Διάλεξη 4

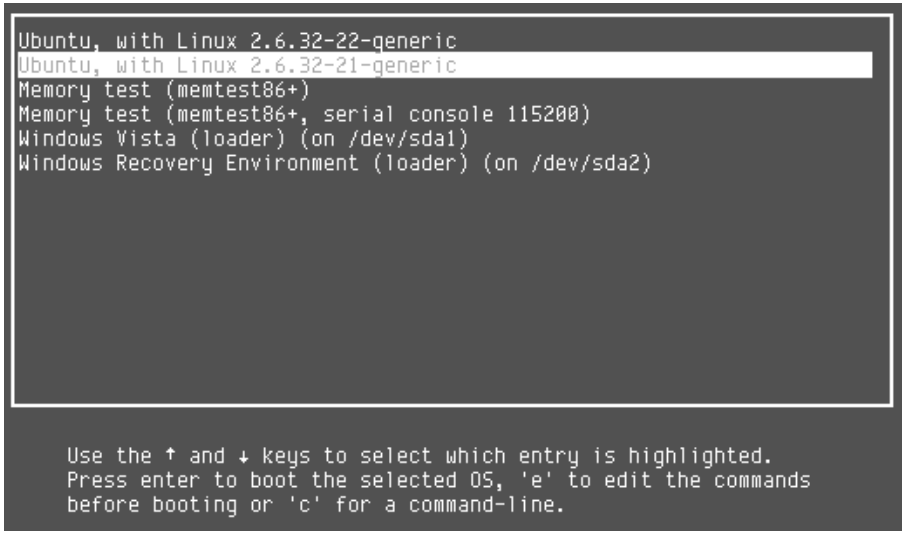
Διαχείριση Συστημάτων UNIX II

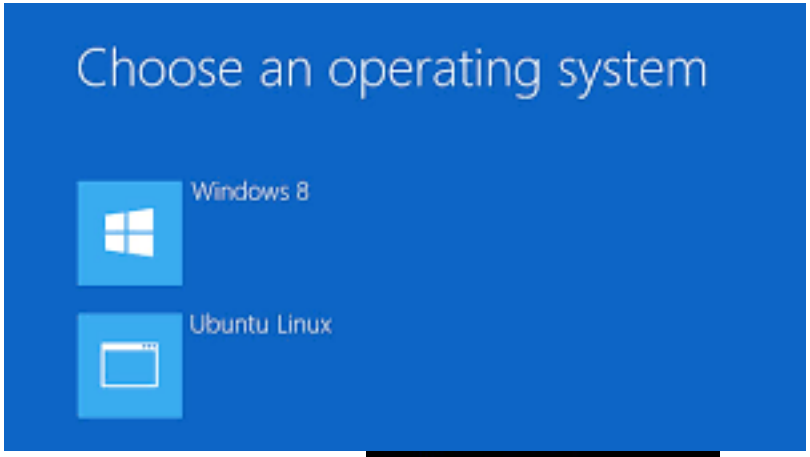
Δημήτρης Ζεϊναλιπούρ

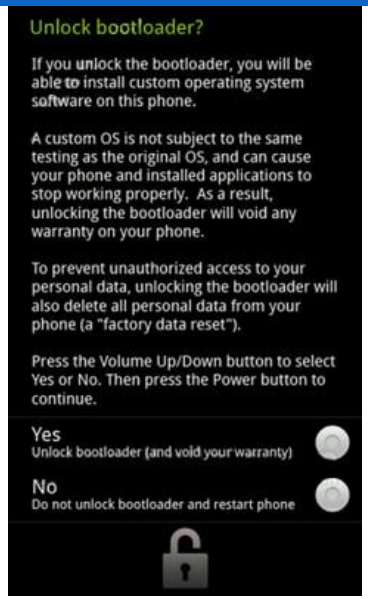
Περιεχόμενο Διάλεξης

- ***Εκκίνηση & Εγκατάσταση Πακέτων:*** *grub, yum, apt-get, port, rpm, dpkg, tzdate*
- ***Δίκτυο:*** *iptables/ufw (Uncomplicated Firewall), tcpdump, nmap, netStat, nslookup, ifconfig, time servers timedatectl / timesyncd, protecting SSH (Fail2Ban)*
- ***Ασφάλεια:*** *ssh-keygen/add, openssl, ssh @RaspberryPI, RSA4096/AES256 and Public/Private Keys, certificates & Let's Encrypt, Apache Virtual Hosts Scenario, SCP*
- ***Ταυτότητες:*** *date, $$, $RANDOM, uuidgen, md5sum, uuencode/uudecode, base64*
- ***Ιστός / HTTP στο UNIX:*** *curl, wget, .htaccess, Pushing Data outside Firewalls*

Εκκίνηση Bootloader (grub)

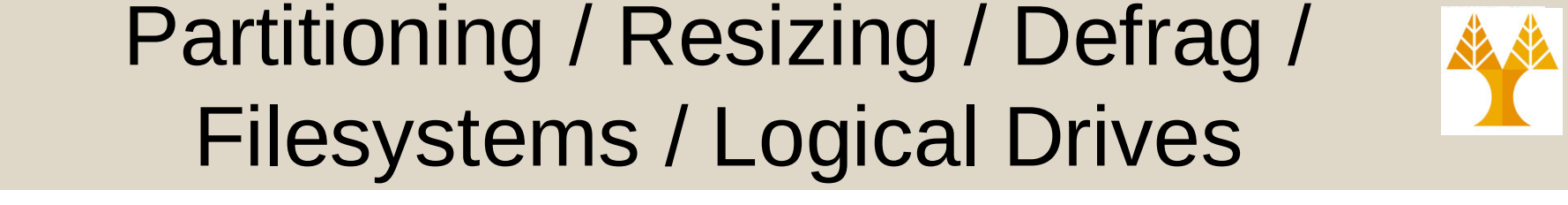




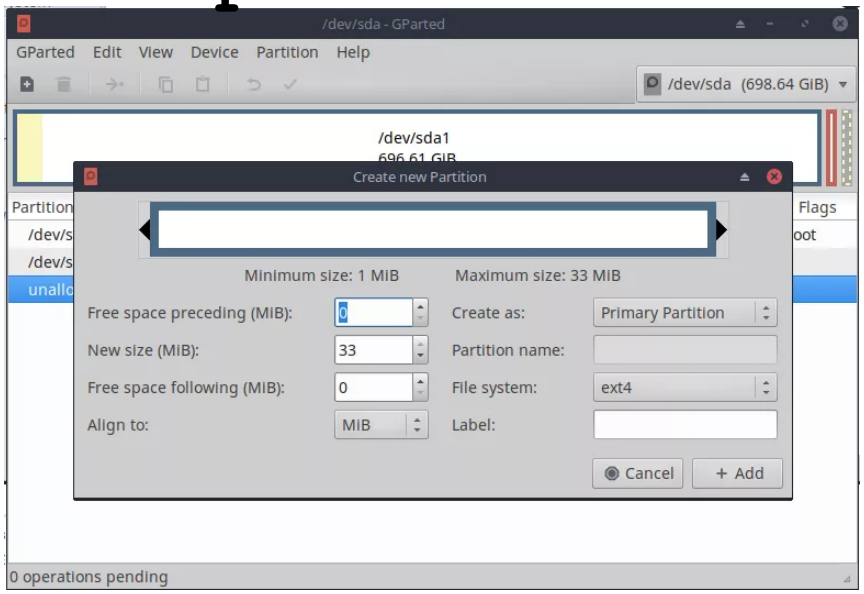


A **boot loader** is a computer program that loads an operating system or some other system software for the computer after completion of the power-on self-tests; it is the loader for the operating system itself.

Partitioning / Resizing / Defrag / Filesystems / Logical Drives



Gparted GUI



- **GParted** is a graphical (plus) front end to the libparted library used by the Parted project. If you want to use the command line then use **parted** instead (note: no **g** in front of name).
- **Parted** is the most sophisticated open source partition resizer,

Command Line with resize2fs

$ df -h

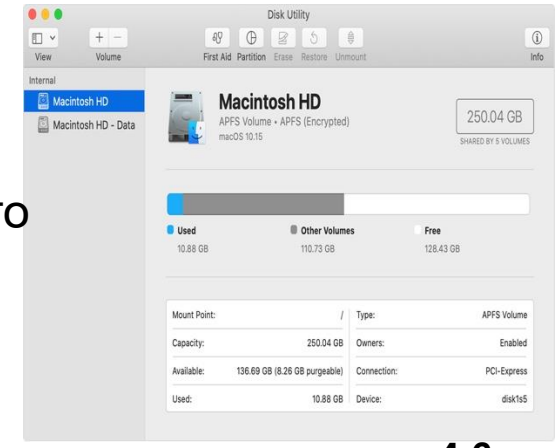
```
> Filesystem                 Size  Used Avail Use% Mounted on
> udev                       3.9G     0  3.9G   0% /dev
> tmpfs                      799M  8.8M  790M   2% /run
> /dev/mapper/AnyplaceDB2--vg-root   51G   21G   28G  44% /
> tmpfs                      3.9G     0  3.9G   0% /dev/shm
> tmpfs                      5.0M     0  5.0M   0% /run/lock
> tmpfs                      3.9G     0  3.9G   0% /sys/fs/cgroup
> /dev/sda1                  472M  467M     0 100% /boot
> tmpfs                      799M     0  799M   0% /run/user/1000
```

$ sudo resize2fs /dev/sda1 450G
$ sudo shutdown -r now

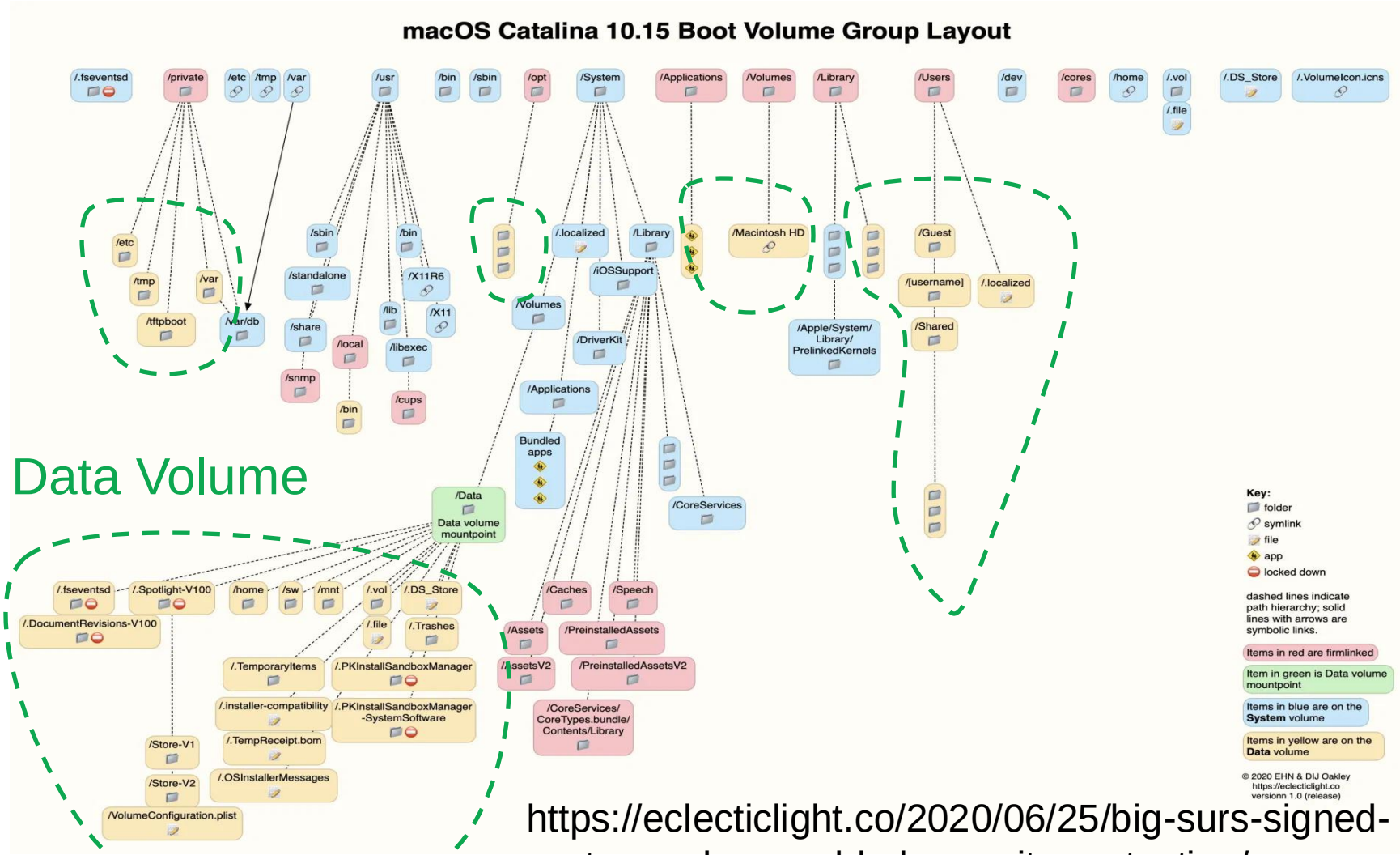
Δομή Καταλόγων MacOS-X

- Παραδοσιακά ακολουθείται η ίδια φιλοσοφία με το UNIX (χωρίς /proc)
- Από την έκδοση Mojave (10.14) η Apple εφαρμόζει πλέον διαμοιρασμό των δεδομένων 2 σε volumes (**System** & **Data**)
  - **Partition:** a logical structure that spans a single disk
  - **Volume:** a logical structure that can span multiple physical disks
  - **APFS Container:** Big Sur's Partition

- Αυτό για να είναι το **System Immutable (mounted Read Only)** και να υπάρχουν λιγότερες απειλές από κακόβουλο λογισμικό.
  - Αργά η βασική ιδέα διαμέρισης του Filesystem στο UNIX ενισχύεται!
  - Υπάρχει και η δυνατότητα για κρυπτογραφημένα partitions (APFS Encrypted).



