ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

Τμήμα Πληροφορικής

ΕΠΛ 421 - Προγραμματισμός Συστημάτων

ΑΣΚΗΣΗ 1 – Εντολές Κελύφους για Διαχείριση Συστημάτων UNIX

Διδάσκων: Δημήτρης Ζεϊναλιπούρ

Υπεύθυνος Εργαστηρίου: Παύλος Αντωνίου

Ημερομηνία Ανάθεσης: Παρασκευή, 4/2/2022
Ημερομηνία Παράδοσης: Παρασκευή, 18/2/2022 και ώρα 13:00 (14 μέρες)

(η λύση να υποβληθεί σε zip μέσω του Moodle)

http://www.cs.ucy.ac.cy/courses/EPL421/

Στόχος Άσκησης

Στόχος αυτής της άσκησης είναι η εξοικείωση με βασικές εντολές του λειτουργικού συστήματος UNIX. Συγκεκριμένα, σε αυτή την άσκηση θα πρέπει να κάνετε **χρήση των εντολών του UNIX** με διοχέτευση **ΧΩΡΙΣ** τη χρήση:

1. Εργαλείων ωφελιμότητας *sed* & *awk*;
2. Ενδιάμεσων αρχείων, τα οποία δημιουργούνται με ανακατευθύνσεις; και
3. Τεχνικών προγραμματισμού κελύφους, κάτι το οποίο θα δούμε στη συνέχεια.

Εισηγούμαστε όπως μελετήσετε τις εντολές τις οποίες έχετε διδαχθεί στις διαλέξεις του μαθήματος και μέσω του εγχειριδίου *man,* έτσι ώστε να ανακαλύψετε και χρησιμοποιήσετε νέες παραμέτρους που είναι διαθέσιμες για τις εντολές αυτές.

ΕΡΩΤΗΜΑΤΑ

Για κάθε ερώτημα που ακολουθεί **δώστε την εντολή (ή σειρά εντολών με διοχέτευση)** που πιστεύετε ότι δίνει πιο αποδοτικά τη ζητούμενη λύση. Επίσης **εξηγήστε εν συντομία** τη δομή της εντολής που έχετε δώσει. Εάν πρόκειται για μια διοχέτευση εντολών τότε περιγράψετε όλους τους επί μέρους όρους της εντολής.

Ερώτημα 1

Να δώσετε την εντολή (ή σειρά εντολών με διοχέτευση) που να παρουσιάζει πόσα user ids στο αρχείο `/etc/passwd` βρίσκονται μεταξύ 28 και 35 συμπεριλαμβανομένου. Για παράδειγμα, μια καταχώρηση μέσα στο αρχείο `/etc/passwd` μπορεί να είναι: `ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin` όπου το user id είναι το 14. Υποθέστε ότι τα user ids δεν αντιστοιχούν ποτέ σε αριθμό που ξεκινά από 0 π.χ. 013.

Ερώτημα 2

Στα συστήματα Linux τα αρχεία συμβάντων (log files) αποθηκεύονται στο /var/log και μόνο ο χρήστης root μπορεί να έχει πρόσβαση σε αυτά. Μερικά αρχεία που βρίσκονται στον κατάλογο αυτό είναι:

/var/log/syslog: Shows general messages and info regarding the system. Basically a data log of all activity throughout the global system.
/var/log/auth.log: Keep authentication logs for both successful or failed logins, and authentication processes.
/var/log/mysql/: a directory containing error_log files of the mysql daemon.
/var/log/apt/: a directory which contains the log entries concerning packages installed by apt

