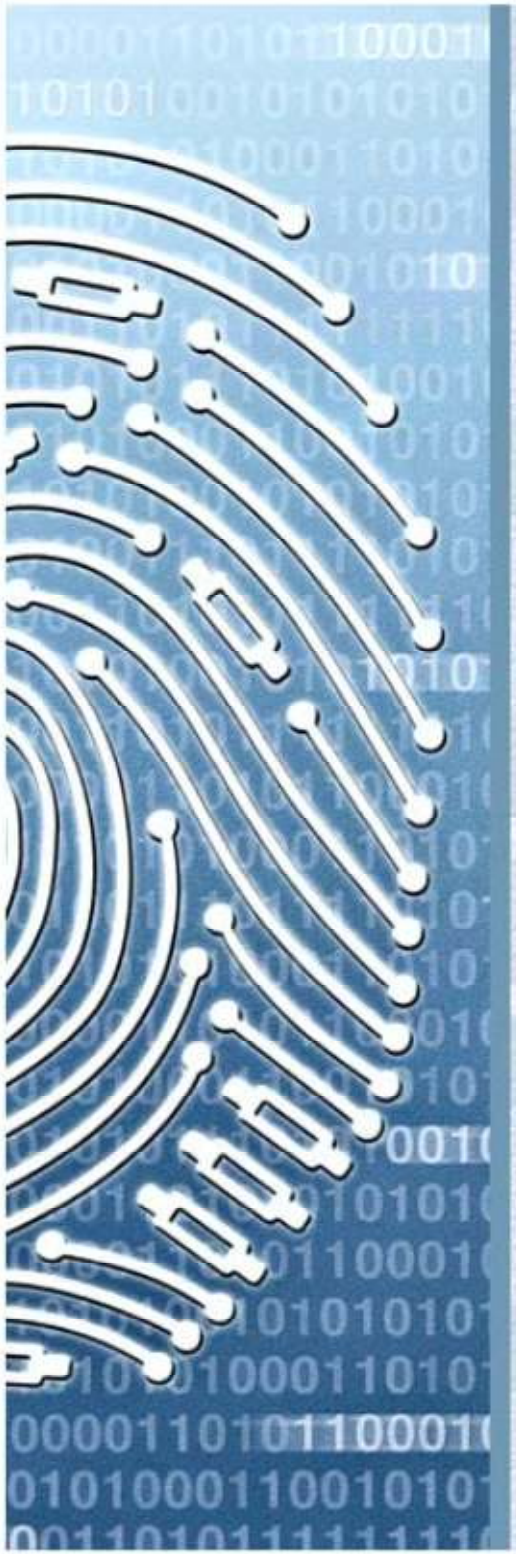
# Strumenti e Tecniche per la creazione di un Falso Alibi Informatico

Vincenzo Calabrò



# Alibi: Definizione

Si intende generalmente una allegazione difensiva di circostanze di fatto prospettabili a difesa dell' imputato o dell' indagato, che si pongono in oggettivo contrasto con i fatti posti a base dell' ipotesi accusatoria

Tale allegazione, frequentemente (ma non unicamente) è volta a dimostrare che il soggetto indagato o imputato, al momento della commissione del reato, si trovava in luogo diverso e lontano rispetto a quello ove il reato stesso sarebbe stato perpetrato o che, comunque, lo stesso non avrebbe potuto commettere quanto a lui contestato

# Alibi Informatico

- E’ possibile provare con certezza che un determinato soggetto sia intento ad utilizzare un Personal Computer in un determinato momento?
- Tali prove sono utilizzabili come alibi?
- L’alibi in oggetto è affidabile o facilmente falsificabile?

**L’informatica per sua stessa definizione vuol dire “informazione automatica”:**

- Esistono degli automatismi atti a simulare le operazioni di un utente, tali da procurargli un falso alibi?
- E’ possibile che tale automatismo intervenuto possa essere scoperto, e con esso il falso alibi?

