O **GoAccess** é uma excelente ferramenta para analisar **Logs** em tempo real, além de contar com uma interface amigável e com informações relevantes ainda pode ser acessada via **Console** ou pelo **Navegador**.

Projeto : github.com/allinurl/goaccess

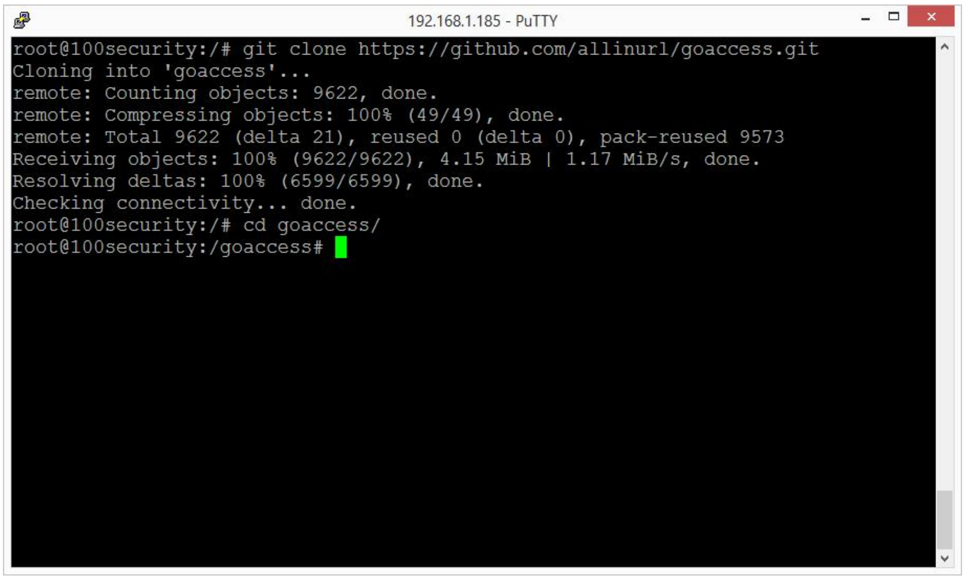
01 - Passo

Realize o clone do **GoAccess** e entre dentro do diretório **goaccess**.

Linux

git clone https://github.com/allinurl/goaccess

cd goaccess/



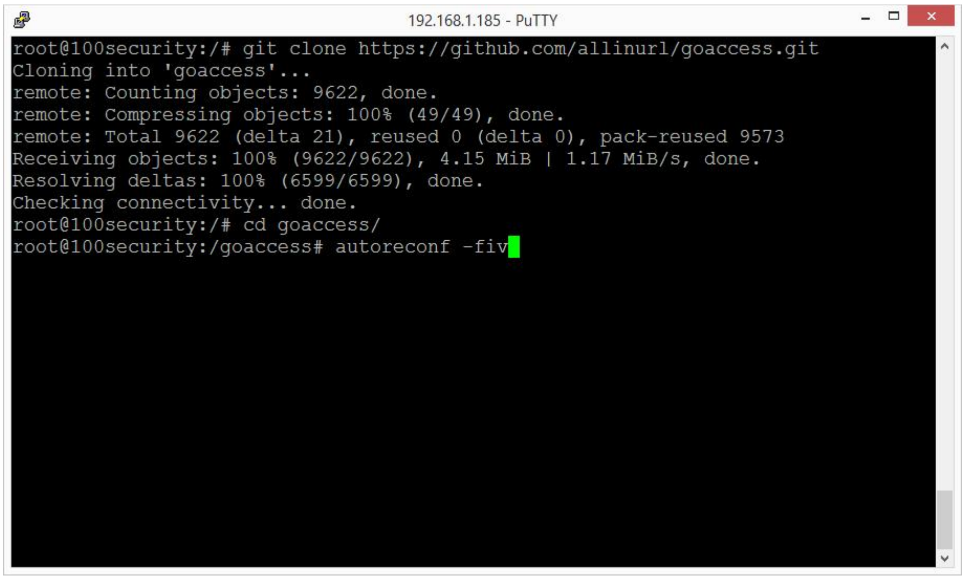
```
root@100security:/# git clone https://github.com/allinurl/goaccess.git
Cloning into 'goaccess'...
remote: Counting objects: 9622, done.
remote: Compressing objects: 100% (49/49), done.
remote: Total 9622 (delta 21), reused 0 (delta 0), pack-reused 9573
Receiving objects: 100% (9622/9622), 4.15 MiB | 1.17 MiB/s, done.
Resolving deltas: 100% (6599/6599), done.
Checking connectivity... done.
root@100security:/# cd goaccess/
root@100security:/goaccess#
```

