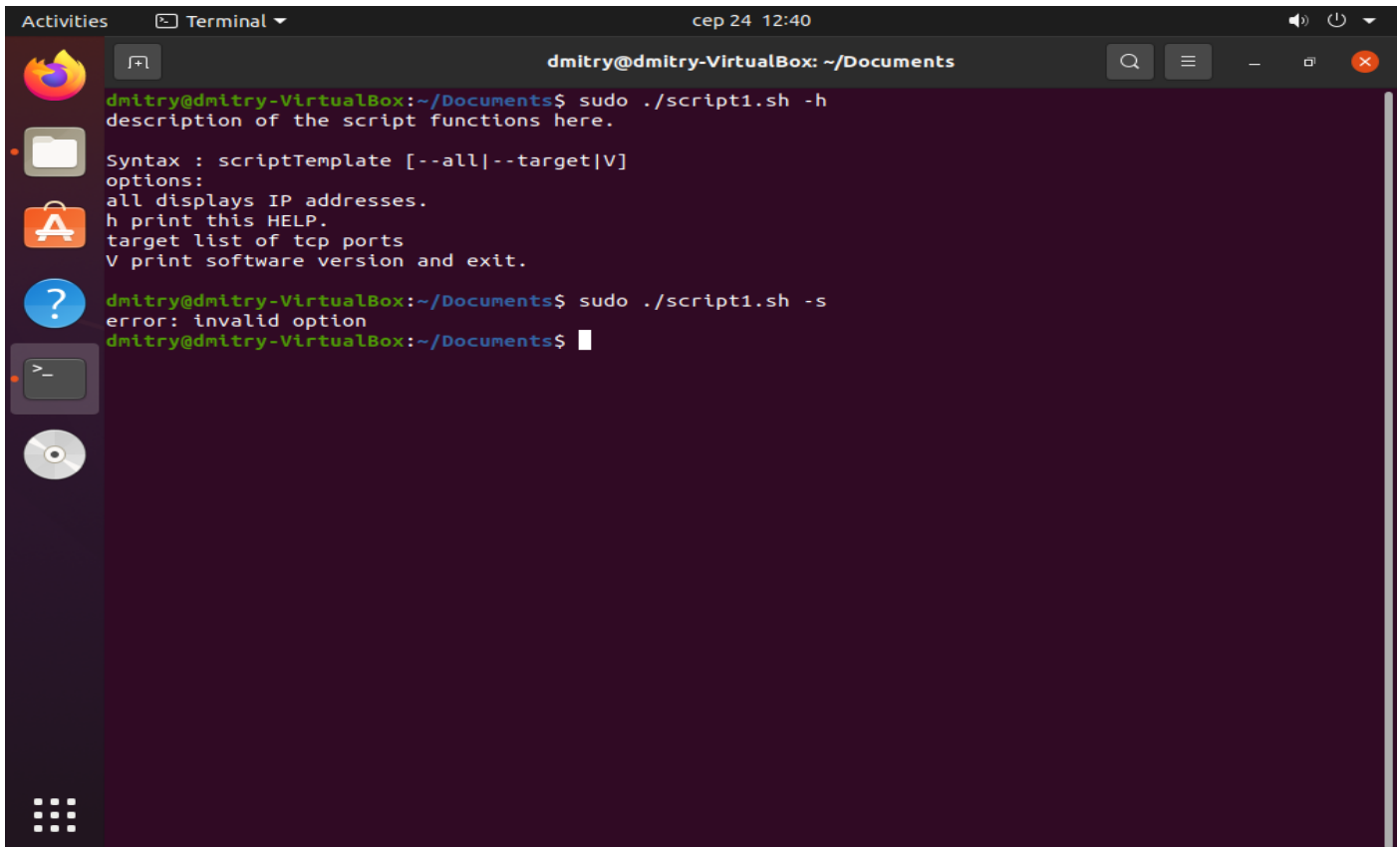


Linux administration with bash

PART 1

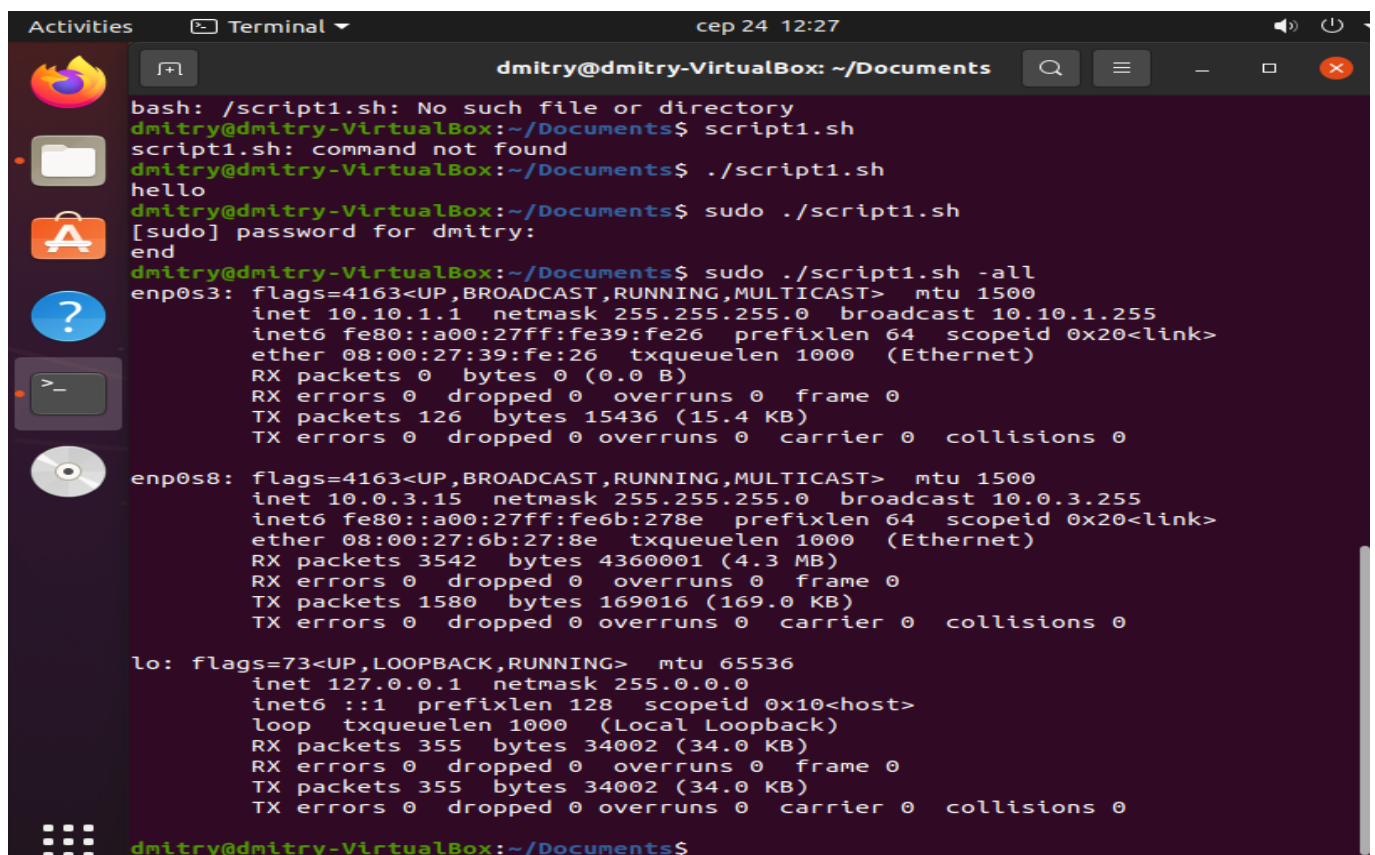
A terminal window titled 'Terminal' with the address bar showing 'dmitry@dmitry-VirtualBox: ~/Documents'. The terminal shows the execution of a script with the -h flag to display help. The output lists the syntax and options for the script.

```
dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script1.sh -h
description of the script functions here.

Syntax : scriptTemplate [--all|--target[V]
options:
all displays IP addresses.
h print this HELP.
target list of tcp ports
V print software version and exit.

dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script1.sh -s
error: invalid option
dmitry@dmitry-VirtualBox:~/Documents$
```

Screenshot 1 – help для скрипта

A terminal window titled 'Terminal' with the address bar showing 'dmitry@dmitry-VirtualBox: ~/Documents'. The terminal shows the execution of a script with the -all flag. The output displays network statistics for three interfaces: enp0s3, enp0s8, and lo.

```
bash: ./script1.sh: No such file or directory
dmitry@dmitry-VirtualBox:~/Documents$ script1.sh
script1.sh: command not found
dmitry@dmitry-VirtualBox:~/Documents$ ./script1.sh
hello
dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script1.sh
[sudo] password for dmitry:
end
dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script1.sh -all
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.1.1 netmask 255.255.255.0 broadcast 10.10.1.255
inet6 fe80::a00:27ff:fe39:fe26 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:39:fe:26 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 126 bytes 15436 (15.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
inet6 fe80::a00:27ff:fe6b:278e prefixlen 64 scopeid 0x20<link>
ether 08:00:27:6b:27:8e txqueuelen 1000 (Ethernet)
RX packets 3542 bytes 4360001 (4.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1580 bytes 169016 (169.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 355 bytes 34002 (34.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 355 bytes 34002 (34.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

dmitry@dmitry-VirtualBox:~/Documents$
```

