# DEFT Linux

WE ARE BACK!

www.deftlinux.net

# $WHOAMI

## GIOVANNI 'sug4r' RATTARO

- IT SECURITY CONSULTANT

OPEN MINDED

- Italian board member old <<back|track Linux project
- Staff DEFT Linux
- BLAH BLAH BLAH...

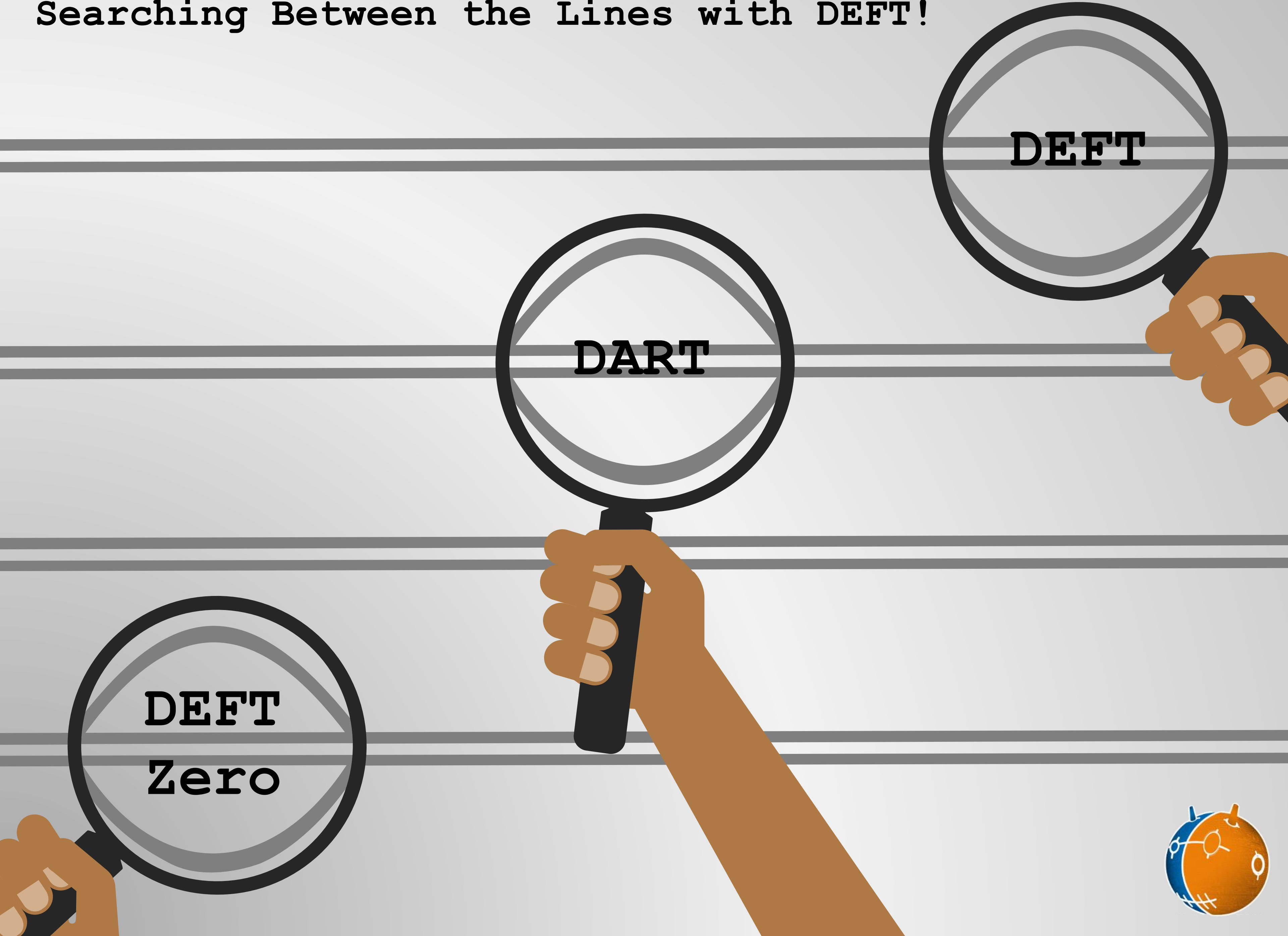
# WHAT IS DEFT?