02 - Passo

Execute o comando **autoreconf -fiv**.

Linux

autoreconf -fiv



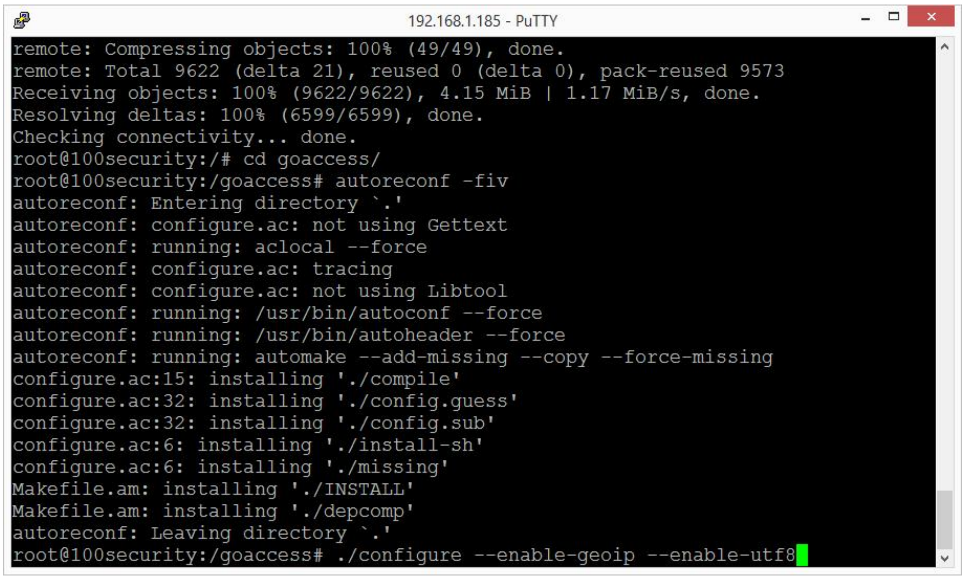
```
root@100security:/# git clone https://github.com/allinurl/goaccess.git
Cloning into 'goaccess'...
remote: Counting objects: 9622, done.
remote: Compressing objects: 100% (49/49), done.
remote: Total 9622 (delta 21), reused 0 (delta 0), pack-reused 9573
Receiving objects: 100% (9622/9622), 4.15 MiB | 1.17 MiB/s, done.
Resolving deltas: 100% (6599/6599), done.
Checking connectivity... done.
root@100security:/# cd goaccess/
root@100security:/goaccess# autoreconf -fiv
```

03 - Passo

Execute o comando de configuração habilitando o **geoip** e **utf-8**.