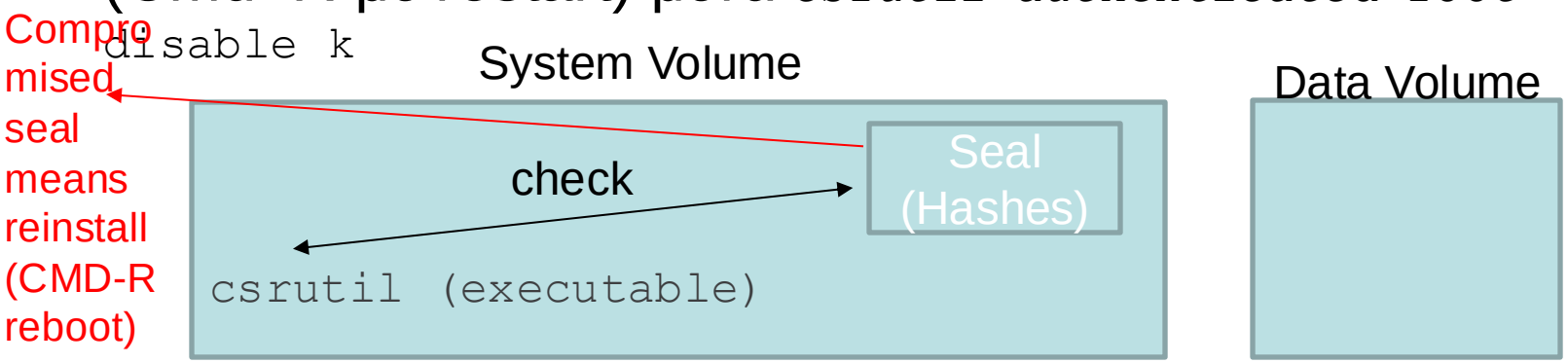
Δομή Καταλόγων MacOS-X
Data vs System Volumes



https://eclecticlight.co/2020/06/25/big-surs-signed-system-volume-added-security-protection/

Δομή Καταλόγων MacOS-X

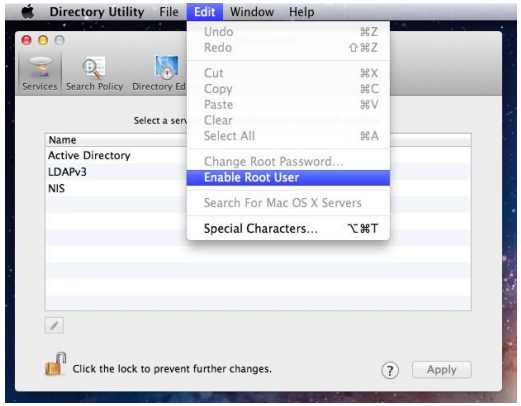
- Στο Big Sur (11.1) εισάγεται και η έννοια του **Signed System Volume (SSV)**.
- Κάθε αρχείο στο Big Sur's System volume έχει και ένα SHA-256 cryptographic hash το οποίο φυλάγεται στις μέτα-πληροφορίες του συστήματος (seal).
  - Επίσης ευκολότερο patching/updates
- Αλλαγές στο SSV απαιτούν boot σε recovery mode (Cmd+R με restart) μετά `csrutil authenticated-root disable k`

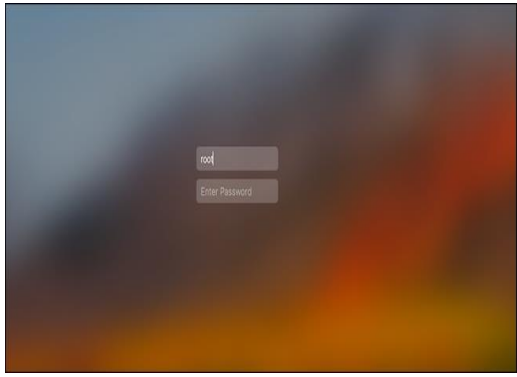


https://eclecticlight.co/2020/06/25/big-surs-signed-system-volume-added-security-protection/

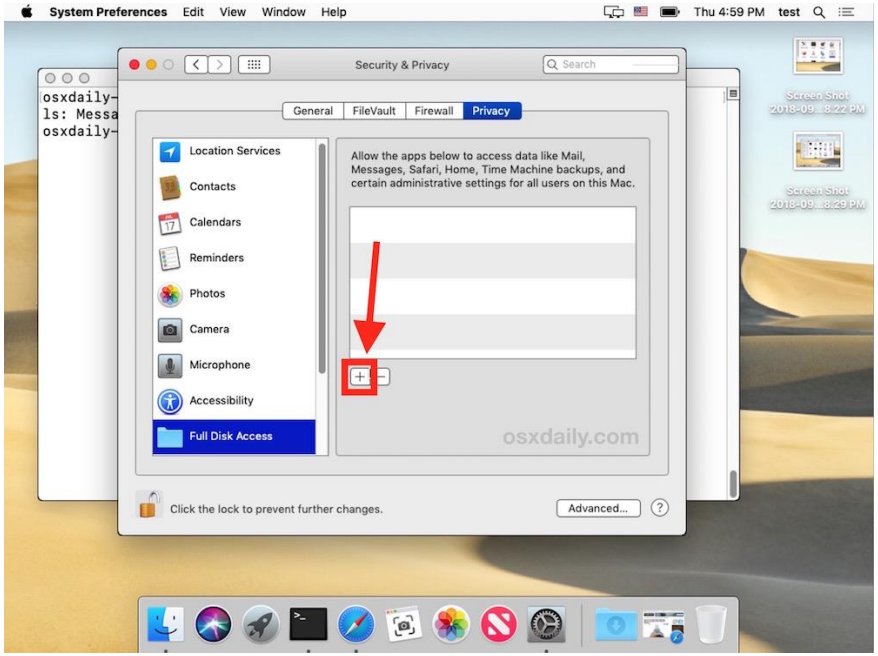
Root Χρήστες στο macOS

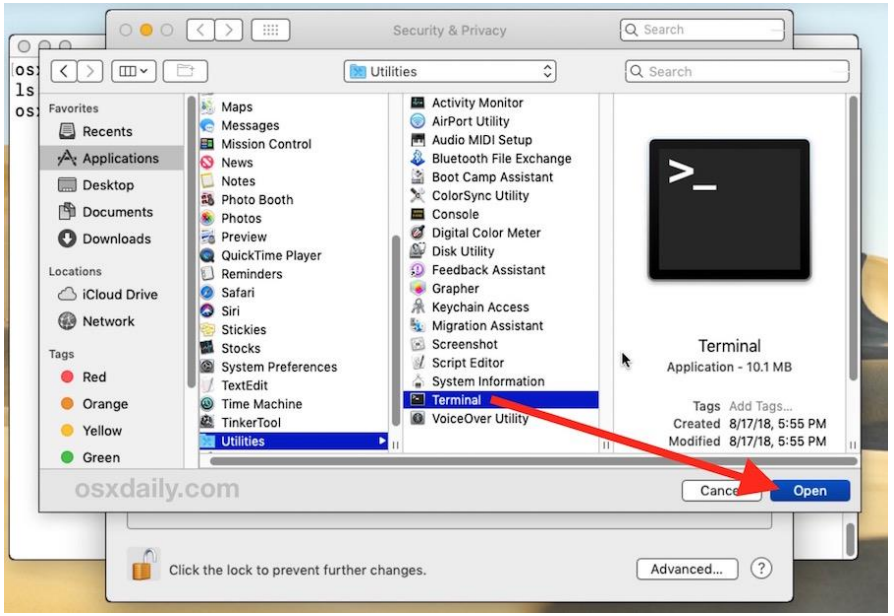
- Πρέπει να έχετε **user** (standard user), **admin** (λογαριασμός εγκατάστασης) και **root** (απενεργοποιημένος αρχικά)
- Το **root** πρέπει να ενεργοποιηθεί για χρήση του **sudo**
- Θα μελετηθεί αργότερα το sudo
  - https://www.howtogeek.com/howto/35132/how-to-enable-the-root-user-in-mac-os-x/
  - https://support.apple.com/guide/directory-utility/about-the-root-user-dirub32398f1/mac





Terminal in MacOS Mojave 10.14 or later

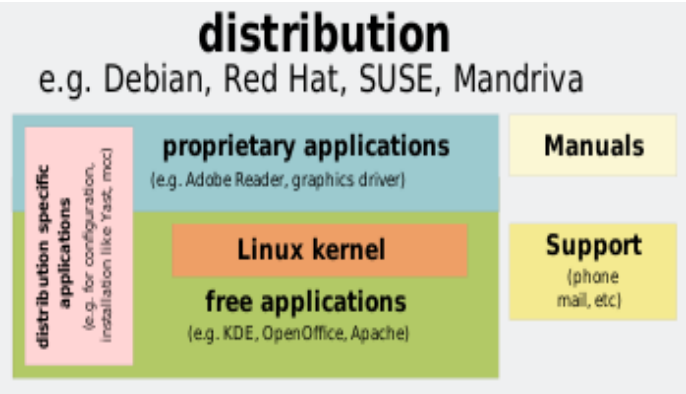


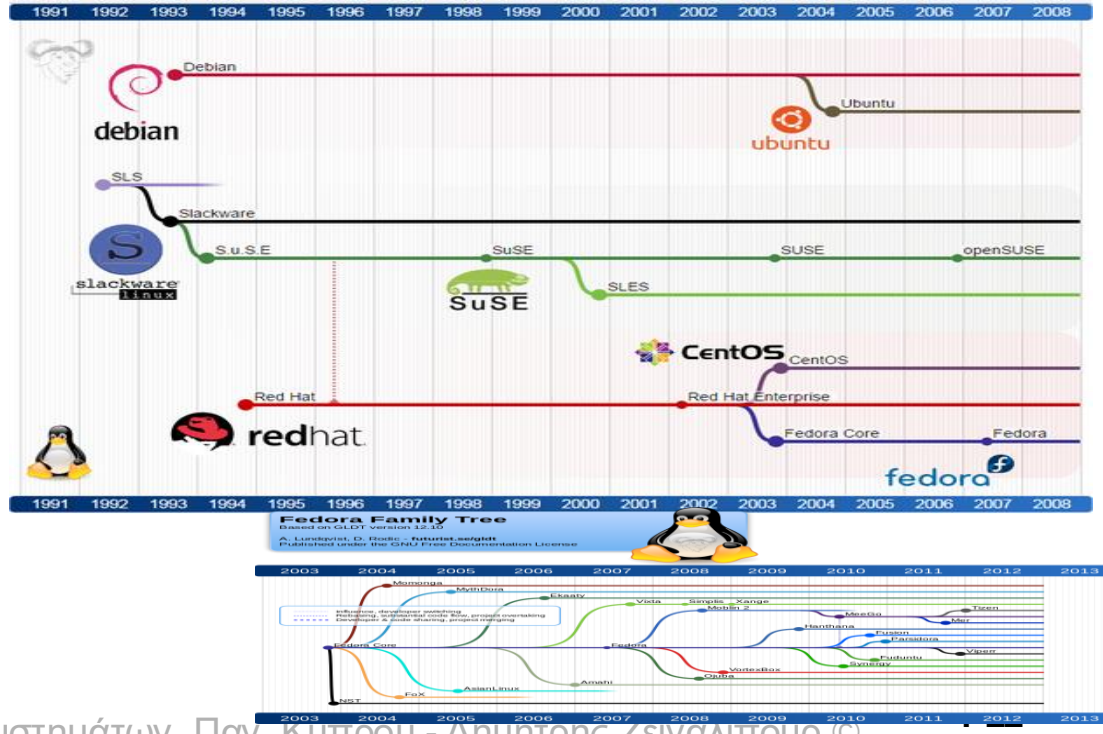


- Remember to ALWAYS execute su, sudo scripts in toy user you created
- Users are always non-root
- Set back to defaults when done

Linux Distributions

- A **Linux distribution** (often abbreviated as **distro**) is an operating system made from a software collection, which is based upon the Linux kernel and, often, a package management system.





