1.A)

@echo off :: Desativa a exibição dos comandos na tela.
cls :: Limpa a tela.

:menu :: Define um rótulo de menu para retornar a este ponto no script.
cls :: Limpa a tela novamente.
color 2 :: Define a cor do texto para verde (2).

echo Programando como um raiz!!! :: Exibe o texto "Programando como um raiz!!!".
echo == :: Exibe uma linha de "=" para visual separador.
echo *1 - Mostre os arquivos que está na pasta* :: Exibe a opção 1 para mostrar os arquivos na pasta atual.
echo *2 - Mostre as informações do sistema onde estou* :: Exibe a opção 2 para mostrar informações do sistema.
echo *3 - Sair* :: Exibe a opção 3 para sair do programa.
echo == :: Exibe uma linha de "=" para visual separador.

set /p opcao= Escolha uma opcao: :: Lê a entrada do usuário e armazena na variável "opcao".
echo ------------------------------ :: Exibe uma linha para separar visualmente a entrada do usuário.

if %opcao% equ 1 goto opcao1 :: Se a opção for "1", vai para o rótulo ":opcao1".
if %opcao% equ 2 goto opcao2 :: Se a opção for "2", vai para o rótulo ":opcao2".
if %opcao% equ 3 goto opcao3 :: Se a opção for "3", vai para o rótulo ":opcao3".
if %opcao% GEQ 4 goto opcao4 :: Se a opção for maior ou igual a "4", vai para o rótulo ":opcao4".

:opcao1 :: Rótulo para a opção 1.
cls :: Limpa a tela.
dir :: Mostra o conteúdo da pasta atual.
echo --------- :: Exibe uma linha separadora.
echo *arquivos lidos* :: Exibe o texto "*arquivos lidos*".
echo --------- :: Exibe outra linha separadora.
pause :: Pausa para que o usuário possa ver os arquivos listados.
goto menu :: Retorna ao menu principal.

:opcao2 :: Rótulo para a opção 2.
cls :: Limpa a tela.
dir :: Mostra o conteúdo da pasta atual (mas não está correto para exibir informações do sistema).
echo --------- :: Exibe uma linha separadora.
echo *este é se sistema* :: Exibe o texto "*este é se sistema*".
echo --------- :: Exibe outra linha separadora.
pause :: Pausa para que o usuário possa ver a saída.
goto menu :: Retorna ao menu principal.

```
:opcao3  :: Rótulo para a opção 3.
cls  :: Limpa a tela.
exit  :: Encerra o programa.

:opcao4  :: Rótulo para opções inválidas.
cls  :: Limpa a tela.
echo ---------  :: Exibe uma linha separadora.
echo *Opção Inválida*  :: Exibe o texto "*Opção Inválida*".
echo ---------  :: Exibe outra linha separadora.
pause  :: Pausa para que o usuário veja a mensagem de erro.
goto menu  :: Retorna ao menu principal.
```

1.B)

```
@echo off
cls

:menu
cls

echo ============================================
echo Escolha uma das opcoes:
echo *0 - Sair*
echo *1 - Abrir o site UOL no Google Chrome*
echo *2 - Abrir o Bloco de Notas*
echo *3 - Trocar a cor do Prompt de Comandos para Amarelo*
echo *4 - Listar todas as tarefas em execução*
echo ============================================

set /p opcao= "Escolha uma opcao: "

if %opcao% equ 0 goto opcao0
if %opcao% equ 1 goto opcao1
if %opcao% equ 2 goto opcao2
if %opcao% equ 3 goto opcao3
if %opcao% equ 4 goto opcao4

cls
echo ---------
echo *Opcao Invalida*
echo ---------
pause
goto menu

:opcao0
cls
exit
```

```
:opcao1
cls
start chrome https://www.uol.com.br
goto menu

:opcao2
cls
start notepad
goto menu

:opcao3
cls
color 6
goto menu

:opcao4
cls
tasklist
pause
goto menu
```

2.A)

Descrição do Problema
O sistema Windows registrou um evento crítico de **Kernel-Power** (ID 41), indicando um reinício inesperado às **20:26 em 25/08/2020** no computador **DESKTOP-RS2L8OU**. Este tipo de erro ocorre quando o dispositivo é reiniciado sem um desligamento adequado e geralmente é causado por falha de energia, travamento do sistema ou erro de hardware.
Detalhes Técnicos

