

ПІДХІД ДО ПРОВЕДЕННЯ ЦИФРОВОЇ ЕКСПЕРТИЗИ ОПЕРАТИВНОЇ ПАМ'ЯТІ КОМП'ЮТЕРІВ В ІНТЕРЕСАХ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

*канд.техн. наук, доц. А.В. Снігуров, магістр М.С. Сірий, Харківський
національний університет радіоелектроніки, м. Харків*

Проведення цифрової експертизи оперативної пам'яті комп'ютеру є одним з основних видів комп'ютерної криміналістики. Оперативна пам'ять (RAM, Random Access Memory) комп'ютерів є потужним джерелом інформації для цифрового криміналіста. Актуальним завданням є створення науково-обґрунтованих методик проведення такої експертизи, розробка рекомендацій для лабораторій цифрової криміналістики, а також для освітнього процесу підготовки студентів з кібербезпеки.

Процес роботи цифрового криміналіста з оперативної пам'яттю комп'ютера поділяється на два етапи: на першому етапі створюється дамп пам'яті, на другому етапі проводиться його аналіз. Перший етап проводиться під час слідчих дій, коли є доступ до працюючого комп'ютера, другий етап проводиться в лабораторії цифрової криміналістики.

В доповіді проведений аналіз різних інструментів для створення дампа пам'яті: AccessData FTK Imager, EnCase/WinEn, ATC-NY Windows Memory Reader, Winpmem, GMG Systems, Inc., KnTTools, F-Response, Mandiant Memoryze, HBGary FastDump.

Для другого етапу цифрової експертизи оперативної пам'яті був проведений аналіз можливостей і результатів практичного використання такого інструменту, як Volatility 2.6 [1]. При цьому були досліджені такі завдання, як отримання списку завантажених DLL для кожного процесу, друк адресів реєстру, отримання інформації про мережеві підключення та останні запущені процеси, а також шляхи до виконуваних файлів, отримання системної інформації, інформації з буферу обміну клавіатури, інформації з робочого стола, інформації щодо підключених пристроїв, інформації про файлову систему, інформації з куца реєстру userassist та інше. Результати дослідження дозволяють перейти к такій фазі цифрової криміналістики, як аналіз кібератак, що є подальшим напрямком дослідження.

Список літератури: 1. Volatility 2.6 (Windows 10 / Server 2016). [Електронний ресурс]. Режим доступу до ресурсу: <https://www.volatilityfoundation.org/26>.