# Triagem rápida em sistemas *Unix-like* utilizando a ferramenta UAC

## *(Unix-like Artifacts Collector)*

Thiago Canozzo Lahr

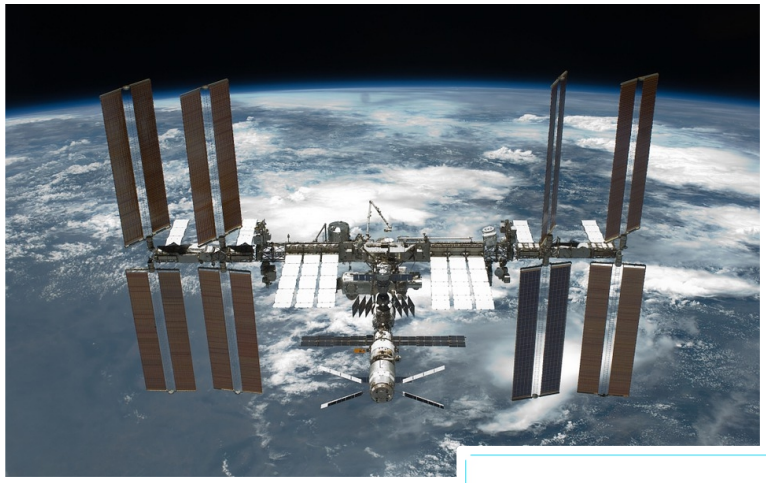
Analista Forense Digital

linkedin.com/in/tclahr

@tclahr

GTER 50 | GTS 36

2021-11-29

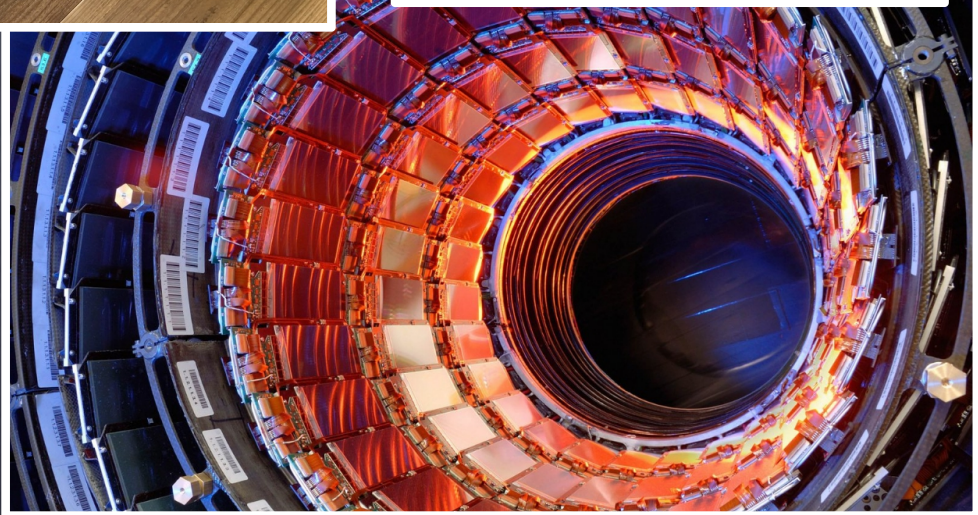


10:12 AM
My Favorites
My Storage
Special Offers
YouTube
NETFLIX
Spotify
Music
Aol HD.
PANDORA
vudu
HD Movies
CinemaNow
hulu PLUS
SnagFilms
vimeo