- **Fonte**: Microsoft-Windows-Kernel-Power
- **Data/Hora**: 25/08/2020 20:26:44
- **Identificação do Evento**: 41
- **Nível**: Crítico
- **BugcheckCode**: 292 (problema de travamento)
- **Parâmetros**:
    - BugcheckParameter1: 0x0
    - BugcheckParameter2: 0xffffc20665ab6028
    - BugcheckParameter3: 0xb6002000
    - BugcheckParameter4: 0xc0000135
- **Status do Sistema**:
    - SleepInProgress: 0
    - PowerButtonTimestamp: 0

Ação Recomendada

1. **Verifique fontes de alimentação**: Confirme que o dispositivo está conectado a uma fonte de energia estável e que não houve quedas de energia recentes.
2. **Reveja drivers e atualizações**: Instale todas as atualizações de drivers e patches críticos que possam corrigir erros do sistema.

3. **Monitoramento adicional**: Considere ativar logs para monitorar outros eventos de Kernel-Power nos próximos dias para observar possíveis padrões e evitar reinicializações inesperadas.

2.B)

Descrição do Evento
O sistema registrou um evento informativo da fonte **Microsoft-Windows-UserModePowerService** (ID 12) em **16/11/2017** às **19:26:45** no computador **HOME**. O serviço do Avast (AvastSvc.exe) ajustou o esquema de política de energia para um perfil específico, embora o GUID inicial e final sejam idênticos, indicando que a ação não mudou efetivamente a configuração.
Detalhes Técnicos

- **Fonte**: Microsoft-Windows-UserModePowerService
- **Data/Hora**: 16/11/2017 19:26:45
- **Identificação do Evento**: 12
- **Nível**: Informações
- **Processo**: AvastSvc.exe
    - **Caminho do Processo**: C:\Program Files\AVAST Software\Avast\AvastSvc.exe
    - **ID do Processo**: 1152
- **Política de Energia**:
    - **GUID Antigo**: {381B4222-F694-41F0-9685-FF5BB260DF2E}
    - **GUID Novo**: {381B4222-F694-41F0-9685-FF5BB260DF2E}

Ação Recomendada

1. **Verificar a Configuração de Energia**: Confirme que o esquema de política de energia definido no sistema é adequado para o uso pretendido, especialmente em sistemas de alta disponibilidade ou restrições de energia.
2. **Monitorar Ações Frequentes**: Caso o Avast ou outros aplicativos estejam redefinindo políticas de energia com frequência, avalie se essas ações impactam a performance do sistema e, se necessário, ajuste as configurações do antivírus.
3. **Confirmar Integridade**: Assegure-se de que o processo AvastSvc.exe seja legítimo e atualizado, de forma a evitar interferências indesejadas com políticas de energia.

2.C)

Descrição do Evento
No computador **AG-CRM-02**, foi registrado um evento de aviso do **Win32k** (ID 700) em **11/11/2024 às 18:59:13**. O evento indica que o **Power Manager** solicitou uma supressão total das entradas de dispositivos de entrada (INPUT_SUPPRESS_REQUEST = 1), uma ação que normalmente ocorre durante transições de estado de energia.
Detalhes Técnicos

- **Fonte**: Win32k
- **Data/Hora**: 11/11/2024 18:59:13
- **Identificação do Evento**: 700
- **Nível**: Aviso
- **Palavras-chave**: Clássico
- **Processo e Thread**:
    - **ProcessID**: 4

