



TLP WHITE

CoRI&IN
2020

TSURUGI Linux

Giovanni Rattaro
 [tsurugi_linux](#)

\$WHOAMI

GIOVANNI 'sug4r' RATTARO

• IT SECURITY CONSULTANT @



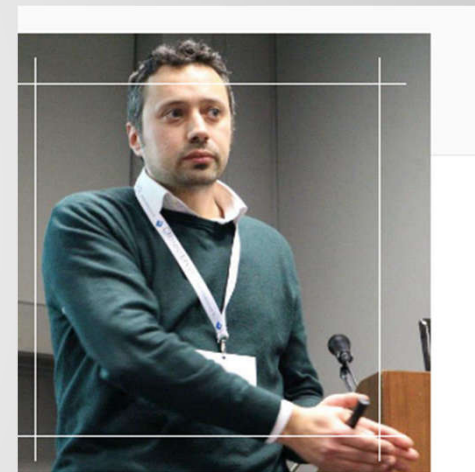
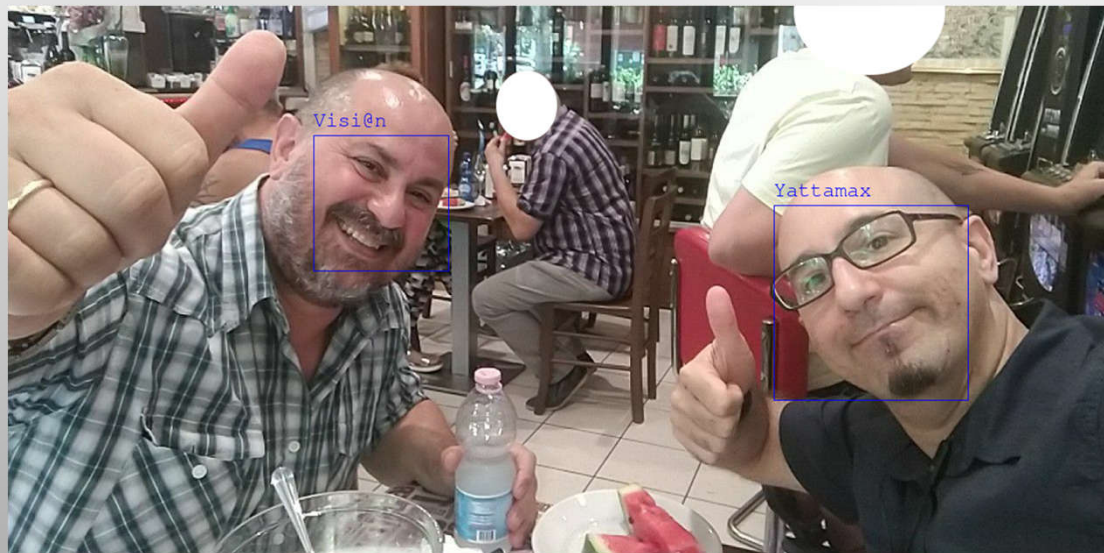
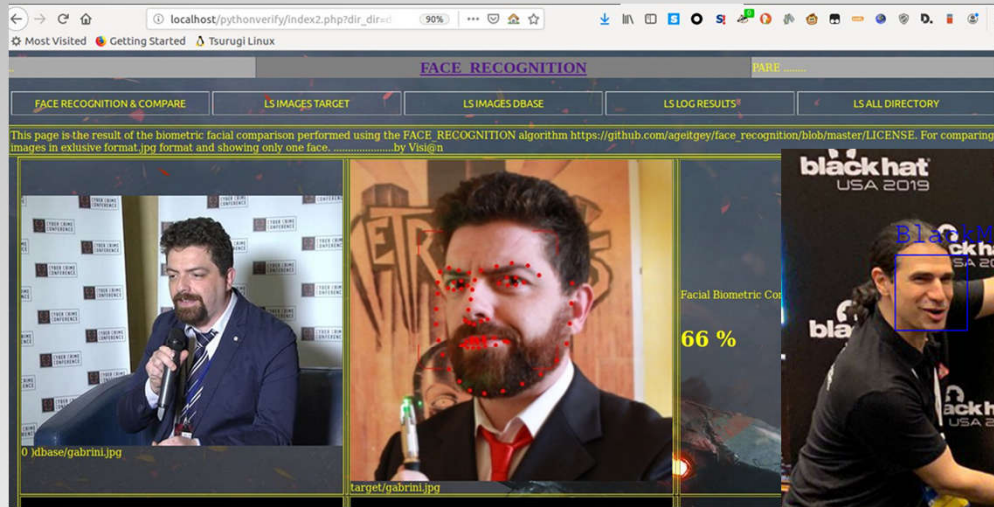
• Italian staff member old <<back|track Linux project

• Ex developer DEFT Linux

• Passionate DFIR instructor

• TSURUGI Linux core developer and project team leader

The team



tsurugi-linux.org



Some conferences



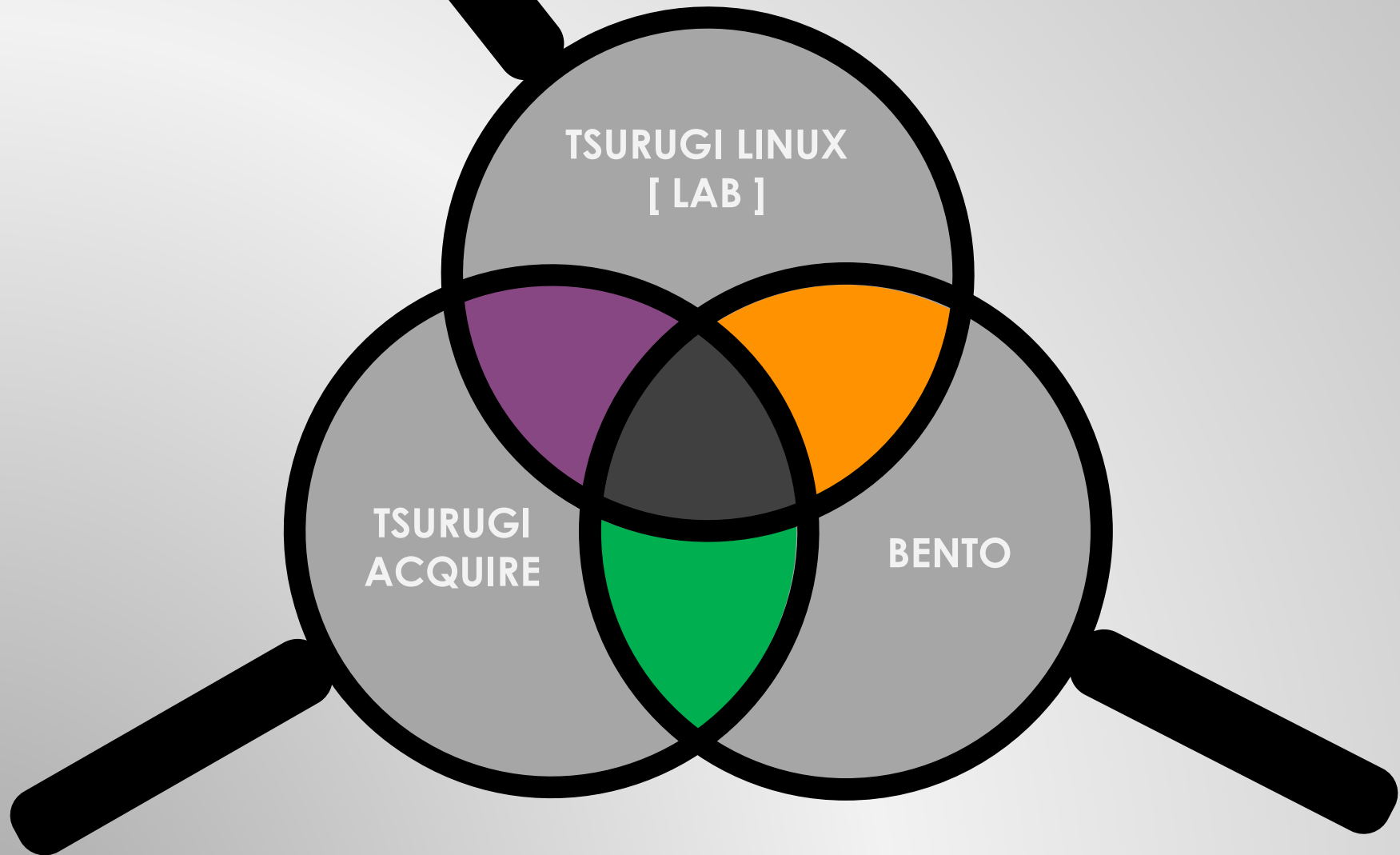
tsurugi-linux.org

TSURUGI LINUX

OPEN SOURCE PROJECT

tsurugi-linux.org

TSURUGI LINUX project





TSURUGI LINUX [LAB]

- 64 bits Linux distribution
- Based on UBUNTU LTS version
- Patched kernel 5.4.2
- DFIR
- OSINT / Malware Analysis / Computer vision
- For educational and/or professional use

- tsurugi's Home
- Onboard
- Displays
- TSURUGI device unlocker
- Install TSURUGI 2019.1
- Trash
- Keyboard
- Mouse keys switch
- OSINT Switcher



SYSTEM

Kernel: 5.1.15-050115-tsurugi
 Uptime: 0h 2m 26s

CPU1: 0%
 CPU2: 0%

RAM: 39%
 F: 2.96GiB U: 908MiB

SWAP: 0%
 F: 0B U: 0B

Processes:	CPU	RAM
Xorg	0.02	1.07
mate-cpufreq-ap	0.55	0.15
conky	0.42	0.07
sleep	0.00	0.00
bash	0.08	0.00
gvfsd-dnssd	0.00	0.00
gvfsd-metadata	0.00	0.01
obexd	0.00	0.00
gvfsd-network	0.00	0.00
notification-ar	0.00	0.00

DATE

01:31
 30 August 2019

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

Cdrom: 0%
 F: 0B U: 3.87GiB

Rofs: 0%
 F: 0B U: 3.79GiB

NETWORK

Up: 0B
 Total: 1.31MiB

Down: 0B
 Total: 184MiB

Local IP: 10.0.2.15

TSURUGI LINUX 2019.1

SPECIALS FEATURES?



