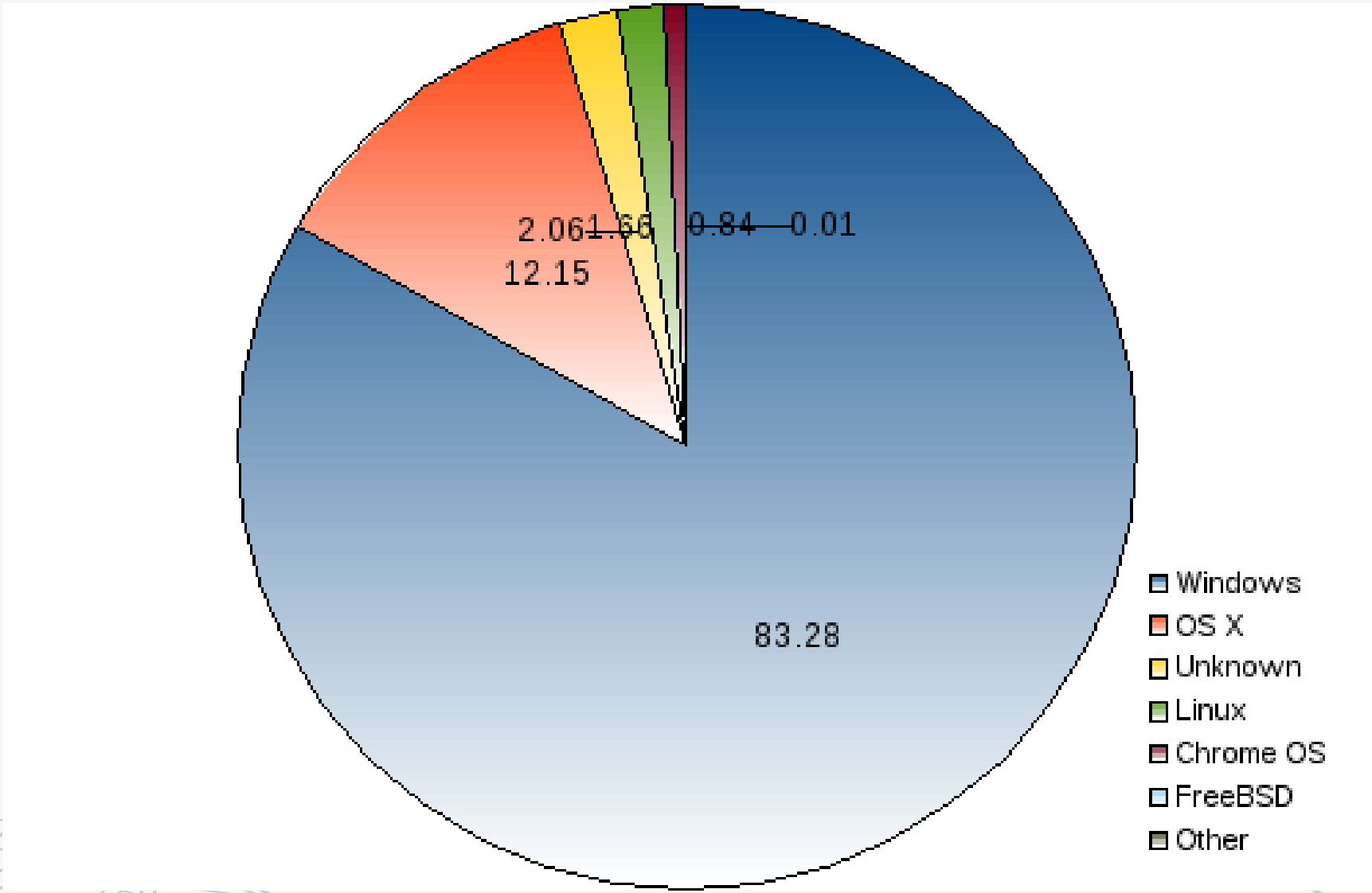
Windows OS

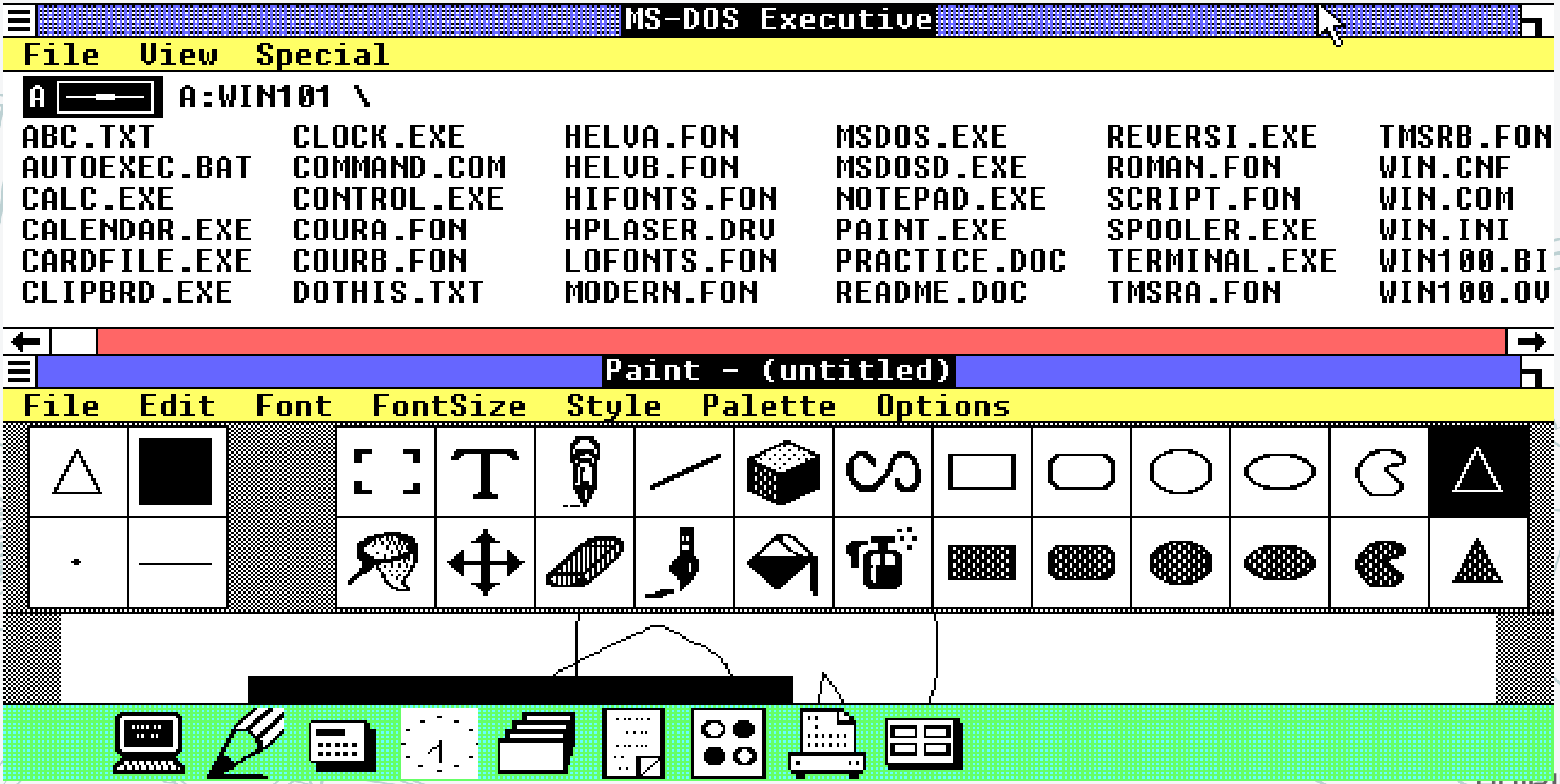
Windows OS

- Windows is an operating system that was first launched in 1985 by Microsoft
- Windows is known with a convenient graphical user interface, using Windows and Mouse
- Today, the operating system is the most common in the world and runs on all PCs and servers

