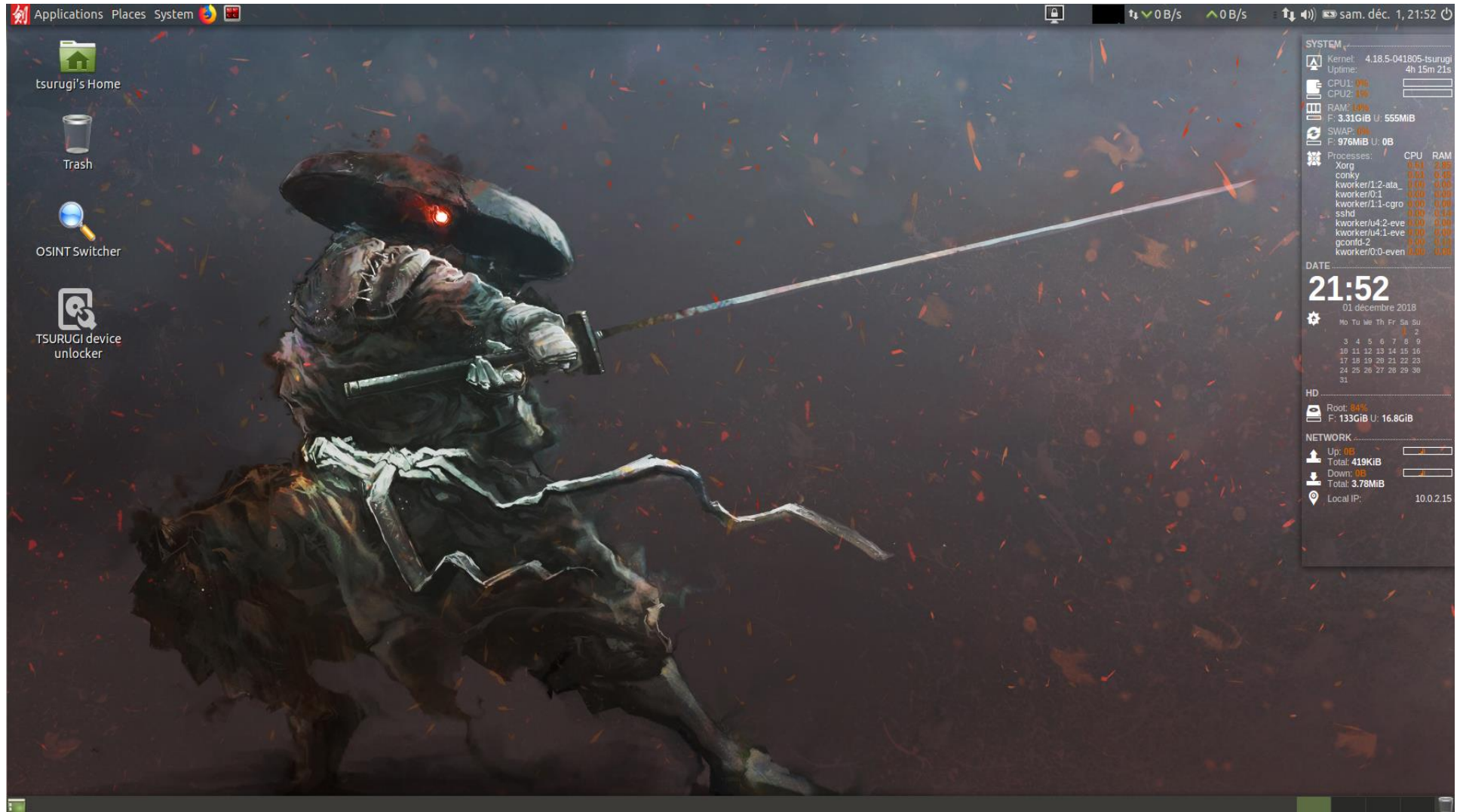


Digital forensics con Tsurugi



Internet, 30 maggio 2020

Tsurugi Team

▶ **Giovanni 'sug4r' Rattaro**

Tsurugi Linux and Tsurugi Acquire core developer
Tsurugi Linux team leader

▶ **Marco 'blackmoon' Giorgi**

Tsurugi Linux and Tsurugi Acquire core developer

▶ **Davide 'rebus' Gabrini**

Bento DFIR toolkit project leader

▶ **Francesco 'dfirfpi' Picasso**

Tsurugi Linux and Tsurugi Acquire developer

▶ **Massimiliano 'YattaMax' Dal Cero**

Tsurugi Linux and Tsurugi Acquire developer

▶ **Antonio 'Visi@n' Broi**

Digital Forensics, OSINT and Computer Vision specialist



Tsurugi Linux

▶ Progetto open source, online da marzo 2018, dedicato a **Digital Forensics** e **OSINT**

www.tsurugi-linux.org

▶ Tre componenti:

▶ **Tsurugi Acquire**

▶ Ricognizione e acquisizione *post mortem* delle fonti di prova

▶ **Tsurugi Lab**

▶ Analisi forense a tutto campo

▶ **Bento**

▶ Live Forensics e Incident Response
(sopralluogo, ispezione, perquisizione, accertamento,
rilievo e acquisizione *live* delle fonti di prova)



