

# Lezione 1: introduzione alla Computer Forensics



A.A. 2021/22

Dott. Lorenzo LAURATO



# Cosa è la Computer Forensics?



# Cosa è la Computer Forensics?

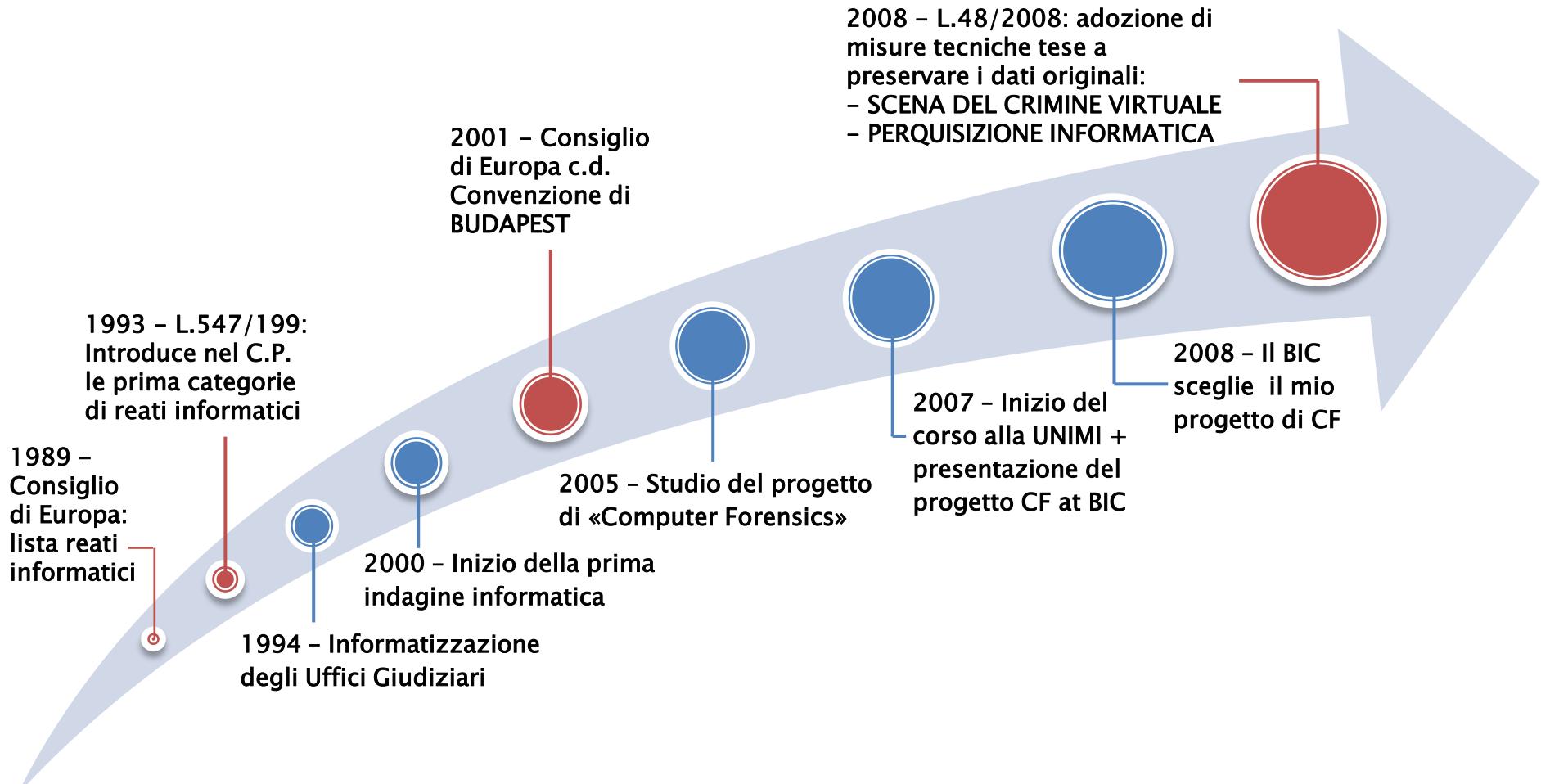
l'insieme di metodologie  
scientificamente provate  
finalizzate alla ricostruzione  
di eventi ai fini probatori che  
coinvolgono direttamente o  
indirettamente  
un supporto digitale

# Lorenzo LAURATO

» la mia storia



# Nascita di un COMPUTER FORENSER...





# ... l'IDEA ...

naturale conseguenza delle  
attività presso gli Uffici  
Giudiziari, nasce dalla  
presa di coscienza del  
problema della “gestione”  
di un reperto digitale

# Nel 2011 nasce...



# Cerimonia di consegna dei premi alla “Giornata dell’Innovazione”



# Interesse dei Media al progetto:

## Sicurezza informatica, gli «acchiappa-criminali» della Rete

### La storia

Così gli 007 della Ssrl cercano negli hard disk le prove dei reati

### Dilettu Capissi

Giustizia computerizzata, informatizzata, più precisa. Che diventa supporto essenziale per le indagini e, soprattutto, per stabilire l'innocenza o la colpevolezza dell'indagato. Ma anche per contrastare l'altra faccia della medaglia, la criminalità informatica: quella dei pedofili, per capirli. O ancora per rintracciare e stancare gli hacker che devastano siti sensibili. È la Computer Forensics, attività all'avanguardia che tuttavia già opera. Per esempio a Napoli. In che modo lo racconta Lorenzo Laurato, 42 anni, amministratore della Ssrl, Sicurezza Sistemi Reti Informatiche. Di cosa stiamo parlando? «È un'attività che consente di analizzare hard disk o altri media digitali alla ricerca di tracce, di informazioni nascoste, di alterazioni o di cancellazioni - spiega Laurato -. La computer forensics ha delle regole, delle procedure e questo significa apprezzamenti, software sofisticati e competenze in continuo aggiornamento». Quando intervenite? Laurato parla con l'orgoglio che nasce dalla competenza: «La delicatezza sta nel-



la gestione del dato che, oltre all'acquisizione, ne prevede principalmente la cristallizzazione». Che significa? «Significa fermarlo a quell'istante in cui avviene un determinato fatto, è un aspetto importante perché può diventare la prova portata in dibattimento. Un esempio eclatante è il caso Garlasco, in cui bisognava controllare l'ora esatta in cui era stato acceso il computer. Bisogna fare in modo da non perdere l'informazione e noi con le nostre strumentazioni riusciamo a lavorare su questo». Insomma una grande responsabilità? «Sicuro - pun-

tualizza Laurato -. Il computer parla, ti racconta tutto. Non ci si può consentire di perdere alcune informazioni fondamentali per il dibattimento». A Laurato piace raccontare come è nata la sua passione per l'informatica. «La mia prima assunzione fu in un'azienda napoletana che cercava del personale per informatizzare gli uffici giudiziari e da lì è cominciata la mia esperienza nel settore del computer forensics. Intuii che questa attività sarebbe esplosa. Adesso mi sto specializzando in sicurezza dei dati informatici, studiando anche diritto pena-

### L'esempio

«Per il caso Garlasco recuperata l'ora di accensione del pc»

### Gli affari

«Siamo un'azienda che fattura poco ma stiamo crescendo»

Il pool Lorenzo Laurato con i suoi collaboratori Marco e Davide



### La scheda

#### Nome società

SSRI - Sicurezza Sistemi Reti Informatiche sas



#### Sede

Via Coroglio 57/D Napoli

La società, nata nel 2010, è specializzata nelle attività di Computer Forensics e di Sicurezza Informatica ed effettua analisi su apparecchiature elettroniche: personal computer, per drive, telefoni cellulari, carte di credito. I crimini informatici riguardano: il sabotaggio, l'intrusione, la falsificazione dei dati e l'aggravamento, la ricerca fraudolenta di informazioni, le intercettazioni, il codice malinteso (malicious code).

#### Amministratore delegato

Lorenzo Laurato, 42 anni, perito informatico e laureando in sicurezza dei dati



#### Collaboratori

Marco Alfè e Davide Barbato



#### Fatturato

200.000 euro

#### I Principali Clienti

Procurie della Repubblica e Tribunali della Campania, Lombardia, Lazio. Studi Legali di alto profilo.



pire che le competenze sono alte e che l'informatica può dare una grande mano. Purtroppo il ministero della Giustizia non ha molti soldi per pagare questo tipo di consulenza». Vi colpisce la crisi economica? Laurato stava sollevato sorride: «Paradossalmente è il contrario». In che senso? «Nel senso che i reati finanziari sono in aumento. Ad esempio c'è un furto di identità in costante crescita. Vengono fuori polizze di assicurazione false, documenti falsi per attivare finanziamenti».

© RIPRODUZIONE RISERVATA

Composite IL\_MATTINO - NAZIONALE - 55 - 07/04/12 ---  
Time: 06/04/12 22:38



# 2011 – 2021: Business area



# Collaborazioni Universitarie:



Università degli Studi di Napoli «Federico II»:  
Seminari di Computer Forensics

Università degli Studi di Milano «La Statale»:  
Assistente dei corsi di «Computer Forensics» e  
«Gestione della sicurezza nei sistemi informativi»

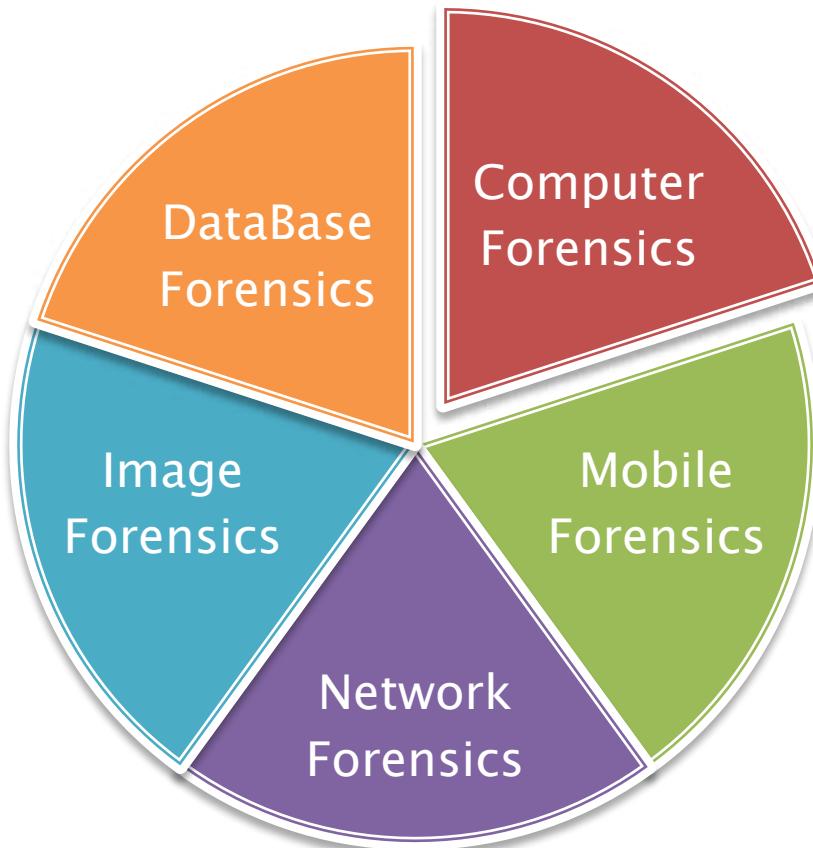


# Digital Forensics

» Introduzione



# Digital Forensics



# Campo d'azione

## Digital Forensics

Consulente Tecnico



Forze dell'ordine



Cyber Security Office



# Cyber Crime

Does Cybercrime Really Cost \$1 Trillion?



National Security Agency Director Gen. Keith Alexander speaks about cybersecurity and the new threats posed to the U.S. economy and military at the American Enterprise Institute in Washington, D.C., on July 9, 2012. (Chip Somodevilla/Getty Images)

by Peter Maass and Megha Rajagopalan  
ProPublica. Aug. 1, 2012. 11:12 a.m.

## An Economic Map of Cybercrime (Working Paper)

Alvaro A. Cárdenas,<sup>1</sup> Svetlana Radosavac,<sup>2</sup> Jens Grossklags,<sup>1</sup>  
John Chuang,<sup>1</sup> Chris Hoofnagle<sup>1</sup>

<sup>1</sup> University of California, Berkeley

<sup>2</sup> DOCOMO Communications Laboratories USA, Inc.

# Panorama Giuridico: evoluzione normativa

*Danneggiamento di S.I. art. 635 bis C.P.*

*Accesso abusivo a S.I. art. 615 ter C.P.*

*Diffusione di programmi infetti art. 615 quinque C.P.*

*Frode informatica art. 640 ter C.P.*

1989 –  
Consiglio di  
Europa:  
lista reati  
informatici

1993 –  
L.547/1993:  
Introduce nel C.P.  
le prima categorie  
di reati informatici

2001 –  
Consiglio di  
Europa c.d.  
Convenzione  
di BUDAPEST

2008 – L.48/2008:  
adozione di misure  
tecniche tese a  
preservare i dati  
originali:  
– SCENA DEL  
CRIMINE VIRTUALE  
– PERQUISIZIONE  
INFORMATICA

# Panorama Giuridico: procedimento penale e civile

CTU  
CTP  
Perito



GIP  
GUP  
Giudice



Persona Offesa  
Indagato  
Imputato



Pubblico Ministero  
Avvocato



# Metodologie

Identificazione

Raccolta

Validazione

Preservazione

Analisi

Interpretazione

Documentazione

Presentazione

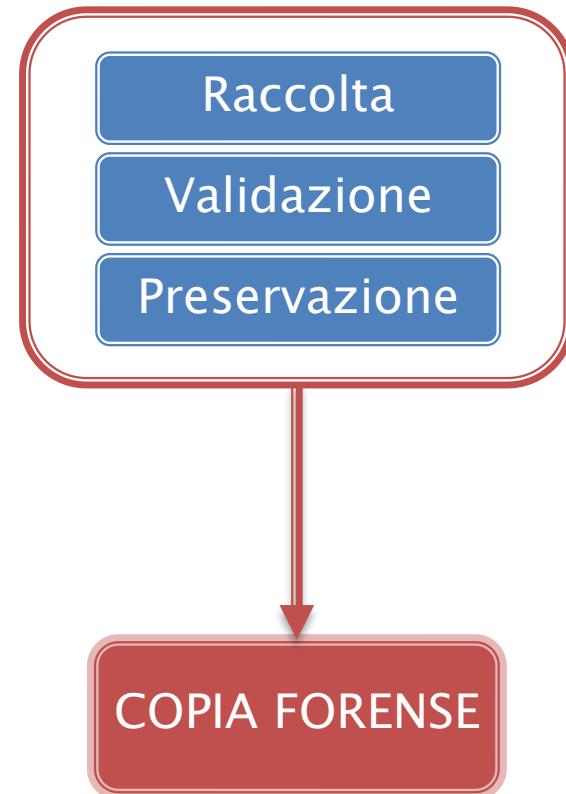
# Metodologie

## Identificazione

**individuare i dispositivi che possono contenere  
dati rilevanti**



# Metodologie



# Metodologie

Analisi

Interpretazione



# Metodologie

Documentazione

Presentazione



# Metodologie



Scienza  
*VS*  
Legge





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# Lezione 2: Il procedimento penale e civile

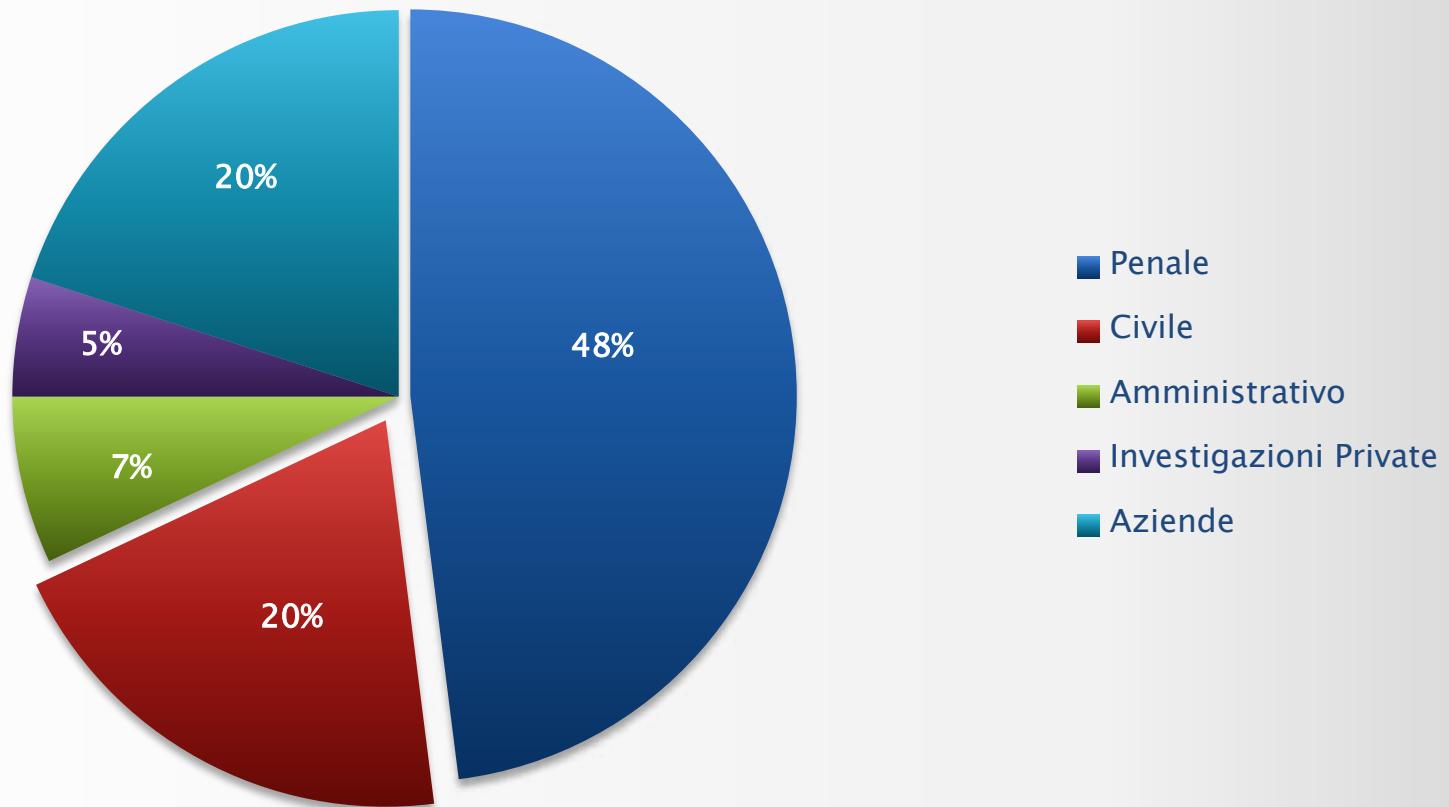


A.A. 2021/22

Dott. Lorenzo LAURATO



# Area di attività del C.F.



# Procedimento Penale

## » Introduzione





### Procura della Repubblica

Il Pubblico Ministero Gestisce  
le Indagini ed ha il potere di  
esercitare l'azione penale

### Tribunale

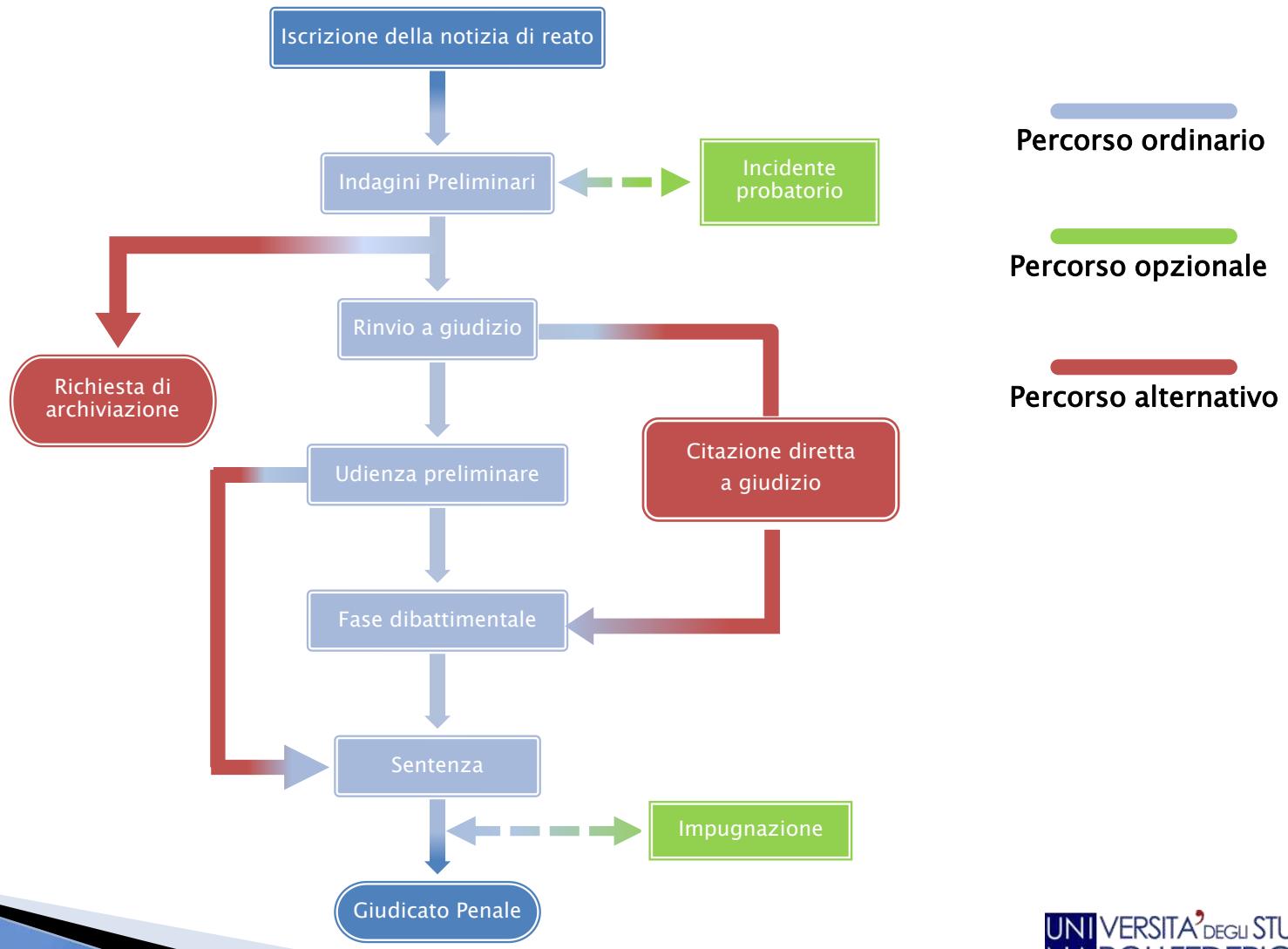
Il Giudice valuta le tesi  
accusatorie e difensive.  
**CONDANNA o ASSOLVE**

# Procura della Repubblica

# Tribunale



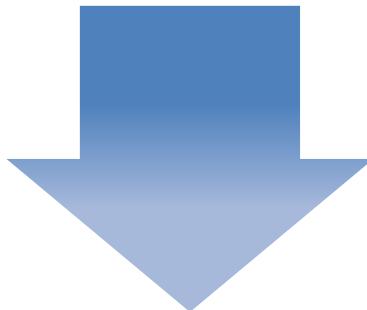
# Procedimento Penale



# Procedimento Penale:

## *fase iniziale*

Iscrizione della notizia di reato



Indagini Preliminari

Quando le autorità giudiziarie ricevono una notizia di reato da parte di un'altra autorità o da un soggetto (persona offesa o testimone), il Pubblico Ministero (P.M.) iscrive tale notizia su un apposito registro: Registro Generale Notizie di Reato (R.G.N.R.)

il P.M. e la Polizia Giudiziaria (PG) svolgono le indagini ritenute necessarie per poter verificare l'attendibilità della notizia di reato, cercando le prove e stabilendo se vi siano o meno i presupposti utili per poter esercitare un'azione penale.

# Procedimento Penale: *le indagini preliminari*

- ▶ il P.M. e la polizia giudiziaria(P.G.) svolgeranno le indagini per appurare che il reato iscritto sussista.
- ▶ Il P.M. e la P.G. durante le indagini possono far uso di due strumenti giuridici: perquisizione e sequestro probatorio. Il primo è utilizzato per verificare la presenza di una prova di reato, il secondo, usato solitamente a seguito di un riscontro positivo del primo, è utilizzato per tutelare la prova da possibili alterazioni:
  - il sequestro probatorio è utilizzato anche in luogo di accertamento (*art.253 c.p.p.*), in pratica quando bisogna far uso di strumenti specifici che non si dispongono nell'immediatezza o quando i tempi di un accertamento possono essere lunghi.
  - Le autorità che hanno disposto un sequestro provvederanno a sigillare il materiale e a custodirlo.

***PARTE LA CATENA DI CUSTODIA***

# Procedimento Penale: *accertamento tecnico* (art. 359 cpp)

- ▶ il P.M. può avere la necessità di svolgere **accertamenti tecnici**, che comportano specifiche conoscenze scientifiche, tecniche o artistiche, che esulano dalle competenze possedute dall'organo inquirente.
- ▶ il P.M. può avvalersi/nominare un Consulente Tecnico.

# Procedimento Penale: *accertamento tecnico irripetibile* (art. 360 cpp)

- ▶ accertamenti che se compiuti comportano l'alterazione della prova e la ripetibilità della procedura non è più garantibile;
- ▶ il P.M. esegue questa attività di accertamento avvisando previamente:
  - l'*indagato* e il suo difensore;
  - la parte offesa e il suo difensore;

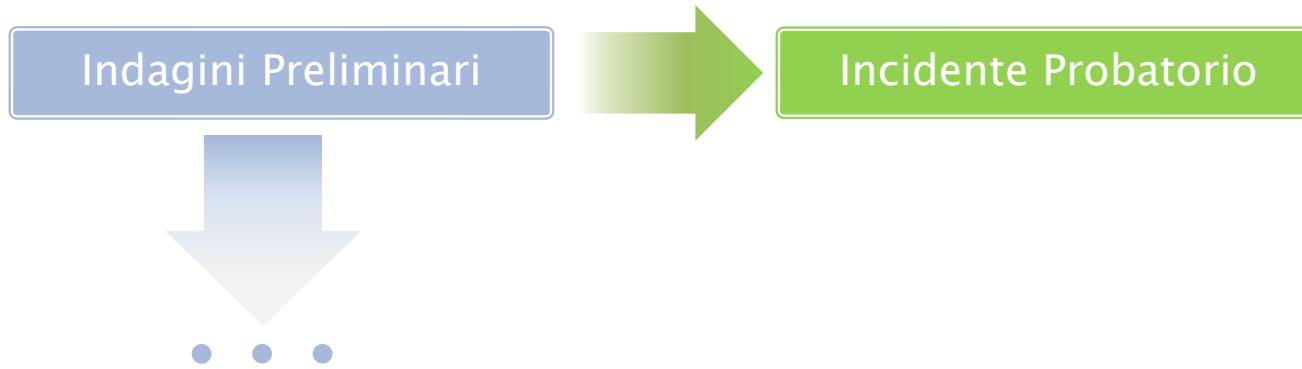
***IN CONTRADDITTORIO***

in modo da dare la possibilità a questi ultimi di assistere a tutta l'operazione a garanzia del rispetto delle procedure.
- ▶ Le parti hanno la facoltà di nominare un proprio Consulente Tecnico.

# Procedimento Penale: *misure cautelari*

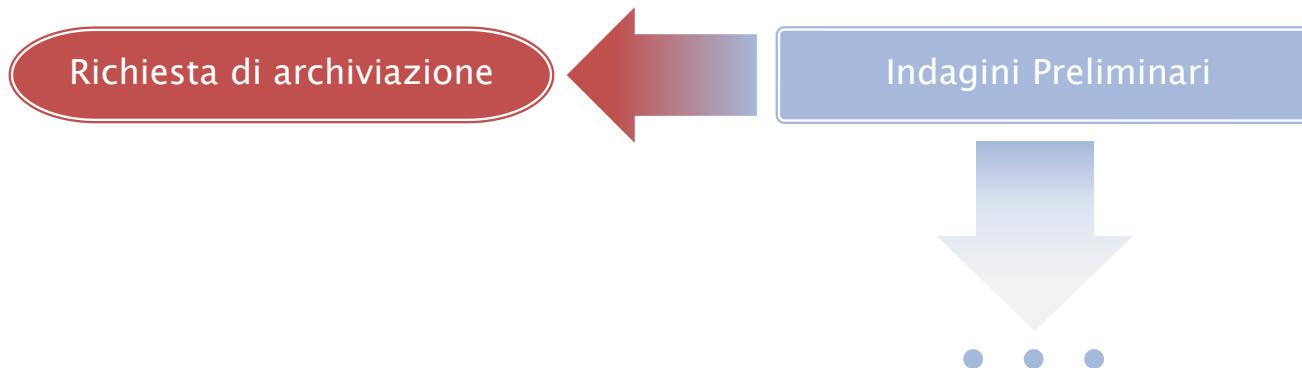
- ▶ sono dei provvedimenti emessi dal Giudice su richiesta del P.M. nel periodo intercorrente tra l'inizio del procedimento penale e l'emanazione della sentenza.
- ▶ **Misure reali:** impediscono la disposizione di determinati **beni o cose** (Es.: *Conti Corrente*);
- ▶ **Misure personali:** comportano una limitazione o privazione della **libertà personale** (*coercitive*), limitano temporaneamente l'esercizio di determinate facoltà o diritti (*interdittive*). Sono emesse quando sussistono i seguenti **rischi**:
  - inquinamento delle prove;
  - fuga dell'indagato/imputato;
  - reiterazione del reato;

# Procedimento Penale: *incidente probatorio*



- ▶ Può essere richiesta dalle parti ed ha la funzione di anticipare l'acquisizione e la formazione di una prova durante le indagini preliminari;
- ▶ Viene richiesta al Giudice per le Indagini Preliminari (GIP);
- ▶ Il GIP, nel caso in cui sono richieste particolari competenze tecniche, può nominare un proprio consulente tecnico: il Perito.

# Procedimento Penale: *richiesta di archiviazione*

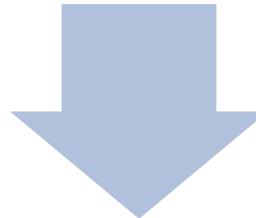


- ▶ Al termine delle Indagini Preliminari, il PM può presentare al GIP la richiesta di archiviazione nei seguenti casi:
  - gli elementi acquisiti nelle indagini non sono idonei a sostenere l'accusa;
  - l'autore del reato è rimasto ignoto;
  - il reato è estinto;
  - il fatto non è previsto dalla legge come reato;
  - Il fatto sia particolarmente tenue;
- ▶ La *parte offesa* può presentare una richiesta motivata di opposizione al GIP;

**AVVISO ARCHIVIAZIONE E PROROGA INDAGINI**

# Procedimento Penale: *rinvio a giudizio*

Indagini Preliminari

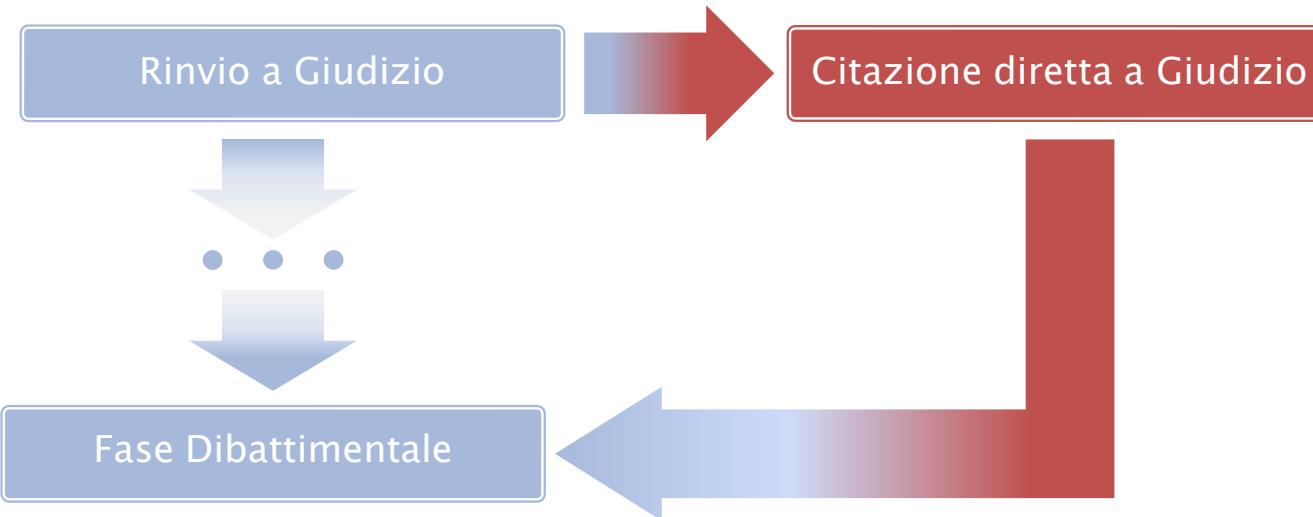


Rinvio a Giudizio

*Con l'avviso 415bis  
l'indagato ha 20  
giorni per depositare  
atti e memorie,  
chiedere ulteriori  
indagini o di essere  
sottoposto ad  
interrogatorio*

- ▶ la richiesta di rinvio a giudizio è l'atto con cui il Pubblico Ministero esercita l'azione penale;
- ▶ Avviso all'indagato della conclusione delle indagini preliminari (*art. 415bis c.p.p.*)
- ▶ Il P.M. indica il capo di imputazione dell'indagato;

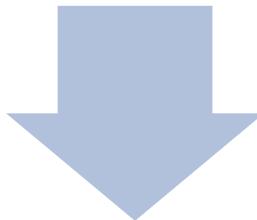
# Procedimento Penale: *citazione diretta a giudizio*



- ▶ E' esercitata dal Pubblico Ministero quando si tratta di:
  - delitti puniti con la pena della reclusione non superiore nel massimo a quattro anni;
  - violenza, minaccia o resistenza a un pubblico ufficiale;
  - oltraggio a un magistrato in udienza aggravato;
  - violazione di sigilli da parte del custode;
  - rissa aggravata senza gravi lesioni;
  - lesioni personali stradali;
  - furto aggravato;
  - ricettazione;

# Procedimento Penale: *udienza preliminare*

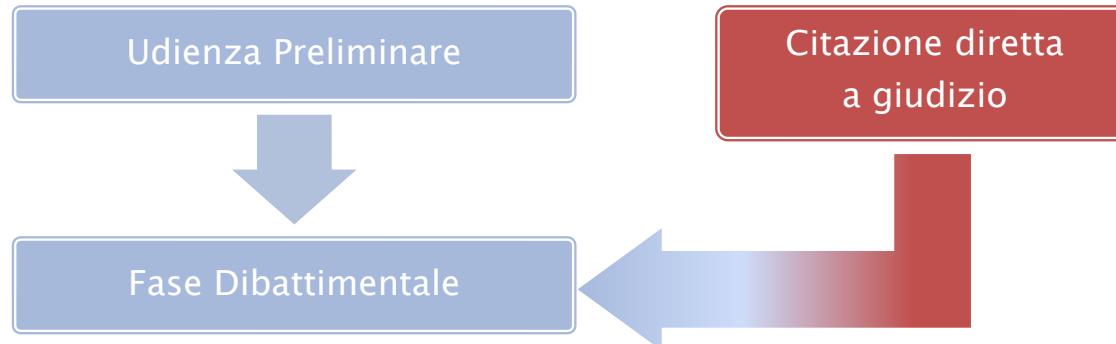
Rinvio a Giudizio



Udienza Preliminare

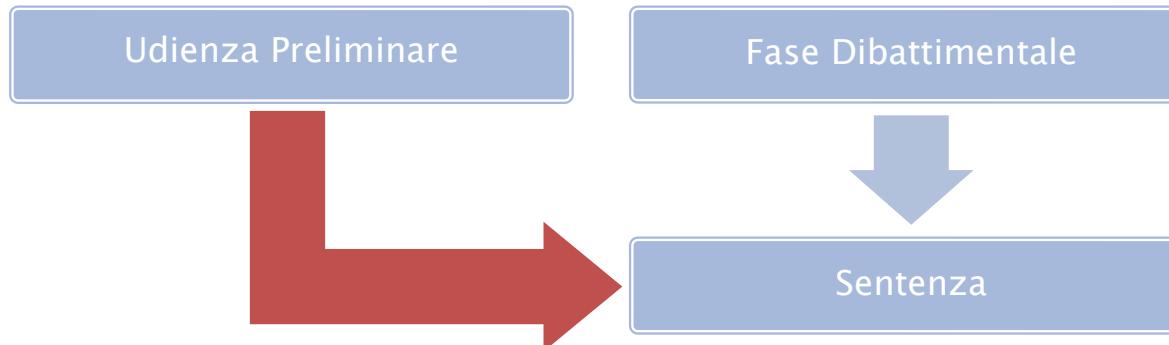
- ▶ Segna il passaggio dalla fase procedimentale a quella processuale;
- ▶ L'indagato si trasforma in imputato;
- ▶ Il GIP viene sostituito dal Giudice dell'Udienza Preliminare (GUP);
- ▶ L'imputato può richiedere al Giudice di:
  - essere prosciolto;
  - rinunciare alla fase dibattimentale (*rito alternativo*)

# Procedimento Penale: *fase dibattimentale*



- ▶ Il dibattimento è la fase centrale del processo penale, nella quale si procede alla raccolta e acquisizione delle prove nel rispetto del contraddittorio delle parti:
  - **prove documentali**: scritti o di altri documenti che rappresentano fatti, persone o cose attraverso la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.
  - **esame testimoniale** che consiste nella deposizione di un soggetto, sottoposto al vincolo del giuramento, su fatti rilevanti per il processo;
  - **la perizia** che è un mezzo di prova al quale si ricorre quando è necessario svolgere indagini o acquisire elementi o valutazioni che richiedono determinate competenze di tipo tecnico, scientifico o artistico;

# Procedimento Penale: *sentenza*

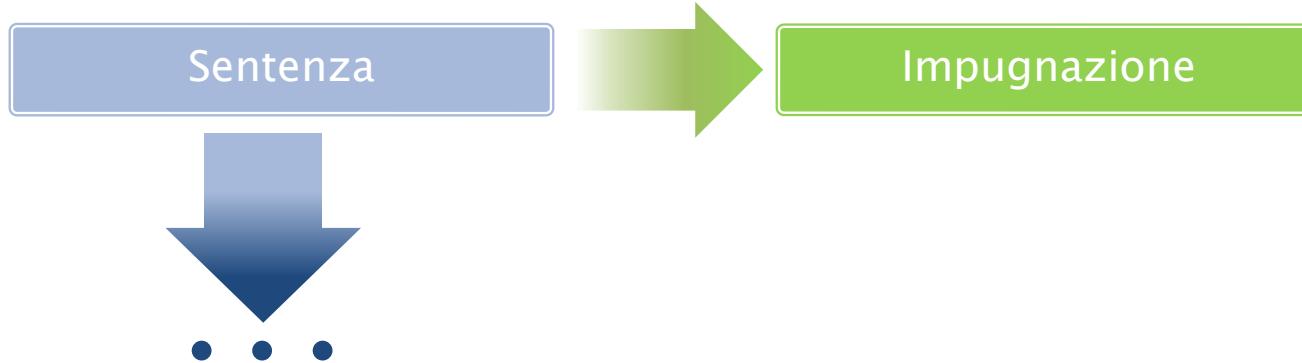


## ▶ Proscioglimento:

- sentenza di non doversi procedere: quando manca una delle condizioni di procedibilità o sussista una causa estintiva del reato (es. morte dell'imputato);
- sentenza di assoluzione: quando il fatto non sussiste, l'imputato non lo ha commesso, il fatto non costituisce reato, il reato è stato commesso da persona non imputabile o non punibile per altra ragione. Il giudice inoltre adotta sentenza di assoluzione quando sono insufficienti le prova di colpevolezza dell'imputato.

## ▶ Condanna: è pronunciata quando l'imputato risulta colpevole del reato contestatogli

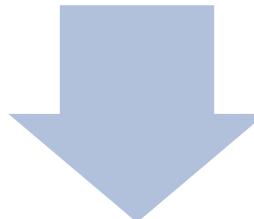
# Procedimento Penale: *impugnazione*



- ▶ è lo strumento attraverso il quale la parte processuale, nei cui confronti sia stato emesso un provvedimento giudiziario svantaggioso ne rimette il controllo ad un giudice diverso:
  - **Secondo grado di giudizio:** si ricorrere alla *Corte d'appello*. Questo secondo grado di giudizio può addirittura ribaltare le sentenze emesse in primo grado.
  - **Terzo grado di giudizio:** si ricorrere alla *Corte di cassazione* quando vi sono elementi per ritenere che il processo sia stato condotto non interpretando bene le leggi e sia dunque illegittimo. Non giudica l'imputato ma la sentenza d'appello ed in caso affermativo si procede al suo annullamento.

# Procedimento Penale: *giudicato penale*

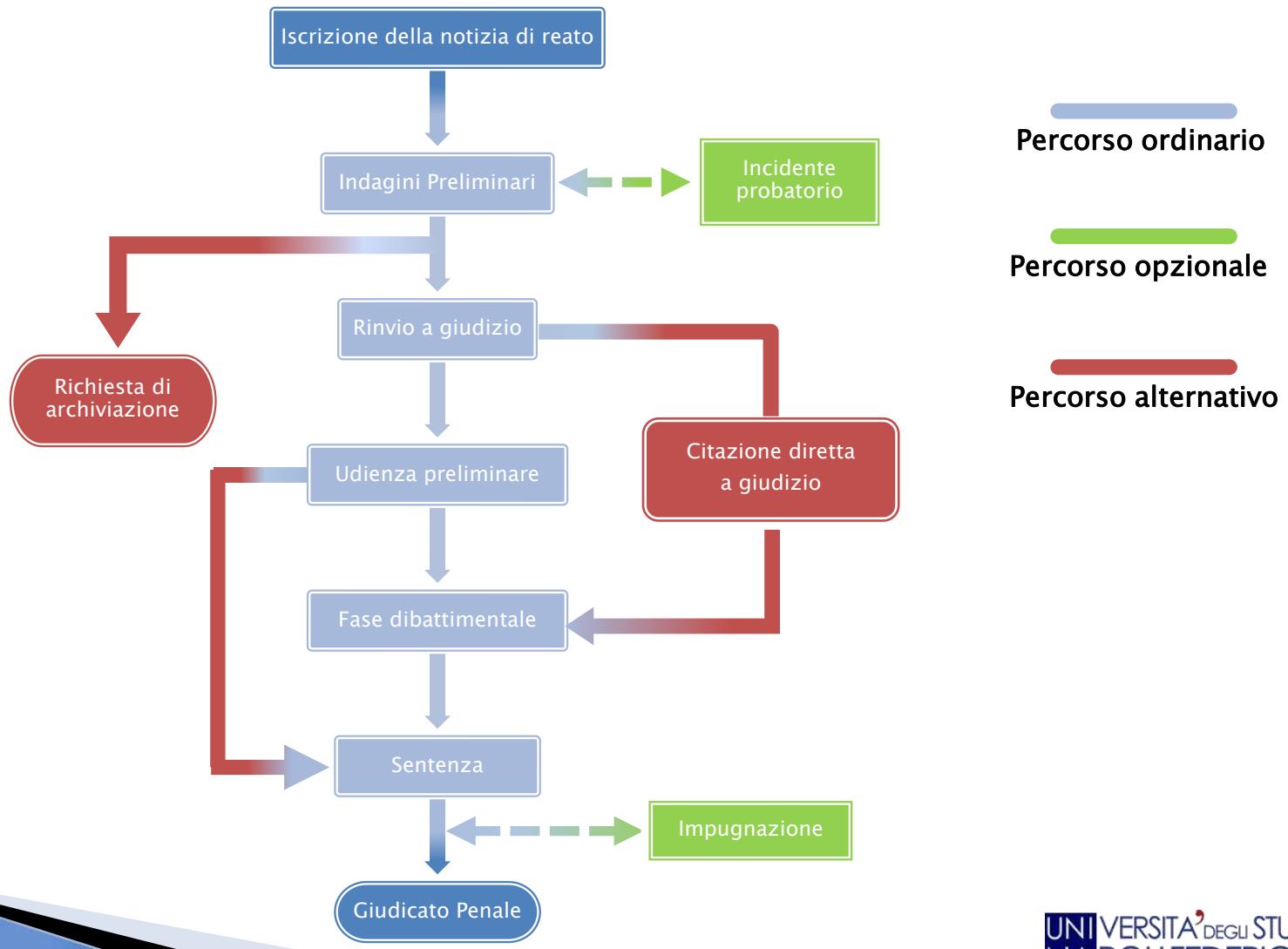
Sentenza



Giudicato Penale

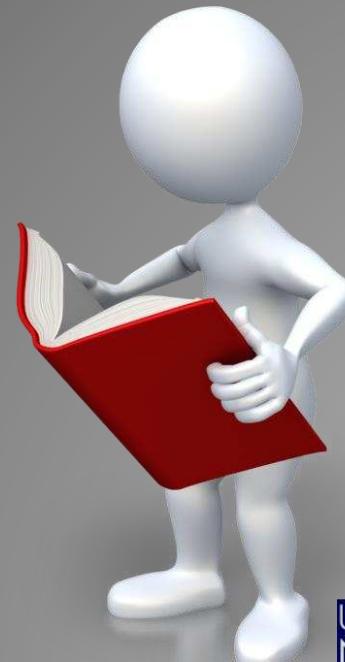
- ▶ La sentenza non è più impugnabile e la decisione di fatto sull'imputato non è più modificabile (**irrevocabile**).
- ▶ L'imputato, prosciolto o condannato, non può essere nuovamente sottoposto a procedimento penale per il medesimo fatto storico.

# Procedimento Penale



# Procedimento Civile

## » Introduzione



# Penale      vs      Civile

1. Diritto Penale;
2. Si realizza in due strutture diverse: Procura e Tribunale;
3. Ha lo scopo di accertare la verità nell'interesse dello Stato e della collettività;
4. Si instaura anche d'ufficio.
5. il giudice non si pone una situazione di indifferenza, ma persegue uno scopo ben preciso: accertare la verità del reato;

1. Diritto Privato;
2. Si realizza in un'unica struttura: il Tribunale;
3. Ha lo scopo di verificare l'esistenza di un diritto reclamato da un privato cittadino nei confronti di un altro e quale, tra le due parti in causa, ha ragione;
4. Si instaura esclusivamente su iniziativa di una parte: l'attore
5. il giudice si attiene solo alle prove presentate dalle parti, ponendosi in una posizione di equidistanza e imparzialità (**principio dispositivo**);

# Procedimento Civile: *procedimento ordinario*

- ▶ **FASE INTRODUTTIVA:** iscrizione a ruolo
  - L'Attore (la parte che instaura un giudizio) tramite l'avvocato espone i fatti che vengono posti a giudizio (*atto di citazione*);
  - L'atto di citazione viene notificato alla controparte: il **convenuto**.
- ▶ **FASE ISTRUTTORIA:** vengono acquisite in giudizio le prove richieste dalle parti, tipicamente:
  - Testimoniali (scritte o orali);
  - Consulenze tecniche di parte (C.T.P.);
  - Il giudice può nominare un Consulente Tecnico d'Ufficio (C.T.U.)
- ▶ **FASE CONCLUSIVA:** le parti devono chiarire definitivamente le proprie richieste, anche alla luce di quanto emerso nel corso del procedimento;
- ▶ **FASE DECISORIA:** il giudice ha tutti gli elementi per pronunciarsi sulla controversia e può finalmente emettere la sentenza.

