Sopralluogo informatico, live forensics e incident response con Bento

Bologna, 27 ottobre 2018

HACK IN BO®
Winter 2018 Edition

Chi vi parla

Davide ‘Rebus’ Gabrini

Trascorsi in Polizia Giudiziaria e Polizia Postale, attualmente V.Ispettore nella Polizia Scientifica

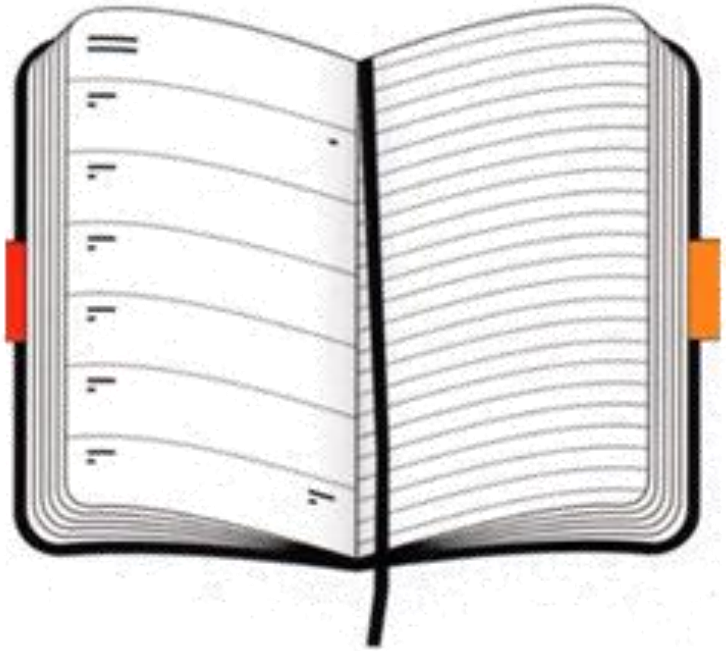
Oltre a ciò:

- Perito informatico
- Consulente tecnico e Perito forense
- Collaboratore Laboratorio di Informatica Forense UniPV
- Docente di sicurezza informatica e digital forensics per privati e P.A.
- Certificazioni CIFI, ACE, AME
- Socio Mensa, IISFA, Tech&Law fellow
- Socio fondatore IHF e Nutria LUG

HACK IN BO® Winter 2018 Edition

Agenda

- Sopralluogo informatico
- Live Forensics
- Incident Response
- Best practices
- Bento



SOPRALLUOGO INFORMATICO

HACK IN BO®
Winter 2018 Edition

Sopralluogo informatico

- Insieme delle attività eseguite sul luogo in cui si è consumato un reato, tendenti ad osservare, individuare, raccogliere o fissare tutti quegli elementi utili alla ricostruzione dell'evento delittuoso ed alla individuazione degli autori del fatto, anche "in relazione ai dati, alle informazioni e ai programmi o ai sistemi informatici o telematici".
- La scena del crimine si è arricchita di una dimensione digitale che non è mai trascurabile

Accertamenti urgenti

Art.354 cpp: Accertamenti urgenti sui luoghi, sulle cose e sulle persone

- 1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
- 2. Se vi è pericolo che le cose le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano altresì le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.
- 3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.

Necessità di una metodologia scientifica

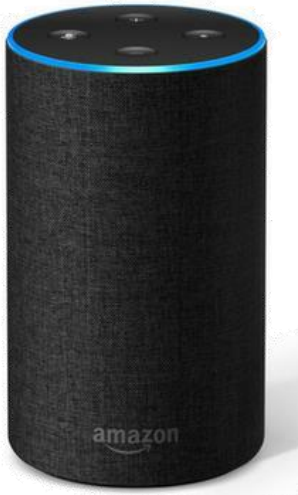
- Nuova specializzazione di polizia scientifica
- Pervasività delle tecnologie digitali
- Improbabile, oggigiorno, una scena del crimine priva di elementi digitali
- Loro implicazione in attività delittuose
  - Come **fine**
  - Come **mezzo**
  - Come **testimone**

Dumb things

HACK IN BO®
Winter 2018 Edition

Pervasive computing

- Smart things
- Smart watches
- Smart home
- Smart cars
- Smart clothes
- Smart crap…