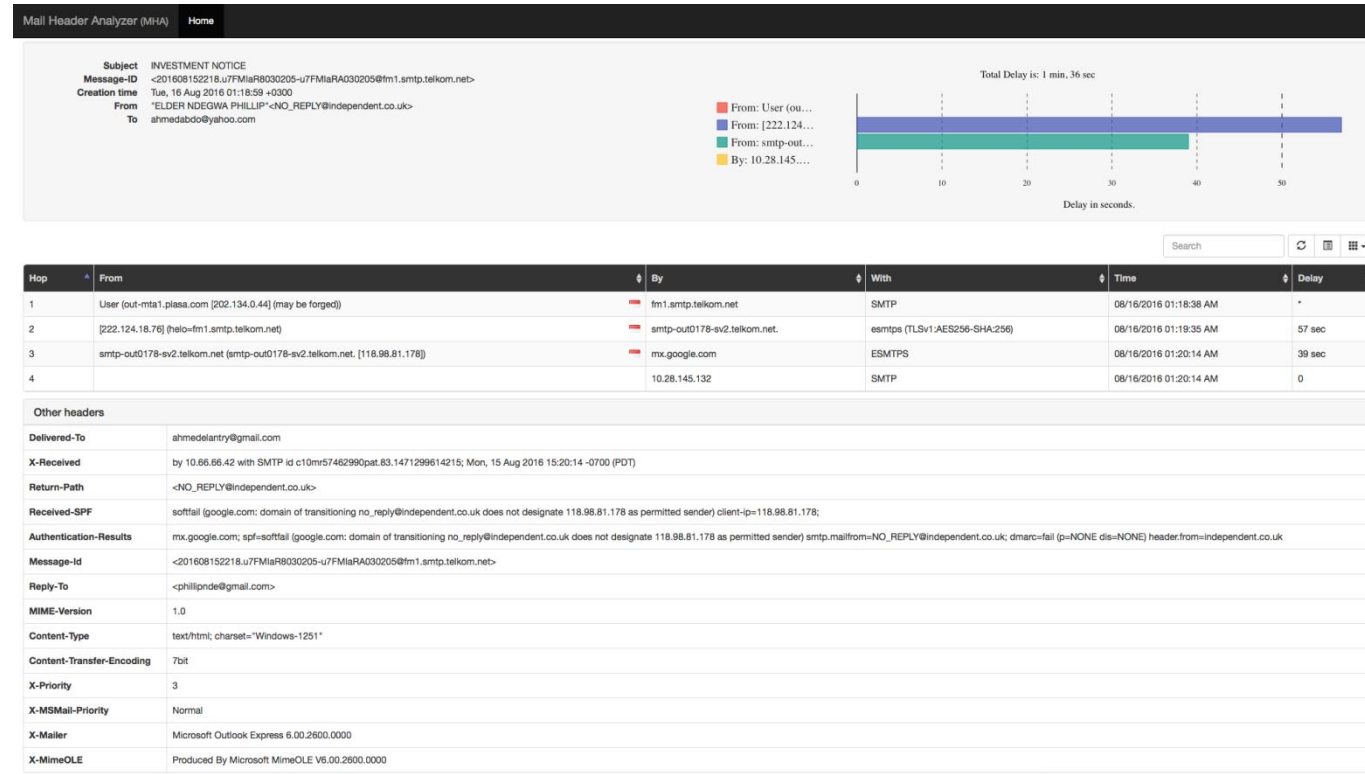
Caso simulato: stalking!

- ▶ La vittima riceve numerosi messaggi e-mail, da indirizzi sempre diversi e sempre sconosciuti, contenenti insulti e minacce di natura fisica.
- ▶ Non dà peso alla cosa, scegliendo di ignorare le e-mail e cancellarle, fino all'ultimo messaggio, in cui il suo stalker mostra di avere precisa conoscenza dei suoi recenti spostamenti e allega anche alcune foto scattate in luoghi pubblici che la ritraggono a sua insaputa.
- ▶ Spaventata dalla consapevolezza di essere pedinata, la vittima sporge querela, allegando soltanto quest'ultima e-mail.



Caso simulato: stalking!

► Usando Mail Header Analyzer da Tsurugi Linux, il consulente tecnico analizza la mail, individua l'IP del mittente e la Procura dispone perquisizione domiciliare



► Si tratta di un ex compagno di scuola con cui la vittima non ha più contatti da almeno 15 anni, e che nega con forza qualsiasi coinvolgimento nella vicenda.

► Nel corso della perquisizione domiciliare, i consulenti tecnici intervengono su un notebook acceso e collegato a Internet utilizzando il toolkit Bento...

LIVE FORENSICS INCIDENT RESPONSE



Live forensics

- ▶ La parte più delicata del *digital forensic process* è la prima interazione con dispositivi in funzione
- ▶ Chi interviene sulla scena ha un'occasione **irripetibile**
- ▶ Osservare gli eventi in corso
- ▶ Eseguire rilievi
- ▶ Monitorare l'evoluzione
- ▶ Catturare informazioni volatili
 - ▶ Contenuto RAM, traffico di rete ecc.
- ▶ Può insomma eseguire quegli accertamenti che vengono indicati come *live forensics*

Ha però anche l'occasione per commettere errori **irrimediabili**

- ▶ Perdita di dati rilevanti
- ▶ Inquinamento delle fonti di prova
- ▶ Alterazione delle timeline
- ▶ Mancata documentazione degli interventi
- ▶ Intralcio alle indagini successive



Live forensics best practices

- ▶ L'intervento dell'utente deve essere ridotto al minimo
- ▶ Ogni azione deve essere indispensabile e meno invasiva possibile
- ▶ Le modifiche ai dati memorizzati staticamente devono essere ridotte all'inevitabile
- ▶ Le acquisizioni hanno priorità secondo l'ordine di volatilità
- ▶ Ogni azione intrapresa deve essere scrupolosamente verbalizzata, con gli opportuni riferimenti temporali
- ▶ Gli strumenti utilizzati devono essere fidati, il più possibile indipendenti dal sistema e impiegare il minimo delle risorse; non devono produrre alterazioni né ai dati né ai metadati
- ▶ I dati estratti vanno sottoposti ad hash e duplicati prima di procedere all'analisi
- ▶ I dati che non sono volatili devono preferibilmente essere acquisiti secondo metodologia tradizionale

BENTO

your forensic launcher box





Cerca



Strumenti

[Contenuti recenti](#)

Bento

Your forensic launcher box

Bento è una suite di programmi utili agli scopi di *live forensics* e *incident response*.

È stato assemblato per fornire uno strumento di supporto ai sopralluoghisti della Polizia Scientifica per le attività di **sopralluogo informatico** e per dare agli altri *first responder* un toolkit in grado di aiutarli ad affrontare le più comuni attività di identificazione, rilievo, acquisizione, repertazione e preservazione di evidenze digitali da sistemi operativi Windows, Linux e Mac OSX in modalità *live*. Non è scopo di Bento fornire strumenti di analisi forense al di fuori degli accertamenti strettamente necessari in modalità *live* e delle finalità di *triage*.

