Open Source Digital Forensics

Di Nanni Bassetti

www.nannibassetti.com

Chi sono

Mi occupo di digital forensics dal 2005/2006, project manager di **CAINE** (distro usata in tutto il mondo)

Fondatore di CFI (Computer Forensics Italy)

Scrittore di parecchi articoli scientifici e software free/open source per la D.F.

Coinvolto in casi di rilevanza nazionale come:

* Consulente tecnico informatico di parte civile nel caso del transessuale "Brenda" (**caso Brenda-Marrazzo**).
* CTP (Consulente tecnico di parte) per gli Avv. Vito Russo ed Emilia Velletri nel caso **Sarah Scazzi (Avetrana (Ta))**
* Consulente tecnico informatico di parte civile nel caso della scomparsa di **Roberto Straccia**
* Consulente tecnico informatico di parte civile nel caso della scomparsa della piccola **Angela Celentano**

Definizione

La Digital Forensics è la disciplina scientifica che serve per identificare, acquisire ed analizzare una fonte di prova digitale, preservandola da eventuali alterazioni.

Scientifica: ripetibile (Galileo Galilei)

è la modalità tipica con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile. Esso consiste, da una parte, nella raccolta di evidenza empirica e misurabile attraverso l'osservazione e l'esperimento; dall'altra, nella formulazione di ipotesi e teorie da sottoporre nuovamente al vaglio dell'esperimento. (Wikipedia)

Fonte di prova: deve garantire il suo uso in tribunale

Chi NON è il digital forensics expert

- Il ragazzo che installa i programmi
- Il negozio di computer
- L'amico “bravo” suggerito da uno non del settore
- Quello che si qualifica coi “tesserini”
- Gli informatici che fanno altro...
- I non informatici che hanno la passione nel tempo libero
- Il cuggggino :-D

Chi è il digital forensics expert

- NESSUNO
- Chi ha delle pubblicazioni online/offline
- Chi ha un C.V. qualificante
- Chi sviluppa sw. Digital forensics
- Chi conosce i sw e hw della digital forensics
- Chi conosce leggi e metodologie della digital forensics

La STORIA

1984 FBI Magnetic Media Program created... this later becomes the Computer Analysis and Response Team (CART)

1995 International Organization on Computer Evidence (IOCE) formed

- RFC3227 -Guidelines for Evidence Collection and Archiving (2002)
- USA –Department of Justice -Searchingand SeizingComputers(2002)
- USA –IACP -Best Practices for Seizing Electronic Evidence (2006)
- USA –DoJ–Electronic Crime Scene Investigation v. 2 (2008)
- UK –ACPO –Computer Based Evidence Guidelines v.4 (2008) - Association of Chief Police Officers (ACPO) guidelines

Computer Forensics Tool Testing (CFTT) by NIST (National Institute of Standards and Technology)

La Storia

Gli esperti britannici sono conformi con l'Associazione dei capi di polizia (**ACPO**) le linee guida. Questi sono costituiti da quattro principi come segue: -

Principio 1: Nessuna azione intrapresa dalle forze dell'ordine o dai loro agenti dovrebbe cambiare i dati memorizzati su uno dei supporti informatici o di archiviazione che successivamente possono essere fatti valere in tribunale.

Principio 2: In circostanze eccezionali, quando una persona si trova nella necessità di accedere ai dati originali conservati su un computer o su supporti di memorizzazione, tale persona sia competente a farlo ed essere in grado di testimoniare e spiegare la rilevanza e le implicazioni delle loro azioni.

Principio 3: Il metodo adottato o altri documenti di tutti i processi applicati alla raccolta delle evidenze elettroniche deve essere creato e conservato. Una terza parte indipendente deve essere in grado di esaminare i processi e ottenere lo stesso risultato.

Principio 4: Il responsabile delle indagini ha la responsabilità generale di assicurare che il diritto e tali principi siano rispettati.