`tsurugi-linux.org`

Custom Boot options

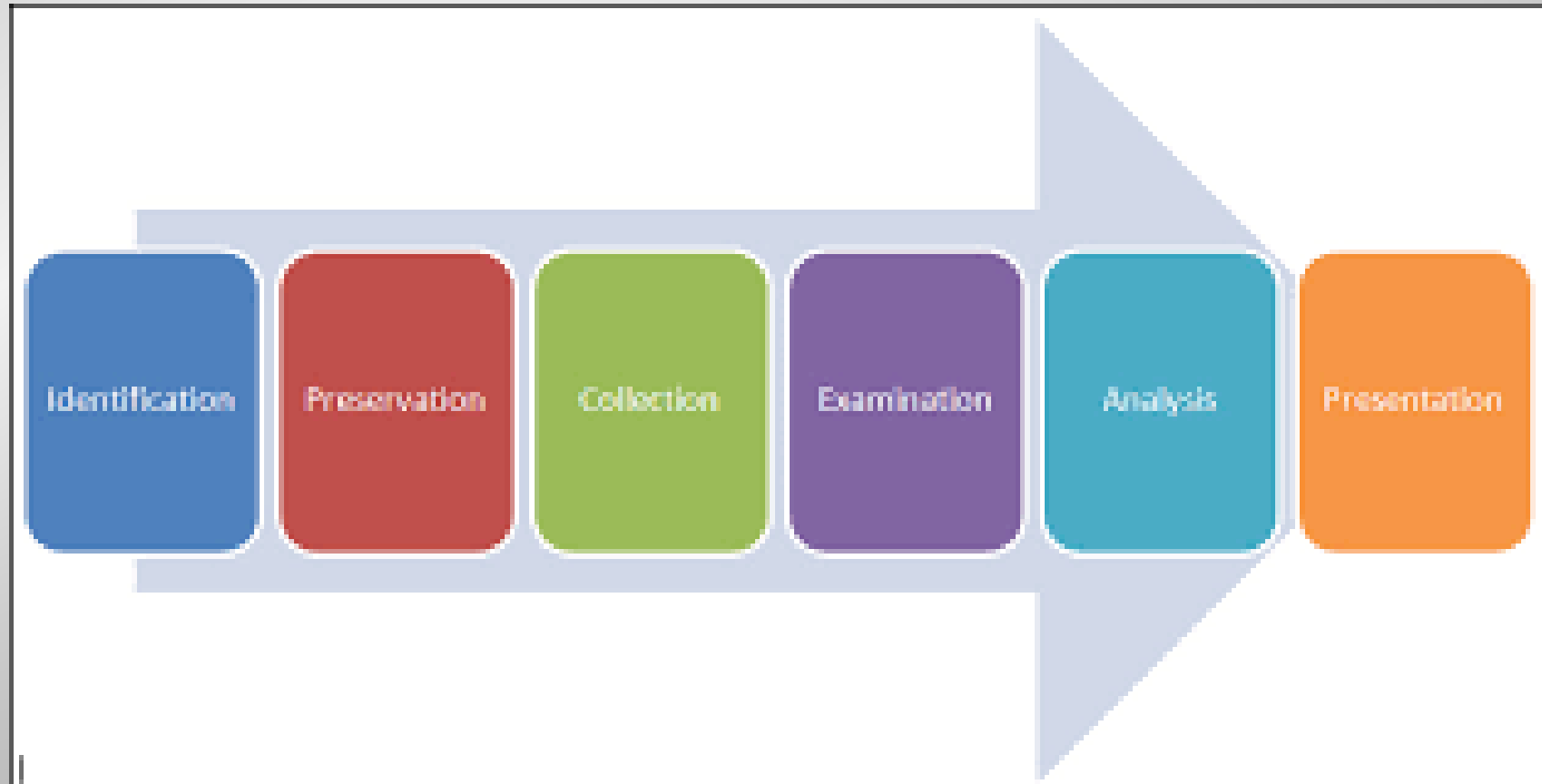


TSURUGI
LINUX

- 1 TSURUGI Linux Live (GUI mode)
TSURUGI Linux Live (GUI mode, RAM preload)
TSURUGI Linux Live (Text mode)
- 2 TSURUGI Linux Live (Text mode, RAM preload)
- 3 TSURUGI Linux Live (GUI mode) – Blacklist nVidia driver
TSURUGI Linux Live (GUI mode) – Blacklist ATI driver
Check disc for defects

F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

Our idea based on investigation 6 phases



TSURUGI Linux main menu & tools classification



- Imaging
- Hashing
- Mount
- Timeline
- Artifacts Analysis
- Data Recovery
- Memory Forensics
- Malware Analysis
- Password Recovery
- Network Analysis
- Picture Analysis
- Mobile Forensics
- OSINT
- Cloud Analysis
- Virtual Forensics
- Crypto Currency
- Other Tools
- Reporting



Imaging menu

The image displays a Linux desktop environment with a dark theme. A nested menu is open, starting from the 'TSURUGI' application. The menu path is: TSURUGI > Imaging > Other Tools > AFF > EWF. The 'EWF' sub-menu is currently selected and expanded, showing the following tools with checkboxes:

- ewfdebug
- ewfexport
- ewfinfo
- ewfrecover
- ewfverify

The 'Other Tools' menu also lists several other utilities:

- cyclone
- dc3dd
- dcfldd
- dd
- dd_rescue
- ddrescue
- DDRescue-GUI
- esximager
- ewfacquire
- ewfacquirestream
- ftkimager
- Guymager

At the bottom of the desktop, there are three utility icons: 'Mouse keys switch', 'Onboard' (with 'O' and 'B' keys highlighted), and 'OSINT Switcher' (with a magnifying glass icon).

Artifacts analysis

The image shows a software application menu with a dark background and a light green highlight on the 'Artifacts Analysis' option. The menu is organized into several columns. The first column contains various utility categories like 'Accessories', 'Internet', and 'System Tools'. The second column lists forensic and analysis tools such as 'Imaging', 'Hashing', 'Mount', and 'Timeline'. The third column, which is currently expanded, lists specific artifact categories like 'Apple/Mac', 'Boot Code', 'Browser', 'Email', 'Files', 'File System', 'Google Takeout', 'Jump List', 'Metadata', 'Office Documents', 'P2P', 'Registry', 'Trash', and 'Windows Logs'. The 'File System' option is further expanded to show file systems like 'BTRFS', 'FAT', 'NTFS', 'XFS', and 'dmde'. At the bottom left, there are icons for 'Mouse keys switch', 'Onboard', and 'OSINT Switcher'.

- TSURUGI
- Accessories
- Internet
- Programming
- Office
- Graphics
- Other
- Sound & Video
- System Tools
- Universal Access
- Mouse keys switch
- Onboard
- OSINT Switcher

- Imaging
- Hashing
- Mount
- Timeline
- Artifacts Analysis
 - Apple/Mac
 - Boot Code
 - Browser
 - Email
 - Files
 - File System
 - BTRFS
 - FAT
 - NTFS
 - XFS
 - dmde
 - Google Takeout
 - Jump List
 - Metadata
 - Office Documents
 - P2P
 - Registry
 - Trash
 - Windows Logs
- Data Recovery
- Memory Forensics
- Malware Analysis
- Password Recovery
- Network Analysis
- Picture Analysis
- Mobile Forensics
- OSINT
- Cloud Analysis
- Virtual Forensics
- Crypto Currency
- Other Tools
- Reporting

Malware analysis



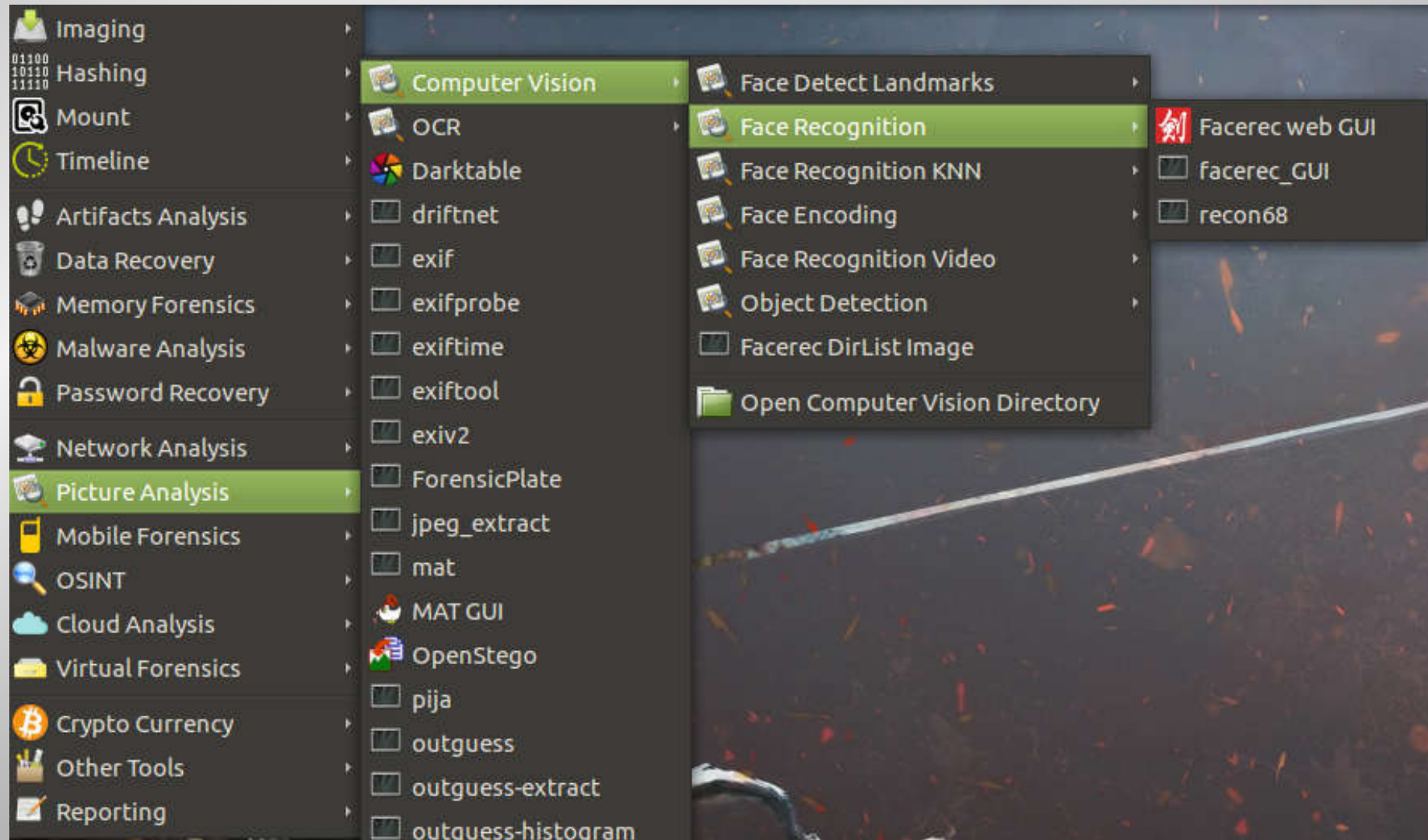
The screenshot shows a Windows Start menu with a custom layout. The left column contains standard Windows categories: TSURUGI (with a red sword icon), Accessories, Internet, Programming, Office, Graphics, Other, Sound & Video, System Tools, and Universal Access. Below these are utility icons: a mouse icon labeled 'Mouse keys switch', a keyboard icon labeled 'Onboard', and a magnifying glass icon labeled 'OSINT Switcher'. The right column contains a list of analysis categories, each with a biohazard icon: Imaging, Hashing, Mount, Timeline, Artifacts Analysis, Data Recovery, Memory Forensics, Malware Analysis (highlighted), Password Recovery, Network Analysis, Picture Analysis, Mobile Forensics, OSINT, Cloud Analysis, Virtual Forensics, Crypto Currency, Other Tools, and Reporting. The 'Malware Analysis' category is expanded, showing a sub-menu with the following items: Binary (highlighted), Debugger, Decoder, Flash, Java, JavaScript, Memory, Office, PDF, Sandbox, Scanner, XOR, Other Tools, colorize, and filecompare. The background of the Start menu is a dark, abstract image with red and orange particles.