HACK IN BO®
Winter 2018 Edition

Smart (?) things

HAIR HEALTH ANALYSIS

Dryness

Follow hair elasticity and learn how to avoid dry hair

Damage

Measure cuticle damage to help ensure moisture retention

Breakage

Control hair quality and resilience to avoid breakage

Tangling

Optimize sebum distribution and avoid tangles

BRUSHING EXPERIENCE

Force & rhythm

Get insight into how to avoid damaging hair

Gesture analysis

Understand and improve brushing habits

Stroke count

Detailed information on how use impacts hair quality

HACK IN BO®
Winter 2018 Edition

...e dispositivi palesemente ostili

Live forensics

- La parte più delicata di un sopralluogo informatico è l'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*

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

Incident Response

- Un incidente informatico è qualcosa di più ampio, che non riguarda necessariamente un evento criminoso, ma comprende imprevisti e malfunzionamenti anche accidentali
- Le procedure di DF ben si inseriscono nel processo di gestione degli incidenti: un processo di IR non è completo senza una fase di *indagine* che spieghi l'accaduto e consenta di migliorare il processo

- Nonostante i possibili obiettivi comuni, DF e IR hanno spesso priorità e finalità diverse: ciò che va bene per l'IR, non necessariamente va altrettanto bene per la DF
  - sempre se si desidera arrivare in sede di giudizio

Le fasi canoniche

- Identificazione

- Acquisizione/Preservazione

- Analisi/Valutazione

- Presentazione

BEST PRACTICES

Best practices: fonti internazionali

- RFC3227: Guidelines for Evidence Collection and Archiving
- ISO 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence
- **Linee guida del Consiglio d'Europa tradotte in italiano: http://bit.ly/eeg-ita-form**
- IACP: International Association of Chiefs of Police
  - Best Practices for Seizing Electronic Evidence
- US Department of Justice:
  - Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
- UK ACPO: Association of Chief Police Officers
  - Good Practice Guide for Digital Evidence
- **In Italia**: PT67, procedura tecnica ad uso interno della Polizia Scientifica

LIVE FORENSICS

HACK IN BO®
Winter 2018 Edition

Analisi Live vs Post-mortem

- Quando si rinviene un sistema acceso, si è davanti ad una scelta:
  - Spegnerlo subito per procedere ad acquisizione e analisi post-mortem
  - **Esaminarlo mentre è in esecuzione**

- Procedere ad una preliminare attività descrittiva
  - Stato esteriore e, in particolare, del display
  - Data e ora del sistema
  - Programmi visibili in esecuzione
  - Stato delle connessioni con l'esterno
- Documentare con rilievi video/fotografici (art. 234 c.p.p. – Prova documentale)
- Procedere all'atto di P.G. (perquisizione, ispezione, sequestro, accertamento urgente…) mediante tecniche di live forensics

Spegnimento

- Cosa si perde sicuramente allo spegnimento:
  - memorie volatili
  - stato di rete, sistema, applicazioni ecc.
    - chat in corso, cronologia di una shell…
    - eventi in corso che non prevedono log
  - **volumi cifrati** (BitLocker, FileVault, TrueCrypt, PGDisk, BestCrypt ecc. ecc.)
  - possibilità di estendere l'attività a contenuti **cloud** connessi
- Talvolta il sistema *non può* essere spento o rimosso
  - La *live forensics* è così l'unica possibilità

Invasività

- Il sistema è in esecuzione, **qualsiasi** azione lo modificherà
  - tanto vale intraprendere azioni utili...
- Il sistema viene sicuramente perturbato
  - le modifiche sono note?
  - sono documentabili?
  - intaccano significativamente il risultato dell'analisi?
  - ogni modifica distrugge qualcosa
    - ne vale la pena?
- Gli accertamenti svolti su sistemi accesi non saranno ripetibili, ma probabilmente piove sul bagnato ;-)

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

STRUMENTI

HACK IN BO®
Winter 2018 Edition

DART

DART è la collezione di programmi portabili per live forensics inclusa in DEFT

- Oltre 300 programmi per Windows, Linux e Mac OSX
- Ultima release: gennaio 2018
- Scaricabile da www.tipiloschi.net

HACK IN BO® Winter 2018 Edition

BENTO

your forensic launcher box

HACK IN BO®
Winter 2018 Edition

TipiLoschi.net

Non è morto ciò che in eterno può attendere

Home | Rebus' Digest | Eventi Loschi | Bento

Home

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*.