Screenshot 2 – -all параметр для скрипта

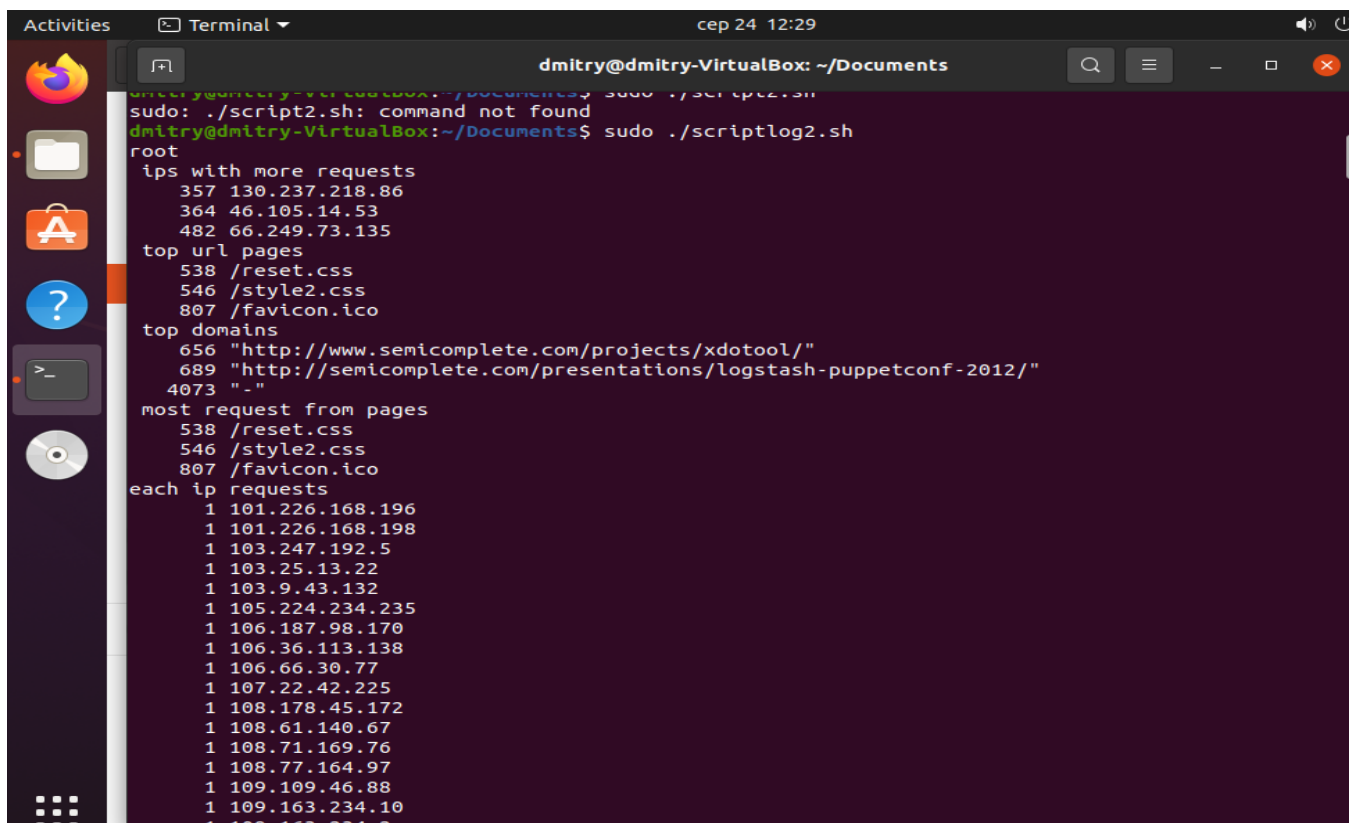
```
Activities Terminal cep 24 12:28
dmitry@dmitry-VirtualBox: ~/Documents

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 355 bytes 34002 (34.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 355 bytes 34002 (34.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script1.sh -t
end
dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script1.sh -target
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 10.10.1.1:53            0.0.0.0:*               LISTEN      670/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      670/named
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      492/systemd-resol
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN      632/cupsd
tcp        0      0 127.0.0.1:953          0.0.0.0:*               LISTEN      670/named
tcp6       0      0 fe80::a00:27ff:fe6b::53 :::*                   LISTEN      670/named
tcp6       0      0 fe80::a00:27ff:fe39::53 :::*                   LISTEN      670/named
tcp6       0      0 ::1:53                 :::*                   LISTEN      670/named
tcp6       0      0 ::1:631                 :::*                   LISTEN      632/cupsd
tcp6       0      0 ::1:953                 :::*                   LISTEN      670/named
dmitry@dmitry-VirtualBox:~/Documents$
```

