Modalità operative

Quali strumenti utilizzare ?

Esistono software commerciali riconosciuti e considerati attendibili dalle corti inglesi ed americane

Quail strumenti utilizzare ?

uno fra tutti:

EnCase® prodotto da Guidance Software

è utilizzato anche dalla Polizia di Stato

Quali strumenti utilizzare ?

Si pone però un problema:

"Quis custodiet ipsos custodies" ?

Computer Forensics

vs

Sicurezza Informatica

Computer Forensics
vs
Sicurezza Informatica

Un sistema è sicuro fino a quando non esiste un modo per violarlo.

L'acquisizione dei reperti informatici richiede la violazione, secondo alcune modalità, del sistema che è oggetto dell'analisi.

Computer Forensics vs Sicurezza Informatica

Un esempio:

il bug di PGP 7.0 individuato nel giugno del 2000

e l'acquisizione di dati da un archivio cifrato con questa versione di software

Computer Forensics vs Sicurezza Informatica

Ergo …

se un sistema è sicuro, non è possibile acquisirne alcun reperto.

L'acquisizione dei reperti informatici spesso richiede tecniche di hacking.

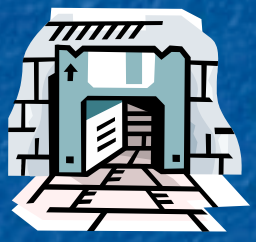
La sicurezza informatica intesa come…….

ONERE

adempimenti relativi alla normativa in materia di trattamento dei dati personali

donato@informaticaforense.it

La sicurezza informatica va intesa come…….



Opportunità

donato@informaticaforense.it

Illustrazione di alcuni casi reali

donato@informaticaforense.it

La Multinazionale:

Azienda multinazionale con sedi in tutto il mondo

- un dirigente si dimette senza alcun preavviso;
- un suo collega scopre casualmente che qualche giorno prima aveva copiato l'intera banca dati azienda utilizzando un disco esterno;

donato@informaticaforense.it

La Multinazionale:

Le fasi di accertamento tecnico:

- assenza di log
- mancanza di profili

La Multinazionale:

Le fasi di accertamento tecnico:

- poca sensibilità al “segreto” da parte dei dipendenti
- ICT e in particolare la sicurezza completamente affidata ad un fornitore esterno (outsourcing)

La Multinazionale:

Cosa è possibile imparare da questo caso:

se fossero state adottate le misure di sicurezza "idonee" previste dalla normativa, sarebbero conseguiti i seguenti vantaggi:

- maggiori elementi di riscontro per accertare e provare il comportamento del dipendente sleale;
- limitatazione del furto di dati;

La Tecnologica:

Azienda di 10 dipendenti specializzata nella meccanica di precisione:

- lamentavano che un'azienda concorrente spesso riuscisse ad anticipare le proprie mosse.

La Tecnologica:

Accertamenti:

- l'azienda aveva un server di posta elettronica all'esterno della rete aziendale
- le password di accesso a questo server erano molto deboli
- però la sensibilità alla "fuga di informazioni" dell'azienda era comunque alta

ergo….

La Tecnologica:

Invece come spesso accade la realtà supera la fantasia:

- ad insaputa dei titolari, "gli apparati di rete" erano stati predisposti per eseguire "l'assistenza remota" al server aziendale
- la fornitura di servizi di assistenza hardware e sui sistemi operativi è erogata da una piccola azienda locale

La Tecnologica:

Ulteriori aspetti:

•Il “concorrente” era cliente della stessa azienda di servizi informatici e aveva adottato la stessa modalità di “assistenza remota”!

ergo….

donato@informaticaforense.it

La Tecnologica:

Considerazioni:

• non fu possibile perseguire penalmente entrambi perché vi era carenza probatoria:

no misure idonee, no log, no prove

• diffidenza nei confronti dei fornitori

donato@informaticaforense.it

La Perfetta:

Multinazionale con più di 1000 dipendenti che opera nel IT, livelli di sicurezza ottimi:

- lamentano fughe di notizie dalla propria organizzazione, in particolare i contenuti di alcune mail, scambiate fra i componenti della dirigenza

La Perfetta:

Accertamenti:

- Struttura molto complessa ed articolata
- Livelli di sicurezza elevati sia a livello fisico che logico
- Elevata cultura della riservatezza

La Perfetta:

Accertamenti:

- la rete e le risorse informatiche dell'intera multinazionale avevano una struttura ad albero, cioè esisteva un servizio centrale che aveva delegato alcune funzioni a referenti locali nelle diverse sedi locali presenti nei vari Stati;
- il servizio di posta elettronica era affidato alla piattaforma Lotus Domino (Notes)

donato@informaticaforense.it

La Perfetta:

su Lotus Domino:

- Crittografia forte
- Necessità di avere una "chiave" oltre alla classica autenticazione utente + password

donato@informaticaforense.it

La Perfetta:

•Gli “amministratori di sistema” avevano l’autorizzazione in lettura delle mail di tutti

•I log non segnalavano nulla di anomalo

ergo….

La Perfetta:

Considerazioni:

• Non trascurare la sicurezza fisica:
- portatili
- nastri salvataggio (backup)

• diffidenza nei confronti di quelli che sono “DIO” sul sistema:

gli “amministratori di sistema”

Conclusioni

Adottare le misure idonee di sicurezza per ottemperare alla normativa sulla privacy sono un'opportunità per l'azienda.

Registrare il traffico di rete e qualsiasi altro dato per tali fini potrebbe rivelarsi in un secondo tempo molto utile

Conclusioni

Diffidare di coloro i quali hanno il completo controllo dell'infrastuttura informatica aziendale…

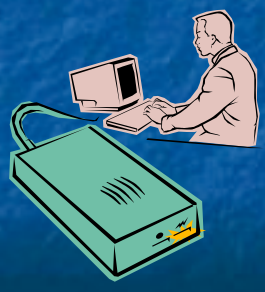
Soprattutto se vi hanno configurato il collegamento Bluetooth fra il cellulare e il portatile…..

Conclusioni

Se per i bilanci di un'azienda esiste la figura del commercialista e quella del certificatore del bilancio…..

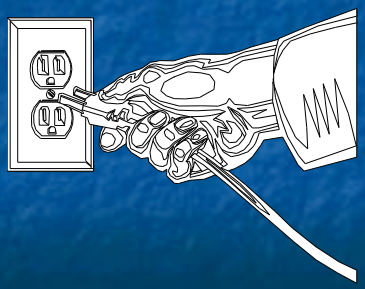
Analogamente anche per la sicurezza informatica sarebbe necessario un controllo incrociato dello stesso tipo altrimenti…..

Disk Forensics



L'acquisizione di un disco: come operare

Prima di acquisire il contenuto di un disco molti eseguono l'UNPLUGGING, cioè staccano la spina…



L'acquisizione di un disco: come operare

L'unplugging,

- rischia di danneggiare sensibilmente il sistema

- cancella irrimediabilmente la RAM, una risorsa importantissima

L'acquisizione di un disco: come operare

Inoltre, se sul sistema è presente un disco crittografato lo spegnimento del sistema renderà impossibile la lettura delle informazioni registrate sul disco stesso.

L'acquisizione di un disco: come operare

Invece, acquisire i dati senza spegnere il sistema comporta molti vantaggi in quanto sarà possibile:

- accedere ai dati;
- recuperare (addirittura) la password presente in RAM;
- acquisire eventuali dischi cifrati;
- acquisire altre informazioni volatili del sistema, come:
  - lo stato delle connessioni di rete
  - stato dei programmi in esecuzione
  - valori di registro del processore

L'acquisizione di un disco: come operare

Ma come si può accedere legittimamente ad un sistema senza conoscerne la password di amministratore ?

Usando tecniche di hacking, sfruttando falle di sicurezza presenti nel sistema per accedervi con i diritti di amministratore.

L'acquisizione di un disco: come operare

vanno attentamente documentate, registrate e riprese le operazioni che vengono eseguite, per evitare il ripudio dell'integrità e della paternità del reperto acquisito.

L'acquisizione di un disco: come operare

Gli strumenti:

Commerciali
- EnCase Guidance Software
- Safeback Forensics Intl

Freeware Opensource
- dd

L'acquisizione di un disco: come operare

Cosa fare:

Eseguire un copia integrale - bit per bit - del disco su un altro dispositivo;

- calcolare l'hash del disco sorgente e del disco copia e confrontarli, meglio se con la firma digitale
- creare almeno tre copie

L'analisi di un disco

analisi contestuale, utilizzando il sistema operativo più confacente e "lavorando" solo su una copia dei dati acquisiti.