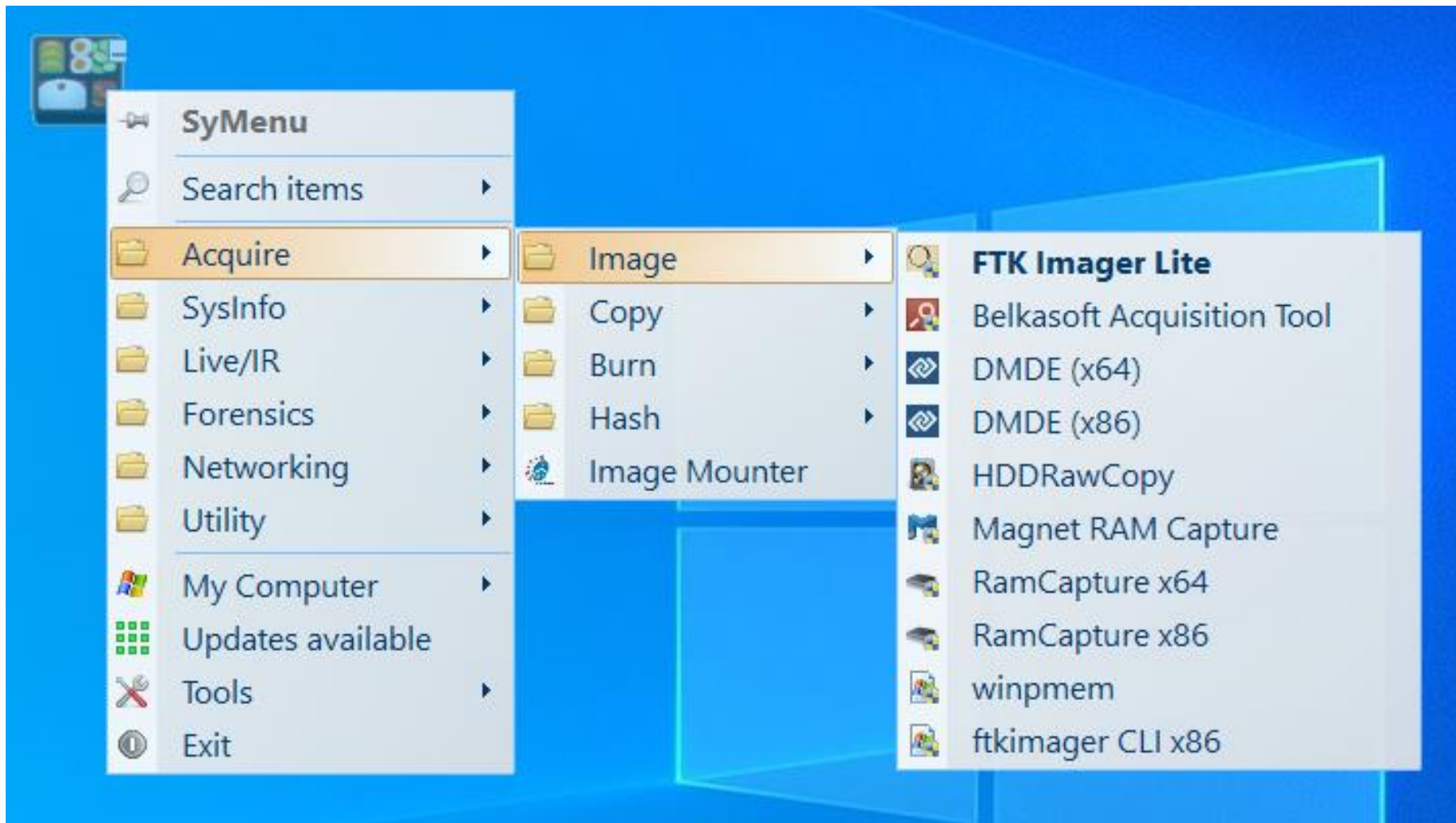


Linee guida di Bento

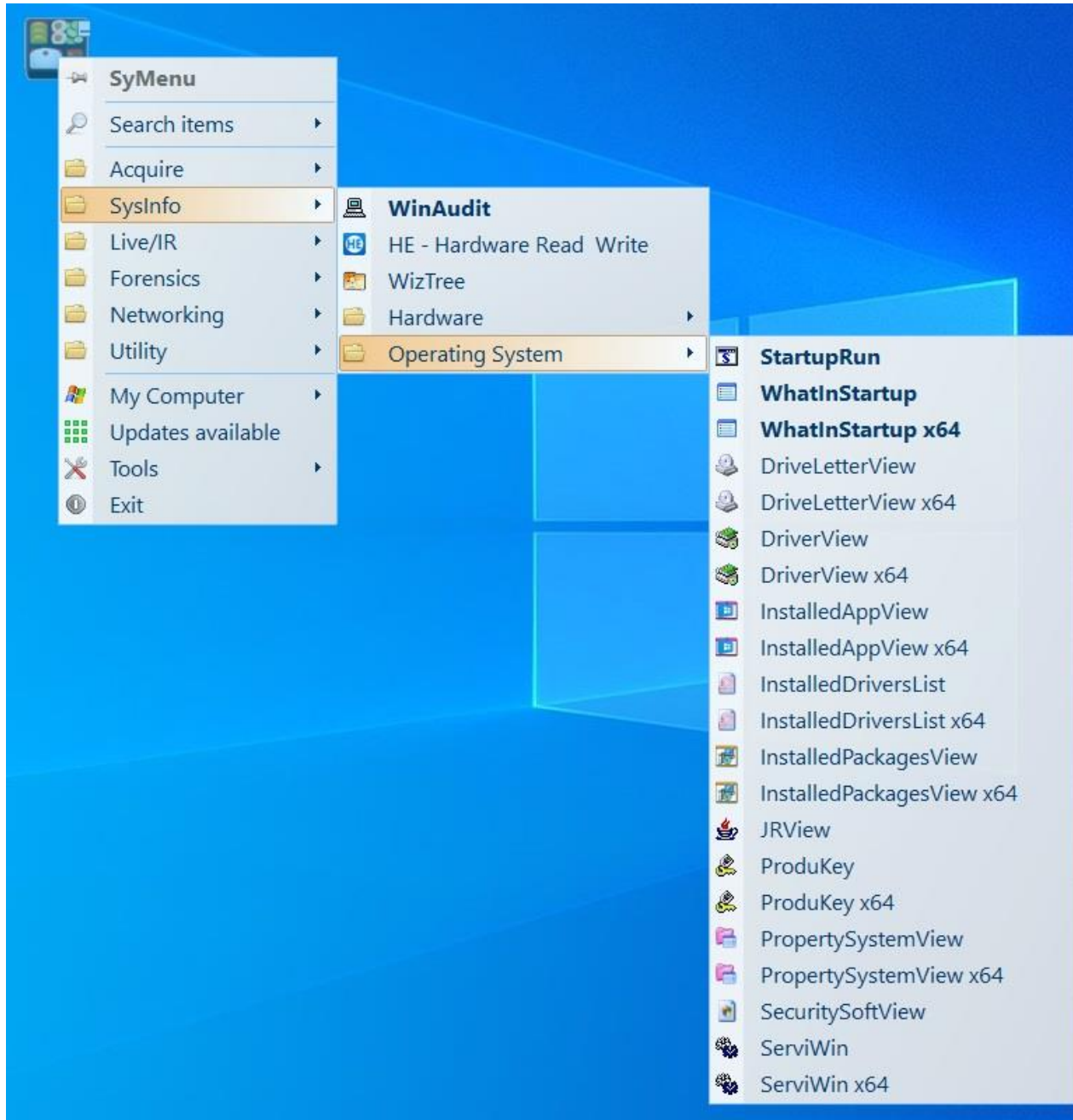


- ▶ Nasce per supportare i *first responder*
- ▶ Orientato al "sopralluogo" informatico
 - ▶ Selezione ristretta di strumenti di analisi
 - ▶ Ampia varietà di strumenti utili a eseguire ricognizione, rilievi, documentazione, accertamenti urgenti, acquisizioni.
- ▶ Esclusi tutti gli abandonware
- ▶ Supporto per l'aggiornamento guidato dei pacchetti
- ▶ Incoraggiamento all'automazione
 - ▶ Per rendere le operazioni semplici, rapide, efficienti, metodiche