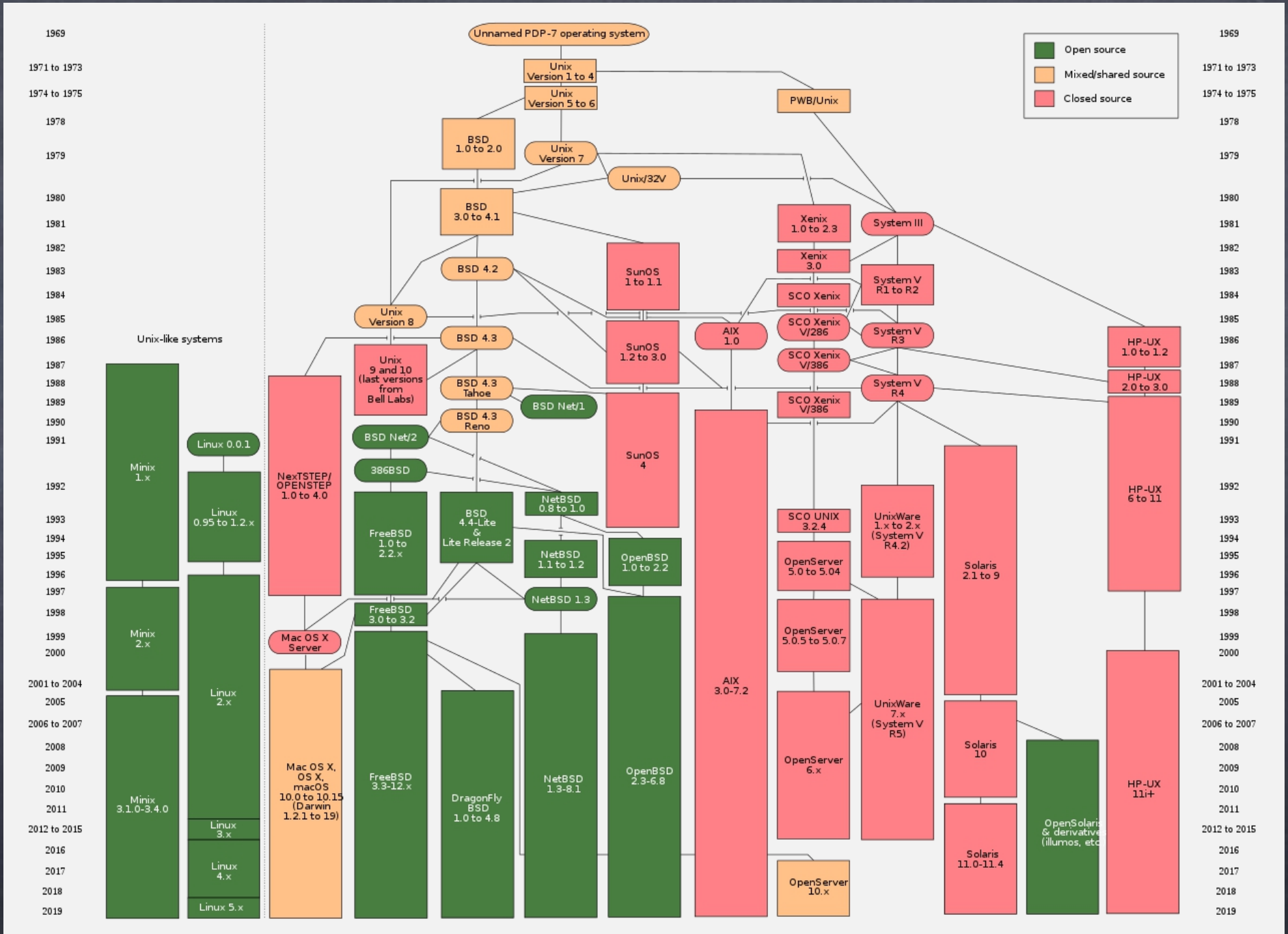
أهلاً و سهلاً
Bienvenue
Welcome Aboard

NetScaler
CITRIX

IBM
summit



# História do Unix



mac
OS

NetBSD

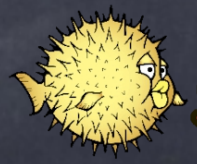
AIX

iOS

hp UX

solaris

FreeBSD



OpenBSD

```
64 bytes from 10.0.2.12: icmp_seq=9 ttl=255 time=11 ms
64 bytes from 10.0.2.12: icmp_seq=10 ttl=255 time=14 ms
64 bytes from 10.0.2.12: icmp_seq=11 ttl=255 time=9 ms
64 bytes from 10.0.2.12: icmp_seq=12 ttl=255 time=7 ms
64 bytes from 10.0.2.12: icmp_seq=13 ttl=255 time=7 ms
64 bytes from 10.0.2.12: icmp_seq=14 ttl=255 time=8 ms
^C
----10.0.2.12 PING Statistics----
15 packets transmitted, 15 packets received, 0% packet loss
round-trip min/avg/max = 6/10/26 ms
# ping 10.0.2.2
PING 10.0.2.2: (10.0.2.2): 56 data bytes
^C
----10.0.2.2 PING Statistics----
24 packets transmitted, 0 packets received, 100% packet loss
# route
usage: route [ -nqCvf ]  cmd [[ -<qualifers> ] args ]
# route show
usage: route [ -nqCvf ]  cmd [[ -<qualifers> ] args ]
0821-274 (botched keyword: show)
# route add 10.0.2.2 1
0821-279 writing to routing socket: Cannot reach the destination network.
1 host 10.0.2.2: gateway 1: 0821-285 ioctl returns 70
Cannot reach the destination network.
# route add default 10
```

# Importância da coleta de artefatos em sistemas ativos

- Artefatos voláteis
  - Processos ativos