L'analisi di un disco

Recupero di file nascosti o cancellati.

L'analisi di un disco

per "patter matching" ossia ricerca per sottostringa, sia all'interno dei file che sull'intera superficie del disco, cioè nella zona dati, slack, e cluster non utilizzati.

L'analisi di un disco

Analisi di frammenti di dati che possono appartenere a file di tipo non testuale es. immagini JPEG, o TIFF, oppure pezzi di brani MP3 o WAVE

L'analisi di un disco

Analisi di file generati da client di posta elettronica come Outlook

L'analisi di un disco

I file cifrati:

esistono dei metodi di cifratura "deboli" che si possono facilmente forzare con l'ausilio di programmi

L'analisi di un disco

Esempio:

Lotus Organizer®

Le prime versioni di Microsoft Word®

L'analisi di un disco

I file cifrati:

metodi di cifratura con chiavi corte 40 bit che si possono aggredire con attacchi a forza bruta che durano al massimo 30 40 giorni

L'analisi di un disco

Esempio:

Microsoft Word® 97, 2000, xp

Winzip 8.0®

L'analisi di un disco

I file cifrati:

metodi di cifratura forte che si possono aggredire con attacchi a forza bruta ma che non danno garanzia di risultato

L'analisi di un disco

I file cifrati:

in questi casi il punto debole è

l'uomo…

La valutazione del reperto

E' la fase in cui del reperto informatico vengono ponderati l'effettivo grado di:

- integrità

- autenticità

.

La valutazione del reperto

Come?
Prendendo in considerazioni i seguenti aspetti:

- chi ha potuto modificare il reperto

- in quale momento sarebbe stato modificato

La valutazione del reperto

Come?

Verificando la presenza di tracce che ne indicano eventuali alterazioni, mediante consultazione di:
- file di Log;
- file temporali;
- contenuto di slack

La valutazione del reperto

Analizzando la successione temporale degli eventi che sono accaduti sul sistema

La valutazione del reperto

Correlando gli eventi del sistema con

quelli di altri sistemi

La valutazione del reperto

Naturalmente tutte queste considerazioni vanno fatte anche per tutti i dati ed i sistemi esaminati !

Computer Forensics

Integrità

Autenticità

Quesiti

- analisi forense del Personal Computer di Paolo Tizio, al fine di determinare gli orari durante i quali il personal computer è stato utilizzato
- modalità di localizzazione di un dispositivo di telefonia mobile (cellulare) e individuazione delle aree geografiche di pertinenza delle singole celle

Quesiti

dalle conclusioni ottenute dall'attività di analisi forense dei reperti informatici e dalla localizzazione del dispositivo di telefonia mobile (cellulare) determinare un'unica successione di eventi spazio temporale

Analisi forense del Personal Computer di Paolo Tizio

- La funzionalità di generazione della "timeline"sul quale vengono annotate in ordine cronologico crescente tutte le operazioni di:
  - creazione
  - modifica
  - lettura di un file

  un vero e proprio giornale di bordo di tutte le operazioni che sono state eseguite sul personal computer

Il trattamento del reperto informatico eseguito dalla PG

"…Prima di lasciare i locali si è provveduto allo spegnimento del personal computer collocato nella stanza interessata dall'episodio delittuoso. Detto computer recava aperti il programma con l'uso del file Word "Parere bilanci di previsione 2003.doc" ed inoltre la cartella "Comune di Alberona". All'atto dello spegnimento, mediante il comando arresta sistema presente nel menu Strart/avvio, il programma in uso andava in crash "impossibile chiudere….". Pertanto veniva selezionata l'opzione "termina adesso" ed il sistema si arrestava mentre l'orologio presente sulla barra indicava le 22.19…"

Conseguenze

- 282 file con la data di ultimo accesso oltre le 14.00 del 13/05/2003
- 91 file con la data di ultima modifica oltre le 14.00 del 13/05/2003

Pertanto sono stati persi dati che sarebbero stati utili al fine di determinare le operazione eseguite sul PC di Paolo Tizio il giorno del suo omicidio

donato@informaticaforense.it

Analisi della timeline

Tizio\Part_1\NONAME-NTFS\Documents and Settings\cd\Dati applicazioni\Microsoft \Word\Salvataggio automatico di Parere bilancio Previsione 2003.asd>>ObjectPool>>_1139917589
13/05/2003 13.28

Tizio\Part_1\NONAME-NTFS\Documents and Settings\cd\Dati applicazioni\Microsoft \Word\Salvataggio automatico di Parere bilancio Previsione 2003.asd>>ObjectPool>>_1108541397
13/05/2003 13.28

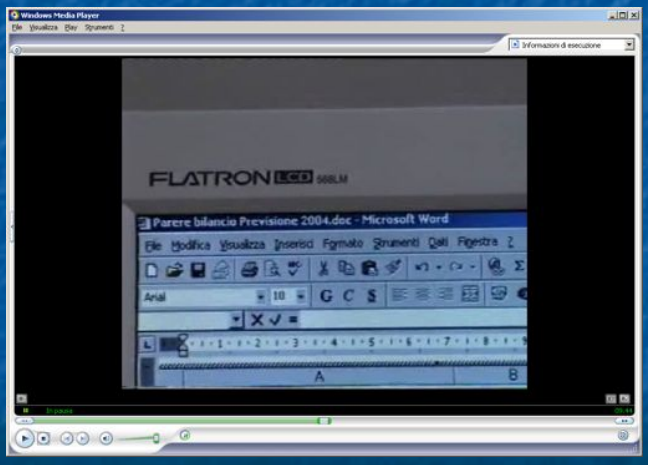
Tizio\Part_1\NONAME-NTFS\Documents and Settings\cd\Impostazioni locali\Temp \~WRF0001.tmp>>_1140254031
13/05/2003 13.29

Tizio\Part_1\NONAME-NTFS\WINDOWS\PCHEALTH\HELPCTR\DataColl \CollectedData_6427.xml
13/05/2003 13.33

Tizio\Part_1\NONAME-NTFS\[orphan]\RP281\RestorePointSize **13/05/2003**

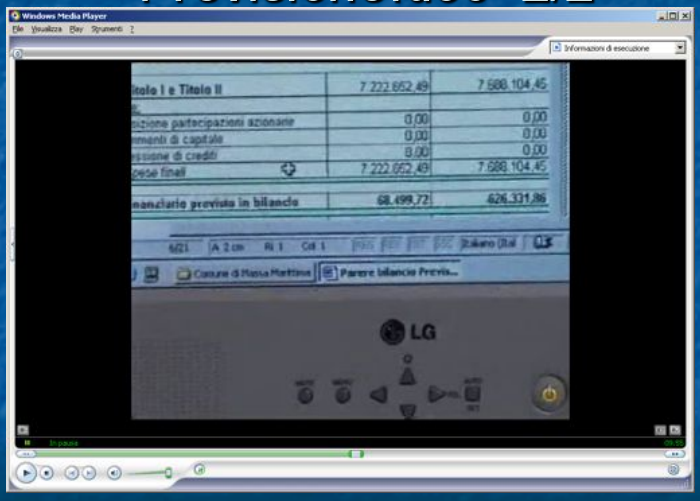
donato@informaticaforense.it

Il documento “Parere bilancio Previsione.doc” 1/2



donato@informaticaforense.it

Il documento “Parere bilancio Previsione.doc” 2/2



donato@informaticaforense.it

Analisi della timeline

Tizio\Part_1\NONAME-NTFS\WINDOWS\PCHEALTH\HELPCTR
\DataColl\CollectedData_6427.xml
13/05/2003 13.33

Tizio\Part_1\NONAME-NTFS\[orphan]
\RP281\RestorePointSize **13/05/2003 13.48**

Attendibilità dell'orario

- In data 13 maggio 2003, a seguito di attività di accertamento della Polizia Postale e delle Comunicazioni – Sezione di Brindisi, è stata verificata la precisione dell'orologio di sistema del PC e ne è stato calcolato uno scostamento in anticipo medio di circa 16,5 secondi.
- Pertanto gli orari indicati vanno corretti, sottraendo a ciascun orario circa 16 secondi