Definizione

I campi d'azione della Digital Forensics sono:

1) Indagini interne ad una azienda
2) Supporto alla Polizia Giudiziaria ed ai PM (CTP) e Giudici (CTU/Perito)
3) Supporto ai privati indagati (CTP)
4) Valutazione danni
5) Spionaggio
6) Frode
7) Pedopornografia
8) Violazione policy
9) Ricatto
10) Terrorismo
11) Ecc.

Definizione

Le fasi principali sono 4:

1) Identificazione

2) Acquisizione e preservazione

3) Analisi e valutazione

4) Presentazione

ACQUISIZIONE

Ci troviamo in un posto dove ci sono solo portatili da acquisire, abbiamo solo un portatile, ci “obbligano” ad acquisire
in situ…che facciamo? Accettiamo la ridicola velocità dell’USB 2.0? :-D

Write Blocker & Co.

Write Blocker & Co.

FONTE: **http://www.marcomattiucci.it/writeblockers.php**

I write-blocker sono di tre tipologie fondamentali:

- (a) Firmware based: orientati ad impiegare le primitive del BIOS ed a gestire la loro inibizione in qualsiasi tipo di scrittura;
- (b) Software o Driver based: sono software di basso livello (in ambiente windows dei driver) orientati ad intercettare qualsiasi interruzione hardware o software che diriga qualsiasi tipo di scrittura verso la memoria di massa considerata. In questo caso è quindi il sistema operativo ad impedire l'alterazione e non il BIOS. Sempre di conseguenza eventuali bug del sistema operativo hanno un immediato effetto sulla garanzia di funzionamento del write-blocker.
- (c) Hardware based: sono veri e propri dispositivi elettronici che "tagliano" il bus di comunicazione tra unità di storage fisica e scheda madre (generalmente) e si interpongono come intermediari valutando ed eventualmente inibendo tutto ciò che entra ed esce dal dispositivo target.

L’Attrezzatura “portatile”


HX-DE-K

OPEN SOURCE DAY
2013

L’Analisi

I tools possono essere commerciali o open source, l’importante che siano accettati dalla comunità dei C.F. experts, al fine di fugare dubbi sull’affidabilità dello strumento usato.

In caso di sviluppo di strumenti nuovi, è utile fornire il codice sorgente.

L’Analisi

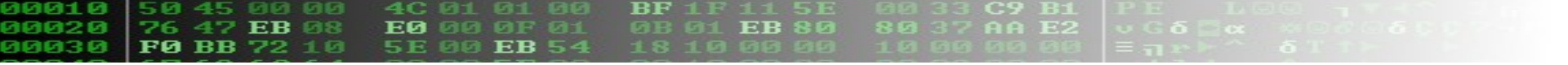
I tools commerciali potrebbero avere varie problematiche, come tutto ciò di cui non si conosce il sorgente:

1) Bugs
2) Formati troppo proprietari
3) Fine dello sviluppo del sw

L’Analisi

I tools Open Source hanno dei vantaggi indiscutibili:

1) Controllo dei Bugs da parte della community degli sviluppatori
2) Formati aperti e compatibili
3) Sorgenti aperti a tutti -> Si sa cosa fanno



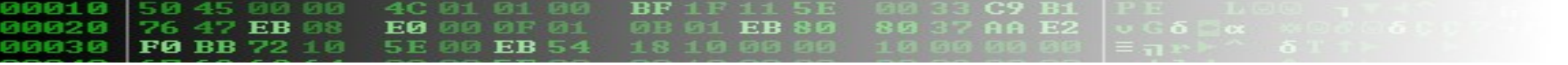
L’Analisi

La scelta NON deve essere radicale, ci sono sw commerciali che fanno cose che gli open source non fanno e viceversa

L'Analisi

TOOLS CLOSED SOURCE:

- Encase(GuidanceSoftware) - $ 2.995 + $500
- ForensicToolkit (Access Data) - $ 3.995 + $500
- X-WaysForensic(X-Ways) - $ 1.115
- P2 Commander(Paraben Corporation) - $ 1.095
- Pro Discover(TechnologyPathways) - $ 2.195
- Macintosh Forensic(Blackbag) - $ 2.600
- IEF – Magnet Forensics - $ 1.600



