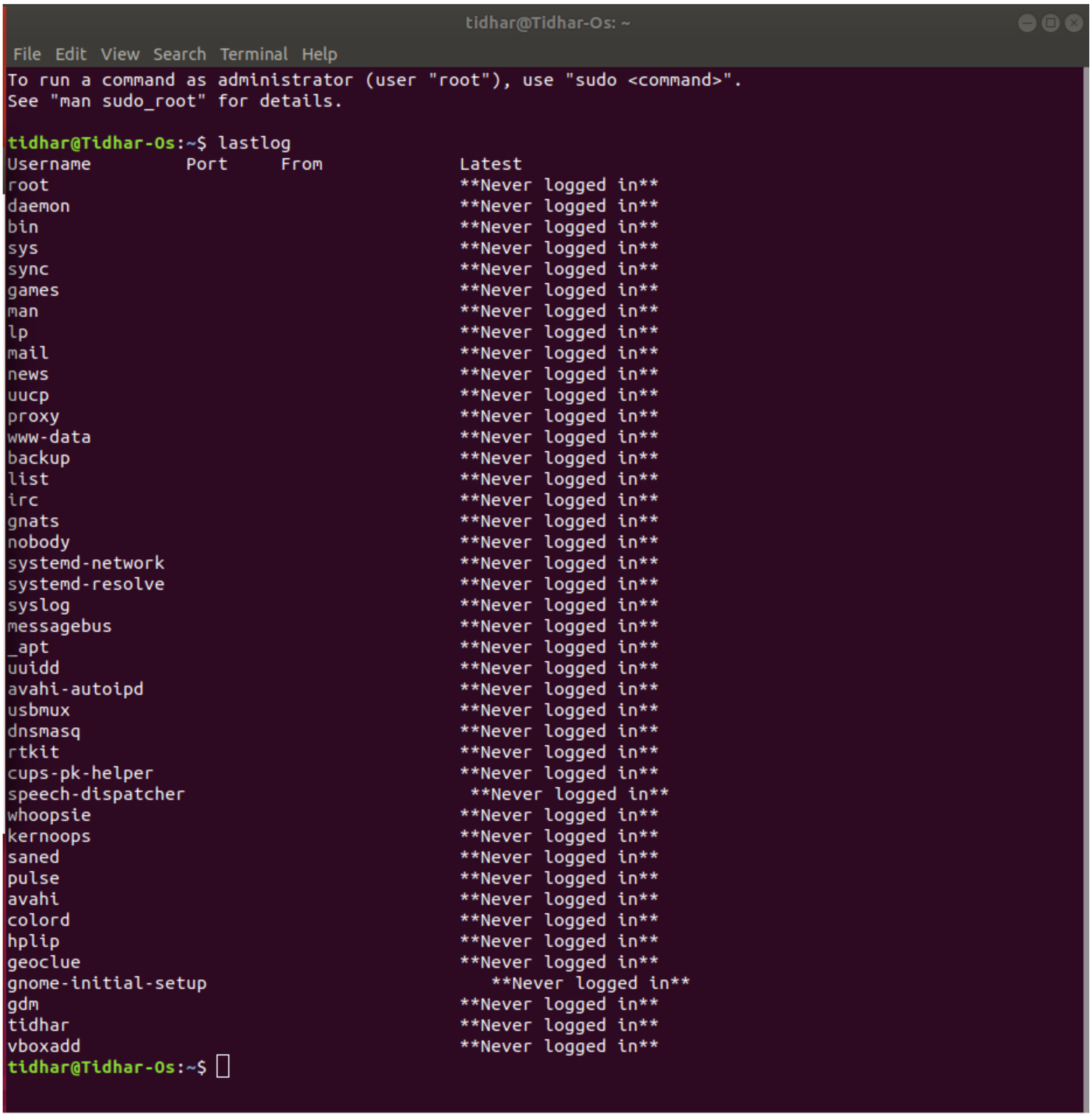
Nama : Tidhar Katon Birowo
NIM : L200170187
Kelas : A

PRAKTIKUM KEAMANAN JARINGAN KOMPUTER
MODUL 3

Percobaan 1

Menggunakkan perintah Lastlog

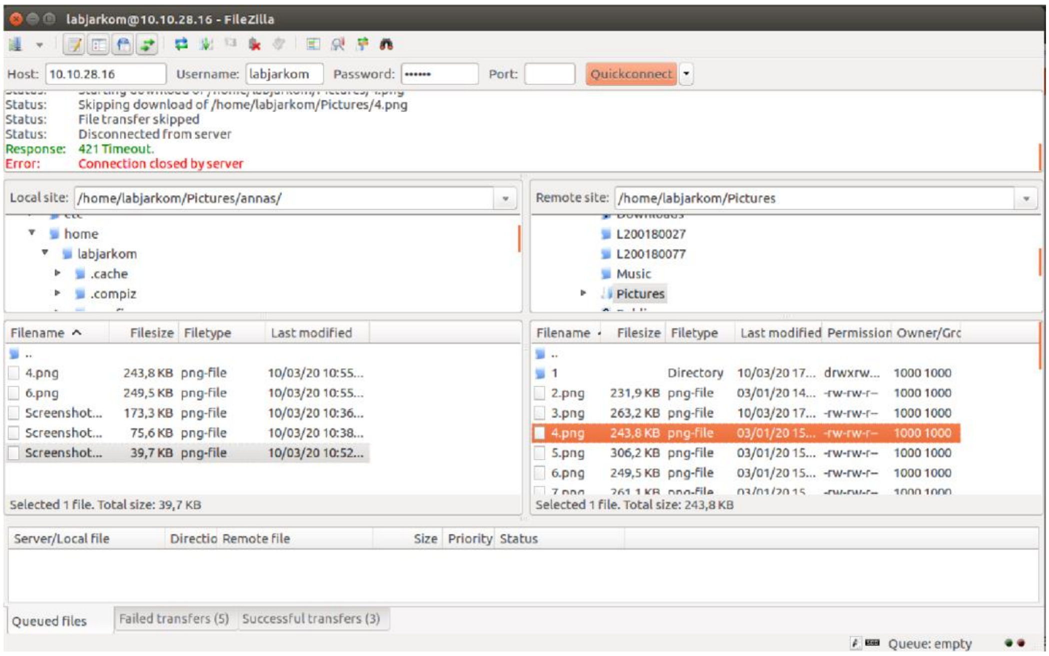


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tidhar@Tidhar-Os:~$ lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
systemd-resolve                            **Never logged in**
syslog                                     **Never logged in**
messagebus                                 **Never logged in**
_apt                                       **Never logged in**
uuidd                                      **Never logged in**
avahi-autoipd                              **Never logged in**
usbmux                                     **Never logged in**
dnsmasq                                    **Never logged in**
rtkit                                      **Never logged in**
cups-pk-helper                             **Never logged in**
speech-dispatcher                           **Never logged in**
whoopsie                                   **Never logged in**
kernoops                                   **Never logged in**
saned                                      **Never logged in**
pulse                                      **Never logged in**
avahi                                      **Never logged in**
colord                                     **Never logged in**
hplip                                      **Never logged in**
geoclue                                    **Never logged in**
gnome-initial-setup                          **Never logged in**
gdm                                        **Never logged in**
tidhar                                     **Never logged in**
vboxadd                                    **Never logged in**
tidhar@Tidhar-Os:~$ 
```

Percobaan 2

Informasi yang pernah login di ftp daemon



Host: 10.10.28.16 Username: labjarkom Password: •••••• Port:

```
Status:     Skipping download of /home/labjarkom/Pictures/4.png
Status:     File transfer skipped
Status:     Disconnected from server
Response:   421 Timeout.
Error:      Connection closed by server
```

Local site: /home/labjarkom/Pictures/annas/

- home
  - labjarkom
    - .cache
    - .compiz

Filename	Filesize	Filetype	Last modified
..			
4.png	243,8 KB	png-file	10/03/20 10:55...
6.png	249,5 KB	png-file	10/03/20 10:55...
Screenshot...	173,3 KB	png-file	10/03/20 10:36...