# Procedimento Civile: *procedimento con ricorso*

## ▶ FASE INTRODUTTIVA:

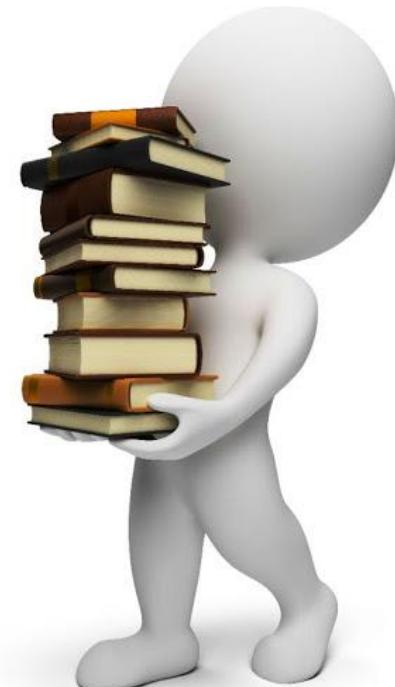
- Il ricorrente (la parte che instaura un giudizio) tramite l'avvocato espone i fatti che vengono posti a giudizio (domanda con ricorso) direttamente al Giudice;
- successivamente il Giudice emette un decreto di fissazione dell'udienza
- Il ricorrente notifica l'udienza alla controparte: **il resistente.**
- Le parti devono già esporre tutte le proprie difese e formulare le istanze istruttorie (rendere più celere il giudizio);

## ▶ FASE CONCLUSIVA

## ▶ FASE DECISORIA

# Bibliografia

- ▶  [it.wikipedia.org](http://it.wikipedia.org)
- ▶  [www.diritto.it](http://www.diritto.it)
- ▶  [www.studiocataldi.it](http://www.studiocataldi.it)
- ▶  [www.laleggepertutti.it](http://www.laleggepertutti.it)
- ▶  [www.altalex.com](http://www.altalex.com)
- ▶  [www.brocaldi.it](http://www.brocaldi.it)
- ▶  [www.albanesi.it](http://www.albanesi.it)





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 3: Gli Attori del Procedimento Penale



A.A. 2021/22  
**Dott. Lorenzo LAURATO**

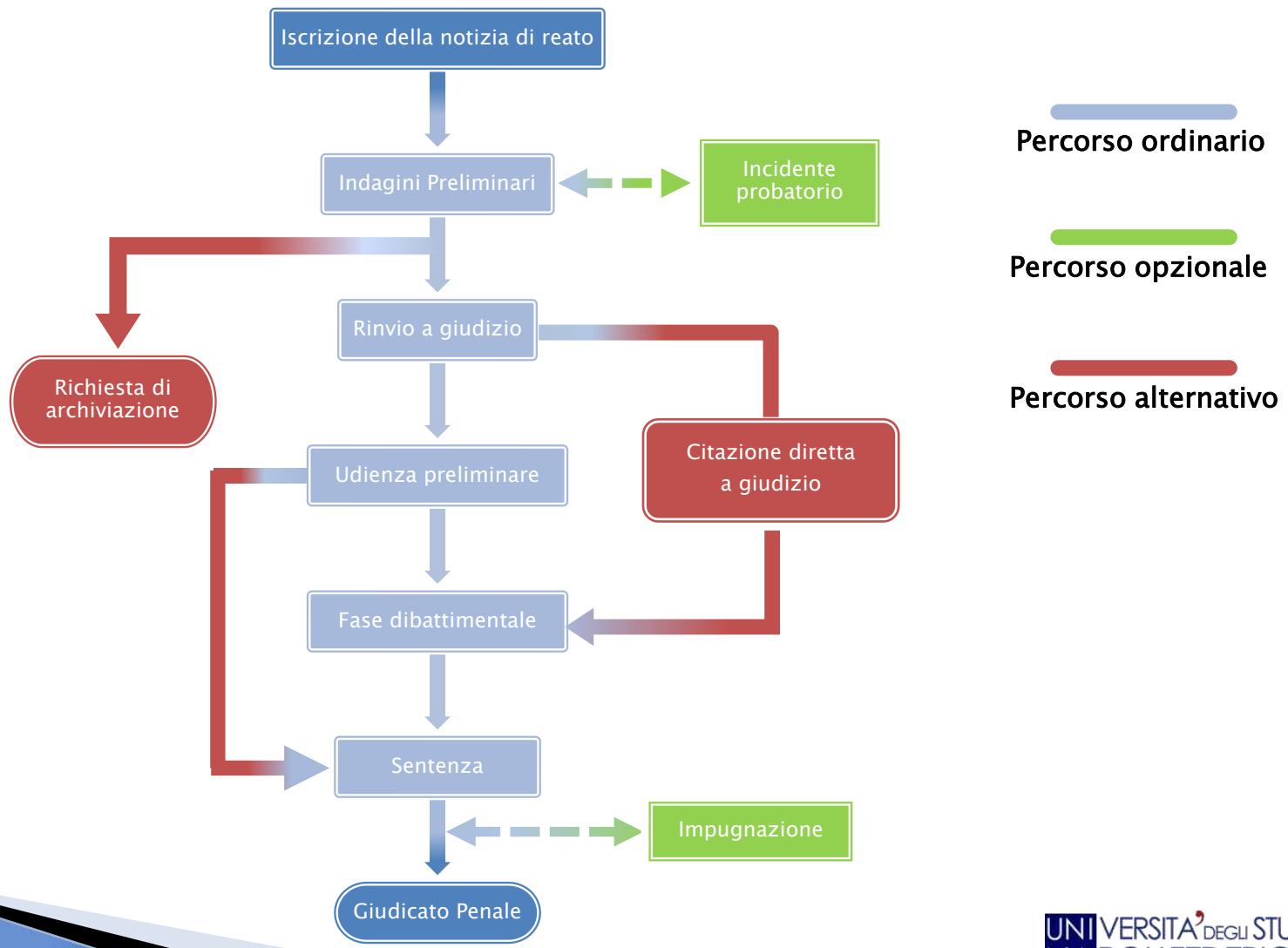


# Procedimento Penale

» Gli attori



# Procedimento Penale



# Gli attori del procedimento

- ▶ Pubblico Ministero (*P.M.*)
- ▶ Polizia Giudiziaria (*P.G.*)
- ▶ Parte Offesa (*P.O.*)
- ▶ Indagato/Imputato
- ▶ Difensore
- ▶ Giudice dell'Indagine Preliminare (*G.I.P.*)
- ▶ Giudice dell'Udienza Preliminare (*G.U.P.*)
- ▶ Giudice del Dibattimento (*Monocratico o Collegiale*)

# Struttura organizzativa

## ▶ Uffici magistratura inquirente:

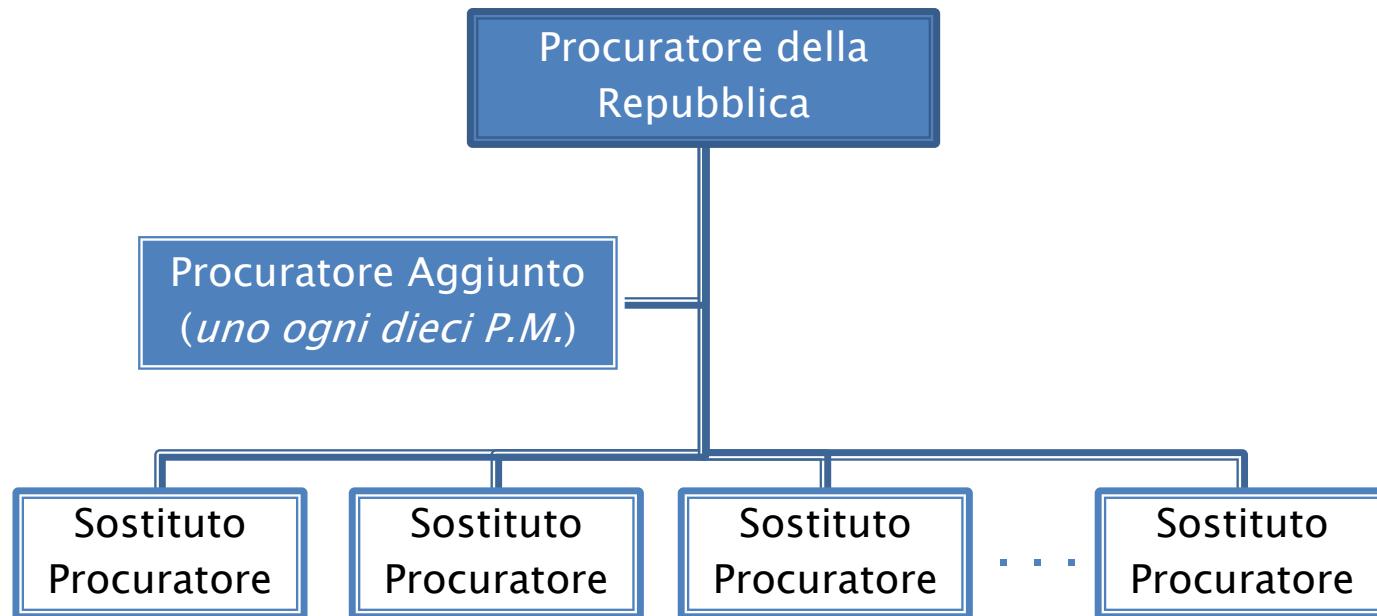
- Procure della Repubblica c/o i Tribunali Ordinari / per i Minorenni / Militari;
- Procure Generali c/o le Corti d'Appello;
- Procura Generale c/o la Suprema corte di Cassazione;

## ▶ Uffici magistratura giudicante:

- Tribunali Ordinari;
- Tribunali per i Minorenni;
- Tribunali Militari;
- Corte di Appello;
- Suprema Corte di Cassazione;

# Organizzazione della Procura

- ▶ Gli Uffici di Procura sono organizzati in gruppi di lavoro (*sezioni*) specializzati nella trattazione di specifici reati.



# Il Pubblico Ministero (P.M.)

- ▶ È un organo dell'amministrazione giudiziaria dello Stato designato per garantire il rispetto della legge e per valutare le azioni penali di un individuo;
- ▶ È il titolare delle indagini ed ha il compito di esercitare l'azione penale;
- ▶ Rappresenta la Pubblica accusa;



# Il Pubblico Ministero (P.M.)

## *i poteri*

- ▶ **Dirige le Indagini Preliminari:** avvalendosi della Polizia Giudiziaria, si occupa di trovare le prove d'accusa nei confronti di coloro che commettono reati, violando le leggi;
- ▶ Nomina consulenti tecnici;
- ▶ Valuta l'esito delle indagini e decide se archiviare o rinviare a giudizio;
- ▶ Esercita l'azione penale, formulando il capo di imputazione e sostiene in giudizio la tesi accusatoria, agendo nell'interesse pubblico;



# La Polizia Giudiziaria (P.G.)

- ▶ Sono forze di polizia che collaborano con il P.M. nelle attività di indagine e che dipendono direttamente dalla Procura;
- ▶ Svolge determinate attività sia in modo autonomo, sia su delega dell'autorità giudiziaria:
  - attività informativa: acquisisce la notizia di reato e la riporta al P.M.;
  - attività investigativa: ricerca dell'autore del reato;
  - attività di prevenzione: impedisce che i reati vengano portati a conseguenze ulteriori (*aggravati*) ;
  - attività assicurativa: individua e protegge le fonti di prova (*sommarie informazioni, accertamenti, rilievi, perquisizioni, sequestri, etc.*) .



## Funzione Repressiva

# La Persona Offesa (P.O.)



- ▶ è il soggetto titolare del bene giuridico (*patrimoniale, morale, personale, etc.*) leso dall'autore di un reato;
- ▶ Ha il diritto di querela in tutti i casi in cui per il reato non debba procedersi d'ufficio o dietro richiesta o istanza;
- ▶ Può presentare **memorie**, indicare **elementi di prova**, e nominare un difensore e consulenti tecnici;

# Esposto, Denuncia e Querela

- ▶ **ESPOSTO:** è la segnalazione all'Autorità Giudiziaria di un fatto allo scopo di far valutare se ricorre un'ipotesi di reato;
- ▶ **DENUNCIA:** è un atto con il quale si informa l'Autorità Giudiziaria di una notizia di reato perseguibile d'ufficio (*senza la denuncia/querela della parte offesa*).
- ▶ **QUERELA:** è una dichiarazione della persona offesa con la quale si esprime la volontà di punire il colpevole per un reato subito, non persegibile d'ufficio. Può essere ritirata (*rimessa*) se non tratta di reati sessuali ai danni di minori (*irrevocabile*).

# L'indagato e l'imputato

- ▶ **L'INDAGATO** è la persona nei confronti vengono svolte delle indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato.
  - La qualità di indagato si conserva fino alla richiesta di rinvio a giudizio o di archiviazione;
- ▶ **L'IMPUTATO** è la persona indagata nei confronti della quale è stata esercitata l'azione penale (*rinvio a giudizio*);
  - La qualità di imputato si conserva in ogni stato e grado del processo, sino a che la sentenza non diventi definitiva.
  - La sua assenza in udienza non né pregiudica il suo corso, che viene ugualmente celebrato (*contumace*) .
- ▶ **ENTRAMBI** hanno l'obbligo di farsi assistere da un difensore.
  - Possono difendersi producendo memorie e possono essere interrogati esclusivamente alla presenza del difensore.
  - Possono avvalersi di consulenti tecnici.



# Avvocato Difensore

- ▶ **Ruolo di assistenza:** resta una collaborazione di natura tecnica, diventando la bocca e l'orecchio “giuridico” del cliente;
- ▶ **Ruolo di rappresentanza:** agisce in sostituzione dell’interessato nell’esercizio di diritti e facoltà;
- ▶ E’ nominato sia dalla parte offesa, sia dalla parte indagata/imputata;
- ▶ La presenza del difensore oltre che un diritto, è condizione prima di legittimità e regolarità dello stesso procedimento penale:
  - Se l’indagato/imputo non nomina un difensore di fiducia, gli viene affidato un **difensore d’ufficio**.
- ▶ Può ottenere un accesso agli atti delle indagini preliminari:
  - *Completo*: solo a seguito dell’avviso di conclusione indagini (*415bis c.p.p.*)
  - *Parziale*: accesso limitato agli atti a sostegno di una singola misura preventiva per poter gestire una eventuale opposizione;



# Giudice dell'Indagine Preliminare (G.I.P.)

- ▶ Funzione di garanzia dell'indagato nella fase delle *indagini preliminari*. Può decidere se accogliere le richieste del P.M. su:
  - applicare misure cautelari;
  - autorizzare e convalidare l'uso delle intercettazioni come mezzi di ricerca della prova;
- ▶ Funzione di garanzia dell'azione penale:
  - accogliere o no la richiesta di archiviazione;
  - ▶ non ha autonomia di iniziativa probatoria: provvede esclusivamente su richiesta della parte;
  - ▶ è privo di un proprio fascicolo: gli atti conosciuti sono quelli che il PM decide di allegare alle istanze che presenta;



# Giudice dell'Udienza Preliminare (G.U.P.)

- ▶ interviene dopo l'esercizio dell'azione penale;
- ▶ giudica la richiesta di rinvio a giudizio:
  - esamina il fascicolo delle indagini preliminari e valuta le fonti delle prove raccolte;
  - ascolta le ragioni della difesa dell'imputato;
- ▶ il Giudice potrà:
  - emettere decreto di rinvio a giudizio;
  - emettere Sentenza di non luogo a procedere.



# Giudice del dibattimento

- ▶ Presiede a tutta la fase dibattimentale e alle relative udienze;
- ▶ Può essere in composizione Monocratica (*singolo*) o Collegiale;
- ▶ Per i reati più efferati è prevista una distinta composizione definita Corte d'Assise dove è presente anche la **Giuria Popolare**;
- ▶ Emette la sentenza;

# Procedimento Penale

» Il Computer Forensi



# Il C.F. nel Procedimento Penale: *le indagini preliminari*

- se sono richieste particolari competenze tecniche, può essere nominato dall'autorità giudiziaria un *consulente tecnico* (art. 348 c. 4 c.p.p)

Pubblico Ministero



Consulente  
Tecnico d'Ufficio  
(CTU)

Polizia Giudiziaria



Ausiliario  
di P.G.

Computer Forensist

# Il C.F. nel Procedimento Penale: *il ruolo del Computer Forensen*

- ▶ Il C.F. deve impiegare metodi e strumenti che garantiscono l'inalterabilità della prova, anche se non dettagliatamente descritti dalla legge.

# Il C.F. nel Procedimento Penale:

## *accertamento irripetibile* (art. 360 cpp)

- ▶ accertamenti che se compiuti comportano l'alterazione della fonte della prova e la ripetibilità della procedura non è più garantita;
  - *Es.:*
    - *dispositivo non è in buono stato;*
    - *il dispositivo cambia autonomamente il proprio stato;*
- ▶ esigenze di restituzione del reperto:
  - *Es.: dispositivi fondamentali per la normale attività di una azienda;*

# Il C.F. nel Procedimento Penale:

## *accertamento irripetibile* (art. 360 cpp)

- il P.M. esegue questa attività di accertamento avvisando previamente l'indagato e il suo difensore in modo da dare la possibilità a questi ultimi di assistere a tutta l'operazione a garanzia del rispetto delle procedure. L'indagato può nominare e farsi assistere un proprio Consulte Tecnico: Consulente Tecnico di Parte (CTP).

Consulente  
Tecnico d'Ufficio  
(CTU)



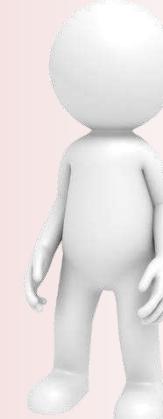
Pubblico  
Ministero



Difensore



Indagato

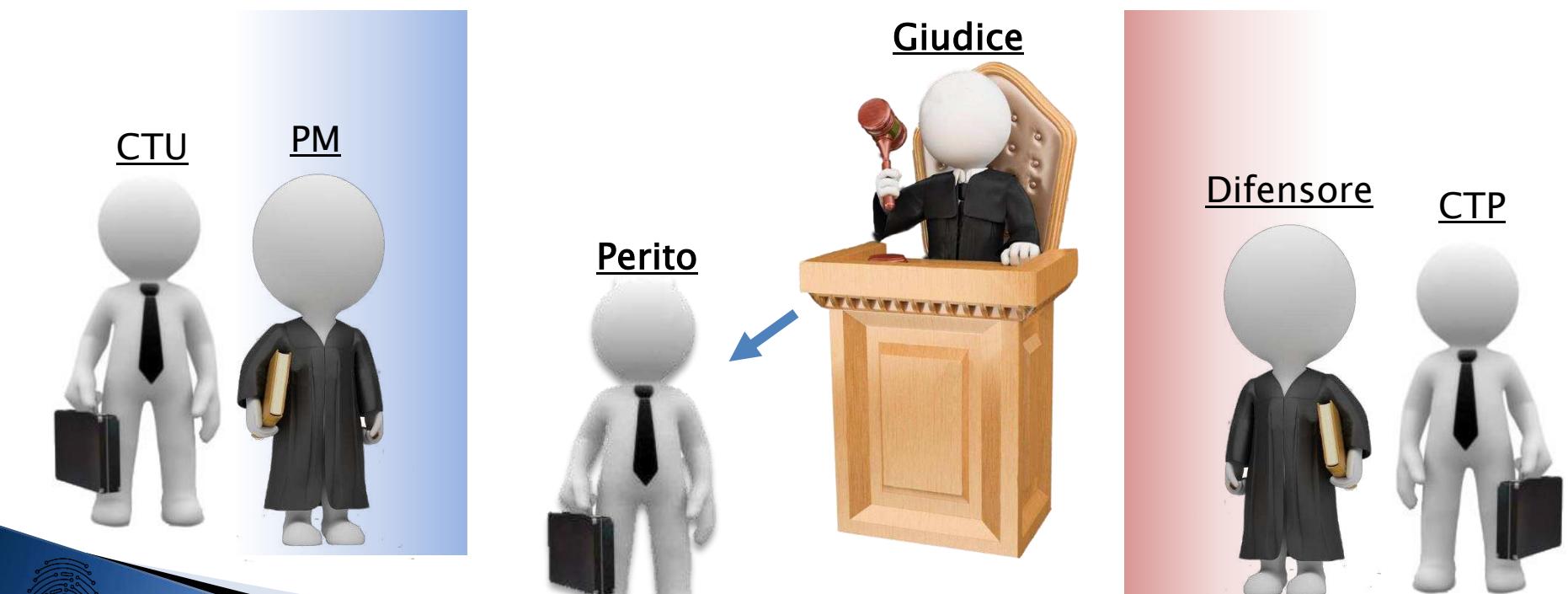


Consulente  
Tecnico di Parte  
(CTP)



# Il C.F. nel Procedimento Penale: *Perito*

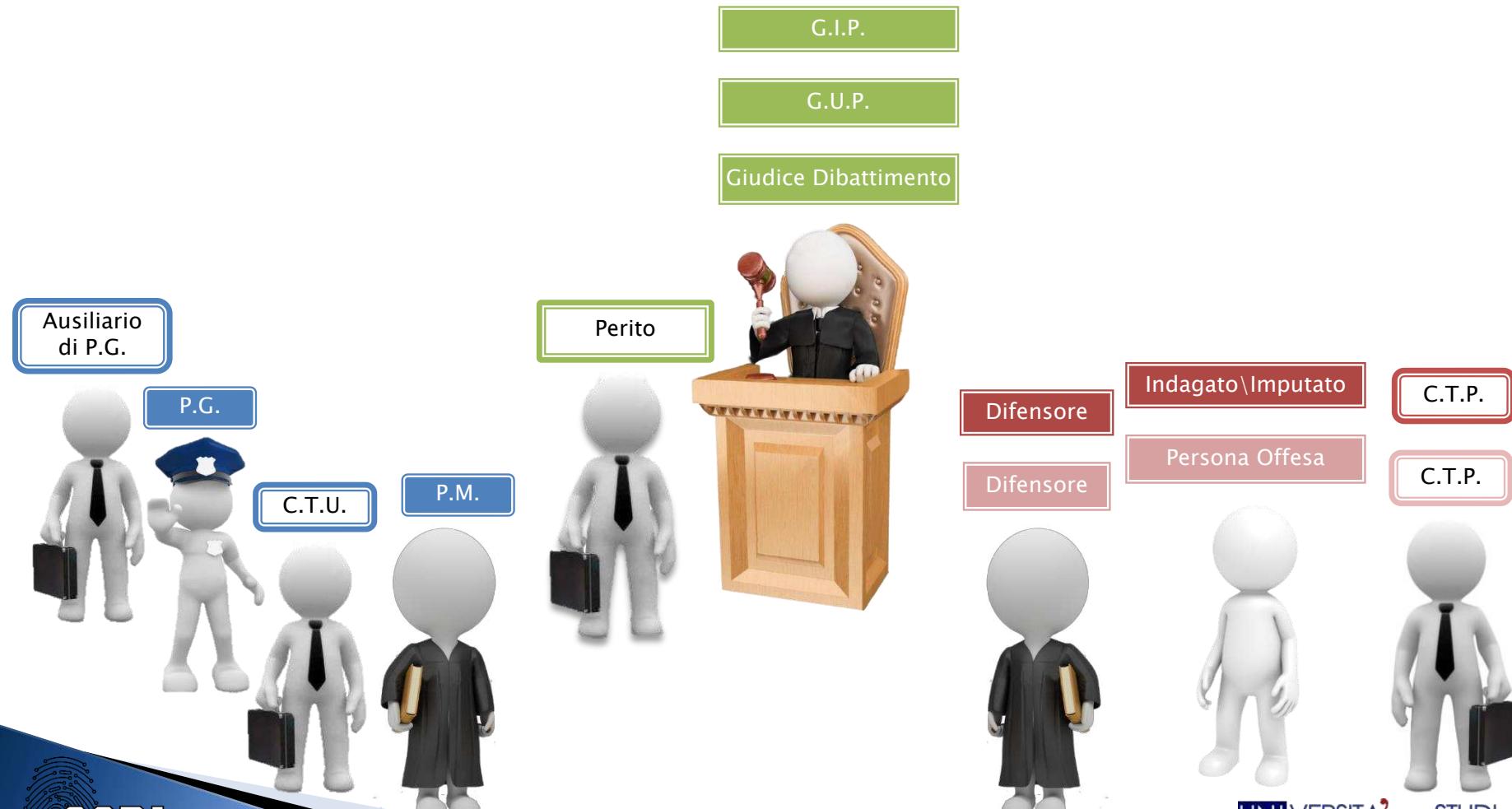
- ▶ In caso di un incidente probatorio o di un'udienza, in cui sono richieste particolari competenze tecniche, il Giudice può nominare un Consulente Tecnico: il Perito.
- ▶ può essere scelto dall'Albo del Tribunale oppure da soggetti non iscritti, se individua in questi particolare competenza tecnica; Il perito viene avvisato degli obblighi e responsabilità che assume con il giuramento.



# Il C.F. nel Procedimento Penale: *riepilogando...*

- ▶ Il Computer Forensen a seconda da chi e da quando viene incaricato assume ruoli diversi all'interno del procedimento:
  - Ausiliario di P.G.: quando il consulente tecnico è incaricato dalla Polizia Giudiziaria durante determinate operazioni;
  - Consulente Tecnico d'Ufficio (CTU): quando il consulente tecnico è incaricato dal Pubblico Ministero (PM) durante le indagini preliminari per svolgere determinati accertamenti;
  - Consulente Tecnico di Parte (CTP): quando una delle parti coinvolte nel procedimento (indagato/imputato e/o persona offesa) incaricano un proprio consulente tecnico:
    - per assisterlo a presentare prove tecniche del reato subito (*parte offesa*)
    - per controbattere a determinate operazioni tecniche compiute dalla parte accusatoria (*indagato*)
  - Perito del Giudice: quando il Giudice ha bisogno di compiere determinati accertamenti tecnici o valutare quelle compiute dalle parti;

# Gli Attori nel Procedimento Penale: *riepilogando...*



# Procedimento Penale

» Esempi di verbali per un C.F.



# Verbale di conferimento incarico

Nr. Procedimento  
Penale

Proc. N. xxxx/aa R.G.N.R. Mod.21



## PROCURA DELLA REPUBBLICA presso il Tribunale di Napoli III<sup>^</sup> Sezione

Accertamento  
irripetibile

### VERBALE DI NOMINA del CTU E DI CONFERIMENTO DELL'INCARICO

- artt. 360, 549 c.p.p., 116 e 117 D. Lv. 271/89 -

Indagato

Il giorno 20 del mese di Settembre dell'anno 2018, alle ore 12.52 in Napoli- Palazzo di Giustizia, presso L'Ufficio del PM in Napoli Centro Direzionale piano, nel procedimento di cui in epigrafe nei confronti di **INDAGATO** + altri, indagati per i reati di cui agli artt. 416, 615ter, 640 ter

Reato

c.p. commessi in Castel Volturno, Marcianise e altri luoghi e altro innanzi al Pubblico Ministero Dott. **MAGISTRATO** Sost. Procuratore della Repubblica presso il Tribunale di Napoli, e alla presenza della dott.ssa **TIROCINANTE**, M.O.T. mirato presso questo Ufficio, sono comparsi citati regolarmente ex art 360 c.p.p.:

P.M.

- il C.T.U. Dott. Lorenzo LAURATO nato a OMISSIS noto all'Ufficio iscritto all'Albo del Tribunale di Napoli domiciliato presso lo studio di Via Coroglio n. 57 /D;
- il CTU Dott. Consulente TECNICO nato a OMISSIS , domiciliato presso lo studio professionale in OMISSIS
- per gli indagati INDAGATO A e INDAGATO B di fiducia; d'ufficio per INDAGATO C , INDAGATO D, l'Avv. DIFENSORE A del foro di Napoli;
- l'Avv. DIFENSORE C per delega – che deposita - dell'Avv. DIFENSORE B, per gli indagati INDAGATO E e INDAGATO F;
- per la persona offesa WIND 3 spa l'Avv. DIFENSORE E in sostituzione dell'Avv. DIFENSORE D del foro di Roma, come da delega che deposita;

# Verbale di conferimento incarico

il PM dà atto che nessun altro è comparso sino alle ore 12.55. Si dà atto che l'avviso ex art 360 c.p.p. è stato ritualmente notificato a tutti gli indagati e loro difensori, nonché alle persone offese.

I CTU a questo punto rendono le proprie generalità:

- *Sono Lorenzo LAURATO nato a . . . OMISSIS domiciliato in Napoli presso la società SSRI in Via Coroglio n.57;*
- *"sono Consulente Tecnico nato a . . . OMISSIS , domiciliato presso lo studio professionale in . . . OMISSIS "*

A domanda se i CTU si trovino in una delle condizioni previste dall'art. 222 c.p.p., il CTU rispondono: "NO";

Il Pubblico Ministero, quindi, informa i consulenti e le parti dell'oggetto dell'incarico e formula i seguenti quesiti:

Quesito

*"Previo esame dei reperti in sequestro (PC, telefoni, supporti informatici), formino i ctu -con softwares e dispositivi idonei allo scopo, collegialmente e d'intesa con la Polizia Postale delegata - copia forense delle memorie informatiche dei dispositivi elettronici in sequestro (come da elenchi inviati dalla Polizia Postale), operando secondo le regole della computer forensics in maniera da non alterare il contenuto dei reperti e da rendere l'esame e l'analisi ulteriormente ripetibile. Effettuino i CTU l'analisi del contenuto dei reperti, illustrando in particolare se emergano dati, documenti o tracce informatiche dell'attività di frode informatica e dei reati per cui si procede, nonchè documentazione relativa all'incasso e movimentazione dei proventi di truffe e di sostituzione di persona. Dicano quant'altro utile a fini di giustizia".*

Vista la complessità dei quesiti, i Consulenti Tecnici chiedono un termine per il deposito della relazione, che il Pubblico Ministero concede nella misura di giorni 60 dall'inizio delle operazioni.

# Verbale di conferimento incarico

Richieste del  
C.T.U.

I CTU chiedono di essere autorizzati: esaminare i reperti in sequestro presso il proprio studio, usare il mezzo proprio per gli spostamenti, e ad avvalersi di collaboratori ausiliari, nonché a noleggiare il dispositivo denominato "CELLEBRITE UFED" essenziali per l'acquisizione forense delle memorie dei telefoni sequestrati; nonché all'acquisto di appositi hard disk per memorizzare le copie forensi.

Il P.M. autorizza quanto sopra richiesto.

Le parti presenti dichiarano che allo stato non intendono nominare propri CTP.

I CTU dichiarano che l'inizio delle operazioni avverrà in data 25.9.2018 ore 10.00 presso lo studio SSRI del dott. Laurato in via Coroglio n.57, con ritiro ed esame reperti.

Verbale chiuso alle ore 10.57 del 19.2.2018 e consta di n. 1 pagina

Letto e sottoscritto.

- I CTU \_\_\_\_\_



I Difensori \_\_\_\_\_

II M.O.T. \_\_\_\_\_

IL PUBBLICO MINISTERO

COPIA CONFORME  
ALL'ORIGINALE  
*2011*

# Verbale di consegna materiale



## Guardia di Finanza

### NUCLEO DI POLIZIA ECONOMICO-FINANZIARIA NAPOLI

Gruppo Tutela Mercato Beni e Servizi - Sezione Polizia Economica ed altre attività di p.g.  
Via Card. G. Sanfelice, 49 - 80134 - Napoli - ☎ 081/9703649 - - na1820000p@pec.gdf.it

#### VERBALE DELLE OPERAZIONI COMPIUTE

L'anno 2019 addì 25 del mese di ottobre, alle ore 13:00, presso gli uffici Nucleo pt in intestazione,  
viene redatto il presente atto.

#### VERBALIZZANTI

Lgt. c.s. AGENTE DI P.G. A  
Lgt. c.s. AGENTE DI P.G. B

#### PARTE

**ALFE' Marco**, nato a **OMISSIS**. Identificato a mezzo patente di guida nr. **OMISSIS/S** rilasciata dalla MCTC di Napoli in data 05.03.2001 nella sua qualità di collaboratore di **LAURATO Lorenzo**, in altri atti già compiutamente generalizzato - CTU informatico del Pubblico Ministero.

#### FATTO

Il dott. P.M. – Sost. Proc. presso il Tribunale di Napoli, nell'ambito del procedimento penale xxxx/18, ha conferito l'incarico di C.T.U. informatico al sig. **LAURATO Lorenzo**, nato a **OMISSIS**, per l'esame del materiale informatico sequestrato in data 14 e 23 ottobre 2019, nei confronti dei seguenti soggetti:

1. **INDAGATO A**, nato ad **OMISSIS** e residente in Avellino alla via

- nr. 1 pc marca HP nr. seriale ABCD123456789;
- nr. 1 pc marca PAVILLION nr. seriale ABCD123456789;
- nr. 1 pc marca ACER Aspire nr. seriale ABCD123456789;
- nr. 1 pc marca ACER Veriton nr. seriale ABCD123456789;
- nr. 1 pc marca GLITE nr. seriale ABCD123456789;

# Verbale di consegna materiale

2. **INDAGATO B** nato a S. Andrea di Conza (AV) il OMISSIS e residente ad Avellino, OMISSIS :

- nr. 1 pc portatile marca HP PAVILLON serial number: 1234ABCD con relativo alimentatore;
- pc fisso, modello ASPIRE AX 3950 serial number: 123456789ABCD
- nr. 1 pendrive marca DIKOM;

3. **INDAGATO C** nato ad Atripalda (AV) il OMISSIS e residente ad Avellino, via OMISSIS :

- telefono cellulare marca XIAOMY corredato della scheda telefonica nr. ;

Per quanto sopra, come concordato telefonicamente con il CTU LAURATO Lorenzo, il materiale sopra descritto viene consegnato a **ALFE' Marco**, per l'espletamento della consulenza tecnica

Si rappresenta che quanto sopra descritto viene consegnato nei plachi approntati in sede di sequestro, come da verbali all'uopo redatti.

L.C.S.

I VERBALIZZANTI

LA PARTE

# Richiesta proroga termini

  
Sicurezza Sistemi Reti Informatiche  
PP N. xxxx/17 R.G.N.R. Mod.21

V°, n° entro il  
nepel, 21/5/19  
IL SOST. PROCURATORE DELLA REPUBBLICA

Procura della Repubblica  
presso il Tribunale di NAPOLI

alla c.a. del Pubblico Ministero  
Dott. PUBBLICO Ministero

**Oggetto : Richiesta Proroga Termini**

I sottoscritti Dott. Lorenzo Laurato e OMISSIS, nominati CTU dalla SVI nell'ambito del procedimento penale nr. xxxx/2017 R.G.N.R., considerata l'enorme quantità del materiale informatico sottoposto a sequestro, e considerato che il giorno 23/03/2019, scadono i termini di presentazione dell'elaborato peritale, con la presente

**C H I E D O N O**

una proroga dei termini di presentazione della relazione peritale di giorni 60 (sessanta) a partire dalla data del **"22-05-2019"**, periodo di scadenza previsto per portare a termine il proprio mandato.

Restando a Vs disposizione per ogni eventuale chiarimento, porge distinti saluti.

Napoli 20/05/2019

I Consulenti Tecnici d'Ufficio  
Dott. Lorenzo Laurato

# Incarico di Perizia

Nr. Procedimento  
Penale

N. XXXX/19 R.G. P.M. e N. YYYYY/19 R.G. Tribunale



COLLEGIO C

Nr. Registro  
Tribunale

Composizione del  
Collegio

## TRIBUNALE DI NOLA SEZIONE PENALE

### VERBALE DI UDIENZA

(ART. 480 E SEGG. C.P.P.)

Il giorno MERCOLEDÌ 4 DICEMBRE 2019, alle ore 10.30, in Nola dinanzi al Tribunale di Nola  
in composizione collegiale, composto da:

Presidente DOTT.SSA GIUDICE A

Giudice DOTT.SSA GIUDICE B

Giudice DOTT. GIUDICE C

con l'assistenza del Cancelliere dott. OMISSIONIS, che espressamente autorizzato si avvale, ove necessario,  
di personale tecnico per la redazione del verbale con la stenotipia sig. / sig.ra .....  
e la riproduzione fonografica sig. / sig.ra ..... sono presenti:  
il Pubblico Ministero P.M.

#### imputati

1. IMPUTATO A

LIBERO/A GIÀ PRESENTE

2. IMPUTATO B

LIBERO/A GIÀ PRESENTE

3. PERSONA OFFESA

testi presenti: ...

#### difensori

DIFID. AVV. DIFENSORE A

ex art. 97 co 4° C.P.P. avv.

delega orale

ex art. 102 C.P.P. avv.

C.S.

ex art. 97 co 4° C.P.P. avv.

delega orale

ex art. 102 C.P.P. avv.

AVV. DIFENSORE B

si da atto ai fini della pratica forense della presenza del/i dott./ri

Imputati

Difensore  
Imputati

Persona Offesa

Difensore  
Persona Offesa

Perito

# Incarico di Perizia

*Il Presidente controlla la regolare costituzione delle parti.*

Compiuto l'accertamento della costituzione delle parti.

Preliminarmente si è accertato il presidente l'ing. Laurato  
per il conferimento d'incarico.  
Il presidente procede al conferimento d'incarico all'ing.  
Laurato incaricato all'ing. Laurato, vedi  
l'allegato verbale stenotipico.  
L'avv. difensore procede alla nomina di n. 2 consulenti  
propri già indicato nella lista Teste nonché l'ing. [Consulente di Parte].  
Questa lista è stata rinvia al 4-3-20  
ore 12.00 per il deposito della perizia.  
Chiusura 10,45

il Dott. Laurato

*Si da atto che è presente l'ing. Laurato per il conferimento d'incarico.  
A questo punto il tribunale procede al conferimento d'incarico all'ing.  
Laurato, vedi l'allegato verbale stenotipico.*

*L'avv. [difensore imputati] procede alla nomina di n. 2 consulenti propri  
già indicato nella lista Teste nonché l'ing. [Consulente di Parte].*

*A questo punto il Tribunale rinvia al 4-3-20 ore 12.00 per il deposito  
della perizia.*

*Perito presente edotto.*

*Chiusura 10,45.*

# Incarico di Perizia

*Dal verbale stenotipico:*

## CONFERIMENTO DELL'INCARICO

PRESIDENTE: No. Va bene, allora, senta, in questo caso noi abbiamo un telefono cellulare con il quale è stata registrata una conversazione tra presenti, cioè, una conversazione tra la Persona Offesa e gli Imputati di questo procedimento, ora, l'accertamento che lei dovrebbe fare, innanzitutto, quello di estrapolare questa conversazione e anche di verificare se la genuinità della stessa, cioè, eventualmente se ci sono delle alterazioni, degli stop and go, qualche elemento che possa far dubitare della genuinità della conversazione, questo è il quesito, adesso, magari, lo specifichiamo un poco meglio, c'è qualcos'altro che le Parti vogliono aggiungere?

# Verbale operazioni compiute

Tribunale di Nola  
Coll. C

PP N. xxxx/19 R.G.N.R. Mod. 21

## VERBALE DI OPERAZIONI COMPIUTE

L'anno 2019, addì 19 del mese di dicembre, in Napoli, presso gli uffici del sottoscritto Dott. Lorenzo Laurato, nominato Perito Tecnico del Tribunale di Nola – Coll. C il 04/12/2019, si redige il presente verbale, al fine di far constatare che, in data odierna, alle ore 10.00 circa sono iniziate le operazioni di Perizia Tecnica disposte nell'ambito del procedimento penale n. xxxx/2019 R.G.N.R. mod. 21 così come da conferimento incarico.

Si da atto che all'inizio delle operazioni è presente:

1) Ing. **C.T. di Parte**, nato a Napoli il OMISSIS res. a Napoli,  
OMISSIS, in qualità di Consulente tecnico delle parti  
IMPUTATO A e IMPUTATO B, identificato a mezzo carta d'identità nr.  
OMISSIS rilasciata il OMISSIS dal Ministero degli Interni.

Le operazioni tecniche odierne consistono nell'acquisizione forense del dispositivo di telefonia mobile marca Samsung modello SM-G531F s/n: ABCD1234 avente IMEI 01234567891011 messo a disposizione della parte offesa nella udienza del 04.12.2019, ivi compresa la SIM CARD TIM avente ICCD 89391234567891011 .

L'acquisizione del telefono cellulare viene eseguita utilizzando il dispositivo denominato **"Cellebrite UFED4PC"**, strumento "Hardware/Software" stand alone preposto alla realizzazione di copie forensi che garantisce l'assoluta inalterabilità dei dati.

# Verbale operazioni compiute

Alle ore 11.18 circa si è conclusa l'acquisizione del reperto:

- Telefono Cellulare Samsung modello SM-G531F s/n: ABCD1234 aente IMEI 01234567891011 comprensivo di SIM Card TIM ICCID:89391234567891011 .

A completamento del presente verbale, vengono stampati i file di log dell'acquisizione del dispositivo suindicato, con il calcolo dell'algoritmo di Hash SHA256, che si rilascia in formato cartaceo allegato al presente verbale.

In merito alle attività svolte il CTP non ha nulla da dichiarare.

Alle ore 11.30 il CTP abbandona le operazioni le quali proseguiranno senza soluzione di continuità.

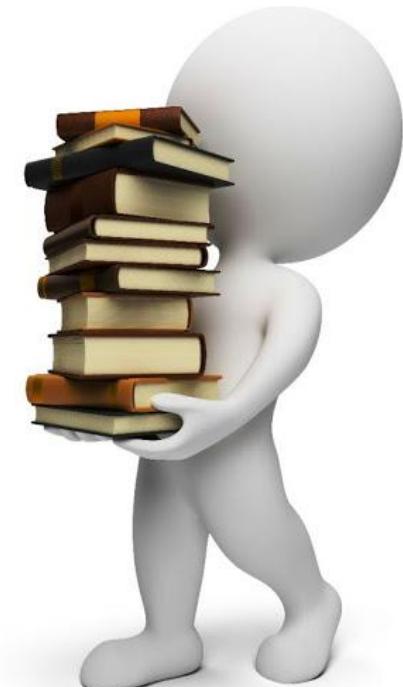
Il presente atto viene confermato e sottoscritto dal Perito e dalla parte intervenuta alle operazioni, alla quale viene rilasciata copia.

✓ Il Perito del Tribunale

La Parte

# Bibliografia

- ▶  [it.wikipedia.org](http://it.wikipedia.org)
- ▶  [www.diritto.it](http://www.diritto.it)
- ▶  [www.studiocataldi.it](http://www.studiocataldi.it)
- ▶  [www.laleggepertutti.it](http://www.laleggepertutti.it)
- ▶  [www.altalex.com](http://www.altalex.com)
- ▶  [www.brocaldi.it](http://www.brocaldi.it)
- ▶  [www.albanesi.it](http://www.albanesi.it)





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 4: Genesi del Diritto Informatico



A.A. 2021/22  
**Dott. Lorenzo LAURATO**



# Il Reato

è quell'illecita azione o omissione,

*contrario  
all'ordinamento  
giuridico*

teso a ledere un bene tutelato giuridicamente  
e a cui viene corrisposta una pena.

- **doloso:** vi è la *consapevolezza e la volontà di commettere un reato*;
- **preterintenzionale:** le *conseguenze sono più gravi di quanto voluto*;
- **colposo:** manca la volontà di determinare un qualsiasi evento costituente reato, ma l'evento si verifica ugualmente per *negligenza, imprudenza, imperizia o per inosservanza di leggi, regolamenti, ordini o discipline*;

*non impedire un evento,  
che si aveva l'obbligo  
giuridico di impedire,  
equivale a cagionarlo*

*sanzione predisposta per la  
violazione di un precezzo  
penale comminata secondo  
il diritto penale*

# Reato Informatico

In ambito penale la definizione si è evoluta nel tempo:

- ▶ *illecito che richiede conoscenze di informatica per la sua realizzazione*
- ▶ *illecito che comporta il coinvolgimento di un qualunque tipo di elaboratore*
- ▶ **illecito nel quale il computer interviene come strumento o come oggetto**

# Reato Informatico

Quelle appena esposte sono tuttavia definizioni troppo ampie che non riescono a delimitare correttamente quale condotta possa essere definita “*reato informatico*”:

- ▶ **A livello internazionale si è rinunciato a dare una vera e propria definizione di reato informatico.**
- ▶ **Si è preferito concordare una tipologia di comportamenti ai quali dare l'etichetta di reati informatici.**

# DIGITAL FORENSICS

» Evoluzione normativa

# Evoluzione Normativa:

1989 –  
Consiglio di  
Europa:  
lista reati  
informatici

1993 –  
L.547/1993:  
Introduce nel C.P.  
le prima categorie  
di reati informatici

2001 –  
Consiglio di  
Europa c.d.  
Convenzione  
di BUDAPEST

2008 – L.48/2008:  
adozione di misure  
tecniche tese a  
preservare i dati  
originali:  
– SCENA DEL  
CRIMINE VIRTUALE  
– PERQUISIZIONE  
INFORMATICA

# 1989 – Consiglio di Europa

## *Raccomandazione N° R (89) 9*

- ▶ Vengono elaborate due liste di abusi:
  - **Lista minima**: condotte criminose che gli Stati devono reprimere mediante una sanzione penale.
  - **Lista facoltativa**: i comportamenti ritenuti non eccessivamente offensivi, la cui repressione è rimandata alla valutazione dei singoli Stati.

# 1989 – Consiglio di Europa

## *Raccomandazione N° R (89) 9*

### LISTA MINIMA

- frode informatica;
- falso in documenti informatici;
- danneggiamento di dati e programmi;
- sabotaggio informatico;
- accesso non autorizzato ad un sistema informatico;
- intercettazione non autorizzata di comunicazioni informatiche;
- riproduzione non autorizzata di un programma protetto;
- riproduzione non autorizzata della topografia di un prodotto a semiconduttori;

# 1989 – Consiglio di Europa

## *Raccomandazione N° R (89) 9*

### LISTA FACOLTATIVA

- alterazione di dati o di programmi (*senza danneggiamento*);
- spionaggio informatico;
- utilizzazione non autorizzata di un elaboratore;
- utilizzazione non autorizzata di un programma informatico;

# Evoluzione Normativa

» Legge n. 547 del 23/12/1993



# Legge n. 547 del 23/12/1993

- ▶ L'Italia recepisce le direttive del Consiglio d'Europa del 1989, introducendo nel codice penale di diverse figure di reato informatico:
  - collocazione in prossimità delle figure di reato già esistenti, che sarebbero applicabili se il fatto non fosse commesso sfruttando la tecnologia informatica

# Legge n. 547 del 23/12/1993

## *art. 392 c.p.*

*(Esercizio arbitrario delle proprie ragioni  
con violenza sulle cose)*

- ▶ Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito, a querela della persona offesa [120; c.p.p. 336, 340], con la multa fino a euro 516.
- ▶ Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione.
- ▶ *Si ha altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.*

# Legge n. 547 del 23/12/1993

## *art. 420 c.p.*

*(Attentato a impianti di pubblica utilità)*

- ▶ Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.
- ▶ *La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti. (\*)*
- ▶ *Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni. (\*)*

*(\*) abrogati con la legge n. 48 del 18/03/2008*

# Legge n. 547 del 23/12/1993

## *art. 491-bis c.p.*

### *(Documenti informatici)*

- ▶ Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico [*o privato*] {*avente efficacia probatoria*}, si applicano le disposizioni del capo stesso concernenti [rispettivamente] agli atti pubblici [*e le scritture private*]
- ▶ A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli (\*)

[ ] *termini soppressi dal d.lgs. n. 7 del 15/01/2016*

{ } *termini aggiunti con la legge n. 48 del 18/03/2008*

(\*) *abrogato con la legge n. 48 del 18/03/2008*

# Legge n. 547 del 23/12/1993

## *art. 615-ter c.p.*

*(Accesso abusivo a un sistema informatico o telematico)*

- ▶ Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
- ▶ La pena è della reclusione da uno a cinque anni:
  - 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
  - 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
  - 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

# Legge n. 547 del 23/12/1993

## *art. 615-ter c.p.*

*(Accesso abusivo a un sistema informatico o telematico)*

- ▶ Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
- ▶ Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio

# Legge n. 547 del 23/12/1993

## *art. 615-ter c.p.*

*(Accesso abusivo a un sistema informatico o telematico)*

### CASO 01

- ▶ Francesco vuole accedere al computer della sua fidanzata Paola, della quale è molto geloso, per leggere alcune e-mail che quest'ultima ha ricevuto da Andrea, un amico di Paola.
- ▶ Francesco per poter leggere le e-mail deve accedere all'account di Paola protetta da password.
- ▶ Francesco con una utility di password cracking trova la password di Paola ed accede alla sua posta elettronica.

# Legge n. 547 del 23/12/1993

## *art. 615-ter c.p.*

*(Accesso abusivo a un sistema informatico o telematico)*

### CASO 02

- ▶ Mario, maresciallo in servizio presso la stazione dei Carabinieri, accede al sistema informatico SDI (Sistema di Indagine), in dotazione alle forze di polizia.
- ▶ Il sistema è protetto da misure di sicurezza, ma Mario dispone delle credenziali di accesso in quanto appartenente all'Arma dei Carabinieri.
- ▶ Mario è autorizzato ad accedere al sistema esclusivamente per ragioni di tutela dell'ordine e della sicurezza pubblica e di prevenzione e repressione dei reati.
- ▶ Pur essendo “fuori servizio” e non dovendo svolgere alcuna indagine sul conto di Luca e Francesca, acquisisce notizie afferenti la sfera privata e le vicende giudiziarie di entrambi, nonché di altre otto persone legate a vario titolo a Luca.
- ▶ Dopo aver acquisito tali informazioni, Mario le comunica a Luca in cambio di denaro.

# Legge n. 547 del 23/12/1993

## *art. 615-ter c.p.*

*(Accesso abusivo a un sistema informatico o telematico)*

### CASO 02

- ▶ Integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere dal soggetto abilitato?
  
- ▶ Integra il delitto previsto dall'art. *615-ter c.p.* la condotta di colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. (**CASS., SEZ. UNITE, 27 OTTOBRE 2011, N. 4694**)

# Legge n. 547 del 23/12/1993

## *art. 615-quater c.p.*

*(Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)*

- ▶ Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a lire 10 milioni (*cinquemilacentosessantaquattro euro*).
- ▶ La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni (*cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro*) se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater.

# Legge n. 547 del 23/12/1993

## *art. 615-quinquies c.p. (\*)*

*(Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico)*

- ▶ Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni.

*(\*) modificato con la legge n. 48 del 18/03/2008*

# Legge n. 547 del 23/12/1993

## *art. 616 c.p.*

*(Violazione, sottrazione e soppressione di corrispondenza)*

- ▶ Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è previsto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da trenta euro a cinquecentosedici euro.
- ▶ Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocimento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni [618].
- ▶ Il delitto è punibile a querela della persona offesa.
- ▶ *Agli effetti delle disposizioni di questa sezione, per "corrispondenza" s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.*

# Legge n. 547 del 23/12/1993

## *art. 617-quater c.p.*

*(Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)*

- ▶ Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
- ▶ Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo d'informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
- ▶ I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
- ▶ Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
  - 1) in danno di un sistema informatico o telematico utilizzato dallo stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
  - 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri e con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
  - 3) da chi esercita anche abusivamente la professione di un investigatore privato

# Legge n. 547 del 23/12/1993

## *art. 617-quinquies c.p.*

*(Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche)*

- ▶ Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
- ▶ La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.

