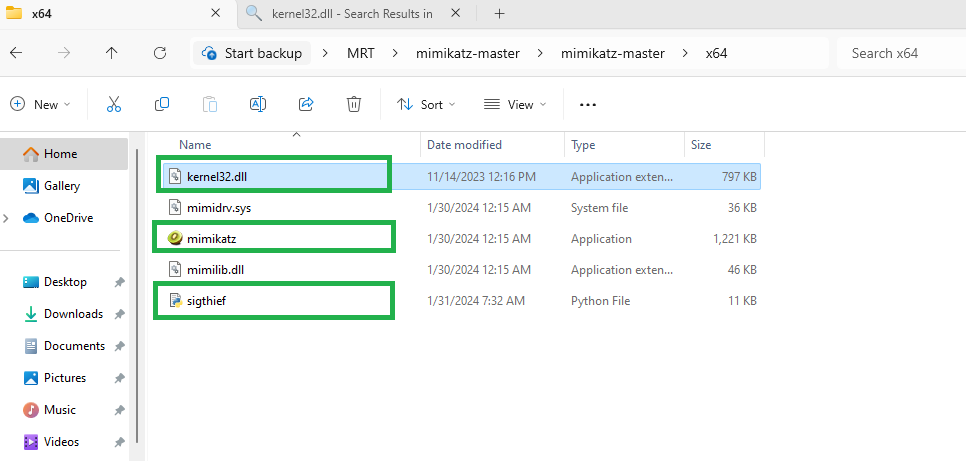
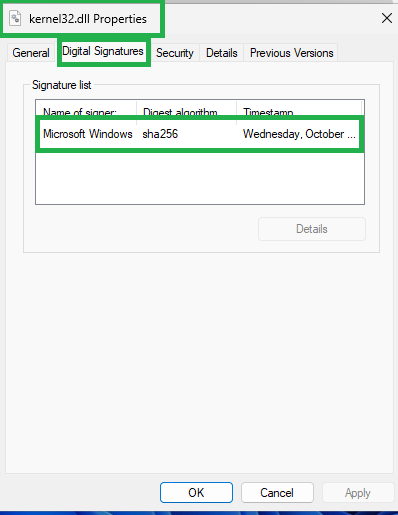
SigThief toolu cihaz üzerindeki dijital imzalı bir dosyada imzayı kopyalayıp bizim istediğimiz dosyaya imzayı enjekte eder ve bu şekilde antivirüs programını atlatmayı amaçlar. Ben örnek olsun diye System32 altında bulunan kernel32.dll dosyasından Microsoft sertifikasını kopyalayıp mimikatz dosyasına enjekte etmeyi göstereceğim. Aşağıdaki resimde kernel32.dll mimikatz.exe ve sigthief.py dosyaları bulunmaktadır.

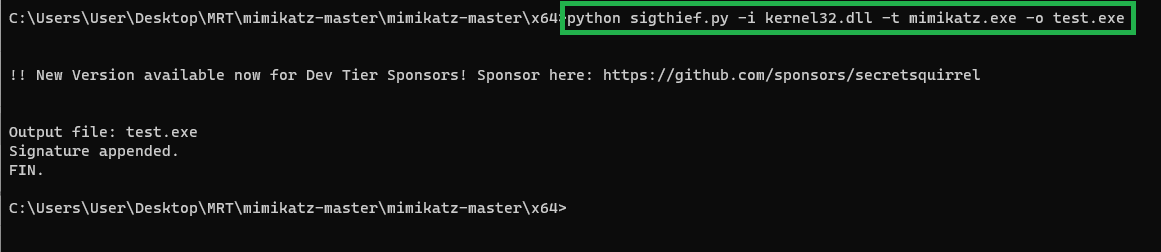


Aşağıdaki dosyada Kernel32.dll dosyasının Microsoft sertifikası görülmektedir.

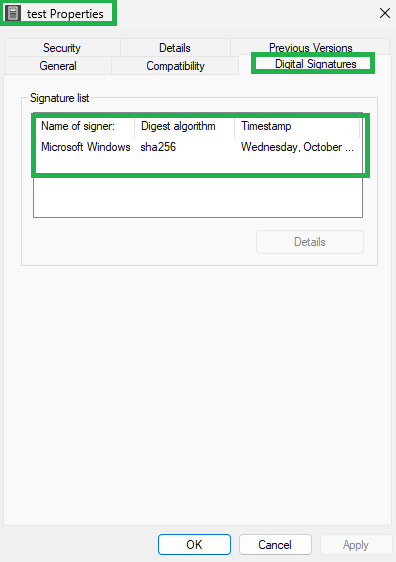


Kernel32.dll dosyasında Microsoft sertifikasını gördüğümüze göre işlemi uygulamaya geçebiliriz. Sigthief toolunu kullanmak için öncelikle cihazınızda Python yüklü olması gerekmektedir ve

**python sigthief.py -i kernel32.dll -t mimikatz.exe -o test.exe**



Kernel32.dll içerisindeki Microsoft sertifikasını kopyalayıp mimikatz.exe dosyasına enjekte etti ve bunuda test.exe olarak kaydetti. Oluşan test.exe dosyasının dijital imzası aşağıdaki gibidir.



Terminalden test.exe dosyasını çalıştırdığımızda mimikatz uygulamamız çalışmış olacaktır.