  - Conexões de rede
  - Arquivos abertos
  - Sistemas de arquivos voláteis
  - Volumes (criptografados) montados
- Dump de memória RAM (quando possível)
- Metadados de arquivos e diretórios
- Nem sempre é possível fazer cópia dos dispositivos de armazenamento
- 99% vs 1%

# Importância da automatização

- Tenho acesso ao sistema, e agora?
- Padronização
- Ferramentas de linha de comando são sólidas e confiáveis
- Tem valor probatório se usado corretamente
- Porque somos preguiçosos :)

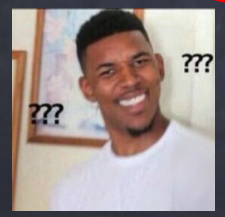
Então é só escrever um script que executa vários comandos e joga a saída para arquivos texto?

# Desafios da automatização

- shells possuem funcionalidades similares, **mas diferentes**!
  - sh (Bourne shell)
  - ksh (Korn shell)
  - bash (Bourne again shell)
  - zsh (Z-shell)

```
tclahr@debian-11-amd64:~$ uname -a
Linux debian-11-amd64 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
tclahr@debian-11-amd64:~$ ls -la /bin/sh
lrwxrwxrwx 1 root root 4 Aug 31 06:47 /bin/sh -> dash
tclahr@debian-11-amd64:~$ sh
$ if ! ls /12345; then echo "fail"; else echo "pass"; fi
ls: cannot access '/12345': No such file or directory
fail
$
```

```
$ uname -a
SunOS solaris-10-i386 5.10 Generic_147148-26 i86pc i386 i86pc
$ echo $SHELL
/bin/sh
$ if ! ls /12345; then echo "fail"; else echo "pass"; fi
!: not found
pass
$
```