Screenshot...	75,6 KB	png-file	10/03/20 10:38...
Screenshot...	39,7 KB	png-file	10/03/20 10:52...

Selected 1 file. Total size: 39,7 KB

Remote site: /home/labjarkom/Pictures

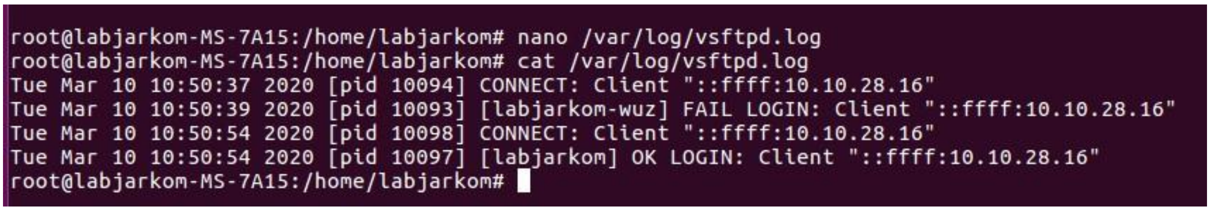
- L200180027
- L200180077
- Music
- Pictures

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grc
..					
1		Directory	10/03/20 17...	drwxrw...	1000 1000
2.png	231,9 KB	png-file	03/01/20 14...	-rw-rw-r--	1000 1000
3.png	263,2 KB	png-file	10/03/20 17...	-rw-rw-r--	1000 1000
4.png	243,8 KB	png-file	03/01/20 15...	-rw-rw-r--	1000 1000
5.png	306,2 KB	png-file	03/01/20 15...	-rw-rw-r--	1000 1000
6.png	249,5 KB	png-file	03/01/20 15...	-rw-rw-r--	1000 1000
7.png	261,1 KB	png-file	03/01/20 15...	-rw-rw-r--	1000 1000

Selected 1 file. Total size: 243,8 KB

Server/Local file	Directio	Remote file	Size	Priority	Status

Vsftpd.log

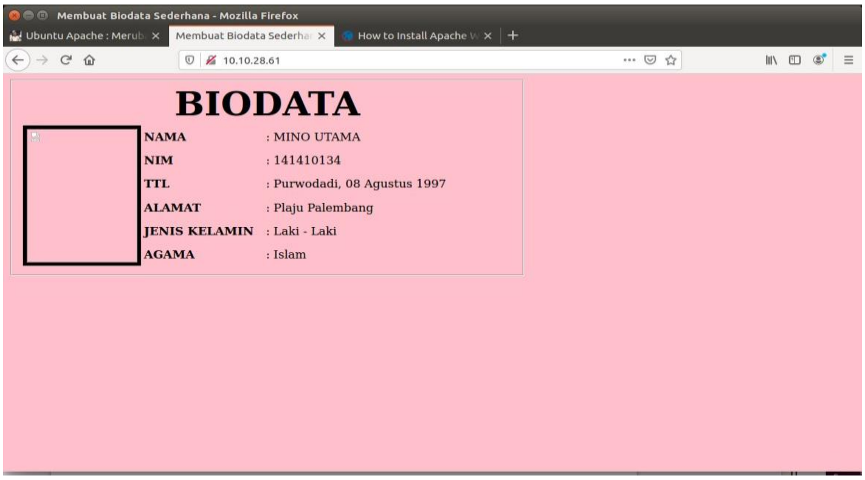


```
root@labjarkom-MS-7A15:/home/labjarkom# nano /var/log/vsftpd.log
root@labjarkom-MS-7A15:/home/labjarkom# cat /var/log/vsftpd.log
Tue Mar 10 10:50:37 2020 [pid 10094] CONNECT: Client "::ffff:10.10.28.16"
Tue Mar 10 10:50:39 2020 [pid 10093] [labjarkom-wuz] FAIL LOGIN: Client "::ffff:10.10.28.16"
Tue Mar 10 10:50:54 2020 [pid 10098] CONNECT: Client "::ffff:10.10.28.16"
Tue Mar 10 10:50:54 2020 [pid 10097] [labjarkom] OK LOGIN: Client "::ffff:10.10.28.16"
root@labjarkom-MS-7A15:/home/labjarkom# 
```

Percobaan 3

Mengamati log pengaksesan sebuah halaman web

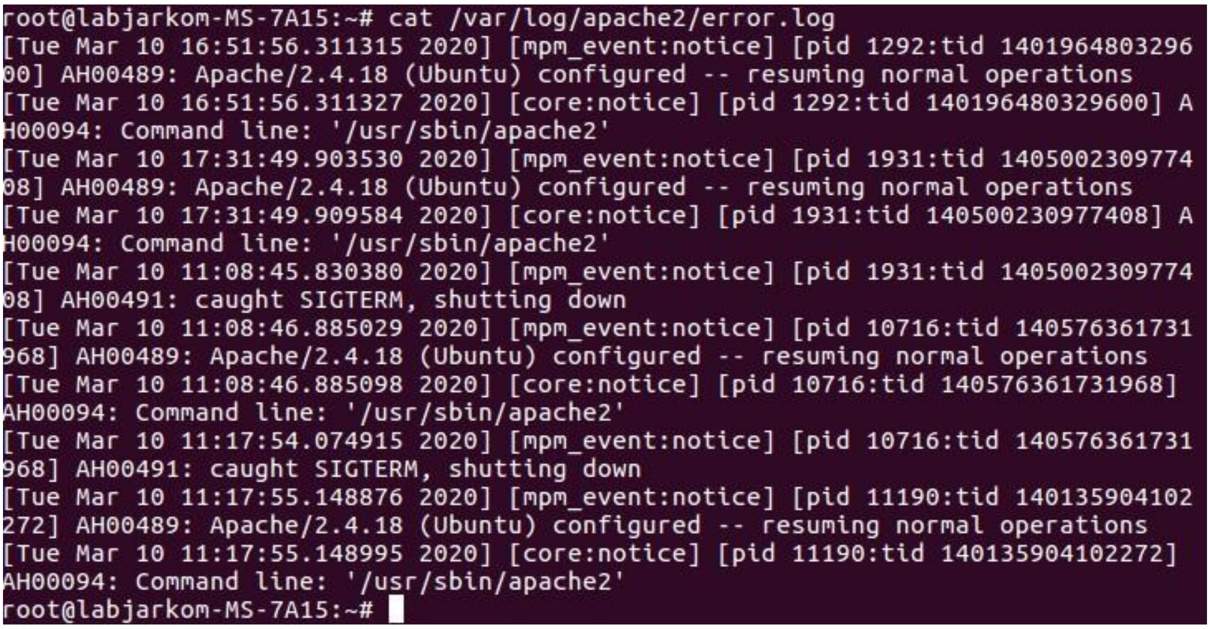
HTTP SERVER



BIODATA

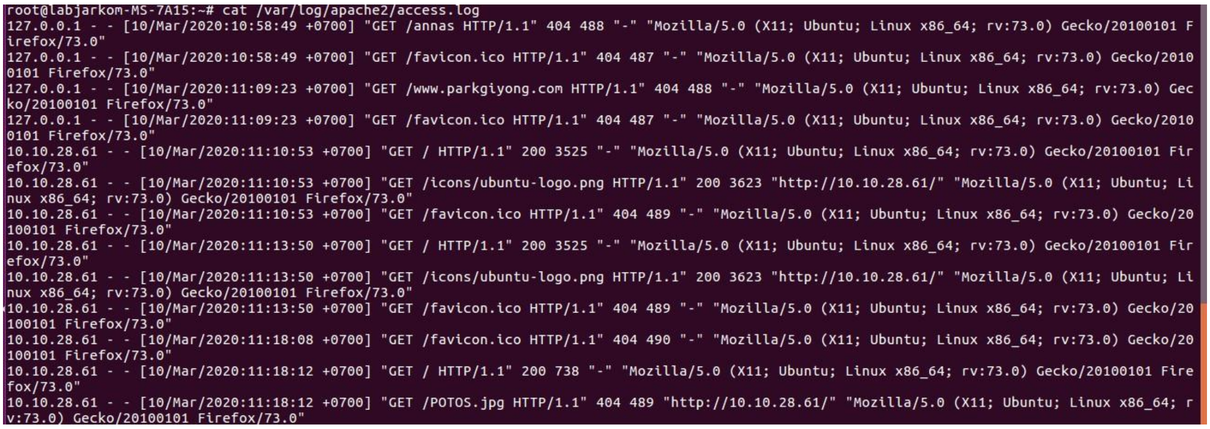
NAMA	: MINO UTAMA
NIM	: 141410134
TTL	: Purwodadi, 08 Agustus 1997
ALAMAT	: Plaju Palembang
JENIS KELAMIN	: Laki - Laki
AGAMA	: Islam

ERROR.LOG



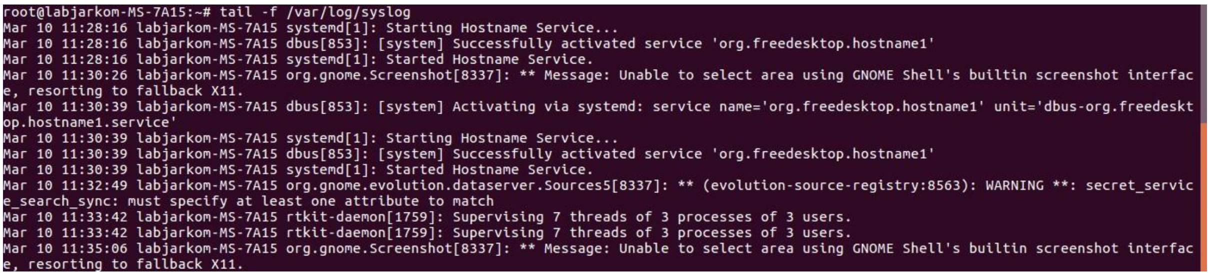