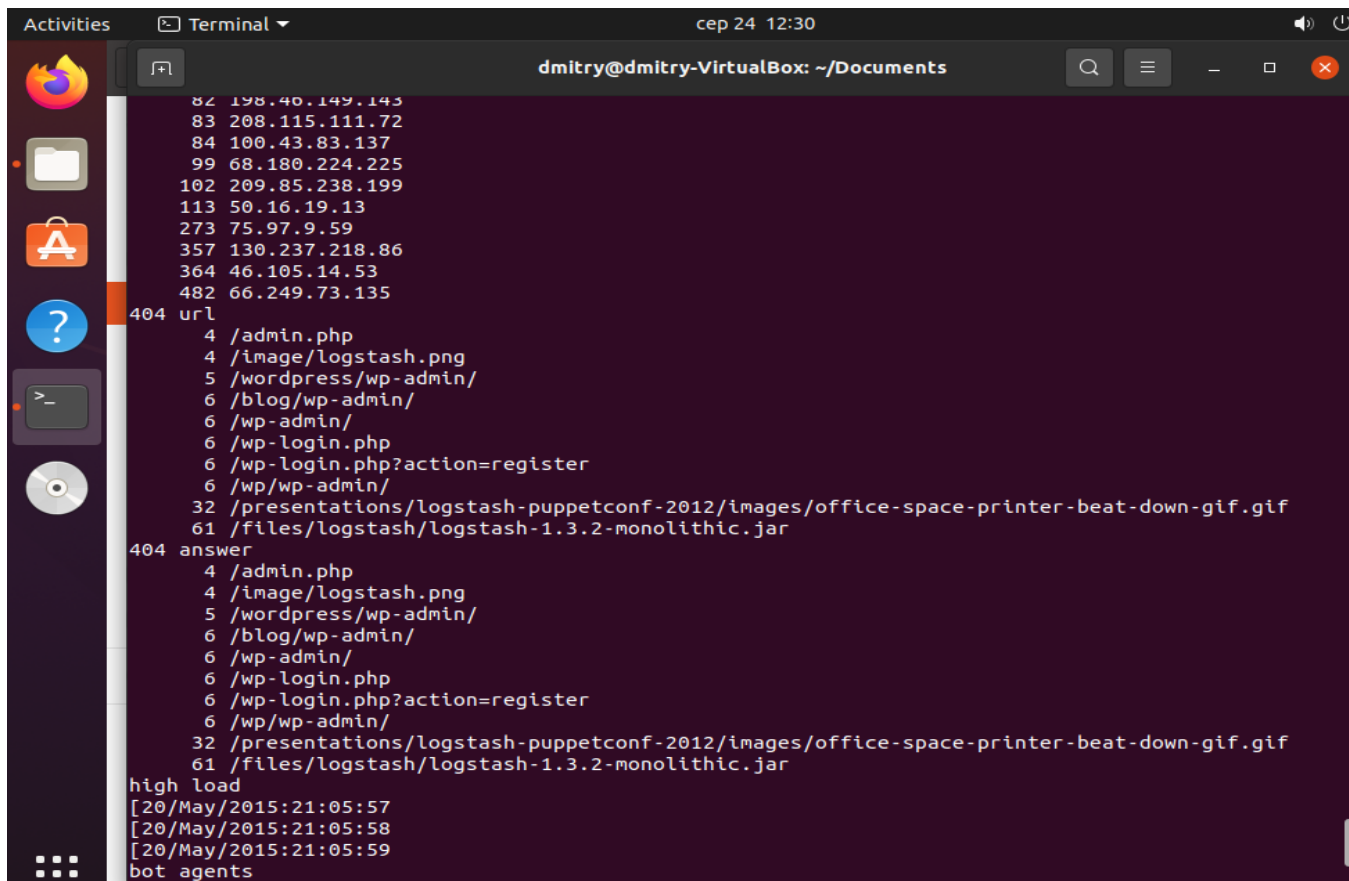
Screenshot 3 – -target параметр для скрипта