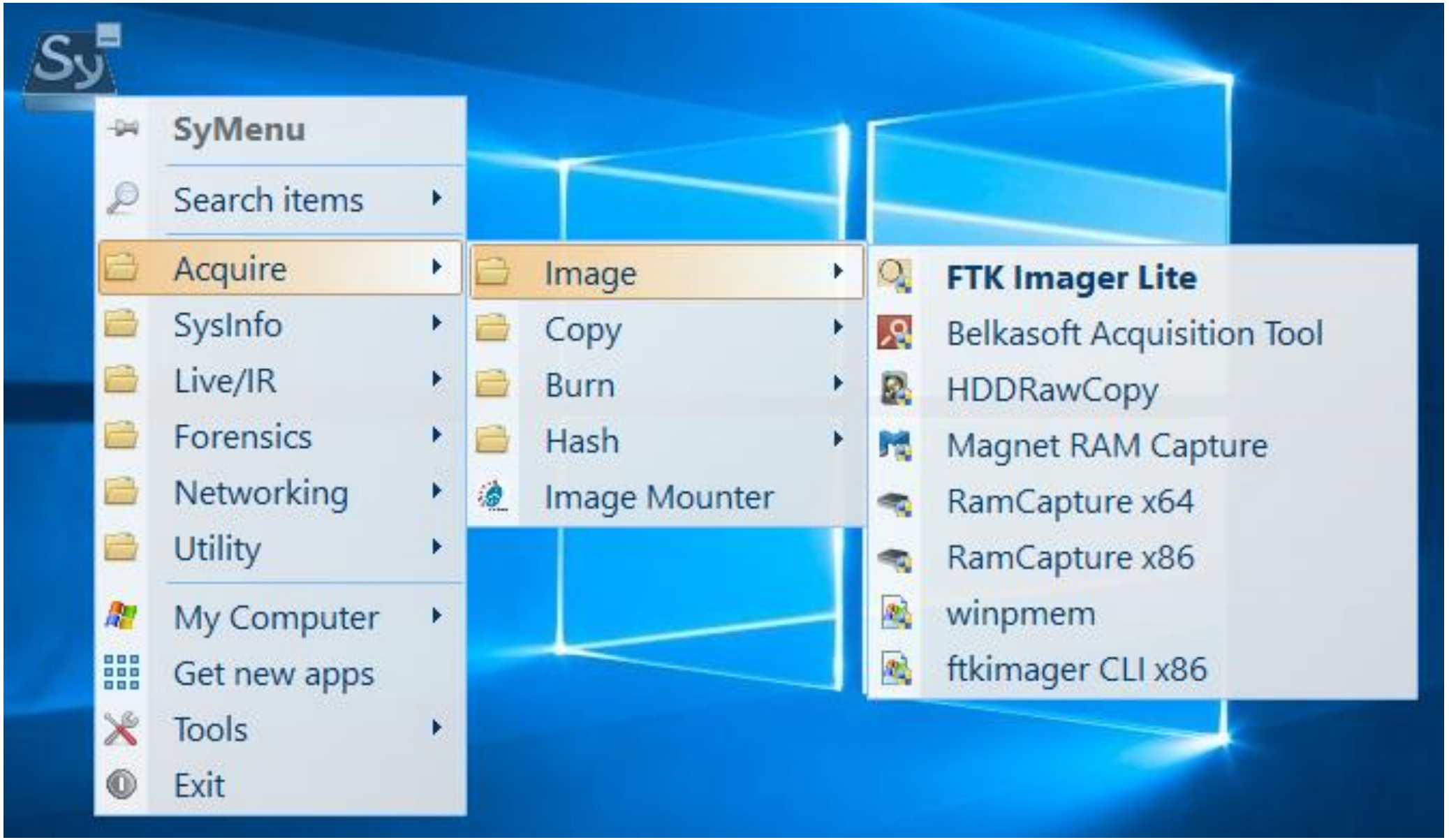
Linee guida di Bento

- Nasce per l'equipaggiamento della Polizia Scientifica
- Orientamento al sopralluogo informatico
  - Ridurre gli strumenti strettamente orientati all'analisi
  - Privilegiare gli strumenti di sopralluogo
    - Rilevamento, ricognizione, accertamento urgente, acquisizione, documentazione…
- Escludere tutti gli abandonware
- Dare supporto per l'aggiornamento di ogni singolo pacchetto
- Fornire diversi approcci all'automazione
  - Per rendere le operazioni semplici, rapide, efficienti, metodiche