Conclusione

si deve ritenere che in data 13 maggio 2003 tale PC sia stato utilizzato con continuità fino alle ore 13.46, orario anteriore all'omicidio del Tizio

Localizzazione del dispositivo di telefonia mobile (cellulare)

modalità di localizzazione di un dispositivo di telefonia mobile (cellulare) e individuazione delle aree geografiche di

pertinenza delle singole celle

Breve descrizione dell'architettura e del sistema radiomobile GSM

- MSC: Mobile services Switching Center
- BSS: Base Station Subsystem
  - BSC: Base Station Controller
  - BTS: Base Transceiver Station

donato@informaticaforense.it

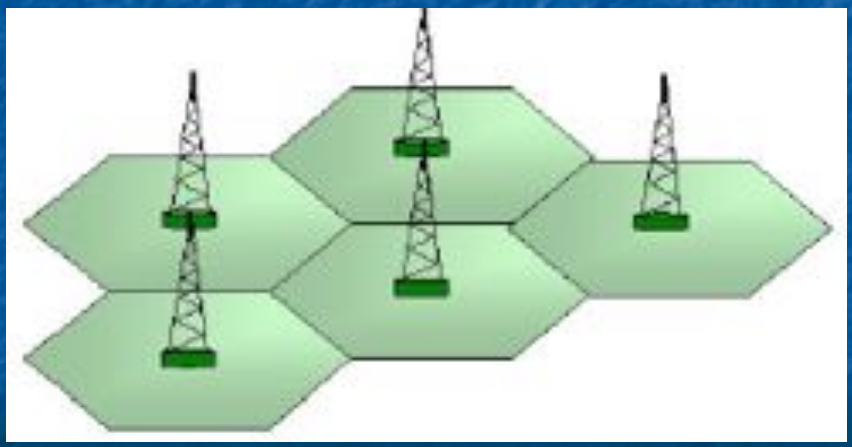
Breve descrizione dell'architettura e del sistema radiomobile GSM

donato@informaticaforense.it

L'elemento rilevante: le BTS

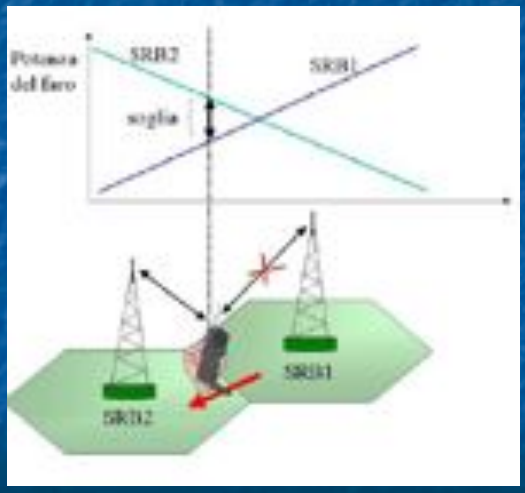
donato@informaticaforense.it

La copertura del territorio in celle



donato@informaticaforense.it

La funzione di “Handover” ossia di passaggio da una cella ad una altra



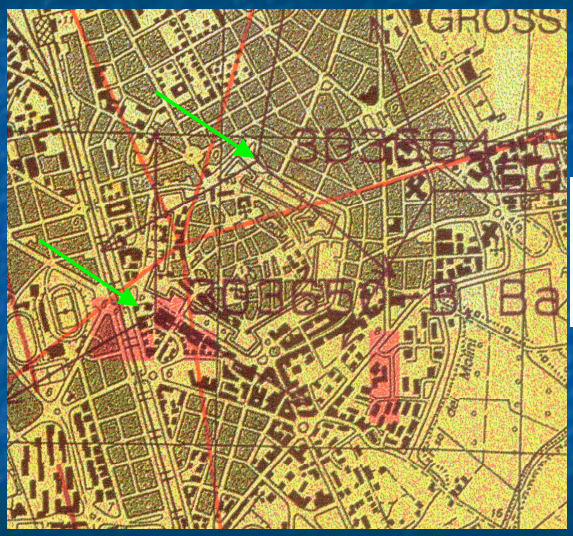
donato@informaticaforense.it

Localizzazione del cellulare +393486969696

Data e ora		Zona e cella
13/05/03	12.40	FG Brindisi Via Ximenes 30
13/05/03	13.42	FG Brindisi Via Piave
13/05/03	14.13	BA Alberona – S. Angelo Scalo
13/05/03	14.29	FG Tertiveri – Montelaterone

donato@informaticaforense.it

Le BTS in Brindisi rilevanti



donato@informaticaforense.it

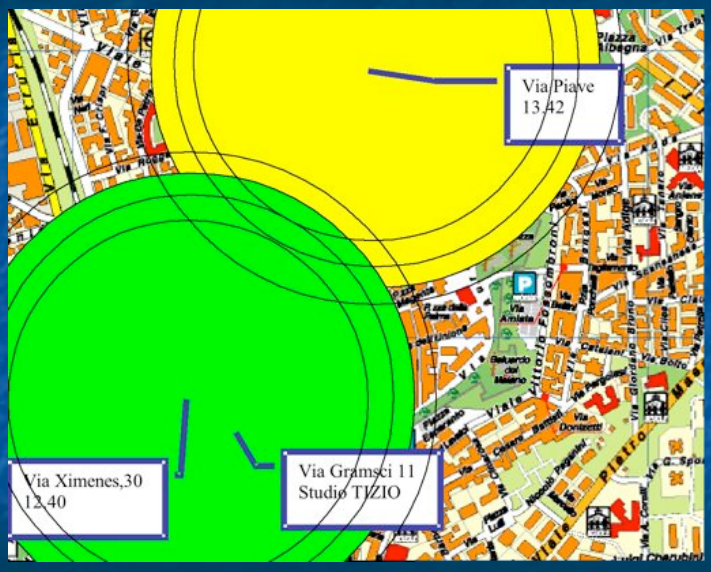
Le BTS in Brindisi rilevanti

donato@informaticaforense.it

Le BTS in provincia di Brindisi rilevanti

donato@informaticaforense.it

La linea di "handover" fra le BTS di Via Piave e di Via Ximenes



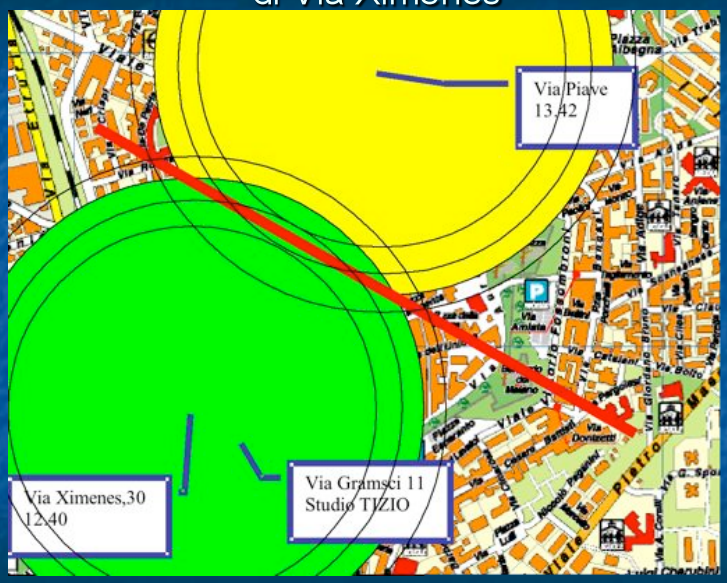
donato@informaticaforense.it

La linea di “handover” fra le BTS di Via Piave e di Via Ximenes

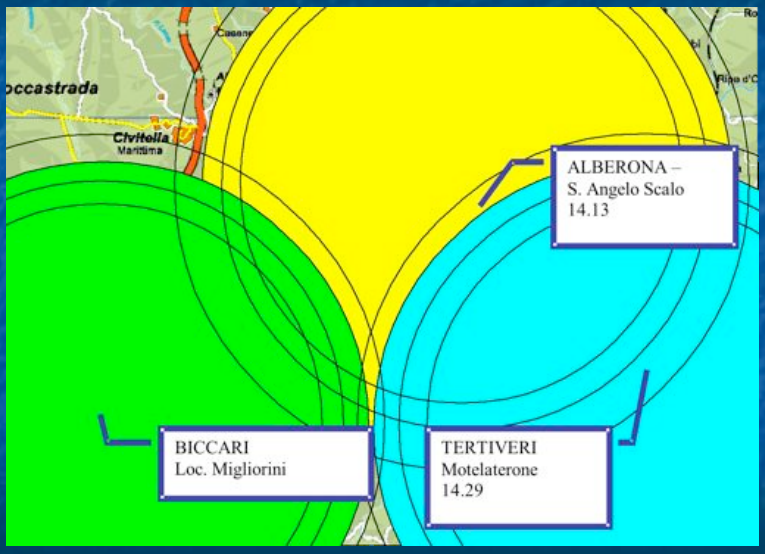
Prendendo in considerazione i seguenti aspetti:

- la condizione geograficamente più sfavorevole per l’imputato
- che la via Manetti e' una strada a senso unico che corre dalla via IV novembre sino all' incrocio con via Gramsci
- che l’imputato, da come risulta in atti, aveva parcheggiato la propria auto in via Alfieri, che e' strada a senso unico
- sensibile l’effetto barriera causato dalle mura di cinta della città di Brindisi

La linea di “handover” fra le BTS di Via Piave e di Via Ximenes

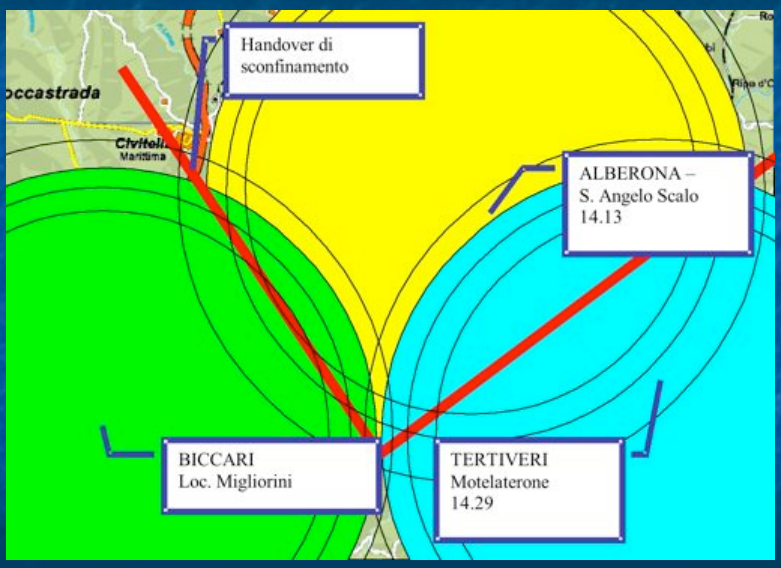


Le linee di "handover" fra le BTS di Biccari, Tricase e Tertiveri



donato@informaticaforense.it

Le linee di "handover" fra le BTS di Biccari, Tricase e Tertiveri



donato@informaticaforense.it

Le linee di "handover" fra le BTS di Biccari, Tricase e Tertiveri

al momento della telefonata delle 14.13 il dispositivo radiomobile percorreva la strada provinciale n. 64 fra Ripalta e Tertiveri, poco dopo la Stazione di Civitella Ripalta nei pressi dell'incrocio con la strada provinciale n. 47

Tratte di percorrenza

DA	A	Tempo	Lung.
Brindisi via Gramsci 11	Via Fossombroni – Via Catalani	3 min.	800 m
Via Fossombroni – Via Catalani	Biccari Tricase	22 min.	20 km
Biccari Tricase	poco dopo Ripalta	13 min.	13 km

Tabella di Percorrenza a ritroso

Luogo	Orario
Ingresso cella BTS di S. Angelo scalo - poco dopo Ripalta	14.13
Biccari – Tricase	14.00
Brindisi Via Fossombroni – Via Catalani	13.38
Studio Paolo Tizio	13.35

donato@informaticaforense.it

Tabella di Percorrenza

Luogo	Orario	Percor.
Studio Paolo Tizio	13.35	0 Km
Brindisi Via Fossombroni – Via Catalani	13.38	1 Km
Biccari – Tricase	14.00	21 Km
Ingresso cella BTS di S. Angelo scalo - poco dopo Ripalta	14.13	34 Km

donato@informaticaforense.it

Conclusioni

Tabella spazio temporale degli eventi

Tabella spazio temporale degli eventi

Luogo	Evento	Orario	Perc.
Studio Paolo Tizio	imputato esce dallo studio	13.35	0 Km
Brindisi Via Fossombroni – Via Catalani	Chiamata telefonica	13.38	1 Km
Studio Paolo Tizio	Attività di utilizzo del PC	13.46	8 Km (stimata)
Biccari – Tricase	Ingresso cella BTS Tricase	14.00	21 Km
Ingresso cella BTS di S. Angelo scalo c/o Ripalta	Chiamata telefonica	14.13	34 Km
Ingresso cella BTS Montelaterone Tertiveri	Chiamata telefonica	14.29	54 Km

Alcune considerazioni finali

- Non solo GSM ma anche Wi Fi
- Tempistica dei percorsi

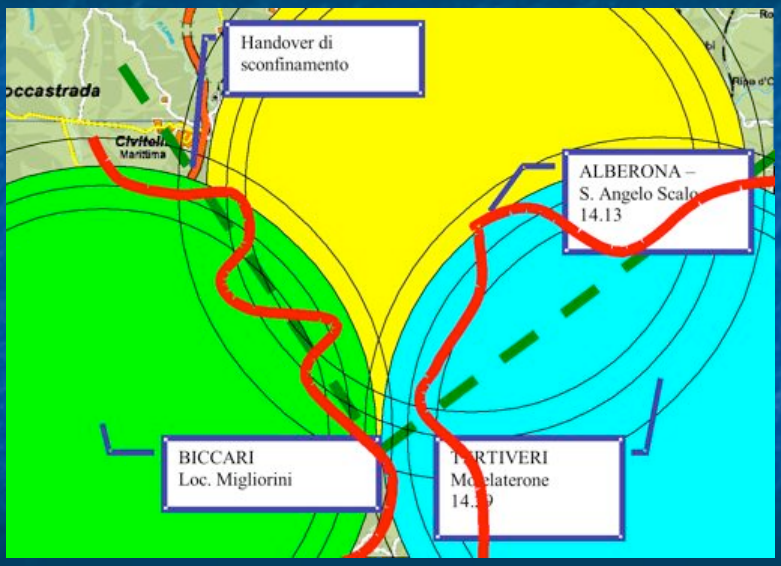
Alcune considerazioni finali

- La determinazione delle linee di handover andrebbe fatta utilizzando dei misuratori di campo

www.marcucci.it

www.rf.com.br

Alcune considerazioni finali



donato@informaticaforense.it

Alcune considerazioni finali

- SIM GSM possono essere clonate

- IMEI dei telefoni GSM/UMTS possono essere clonati

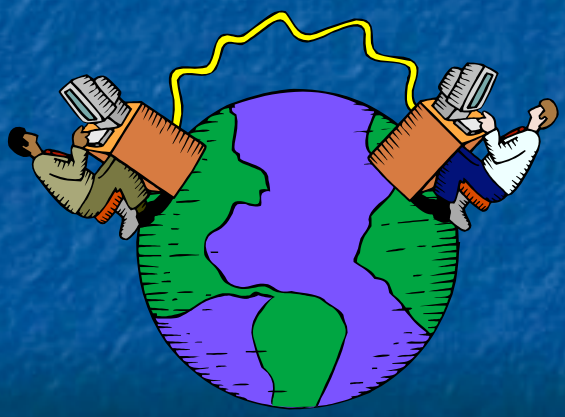
donato@informaticaforense.it

Alcune considerazioni finali

- La documentazione del traffico ha inizialmente un mero valore indiziario
- Vanno sempre individuati ulteriori elementi di riscontro

donato@informaticaforense.it

Network Forensics



Network Forensics

Cosa è una Rete di computer?