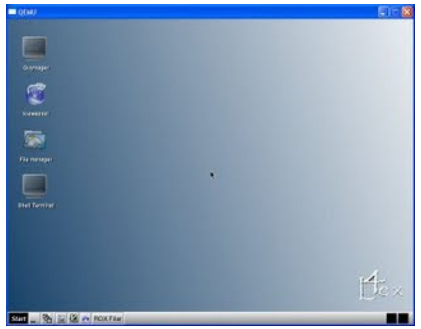
- E se troviamo un RAID?

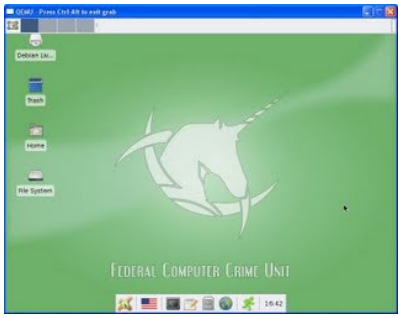
Arrivano le Live DISTRO!

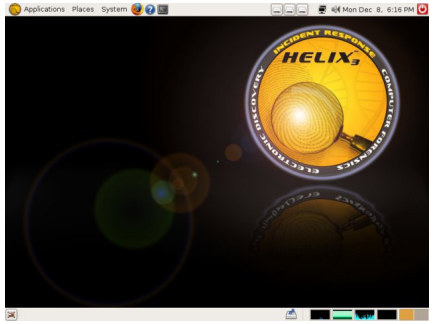
OPEN SOURCE:

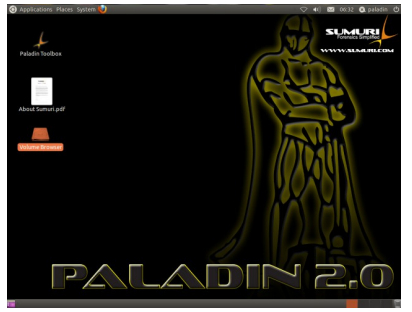
Live distro Linux:

1. CAINE
2. DEFT
3. FORLEX
4. FCCU
5. HELIX
6. PALADIN









Open Source Day 2013

CAINE 4.0 “Pulsar”

Open Source for D.F.

Entriamo nel vivo!

- I bash script risolvono
- SFDumper
- Raw2FS
- NBTempo
- KS
- Tanti altri tool nel mondo e creati da amici e da sconosciuti.
  Ma qui per sintesi parlerò solo di quelli miei ;-P

Open Source for D.F.

TEST DI DAUBERT VS. OPEN SOURCE

http://www.digital-evidence.org/papers/opensrc_legal.pdf

U.S. Supreme Court's ruling in Daubert vs. Merrell Dow Pharmaceuticals (1993)

- **Testing**: La procedura può ed è stata testata?
- **Error Rate**: la procedura ha un tasso d'errore noto?
- **Publication**: la procedura è stata pubblicata e peer reviewed?
- **Acceptance**: la procedura è accettata dalla comunità scientifica?

http://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-17.pdf

Open Source for D.F.

SFDumper (Selective File Dumper) nasce da un'idea mia e di Denis Frati, al fine di estrarre tutti i file di un certo tipo e cercare le keywords tra essi.

Nel 2008 finisce in questo libro:

Open Source for D.F.

link.springer.com/chapter/10.1007%2F978-1-4419-5803-7_8

Uscita dal servizio di... | Cracking WPA in 10 ... | 联通iphone不越狱... | E-Evidence Informat... | sep-history-viewer -... | digitalforensicssolut... | Cerchiam

Springer Link

Sign up / Log in | English | Acade

Search

Home • Contact Us

» Look Inside » Get Access

Find out how to access preview-only content

2010, pp 117-124

Selective File Dumper

Nanni Bassetti, Denis Frati

Purchase on Springer.com
$29.95 / €24.95 / £19.95*
Buy now

Buy this eBook
* Final gross prices may vary according to local VAT.