# Desafios da automatização

- Nem todos os SOs possuem as mesmas ferramentas
  - Ferramentas GNU
  - BusyBox

```
tclahr@debian-11-amd64:~$ find --help
Usage: find [-H] [-L] [-P] [-Olevel] [-D debugopt

default path is the current directory; default ex
expression may consist of: operators, options, te
operators (decreasing precedence; -and is implici
      ( EXPR )   ! EXPR   -not EXPR   EXPR1 -a EX
      EXPR1 -o EXPR2   EXPR1 -or EXPR2   EXPR1 ,
positional options (always true): -daystart -foll

normal options (always true, specified before oth
      -depth --help -maxdepth LEVELS -mindepth LE
      --version -xdev -ignore_readdir_race -noign
tests (N can be +N or -N or N): -amin N -anewer F
      -cnewer FILE -ctime N -empty -false -fstype
      -ilname PATTERN -iname PATTERN -inum N -iwh
      -links N -lname PATTERN -mmin N -mtime N -n
      -nouser -nogroup -path PATTERN -perm [-/]MO
      -readable -writable -executable
      -wholename PATTERN -size N[bcwkMG] -true -t
      -used N -user NAME -xtype [bcdpfls]      -o

actions: -delete -print0 -printf FORMAT -fprintf
      -fprint0 FILE -fprint FILE -ls -fls FILE -prune -quit
      -exec COMMAND ; -exec COMMAND {} + -ok COMMAND ;
      -execdir COMMAND ; -execdir COMMAND {} + -okdir COMMAND ;
```

```
linux-embedded[~]$ ls -l /usr/bin/find
lrwxrwxrwx    1 1000     default        17 Jan  1  2000 /usr/bin/find -> ../../bin/busybox*
linux-embedded[~]$ find --help
BusyBox v1.00 (2008.04.24-06:54+0000) multi-call binary

Usage: find [PATH...] [EXPRESSION]

Search for files in a directory hierarchy.  The default PATH is
the current directory; default EXPRESSION is '-print'

EXPRESSION may consist of:
        -follow         Dereference symbolic links.
        -name PATTERN   File name (leading directories removed) matches PATTERN.
        -print          Print (default and assumed).

        -type X         Filetype matches X (where X is one of: f,d,l,b,c,...)
        -perm PERMS     Permissions match any of (+NNN); all of (-NNN);
                        or exactly (NNN)
        -mtime TIME     Modified time is greater than (+N); less than (-N);
                        or exactly (N) days

linux-embedded[~]$
```

# Desafios da automatização

```
root@apache-server:~# netstat -lpeanut
-bash: netstat: command not found
root@apache-server:~#
```

```
root@p1375-pvm1:/proc/4260098/object # md5sum a.out
ksh: md5sum:  not found
root@p1375-pvm1:/proc/4260098/object #
```

