Ordine degli Ingegneri di Pisa
Talent Garden Pisa
Via Umberto Forti 6, Montacchiello (PI)
10 Marzo 2017 – 14:00-19:00

IISFA European Chapter

Introduzione alla Computer Forensics

CSI (o meglio RIS) demistificati

Marco A. CALAMARI – marco.calamari@ordineingegneripisa.it

IISFA - Information Systems Forensics Association: Italian Chapter

Il vostro anfitrione

https://www.linkedin.com/in/marcocalamari/

- Marco Calamari, classe 1955, ingegnere nucleare, si cimenta a rotazione tra attivita' di consulenza tecnica, editoriali e di formazione.
- Qualche sigla: IISFA, AIP, Opsi.
- Appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.
- Fondatore del Progetto Winston Smith e del Centro Hermes per la Trasparenza ed i diritti digitali.
- In concorrenza con i veri giornalisti, dal 2003 scrive su Punto Informatico ed altrove la rubrica settimanale "Cassandra Crossing", che e' arrivata alla 400ma puntata … (www.cassandracrossing.org)

L’obbiettivo di oggi

La computer forensics (autopsia informatica) e' una disciplina tecnica come tante altre affrontate quotidianamente da ingegneri, sia come tecnici che come consulenti di parte o del Giudice.

Vista come attivita' di massimi esperti hacker, ormai immancabili in qualsiasi fiction televisiva, richiede passione, anni di studio e di esperienza.

Ma affrontata a livelli ordinari puo' essere rapidamente ripulita dalla patina di irraggiungibilita' e rivelarsi tranquillamente alla nostra portata.

Quindi parleremo di ...

Prima parte

- La realtà romanzesca e quella tecnica.
- Elementi di informatica e crittografia
- Incidenti informatici e tracce informatiche

Seconda parte

- Hardware e software necessari: niente mutuo, Ebay e FOSS sono nostri amici

Terza Parte

- Aspetti giuridici; prove informatiche, ripetibilita' e catena di custodia.
- La dimensione tempo; timeline
- I problemi pratici; il 90% delle volte ....
- Dalla parte del CTU; tipologie di quesiti.

Quarta parte: Caso di studio
acquisizione e carving di un laptop

Standard Disclaimer

IISFA European Chapter

Le informazioni contenute in questa presentazione, se male utilizzate, possono produrre effetti negativi come, ma non limitati a:

- **Perdita di dati**
- **Cancellazione di file**
- **Blocco del computer**
- **Distruzione di informazioni**
- **Scongelamento del frigorifero**
- **Rottura di relazioni sentimentali**

(aggiungete altri vostri incubi a piacere...)

QUINDI, OCCHIO!

Io, comunque, vi avevo avvertito


International Information Systems
iisfa
Forensics Association
IISFA
European Chapter

Prima parte

Chi dice le cose giuste?

IISFA European Chapter

RIS contro Pubblicita'

Hardware e software necessari

TEST:
Prerequisiti ad un corso di computer forensics?

1)I file messi nel cestino sono cancellati?
2)I file messi nel cestino svuotato sono cancellati?
3)I file di un computer reinstallato sono cancellati?
4)I file di un hard disk formattato sono cancellati?
5)I file di un disco formattato a basso livello sono cancellati?
6)I file di un hard disk portato sopra il punto di Curie sono cancellati? (Non chiedetemi cos'e' il punto di Curie per favore)
7)I file di un hard disk tritato in pezzi cosi fini che passino tutti da un setaccio di 3 mm. sono cancellati? (non e' uno scherzo ma uno standard DoD)

Esempio di file cancellati

IISFA
European Chapter

Esempi di file NON cancellati

IISFA
European Chapter

Incidenti e tracce

Quale e' la differenza principale?

Risolvere un incidente informatico per il consulente implica recuperare allo stato originario un sistema informatico danneggiato (in hardware e/o software) o "cancellato".

Trovare tracce informatiche per il consulente implica recuperare alcune informazioni di interesse da un sistema informatico danneggiato (in hardware e/o software) o "cancellato".

Quale e' la cosa piu' difficile?

Incidenti e tracce 2

Ci sono altre differenze

Risolvere un incidente informatico e' una attivita' tecnica che spesso si puo' comprare "un tanto al chilo".
La controparte e' un cliente che deve essere soddisfatto nel modo piu' veloce ed economico possibile.