Linux

./configure —-enable-geoip —-enable-utf-8



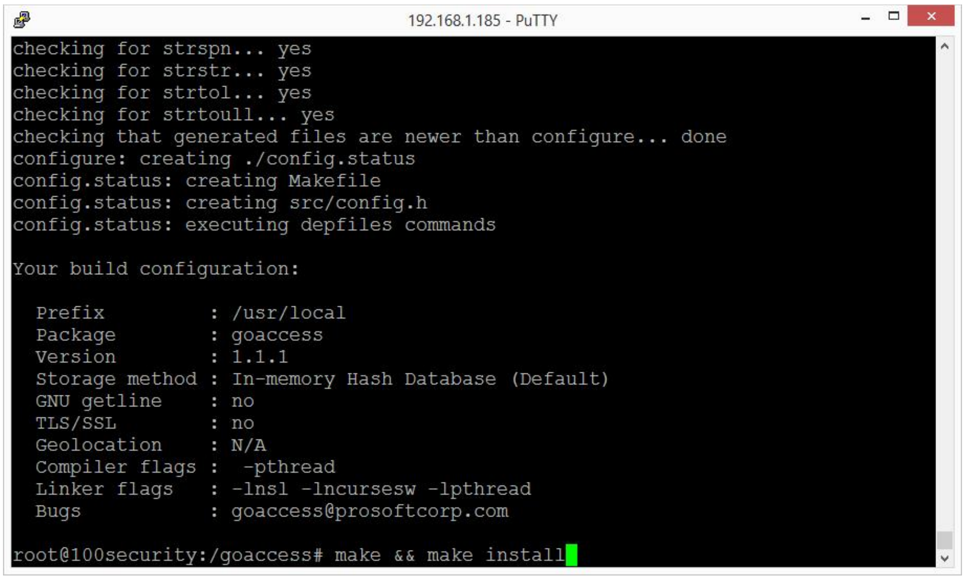
```
remote: Compressing objects: 100% (49/49), done.
remote: Total 9622 (delta 21), reused 0 (delta 0), pack-reused 9573
Receiving objects: 100% (9622/9622), 4.15 MiB | 1.17 MiB/s, done.
Resolving deltas: 100% (6599/6599), done.
Checking connectivity... done.
root@100security:/# cd goaccess/
root@100security:/goaccess# autoreconf -fiv
autoreconf: Entering directory `.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force
autoreconf: configure.ac: tracing
autoreconf: configure.ac: not using Libtool
autoreconf: running: /usr/bin/autoconf --force
autoreconf: running: /usr/bin/autoheader --force
autoreconf: running: automake --add-missing --copy --force-missing
configure.ac:15: installing './compile'
configure.ac:32: installing './config.guess'
configure.ac:32: installing './config.sub'
configure.ac:6: installing './install-sh'
configure.ac:6: installing './missing'
Makefile.am: installing './INSTALL'
Makefile.am: installing './depcomp'
autoreconf: Leaving directory `.'
root@100security:/goaccess# ./configure --enable-geoip --enable-utf8
```

04 - Passo

Execute os comando **make e make install** para realizar a instalação.