Find Distribution:

```
$ cat /etc/*-release
```

Find Kernel:

```
$ uname -a
```

Finding Distribution / Kernel

```
$ cat /etc/*-release
CentOS Linux release 7.4.1708 (Core)
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"
CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"
CentOS Linux release 7.4.1708 (Core)
CentOS Linux release 7.4.1708 (Core)
```

$cat /proc/version

Linux version 5.4.0-96-generic (buildd@lgw01-amd64-051) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #109-Ubuntu SMP Wed Jan 12 16:49:16 UTC 2022

```
$uname -a
Linux b103ws1 3.10.0-693.5.2.el7.x86_64 #1 SMP Fri Oct 20 20:32:50 UTC 2017 x86_64 x86_64
x86_64 GNU/Linux
```

Package Management (rpm, dpkg, wget)

Α) Από πηγαίο κώδικα

- Διαθέσιμο στον ιστό, CVS, Github, κτλ μεταγλωττίζεται με make ή αντίστοιχα **build automation software** (Apache Ant ή Maven / JAVA, GNU Build System / Autotools: Autoconf, Automake, Libtool)
- Συνηθέστερο σε εκδόσεις μη-διαδεδομενα UNIX (π.χ., HP-UX, AIX) αλλά και παλαιότερα στο Linux ή Linux/Android on ARM, κτλ.
- wget [program].tar.gz -> unpack -> ./configure -> make -> make install
- (βλέπε παράδειγμα στην επόμενη διαφάνεια)

Β) Από πακέτα εγκατάστασης:

•Σε RPM (Rocky, Redhat, Fedora, Suse, Madriva, Oracle Linux, CentOS, Scient. Linux)

- Ανάκτηση RPM (Red Hat Package Manager) από ιστό
- rpm –i installer.rpm # Install
- rpm –V installer.rpm # Verify (for conflicts before install)

•Σε non-RPM Linux Distributions

- **Debian Linux: dpkg --install foo_VVV-RRR.deb**
- **Slackwere Linux: installpkg [packagename].tgz**

>> Mirrors

Παράδειγμα Εγκατάστασης Python 3.8 από Πηγαίο Κώδικα σε Raspberry

- First install the dependencies needed to build:
  - `sudo apt-get update; sudo apt-get install -y build-essential tk-dev libncurses5-dev libncursesw5-dev libreadline6-dev libdb5.3-dev libgdbm-dev libsqlite3-dev libssl-dev libbz2-dev libexpat1-dev liblzma-dev zlib1g-dev libffi-dev`
- Compile (yes… it takes a while)
  - `wget https://www.python.org/ftp/python/3.8.0/Python-3.8.0.tar.xz;`
  - `tar xf Python-3.8.0.tar.xz`
  - `cd Python-3.8.0`
  - `./configure --enable-optimizations --prefix=/usr`
  - `make`
- Let's install what was compiled!
  - `sudo make altinstall`
- And remove the files you don't need anymore
  - `cd .. ; sudo rm -r Python-3.8.0 ; rm Python-3.8.0.tar.xz; . ~/.bashrc;`
  - `# verify` python -V

Package Management (yum, apt-get, port)

Γ) Από βιβλιοθήκες πακέτων

- RPM Linux: **`yum search <package>`**
  - yum is an additional wrapper around rpm. It keeps its own database of rpm files available for your distribution, generally in online repositories.
- DEBIAN Linux: **`apt-get search <package>`**
  - On Debian systems, the equivalent repository and dependency-resolution tools are provided by Apt (apt-get and aptitude).
- MACOSX (Macports Project – requires Xcode/sudo):
  - **`sudo port search <package>`**
  - **`sudo port install <package>`**
  - sudo port select --set python python35
  - A more limited package manager for MacOSX is called homebrew (brew/ruby)

Mirroring YUM Repositories

- How to Setup Local HTTP Yum Repository on CentOS 7?
  - https://www.tecmint.com/setup-local-http-yum-repository-on-centos-7/
- Server
  - Install Apache, Nginx or other HTTP server
  - mkdir -p /var/www/html/repos/{base,centosplus,extras,updates}
  - reposync -g -l -d -m --repoid=base --newest-only --download-metadata
  - createrepo -g comps.xml /var/www/html/repos/base/
  - vim /etc/cron.daily/update-localrepos # cron daily
- Client
  - # vim /etc/yum.repos.d/local-repos.repo # Add new server
  - yum repolist all # check if new mirror is ok on client

Time Servers & NTP Port 123

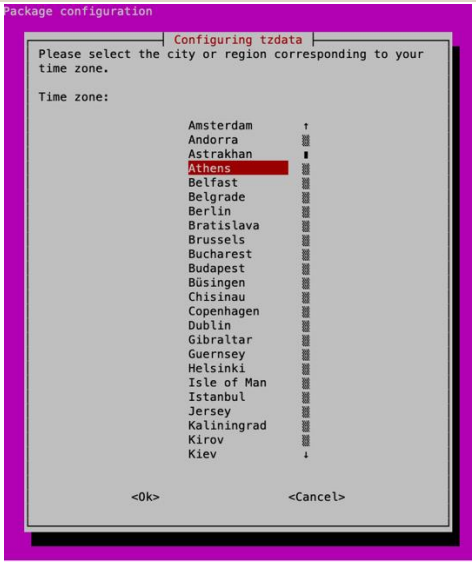
- **IANA time zone database.**
- **vgate@vgate**:~$ date
- Thu Oct 24 06:56:47 UTC 2024
- **vgate@vgate**:~$ sudo apt-get update

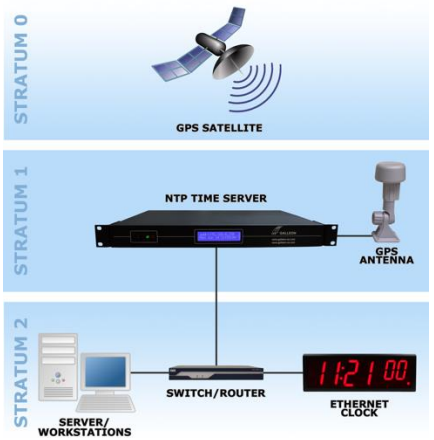
Reading package lists… Done

- **vgate@vgate**:~$ sudo apt-get install tzdata
- **vgate@vgate**:~$ sudo dpkg-reconfigure tzdata

- Current default time zone: 'Europe/Athens'
- Local time is now: Thu Oct 24 09:58:24 EEST 2024.
- Universal Time is now: Thu Oct 24 06:58:24 UTC 2024.

- **vgate@vgate**:~$ date
- Thu Oct 24 09:58:28 EEST 2024





Port 123

- time.google.com
- time.apple.com
- time.Microsoft.com
- ntp.ubuntu.com

….

https://gist.github.com/mutin-sa/eea1c396b1e610a2da1e5550d94b0453

Ubuntu uses **timedatectl / timesyncd**

```
vgate@vgate:~$ timedatectl timesync-status
       Server: 185.125.190.56 (ntp.ubuntu.com)
Poll interval: 34min 8s (min: 32s; max 34min 8s)
         Leap: normal
      Version: 4
      Stratum: 2
    Reference: 11FD1C7B
    Precision: 1us (-25)
Root distance: 930us (max: 5s)
       Offset: -1.875ms
        Delay: 56.552ms
       Jitter: 4.390ms
 Packet count: 73
    Frequency: +18.293ppm
```

Τερματισμός Λ.Σ.
Εντολή **shutdown**

- **shutdown** -- close down the system at a given time
  - The **shutdown** utility provides an automated shutdown procedure for super-users to nicely (SIGTERM – Signal #2) notify users when the system is shutting down.
- `$shutdown –r now`
  - # Restart System now
- `$shutdown –r +number or yymmddhhmm`
  - # Restart at specific time
  - `+number`: brings system down in number minutes.
- `$shutdown –h now`
  - # Halt (Stop) system now (don't use on VPS as you won't have a way to restart.

* Computer Capacitors (Πυκνωτές) – small in size - require a few seconds to discharge, so shutdown –h and counting a few seconds might be the only way for a true hardware shutdown. A photovoltaic inverter (jumbo) capacitor might need 15 minutes to fully discharge!

Sleep/ Hibernate/ Shutdown

- **Hibernate Mode**: It writes all active data to the disk and then switches off the components as if the computer were fully turned off.
  - You can cut the the power of a system in hibernation, since it does not pose any risk to your data. Once the computer is powered back on it reads the data from disk and sends them back to RAM—this process can take few seconds to minutes. The data is restored to the point at which they entered hibernation. (good when boarding a plane or travelling).
  - pmset –a hibernatemode 0
    - Memory ON, no image on disk # sleep-mode!
  - **pmset –a hibernatemode 3 (default)**
    - Image on disk, Memory on => instant boot!
  - pmset –a hibernatemode 25 (best for battery)
    - Full Image on disk, **ALL Components OFF**

Setting Shutdown modes on MacOSX

```
$ pmset -g
System-wide power settings:
Currently in use:
 lidwake               1
 autopoweroff          1
 standbydelayhigh      86400
 autopoweroffdelay     28800
 standbydelaylow       10800
 standby               1
 ttyskeepawake         1
 hibernatemode         25
 powernap              1
 gpuswitch             2
 hibernatefile         /var/vm/sleepimage
 highstandbythreshold 50
 womp                  0
 displaysleep          60
 networkoversleep      0
 sleep                 60
 tcpkeepalive          0
 halfdim               1
 acwake                0
 disksleep             10
```

Sleep/ Hibernate/ Shutdown

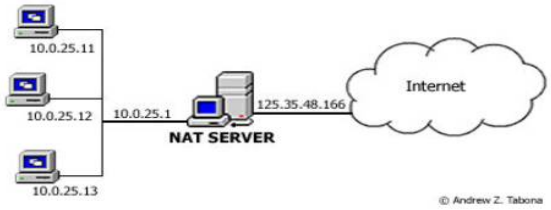
- **sudo pmset -a tcpkeepalive 0**
  - Warning: This option disables TCP Keep Alive mechanism when sytem is sleeping. This will result in some critical features like 'Find My Mac' not to function properly
- sudo pmset -a womp 0
  - womp wake on "magic" Ethernet packet, 1 to enable or 0 to disable
- More: https://en.wikipedia.org/wiki/Pmset

Setting Shutdown modes on MacOSX

```
$ pmset -g
System-wide power settings:
Currently in use:
 lidwake              1
 autopoweroff         1
 standbydelayhigh     86400
 autopoweroffdelay    28800
 standbydelaylow      10800
 standby              1
 ttyskeepawake        1
 hibernatemode        25
 powernap             1
 gpuswitch            2
 hibernatefile        /var/vm/sleepimage
 highstandbythreshold 50
 womp                 0
 displaysleep         60
 networkoversleep     0
 sleep                60
 tcpkeepalive         0
 halfdim              1
 acwake               0
 disksleep            10
```

Διαχείριση Δικτύου ipTables

- Εντολή ***ipTables***
  - Administration tool for IPv4 packet filtering. Provides means to setup a “firewall” on UNIX Systems.
  - It also allows Network Address Translation (NAT): a way to map an entire network (or networks) to a single IP address.
- **Iptables** is used to set up, maintain, and inspect the tables of IPv4 packet filter rules in the Linux kernel.



- **Several different tables may be defined.**
  - Each table contains a number of **built-in chains and may also contain user-defined chains.**

Διαχείριση Δικτύου ipTables

 # Start/Stop/Restart iptables service

•/etc/init.d/iptables start/stop/restart

 # LIST all configurations of INPUT chain (initially empty)

•sudo iptables -L INPUT

 # Adding & Removing Rules:

•sudo iptables -D INPUT # DELETE ALL RULES

•sudo iptables -L INPUT # LIST ALL RULES

•sudo iptables -A INPUT # ADD ALL RULES

Protecting Server ipTables

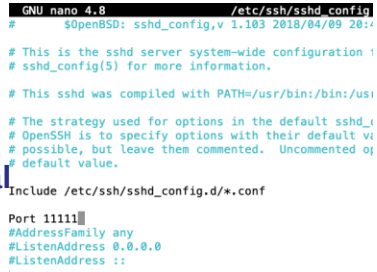
```
# backup current rules & display on screen
sudo iptables -S | tee ~/.iptables.log.$(date '+%F_%H:%M:%S')

# drop all existing rules
# sudo iptables -P INPUT DROP
# sudo iptables -P FORWARD DROP
# sudo iptables -P OUTPUT DROP

# http and https traffic - remember to enable apached
sudo iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j
ACCEPT
sudo iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j
ACCEPT
sudo iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j
ACCEPT

# custom server, e.g., Jupyter Notebook Single User Server
sudo iptables -A INPUT -i eth0 -p tcp --dport 8888 -m state --state NEW,ESTABLISHED -j
ACCEPT
sudo iptables -A OUTPUT -o eth0 -p tcp --sport 8888 -m state --state ESTABLISHED -j
ACCEPT

# ssh
sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

# list final rules
```

Final Check!

```
$ nmap -P0 dmslv100.in.cs.ucy.ac.cy
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-21 10:13 UTC
Nmap scan report for dmslv100.in.cs.ucy.ac.cy (10.16.20.13)
Host is up (0.00055s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https
8888/tcp closed sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds
```

Protecting SSHD / Fail2Ban

- **A) Change Default port** from 22 to some number >1024 (now only nmap can find that ssh is enabled
  - **sudo nano /etc/ssh/sshd_config**
  - **sudo ufw allow 11111/tcp**
  - **sudo ufw deny 22/tcp # ufw (uncomplicated firewal**
  - **sudo ufw reload**
  - **sudo ufw enable; sudo ufw status;**
  - **sudo shutdown –r now**

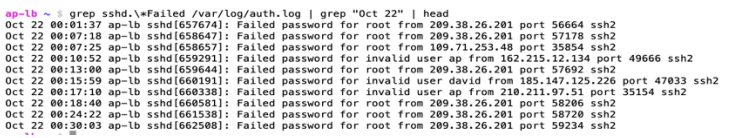


ssh -l name
server.name -p 11111

- **B) Enable Fail2Ban:** scans log files like /var/log/auth.log and bans IP addresses conducting too many failed login attempts. It does this by updating system firewall (e.g., banning for 10 min the user)
  - **sudo apt update**
  - **sudo apt install fail2ban**
  - **systemctl status fail2ban.service**
  - **cd /etc/fail2ban**
  - **sudo cp jail.conf jail.local**
  - **sudo systemctl restart fail2ban.service**
  - **sudo systemctl status fail2ban.service**

Finding Attacks!

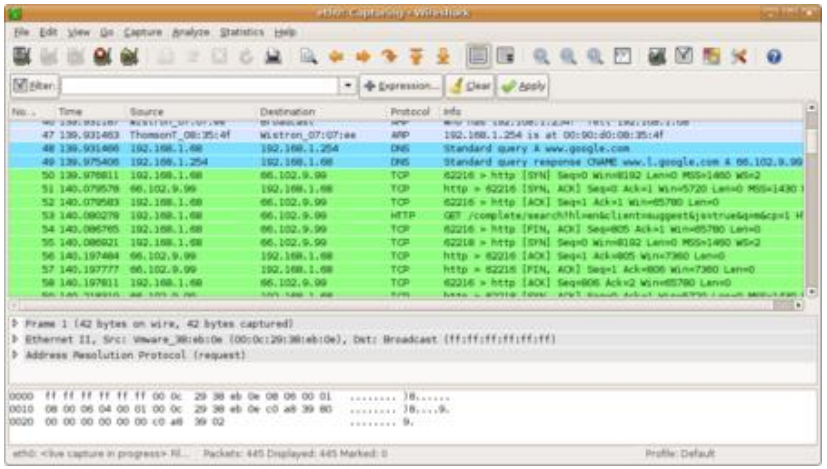
grep sshd.*Failed /var/log/auth.log | grep "Oct 22" | head



- **C) Enable WireGuard:** lightweight Virtual Private Network (VPN) that supports IPv4 and IPv6 connections In front of ssh.
  - More: https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-20-04

Διαχείριση Δικτύου TCPDump

- **tcpdump** is a common **packet** analyzer that runs under the command line.
  - It allows the user to display **TCP**/IP and other packets being transmitted or received over a network to which the computer is attached.
- tcpdump uses the libpcap library to capture packets
- **Libpcap** is also used in Wireshark (prior Ethereal).
  - The port of tcpdump for Windows
- Requires **root** access to install it, as it is installed libpcap is installed very low in the OS stack (kernel).



