Fuhndamentos de Redes de Computadores

Nome: *Gabriel Domingues Silva* ***Turma:*** *24E3-1*

Tema: Teste de Performance 3 - Windows, Linux e Virtualização

Prof. Fabiano Alves Gisbert

Instituto Infnet

]

1 Mostre onde fica a aba de atalhos de comandos na Área de Trabalho.

Clicar com botão direito no menu iniciar, a seguir a aba de atalhos de comandos:

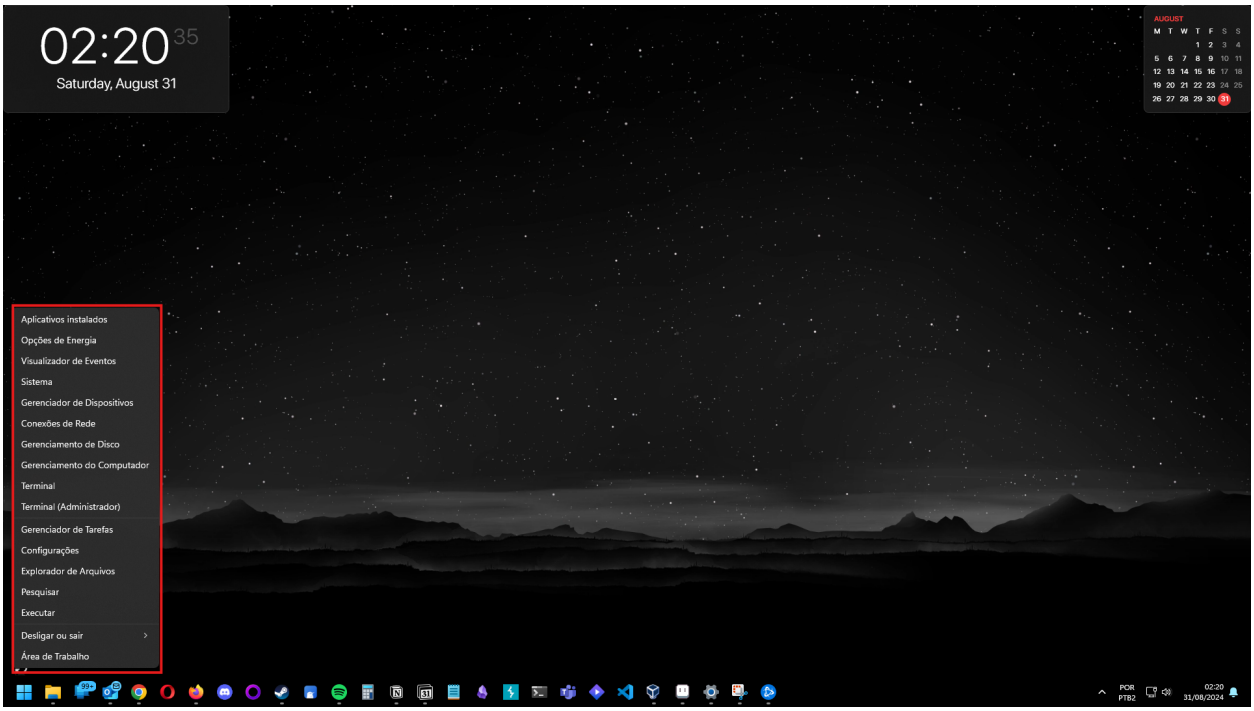

Figura 1: Aba de atalhos de comandos

2 Caso uma placa de vídeo apresente mau funcionamento e você identifique a necessidade de trocar o driver para um mais atualizado, mostre onde e como será feito o procedimento de troca deste driver.

Clicar com botão direito no menu iniciar e clicar em gerenciador de dispositivos, onde vc pode manipular os drivers dos dispositivos, como ilustrado na figura a seguir:

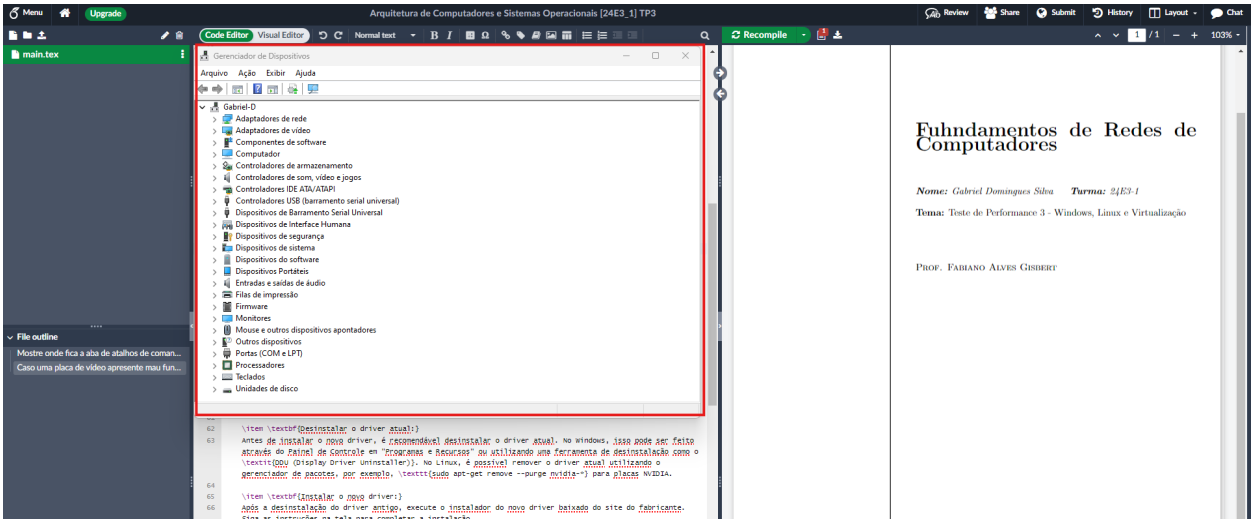

Figura 2: Janela do Gerenciador de Dispositivos

Caso uma placa de vídeo apresente mau funcionamento e seja necessário trocar o driver por um mais atualizado, o procedimento pode ser realizado da seguinte maneira:

1. **Identificar o modelo da placa de vídeo:** Primeiro, é necessário identificar o modelo exato da placa de vídeo instalada no sistema. Isso pode ser feito através do Gerenciador de Dispositivos no Windows ou utilizando comandos como `lspci | grep VGA` no Linux.

2. **Baixar o driver mais recente:** Acesse o site oficial do fabricante da placa de vídeo (por exemplo, *NVIDIA* ou *AMD*) e navegue até a seção de suporte ou downloads. Utilize as informações do modelo da placa para encontrar o driver mais recente compatível com o seu sistema operacional.

3. **Desinstalar o driver atual:** Antes de instalar o novo driver, é recomendável desinstalar o driver atual. No Windows, isso pode ser feito através do Painel de Controle em "Programas e Recursos"ou utilizando uma ferramenta de desinstalação como o *DDU (Display Driver Uninstaller)*. No Linux, é possível remover o driver atual utilizando o gerenciador de pacotes, por exemplo, `sudo apt-get remove --purge nvidia-*` para placas NVIDIA.

4. **Instalar o novo driver:** Após a desinstalação do driver antigo, execute o instalador do novo driver baixado do site do fabricante. Siga as instruções na tela para completar a instalação.

5. **Reiniciar o sistema:** Após a instalação, é importante reiniciar o sistema para garantir que todas as alterações sejam aplicadas corretamente.

6. **Verificar o funcionamento:** Após a reinicialização, verifique se a placa de vídeo está funcionando corretamente com o novo driver. Isso pode ser feito observando o desempenho gráfico em jogos ou aplicativos que exigem aceleração de hardware.

3 Execute um comando de verificação de status da rede do seu sistema Windows.

Clicar com botão direito no menu Iniciar e clicar em Terminal, executar o comando `ipconfig` no console como ilustrado abaixo:

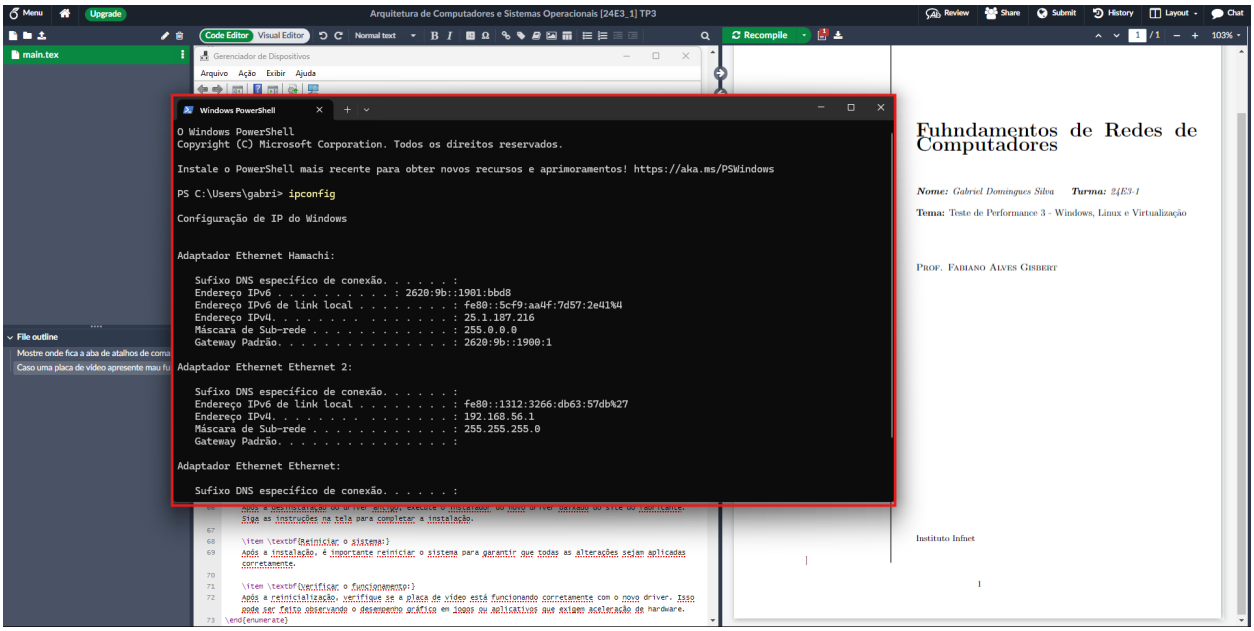

Figura 3: Janela do PowerSHell

4 Um cliente reportou uma extrema lentidão no sistema Windows. Como primeiro passo de diagnóstico, liste os processos em execução em ordem de uso de CPU.