    - **ThreadID**: 7348
- **Computer**: AG-CRM-02

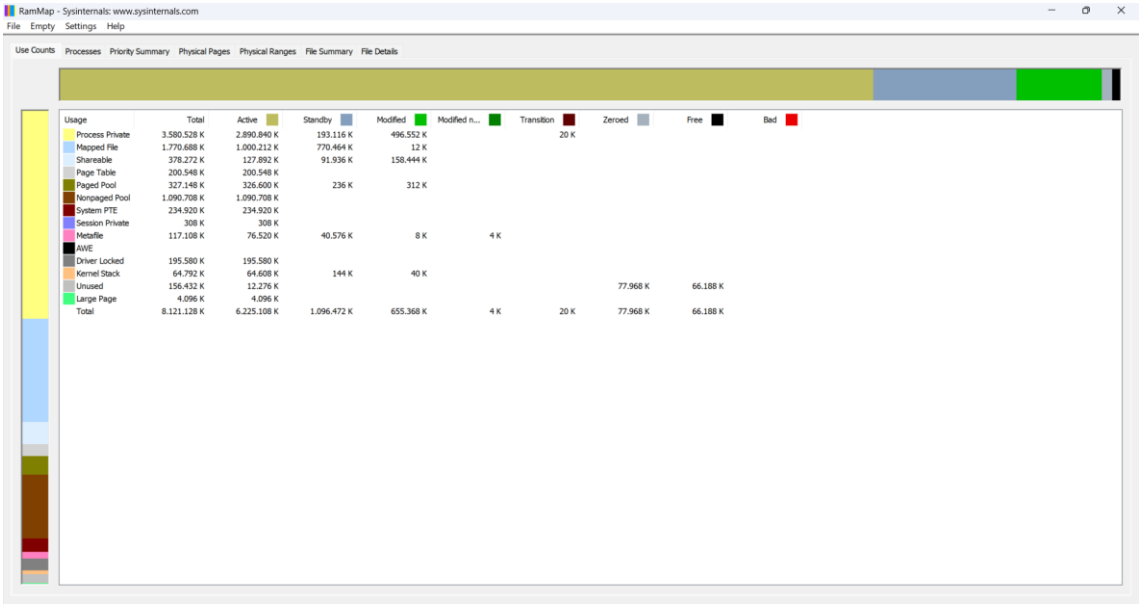
Ação Recomendada

1. **Verificar Políticas de Energia**: Avalie as políticas de energia configuradas no sistema para confirmar se essa supressão de entrada é intencional (comum em configurações de economia de energia).
2. **Análise de Frequência**: Caso o evento ocorra frequentemente, verifique se há inconsistências nas configurações de energia ou problemas nos componentes que gerenciam estados de suspensão.
3. **Monitorar Comportamento do Sistema**: Se houver impacto na usabilidade, analise a possibilidade de ajustar as configurações de gerenciamento de energia ou atualizar os drivers relacionados ao Power Manager.

3.A)

O objetivo do aplicativo RAMMap é permitir obter noção da alocação de memória RAM do Windows, como ela se dá e como ela está sendo utilizada pelas aplicações. Ele oferece recursos para esse fim.

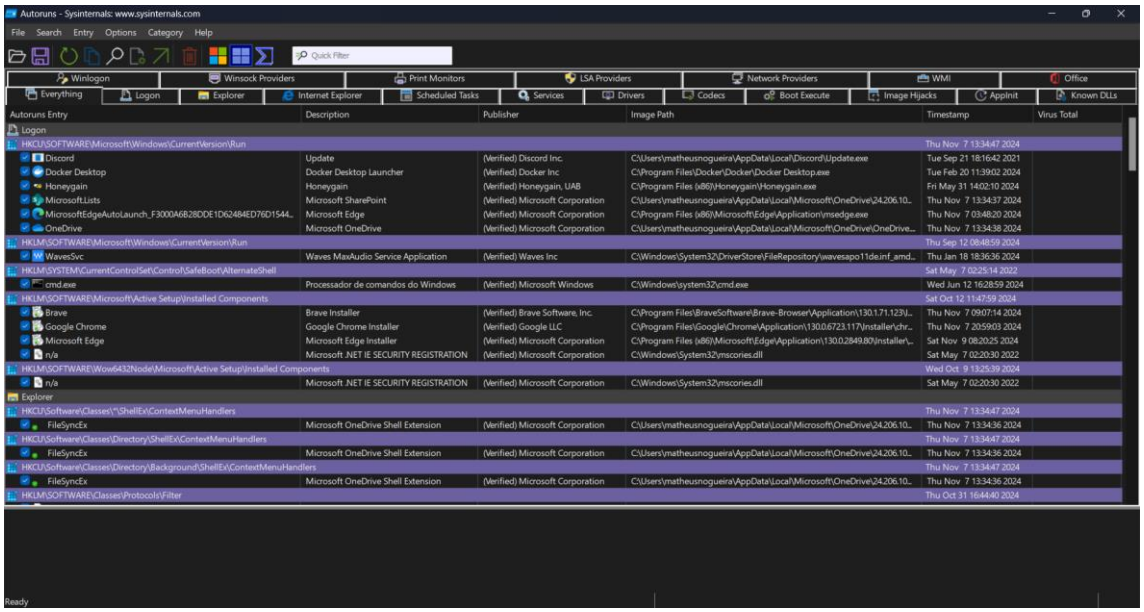
3.B)



4.A)

O objetivo da aplicação Autoruns é monitorar e apresentar de forma aprofundada múltiplos programas e processos configurados para iniciarem automaticamente, seja no *boot* do computador ou em outras circunstâncias.