PART 2



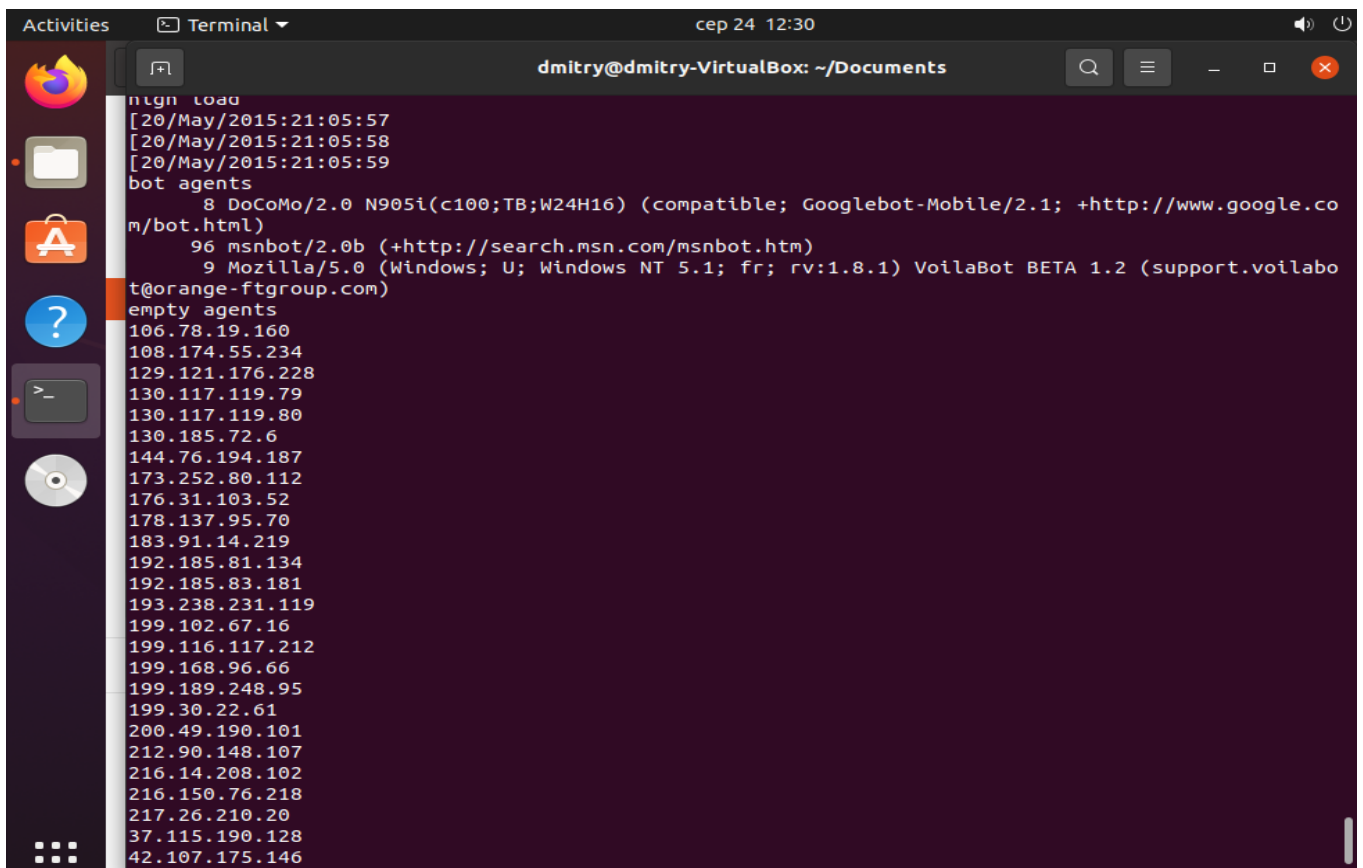
```
dmitry@dmitry-VirtualBox: ~/Documents
dmitry@dmitry-VirtualBox:~/Documents$ sudo ./script2.sh
sudo: ./script2.sh: command not found
dmitry@dmitry-VirtualBox:~/Documents$ sudo ./scriptlog2.sh
root
ips with more requests
357 130.237.218.86
364 46.105.14.53
482 66.249.73.135
top url pages
538 /reset.css
546 /style2.css
807 /favicon.ico
top domains
656 "http://www.semicomplete.com/projects/xdotool/"
689 "http://semicomplete.com/presentations/logstash-puppetconf-2012/"
4073 "-"
most request from pages
538 /reset.css
546 /style2.css
807 /favicon.ico
each ip requests
1 101.226.168.196
1 101.226.168.198
1 103.247.192.5
1 103.25.13.22
1 103.9.43.132
1 105.224.234.235
1 106.187.98.170
1 106.36.113.138
1 106.66.30.77
1 107.22.42.225
1 108.178.45.172
1 108.61.140.67
1 108.71.169.76
1 108.77.164.97
1 109.109.46.88
1 109.163.234.10
1 109.163.234.2
```