Linux

make && make install



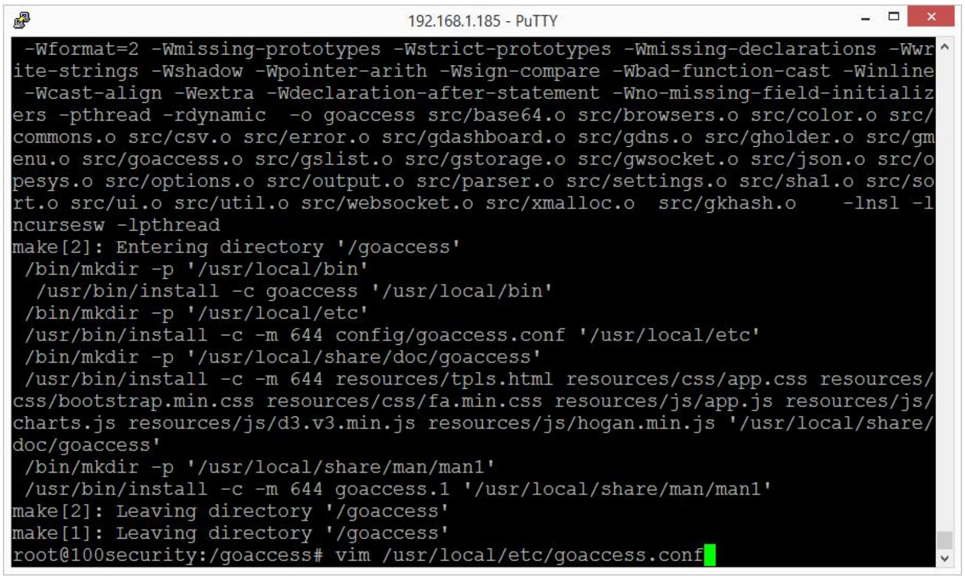
```
checking for strspn... yes
checking for strstr... yes
checking for strtol... yes
checking for strtoull... yes
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating Makefile
config.status: creating src/config.h
config.status: executing depfiles commands

Your build configuration:

  Prefix         : /usr/local
  Package        : goaccess
  Version        : 1.1.1
  Storage method : In-memory Hash Database (Default)
  GNU getline    : no
  TLS/SSL        : no
  Geolocation    : N/A
  Compiler flags :  -pthread
  Linker flags   : -lnsl -lncursesw -lpthread
  Bugs           : goaccess@prosoftcorp.com

root@100security:/goaccess# make && make install
```

05 - Passo

Edite o arquivo de configurações **goaccess.conf**.

Linux

vim /usr/local/etc/goaccess.conf



```
 -Wformat=2 -Wmissing-prototypes -Wstrict-prototypes -Wmissing-declarations -Wwr
ite-strings -Wshadow -Wpointer-arith -Wsign-compare -Wbad-function-cast -Winline
 -Wcast-align -Wextra -Wdeclaration-after-statement -Wno-missing-field-initializ
ers -pthread -rdynamic  -o goaccess src/base64.o src/browsers.o src/color.o src/
commons.o src/csv.o src/error.o src/gdashboard.o src/gdns.o src/gholder.o src/gm
enu.o src/goaccess.o src/gslist.o src/gstorage.o src/gwsocket.o src/json.o src/o
pesys.o src/options.o src/output.o src/parser.o src/settings.o src/sha1.o src/so
rt.o src/ui.o src/util.o src/websocket.o src/xmalloc.o  src/gkhash.o    -lnsl -l
ncursesw -lpthread
make[2]: Entering directory '/goaccess'
 /bin/mkdir -p '/usr/local/bin'
  /usr/bin/install -c goaccess '/usr/local/bin'
 /bin/mkdir -p '/usr/local/etc'
 /usr/bin/install -c -m 644 config/goaccess.conf '/usr/local/etc'
 /bin/mkdir -p '/usr/local/share/doc/goaccess'
 /usr/bin/install -c -m 644 resources/tpls.html resources/css/app.css resources/
css/bootstrap.min.css resources/css/fa.min.css resources/js/app.js resources/js/
charts.js resources/js/d3.v3.min.js resources/js/hogan.min.js '/usr/local/share/
doc/goaccess'
 /bin/mkdir -p '/usr/local/share/man/man1'
 /usr/bin/install -c -m 644 goaccess.1 '/usr/local/share/man/man1'
make[2]: Leaving directory '/goaccess'
make[1]: Leaving directory '/goaccess'
root@100security:/goaccess# vim /usr/local/etc/goaccess.conf
```