# Desafios da automatização

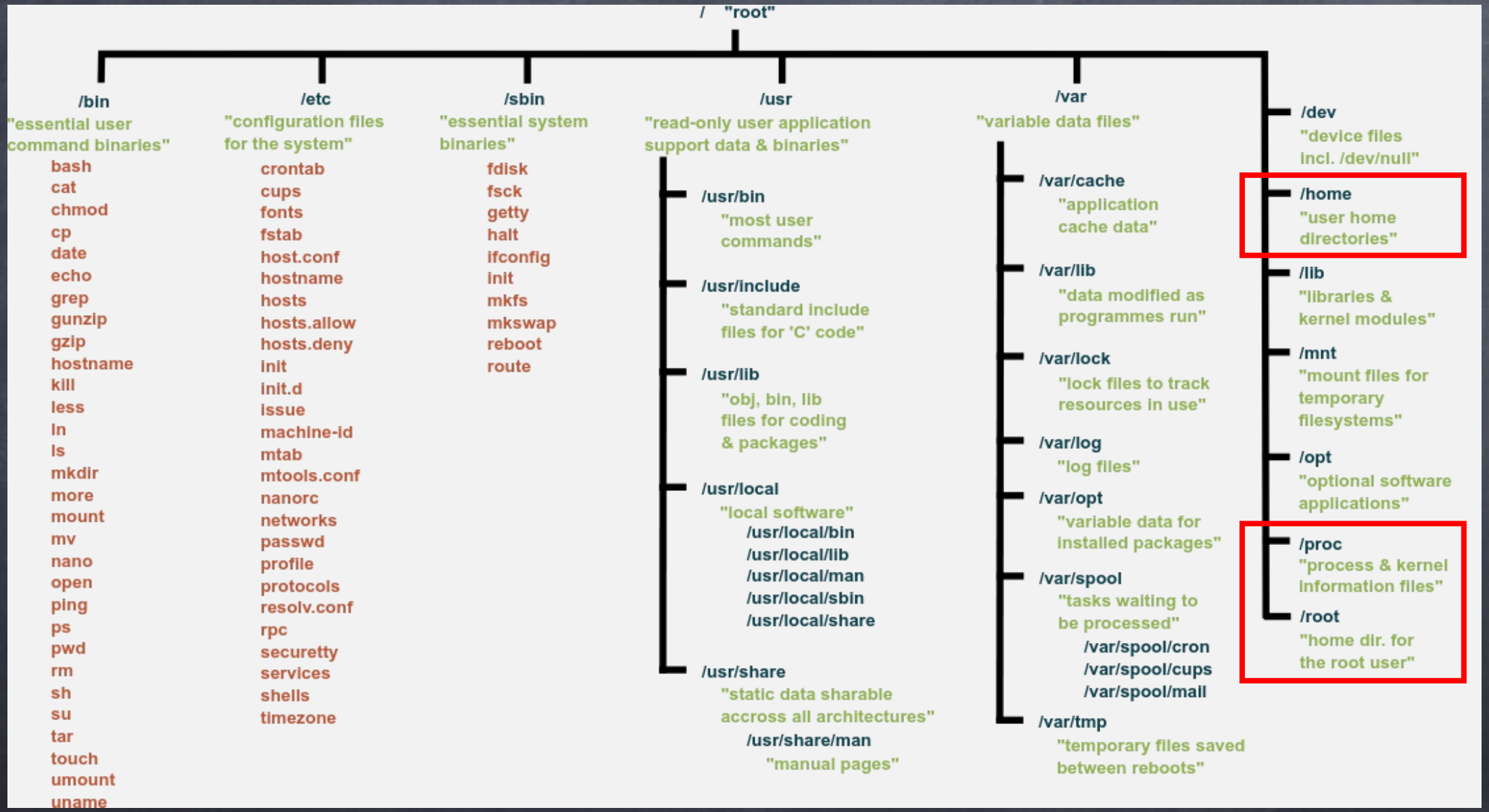
- Nem sempre ferramentas possuem as mesmas funcionalidades

```
$ find --version
find (GNU findutils) 4.6.0.225-235f
Copyright (C) 2019 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Eric B. Decker, James Youngman, and Kevin Dalley.
Features enabled: D_TYPE O_NOFOLLOW(enabled) LEAF_OPTIMISATION FTS(FTS_CWDFD) CBO(level=2)
$ find / -maxdepth 2 -type f
/proc/fb
/proc/dma
/proc/keys
/proc/kmsg
/proc/misc
/proc/mtrr
```

```
cecuser@p1375-pvm1:/ $ uname -s
AIX
cecuser@p1375-pvm1:/ $ find --version
Usage: find [-H | -L] path-list [predicate-list]
cecuser@p1375-pvm1:/ $ find / -maxdepth 2 -type f
find: bad option -maxdepth
cecuser@p1375-pvm1:/ $
```

# Filesystem Hierarchy Standard (FHS)



# $HOME

```
$ uname -a
SunOS solaris-10-i386 5.10 Generic_147148-26 i86pc i386 i86pc
$ ls /home
$ ls /export/home
oracle  tclahr
$
```

```
tclahr@tclahrs-iPro ~ % uname -a
Darwin tclahrs-iPro 19.6.0 Darwin Kernel Version 19.6.0: Thu Oct 29 22:56:45 PDT 2020; root:xnu-6153.141.2.2~1/RELEASE_X86_64 x86_64
tclahr@tclahrs-iPro ~ % ls /home
tclahr@tclahrs-iPro ~ % ls /Users
Shared  tclahr
tclahr@tclahrs-iPro ~ %
```

```
heroltexx:/ $ uname -a
Linux localhost 3.18.140-g1beea6a776c7 #1 SMP PREEMPT Sun Sep 5 13:11:29 PDT 2021 aarch64
heroltexx:/ $ getprop ro.build.version.release
11
heroltexx:/ $ ls /home
ls: /home: No such file or directory
1|heroltexx:/ $
```

