

# 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) “\Vproc/” -e “\Vbin” -e “\Vbin\.*?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
- aircrack-ng
- paros
- hping2
- ettercap
- aircrack
- aircrack-ng
- aircrack-ng
- aircrack-ng
- nc (netcat)

From:

<https://www.cis.hr/WikiS/> - **wikiS**

Permanent link:

[https://www.cis.hr/WikiS/doku.php?id=old\\_zabrisati:keyword\\_search](https://www.cis.hr/WikiS/doku.php?id=old_zabrisati:keyword_search)

Last update: **2015/01/21 13:37**