4.B)


Autoruns - Sysinternals: www.sysinternals.com
File Search Entry Options Category Help
Quick Filter
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 Known DLLs
Autoruns Entry Description Publisher Image Path Timestamp Virus Total
Logon
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Thu Nov 7 13:34:47 2024
Discord Update (Verified) Discord Inc. C:\Users\matheusnogueira\AppData\Local\Discord\Update.exe Tue Sep 21 18:16:42 2021
Docker Desktop Docker Desktop Launcher (Verified) Docker Inc C:\Program Files\Docker\Docker\Docker Desktop.exe Tue Feb 20 11:39:02 2024
Honeygain Honeygain (Verified) Honeygain, UAB C:\Program Files (x86)\Honeygain\Honeygain.exe Fri May 31 14:02:10 2024
MicrosoftLists Microsoft SharePoint (Verified) Microsoft Corporation C:\Users\matheusnogueira\AppData\Local\Microsoft\OneDrive\24.206.10... Thu Nov 7 13:34:37 2024
MicrosoftEdgeAutoLaunch_F3000A6B28DDE1D62484ED76D1544... 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\matheusnogueira\AppData\Local\Microsoft\OneDrive\OneDrive... Thu Nov 7 13:34:38 2024
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Thu Sep 12 08:48:59 2024
WavesSvc Waves MaxAudio Service Application (Verified) Waves Inc C:\Windows\System32\DriverStore\FileRepository\wavesapo11de.inf_amd... Thu Jan 18 18:36:36 2024
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell Sat May 7 02:25:14 2022
cmd.exe Processador de comandos do Windows (Verified) Microsoft Windows C:\Windows\system32\cmd.exe Wed Jun 12 16:28:59 2024
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components Sat Oct 12 11:47:59 2024
Brave Brave Installer (Verified) Brave Software, Inc. C:\Program Files\BraveSoftware\Brave-Browser\Application\130.1.71.123\I... Thu Nov 7 09:07:14 2024
Google Chrome Google Chrome Installer (Verified) Google LLC C:\Program Files\Google\Chrome\Application\130.0.6723.117\Installer\chr... Thu Nov 7 20:59:03 2024
Microsoft Edge Microsoft Edge Installer (Verified) Microsoft Corporation C:\Program Files (x86)\Microsoft\Edge\Application\130.0.2849.80\Installer\... Sat Nov 9 08:20:25 2024
n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\System32\mscories.dll Sat May 7 02:20:30 2022
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components Wed Oct 9 13:25:39 2024
n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\System32\mscories.dll Sat May 7 02:20:30 2022
Explorer
HKCU\Software\Classes*\ShellEx\ContextMenuHandlers Thu Nov 7 13:34:47 2024
FileSyncEx Microsoft OneDrive Shell Extension (Verified) Microsoft Corporation C:\Users\matheusnogueira\AppData\Local\Microsoft\OneDrive\24.206.10... Thu Nov 7 13:34:36 2024
HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers Thu Nov 7 13:34:47 2024
FileSyncEx Microsoft OneDrive Shell Extension (Verified) Microsoft Corporation C:\Users\matheusnogueira\AppData\Local\Microsoft\OneDrive\24.206.10... Thu Nov 7 13:34:36 2024
HKCU\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers Thu Nov 7 13:34:47 2024
FileSyncEx Microsoft OneDrive Shell Extension (Verified) Microsoft Corporation C:\Users\matheusnogueira\AppData\Local\Microsoft\OneDrive\24.206.10... Thu Nov 7 13:34:36 2024
HKLM\SOFTWARE\Classes\Protocols\Filter Thu Oct 31 16:44:40 2024
Ready