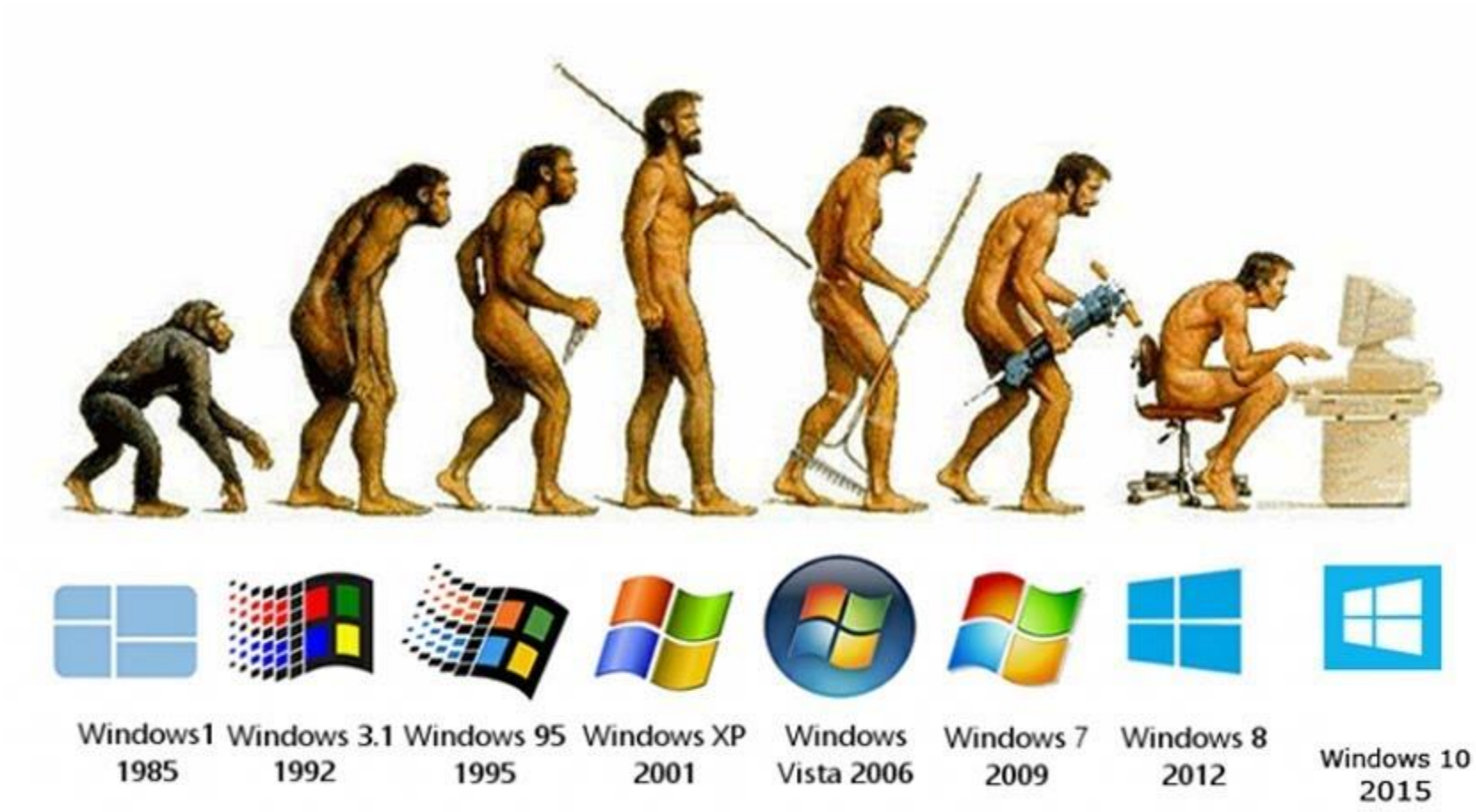
Windows OS



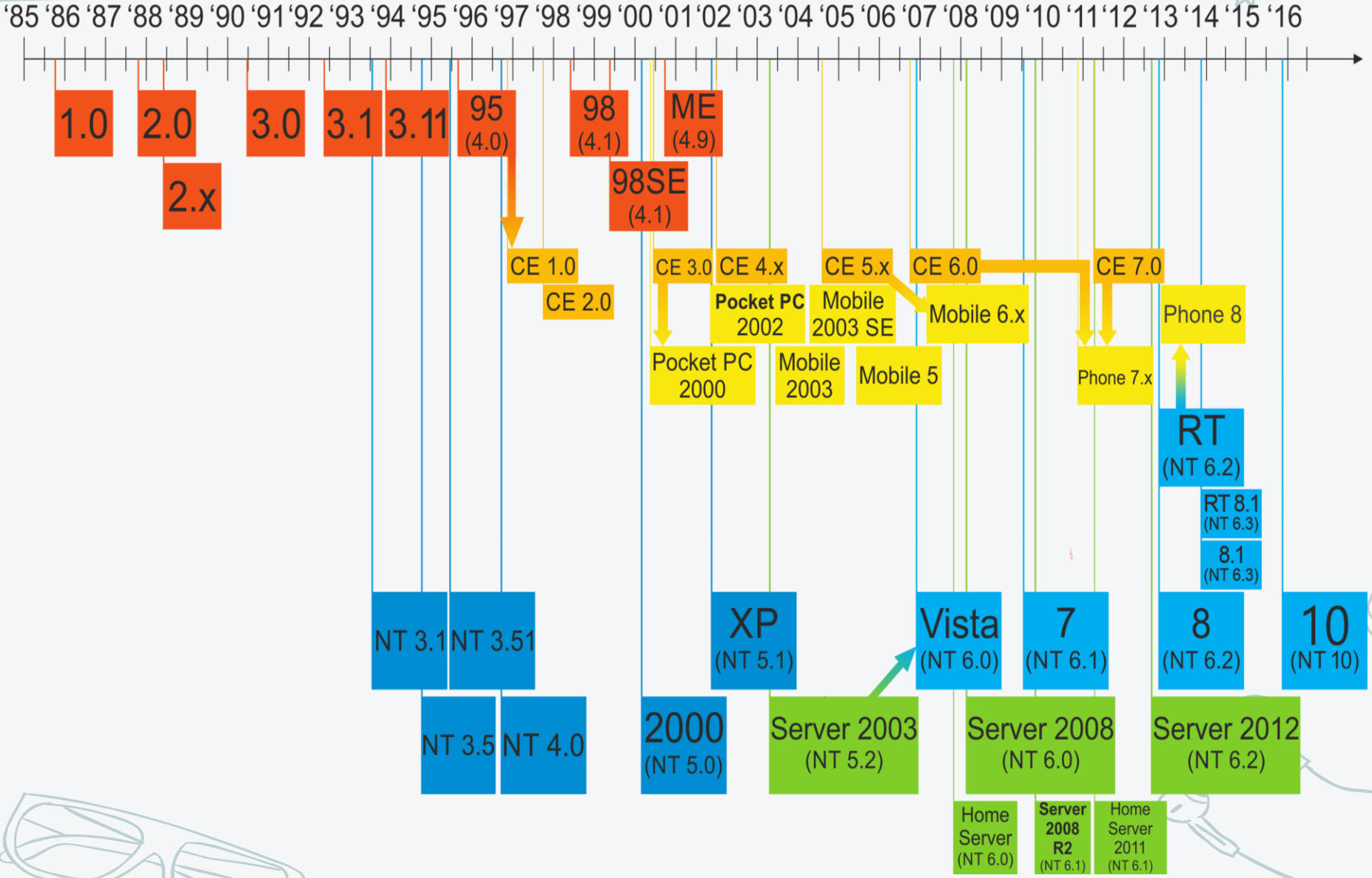
Windows 1.0


MS-DOS Executive
File View Special
A
A:WIN101 \
ABC.TXT
AUTOEXEC.BAT
CALC.EXE
CALENDAR.EXE
CARDFILE.EXE
CLIPBRD.EXE
CLOCK.EXE
COMMAND.COM
CONTROL.EXE
COURA.FON
COURB.FON
DOTHIS.TXT
HELVA.FON
HELVB.FON
HIFONTS.FON
HPLASER.DRV
LOFONTS.FON
MODERN.FON
MSDOS.EXE
MSDOSD.EXE
NOTEPAD.EXE
PAINT.EXE
PRACTICE.DOC
README.DOC
REVERSI.EXE
ROMAN.FON
SCRIPT.FON
SPOOLER.EXE
TERMINAL.EXE
TMSRA.FON
TMSRB.FON
WIN.CNF
WIN.COM
WIN.INI
WIN100.BI
WIN100.OV
Paint - (untitled)
File Edit Font FontSize Style Palette Options

Windows Evolution



Windows Desktop OS Evolution



Windows - Commands

- hostname - Shows the name of the computer I am logged in

```
Microsoft Windows [Version 10.0.17134.950]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\itaym>hostname
makisPC2
```