# Casi noti e notevoli

Alibi ritenuti attendibili

- Il Caso GERI : date dei files su floppy disk
- Il Caso BRADFORD : aggiornamento profilo facebook
- Il Caso GARLASCO : utilizzo del portatile per tesi

Alibi ritenuti inattendibili

- Il Caso MEREDITH : al computer a vedere un film
- Il Caso DOUGLAS-PLUDE : utilizzo di due portatili
- Il Caso FERRAGUTO: il “viaggio” del cellulare

# Metodo d'analisi

Schema di 8 domande a cui il consulente tecnico deve tentare di dare una risposta:

1. Who (Chi) ?
2. What (Cosa) ?
3. When (Quando) ?
4. Where (Dove) ?
5. Why (Perché) ?
6. How (Quanto) ?
7. Whereby (In che modo) ?
8. What means (Con quali mezzi) ?

# Classificazione - 1

Generati durante, o contemporaneamente, l'evento criminoso:

1. l'imputato ha generato direttamente tracce informatiche su dispositivi distanti dalla scena del crimine;
2. un sistema informatizzato ha eseguito "automaticamente" azioni ed eventi pianificati che, producendo tracce informatiche, simulano la presenza e l'interazione dell'imputato in un luogo diverso dalla scena del crimine;
3. un terzo, persona fisica o sistema automatico, ha registrato tracce che potrebbero giustificare la presenza dell'imputato in luoghi diversi dalla scena del crimine;
4. un terzo, un complice, ha eseguito azioni, per nome e per conto dell'imputato, che producono tracce informatiche su dispositivi distanti dalla scena del crimine.

# Classificazione - 2

Creati in un momento diverso, antecedente o seguente, dell'atto delittuoso:

5. l'imputato (o chi per lui) realizza una prova ex novo, facendo attenzione che gli elementi caratterizzanti il tempo rivelino la contemporaneità con l'azione criminale.
6. l'imputato (o chi per lui) riutilizza una traccia informatica già esistente, alterando gli elementi utili a dimostrare la correlazione temporale tra il momento della produzione e l'evento criminoso.

# Ipotesi A

## L'imputato ha generato direttamente tracce informatiche a distanza

**Attraverso l'uso di dispositivi o software di controllo remoto**

- rilevarne la presenza, l'installazione e/o disinstallazione;
- cercare ed analizzare tracce utili a svelarne l'esecuzione (p.e. file prefetch, chiavi di registro, file di configurazione);
- cercare ed analizzare eventuali log degli stessi rilevati;
- analizzare la configurazione di eventuali router o firewall che permettono l'accesso da remoto;
- analizzare i tabulati ed i log di connessione del fornitore di connessione;
- analizzare gli indirizzi di destinazione con quelli dei dispositivi presenti;
- confrontare tutti i suddetti log e lo storico delle connessioni presenti sul dispositivo;
- incrociare le suddette informazioni con i dati estrapolati dall'evidenza.

# Ipotesi B

## Un sistema automatizzato ha simulato un utilizzo in presenza

Per simulare l'utilizzo di un personal computer vi sono varie soluzioni

1. **Script**.
2. **Macro Recorder**.
3. **Auto Typer e Auto Clicker**.

Si può tentare di trovare

- software che rientrano nelle categorie suddette;
- operazioni pianificate nell'intervallo di tempo in cui è stato commesso il reato;
- l'elenco dei file aperti nell'intervallo di tempo da esaminare;
- connessioni di periferiche esterne;
- connessioni da e verso l'esterno;
- file temporanei e cancellati.

# Ipotesi C

## Un terzo, persona fisica o sistema automatizzato, ha registrato tracce informatiche

Alcuni esempi:

- i sistemi di video sorveglianza;
- gli accessi controllati;
- i tabulati telefonici;
- le tracce di spostamento del telefonino;
- il telepass;
- gli sportelli bancomat ed i pos;
- i rilevatori ed i navigatori gps;
- l'applicazione google latitude; ecc.