Trovare tracce informatiche e' una attivita' tecnica in cui conta non solo il risultato finale, ma anche tutto il procedimento con cui lo si e' ottenuto.
La controparte e' un avvocato od un giudice che devono avere risultati utili e poterli utilizzare.

Torneremo su questi aspetti nella terza parte

Informatica Forense

Possiamo darne una definizione?

Tentiamo …

> ***"L'insieme delle metodologie applicabili per la ricerca e la conservazione di evidenze di natura digitale utilizzabili per svolgere attività investigativa o come prova in un processo."***

… in quale ambito?

Non pensate solo ai computer, ma anche a:

- **Penne USB**
- **Dischi esterni**
- **Tablet**
- **Navigatori GPS**
- **Lettori Mp3**
- **Cellulari e Smartphone**
- **Macchine fotografiche**
- **Automobili**
- **IoT – Pupazzi per bimbi, Nabaztag, Echo, SmartTV**

Tutto molto spesso connesso ad internet in vari modi (ADSL, GSM, UMTS, WiFi, Radio)

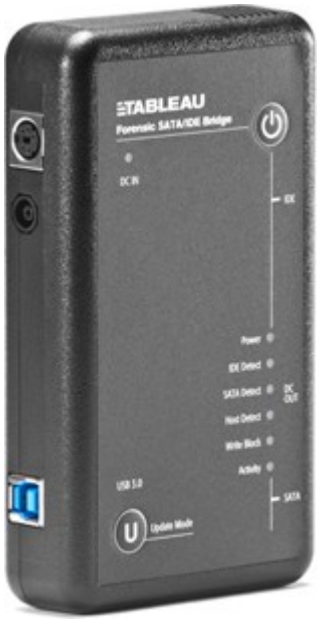
Seconda parte

Hardware e software

Per lavori complessi quali:

- ***estrazione dati da telefoni cellulari***
- ***raccolta automatica di dati specifici (foto...)***
- ***recupero dati da hardware danneggiato***
- ***estrazione dati da computer accesi***
- ***acquisizione rapida di RAID, NAS etc.***

Servono parecchi hardware e software commerciali, che hanno costi dell'ordine di 1 – 10 k€ l'uno.



Hardware e software 2

D'altra parte i lavori "semplici" sono frequenti, e per questi i prezzi stracciati dell'elettronica cinese, l'e-commerce ed il software libero (FOSS) ci vengono in aiuto; i numeri allora cambiano molto.

Ribadiamo pero' un concetto ben noto: si impara a camminare e poi a volare, dal semplice al complesso.

L'uso esclusivo che faremo di software libero non significa che per il fini dell'analisi forense sia migliore o peggiore di quello proprietario, ne' e' ispirato a considerazioni filosofiche.

Il motivo banale e' che il suo uso abbassa, anzi quasi azzera la soglia di ingresso economica per chi vuol crescere in questa direzione … e non e' poco!

Hardware e software 3

Lista dei tool per un laboratorio forense di base

1)Un desktop/laptop dotato di porte **USB3**

2)Un disco esterno USB3 da **1 TB** o piu' (50-80 €)

3)Un DVD-RW USB esterno (se il laptop e' senza - 25€)

4)Un cavo adattatore SATA-EIDE to USB3 (35€)

5)Una distribuzione Linux per attivita' forensi (0€)

Con 150 € circa si puo' preparare un "laboratorio" in grado di gestire i casi piu' comuni (e piu' frequenti) di perizie tecniche informatiche.
Questi oggetti si comprano facilmente su eprice.it, ebay.it ed amazon.it; occhio pero' a leggere bene le caratteristiche tecniche e confrontare i prezzi.

Hardware e software 4

Il laptop USB3 e magari anche multicore, perche'?

La durata del processo di estrazione e lettura di un hard disk dipende dalla dimensione dell'hard disk (non la controllate mica voi!), se va bene sono 320 GigaByte, se va male anche uno o piu' Terabyte.
Un'interfaccia USB2 se siete fortunati permette velocita' di 20/30 MegaByte al secondo, USB3 vi permette di arrivare a 100 MegaByte al secondo.
Se pensate che andare quattro volte piu' veloci, non sia indispensabile facciamo due conti per un hard disk piccolino, da solamente 320 GigaByte.