# /root

```
[root@redhat-6-5 ~]# uname -a
Linux redhat-6-5 2.6.32-431.el6.x86_64 #1 SMP Sun Nov 10 22:19:54 EST 2013 x86_64 x86_64 x86_64 GNU/Linux
[root@redhat-6-5 ~]# ls /root
anaconda-ks.cfg  install.log  install.log.syslog
[root@redhat-6-5 ~]#
```

```
root@freebsd-12-amd64:~ # uname -a
FreeBSD freebsd-12-amd64 12.0-RELEASE FreeBSD 12.0-RELEASE r341666 GENERIC  amd64
root@freebsd-12-amd64:~ # ls /root
.cshrc          .history        .k5login        .login          .profile
root@freebsd-12-amd64:~ #
```

```
tclahr@tclahrs-iPro ~ % uname -a
Darwin tclahrs-iPro 19.6.0 Darwin Kernel Version 19.6.0: Thu Oct 29 22:56:45 PDT 2020; root:xnu-6153.141.2.2~1/RELEASE_X86_64 x86_64
tclahr@tclahrs-iPro ~ % ls /root
ls: /root: No such file or directory
tclahr@tclahrs-iPro ~ %
```

```
root@p1375-pvm1:/ # uname -a
AIX p1375-pvm1 2 7 00F9059E4C00
root@p1375-pvm1:/ # ls /root
/root not found
root@p1375-pvm1:/ # grep ^root /etc/passwd
root:!:0:0::/:/usr/bin/ksh
root@p1375-pvm1:/ #
```

# procfs

```
root@openwrt-17-amd64:~# uname -a
Linux openwrt-17-amd64 4.4.182 #0 SMP Tue Jun 18 18:45:43 2019 x86_64 GNU/Linux
root@openwrt-17-amd64:~# ls /proc
1          1463       433        600        719        cpuinfo    kmsg       stat
10         1476       434        603        724        crypto     loadavg    swaps
1085       187        435        606        725        devices    meminfo    sys
1094       189        5          609        787        diskstats  misc       sysrq-trigger
11         190        523        631        8          dma        modules    sysvipc
1143       191        525        632        801        driver     mounts     thread-self
1173       193        546        635        9          fb         mpt        uptime
1234       2          553        636        931        filesystems mtrr      version
1275       256        586        639        932        fs         net        vmstat
1316       257        591        679        933        interrupts partitions
1398       3          594        680        acpi       iomem      scsi
```

```
tclahr@tclahrs-iPro ~ % uname -a
Darwin tclahrs-iPro 19.6.0 Darwin Kernel Version 19.6.0: Thu Oct 29 22:56:45 PDT 2020; root:xnu-6153.141.2.2~1/RELEASE_X86_64 x86_64
tclahr@tclahrs-iPro ~ % ls /proc
ls: /proc: No such file or directory
tclahr@tclahrs-iPro ~ %
```

```
netbsd-7-amd64$ ls /proc
0       1017    184     470     567     655     731     869     909     996     curproc loadavg mounts  stat    version
1       1036    282     498     643     671     764     894     974     cpuinfo devices meminfo self    uptime
netbsd-7-amd64$
```

```
openbsd-6-5-amd64$ uname -a
OpenBSD openbsd-6-5-amd64 6.5 GENERIC#3 amd64
openbsd-6-5-amd64$ ls /proc
ls: /proc: No such file or directory
openbsd-6-5-amd64$
```