Bento - Acquisizione



Bento – System Information Gathering



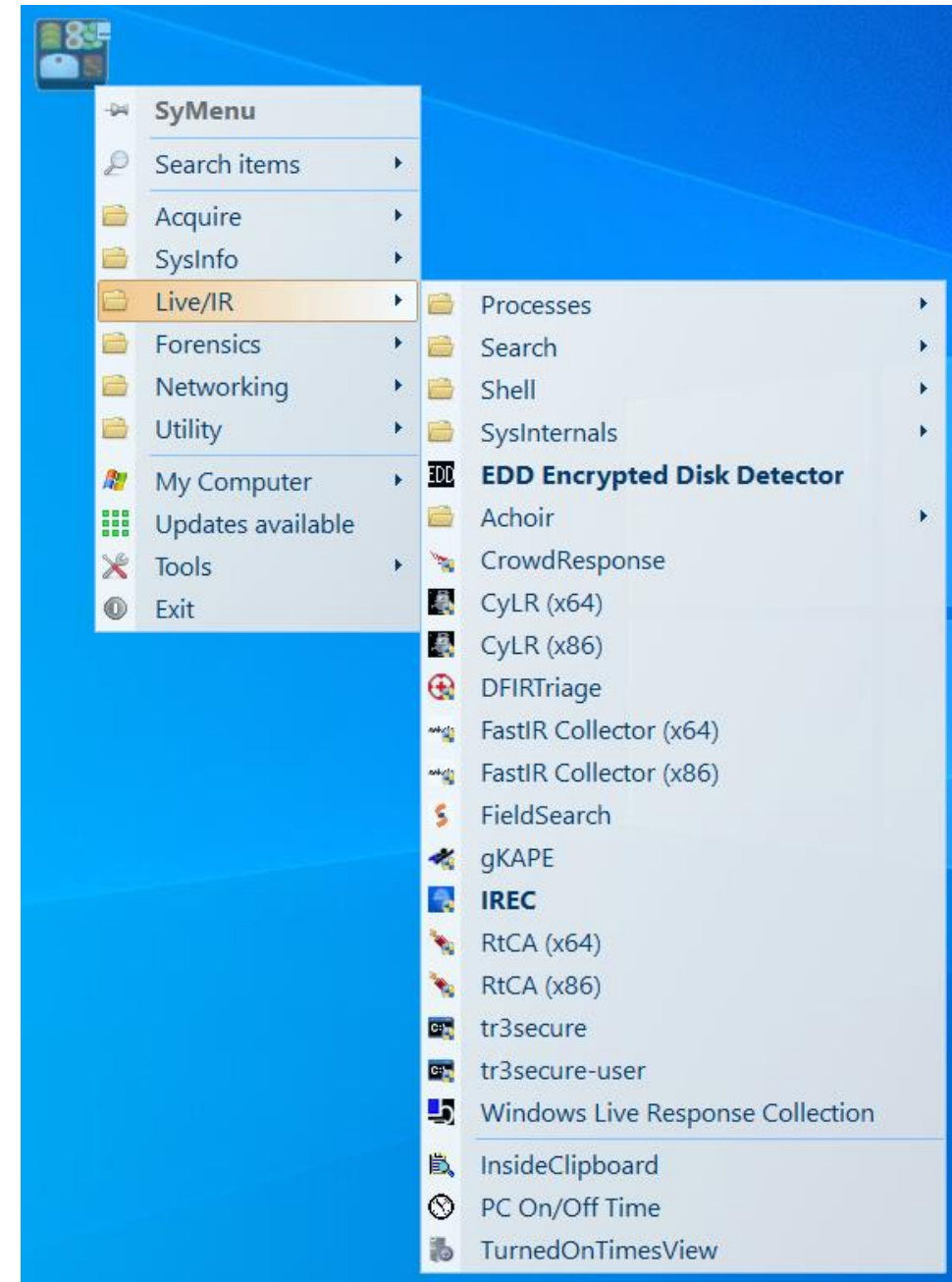
Bento – Live Forensics / Incident Response

▶ Bento include programmi automatizzati e batch script per **Windows, Linux** e **Mac OS X** per raccogliere informazioni sul sistema su cui vengono avviati

▶ Possono salvare un report in locale (p.e. in \Bento\Reports) o in uno share di rete

▶ Consentono di velocizzare e standardizzare rilievi che, fatti da un operatore umano, richiederebbero tempo e competenze specifiche approfondite

▶ Arma a doppio taglio, ma agevole, metodica, standardizzata, rapida, efficiente



Oltre al menu: Linux, OSX e Windows CLI



Three overlapping Windows File Explorer windows showing the directory structure of a bento box installation.

The top window shows the path: `D:\Bento\ProgramFiles\linux`.

The middle window shows the path: `D:\Bento\ProgramFiles\macosx`.

The bottom window shows the path: `D:\Bento\ProgramFiles\windows-cli`.

The bottom window displays a list of files and folders:

Nome	Tipo	Dimensione	Ultima modifica
cygwin	Cartella di file		27/09/2018 12:12
ftkimgager	Cartella di file		30/09/2017 18:36
LaZagne	Cartella di file		02/09/2018 22:32
sleuthkit-win32	Cartella di file		27/09/2018 13:08
tr3secure	Cartella di file		30/09/2017 18:35
win2k3-32	Cartella di file		30/09/2017 18:34
win2k-32	Cartella di file		30/09/2017 18:35
win7-32	Cartella di file		30/09/2017 18:34
win7-64	Cartella di file		30/09/2017 18:35
win10-32	Cartella di file		30/09/2017 18:26
win10-64	Cartella di file		02/11/2017 19:41
winvista-32	Cartella di file		30/09/2017 18:26
winxp-32	Cartella di file		30/09/2017 18:35
filelist.txt	File TXT	1 KB	02/11/2017 18:25
WindowsTrustedBinariesCollection.bat	File batch Windows	2 KB	02/11/2017 18:18

Attiva Windows
Passa a Impostazioni per attivare Windows.