Network analysis

A screenshot of a forensic tool's main menu. The 'Network Analysis' category is highlighted in green. The 'Logs' sub-menu is also highlighted in green and expanded to show various log analysis tools. The background of the application is a dark, abstract image with a sword and a hand holding a knife.

- Imaging
- Hashing
- Mount
- Timeline
- Artifacts Analysis
- Data Recovery
- Memory Forensics
- Malware Analysis
- Password Recovery
- Network Analysis**
 - Picture Analysis
 - Mobile Forensics
 - OSINT
 - Cloud Analysis
 - Virtual Forensics
 - Crypto Currency
 - Other Tools
 - Reporting
- Logs
 - CSV
 - BooLet
 - bro
 - bro-cut
 - ccze
 - glogg
 - grepcidr
 - Inav
 - log
 - multitail
 - Elastic Search
 - Logstash
 - Kibana
- Pcap
- Wireless
 - arp-scan
 - dnstwist
 - findserver
 - hping3
 - ipcalc
 - iptraf
 - lft
 - Maltrail Sensor
 - Maltrail Server
 - masscan
 - netsec
 - nmap
 - passiveDNS
 - scapy
 - ssldump
 - tcptraceroute
 - torify
 - traceroute
 - whois
 - Zenmap
 - Zenmap (as root)

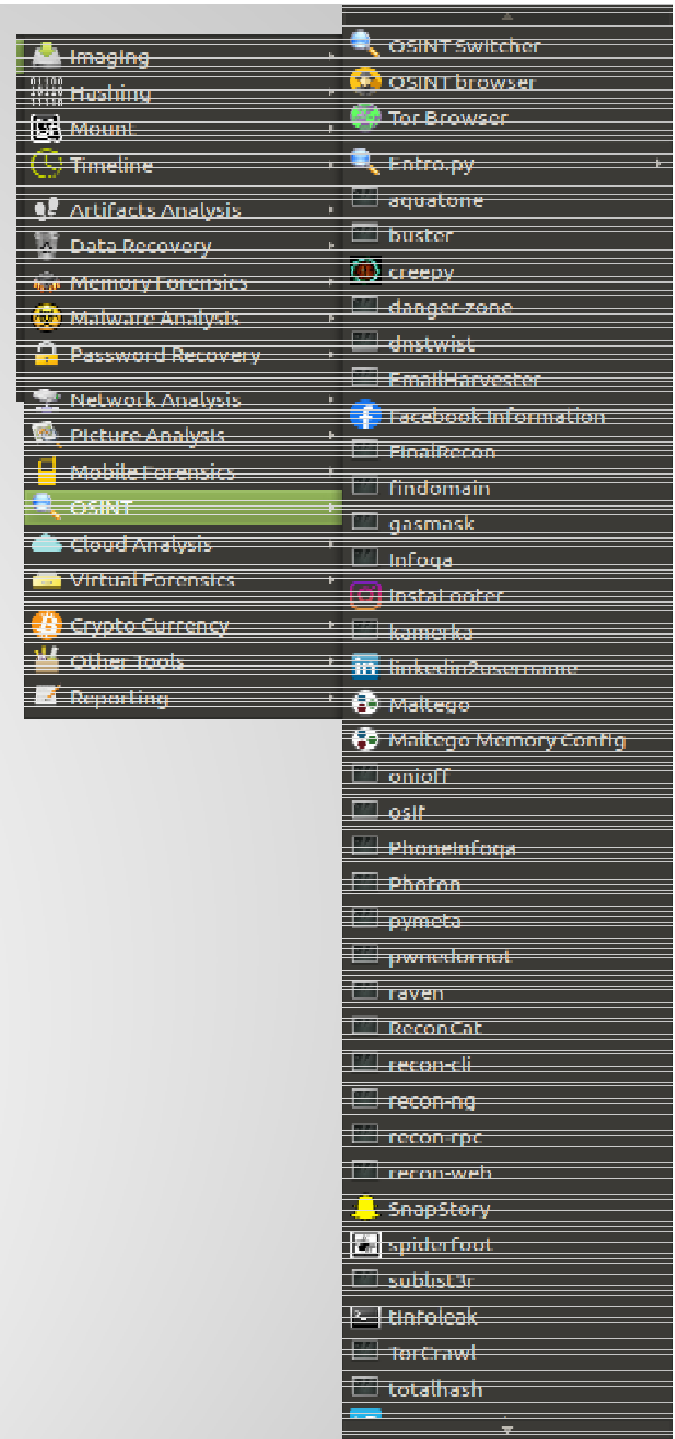
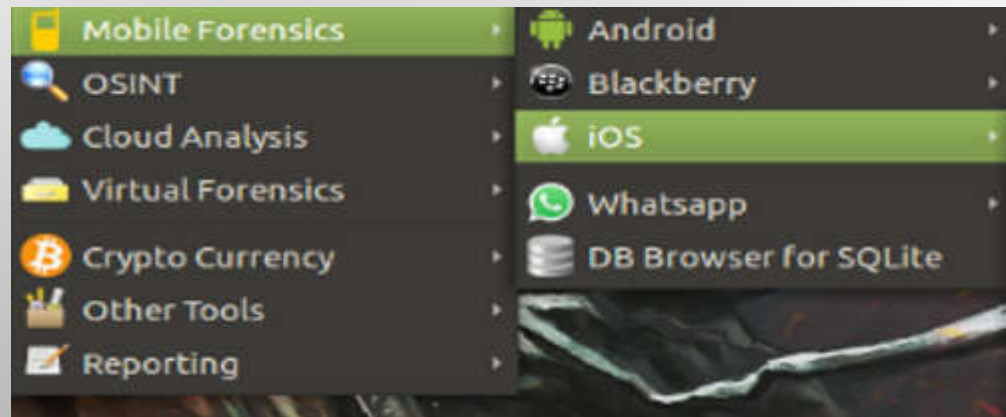
Computer vision



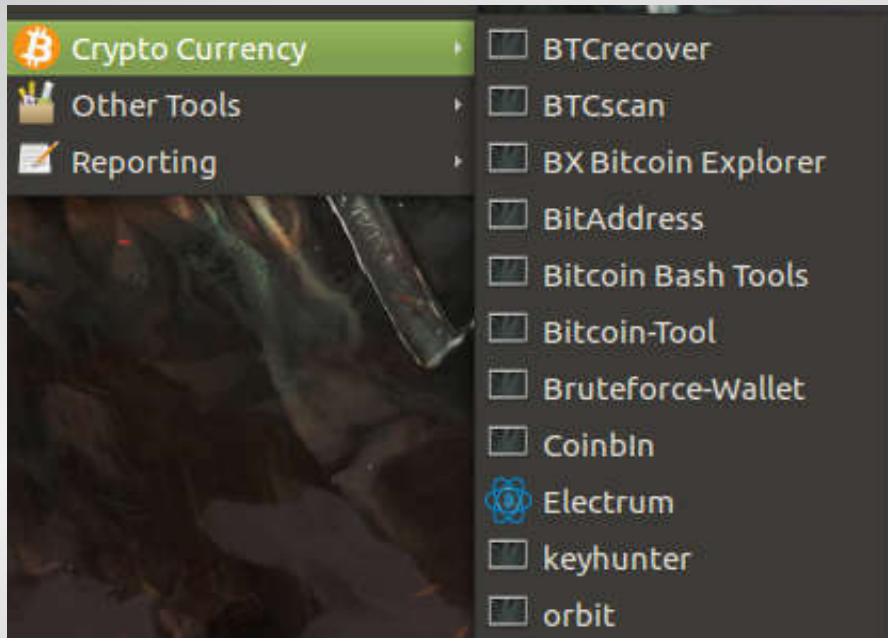


OSINT

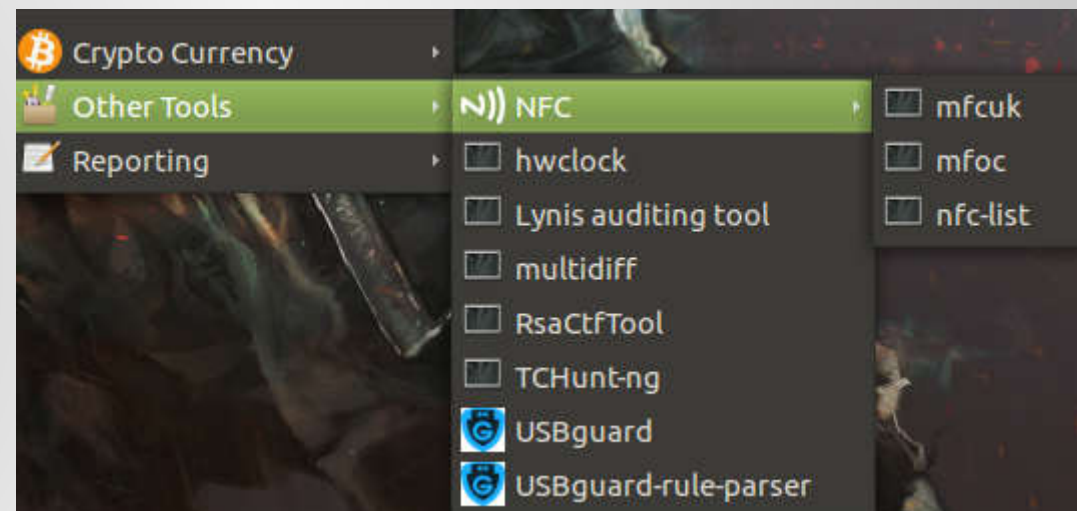
Mobile forensics



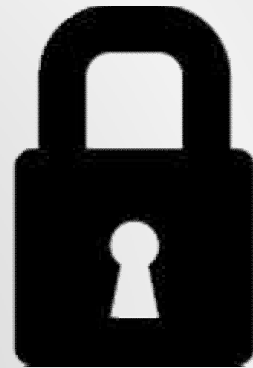
Crypto currency



Other tools



KERNEL WRITE BLOCKER



KERNEL WRITE BLOCKER

All connected devices by default are in

READ ONLY mode

tsurugi-linux.org

KERNEL WRITE BLOCKER

WHY A DEVICE WRITE BLOCKER
AT KERNEL LEVEL?