**Free DFIR Linux distribution (since 2005)**

Digital Evidence & Forensic Toolkit

**Live || Install your Forensic LAB!**

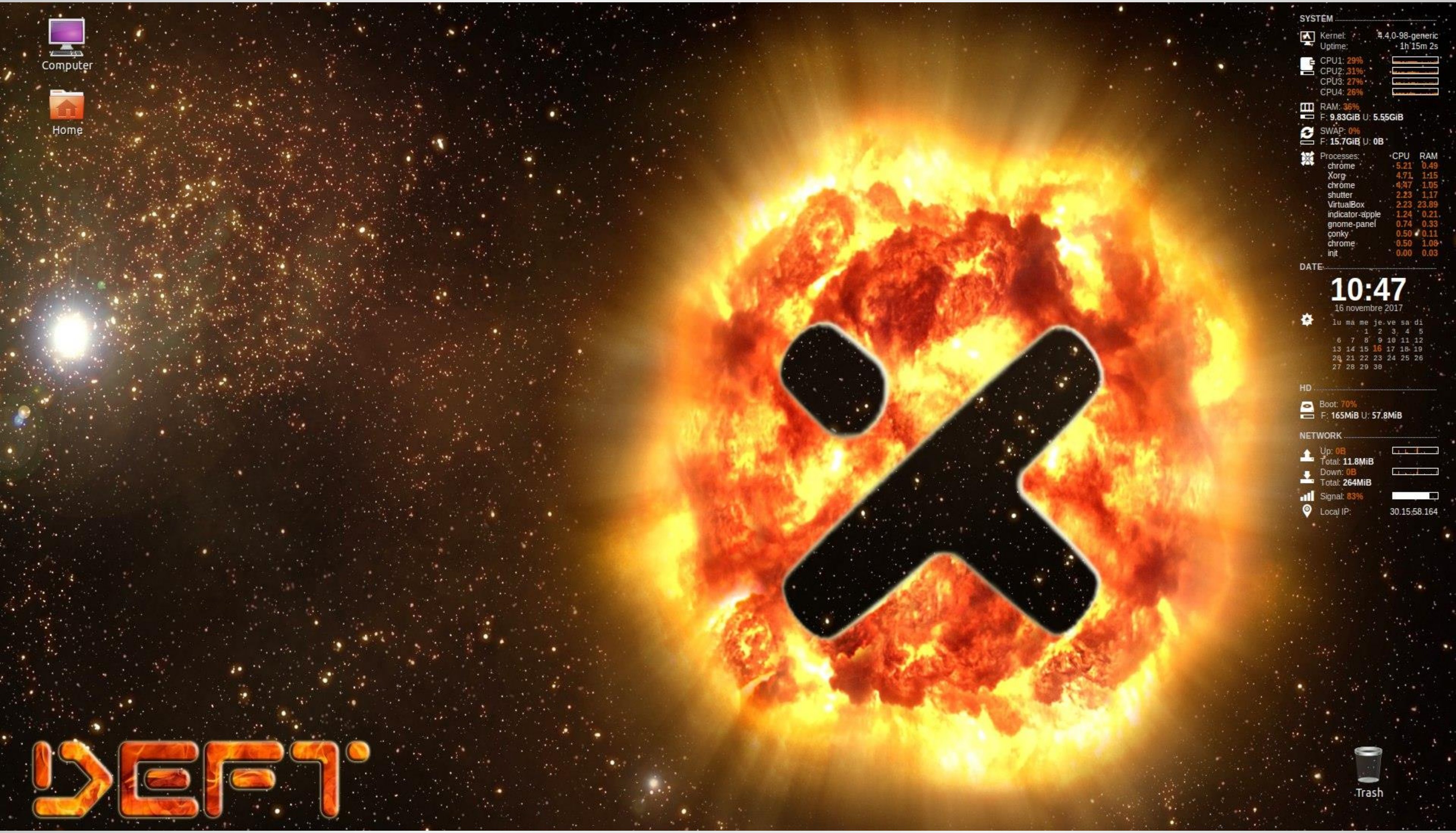
# Searching Between the Lines with DEFT!



