Alibi Informatico

Prof. Sebastiano Battiato

A.A. 2023/2024

Corso di Laurea in Informatica
Università di Catania
Dipartimento di Matematica e Informatica

IMAGE PROCESSING LABORATORY

1

Premesse

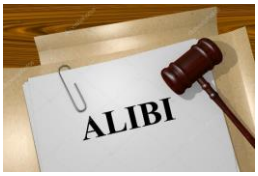
Il ricorso sempre più massiccio all'uso di strumenti elettronici, informatici e telematici per lo svolgimento di attività lavorative e ricreative, ha determinato una enorme produzione di dati digitali.

Ci prefiggiamo l'obiettivo di illustrare in quali casi l'attività informatica, svolta dall'indiziato, sia stata utile all'accertamento della verità e i casi in cui, con l'ausilio della tecnica, sia stato reso possibile precostituire un **alibi** ricorrendo a tecniche di **antiforensics**.

- Il termine ***alibi*** deriva dal latino col significato di "altrove", "in altro luogo", ecc.

2

Premesse



L'alibi rappresenta l'*"altro luogo"* in cui si trovava l'indiziato nello stesso arco temporale in cui veniva commesso un delitto.

Il termine, in ambito giudiziario, appare suscettibile di assurgere ad elemento di prova se corroborato da elementi di riscontro **oggettivi** capaci di dimostrare appunto che al momento in cui veniva commesso il reato, l'indiziato, nello stesso orario, si **trovava** in un **luogo** diverso.

- Distinzione tra **alibi** e **cause di giustificazione**

Premesse

- L'alibi, indica la "**non presenza**" dell'indiziato sul luogo del delitto che quindi esclude la sua partecipazione all'azione delittuosa.

- Infatti, all'esito della celebrazione di un processo penale, il giudice, in presenza di un alibi (di ferro) deve emettere sentenza di assoluzione nei confronti dell'imputato "**per non aver commesso il fatto**"; viceversa, se si trovasse a decidere il caso giudiziario di un soggetto che ha agito in presenza di una causa di giustificazione, dovrà emettere sentenza di assoluzione "perché il fatto non costituisce reato".

Aspetti Generali

Per "alibi" 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.

E’ volta a dimostrare che il soggetto indagato/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.

Aspetti Generali

Trattasi di una prova o dimostrazione logico-fattuale controdeduttiva, rispetto alle tesi accusatorie, proposta dalla difesa al fine di minare elementi fondamentali della ricostruzione avversa e ciò si dice in un' ottica che, pur nella "parità" fra accusa e difesa prevista nel nostro ordinamento processuale, vede comunque solo la prima tenuta a dimostrare puntualmente tutti i suoi assunti e percorsi "**oltre ogni ragionevole dubbio**“.

Per la difesa è sufficiente che le stesse siano ragionevoli e coerenti e tali da impedire all' accusa il raggiungimento di detto punto di certezza.

Aspetti Generali

Il trovarsi "in altro luogo" infatti, può e deve essere inteso sia in senso letterale che nel senso figurato di non essersi trovato in situazione tale da poter commettere il reato;

Doppia proposizione da dimostrare:

- **negativa** il "non essere nel luogo" e
- **positiva** "perché si è in altro luogo".

Il tutto legato dalla dimostrazione dell'impossibilità, per ragioni di spazio e di tempo, di trascendere dall'uno all' altro dei luoghi individuati al momento della commissione del fatto.

Su questi elementi interviene l'opera ricostruttiva dei consulenti, chiamati a coadiuvare i singoli soggetti del procedimento con le loro indagini.

Aspetti Generali

E' ovvio che tali ragioni e tali percorsi mutino grandemente di significato allorquando la commissione del reato avvenga (e quindi la condotta si svolga) in tutto o in parte non in un ambito meramente "fisico", ma coinvolga ambiti "**virtuali**" per esempio sul **Web**; oppure quando tracce ed elementi di prova attingano detti ambiti (ad esempio indagini su supporti o **sistemi informatici**, collegati o meno alla rete, volte alla dimostrazione dello svolgimento di "attività informatica" in un certo luogo da parte di un certo soggetto).