# Legge n. 547 del 23/12/1993

## *art. 617-sexies c.p.*

*(Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)*

- ▶ Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.
- ▶ La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma del l'art. 617-quater.
- ▶ Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.(\*)

*(\*) aggiunto con il D.Lgs. n. 36 del 10/04/2018*

# Legge n. 547 del 23/12/1993

## *art. 621 c.p.*

*(Rivelazione del contenuto di documenti segreti)*

- ▶ Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altri atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero l'impiega a proprio o altrui profitto, è punito, se dal fatto deriva documento, con la reclusione fino a tre anni o con la multa da centotré euro a milletrentadue euro.
- ▶ *Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.*
- ▶ Il delitto è punibile a querela della persona offesa.

# Legge n. 547 del 23/12/1993

## *art. 623-bis c.p.*

### *(Altre comunicazioni e conversazioni)*

- ▶ Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza dei suoni, immagini o altri dati

# Legge n. 547 del 23/12/1993

## *art. 635-bis c.p. (\*)*

*(Danneggiamento di sistemi informatici e telematici)*

- ▶ Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.
- ▶ Se ricorre una o più delle circostanze di cui al secondo comma dell'art. 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

*(\*) modificato con la legge n. 48 del 18/03/2008*

# Legge n. 547 del 23/12/1993

## *art. 640-ter c.p. (Frode informatica)*

- ▶ Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire 100 mila a 2 milioni (*cinquantuno euro a millecentrentadue euro*).
- ▶ La pena è della reclusione da uno a cinque anni e della multa da lire 600 mila a 3 milioni (*euro 600 a euro 3.000*) se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
- ▶ Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante

# Frode Informatica

- ▶ Manipolazioni di dati: *input, output*
- ▶ Manipolazioni di programma
- ▶ Manipolazioni di hardware

**Il risultato finale sarà sempre un output falso**

# Frode Informatica

Manipolazioni di dati: *input*

## Esempio

Il funzionario di una banca modifica i dati relativi ai bonifici effettuati a favore dei clienti, aumentandone l'importo; provvede poi a stornare la somma in eccesso sul proprio conto corrente.

*(Modifica di dati veri)*

# Legge n. 547 del 23/12/1993

## *art. 266-bis c.p.p.*

*(Intercettazioni di comunicazioni informatiche o telematiche)*

1. Nei procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi".

# Legge n. 547 del 23/12/1993

## *art. 268 c.p.p.*

### *(Esecuzione delle operazioni)*

[...]

3-bis. Quando si procede a intercettazioni di comunicazioni informatiche o telematiche il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati.

[...]

6. Ai difensori delle parti è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche. Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno 24 ore prima.

# Legge n. 547 del 23/12/1993

## *art. 268 c.p.p.*

### *(Esecuzione delle operazioni)*

7. Il giudice dispone la trascrizione integrale delle registrazioni ovvero la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento.
8. I difensori possono estrarre copia delle trascrizioni e fare eseguire la trasposizione della registrazione su nastro magnetico. In caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono chiedere copia su idoneo supporto dei flussi intercettati, ovvero copia della stampa prevista comma 7.

# Evoluzione Normativa

» Legge n. 48 del 18/03/2008



# 2001 – Consiglio di Europa (Budapest)

## *Convenzione sulla criminalità informatica*

- ▶ è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche:
  - le violazioni dei diritti d'autore
  - la frode informatica
  - la pornografia infantile
  - le violazioni della sicurezza della rete.
- ▶ Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati.
- ▶ **obiettivo principale:** perseguire una politica penale comune per la protezione della società contro la cybercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

# Legge n. 48 del 18/03/2008

- ▶ L'Italia recepisce le direttive del Consiglio d'Europa del 2001:
  - **danneggiamento informatico** (c.p. artt. 635-bis, 635-ter, 635-quater, 635-quinquies):
    - distinzione tra danneggiamento dell'integrità dei dati e il danneggiamento dell'integrità del sistema;
    - differenziazione a seconda che l'oggetto della tutela abbia, o meno, rilevanza a fini pubblicistici.
  - **ridefinizione di documento informatico** (art. 491-bis c.p.);
  - **gestione della scena del crimine informatica** (c.p.p. artt. 244, 247, 248, 254-bis, 256, 259, 260, 352, 353, 354)

# Legge n. 48 del 18/03/2008

## *art. 491-bis c.p.*

*(Documenti informatici)*

- ▶ Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico, *avente efficacia probatoria*, si applicano le disposizioni del capo stesso concernenti agli atti pubblici.
- ▶ A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli

# **Legge n. 48 del 18/03/2008**

## ***art. 495-bis c.p.***

*(Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri)*

- ▶ Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno

# Legge n. 48 del 18/03/2008

## *art. 615-quinquies c.p.*

*(Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*

- ▶ Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

# Legge n. 48 del 18/03/2008

## *art. 635-bis c.p.*

*(Danneggiamento di informazioni, dati e programmi informatici)*

- ▶ Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
- ▶ Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio

# Legge n. 48 del 18/03/2008

## *art. 635-ter c.p.*

*(Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)*

- ▶ Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
- ▶ Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
- ▶ Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

# Legge n. 48 del 18/03/2008

## *art. 635-quater c.p.*

*(Danneggiamento di sistemi informatici o telematici)*

- ▶ Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
- ▶ Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

# Legge n. 48 del 18/03/2008

## *art. 635-quinquies c.p.*

*(Danneggiamento di sistemi informatici o telematici  
di pubblica utilità)*

- ▶ Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
- ▶ Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
- ▶ Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata

# Legge n. 48 del 18/03/2008

## *art. 640-quinquies c.p.*

*(Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)*

- ▶ Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

# Legge n. 48 del 18/03/2008

## *art. 420 c.p.*

*(Attentato a impianti di pubblica utilità)*

- ▶ Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.
- ▶ La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici e telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti.
- ▶ Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni.

# Legge n. 48 del 18/03/2008

## *art. 244 c.p.p.*

*(Casi e forme delle ispezioni)*

1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, *anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

# Legge n. 48 del 18/03/2008

## *art. 247 c.p.p.*

*(Casi e forme delle perquisizioni)*

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

*1bis Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

2. La perquisizione è disposta con decreto motivato.
3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

# Legge n. 48 del 18/03/2008

## *art. 248 c.p.p.*

*(Richiesta di consegna)*

1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini .
2. Per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare *atti, documenti e corrispondenza presso banche presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici.* In caso di rifiuto, l'autorità giudiziaria procede a perquisizione.

# Legge n. 48 del 18/03/2008

## art. 254 c.p.p.

(Sequestro di corrispondenza)

1. *Presso coloro che forniscono servizi postali, telegрафici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa o che comunque possono avere relazione con il reato.*
2. Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli *o alterarli* e senza prendere altrimenti conoscenza del loro contenuto.
3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.

# Legge n. 48 del 18/03/2008

## *art. 254-bis c.p.p.*

*(Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni)*

1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali

# Legge n. 48 del 18/03/2008

## *art. 256 c.p.p.*

*(Dovere di esibizione e segreti)*

1. Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, *nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto*, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inherente al loro ufficio o professione.

[...]

# Legge n. 48 del 18/03/2008

## *art. 259 c.p.p.*

*(Custodia delle cose sequestrate)*

1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'articolo 120.
2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. *Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salvo, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria.* Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.

# Legge n. 48 del 18/03/2008

## *art. 260 c.p.p.*

*(Apposizione dei sigilli alle cose sequestrate. Cose deperibili.  
Distruzione di cose sequestrate)*

1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, *anche di carattere elettronico o informatico*, idoneo a indicare il vincolo imposto a fini di giustizia.
2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'articolo 259. *Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.*

[...]

# Legge n. 48 del 18/03/2008

## *art. 352 c.p.p.*

### *(Perquisizioni)*

[...]

*1-bis.* Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

[...]

# Legge n. 48 del 18/03/2008

## *art. 353 c.p.p.*

*(Acquisizione di plichi o di corrispondenza)*

1. Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.
2. Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata *e l'accertamento del contenuto*.
3. Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, *anche se in forma elettronica o se inoltrati per via telematica*, per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, *telegrafico, telematico o di telecomunicazione* di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati.

# Legge n. 48 del 18/03/2008

## *art. 354 c.p.p.*

*(Accertamenti urgenti sui luoghi, sulle cose e sulle persone.  
Sequestro)*

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. *In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.* Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.

[...]

# Esempio conclusivo

## *i ransomware*

- ▶ I dati presenti sul PC sono cifrati cancellando perennemente gli originali e proteggendoli con una chiave di cifratura che l'utente non conosce e che quindi non potrà utilizzare per ripristinare i propri documenti.
- ▶ Chi ha creato o diffuso il ransomware richiede il pagamento di un riscatto da versarsi in Bitcoin entro alcuni giorni, pena la cancellazione permanente della chiave, il che implica l'impossibilità di riottenere i propri documenti.

**Quali reati sono stati compiuti?**

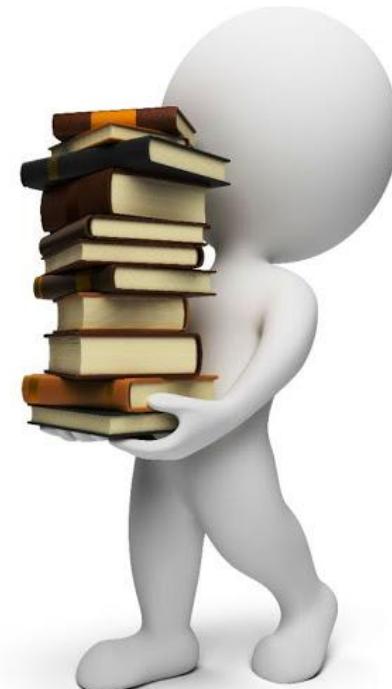
# Esempio conclusivo

## *i ransomware*

- ▶ Dal punto di vista giuridico, l'utilizzo di questo tipo di *malware* implica la commissione di almeno tre reati:
  - Accesso abusivo a sistema informatico (*art. 615-ter*)
  - Danneggiamento di informazioni, dati e programmi informatici (*art. 635-bis c.p./art. 635-ter c.p.*)
  - Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (*art. 615-quinquies*)

# Bibliografia

- ▶  [www.interlex.it](http://www.interlex.it)
- ▶  [www.altalex.com](http://www.altalex.com)
- ▶  [www.brocardi.it](http://www.brocardi.it)
- ▶  [www.coe.int](http://www.coe.int)
- ▶  Diritto penale dell'informatica  
C. Pecorella – (2006) CEDAM





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# Lezione 5: Question Time



A.A. 2019/20  
**Dott. Lorenzo LAURATO**



# Domanda nr. 01



## Il GIP Giudice per le Indagini Preliminari

- |                                     |  |   |
|-------------------------------------|--|---|
| <input type="checkbox"/>            | è l'unico interlocutore del Pubblico Ministero   | X |
| <input type="checkbox"/>            | emette una sentenza                              | X |
| <input checked="" type="checkbox"/> | provvede sulle misure cautelari                  | ✓ |
| <input checked="" type="checkbox"/> | può non accogliere la richiesta di archiviazione | ✓ |

# Giudice dell'Indagine Preliminare (G.I.P.)

- ▶ Funzione di garanzia dell'indagato nella fase delle *indagini preliminari*. Può decidere se accogliere le richieste del P.M. su:
  - applicare misure cautelari;
  - autorizzare e convalidare l'uso delle intercettazioni come mezzi di ricerca della prova;
- ▶ Funzione di garanzia dell'azione penale:
  - accogliere o no la richiesta di archiviazione;
  - ▶ non ha autonomia di iniziativa probatoria: provvede esclusivamente su richiesta della parte;
  - ▶ è privo di un proprio fascicolo: gli atti conosciuti sono quelli che il PM decide di allegare alle istanze che presenta;



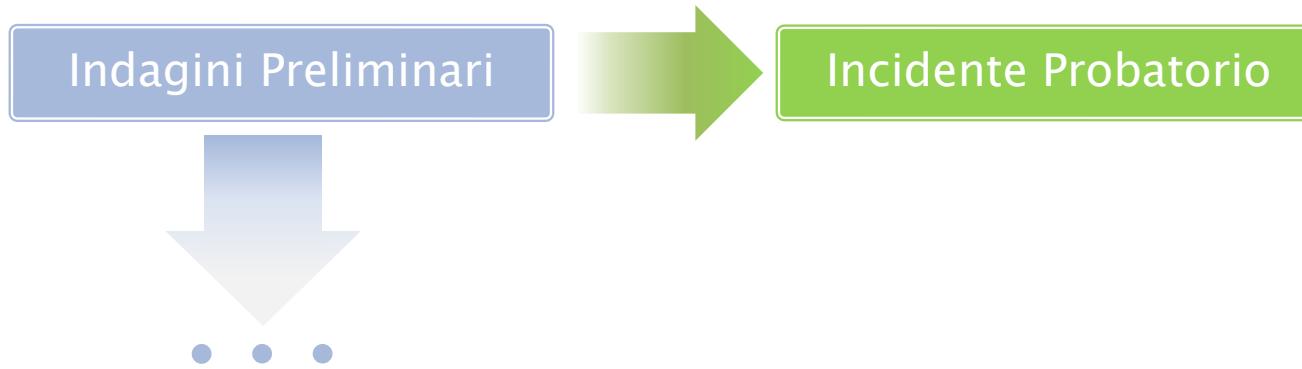
# Domanda nr. 02

L'incidente probatorio...

- viene richiesto solo dal P.M. ✗
- ha lo scopo di formare la prova ✓
- viene richiesto per velocizzare il procedimento ✗
- nessuna delle precedenti ✗



# Procedimento Penale: *incidente probatorio*



- ▶ Può essere richiesta dalle parti ed ha la funzione di anticipare l'acquisizione e la formazione di una prova durante le indagini preliminari;
- ▶ Viene richiesta al Giudice per le Indagini Preliminari (GIP);
- ▶ Il GIP, nel caso in cui sono richieste particolari competenze tecniche, può nominare un proprio consulente tecnico: il Perito.

# Domanda nr. 03



Il PM conferisce incarico ai sensi dell'art. 360 c.p.p.

- Quando occorre agire in assoluta urgenza a causa della deperibilità del reperto ✗
- Quando sussiste il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di analisi ✓
- Indica al Perito che deve eseguire un accertamento tecnico non ripetibile ✗
- Quando il PM vuole fornire la più ampia garanzia alle parti escludendo il rischio di successive eccezioni ✗

# Procedimento Penale:

## *accertamento tecnico* (art. 359 cpp)

- ▶ il P.M. può avere la necessità di svolgere **accertamenti tecnici**, che comportano specifiche conoscenze scientifiche, tecniche o artistiche, che esulano dalle competenze possedute dall'organo inquirente.
- ▶ il P.M. può avvalersi/nominare un Consulente Tecnico.

# Procedimento Penale: *accertamento tecnico irripetibile* (art. 360 cpp)

- ▶ accertamenti che se compiuti comportano l'alterazione della prova e la ripetibilità della procedura non è più garantibile;
- ▶ il P.M. esegue questa attività di accertamento avvisando previamente:
  - *l'indagato e il suo difensore;*
  - *la parte offesa e il suo difensore;*in modo da dare la possibilità a questi ultimi di assistere a tutta l'operazione a garanzia del rispetto delle procedure.
- ▶ Le parti hanno la facoltà di nominare un proprio *Consulente Tecnico.*



# Domanda nr. 04

L'Organo Giudiziario con funzione requirente/inquirente è



il PM



il GIP



la Polizia Giudiziaria



il Consulente Tecnico d'Ufficio



il Perito



# Struttura organizzativa

- ▶ Uffici magistratura inquirente:
  - Procure della Repubblica c/o i Tribunali Ordinari / per i Minorenni / Militari;
  - Procure Generali c/o le Corti d'Appello;
  - Procura Generale c/o la Suprema corte di Cassazione;
- ▶ Uffici magistratura giudicante:
  - Tribunali Ordinari;
  - Tribunali per i Minorenni;
  - Tribunali Militari;
  - Corte di Appello;
  - Suprema Corte di Cassazione;



# Domanda nr. 05

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art 359 c.p.p.?

- l'indagato con il proprio difensore ✗
- la persona offesa ✗
- il consulente tecnico dell'indagato (CTP) ✗
- il consulente tecnico del P.M. (CTU) ✓



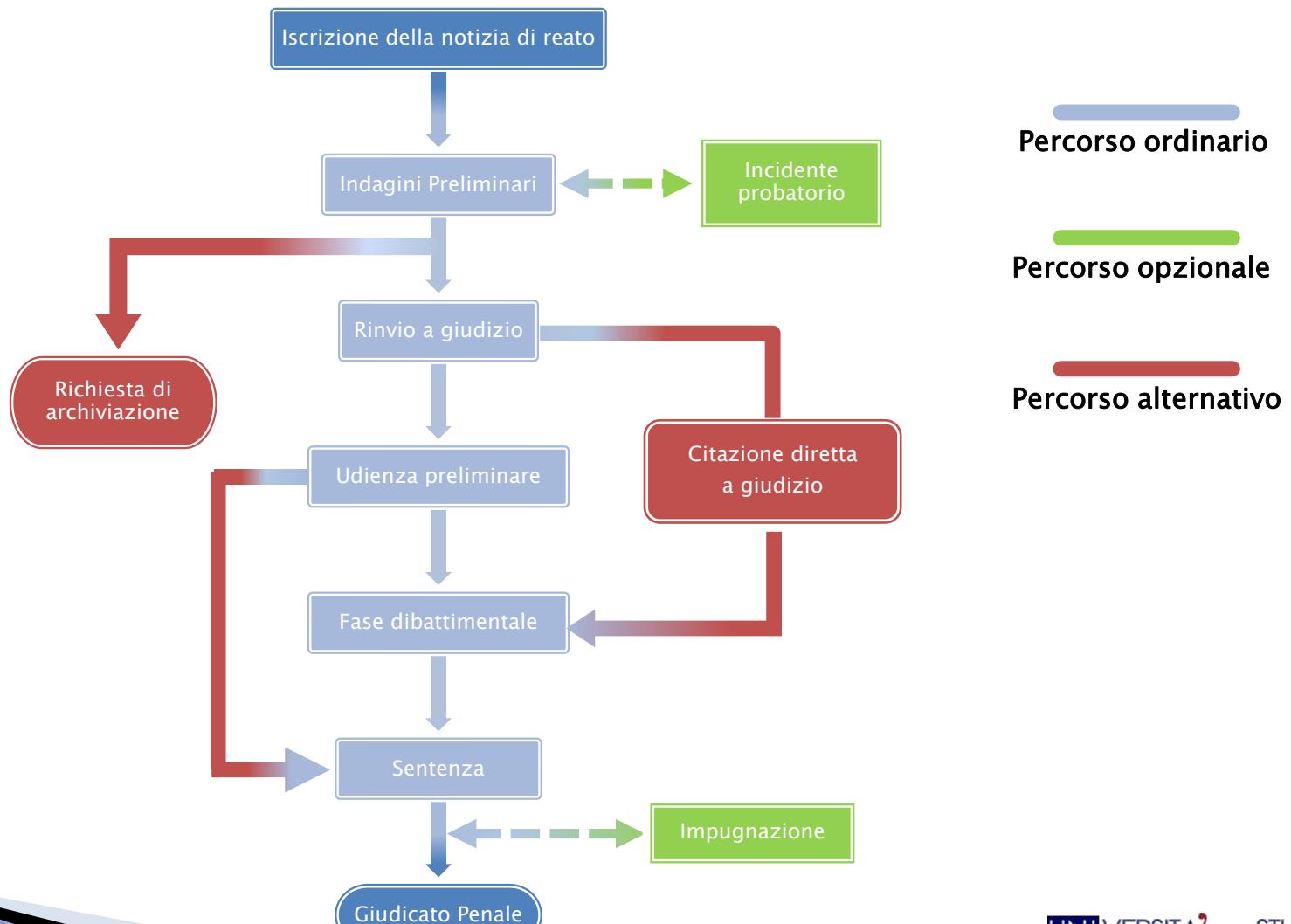
# Domanda nr. 06

Chi può prendere parte agli accertamenti tecnici ai sensi dell'art 360 c.p.p.?

- il difensore dell'imputato ✗
- il difensore dell'imputato accompagnato dal proprio consulente tecnico (CTP) ✗
- il consulente tecnico di parte della persona offesa (CTP) ✓
- il Perito ✗



# Procedimento Penale



# L'indagato e l'imputato

- ▶ **L'INDAGATO** è la persona nei confronti vengono svolte delle indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato.
  - La qualità di indagato si conserva fino alla richiesta di rinvio a giudizio o di archiviazione;
- ▶ **L'IMPUTATO** è la persona indagata nei confronti della quale è stata esercitata l'azione penale (*rinvio a giudizio*);
  - La qualità di imputato si conserva in ogni stato e grado del processo, sino a che la sentenza non diventi definitiva.
  - La sua assenza in udienza non né pregiudica il suo corso, che viene ugualmente celebrato (*contumace*).
- ▶ **ENTRAMBI** hanno l'obbligo di farsi assistere da un difensore.
  - Possono difendersi producendo memorie e possono essere interrogati esclusivamente alla presenza del difensore.
  - Possono avvalersi di consulenti tecnici.



# Il C.F. nel Procedimento Penale:

## *accertamento irripetibile* (art. 360 cpp)

- il P.M. esegue questa attività di accertamento avvisando previamente l'indagato e il suo difensore in modo da dare la possibilità a questi ultimi di assistere a tutta l'operazione a garanzia del rispetto delle procedure. L'indagato può nominare e farsi assistere un proprio Consulte Tecnico: Consulente Tecnico di Parte (CTP).

Consulente  
Tecnico d'Ufficio  
(CTU)



Pubblico  
Ministero



Difensore



Consulente  
Tecnico di Parte  
(CTP)



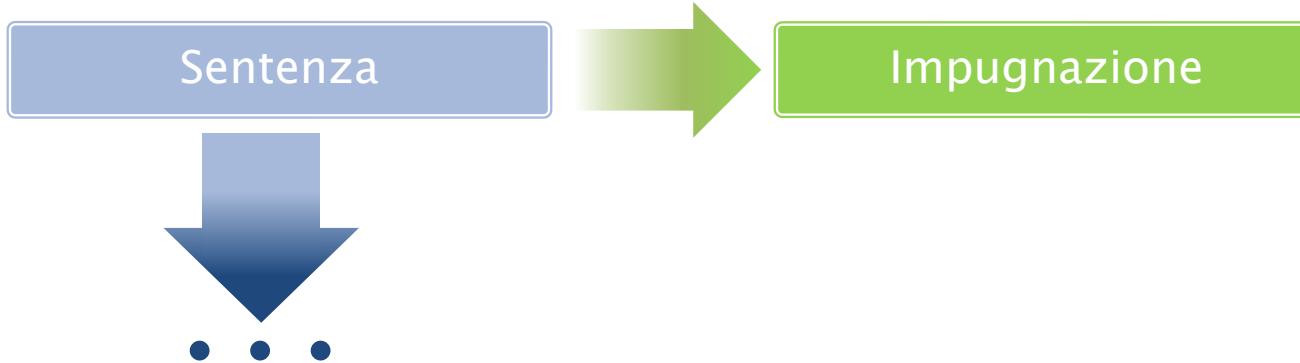
# Domanda nr. 07



Quando si giunge al Giudicato Penale?

- Quando il giudice deposita la sentenza ✗
- Quando viene emessa la sentenza dalla Corte di Cassazione. ✓
- Quando viene emessa la sentenza dalla Corte di Appello ✗
- Quando sono decorsi i termini per proporre opposizione\impugnazione ✓

# Procedimento Penale: *impugnazione*



- ▶ è lo strumento attraverso il quale la parte processuale, nei cui confronti sia stato emesso un provvedimento giudiziario svantaggioso ne rimette il controllo ad un giudice diverso:
  - **Secondo grado di giudizio:** si ricorrere alla *Corte d'appello*. Questo secondo grado di giudizio può addirittura ribaltare le sentenze emesse in primo grado.
  - **Terzo grado di giudizio:** si ricorrere alla *Corte di cassazione* quando vi sono elementi per ritenere che il processo sia stato condotto non interpretando bene le leggi e sia dunque illegittimo. Non giudica l'imputato ma la sentenza d'appello ed in caso affermativo si procede al suo annullamento.

# Domanda nr. 08



Quali caratteristiche sono proprie della Persona Offesa

In alcuni casi può chiedere l'archiviazione del procedimento ✗

Può sporgere denuncia e fare esposti ✓

Può prendere parte sia alla fase delle indagini preliminari che a quella del giudizio ✓

Non può sporgere querela ✗

Può farsi assistere da un proprio Consulente Tecnico ✓

# La Persona Offesa (P.O.)



- ▶ è il soggetto titolare del bene giuridico (*patrimoniale, morale, personale, etc.*) leso dall'autore di un reato;
- ▶ Ha il diritto di querela in tutti i casi in cui per il reato non debba procedersi d'ufficio o dietro richiesta o istanza;
- ▶ Può presentare **memorie**, indicare **elementi di prova**, e nominare un difensore e consulenti tecnici;

# Esposto, Denuncia e Querela

- ▶ **ESPOSTO:** è la segnalazione all'Autorità Giudiziaria di un fatto allo scopo di far valutare se ricorre un'ipotesi di reato;
- ▶ **DENUNCIA:** è un atto con il quale si informa l'Autorità Giudiziaria di una notizia di reato perseguibile d'ufficio(*senza la denuncia/querela della parte offesa*).
- ▶ **QUERELA:** è una dichiarazione della persona offesa con la quale si esprime la volontà di punire il colpevole per un reato subito, non persegibile d'ufficio. Può essere ritirata (*rimessa*) se non tratta di reati sessuali ai danni di minori (*irrevocabile*).



# Domanda nr. 09



L'intervento di un computer forensen può essere richiesto da:

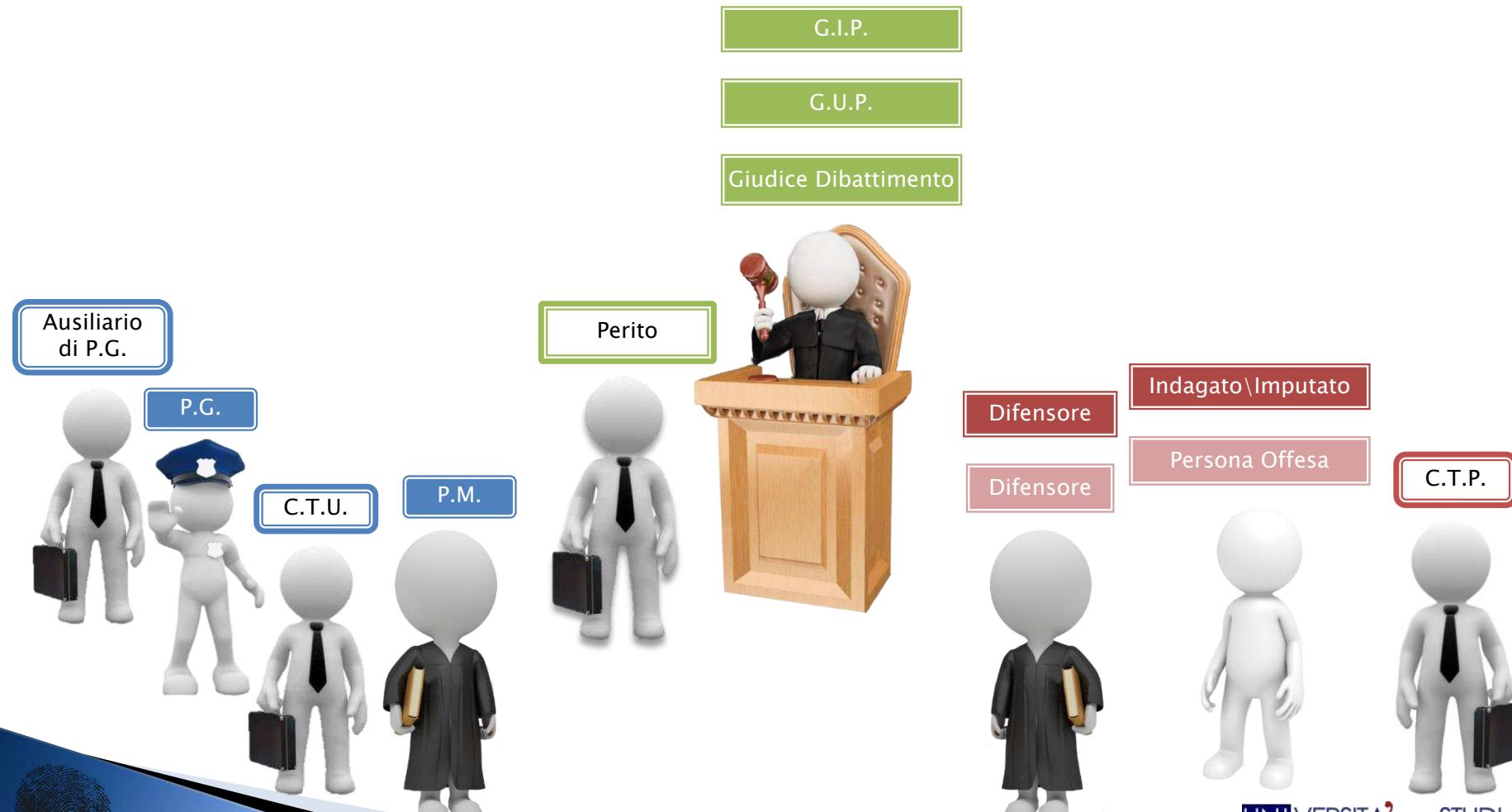
- Il Giudice dibattimentale in composizione monocratica ✓
- Il Pubblico Ministero ✓
- L'indagato ✓
- la Polizia Giudiziaria ✓
- La Parte Offesa ✓

# Il C.F. nel Procedimento Penale: *riepilogando...*

- ▶ Il Computer Forensi a seconda da chi e da quando viene incaricato assume ruoli diversi all'interno del procedimento:
  - Ausiliario di P.G.: quando il consulente tecnico è incaricato dalla Polizia Giudiziaria durante determinate operazioni;
  - Consulente Tecnico d'Ufficio (CTU): quando il consulente tecnico è incaricato dal Pubblico Ministero (PM) durante le indagini preliminari per svolgere determinati accertamenti;
  - Consulente Tecnico di Parte (CTP): quando una delle parti coinvolte nel procedimento (indagato/imputato e/o persona offesa) incaricano un proprio consulente tecnico:
    - per assisterlo a presentare prove tecniche del reato subito (*parte offesa*)
    - per controbattere a determinate operazioni tecniche compiute dalla parte accusatoria (*indagato*)
  - Perito del Giudice: quando il Giudice ha bisogno di compiere determinati accertamenti tecnici o valutare quelle compiute dalle parti;



# Gli Attori nel Procedimento Penale: *riepilogando...*



# Domanda nr. 10

Qual'è l'ambito di applicazione della computer forensics

- I reati che hanno come obiettivo un sistema informatico ✗
- I reati che hanno come mezzo un sistema informatico ✗
- Qualsiasi reato dove possa esistere un sistema informatico coinvolto a qualsiasi titolo ✓
- I reati informatici descritti dal codice penale ✗



# Legge n. 48 del 18/03/2008

## *art. 247 c.p.p.*

*(Casi e forme delle perquisizioni)*

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
- 1bis* *Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*
2. La perquisizione è disposta con decreto motivato.
3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

# Domanda nr. 11

La scelta degli strumenti tecnici e delle metodologie che il computer forensi deve impiegare nella corretta conduzione della propria opera è dettato da:

- Il Pubblico Ministero in fase di conferimento dell'incarico ✗
- Il Codice di Procedura Penale ✗
- La comunità scientifica internazionale ✓
- La legge 48/2008, Legge di ratifica del Consiglio di Europa di Budapest del 2001 ✗



# Il C.F. nel Procedimento Penale: *il ruolo del Computer Forensi*

- ▶ Il C.F. deve impiegare metodi e strumenti che garantiscono l'inalterabilità della prova, anche se non dettagliatamente descritti dalla legge.



# Legge n. 48 del 18/03/2008

## *art. 354 c.p.p.*

*(Accertamenti urgenti sui luoghi, sulle cose e sulle persone.  
Sequestro)*

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. *In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.* Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.

[...]

# Domanda nr. 12

Luca nota il suo vicino di casa costruire una mansarda. Egli può fare:

un esposto



una denuncia



una querela



nessuna delle precedenti



# Domanda nr. 13

Luca scopre che il suo vicino detiene materiale di pornografia minorile. Egli può fare:

- un esposto ✗
- una denuncia ✓
- una querela ✗
- nessuna delle precedenti ✗



# Domanda nr. 14

Luca nota che Mario percuote Francesca. Egli può fare:

- un esposto
- una denuncia
- una querela
- nessuna delle altre risposte

✗

✗

✗

✓



# Esposto, Denuncia e Querela

- ▶ **ESPOSTO:** è la segnalazione all'Autorità Giudiziaria di un fatto allo scopo di far valutare se ricorre un'ipotesi di reato;
- ▶ **DENUNCIA:** è un atto con il quale si informa l'Autorità Giudiziaria di una notizia di reato perseguibile d'ufficio(*senza la denuncia/querela della parte offesa*).
- ▶ **QUERELA:** è una dichiarazione della persona offesa con la quale si esprime la volontà di punire il colpevole per un reato subito, non persegibile d'ufficio. Può essere ritirata (*rimessa*) se non tratta di reati sessuali ai danni di minori (*irrevocabile*).



# Domanda nr. 15

Analizzando il seguente documento si evince:



agli indagati viene addebitato il reato di "Accesso abusivo a un sistema informatico" ✓

agli indagati viene addebitato il reato di "Diffusione di programmi informatici diretti a danneggiare un sistema informatico" ✗

gli indagati hanno nominato un proprio Consulente Tecnico ✗

il PM dispone un accertamento tecnico irripetibile ✓



# Verbale di conferimento incarico

Proc. N. xxxx/aa R.G.N.R. Mod.21



## PROCURA DELLA REPUBBLICA presso il Tribunale di Napoli III<sup>^</sup> Sezione

Accertamento irripetibile

### VERBALE DI NOMINA del CTU E DI CONFERIMENTO DELL'INCARICO

- artt. 360, 549 c.p.p., 116 e 117 D. Lv. 271/89 -

Reato

Il giorno 20 del mese di Settembre dell'anno 2018, alle ore 12.52 in Napoli- Palazzo di Giustizia, presso L'Ufficio del PM in Napoli Centro Direzionale piano, nel procedimento di cui in epigrafe nei confronti di **INDAGATO** + altri, indagati per i reati di cui agli artt. 416, 615ter, 640 ter c.p. commessi in Castel Volturno, Marcianise e altri luoghi e altro innanzi al Pubblico Ministero Dott. MAGISTRATO Sost. Procuratore della Repubblica presso il Tribunale di Napoli, e alla presenza della dott.ssa TIROCINANTE, M.O.T. mirato presso questo Ufficio, sono comparsi citati regolarmente ex art 360 c.p.p.:

- il C.T.U. Dott. Lorenzo LAURATO nato a OMISSIS noto all'Ufficio iscritto all'Albo del Tribunale di Napoli domiciliato presso lo studio di Via Coroglio n. 57 /D;
- il CTU Dott. Consulente TECNICO nato a OMISSIS , domiciliato presso lo studio professionale in OMISSIS
- per gli indagati INDAGATO A e INDAGATO B di fiducia; d'ufficio per INDAGATO C , INDAGATO D, l'Avv. DIFENSORE A del foro di Napoli;
- l'Avv. DIFENSORE C per delega – che deposita - dell'Avv. DIFENSORE B, per gli indagati INDAGATO E e INDAGATO F;
- per la persona offesa WIND 3 spa l'Avv. DIFENSORE E in sostituzione dell'Avv. DIFENSORE D del foro di Roma, come da delega che deposita;

Consulente Tecnico

Difensori Indagati

Difensore P.O.

SSRI

Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI  
NAPOLI FEDERICO II

# Legge n. 547 del 23/12/1993

## *art. 615-ter c.p.*

*(Accesso abusivo a un sistema informatico o telematico)*

- ▶ Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
- ▶ La pena è della reclusione da uno a cinque anni:
  - 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
  - 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
  - 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

# Legge n. 547 del 23/12/1993

## *art. 640-ter c.p. (Frode informatica)*

- ▶ Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire 100 mila a 2 milioni (*cinquantuno euro a millecentrentadue euro*).
- ▶ La pena è della reclusione da uno a cinque anni e della multa da lire 600 mila a 3 milioni (*euro 600 a euro 3.000*) se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
- ▶ Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante

# Domanda nr. 16



## L'indagato\l'imputato

ha l'obbligo di farsi assistere da un difensore



ha l'obbligo di farsi assistere da un consulente tecnico quanto viene eseguito un accertamento tecnico



ha l'obbligo di presenziare in udienza



# L'indagato e l'imputato

- ▶ **L'INDAGATO** è la persona nei confronti vengono svolte delle indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato.
  - La qualità di indagato si conserva fino alla richiesta di rinvio a giudizio o di archiviazione;
- ▶ **L'IMPUTATO** è la persona indagata nei confronti della quale è stata esercitata l'azione penale (*rinvio a giudizio*);
  - La qualità di imputato si conserva in ogni stato e grado del processo, sino a che la sentenza non diventi definitiva.
  - La sua assenza in udienza non né pregiudica il suo corso, che viene ugualmente celebrato (*contumace*).
- ▶ **ENTRAMBI** hanno l'obbligo di farsi assistere da un difensore.
  - Possono difendersi producendo memorie e possono essere interrogati esclusivamente alla presenza del difensore.
  - Possono avvalersi di consulenti tecnici.



# (Avvocato) Difensore

- ▶ **Ruolo di assistenza:** resta una collaborazione di natura tecnica, diventando la bocca e l'orecchio “giuridico” del cliente;
- ▶ **Ruolo di rappresentanza:** agisce in sostituzione dell’interessato nell’esercizio di diritti e facoltà;
- ▶ E’ nominato sia dalla parte offesa, sia dalla parte indagata/imputata;
- ▶ La presenza del difensore oltre che un diritto, è condizione prima di legittimità e regolarità dello stesso procedimento penale:
  - Se l’indagato/imputo non nomina un difensore di fiducia, gli viene affidato un **difensore d’ufficio**.
- ▶ Può ottenere un accesso agli atti delle indagini preliminari:
  - *Completo*: solo a seguito dell’avviso di conclusione indagini (*415bis c.p.p.*)
  - *Parziale*: accesso limitato agli atti a sostegno di una singola misura preventiva per poter gestire una eventuale opposizione;



# Domanda nr. 17



## Il procedimento civile...

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Le parti in giudizio sono: l'attore ed il convenuto                     | ✓ |
| <input checked="" type="checkbox"/> Le parti in giudizio sono: il ricorrente ed il resistente               | ✓ |
| <input type="checkbox"/> Ha lo scopo di accertare la verità nell'interesse dello Stato e della collettività | ✗ |
| <input checked="" type="checkbox"/> Si instaura esclusivamente su iniziativa di una parte                   | ✓ |
| <input type="checkbox"/> Solo le parti in giudizio possono nominare un Consulente Tecnico                   | ✗ |

# Penale      vs      Civile

1. Diritto Penale;
2. Si realizza in due strutture diverse: Procura e Tribunale;
3. Ha lo scopo di accertare la verità nell'interesse dello Stato e della collettività;
4. Si instaura anche d'ufficio.
5. il giudice non si pone una situazione di indifferenza, ma persegue uno scopo ben preciso: accertare la verità del reato;

1. Diritto Privato;
2. Si realizza in un'unica struttura: il Tribunale;
3. Ha lo scopo di verificare l'esistenza di un diritto reclamato da un privato cittadino nei confronti di un altro e quale, tra le due parti in causa, ha ragione;
4. Si instaura esclusivamente su iniziativa di una parte: l'attore
5. il giudice si attiene solo alle prove presentate dalle parti, ponendosi in una posizione di equidistanza e imparzialità (**principio dispositivo**);

# Procedimento Civile: *procedimento ordinario*

- ▶ **FASE INTRODUTTIVA:** iscrizione a ruolo
  - L'Attore (la parte che instaura un giudizio) tramite l'avvocato espone i fatti che vengono posti a giudizio (*atto di citazione*);
  - L'atto di citazione viene notificato alla controparte: il **convenuto**.
- ▶ **FASE ISTRUTTORIA:** vengono acquisite in giudizio le prove richieste dalle parti, tipicamente:
  - Testimoniali (scritte o orali);
  - Consulenze tecniche di parte (C.T.P.);
  - Il giudice può nominare un Consulente Tecnico d'Ufficio (C.T.U.)
- ▶ **FASE CONCLUSIVA:** le parti devono chiarire definitivamente le proprie richieste, anche alla luce di quanto emerso nel corso del procedimento;
- ▶ **FASE DECISORIA:** il giudice ha tutti gli elementi per pronunciarsi sulla controversia e può finalmente emettere la sentenza.

# Procedimento Civile: *procedimento con ricorso*

## ▶ FASE INTRODUTTIVA:

- Il ricorrente (la parte che instaura un giudizio) tramite l'avvocato espone i fatti che vengono posti a giudizio (domanda con ricorso) direttamente al Giudice;
- successivamente il Giudice emette un decreto di fissazione dell'udienza
- Il ricorrente notifica l'udienza alla controparte: **il resistente.**
- Le parti devono già esporre tutte le proprie difese e formulare le istanze istruttorie (rendere più celere il giudizio);

## ▶ FASE CONCLUSIVA

## ▶ FASE DECISORIA

# Domanda nr. 18



## La c.d. "preview"

è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione



il suo uso è indicato nel codice di penale



Può essere compiuto da qualsiasi agente della P.G. poiché ha un basso rischio di alterazione della prova



agevola l'individuazione di fonti di prova





## SSRI Lorenzo Laurato s.r.l.



Via Coroglio nr. 57/D (BIC- Città della Scienza)  
80124 Napoli



Tel. 335.54.56.550 - 081.19804755



Fax 081.19576037

[lorenzo.laurato@ssrilab.com](mailto:lorenzo.laurato@ssrilab.com) - [info@ssrilab.com](mailto:info@ssrilab.com)  
[ssri@legalmail.it](mailto:ssri@legalmail.it)

# COMPUTER FORENSICS

## Lezione 6: Fasi del trattamento *identificazione e raccolta*



A.A. 2021/22

Dott. Lorenzo LAURATO



# Cosa è la Computer Forensics?

l'insieme di metodologie  
scientificamente provate  
finalizzate alla ricostruzione  
di eventi ai fini probatori che  
coinvolgono direttamente o  
indirettamente  
un supporto digitale

# Fasi



# Identificazione dell'evidence

- ▶ Ricercare la fonte di prova che può dare una svolta alle indagini: la prima fase è volta a individuare dove un dato è conservato.



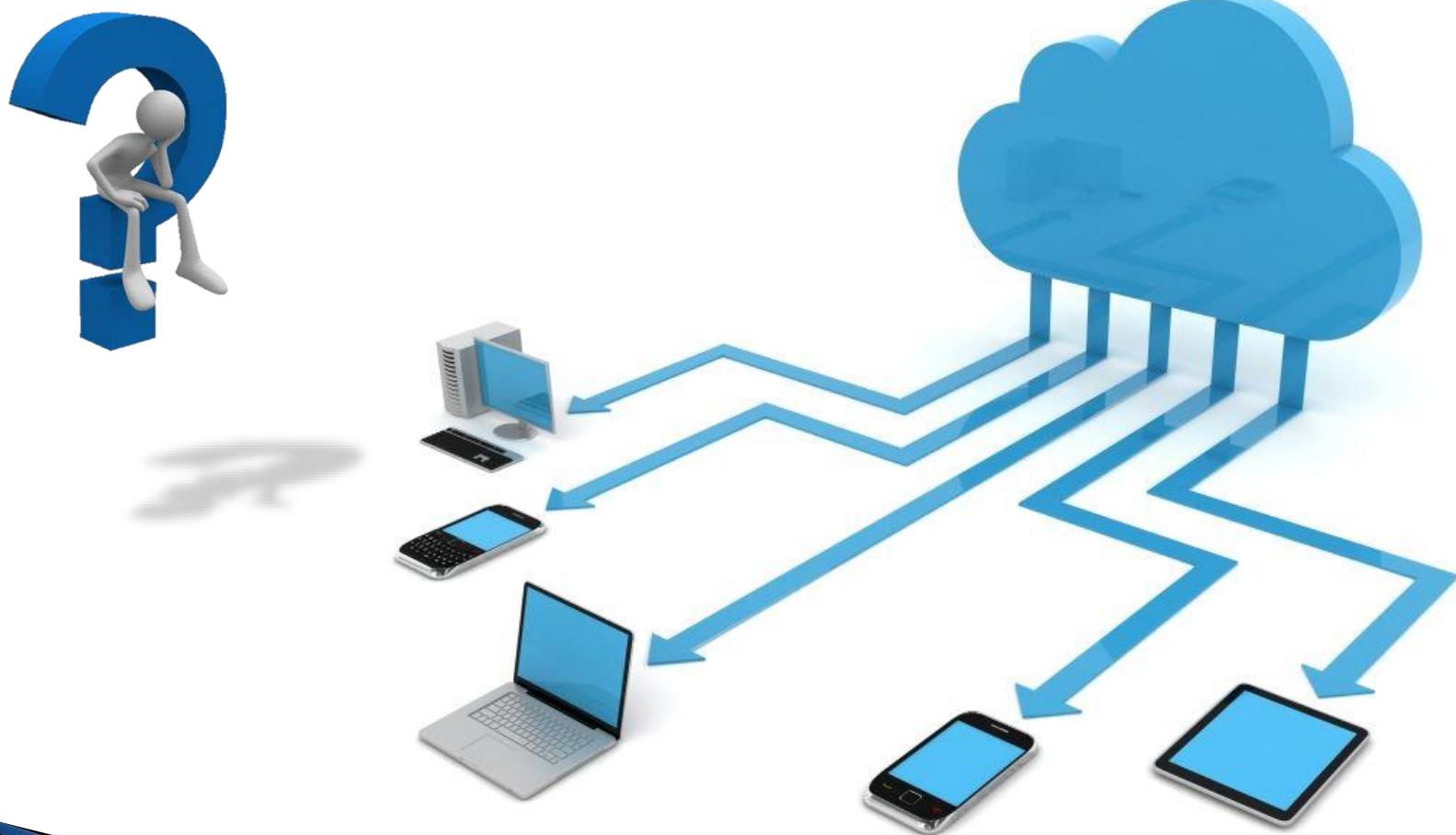
# Identificazione dell'evidence

Vanno individuati tutti i dispositivi che possono contenere dati rilevanti:

- ▶ Computer/Notebook
- ▶ Cellulari e Tablet
- ▶ Memory Card, PenDrive, Hard Disk Esterni, CD/DVD
- ▶ Fotocamere e Videocamere
- ▶ Server
- ▶ Stampanti, Fax, Router

# Identificazione dell'evidence

## *il Cloud*



# Identificazione dell'evidence

individuare i dispositivi che possono contenere  
dati rilevanti



# Legge n. 48 del 18/03/2008

## *art. 247 c.p.p.*

*(Casi e forme delle perquisizioni)*

[...]

*1bis Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

[...]

# Identificazione dell'evidence

## *la «preview»*

- ▶ Consente di eseguire un'analisi di primo livello delle memorie dei dispositivi allo scopo di individuare possibili elementi di interesse investigativo.
- ▶ utilizzo di write blocker (*software/hardware ad hoc*)
- ▶ rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova;

# Identificazione dell'evidence

## *la «preview»*

### DEAD

- ▶ è un'analisi eseguita con il S.O. spento.
- ▶ uso di **write block**: permette di non alterare il dispositivo da analizzare;
  - Hardware

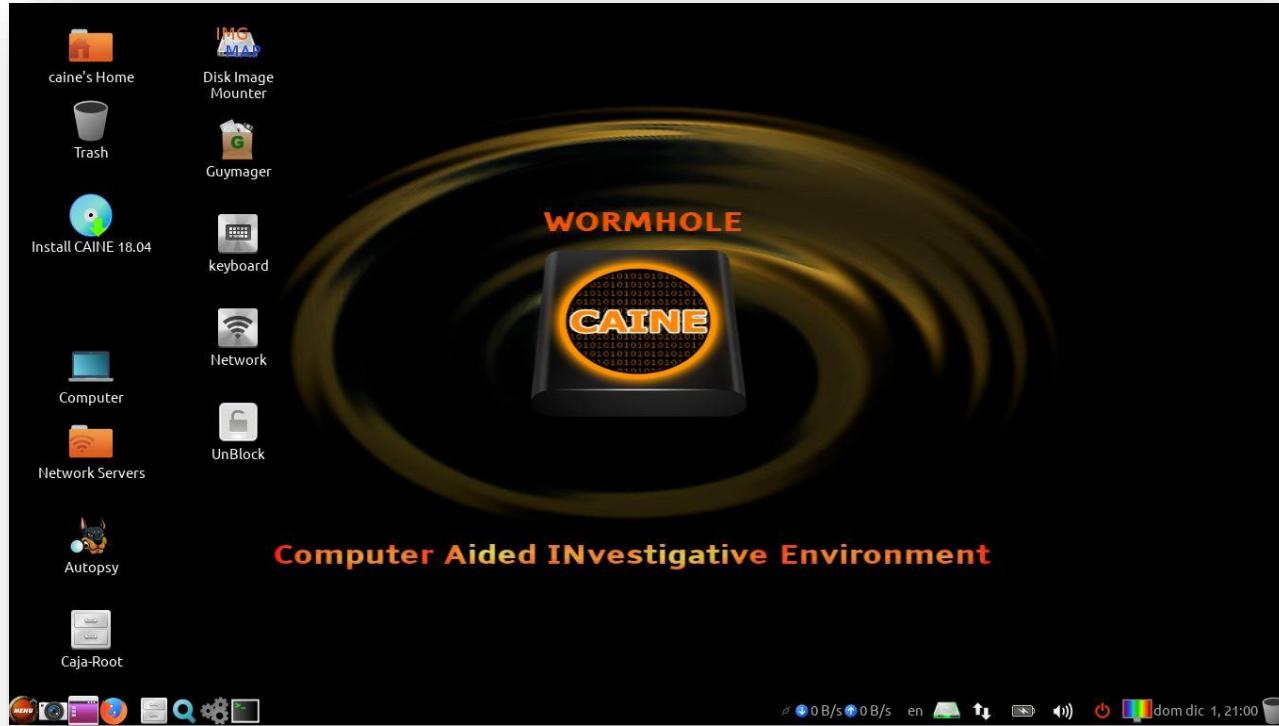


# Identificazione dell'evidence

*la «preview»*

## DEAD

- Software: distro Linux Live



# Identificazione dell'evidence

*la «preview»*

## DEAD

▶ **PRO:**

- Permette di non alterare il dispositivo;
- Consente di utilizzare diversi strumenti per analizzare la memoria del dispositivo.