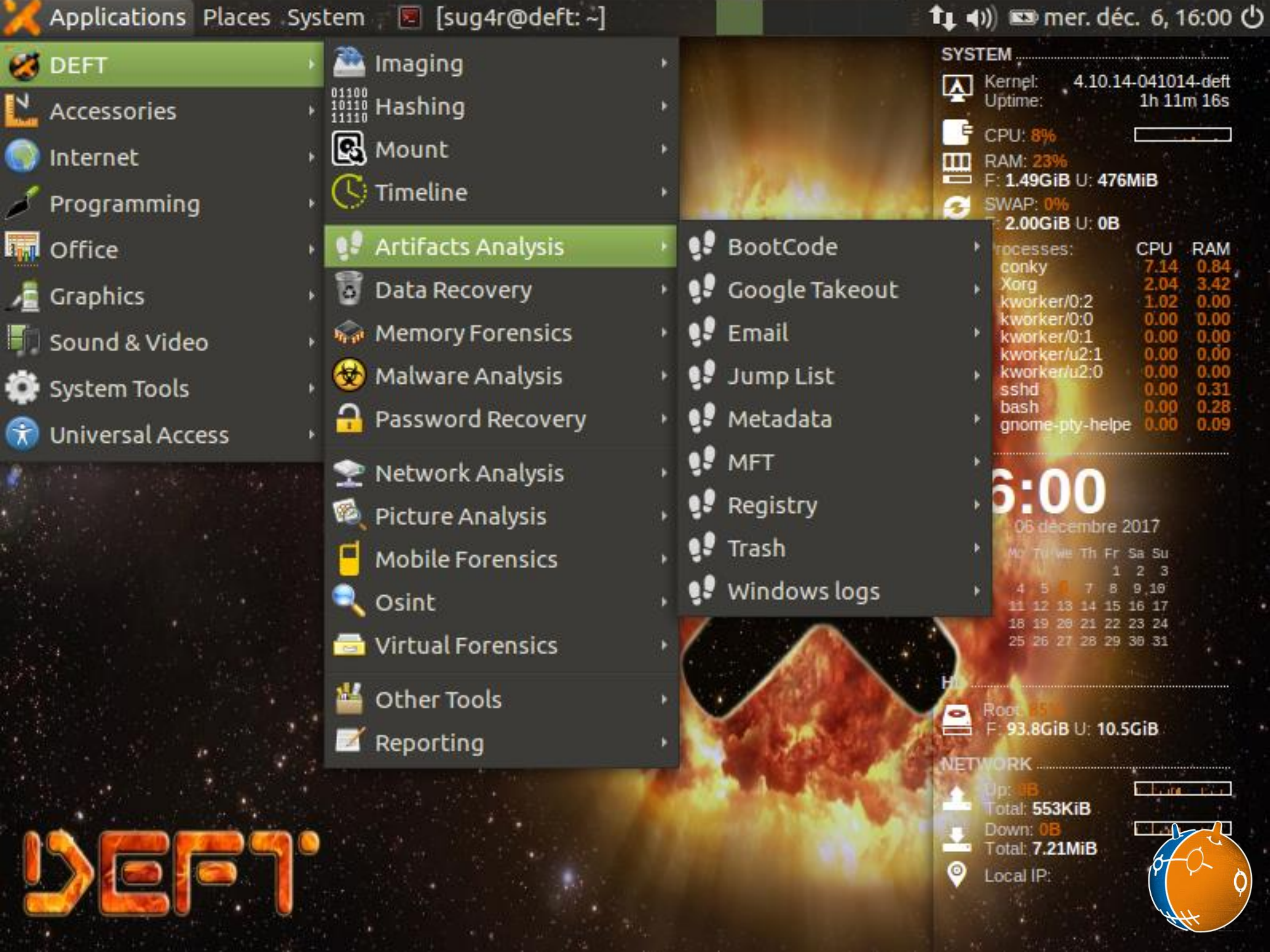
# Next release "DEFT X"