Μέσα στο τελευταίο directory υπάρχει το αρχείο history.log που δείχνει μια λίστα με πακέτα και οι ενέργειες (Install, Remove, Upgrade) που λήφθηκαν όπως φαίνεται πιο κάτω:

```
Start-Date: 2022-01-07  12:56:20
Commandline: apt-get install apache2
Requested-By: csdeptucy (1000)
Install: libaprutil1:amd64 (1.6.1-4ubuntu2, automatic), libaprutil1-
dbd-sqlite3:amd64 (1.6.1-4ubuntu2, automatic), apache2-data:amd64
(2.4.41-4ubuntu3.1, automatic), libapr1:amd64 (1.6.5-1ubuntu1,
automatic), libaprutil1-ldap:amd64 (1.6.1-4ubuntu2, automatic),
liblua5.2-0:amd64 (5.2.4-1.1build3, automatic), apache2-bin:amd64
(2.4.41-4ubuntu3.1, automatic), apache2:amd64 (2.4.41-4ubuntu3.1),
apache2-utils:amd64 (2.4.41-4ubuntu3.1, automatic)
End-Date: 2021-01-07  12:56:28

Start-Date: 2022-01-19  07:13:23
Commandline: /usr/bin/unattended-upgrade
Upgrade: firefox-locale-en:amd64 (84.0.1+build1-0ubuntu0.20.04.1,
84.0.2+build1-0ubuntu0.20.04.1)
End-Date: 2021-01-19  07:13:23

Start-Date: 2022-01-21  12:53:53
Commandline: /usr/bin/unattended-upgrade
Remove: linux-headers-5.4.0-58:amd64 (5.4.0-58.64), linux-headers-
5.4.0-58-generic:amd64 (5.4.0-58.64)
End-Date: 2021-01-21  12:53:55
```

Για παράδειγμα, η πρώτη καταχώρηση αναφέρεται σε εγκατάσταση (Install) πολλαπλών πακέτων όπως `libaprutil1` (πρώτο πακέτο που εγκαθίσταται) και `libaprutil1-dbd-sqlite3` (δεύτερο πακέτο που εγκαθίσταται). Η δεύτερη καταχώρηση αναφέρεται σε αναβάθμιση (Upgrade) ενός μόνο πακέτου του `firefox-locale-en`. Η τρίτη καταχώρηση αναφέρεται στην διαγραφή (Remove) 2 πακέτων, του `linux-headers-5.4.0-58` και του `linux-headers-5.4.0-58-generic`. Στις πιο πάνω καταχωρήσεις, με πράσινο highlighted φαίνεται το πρώτο πακέτο που επηρεάζεται σε κάθε καταχώρηση. Σημειώνεται ότι μας ενδιαφέρει το όνομα του πακέτου μέχρι το χαρακτήρα :

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) που να εμφανίζει ταξινομημένα κατά αύξουσα αλφαβητική σειρά μόνο το όνομα του πρώτου πακέτου που ενημερώνεται σε κάθε καταχώρηση τύπου Upgrade, των οποίων το όνομα αρχίζει από fi **ή** li. Το κάθε πακέτο (package) να εμφανίζεται μόνο μια φορά.

Ερώτημα 3

Να δώσετε την εντολή (ή σειρά εντολών με διοχέτευση) που να τυπώνει τον συνολικό αριθμό γραμμών που βρίσκονται σε όλα τα αρχεία .log στον τρέχων κατάλογο και σε οποιοδήποτε υποκατάλογο (κάτω από τον τρέχων).

Ερώτημα 4

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) που να εμφανίζει ταξινομημένα κατά αύξουσα αλφαβητική σειρά τα usernames των χρηστών που είναι συνδεδεμένοι στο σύστημα, των οποίων το username αρχίζει από cs **ΚΑΙ** τελειώνει σε 1. Το username κάθε χρήστη να εμφανίζεται μόνο μια φορά (δοκιμάστε το καλύτερα στις μηχανές του εργαστηρίου όπου θα υπάρχουν και άλλοι χρήστες ενωμένοι)

Ερώτημα 5

Μέσα στο HOME κατάλογο κάθε χρήστη υπάρχει ένα κρυφό (hidden) αρχείο με το όνομα `.bash_history` το οποίο περιέχει τις προηγούμενες εντολές που εκτέλεσε ο χρήστης (ιστορικό εντολών) στο κέλυφος bash. Σε κάθε γραμμή του αρχείου υπάρχει μια εντολή ή ένα σύνολο εντολών με διοχέτευση ή/και ανακατεύθυνση. Οι HOME κατάλογοι των χρηστών (εκτός του root) βρίσκονται μέσα στον κατάλογο `/home`. Για παράδειγμα ο χρήστης με username "johnsmith" έχει σαν HOME κατάλογο το `/home/johnsmith`. Ο HOME κατάλογος του root που είναι προσπελάσιμος μόνο από τον root βρίσκεται στο /root.

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) η οποία θα παρουσιάζει τις πρώτες 20 σελίδες **man** της εντολής που εκτέλεσε τις περισσότερες φορές ο χρήστης root και ΔΕΝ περιλαμβάνει διοχέτευση (|) ή ανακατεύθυνση (>, <). Σε περίπτωση περισσότερων από μια χρησιμοποιήστε όποια εντολή επιθυμείτε.

