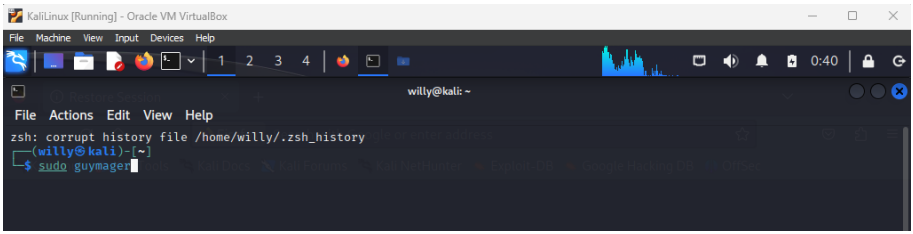
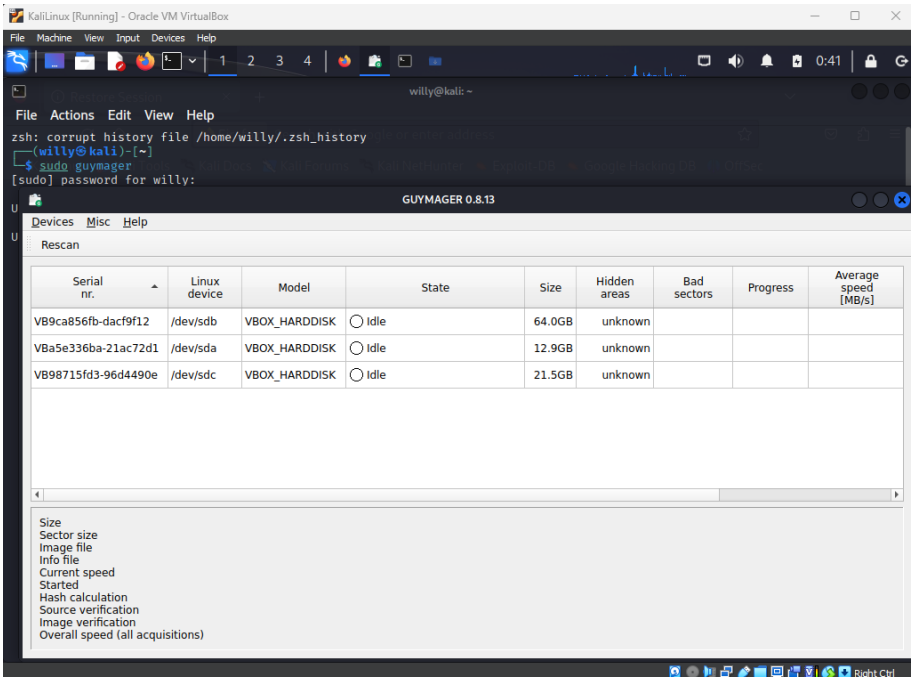
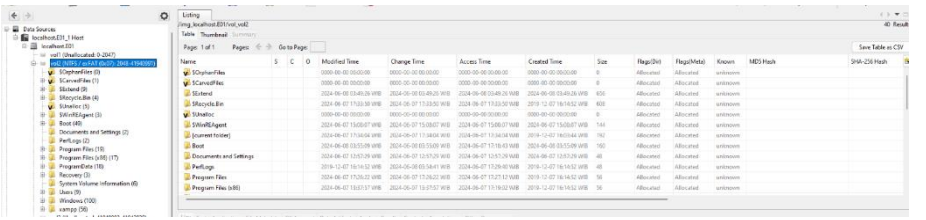
Pada bagian Windows Forensics, saya membantu dalam pembuatan image dan analisis. Pengambilan Data menggunakan Guymager pada Linux dan analisisnya menggunakan autopsy dan fileParser Lizard. Berikut beberapa dokumentasinya.