▶ **CONTRO:**

- Buona conoscenza del sistema e dei software da analizzare
- Non sempre praticabile: sistemi embedded;

# Identificazione dell'evidence

## *la «preview»*

### LIVE

- ▶ è un'analisi eseguita impiegando il S.O. presente sul dispositivo da analizzare;
- ▶ deve essere documentata e verbalizzata;
- ▶ **PRO:**
  - consente di avere una visione dell'ambiente in cui opera l'utente;
  - è veloce nell'analisi dei software installati;
- ▶ **CONTRO:**
  - Alterazione del reperto
  - Strumenti adeguati al sistema

# Identificazione dell'evidence

## *la «preview»*

### Live

*Analisi su sistemi attivi*

Visualizzazione a livello utente

Analisi dei software

Tool ad hoc

Alto rischio di alterabilità

### Dead

*Analisi su sistemi spenti*

Basso rischio di alterabilità

Maggiori strumenti a disposizione

Non sempre impiegabile  
(Raid, cifratura, etc.)

Conoscenza del S.O.

# Cambiamento di stato del dispositivo

Acceso → Spento

Spento → Acceso

# Cambiamento di stato del dispositivo

## *shutdown*

- ▶ Prima di eseguirlo valutare le seguenti criticità:
  - Cifratura
  - Software in esecuzione
  - Dump della RAM
- ▶ Come spegnere il dispositivo che si vuole analizzare/sequestrare:
  - Scollegarlo dalla rete elettrica (*unplug*):
    - Potrebbe compromettere il funzionamento del sistema (Server, Raid, etc.)
  - Eseguire lo spegnimento mediante il S.O.:
    - Vengono eseguite sul disco diverse operazioni (Aggiornamenti, esecuzioni di batch, etc.)

# Cambiamento di stato del dispositivo *accensione*

- ▶ Valutare se le informazioni che perderemo sono meno importanti dell'urgenza dell'accertamento:
  - Ultimo accesso al sistema;
  - Esecuzione sul disco di diverse operazioni;

# Fasi



# La Raccolta: *il sequestro*

- ▶ Dopo aver identificato i dispositivi o i dati di possibile interesse investigativo si procede con il sequestro:
  - **Fisico**: prendere fisicamente il supporto su cui il dato di possibile interesse risiede.
  - **Logico**: eseguire una copia totale o parziale della memoria del dispositivo

# La Raccolta: *il sequestro fisico*

- ▶ Prendere semplicemente il supporto contenente i dati, posticipando le problematiche derivanti dall'acquisizione del dato;
- ▶ Preoccuparsi solo di identificare e verbalizzare i reperti:
  - *Catena di custodia (Chain of Custody)*

# La Raccolta: *la catena di custodia*

- ▶ Uno o più documenti (verbale/i) in cui devono essere riportati tutte le informazioni sul dispositivo che è stato sottoposto a sequestrato (fisico o logico):
  - Luogo, data e operatore che ha reperito e collezionato la fonte di prova;
  - Luogo, data e operatore che ha gestito e/o esaminato la fonte di prova;
  - Chi ha la responsabilità della custodia delle digital evidences.
  - Metodo di conservazione del reperto;
  - Eventuali trasferimenti di location dell'evidenza

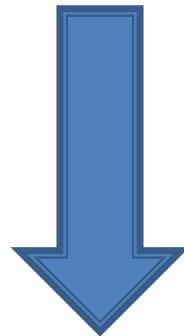
# La Raccolta: *il sequestro fisico*

non è sempre fattibile

- ▶ sistemi che non possono essere fermati/spenti;
- ▶ sistemi distribuiti su decine di rack;

# La Raccolta: *il sequestro logico*

- ▶ Duplicazione dei dati di [*possibile*] interesse investigativo;

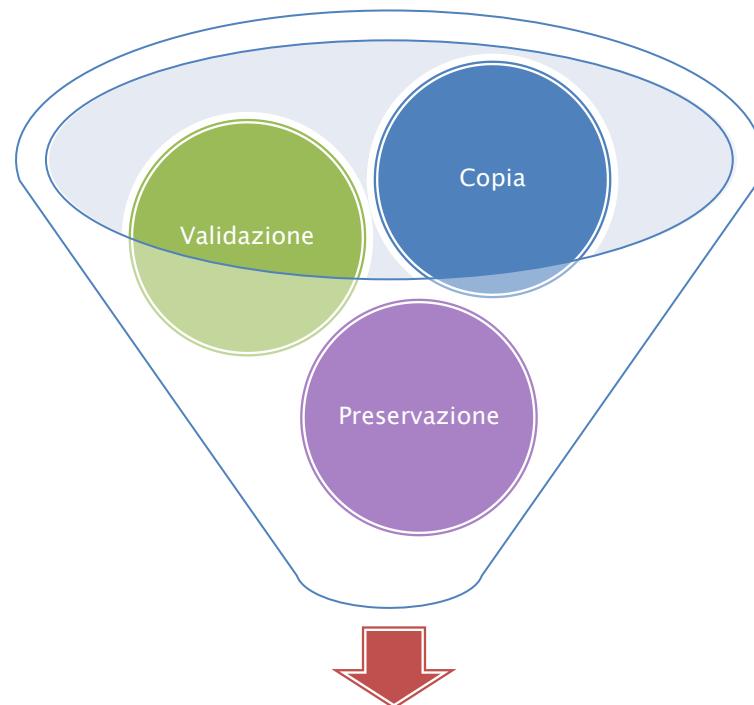


## COPIA FORENSE

# La Raccolta: *Copia Forense*

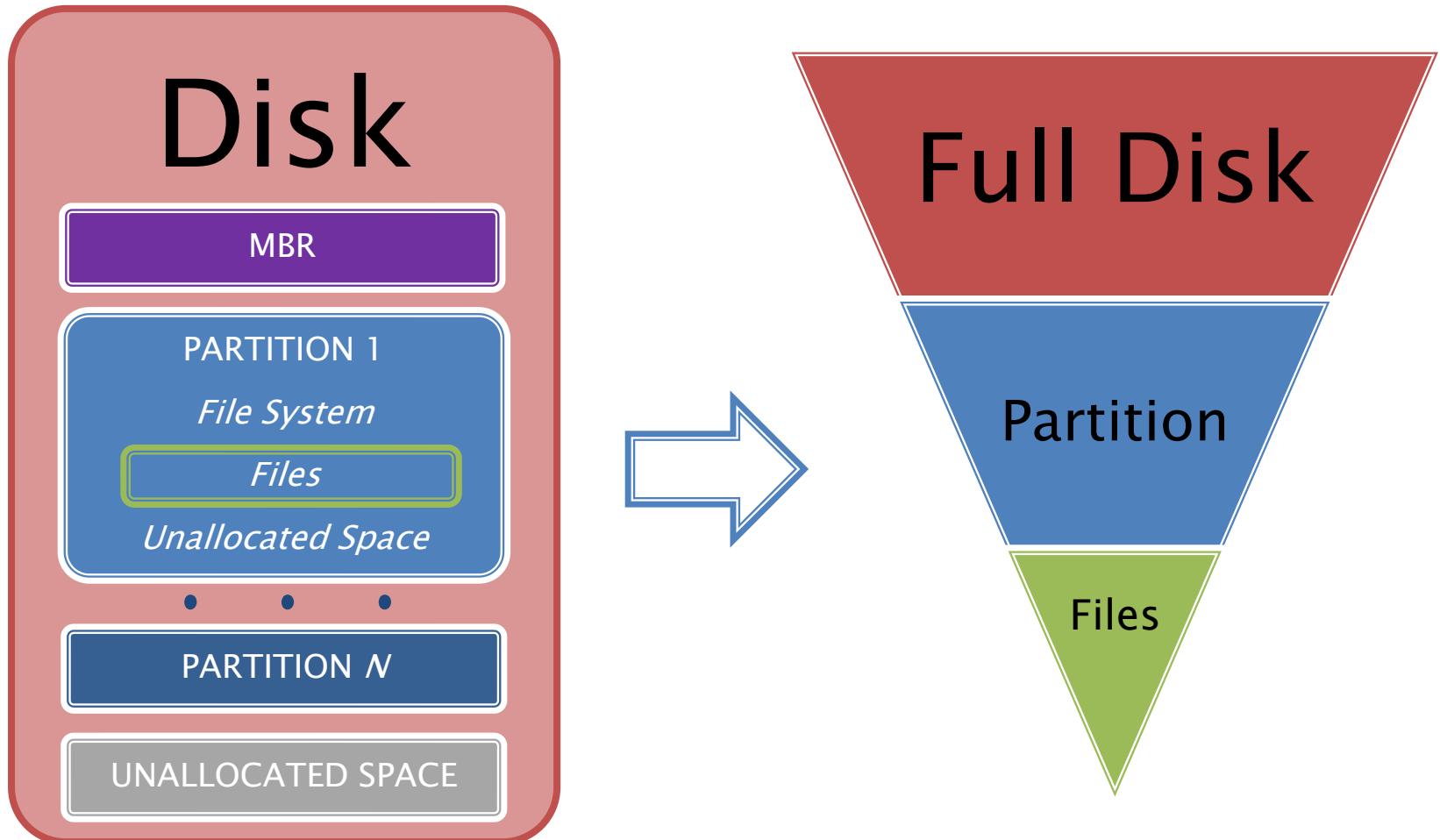
**GARANZIA DI RIPETIBILITA' DEI SUCCESSIVI  
ACCERTAMENTI CHE VERRANNO ESEGUITI  
SULLA COPIA FORENSE**

# La Raccolta: *Copia Forense*



**Copia Forense**

# La Raccolta: *Copia Forense*



# Copia Forense

## *Acquisizione Fisica*

- ▶ Copia «*bit a bit*» dell'intero supporto di memoria: dati e qualsiasi informazione sulla gestione dei dati (*tabella partizioni, Master Boot Record, meta dati del file system, etc.*):



Clonazione



File Immagine

# Copia Forense

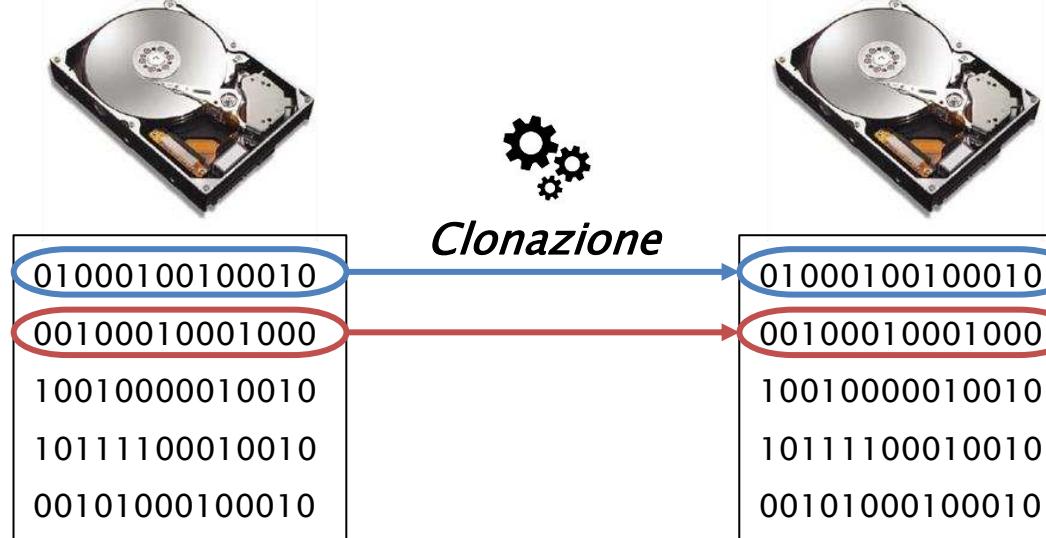
## *Acquisizione Fisica*

- ▶ La **Clonazione** ha come risultato un supporto pressoché identico a quello originale.
  - È facilmente alterabile
  - E' utilizzato solo in casi particolari: bisogna analizzare il supporto reinserendolo all'interno del proprio habitat;

Disco di Origine X



Disco di Destinazione Y

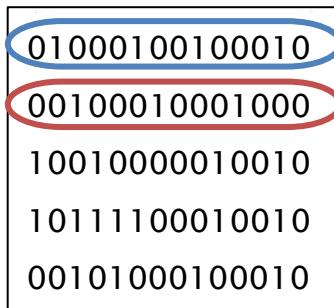


# Copia Forense

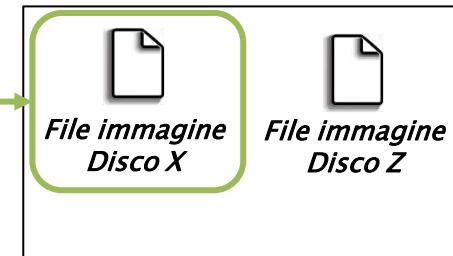
## Acquisizione Fisica

- ▶ La generazione di un **file immagine** (*bit stream image*) ha come risultato un file rappresentante il supporto originale.
  - è maneggevole;
  - può essere utilizzato per generare un disco clone;

Disco di Origine X



Disco di Destinazione Y



# Copia Forense

## *gli strumenti*

Hardware



Software

deft

VS



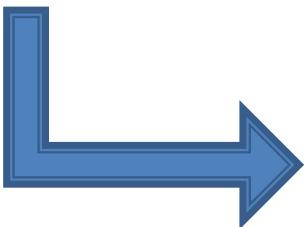
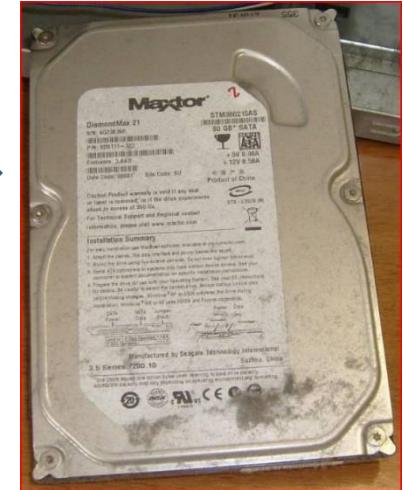
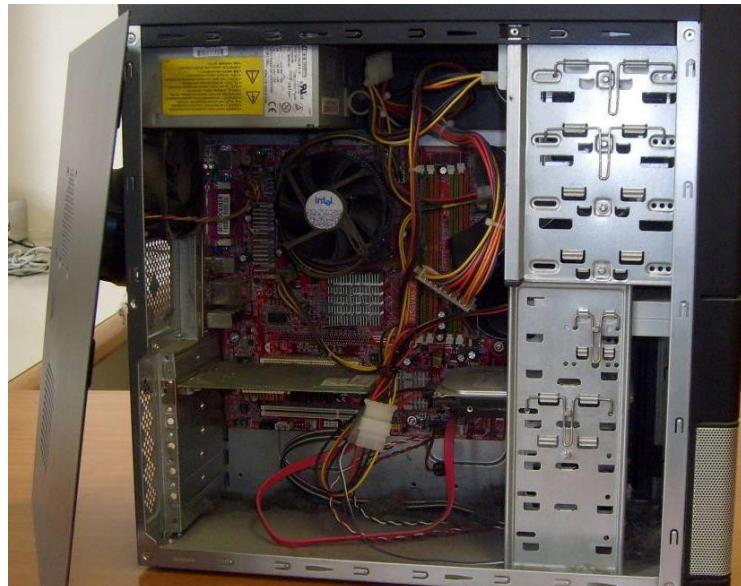
# Copia Forense

## *gli strumenti*

- ▶ **Hardware:** duplicatori forensi
  - Certificati
  - Prestanti
  - Costosi
  
- ▶ **Software:** distro linux live forensi
  - Gratuiti
  - OpenSource
  - Versatili

# Copia Forense

## *gli strumenti*



# Copia Forense

## *gli strumenti*



# Copia Forense

## Copia Forense del «Disco Origine»

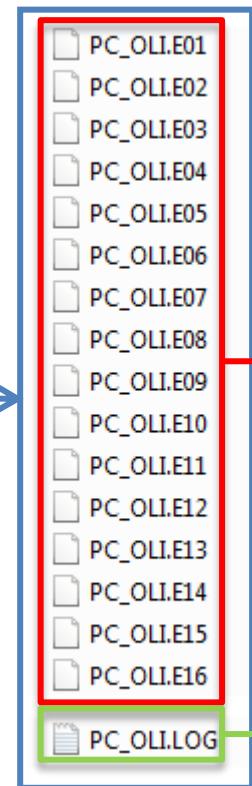


Immagine (*formato E01*)  
diviso in 16 file del  
«Disco Origine»

File LOG della realizzazione  
della copia forense



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 7: Fasi del trattamento *validazione e preservazione*



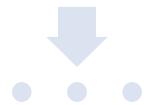
A.A. 2021/22

Dott. Lorenzo LAURATO

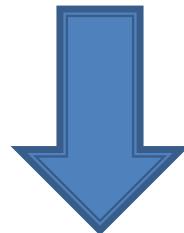


# Nella puntata precedente...

Identificazione



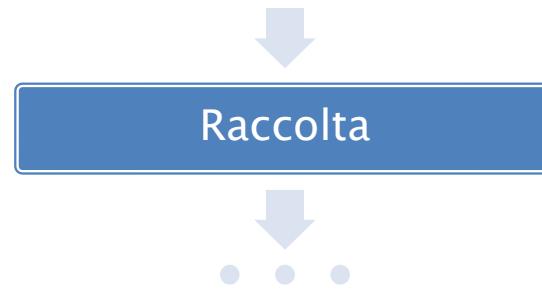
Ricercare la fonte di prova, individuare dove il dato di possibile interesse è conservato.



Preview

*(Perquisizione informatica)*

# Nella puntata precedente...

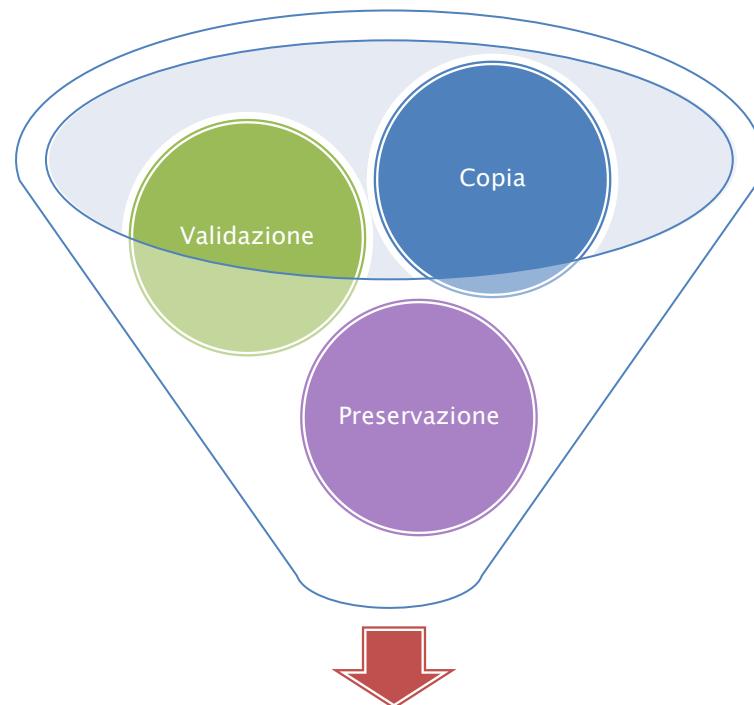


Raccogliere i dati di possibile interesse investigativo unitamente ai dati che permettono la ricostruzione dell'evento probatorio.



Copia Forense

# La Raccolta: *Copia Forense*



**Copia Forense**

# Legge n. 48 del 18/03/2008

## *art. 354 c.p.p.*

*(Accertamenti urgenti sui luoghi, sulle cose e sulle persone.  
Sequestro)*

2. [...] In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. [...]

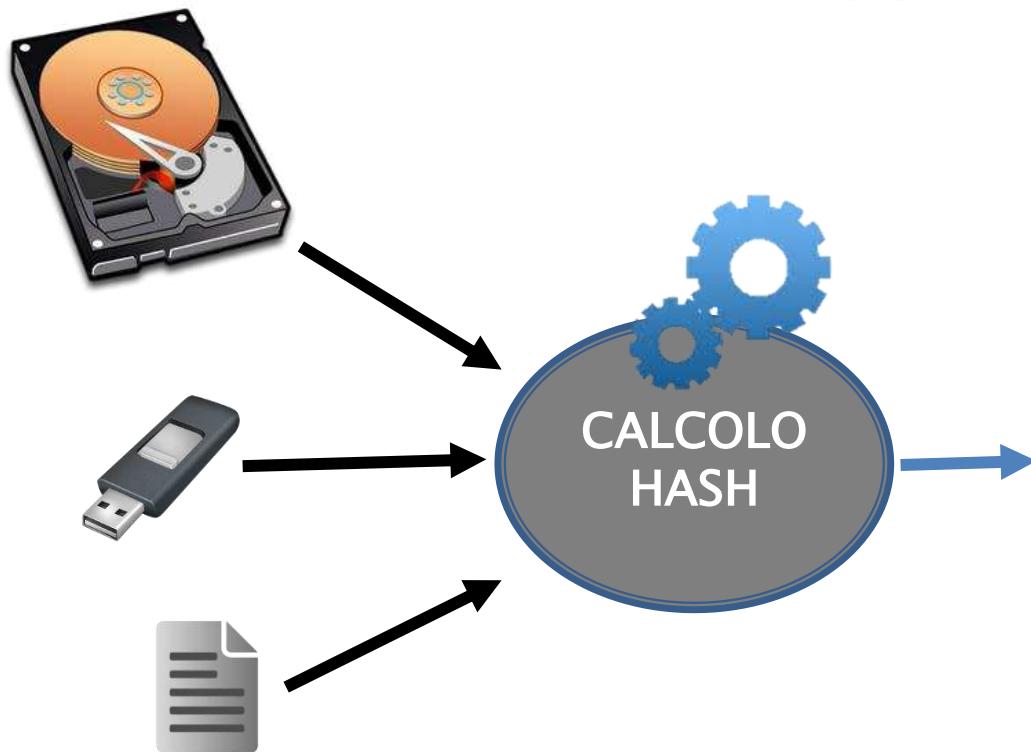
# Copia Forense

## *Hash*

- ▶ L'algoritmo restituisce una stringa a lunghezza fissa di esadecimali a partire da un flusso di bit (dati) di dimensione qualsiasi.
- ▶ La stringa prodotta in output è univoca per ogni file e ne è un identificatore.
- ▶ L'algoritmo non è invertibile, ossia non è possibile ricostruire il dato originale a partire dalla stringa che viene restituita in output.

# Copia Forense

## *Hash*



HASH 1:  
12ADHG56CEEE3984  
66PIZXXXK334F6GC3

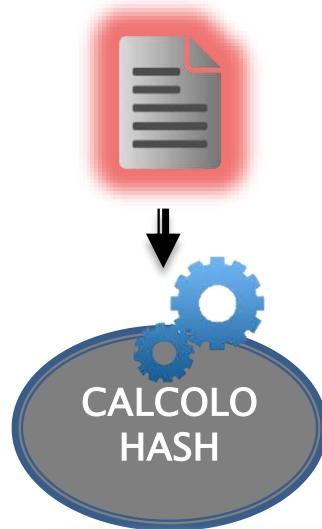
HASH 2:  
HHBN78FV54090934  
346HHFC53JHCORUY

HASH 3:  
2739BD268BA0E1D6  
5255E5276DD8C66E

# Copia Forense

## Hash

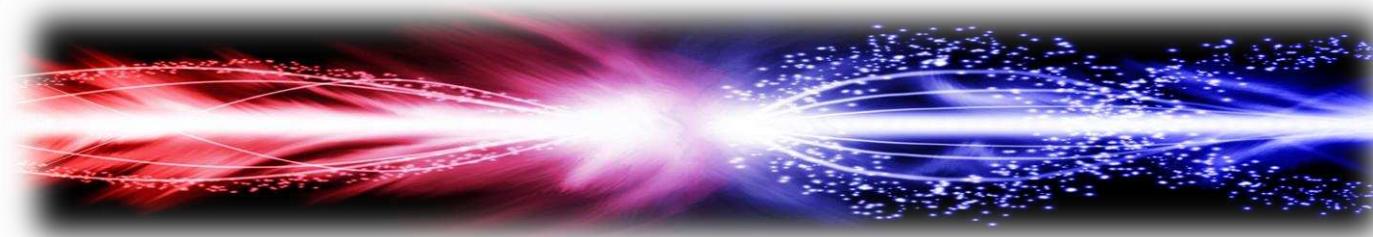
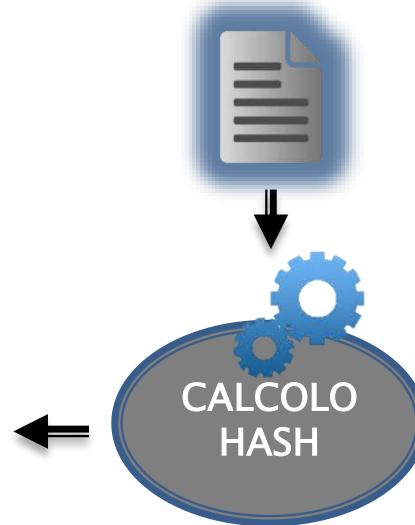
File 01



2739BD268BA0E1D6  
5255E5276DD8C66E



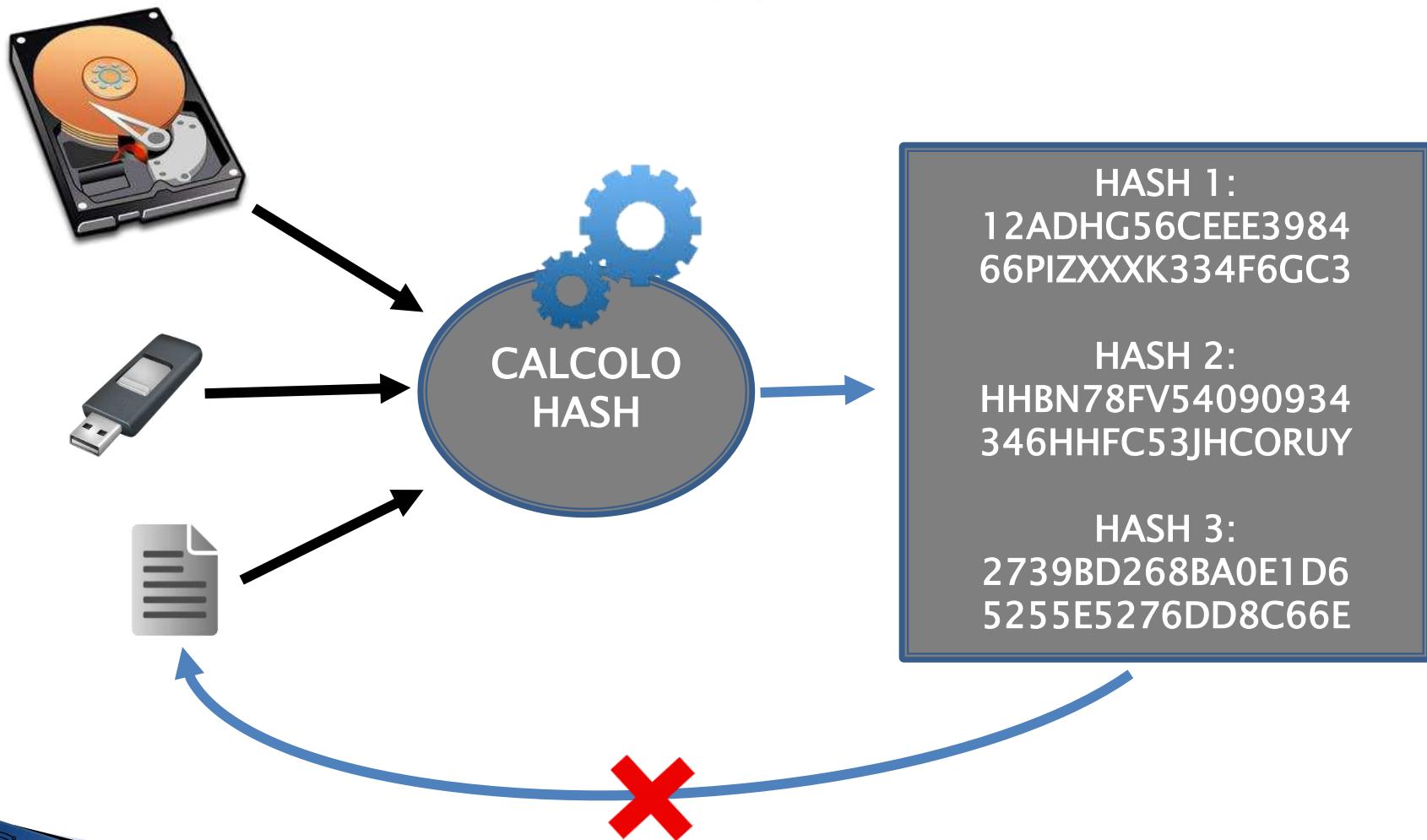
File 02



## COLLISIONE

# Copia Forense

## Hash



# Copia Forense

## Hash

File 01

CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5

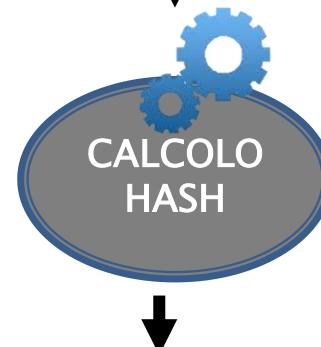


File 02

CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5  
CALCOLO MD5 CALCOLO MD5.



2739BD268BA0E1D6  
5255E5276DD8C66E



872207A67BB4EBB7  
2590F11BD68B131C

# Fasi

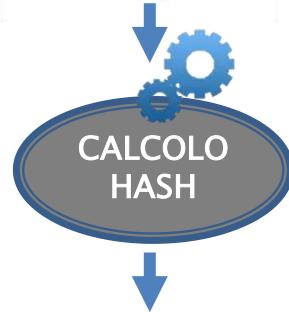


# Copia Forense

## *hash*

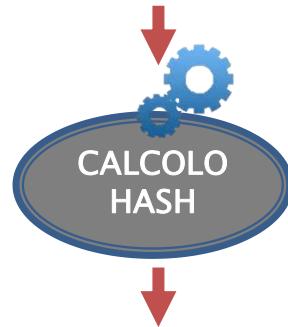
- ▶ **Validazione:** garantisce che la copia eseguita è identica al dato originale.

Disco di Origine X



555F1D268BBE1D6  
5255E1176DD8C66E

Disco di Destinazione Y



555F1D268BBE1D6  
5255E1176DD8C66E

# Copia Forense

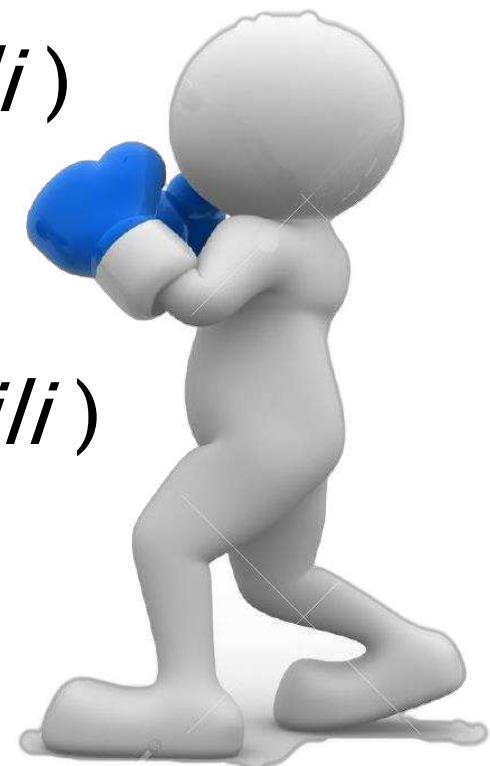
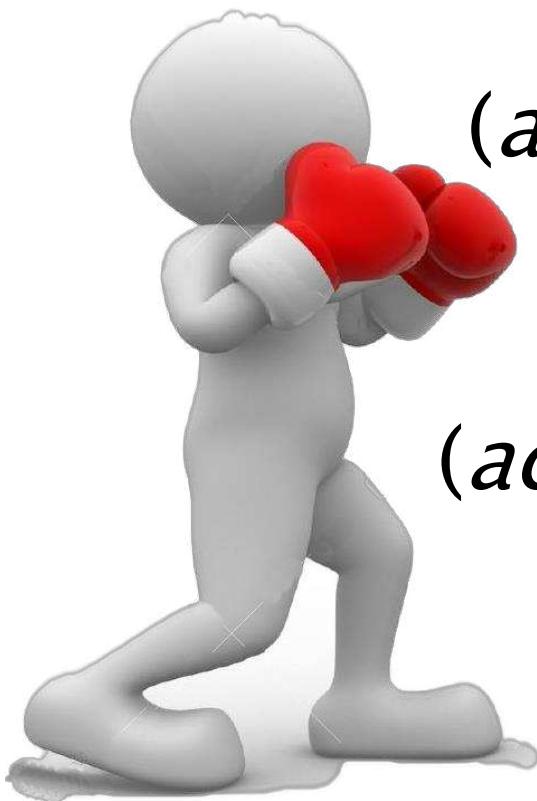
Art. 359 c.p.p

*(accertamenti ripetibili)*

**VS**

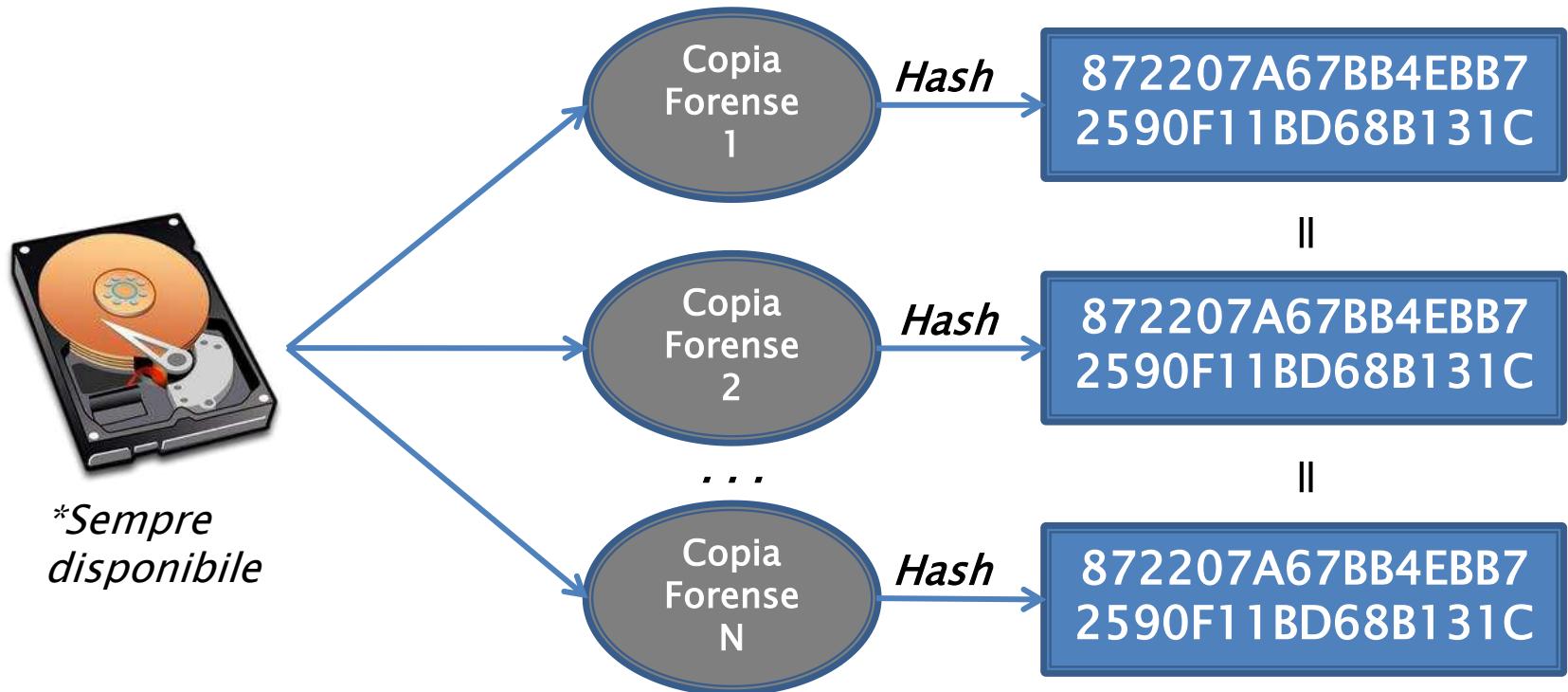
Art. 360 c.p.p.

*(accertamenti irripetibili)*



# Copia Forense

## Art. 359 c.p.p (accertamenti ripetibili)



Memorie di massa in buono stato

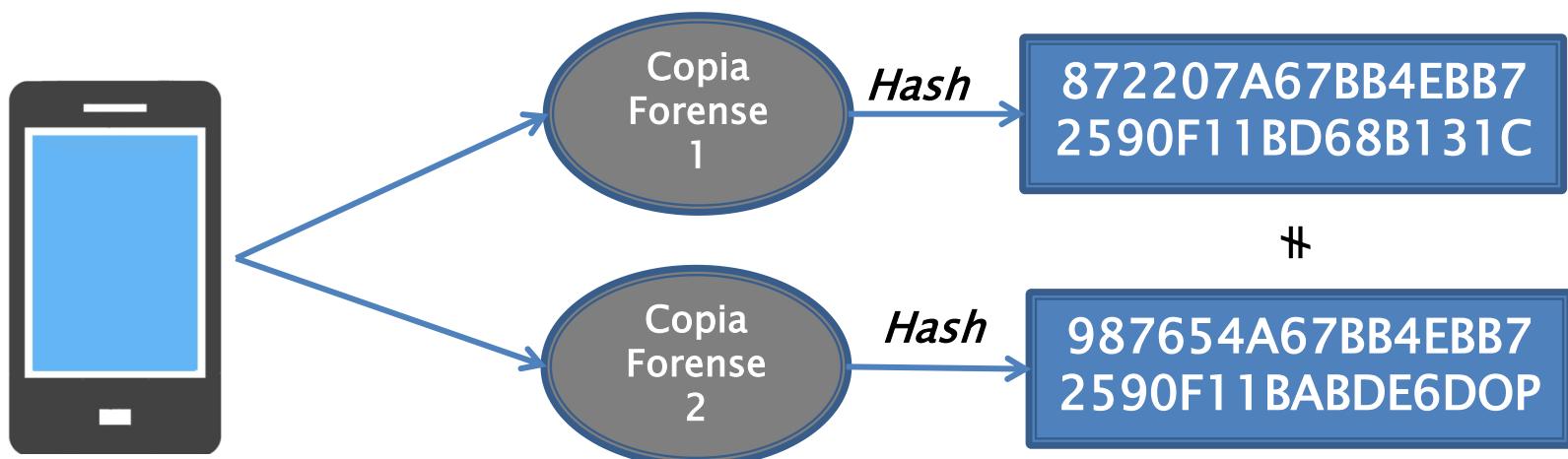
# Copia Forense

## Art. 360 c.p.p (*accertamenti irripetibili*)

- ▶ Memorie di massa non in buono stato;
- ▶ Live Acquisition: il sistema operativo del dispositivo deve essere avviato per poter realizzare la copia forense (*Es.: dispositivi cellulare, server, etc.*);
- ▶ Cloud (Acquisizione remota);
- ▶ Dispositivo di origine non disponibile nel tempo (*Es.: dissequestro, restituzione, etc.*);

# Copia Forense

## Art. 360 c.p.p (accertamenti irripetibili )



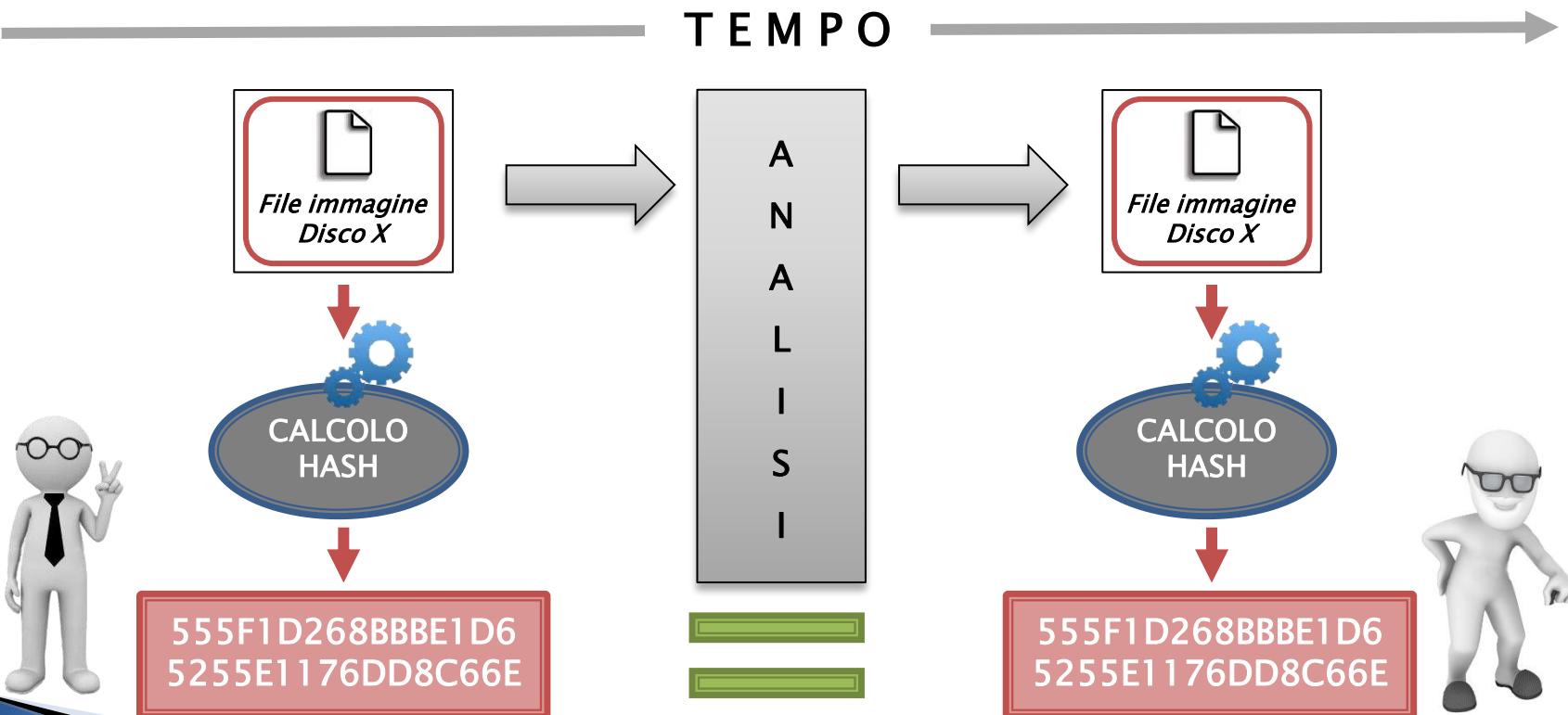
# Fasi



# Copia Forense

## *hash*

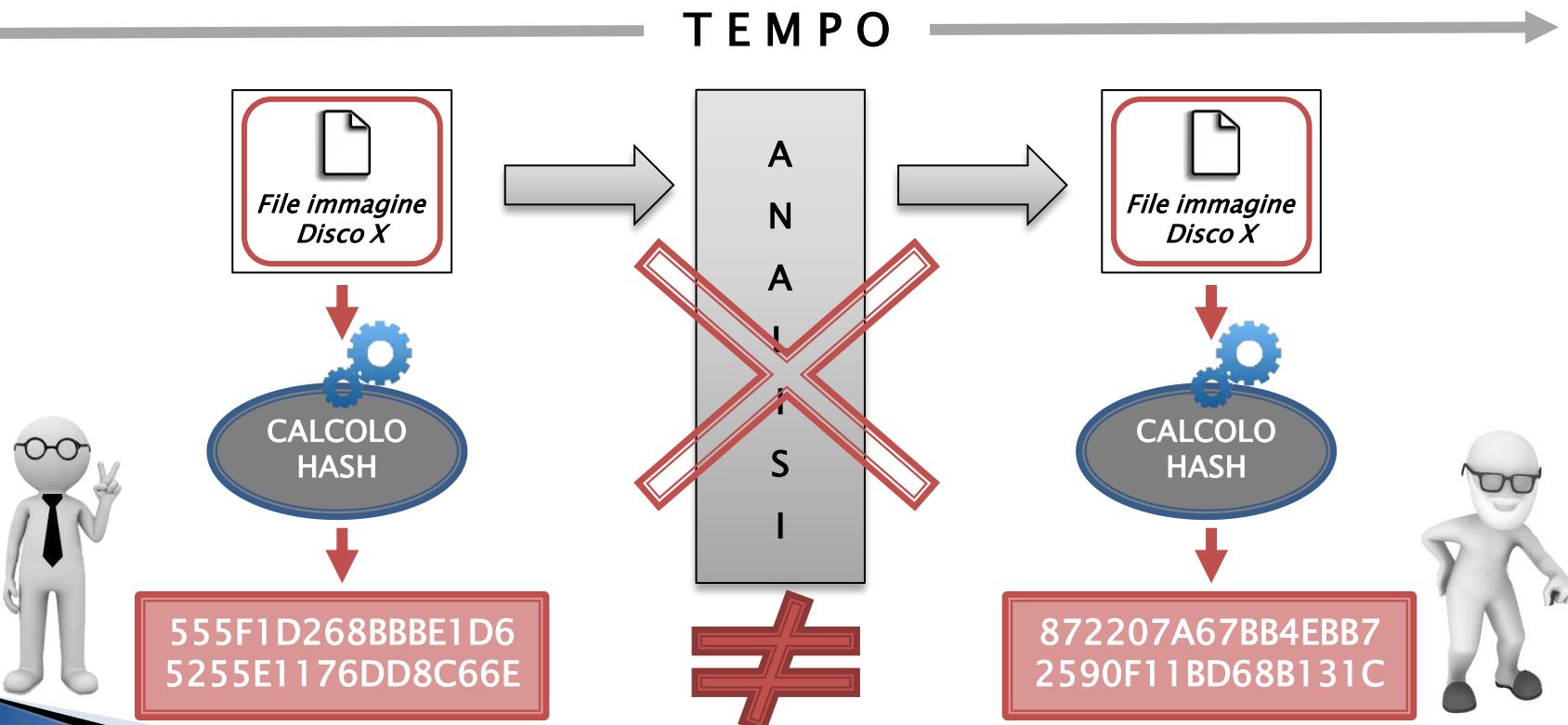
- ▶ Preservazione: garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



# Copia Forense

## *hash*

- ▶ **Preservazione:** garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



# Copia Forense

## Copia Forense del «Disco Origine»

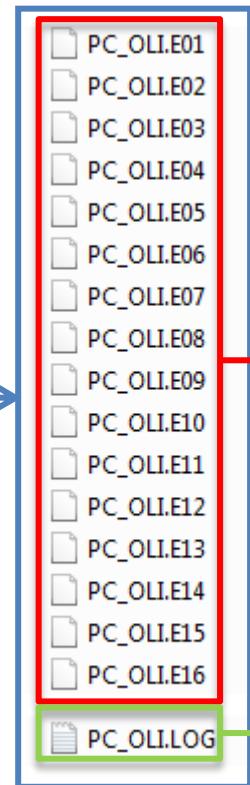


Immagine (*formato E01*)  
diviso in 16 file del  
«Disco Origine»

