Pretraga po ključnim riječima

U knjizi Unix and Linux Forensic Analysis DVD Toolkit, autor navodi popis ključnih riječi koje pretražuje u svakom forenzičkom slučaju. Navodi se taj popis u svrhu davanja ogledne ideje kako bi trebao izgledati i na što istražitelj treba obratiti pažnju.

File and Directory Names

- grep –e (the "–e" is used here for pattern matching) "\/proc/" –e "\/bin" –e "\/bin\/.*?sh" <filename>
- grep –e "ftp" –e "root" <filename>
- grep –e "rm –r" <filename>
- grep –e ".tgz" <filename>

IP Addresses and Domain Names

- grep –e "[0-9]\+\.[0-9]\+\.[0-9]\+\.[0-9]\+" <filename>
- grep –e "\.pl\" <filename>

Tool Keywords

- msf (Metasploit Framework)
- select
- insert
- dump
- update
- nmap
- nessus
- nikto
- wireshark
- tcpdump
- kismet
- airsnarf
- paros
- hping2
- ettercap
- aircrack
- aircrack-ng
- airsnort
- nc (netcat)