```
root@labjarkom-MS-7A15:~# cat /var/log/apache2/error.log
[Tue Mar 10 16:51:56.311315 2020] [mpm_event:notice] [pid 1292:tid 1401964803296
00] AH00489: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 16:51:56.311327 2020] [core:notice] [pid 1292:tid 140196480329600] A
H00094: Command line: '/usr/sbin/apache2'
[Tue Mar 10 17:31:49.903530 2020] [mpm_event:notice] [pid 1931:tid 1405002309774
08] AH00489: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 17:31:49.909584 2020] [core:notice] [pid 1931:tid 140500230977408] A
H00094: Command line: '/usr/sbin/apache2'
[Tue Mar 10 11:08:45.830380 2020] [mpm_event:notice] [pid 1931:tid 1405002309774
08] AH00491: caught SIGTERM, shutting down
[Tue Mar 10 11:08:46.885029 2020] [mpm_event:notice] [pid 10716:tid 140576361731
968] AH00489: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 11:08:46.885098 2020] [core:notice] [pid 10716:tid 140576361731968]
AH00094: Command line: '/usr/sbin/apache2'
[Tue Mar 10 11:17:54.074915 2020] [mpm_event:notice] [pid 10716:tid 140576361731
968] AH00491: caught SIGTERM, shutting down
[Tue Mar 10 11:17:55.148876 2020] [mpm_event:notice] [pid 11190:tid 140135904102
272] AH00489: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 11:17:55.148995 2020] [core:notice] [pid 11190:tid 140135904102272]
AH00094: Command line: '/usr/sbin/apache2'
root@labjarkom-MS-7A15:~#
```

ACCESS.LOG



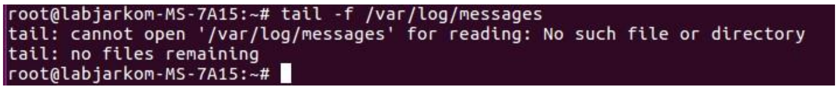
```
root@labjarkom-MS-7A15:~# cat /var/log/apache2/access.log
127.0.0.1 - - [10/Mar/2020:10:58:49 +0700] "GET /annas HTTP/1.1" 404 488 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 F
irefox/73.0"
127.0.0.1 - - [10/Mar/2020:10:58:49 +0700] "GET /favicon.ico HTTP/1.1" 404 487 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/2010