Con USB2 320.000/ 25/3600 = tre ore e mezzo
Con USB3 320.000/100/3600 = 53 minuti

Hardware e software 5

E multicore, perche'?

Molte fasi dell'analisi forense, spesso da eseguire ciascuna piu' volte, sono CPU bound, e quasi sempre parallelizzabili.

Software come Bulk Extractor, sui multicore, sfruttano al massimo questo parallelismo, ed i tempi si riducono in proporzione inversa all'aumentare dell numero di core, ed ovviamente anche della velocita' di clock.

Bulk Extractor ad esempio vi comunica ad ogni run se il collo di bottiglia e' stato la velocita' del disco od il numero di core.

Hardware e software 6

Ho un pc fisso, USB2, monocore e lento; no way?

Per fortuna no, in molti casi potrete lavorare ugualmente bene, sopperendo con un allungamento dei tempi di analisi e con un consumo spropositato della vostra pazienza.
Ma potrete lavorare. **Anche un computer fisso va bene, il laptop e' solo molto comodo se dovete svolgere operazioni fuori sede.**

Una importantissima raccomandazione finale.

Se usate non un laptop dedicato senza dati ma il vostro prezioso laptop di lavoro con dentro tutti i vostri preziosi dati, fate un backup di tutto il disco (una bella immagine forense compressa!) e copiatelo su un disco esterno.
E' vero che una distribuzione live non tocca l'hard disk, ma c'e' l'elemento umano (voi). Un errore di montaggio e smontaggio disco, un comando di scrittura sbagliato e vi potete piallare tutto in una frazione di secondo……

Cavo SATA-EIDE to USB3

IISFA European Chapter

Cavo SATA-EIDE to USB3

IDE 44Pin for 2.5"HDD

IDE 40Pin for 3.5"HDD

IDE 40Pin for CD-ROM

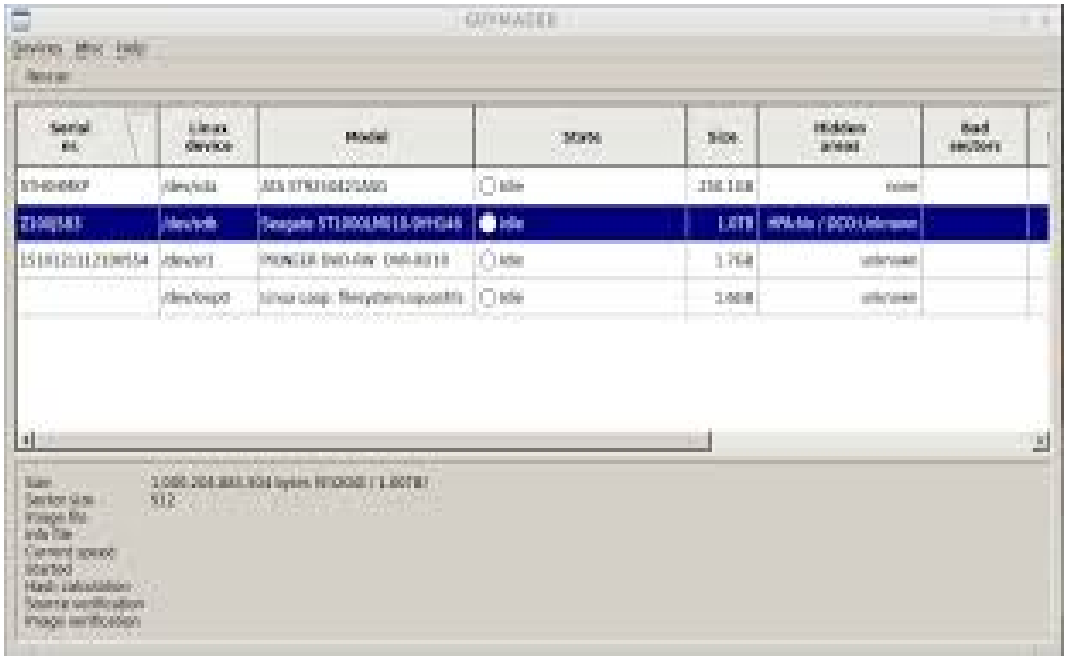
For 3.5" SATA HDD

For 2.5" SATA HDD

Software per copia forense

IISFA European Chapter

- Il classico dd e la sua versione speciale per recupero di supporti con settori danneggiati ddrescue e dd_rescue
- Guymager, interfaccia grafica per il cloning dei device in vari formati (EWF, AFF, RAW)
- Cyclone, tool a linea di comando per copie in formato EWF e RAW