06 - Passo

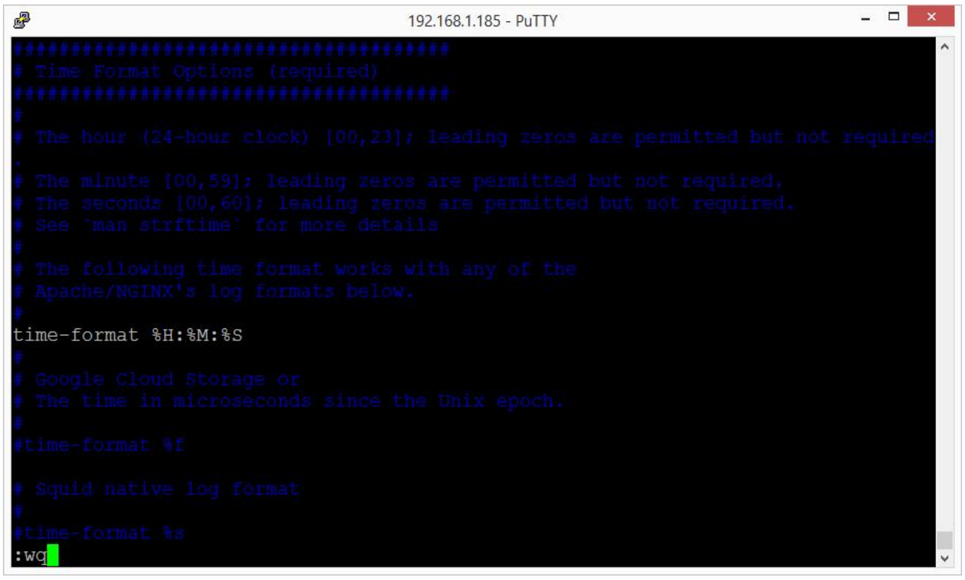
Descomente as linhas **(13, 36 e 70)**.

Linux

```
# Apache/NGINX's log formats below.
#
time-format %H:%M:%S
```

```
# Apache/NGINX's log formats below.
#
date-format %d/%b/%Y
```

# Common Log Format (CLF)
log-format %h %^[%d:%t %^] "%r" %s %b



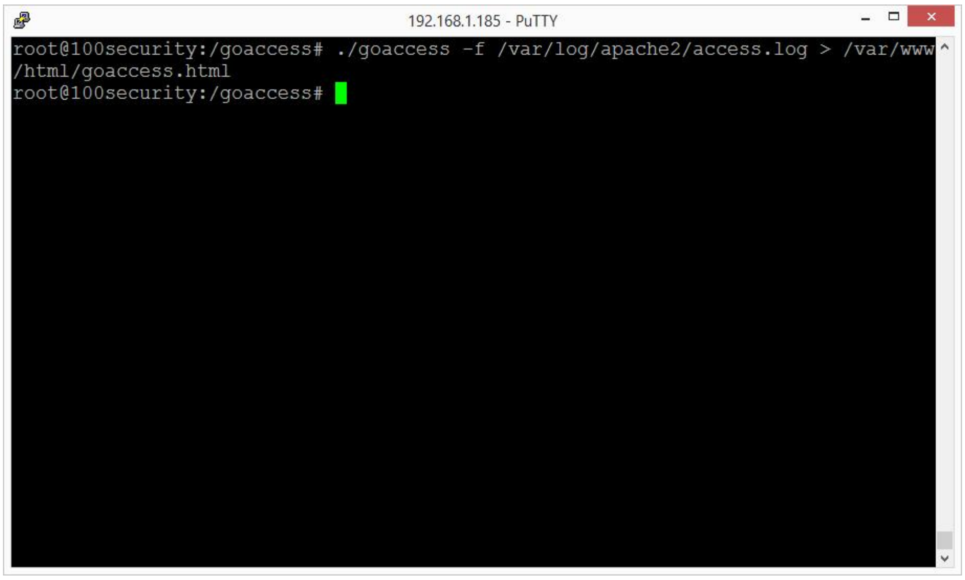
```
######################################
# Time Format Options (required)
######################################
#
# The hour (24-hour clock) [00,23]; leading zeros are permitted but not required
.
# The minute [00,59]; leading zeros are permitted but not required.
# The seconds [00,60]; leading zeros are permitted but not required.
# See `man strftime` for more details
#
# The following time format works with any of the
# Apache/NGINX's log formats below.
#
time-format %H:%M:%S
#
# Google Cloud Storage or
# The time in microseconds since the Unix epoch.
#
#time-format %f

# Squid native log format
#
#time-format %s
:wq
```

07 - Passo

Gerar o **relatório** no formato **HTML** do Log de **Acesso do Apache**.