0101 Firefox/73.0"
127.0.0.1 - - [10/Mar/2020:11:09:23 +0700] "GET /www.parkgiyong.com HTTP/1.1" 404 488 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gec
ko/20100101 Firefox/73.0"
127.0.0.1 - - [10/Mar/2020:11:09:23 +0700] "GET /favicon.ico HTTP/1.1" 404 487 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/2010
0101 Firefox/73.0"
10.10.28.61 - - [10/Mar/2020:11:10:53 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Fir
efox/73.0"
10.10.28.61 - - [10/Mar/2020:11:10:53 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://10.10.28.61/" "Mozilla/5.0 (X11; Ubuntu; Li
nux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0"
10.10.28.61 - - [10/Mar/2020:11:10:53 +0700] "GET /favicon.ico HTTP/1.1" 404 489 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20
100101 Firefox/73.0"
10.10.28.61 - - [10/Mar/2020:11:13:50 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Fir
efox/73.0"
10.10.28.61 - - [10/Mar/2020:11:13:50 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://10.10.28.61/" "Mozilla/5.0 (X11; Ubuntu; Li
nux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0"
10.10.28.61 - - [10/Mar/2020:11:13:50 +0700] "GET /favicon.ico HTTP/1.1" 404 489 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20
100101 Firefox/73.0"
10.10.28.61 - - [10/Mar/2020:11:18:08 +0700] "GET /favicon.ico HTTP/1.1" 404 490 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20
100101 Firefox/73.0"
10.10.28.61 - - [10/Mar/2020:11:18:12 +0700] "GET / HTTP/1.1" 200 738 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Fire
fox/73.0"
10.10.28.61 - - [10/Mar/2020:11:18:12 +0700] "GET /POTOS.jpg HTTP/1.1" 404 489 "http://10.10.28.61/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; r