Categorie ▾

Cerca su Groupon

Monza Brianza



Accedi ▾



Evviva la primavera!

Nuovi modi per rifiorire

Scopri

Ciao, Regalati una grande offerta oggi



SCELTI DA VOI

10 T-shirt Fruit Of The Loom

~~€ 39,90~~ Da **€ 18,90** 52% di sconto

1.000+ acquistati



ASPORTO O CONSEGNA A DOMICILIO

Uber Eats

1.000+ acquistati

€ 0

Buono per Uber Eats





SCELTI DA VOI

Mascherine riutilizzabili

Da **€ 3,90**

5.000+ acquistati

https://www.groupon.it/deals/mascherine-riutilizzabili-poliuretano-2



Ciao, Regalati una grande offerta oggi

SCELTI DA VOI

10 T-shirt Fruit Of The Loom

~~€ 39,90~~ Da **€ 18,90** 52% di sconto

1.000+ acquistati

ASPORTO O CONSEGNA A DOMICILIO

Uber Eats

1.000+ acquistati

€ 0

Buono per Uber Eats

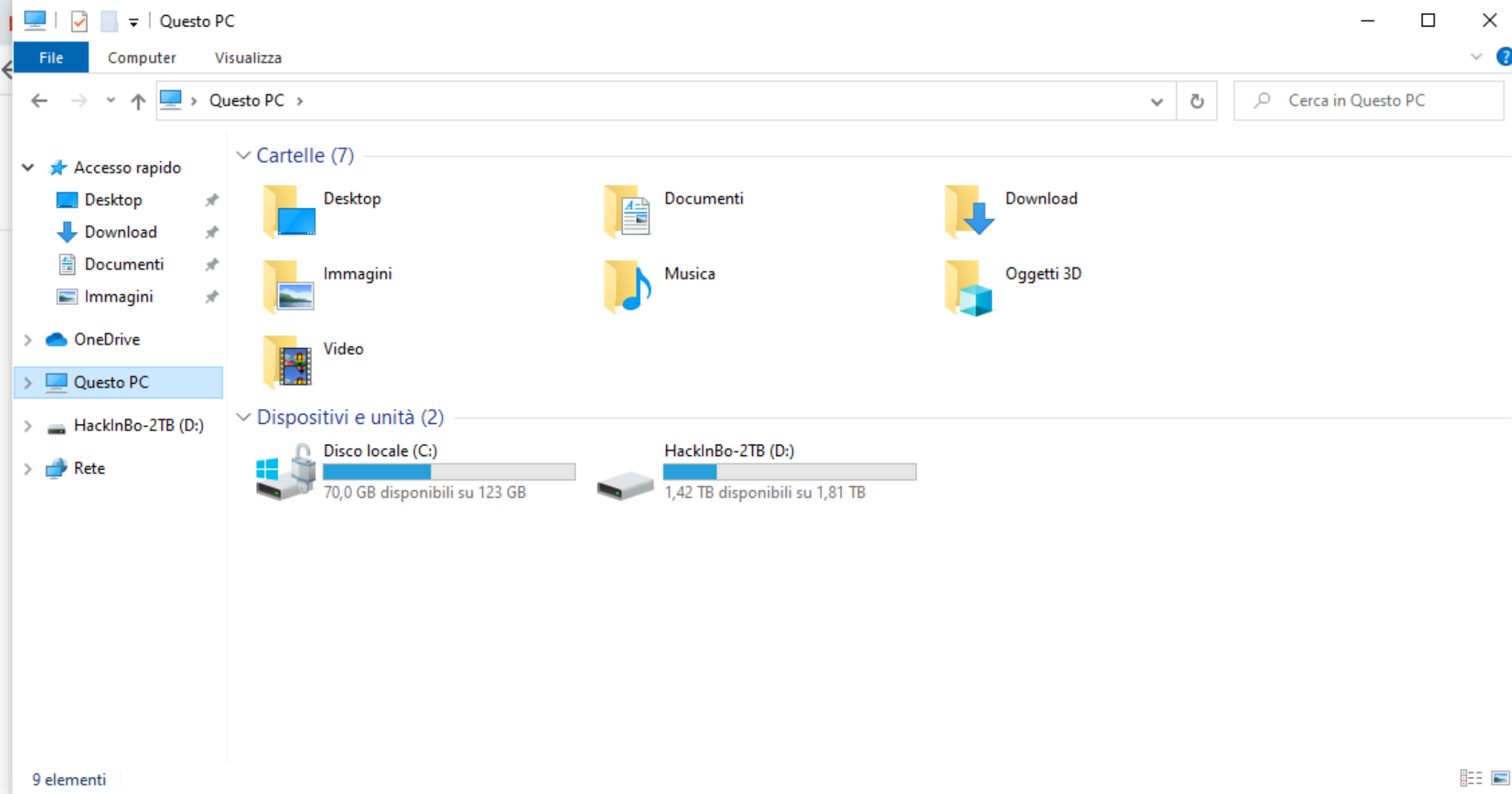
SCELTI DA VOI

Mascherine riutili

Da **€ 3,90**

5.000+ acquistati

Avira
Status: Protected
Last update: Today



10 T-shirt Fruit Of The Loom

~~€ 39,90~~ Da **€ 18,90** 52% di sconto

1.000+ acquistati

Uber Eats

1.000+ acquistati

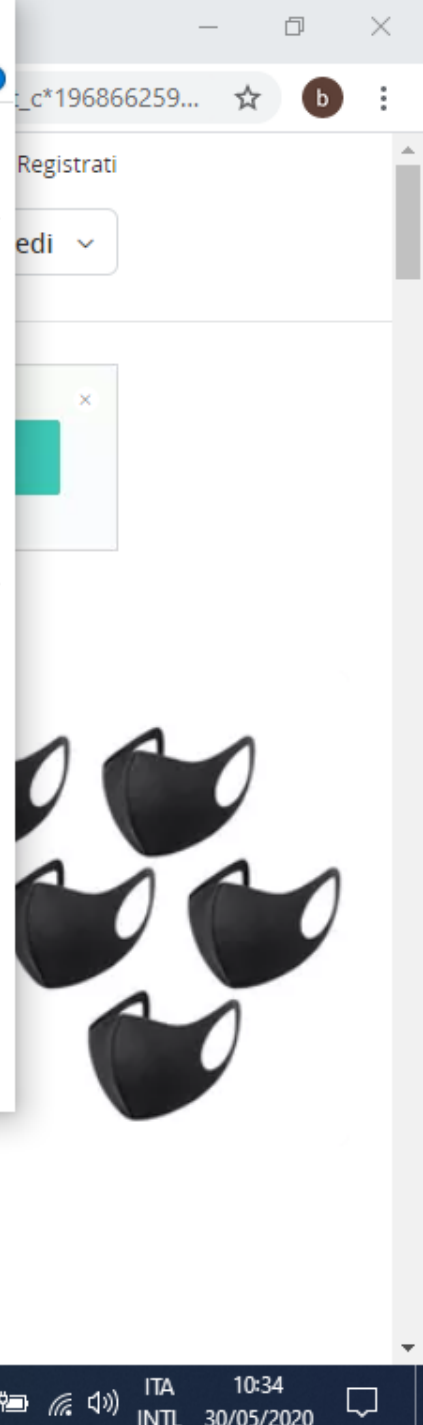
€ 0

Buono per Uber Eats

Mascherine riutilizzabili

Da **€ 3,90**

5.000+ acquistati



Gestisci

HackInBo-2TB (D:)

File

Home

Condividi

Visualizza

Strumenti applicazioni

← → ↕ ↗

Questo PC > HackInBo-2TB (D:)

Cerca in HackInBo-2TB (D:)

Accesso rapido

Desktop

Download

Documenti

Immagini

screenshot

OneDrive

Questo PC

HackInBo-2TB (D:)

Rete

Nome	Ultima modifica	Tipo	Dimensione
Bento	30/05/2020 10:34	Cartella di file	
Download	06/11/2019 13:17	Cartella di file	
Evidence	05/11/2019 16:02	Cartella di file	
Live	06/11/2019 12:36	Cartella di file	
no	04/11/2019 13:59	Cartella di file	
screenshot	30/05/2020 10:34	Cartella di file	
Bento	07/02/2019 13:05	Applicazione	155 KB
Bento-2020.5-full	15/05/2020 10:19	7z Archive	709.901 KB
start-Bento	07/02/2019 13:35	File batch Windows	1 KB

9 elementi 1 elemento selezionato 154 KB

10 T-shirt Fruit Of The Loom

~~€ 39,90~~ Da **€ 18,90** 52% di sconto

1.000+ acquistati

Uber Eats

1.000+ acquistati

€ 0

Buono per Uber Eats

