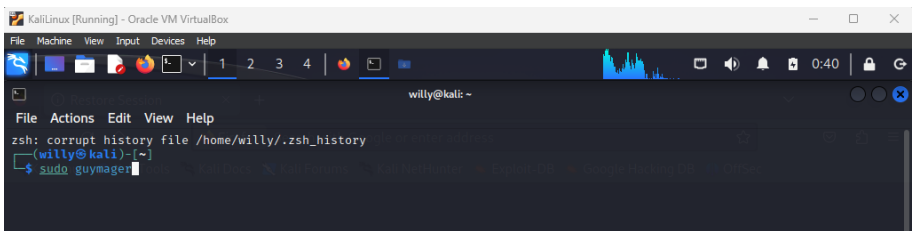
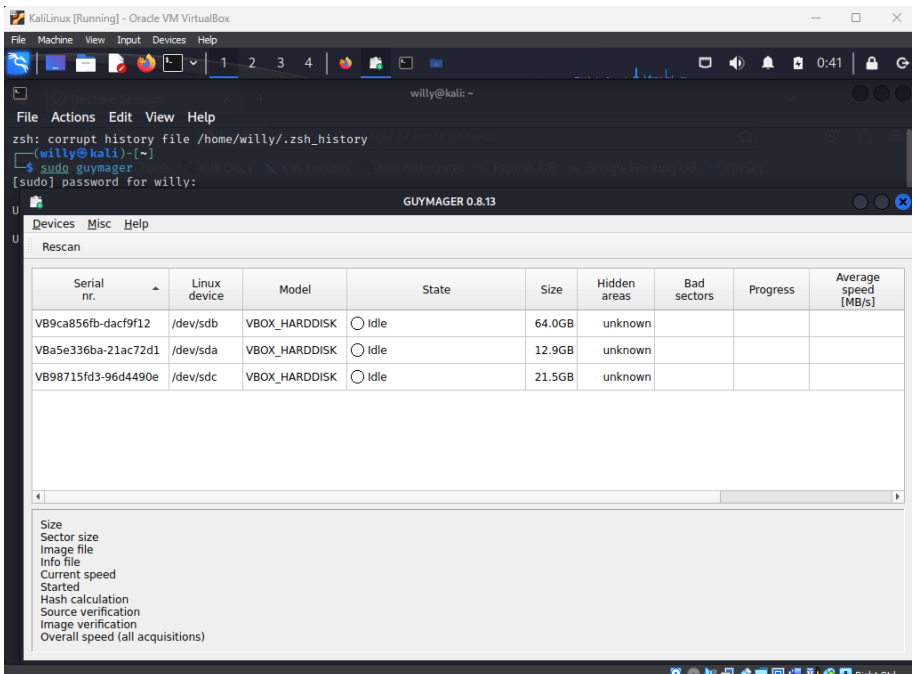


Pada bagian Windows Forensics, saya membantu dalam pembuatan image dan analisis. Pengambilan Data menggunakan Guymager pada Linux dan analisisnya menggunakan autopsy dan fileParser Lizard. Berikut beberapa dokumentasinya.



Menjalankan guymager di dalam linux



Tampilan awal guymager

This PC > Windows-SSD (C:) > extract > evtb-extract > Logs

Name	Date modified	Type	Size
Application.evtx	09/06/2024 11:47	Event Log	1.092 KB
Application.evtx-slack	09/06/2024 11:47	EVTX-SLACK File	768 KB
HardwareEvents.evtx	09/06/2024 11:47	Event Log	68 KB
Internet Explorer.evtx	09/06/2024 11:47	Event Log	68 KB
Key Management Service.evtx	09/06/2024 11:47	Event Log	68 KB
Microsoft-Client-Licensing-Platform%4A...	09/06/2024 11:47	Event Log	1.028 KB
Microsoft-Client-Licensing-Platform%4A...	09/06/2024 11:47	EVTX-SLACK File	832 KB
Microsoft-Windows-AAD%4Operational...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-Application-Experie...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-Application-Experie...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-Application-Experie...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-Application-Experie...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-AppModel-Runtime...	09/06/2024 11:47	Event Log	1.028 KB
Microsoft-Windows-AppModel-Runtime...	09/06/2024 11:47	EVTX-SLACK File	768 KB
Microsoft-Windows-AppReadiness%4Ad...	09/06/2024 11:47	Event Log	1.092 KB
Microsoft-Windows-AppReadiness%4Ad...	09/06/2024 11:47	EVTX-SLACK File	896 KB
Microsoft-Windows-AppReadiness%4Op...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-AppXDeployment%...	09/06/2024 11:47	Event Log	1.028 KB
Microsoft-Windows-AppXDeployment%...	09/06/2024 11:47	EVTX-SLACK File	448 KB
Microsoft-Windows-AppXDeploymentSe...	09/06/2024 11:47	Event Log	5.124 KB
Microsoft-Windows-AppXDeploymentSe...	09/06/2024 11:47	EVTX-SLACK File	256 KB
Microsoft-Windows-AppXDeploymentSe...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-AppxPackaging%4...	09/06/2024 11:47	Event Log	1.028 KB
Microsoft-Windows-AppxPackaging%4...	09/06/2024 11:47	EVTX-SLACK File	768 KB
Microsoft-Windows-Audio%4CaptureM...	09/06/2024 11:47	Event Log	68 KB
Microsoft-Windows-Audio%4Operationa...	09/06/2024 11:47	Event Log	68 KB

Hasil Ekstraksi C:\windows\system32\winevt\logs\,