Διαχείριση Δικτύου
Tcpdump Example

```
$ ifconfig | head
eth2      Link encap:Ethernet  HWaddr 52:54:00:7B:CA:99
          inet addr:10.16.1.101  Bcast:10.16.1.127  Mask:255.255.255.224
          inet6 addr: fe80::5054:ff:fe7b:ca99/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:214252728 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148649576 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:156620098878 (145.8 GiB)  TX bytes:93799079896 (87.3 GiB)

lo        Link encap:Local Loopback

Receive packets flows on a particular port using tcpdump port
$ tcpdump -i eth0 port 22

19:44:44.934459 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.63897: P
18932:19096(164) ack 105 win 71 19:44:44.934533 IP valh4.lell.net.ssh >
zz.domain.innetbcp.net.63897: P 19096:19260(164) ack 105 win 71
19:44:44.934612 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.63897: P
19260:19424(164) ack 105 win 71

# Capture packets for particular destination IP and Port
$tcpdump -w xpackets.pcap -i eth0 dst 10.181.140.216 and port 22
```

Διαχείριση Δικτύου
nMap Port Scanner

- **Nmap is a security scanner**
  - Most well known port scanner on Unix.

https://zmap.io/ aster Nmap: With a 10gigE connection and ZMap can scan the IPv4 address space in 5 minutes.!

- **Features:**
  - **Host discovery** – Identifying hosts on a network. (e.g., listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
  - **Port scanning** – Enumerating the open ports on target hosts.
  - **Version detection** – Interrogating network services on remote devices to determine application name and version number.
  - **OS detection** – Determining the operating system and hardware characteristics of network devices.
- **Usage:**
  - Auditing, Find and exploit vulnerabilities, Generating traffic to hosts on a network, Network inventory, network mapping, maintenance and asset management.

Διαχείριση Δικτύου
Nmap Example

```
$ nmap  www.cs.ucy.ac.cy

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-11 22:06 EET
Nmap scan report for www.cs.ucy.ac.cy (194.42.17.135)
Host is up (0.00092s latency).
rDNS record for 194.42.17.135: clio.cs.ucy.ac.cy
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3128/tcp open  squid-http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.12 seconds
```

Διαχείριση Δικτύου
Ping (Host Latency)

- **Ping** is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer and back.
- A host might not respond to ICMP (ping) messages!
  - ICMP is a subprotocol of IP.
- **Example:**

```
$ ping www
PING clio.cs.ucy.ac.cy (194.42.17.135) 56(84) bytes of data.
64 bytes from clio.cs.ucy.ac.cy (194.42.17.135): icmp_seq=1 ttl=64
   time=0.883 ms
64 bytes from clio.cs.ucy.ac.cy (194.42.17.135): icmp_seq=2 ttl=64
   time=0.942 ms
64 bytes from clio.cs.ucy.ac.cy (194.42.17.135): icmp_seq=3 ttl=64
   time=0.873 ms
```

Διαχείριση Δικτύου
Traceroute (Path Latency)

- **traceroute** is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
- Quite similar to ping, but shows intermediate routers that respond to traceroute requests.

- **Example:**

three round trip times in milliseconds.

```
$ traceroute www.cs.ucr.edu
traceroute to thoth.cs.ucr.edu (169.235.30.15), 64 hops max, 52 byte packets
 1  10.16.16.254 (10.16.16.254)  1.720 ms  1.182 ms  1.144 ms
 2  cs-sw7.cs.ucy.ac.cy (194.42.17.65)  1.128 ms  0.836 ms  0.778 ms
 3  194.42.0.139 (194.42.0.139)  1.046 ms  1.001 ms  1.012 ms
 4  194.42.0.42 (194.42.0.42)  1.260 ms  1.109 ms  1.055 ms
 5  ip6.vega2.ucy.ac.cy (194.42.13.150)  1.300 ms  1.370 ms  1.328 ms
 6  82.116.192.190 (82.116.192.190)  1.335 ms  1.577 ms  1.463 ms
 7  cynet-ap2.mx1.fra.de.geant.net (62.40.124.149)  58.767 ms  58.830 ms
58.739 ms
```

Διαχείριση Δικτύου netStat (Network Statistics)

- **netstat** (***net****work* ***stat****istics*) is a command-line tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics
- **Example:**

```
$ netstat
•  tcp4       0      0  cs.in.cs.ucy.49526 ec2-52-185-66.https CLOSE_WAIT
•  tcp4       0      0  cs.in.cs.ucy.49515 wk-in-f94..https ESTABLISHED
•  tcp4       0      0  cs.in.cs.ucy.49506 theano.cs.ucy.ac.imap  ESTABLISHED
•  tcp4       0      0  cs.in.cs.ucy.49473 ec2-52-2-24.https CLOSE_WAIT
•  tcp4       0      0  cs.in.cs.ucy.49471 17.172.232.9.5223      ESTABLISHED
•  tcp4       0      0  cs.in.cs.ucy.49379 17.110.225.84.5223     ESTABLISHED
•  tcp4      31      0  cs.in.cs.ucy.49373 45.58.74.129.https     CLOSE_WAIT
•  tcp4       0      0  cs.in.cs.ucy.49230 theano.cs.ucy.ac.imap  ESTABLISHED
```

Διαχείριση Δικτύου
Nslookup (DNS Resolution)

- **nslookup** is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

Example:

```
$ nslookup www.google.com
```

```
$ nslookup www.google.com
Server:                 10.16.1.118
Address:        10.16.1.118#53

Non-authoritative answer:
Name: www.google.com
Address: 74.125.206.147
Name: www.google.com
Address: 74.125.206.106
Name: www.google.com
Address: 74.125.206.105
Name: www.google.com
Address: 74.125.206.104
```

Διαχείριση Δικτύου (Ifconfig - Network Settings)

- **ifconfig** is a system administration utility in Unix-like operating systems for network interface configuration. (Windows: ipconfig /all)
- **Example:**
- $ ifconfig

```
en2: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=4<VLAN_MTU>
    ether 10:9a:dd:42:59:19
    inet6 fe80::129a:ddff:fe42:5919%en2 prefixlen 64 scopeid 0x4
    inet 10.16.16.188 netmask 0xffffff00 broadcast 10.16.16.255
    nd6 options=1<PERFORMNUD>
    media: autoselect (100baseTX <full-duplex,flow-control>)
    status: active
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether a8:66:7f:29:09:27
    inet6 fe80::aa66:7fff:fe29:927%en0 prefixlen 64 scopeid 0x5
    inet 10.16.4.248 netmask 0xfffffe00 broadcast 10.16.5.255
    nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
```

Public/Private RSA Keys (used for SSH)

- Generate Keys on PC

```
$ mkdir -p ~/.ssh # if not already created
$ chmod 700 ~/.ssh; cd ~/.ssh
$ ssh-keygen -t rsa-sha2-256 -b 4096
# Generate rsa|dsa key
```

  - Enter file in which to save the key **(/home/user/.ssh/id_rsa):**
  - Enter passphrase (empty for no passphrase): Enter same passphrase again:
  - Your identification has been saved in **/home/user/.ssh/id_rsa.**
  - Your public key has been saved in **/home/user/.ssh/id_rsa.pub.**

- Transfer **id_rsa.pub** to SERVER.

```
$cat id_rsa.pub >> .ssh/authorized_keys; chmod 600
   .ssh/authorized_keys
```

- Add **ssh/id-rsa** to PC keychain

```
$ssh-add -K ~/.ssh/id-rsa
```

- **Troubleshooting!**

```
$ssh -vvv -l <user> <host> # 3 levels of verbose / debugging -v, -
   vv, -vvv, -l: different login name
```

- AES. The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government, as well as other organizations. ...
- Triple DES. ...
- RSA. ...
- Blowfish. ...
- Twofish. ...
- Rivest-Shamir-Adleman (RSA).

- AE

Public/Private RSA Keys (~/.ssh/known_hosts)

When we connect to some node, we are requested to validate its authenticity. The given is recorded in the known_hosts file.

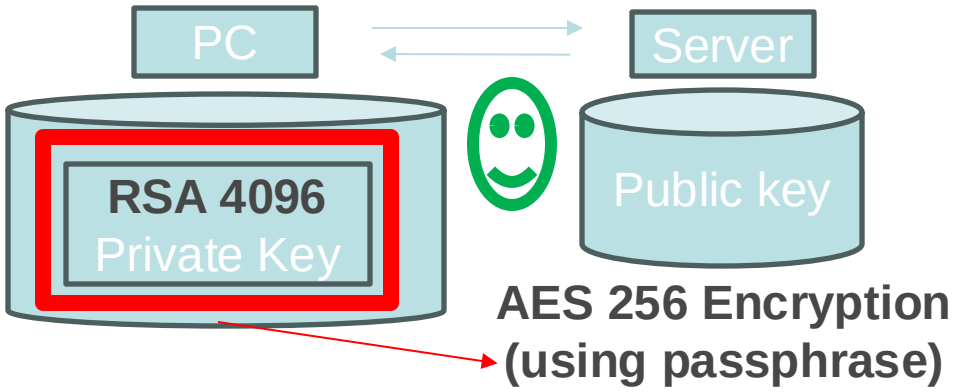
```
$ ssh b103ws6
The authenticity of host 'b103ws6 (10.16.6.243)' can't be established.
RSA key fingerprint is 01:9a:eb:42:02:ca:b4:cc:c0:c3:58:2c:49:85:45:e4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'b103ws6,10.16.6.243' (RSA) to the list of known
hosts.
```

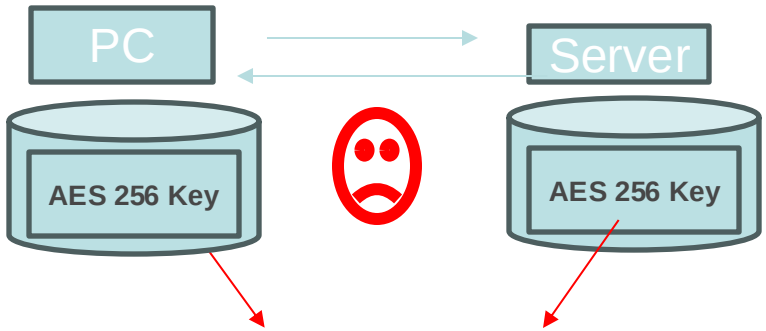
```
$tail ~/.ssh/known_hosts
b103ws6,10.16.6.243 ssh-rsa
AAAAAABIwAAAQEAtrjdSBK4Q60/7PtKRfotLLrxnqWG1QAMqLPtQFUZhV08fdQJANS4BoANYp9A
AvMPGME8tz1Ko0hIm9FkNFm5jDoXa3NkiUC/wbcqa8IwrW4kAI61m4PMpMYVDpPGk9/QvgzzBYK
cAvUHMMyfzHvWq2AQRHVcaeFafQEL9s343mUHlBhVe…
```

Why? If some attacker masquerates that IP/node, we will know as the RSA key fingerprint of the attacker won't match

AES256 Symmetric Cryptography

- AES128/256 (Advanced Encryption Standard with 256-bit key) is a widely used encryption algorithm designed to protect data through symmetric key cryptography.
  - AES-256 is not considered fully "quantum-proof," but the closest!
- Not used as **substitute** to asymmetric RSA Public/Private Cryptography, rather complementary used **to stronger local encryption** of **private key**






```
> openssl rsa -in private_key.pem -aes256 -out
encrypted_private_key.pem
```

Enter PEM pass phrase: Verifying - Enter PEM pass phrase:

> Similar idea with Elliptic Curves:

openssl ec -in encrypted_ec_private_key.pem -out decrypted_ec_private_key.pem

Generating Strong Passwords

- Many users rely on the generation of STRONG passwords from public websites.
- This is dangerous as those passwords might be logged into databases exploited later by hackers …
- Use the safe way (generate on your own system):

```
$ openssl rand -base64 6
ZP9o9rBI
```

Why 6? Many programs require 8 chars at most. Password truncated to 8 characters by CRYPT algorithm.

The above command will generate a **6 byte random value** encoded with base64.