Aspetti Generali

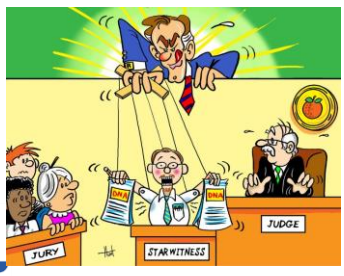
- I fatti, le condotte, gli eventi e le relative dimostrazioni, dirette, indirette e contrarie dovranno, quindi tener conto del "luogo" ove si svolgono (o si sarebbero svolti) i fatti, sia per la loro ricostruzione, sia per la loro acquisizione processuale, sia, infine, per la loro valutazione.

- Alibi come **scelta difensiva**:
  - **Assenza di Alibi non implica colpevolezza**
  - **Fallimento dell'alibi**

Aspetti Generali

Falso Alibi

Il rilievo della falsità dell'alibi, come la dimostrazione del fatto che lo stesso era stato artatamente preordinato o si è dimostrato puramente mendace, può essere (ma non deve, mancando una *regula iuris* in proposito) "posto in correlazione con altre circostanze di prova a carico e valutato come indizio, nel contesto delle complessive risultanze probatorie, se appaia finalizzato alla sottrazione del reo alla giustizia".



Alibi: Esempio di Procedure Operative

Fase 1:

dichiarazione di quanto ricorda l'indagato;

Fase 2:

ricerca di ulteriori informazioni a sostegno dell'alibi. Tale fase può essere curata sia dallo stesso indagato che dagli investigatori.

Alibi: Esempio di Procedure Operative

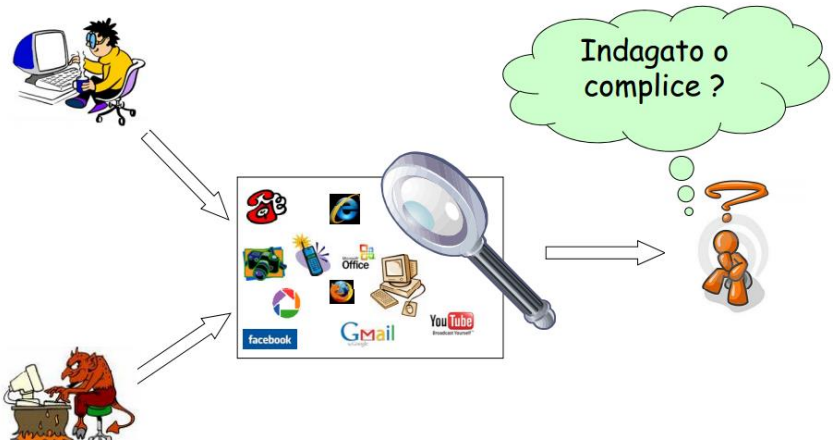
Il processo si sposta, successivamente, nel dominio della "**credibilità**" che riguarda come le persone accertano e valutano alibi:

Valutazione:

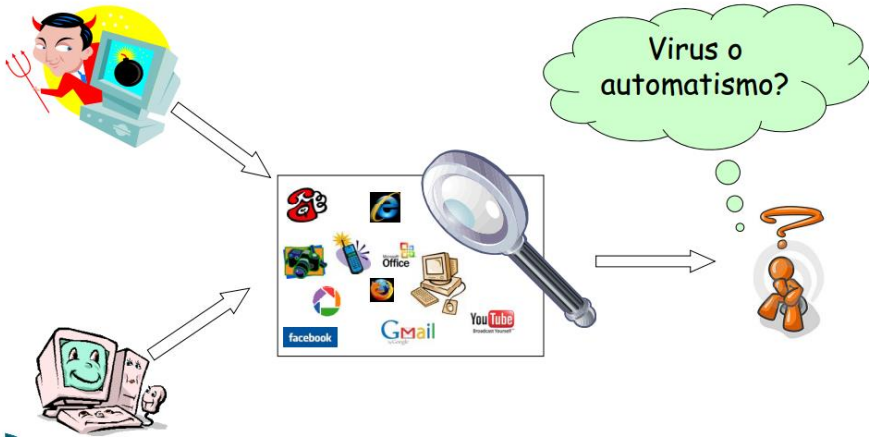
è svolta, come detto, nella fase preliminare delle indagini, da chiunque ne abbia necessità (investigatori, parti offese, avvocati);

Finalizzazione:

un alibi non sempre arriva a questa fase. Si tratta del caso in cui la valutazione sia stata costruita da chi ne abbia avuto interesse e quindi ora tale analisi è rimessa al dibattimento e alla decisione del Giudice. In questa delicata fase si ricostruirà quanto studiato nelle fasi precedenti e si verificherà la consistenza dell'alibi all'interno di un più ampio contesto investigativo.