**codename: Xplosion**

# DEFT X



```
SYSTEM
Kernel:                4.4.0-98-generic
Uptime:                      1h 15m 2s
CPU1: 29%
CPU2: 31%
CPU3: 27%
CPU4: 26%
RAM: 36%
F: 9.83GiB U: 5.55GiB
SWAP: 0%
F: 15.7GiB U: 0B
Processes:             CPU    RAM
  chrome               5.21   0.49
  Xorg                 4.71   1.15
  chrome               4.47   1.05
  shutter              2.23   1.17
  VirtualBox           2.23  23.89
  indicator-apple      1.24   0.21
  gnome-panel          0.74   0.33
  conky                0.50   0.11
  chrome               0.50   1.08
  init                 0.00   0.03
DATE
        10:47
   16 novembre 2017
   lu ma me je ve sa di
          1  2  3  4  5
    6  7  8  9 10 11 12
   13 14 15 16 17 18 19
   20 21 22 23 24 25 26
   27 28 29 30
HD
Boot: 70%
F: 165MiB U: 57.8MiB
NETWORK
Up: 0B
Total: 11.8MiB
Down: 0B
Total: 264MiB
Signal: 83%
Local IP:          30.15.58.164
```



```
SYSTEM
Kernel:     4.10.14-041014-deft
Uptime:             1h 11m 16s
CPU: 8%
RAM: 23%
F: 1.49GiB U: 476MiB
SWAP: 0%
F: 2.00GiB U: 0B
rocesses:            CPU   RAM
 conky               7.14  0.84
 Xorg                2.04  3.42
 kworker/0:2         1.02  0.00
 kworker/0:0         0.00  0.00
 kworker/0:1         0.00  0.00
 kworker/u2:1        0.00  0.00
 kworker/u2:0        0.00  0.00
 sshd                0.00  0.31
 bash                0.00  0.28
 gnome-pty-helpe     0.00  0.09
6:00
 06 décembre 2017
 Mo Tu We Th Fr Sa Su
              1  2  3
  4  5  6  7  8  9 10
 11 12 13 14 15 16 17
 18 19 20 21 22 23 24
 25 26 27 28 29 30 31
HD
Root:
F: 93.8GiB U: 10.5GiB
NETWORK
Up: 0B
Total: 553KiB
Down: 0B
Total: 7.21MiB
Local IP:
```

deft
zero

# DEFT Zero

- ☑ Live minimal version
- ☑ "Disk image" ONLY
- ☑ 32bit
- ☑ It runs on every PC
- □ Fully updated