Για παράδειγμα εάν το αρχείο `/root/.bash_history` περιέχει τις πιο κάτω εντολές

```
ls
mv mylist.c list.c
ls | sort | uniq
man sort
cat lab3.c > lab4.c
grep –v "include" lab4.c
ls -ltr
ls -l
rm test1.txt
ls –a
```

τότε εκτελώντας τις εντολές σας θα πρέπει να παρουσιάζει τις πρώτες 20 γραμμές του ***man ls***, εφόσον η εντολή αυτή παρουσιάζεται 4 φορές. Οι εντολές με έντονα γράμματα λαμβάνονται υπόψη και οι γραμμές με κόκκινα γράμματα πρέπει να αγνοηθούν.

Ερώτημα 6

Αρκετές φορές ο διαχειριστής του συστήματος (root) χρειάζεται να κάνει backup κάποια αρχεία. Έστω ότι θέλει να κάνει backup το αρχείο notes αντιγράφοντας το σε ένα νέο αρχείο με το όνομα notes.HHMM όπου HHMM είναι η παρούσα ώρα (HH είναι οι ώρες και MM τα λεπτά). Ο διαχειριστής θέλει να διαγράψει τα παλαιότερα πέντε αρχεία του με τη χρήση μιας εντολής και χωρίς να γράφει το όνομα του κάθε αρχείου ξεχωριστά. Να δώσετε την εντολή (ή σειρά εντολών με διοχέτευση) που διαγράφει τα παλαιότερα πέντε αρχεία που έγιναν backup.

Ερώτημα 7

Η διατήρηση αρχείων συμβάντων (logging) είναι βασική λειτουργία του λειτουργικού συστήματος UNIX. Το σύστημα κρατάει αρχεία συμβάντων για δραστηριότητες που γίνονται στο σύστημα, για παράδειγμα καταγραφή δραστηριοτήτων χρηστών που συνδέονται (logged in) και αποσυνδέονται (logged out) από το σύστημα. Τα αρχεία `/var/run/utmp`, `/var/log/wtmp` και `/var/log/btmp` περιέχουν ιστορικό (logs) για logins και logouts

αντίστοιχα αλλά είναι δυαδικά (binary) και η επισκόπησή τους δεν μπορεί να γίνει με κάποιο text editor ή εντολή όπως είναι η less. Κάποιες εντολές χρησιμοποιούν αυτά τα 2 αρχεία για να παρουσιάσουν πληροφορίες.
Για παράδειγμα, το αρχείο `/var/run/utmp` περιέχει πληροφορίες για τους χρήστες που είναι τώρα συνδεδεμένοι στο σύστημα και η εντολή `who` το χρησιμοποιεί για να απεικονίσει τους χρήστες αυτούς.
Το αρχείο `/var/log/wtmp` είναι κάτι σαν ιστορικό για το αρχείο `/var/run/utmp`, διότι διατηρεί αρχείο συμβάντων για όλους τους χρήστες που συνδέθηκαν (logged in) και αποσυνδέθηκαν (logged out) στο παρελθόν. Η εντολή `last` χρησιμοποιεί το αρχείο αυτό για να απεικονίσει τους χρήστες που συνδέθηκαν τελευταίοι στο σύστημα.
Το αρχείο `/var/log/btmp` κρατάει πληροφορίες σχετικά με λάθος προσπάθειες σύνδεσης (bad login attempts). Χρησιμοποιείται από την εντολή `lastb`.
Δείτε ένα παράδειγμα της εξόδου της εντολής `last`