Network Forensics

Rete di computer

"un insieme di computer collegati fra loro che scambiano dati reciprocamente"

Rete locale

"trasmissione dati ad alta velocità nell'ambito di una limitata area geografica"

Rete geografica

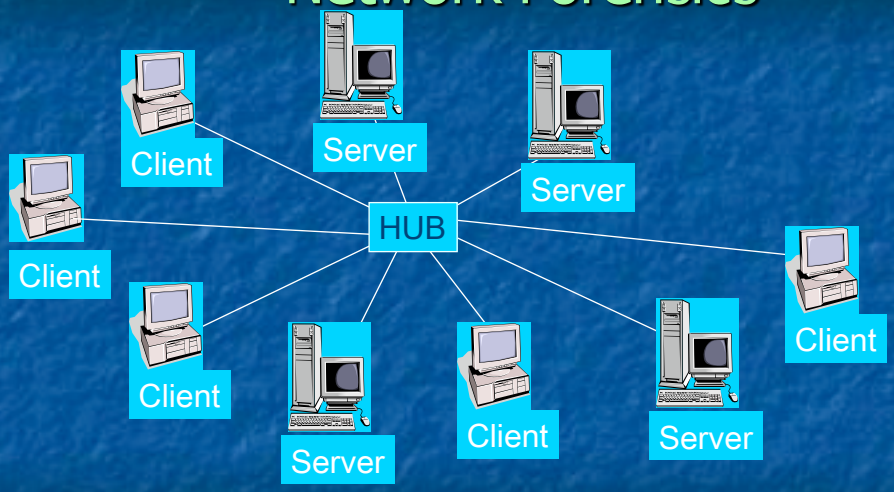
"trasmissione dati a bassa velocità nell'ambito di area geografica estesa"

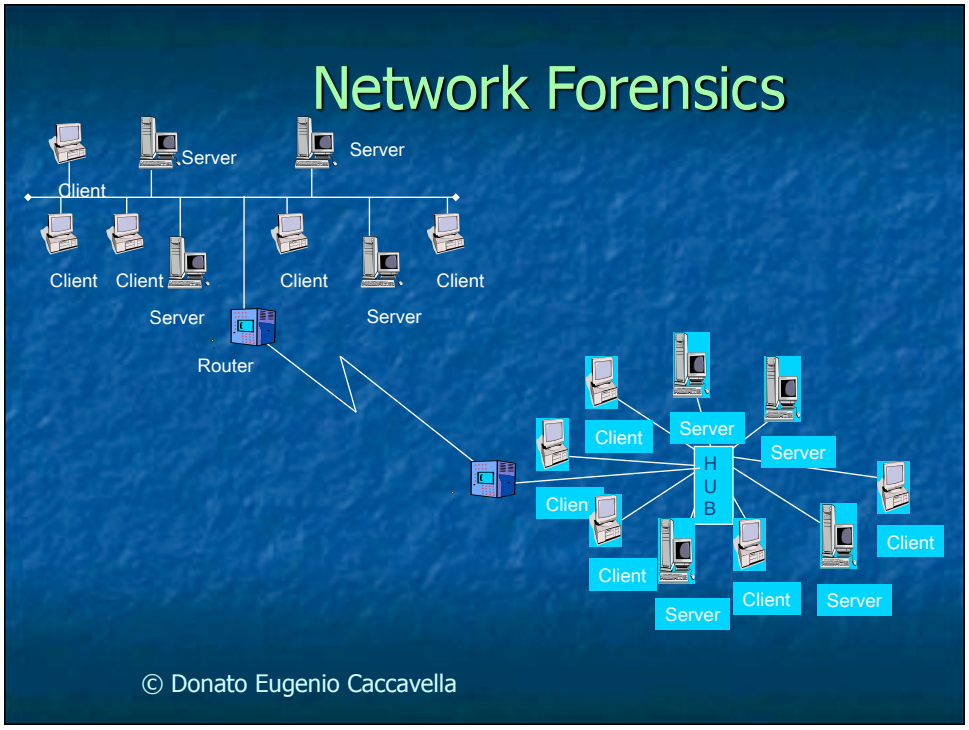
Network Forensics

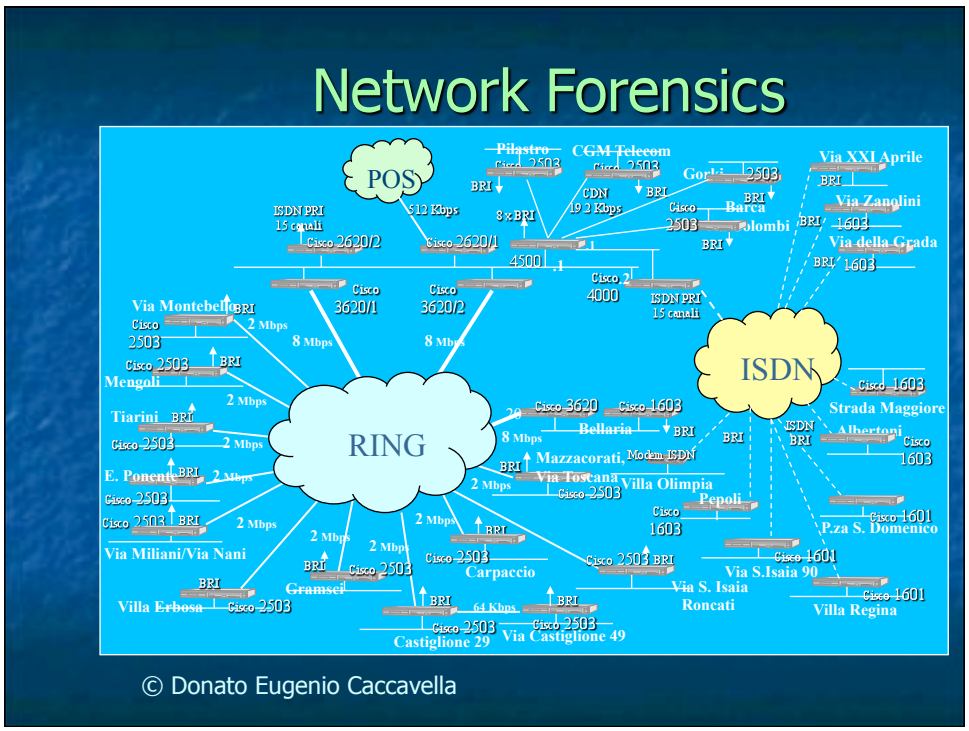
Server
"computer che fornisce un servizio agli altri computer collegati alla rete"
Es. dischi, stampanti, unità nastro, posta elettronica, fax, etc.

Client
"computer collegato alla rete che utilizza i servizi forniti dai server"

Network Forensics




Network Forensics
Client
Server
Server
Client
Client
Server
Client
Client
Server
Router
Client
Server
Server
H
U
B
Clien
Client
Client
Server
Client
Server
© Donato Eugenio Caccavella


Network Forensics
POS
RING
ISDN
Pilastro
CGM Telecom
Via XXI Aprile
Via Zanolini
Via della Grada
ISDN PRI
15 canali
Cisco 2620/2
Cisco 2620/1
512 Kbps
8 x BRI
CDN
19.2 Kbps
4500
Cisco 2
4000
Cisco
3620/1
Cisco
3620/2
8 Mbps
Via Montebello
Cisco
2503
Mengoli
Tiarini
E. Ponente
Via Miliani/Via Nani
Villa Erbosa
Gramsci
Castiglione 29
Via Castiglione 49
Carpaccio
Mazzacorati
Via Toscana
Bellaria
Villa Olimpia
Pepoli
Via S. Isaia
Roncati
Via S.Isaia 90
P.za S. Domenico
Villa Regina
Strada Maggiore
Albertoni
Cisco 3620
Cisco 1603
Cisco 2503
Modem ISDN
64 Kbps
2 Mbps
BRI
ISDN
BRI
© Donato Eugenio Caccavella

Network Forensics

Si ricorre alla Network Forensics, ad esempio in caso di:

Acquisizione dei reperti per individuare gli autori di un accesso non autorizzato ad un sistema telematico ex 615 ter. C.P.

Network Forensics

Unendo tecniche sofisticate di indagine informatica alle modifiche legislative entrate in vigore il mese scorso, si è arrivati a colpire non solo i siti che diffondono materiale coperto da copyright, ma anche lo scambio diretto tra utenti della rete,

il peer-to-peer

che costituisce - dopo l'offensiva americana contro Napster e i suoi successori - il principale canale di circolazione del "sapere elettronico".