# # ls -la /proc/PID

```
root@p1375-pvm1:/proc/4260098 # ls -la
total 16
dr-xr-xr-x    1 cecuser  cecuser          0 Oct 21 15:30 .
dr-xr-xr-x    1 root     system           0 Oct 21 15:30 ..
-rw-------    1 cecuser  cecuser          0 Oct 21 15:30 as
-r--------    1 cecuser  cecuser        128 Oct 21 15:30 cred
--w-------    1 cecuser  cecuser          0 Oct 21 15:30 ctl
lr-x------    6 cecuser  cecuser          0 Oct 21 15:30 cwd -> /tmp/
dr-x------    1 cecuser  cecuser          0 Oct 21 15:30 fd
dr-xr-xr-x    1 cecuser  cecuser          0 Oct 21 15:30 lwp
-r--------    1 cecuser  cecuser          0 Oct 21 15:30 map
-r--------    1 cecuser  cecuser          0 Oct 21 15:30 mmap
dr-x------    1 cecuser  cecuser          0 Oct 21 15:30 object
-r--r--r--    1 cecuser  cecuser        448 Oct 21 15:30 psinfo
lr-x------   20 cecuser  cecuser          0 Oct 21 15:29 root -> /
-r--------    1 cecuser  cecuser      12288 Oct 21 15:30 sigact
-r--------    1 cecuser  cecuser       1520 Oct 21 15:30 status
-r--r--r--    1 cecuser  cecuser          0 Oct 21 15:30 sysent
root@p1375-pvm1:/proc/4260098 #
```

```
total 0
dr-xr-xr-x   9 tclahr tclahr 0 Oct 21 16:44 .
dr-xr-xr-x 228 root   root   0 Oct 21 09:33 ..
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 arch_status
dr-xr-xr-x   2 tclahr tclahr 0 Oct 21 16:46 attr
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 autogroup
-r--------   1 tclahr tclahr 0 Oct 21 16:46 auxv
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 cgroup
--w-------   1 tclahr tclahr 0 Oct 21 16:46 clear_refs
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:44 cmdline
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 comm
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 coredump_filter
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 cpu_resctrl_groups
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 cpuset
lrwxrwxrwx   1 tclahr tclahr 0 Oct 21 16:46 cwd -> /tmp
-r--------   1 tclahr tclahr 0 Oct 21 16:46 environ
lrwxrwxrwx   1 tclahr tclahr 0 Oct 21 16:46 exe -> '/tmp/sshd (deleted)'
dr-x------   2 tclahr tclahr 0 Oct 21 16:46 fd
dr-xr-xr-x   2 tclahr tclahr 0 Oct 21 16:46 fdinfo
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 gid_map
-r--------   1 tclahr tclahr 0 Oct 21 16:46 io
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 limits
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 loginuid
dr-x------   2 tclahr tclahr 0 Oct 21 16:46 map_files
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 maps
-rw-------   1 tclahr tclahr 0 Oct 21 16:46 mem
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 mountinfo
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 mounts
-r--------   1 tclahr tclahr 0 Oct 21 16:46 mountstats
dr-xr-xr-x  55 tclahr tclahr 0 Oct 21 16:46 net
dr-x--x--x   2 tclahr tclahr 0 Oct 21 16:46 ns
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 numa_maps
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 oom_adj
-r--r--r--   1 tclahr tclahr 0 Oct 21 16:46 oom_score
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 oom_score_adj
-r--------   1 tclahr tclahr 0 Oct 21 16:46 pagemap
-r--------   1 tclahr tclahr 0 Oct 21 16:46 patch_state
-r--------   1 tclahr tclahr 0 Oct 21 16:46 personality
-rw-r--r--   1 tclahr tclahr 0 Oct 21 16:46 projid_map
lrwxrwxrwx   1 tclahr tclahr 0 Oct 21 16:46 root -> /
```

Então é só escrever um script que executa vários comandos e joga a saída para arquivos texto?

