goede OpenSource tools

context

dit document geeft enkele goeie OpenSource tools gebruikt voor digitaal forensics

overzicht

- Autopsy
- Foremost (carve data): http://foremost.sourceforge.net/
- network miner: https://sourceforge.net/projects/networkminer/
- wireshark
- registry explorer (lijkt onderdeel te zijn van Eric Zimmerman's Tools)
- Volatility: https://www.volatilityfoundation.org/26
- Dumpit (memory dump): https://zeltser.com/memory-acquisition-with-dumpit-for-dfir-2/

digital forensics, USB