Indagato o complice ?
Office
facebook
Gmail
YouTube

13


Virus o automatismo?
Office
facebook
Gmail
YouTube

14

Caso «Geri» (1999)

Alessandro Geri, ritenuto "il telefonista" delle Brigate Rosse coinvolte nell'omicidio del Prof. Massimo D'Antona, viene scagionato grazie ad una consulenza tecnica espletata su alcuni file presenti su un **floppy disk** acquisito dagli investigatori, che fornirono l'alibi già nella prima fase delle indagini.

Nella memoria principale del dischetto i tecnici rinvennero e sottoposero ad esame una ventina di lavori; mentre nella memoria secondaria ne furono rinvenuti soltanto cinque. Il primo file risultava salvato alle **18.03** mentre l'ultimo alle **19.32**. La rivendicazione dell'attentato, da parte dei terroristi al Corriere della Sera, risultava essere avvenuta alle **19.04**. I magistrati requirenti, in possesso anche di altri elementi di prova utili a ricostruire l'attività svolta dall'indiziato in concomitanza con le fasi dell'agguato, hanno ritenuto **attendibile** l'alibi informatico sebbene i file recassero la data del 20 maggio 1990 anziché la data del 20 maggio 1999, giorno in cui si erano verificati i gravi fatti di sangue.

Caso «Douglas Plude» (1999)

On the night of October 21, shortly before Genell died, both computers were active around 10 p.m. Genell's computer shows the user conducted online searches for information on Fioricet. Plude's computer shows Internet activity and use of a photo editing program between 10 p.m. and 10:30 p.m.

Caso «Douglas Plude» (1999)

L'alibi fornito tendeva a dimostrare che la moglie, la sera stessa del decesso, aveva navigato sul suo **notebook** ed aveva aperto la pagina web dedicata a tale farmaco per verificare gli effetti mortali che derivavano dall'assunzione di dosi massicce e quindi col chiaro intendo di suicidarsi. Tutto ciò avveniva nello stesso momento in cui l'indiziato era impegnato ad editare foto sul proprio portatile.

Ebbene il giudice **non ha ritenuto degno di credibilità l'alibi** argomentando:

che risultava visionata la sola pagina relativa al farmaco e non erano state consultate le parti di essa che trattavano del dosaggio;

che, tutto sommato, lo stesso indiziato avrebbe potuto usare entrambi i computer, visto che erano portatili e facilmente collocabili in prossimità dell'operatore.

«Strage di Duisburg/ Faida di San Luca» (2006)

Viene casualmente ritrovata una cassetta, in cui l'imputato festeggia con i parenti il Natale

- **Perizia di parte** ne avvalora l'autenticità entrando anche nel merito del filmato (trasmissioni televisive, coincidenze sugli orari, ecc.)
- **Perizia dell'accusa** controbatte nel merito (luce, orari, ecc.)
- …..

«Strage di Duisburg/ Faida di Locri» (2006)
Perizia del Giudice

"Effettuino i periti una perizia finalizzata a verificare l'integrità del filmato girato con telecamera ad uso domestico il 25-12-XXXX, prodotto dalla difesa di XXXXXXXXXXX, tenendo conto della CTP ing. XXXXXX, della audizione dibattimentale di quest'ultimo, della memoria depositata, nonché delle dichiarazioni rese in dibattimento di tutti i documenti allegati alla relazione del consulente e alla deposizione del teste, esaminando il nastro originale (riproducente il filmato) ed il DVD."