dart

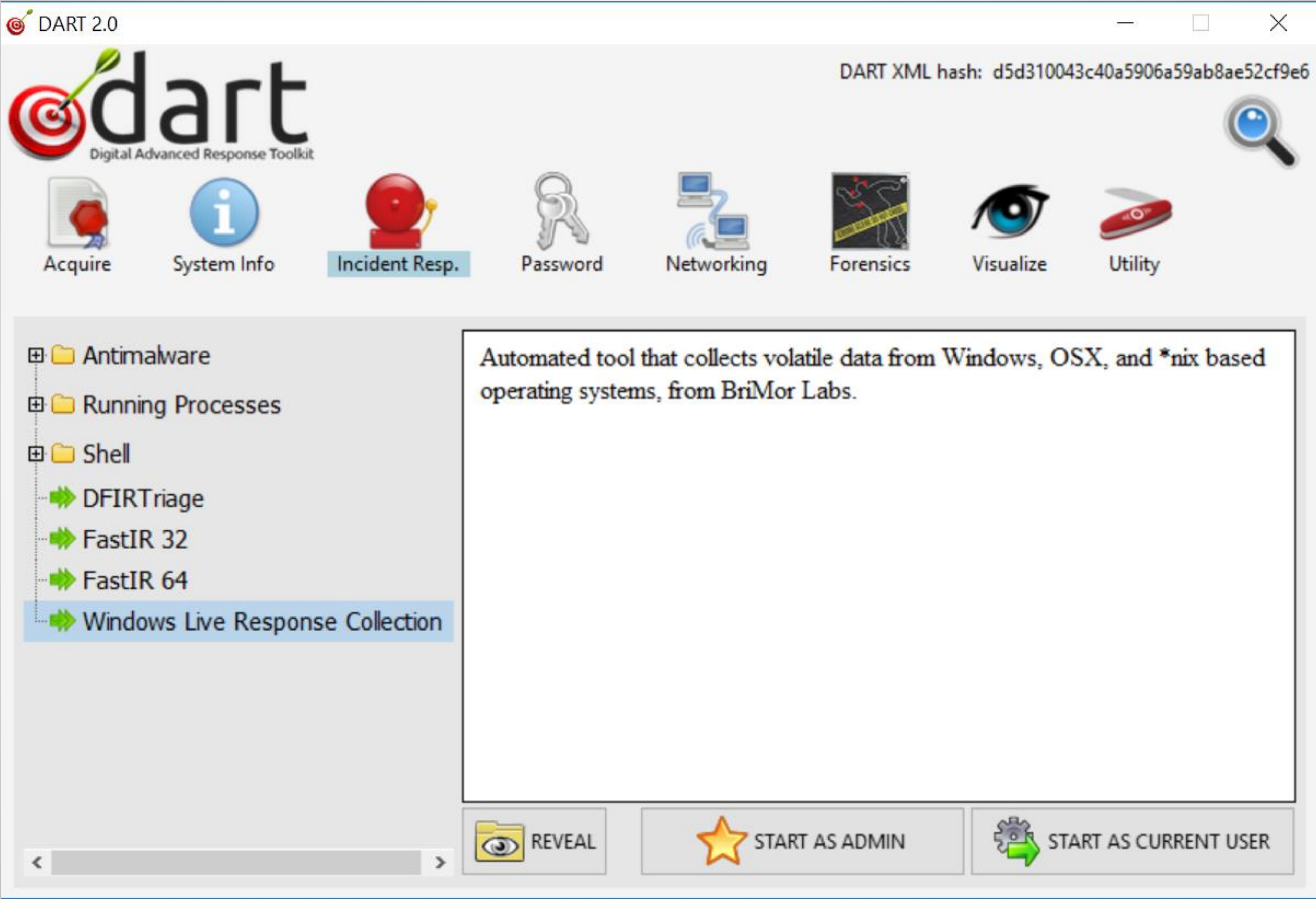
Digital Advanced Response Toolkit

DART

Digital Advanced Response Toolkit

1. Live Forensic Analysis
2. Incident response
3. About 300 tools (Win, Linux, OSX)
4. Customizable

# DART 2018

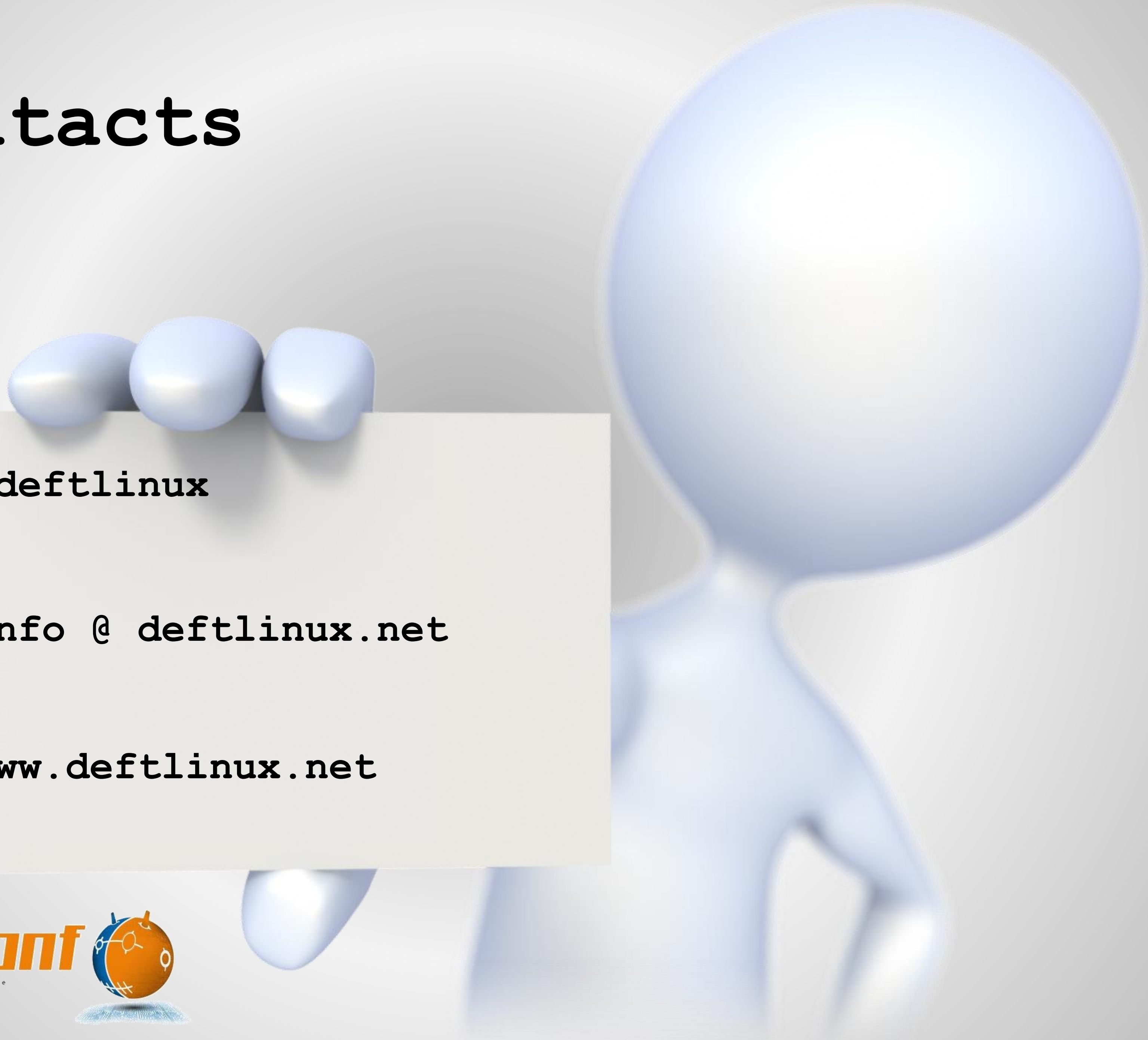


Automated tool that collects volatile data from Windows, OSX, and *nix based operating systems, from BriMor Labs.

Thank You!

www.deftlinux.net

# Contacts



@deftlinux

✉ info @ deftlinux.net

WWW www.deftlinux.net

botconf

The botnet fighting conference