tsurugi-linux.org

The /mnt DIRECTORY



```
/mnt
----
aff1
aff2
aff3
aff4
aff5
bitlocker1
bitlocker2
bitlocker3
bitlocker4
bitlocker5
c
cifs
d
e
ewf1
ewf2
ewf3
ewf4
ewf5
f
g
h
pxe
raw1
raw2
raw3
raw4
raw5
shadow1
shadow2
shadow3
shadow4
shadow5
sshfs
t2t
virtual1
virtual2
virtual3
virtual4
virtual5
```

OSINT PROFILE SWITCHER



- tsurugi's Home
- TSURUGI device unlocker
- Displays
- Trash
- Keyboard
- Mouse keys switch
- Onboard
- OSINT Switcher



SYSTEM

Kernel: 5.1.15-050115-tsurugi
Uptime: 0h 1m 7s

CPU1: 99%
CPU2: 01%

RAM: 96%
F: 3.48GiB U: 374MiB

SWAP: 0%
F: 975MiB U: 0B

Processes	CPU	RAM
freshclam	98.00	0.47
dbus-daemon	1.00	0.13
NetworkManager	4.00	0.43
polkitd	1.00	0.20
conky	1.00	0.04
systemd	0.50	0.10
systemd-journal	0.03	0.09
Xorg	0.03	1.50
mate-multiloader	0.00	0.01
sleep	0.00	0.00

DATE

01:04
30 août 2019

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: 85%
F: 135GiB U: 13.6GiB

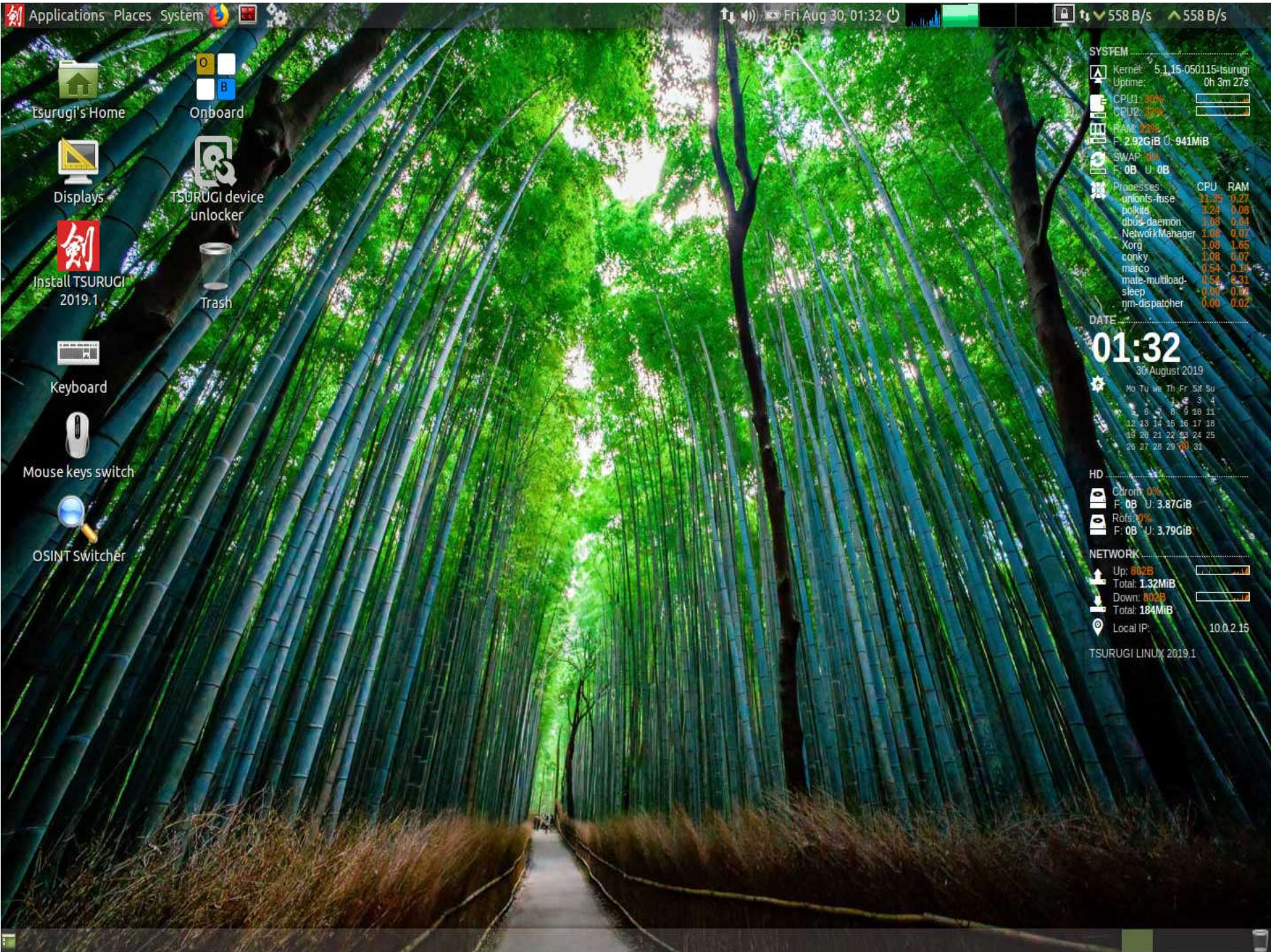
NETWORK

Up: 64B
Total: 703KiB

Down: 170B
Total: 31.7MiB

Local IP: 10.0.2.15

TSURUGI LINUX 2019.1



SYSTEM

Kernel: 5.1.15-050115-tsurugi
 Uptime: 0h 3m 27s

CPU1: 30%
 CPU2: 32%

RAM: 28%
 F: 2.92GiB U: 941MiB

SWAP: 0%
 F: 0B U: 0B

Processes:	CPU	RAM
unions-fuse	11.35	0.27
polkitd	3.24	0.08
dbus-daemon	1.08	0.04
NetworkManager	1.08	0.07
Xorg	1.08	1.65
conky	1.08	0.07
mateo	0.54	0.14
mate-multload	0.54	8.31
sleep	-0.00	0.06
nm-dispatcher	0.00	0.02

DATE

01:32
 30 August 2019

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

Citrom: 0%
 F: 0B U: 3.87GiB

Rols: 0%
 F: 0B U: 3.79GiB

NETWORK

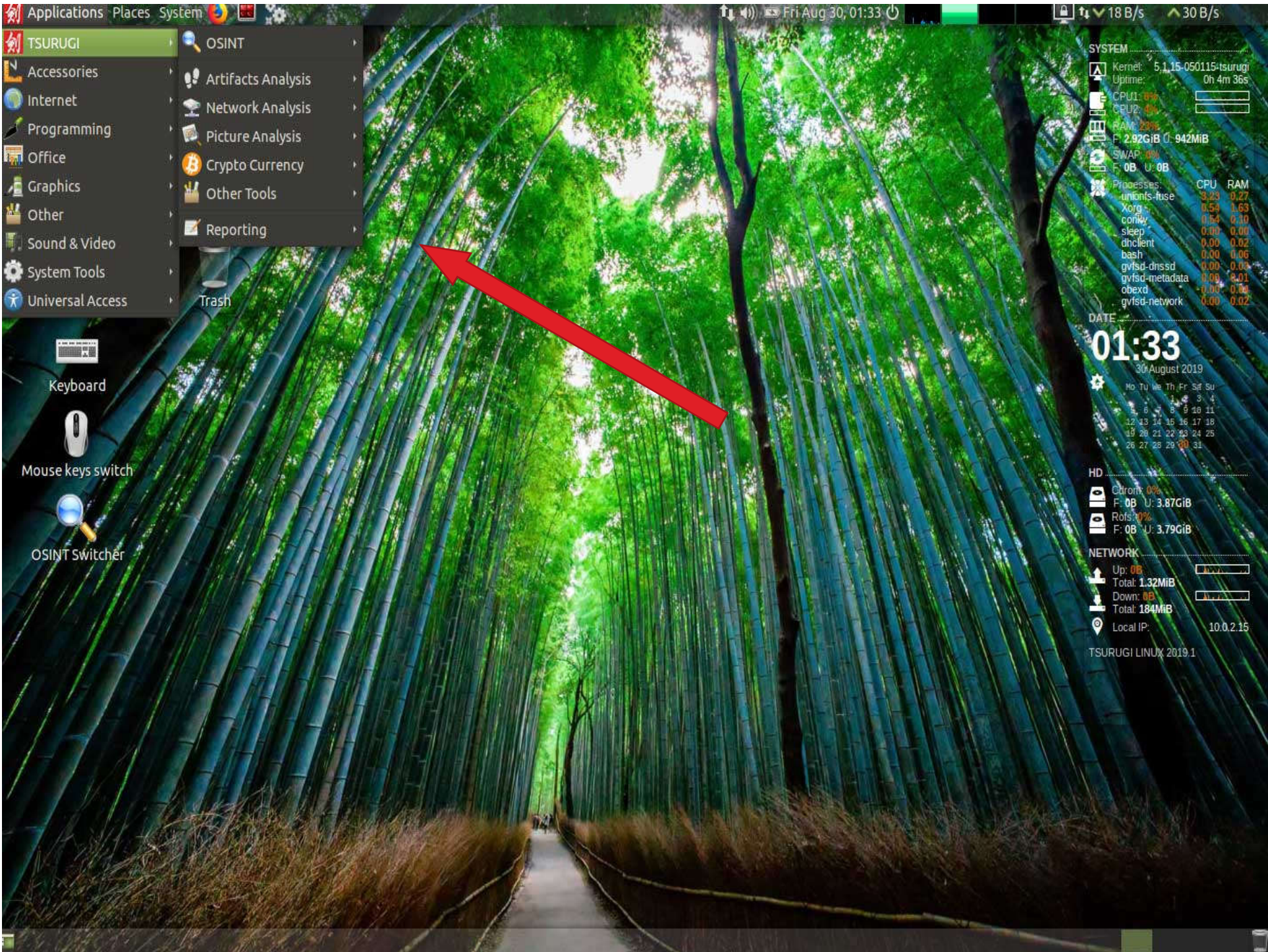
Up: 802B
 Total: 1.32MiB

Down: 802B
 Total: 184MiB

Local IP: 10.0.2.15

TSURUGI LINUX 2019.1

- Tsurugi's Home
- Onboard
- Displays
- TSURUGI device unlocker
- Trash
- Keyboard
- Mouse keys switch
- OSINT Switcher
- Install TSURUGI 2019.1



WE CARE ABOUT DETAILS...



