
ΑΝΑΦΟΡΑ ΕΡΓΑΣΤΗΡΙΑΚΗΣ:

“PART I”

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ

(CEID1135)

Ερώτημα 1: Shell Scripting

Αρχικά χρησιμοποιούμε δομή ελέγχου case

```
case $# in
```

στην οποία ανάλογα με τον αριθμό των ορισμάτων που δίνονται κατά την κλήση του αρχείου και την τιμή του ορίσματος να οδηγούμαστε στην κατάλληλη περίπτωση.

[./logparser.sh](#)

Για κανένα όρισμα κατά την κλήση του αρχείου

```
case $# in
    0) echo "1084581|1084583|1084516"
        echo "1084581|1084583|1084516" > AM.txt;;

```

εκτυπώνεται:

```
[root💀kali㉿kali:[/home/kali/Desktop]
# ./logparser.sh
1084581|1084583|1084516
```

Εκτυπώνονται τα AM των μελών της ομάδας σε συγκεκριμένο format και επισης δημιουργείται αντίστοιχο αρχείο για κάθε περαιτέρω χρήση του αποτελεσματος.

./logparser.sh access.log

Για την κλήση του αρχείου (με ένα όρισμα) το όνομα του αρχείου access.log που μας δόθηκε

```
1) awk '{print NR,$0}' $1  
awk '{print $0}' $1 > access_copy.log  
;;
```

εκτυπώνεται το περιεχόμενό του και παράλληλα εξάγουμε σε αρχείο αντίγραφό του με όνομα access_copy.log για κάθε περαιτέρω χρήση του αποτελέσματος.

```
└# ./logparser.sh access.log  
1 127.0.0.1 - root - [29/Mar/2021:16:47:19 +0300] "GET / HTTP/1.1" 302  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
2 127.0.0.1 - - [29/Mar/2021:16:47:19 +0300] "GET /dashboard/ HTTP/1.1" 200  
7577 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
3 127.0.0.1 - admin - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/normalize.css HTTP/1.1" 200 6876 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
4 127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/all.css HTTP/1.1" 200 481698 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
5 127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/modernizr.js HTTP/1.1" 200 51365 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
6 127.0.0.1 - user1 - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/all.js HTTP/1.1" 200 188385 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
7 127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/bitnami-xampp.png HTTP/1.1" 200 22133 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
8 127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/fastly-logo.png HTTP/1.1" 200 1770 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
9 127.0.0.1 - root - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/xampp-logo.svg HTTP/1.1" 200 5427 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
10 127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/social-icons.png HTTP/1.1" 200 3361 "http://localhost/dashboard/stylesheets/all.css" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"  
11 127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/favicon.png HTTP/1.1" 200 2508 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
```

3.1 ./logparser.sh access.log --usrid

Καλείται η συνάρτηση mining_username

```
2) if [ "$2" = "--servprot" ]; then
    echo "Wrong Network Protocol" > server_protocol.txt
    echo "Wrong Network Protocol"
fi

if [ "$2" = "--method" ]; then
    echo "Wrong Method Name" > server_protocol.txt
    echo "Wrong Method Name"
fi

if [ "$2" = "--datum" ]; then
    echo "Wrong Date" > date.txt
    echo "Wrong Date"
fi

if [ "$2" = "--usrid" ]; then
    mining_username
    awk '{print $0}' user_counter.txt
fi

mining_username () {
    awk '{ print $3 }' $filename | sort | uniq -c > user_counter.txt
}
```

μέσω της οποίας γράφεται σε αρχείο με ονομασία user_counter.txt ο αριθμός εμφανίσεων κάθε username αλφαριθμητικά για κάθε περαιτέρω χρήση του αποτελέσματος και ύστερα τυπώνεται στο command line.

```
[root@kali ~]# ./logparser.sh access.log --usrid
15710 -
124 admin
34 president
181 root
110 user1
91 user2
39 user3
```

