

Convegno di Studi  
"Documento Informatico: Problematiche di  
formazione e probatorie"

Verona 7 maggio 2004

## "Modalità di valutazione del documento informatico"

© Donato Eugenio Caccavella

donato@vodafone.it

Il dato informatico,  
questo sconosciuto...

Allora il dato è inattendibile ?



No !  
Un esempio ?  
la Firma Digitale

© Donato Eugenio Caccavella

donato@vodafone.it

## De documento informatico

fasi trattamento:

- individuazione
- acquisizione
- analisi
- valutazione

## **Valutazione** del documento informatico:

Perché è necessario anche un momento di valutazione del documento, se il bit può assumere solo il valore di 0 o 1 ?



## Valutazione del documento informatico:

Perché il documento informatico può essere facilmente:

- alterato
- inquinato
- contraffatto

## Valutazione del documento informatico:

Inoltre, bisogna verificare  
se le operazione di  
acquisizione del documento  
informatico sono state  
legittime

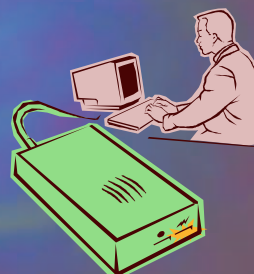
## Valutazione del documento informatico:

Quindi vanno espressi giudizi di merito circa:

- l'attendibilità
- l'integrità
- l'autenticità

del documento stesso

# Disk Forensics



Informatica Forense

VS

Sicurezza Informatica

© Donato Eugenio Caccavella

donato@vodafone.it

Informatica Forense

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.

© Donato Eugenio Caccavella

donato@vodafone.it

## 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, 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

I file cifrati:

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

## L'analisi di un disco

### I file cifrati:

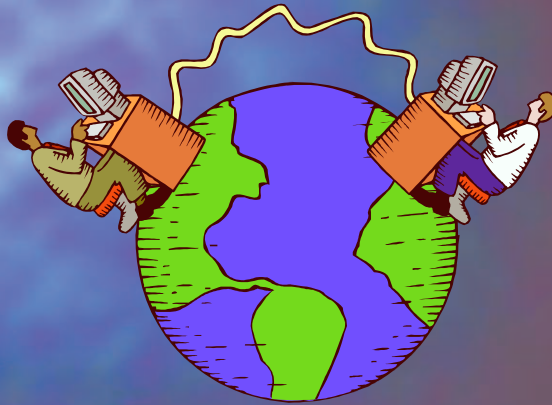
metodi di cifratura "forte" che si possono aggredire con attacchi a forza bruta ma che non danno garanzia di risultato

## L'analisi di un disco

### I file cifrati:

in questi casi il punto debole è  
l'uomo...