TSURUGI LINUX [LAB]

- Device automount/autoexec disabled
- System hibernation disabled
- After each session starts the defaults custom values are set
- Automatic set HI-DPI
- Mouse keys switch
- Boot cleaner script
- RAM saturation workaround

194

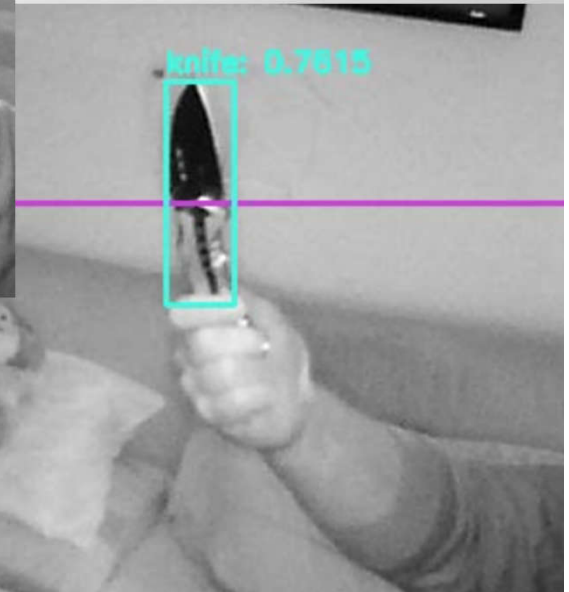
81+87+26

builds

tsurugi-linux.org

COMPUTER VISION

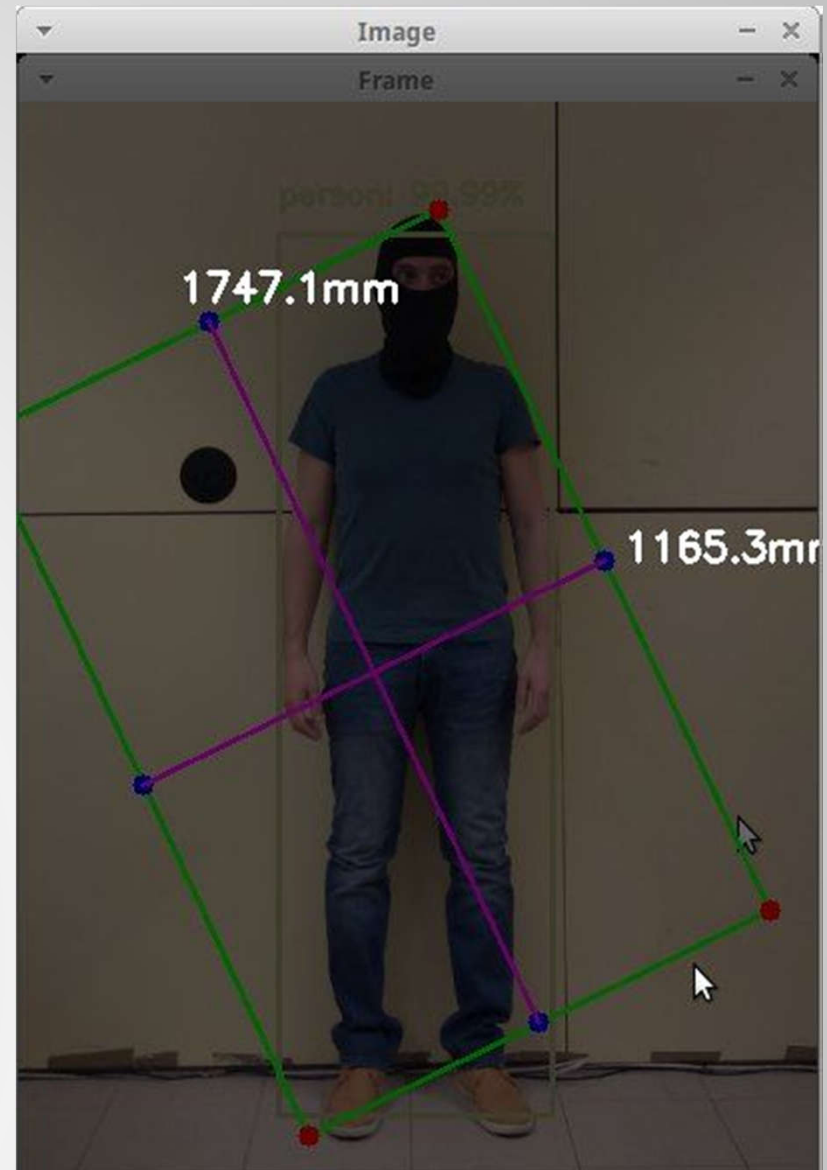
COMPUTER VISION object detection



CoRI&IN
2020

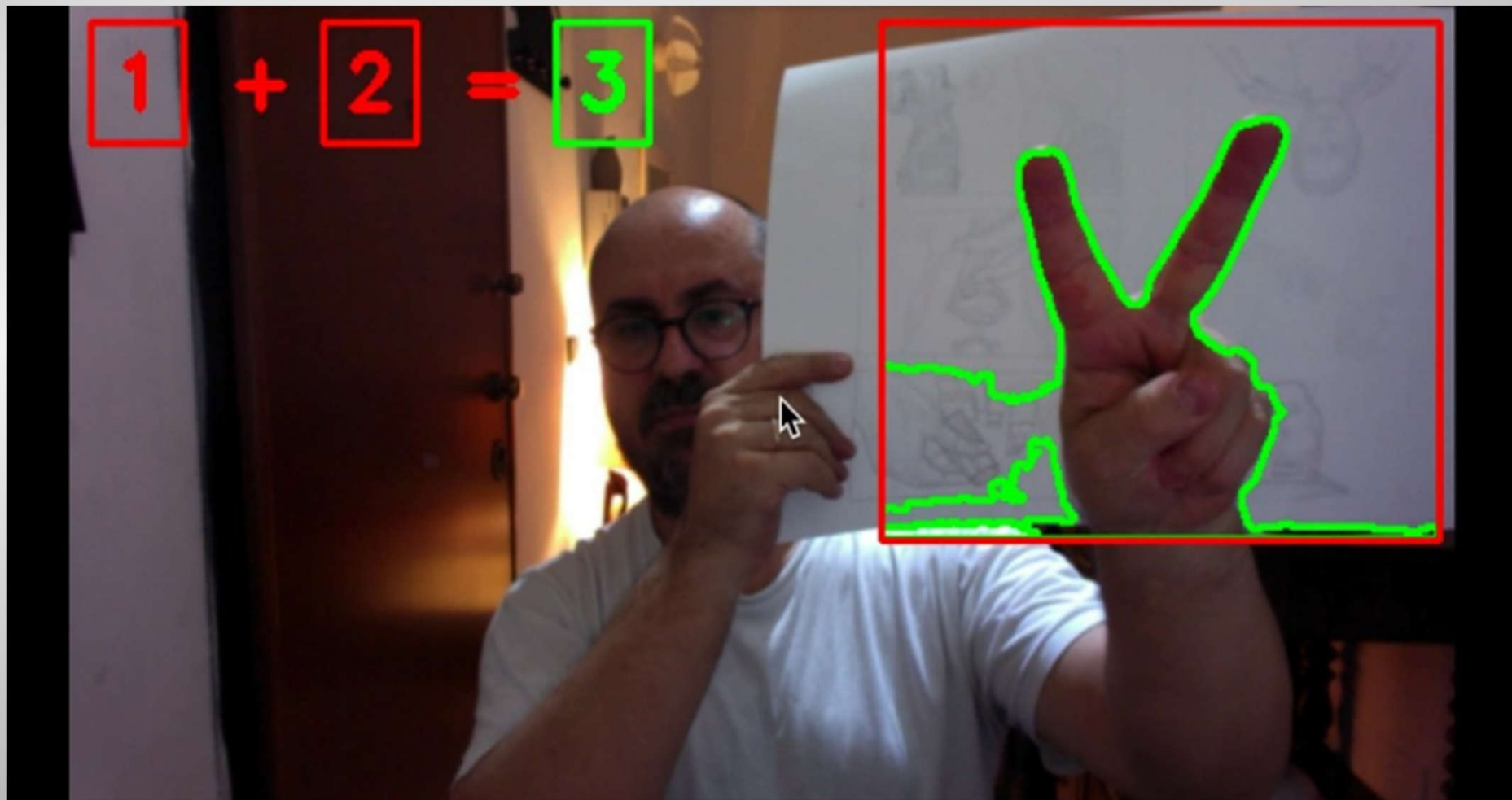
tsurugi-linux.org

COMPUTER VISION calculating sizes



tsurugi-linux.org

COMPUTER VISION: gesture detection



tsurugi-linux.org

BENTO TOOLKIT



Bento

your forensic launcher box

v2019.02

TSURUGI

the sharpest weapon in your DFIR arsenal

www.tsurugi-linux.org



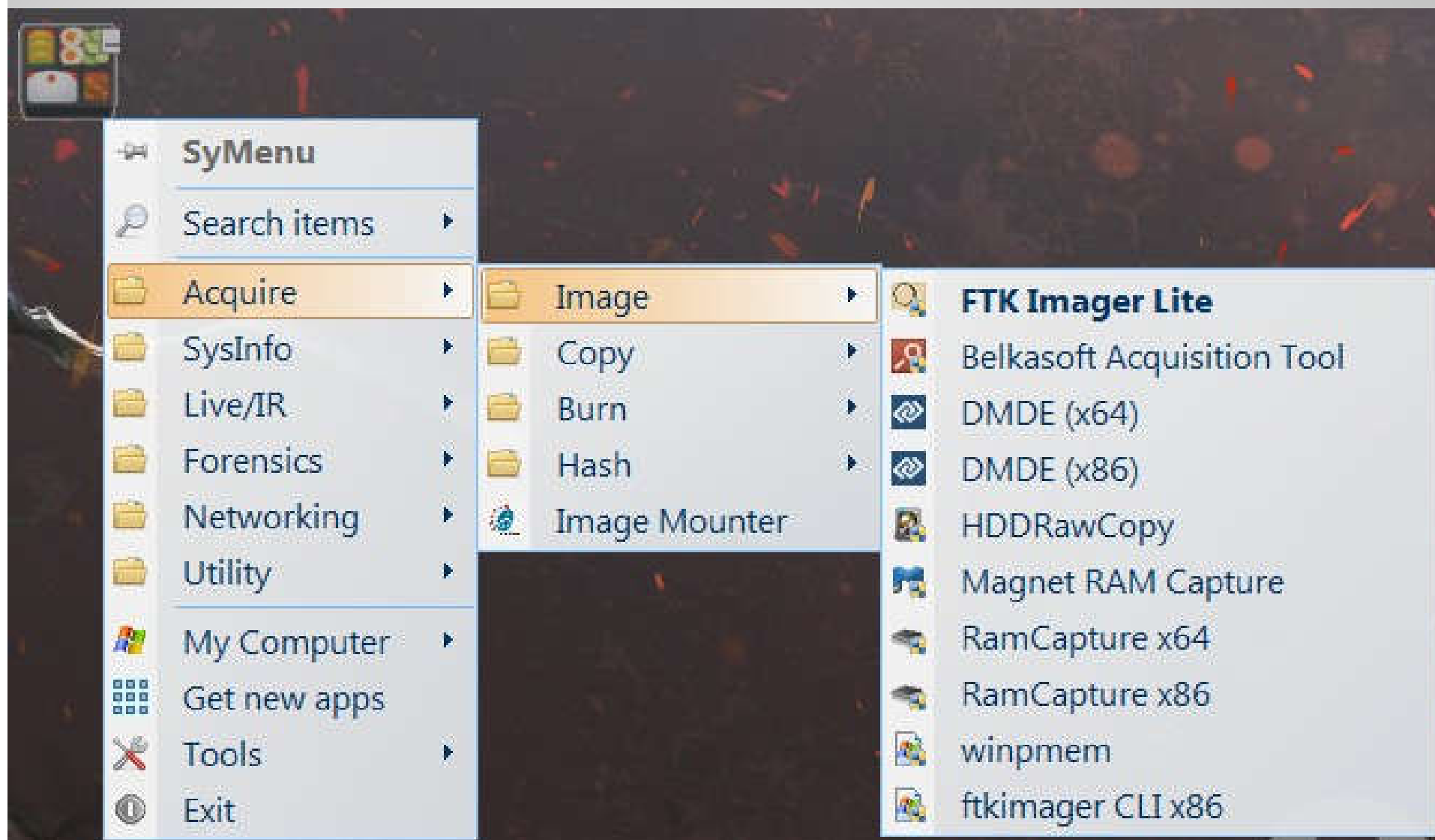
tsurugi-linux.org



BENTO

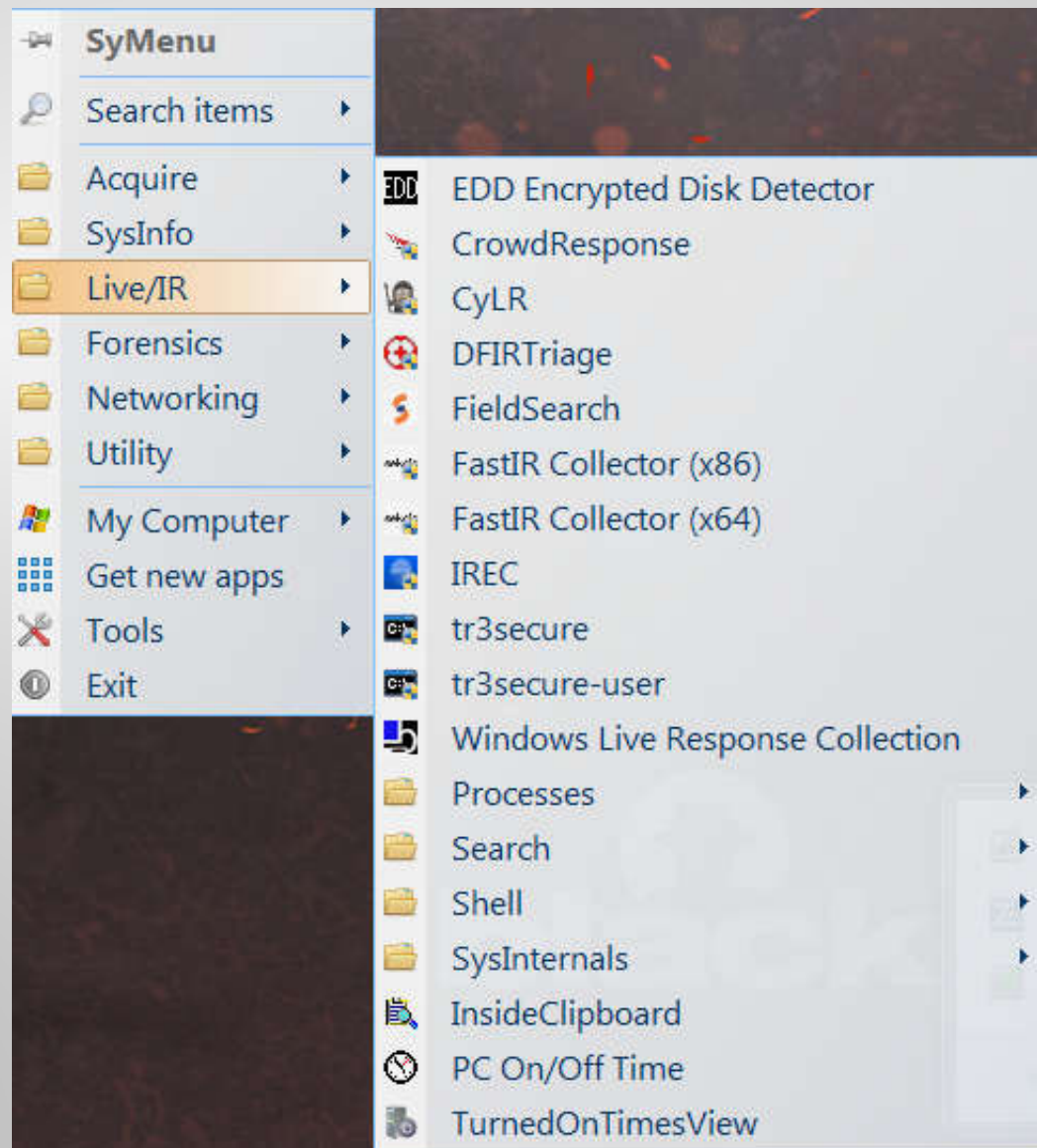
- Live forensics analysis toolkit
- About 300 tools
(Windows, Linux, macOS)

BENTO TOOLKIT



tsurugi-linux.org

BENTO TOOLKIT



tsurugi-linux.org

BENTO UPDATE MANAGER

SyMenu Suite | NirSoft Suite | Sysinternals Suite | BentoSuite

Name	Category	Released on	Version	Size	Status
AdapterWatch	Internet	2009/05/18	1.05	37 Kb	Added
AdvancedRun	Utilities	2018/09/11	1.06	59 Kb	Added
AdvancedRun x64	Utilities	2018/09/11	1.06	71 Kb	Added
AllThreadsView	Utilities	2018/04/01	1.00	53 Kb	Added
AllThreadsView x64	Utilities	2018/04/01	1.00	63 Kb	Added
AlternateStreamView	Utilities	2018/09/29	1.54 ⇒ 1.55	52 Kb	Update
AlternateStreamView x64	Utilities	2018/09/29	1.54 ⇒ 1.55	67 Kb	Update
AltStreamDump	Utilities	2012/02/19	1.05	10 Kb	Added
AppNetworkCounter	Internet	2018/10/11	1.05 ⇒ 1.06	58 Kb	Update
AppNetworkCounter x64	Internet	2018/10/11	1.05 ⇒ 1.06	68 Kb	Update
AppReadWriteCounter	Utilities	2018/07/18	1.05	58 Kb	Added
AppReadWriteCounter x64	Utilities	2018/07/18	1.05	68 Kb	Added
BatteryInfoView	Utilities	2017/08/11	1.23	115 Kb	Added