Linux

./goaccess -f /var/log/apache2/access.log > /var/www/html/goaccess.html

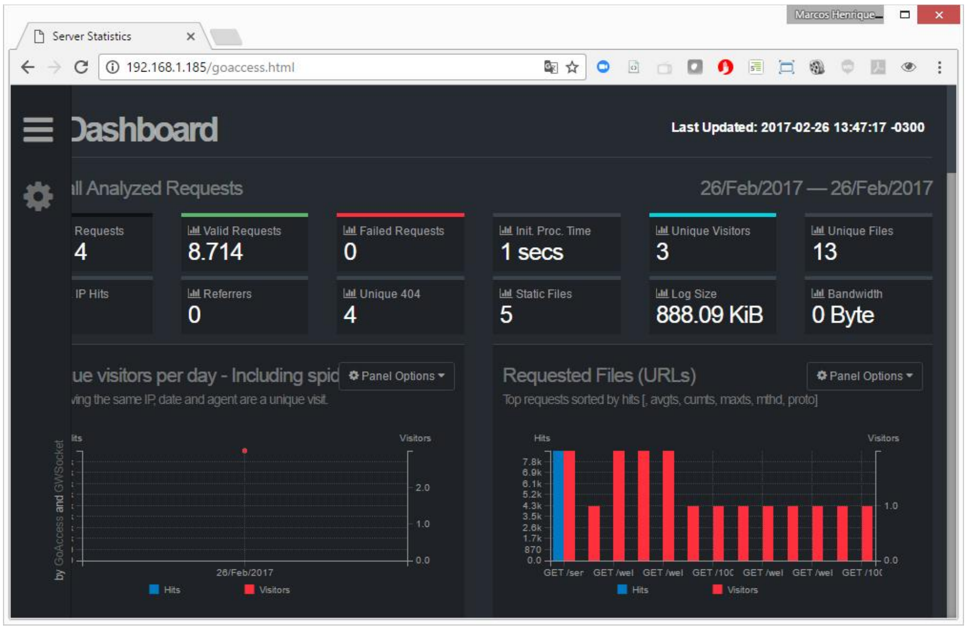


```
root@100security:/goaccess# ./goaccess -f /var/log/apache2/access.log > /var/www
/html/goaccess.html
root@100security:/goaccess# 
```

08 - Passo

Acesse o arquivo **HTML** através do navegador.