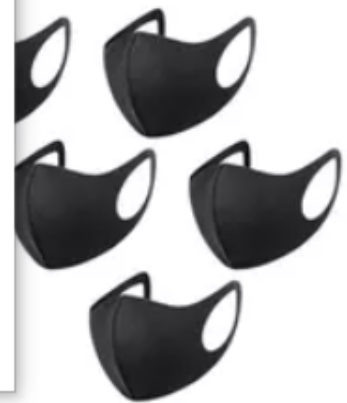
Mascherine riutilizzabili

Da **€ 3,90**

5.000+ acquistati

Registrati

edi



File

Home

Condividi

Visualizza

Gestisci

Strumenti applicazioni

HackInBo-2TB (D:)

← → ↕ ↻

Questo PC > HackInBo-2TB (D:)

Cerca in HackInBo-2TB (D:)

	Nome	Ultima modifica	Tipo	Dimensione
Accesso rapido	Desktop			
	Download			
	Documenti			
	Immagini			
	screenshot			
	OneDrive			
	Questo PC			
	HackInBo-2TB (D:)			
Rete				
	Bento	30/05/2020 10:34	Cartella di file	
	Download	06/11/2019 13:17	Cartella di file	
	Evidence	05/11/2019 16:02	Cartella di file	
	Live	06/11/2019 12:36	Cartella di file	
	no	04/11/2019 13:59	Cartella di file	
	screenshot	30/05/2020 10:35	Cartella di file	
	Bento	07/02/2019 13:05	Applicazione	155 KB
	Bento-2020.5-full	15/05/2020 10:19	7z Archive	709.901 KB
	start-Bento	07/02/2019 13:35	File batch Windows	1 KB

9 elementi

1 elemento selezionato 154 KB

SyMenu

Search items

Acquire

SysInfo

Live/IR

Forensics

Networking

Utility

My Computer

Updates available

Tools

Exit

Image

Copy

Burn

Hash

Image Mounter

FTK Imager Lite

Belkasoft Acquisition Tool

DMDE (x64)

DMDE (x86)

HDDRawCopy

Magnet RAM Capture

RamCapture x64

RamCapture x86

winpmem

ftkimager CLI x86

10 T-shirt Fruit Of The Loom

€ 39,90 Da € 18,90 52% di sconto

1.000+ acquistati

Uber Eats

1.000+ acquistati

€ 0

Buono per Uber Eats

Mascherine riutilizzab

Da € 3,90

5.000+ acquistati

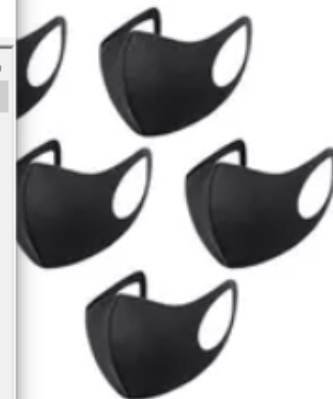
Scrivi qui per eseguire la ricerca

ITA

INTL

10:35

30/05/2020



Memory Capture

\\.\PHYSICALDRIVE0

- Partition 1 [549MB]
- Partition 2 [126893MB]
- Unrecognized file system [HPFS/NTFS]
- Partition 3 [555MB]
- Unpartitioned Space [basic disk]

C:\

- NONAME [NTFS]
 - [root]
 - [unallocated space]
 - [orphan]

Destination path:

D:\Evidence

[Browse](#)

Destination filename:

memdump.mem

☒ Include pagefile

pagefile.sys

☒ Create AD1 file

memcapture.ad1

Capture Memory

Cancel

Custom Content Sources

Evidence:File System	Path	File	Options
----------------------	------	------	---------