BluetoothCL	Internet	2014/02/16	1.07	13 Kb	Added
BluetoothLogView	Internet	2016/10/20	1.12	269 Kb	Added
BluetoothView	Internet	2013/02/17	1.66	52 Kb	Added
BrowsingHistoryView	Internet	2018/07/16	2.17	248 Kb	Added
BrowsingHistoryView x64	Internet	2018/07/16	2.17	295 Kb	Added
BulletsPassView	Utilities	2015/03/01	1.32	59 Kb	Added
BulletsPassView x64	Utilities	2015/03/01	1.32	69 Kb	Added
ChromeCacheView	Internet	2018/09/25	1.80 ⇒ 1.85	71 Kb	Update
ChromeCookiesView	Internet	2018/05/08	1.47	180 Kb	Added
ChromeHistoryView	Internet	2018/03/20	1.35	181 Kb	Added
ChromePass	Utilities	2018/01/27	1.46	153 Kb	Added
CredentialsFileView	Utilities	2017/10/29	1.07	74 Kb	Added



Search by

- Name
- Category
- Description
- Publisher

Text to search

CTRL + S

Status

- All
- Available
- Update
- New
- Added

Search



Apply all

Exit

Free space on F: 17.4/1001.7GB

BENTO PACKAGE MANAGER

SyMenu Suite | NirSoft Suite | Sysinternals Suite | **BentoSuite**

Name	Category	Released on	Version	Size	Status
CrowdInspect	Security - Forensi...	2017/02/14	1.5	530 Kb	Available
CrowdResponse	Security - Forensi...				
CyLR	Security - Forensi...				
DFIRTriage	Security - Forensi...				
DMDE (x64)	Security - Forensi...				
DMDE (x86)	Security - Forensi...				
FastIR Collector (x64)	Security - Forensi...				
FastIR Collector (x86)	Security - Forensi...				
glogg	Text - Viewers				
HDD Raw Copy	Security - Forensi...				
IREC Free	Security - Forensi...				
KAPE	Security - Forensi...				
LaZagne	Security - Forensi...				

KAPE 0.8.1.0

KAPE is an efficient and highly configurable triage program that will target essentially any device or storage location, find forensically useful artifacts, and parse them within a few minutes.

[App publisher](#) [Contact reviewer](#)

Add hashtags
Kroll
Rebus

License: <https://learn.duffandphelps.com/kape-license-agreement>

Free space on F: 19.0/1001.7GB

Start process...

