Abstract

The growing of encryption techniques and the increase of storage capacity make the traditional forensics are inadequate. Therefore as replacement used the live forensics to do the investigation. It technique need special attention, because the volatile data on RAM is very fragile, it can be lost if the system is dead, also there are posibilities of overwriting on the valuable data by the other aplication. Therefore we need the method and live forensics tools that can ensure the integrity of the volatile data without losing the potential evidence.

This thesis analyze and compare the method also live forensics tools that have the best performance to do the live forensics analysis. It is mean the method and tools it must have small memory footprint, does not change file system, high accuracy, fast and easy to use.

The result is the method and tools which have the best performance are the external method using ManTech for the image acquisition tools and Volatility as the analysis tools. It use 24,492 KB of virtual memory, 1,388 KB working sets, write 8 keys on Windows registry with 75% accuration, 311 second and 22 steps to finish the investigation.

Key word: ***live forensics, tools, method, windows xp, memory, investigation***