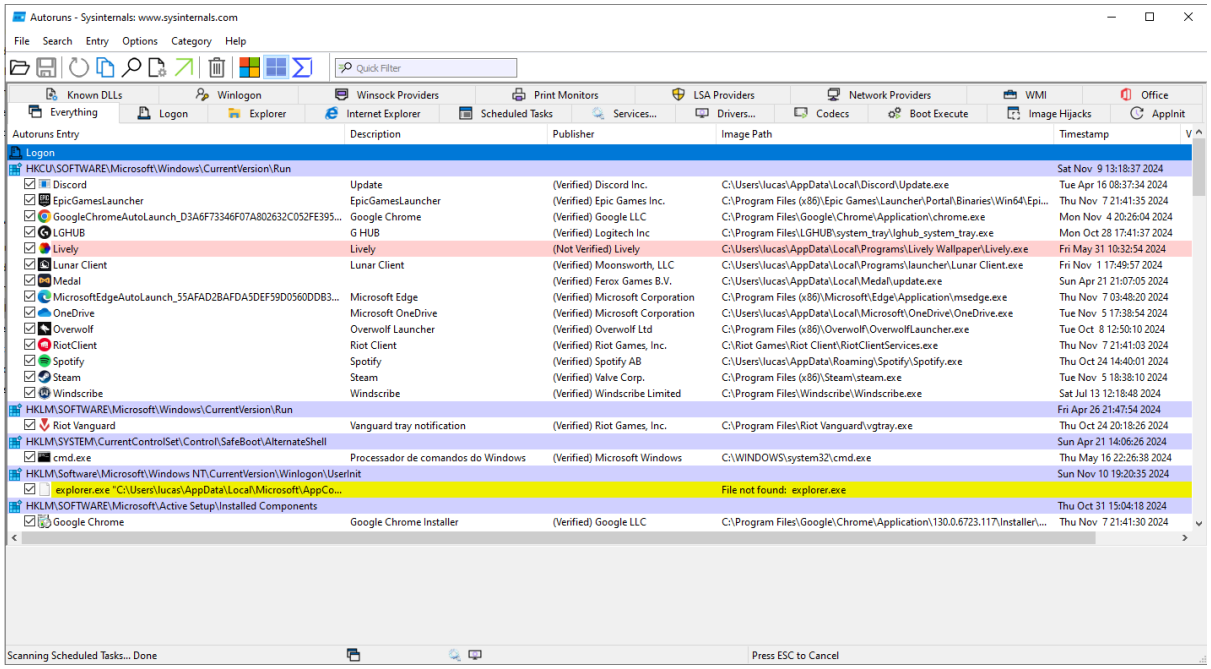
alocada, mostrando o consumo por processo, tipo de memória e outras áreas do sistema. É útil para diagnosticar problemas de memória, otimizar o desempenho e monitorar o uso de memória física e buffers de arquivos. Ideal para administradores de sistemas e técnicos.

B-



Atividade 4

A- O **Autoruns** é uma ferramenta que permite visualizar e gerenciar todos os programas que são configurados para iniciar automaticamente no Windows. Ela oferece uma visão detalhada de itens de inicialização, como programas, drivers e serviços, ajudando a identificar e desabilitar itens desnecessários ou maliciosos, melhorando o desempenho do sistema e a segurança.


Autoruns - Sysinternals: www.sysinternals.com
File Search Entry Options Category Help
Quick Filter
Known DLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services... Drivers... Codecs Boot Execute Image Hijacks AppInit
Autoruns Entry Description Publisher Image Path Timestamp
Logon
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Sat Nov 9 13:18:37 2024
Discord Update (Verified) Discord Inc. C:\Users\lucas\AppData\Local\Discord\Update.exe Tue Apr 16 08:37:34 2024
EpicGamesLauncher EpicGamesLauncher (Verified) Epic Games Inc. C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\Epi... Thu Nov 7 21:41:35 2024
GoogleChromeAutoLaunch_D3A6F73346F07A802632C052FE395... Google Chrome (Verified) Google LLC C:\Program Files\Google\Chrome\Application\chrome.exe Mon Nov 4 20:26:04 2024
LGHUB G HUB (Verified) Logitech Inc C:\Program Files\LGHUB\system_tray\lghub_system_tray.exe Mon Oct 28 17:41:37 2024
Lively Lively (Not Verified) Lively C:\Users\lucas\AppData\Local\Programs\Lively Wallpaper\Lively.exe Fri May 31 10:32:54 2024
Lunar Client Lunar Client (Verified) Moonsworth, LLC C:\Users\lucas\AppData\Local\Programs\launcher\Lunar Client.exe Fri Nov 1 17:49:57 2024
Medal (Verified) Ferox Games B.V. C:\Users\lucas\AppData\Local\Medal\update.exe Sun Apr 21 21:07:05 2024
MicrosoftEdgeAutoLaunch_55AFAD2BAFDA5DEF59D0560DDB3... Microsoft Edge (Verified) Microsoft Corporation C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Thu Nov 7 03:48:20 2024
OneDrive Microsoft OneDrive (Verified) Microsoft Corporation C:\Users\lucas\AppData\Local\Microsoft\OneDrive\OneDrive.exe Tue Nov 5 17:38:54 2024
Overwolf Overwolf Launcher (Verified) Overwolf Ltd C:\Program Files (x86)\Overwolf\OverwolfLauncher.exe Tue Oct 8 12:50:10 2024
RiotClient Riot Client (Verified) Riot Games, Inc. C:\Riot Games\Riot Client\RiotClientServices.exe Thu Nov 7 21:41:03 2024
Spotify Spotify (Verified) Spotify AB C:\Users\lucas\AppData\Roaming\Spotify\Spotify.exe Thu Oct 24 14:40:01 2024
Steam Steam (Verified) Valve Corp. C:\Program Files (x86)\Steam\steam.exe Tue Nov 5 18:38:10 2024
Windscribe Windscribe (Verified) Windscribe Limited C:\Program Files\Windscribe\Windscribe.exe Sat Jul 13 12:18:48 2024
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Fri Apr 26 21:47:54 2024
Riot Vanguard Vanguard tray notification (Verified) Riot Games, Inc. C:\Program Files\Riot Vanguard\vgtray.exe Thu Oct 24 20:18:26 2024
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell Sun Apr 21 14:06:26 2024
cmd.exe Processador de comandos do Windows (Verified) Microsoft Windows C:\WINDOWS\system32\cmd.exe Thu May 16 22:26:38 2024
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userlnit Sun Nov 10 19:20:35 2024
explorer.exe "C:\Users\lucas\AppData\Local\Microsoft\AppCo... File not found: explorer.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components Thu Oct 31 15:04:18 2024
Google Chrome Google Chrome Installer (Verified) Google LLC C:\Program Files\Google\Chrome\Application\130.0.6723.117\Installer\... Thu Nov 7 21:41:30 2024
Scanning Scheduled Tasks... Done
Press ESC to Cancel