Computer Forensic

in chiave open source

Giuseppe Augiero

Augiero.it

Agenda

- La scienza.
- Le procedure.
- Open Source.
- I tool comuni e forensi.
- Aspetti complementari.

Augiero.it

La scienza

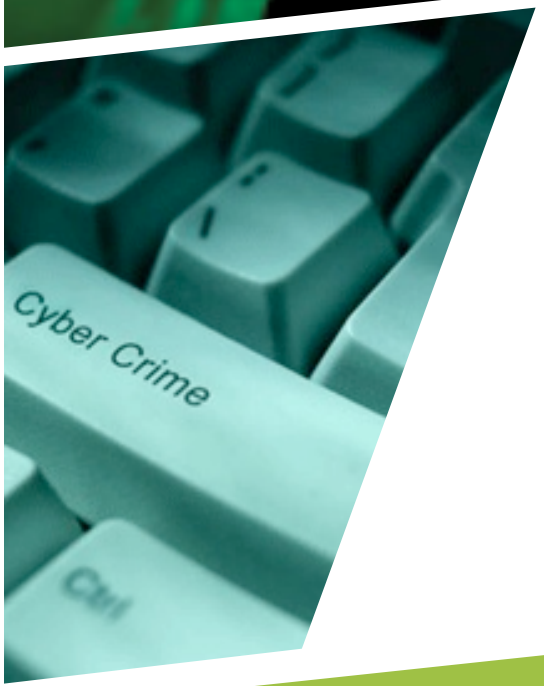
19 gennaio 2011 - La Limonaia - Pisa - Giuseppe Augiero - talk @ augiero.it

Augiero.it

Computer Forensic

- L'informatica forense è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico.

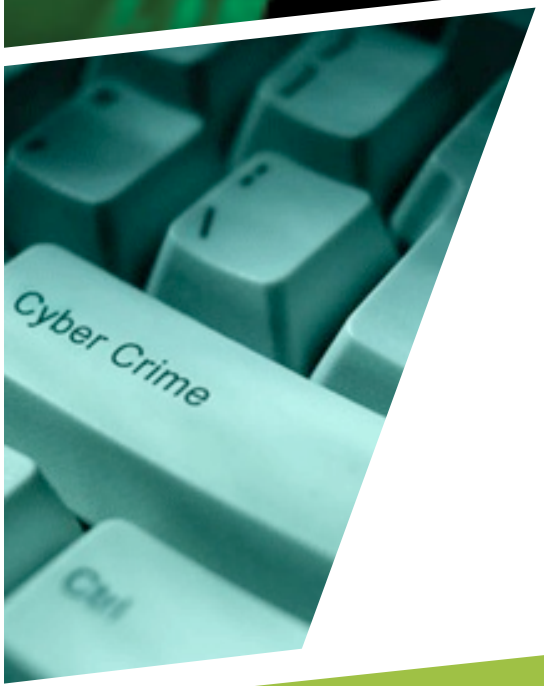
Augiero.it



Come nasce?

- E’ una disciplina di recente formazione.
- Nasce intorno ai primi anni 80 ad opera dei laboratori della FBI.
- Spesso viene erroneamente identificata come una parte dell’ IT Security.

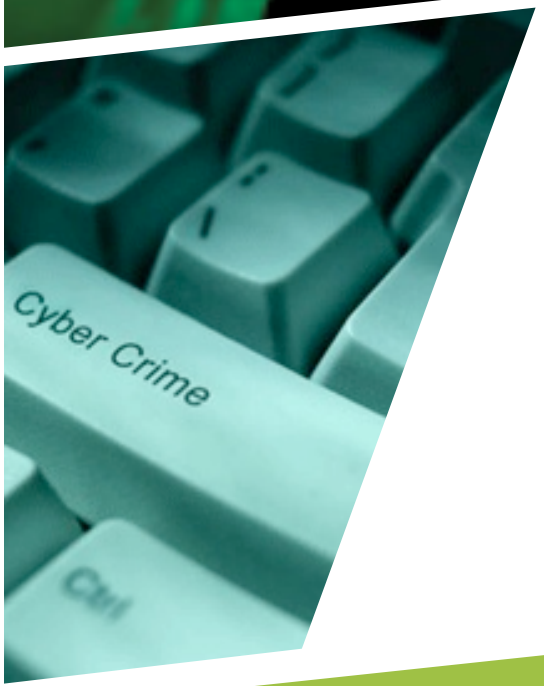
Augiero.it



Campi forensi

- Computer Forensic.
- Network Forensic.
- Software Forensic.
- Live System Forensic.