You can count the number of characters in the above random value by decoding it using command

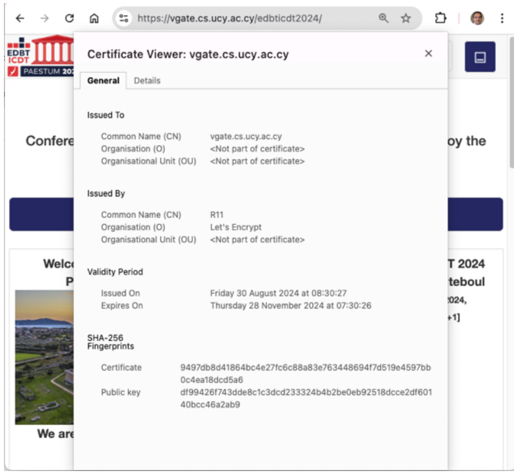
```
– echo "ZP9o9rBI" | base64 -d | wc -c 6
```

Πιστοποιητικά ασφαλείας (Certificates / openssl)

- Στην Κρυπτογραφία, ένα **public key certificate,** γνωστό ως **digital certificate** ή **identity certificate,** είναι ένα ηλεκτρονικό αρχείο το οποίο χρησιμοποιείται για το **ownership** (ιδιοκτησία) ενός **public key.**
  - **OpenSSL** περιέχει μια ανοικτού πηγαίου υλοποίησή των πρωτοκόλλων **SSL** και **TLS** (κρυπτογραφημένη επικοινωνία μεταξύ διαδικτυακών κόμβων)
  - Παράδειγμα Εξέτασης certificate : `openssl s_client -showcerts -connect www.cs.ucy.ac.cy:443`
  - Δημιουργία του δικού σας Certificate & Εγκατάσταση στο Server σας: Συνήθως έχει κάποιο κόστος εφόσον απαιτεί κάποιο γνωστό Certification Authority.
  - Το https://letsencrypt.org/ σας δίνει τη δυνατότητα να δημιουργήσετε δωρεάν – βλέπε vgate case and certificate chains

Let's Encrypt Certificate

- Step 1 — Installing Certbot
  - `sudo apt install certbot python3-certbot-apache`
- Step 2 — Checking your Apache Virtual Host Configuration
  - sudo nano /etc/apache2/sites-available/your_domain.conf
  - sudo apache2ctl configtest
  - sudo systemctl reload apache2
- Step 3 — Allowing HTTPS Through the Firewall
  - sudo ufw status
  - sudo ufw allow 'Apache Full'
  - sudo ufw delete allow 'Apache'
- Step 4 — Obtaining an SSL Certificate
  - sudo certbot –apache
  - Which names would you like to activate HTTPS for? - 1: your_domain 2: www.your_domain
  - Please choose whether or not to redirect HTTP traffic to HTTPS, choose 2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for

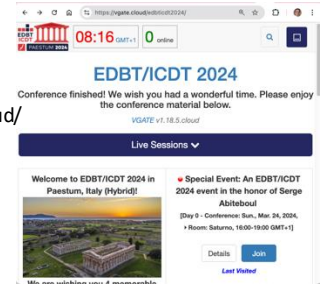


- Step 5 — Verifying Certbot Auto-Renewal
  - sudo certbot renew --dry-run
  - https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-20-04

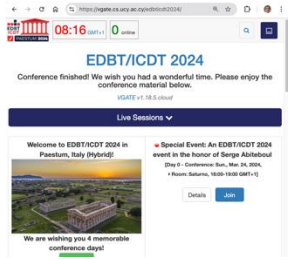
Apache Virtual Host with Certificate Scenario

- Two Web Portals with 1 Server Scenario

/etc/apache2/sites-enabled/**vgate.cloud.conf**
sudo apache2ctl configtest
sudo service apache2 restart




```
<VirtualHost 143.42.58.208>
    ServerName vgate.cloud
    ServerAdmin vgate@vgate.cloud
    DocumentRoot /var/www/html
                Redirect permanent / https://vgate.cloud/
                ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
<VirtualHost vgate.cloud:80>
    ServerName vgate.cloud
    ServerAdmin vgate@vgate.cloud
    DocumentRoot /var/www/html
    RewriteEngine on
    RewriteCond %{SERVER_NAME} =vgate.cloud
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
<VirtualHost vgate.cloud:443>
    ServerName vgate.cloud
    ServerAdmin vgate@vgate.cloud
    DocumentRoot /var/www/html
                SSLEngine on
                SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
                SSLHonorCipherOrder on
                SSLCipherSuite
ECDH+AESGCM:ECDH+CHACHA20:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES1
28:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!AESCCM
                SSLCertificateFile /etc/letsencrypt/live/vgate.cloud/cert.pem
                SSLCertificateKeyFile
/etc/letsencrypt/live/vgate.cloud/privkey.pem
                SSLCertificateChainFile
/etc/letsencrypt/live/vgate.cloud/chain.pem
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```




```
<VirtualHost vgate.cs.ucy.ac.cy:80>
    ServerName vgate.cs.ucy.ac.cy
    ServerAdmin vgate@vgate.cloud
    DocumentRoot /var/www/html
    RewriteEngine on
    RewriteCond %{SERVER_NAME} =vgate.cs.ucy.ac.cy
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
<VirtualHost vgate.cs.ucy.ac.cy:443>
    ServerName vgate.cs.ucy.ac.cy
    ServerAdmin vgate@vgate.cloud
    DocumentRoot /var/www/html
    Redirect permanent / https://vgate.cloud/
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLHonorCipherOrder on
    SSLCipherSuite
ECDH+AESGCM:ECDH+CHACHA20:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES
128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!AESCCM
    SSLCertificateFile /etc/letsencrypt/live/vgate.cs.ucy.ac.cy/cert.pem
    SSLCertificateKeyFile  /etc/letsencrypt/live/vgate.cs.ucy.ac.cy/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/vgate.cs.ucy.ac.cy/chain.pem
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Secure File Transfer **(SCP)**

- **scp** copies files between hosts on a network.
  - It uses ssh for data transfer, and uses the same authentication and provides the same security as ssh.
- Many protocols for File Transfer => the older were not unecrypted, but the newer introduced encryption.
  - e.g., FTP evolved to i) **FTP-SSL (FTPS);** ii) **SSH FTP (SFTP);** iii) **FTP over SSH** (i.e., tunneling FTP through an SSH connection - see next slide)
  - FTP originally had two channels (authentication and data transfer): encryption can apply to either channel or both.

Secure File Transfer (SCP)

- Here we focus on a single tool, i.e., scp, similar concepts with other tools as well.
  - Transfer Data from Production to Development server:
- `scp anyplace@ap.cs.ucy.ac.cy:/home/anyplace/anyplace_v3/floor_plans.tar.gz /home/anyplace/anyplace_v3/floor_plans.tar.gz`
  - Having the public/private key in place will circumvent the requirement of giving user/pass each time

SSH Port Forwarding (SSH Tunelling)

- SSH port forwarding is a mechanism in SSH for tunneling application ports from the client machine to the server machine, or vice versa.
- Usage:
  - *Adding encryption to legacy applications* e.g., you have a proprietary protocol that is not encrypted => you tunnel it over SSH to make it secure from eavesdropping!
  - *Opening backdoors* into the internal network from their home machines. (Dangerous as we bypass the Firewall)

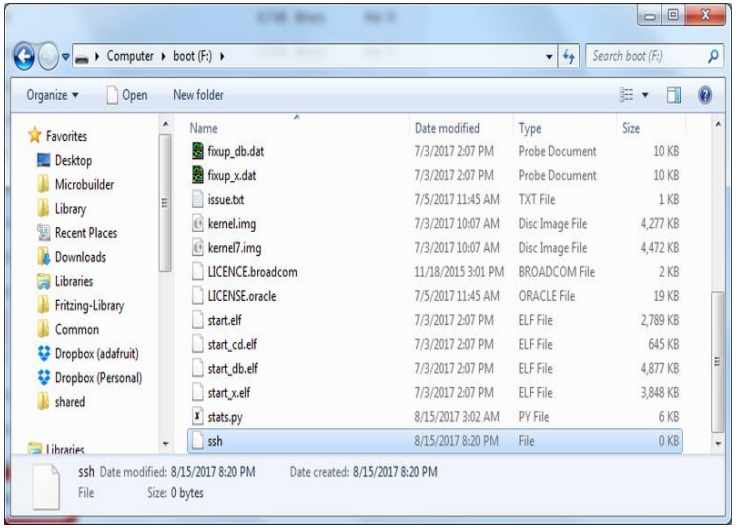
- How it works:
  - the SSH client listens for connections on a configured port, and when it receives a connection, it tunnels the connection to an SSH server

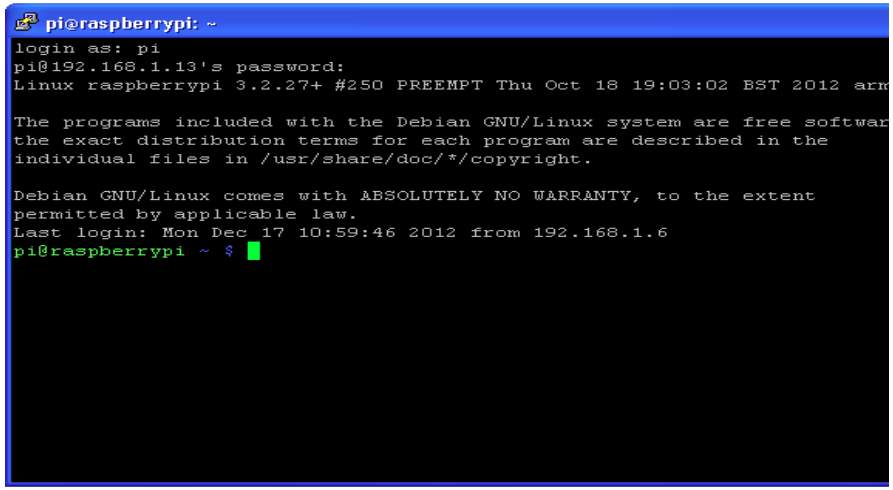
SSH Tunneling Example (Jump Server)

- Creating a Jump Server
  - E.g., CryptoAuditor can act as a jump server, record all sessions, and pass session contents to analytics for early warning of suspicious activity.
  - `ssh -L 127.0.0.1:80:web.example.com:80 jumpserver.example.com`
  - `(only local web service is permitted to be forwarded to jumpserver – no external traffic)`
  - More: https://www.ssh.com/ssh/tunneling/example

Raspberry PI SSH Server

- Add file named “ssh” to SDCard.
- Load the SD Card.
- Now ssh to node “pi” from PC





- From there it is all UNIX!
- Just type sudo raspi-config

Timestamp Identifier

- Many times we need to create an identifier (unique name) for separating data.
- **Use the machine clock time.**
  - Time since 1/1/1970 (epoch time). UNIX time!
  - Initially this time was since 1971-1-1.
  - A 32-bit *signed* integer using 1970-1-1 as its epoch can represent dates up to 2038-1-19.

```
$ date +"%s"          #seconds
1457034425
$date +%s%m #milliseconds
145703476903
```

- Nanoseconds is not available on all UNIXes

```
(ada)$ date +%s%N #nanoseconds
1457034579278836206
```

- date +"%Y%m%d_%H%M%S"
- 20180921_160726

Timestamp to Date:

Linux:

date -d @1267619929

MacOSX:

date -r 1267619929

>> Sat Apr 30 06:32:13 CET 48631

Other Identifiers

- Process Identifier:
  - $ echo $$ => 28835
- Random Identifier
  - $ echo $RANDOM => 23953
- Hostname Identifier
  - $echo $HOSTNAME => ada.in.cs.ucy.ac.cy
- Print Sequences of Numbers
  - `seq -f "test%g" 8 10`
    - `test8`
    - `test9`
    - `test10`

Cryptographic Identifier (**uuid RFC4122**)

- The **RFC4122 UUID** standard generates a **128-bit Unique Identifier** that is unique in space and time.
- The Result is usually printed in **Hexadecimal format** with or without dashes.

- **$uuidgen**
  - E.g., EEF45689-BBE5-4FB6-9E80-41B78F6578E2
- **$cat /proc/sys/kernel/random/uuid**
  - d6aa801c-6cd5-4c90-b16a-aaca0eeae1ec
- **$dbus-uuidgen** #dbus package on Debian
  - 52195bef65c5faab6ea13b4c0000b443

Cryptographic Identifier (**md5sum RFC1321**)

- The MD5 message digest is a way to compute a 128-bit sequence that is unique for the same sequence.
  - Widely used for **disseminating packages** on the internet (e.g., an ZIP, AVI, MP3 package has an accompanying MD5 digest to enable the downloader verify that the download was complete.
  - Not **cryptographically strong** and not used for encryption anymore, even though called a cryptographic hash function.

Download (only 249KB):

WinMD5 Freeware Download

WinMD5Free.zip MD5: 73f48840b60ab6da68b03acd322445ee

WinMD5Free.exe MD5: 944a1e869969dd8a4b64ca5e6ebc209a

- **$md5sum WinMD5Free.zip**

73f48840b60ab6da68b03acd322445ee WinMD5Free.zip

Binary-to-Text (uuencode / uudecode)

- **Uuencoding** is a form of **binary-to-text** encoding that originated in the **Unix** program **uuencode**, for encoding binary data for transmission over the **UUCP mail system**.
- **uuencode file.zip newname.zip > myfile.uue**
  - The purpose of the uuencode program is to translate a binary file that contains **unprintable (non-text) characters** into a format that is entirely readable.
  - This prevents mail, news, and terminal programs from **misinterpreting** non-text characters as special instructions.
  - Also helps with Endianess issues in transmission.