Segurar as teclas Ctrl + Shift + Esc, irá abrir o Gerenciador de Tarefas, lugar em que se encontram os processos do sistema e filtrar por uso de CPU, como na figura a seguir:

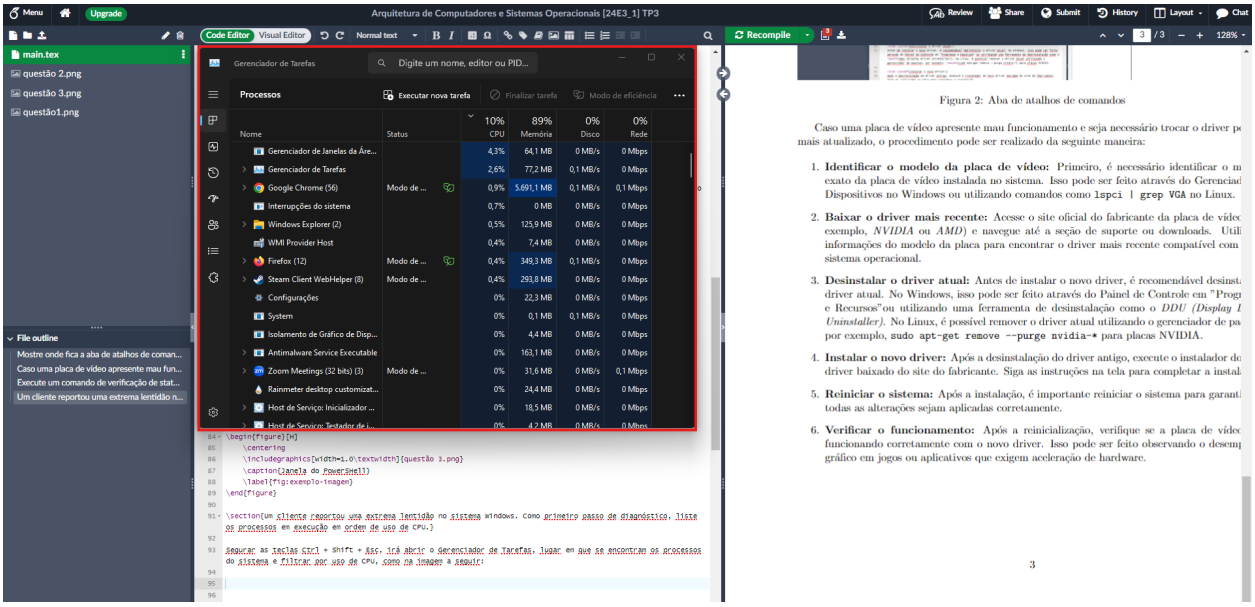

Figura 4: Janela do PowerSHell

5 Qual o comando do Prompt que executa uma verificação de integridade do sistema.

O comando do Prompt de Comando que executa uma verificação de integridade do sistema é:

```
sfc /scannow
```

Explicação:

- `sfc`: Abreviação de *System File Checker*, é uma ferramenta que verifica a integridade dos arquivos de sistema do Windows.
- `/scannow`: Esse parâmetro instrui o `sfc` a verificar todos os arquivos de sistema protegidos e substituir os arquivos corrompidos por uma cópia correta do cache do sistema.

6 Liste os principais componentes do Windows Security.

Principais componentes do Windows Security:

1. **Proteção contra vírus e ameaças**: Oferece monitoramento em tempo real para detectar, prevenir e remover vírus, malware e outras ameaças. Inclui a capacidade de realizar verificações manuais e automáticas do sistema.
2. **Firewall e proteção de rede**: Gerencia as configurações do Firewall do Windows Defender, ajudando a proteger o sistema contra acessos não autorizados e ameaças baseadas na rede.
3. **Controle de aplicativos e navegador**: Protege o sistema contra aplicativos potencialmente perigosos e sites maliciosos. Inclui recursos como a Proteção de Exploração e o SmartScreen do Windows Defender, que ajudam a bloquear conteúdo potencialmente nocivo.
4. **Segurança de dispositivo**: Verifica a integridade do dispositivo e oferece opções de segurança baseadas em hardware, como inicialização segura e isolamento do núcleo.
5. **Desempenho e integridade do dispositivo**: Monitora o estado geral do dispositivo, incluindo drivers, armazenamento e integridade do sistema, e oferece recomendações para otimização.
6. **Opções de família**: Permite que os pais gerenciem as atividades online de seus filhos, incluindo limites de tempo de tela, filtros de conteúdo e relatórios de atividades.
7. **Proteção de conta**: Gerencia as opções de segurança de conta, como a autenticação de dois fatores e o Windows Hello, que oferece métodos de autenticação biométrica.