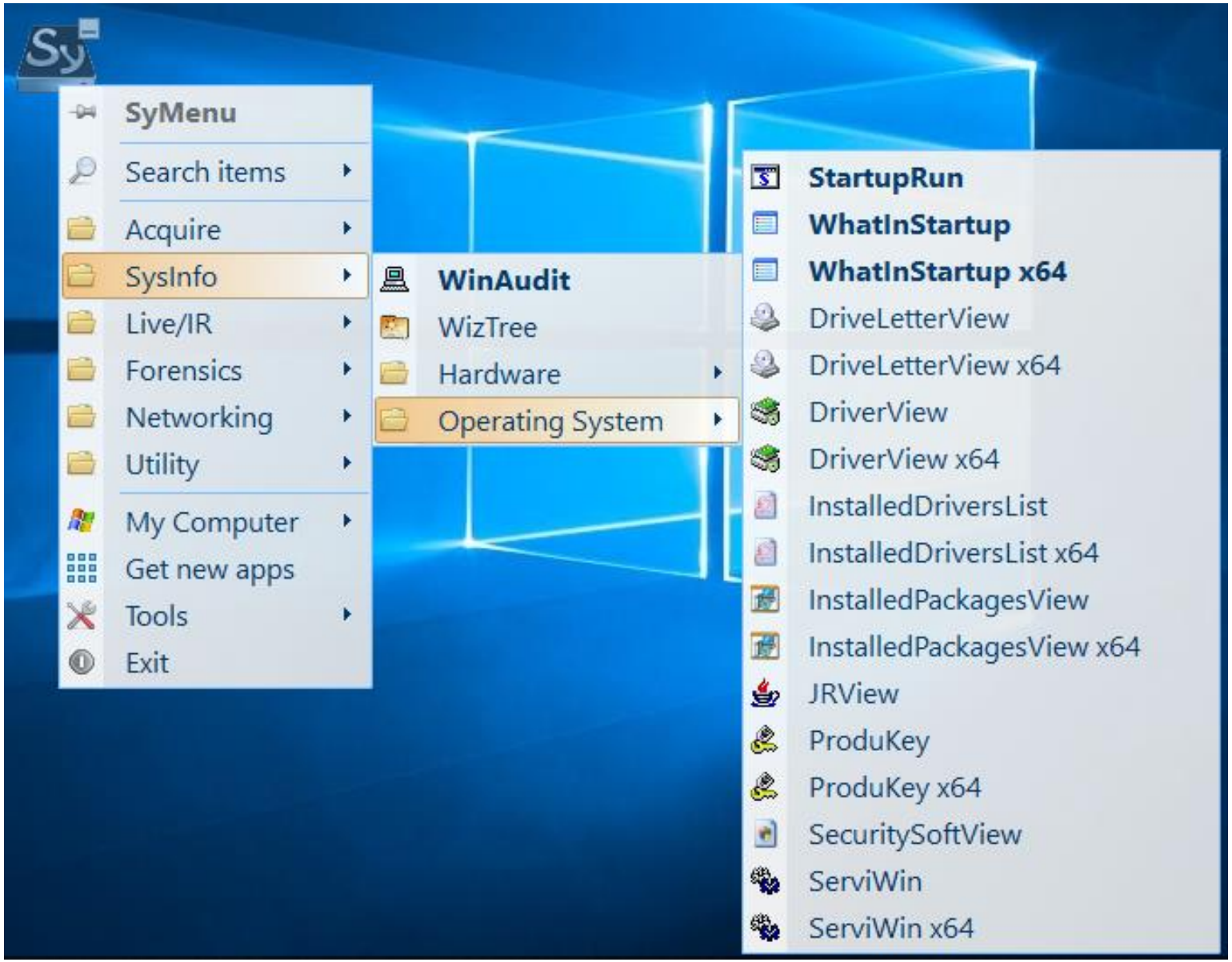
SyMenu

- Tanto semplice nell'immediatezza,
tanto complesso se occorre approfondire
- Elevata personalizzazione dell'interfaccia
- Tecnologia SPS: Standard for Portable Software
  - Supporto per installazione, aggiornamento e rimozione dei pacchetti software
  - Già supportate le suite Sysinternals, Nirsoft, e centinaia di altri programmi
  - Facile predisporre il supporto per ulteriori programmi
- Gestione integrata dei privilegi e dei parametri di avvio
- Facile accesso alla configurazione o alla cartella dei programmi
- Barra di ricerca integrata
- Supporto multilingua
- Freeware
- Sviluppato in Italia