…omissis…

È stata un'indagine tecnicamente ostica, costretta a inseguire quasi sempre "Ip dinamici", indirizzi il cui destinatario reale cambia domicilio elettronico ogni cinque minuti, e account solo apparentemente italiani, dietro i quali si celano inafferrabil siti moldavi, lituani e di altri paesi dell'Europa orientale.

Network Forensics

Con decreti concessi dal giudice per le indagini preliminari, per la prima volta sono stati intercettati in modo massiccio anche i messaggi di posta elettronica - spesso criptati - che fornitori e clienti si scambiavano: i gestori dei server sono stati costretti dalla Guardia di finanza ad inaugurare dei "lock", delle caselle-ombra di posta elettronica cui arrivavano in copia tutti i messaggi destinati agli indagati.
…omissis…
"Ci siamo accorti - spiegano gli inquirenti - che quasi tutti gli archivi si nutrivano da siti molto diffusi, come Kazaa, Gnutella, Winmx, Morpheus", luoghi della rete che gli investigatori definiscono "sostanzialmente incontrollabili".
"Due giorni fa - dice uno dei cibermarescialli - intorno alle nove di sera erano collegati alla rete di Kazaa più tre milioni di utenti": un oceano di contatti in cui la caccia ai pirati si annuncia un'impresa titanica

Network Forensics

I controlli, che non hanno riguardato gli utilizzatori di sistemi file sharing tipo "peer to peer", ma esclusivamente a soggetti dediti a produzione e vendita di prodotti tutelati dal copyright, si sono sviluppati attraverso il **monitoraggio di 12 siti web** e l'intercettazione **28 account e-mail** utilizzati dagli indagati per porre in essere l'illecita attività.

Posti sotto sequestro due siti INTERNET mediante i quali avveniva l'illecita commercializzazione.
Nel corso delle perquisizioni, operate in ben 30 province italiane, i BASCHI VERDI hanno rinvenuto masterizzatori per **CD e DVD** dell'ultimissima generazione, programmatori per Smart Card per TV satellitare, migliaia di supporti ottici contenenti opere illecitamente riprodotte e DVD contenenti le ultimissime uscite cinematografiche.

Network Forensics

Criticità:

Complessità dovuta al numero elevato di sistemi collegati in rete

Accuratezza delle informazioni presenti su questi sistemi

Network Forensics

Legittimità

buona parte delle attività inerenti la network forensics sono costituite da intercettazioni!

Network Forensics

Esempio:
l'amministratore di un sistema multi utente che intercetta il traffico in essere fra il sistema stesso e altri sistemi.

E' lecito ?

E' utilizzabile?

Network Forensics

L'analisi forense del disco di un sistema viene eseguita dopo che l'evento si è verificato (post mortem)

La network forensics può essere eseguita anche mentre l'evento si sta verificando

Network Forensics

In quest'ultimo caso potrebbe non essere possibile spegnere il sistema (es. un sistema di home banking, il server di uno studio commercialista o di uno studio legale)

Network Forensics

In questi casi vengono eseguite attività di:

- Network Forensics
- Incident response

Elevato rischio di alterazione o distruzione del reperto.

Network Forensics

In dettaglio:

- Disamina e correlazione dei file di log di uno o più sistemi
- Ricerca di strumenti atti ad intercettare le trasmissioni di dati (sniffer)
- Ricerca di strumenti atti ad intercettare le operazioni eseguite dagli uteni sul sistema (remote control program, es. BO)

Network Forensics

- Ricerca di possibili condivisioni di risorse o programmi di comunicazione
- Ricerca di alterazioni nei file di sistema
- Disamina delle alterazione dei file contenti le password e della presenza di nuovi utenti
- Verifica della configurazione del sistema
- Ricerca di file "anomali"

Network Forensics

Tutte queste operazioni devono essere eseguite su tutti i sistemi coinvolti !

Network Forensics

Individuare l'origine.

Ad ogni sistema presente su una rete è assegnato un indirizzo IP.

Nel caso di Internet Provider un indirizzo IP viene assegnato a sistemi diversi in momenti diversi.

E' possibile determinare il sistema al quale in un dato momento era stato assegnato un ben preciso indirizzo IP

Network Forensics

Spesso dei sistemi vengono utilizzati come ponte in modo da rendere complicato o addirittura impossibile l'individuazione del sistema da cui sono state eseguite le operazioni

Network Forensics

Correlazione fra Disk Forensic e Network Forensics:

Network Forensics pemette di convalidare l'integrità e l'autenticità dei reperti acquisiti su un sistema.

Disk Forensics fornisce gli strumenti per acquisire i dati necessari per la Network Forensics

Quali strumenti utilizzare ?

Esistono software commerciali riconosciuti e considerati attendibili dalle corti inglesi ed americane

Quail strumenti utilizzare ?

uno fra tutti:

EnCase® prodotto da Guidance Software

è utilizzato anche dalla Polizia di Stato

Quali strumenti utilizzare ?

Si pone però un problema:

"Quis custodiet ipsos custodies" ?

Quali strumenti utilizzare ?

per poter verificare che un programma esegua operazioni ben precise, deve essere possibile consultarne il codice sorgente

Quali strumenti utilizzare ?

Lo stesso principio vale anche per il sistema operativo che ospita il programma di acquisizione ed analisi forense !

Quali strumenti utilizzare ?

Quindi, bisogna utilizzare strumenti **open source**, in modo che sia consentita la verifica anche di singoli dettagli delle operazioni eseguite sui dati

Quali strumenti utilizzare ?

Alcuni strumenti Open Source:

- Open BSD
- Free BSD
- Linux
- Anche il buon vecchio MS-DOS ?!

Linux

Vantaggi:

Controllo completo e capillare dello sistema

Flessibilità: possibilità di fare un boot da CD (Koppix)

Potenzialità: dotazione di numerosi strumenti di diagnostica

Linux

In particolare:

dd: per l'acquisizione in modalità forense dei supporti. (bit stream image)

md5sum e sha1sum per il calcolo degli hash per garantire l'integrità dei reperti acquisiti.

Linux

In particolare:

fdisk per determinare la geometria del disco

grep per il pattern matching

file per determinare il contenuto di un file

Linux

In particolare:

il loop device!

ghex e khexedit!

Linux

Altri strumenti avanzati specifici:

Sleuthkit di Dan Farmer e Wietse Venema www.sleuthkit.org attualmente Brian Carrier

Linux

Altri strumenti avanzati specifici:

Autopsy: front end grafico degli strumenti forniti in sleuthkit

Linux

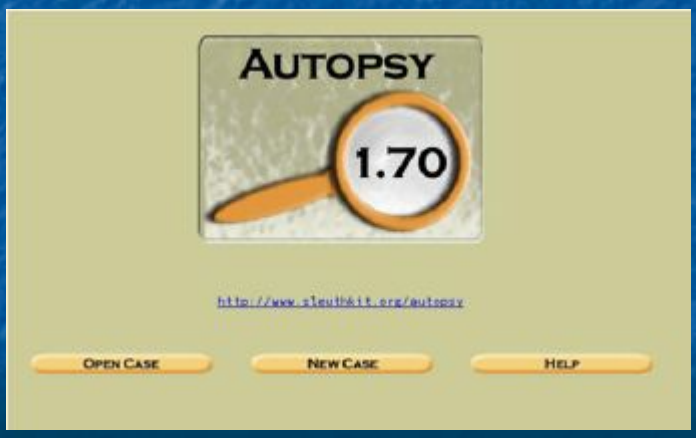
Autopsy:

Gestione dei casi
Per ogni caso gestione multi host per ogni host multi device

Recupero dei file cancellati

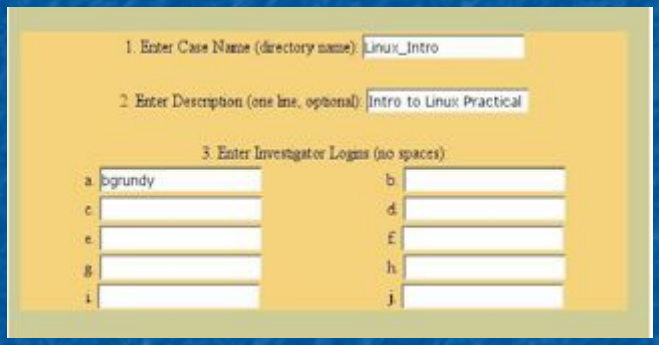
Supporto di svariati file system

Autopsy



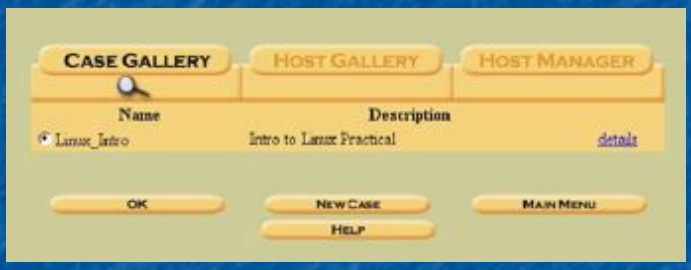
donato@informaticaforense.it

Autopsy



donato@informaticaforense.it

Autopsy



donato@informaticaforense.it

Autopsy

donato@informaticaforense.it

Autopsy

donato@informaticaforense.it

Autopsy

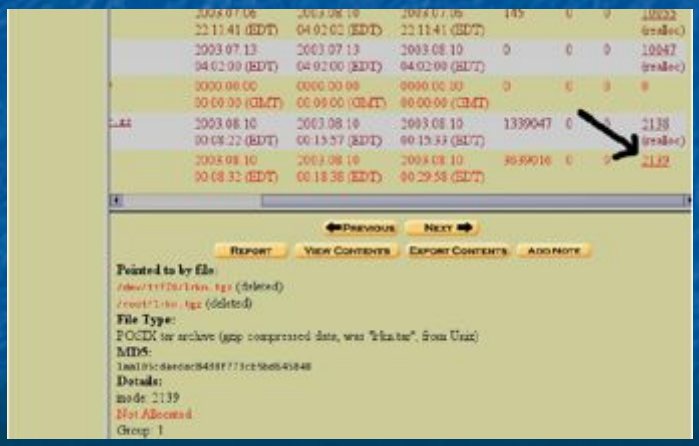
Autopsy

Autopsy

Autopsy

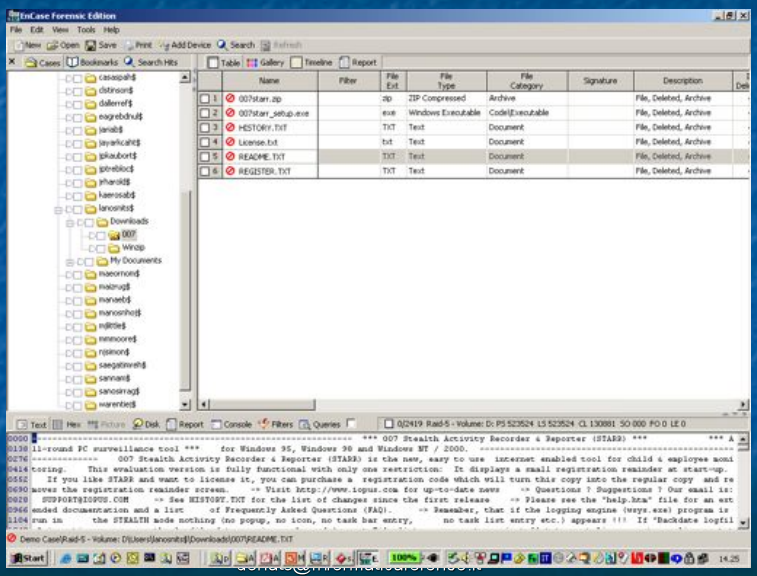
donato@informaticaforense.it

Autopsy

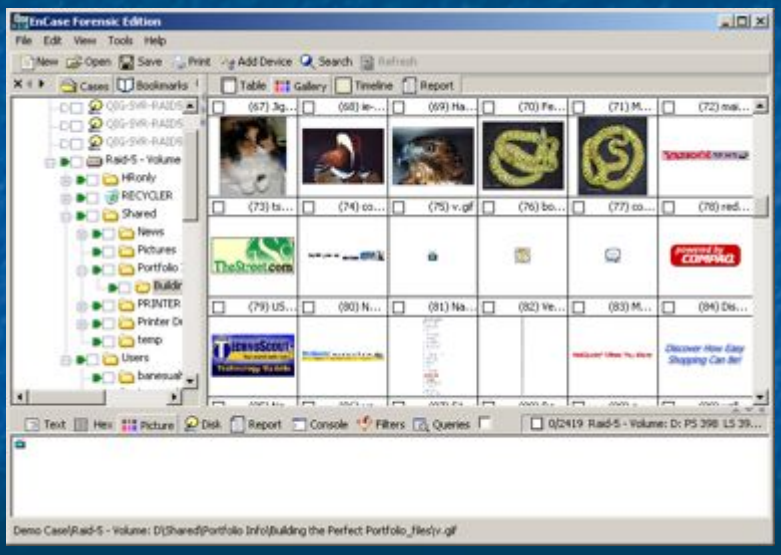


donato@informaticaforense.it

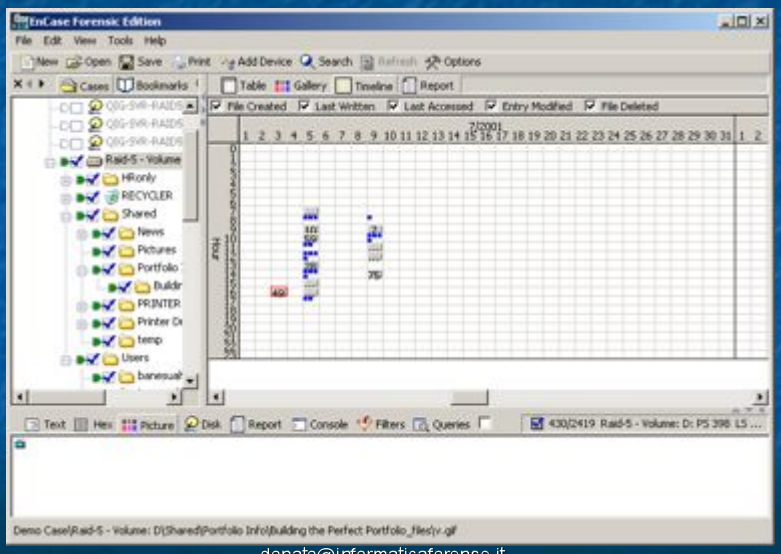
EnCase



EnCase

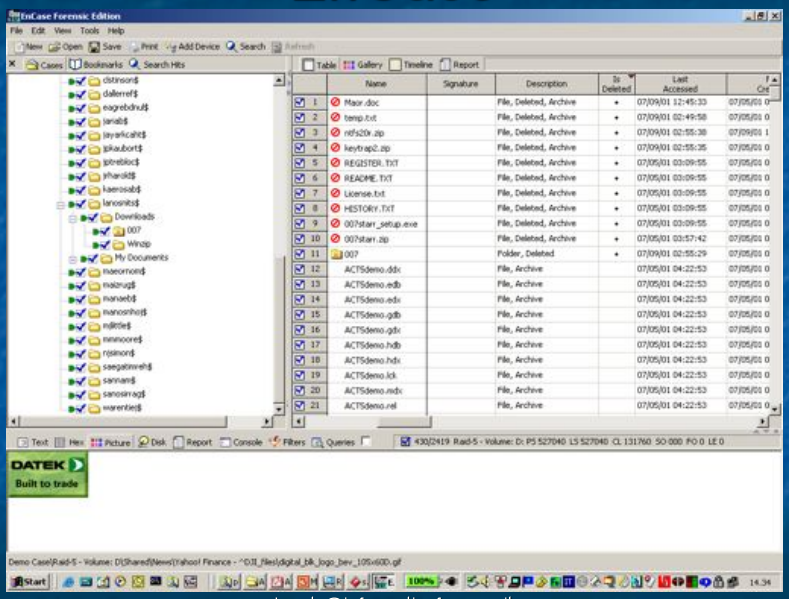


EnCase



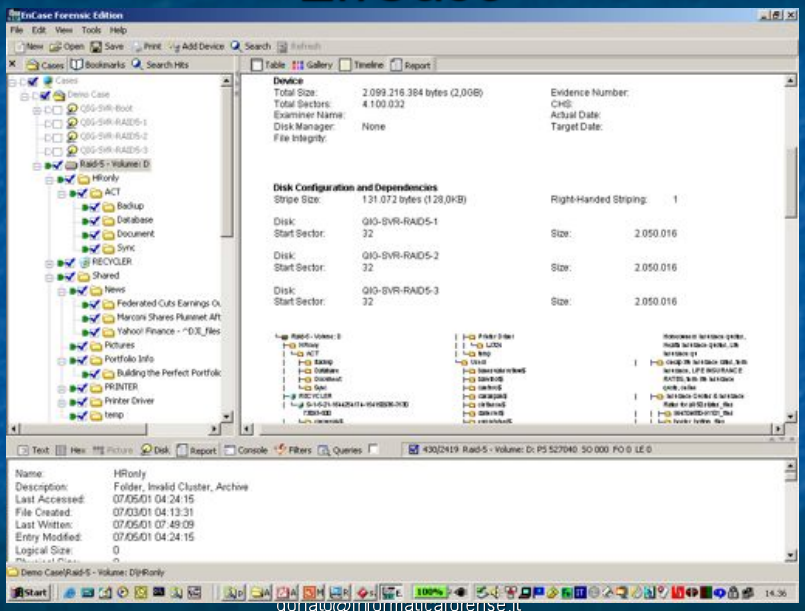
donato@informaticaforense.it

EnCase



donato@informaticaforense.it

EnCase



Criticità

Formati proprietari in fase di acquisizione e analisi Es. *.PST *.NSF

Acquisizione da dispositivi non "standard" es. Cellulari, Palmari, veicoli, ECG…

Criticità

Difficoltà d'uso

Necessità di competenza sistemistica

Una mia opinione

chi usa EnCase

chi usa Linux

Bisogna governare gli "strumenti" senza farsi governare da questi

L'uso delle macchine virtuali nella disk forensics

Cosa è una macchina virtuale?

L'uso delle macchine virtuali nella disk forensics

"è un computer virtuale che simula un computer reale"

L'uso delle macchine virtuali nella disk forensics

Si ricostruisce in modo virtuale, a meno di qualche dettaglio non significativo, la medesima fattispecie reale, ovvero un personal computer simile a quello oggetto del sequestro/ acquisizione.

donato@informaticaforense.it

Simulazione….

vmware e non solo

donato@informaticaforense.it

Primo caso…

L'uso delle macchine virtuali nella disk forensics

Obiettivo: far comprendere al giudice la semplicità di alcune operazioni al fine di permettere un corretto apprezzamento del valore probatorio di alcuni reperti.

L'uso delle macchine virtuali nella disk forensics

Alcuni report sono molto "aridi":

Data Target:	27/04/05 13:06:46
Dimensioni Totali:	2.111.864.832 byte (2GB)
Settori Totali:	4.124.736
Integrità File:	Verifica Completata, 0 Errori
Versione EnCase:	3.22c
Versione Sistema:	Windows 2000

L'uso delle macchine virtuali nella disk forensics

Alcuni report sono molto "aridi":

L'uso delle macchine virtuali nella disk forensics

mentre una macchina virtuale comuni
più di mille parole….

simulazione vmware

L'uso delle macchine virtuali nella disk forensics

L'uso delle macchine virtuali nella disk forensics

donato@informaticaforense.it

L'uso delle macchine virtuali nella disk forensics

Aneddoto:
Durante l'esame del CT o meglio durante la simulazione si misero in evidenza alcune "gravi contraddizioni" di un teste ascoltato poco prima!"

Giuridicamente come si pone la questione?

donato@informaticaforense.it

L’uso delle macchine virtuali nella network forensics

Secondo caso…

L’uso delle macchine virtuali nella network forensics

Obietivo: determinare il comportamento reale di un server nel momento in cui veniva consultato da un utente..

L'uso delle macchine virtuali nella network forensics

Problematiche:

molteplicità dei possibili client che potevano accedere

quali eventi potevano condizionare il contesto

donato@informaticaforense.it

L'uso delle macchine virtuali nella network forensics

Approccio metodolgico:

Creare un "microsistema" (nell'accezione microbiologica) per osservare il comportamento dei suoi componenti!

donato@informaticaforense.it

L'uso delle macchine virtuali nella network forensics

•Approccio metodolgico:

Quindi è stato creata una rete di sistemi virtuali composta da:

Il server;
Un client "puro" Microsoft windows 98
Un client "puro" Microsoft windows 2000