Screenshot 4 – выполнение скрипта и отображение наибольшего количества запросов



```
82 198.40.149.143
83 208.115.111.72
84 100.43.83.137
99 68.180.224.225
102 209.85.238.199
113 50.16.19.13
273 75.97.9.59
357 130.237.218.86
364 46.105.14.53
482 66.249.73.135
404 url
4 /admin.php
4 /image/logstash.png
5 /wordpress/wp-admin/
6 /blog/wp-admin/
6 /wp-admin/
6 /wp-login.php
6 /wp-login.php?action=register
6 /wp/wp-admin/
32 /presentations/logstash-puppetconf-2012/images/office-space-printer-beat-down-gif.gif
61 /files/logstash/logstash-1.3.2-monolithic.jar
404 answer
4 /admin.php
4 /image/logstash.png
5 /wordpress/wp-admin/
6 /blog/wp-admin/
6 /wp-admin/
6 /wp-login.php
6 /wp-login.php?action=register
6 /wp/wp-admin/
32 /presentations/logstash-puppetconf-2012/images/office-space-printer-beat-down-gif.gif
61 /files/logstash/logstash-1.3.2-monolithic.jar
high load
[20/May/2015:21:05:57
[20/May/2015:21:05:58
[20/May/2015:21:05:59
bot agents
```