Binary-to-Text (uuencode / uudecode)

$ uuencode 01.pdf hi.pdf > encoded.txt

$ cat encoded.txt

```
begin 755 hi.pdf
M)5!$1BTQ+C4-"B6UM;6U#0HQ(#`@;V)J#0H\/"]4>7!E+T-A=&%L;V<O4&%G
M97,@,B`P(%(O3&%N9RAE;BU54RD@+U-T<G5C=%1R9652;V]T(#(P,B`P(%(O
M36%R:TEN9F\\/"]-87)K960@=')U93X^/CX-"F5N9&]B:@T*,B`P(&]B:@T*
…
…
…
4>')E9@T*,30Q-S(T,@T*)25%3T8`
`
end
```

$ uudecode encoded.txt

$ ls hi.pdf

hi.pdf

Binary-to-Text Conversion (base64)

- **base64** encodes/decodes Base64 data (RFC 4648): from non-printable to printable bytes.
  - 64 Characters are used in the output: A–Z (26) , a–z (26), and 0–9 (10) and + / (2)
  - Widely used in email attachments (IMAP & POP3)

```
X-mxHero-InitialSizeLimiter: rule=158
Sender: iss@ucy.ac.cy
X-Zimbra-DL: ucyacall@ucy.ac.cy

This is a multipart message in MIME format.
------=_NextPart_000_014D_01D17089.55100A00
Content-Type: multipart/alternative;
    boundary="----=_NextPart_001_014E_01D17089.55100A00"

------=_NextPart_001_014E_01D17089.55100A00
Content-Type: text/plain;
    charset="iso-8859-7"
Content-Transfer-Encoding: base64

xMnBxMnKwdPJwSDK0cHUx9PH0yDF0cPB09TH0cnZzSDHy8XK1NHPzcnK2c0g1dDPy8/DydPU2c0g
1MfTINXQ0w0KDQogDQoNCsjhIOjd6+Hs5SDt4SDz4flg5e3n7OXx/vPv9ezlIPz06SwgyvHc9Ofz
5yDF8ePh8/Tn8d/v9S/57SDH6+Xq9PHv7enq/u0NCtXw7+vv4+nz9P7tIOzw7/Hl3yDt4SDj3+3l
6SDh8Pwg7/Dv6e/k3vDv9OUg8PH84/Hh7OzhIPDl8ene4+fz5/Ig5Onh5Onq9P3v9Q0KKHdlYiBi
cm93c2VyKSDs3fP5IPTv9SAi0/3z9Ofs4fTv8iDK8eH03vPl+e0gxfHj4fP05/Hf+e0g9OfyINXQ
0yIg8/Tv7Q0K8/3t5OXz7O8gIDxodHRwOi8vd3d3LnVjeS5hYy5jeS9sYWJfcmVzZXJ2PiBodHRw
Oi8vd3d3LnVjeS5hYy5jeS9sYWJfcmVzZXJ2DQrelOrh6SDh8Pwg9O/tIPP97eTl8+zvIKvV8Ofx
```

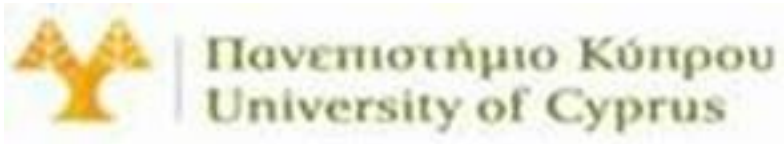
Binary-to-Text Conversion (base64)

```
$ echo "UNIX rocks" > a.txt

# encode
$ base64 -w 0 a.txt > a-b64.txt

# view encoded
$ cat a-b64.txt
VU5JWCBYb2Nrcwo=

# decode
$ base64 -D a-b64.txt
UNIX rocks
```

Output without \n

Binary-to-Text Conversion (base64)

```
# Add red content to
# encoded.txt

# decode
$ base64 -D
  encoded.txt > a.jpg
```



----------0501050408070902050205 08Content-Type:
image/jpeg
Content-Transfer-Encoding:
base64Content-ID:part1.01080202.01010401@cs.ucy.ac.cy
/9j/4AAQSkZJRgABAQEAeAB4AAD/2wBDAAoHBwgHBgoICAgLCgoLDhgQDg0NDh0VFhEYIx8lJCIfIiEmKzcvJik0KSEiME ExND k7Pj4+JS5ESUM8SDc9Pjv/2wBDAQoLCw4NDhwQEBw7KCIoOzs7Ozs7Ozs7Ozs7Ozs7Ozs7Ozs7Ozs7Ozs7Oz s7Ozs7Ozs7Ozv/wAARCAA2ASUDASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAQIDBAUGBwgJCgv/8QAt RAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoK So0NTY 3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDx MXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAt REAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJyg pKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba 3uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD2Jcjk0yaVYkLyEBRTyMD6fWH rF8WlSGICRA3zj0rnr1lTjc0pwc5WNaGWOYMYmBG7mp+Otc7ZXrQ35G3bA3UmuhB3Llenapw9f2yuwq03TdkDZ6ioUuYZH8tW BNQajdm3gIjwZW6KayPtMkQgaOHDk/NWFfFqE1EqFKUIc6UUtQ286zRBlOTUucDNd0ZqUU0YtOLaFoqOKYSqT0xVPVdYh0iN ZbhGKOwUbad7biNCisy51tLS0N1NbSrCBkt6Vasr1b62W5RSqMMru7ijmixImimCVcbgwYUFwBncMevammmgH0UwyKF3bgB6k8 UeYuM7hjPBz1o5kA+im+YmQN46+tBcA4J59BRdAOoppYLwzAZ6c0gkXOCwz2ANF0gH0U0yLjO4Y9c1XN/ELsWo5kIz7Gpbim Baopu4DgkZ/lShhzyDj3quZALRTQ4OBnnGeKQSKeAykjqAad0A+imlsKSuW9qzbTX7e8u5rZI3DQf60notS2gNSiqNnqi3ryCOF1R Dje3AP0qQX8RvDaodzgZYnoBTUkBaoppdQwBcZ9M0eYvTcCewFHMgHUU0uucbgD6ZpN+OW+Udye1HMgH0U0MDk7hgeILu HXcMU7pgLRSA8etFGgGfquopY2xPJkxgAVzEZ8+dXhZhIzZYGuyltoZiDlgYj1pn2K1B/wBUoPXlFebiMLUqy30OmlXjSj5nK3wbzy 1y2wJyFXvWtpWtJNbESHaU6ZqfVNKjukMirhlFczLINxxtZeMCvIrTqYOTZ204wrxt1L91dLfXDMX2FfutT5Y53hiRj8o6sKr6Npx1CTf IT5SeneuqS1hCLH5fyL2NXh8LUxMXOXUipVjSfKjE0rUY4pjAqttzgE10C8gn2qNbS3ByIlB9QKmHAlxgYr2sLRnSjyyZwVJqTuVrLi Ns8/NWJ42ZV0yEE8+cMe1bll/q3/3jS3Nta3CqLlUdQeN/rXRKNzMydflUeFpWJDAxDt1rLlvJYtK0aGJmjtpsCVwPu/WuqltrZ4fLkRT EB909MUi2lqYPJEamI9u34Vl7J9wOeWSNPF6W0MzNG8PKg8fWoYbi6sbu50SZnczNmBuvB7108dhawspSBQyjAbvipPJhabzjG hkUY3dxVKD7gcxetLFrttYrlzRCPD7jgE+tP8QltlorSRTuzBxt2muhntLe4YedErt69xSGytTF5TQgx9geaHCQHNampibR2SSQec67 +farRleLxil1ZipgO1SeM1uta28gRXjUiPlc/wAJpWtoWlEpjUyD+PHNChK4HKWkhvdM1B7+4kW4jdsAHlfTFOZm/hCTdSb0uQpww PzEZrpnsbR5CzxJnv7/WpDHGyGJkBjPGMcYp8jbA56XZ/wiHnJMxkMWd2eQ1Z10j23h+x1BJ3+07lBb1HeuvWytVtzAlV8o9VoNl btCIGiUx4+7jpSlTbAwb+5kh8Q6a3n7IpF/eAng8U3TroTeJ9ShWVymzjnj8KualobX2o2lyNoituDGepFaa2lrExkjhVXI5lqVCSA5KC +vlvDl8YZHaaO4wSeqrVm/c21tpktjKzzyOAQDndnmuiis1MiRJHlz8y/3qWKxtYWvkgCkdB6VootATKTxu4bGSa4RY7uXxDqctm 4ZUky8XTeK7svGeGkU8Yxmoo7K0hl82KFVc87h1NJxdgMN9Ug1HQLmK2Rop4UO6EcMDVC7umbw7p8kUh+0l1B2/ePe1rrBZ2y zGVYVDt95gOv1pi6fZJMJVgUPnjilyOwGFfsT4nsIDI4DJlwD7U22dofEeox+a+2OLfGCeOldE1rbvOszxgy44fFMuLOKRXZI1EzoV D4ocJAczZy/a/D099LcN9pBYrg9COgp0t/ezLpCXLPHFOv71sdT7+laui6INPszFcqkr7ywi6VqS20M0flyxqyjoMdKShIDBieWLxML W3dpLR4D5nOdpqlZXMg8P6jHcXDCSORtm44brxXVQ20MLExRBGPVvWmSadaSymV4FL55z3qlCSAdpxY6dbliSTGM5oqcAA YHAHQUVdmACklpR0oxVJvcVrrUjlkWKJmbpiuLvGEs0kgOF3Gunv7G4u8qJtifzrOfw07KFE2a8DMqNavJKK0R34WpCk7sd4ZuE 8hkJAbNb59etc9B4duLaXzIrjBrehRki2yNuNd+D9pGHJJWMcQ4uXNFkg6elB6H6UDpS4yCK9BKxzlWy/1b/75rE8all02J43ZG80L wa6CGIxIR6mqetaUNWsjb7tjDlWqKl2tAGXUeNF27jkRjmqdzq7aRZ2S+QZ/O4HtVoWV7JZrazTJsxywHWmanoz3ptBC+1bcg1ny sBLfWpf7WGn3FuUd13l1V7XU2EupskbSNbnJX+9VyfSXl1qDUVIAES7SDRY6O1nqNzdNIrJc9VxRaSAji14XVjbXFvHuadtrJ3FR yel1864it4zJ9mX58djUmmeH107U57IZd0b8pH/AHKZDoclqVxcWjIY7g7mjYd6PfAbdeJBb6dbXq2zSJO2wr3DU6512ayt4nu7Voz K+1SOi/Wnalp8+ox2oEiQvDJ5mFHBq7d280+wfunQcMrjg0XmBRu9Qdtlu2pFygfxIeoqteaxdw2mmGzUFblgp3dali8OtFp97a+f/x9 HIHZPpSy6FPLp9lEkyrJaHlbFL3wLM2sNaatFZXEW1JR8svbNWbK8ku3lUx7Y0bCv61meIYo7y1jspGb7UWG0qPzrYtbdbW2it1J by1A+tWnJAUZdY3ao2n2sfmTRruc+gqo+ttdaZfxonk3Vuh3le3vViXSZItabUrWQb3Xa6H+KmQ6C0cF6fNBubsEM/8AdBqZOTYEf hilXGm297Kh83adrE/eFN8Tanc2jWlnbtsa6fDP6CtLSLKXTbBLWSRXMfCkCmaxpMOrwqjkpIhzHlvY1dpWAcNJhMHIlm3kcvnrVZ NSXTtRi0uZWVGQlJm6EjtUkVtqyWv2dp42YDAfHNUNat1vYLbT2dnvlYFXUcL61D5kBauNcmg06a++zFo4mwB/e96jk8QParbXF xDtt7nGG/u5o8QW62/heaFSRtUcjuaZDpU2qWNkLpgII0DbPU1LcmBJc67cR6sdOt7QySFPMVvaphrD/wBrQ6dNBteWPcT6Uf2T KuujUVI+RYvL20X+kvNq8GpQSqrRLhgR1qryALbWvPub23aA77T0/iFN07XP7R2vGoKscMndaj07Rbuxury5a5V5LrpxwKF0FmvoI LyQpE8Z5EfR6ceYDcAlJ54x0p1IDnPtS1smwCiiimAYooopgxMUYooqVuCDFAUCiih7i6i0UUUxhRiiikAmKMUUUwDaAMdqWiim AmB+NG0e/50UUAG0enajaD2oooAXFGKKKAGGKMuHKAsOhxzTgADnvRRQAFQTnv60AAdqKKAFxSbQM+hoooAXFN8tN+/a N2MZxRRSsAPGkilXUMp6g9KFjVF2qMAdBRRRZALgDPvS4FFFMBAMUuKKKADFFFFIAoooo A//Z
----------0501050408070902050205 08--

Internet Bots (curl, wget)

- An **Internet bot,** also known as **web robot**, WWW robot or simply bot, is a **software application** that runs **automated tasks (scripts)** over the Internet.
  - Typically, **bots perform tasks** that are both **simple** and **structurally repetitive**, at a much **higher rate** than would be possible for a human alone.
    - Think about a bot running on a dozen of UNIX machines (see Bash Programming)
- The largest use of bots is in web spidering, in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human.
  - Wikipedia

Internet Bots (curl, wget)

- **curl is a tool to transfer data from or to a server, using one of the supported protocols**
  - DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP.
- **Simple Example:**
  - `$ curl www.cs.ucy.ac.cy > index.html`
- **HTTP GET Example:**
  - `$ curl http://moodle.cs.ucy.ac.cy/enrol/index.php?id=42`
- **HTTP authentication (do only with SSL):**
  - `$` curl -u user:password https://example.org/
- **HTTP POST Example (e.g., do only with SSL) :**
  - `$` curl --data "user=<name>&pass=hi" https://www.example.com/login.php
- HTTP HEAD Example (e.g., find when a file was created!)
  - $ curl --head https://www2.cs.ucy.ac.cy/docs/prospectus.pdf

Curl Example (Acting as Mobile App)

- curl **-vvv -i -H** "Host: 192.168.3.90:25000" -H "Content-Type: application/json" **-H** "Connection: keep-alive" **-H** "Accept: */*" **-H** "User-Agent: HomeChargerApp/1.0.1 CFNetwork/1209 Darwin/20.2.0" -H "Content-Length: 140" **-H** "Accept-Language: en-us" **-H** "Accept-Encoding: gzip, deflate" **-d** *'{"DevName":null,"LocTime":"`date +%s`","Summer":false,"Tz":120,"FixedVehCosts":null,"OldVehCosts":null,"Battery":null,"DevMode":"HomeManager"}'* **--trace-ascii /dev/stdout** -X POST http://192.168.3.90:25000/MHCP/1.0/DevInfo?DevKey=XXXXXX

-i Include the HTTP response headers in the output.
-v, --verbose: Makes curl verbose during the operation.
-H -H, --header <header/@file>: HTTP Request Header to server
-d, --data <data>: HTTP data in a POST request to the HTTP server
--trace-ascii /dev/stdout: shows POST request
`date +%s`: get unix epoch