» Get Access

Share

Abstract

During a computer forensics investigation we faced a problem how to get all the interesting files we need fast. We work, mainly, using the Open Source software products and Linux OS, and we consider the Sleuthkit and the Foremost two very useful tools, but for reaching our target they were too complicated and time consuming to use. For this reason we developed the Selective File Dumper, a Linux Bash script which makes it possible to extract all the referenced, deleted and

m a keyword search, in a simple way.

ajax.googleapis.com...

Open Source for D.F.

Raw2FS – nasce nel 2009, serve a recuperare il nome di un file a partire da un numero di offset in bytes ed effettuare delle ricerche per keywords.

Nel 2011 è finito in questo libro:

Open Source for D.F.

https://www.novapublishers.com/catalog/product_info.php?cPath=185_232_235&products_id=23887

Uscita dal servizio di... | Cracking WPA in 10 ... | 联通iphone不越狱... | E-Evidence Informat... | sep-history-viewer -... | digitalforensicssolut...

ACCOUNT | VIEW CART

NOVA Publishers

Home | Books | Series | Journals | Reference | eBooks | Information | Sales | Imprints | for Authors

» Science and Technology » Computer Science »

Horizons in Computer Science Research. Volume 3

Editors: Thomas S. Clary

Book Description:
This book presents original research results on the leading edge of computer science research. Each article has been carefully selected in an attempt to results across a broad spectrum. (Imprint: Nova Press)

Table of Contents:
Preface

Open-Source Software for Computational Neuroscience: Bridging the Gap between Models and Behavior
(Massimiliano Versace, Department of Cognitive and Neural Systems, and
Center of Excellence for Learning in Education, Science, and Technology
Boston University, Boston, Massachusetts)

RAW2FS and Open Source Tool from a Need to the Idea
(Nanni Bassetti, ISSA Member, Italy)

A Novel Middleware Architecture for Ubiquitous Healthcare Applications
(Mangal Sain, Hoon-Jae Lee, Dept. of Ubiquitous IT, Graduate School of Design & IT, Dongseo University, Busan, Kor

Open Source for D.F.