Screenshot 5 – Отображение 404 ошибок и времени высокой нагрузки

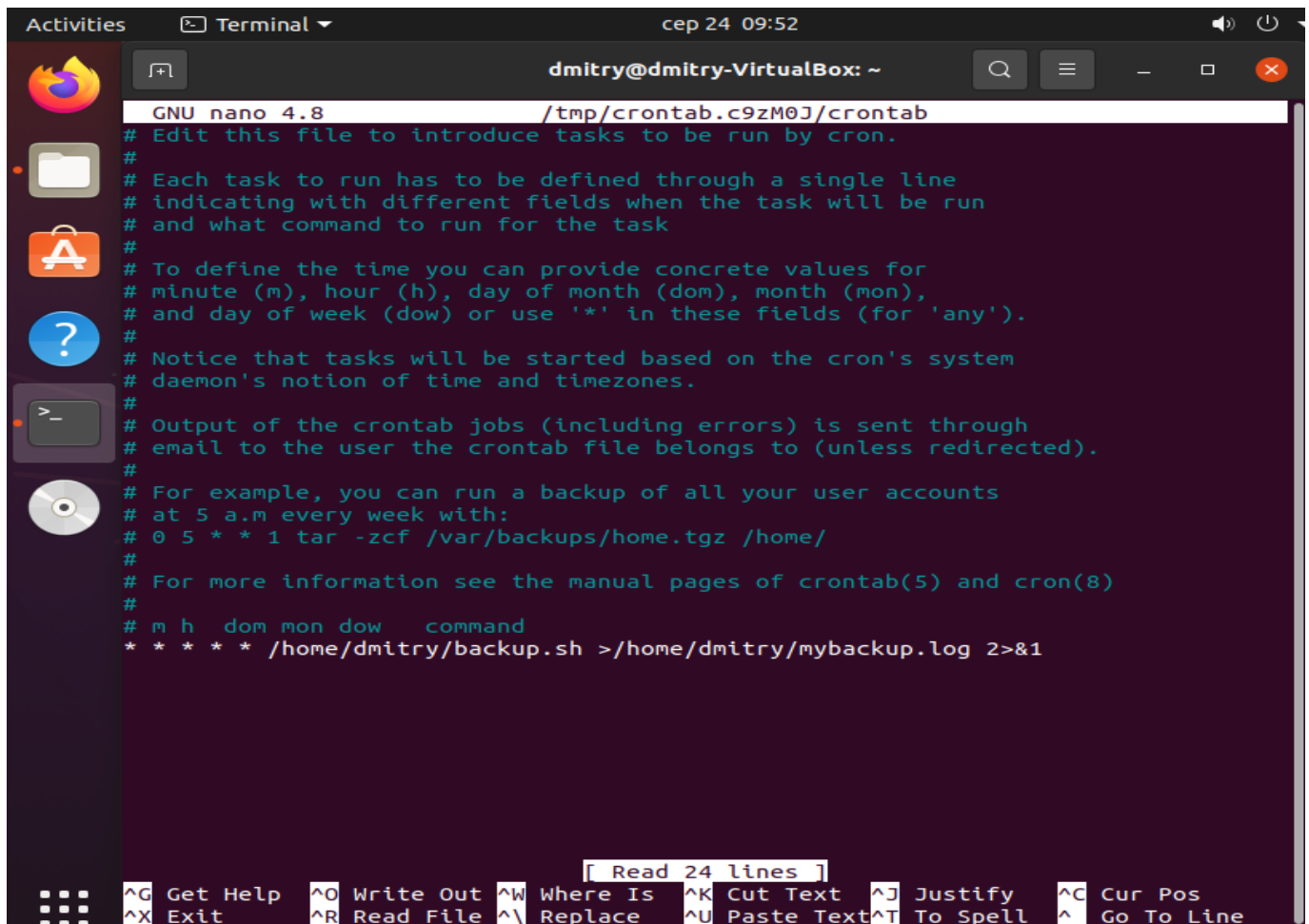


The screenshot shows a terminal window titled "Terminal" with the user "dmitry@dmitry-VirtualBox" in the directory "~/Documents". The terminal output displays the results of a command, likely related to network scanning or bot detection. It lists search bots and empty agents with their respective IP addresses.

```
ntgn load
[20/May/2015:21:05:57
[20/May/2015:21:05:58
[20/May/2015:21:05:59
bot agents
  8 DoCoMo/2.0 N905i(c100;TB;W24H16) (compatible; Googlebot-Mobile/2.1; +http://www.google.co
m/bot.html)
  96 msnbot/2.0b (+http://search.msn.com/msnbot.htm)
  9 Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.8.1) VoilaBot BETA 1.2 (support.voilabo
t@orange-ftgroup.com)
empty agents
106.78.19.160
108.174.55.234
129.121.176.228
130.117.119.79
130.117.119.80
130.185.72.6
144.76.194.187
173.252.80.112
176.31.103.52
178.137.95.70
183.91.14.219
192.185.81.134
192.185.83.181
193.238.231.119
199.102.67.16
199.116.117.212
199.168.96.66
199.189.248.95
199.30.22.61
200.49.190.101
212.90.148.107
216.14.208.102
216.150.76.218
217.26.210.20
37.115.190.128
42.107.175.146
```