7 O que é Windows Registry e qual a ferramenta que permite sua edição.

Windows Registry é uma base de dados hierárquica utilizada pelo sistema operacional Windows para armazenar informações de configuração e opções para o sistema operacional, aplicativos, dispositivos de hardware e usuários. Ele contém dados essenciais que controlam como o Windows

funciona e como os programas se comportam.

A ferramenta que permite a edição do Windows Registry é chamada de **Editor do Registro**, acessada através do comando: `regedit`

Essa ferramenta fornece uma interface gráfica para visualizar e modificar as chaves e valores do registro.

8 Abra essa ferramenta e indique a chave que permite edição de componentes de hardware

Para abrir o `regedit` (Editor do Registro), você pode seguir estas etapas:

1. Pressione `Win + R` para abrir a caixa de diálogo Executar.
2. Digite `regedit` e pressione `Enter`.
3. Se solicitado pelo Controle de Conta de Usuário, clique em `Sim` para permitir a abertura do Editor do Registro.

A chave do Registro que permite a edição de componentes de hardware pode variar dependendo do que você deseja editar. No entanto, para configurações gerais de hardware, você pode encontrar informações relevantes em:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class`

Como ilustrado na figura a seguir:

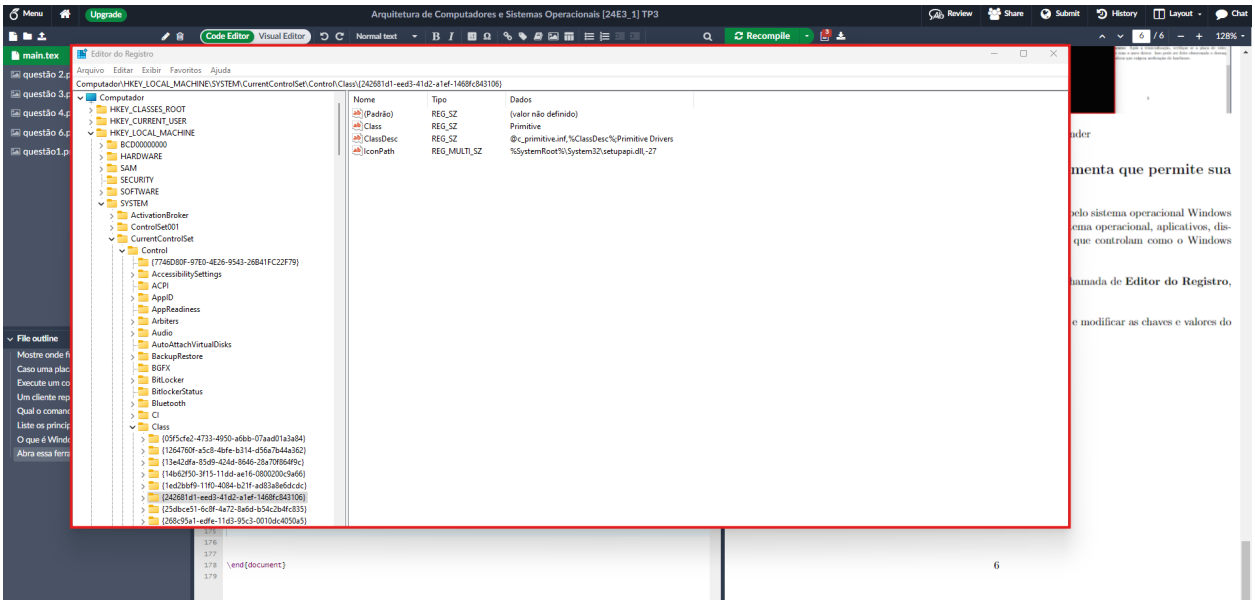

Figura 5: Editor de registro do Windows

9 Abra o Performance Monitor e gere uma evidência de análise de memória e CPU do Windows.

Abriu-se o Monitor de Recursos do Windows 11 para realizar os testes, abrindo o mesmo jogo, observamos um aumento de uso dos recursos CPU e RAM:

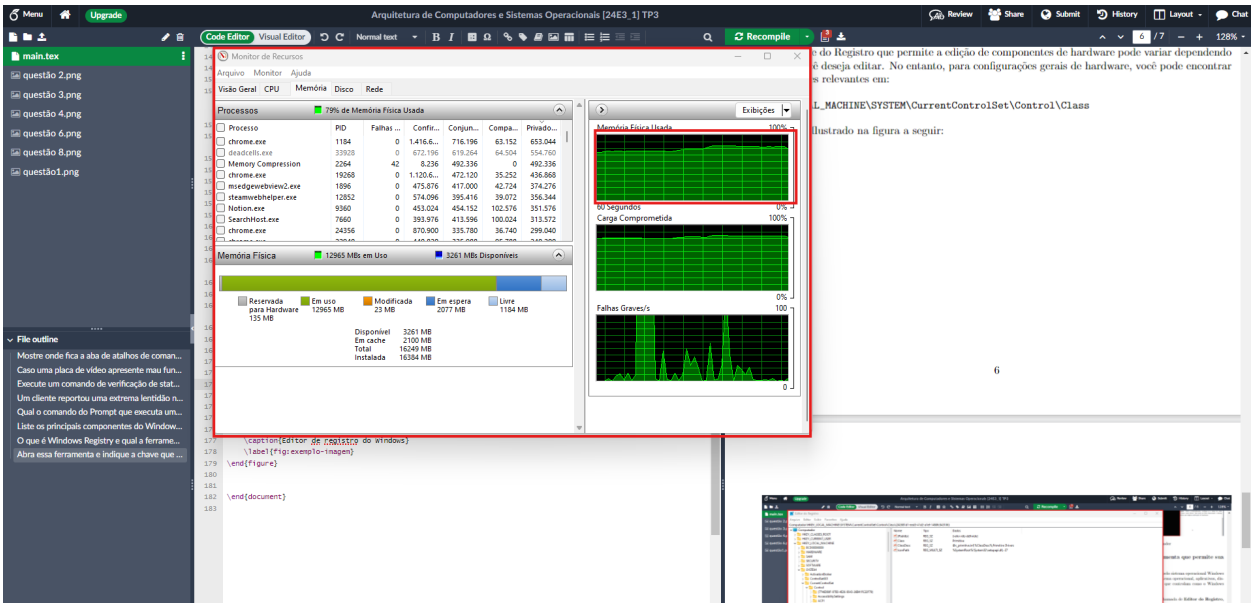

Figura 6: Registro de uso de RAM aumentando

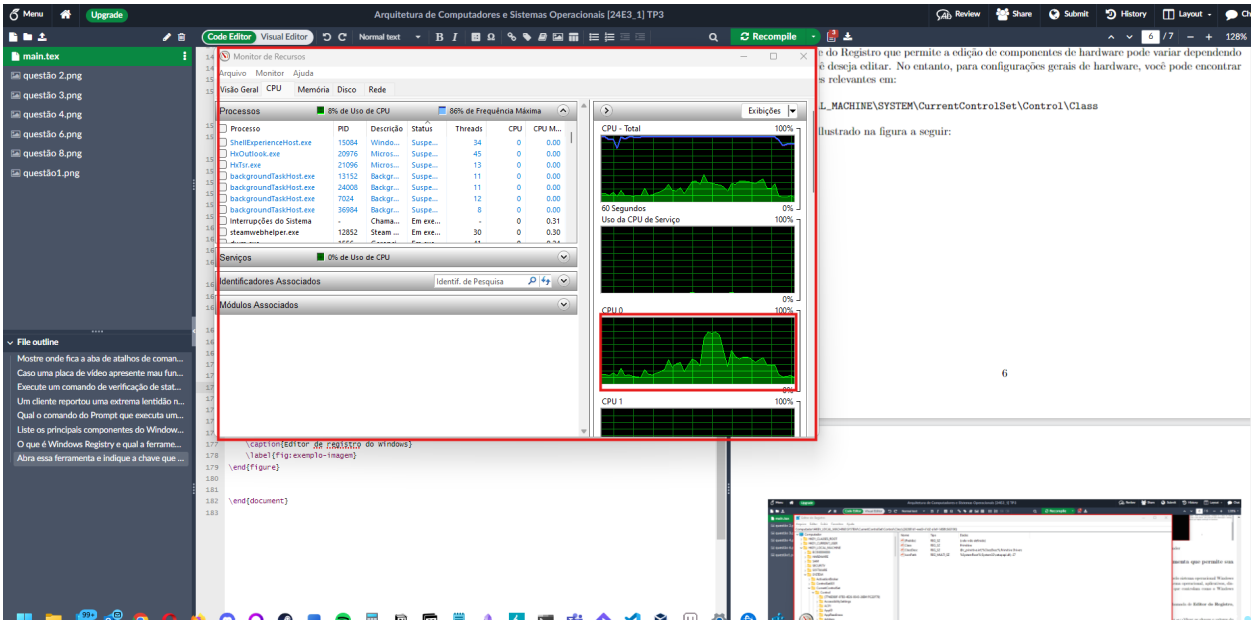

Figura 7: Registro de uso de CPU aumentando

10 Qual a versão do Kernel do Windows em uso nestas questões?

Abriu-se o Prompt de Comando e digitou-se `ver` como ilustrado na figura a seguir:

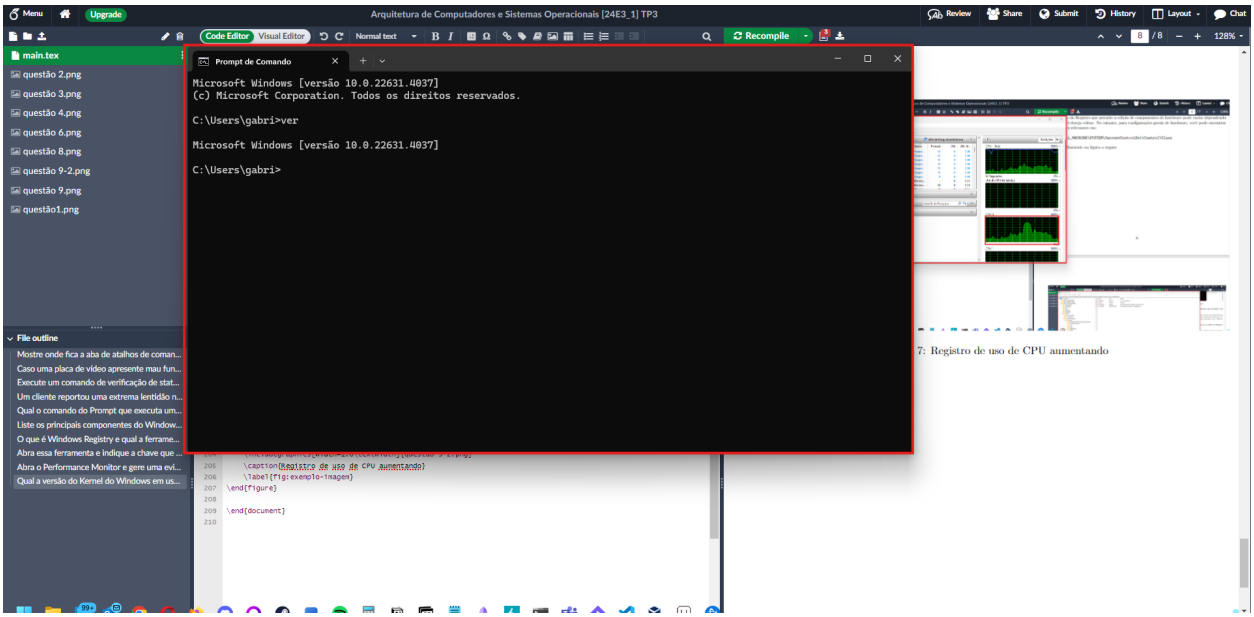

Figura 8: Prompt de Comando com a versão do kernel

11 No Linux, o usuário se comunica com o sistema operacional usando a CLI ou a GUI. Explique a diferença entre essas duas interfaces, dando exemplo de aplicativos que entregam essas interfaces.

No Linux, as interfaces de usuário podem ser divididas em dois tipos principais: CLI (Command Line Interface) e GUI (Graphical User Interface). Cada uma delas oferece uma forma distinta de interação com o sistema.

Interface CLI

A CLI permite a interação com o sistema operacional através de comandos digitados em uma linha de comando. Os usuários precisam digitar comandos específicos para realizar tarefas e operações. A CLI é geralmente mais eficiente para usuários avançados e para automação de tarefas, pois permite a execução rápida e precisa de comandos.

Exemplos de aplicativos CLI:

- `bash` - O Bourne Again Shell, um dos shells mais populares no Linux.
- `vim` - Um editor de texto poderoso que é operado inteiramente a partir da linha de comando.
- `grep` - Uma ferramenta de busca que permite procurar texto dentro de arquivos.

Interface GUI

A GUI fornece uma interface gráfica com ícones, janelas e menus que facilitam a interação com o sistema operacional. Os usuários podem clicar em ícones e usar menus para realizar tarefas, tornando a GUI mais intuitiva e acessível para iniciantes.

Exemplos de aplicativos GUI:

- `GIMP` - Um editor de imagens gráfico com uma interface de usuário completa.
- `Firefox` - Um navegador web com uma interface gráfica que permite navegação na internet.
- `LibreOffice` - Um pacote de software de escritório que inclui um processador de texto, planilhas e apresentações, todos com interfaces gráficas.