Augiero.it



Cosa permette?

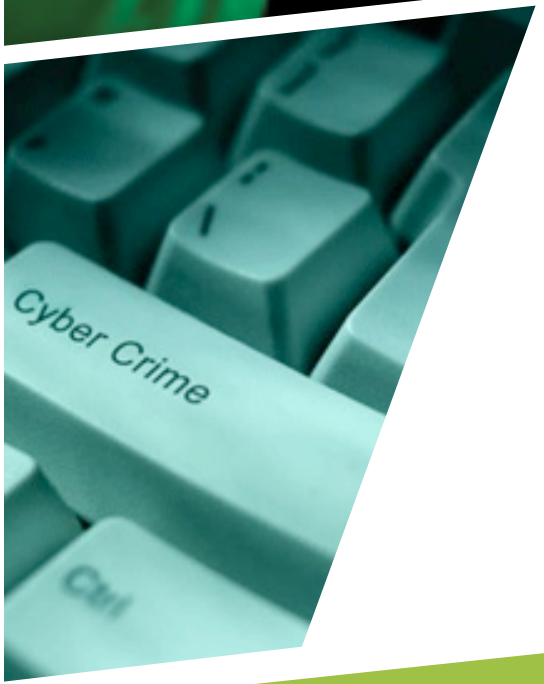
- Aiuta a ricostruire eventi passati e attività svolte.
- Mostra l'uso e l'abuso di infrastrutture IT.
- Mostra segni di violazione della normativa o di attività illecite.
- Permette di dimostrare possesso e gestione dei dati digitali.

Augiero.it

IT Security

- Esiste un filo di collegamento tra il mondo della sicurezza informatica e quello della informatica forense.

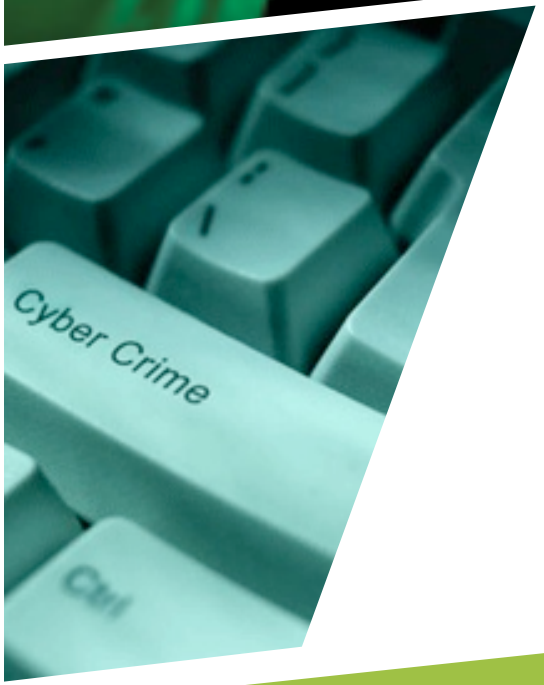
Augiero.it



Normativa

- Esiste una normativa di riferimento che disciplina le attività della computer forensic.

Augiero.it



Reati

- Reati informatici.
- Reati non informatici in cui sono stati utilizzati mezzi tecnologici.

Il percorso

Augiero.it

Attività

- Individuazione.
- Acquisizione.
- Analisi.
- Valutazione.

Augiero.it

Individuazione

- Riconoscere quali dati acquisire.
- Spegnere il prima possibile i sistemi.