Screenshot 6 – Отображение поисковых ботов и ip пустых агентов

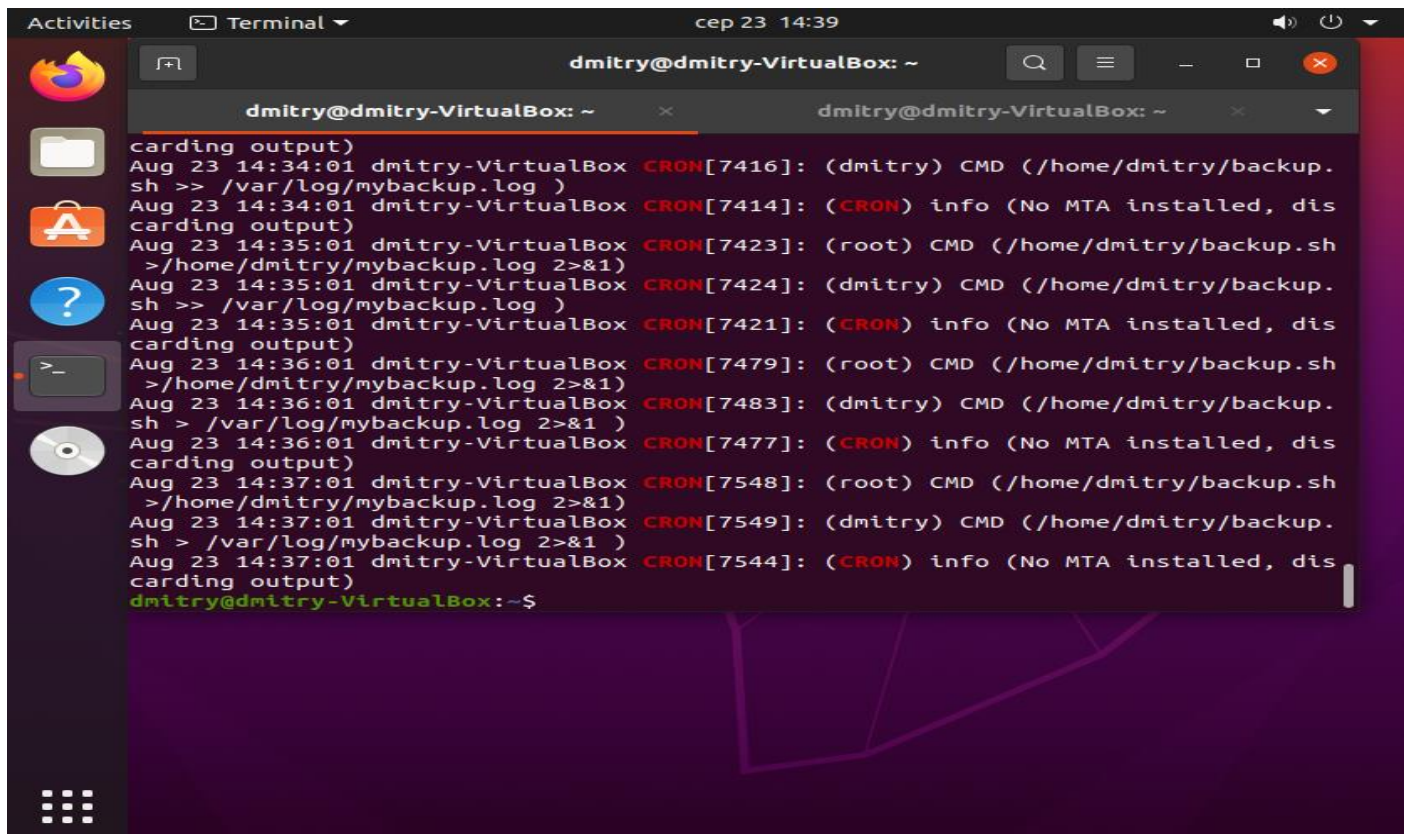
Part 3



```
Activities Terminal cep 24 09:52
dmitry@dmitry-VirtualBox: ~
GNU nano 4.8 /tmp/crontab.c9zM0J/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
* * * * * /home/dmitry/backup.sh >/home/dmitry/mybackup.log 2>&1

[ Read 24 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

Screenshot 7- Crontab запуск скрипта каждую минуту и запись лог файла



```
Activities Terminal cep 23 14:39
dmitry@dmitry-VirtualBox: ~
dmitry@dmitry-VirtualBox: ~
carding output)
Aug 23 14:34:01 dmitry-VirtualBox CRON[7416]: (dmitry) CMD (/home/dmitry/backup.
sh >> /var/log/mybackup.log )
Aug 23 14:34:01 dmitry-VirtualBox CRON[7414]: (CRON) info (No MTA installed, dis
carding output)
Aug 23 14:35:01 dmitry-VirtualBox CRON[7423]: (root) CMD (/home/dmitry/backup.sh
>/home/dmitry/mybackup.log 2>&1)
Aug 23 14:35:01 dmitry-VirtualBox CRON[7424]: (dmitry) CMD (/home/dmitry/backup.
sh >> /var/log/mybackup.log )
Aug 23 14:35:01 dmitry-VirtualBox CRON[7421]: (CRON) info (No MTA installed, dis
carding output)
Aug 23 14:36:01 dmitry-VirtualBox CRON[7479]: (root) CMD (/home/dmitry/backup.sh
>/home/dmitry/mybackup.log 2>&1)
Aug 23 14:36:01 dmitry-VirtualBox CRON[7483]: (dmitry) CMD (/home/dmitry/backup.
sh > /var/log/mybackup.log 2>&1 )
Aug 23 14:36:01 dmitry-VirtualBox CRON[7477]: (CRON) info (No MTA installed, dis
carding output)
Aug 23 14:37:01 dmitry-VirtualBox CRON[7548]: (root) CMD (/home/dmitry/backup.sh
>/home/dmitry/mybackup.log 2>&1)
Aug 23 14:37:01 dmitry-VirtualBox CRON[7549]: (dmitry) CMD (/home/dmitry/backup.
sh > /var/log/mybackup.log 2>&1 )
Aug 23 14:37:01 dmitry-VirtualBox CRON[7544]: (CRON) info (No MTA installed, dis
carding output)
dmitry@dmitry-VirtualBox:~$
```

Screenshot 8- Grep cron из лог файла