3.2 ./logparser.sh access.log --usrid <user_id>

Σε αυτή την κλήση δίνονται 3 ορίσματα, το τρίτο όρισμα καθορίζει το user_id που θα ψάξουμε στο αρχείο access.log. Στην αρχή καλούμε την συνάρτηση mining_username

```
mining_username () {  
    awk '{ print $3 }' $filename | sort | uniq -c > user_counter.txt  
}
```

και μέσα από το αρχείο που μας δίνει αυτή η συνάρτηση ελέγχουμε αν το user_id που δόθηκε ως όρισμα υπάρχει. Αν υπάρχει εκτυπώνονται οι γραμμές του αρχείου access.log που το περιέχουν και εξάγονται και σε αρχείο με ονομασία with_username.txt, αλλιώς εμφανίζεται μήνυμα στην οθόνη και στο αρχείο with_username.txt

“Username Not Found”.

```
3)  
if [ "$2" = "--usrid" ]; then  
    mining_username  
    if grep -Ewq "$3" user_counter.txt; then  
        awk '/'$3' -/ {print $0 }' $1 > with_username.txt  
        awk '/'$3' -/ {print $0 }' $1  
    else  
        echo "Username Not Found" > with_username.txt  
        echo "Username Not Found"  
    fi  
fi
```

Ακολουθούν παραδείγματα κλήσεων με διάφορα user_id:

[./logparser.sh access.log --usrid root](#)

```
(root💀kali)-[~/home/kali/Desktop]
# ./logparser.sh access.log --usrid root
127.0.0.1 - root - [29/Mar/2021:16:47:19 +0300] "GET / HTTP/1.1" 302 "-"-
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/xamp
p-logo.svg HTTP/1.1" 200 5427 "http://localhost/dashboard/" "Mozilla/5.0 (W
indows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/dist/aj
ax.js?v=5.1.1 HTTP/1.1" 200 31313 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/vendor/
jquery/jquery.ba-hashchange-2.0.js?v=5.1.1 HTTP/1.1" 200 10505 "-" "Mozilla
/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/dist/co
nfig.js?v=5.1.1 HTTP/1.1" 200 24956 "-" "Mozilla/5.0 (Windows NT 10.0; Win6
4; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/vendor/
codemirror/addon/runmode/runmode.js?v=5.1.1 HTTP/1.1" 200 2773 "-" "Mozilla
/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:25 +0300] "GET /phpmyadmin/themes/pma
homme/img/left_nav_bg.png HTTP/1.1" 200 146 "http://localhost/phpmyadmin/th
emes/pmahomme/css/theme.css?v=5.1.1&nocache=2594244035ltr&server=1" "Mozill
a/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [30/Mar/2021:16:47:25 +0300] "GET /phpmyadmin/themes/pma
homme/img/b_sql.png HTTP/1.1" 200 680 "http://localhost/phpmyadmin/themes/p
mahomme/css/theme.css?v=5.1.1&nocache=2594244035ltr&server=1" "Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [30/Mar/2021:16:47:25 +0300] "GET /phpmyadmin/themes/pma
homme/img/console.png HTTP/1.1" 200 292 "http://localhost/phpmyadmin/themes/p
mahomme/css/theme.css?v=5.1.1&nocache=2594244035ltr&server=1" "Mozilla/5.
0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [30/Mar/2021:16:47:52 +0300] "GET /phpmyadmin/js/dist/se
rver/databases.js?v=5.1.1 HTTP/1.1" 200 4917 "-" "Mozilla/5.0 (Windows NT 1
```