http://ip-do-servidor/goaccess.html

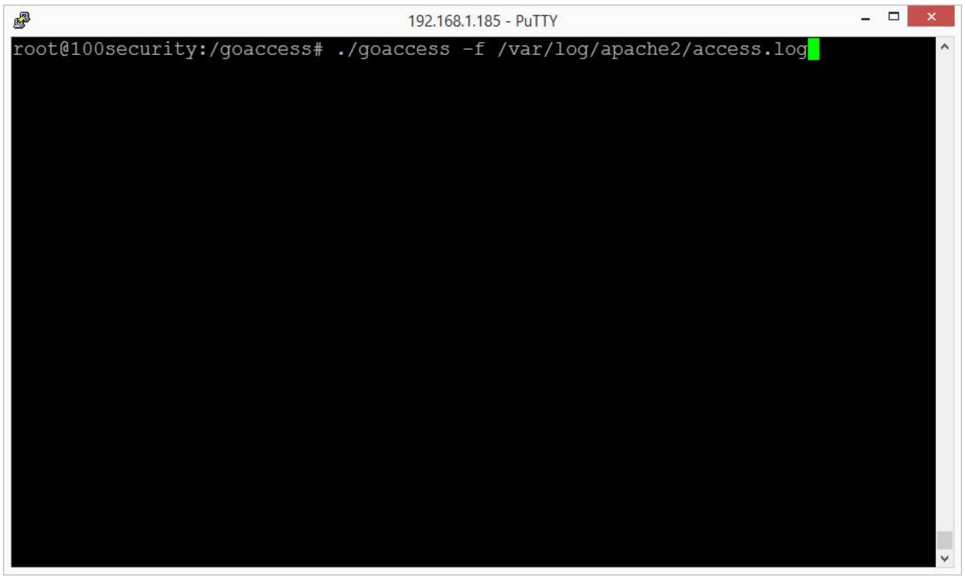


Acesso via Console

Execute o **GoAccess** seguido do **Log de Acesso** do **Apache**.

Linux

./goaccess -f /var/log/apache2/access.log

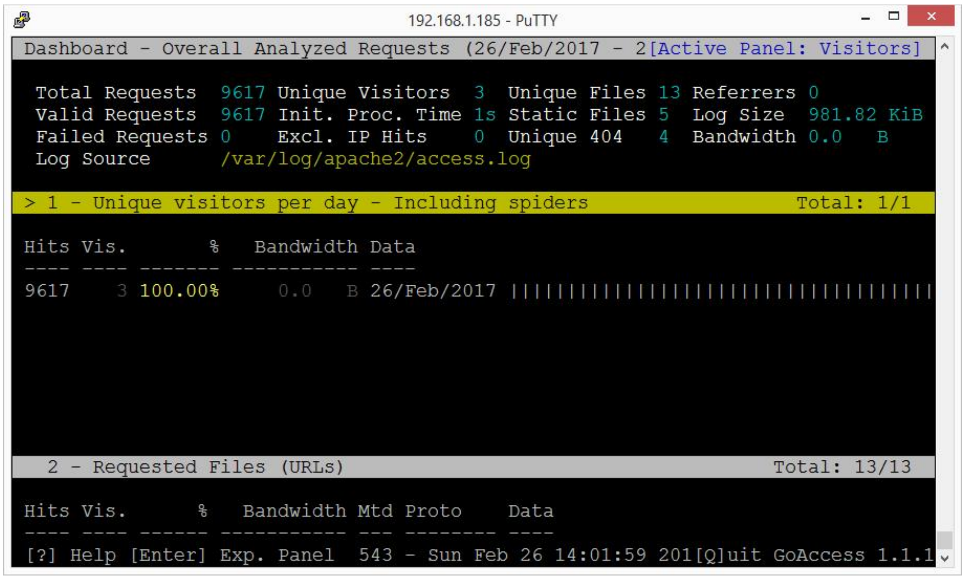


```
root@100security:/goaccess# ./goaccess -f /var/log/apache2/access.log
```

Visualização via **Console**.

Linux

Q – Para sair



```
Dashboard - Overall Analyzed Requests (26/Feb/2017 - 2[Active Panel: Visitors]

 Total Requests  9617 Unique Visitors  3  Unique Files 13 Referrers 0
 Valid Requests  9617 Init. Proc. Time 1s Static Files 5  Log Size  981.82 KiB
 Failed Requests 0    Excl. IP Hits    0  Unique 404   4  Bandwidth 0.0    B
 Log Source      /var/log/apache2/access.log

> 1 - Unique visitors per day - Including spiders                Total: 1/1

Hits Vis.       %  Bandwidth Data
---- ---- ------- ----------- ----
9617    3 100.00%      0.0   B 26/Feb/2017 |||||||||||||||||||||||||||||||||||||

  2 - Requested Files (URLs)                                    Total: 13/13

Hits Vis.      %   Bandwidth Mtd Proto    Data
---- ---- ------ ----------- --- -------- ----
[?] Help [Enter] Exp. Panel  543 - Sun Feb 26 14:01:59 201[Q]uit GoAccess 1.1.1
```