File LOG della realizzazione  
della copia forense

# Copia Forense

## *File LOG*

- ▶ File descrittivo in cui sono presenti le informazioni sulla copia forense realizzata:
  - Informazioni sullo strumento impiegato: *nome, versione, etc.*
  - Informazioni del disco di origine: *modello, capacità, S/N, etc.*
  - Informazioni dell'immagine forense: *nr. di file, dimensioni, etc.*
  - Altre informazioni: *data e ora, nr. di settori saltati, etc.*
- **HASH:** *MD5, SHA1, SH256, SHA512, etc.*

# Copia Forense

## File LOG

Nome e Versione  
dello strumento

Informazioni del  
«disco sorgente»

```
*** Forensic Dossier -- Serial No.:78265 --
Software: V3.3.3RC16 Firmware: V1.14.2 fs:NTFS
*
* Acquired by _____ Location _____
*
* Acquired on _____ AT _____
***** SESSION SETTINGS *****
* Operating Mode: 4G E01:S2=>D2 Address Mode: LBA
* Verify : Hash-Dsk+V Speed : UDMA-5
* Connection : Direct
*
*
E01 CAPTURE OF S2 HAS BEEN ACHIEVED.
*****
***** SOURCE DRIVE(S) ***** DESTINATION DRIVE(S) *****
*           S1          D1
* Model : ST380815AS Model : ST2000DM008-2FR102
* Serial: 5RW2FPXX Serial: WFL1C8EV
*
* C: 155009 H: 16 S: 63
* Total Sectors Drive Size
* 156250000 74.0GB
* C: 3876021H: 16 S: 63
* Total Sectors Drive Size
* 3907029168 1863.0GB
*****
*** PC_OLI.E01: S1: 0 To:8667135
* start MD5: 67452301 EFCDAB89 98BADCFE 10325476
* end MD5: A18B0EE6 C7E71924 EEA6B83F 88ADDF742
* Verified : A18B0EE6 C7E71924 EEA6B83F 88ADDF742
*** PC_OLI.E02: S1: 8667136 To:18759679
* start MD5: A18B0EE6 C7E71924 EEA6B83F 88ADDF742
* end MD5: DEB75F20 10AA171F 9B05B385 AF4EEC01
* Verified : DEB75F20 10AA171F 9B05B385 AF4EEC01
*** PC_OLI.E03: S1: 18759680 To:27312127
* start MD5: DEB75F20 10AA171F 9B05B385 AF4EEC01
* end MD5: 46FA2898 B2528064 2BB26D4D B9E6F5EF
* Verified : 46FA2898 B2528064 2BB26D4D B9E6F5EF
```

# Copia Forense

## *File LOG*

Hash MD5

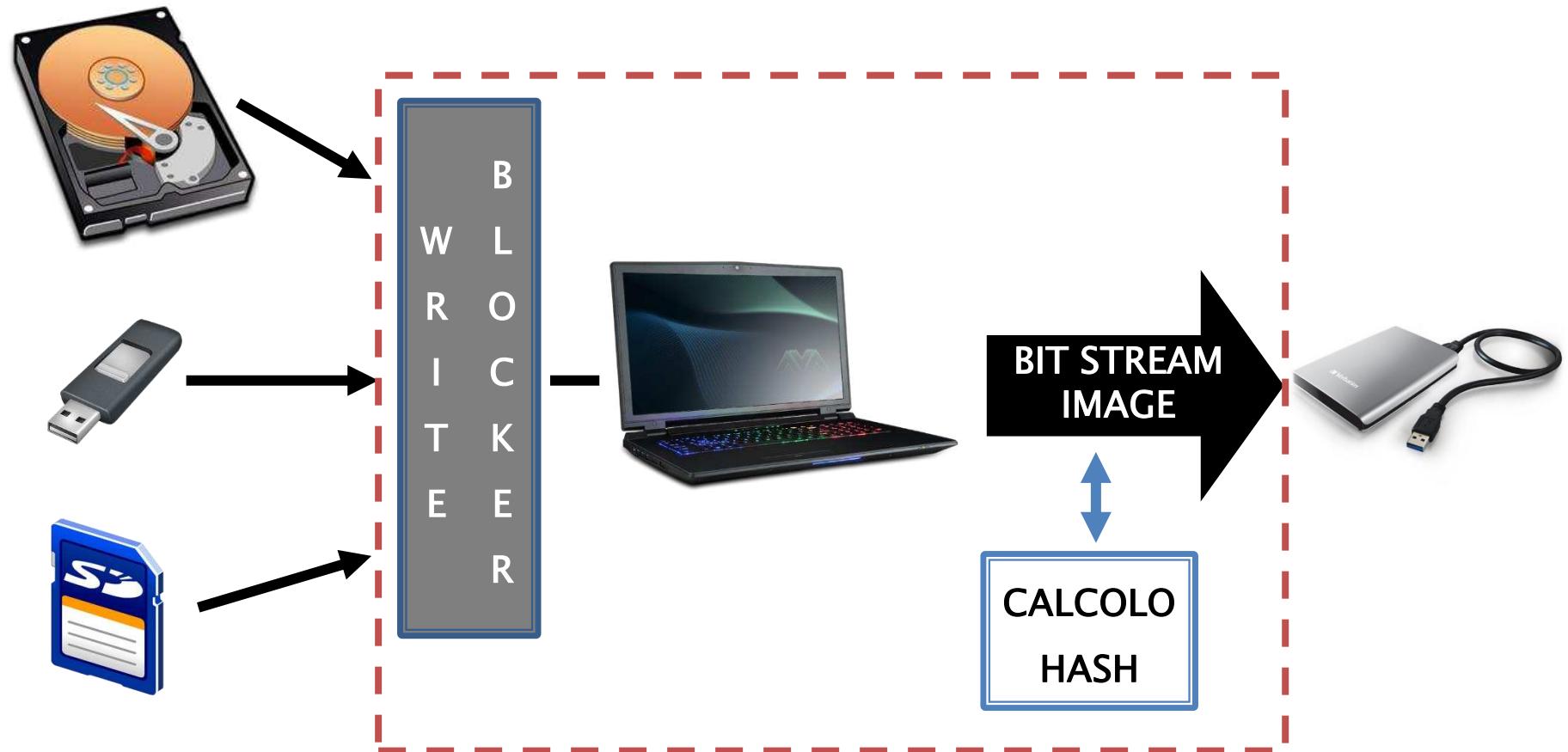
```
*** PC_OLI.E16: S1: 128294912 To:156249999
* start MD5: B8D79829 OFA6CCE3 296C8D89 729B04F2
* end MD5: 5618D5BD 398160A8 2376C70F 3B3D744E
* Verified : 5618D5BD 398160A8 2376C70F 3B3D744E
*** S1 From: 0, To: 156249999, size: 156250000
* Source MD5:
* ...EF184313 9669170C 593356DD A8849F1B...
* Verified :
* ...EF184313 9669170C 593356DD A8849F1B...
```

Altre Informazioni

```
*
*      Skipped Sectors: 0     Recovered Sectors: 0
*
*****
Compression Ratio is : 4.47 : 1
Completion Time: 08/08/2008 08:08:00
Audit Trail Checksum: 077C3058 5E1293AB DD8BB848 43EE6E86
```

# Copia Forense

## *riepilogando...*



# Copia Forense

» Comandi



# Copia Forense

## comando «*DD*»

- ▶ È presente nella gran parte di tutte le distribuzioni UNIX Like

```
DD(1)                                         User Commands

NAME
      dd - convert and copy a file

SYNOPSIS
      dd [OPERAND]...
      dd OPTION
```

# Copia Forense

## comando «*DD*»

*/dev*

tutti i file al suo interno rappresentano dispositivi:

- **Character device:** dispositivi che trasmettono/trasferiscono dati
  - *dsp[0]: dispositivo audio*
  - *lp[0]: porta parallela*
- **Block device:** dispositivi che memorizzano/conservano dati
  - *hd[a]: hard disk ide*
  - *sd[a]: hard disk scsi, memory stick, memory card, etc.*

# Copia Forense

## comando «*DD*»

- ▶ Lista dei dispositivi agganciati:

```
root@caine:/# fdisk -l
```

```
Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x72a3c36c
```

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1		2048	2099199	2097152	1G	b	W95 FAT32
/dev/sda2		2099200	8388607	6289408	3G	b	W95 FAT32

Disco target

```
Disk /dev/sdb: 20 GiB, 21474836480 bytes, 41943040 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

# Copia Forense

## comando «*DD*»

- ▶ Lista dei dispositivi agganciati:

```
Disk /dev/sdc: 8 GiB, 8589934592 bytes, 16777216 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x9a847d68
```

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sdc1		2048	16777215	16775168	8G	7	HPFS/NTFS/exFAT

Disco di destinazione

# Copia Forense

## comando «*DD*»

- ▶ Prepariamo il nostro disco di destinazione della copia forense:

```
root@caine:/# mkdir /mnt/dest
root@caine:/# mount /dev/sdc1 /mnt/dest/
root@caine:/# mkdir /mnt/dest/dd_image
```

# Copia Forense

## comando «*DD*»

### ▶ Eseguiamo la copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

IF = input file [*disco sorgente «sda»*]

OF = output file [*file immagine «sda.dd»*]

BS = block size in byte (default 512) [*dimensione del blocco di lettura «2048 byte»*]

CONV = esegue l'elaborazione in base ai parametri indicati

noerror = continua ad elaborare in caso di errore di lettura

sync = sostituisce i blocchi di memoria non letti nella destinazione con NULs (mantiene sincronizzata la dimensione della destinazione con quella della sorgente)

# Copia Forense

## comando «*DD*»

### ▶ Risultato della copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
2097152+0 records in
2097152+0 records out
4294967296 bytes (4,3 GB, 4,0 GiB) copied, 302,094 s, 14,2 MB/s
```

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194304
-rwxrwxrwx 1 root root 4294967296 apr  7 23:26 sda.dd
```

# Copia Forense comando «*DD*»

## ► Comandi avanzati:

**SKIP = *[n]*** salta la lettura del numero «*n*» di blocchi di memoria, partendo dall'inizio

**COUNT= *[n]*** indica all'elaborazione di terminare dopo aver letto il numero «*n*» di blocchi di memoria

# Copia Forense

## comando «*DD*»

### ► Acquisire una sola partizione

```
Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device      Boot   Start     End  Sectors  Size Id Type
/dev/sda1        2048 2099199 2097152    1G  b W95 FAT32
/dev/sda2    2099200 8388607 6289408    3G  b W95 FAT32
```

```
root@caine:/# dd if=/dev/sda2 of=/mnt/dest/dd_image/sda_p2.dd bs=2048
572352+0 records in
1572352+0 records out
3220176896 bytes (3,2 GB, 3,0 GiB) copied, 238,845 s, 13,5 MB/s
```

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 3144704
-rwxrwxrwx 1 root root 3220176896 apr  7 23:36 sda_p2.dd
```

# Copia Forense comando «*DD*»

- ▶ Acquisire una sola partizione

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda_p2.dd skip=2099199 count=6289408
6289408+0 records in
6289408+0 records out
3220176896 bytes (3,2 GB, 3,0 GiB) copied, 764,928 s, 4,2 MB/s
```

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 3144704
-rwxrwxrwx 1 root root 3220176896 apr  7 23:55 sda_p2.dd
```

# Copia Forense

## comando «*DD*»

### ► Dividere il file immagine:

Blocchi da 1GB (1024 Byte x 1.000.000)

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.000 bs=1024 count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 200,268 s, 5,1 MB/s
```

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.001 bs=1024 skip=1000000
count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 226,651 s, 4,5 MB/s
```

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.002 bs=1024 skip=2000000
count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 213,783 s, 4,8 MB/s
```

# Copia Forense

## comando «*DD*»

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.003 bs=1024 skip=3000000  
count=1000000  
1000000+0 records in  
1000000+0 records out  
1024000000 bytes (1,0 GB, 977 MiB) copied, 220,863 s, 4,6 MB/s  
  
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.004 bs=1024 skip=4000000  
194304+0 records in  
194304+0 records out  
198967296 bytes (194,3 MB, 185 MiB) copied, 220,863 s, 3,7 MB/s  
  
root@caine:/# ls -l /mnt/dest/dd_image/  
total 4194304  
-rwxrwxrwx 1 root root 1024000000 apr 8 00:03 sda.000  
-rwxrwxrwx 1 root root 1024000000 apr 8 00:04 sda.001  
-rwxrwxrwx 1 root root 1024000000 apr 8 00:04 sda.002  
-rwxrwxrwx 1 root root 1024000000 apr 8 00:05 sda.003  
-rwxrwxrwx 1 root root 1024000000 apr 8 00:06 sda.004
```

# Copia Forense

## comando «*DD*»

### ▶ Dividere il file immagine:

```
root@caine:/# dd if=/dev/sda bs=2048 | split -d -b 2G - mnt/dest/dd_image/sda.
```

#### ▶ SPLIT

- **-D** = indica di appendere al nome del file un contatore decimale [*sda.00*]
- **-B** = [*n/n(K/M/G/T/P/E/Z/Y)*] specifica la dimensione massima di ciascuna parte [*2GB*]

```
2097152+0 records in
2097152+0 records out
4294967296 bytes (4,3 GB, 4,0 GiB) copied, 157,836 s, 27,2 MB/s
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194304
-rwxrwxrwx 1 root root 2147483648 apr  8 00:12 sda.00
-rwxrwxrwx 1 root root 2147483648 apr  8 00:13 sda.01
```

# Copia Forense comando «DD»

## Calcolare l'Hash

### ▶ Metodo nr. 1:

- Calcoliamo l'hash del dispositivo sorgente «**sda**» e lo memorizziamo in un file «**sda\_orig.hash**»

```
root@caine:/# md5sum /dev/sda > /mnt/dest/dd_image/sda_orig.hash
root@caine:/# cat /mnt/dest/dd_image/sda_orig.hash
d7a09df1018710f2b40744ba62445c7b  /dev/sda
```

- Calcoliamo l'hash dell'immagine «**sda.dd**» ottenuta in precedenza ed anche esso lo memorizziamo all'interno di un file «**sda\_dd.hash**»

```
root@caine:/# md5sum /mnt/dest/dd_image/sda.dd > /mnt/dest/dd_image/sda_dd.hash
root@caine:/# cat /mnt/dest/dd_image/sda_dd.hash
d7a09df1018710f2b40744ba62445c7b  /mnt/dest/dd_image/sda.dd
```

# Copia Forense comando «DD»

## Calcolare l'Hash

- Oppure se la nostra immagine è divisa in più file, dovremo adoperare CAT:

```
root@caine:/# cat /mnt/dest/dd_image/sda.* | md5sum >> /mnt/dest/dd_image/sda_merge.hash
root@caine:/# cat /mnt/dest/dd_image/sda_merge.hash
d7a09df1018710f2b40744ba62445c7b -
```

Hash dispositivo di origine = Hash file immagine  
(to match)

# Copia Forense comando «DD»

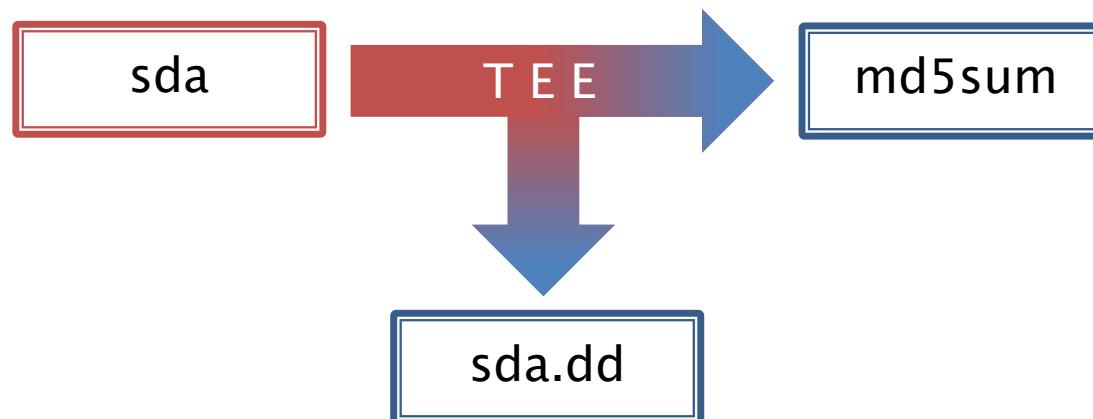
## Calcolare l'Hash

### ▶ Metodo nr. 2:

- Calcoliamo l'hash durante l'elaborazione della copia

```
root@caine:/# dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |  
md5sum > /mnt/dest/dd_image/ sda.hash
```

TEE = biforca\duplica lo stream [una viene utilizzata per generare il file immagine, l'altra viene trasmesso al comando successivo «md5sum»]



# Copia Forense comando «DD»

## Calcolare l'Hash

```
root@caine:/# dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |  
md5sum > /mnt/dest/dd_image/ sda.hash
```

```
root@caine:/# ls -l /mnt/dest/dd_image/  
total 4194305  
-rwxrwxrwx 1 root root 4294967296 apr 8 00:56 sda.dd  
-rwxrwxrwx 1 root root 36 apr 8 00:56 sda.hash
```

```
root@caine:/# cat /mnt/dest/dd_image/sda.hash  
d7a09df1018710f2b40744ba62445c7b -
```

# Copia Forense comando «DC3DD»

## ▶ Patch del comando DD

```
root@caine:/# dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5  
hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on
```

OFS = output diviso in più file [*file immagine «sda.000»*]

OFSZ = dimensione massima di ogni file [2 GB]

BUFSZ = BS = block size in byte (default 512) [*dimensione del blocco di lettura «2048 byte»*]

HASH = [MD5|SHA1|SHA256|SHA512] calcola dell'Hash indicato [*MD5 e SHA256*]

LOG = salva il report dell'elaborazione in un file [*sda.log*]

VERB=ON indica di generare un report dettagliato (verbose)

# Copia Forense comando «DC3DD»

```
root@caine:/# dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5
hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on

dc3dd 7.2.646 started at 2020-04-08 01:07:42 +0200
compiled options:command line: dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G
bufsz=2k hash=md5 hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on
device size: 8388608 sectors (probed), 4,294,967,296 bytes
sector size: 512 bytes (probed)
4294967296 bytes ( 4 G ) copied ( 100% ), 959 s, 4,3 M/s

input results for device `/dev/sda':
8388608 sectors in
0 bad sectors replaced by zeros
d7a09df1018710f2b40744ba62445c7b (md5)
f4d40a9fc0979b1dce6c9f45cf3fedc1f9d6fea23725511356d8fb1b99b7ef3a (sha256)

output results for files `/mnt/dest/dd_image/sda.000':
8388608 sectors out
4194304 sectors out to `/mnt/dest/dd_image/sda.000'
4194304 sectors out to `/mnt/dest/dd_image/sda.001'
dc3dd completed at 2020-04-08 01:23:41 +0200
```

# Copia Forense comando «*DC3DD*»

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194308
-rwxrwxrwx 1 root root 2147483648 apr  8 01:16 sda.000
-rwxrwxrwx 1 root root 2147483648 apr  8 01:23 sda.001
-rwxrwxrwx 1 root root       823 apr  8 01:23 sda.log
```

# Copia Forense comando «*DC3DD*»

## ► Comandi avanzati:

REC=OFF interrompe l'elaborazione in caso di un errore di lettura di un blocco di memoria

HOFS= l'output viene diviso in più file e per ciascuno di essi viene calcolato l'hash;



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 8: Raccolta e Validazione *Disk Image e Tool*

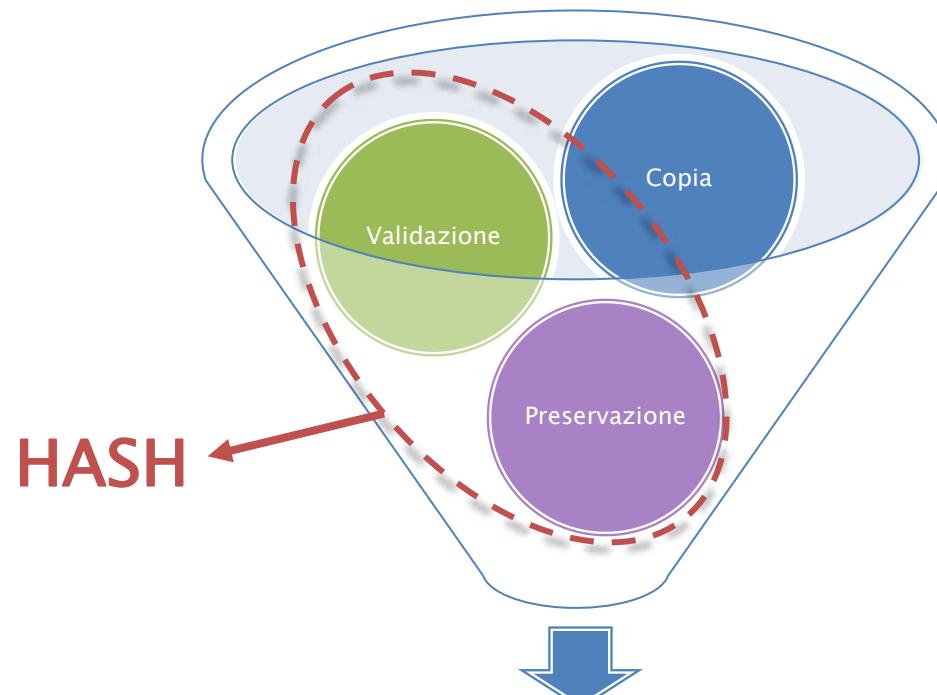


A.A. 2021/22

Dott. Lorenzo LAURATO



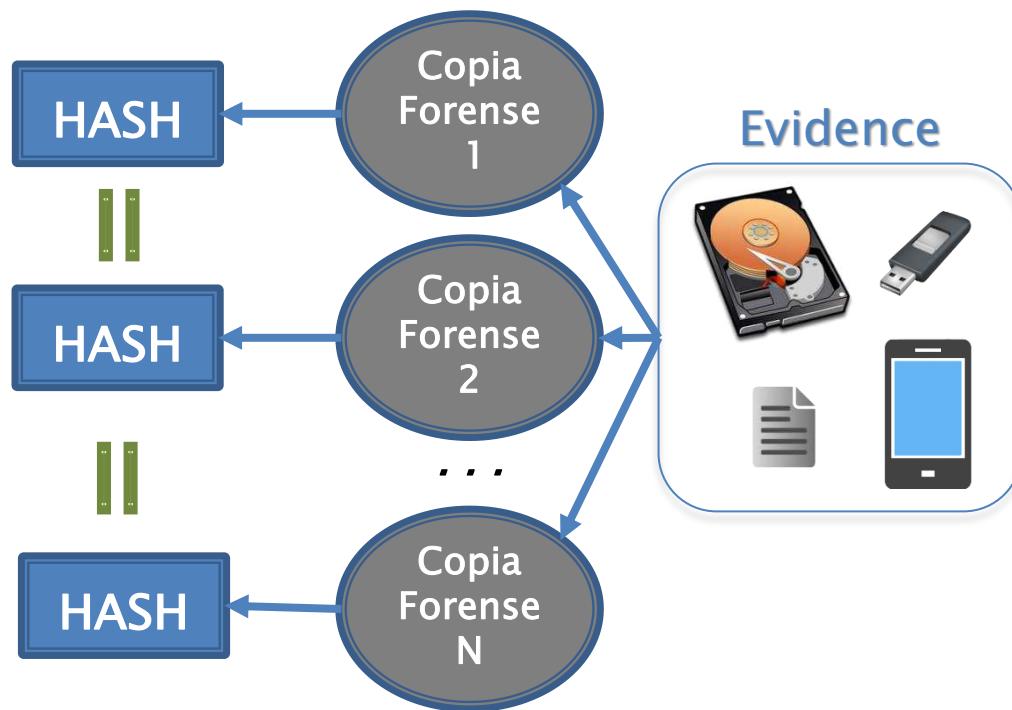
# Nella puntata precedente...



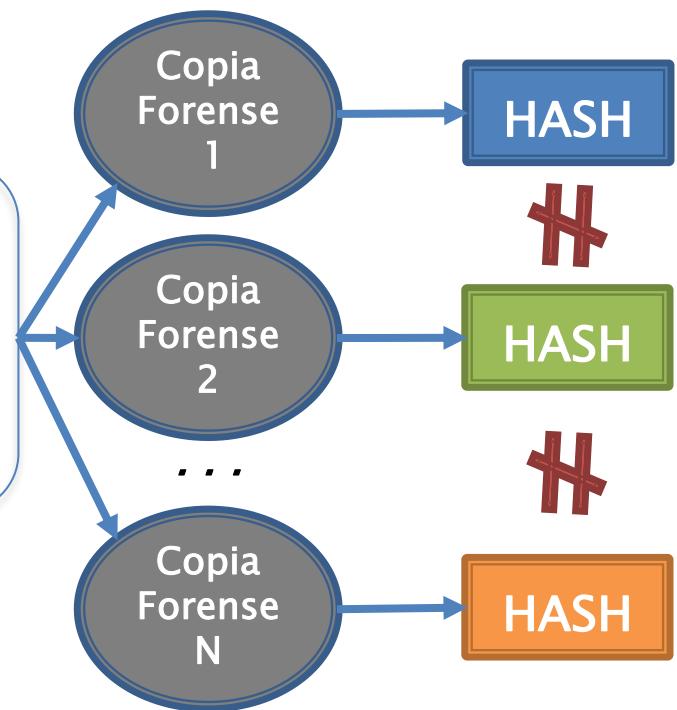
Copia Forense

# Nella puntata precedente...

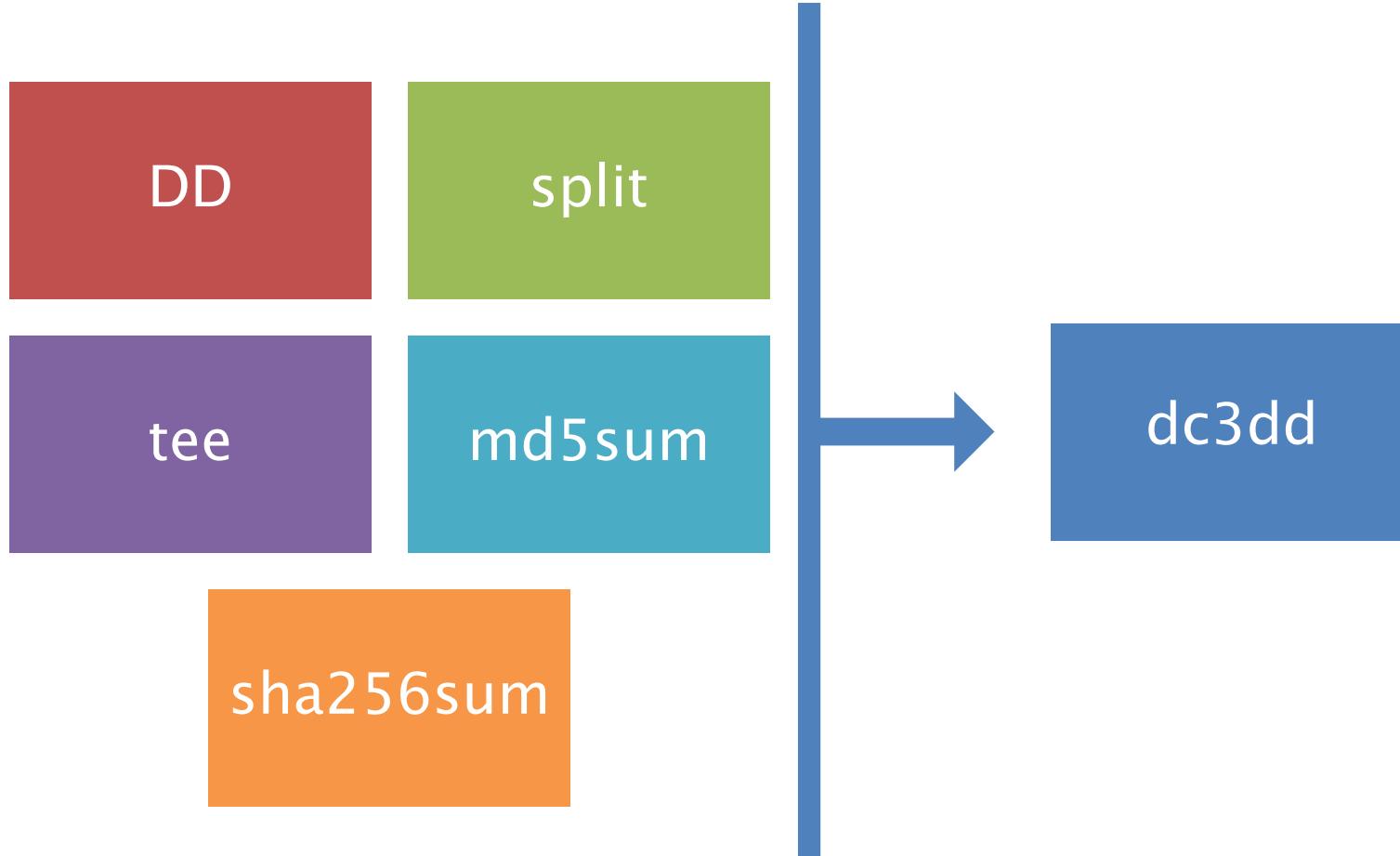
Art. 359 c.p.p  
*(accertamenti ripetibili)*



Art. 360 c.p.p  
*(accertamenti irripetibili)*

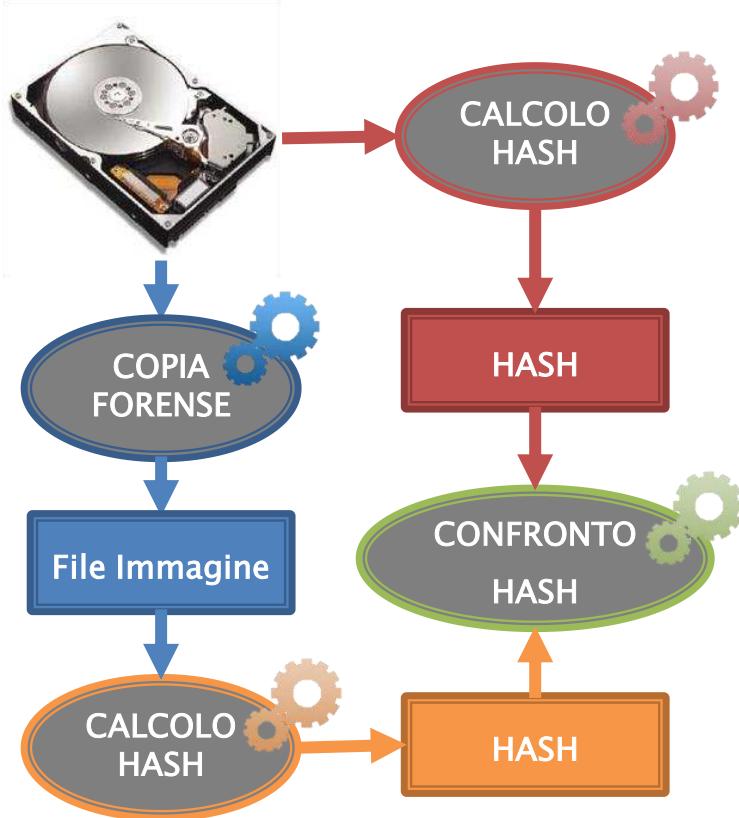


# Nella puntata precedente...

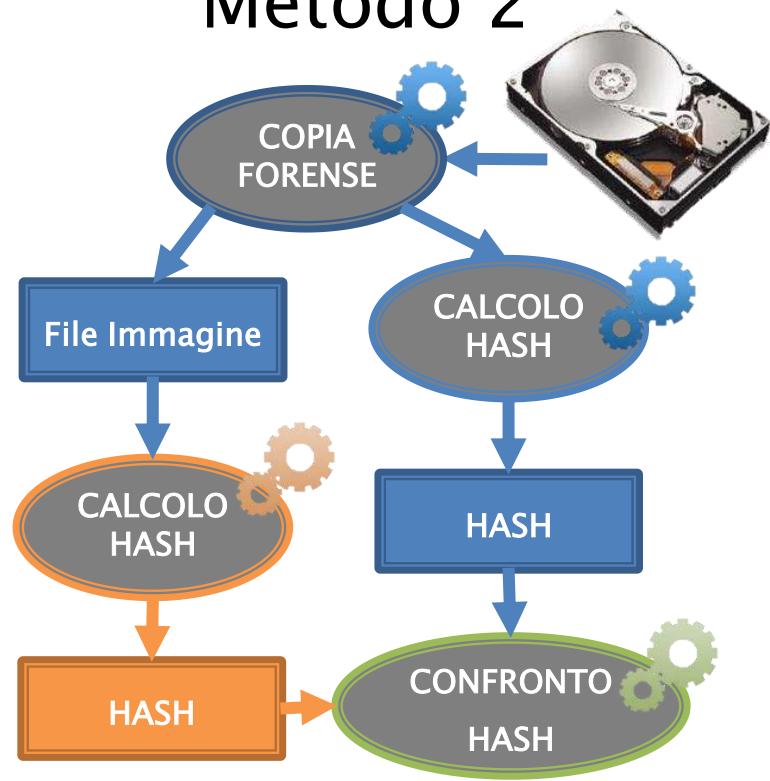


# Calcolo dell'hash: validazione

Metodo 1



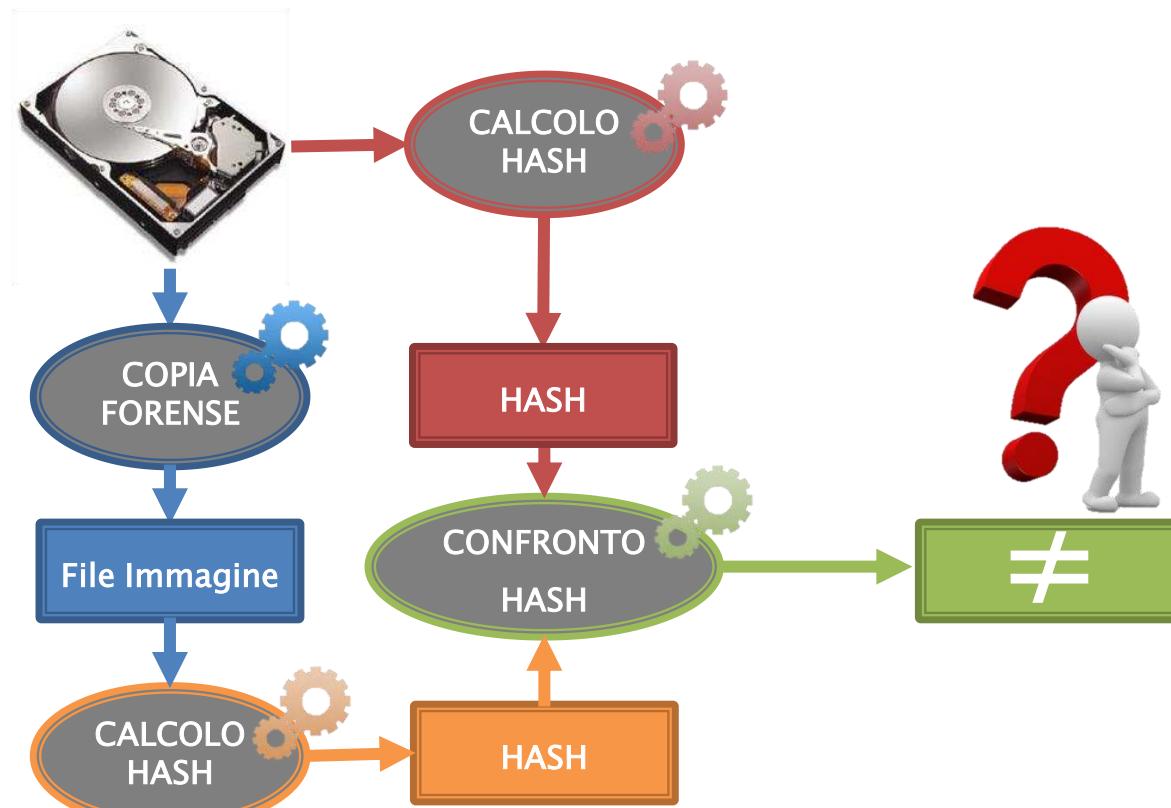
Metodo 2



Hashing on the fly

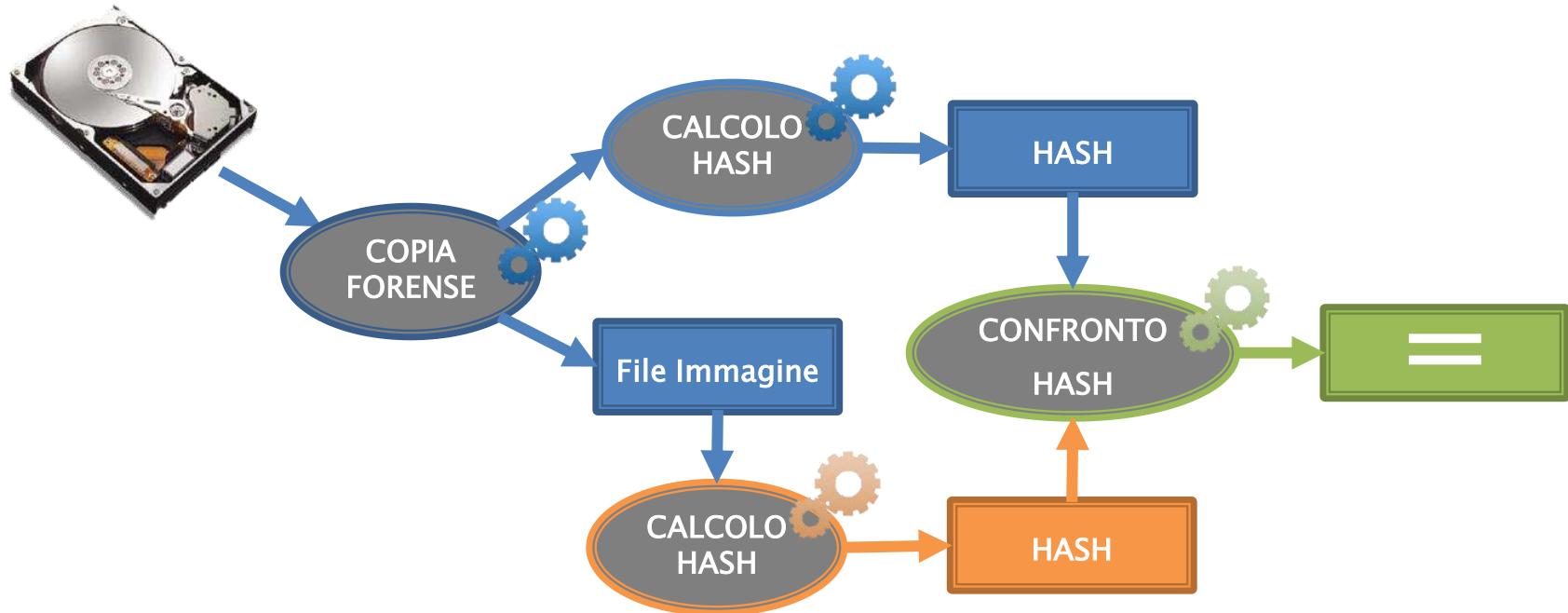
# Calcolo dell'hash: validazione *evidence mutevole* (art. 360 c.p.p.)

## Metodo 1



# Calcolo dell'hash: validazione *evidence mutevole* (art. 360 c.p.p.)

## Metodo 2



# Copia Forense

» Disk Image



# Copia Forense

## *Acquisizione Fisica*

- ▶ Copia «*bit a bit*» dell'intero supporto di memoria: dati e qualsiasi informazione sulla gestione dei dati (*tabella partizioni, Master Boot Record, meta dati del file system, etc.*):



**Clonazione**



**File Immagine  
(*Disk Image*)**

# Disk Image: *le origini*

*Anni '60*

Mondo aziendale



*Disaster Recovery*



Backup

# Disk Image:

## *le origini*

Mondo consumer

Duplicazione supporti ottici

backup

Facilitare  
la masterizzazione

Internet

Diffusione  
software/utility

# Disk Image: *supporti ottici*



Formato ISO: più comune

---

Formato .BIN/.CUE

Copia RAW

Metadati

# Disk Image: *dischi virtuali*



↓  
Formato VMDK



↓  
Formato VDI



Microsoft

↓  
Formato VHD



Apple



↓  
Formato DMG

# Disk Image: *formato DD/RAW*

Formato semplice: è un container dello stream

## ▶ Problematiche:

- Non conserva metadati dell'evidence: *modello, seriale, dimensione, etc.*
- Non conserva hash calcolati;
- Non esegue compressione;
- Non può contenere più di un file/stream;

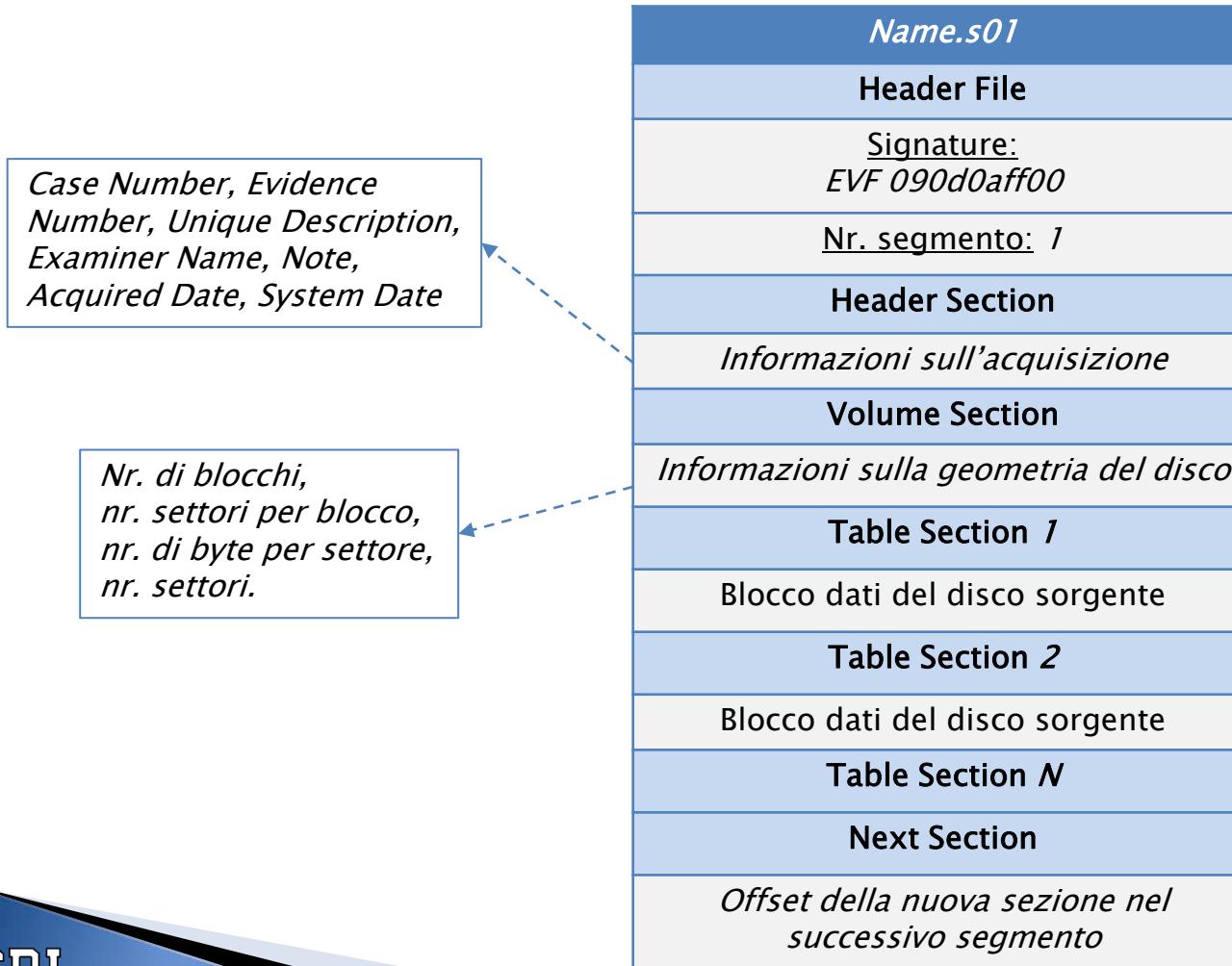
# Disk Image: *Expert Witness Disk Image Format (EWF)*

- ▶ File immagine composto in sezioni
- ▶ Compressione: algoritmo deflate
- ▶ Segmentazione dell'immagine

# Disk Image: *SMART (Famiglia EWF)*

- ▶ Obiettivo: accesso veloce ad una parte dell'immagine
- ▶ Segmentazione dell'immagine: *.s01, .s02, etc.*
- ▶ Ogni segmento è composto da:
  - Header File: *Signature e nr. di segmento.*
  - Una o più sezioni: 4 tipi sezioni.
    - *header section*
    - *volume section*
    - *table section*
    - *next/done sections*

# Disk Image: *SMART (Famiglia EWF)*



# Disk Image: *SMART (Famiglia EWF)*

<i>Name.s02</i>
<b>Header File</b>
<u>Signature:</u> EVF 090d0aff00
<u>Nr. segmento:</u> 2
<b>Table Section <math>N+1</math></b>
Blocco dati del disco sorgente
<b>Table Section N+2</b>
Blocco dati del disco sorgente
<b>Table Section <math>N+M</math></b>
<b>Next Section</b>
<i>Offset della nuova sezione nel successivo segmento</i>

...

<i>Name.s[k]</i>
<b>Header File</b>
<u>Signature:</u> EVF 090d0aff00
<u>Nr. segmento:</u> k
<b>Table Section <math>[k-1]n+1</math></b>
Blocco dati del disco sorgente
<b>Table Section <math>[k-1]n+1</math></b>
Blocco dati del disco sorgente
<b>Table Section <math>N+k</math></b>
<b>Done Section</b>

# Disk Image: *Encase E01 Bitstream (Famiglia EWF)*

- ▶ Basato sul formato SMART
- ▶ Segmentazione dell'immagine: *.e01, .e02, etc.*
- ▶ Tre livelli di compressione: *no, good, best*
- ▶ Impiega nr. 13 sezioni (+ 9 al formato SMART):
  - Header2 section;
  - Disk section;
  - Sectors section;
  - Table2 section;
  - Data section;
  - Errors2 section;
  - Session section;
  - **Hash section;**
  - **Digest section;**

# Disk Image: *Encase L01 Logical (Famiglia EWF)*

- ▶ Acquisizione di file logici.
- ▶ Segmentazione dell'immagine: *.l01, .l02, etc.*
- ▶ Impiega nr. 15 sezioni (+ 2 al formato E01):
  - Ltree section
  - Ltypes section

# Disk Image: Advanced Forensics Format (*AFF/AFF4*)

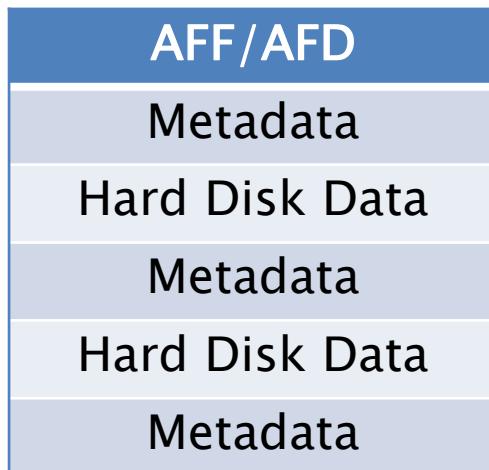
## AFF

- ▶ Formato Open ed estensibile
- ▶ Creato prima dell'implementazione open source di “libewf” (*libreria per il formato EWF*)

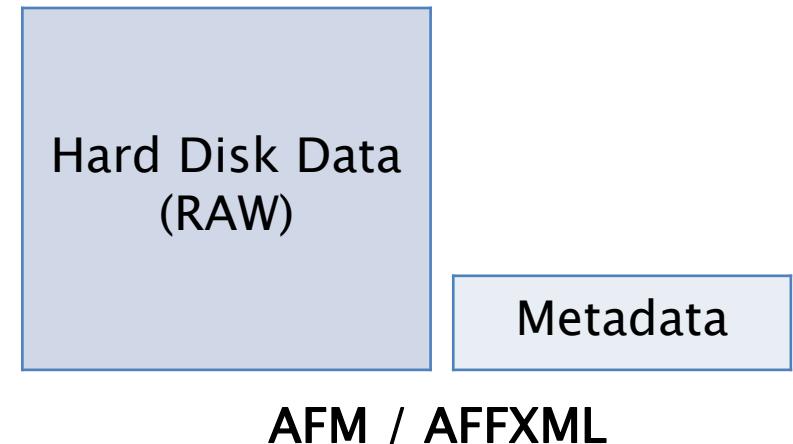
# Disk Image: Advanced Forensics Format (AFF/AFF4)

## AFF

- ▶ Ogni disco viene separato in due layer:
  - disk-rappresentation layer (*metadato*);
  - data-storage layer (*dato*);



VS



# Copia Forense

» Guymager

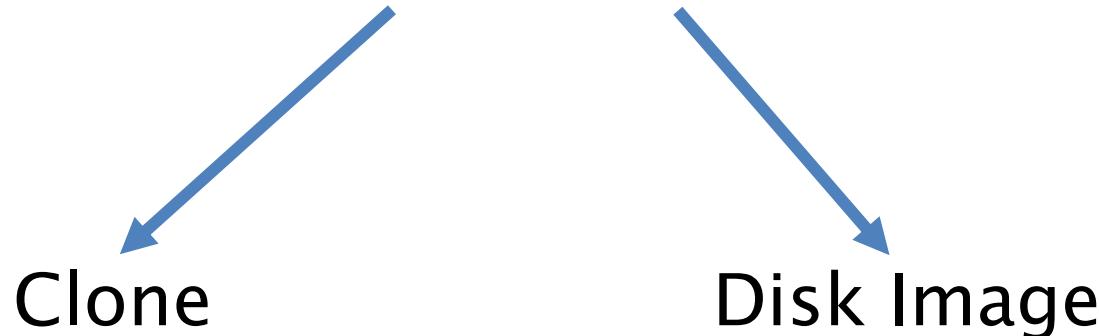


# Tool di acquisizione

## *Guymager*



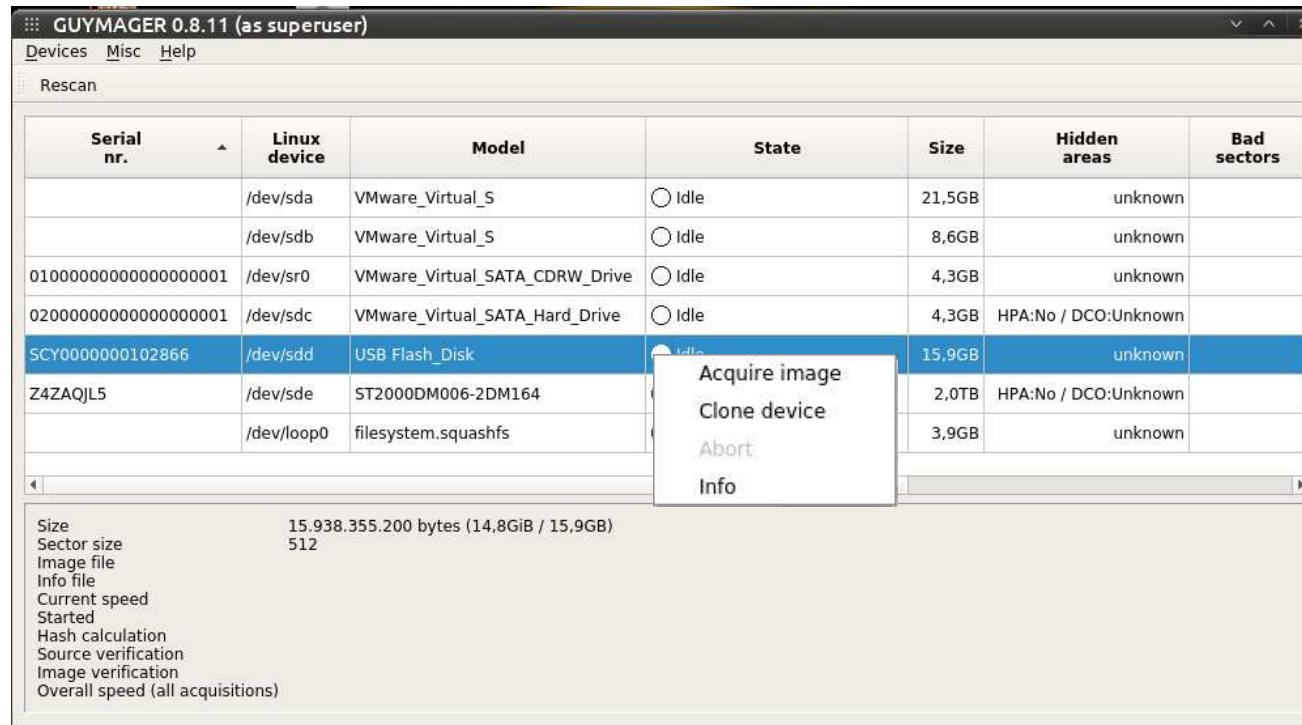
- ▶ Sviluppato da Guy Voncken
- ▶ Licenza: *Free OpenSource*
- ▶ Piattaforma: *O.S. Linux*
- ▶ Basato sulla libreria «libewf»



# Tool di acquisizione

## *Guymager: Disk Image*

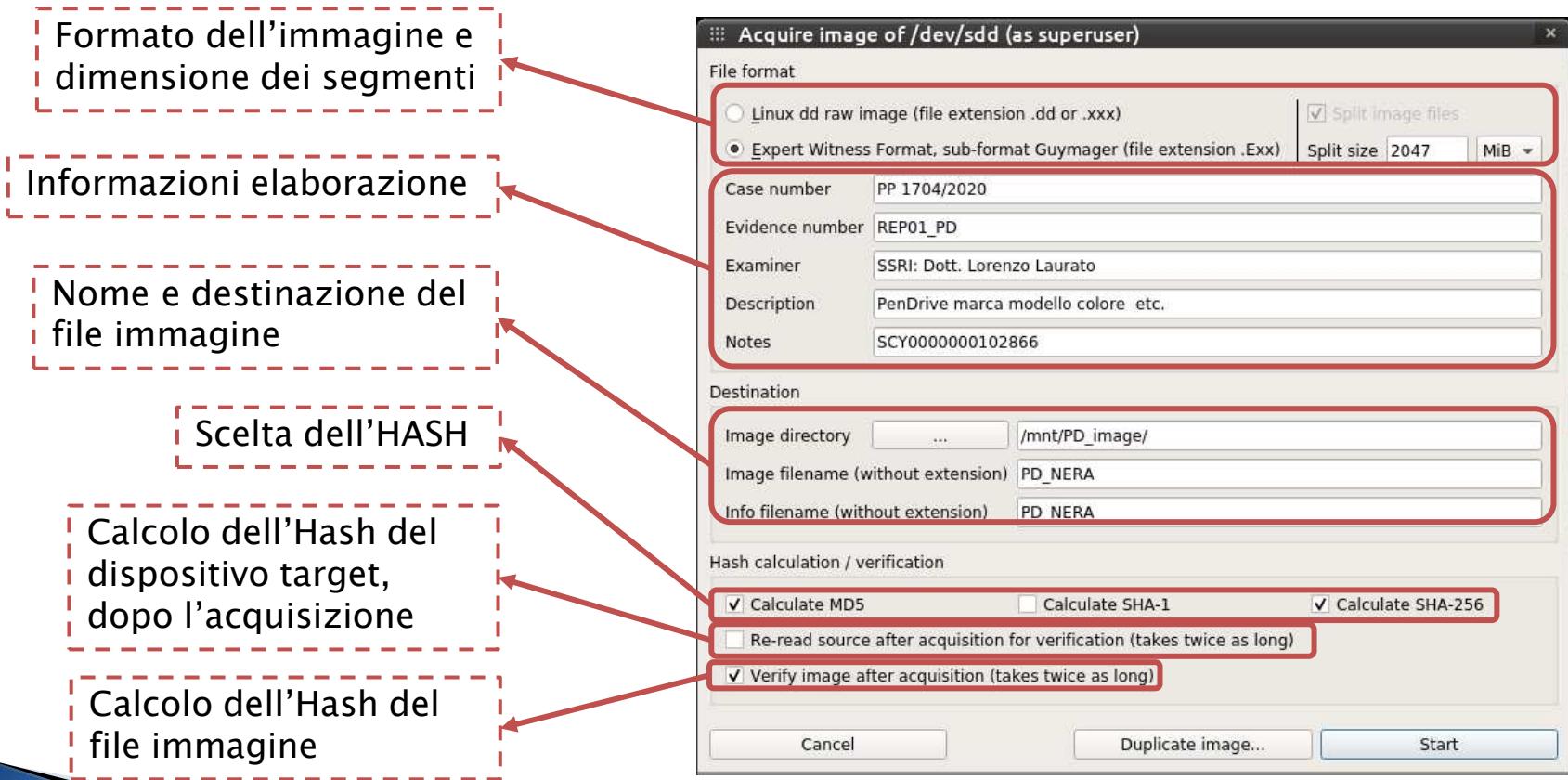
- ▶ scelta del dispositivo da acquisire (*/dev/sdd - USB Flash\_Disk*)



# Tool di acquisizione

## *Guymager: Disk Image*

### ▶ Settaggio dell'elaborazione



# Tool di acquisizione

## *Guymager: Disk Image*

- ▶ l'elaborazione...

The screenshot shows the 'Devices' tab of the Guymager interface. A red dashed box labeled 'Statistiche sull'elaborazione' points to the status bar at the bottom of the table, which displays acquisition details. A red arrow points from this status bar to another red dashed box labeled 'Riepilogo delle impostazioni' at the bottom right.

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
	/dev/sda	VMware_Virtual_S	Idle	21,5GB	unknown					
	/dev/sdb	VMware_Virtual_S	Idle	8,6GB	unknown					
01000000000000000000000000000001	/dev/sr0	VMware_Virtual_SATA_...	Idle	4,3GB	unknown					
02000000000000000000000000000001	/dev/sdc	VMware_Virtual_SATA_...	Idle	4,3GB	HPA:No / ...					
SCY00000000102866	/dev/sdd	USB Flash_Disk	Running	15,9GB	unknown	0	4%	10,52	00:46:05	r 100 h 64 c ...
Z4ZAQJL5	/dev/sde	ST2000DM006-2DM164	Idle	2,0TB	HPA:No / ...					

Size: 15.938.355.200 bytes (14,8GiB / 15,9GB)  
Sector size: 512  
Image file: /mnt/PD\_image/PD\_NERA.Exx  
Info file: /mnt/PD\_image/PD\_NERA.info  
Current speed: 14,27 MB/s  
Started: 16. aprile 15:35:14 (00:02:03)  
Hash calculation: MD5 and SHA-256  
Source verification: off  
Image verification: on  
Overall speed (all acquisitions): 14,27 MB/s

Riepilogo delle impostazioni

# Tool di acquisizione

## *Guymager: Disk Image*

- ▶ Termine dell'elaborazione

The screenshot shows the 'Devices' tab of the Guymager 0.8.11 application window. It lists several devices in a table:

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]
	/dev/sda	VMware_Virtual_S	○ Idle	21,5GB	unknown			
	/dev/sdb	VMware_Virtual_S	○ Idle	8,6GB	unknown			
01000000000000000000000000000001	/dev/sr0	VMware_Virtual_SATA_...	○ Idle	4,3GB	unknown			
02000000000000000000000000000001	/dev/sdc	VMware_Virtual_SATA_...	○ Idle	4,3GB	HPA:No / ...			
SCY0000000102866	/dev/sdd	USB Flash_Disk	● Finished - Verified & ok	15,9GB	unknown	0	100%	16,99
Z4ZAQJL5	/dev/sde	ST2000DM006-2DM164	○ Idle	2,0TB	HPA:No / ...			

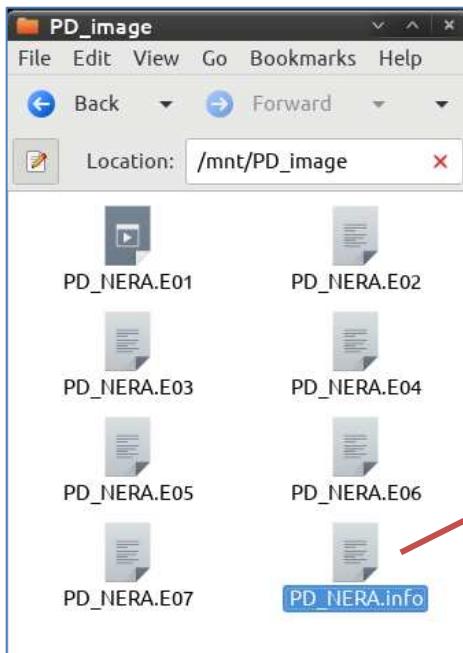
Below the table, a summary of acquisition parameters is shown:

Size	15.938.355.200 bytes (14,8GiB / 15,9GB)
Sector size	512
Image file	/mnt/PD_image/PD_NERA.Exx
Info file	/mnt/PD_image/PD_NERA.info
Current speed	
Started	16. aprile 15:35:14 (00:29:49)
Hash calculation	MD5 and SHA-256
Source verification	off
Image verification	on
Overall speed (all acquisitions)	

# Tool di acquisizione

## *Guymager: Disk Image*

- ▶ Termine dell'elaborazione



