Dumpit

Memory has plenty of useful information for incident handlers such as open files, network connections and encryption keys. With pulling the plug forensics methodology you are losing all this information and you're putting your skills into question if the case go to the court.

While analyzing memory require a set of skills, acquiring memory isn't that difficult with the new tools available. On a previous diary Mark Baggett wrote about using winpmem to acquire memory.

This diary will be about using similar tools which is Dumpit. Dumpit is a free tool written by Matthieu Suiche from MoonSols. Dumpit support both 64-bit and 32-bit Windows operating systems.

More information

https://isc.sans.edu/forums/diary/Acquiring+Memory+Images+with+Dumpit/17216/