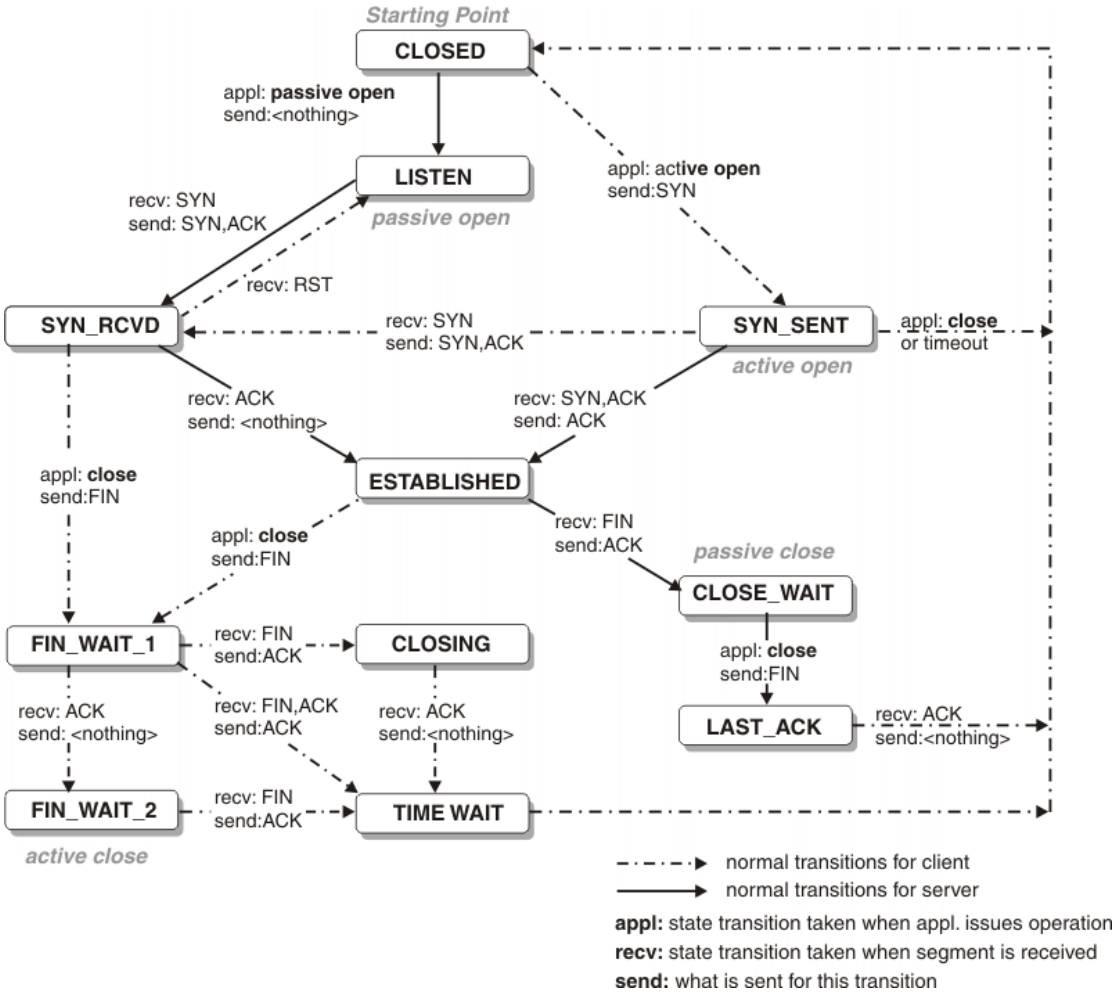
```
root     pts/0    b103ws10.in.cs.u Tue Feb  2 02:04   still logged in
evasto01 pts/0    b103ws10.in.cs.u Fri Jan 29 17:20 - 18:10  (00:49)
csp6pr2  pts/0    b103ws10.in.cs.u Fri Jan 29 16:55 - 17:09  (00:14)
root     pts/0    b103ws10.in.cs.u Fri Jan 29 03:21 - 12:57  (09:36)
csp6pr2  pts/0    b103ws10.in.cs.u Thu Jan 28 16:41 - 19:34  (02:53)
csp6pr2  pts/0    cs7156.cs.ucy.ac Thu Jan 28 09:58 - 13:36  (03:38)
root     pts/0    cs7156.cs.ucy.ac Wed Jan 27 08:35 - 10:53  (02:17)
reboot  system boot  2.6.32-042stab09 Wed Jan 27 08:19 - 02:09 (5+17:50)

wtmp begins Wed Jan 27 08:19:45 2016
```

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) που βρίσκει ποιος είναι **ο μήνας** με τις περισσότερες συνδέσεις (τα reboots να μη ληφθούν υπόψη) και να τον τυπώνει. Στο πιο πάνω παράδειγμα, θα έπρεπε να τυπώσει:

```
Jan
```

Ερώτημα 8

Μια σύνδεση TCP διέρχεται από μια σειρά καταστάσεων κατά τη διάρκεια του χρόνου ζωής της. Το πιο κάτω διάγραμμα απεικονίζει τις πιθανές καταστάσεις για μια σύνδεση TCP
και τον τρόπο μετάβασης από μια κατάσταση σε μια άλλη με βάση διάφορα συμβάντα είτε του δικτύου (π.χ. λήψη κάποιου πακέτου από απομακρυσμένη μηχανή) ή της τοπικής μηχανής (λήψη δεδομένων από μέσω socket από μια τοπική διαδικτυακή εφαρμογή).