```
Acquisition
=====
Linux device      : /dev/sdd
Device size       : 15938355200 (15,9GB)
Format            : Expert Witness Format, sub-format Guymager - file
extension is .Exx
Image meta data
  Case number     : PP 1704/2020
  Evidence number : REP01_PD
  Examiner        : SSRI: Dott. Lorenzo Laurato
  Description      : PenDrive marca modello colore etc.
  Notes           : SCY0000000102866

Image path and file name: /mnt/PD_image/PD_NERA.Exx
Info  path and file name: /mnt/PD_image/PD_NERA.info

Hash calculation    : MD5 and SHA-256
Source verification : off
Image verification  : on

No bad sectors encountered during acquisition.
State: Finished successfully
MD5 hash           : a087165bf957367efa39dd0e7372994d
MD5 hash verified source : --
MD5 hash verified image  : a087165bf957367efa39dd0e7372994d
SHA1 hash          : --
SHA1 hash verified source : --
SHA1 hash verified image  : --
SHA256 hash         :
8bd5f8f7a19cb4fcfa726fbb29cb419151bf4c7f711c4b9480b74a3b8e3dae30c
SHA256 hash verified source: --
SHA256 hash verified image :
8bd5f8f7a19cb4fcfa726fbb29cb419151bf4c7f711c4b9480b74a3b8e3dae30c
Image verification OK. The image contains exactly the data that was written.

Acquisition started : 2020-04-16 15:35:14 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2020-04-16 15:57:25
Ended              : 2020-04-16 16:05:03 (8 hours, 29 minutes and 49 seconds)
Acquisition speed  : 11.43 MByte/s (8 hours, 22 minutes and 10 seconds)
Verification speed : 33.19 MByte/s (8 hours, 7 minutes and 38 seconds)
```

# Copia Forense

» FTK Imager

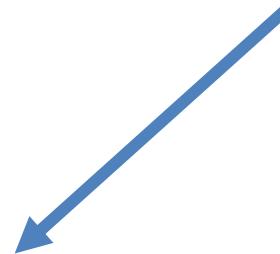


# Tool di acquisizione

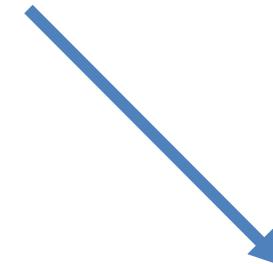
## *FTK Imager*



- ▶ Prodotto dalla AccessData
- ▶ Licenza: *Freeware*
- ▶ Piattaforma: *O.S. Microsoft Windows*



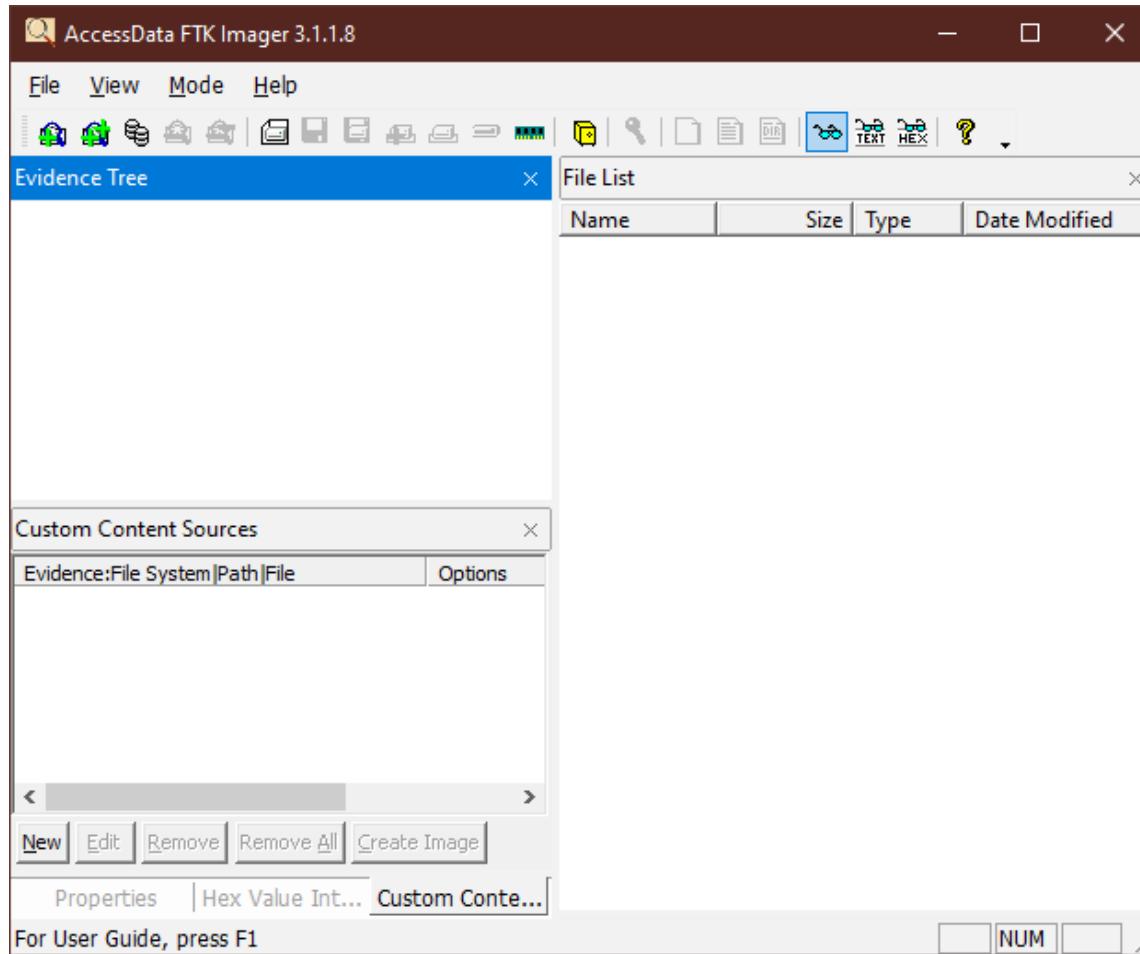
Lite Version



Install Version

# Tool di acquisizione

## *FTK Imager*



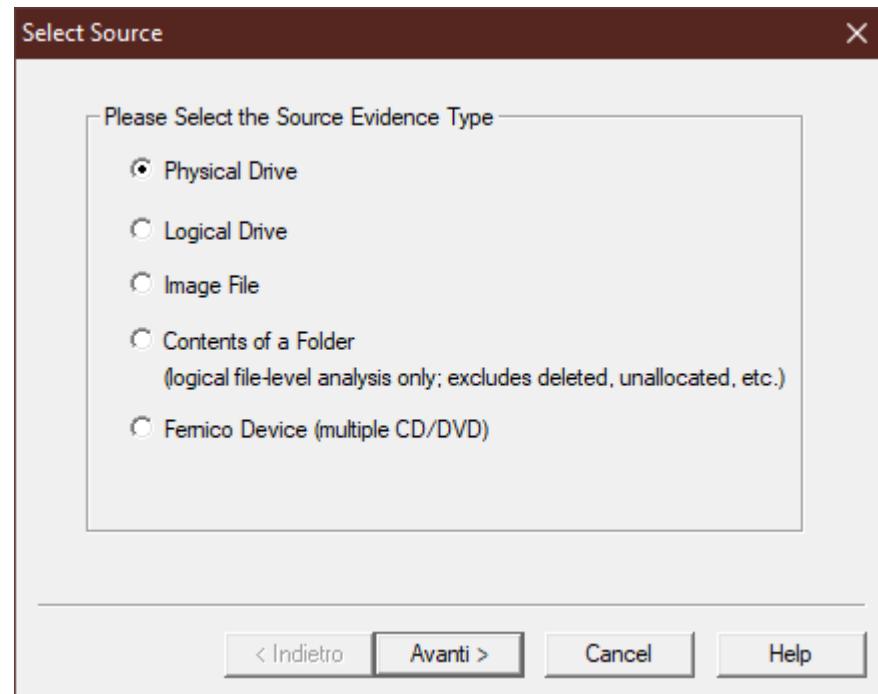
# Tool di acquisizione

## *FTK Imager*

- ▶ File>Create Disk Image...

- ▶ Tipi di acquisizioni:

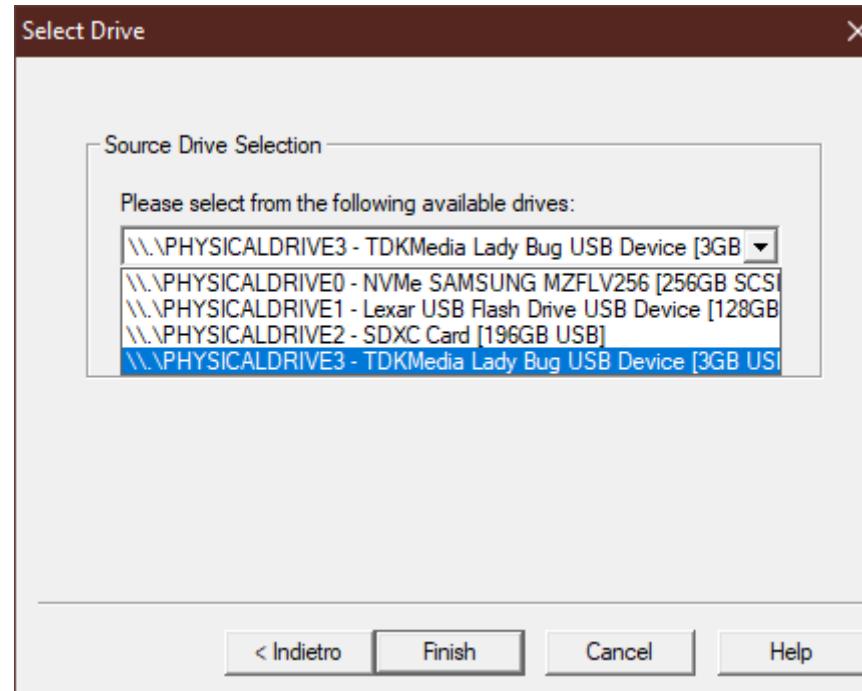
- Physical Drive
- Logical Drive
- Image File
- Content of folder
- Fenico Device



# Tool di acquisizione

## *FTK Imager: Physical Drive*

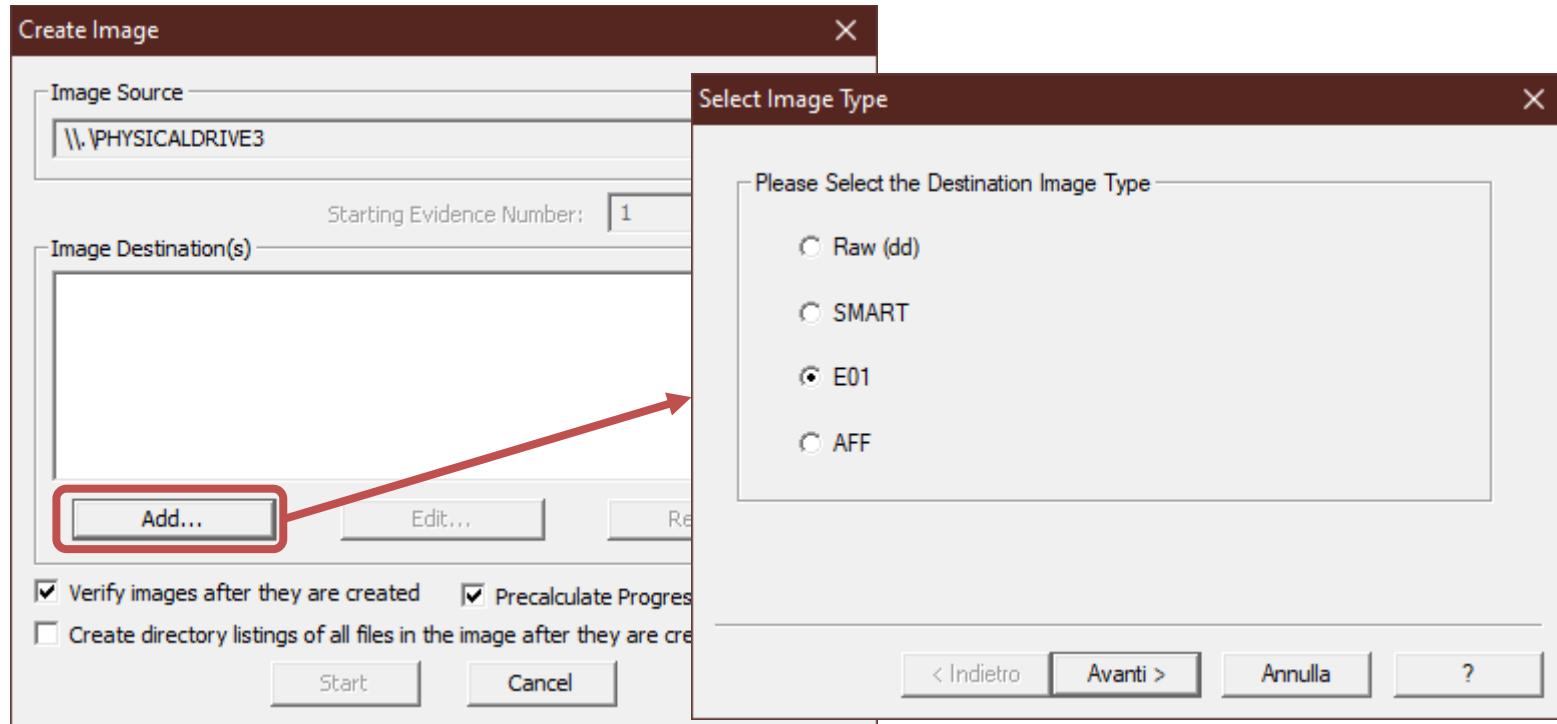
- ▶ **Source Drive Selection:** scelta del dispositivo da acquisire (*PhysicalDrive3 – TDKMedia...*)



# Tool di acquisizione

## *FTK Imager: Physical Drive*

### ▶ Scelta del formato immagine



# Tool di acquisizione

## *FTK Imager: Physical Drive*

### ▶ Inserimento informazioni caso

Evidence Item Information X

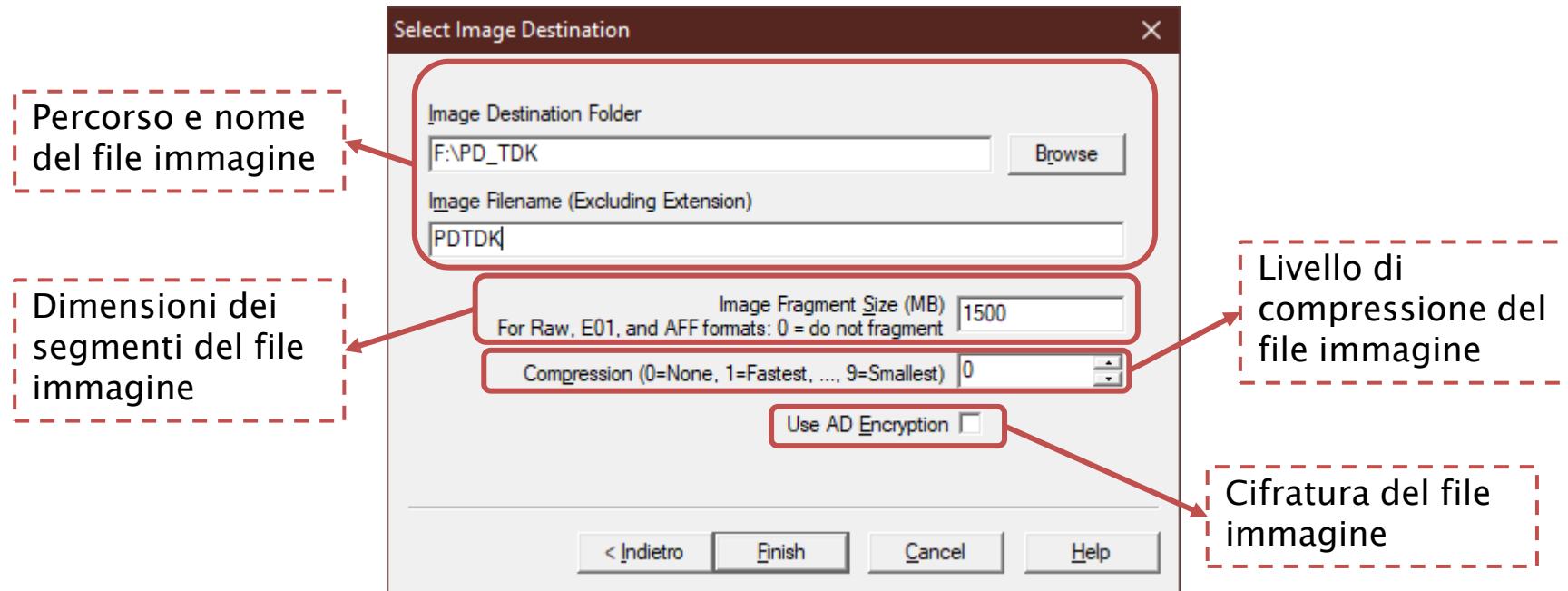
Case Number:	Nr. 1704/2020
Evidence Number:	REP1_PDTDK
Unique Description:	PenDrive TDK S.N:123456XYZ
Examiner:	SSRI: Dott. Lorenzo Laurato
Notes:	di Tizio INCOGNITO

[< Indietro](#) [Avanti >](#) [Cancel](#) [Help](#)

# Tool di acquisizione

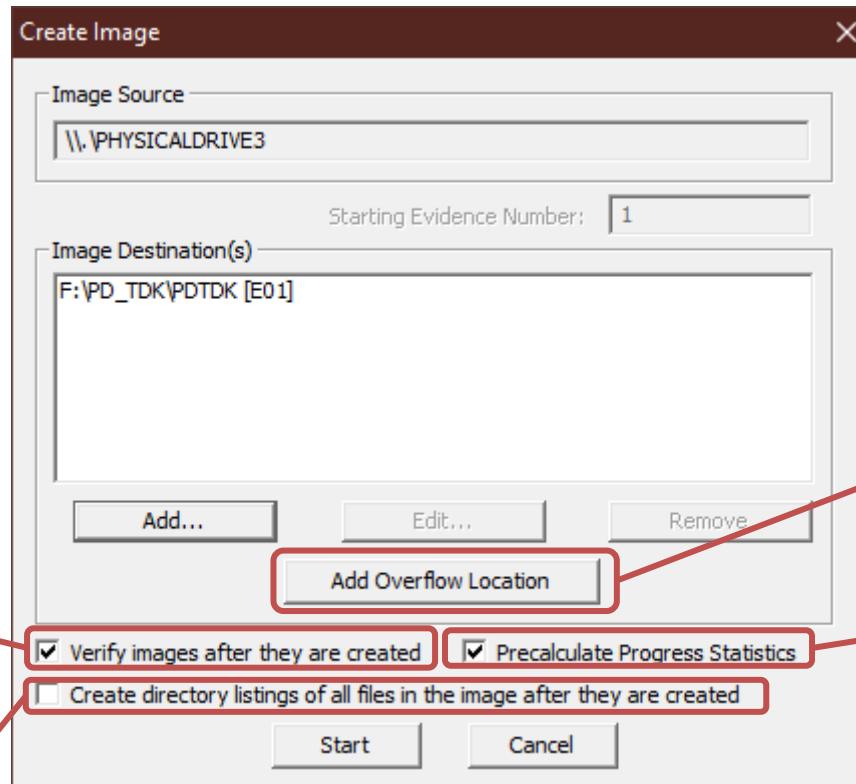
## *FTK Imager: Physical Drive*

### ▶ Definizione del file immagine



# Tool di acquisizione

## *FTK Imager: Physical Drive*



Calcolo e verifica  
dell'Hash del file  
immagine con il  
dispositivo target

Generazione di un  
file CSV di tutti i file  
e cartelle presenti

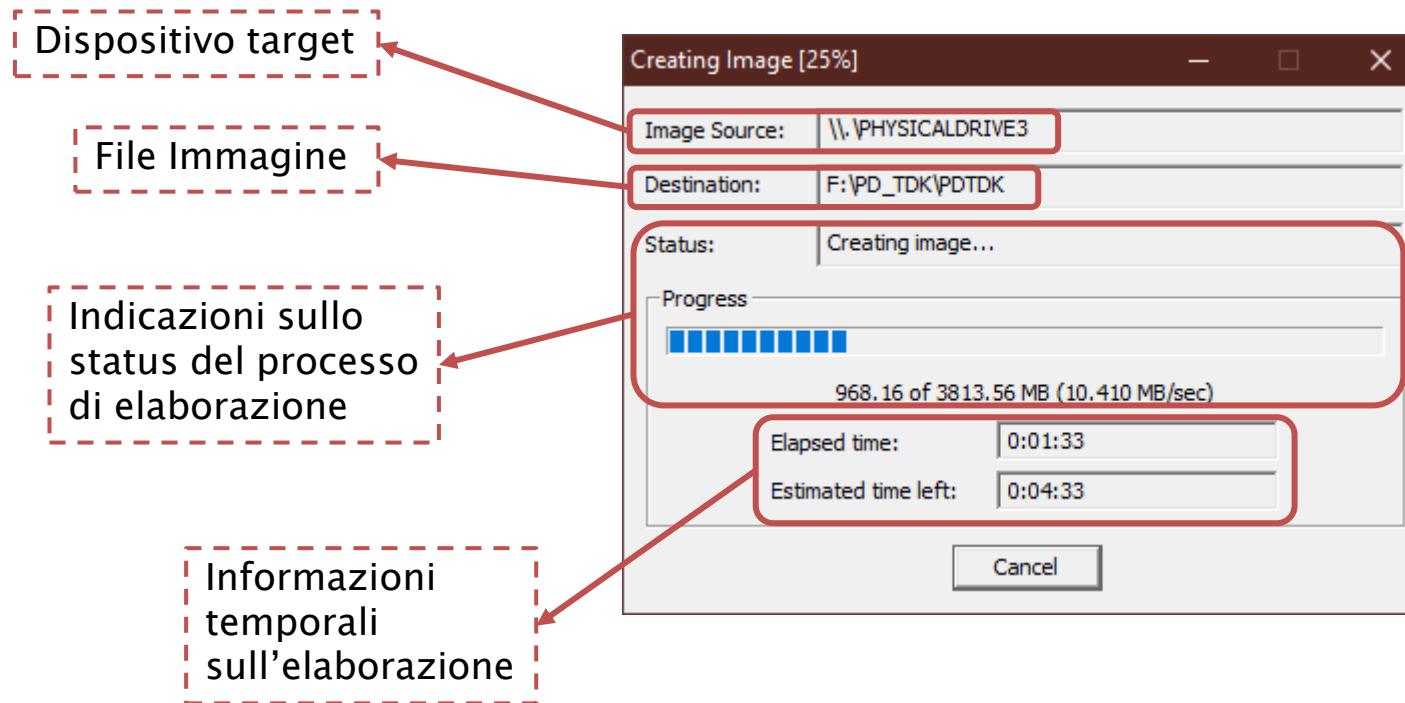
Aggiungere  
ulteriore spazio di  
archiviazione per il  
file immagine  
(install version)

permette di  
visionare il tempo  
rimanente per  
l'elaborazione della  
copia forense

# Tool di acquisizione

## *FTK Imager: Physical Drive*

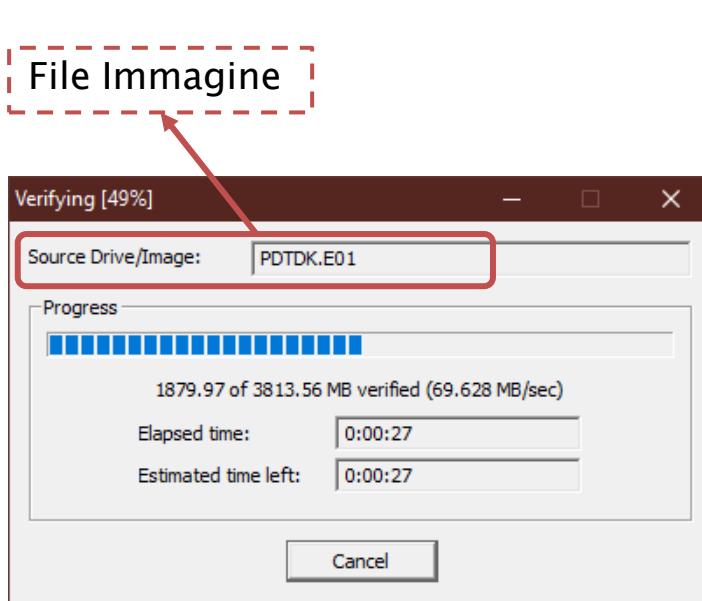
### ▶ Elaborazione...



# Tool di acquisizione

## *FTK Imager: Physical Drive*

### ▶ Processo di validazione...

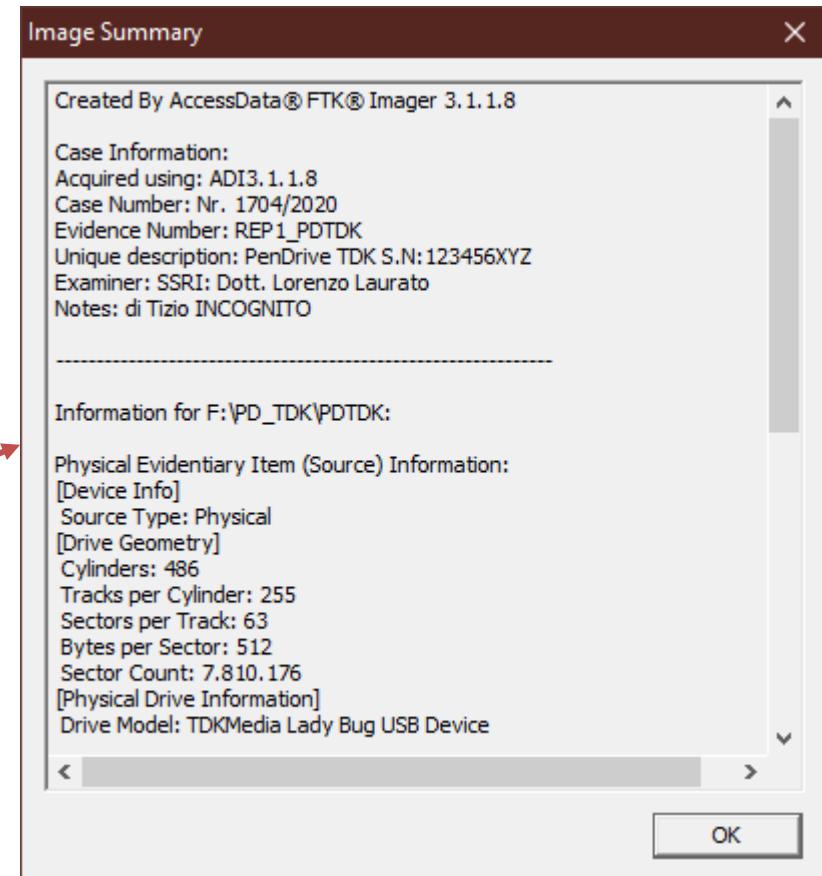
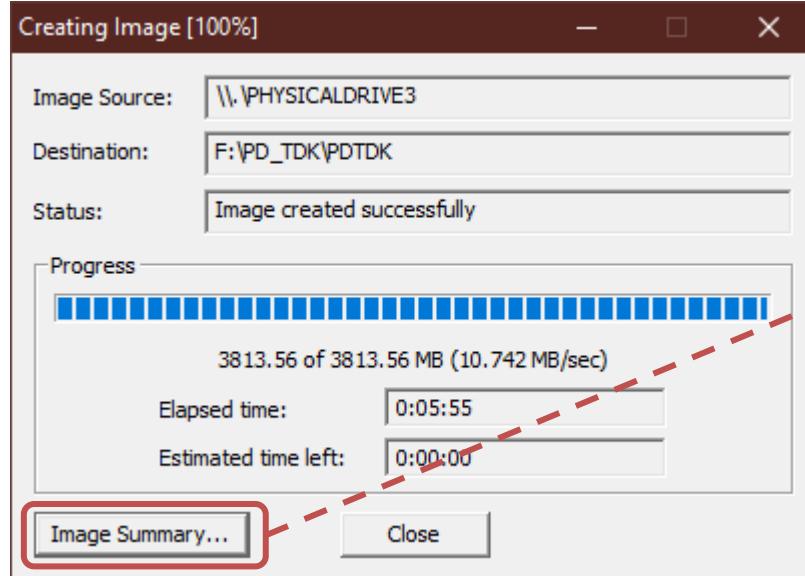


Drive/Image Verify Results	
Name	PDTDK.E01
Sector count	7810176
MD5 Hash	
Computed hash	452bf980755fb43da7913aef44bc901e
Stored verification hash	452bf980755fb43da7913aef44bc901e
Report Hash	452bf980755fb43da7913aef44bc901e
Verify result	Match
SHA1 Hash	
Computed hash	9f738ab4bd4430152e5cc4e4ecda18ffd58958a6
Stored verification hash	9f738ab4bd4430152e5cc4e4ecda18ffd58958a6
Report Hash	9f738ab4bd4430152e5cc4e4ecda18ffd58958a6

# Tool di acquisizione

## *FTK Imager: Physical Drive*

### ▶ Termine dell'elaborazione



# Tool di acquisizione

## *FTK Imager: Physical Drive*

### ▶ Termine dell'elaborazione

PD_TDK			
Condividi Visualizza			
Unità USB (F:) > PD_TDK			
Nome	Ultima modifica	Tipo	Dimensione
PDTDK.E01	15/04/2020 21:41	File E01	1.535.925 KB
PDTDK.E02	15/04/2020 21:43	File E02	1.535.925 KB
PDTDK.E03	15/04/2020 21:44	File E03	834.676 KB
PDTDK.E01.csv	15/04/2020 21:44	File con valori sepa...	15 KB
PDTDK.E01.txt	15/04/2020 21:45	Documento di testo	2 KB

The screenshot shows the FTK Imager interface with two windows open. The left window displays a file list from a USB drive named 'PD\_TDK'. A red dashed arrow points from the file 'PDTDK.E01.txt' in this list to the right-hand details window. The right window is titled 'PDTDK.E01.txt - Blocco note di Windows' and contains the following information:

File Modifica Formato Visualizza ?  
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:  
Acquired using: ADI3.1.1.8  
Case Number: Nr. 1704/2020  
Evidence Number: REP1\_PDTDK  
Unique description: PenDrive TDK S.N:123456XYZ  
Examiner: SSRI: Dott. Lorenzo Laurato  
Notes: di Tizio INCOGNITO

Information for F:\PD\_TDK\PDTDK:

Physical Evidentiary Item (Source) Information:  
[Device Info]  
Source Type: Physical  
[Drive Geometry]  
Cylinders: 486  
Tracks per Cylinder: 255  
Sectors per Track: 63  
Bytes per Sector: 512  
Sector Count: 7.810.176  
[Physical Drive Information]  
Drive Model: TDKMedia Lady Bug USB Device  
Drive Serial Number: 07B609035113FBCC  
Drive Interface Type: USB  
Removable drive: True  
Source data size: 3813 MB  
Sector count: 7810176  
[Computed Hashes]  
MD5 checksum: 452bf980755fb43da7913aef44bc901e  
SHA1 checksum: 9f738ab4bd4430152e5cc4e4ecda18ffd58958a6

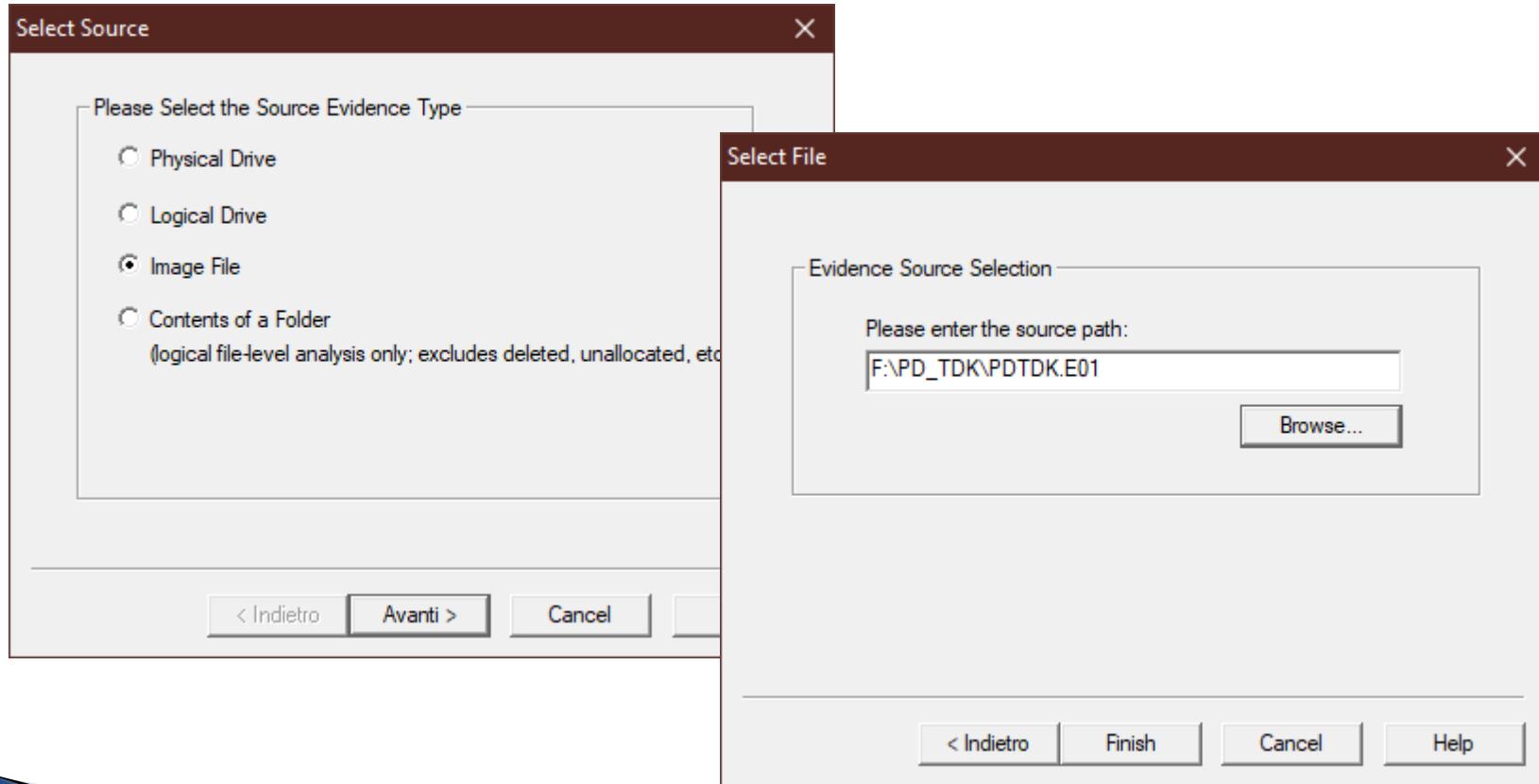
Image Information:  
Acquisition started: Wed Apr 15 21:38:43 2020  
Acquisition finished: Wed Apr 15 21:44:38 2020  
Segment list:  
F:\PD\_TDK\PDTDK.E01  
F:\PD\_TDK\PDTDK.E02  
F:\PD\_TDK\PDTDK.E03

Image Verification Results:  
Verification started: Wed Apr 15 21:44:38 2020  
Verification finished: Wed Apr 15 21:45:32 2020  
MD5 checksum: 452bf980755fb43da7913aef44bc901e : verified  
SHA1 checksum: 9f738ab4bd4430152e5cc4e4ecda18ffd58958a6 : verified

# Tool di acquisizione

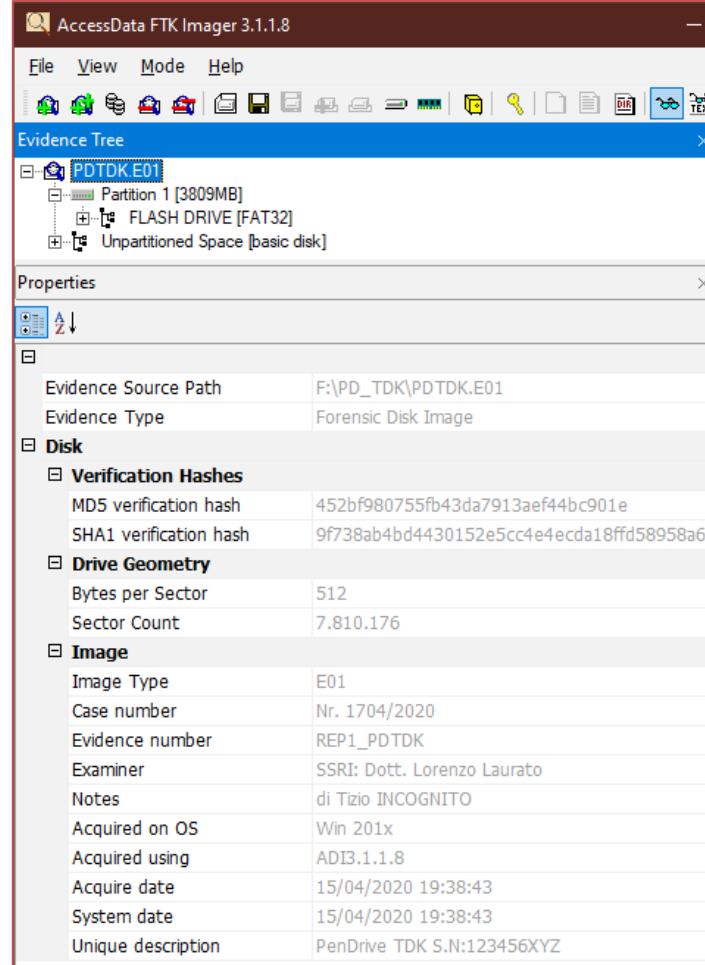
## *FTK Imager: apertura file immagine*

- ▶ File>Add Evidence Item...



# Tool di acquisizione

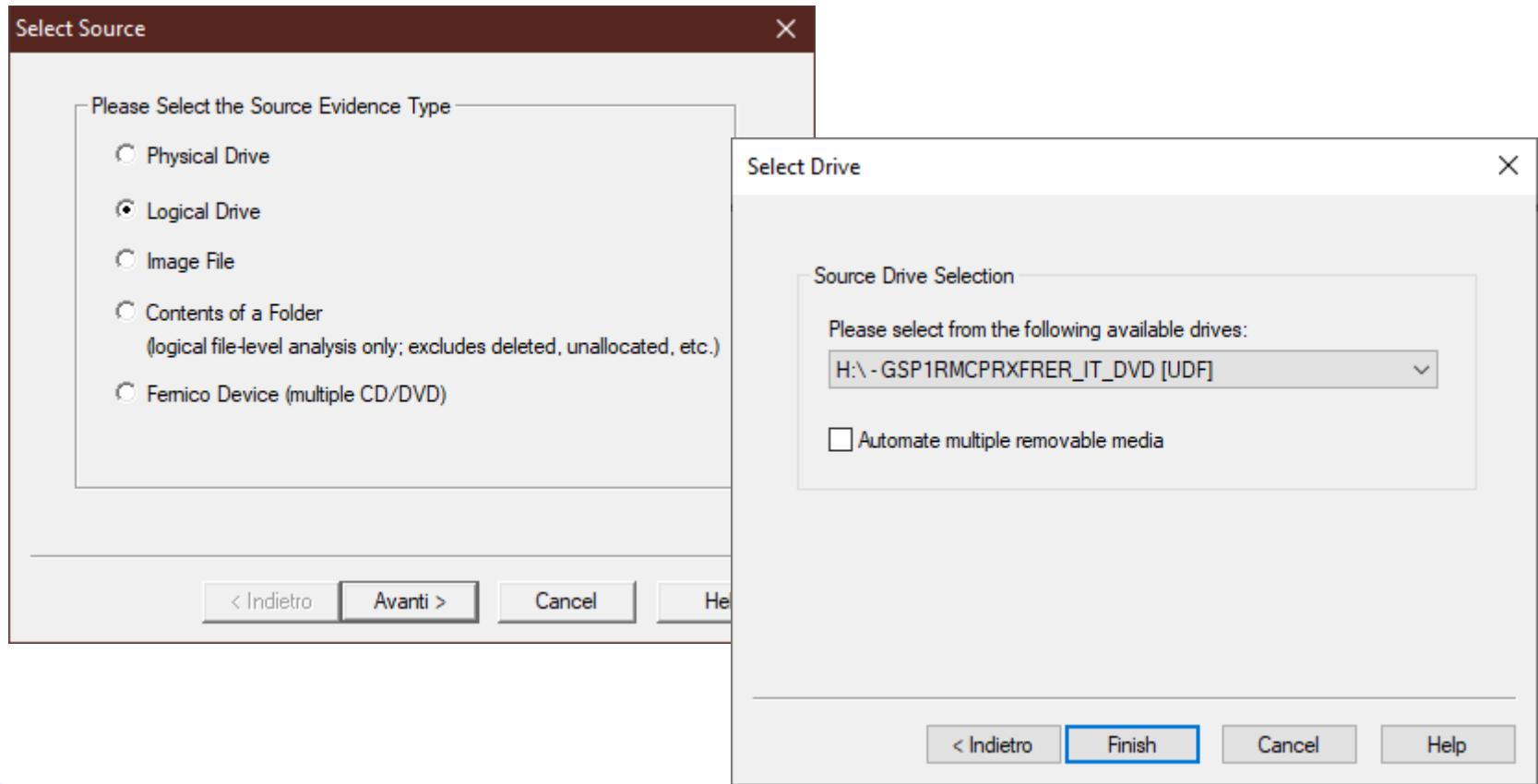
## *FTK Imager: apertura file immagine*



# Tool di acquisizione

## *FTK Imager: Logical Drive*

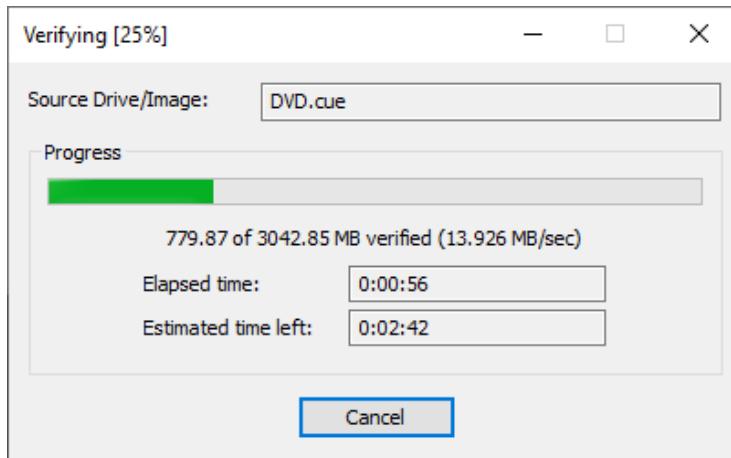
- ▶ File>Create Disk Image...



# Tool di acquisizione

## *FTK Imager: Logical Drive*

### ▶ Acquisizione supporto ottico



Drive/Image Verify Results	
Name	DVD.cue
Sector count	1557941
MD5 Hash	Computed hash: 33fda618c6ed880d43ef7ce1debd7a99
SHA1 Hash	Computed hash: c4c4a6493e2c45649baf75a045ca922db0c7ca58
Bad Blocks List	Bad block(s) in image: No bad blocks found in image

# Tool di acquisizione

## *FTK Imager: Logical Drive*

### ▶ Acquisizione supporto ottico

Nome	Ultima modifica	Tipo	Dimensione
DVD.cue	16/04/2020 12:24	CUE Other File (VLC)	1 KB
DVD.cue.txt	16/04/2020 12:38	Documento di testo	2 KB
DVD.iso	16/04/2020 12:20	File Immagine disco	1.048.576 KB
DVD.iso01	16/04/2020 12:22	File ISO01	1.048.576 KB
DVD.iso02	16/04/2020 12:24	File ISO02	1.018.730 KB

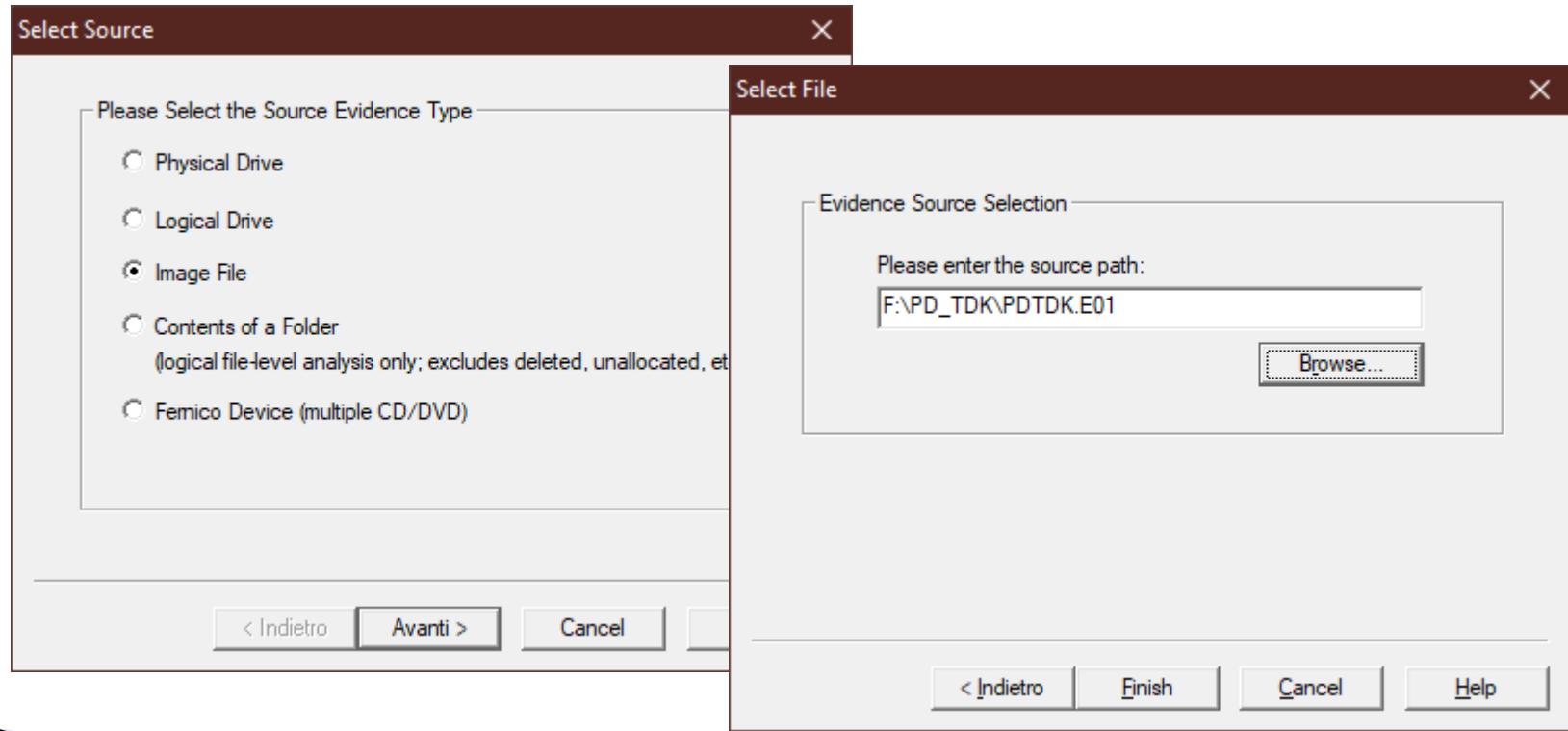
```
DVD.cue.txt - Blocco note di Windows
File Modifica Formato Visualizza ?
Created By AccessData® FTK® Imager 4.3.0.18