0000000000	EB 58 90 2D 46 56 45 2D-46 53 2D 00 02 08 00 00	ÈX--FVE-FS-....
0000000010	00 00 00 00 00 F8 00 00-3F 00 FF 00 00 30 11 00ø-?-ÿ-0-
0000000020	00 00 00 00 00 E0 1F 00 00-00 00 00 00 00 00 00â.....
0000000030	01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00
0000000040	80 00 29 00 00 00 00 00-4E-20 20 4E 41 4D 45 20 20	..-)---NO NAME
0000000050	20 20 46 41 54 33 32 20-4F 20 33 C9 8E D1 BC F4	FAT32 3È-Ñ-ø
0000000060	7B 8E C1 8E D9 BD 00 7C-A0 FB 7D B4 7D 8B F0 AC	{.Ã-Ù- û'}-ø-
0000000070	98 40 74 0C 48 74 0E B4-0E BB 07 00 CD 10 EB EF	·@t·Ht·'·»··í·ëí
0000000080	A0 FD 7D EB E6 CD 16 CD-19 00 00 00 00 00 00 00 00	ý)ëæí·í.....
0000000090	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000000a0	3B D6 67 49 29 2E D8 4A-83 99 F6 A3 39 E3 D0 01	;ÖgI).ØJ·-øì9âÐ-
00000000b0	00 00 3A 04 00 00 00 00-00 F0 20 5C 00 00 00 00 00	..:.....ø \.....
00000000c0	00 B0 6B 25 01 00 00 00-00 00 00 00 00 00 00 00	·°k\$.....
00000000d0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000000e0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

Cursor pos = 0; log sec = 0; phy sec = 1126400

For User Guide, press F1



Ciao, Regalati una grande offerta



SCELTI DA VOI

10 T-shirt Fruit Of The Loom
~~€ 39,90~~ Da **€ 18,90** 52% di sconto
1.000+ acquistati

Don't Sleep 6.51 - OS:10.0 18363 x64

Don't Sleep Opzioni Sistema Computer Monitor # ? # LNG Barra sistema

Disabilita ☐

☒ Non andare in sleep ☒ Vai in sleep

Impostazioni

Blocco

☒ Standby/sleep ibrido/ibernazione
☒ Blocca spegnimento
☒ Disconnessione
☒ Screensaver/spegni monitor

Opzioni

Timer Batteria CPU Rete

30/05/2020 10:39:34 Off #

Esci e ferma blocco

Usa timer ☐

Freeware (c) Nenad Hrg 2010-2020 # http://www.softwareok.com Dona Esci

Don't Sleep

Scopri



SCELTI DA VOI

Uber Eats
1.000+ acquistati
€ 0
Buono per Uber Eats

Mascherine riutilizzabili
Da **€ 3,90**
5.000+ acquistati



* Checking physical drives on system... *

Checking PhysicalDrive0 - INTEL SSDSC2CW240A (240 GB) - Status: OK

Checking PhysicalDrive1 - TOSHIBA External USB 3.0 USB Device (2.000 GB) - Status: OK

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 133 GB, Free Space: 75 GB

Drive D: [Label: HackInBo-2TB] (PhysicalDrive1), Drive Type: Fixed, Filesystem: NTFS, Size: 2.000 GB, Free Space: 1.571 GB

* Completed checking logical volumes on system. *

* Running Secondary Bitlocker Check... *

Volume C: [] is encrypted using Bitlocker.

* Completed Secondary Bitlocker Check... *

* Checking for running processes... *

* Completed checking running processes. *

*** Encrypted volumes and/or processes were detected by EDD. ***

Press any key to continue...

(use 'EDD /batch' to bypass this prompt next time)

—



Categorie

- [-] Descrizione Del Siste
- [+] Software installato
- [-] Sistema Operativo
- [-] Periferiche
- [+] Sicurezza
- [+] Gruppi e Utenti
- [+] Operazioni Pianificate
- [-] Statistiche Uptime
- [-] Environment Variable
- [-] Regional Settings
- [+] Rete Windows
- [+] TCP/IP di rete
- [+] Dispositivi hardware
- [+] Visualizza capacità
- [+] Display Adapters
- [+] Stampanti installate
- [-] Versione BIOS
- [+] Amministrazione di Si
- [+] Processori
- [-] Memoria
- [+] Dischi fisici
- [+] Drives
- [+] Porte di Comunicazione
- [-] Programmi in esecuzi
- [+] Servizi
- [-] Programmi in esecuzi
- [+] ODBC Information
- [-] OLE DB Providers

Audit

Computer Audit for DESKTOP-SHC850U

1) Descrizione Del Sistema

Item	Value
Computer Name	DESKTOP-SHC850U
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server
Description	
Operating System	Microsoft Windows 10 Pro 64-Bit
Manufacturer	CLEVO CO.
Model	W110ER
Serial Number	N/A
Asset Tag	To Be Filled By O.E.M.
Number of Processors	1
Processor Description	Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz
Total Memory	16384KB
Total Hard Drive	2.04TB
Display	M116NWR1 R1 , 11.6" (26cm x 14cm)
BIOS Version	ALASKA - 1072009
User Account	godric
System Uptime	0 Days 0 Hours 52 Minutes
Local Time	2020-05-30 10:38:37

2) Software installato

3) Active Setup

Name	Version	Installed
.NET Framework	4,0,30319,0	No
.NET Framework	4,0,30319,0	No
.NET Framework	4,0,30319,0	No
Active Directory Service	5.0.00.0	Yes

Selezione: [C:] Disco locale

Analizza

Selezione: [C:] Disco locale

Spazio totale: 123,9 GB

Spazio usato: 57,6 GB (46,47%)

Spazio libero: 66,3 GB (53,53%)



WizTree v3.33 (64bit)

© 2020 Antibody Software

www.antibody-software.com

Donate



Aiutaci a migliorare WizTree!

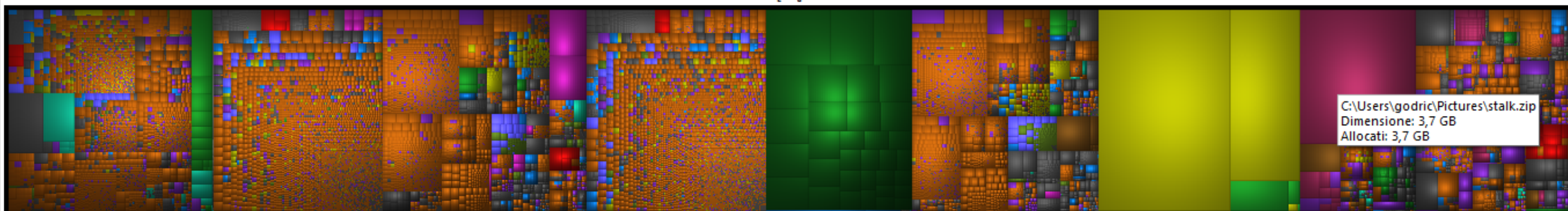
(puoi nascondere il pulsante Dona facendo una donazione)