Bento - Acquisizione

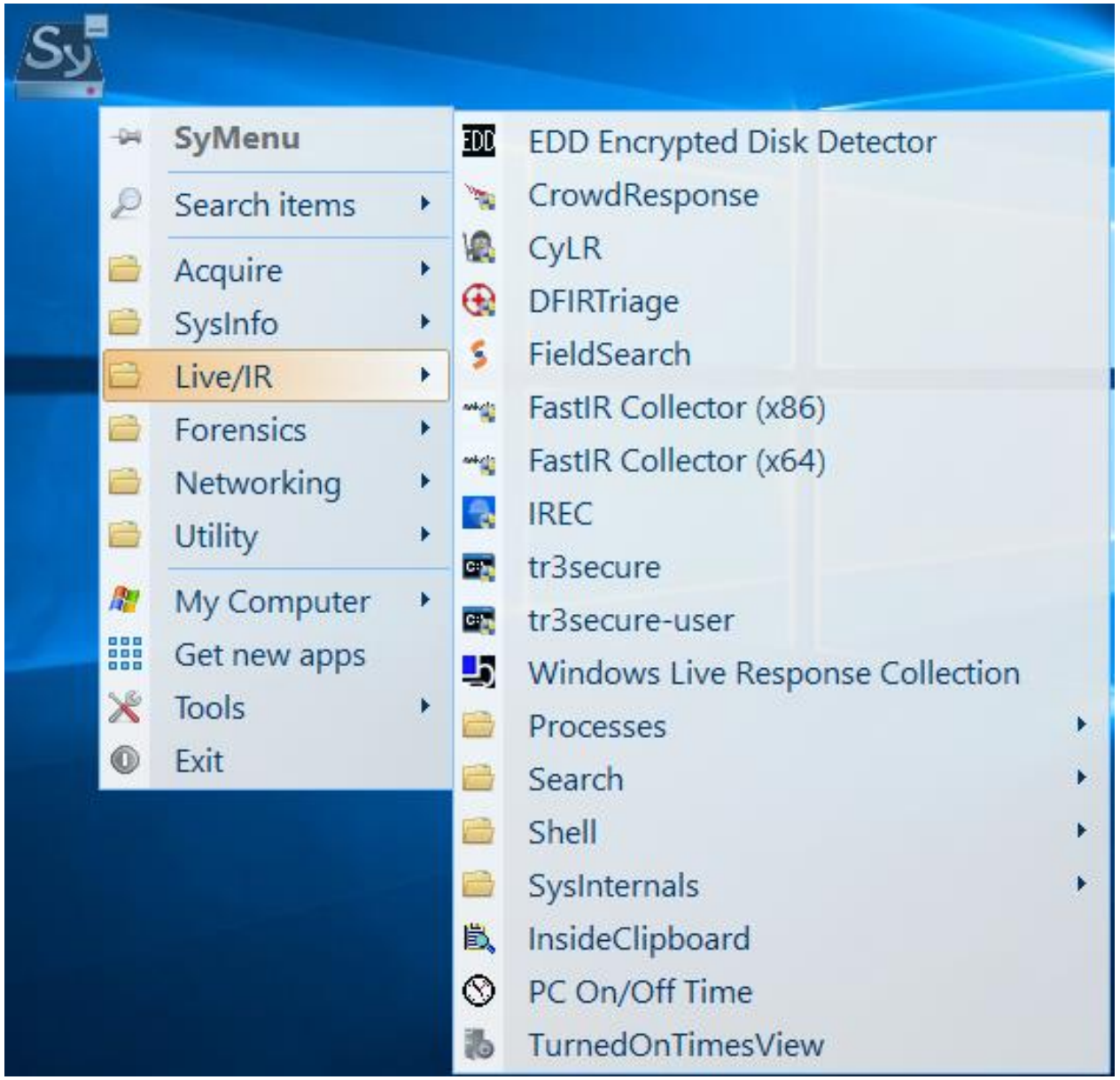


Bento – System Information Gathering



HACK IN BO®
Winter 2018 Edition

Bento – Live Forensics / Incident Response



HACK IN BO®
Winter 2018 Edition

Elevata configurabilità

SyMenu [D:] - v.6.05.6775

File Item Manager Advanced Help

Start Search (CTRL + S)

- Acquire
- SysInfo
- Live/IR
  - EDD Encrypted Disk Detector
  - CrowdResponse
  - CyLR
  - DFIRTriage
  - FieldSearch
  - FastIR Collector (x86)
  - FastIR Collector (x64)
  - IREC
  - tr3secure
  - tr3secure-user
  - Windows Live Response Collec
- 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

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

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

HACK IN BO® Winter 2018 Edition

Oltre al menu: Linux, OSX e Windows CLI

D:\Bento\ProgramFiles\linux

File Home Condividi Visualizza

6 elementi

D:\Bento\ProgramFiles\macosx

File Home Condividi Visualizza

10 elementi

D:\Bento\ProgramFiles\windows-cli

File Home Condividi Visualizza

Questo PC › BENTO (D:) › Bento › ProgramFiles › windows-cli

Cerca in windows-cli

BENTO (D:)
- Bento
  - Config
  - Icons
  - Lang
  - Plugin
  - Profiles
  - ProgramFiles
    - linux
    - macosx
    - SPSSuite
    - windows-cli
      - cygwin
      - ftkimager
      - LaZagne
      - sleuthkit-win32