Conclusione: FALSO ALIBI

Caso «Garlasco» (2007)

Tale caso giudiziario è caratterizzato da un serrato confronto tra risultati di analisi effettuati su ogni tipo di reperto: dal **DNA** su tracce ematiche alle digital evidence sui PC in uso alla vittima e all'indiziato. A tali accertamenti si sono affiancate anche tecniche tradizionali di ricerca di mezzi di prova consistiti nella raccolta di informazioni e testimonianze rese da soggetti informati sui fatti.

Quattro i tipi di accertamenti peritali

- **una perizia tecnico/informatica,**
- **una medico/legale,**
- **una chimico/ sperimentale e**
- **la quarta definita come "semi-virtuale" –**

ai quali si aggiungono le consulenze tecniche disposte dalle altre parti processuali.

Caso «Garlasco» (2007)

L'attenzione comunque si è focalizzata sull'accertamento dell'alibi digitale fornito da Stasi il quale ha dichiarato, offrendo agli inquirenti il proprio computer portatile affinché venisse analizzato, di essere stato a casa sua, distante circa 2 km dal luogo del delitto, a scrivere sul computer la tesi di laurea proprio nell'orario in cui Chiara sarebbe stata uccisa nonché di aver effettuato alcune telefonate sull'utenza telefonica mobile della fidanzata.

Caso «Garlasco» (2007)

motivazione sentenza:

"…. tenuto conto della grave anomalia rappresentata dalle alterazioni del contenuto informativo dovute agli accessi dei carabinieri che ben potevano aver determinato la cancellazione delle normali evidenze presenti all'interno del sistema operativo …i metadati ed il loro contenuto attestano con certezza … l'interazione diretta e sostanzialmente continuativa dell'utente con il computer dalle ore 10.17 fino alle ore 12.20 del giorno 13 agosto".

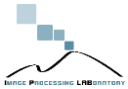
Ciò significa che l'alibi digitale, sebbene minato da errori ……. sembra aver fornito al giudice la chiave per "collocare" l'indiziato al lavoro davanti al suo computer portatile in quel lasso di tempo critico correlato all'omicidio della sua fidanzata".

Caso «Meredith Kercher» (2007)

The police computer analysts told the murder trial that there was "no trace of human interaction" on Mr Sollecito's computer between 9.10pm on Nov 1, 2007, and 5.32am the next morning – the period in which Miss Kercher was stabbed to death in a frenzied attack at her flat.

The police computer expert, said that an examination of Mr Sollecito's laptop showed that the film had been watched from around 6.30pm that evening.

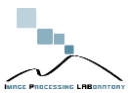
The next sign of activity on the computer was at 9.10pm at around the time Miss Kercher was heading home after eating pizza and apple crumble with a group of English friends. The laptop was then untouched until 5.32am, the officer told the court.



Caso «Meredith Kercher» (2007)

- I consulenti tecnici hanno sostenuto che non era stata riscontrata "**alcuna traccia di interazione umana**" sul computer di Sollecito nell'arco temporale, compreso tra le 21,10 e le 05,32 della mattina successiva, coincidente con l'arco temporale in cui risulta essere stata barbaramente accoltellata la studentessa inglese nel suo appartamento di Perugia.

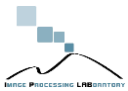
- In tale caso la inattività del PC, ovvero la mancata interazione tra l'utente ed il PC, ha dato al giudice la possibilità di ritenere inattendibile l'alibi informatico addotto dalla difesa dell'indagato e di ritenere la sua presenza sul luogo dell'omicidio perfettamente compatibile con altre risultanze d'indagini.



Caso «Rodney Bradford» (2009)

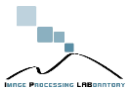
Bradford's defense lawyer said the young man couldn't have committed the crime because at the time of the robbery he posted a Facebook status update from a computer at his father's apartment in Harlem.
Message: "On the phone with this fat chick... ...where my IHOP."

...Result: "Facebook can keep you out of jail !"



Caso «Rodney Bradford» (2009)

Alle osservazioni mosse alla difesa di Rodney - nel senso che chiunque, amico o parente, al suo posto avrebbe potuto aggiornare il suo profilo dietro disposizioni impartite dallo stesso Rodney - l'avvocato difensore ha risposto che sebbene teoricamente possibile, nel caso di specie tale possibilità andava esclusa in quanto l' attività informatica preparatoria avrebbe connotato un livello di genio criminale inusuale in un ragazzo così giovane.