Device Name : HL-DT-ST DVD+-RW GH70N
Media Type : DVD-ROM
Bytes per Sector : 2.048
Sector Count : 1.557.941
Session Count : 1
UTC Timestamps : True
<<<<
    File Class : Session
    File Size : 3.190.663.168
    Physical Size : 3.190.663.168
    Actual File : True
    LBA : 0
    Logical Block Count : 1.557.941
    ++++++
        File Class : Track
        File Size : 3.190.663.168
        Physical Size : 3.190.663.168
        Actual File : True
        Track type : Data
        LBA : 0
        Logical Block Count : 1.557.941
    -----
        File Class : File System
        File Size : 2.048
        Physical Size : 2.048
        Actual File : True
        File system type : ISO 9660
        LBA : 16
        Logical Block Count : 1
    -----
        File Class : File System
        File Size : 2.048
        Physical Size : 2.048
        Actual File : True
        File system type : El Torito
        LBA : 17
        Logical Block Count : 1
    -----
        File Class : File System
        File Size : 2.048
        Physical Size : 2.048
        Actual File : True
        File system type : UDF
        UDF Version : 2.58
        LBA : 257
        Logical Block Count : 1
>>>>
```

# Tool di acquisizione

## *FTK Imager: Image File*

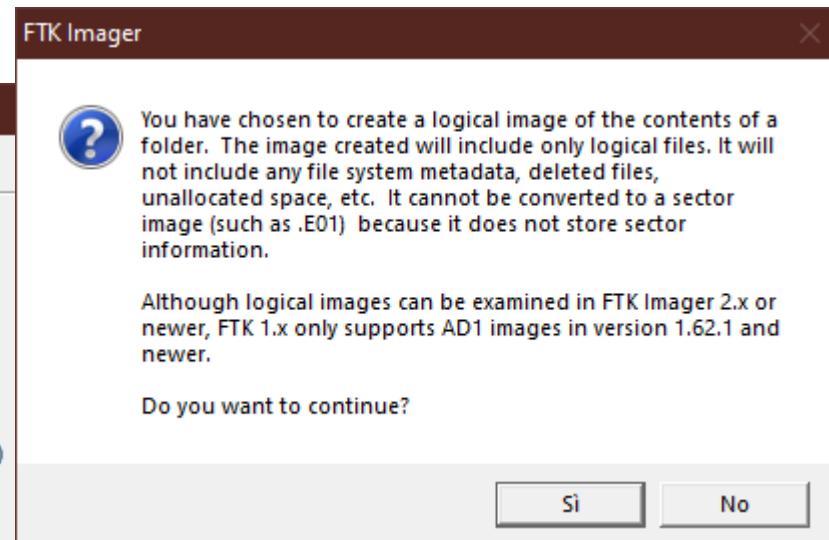
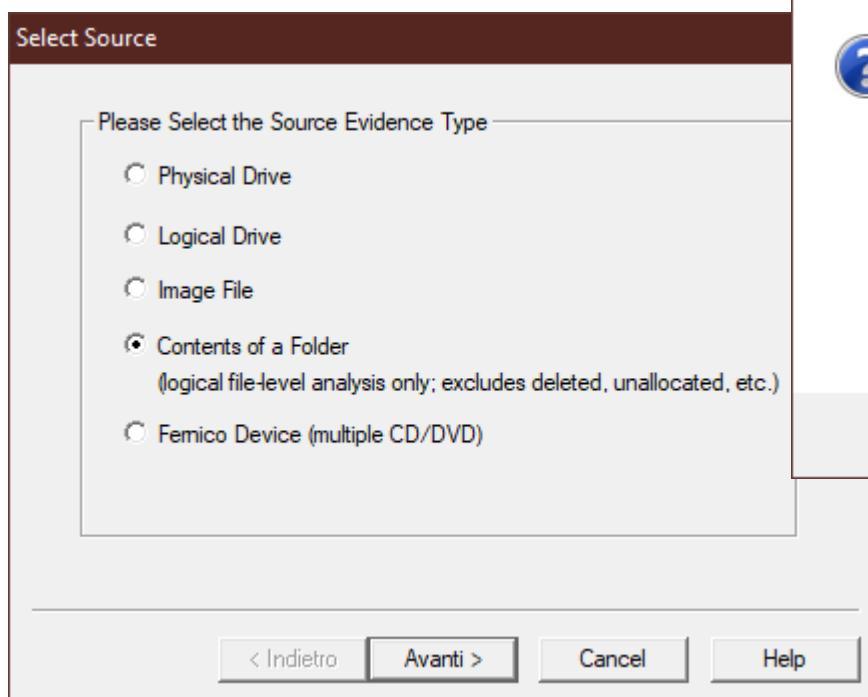
- ▶ Impiegato principalmente per convertire un file immagine da un formato ad un altro: Es. E01->DD



# Tool di acquisizione

## *FTK Imager: Contents of a Folder*

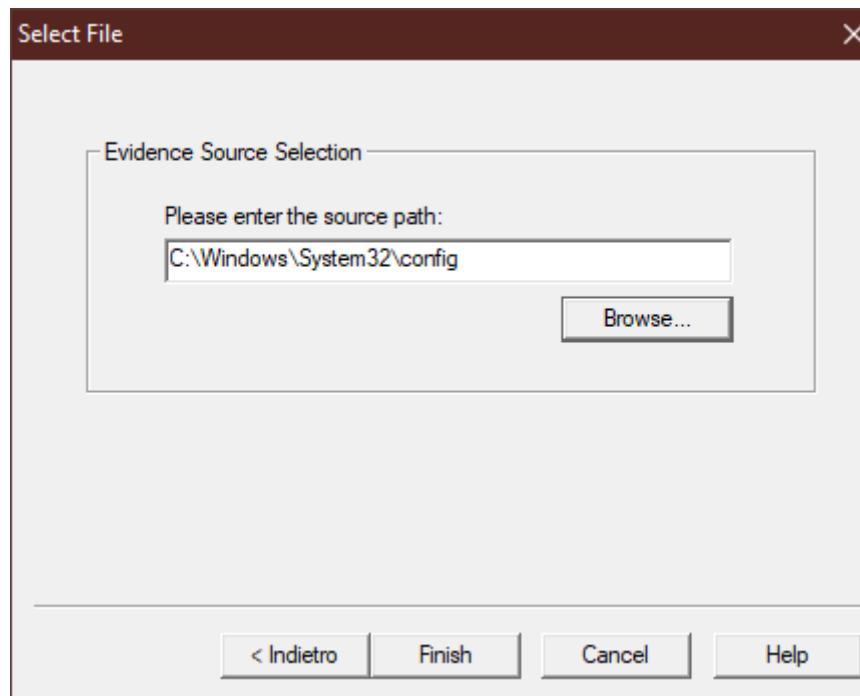
- ▶ Acquisizione logica di file in una determinata cartella



# Tool di acquisizione

## *FTK Imager: Contents of a Folder*

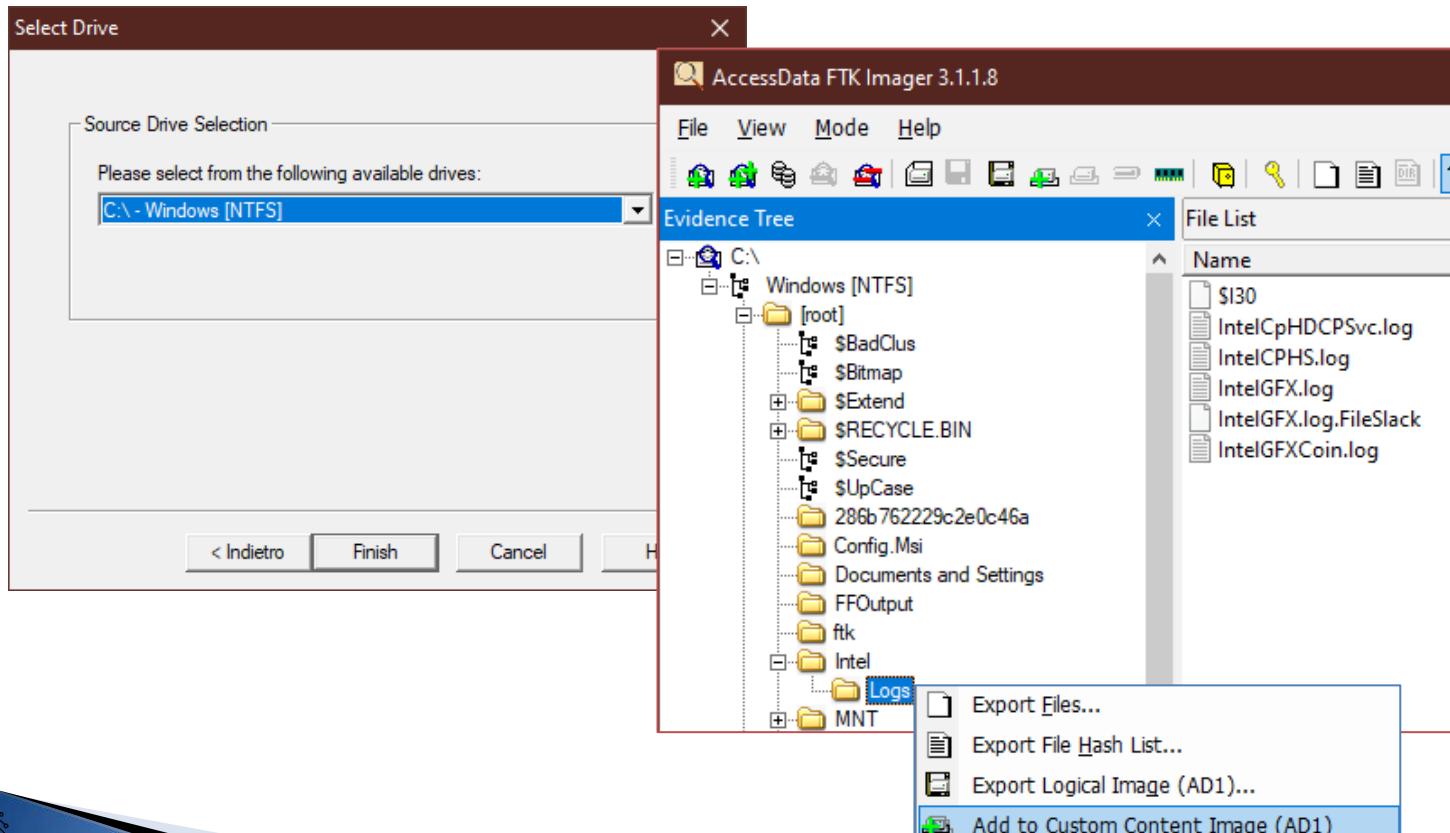
- ▶ Acquisizione logica di file in una determinata cartella



# Tool di acquisizione

## *FTK Imager: Custom Content Image*

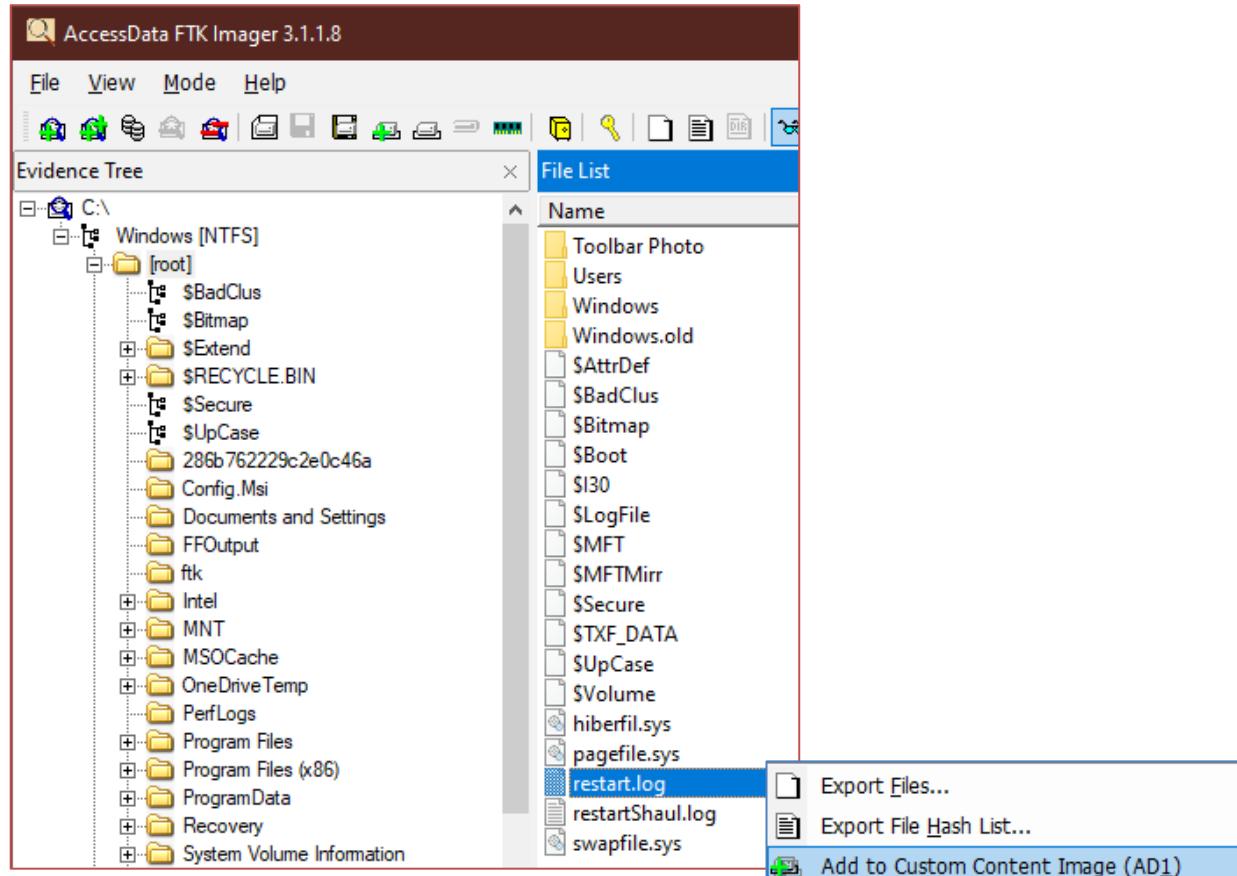
- ▶ Elaborazione di un immagine personalizzata
  - File->**Add Evidence Item...**



# Tool di acquisizione

## *FTK Imager: Custom Content Image*

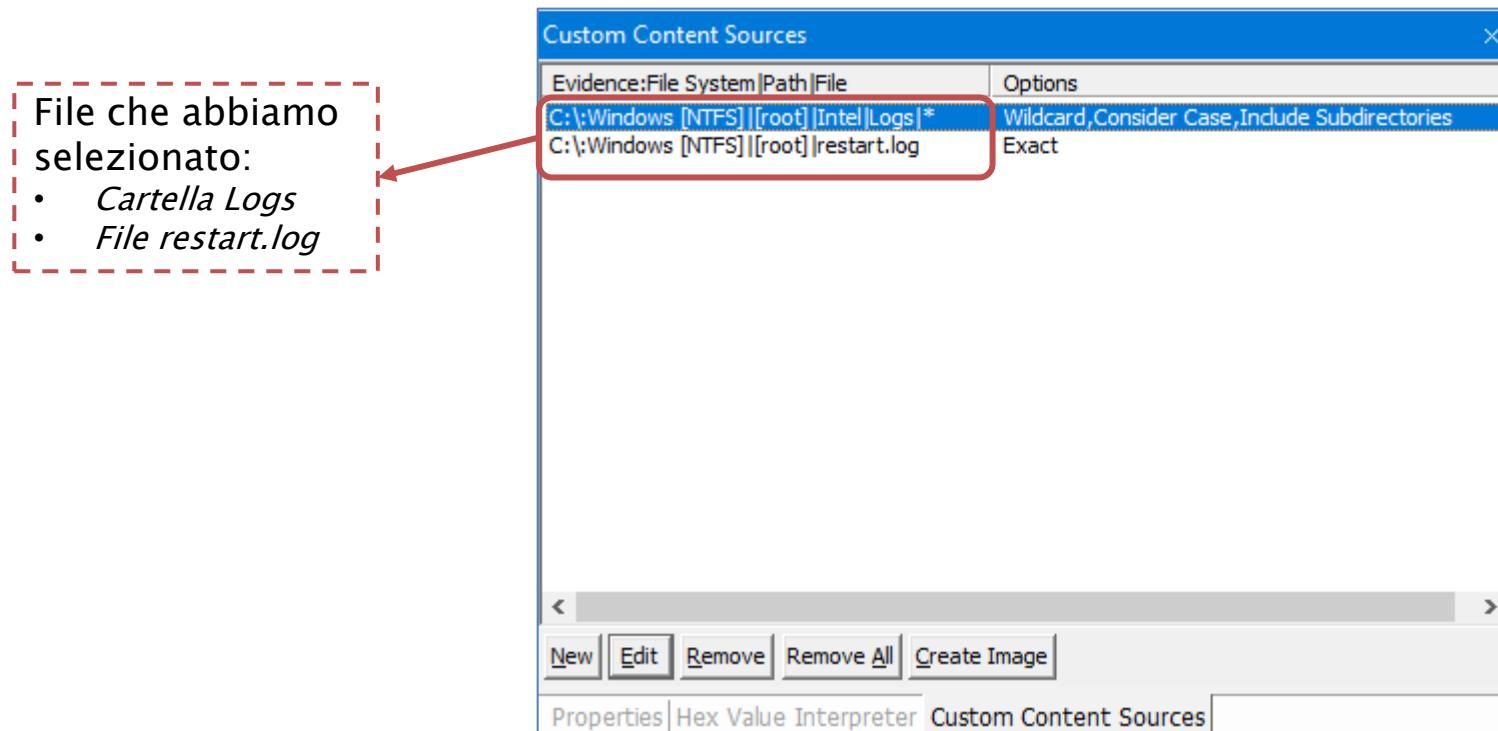
- ▶ Elaborazione di un immagine personalizzata



# Tool di acquisizione

## *FTK Imager: Custom Content Image*

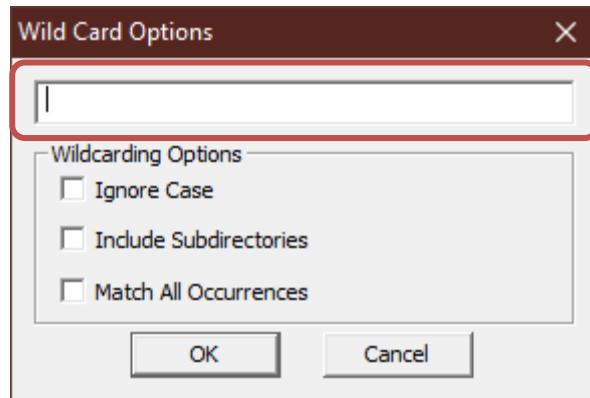
- ▶ Elaborazione di un immagine personalizzata



# Tool di acquisizione

## *FTK Imager: Custom Content Image*

- ▶ Elaborazione di un immagine personalizzata: *Wild Card Options*



Filtro testuale in cui è possibile inserire un percorso di una cartella o un file in formato completo o parziale:  
? = qualunque carattere  
\* = qualunque serie di caratteri  
| (pipe) = separatore di directory e file

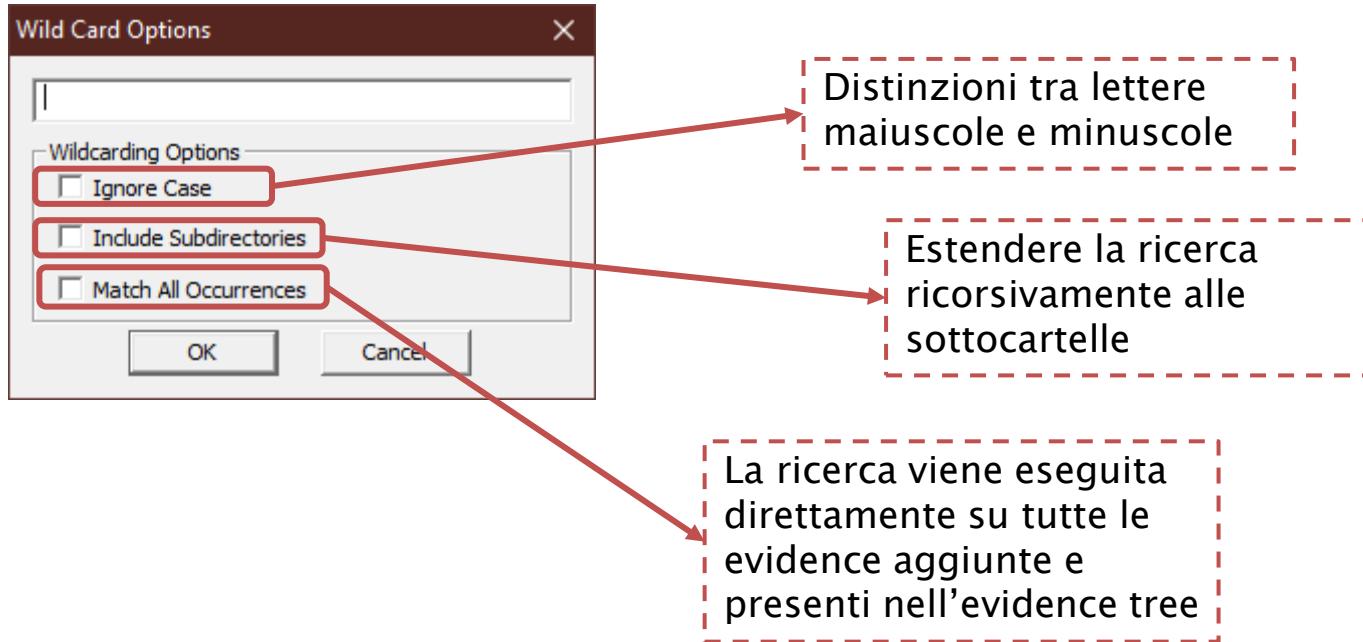
Esempio 1: Documents|\*.doc? => tutti i file Office Word (doc, docx) presenti all'interno di una qualunque cartella denominata «Documents».

Esempio 2: |Microsoft|Outlook|\*.pst => tutti gli archivi di posta elettronica Microsoft Outlook di tutti gli utenti configurati sul sistema

# Tool di acquisizione

## *FTK Imager: Custom Content Image*

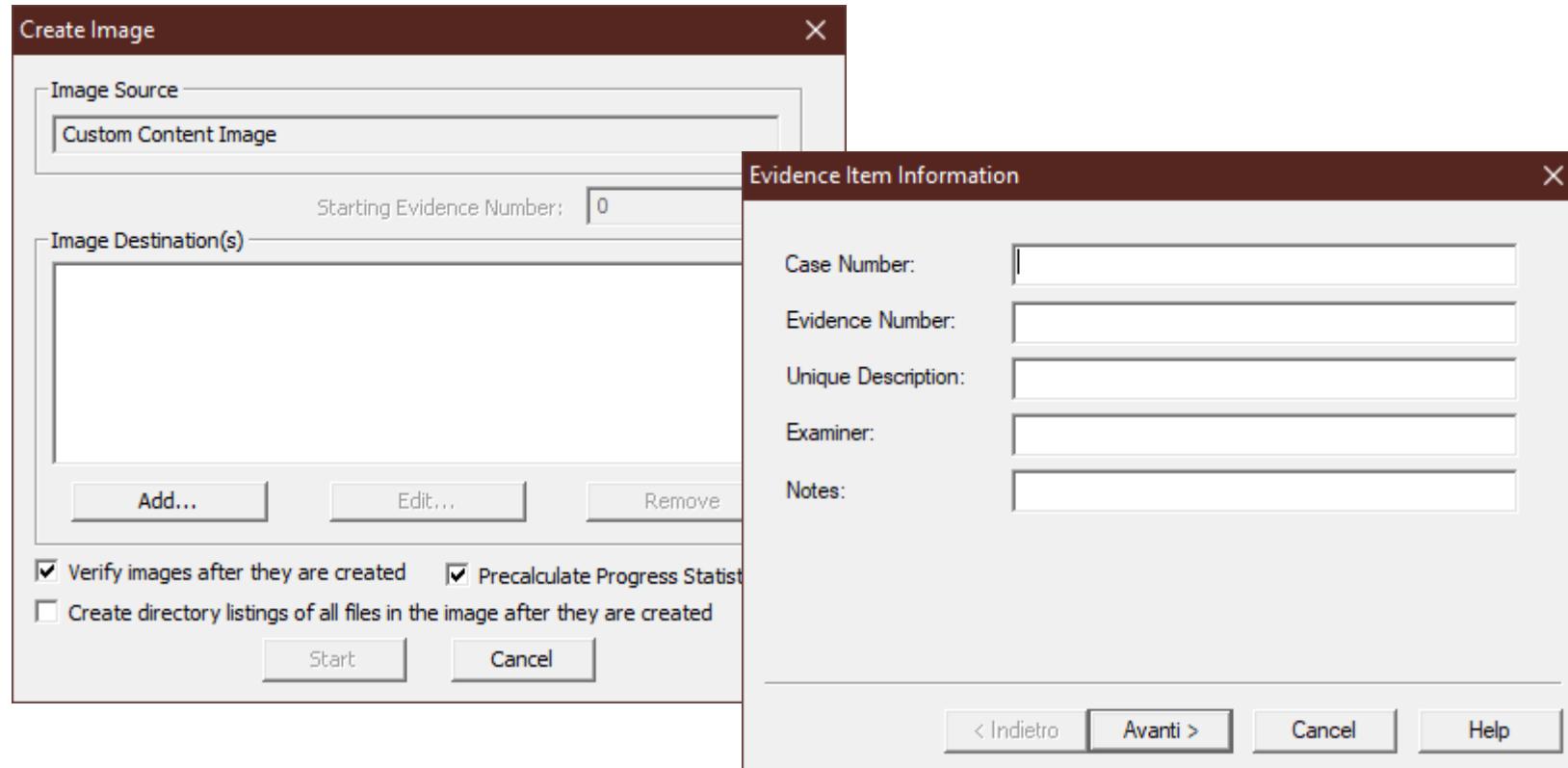
- ▶ Elaborazione di un immagine personalizzata: *Wild Card Options*



# Tool di acquisizione

## *FTK Imager: Custom Content Image*

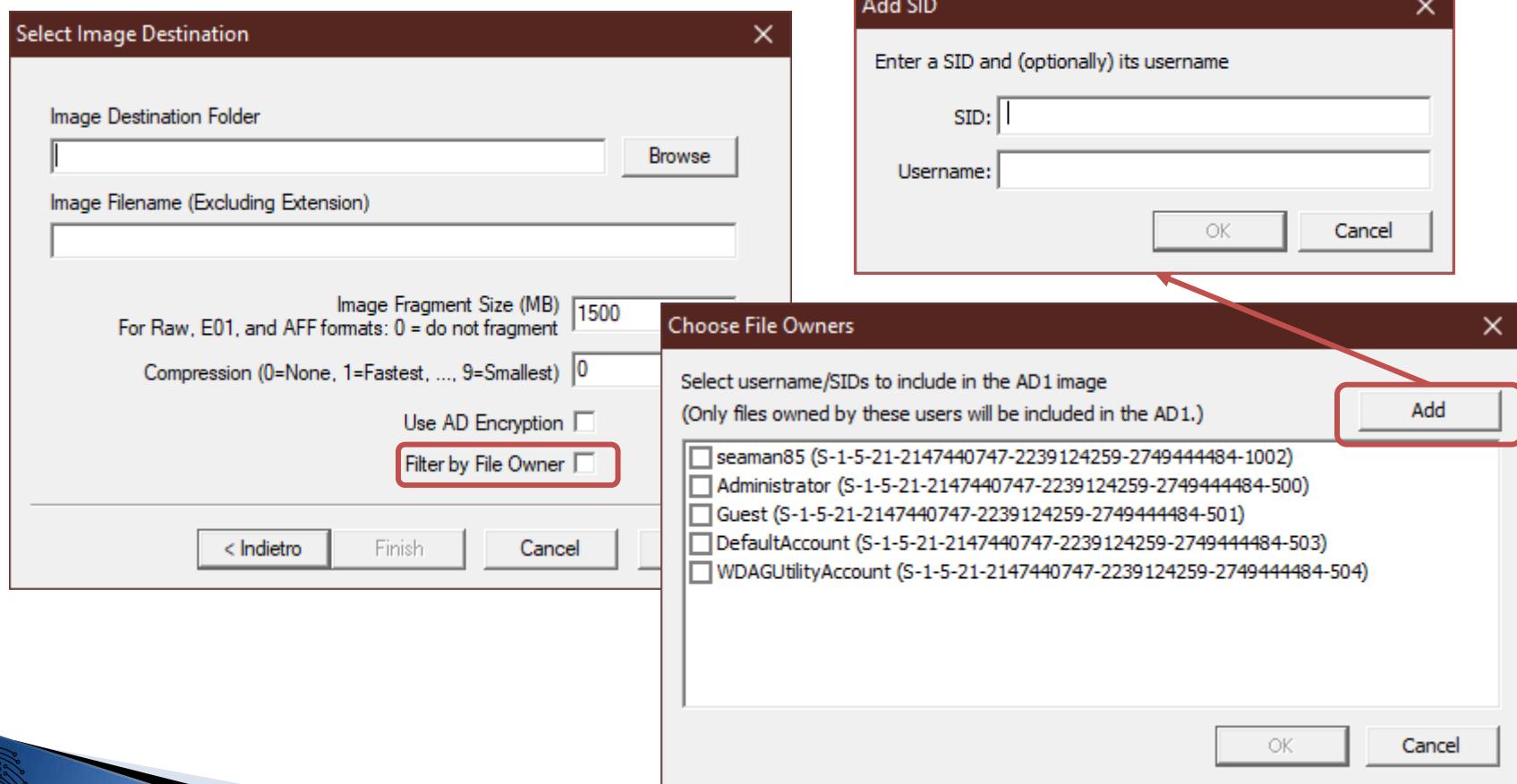
- ▶ Elaborazione di un immagine personalizzata



# Tool di acquisizione

## *FTK Imager: Custom Content Image*

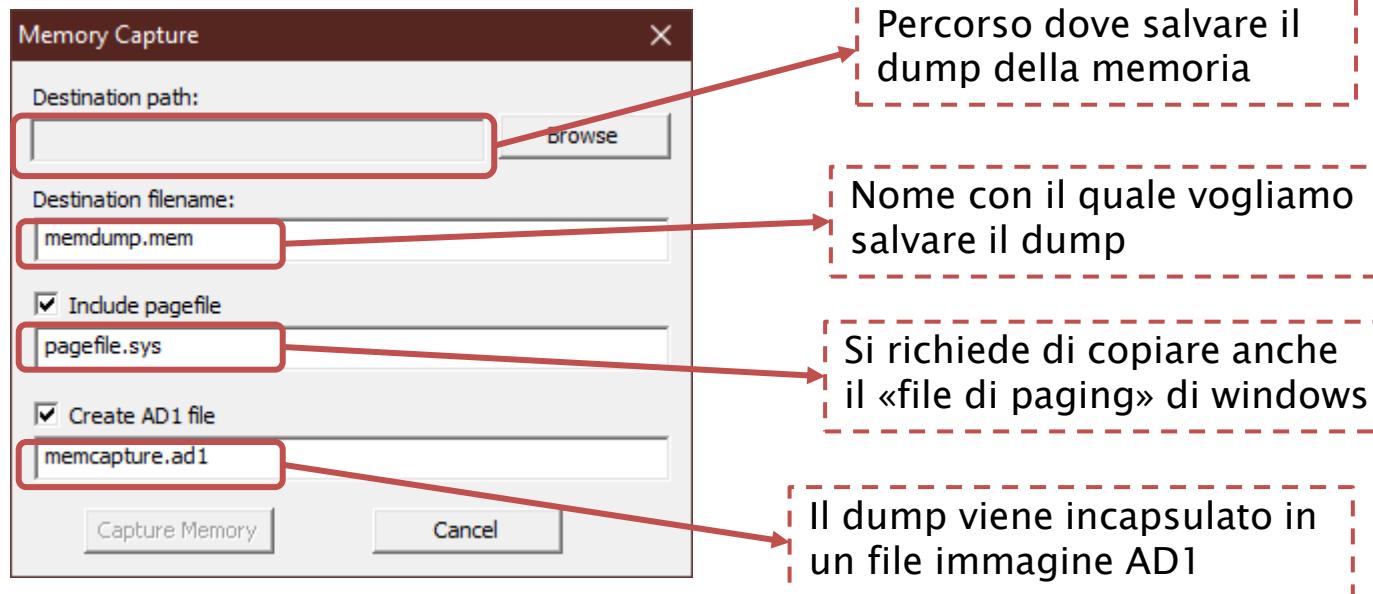
### ▶ Filter by File Owner



# Tool di acquisizione

## *FTK Imager: dump memoria volatile*

### ▶ File>Capture Memory





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 9: Protocolli Crittografici

### *Funzioni di hash*

(1<sup>a</sup> parte)

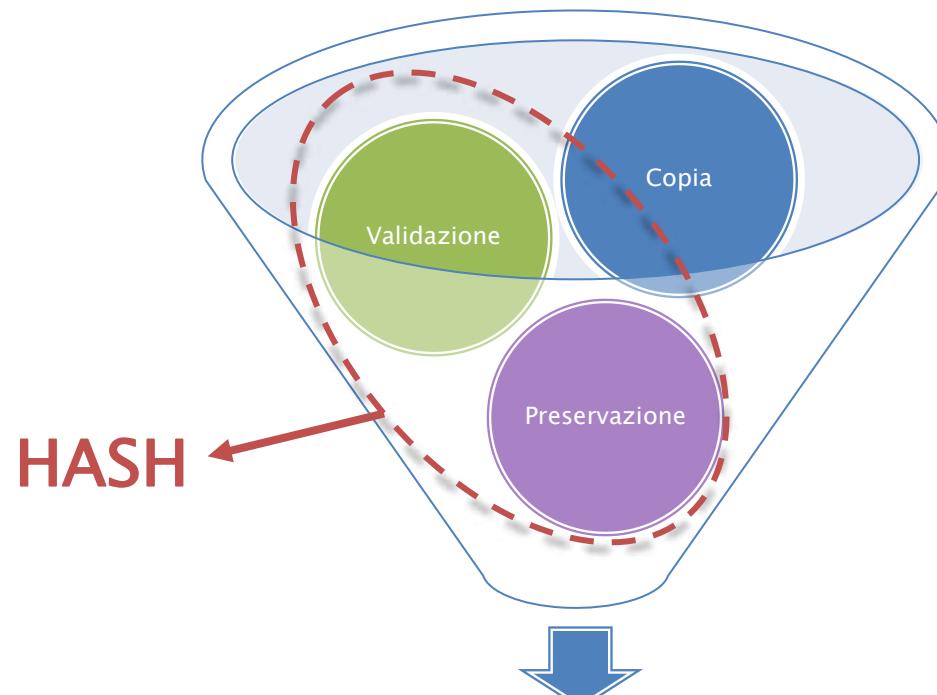


A.A. 2021/22

Dott. Lorenzo LAURATO



# Nella puntata precedente...



Copia Forense

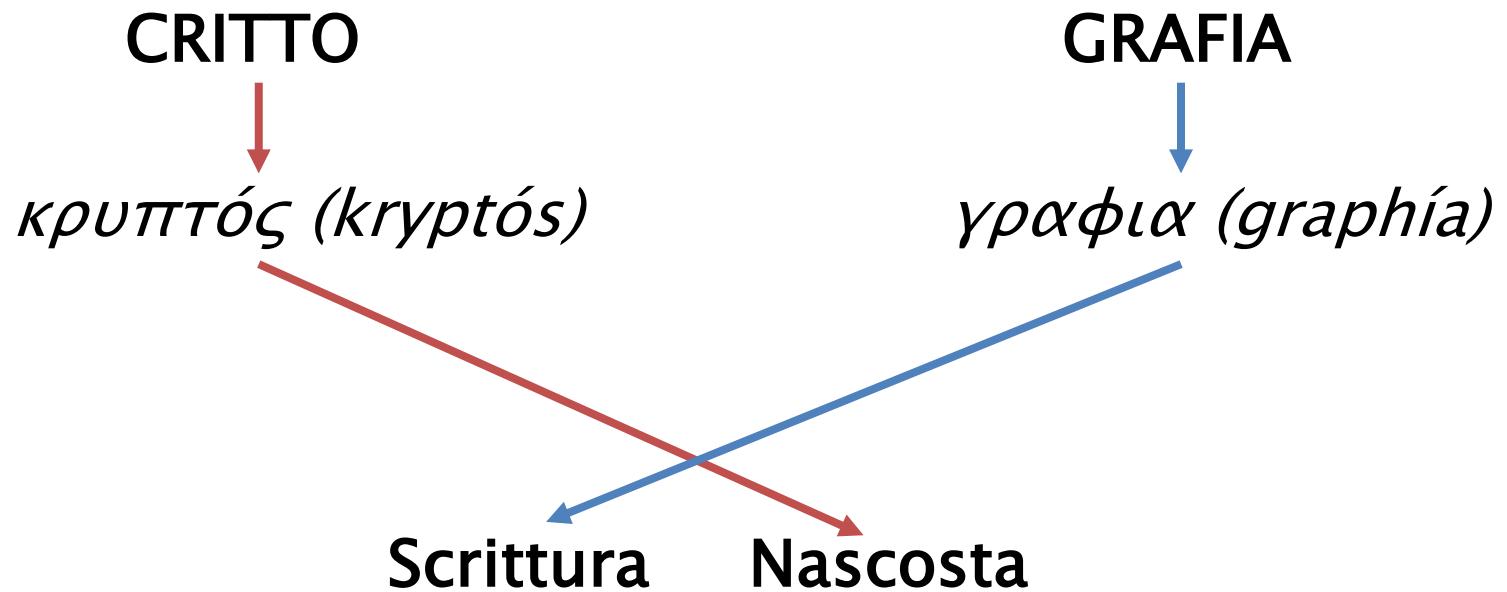
# Crittografia

» Introduzione



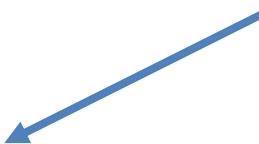
# La crittografia...

- ▶ Rendere oscuro ciò che scrivi o vuoi comunicare.



# La crittologia:

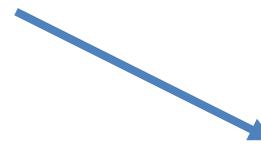
- ▶ scienza che si occupa della comunicazione in forma sicura e di solito segreta.



## Crittografia

studio e applicazione dei principi e delle tecniche per rendere l'informazione inintelligibile a tutti tranne che al destinatario

**VS**



## Crittoanalisi

scienza e arte di risolvere i crittosistemi per recuperare l'informazione nascosta

# La crittografia: storia

## ▶ utilizzo dall'antichità:

- comunicazioni private
- arte/religione
- usi Militari e Diplomatici

# La crittografia: storia

## *scritture segrete*

- ▶ trasformazione delle parole per renderne incomprendibile il significato

### Geroglifico

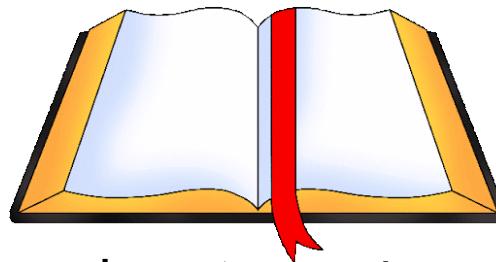


- conferire dignità e onorificenza al defunto (incisione funebre)
- mistero
- senso dell'arcano
- conferire potere magico alle parole

# La crittografia: storia *testi sacri*

## Bibbia

(*tre tecniche di cifratura a sostituzione*)



- ▶ **Atbash:** alfabeto rovesciato (a->Z; b->Y; c->X; ... ; m->N)
- ▶ **Albam:** alfabeto diviso in due metà (a->N;b->O;c->P; ... ;m->Z)
- ▶ **Atbah:** relazione numerica fra le lettere (a=1; b=2; ...; z=26)
  - Prime 9 lettere (a-i): 10 - lettera => lettera sostituente;
  - Successive 9 lettere (j-s): 28 - lettera => lettera sostituente;
  - Ultime 8 lettere (t-z): 45 - lettera => lettera sostituente

# La crittografia: storia

## *cifrario di Cesare*

- ▶ lettera di Cesare a Cicerone (100-44 a.c.)

RPQLD JDOOLD HVW GLYLVD LQ  
SDUWHV WUHV



- *cifratura a sostituzione*
- relazione numerica fra le lettere (A=1; B=2; ...; Z=26)

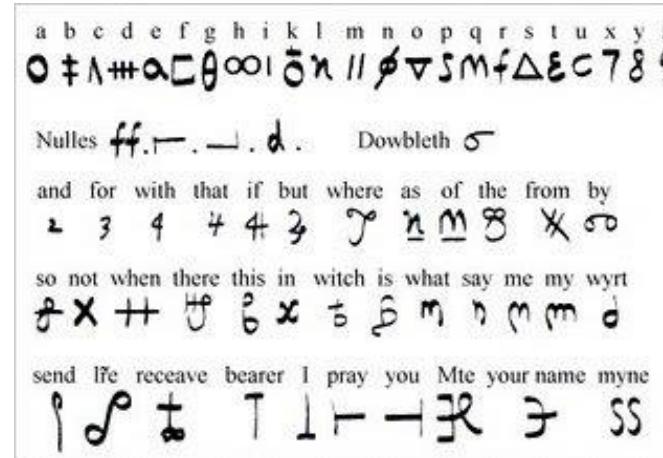
$$C(M_i) \Rightarrow M_{i+3} \bmod 26$$

OMNIA GALLIA EST DIVISA IN  
PARTES TRES

# La crittografia: storia *congiura di Babington*

- ▶ Maria Stuarda (Regina di Scozia) e Anthony Babington stavano cospirando contro Elisabetta I
- ▶ I messaggi venivano nascosti in botti di birra e cifrati:

- *Lettera = Simbolo;*
- *Simbolo = doppia lettera;*
- *4 simboli falsi;*
- *35 simboli per parole/frasi;*



- ▶ Il corriere (Gilbert Gifford) consegnava i messaggi anche al nemico, poi decifrati da Thomas Phelippes;

# La crittografia: storia *macchina cifrante*

## ENIGMA

*(dispositivo elettromeccanico per cifrare e decifrare messaggi)*



- ▶ Sviluppata da Arthur Scherbius [1918]
- ▶ Usata nella II Guerra Mondiale dai tedeschi.
- ▶ Decifrata nel 1932 da un gruppo di matematici polacchi.

# La crittografia: storia *i tre stadi*

## ▶ Primo stadio

- Dalle prime civiltà fino al secolo scorso
- Algoritmi sviluppati e implementati “a mano”

## ▶ Secondo stadio

- Seconda guerra mondiale
- Apparizione delle prime macchine cifranti

## ▶ Terzo stadio

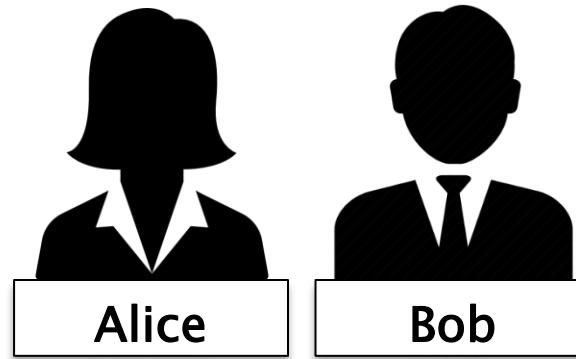
- Ultimi 50 anni
- Utilizzo di computer
- Fondamenti matematici

# La crittografia: storia *età moderna*

- ▶ Avvento dei computer come strumento di calcolo:
  - nuovi algoritmi di crittografia;
  - nuove tecniche di crittoanalisi;
- ▶ nuovi campi di applicazione
- ▶ è fondata su solide basi matematiche
- ▶ si occupa anche del progetto e della valutazione di metodi e tecniche per la protezione dell'informazione

# La crittografia: protocolli

- ▶ Un protocollo o schema definisce le interazioni fra le parti per ottenere le proprietà di sicurezza desiderate.
- ▶ Parti: entità coinvolte nello schema;



- ▶ Proprietà di sicurezza: segretezza, autenticità

# La crittografia: primitive

- ▶ I protocolli di basano su una serie di protocolli più semplici detti primitive crittografiche:
  - risolvono problemi “facili”
  - possono essere usate per risolvere problemi più complessi
- ▶ Fonti:
  - Costrutti (*Es. DES*) ;
  - Problemi matematici (*Es. teoria dei numeri*) ;

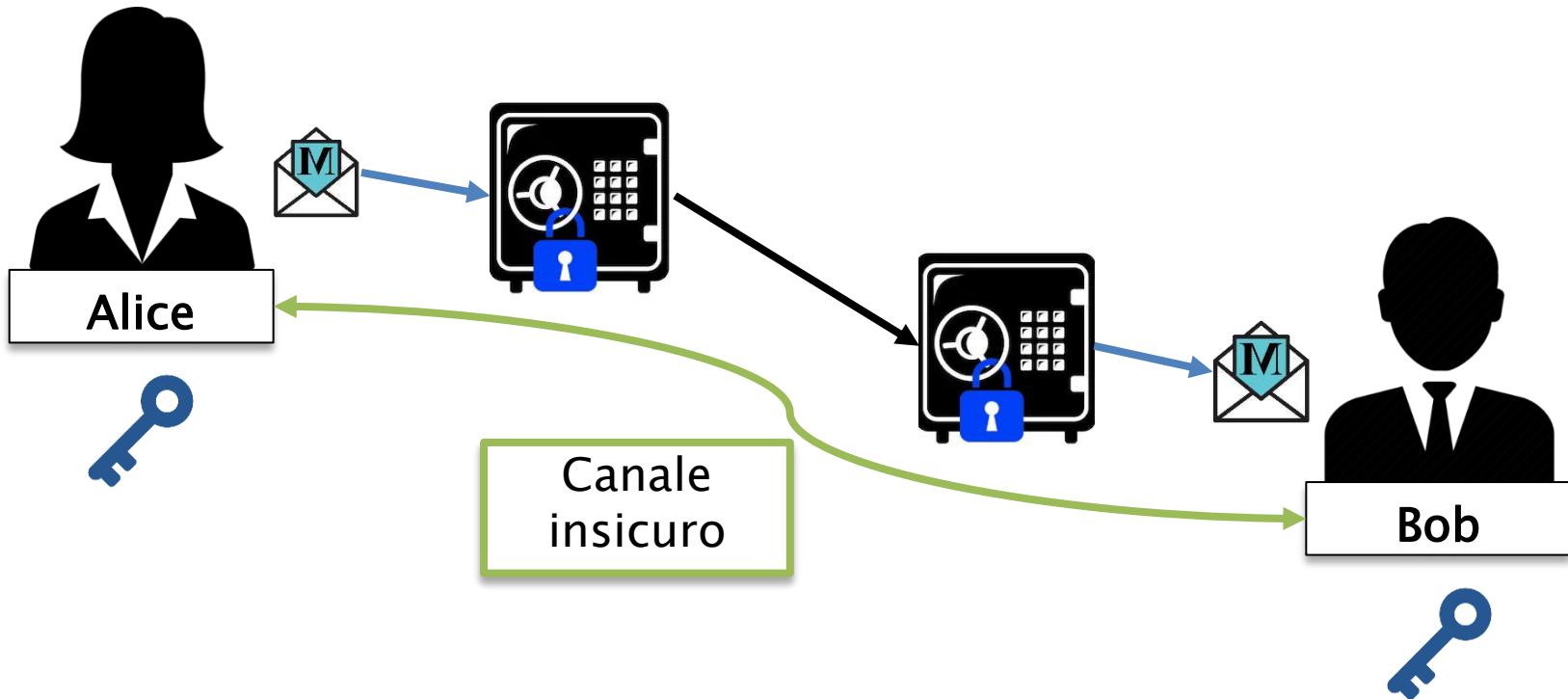
# La crittografia: primitive

▶ risolvono i seguenti problemi:

- Cifratura: *cifrari simmetrici o asimmetrici o a chiave pubblica;*
- Autenticazione ed integrità: *Funzioni Hash e MAC*
- Firme digitali
- Altro: *generazione di numeri pseudo-casuale, prove zero-knowledge, etc.*

# Le primitive crittografiche

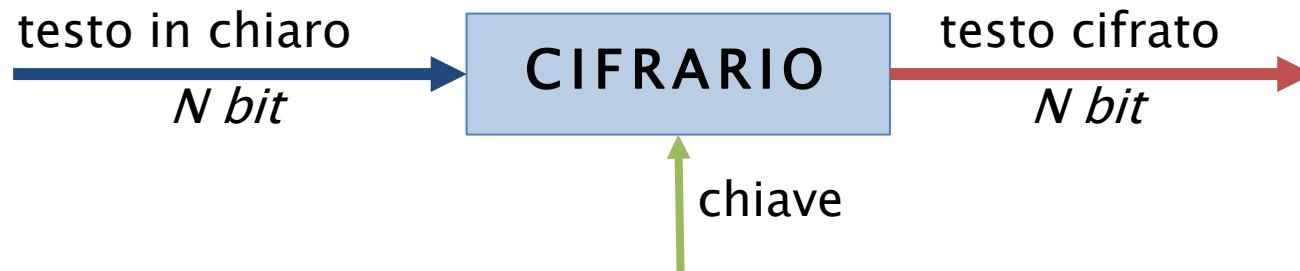
## *cifrario simmetrico*



Condividono la stessa chiave

# Le primitive crittografiche

## *cifrario simmetrico*

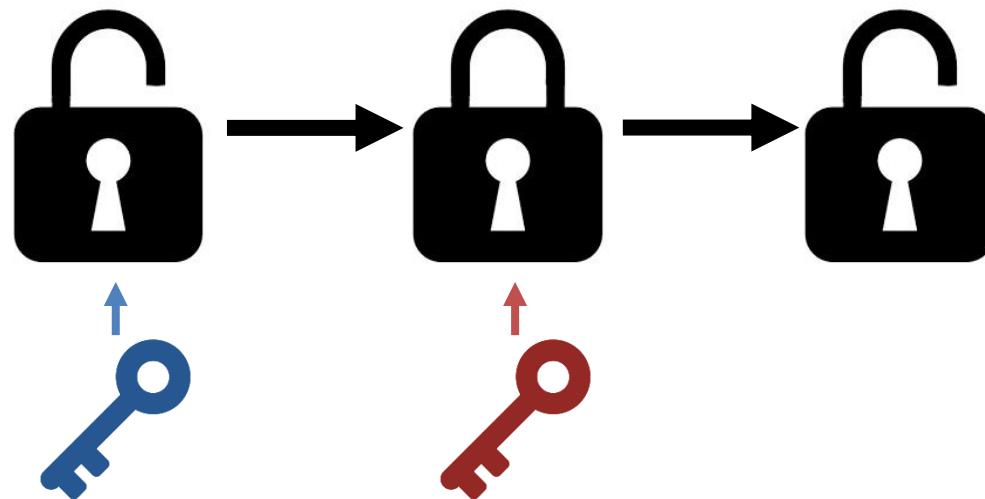


- ▶ Data Encryption Standard (DES)
  - *DES triplo, modalità di cifratura*
- ▶ RC2, RC4, RC5, RC6
- ▶ Advanced Encryption Standard (AES)
- ▶ Blowfish

# Le primitive crittografiche

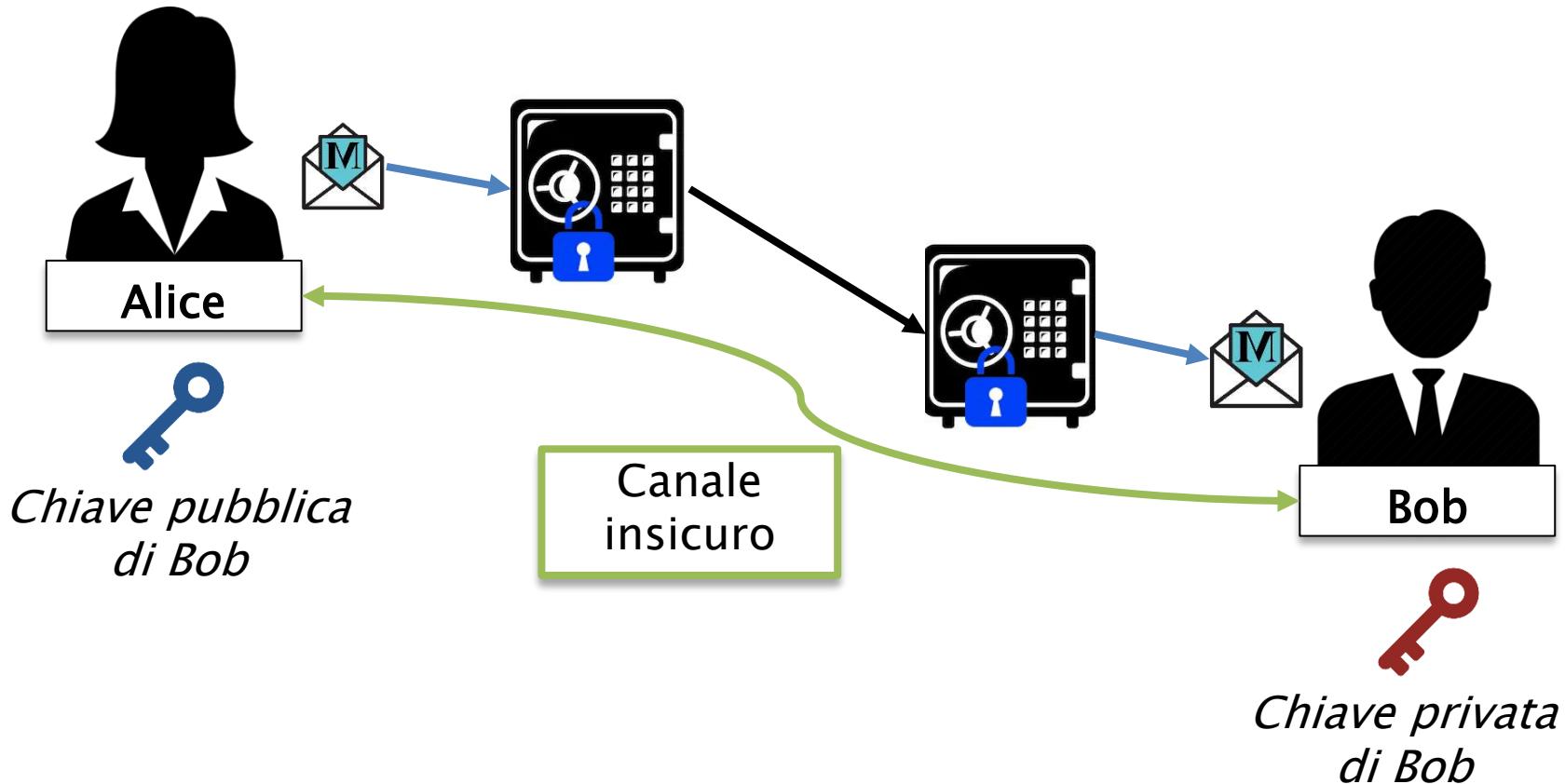
## *cifrario asimmetrico*

- ▶ Si impiegano due chiavi differenti:
  - **Chiave Pubblica**: impiegata per cifrare
  - **Chiave Privata**: impiegata per decifrare



# Le primitive crittografiche

## *cifrario asimmetrico*



# Le primitive crittografiche

## *firma digitale*

- ▶ *Apposizione di una firma ad un documento digitale*
- ▶ **Proprietà:**
  - La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario.
  - Nessun utente deve poter riprodurre la firma di altri.
  - Chiunque può facilmente verificare una firma
- ▶ **Algoritmi:**
  - RSA
  - Digital Signature Standard (DSS)



# Le primitive crittografiche

## *funzione hash*

- ▶ il valore hash  $h(M)$  è una rappresentazione non ambigua e non falsificabile del «*messaggio M*»



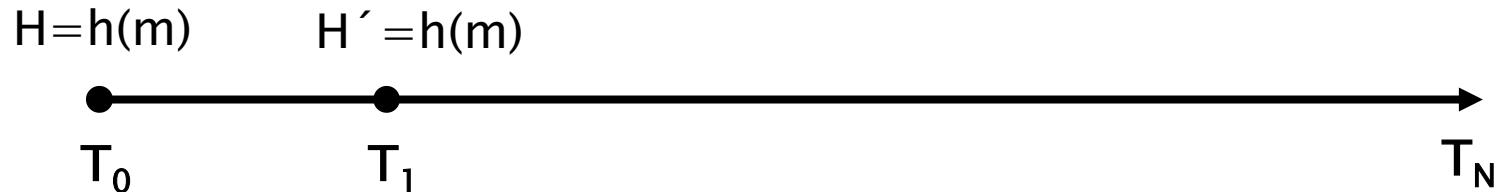
- ▶ **Impiego:**
  - Firma digitale
  - Integrità dei dati
  - Certificazione del tempo

# Le primitive crittografiche

## *funzione hash (integrità)*

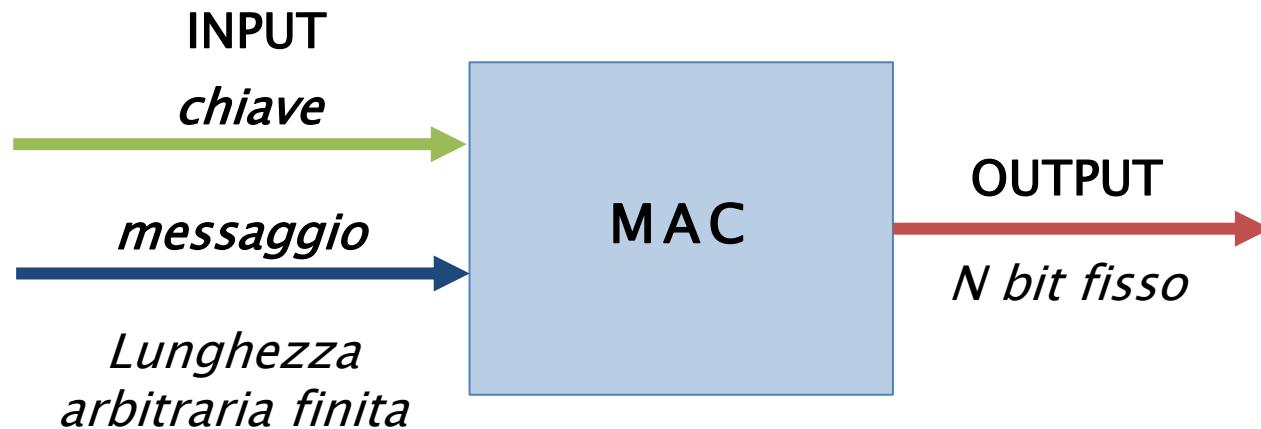
- ▶ Computo al **tempo  $T_0$**  il valore hash del file  $M$ :  $H = h(M)$
- ▶ Per controllare se il file è stato successivamente modificato:
  - al **tempo  $T_1$**  calcolo:  $H' = h(M)$ ;
  - verifico se  $H' = H$ ;

$h(M)$  è l'impronta digitale del file



# Le primitive crittografiche

## *funzione Message Authentication Code (MAC)*



- ▶ **Impiego:**
  - Integrità dei dati
  - Autenticità dei dati: verificare chi è stato il mittente dei dati