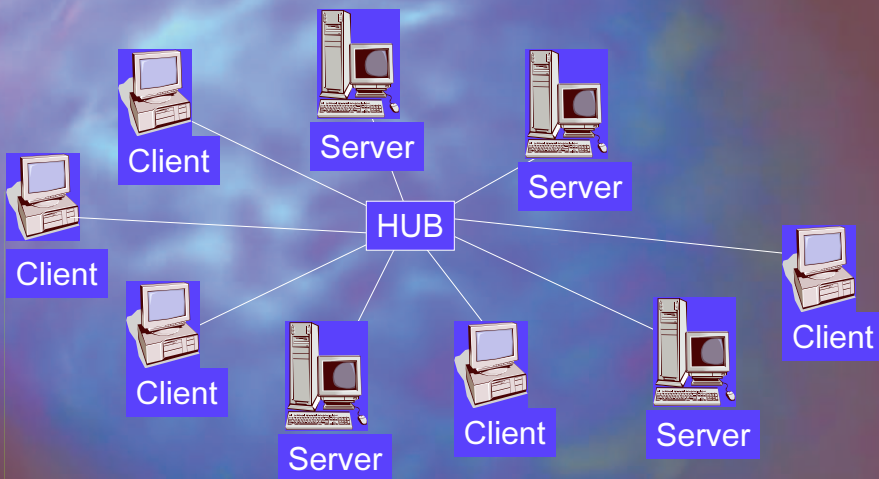
# Network Forensics



© Donato Eugenio Caccavella

donato@vodafone.it

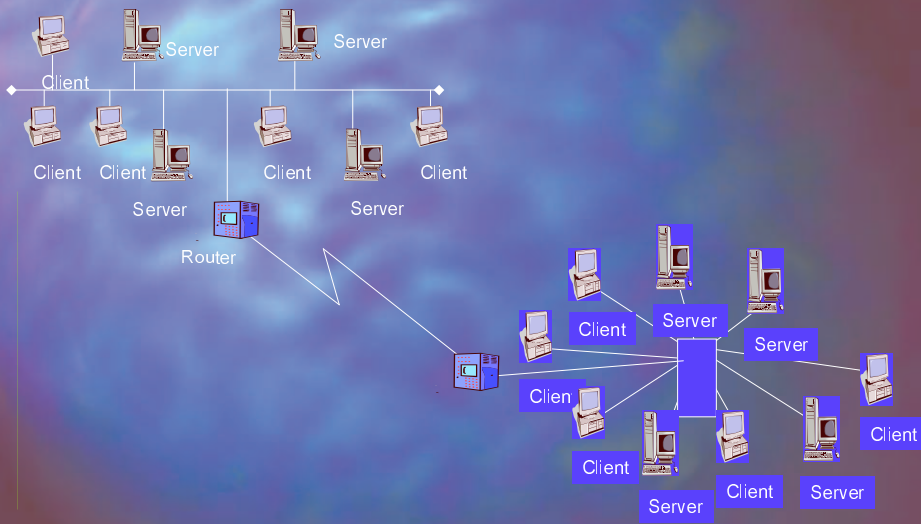
# Network Forensics



© Donato Eugenio Caccavella

donato@vodafone.it

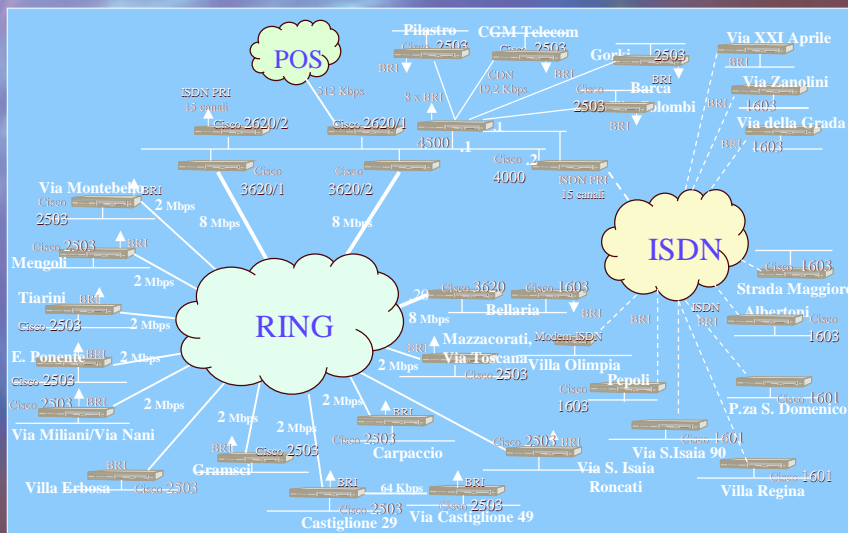
# Network Forensics



© Donato Eugenio Caccavella

donato@vodafone.it

# Network Forensics



© Donato Eugenio Caccavella

donato@vodafone.it

## 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

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 utenti sul sistema (remote control program, es. BO)

## Network Forensics

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



© Donato Eugenio Caccavella

donato@vodafone.it

## 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

© Donato Eugenio Caccavella

donato@vodafone.it

## Network Forensics VS Disk Forensics

Correlazione fra Disk Forensic e Network Forensics:

Network Forensics permette 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

## La valutazione del documento

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

- integrità
- autenticità

## La valutazione del documento

Come?

Prendendo in considerazione i seguenti aspetti:

- chi ha potuto modificare il documento
- in quale momento sarebbe stato modificato

## La valutazione del documento

Come?

Verificando la presenza di tracce che ne indicano eventuali alterazioni, mediante consultazione di:

- file di Log;
- file temporali;
- contenuto di frammenti di dati presenti sul disco

## La valutazione del documento

Analizzando la successione temporale degli eventi che sono accaduti sul sistema

## La valutazione del documento

Correlando gli eventi del sistema con quelli di altri sistemi



Integrità

Autenticità

© Donato Eugenio Caccavella

[donato@vodafone.it](mailto:donato@vodafone.it)