v:73.0) Gecko/20100101 Firefox/73.0"
```

SYSLOG



```
root@labjarkom-MS-7A15:~# tail -f /var/log/syslog
Mar 10 11:28:16 labjarkom-MS-7A15 systemd[1]: Starting Hostname Service...
Mar 10 11:28:16 labjarkom-MS-7A15 dbus[853]: [system] Successfully activated service 'org.freedesktop.hostname1'
Mar 10 11:28:16 labjarkom-MS-7A15 systemd[1]: Started Hostname Service.
Mar 10 11:30:26 labjarkom-MS-7A15 org.gnome.Screenshot[8337]: ** Message: Unable to select area using GNOME Shell's builtin screenshot interfac
e, resorting to fallback X11.
Mar 10 11:30:39 labjarkom-MS-7A15 dbus[853]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedeskt
op.hostname1.service'
Mar 10 11:30:39 labjarkom-MS-7A15 systemd[1]: Starting Hostname Service...
Mar 10 11:30:39 labjarkom-MS-7A15 dbus[853]: [system] Successfully activated service 'org.freedesktop.hostname1'
Mar 10 11:30:39 labjarkom-MS-7A15 systemd[1]: Started Hostname Service.
Mar 10 11:32:49 labjarkom-MS-7A15 org.gnome.evolution.dataserver.Sources5[8337]: ** (evolution-source-registry:8563): WARNING **: secret_servic
e_search_sync: must specify at least one attribute to match
Mar 10 11:33:42 labjarkom-MS-7A15 rtkit-daemon[1759]: Supervising 7 threads of 3 processes of 3 users.
Mar 10 11:33:42 labjarkom-MS-7A15 rtkit-daemon[1759]: Supervising 7 threads of 3 processes of 3 users.
Mar 10 11:35:06 labjarkom-MS-7A15 org.gnome.Screenshot[8337]: ** Message: Unable to select area using GNOME Shell's builtin screenshot interfac
e, resorting to fallback X11.
```

MESSAGES



```
root@labjarkom-MS-7A15:~# tail -f /var/log/messages
tail: cannot open '/var/log/messages' for reading: No such file or directory
tail: no files remaining
root@labjarkom-MS-7A15:~#
```