In questi caso il tecnico può solo verificare l'attendibilità dell'evidenza, accertandosi che il sistema di rilevazione non abbia evidenziato falle tecnologiche tali da rendere non ammissibile giuridicamente la prova informatica.

# Ipotesi D

## Un complice ha eseguito azioni per conto dell'indiziato

Alcuni esempi:

- consegnare il cellulare a qualcuno chiedendogli di spostarsi e di utilizzarlo,
- oppure prestare la propria vettura, dotata di antifurto satellitare e telepass, invitandolo a dirigersi in un luogo distante,
- oppure fornire le proprie credenziali di accesso e il proprio notebook raccomandandosi di adoperarlo.

Per il consulente tecnico sarà difficile, se non impossibile, dimostrare che siano false.

In questo caso sarà cura degli investigatori rinvenire ulteriori informazioni che dimostrino il falso.

# Ipotesi E

## L'indiziato (o chi per lui) realizza una prova ex novo

Quasi tutti i dispositivi elettronici consentono di reimpostare la data e l'ora. In questo modo, ed utilizzando semplici tecniche di anti-forensics, è possibile utilizzare dette apparecchiature e costruire prove in tempi desiderati.

Il consulente tecnico, in questi casi, deve dapprima estrapolare ed incrociare la time-line di funzionamento della macchina con i metadati dei file e con le altre informazioni temporali presenti sul File System, includendo nell'analisi anche i file temporanei ed i file cancellati (p.e. è impossibile che una modifica di un documento di word non crei alla stessa data/ora altri file secondari) ed in seguito verificare, nell'arco temporale di riferimento, che ci siano altre tracce, quali connessioni ad internet, altri programmi o file aperti, ecc.

Vale la pena osservare che solitamente questa ipotesi è la più semplice da verificare e smascherare in quanto le informazioni sono molteplici e difficilmente armonizzabili.

# Ipotesi F

## L'indiziato (o chi per lui) riutilizza una traccia informatica già esistente

Si ipotizza che siano state utilizzate prove già esistenti, i cui riferimenti temporali sono stati modificati per dimostrare la contemporaneità con l'evento criminoso.

Anche in questo caso è possibile, utilizzando tools commerciali o freeware, oppure semplici comandi del S.O., modificare le date presenti sul file system o nei metadati dei file per farli coincidere con quelli desiderati.

Le tecniche di analisi sono simili a quelle dell'ipotesi precedente.

# L’alibi perfetto

La facilità è strettamente correlata alle proprietà intrinseche delle tecnologie informatiche, quali:

**IMMATERIALITÀ**. Un’informazione digitale è immateriale e, di conseguenza, non contiene elementi fisici che possano caratterizzarla come il DNA, le impronte o altre tracce. Un file copiato è identico all’originale