Augiero.it

Difficoltà

- Facile da distruggere.
- Variazione dei timestamp.
- Modifica dei file.
- Traffico di rete “effimero”.

Augiero.it

Ripetibilità

- Tutte le operazioni effettuate durante una attività di computer forense devono essere controllabili e ripetibili.

Acquisizione

- L’acquisizione delle informazioni deve avvenire attraverso una operazione di “bit stream image”.
- Non è corretto effettuare una semplice copia del contenuto del file system.

Acquisizione (II)

- L'acquisizione è necessaria in quanto l'attività di analisi può essere effettuata unicamente sui dischi di copia e mai sugli originali.

Augiero.it

Validazione

- Occorre calcolare l'hash dei dischi "originali" e delle copie per validarne la perfetta corrispondenza.

Augiero.it

Intercettazione

- Una seconda modalità di acquisizione dei dati può essere rappresentata dall'intercettazione.
- E' l'unico modo per analisi di "live system".

Augiero.it

Analisi

- Attraverso l'analisi dei dati acquisiti si va in cerca in prove utili per il caso.
- L'analisi avviene tipicamente in laboratorio e può richiedere anche molte ore di lavoro.

Augiero.it

Valutazione

- Le prove acquisite vanno valutate.
- E’ una delle attività più complesse e lunghe dell’intera operazione.

Augiero.it

Open Source

19 gennaio 2011 - La Limonaia - Pisa - Giuseppe Augiero - talk @ augiero.it

Augiero.it

Open Source

- Il mondo dell'open source offre una ampio gamma di tool e software che possono essere di aiuto al mondo della computer forensic.
- I comandi standard di Linux possono permettere l'acquisizione e l'analisi dei dati,mentre software open forensi aiutano nelle attività di routine.

Augiero.it

Think different

- Per risolvere un problema o per riuscire ad effettuare una attività non canonica può capire che occorrà vedere ed analizzare la questione da un punto di vista differente.

Augiero.it

Semplicità

- Nel puro stile Unix le soluzioni si trovano utilizzando comandi semplici e spesso concatenati gli uni agli altri.

My Soft

- Con il mondo Linux e open source è facile scrivere uno script secondo le proprie esigenze o migliorare le caratteristiche di un software (open) già esistente in modo da realizzare tool ad hoc.

Inalterabilità

- I prodotto Open Source rispondono a pieno titolo alla necessità di inalterazione della prova acquisita.
- E’ possibile compilare, verificando i sorgenti, i prodotti open source utilizzati per l’indagine.

Augiero.it

I tools

Augiero.it

Disk Dumper

- La copia “bit a bit” per l’acquisizione delle prove può essere effettuata con il comando **dd**.

Traccia zero

- La traccia zero può essere utilizzata dai dischi fissi per parcheggiare le testine, per questo motivo normalmente non è usata per immagazzinare dati.
- Buona parte delle partizioni inizia dal settore 63.
- Abbiamo circa 30Kb di spazio che può essere utilizzato.

Augiero.it

Mount

- Linux riesce a gestire un grande numero di file system.
- Il file system può essere montato in read-only.
- E’ possibile usare fuse.

Mount

- Linux riesce a gestire un grande numero di file system.
- Il file system può essere montato in read-only.
- E’ possibile usare fuse.

Raid

- Un qualsiasi sistema Linux permette la gestione di dischi in raid (0-1-5).
- Senza il supporto raid è impossibile leggere i dischi (raid 5).
- Il tool per gestire il raid prende il nome di **mdadm**.

Hexedit

- Attraverso hexedit è possibile visualizzare in esadecimale qualsiasi file, testuale o binario, presente sul file system

Data Hiding

- Può capitare che spesso alcuni dati vengano letteralmente nascosti nel file system in modo da proteggerli da occhi indesiderati.
- Ecco alcune tecniche (NTFS):
- Bad block.
- Sparse attribute.
- Boot sector.

Augiero.it

Find

- Il comando find cerca all'interno di una directory, anche in maniera ricorsiva, la presenza di un determinato file.
- E' possibile cercare attributi di un determinato file.