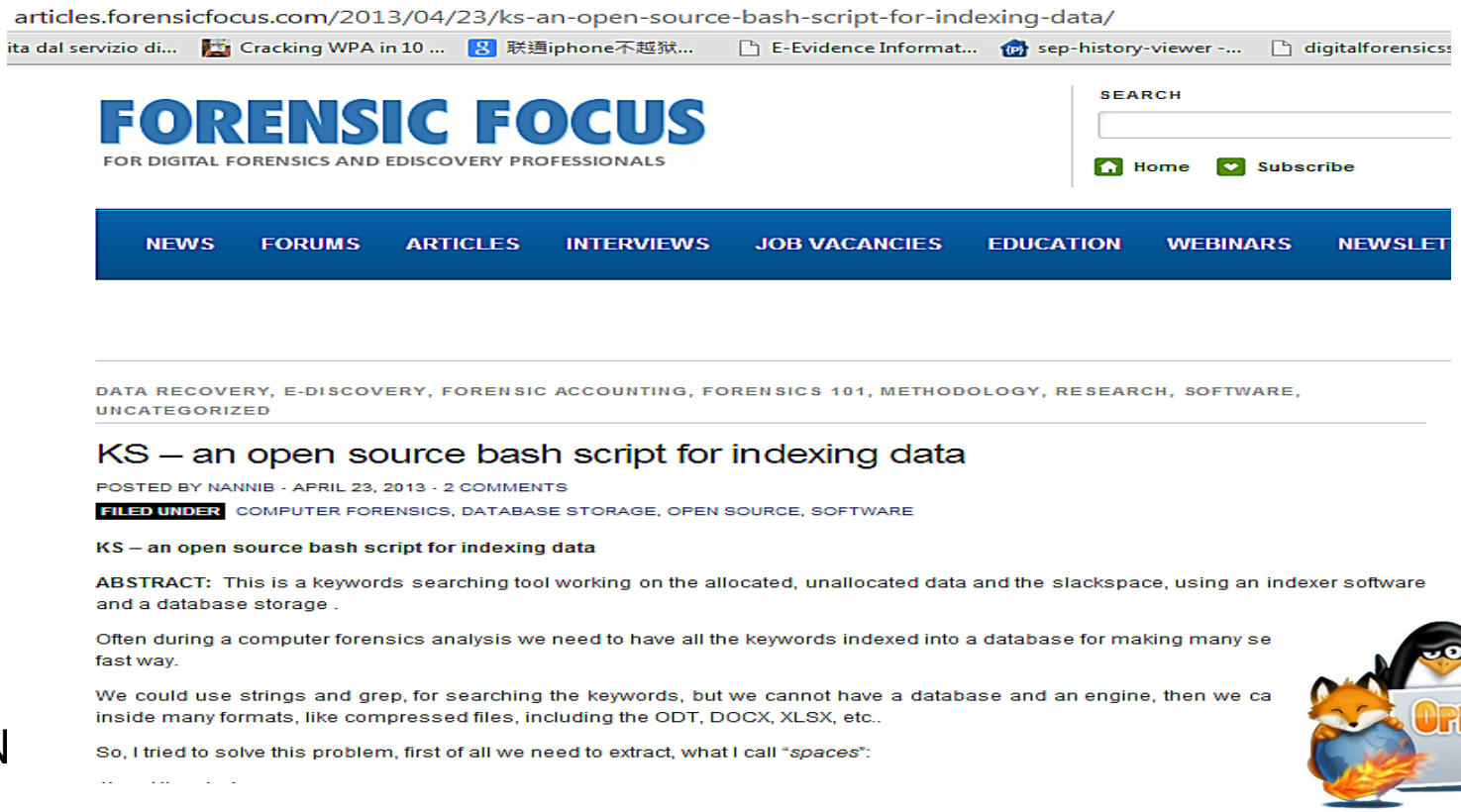
NBTempo – nasce nel 2011, una GUI per creare timeline basata su Sleuthkit

Nel 2012 è finito su HTML.IT:

Open Source for D.F.

KS – nasce nel 2012, indicizza tutto in db...vedremo in seguito altre features...

Nel 2013 è finito su ForensicFocus.com:



N

Open Source for D.F.

ISSA | The Global Voice of Information Security

ISSA Journal | September 2009

The $LogFile and Device Alteration: An experiment

By Nanni Bassetti – ISSA member, Italy Chapter

By this experiment we can affirm that if a computer investigator connects an NTFS drive for duplication without using a write blocker and without browsing it, the drive will be modified,

Open Source for D.F.

Fuori slides vedremo i sorgenti di questi tools e commenteremo, ma il senso è che a volte programmini/oni sviluppati in proprio possono risolvere tanti problemi, a volte bastano pochi giorni, per i tool più complessi magari ci vogliono mesi, ma la soddisfazione di automatizzare tante operazioni, aver creato e...non aver speso soldi...è IMPAGABILE!! :-P

```
cat system7.csv | grep -f events.txt | awk -F "," '{print $2,$4}' | sed
's/ 13$/ Off/'| sed 's/ 12$/ On/' | sed 's/ 42$/ Sleep/' | sed 's/ 1$/
Awake/'| sed 's/ 41$/ Crash/'
```


Open Source for D.F.

TESTI SACRI

http://www.linuxleo.com/- B. Grundy

http://www.amazon.com/exec/obidos/ASIN/0321268172/ (file system forensic analisys) B. Carrier.

Digital Forensics with Open Source Tools:

Using Open Source Platform Tools ..

Di Cory Altheide,Harlan Carvey

Conclusioni

Arrivederci e buona caccia! ☺

CONTATTI

NBS di Nanni Bassetti

Information Technology Consultant

http://www.nannibassetti.com

E-Mail: digitfor@gmail.com

Cell. +39-3476587097