- whoami - Shows the name of the user I am logged in

```
C:\Users\itaym>whoami
makispc2\itaym
```

- Useful in case of switching between users

Windows - Commands

- whoami \groups – shows a list of user's groups permission

```
C:\Users\itaym>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                                 Type             SID
                                                                          Attributes
========================================================== ================ ==============================
==================================================================== ==================================
===============
Mandatory Label\Medium Mandatory Level                     Label            S-1-16-8192

Everyone                                                   Well-known group S-1-1-0
                                                                          Mandatory group, Enabled by default
, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114
                                                                          Group used for deny only
BUILTIN\Administrators                                     Alias            S-1-5-32-544
                                                                          Group used for deny only
BUILTIN\Users                                              Alias            S-1-5-32-545
                                                                          Mandatory group, Enabled by default
, Enabled group
```

Windows - Commands

- Ipconfig /all - Displays computer's network cards IP addresses and MAC addresses

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 38-BA-F8-E8-10-5C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.60.46.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 20 August, 2019 04:02:51 PM
   Lease Expires . . . . . . . . . . : 20 August, 2019 04:40:49 PM
   Default Gateway . . . . . . . . . : 10.60.46.254
   DHCP Server . . . . . . . . . . . : 10.193.2.1
   DNS Servers . . . . . . . . . . . : 185.149.252.250
                                       208.67.222.222
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Windows - Commands

- Ping – network connectivity check

```
C:\Users\itaym>ping 10.60.46.254

Pinging 10.60.46.254 with 32 bytes of data:
Reply from 10.60.46.254: bytes=32 time=3ms TTL=254
Reply from 10.60.46.254: bytes=32 time=2ms TTL=254
Reply from 10.60.46.254: bytes=32 time=2ms TTL=254
Reply from 10.60.46.254: bytes=32 time=3ms TTL=254
```

Windows - Commands

- tracert – network connectivity to each router hop to chosen IP address

```
C:\Users\itaym>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1     5 ms     3 ms     2 ms  192.168.43.1
  2    58 ms   256 ms   235 ms  10.194.248.150
  3    49 ms    27 ms    26 ms  192.168.249.113
  4    81 ms    29 ms    35 ms  192.168.234.1
  5     *        *        *     Request timed out.
  6    49 ms    22 ms    29 ms  192.168.234.17
  7     *        *        *     Request timed out.
  8   298 ms   191 ms    32 ms  82.102.132.78
  9    88 ms    88 ms    87 ms  80.179.166.142
 10   112 ms    98 ms    95 ms  72.14.216.121
 11   111 ms   103 ms    97 ms  108.170.251.129
 12    89 ms    89 ms    87 ms  66.249.94.245
 13   102 ms   100 ms    85 ms  8.8.8.8
```

Windows - Commands

- arp – a

```
c:\Users>arp -a

Interface: 192.168.43.166 --- 0x7
  Internet Address      Physical Address      Type
  192.168.43.1          4a-2c-a0-3c-16-01     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Windows - Commands

- nslookup - The DNS Query request serves to DNS server to identify an IP address / URL

```
c:\Users>nslookup 8.8.8.8
Server:  UnKnown
Address:  192.168.43.1

Name:    dns.google
Address:  8.8.8.8
```

```
c:\Users>nslookup dns.google
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    dns.google
Addresses:  2001:4860:4860::8844
          2001:4860:4860::8888
          8.8.8.8
          8.8.4.4
```

Windows - Commands

- route print – display all the routings that configure

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.43.1   192.168.43.166     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0      255.255.0.0         On-link      169.254.68.2    281
      169.254.0.0      255.255.0.0         On-link    169.254.152.173    281
    169.254.68.2  255.255.255.255         On-link      169.254.68.2    281
  169.254.152.173  255.255.255.255         On-link    169.254.152.173    281
  169.254.255.255  255.255.255.255         On-link      169.254.68.2    281
  169.254.255.255  255.255.255.255         On-link    169.254.152.173    281
     192.168.43.0    255.255.255.0         On-link     192.168.43.166    311
   192.168.43.166  255.255.255.255         On-link     192.168.43.166    311
   192.168.43.255  255.255.255.255         On-link     192.168.43.166    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      169.254.68.2    281
        224.0.0.0        240.0.0.0         On-link    169.254.152.173    281
        224.0.0.0        240.0.0.0         On-link     192.168.43.166    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      169.254.68.2    281
  255.255.255.255  255.255.255.255         On-link    169.254.152.173    281
  255.255.255.255  255.255.255.255         On-link     192.168.43.166    311
===========================================================================
Persistent Routes:
  None
```