FastIR Collector (x64) 1.1 *Installation completed*

KAPE 0.8.1.0

Downloading from the web site: s3.amazonaws.com

016123/115157Kb

Stop

Update
New
Added

Search

Apply all

Exit

BENTO TOOLKIT

SyMenu [D:] - v.6.05.6775

File Item Manager Advanced Help

- Acquire
- SysInfo
- Live/IR
 - EDD Encrypted Disk Detector
 - CrowdResponse
 - CyLR
 - DFIR Triage
 - FieldSearch
 - FastIR Collector (x86)
 - FastIR Collector (x64)
 - IREC
 - tr3secure
 - tr3secure-user
 - Windows Live Response Collector
- Processes
- Search
- Shell
- SysInternals
- InsideClipboard
- PC On/Off Time
- TurnedOnTimesView
- Forensics
- Networking
- Utility

Program 0 Executions

CrowdResponse

Path
.\ProgramFiles\SPSSuite\SyMenuSuite\CrowdResponse_sps\CrowdRespon...

Icon Path
.\Icons\CrowdResponse.exe.ico

Description
Crowd Response is a lightweight Windows console application designed to

Shortcut ⓘ

Url [Visit web site](https://www.crowdstrike.com/resources/community-tools/crowdresponse)
https://www.crowdstrike.com/resources/community-tools/crowdresponse

Additional Params | Gesture | Advanced

Program arguments (if necessary surround with double quotes)
-i %ad%config.txt -v -e -o ..\..\..\..\..\Report\%computername%\CrowdRe:

Version
1.0.6

Start Search (CTRL + S)

- Autoexec on start ⓘ
- Autoexec on close ⓘ
- Extension Manager ⓘ
- Run elevated 🌐
- Output Command ⓘ
- Single Instance Only ⓘ
- Suppress notification
- Desktop shortcut ⓘ

Reset

Save

Save & Exit

Free space on D: 5.6/7.2GB

TSURUGI ACQUIRE

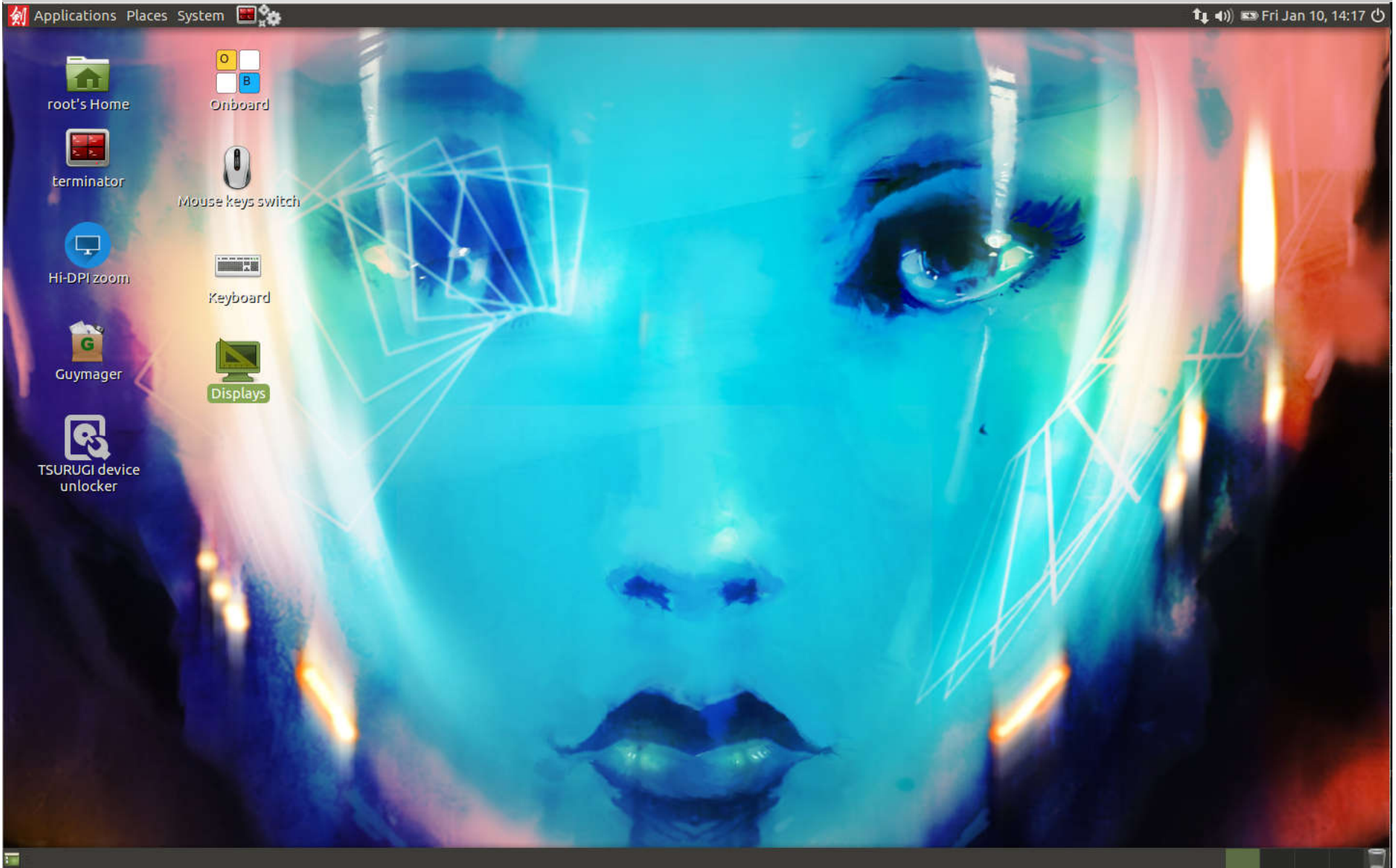
tsurugi-linux.org



TSURUGI ACQUIRE

- 32 bits Linux distribution
- Live minimal version
- Only for “disk acquisition”
- KERNEL WRITE BLOCKER

TSURUGI ACQUIRE



tsurugi-linux.org

TSURUGI ACQUIRE



tsurugi-linux.org

NEXT STEPS & OUR ROADMAP

- System upgrade to new 20 LTS version [Q3 2020]
- New Amazing feature! (Use Tsurugi Linux and try to find the hint...) [Q3 2020]
- New Tsurugi Acquire based on Debian
- Create free basic DFIR trainings [Q4 2020]
- Don't forget to sleep... ☺ [Q4 2021]

tsurugi-linux.org

OUR GOALS?