./logparser.sh access.log --usrid admin

```
[root💀kali]-[~/home/kali/Desktop]
└─# ./logparser.sh access.log --usrid admin
127.0.0.1 - admin - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/normalize.css HTTP/1.1" 200 6876 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:21 +0300] "GET /phpmyadmin/ HTTP/1.1" 200 15865 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/vendor/jquery/jquery.validate.js?v=5.1.1 HTTP/1.1" 200 50963 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/dist/rte.js?v=5.1.1 HTTP/1.1" 200 40074 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/dist/shortcuts_handler.js?v=5.1.1 HTTP/1.1" 200 3326 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:25 +0300] "GET /phpmyadmin/js/dist/codemirror/addon/lint/sql-lint.js?v=5.1.1 HTTP/1.1" 200 959 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [30/Mar/2021:16:47:25 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_tblops.png HTTP/1.1" 200 537 "http://localhost/phpmyadmin/themes/pmahomme/css/theme.css?v=5.1.1&nocache=2594244035ltr&server=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [30/Mar/2021:16:47:42 +0300] "POST /phpmyadmin/index.php?route=/import HTTP/1.1" 200 9527 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [30/Mar/2021:16:48:02 +0300] "GET /phpmyadmin/js/dist/table/change.js?v=5.1.1 HTTP/1.1" 200 28848 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [16/Jun/2021:16:48:17 +0300] "GET /phpmyadmin/themes/pma
```

./logparser.sh access.log --usrid -

```
[root@kali]~[/home/kali/Desktop]
# ./logparser.sh access.log --usrid -
127.0.0.1 - - [29/Mar/2021:16:47:19 +0300] "GET /dashboard/ HTTP/1.1" 200 7
577 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101
Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/all.
css HTTP/1.1" 200 481698 "http://localhost/dashboard/" "Mozilla/5.0 (Window
s NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/mode
rnizr.js HTTP/1.1" 200 51365 "http://localhost/dashboard/" "Mozilla/5.0 (Wi
ndows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/bitnami-x
ampp.png HTTP/1.1" 200 22133 "http://localhost/dashboard/" "Mozilla/5.0 (Wi
ndows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/fastly-lo
go.png HTTP/1.1" 200 1770 "http://localhost/dashboard/" "Mozilla/5.0 (Windo
ws NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/social-ic
ons.png HTTP/1.1" 200 3361 "http://localhost/dashboard/stylesheets/all.css"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox
/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/favicon.p
ng HTTP/1.1" 200 2508 "http://localhost/dashboard/" "Mozilla/5.0 (Windows N
T 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/vendor/codem
irror/addon/hint/show-hint.css?v=5.1.1 HTTP/1.1" 200 623 "-" "Mozilla/5.0 (
Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/js/vendor/codem
irror/lib/codemirror.css?v=5.1.1 HTTP/1.1" 200 8722 "-" "Mozilla/5.0 (Windo
ws NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:24 +0300] "GET /phpmyadmin/themes/pmahomme
/jQuery/jquery-ui.css HTTP/1.1" 200 36566 "-" "Mozilla/5.0 (Windows NT 10.0
; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
```

4 .*logparser.sh* access.log -method <method name>

Πραγματοποιείται η παραπάνω κλήση με δύο εναλλακτικές στο τρίτο όρισμα, καλείται είτε με GET είτε με POST. Με έλεγχο μέσω της δομής if-elif-else προσδιορίζουμε ποιά τιμή έχει το τρίτο όρισμα. Στην περίπτωση που δεν έχει δοθεί ένα εκ των GET ή POST εμφανίζεται μήνυμα “Wrong Method Name”. Στις άλλες δύο περιπτώσεις εμφανίζονται στην οθόνη η γραμμές του αρχείου access.log που περιέχουν το method name που αναζητούμε. Επιπλέον εξάγουμε ότι εμφανίζεται στην οθόνη σε αρχείο με ονομασία method_name.txt για κάθε περαιτέρω χρήση του αποτελέσματος.

```
if [ "$2" = "--method" ]; then
    if [[ "$3" = "GET" ]]; then
        awk '/GET/ {print $0 }' $1 > method_name.txt
        awk '/GET/ {print $0 }' $1
    elif [[ "$3" = "POST" ]]; then
        awk '/POST/ {print $0 }' $1 > method_name.txt
        awk '/POST/ {print $0 }' $1
    else
        echo "Wrong Method Name"
        echo "Wrong Method Name" > method_name.txt
    fi
fi
```

Ακολουθούν παραδείγματα με κλήση GET, POST και λάθος method name αντίστοιχα:

[./logparser.sh access.log -method GET](#)

```
[root@kali ~]# ./logparser.sh access.log --method GET
127.0.0.1 - root - [29/Mar/2021:16:47:19 +0300] "GET / HTTP/1.1" 302 - "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:19 +0300] "GET /dashboard/ HTTP/1.1" 200 7
577 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/normalize.css HTTP/1.1" 200 6876 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/all.css HTTP/1.1" 200 481698 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/mernizr.js HTTP/1.1" 200 51365 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - user1 - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/all.js HTTP/1.1" 200 188385 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/bitnami-xampp.png HTTP/1.1" 200 22133 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/fastly-logo.png HTTP/1.1" 200 1770 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/xamp-p-logo.svg HTTP/1.1" 200 5427 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/social-icons.png HTTP/1.1" 200 3361 "http://localhost/dashboard/stylesheets/all.css" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
```

./logparser.sh access.log -method POST

```
[root@kali ~]# ./logparser.sh access.log --method POST
127.0.0.1 - - [30/Mar/2021:16:47:25 +0300] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 1563 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [30/Mar/2021:16:47:25 +0300] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 1654 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [30/Mar/2021:16:47:25 +0300] "POST /phpmyadmin/index.php?route=/navigation&ajax_request=1 HTTP/1.1" 200 2266 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [30/Mar/2021:16:47:25 +0300] "POST /phpmyadmin/index.php?route=/database/structure/favorite-table&ajax_request=1&favorite_table=1&sync_favorite_tables=1&lang=en HTTP/1.1" 200 155 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - user1 - [30/Mar/2021:16:47:25 +0300] "POST /phpmyadmin/index.php?route=/version-check HTTP/1.1" 200 64 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [30/Mar/2021:16:47:25 +0300] "POST /phpmyadmin/index.php?route=/config/set HTTP/1.1" 200 1554 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [30/Mar/2021:16:47:42 +0300] "POST /phpmyadmin/index.php?route=/import HTTP/1.1" 200 9527 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [30/Mar/2021:16:47:43 +0300] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 1565 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - user1 - [30/Mar/2021:16:47:43 +0300] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 1656 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
```

./logparser.sh access.log -method POS

```
[root@kali ~]# ./logparser.sh access.log --method POS
Wrong Method Name
```

5 [./logparser.sh access.log --serverprot <Network Protocol>](#)

Παρόμοια με το προηγούμενο ερώτημα αντί για method name αναζητούμε network protocol. Το τρίτο όρισμα σε αύτη την περίπτωση μπορεί να είναι IPv4 ή IPv6. Κάθε άλλο θα επιστρέφει μήνυμα “Wrong Network Protocol”. Η ανίχνευση το network protocol μέσα από κάθε γραμμή γίνεται με βάση τον πρώτο χαρακτήρα που συναντάμε σε κάθε γραμμή του αρχείου access.log. Αν ο πρώτο χαρακτήρας είναι 1 τότε χρησιμοποιείται IPv4 πρωτόκολλο, αν είναι :: τότε χρησιμοποιείται IPv6 πρωτόκολλο και κάθε άλλη περίπτωση πρόκειται για λάθος network protocol. Το αποτέλεσμα τυπώνεται και αποθηκεύεται σε αρχείο με όνομα server_protocol.txt για κάθε περαιτέρω χρήση του αποτελέσματος.

```
if [ "$2" = "--servprot" ]; then
    if [ "$3" = "IPv4" ]; then
        awk '/^1/ {print $0 }' $1 > server_protocol.txt
        awk '/^1/ {print $0 }' $1
    elif [ "$3" = "IPv6" ]; then
        awk '/::/ {print $0 }' $1 > server_protocol.txt
        awk '/::/ {print $0 }' $1
    else
        echo "Wrong Network Protocol"
        echo "Wrong Network Protocol" > server_protocol.txt
    fi
fi
```

Ακολουθούν παραδείγματα κλήσεων με IPv4, IPv6 και λάθος network protocol:

./logparser.sh access.log --serverprot IPv4

```
[root@kali ~]# ./logparser.sh access.log --serverprot IPv4
127.0.0.1 - root - [29/Mar/2021:16:47:19 +0300] "GET / HTTP/1.1" 302 - "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:19 +0300] "GET /dashboard/ HTTP/1.1" 200 7
577 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - admin - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/normalize.css HTTP/1.1" 200 6876 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/stylesheets/all.css HTTP/1.1" 200 481698 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/modernizr.js HTTP/1.1" 200 51365 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - user1 - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/javascripts/all.js HTTP/1.1" 200 188385 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/bitnami-xampp.png HTTP/1.1" 200 22133 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/fastly-logo.png HTTP/1.1" 200 1770 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - root - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/xamp-logo.svg HTTP/1.1" 200 5427 "http://localhost/dashboard/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
127.0.0.1 - - [29/Mar/2021:16:47:20 +0300] "GET /dashboard/images/social-icons.png HTTP/1.1" 200 3361 "http://localhost/dashboard/stylesheets/all.css" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
```

./logparser.sh access.log --servprot IPv6

```
[root💀kali㉿kali:/home/kali/Desktop]
# ./logparser.sh access.log --servprot IPv6
::1 - - [26/Aug/2021:10:36:14 +0300] "GET / HTTP/1.1" 302 -
::1 - root - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/ HTTP/1.1" 200 75
77
::1 - - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/stylesheets/normalize.css HTTP/1.1" 200 6876
::1 - - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/stylesheets/all.css HTTP/1.1" 200 481698
::1 - root - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/javascripts/modernizr.js HTTP/1.1" 200 51365
::1 - - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/javascripts/all.js HTTP/1.1" 200 188385
::1 - root - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/images/bitnami-xampp.png HTTP/1.1" 200 22133
::1 - - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/images/fastly-logo.png HTTP/1.1" 200 1770
::1 - - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/images/xampp-logo.svg HTTP/1.1" 200 5427
::1 - root - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/images/social-icons.png HTTP/1.1" 200 3361
::1 - - [26/Aug/2021:10:36:14 +0300] "GET /dashboard/images/favicon.png HTTP/1.1" 200 2508
::1 - - [26/Aug/2021:10:36:15 +0300] "GET /phpmyadmin/ HTTP/1.1" 200 16461
::1 - admin - [26/Aug/2021:10:36:20 +0300] "GET /phpmyadmin/ HTTP/1.1" 200 16463
::1 - root - [26/Aug/2021:10:36:21 +0300] "GET /phpmyadmin/themes/pmahomme/jquery/jquery-ui.css HTTP/1.1" 200 36566
::1 - - [26/Aug/2021:10:36:21 +0300] "GET /phpmyadmin/js/vendor/codemirror/addon/hint/show-hint.css?v=5.1.1 HTTP/1.1" 200 623
::1 - - [26/Aug/2021:10:36:21 +0300] "GET /phpmyadmin/js/vendor/codemirror/lib/codemirror.css?v=5.1.1 HTTP/1.1" 200 8722
```

./logparser.sh access.log --servprot IPv5

```
[root💀kali㉿kali:/home/kali/Desktop]
# ./logparser.sh access.log --servprot IPv5
Wrong Network Protocol
```