Vista struttura Vista file Info sul programma

Cartella	Percentuale genitore	Dimensione	Allocati	Elementi	File
C:\	100,0 %	75,5 GB	57,3 GB	415.764	336.905
Windows.old	37,0 %	27,9 GB	21,9 GB	225.940	180.697
Windows	32,7 %	24,7 GB	13,8 GB	127.350	102.228
[13 File in C:]	12,9 %	9,7 GB	9,7 GB	27	13
Users	7,4 %	5,6 GB	5,6 GB	10.308	7.040
Program Files	5,7 %	4,3 GB	3,2 GB	45.236	41.402
Program Files (x86)	3,0 %	2,3 GB	2,3 GB	4.798	4.043
ProgramData	1,3 %	978,4 MB	775,6 MB	2.064	1.452
\$Extend	0,0 %	20,1 MB	60,4 MB	13	9
Intel	0,0 %	734,9 KB	748,0 KB	7	6
System Volume Information	0,0 %	285,1 KB	292,0 KB	14	12
\$Recycle.Bin	0,0 %	387 Byte	0	6	3
Recovery	0,0 %	0	0	0	0
Programmi	0,0 %	0	0	0	0
PerfLogs	0,0 %	0	0	1	0
Documents and Settings	0,0 %	0	0	0	0

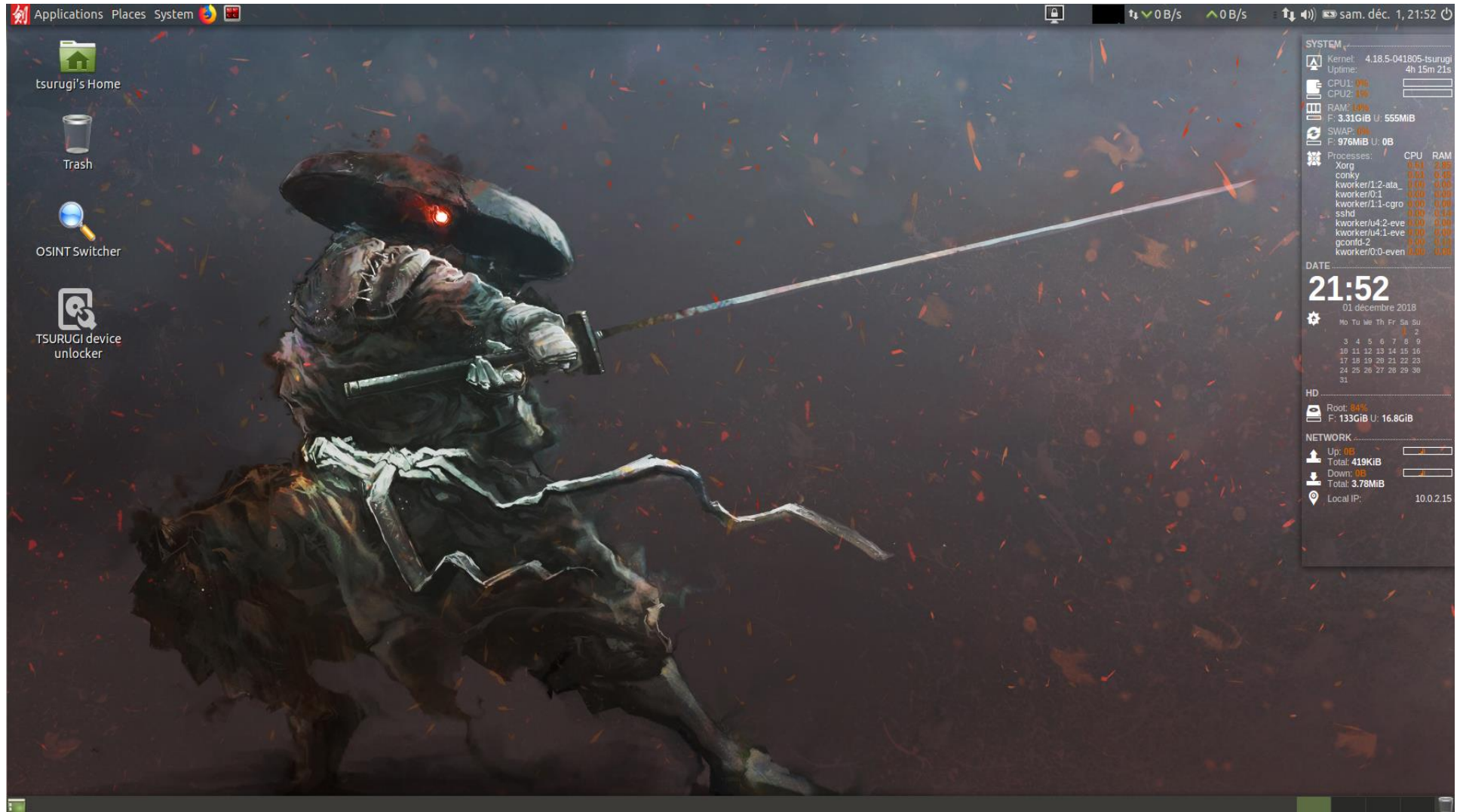
Estensione	Tipo file	Percen...	Dimensione	Allocati	File
.dll	Estensione dell'app	39,4 %	29,7 GB	19,6 GB	64.080
.sys	File di sistema	14,2 %	10,8 GB	10,1 GB	4.797
(nessuna estensio		11,7 %	8,8 GB	6,3 GB	3.456
.exe	Applicazione	5,9 %	4,5 GB	3,3 GB	9.326
.zip	zip Archive	5,8 %	4,4 GB	4,4 GB	101
.dat	File DAT	1,8 %	1,4 GB	980,5 MB	1.205
.ttc	File tipi di caratter	1,5 %	1,1 GB	680,9 MB	116
.wim	wim Archive	1,3 %	1,0 GB	985,9 MB	16
.vdm	File VDM	1,1 %	832,8 MB	517,3 MB	28
.ttf	File del tipo di cara	1,0 %	811,9 MB	534,5 MB	1.538
.cab	cab Archive	1,0 %	748,1 MB	750,2 MB	436
.msi	Pacchetto di Wind	1,0 %	744,3 MB	744,3 MB	20
.esd	File ESD	0,7 %	550,6 MB	550,6 MB	2
.mun	File MUN	0,7 %	514,1 MB	302,2 MB	556
.mui	File MUI	0,6 %	488,0 MB	231,4 MB	19.042
.cat	Catalogo sicurezza	0,5 %	395,3 MB	195,1 MB	16.174
.ocx	Controllo ActiveX	0,5 %	361,2 MB	257,1 MB	113
.xml	Documento XML	0,5 %	348,9 MB	230,3 MB	11.338

[C:]



C:\Users\godric\Pictures\stalk.zip

Digital forensics con Tsurugi



www.tsurugi-linux.org

HACK IN BO®
Safe Edition