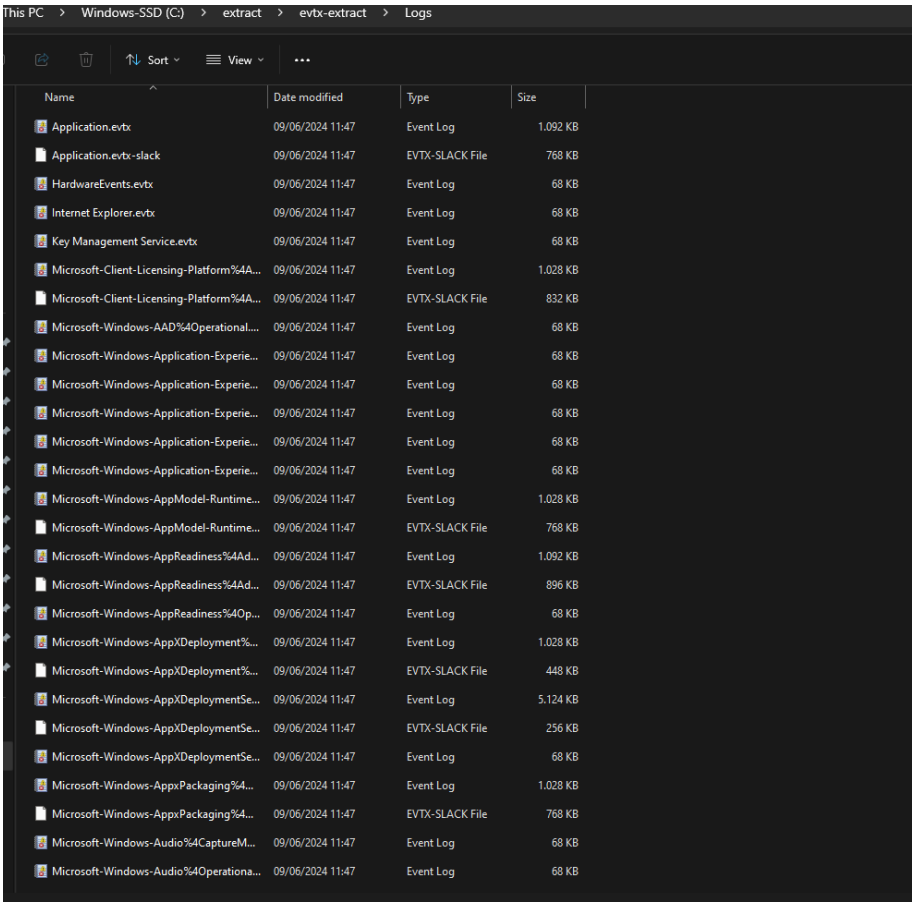
Menjalankan guymager di dalam linux



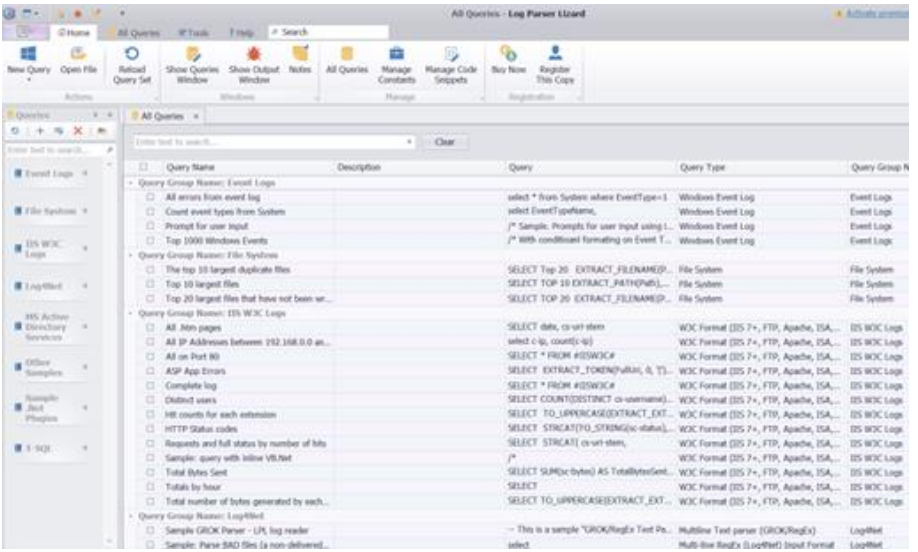
Tampilan awal guymager



Tampilan Awal Autopsy



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



Analisis menggunakan FileParser Lizard