Augiero.it

Grep

- Il comando grep permette di effettuare ricerche all'interno di file di un particolare pattern.

Diff

- Il comando diff confronta il contenuto di due file e mostra in output le differenze.

md5sum

- Il comando md5sum permette di calcolare l'hash md5 di un qualsiasi file.

Dsniff

- Dsniff rappresenta un vero coltellino svizzero per lo sniffing e l'analisi di rete.
- Ottimo per l'utilizzo in contesti analisi live.

Ettercap

- Sniffer evoluto che permettere l'analisi del traffico di rete.
- E' possibile recuperare password anche se all'interno di uno stream ssl.

Augiero.it

Tshark

- Versione command-line di Wireshark.
- Permette l'analisi dei flussi di rete.
- Veloce e minore uso di risorse.

Augiero.it

I forensic tools

19 gennaio 2011 - La Limonaia - Pisa - Giuseppe Augiero - talk @ augiero.it

Augiero.it

Dcfldd

- Sviluppato da Us. Defense Forensic Lab.
- Basato sul tradizionale dd.
- Offre funzionalità di conservazione delle prove, gestione degli errori e il controllo di quanto acquisito.

Sleuthkit suite

- Sviluppato da Brian Carrier.
- Insieme di tool per l'analisi e il recupero di informazioni di:
- disk layout, partizioni.
- file system, directory, file.
- timestamps.
- files cancellati o spazio non allocati.

Augiero.it

Autopsy

- Sviluppato sempre da Brian Carrier.
- Interfaccia web di front-end er:
- la gestione dei casi forensici
- analisi attraverso i sleuthkit suite.

Foremost

- Basato su scapel.
- Permette di effettuare il “data carving”.
- Analizza l’intestazione e il footer di qualsiasi file con formato conosciuto.
- Ottimo per analizzare dischi di swap, dischi corrotti, traffico di rete.

Augiero.it

PyFlag

- Tool grafico per l'analisi dei log.
- L'interfaccia e' di tipo web-based.
- Permette l'analisi di:
- disk device e disk image.
- file che contengono la cattura di traffico di rete.
- log.

NSRL Database

- National Software Reference Library.
- E’ un database di hash che indentificano file provenienti da software “conosciuto”.
- Può essere usato per escludere i “file buoni”.

Md5deep

- E’ una sorta di md5sum evoluto.
- Supporta non solo md5 ma anche sha-1, sha-256, tiger, mulinello.
- E’ possibile utilizzarlo in maniera ricorsiva.

Caine

- Live cd.
- Progetto Italiano.
- Continene svariati tool open source per l'analisi forense.
- Permette una generazione semi automatica del report finale.

Augiero.it

DeftLinux

- Distribuzione linux.
- Progetto 100% Italiano.
- DeftLinux Extra.

Augiero.it

Aspetti complementari

19 gennaio 2011 - La Limonaia - Pisa - Giuseppe Augiero - talk @ augiero.it

Augiero.it

Net Forensic

- Cosa è la Net Forensic.
- Problema della validazione del dato in transito.
- Utilizzo di Ids.
- Intercettazione dei dati.
- Problemi di gestione dei flussi.

Augiero.it

Steganalisi

- E’ il processo mediante il quale è possibile affermare se un dato contiene nascosti dati steganografici.
- La steganografia permette di nascondere l’esistenza di una informazione, ma non nasconde l’informazione.

Augiero.it

Non convenzionale

- Ormai i nostri dati possono risiedere non solo su pc ma anche su memory card o ssd o quant'altro presenti su letturi musicali, cellulari, smartphone, macchine fotografiche e quant'altro.
- Come acquisire queste informazioni?

Augiero.it

Concatenazione di eventi

- Come sono state eseguite determinate azioni?
- Qual è l'ordine?
- Come è avvenuto un'attacco informatico?

Augiero.it

Augiero.it


GRAZIE
www.augiero.it
giuseppe@augiero.it
Augiero.it

Licenza di utilizzo