Cuckoo ile Volatility'i kullanabilir miyim?

Sürüm 0.5 ile yeni eklenen özellik: Cuckoo, analiz sürecinin sonunda oluşturulan isteğe bağlı memory dump destekler. Bu memory dumpları kullanarak Volatility gibi memory forensic analizlerini gerçekleştirebilirsiniz.

Ayrıca, lütfen bunu özellikle teşvik etmediğimizi göz önünde bulundurun: Cuckoo, işlemlerini gerçekleştirmek için bazı rootkit benzeri teknolojiler kullanır, bu nedenle bir forensic analizin sonuçları, sandbox'ın bileşenleri tarafından kirletilebilir.

Revision #1
Created 7 December 2023 11:39:57 by LastGuard
Updated 7 December 2023 11:41:10 by LastGuard