Software per Analisi e Carving

Sono programmi che analizzano il contenuto del disco sia via file system sia accedendo direttamente al supporto senza usareil file system):

1) **Tool generici per l'esame del contenuto dei supporti informatici**
   - **The Sleuth Kit + Autopsy**
   - **Bulk extractor**
2) **Tool specifici per tipo di analisi**
   - **Analisi della navigazione internet**
   - **Analisi della posta elettronica**
   - **Analisi chat, immagini, …**
3) **Tool per il recovery di file e partizioni**
   - **Testdisk**
   - **Photorec**
   - **Foremost**
   - **Scalpel**

Un problema ...

“Ma io mi ritrovo davvero male con Linux e comandi arcani da battere.”

Tranquillo, la risposta c’e’, ed e’ ancora Linux; ecco a voi ...

Distribuzioni GNU/Linux forensi


International Information Systems
iisfa
Forensics Association
IISFA
European Chapter

Terza parte

Aspetti giuridici

Il ruoli in cui un esperto di computer forensics si puo' trovare, escludendo quello atipico di "recuperatore" di dati per fidanzate/i, amici o meglio clienti paganti sono:

CTP – Consulente tecnico di parte; il rapporto e' con un privato, come una consulenza normale.

CTU – Consulente tecnico d'ufficio; il rapporto e' con la magistratura, e quindi il ruolo e' normato da appositi articoli, mentre le operazioni tecniche differiscono poco da una equivalente consulenza. La nomina puo' essere declinata.

APG – Ausiliario di polizia giudiziaria; il rapporto e' con la polizia giudiziaria, che puo' nominare di imperio chiunque. La nomina di APG puo' includere il partecipare ad operazioni di polizia. E' un aspetto importante.

Aspetti giuridici 2

Indipendentemente dal ruolo assunto, ma particolarmente nel caso di CTU ed APG in campo penale, diventano aspetti primari il confezionamento, la conservazione e la trasmissione delle evidenze informatiche, che assumono il ruolo di prove.

Argomenti quali:

- accertamento ripetibile o non ripetibile
- catena di custodia della prova

diventano fondamentali operando come CTU od APG perche' possono rendere vana la tecnicamente piu' perfetta delle consulenze.
In un corso introduttivo non e' possibile trattare questi aspetti, che da soli richiederebbero un corso a parte, piu' lungo e meno divertente.

Nomina e giuramento

Nel caso siate nominati CTU, un giudice vi convochera' ad una apposita udienza chiamata appunto "Nomina e giuramento CTU".
In questa sede vi si chiedera', dopo un'illustrazione che puo' andare da nulla ad un'ora di discussione con avvocati e giudice, se accettate l'incarico.
In qualche caso dovrete pronunciare la breve formula del giuramento, di solito incollata alla scrivania.
Fondamentale e' la formulazione del quesito a cui dovrete rispondere.
Se ve lo trovate gia' confezionato, i giochi sono fatti; dovrete rispondere a quello, per quanto fumoso, contraddittorio e poco comprensibile sia.
Se avrete la fortuna di poter discutere del quesito, la possibilita' di guidarne la formulazione in modo che sia chiaro e centri il problema e' impagabile.
Fatene tesoro ma senza esagerare.

Tipi di analisi

Indipendentemente dal caso su cui si e' chiamati ad operare, esiste un numero limitato di tipologie di analisi da eseguire che compaiono nel 90% delle consulenze.

- **Acquisizione di una immagine forense**
- **Recupero di particolari file da un'immagine forense**
- **Interpretazione di particolari file estratti, come archivi di posta elettronica, documenti corrotti, database, file di log ...**
- **Recupero di informazioni cancellate (Carving)**
- **Analisi temporale degli eventi (Timeline)**

Quarta parte

Un caso di studio

Quale potrebbe essere un caso tipico ma non banale di analisi forense alla nostra portata?