12 Crie um arquivo chamado teste.doc no diretório de usuário /usr

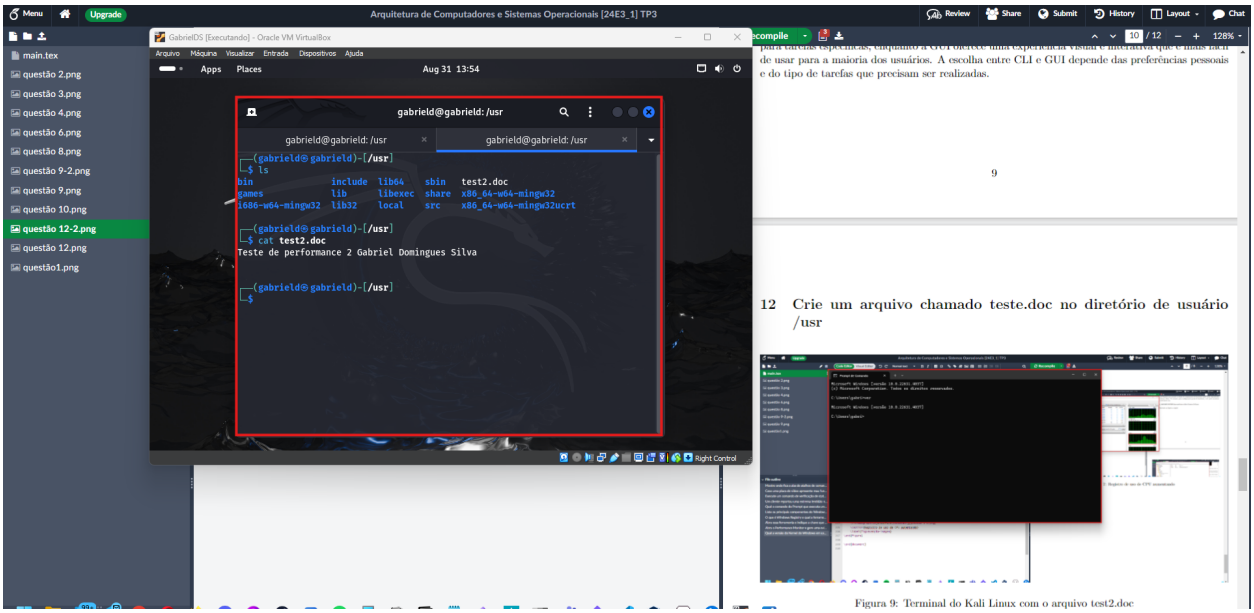

Figura 9: Terminal do Kali Linux com o arquivo test2.doc

13 O terminal Linux está apresentando problemas de conectividade e você precisa verificar se ele está com o endereço IP configurado corretamente. Quais os caminhos que você faria (em GUI ou em CLI) para fazer essa verificação?

Via CLI, basta abrir o Terminal do Linux e digitar `ifconfig` como na figura a seguir:

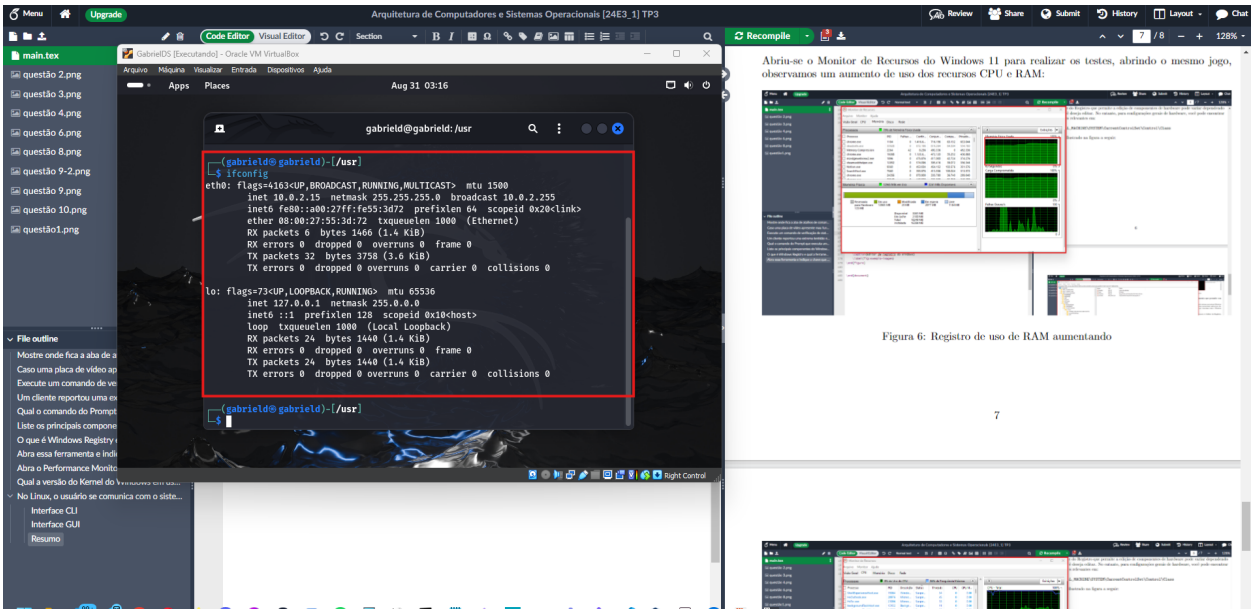

Figura 10: Terminal do Kali Linux comando ifconfig

Via GUI basta clicar no ícone de rede e clicar em configurações como mostra a firgura a seguir:

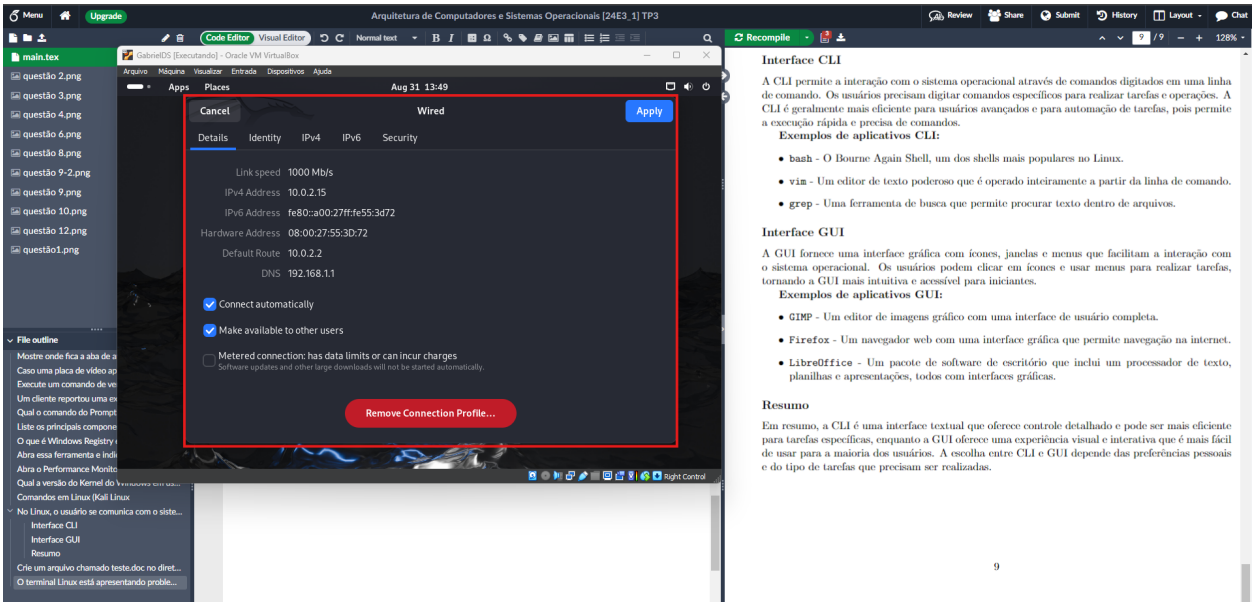

Figura 11: Configurações de rede via GUI Kali Linux

14 Explique como verificar os estados de um processo no terminal Linux e descreva o comando para encerrar o processo 511 que está apresentando instabilidade

Para verificar os estados de um processo no terminal Linux, você pode usar o comando `ps` ou `top`. O comando `ps` exibe informações sobre processos em execução, e o comando `top` fornece uma visão

em tempo real dos processos do sistema.

Para verificar o estado do processo com ID 511, você pode usar:

```
ps -p 511
```

Para encerrar o processo com ID 511, você pode usar o comando:

```
kill 511
```

Se o processo não encerrar com o comando `kill`, você pode usar o sinal `-9` para forçar o encerramento:

```
kill -9 511
```

15 O que é um SOC? Cite um programa de Linux que pode auxiliar no monitoramento da segurança de rede

Em Linux, SOC (Security Operations Center) refere-se a uma unidade ou equipe dedicada à monitorização, detecção e resposta a incidentes de segurança cibernética.

Um programa de Linux que pode auxiliar no monitoramento da segurança de rede é o `Wireshark`.

16 Qual a ferramenta de IDS presente no sistema Linux? Mostre o comando que nos possibilita analisar o log desta ferramenta.

Uma ferramenta de IDS (Intrusion Detection System) presente no sistema Linux é o `Snort`.

Para analisar o log gerado por essa ferramenta, pode-se usar o seguinte comando:

```
tail -f /var/log/snort/alert
```

Este comando permite visualizar em tempo real as entradas do arquivo de log de alertas do `Snort`. Como mostra a figura a seguir (como se trata de uma versão limpa do sistema, não existem logs a serem analisados):

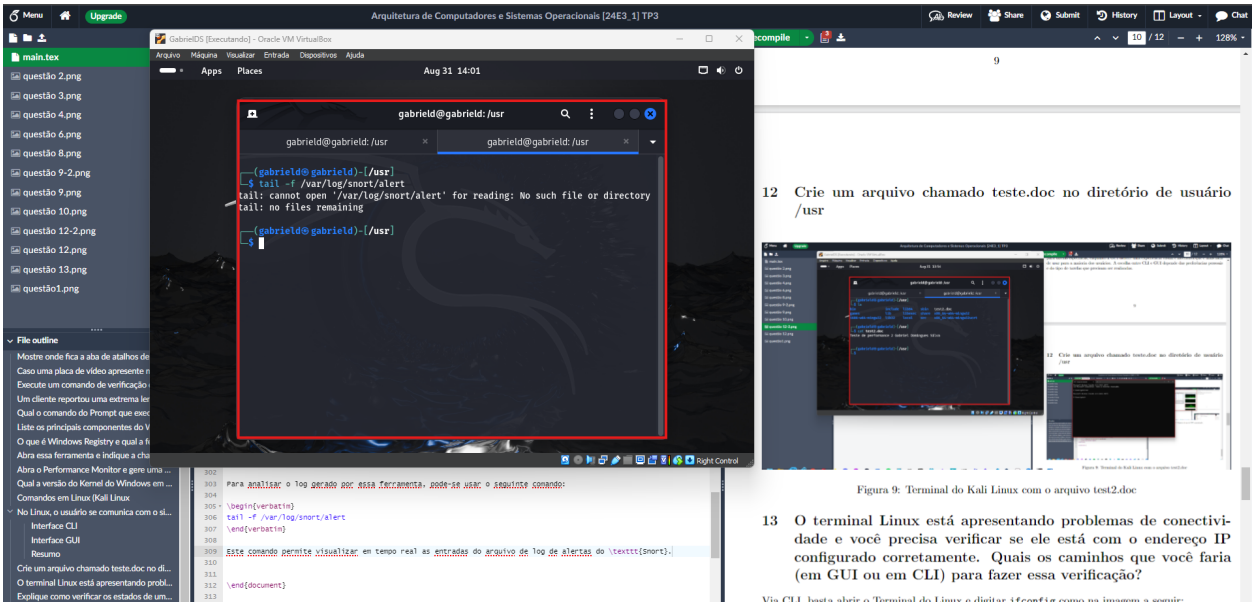

Figura 9: Terminal do Kali Linux com o arquivo test2.doc

Figura 12: Terminal com comando IDS