Verifica di un alibi

- Cerchiamo di capire come si possa dimostrare la solidità, od eventualmente l'inconsistenza, di un alibi, nella fattispecie, informatico.
- La verifica, che consiste nell'applicare il seguente schema di 8 domande:
  - cinque riguardano l'**oggetto**:
    «Chi», «Cosa», «Quando», «Dove», «Perché»
  - tre riguardano il **soggetto agente**:
    «Quanto», «In che modo», «Con quali mezzi»
- Difficilmente il consulente tecnico riuscirà a fornire una risposta a tutte le domande suggerite, ma tentare aiuta a rappresentare una evidenza digitale in maniera completa e consente, all'organo giudicante, di potersi determinare più facilmente circa l'eventuale ammissibilità o meno della stessa.

Alibi Informatico: classificazione

Se valutiamo la variabile tempo, possiamo distinguere due classi di alibi:

1. quelli generati durante, o **contemporaneamente**, l'evento criminoso;
2. quelli creati in un momento diverso, **antecedente** o **seguente**, dell'atto delittuoso.

Contemporaneità

Le tracce informatiche sono prodotte nello stesso istante in cui si consuma il reato.

Distinguiamo quattro fattispecie:

a. l'imputato ha generato direttamente tracce informatiche su dispositivi distanti dalla scena del crimine;
b. 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;
c. un terzo, persona fisica o sistema automatico, ha registrato tracce che potrebbero giustificare la presenza dell'imputato in luoghi diversi dalla scena del crimine;
d. 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.

Falso Alibi

In questa ultima categoria possiamo distinguere altre due fattispecie in aggiunta alle precedenti:

1. 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.
2. 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

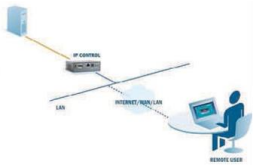
- **Ipotesi A** - L'imputato ha generato direttamente tracce informatiche a distanza.
- **Ipotesi B** - Un sistema automatizzato ha simulato un utilizzo in presenza.
- **Ipotesi C** - Un terzo, persona fisica o sistema automatizzato, ha registrato tracce informatiche.
- **Ipotesi D** - Un complice ha eseguito azioni per conto dell'indiziato.
- **Ipotesi E** - L'indiziato (o chi per lui) realizza una prova ex novo.
- **Ipotesi F** - L'indiziato (o chi per lui) riutilizza una traccia informatica già esistente.

Esempio (1/2)

Creazione alibi:

1. Ci procuriamo una console KVM over IP;
2. Assegniamo un indirizzo IP statico alla console per evitare che il DHCP server registri il mac address della stessa;
3. Abilitiamo, sul router, il port per la connessione in entrata e la regola di inoltro specifica per la console;
4. Configuriamo il servizio DNS dinamico (presente su tutti i router commerciali);
5. Colleghiamo la console al router;
6. Scolleghiamo la tastiera, il mouse ed il video da pc e connettiamo la console KVM;

Esempio (2/2)



7. Accendiamo il personal computer;
8. Ci connettiamo, da un luogo a distanza, attraverso un browser web, utilizzando il nome mnemonico registrato, da un'altra postazione (o con un dispositivo mobile) ed utilizziamo alcune applicazione presenti sul personal computer;
9. Ritornati a casa, spegniamo il pc, scolleghiamo e occultiamo la console KVM;
10. Resettiamo il router ripristinando le impostazioni di default.

Analisi

Personal computer

1. L'analisi del file di registro e del file system confermano l'utilizzo delle applicazioni e la creazione delle digital evidence che sono state esibite dall'imputato;
2. La time-line di accensione conferma gli orari di creazione e modifica dei file;
3. Viene rilevato del traffico di rete;
4. Il firewall è abilitato con tutti i port chiusi;
5. Non è presente alcun software di gestione remota.

Analisi

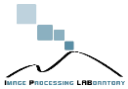
Router

1. E' impostato con i parametri di default; Il firewall è abilitato;
2. Dai file di log si rileva che è stato riavviato in un momento successivo alla data e ora dell'alibi; Non vi sono tracce di collegamenti antecedenti alla data ed ora del riavvio.