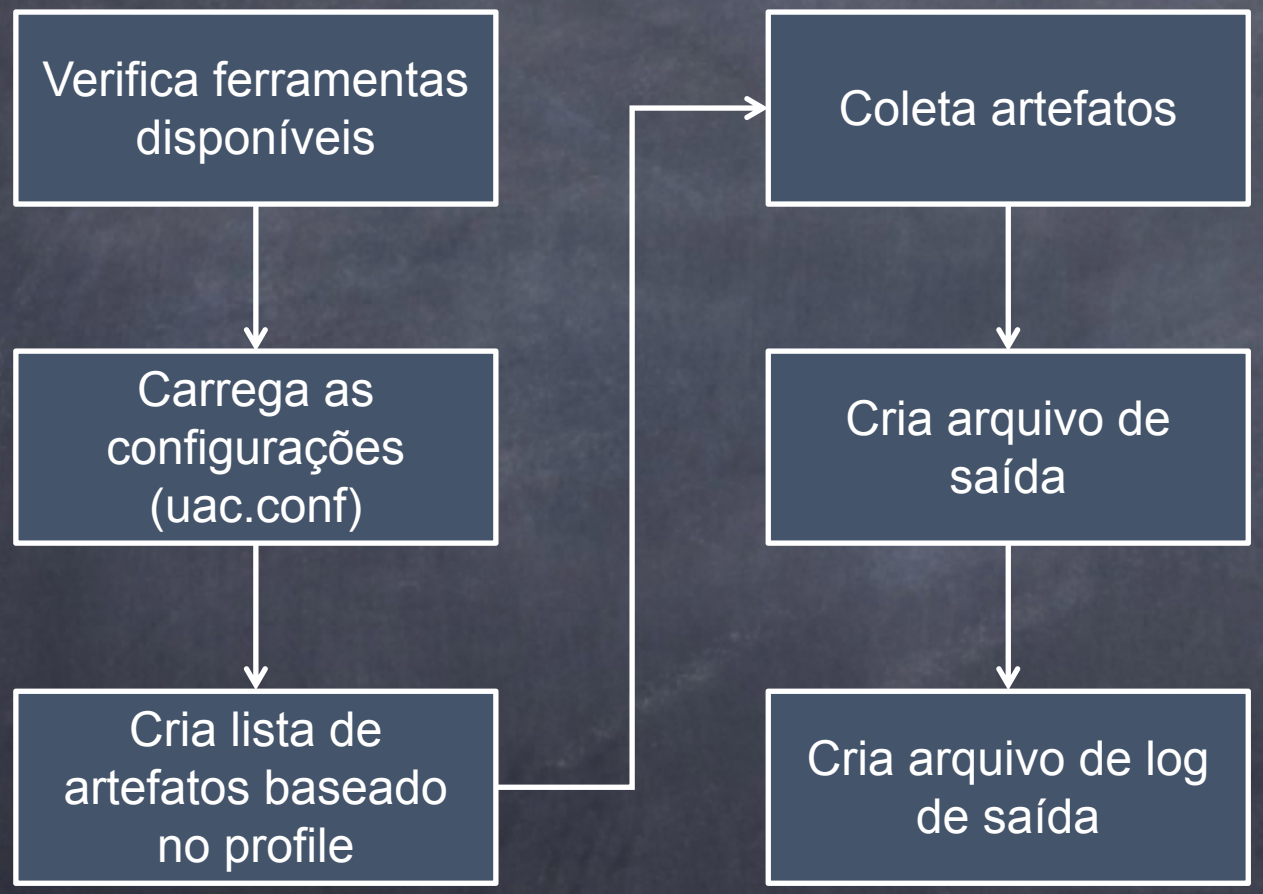
# UAC (Unix-like Artifacts Collector)

- Ferramenta para coleta automatizada de artefatos em sistemas ativos
- Utiliza comandos/ferramentas *built-in* do sistema operacional
- Coleta de artefatos é baseada em arquivos YAML
- Respeita a ordem de volatilidade dos dados
- Não necessita instalação
- Suporta 9 diferentes sistemas operacionais
  - android, aix, freebsd, linux, macos, netbsd, netscaler, openbsd e solaris
- Escrita em *shell script*
  - perl
  - C
- Open Source
- Download: github.com/tclahr/uac

# Alguns dos artefatos coletados pelo UAC

- Informações sobre processos ativos
  - Processos onde o binário tenha sido excluído
  - Cálculo do hash
  - Extração das strings
  - Informações do procfs
- Conexões de rede
- Serviços ativos
- Informações sobre discos, volumes e sistemas de arquivos
- Pacotes instalados
- Informações sobre o hardware
- Containers e VMs
- Criação do *bodyfile* (wiki.sleuthkit.org/index.php?title=Body_file)
- Hash dos executáveis
- Coleta de logs, arquivos de configurações, histórico de comandos...
- Dump de memória RAM em sistemas Linux x86_64

# Por trás das cortinas



# Demonstração

# Obrigado!

Thiago Canozzo Lahr

linkedin.com/in/tclahr

@tclahr

github.com/tclahr/uac