      - tr3secure
      - win2k3-32

Nome	Tipo	Dimensione	Ultima modifica
cygwin	Cartella di file		27/09/2018 12:12
ftkimager	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

15 elementi

Supporto e futuri sviluppi di Bento

- Collaborazione col team di Tsurugi Linux, che adotta Bento come strumento per LF/IR
- Collaborazione con DEFT in corso di definizione
- Collaborazione con Gianluca Negrelli, sviluppatore di SyMenu, per valutare nuove feature:
  - Log dei programmi avviati
  - Verifica di integrità degli eseguibili e dei componenti critici
  - Accreditamento come *trusted editor* per nuovi SPS
- Proposta di collaborazione con il Laboratorio di Informatica Forense di UniPV e il Servizio Polizia Scientifica per la definizione delle procedure tecniche del sopralluogo informatico

tsurugi-linux.org

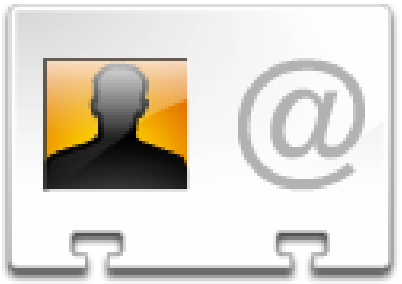
HACK IN BO®
Winter 2018 Edition

Teniamoci in contatto...

Davide Rebus Gabrini

e-mail: rebus@tipiloschi.net

GPG Public Key: www.tipiloschi.net/rebus.asc, KeyID: 0x176560F7



Queste e altre cazzate su

www.tipiloschi.net

facebook.com/gabrini

twitter.com/therebus

it.linkedin.com/in/rebus

- **Rebus' Digest**
  newletter su cybercrime, hacking, digital forensics…
- **EventiLoschi**
  calendario delle conferenze pubbliche in materia

HACK IN BO® Winter 2018 Edition