Η εντολή netstat μπορεί να μας δώσει την κατάσταση της κάθε σύνδεσης TCP. Επιπλέον για κάθε σύνδεση, μας παρουσιάζει σε ξεχωριστές στήλες, την τοπική (Local) διεύθυνση IP και θύρα (port) καθώς και την απομακρυσμένη (Foreign) διεύθυνση IP και θύρα, δηλαδή τα 2 άκρα μιας σύνδεσης. Η διεύθυνση IP ξεχωρίζει από τη θύρα μέσω του χαρακτήρα :. Όταν μια θύρα είναι γνωστή (well-known) άρα δηλαδή ανήκει σε μια γνωστή υπηρεσία (μπορείτε να δείτε όλες τις γνωστές υπηρεσίες στο αρχείο /etc/services) τότε μας παρουσιάζει το όνομα της υπηρεσίας και όχι τον αριθμό της θύρας της.
Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) που να βρίσκει τις συνδέσεις TCP που βρίσκονται σε φάση ESTABLISHED ή TIME_WAIT ή SYN_SENT οι οποίες ξεκινούν από τη μηχανή σας και καταλήγουν σε μια απομακρυσμένη γνωστή υπηρεσία. Να ταξινομήσετε την κάθε υπηρεσία ως προς τον αριθμό των συνδέσεων που υπάρχουν για την κάθε υπηρεσία. Για παράδειγμα αν είχαμε αυτές τις συνδέσεις:

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 103ws12.in.cs.ucy.ac.cy:ssh vpn3-5.in.cs.ucy.ac.cy:nfa ESTABLISHED
tcp        0      0 103ws12.in.cs.ucy.ac.cy:57944 ariadni.in.cs.ucy.ac.cy:ldap ESTABLISHED
tcp        0      0 103ws12.in.cs.ucy.ac.cy:ssh vpn3-5.in.cs.ucy.ac.cy:iascontrol-oms ESTABLISHED
tcp        0      0 103ws12.in.cs.ucy.ac.cy:ssh vpn3-5.in.cs.ucy.ac.cy:fpitp ESTABLISHED
tcp        0      0 103ws12.in.cs.ucy.ac.cy:fcp-udp pallene.in.cs.ucy.ac.cy:nfs ESTABLISHED
tcp        0     96 103ws12.in.cs.ucy.ac.cy:ssh vpn3-5.in.cs.ucy.ac.cy:mtqp ESTABLISHED
tcp        0      0 103ws12.in.cs.ucy.ac.cy:795 kallimachos.in.cs.ucy.ac.cy:nfs ESTABLISHED
tcp        0      1 103ws12.in.cs.ucy.ac.cy:51056 cronos.cs.ucy.ac.cy:https SYN_SENT
tcp6       0      0 103ws12.in.cs.ucy.ac.cy:51454 172.20.116.200:sun-as-jpda ESTABLISHED
```

τότε θα έπρεπε να τυπώσετε:

```
2 nfs
1 sun-as-jpda
```

```
      1 nfa
      1 mtqp
      1 ldap
      1 iascontrol-oms
      1 https
      1 fpitp
```

Σημειώση: Δοκιμάστε τις εντολές σε μηχανή του εργαστηρίου 103 ή B103 που υπάρχουν ενεργές συνδέσεις. Επίσης μπορείτε πριν την κλήση των εντολών σας να δοκιμάσετε να ανοίξετε με τον browser κάποιες ιστοσελίδες για να δημιουργήσετε κίνηση.

Ερώτημα 9

Η εντολή `tcpdump` μας βοηθά να συλλέξουμε (capture) τα πακέτα που στέλνονται ή λαμβάνονται από το σύστημα μας για κάποιο χρονικό διάστημα (αντίστοιχα με το Wireshark – winpcap library ειδικότερα - στα Windows). Χρησιμοποιώντας τους κατάλληλους διακόπτες μπορούμε:
(α) να δούμε πλήρεις πληροφορίες για κάθε πακέτο π.χ. τα περιεχόμενα των κεφαλίδων των πρωτοκόλλων (διακόπτης `-v`)
(β) να λάβουμε μόνο συγκεκριμένο αριθμό πακέτων (διακόπτης `-c` ακολουθούμενος από ένα νούμερο π.χ. `-c 100` σημαίνει ότι θέλουμε να λάβουμε μόνο 100 πακέτα),
(γ) να αναλύσουμε το περιεχόμενο των πακέτων σε δεκαεξαδική μορφή (διακόπτης -XX),
(δ) να τυπώσουμε το χρόνο (timestamp) σε πιο εύληπτη μορφή (διακόπτης -tttt)
Για να παράξουμε κάποια επιπλέον κίνηση (πέρα από την συνήθη TCP/UDP κίνηση που θα βλέπει η NIC του host σας), θα μπορούσαμε προαιρετικά να τρέχουμε την εντολή:

```
ping www.cs.ucy.ac.cy -c 100 > /dev/null  &
```

η οποία (ping) αποτελεί μια μέθοδο για τον εντοπισμό της διαθεσιμότητας και της απόδοσης ενός απομακρυσμένου πόρου του δικτύου και αποτελείται από κάποια REQUESTs και κάποια RESPONSEs. Αμέσως μετά την πιο πάνω εντολή τρέχουμε το πιο κάτω:

```
tcpdump -c 100 -XX -tttt -vv > /root/packet
```

για να ξεκινήσει η συλλογή των πακέτων (δεν σημαίνει ότι θα προλάβουμε να δούμε και τα 100 ICMP πακέτα που στάλθηκαν με το ping). Ειδικότερα το transport πρωτόκολλο του κάθε IP πακέτου αναγράφεται στο σημείο «proto X» (όπου X είναι ICMP, TCP ή UDP). Τα περιεχόμενα του αρχείου `/root/packet` έχουν την πιο κάτω μορφή (πιο κάτω φαίνονται πληροφορίες μόνο για 2 πακέτα):

```
2015-01-29 10:07:33.189005 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length
84)
    Asia > clio.cs.ucy.ac.cy: ICMP echo request, id 9759, seq 15, length 64
        0x0000:  0004 ffff 0000 0000 0000 0000 0000 0800  ................
        0x0010:  4500 0054 0000 4000 4001 4d7b 0a10 0f6d  E..T..@.@.M{...m
        0x0020:  c22a 1187 0800 567b 261f 000f b54c ca54  .*....V{&....L.T
        0x0030:  0000 0000 3ae2 0200 0000 0000 1011 1213  ....:...........
        0x0040:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0050:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0060:  3435 3637                                4567
2015-01-29 10:07:33.189878 IP (tos 0x0, ttl 61, id 11862, offset 0, flags [none], proto ICMP (1),
length 84)
    clio.cs.ucy.ac.cy > Asia: ICMP echo reply, id 9759, seq 15, length 64
        0x0000:  0000 ffff 0000 0000 0000 0000 0000 0800  ................
        0x0010:  4500 0054 2e56 0000 3d01 6225 c22a 1187  E..T.V..=.b%.*..
        0x0020:  0a10 0f6d 0000 5e7b 261f 000f b54c ca54  ...m..^{&....L.T
        0x0030:  0000 0000 3ae2 0200 0000 0000 1011 1213  ....:...........
        0x0040:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0050:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0060:  3435 3637
```

Όταν τελειώσει η πιο πάνω εντολή δώστε την εντολή (ή σύνολο εντολών) που βρίσκει και τυπώνει στην οθόνη πόσα TCP πόσα UDP και πόσα ICMP πακέτα στάλθηκαν. Για παράδειγμα:

```
92 ICMP
 6 UDP
 2 TCP
```

Ερώτημα 10

Δημιουργήστε μια λίστα από ΟΛΕΣ τις διεργασίες που εκτελούνται στο σύστημα και φυλάξετε τις στο αρχείο processes.txt. Παράλληλα εκτυπώστε στην οθόνη τις τελευταίες οκτώ (8) γραμμές ταξινομημένες (σε αύξουσα αλφαβητική σειρά) ως προς το όνομα της διεργασίας. Η εντολή δεν γίνεται να χρησιμοποιεί ανακατεύθυνση αλλά μόνο διοχέτευση.

Καλή Επιτυχία !