Analisi di un laptop alla ricerca di documenti riservati che potrebbero essere stati inviate per posta e/o cancellati

Step da eseguire

- **Documentazione fotografica del laptop**
- **Creazione dell'immagine forense del disco**
- **Estrazione dei file di interesse**
- **Elaborazione di file particolari (posta elettronica)**
- **Carving alla ricerca di file cancellati**
- **Creazione di una Timeline degli eventi**

Acquisizione immagine forense

IISFA European Chapter

Acquisizione immagine forense

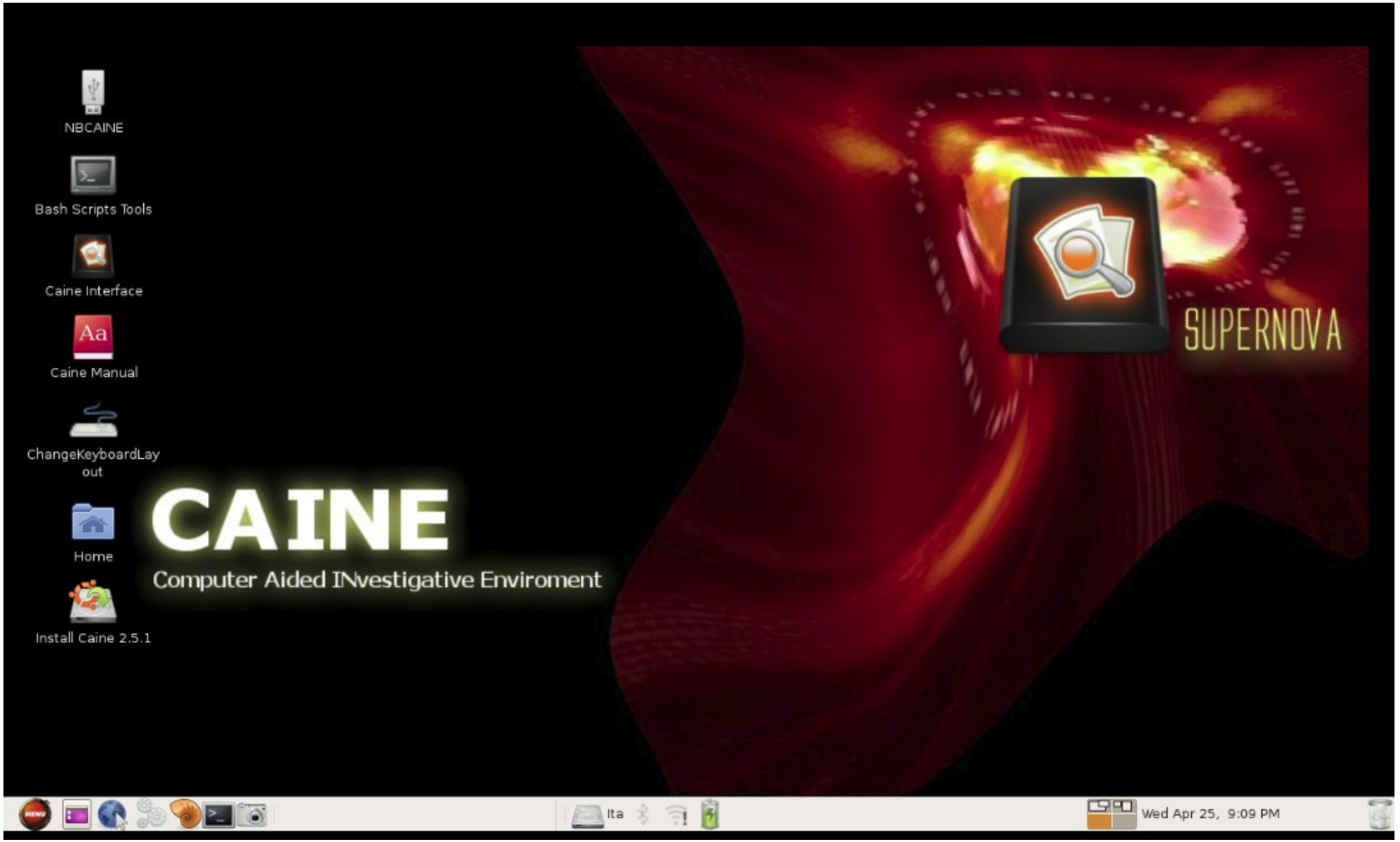
IISFA European Chapter

Acquisizione immagine forense