Tabulati del traffico dati

1. Si rileva traffico entrante, per gran parte, coincidente con quello presente sul pc;
2. Si rileva traffico uscente, proveniente da indirizzo IP afferenti ad alcuni internet service provider, non riscontrabile sul pc.

Soluzione: In presenza di queste evidenze non si potrà affermare che l'alibi sia falso.



Altre tipologie (da approfondire)

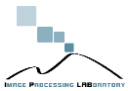
- **Connessione remota tramite Software**

  Controllo Remoto (es. Team Viewer su USB)

- **Simulare, attraverso automatismi, l'utilizzo di un computer.**

  Utilizzo di Linguaggi di Scripting

- **Realizzare una prova ex novo, prima o dopo un determinato evento.**



Evidenze digitali automatismo “indesiderate”

- Script che ha prodotto **l’alibi digitale**
- Tracce esecuzione script
  - **Registro di sistema**
  - **Prefetch**
  - **File memoria virtuale**
- **Evidenze digitali sospette** (potrebbero essere state utili per la costruzione di un automatismo)
  - Esecuzione di programmi o comandi sospetti
  - Presenza degli strumenti per la produzione dello script o per la sua esecuzione
  - Tracce dell’attività necessaria per la produzione dello script

Metodologia creazione automatismo per un generico sistema operativo

- Automatizzare alibi
- Analisi rilevamento tracce
- Impostazioni S.O. per **minimizzare tracce**
- Rendere “**indistinguibile**” l’esecuzione automatica da quella umana. Cancellare solo le “poche” tracce connesse all’esistenza dell’automatismo (dopo la sua esecuzione) che proverebbero che è stato eseguito da uno script anziché dall’uomo
- Verificare se rimangono tracce digitali “indesiderate”, nel caso ripetere il processo dall’inizio

E' necessario essere un hacker esperto?

Automazione	Facile
Cancellazione tracce indesiderate	Abbastanza facile
Autocancellazione	Non facile
In alternativa, cancellazione manuale / supporto CD / DVD / Pendrive	Abbastanza facile

Occorrono strumenti costosi/illeciti/introvabili?

No, comune computer e software freeware!

Conclusioni

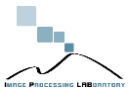
- Nel caso della ***computer forensics***, il mutamento e l'evoluzione coinvolgono radicalmente non soltanto i tool e le metodiche necessari per l'individuazione, repertamento ed analisi delle tracce digitali ma anche le componenti strutturali ed elettroniche degli stessi "fenomeni" oggetto dell'analisi.

- Risulta evidente la necessità di ricorrere, non solo ad un costante ammodernamento degli strumenti di ***forensic analisys***, ma anche ad un aggiornamento delle stesse tecniche di analisi e delle conoscenze di base in materia (ad esempio comportamento ed interazione dei programmi, etc.).

Referenze

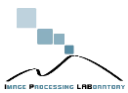
L'alibi Informatico: Aspetti Tecnici e Giuridici – V. Calabrò, G. Costabile, S. FratePietro, M.Ianulardo, G. Nicosia – Cap12 – IISFA Memberbook 2010

Automated Construction of a False Digital Alibi – A. De Santis, A. Castiglione, G. Cattaneo, G. De Maio, M. Ianulardo – ARES 11' Proceedings



Altri approfondimenti

- Software di Scripting per i vari SO (Es, AutoIT x Windows)
- Cancellazione (autocancellazione)
- Analisi di Registro
- Utilizzo di SW installato su periferiche esterne (USB Pen Drive)
- Automatizzazione invio telefonate ed SMS

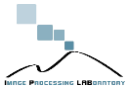


Esercitazione opzionale

Create ad-hoc un falso alibi informatico su un dato device e un dato SO

Analizzate il caso da un punto di vista tecnico e presupponendo che siano state attuate o meno opportune tecniche di (antiforensics)

Lavorare in gruppi di 2-3 persone.



Contatti

- Per ulteriori dettagli o info si visiti il sito
  www.dmi.unict.it/~battiato/CF
- Email
  battiato@dmi.unict.it