Windows - Commands

- route - Create, view and delete existing routings
  - route add – route add –p { network and mask } via { gateway IP }
  - route delete – route add –p { network and mask } via { gateway IP }

Windows - Commands

- telnet - Perform an attempt to connect to communication equipment or servers

- Mainly used to check the network connection in front of a destination IP

```
c:\Users>telnet 8.8.8.8 23
Connecting To 8.8.8.8...
```

```
c:\Users>telnet 8.8.8.8 443
```

Windows - Commands

- netstat –noa

- View network traffic on the local computer

```
TCP    192.168.43.166:139     0.0.0.0:0              LISTENING       4
TCP    192.168.43.166:49410   52.139.250.253:443     ESTABLISHED     4772
TCP    192.168.43.166:50872   52.139.250.253:443     ESTABLISHED     12876
TCP    192.168.43.166:50878   108.177.126.188:5228   ESTABLISHED     13420
TCP    192.168.43.166:51214   23.221.151.154:443     CLOSE_WAIT      12084
TCP    192.168.43.166:51215   23.221.151.154:443     CLOSE_WAIT      12084
TCP    192.168.43.166:51216   23.221.151.154:443     CLOSE_WAIT      12084
TCP    192.168.43.166:51219   23.221.151.154:443     CLOSE_WAIT      12084
TCP    192.168.43.166:51220   23.221.151.154:443     CLOSE_WAIT      12084
TCP    192.168.43.166:51223   23.221.142.3:80        CLOSE_WAIT      12084
TCP    192.168.43.166:51224   23.221.142.3:80        CLOSE_WAIT      12084
TCP    192.168.43.166:51225   23.221.142.3:80        CLOSE_WAIT      12084
```

Windows - Commands

- cd: Switch between folders

- dir: display list of all the files

```
C:\Users\itaym>
C:\Users\itaym>
C:\Users\itaym>cd c:\

c:\>cd users

c:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 44CD-ADA5

 Directory of c:\Users

19-Aug-19  05:26 PM    <DIR>          .
19-Aug-19  05:26 PM    <DIR>          ..
19-Aug-19  05:27 PM    <DIR>          Itay-TEST
20-Aug-19  03:49 PM    <DIR>          itaym
02-Nov-18  07:58 AM    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)  157,979,435,008 bytes free
```

Windows - Commands

- echo <string> > <file_name>
- type NUL > <file_name> : create empty file
- del <file_name>: delete the file

```
C:\Users\itaym>echo TEST > TEST.txt
C:\Users\itaym>dir
 Directory of C:\Users\itaym
20-Aug-19  06:19 PM                 7 TEST.txt
```

```
C:\Users\itaym>type NUL > TEST2.txt

C:\Users\itaym>del TEST2.txt
```

Windows - Commands

- task list: Display all the running processes on your computer

```
C:\Users\itaym>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      7,684 K
Registry                       120 Services                   0     28,296 K
smss.exe                       512 Services                   0        976 K
csrss.exe                      532 Services                   0      4,712 K
wininit.exe                   1068 Services                   0      5,400 K
csrss.exe                     1084 Console                    1      5,916 K
services.exe                  1144 Services                   0     10,728 K
lsass.exe                     1160 Services                   0     17,296 K
winlogon.exe                  1244 Console                    1      9,576 K
svchost.exe                   1356 Services                   0      5,616 K
fontdrvhost.exe               1376 Services                   0      2,600 K
fontdrvhost.exe               1384 Console                    1      9,736 K
WUDFHost.exe                  1428 Services                   0      7,336 K
svchost.exe                   1484 Services                   0     30,904 K
WUDFHost.exe                  1544 Services                   0     15,036 K
```

Windows - Commands

- task kill: ending specific running processes on your computer

```
C:\Users\itaym>taskkill /PID 18724
SUCCESS: Sent termination signal to the process with PID 18724.
```

- sc: display all the services running on your computer

```
C:\Users\itaym>sc query

SERVICE_NAME: AdobeARMservice
DISPLAY_NAME: Adobe Acrobat Update Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Q\A