IISFA European Chapter

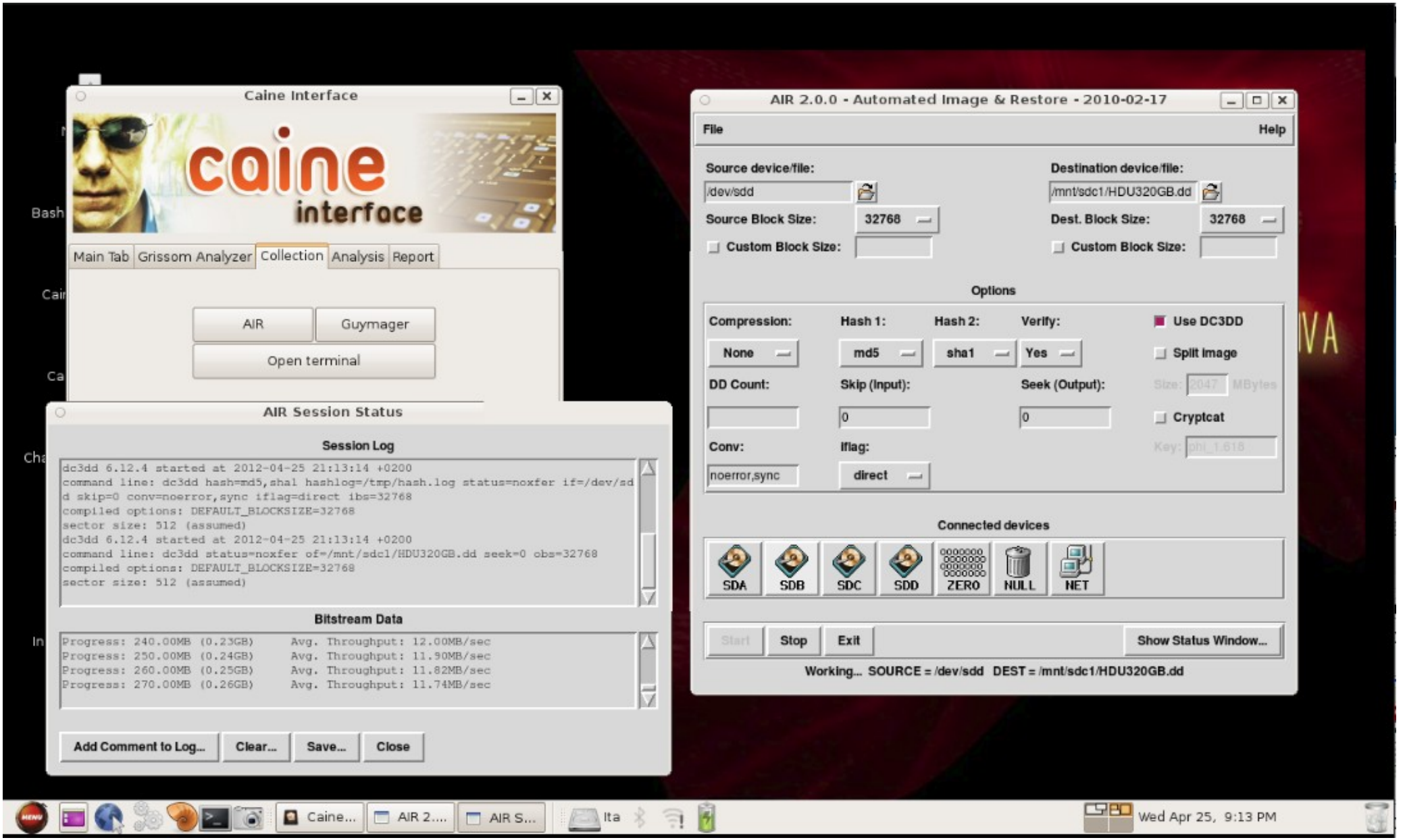
Acquisizione immagine forense

IISFA European Chapter



Acquisizione immagine forense

IISFA European Chapter



E adesso …

Lo facciamo davvero!

IISFA European Chapter

Grazie per l'attenzione

Q&A time

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+

PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698
DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B
Tel: (+39) 050 576031 Cell: (+39) 347 8530279
Fax: (+39) 050 7849817 Skype-Twitter: calamarim

+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ----------+