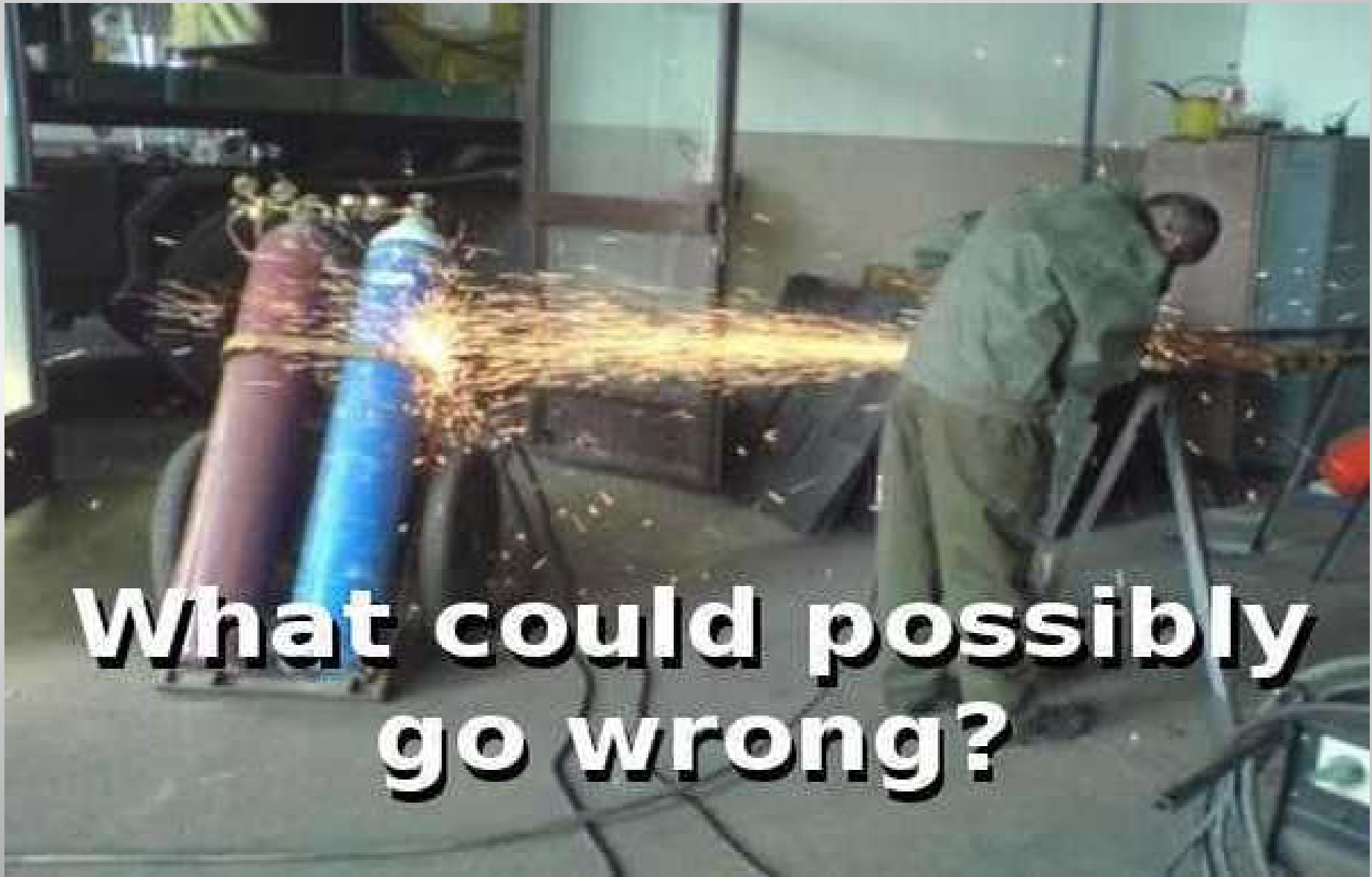
SHARE KNOWLEDGE

&

GIVE BACK TO THE COMMUNITY

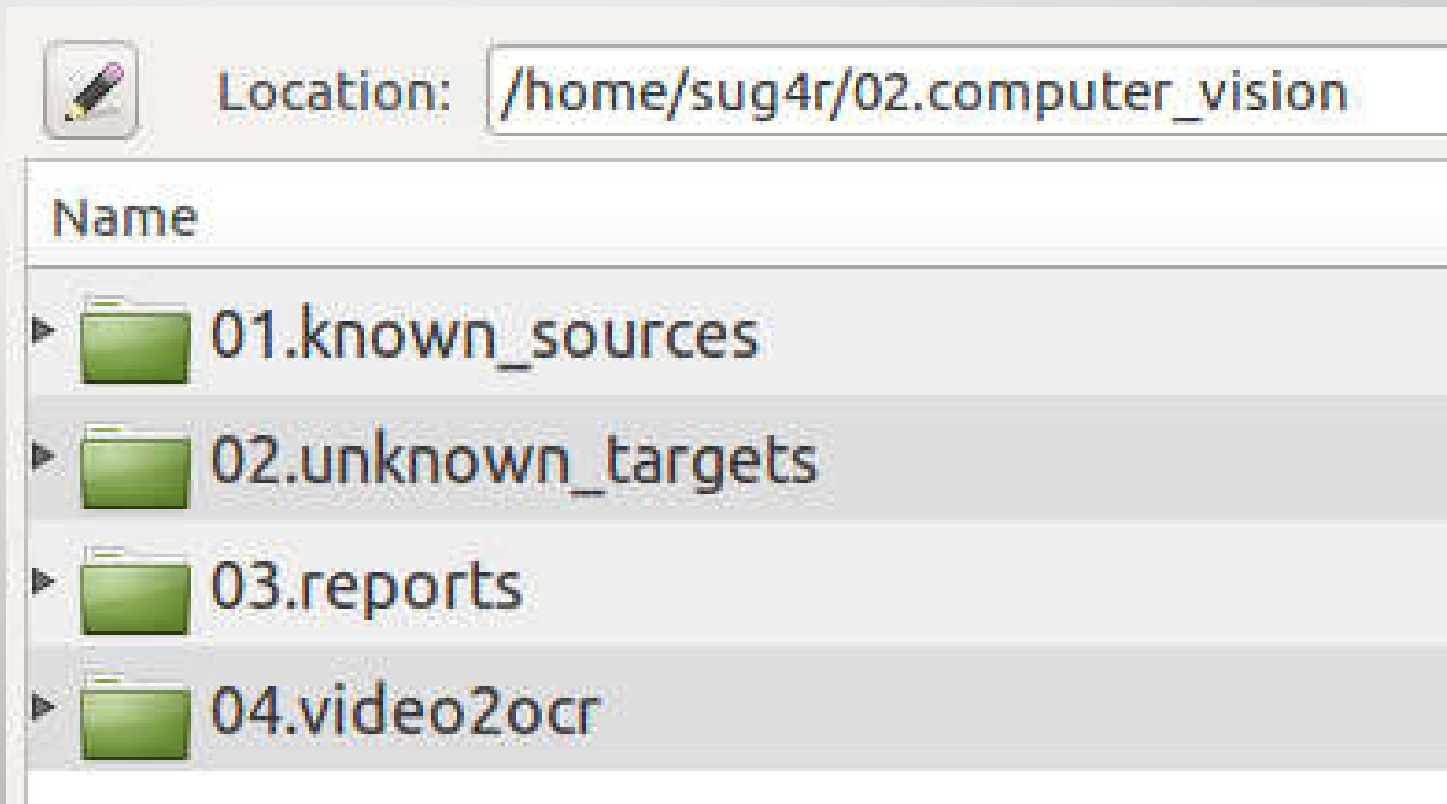
`tsurugi-linux.org`

DEMO TIME!



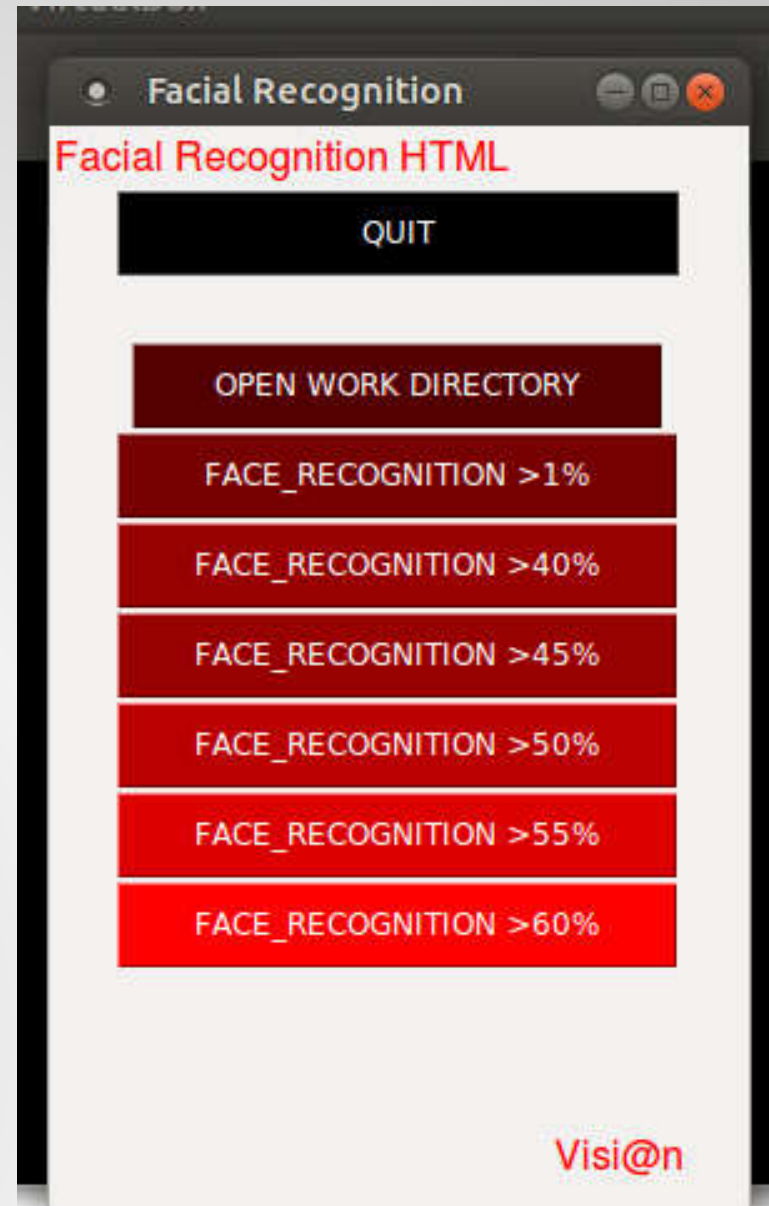
What could possibly go wrong?

COMPUTER VISION



COMPUTER VISION

facerec_WEB_GUI



tsurugi-linux.org

0Antonio_Broi.jpg	visi@n.jpg		
 <p>916698514</p>	 <p>Michelle.jpg</p>	54.6642 %	<p>This facial recognition system is based on the Python library face_recognition and the results percentages must be interpreted in this way:</p> <ul style="list-style-type: none">< 40% Insufficient> 40% Minimum> 50% Optimal> 60% Maximum

FACE LANDMARKS



A problem has been detected and windows has been shut down to prevent damage to your computer.

If this is the first time you've seen this stop error screen, restart your computer. If this error appears again, follow these steps:

Questions?

Check to be sure you have adequate disk space. If a driver is identified in the Stop message, disable the driver or check with the manufacturer for driver updates. Try changing video adapters.

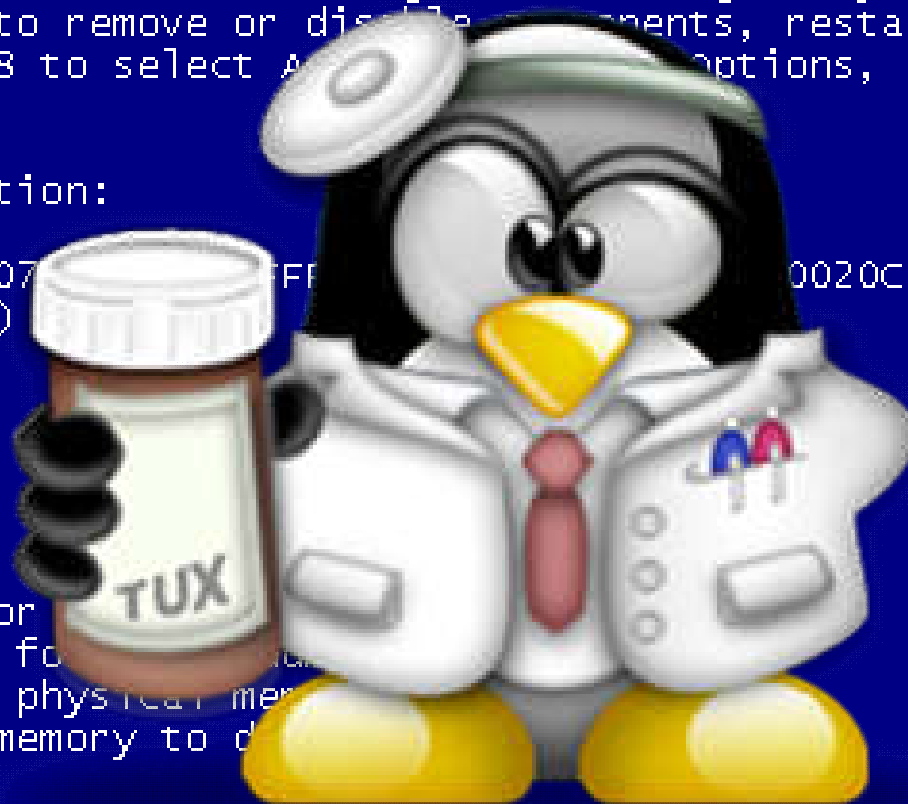
Check with your hardware vendor for any BIOS updates. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced options, and then select Safe Mode.

Technical information:

```
*** STOP: 0x0000007E (0x00000000, 0x00000000, 0x0020C592B, 0xFFFFF880032839F8, 0xFFFFF88003283250)
```

```
***   srv2.sys (ffff8020a1000, DateStamp 494319e9)
```

```
Collecting data for debugging...
Initializing disk for crash dump...
Beginning dump of physical memory...
Dumping physical memory to d:\crash.dmp
```



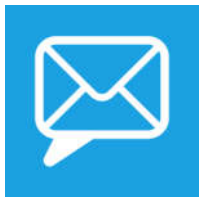
THANK YOU



@tsurugi_linux
@Sug4r7



www.linkedin.com/in/giovannirattaro



info [at] tsurugi-linux [dot] org

tsurugi-linux.org