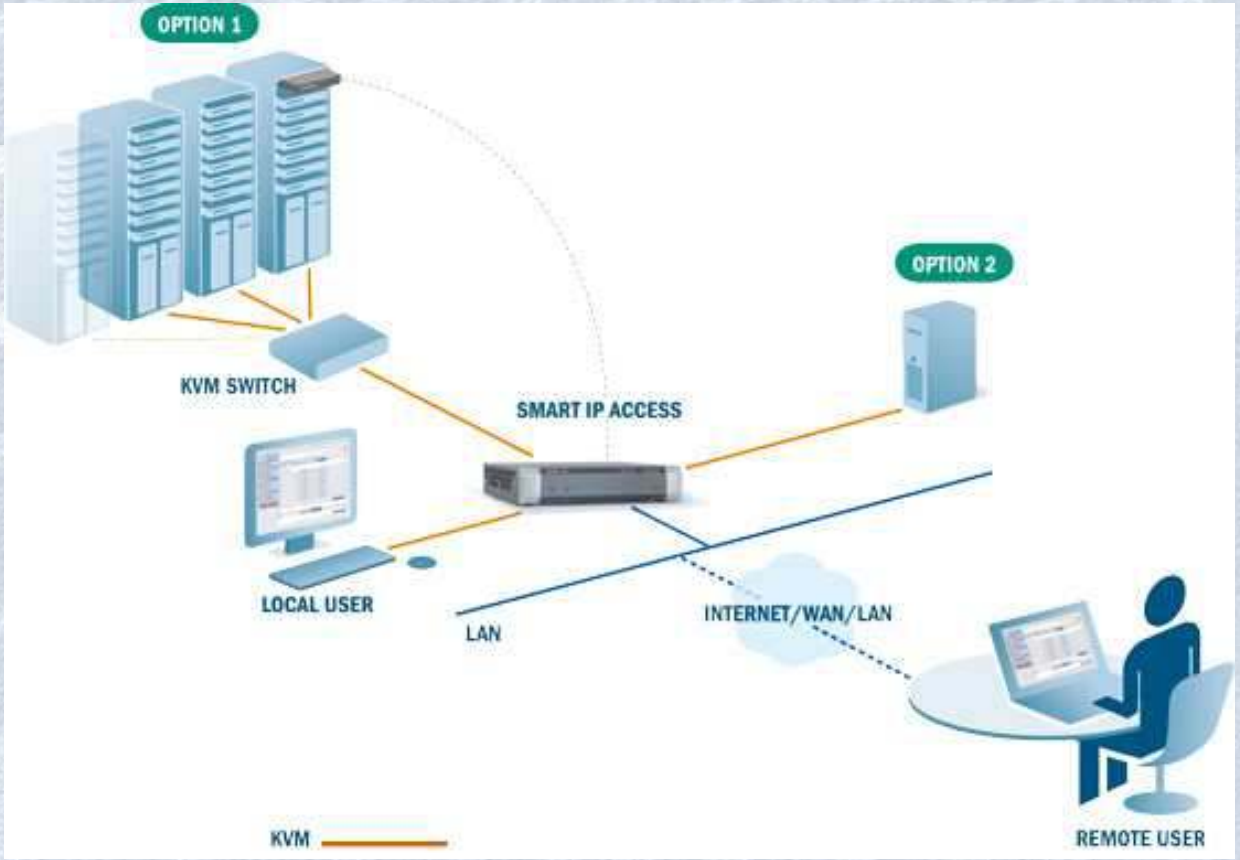
**ANONIMATO**. La maggior parte delle transazioni in rete avviene in forma anonima o, peggio, attraverso l’utilizzo di false credenziali.

**VIRTUALIZZAZIONE**. E’ tecnicamente possibile realizzare o modificare prove informatiche che riportano date e luoghi opportuni.

**MEDIAZIONE TECNOLOGICA**. Tutte le azioni informatiche e telematiche si realizzano con l’uso di tecnologie informatiche, per cui lo strumento diventa spesso il mezzo di formazione e di conservazione della prova. Ciò può dar luogo a situazioni di auto formazione, ovvero prove che si creano automaticamente o in modo indipendente.