6 .*Logparser.sh* access.log -- browsers

Για την ανίχνευση των browsers χωρίζουμε την κάθε γραμμή του αρχείου access.log με βάση τα εισαγωγικά “ και εξάγουμε σε αρχείο με ονομασία output1.txt το έκτο κομμάτι. Ακολούθως από το νέο αρχείο που δημιουργήθηκε ψάχνουμε με την match σε κάθε γραμμή να βρούμε λέξεις που έχουν στο τέλος τους τον χαρακτήρα / . Οι λέξεις αυτές που εμφανίζονται σε κάθε γραμμή τις εξάγουμε σε νέο αρχείο με όνομα output2.txt το οποίο θα περιέχει τους browsers με τον χαρακτήρα / στο τέλος τους. Εκμεταλλευόμενοι αυτό το pattern χωρίζουμε την κάθε γραμμή με βάση τα forward slashes και οι λέξεις που χωρίζονται από αυτά εξάγονται στο αρχείο output1.txt με αλφαριθμητική σειρά και αναγράφοντας μπροστά τους τον αριθμό των εμφανίσεων κάθε browser. Για να ακολουθεί η τελική εκτύπωση το πρότυπο το οποίο ζητείται στην εκφώνηση όπου πρώτα αναφέρεται ο browser και έπειτα ο αριθμός εμφανίσεων αντιστρέφουμε σε κάθε γραμμή την πρώτη με τη δεύτερη λέξη. Το τελικό ζητούμενο της άσκησης εκτυπώνεται στην οθόνη αλλά δημιουργείται και αρχείο με ονομασία output1.txt για κάθε περαιτέρω χρήση του αποτελέσματος.

```
if [ "$2" = "--browsers" ]; then
    count_browsers () {

        awk -F'/' '{print $6}' $1 > output1.txt
        awk '{
            for(i=1; i<NF; i++) {
                temp=match($i, /[a-zA-Z]+[\/]/)
                if(temp) {
                    print $i
                }
            }
        }' output1.txt > output2.txt
        awk -F '/' '{print $1}' output2.txt | sort | uniq -c > output1.txt
        awk '{print $2, $1}' output1.txt > output2.txt
        awk '{print $2, $1}' output1.txt
    }
    count_browsers $filename
fi
;;
```

Τελικό αποτέλεσμα που εκτυπώνεται στην οθόνη:

```
(root💀kali)-[~/home/kali/Desktop]
└─# ./logparser.sh access.log --browsers
AppleWebKit 124
Chrome 124
Edg 63
Firefox 933
Gecko 933
HomeNet 1
Mozilla 1057
Safari 124
```

7 [./logparser.sh access.log --datum <Date>](#)

Στην κλήση αυτή δίνεται σαν τρίτο όρισμα ένας μήνας και επιστρέφονται οι γραμμές του αρχείου access.log που περιέχουν αυτόν τον μήνα. Αν το τρίτο όρισμα είναι ένας από τους μήνες που φαίνονται στην παρακάτω εικόνα τότε αναζητεί τις γραμμές που τον περιέχουν και αυτές οι γραμμές εξάγονται σε αρχείο με ονομασία date.txt για κάθε περαιτέρω χρήση του αποτελέσματος και εκτυπώνονται στην οθόνη. Σε κάθε άλλη περίπτωση όπου το τρίτο όρισμα δεν είναι ένας από τους μήνες εμφανίζεται μήνυμα “Wrong Date”.

```
if [ "$2" = "--datum" ]; then
    if [ "$3" = "Jan" ] ||
    [ "$3" = "Feb" ] ||
    [ "$3" = "Mar" ] ||
    [ "$3" = "Apr" ] ||
    [ "$3" = "May" ] ||
    [ "$3" = "Jun" ] ||
    [ "$3" = "Jul" ] ||
    [ "$3" = "Aug" ] ||
    [ "$3" = "Sep" ] ||
    [ "$3" = "Oct" ] ||
    [ "$3" = "Nov" ] ||
    [ "$3" = "Dec" ]; then
        awk '/'$3'/{print $0}' $1 > date.txt
        awk '/'$3'/{print $0}' $1
    else
        echo "Wrong Date" > date.txt
        echo "Wrong Date"
    fi
fi;;
esac
```

Ακολουθούν παραδείγματα με δύο κλήσεις οι οποίες έχουν σώστο το τρίτο όρισμα ενώ η τελευταία κλήση έχει λανθασμένο το τρίτο όρισμα:

[./logparser.sh access.log --datum Jan](#)

```
[root💀kali]-[~/home/kali/Desktop]
└─# ./logparser.sh access.log --datum Jan
::1 - - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/ HTTP/1.1" 200 5328
::1 - - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/scripts/jquery-1.9.1.min.js HTTP/1.1" 200 92596
::1 - user1 - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/css/bootstrap.min.css HTTP/1.1" 200 163873
::1 - admin - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/css/dashboard.css HTTP/1.1" 200 1573
::1 - - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/images/oke2.svg HTTP/1.1" 200 2441
::1 - user2 - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/images/en.jpg HTTP/1.1" 200 759
::1 - - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/images/logo.jpg HTTP/1.1" 200 55235
::1 - root - [14/Jan/2022:14:26:15 +0300] "GET /MyDocs/AEKX/images/en_on.jpg HTTP/1.1" 200 661
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/ HTTP/1.1" 200 5328
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/scripts/jquery-1.9.1.min.js HTTP/1.1" 200 92596
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/css/bootstrap.min.css HTTP/1.1" 200 163873
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/images/oke2.svg HTTP/1.1" 200 2441
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/css/dashboard.css HTTP/1.1" 200 1573
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/images/en.jpg HTTP/1.1" 200 759
::1 - - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/images/logo.jpg HTTP/1.1" 200 55235
::1 - admin - [14/Jan/2022:16:29:25 +0300] "GET /MyDocs/AEKX/images/en_on.jpg HTTP/1.1" 200 661
```

./logparser.sh access.log --datum Feb

```
[root💀kali㉿kali:/home/kali/Desktop]
# ./logparser.sh access.log --datum Feb
::1 - root - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/dot.gif HTTP/1.1" 200 43
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/css/printview.css?v=5.1.1 HTTP/1.1" 200 1392
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/left_nav_bg.png HTTP/1.1" 200 146
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/s_logoff.png HTTP/1.1" 200 626
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_home.png HTTP/1.1" 200 734
::1 - admin - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_docs.png HTTP/1.1" 200 705
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_sqlhelp.png HTTP/1.1" 200 512
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/s_cog.png HTTP/1.1" 200 442
::1 - user1 - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_plus.png HTTP/1.1" 200 143
::1 - president - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/s_link.png HTTP/1.1" 200 280
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/s_db.png HTTP/1.1" 200 328
::1 - root - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/s_reload.png HTTP/1.1" 200 527
::1 - user3 - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_newdb.png HTTP/1.1" 200 585
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/b_group.png HTTP/1.1" 200 682
::1 - - [11/Feb/2022:15:52:30 +0300] "GET /phpmyadmin/themes/pmahomme/img/s_host.png HTTP/1.1" 200 591
```

./logparser.sh access.log --datum NotValid

```
[root💀kali㉿kali:/home/kali/Desktop]
# ./logparser.sh access.log --datum NotValid
Wrong Date
```

Ερώτημα 2 Διεργασίες Υπολογισμός ολοκληρώματος συνάρτησης

Για την υλοποίηση της ουράς μηνυμάτων FIFO (First In First Out) για τον παράλληλο υπολογισμό του ολοκληρώματος (fork). Ακολουθούμε τα έξεις βήματα:

Βήμα 1 – Δημιουργούμε δυο συναρτήσεις, η μία είναι για αποστολή στην ουρά μηνυμάτων server και μια άλλη είναι για ανάκτηση από την ουρά μηνυμάτων client

Βήμα 2 – Σε κάθε προαναφερθεσα συνάρτηση δημιουργούμε και από ένα κλειδί, χρησιμοποιώντας τη συνάρτηση ftok(). Για αυτό, αρχικά δημιουργείται το αρχείο στο Desktop για να ληφθεί ένα μοναδικό κλειδί.