Un client "puro" Microsoft windows XP

donato@informaticaforense.it

L'uso delle macchine virtuali nella network forensics

Metodo Galileano ….

simulazione vmware

donato@informaticaforense.it

L’uso delle macchine virtuali nell’informatica forense

Sempre più frequentemente si por
l’esigenza di simulare e studiare il comportamento di un o più sistemi informatici.

donato@informaticaforense.it

L’uso delle macchine virtuali nell’informatica forense

La complessità e la variabilità dei siste
informatici e delle loro componenti software, non sempre permette di avere un approccio deterministico,

donato@informaticaforense.it

L'uso delle macchine virtuali nell'informatica forense

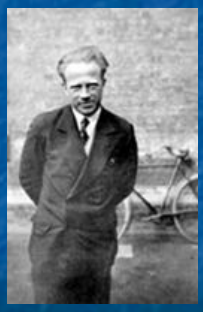
Ad esempio per comprendere funzionamento di un programma, potrebbe non essere sufficiente conoscerne il codice sorgente, perché il suo funzionamento potrebbe essere condizionato da fattori esterni, come il sistema operativo, i vari service pack, software installato dall'utente, etc. etc.

L'uso delle macchine virtuali nell'informatica forense

elementi questi ch potrebbero essere non noti o correttamente acquisiti

L'uso delle macchine virtuali nell'informatica forense

arrivando ad un sorta di… principio di indeterminazione di Heisenberg per l'informatica forense…

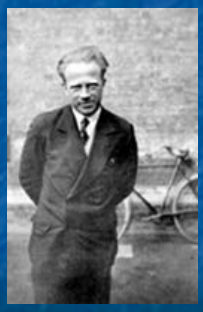


http://it.wikipedia.org/wiki/Immagine:Heisenberg.jpg

donato@informaticaforense.it

L'uso delle macchine virtuali nell'informatica forense

Il comportamento di un insieme complesso di sistemi informatici, non compleatemente definito, può essere determinato solo probabilisticamente.



http://it.wikipedia.org/wiki/Immagine:Heisenberg.jpg

donato@informaticaforense.it

L'uso delle macchine virtuali nell'informatica forense

Pertanto sarebbe opportuno che in contesto informatico complesso, ogni accertamento tecnico fosse confortato da riscontri "sperimentali", eseguiti con macchine virtuali, massimizzandone la rappresentatività.

donato@informaticaforense.it

La link analisys

Si pone inoltre il problema in generale di analizzare banche dati sempre più voluminose spesso non strutturare difficilmente interrogabili in modo "fuzzy"

donato@informaticaforense.it

La link analisys

La link analysis è il processo di costruzione di una rete di oggetti o item interconnessi nel tempo e con l'uso di tecniche speciali, di strumenti software finalizzati a: formare, esaminare, modificare, analizzare, cercare e mostrare modelli di comportamento, specialmente di tipo illecito.

Questi oggetti o item consistono in entità, eventi e associazioni. Di solito le entità di rilevanti sono:

- Luoghi fisico o di rete IP,
- Organizzazioni, come cellule, strutture aziendali, governi, unità commerciali o militari
- Servizi, come aziende, aeroporti, hotel, scuole, magazzini
- Individui, come nomi, titoli o numeri identificativi
- Prodotti, come chimici, fertilizzanti, maschere, acidi
- Tipi di Documenti, come passaporti, patenti di guida, e-mails
- Denaro, come contanti, trasferimenti via cavo, ordini di denaro
- Veicoli, come aeroplani, camion, barche, macchine
- Droghe, come tipo, peso, fonte

donato@informaticaforense.it

La link analisys

Inoltre, per entità, come soggetto di accertamento, possono essere disponibili altre dimensioni più dettagliate, come nome, pseudonimi, genere, appartenenza, affiliazione, religione, stato civile, cittadinanza, razza, data di nascita, occupazione, paese d'origine, colore dei capelli, occhi, altezza, peso, paesi visitati, tra le altre cose.

Per eventi la natura dell'accertamento è determinare le dimensioni dei dati ad esempio numero di venti o quantita di byte trasmessi.

donato@informaticaforense.it

Q & A

Grazie

Dott. Donato Eugenio Caccavella

donato@informaticaforense.it