Primo esempio

# Connessione remota tramite KVM over IP



secondo esempio

# Connessione remota tramite Software


Terzo esempio

# Simulare, attraverso automatismi, l'utilizzo di un computer

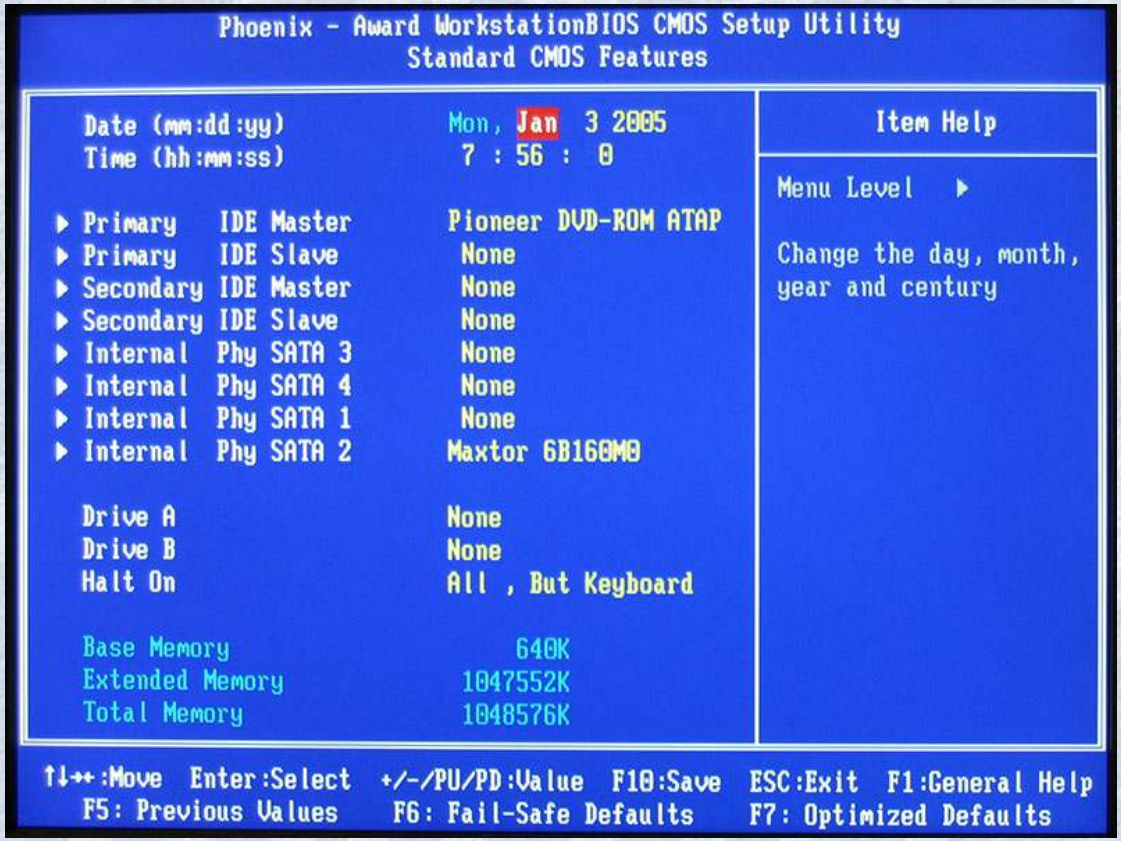
*# script che simula la digitazione di un documento Word e la navigazione di siti Internet*

```
send ("#m")
MouseClick("leA",630,250,2)
WinWaitAcIve("tesi","")
MouseClick("leA",255,120,2)
WinWaitAcIve("Doc")
send ("Testo che voglio scrivere")
send ("{Enter}")
send ("{Enter}")
send ("{Enter}")
sleep (5000)
send ("Altro testo che voglio scrivere")
run ("C:\Program Files\Mozilla Firefox\firefox.exe")
send ("^t")
send ("www.google.it")
send ("{ENTER}")
send ("Notizie per la mia tesi")
send ("{ENTER}")
```


Quarto esempio

# Realizzare una prova ex novo, prima o dopo un determinato evento

Spostiamo la data del Bios al momento desiderato, effettuiamo delle operazioni e ripristiniamo l'orario



# Conclusioni

- *E’ possibile provare con certezza che un determinato soggetto sia intento ad utilizzare un Personal Computer in un determinato momento?*

**NO**

- *Tale prove sono utilizzabili come alibi?*

**NO**

- *L’alibi in oggetto è affidabile ?*

**NO**

# Grazie per l’attenzione

www.vincenzocalabro.it