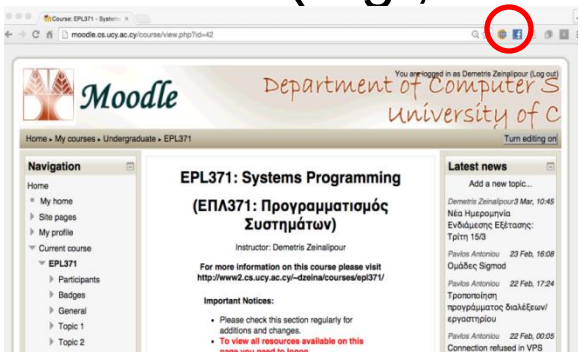
Curl Example (Response)

```
== Info: Expire in 0 ms for 6 (transfer 0x807880)
== Info:   Trying 192.168.3.9...
== Info: TCP_NODELAY set
== Info: Expire in 200 ms for 4 (transfer
0x807880)
== Info: Connected to 192.168.3.9 (192.168.3.9)
port 25000 (#0)
=> Send header, 284 bytes (0x11c)
0000: POST /MHCP/1.0/DevInfo?DevKey=XXZXXXX
HTTP/1.1
002f: Host: 192.168.3.9:25000
0049: Content-Type: application/json
0069: Connection: keep-alive
0081: Accept: */*
008e: User-Agent: HomeChargerApp/1.0.1
CFNetwork/1209 Darwin/20.2.0
00cd: Content-Length: 140
00e2: Accept-Language: en-us
00fa: Accept-Encoding: gzip, deflate
```

```
011a:
=> Send data, 140 bytes (0x8c)
0000:
{"DevName":null,"LocTime":1636869039,"Summer":false,"Tz
":120,"Fi
0040:
xedVehCosts":null,"OldVehCosts":null,"Battery":null,"De
vMode":"H
0080: omeManager"}
== Info: upload completely sent off: 140 out of 140
bytes
<= Recv header, 17 bytes (0x11)
0000: HTTP/1.1 200 OK
HTTP/1.1 200 OK
<= Recv header, 19 bytes (0x13)
0000: CONNECTION: close
CONNECTION: close
<= Recv header, 19 bytes (0x13)
0000: Content-Length: 0
Content-Length: 0


<= Recv header, 2 bytes (0x2)
0000:
== Info: Closing connection 0
```

Cookie-based Crawling (wget)

- Most websites use session cookies for retaining authenticated users online.
  - HTTP Cookies are small pieces of data sent from a website and stored in the user's web browser.
  - Every time the user loads the website, the browser sends the cookie back to the server to notify the user's previous activity
- **How to Crawl a Site with Cookies?**
  - Fetch Cookie using Web Browser extension (e.g., cookies.txt in Chrome)

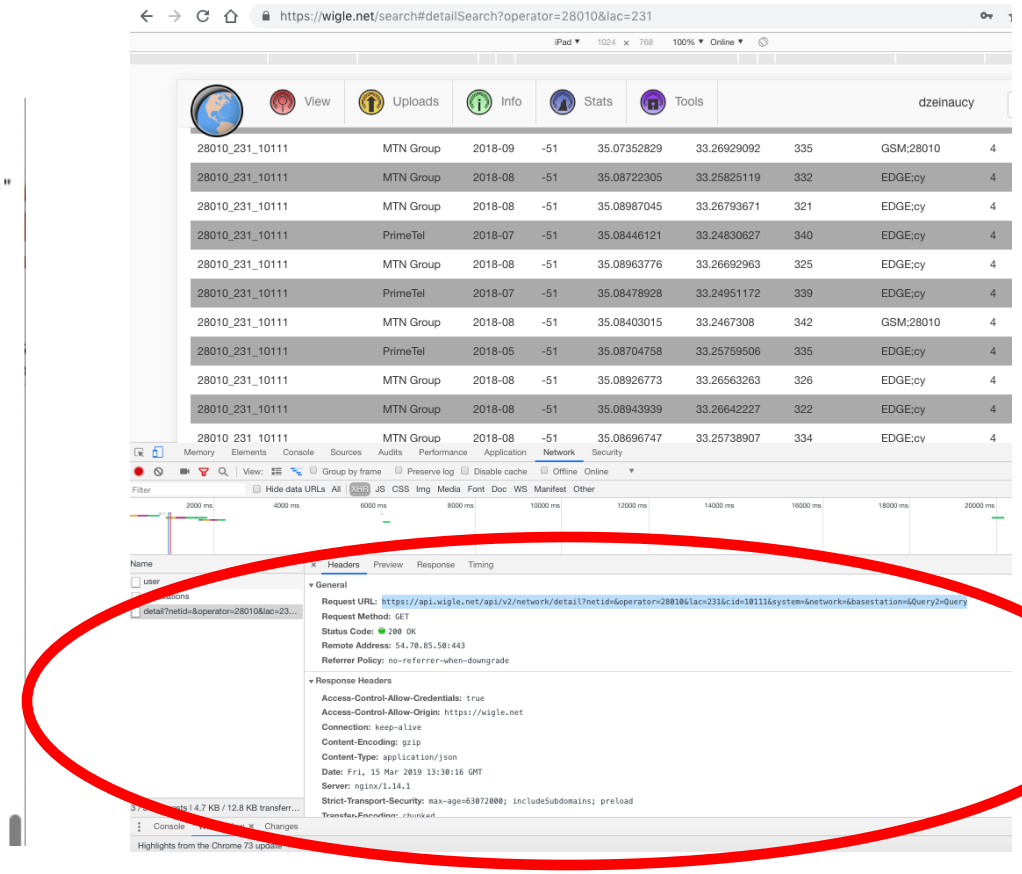


  - `$ wget -x --load-cookies cookies.txt http://moodle.cs.ucy.ac.cy/course/view.php?id=42`

Crawling AJAX Calls

Problem: No data ☹

```
<script id="searchResultsRows" type="text/template">
  {{#results}}
  <tr>
    <td><a href="javascript:void(0);" class="mapLink" map-lat="
{{trilat}}" map-lon="{{trilong}}" map-ssid="{{ssid}}" map-
netid="{{netid}}" title="click to view on map">map</a></td>
    <td><a href="javascript:void(0);" class="detailLink"
bssid="{{netid}}" title="click for detail">{{netid}}</a></td>
    <td>{{ssid}}</td>
    <td>{{name}}</td>
    <td>{{type}}</td>
    <td>{{firsttime}}</td>
    <td>{{lasttime}}</td>
    <td>{{networkIcon wep gentype}}</td>
    <td>{{trilat}}</td>
    <td>{{trilong}}</td>
    <td>{{channel}}</td>
    <td>{{bcninterval}}</td>
    <td>{{qos}}</td>
    <td>{{userfound}}</td>
    <td>{{free}}</td>
    <td>{{pay}}</td>
    <td netcomment="{{netid}}" class="commentcell"
id="commentcell-{{netid}}">{{comment}}</td>
    <td><input class="commentbtn" type="button"
id="comment{{netid}}" netid="{{netid}}"  value="add comment"/>
</td>
  </tr>
  {{/results}}
</script>
```



Chrome Developers Tools or Similar (e.g., Safari) can help us to find the underlying calls / HTTP headers upon which we can initiate the wget/curl commands

Crawl Complete Domain

- $ wget \ --recursive \ --no-clobber \ --page-requisites \ --html-extension \ --convert-links \ --restrict-file-names=windows \ --domains www.ucy.ac.cy \ --no-parent \ www.ucy.ac.cy/test/html/

- The options are:
- --recursive: download the entire Web site.
- --domains www.ucy.ac.cy : don't follow links outside www.ucy.ac.cy.
- --no-parent: don't follow links outside the directory tutorials/html/.
- --page-requisites: get all the elements that compose the page (images, CSS and so on).
- --html-extension: save files with the .html extension.
- --convert-links: convert links so that they work locally, off-line.
- --restrict-file-names=windows: modify filenames so that they will work in Windows as well.
- --no-clobber: don't overwrite any existing files (used in case the download is interrupted and resumed).

Διαχείριση Αρχείων XML / JSON (xmllint, jq)

- Στην εποχή των ανοικτών δεδομένων (Open Data) διατίθενται πλέον στον ιστό σωρεία δεδομένων προς κατανάλωση, π.χ.,
  - π.χ., δεδομένα κλινικών δοκιμών από το https://clinicaltrials.gov/ διαθέτει δεδομένα σε XML
  - Wikidata.org διαθέτει μια XML έκδοση της Wikipedia σε XML.
  - Οι πλείστες Web 2.0 υπηρεσίες (π.χ., Google, FB, Twitter, κτλ.) παρέχουν JSON APIs τα οποία επιτρέπουν την προσπέλαση σε JSON (lightweight XML) δεδομένα σε συνεχομένη βάση
- Τι είδους εργαλεία χρειαζόμαστε για να επεξεργαστούμε γρήγορα τέτοια δεδομένα;

Διαχείριση Αρχείων XML / JSON (xmllint, jq)

```
# Παρουσίαση περιεχομένου XML
$ xmllint --format 3178056.nxml
```

```
<ref id="B72">
  <label>72</label>
  <element-citation publication-type="journal">
   <person-group person-group-type="author">
    <name>
     <surname>Price</surname>
     <given-names>MN</given-names>
    </name>
    <name>
     <surname>Dehal</surname>
     <given-names>PS</given-names>
    </name>
    <name>
     <surname>Arkin</surname>
     <given-names>AP</given-names>
    </name>
```

Διαχείριση Αρχείων XML / JSON (xmllint, jq)

```
# Ανάκτηση και μορφοποίηση περιεχομένου JSON
$ curl -s
   'http://api.nytimes.com/svc/elections/us/v3/finances/2008/president/to
   tals.json?api-key=super-secret' | jq '.' | head
```


```
{
 "results": [
   {
     "candidate_id": "P80003338",
     "date_coverage_from": "2007-01-01",
     "date_coverage_to": "2008-11-24",
     "candidate_name": "Obama, Barack",
     "name": "Barack Obama",
     "party": "D",
```


Επιπλέον Εργαλεία για Data Science:

- **json2csv - convert JSON to CSV | xml2json - convert XML to JSON**
- **csvkit - suite of utilities for converting to and working with CSV**

Sqlite 3 – The power of SQL!

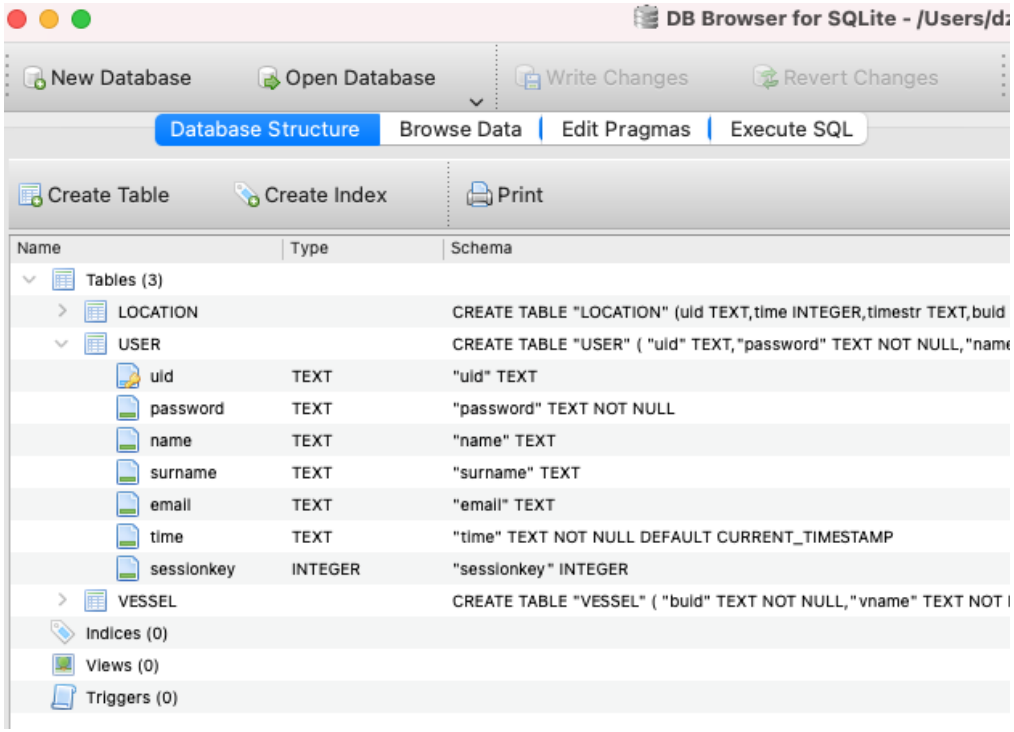
- **SQLite** is a C-language library that implements a small, fast, self-contained, high-reliability, full-featured, SQL database engine.
- SQLite is the most used database engine in the world!
  - Android, iOS, Shell, php, python, bash, etc!
- Structure your files and move querying logic down to SQL => saves time!