Βήμα 3 – Η συνάρτηση server παίρνει ως όρισμα δυναμικά μια μεταβλητή double εν συνέχεια με την msgget() δημιουργούμε μια ουρά μηνυμάτων ή συνδεόμαστε σε μια ήδη υπάρχουσα ουρά. Το πρώτο όρισμα της είναι το κλειδί και αναγνωρίζει την ουρά μηνυμάτων , Το δεύτερο όρισμα, shmflg, καθορίζει τις απαιτούμενες σημαίες ουράς μηνυμάτων, εδώ χρησιμοποιούμε το IPC_CREAT (δημιουργία ουράς μηνυμάτων εάν δεν υπάρχει). Τέλος σε αυτή την συναρτήσει με την msgsnd() πραγματοποιούμε την εγράφη στην ουρά. Η msgsnd έχει την ακολουθεί δομή (κλειδί , μήνυμα προς εγράφη , μέγεθος του μηνύματος, η σημαία το μνήματός εδώ 0)

```
void server(double s, int i) {  
  
    key_t key;  
    int msgid;  
  
    key = ftok("Desktop", 65);  
    msgid = msgget(key, 0666 | IPC_CREAT);  
    message.msg_type = 1;  
    message.msg_data = s;  
    msgsnd(msgid, &message, sizeof(message), 0);  
    message.msg_data = 11;  
    int child_pid = waitpid(-1, NULL, 0);  
    msgctl(msgid, IPC_RMID, NULL);  
    exit(1);  
}
```

Βήμα 4 – Η συνάρτηση client επιστρέφει μια double εν συνέχεια με την msgget() δημιουργούμε μια ουρά μηνυμάτων ή συνδεόμαστε σε μια ήδη υπάρχουσα ουρά. Το πρώτο όρισμα της είναι το κλειδί και αναγνωρίζει την ουρά μηνυμάτων , Το δεύτερο όρισμα, shmflg, καθορίζει τις απαιτούμενες σημαίες ουράς μηνυμάτων, εδώ χρησιμοποιούμε το IPC_CREAT (δημιουργία ουράς μηνυμάτων εάν δεν υπάρχει). Τέλος σε αυτή την συναρτήσει με την msgrcv() πραγματοποιούμε την ανάγνωση από την ουρά μηνυμάτων. Η msgrcv() έχει την ακολουθεί δομή (κλειδί , μήνυμα προς επιστροφή , μέγεθος του μηνύματος, η σημαία το μνήματός εδώ 0)

```
double client() {  
    key_t key;  
    int msgid;  
  
    key = ftok("Desktop", 65);  
    msgid = msgget(key, 0666 | IPC_CREAT);  
    msgrcv(msgid, &message, sizeof(message), 0, 0);  
    message.msg_type = 2;  
    double sum = message.msg_data;  
}
```

Βήμα 5 – Για την υλοποίηση του fork και τον κατακερματισμό σε διεργασίες χρησιμοποιούμε την εξής λογική καλούμε την fork με την χρήση μιας for όσες φορές έχει θέσει ο χρήστες για την δημιουργία των διεργασιών και για κάθε if(pid>0) υπολογίζουμε το υπό ολοκλήρωμα και με την κλήση της server στέλνουμε το αποτέλεσμα στη κοινή ουρά. Ενώ για την πρόσθεση των αποτελεσμάτων υλοποιούμε μια ακόμα for με αριθμό επαναλήψεων όσες ο αριθμός των fork και για pid =0 καλούμε την client και εν συνέχεια προσθέτουμε τα αποτελέσματα του κάθε ολοκληρώματος.

```
int pid;
for (int i=0; i<procedures; i++) {
    pid = fork();
    if (pid > 0) {
        double s = get_integral(a+((b-a)/procedures)*i, a+((b-a)/procedures)*(i+1), size_of_procedure);
        server(s,i);
    }
}
for (int i=0; i<procedures; i++)
if (pid == 0) {
    client();
    total = total + message.msg_data;
}
```

Αποτελέσματα

Χρόνος πριν την υλοποιήση με ουρές μηνυμάτων και fork.

```
orestisantonismakris@pop-os:~/Downloads$ ./a.out
Time=18.266182 seconds, Result=4.28245881
```

Διάφοροι χρόνοι μετά την υλοποίηση με ουρές μηνυμάτων και fork , για διάφορα input values.

```
orestisantonismakris@pop-os:~/Downloads$ ./a.out 100
Time=7.635661 seconds, Result=4.28245881
orestisantonismakris@pop-os:~/Downloads$ ./a.out 10
Time=7.562351 seconds, Result=4.28245881
orestisantonismakris@pop-os:~/Downloads$ ./a.out 80
Time=7.560206 seconds, Result=4.28245881
```