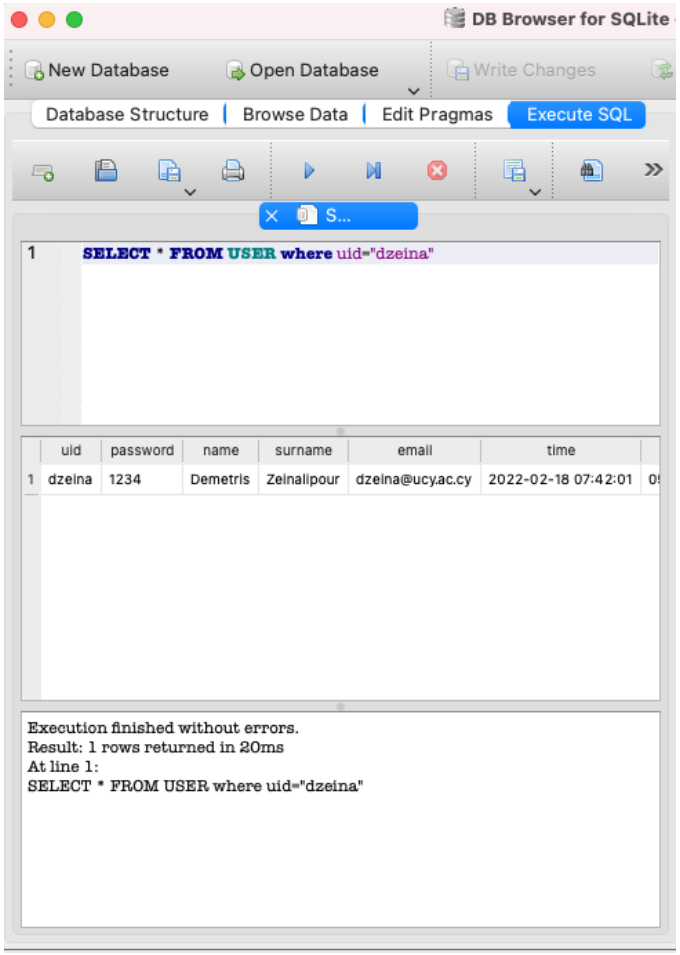
SQLite 3 Interactive

```
sqlite3 ex1
SQLite version 3.36.0 2021-06-18 18:36:39 Enter ".help"
for usage hints.
sqlite> create table tbl1(one text, two int);
sqlite> insert into tbl1values('hello!',10);
sqlite> insert into tbl1 values('goodbye', 20);
sqlite> select * from tbl1;
hello!|10
goodbye|20
sqlite>
```

SQLite Interactive (GUI)

- DB Browser for SQLite





SQLite Examples

- Using **Here String <<<**

```
FULL_DB_NAME="test.db”
uid="dzeina"
SESSION_KEY=`sqlite3 $FULL_DB_NAME <<< "SELECT
sessionkey FROM USER WHERE uid=\"$uid\""`
```

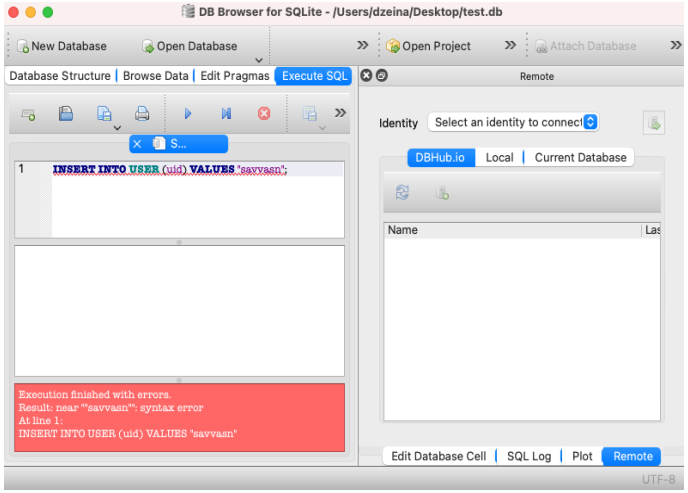
- Using Here Document <<

```
#!/bin/sh sqlite3 /var/www/dbs/ha.db <<'END_SQL'
CREATE TABLE IF NOT EXISTS table2 AS SELECT * FROM
table1; INSERT INTO table2 SELECT * FROM table1;
DELETE FROM table1;
END_SQL
```

Sqlite in Action!
Create Table, Insert, Select

 # Create & Truncate Table

```
sqlite3 test.db <<< "CREATE
TABLE IF NOT EXISTS USER (uid
TEXT PRIMARY KEY); DELETE FROM
USER;";
```



Debug SQL in GUI!

 # Insert to Table

```
for i in `ps -ef | awk -F" "
'{print $1}' | sort | uniq | sed
'/UID/d'`; do sqlite3 test.db
<<< "INSERT INTO USER(uid)
VALUES (\"$i\");"; done
```

 # SELECT from Table

```
sqlite3 test.db <<< "SELECT * FROM USER;";
```

Google SMTP Mailer

- Outgoing Email requires an SMTP server.
- Google allows you to use your GMAIL account SMTP server (similarly to other providers)
- Below we show how to make all mails in your account sent through GMAIL.
- You are not required to be root for the below functionality (but you can configure this centrally for all users if necessary)

Configure SMTP Mailer with Gmail!

- This will basically let you send email from the terminal, using mailx and Gmail as SMTP server.
- First, create a certificate directory then create new certificate and key databases:
- `$ mkdir ~/.certs`
- `$ certutil -N -d ~/.certs`
- Then fetch the certificate from Gmail and import the cert file into the new database:
- `$ echo -n | openssl s_client -connect smtp.gmail.com:465 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ~/.certs/gmail.crt $ certutil -A -n "Google Internet Authority" -t "C,," -d ~/.certs -i ~/.certs/gmail.crt`
- Now, send a mail:
- `$ echo -e "Email content" | mailx -v -s "Email subject" -S smtp-use-starttls -S ssl-verify=ignore -S smtp-auth=login -S smtp=smtp://smtp.gmail.com:587 -S` **`from="username@gmail.com(John Doe)" -S smtp-auth-user=username@gmail.com -S smtp-auth-password=s0m3p@zzW0rD -`**`S ssl-verify=ignore -S nss-config-dir=~/.certs recipient@some.com`

https://sites.google.com/site/debjyotidoc/home/documentation/linux-tips/send-mail-with-gmail-auth

Set ~/.mailrc (user) or /etc/mail.rc (all)

```
$ vi ~/.mailrc
set smtp-use-starttls
set ssl-verify=ignore
set smtp-auth=login
set smtp=smtp://smtp.gmail.com:587
set from="=<YOUREMAIL>@gmail.com(Demetris Zeinalipour)"
set smtp-auth-user=<YOUREMAIL>@gmail.com
set smtp-auth-password=<YOURPASSWORD>
set ssl-verify=ignore
set nss-config-dir=/home/faculty/dzeina/.certs
```

OR

```
$ vi ~/.mailrc
```

account gmail {

…

}

```
# Now mail reads the new settings
```

$ mail -a some-attachment.txt l -s ‘Subject’ ‘<YOURGMAIL@gmail.com>'

More: https://kb.novaordis.com/index.php/Configure_mailx_to_Relay_via_a_Google_SMTP_Server

Web Server Stress Testing

Tips:

1) Carry out advanced configurations if necessary

```
$ vi /etc/apache2/apache2.conf
```

2) Run you php, python, etc. script and make sure that the apache webserver log file has no errors. Repeated errors can have a dramatic impact on webserver stability.

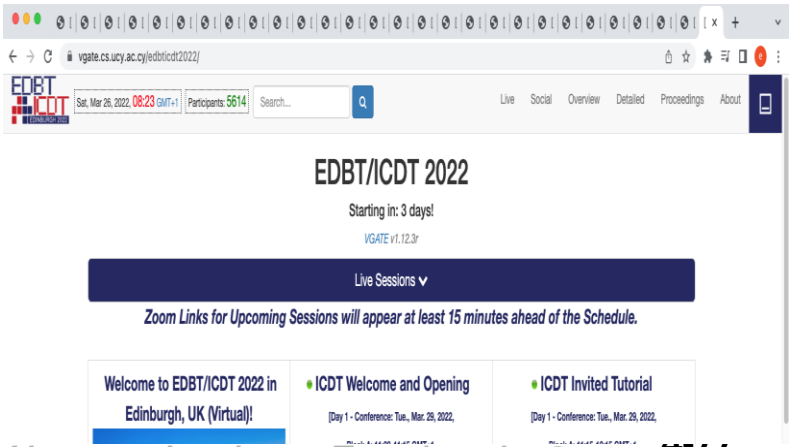
```
$ sudo cat /var/log/apache2/error.log
```

```
[Sat Mar 26 07:32:48.947781 2022] [auth_basic:error] [pid 3530105] [client 66.205.83.228:5
3309] AH01618: user edbtocdt2022 not found: /edbticdt2022/clock/, referer: https://vgate.c
s.ucy.ac.cy/edbticdt2022/
[Sat Mar 26 07:32:48.954235 2022] [auth_basic:error] [pid 3524946] [client 66.205.83.228:5
3310] AH01618: user edbtocdt2022 not found: /edbticdt2022/data/index.php, referer: https:/
/vgate.cs.ucy.ac.cy/edbticdt2022/
[Sat Mar 26 07:56:27.533207 2022] [php7:warn] [pid 3525047] [client 194.42.17.196:49202] P
HP Warning:  SQLite3::exec(): UNIQUE constraint failed: zoom.id in /home/vgate/website/web
hooks/webhookagent-central.php on line 147
[Sat Mar 26 07:56:42.749840 2022] [php7:warn] [pid 3525021] [client 194.42.17.196:49206] P
HP Warning:  SQLite3::exec(): UNIQUE constraint failed: zoom.id in /home/vgate/website/web
hooks/webhookagent-central.php on line 147
[Sat Mar 26 07:59:54.196969 2022] [php7:warn] [pid 3525001] [client 194.42.17.196:49214] P
HP Warning:  SQLite3::exec(): UNIQUE constraint failed: zoom.id in /home/vgate/website/web
hooks/webhookagent-central.php on line 147
vgate@vgate:~$ sudo cat /var/log/apache2/error.log
```

Example: Stress Testing HTTP Webhook

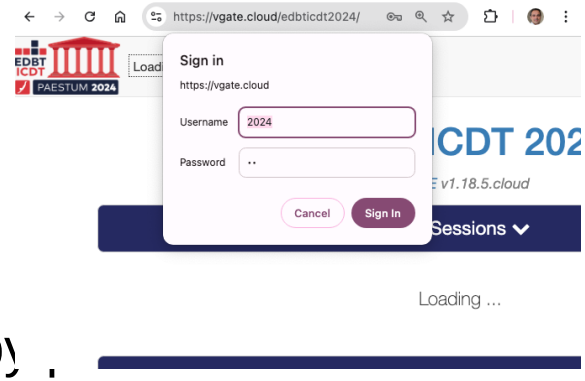
```
while [ $i -lt $REPEATS ];
do
 echo -n "Starting $i ..."
 #set -xv
curl $1 --insecure -H "Authorization: $AUTHORIZATION" -d
'{"payload":{"account_id":”ffasdfasrg","object":{"uuid":"9ffafdfdsMQ==","pa
rticipant":{"user_id":"'$i'","user_name":"'$i'","id":”daFDafaffdgragasfgsaf
ga","join_time":"2021-02-
21T07:37:40Z","email":"xxxx@ucy.ac.cy"},"id":"'$ZOOM'","type":3,"topic":"Ro
om #16","host_id":"V6B6NPQLkA","duration":60,"start_time":"2021-02-
21T07:37:41Z","timezone":"Asia/Nicosia"}},"event_ts":1613893062942,"event":
"meeting.participant_joined"}' -X POST $URL &
done
```

```
top - 08:24:20 up 51 days, 20:55,  2 users,  load average: 27.15, 11.21, 6.24
Tasks: 292 total,  33 running, 259 sleeping,   0 stopped,   0 zombie
%Cpu(s): 81.5 us, 17.9 sy,  0.0 ni,  0.0 id,  [illegible] wa,  0.0 hi,  0.7 si,  0.0 st
MiB Mem :   3931.7 total,   1988.5 free,    397.7 used,   1545.6 buff/cache
MiB Swap:   2048.0 total,   2039.4 free,      8.6 used.   3266.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
3573745 vgate     20   0   12116   8208   1736 R   5.6   0.2   0:04.77 bash
3561940 www-data  20   0  197296  19120  13792 S   3.3   0.5   0:05.34 apache2
3569052 www-data  20   0  197292  18936  13600 S   3.3   0.5   0:03.16 apache2
3570965 www-data  20   0  197292  18876  13628 S   3.3   0.5   0:03.72 apache2
3571205 www-data  20   0  197292  18988  13700 R   3.3   0.5   0:03.68 apache2
3571570 www-data  20   0  197292  19120  13832 S   3.3   0.5   0:03.91 apache2
3524965 www-data  20   0  197384  19440  13576 S   3.0   0.5   0:10.03 apache2
3570544 www-data  20   0  197292  19156  13684 S   3.0   0.5   0:03.50 apache2
3572815 www-data  20   0  197292  18952  13516 S   3.0   0.5   0:03.69 apache2
3573837 www-data  20   0  197320  18792  13604 R   3.0   0.5   0:02.90 apache2
3574499 www-data  20   0  197284  18992  13620 S   3.0   0.5   0:02.93 apache2
3578857 www-data  20   0  197272  18500  13492 S   3.0   0.5   0:02.32 apache2
3583559 www-data  20   0  197260  18144  13104 S   3.0   0.5   0:01.33 apache2
3587611 www-data  20   0  197260  18144  13104 R   3.0   0.5   0:00.33 apache2
3570352 www-data  20   0  197292  18872  13584 S   2.7   0.5   0:03.81 apache2
3571401 www-data  20   0  197292  19416  13872 R   2.7   0.5   0:01.60 apache2
3571411 www-data  20   0  197292  19084  13796 S   2.7   0.5   0:03.69 apache2
3571418 www-data  20   0  197292  19064  13636 S   2.7   0.5   0:03.48 apache2
3571793 www-data  20   0  197292  19020  13732 R   2.7   0.5   0:03.04 apache2
3572690 www-data  20   0  197292  19256  13732 R   2.7   0.5   0:01.53 apache2
```



Securing Web Folders with .htaccess

- Enable Apache for htaccess
  - sudo nano /etc/apache2/sites-available/your_domain.conf
  - sudo service apache2 restart
- Generate Password
  - sudo htpasswd -c /not-web-folder/.htpasswd dzeina
- Add guideline to protected folder
  - sudo nano /your-web-folder/.htaccess
    - AuthType Basic
    - AuthName "Restricted Content"
    - AuthUserFile /not-web-folder/.htpasswd
    - Require valid-user



- Test through Web Browser !
- Benefits: Every path inside folder protected by . quickly sharing complex folders to web audience
- https://www.digitalocean.com/community/tutorials/how-to-use-the-htaccess-file

Pushing Data Outside Firewalls

- When we want to access funtionality inside an environment that has a firewall (e.g., smart-home), one common idea is to open ports. (e.g., with iptables or even setup VPN servers on low end devices (e.g., raspberries)
  - This is dangerous as hackers can randomly find these open ports nmap/zmap etc. and brake into your space
  - Better idea: push your inside firewall data outside your firewall to some cloud folder. Access your data from there
  - e.g., curl -u "$HTACCESS_USER:$HTACCESS_PASS" -k -H 'Cache-Control: no-cache' -d "state=$PHASESFULL" -X POST "$CLOUD_URL/state.php"