# Le primitive crittografiche

## *proprietà di sicurezza*

- ▶ **Confidenzialità:** protezione del dato da uno soggetto estraneo
- ▶ **Autenticazione:** certezza di indentificare l'interlocutore
- ▶ **Integrità:** verificare che il messaggio non è stato modificato durante la trasmissione.
- ▶ **Non-ripudio:** negare il disconoscimento del messaggio al mittente o al destinatario;
- ▶ **Anonimia:** nascondere l'identità di chi a compiuto una determinata azione nel contesto crittografico.

# Le primitive crittografiche

## *proprietà di sicurezza: confidenzialità*

Privacy

Segretezza



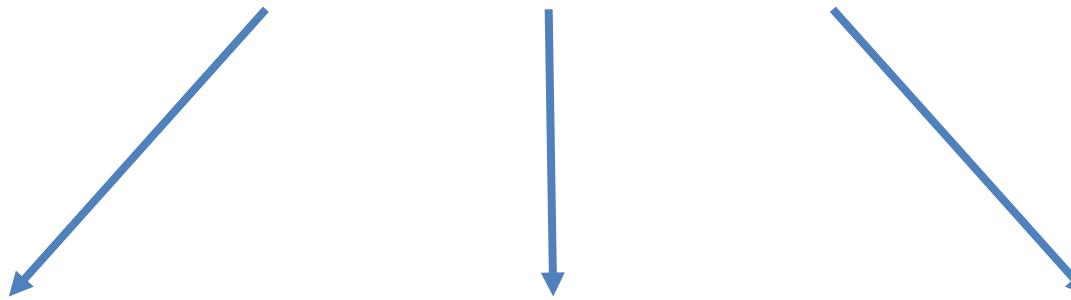
Protezione dell'informazione trasmessa dall'accesso da soggetti non autorizzati



Sistema di cifratura simmetrici/asimmetrici

# Le primitive crittografiche

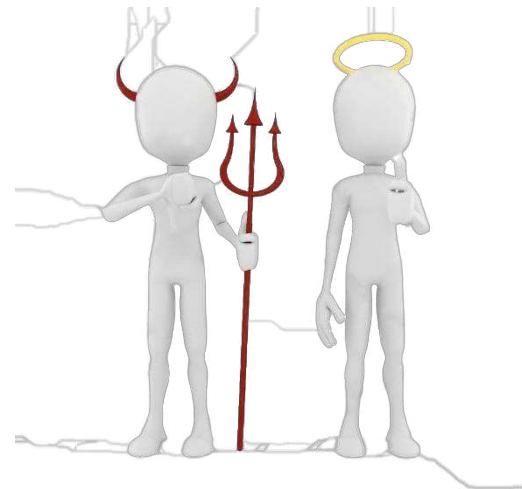
## *proprietà di sicurezza: autenticazione*



Origine del messaggio



Soggetto\Entità  
con il quale si sta  
interloquendo



Temporale



# Le primitive crittografiche

## *proprietà di sicurezza: integrità*

- ▶ Solo chi è autorizzato può modificare l'attività di un sistema o le informazioni trasmesse

scrittura, cambiamenti,  
cancellazione, creazione,  
ritardi, replay e  
riordino di messaggi, etc.

# Le primitive crittografiche

## *proprietà di sicurezza: non ripudiabilità*

- ▶ è impossibile negare l'occorrenza di una determinata azione



# Le primitive crittografiche

## *proprietà di sicurezza: anonimia*



- ▶ proteggere l'identità di chi sta utilizzando un servizio o proteggere l'accesso al servizio stesso: **grado di anonimia**

# Hash

» MD4/5 e SHA1



# Funzione Hash

- il valore hash  $h(M)$  è una rappresentazione non ambigua e non falsificabile del «*messaggio M*»



Integrità dei dati

# Funzione Hash

## *collisione*

$$h: \Sigma^* \rightarrow \Sigma^n$$

$$h(m_1) = h(m_2)$$



Esistono infinite collisioni

# Funzione Hash

## *proprietà*

- ▶ **One-way (*pre-image resistant*):**
  - dato un *hash*  $y$ , è computazionalmente difficile trovare  $M \mid y=h(M)$
- ▶ **Sicurezza debole (*2nd pre-image resistance*):**
  - dato  $M$ , è computazionalmente difficile trovare una variazione di  $M$ ,  $M' \mid h(M)=h(M')$
- ▶ **Sicurezza forte (*collision resistance*):**
  - computazionalmente difficile trovare 2 diversi messaggi con lo stesso valore hash

# Funzione Hash

## *definizioni*

- ▶ **Una One-Way Hash Function (OWHF):**
  - verifica le proprietà pre-image e 2nd pre-image resistant;
  - viene detta *weak one-way hash function*
- ▶ **Una Collision Resistant Hash Function (CRHF):**
  - verifica la proprietà di collision resistance
  - viene detta *strong one-way hash function*

# Funzione Hash

## *costruzione*

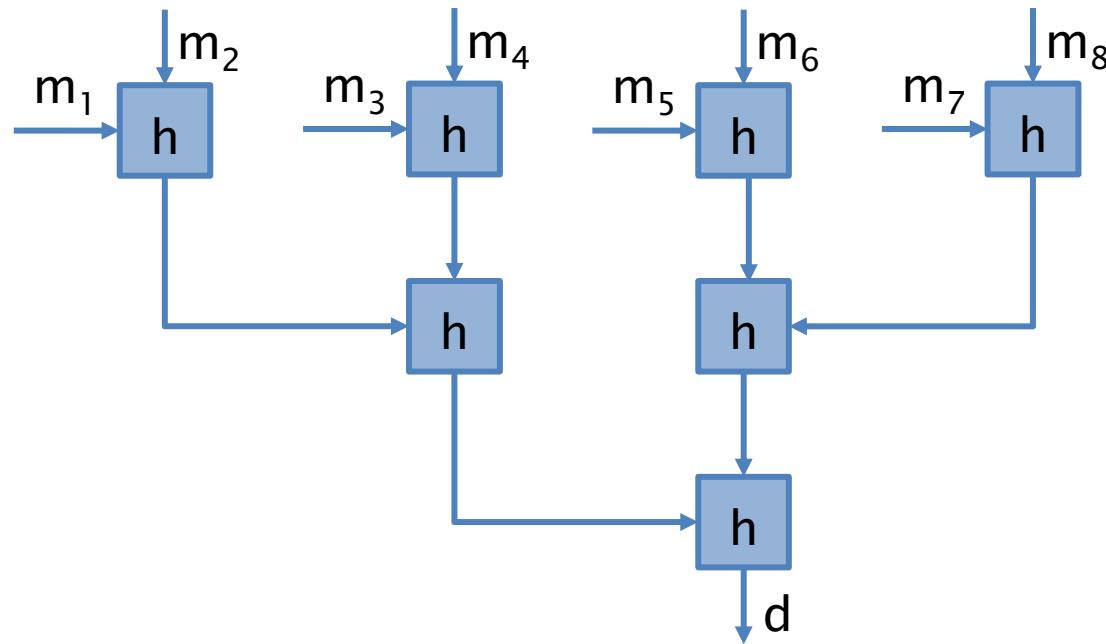
Messaggi di lunghezza arbitraria sono trattati utilizzando hash con input fisso:

- ▶ il messaggio input  $M$  viene diviso in  $k$  blocchi di lunghezza fissa:  $m_1, m_2, \dots, m_k$
- ▶ i blocchi vengono trattati in modo:
  - seriale/iterato
  - parallelo

# Funzione Hash

## *costruzione*

### Modello hash parallelo

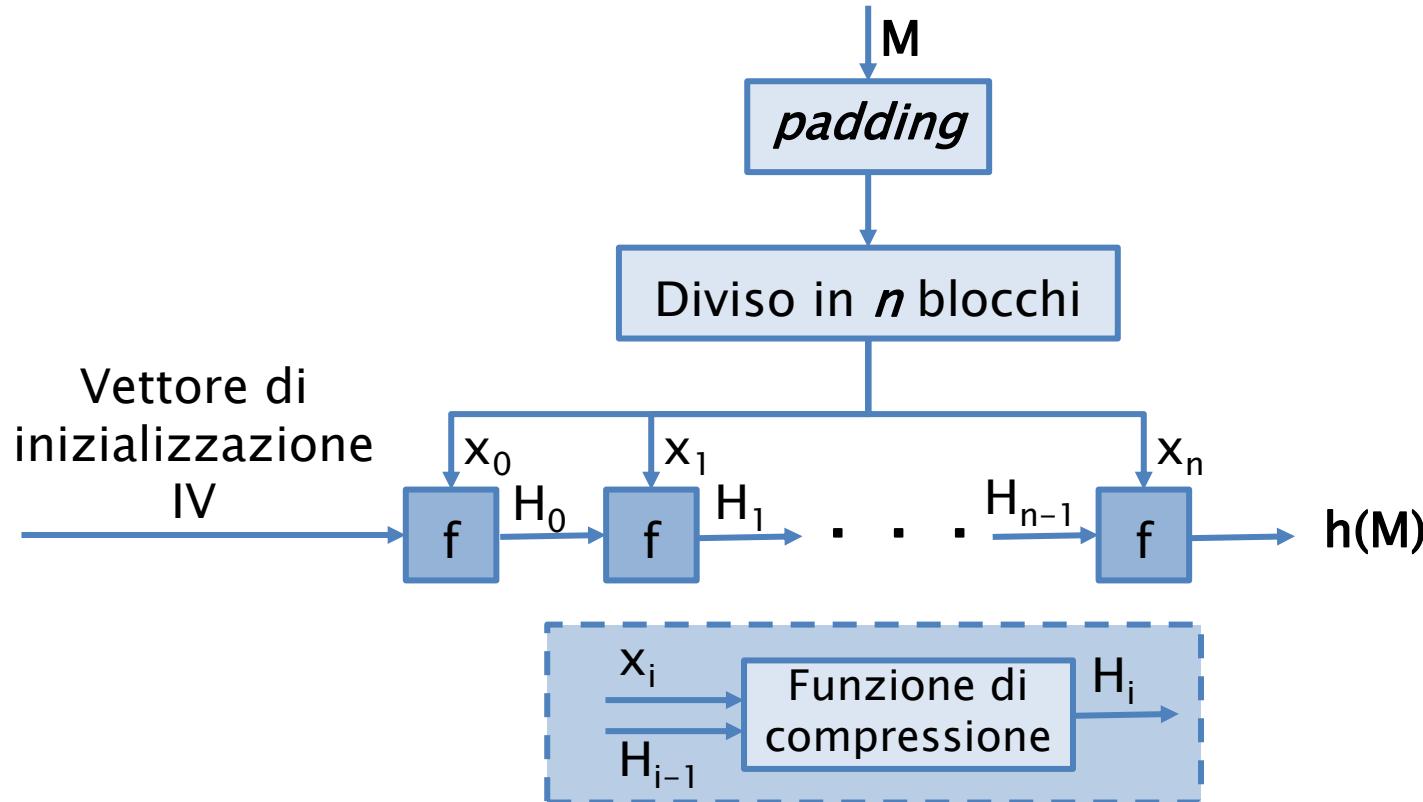


*È resistente alle collisioni se lo è la funzione h*

# Funzione Hash

## *costruzione*

### Modello hash iterato

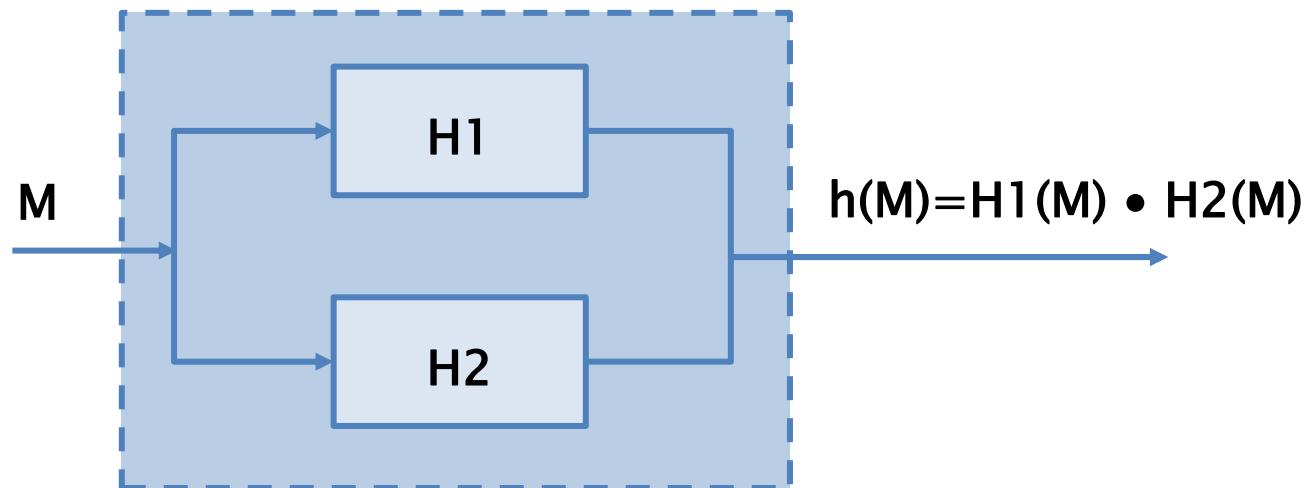


*una collisione per  $h(M)$  implica una collisione di  $f$*

# Funzione Hash

## *costruzione*

### Modello hash cascata



una collisione per  $h(M)$  vuol dire trovare  
una collisione sia per  $H1$  che per  $H2$

# Funzione Hash

## *costruzione*

### Cifrari a blocchi

- ▶ Cifrario a blocchi  $E_k$  (•) per input ad  $n$  bit
  - ▶ Funzione  $g$  che da  $n$  bit produce una chiave
    - $M'_1 \dots M'_{t'}$  : è il messaggio  $M$  con eventuale *padding*
    - $H_0$  : è una costante predefinita
    - $H_t$  : è il valore hash
- 
- $H_i = E_{g(H_{i-1})} (M'_i) \oplus M'_i$  [Matyas–Meyer–Oseas]
  - $H_i = E_{g(H_{i-1})} (M'_i) \oplus M'_i \oplus H_{i-1}$  [Miyaguchi–Preneel]
  - $H_i = E_{M'_i} (H_{i-1}) \oplus H_{i-1}$  [Davies–Meyer]

# Fine prima parte...



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# Lezione 11: Question Time



A.A. 2019/20  
**Dott. Lorenzo LAURATO**



# Domanda nr. 01



Nella fase di identificazione, la preview...

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> è una perquisizione informatica                      | ✓ |
| <input type="checkbox"/> è una fase in cui non vi è alcun rischio di alterare il reperto | ✗ |
| <input type="checkbox"/> deve essere sempre eseguita su un sistema spento                | ✗ |
| <input type="checkbox"/> non possono essere accesi i dispositivi rinvenuti spenti        | ✗ |

# Legge n. 48 del 18/03/2008

## *art. 247 c.p.p.*

*(Casi e forme delle perquisizioni)*

[...]

*1bis Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

[...]

# Identificazione dell'evidence

## *la «preview»*

- ▶ Consente di eseguire un'analisi di primo livello delle memorie dei dispositivi allo scopo di individuare possibili elementi di interesse investigativo.
- ▶ utilizzo di **write blocker** (*software/hardware ad hoc*)
- ▶ rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova;

# Domanda nr. 02

la preview in un sistema acceso (LIVE)

- può essere eseguita con una distro live forensic oriented ✗
- rende veloce l'analisi dei software presenti nel sistema; ✓
- può essere eseguito con qualsiasi tool forensic oriented indipendentemente dal sistema da analizzare ✗
- è consigliabile eseguirla con un write blocker ✗



# Identificazione dell'evidence

## *la «preview»*

### LIVE

- ▶ è un'analisi eseguita impiegando il S.O. presente sul dispositivo da analizzare;
- ▶ deve essere documentata e verbalizzata;
- ▶ **PRO:**
  - consente di avere una visione dell'ambiente in cui opera l'utente;
  - è veloce nell'analisi dei software installati;
- ▶ **CONTRO:**
  - Alterazione del reperto
  - Strumenti adeguati al sistema

# Identificazione dell'evidence

*la «preview»*

## DEAD

### ▶ PRO:

- Permette di non alterare il dispositivo;
- Consente di utilizzare diversi strumenti per analizzare la memoria del dispositivo.

### ▶ CONTRO:

- Buona conoscenza del sistema e dei software da analizzare
- Non sempre praticabile: sistemi embedded;

# Domanda nr. 03



il sequestro fisico...

- |                                     |  |   |
|-------------------------------------|--|---|
| <input type="checkbox"/>            | viene eseguito elaborando la copia forense         | ✗ |
| <input type="checkbox"/>            | è sempre possibile eseguirlo                       | ✗ |
| <input checked="" type="checkbox"/> | bisogna preoccuparsi del problema dello "shutdown" | ✓ |

# La Raccolta: *il sequestro fisico*

- ▶ Prendere semplicemente il supporto contenente i dati, posticipando le problematiche derivanti dall'acquisizione del dato;
- ▶ Preoccuparsi solo di identificare e verbalizzare i reperti:
  - *Catena di custodia (Chain of Custody)*



# La Raccolta: *il sequestro fisico*

non è sempre fattibile

- ▶ sistemi che non possono essere fermati/spenti;
- ▶ sistemi distribuiti su decine di rack;

# Domanda nr. 04

il sequestro logico...

- |                                     |  |   |
|-------------------------------------|--|---|
| <input checked="" type="checkbox"/> | viene eseguito elaborando la copia forense         | ✓ |
| <input checked="" type="checkbox"/> | è sempre possibile eseguirlo                       | ✓ |
| <input type="checkbox"/>            | bisogna preoccuparsi del problema dello "shutdown" | ✗ |



# La Raccolta: *il sequestro logico*

- ▶ Duplicazione dei dati di [*possibile*] interesse investigativo;



## COPIA FORENSE

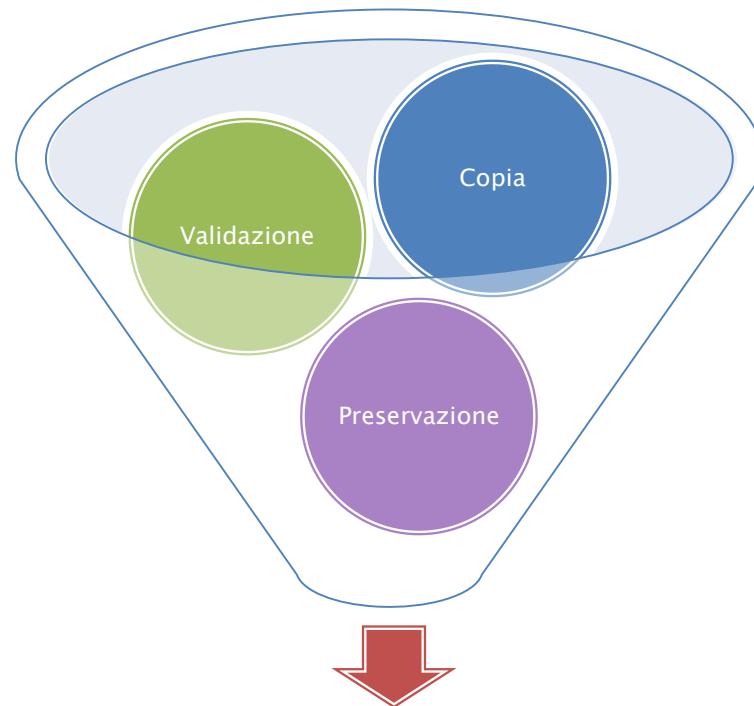
# Domanda nr. 05

La copia forense è...

- una duplicazione dei dati di interesse investigativo ✗
- una copia "bit a bit" dell'intero supporto di memoria ✗
- una qualunque copia di dati che rispetta le caratteristiche di validazione e preservazione ✓
- una duplicazione dei dati eseguita in modo tale da garantire la ripetibilità dell'operazione ✗



# La Raccolta: *Copia Forense*



**Copia Forense**

# Domanda nr. 06

Per validazione si intende che

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> l'hash della copia forense coincide con l'hash calcolato dal supporto originale            | ✓ |
| <input type="checkbox"/> l'hash della copia forense coincide con l'hash calcolato da una successiva copia forense              | ✗ |
| <input type="checkbox"/> l'hash della copia forense coincide con quello calcolato dalla medesima copia dopo la fase di analisi | ✗ |
| <input checked="" type="checkbox"/> i dati della copia forense sono identici ai dati originali                                 | ✓ |

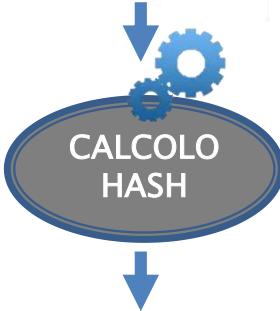


# Copia Forense

## *hash*

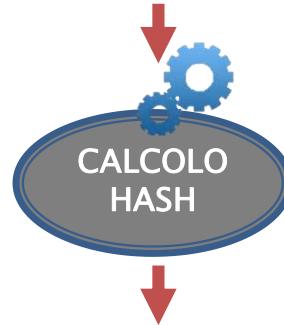
- ▶ **Validazione:** garantisce che la copia eseguita è identica al dato originale.

Disco di Origine X



555F1D268BBE1D6  
5255E1176DD8C66E

Disco di Destinazione Y



555F1D268BBE1D6  
5255E1176DD8C66E

# Domanda nr. 07



Per preservazione si intende che

- l'hash della copia forense coincide con quello calcolato dalla medesima copia dopo la fase di analisi ✓

- la copia forense sarà immodificabile ✗

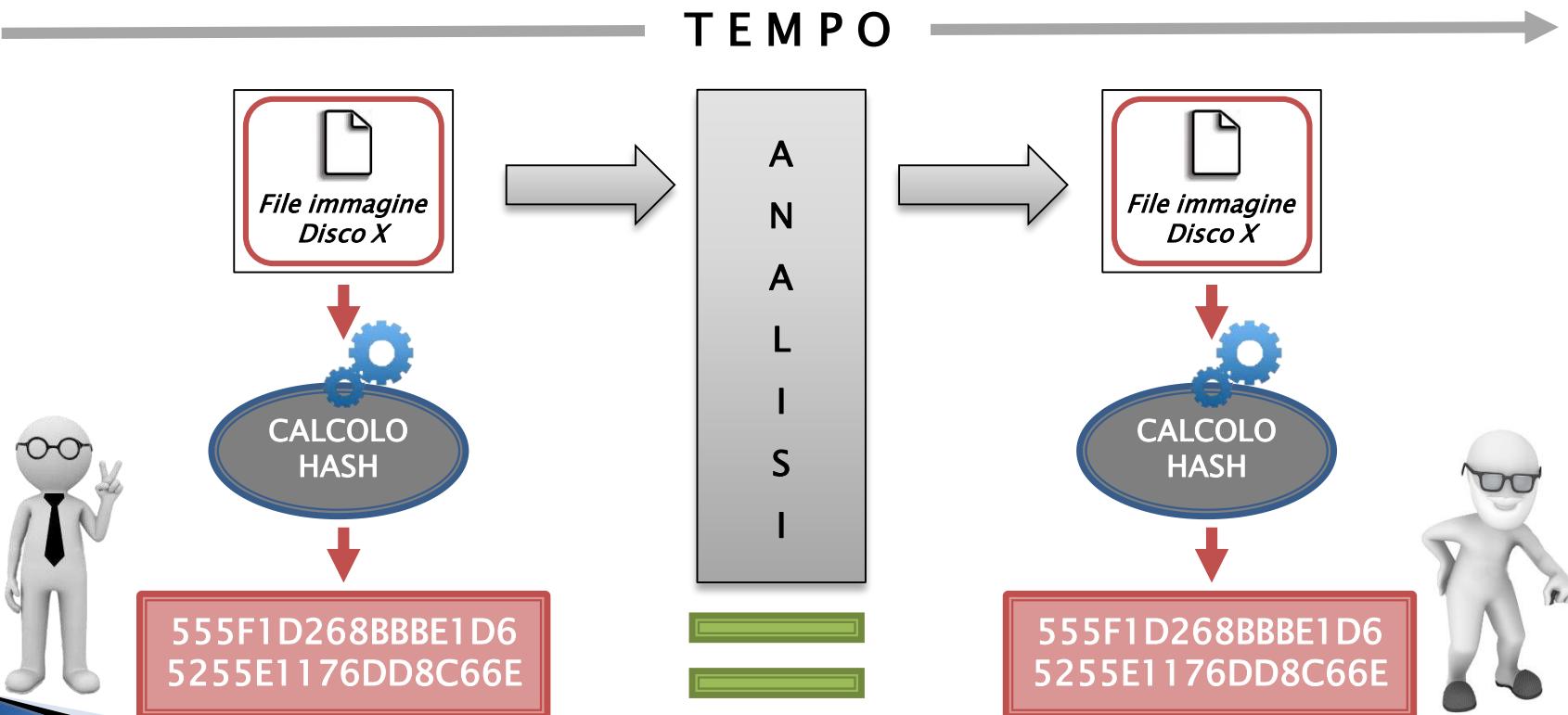
- l'hash della copia forense coincide con l'hash calcolato da una successiva copia forense ✗

- l'hash delle copia forense varierebbe alla minima alterzione della copia stessa ✓

# Copia Forense

## *hash*

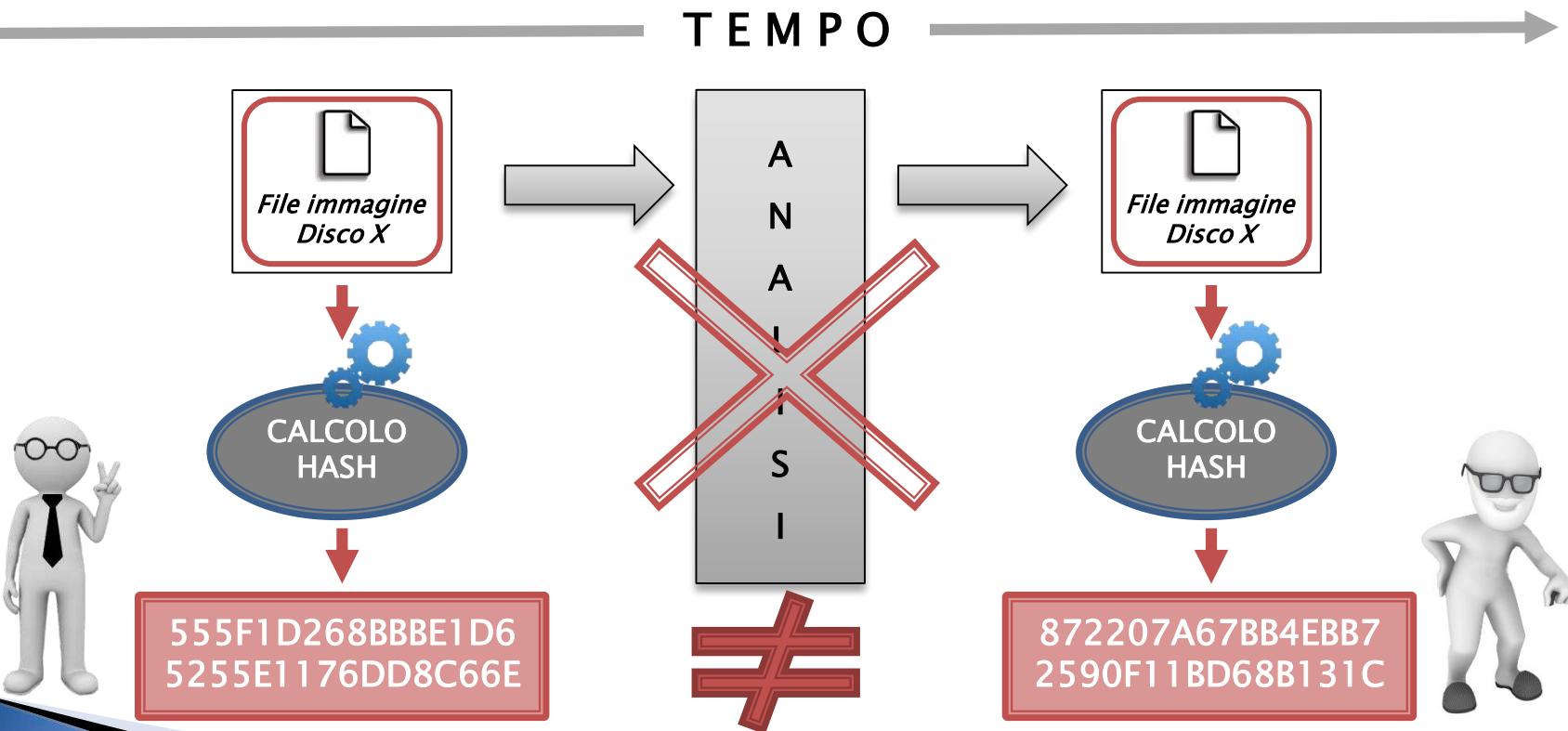
- ▶ **Preservazione:** garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



# Copia Forense

## *hash*

- ▶ **Preservazione:** garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



# Domanda nr. 08



## il comando DD

- |                                     |   |   |
|-------------------------------------|---|---|
| <input type="checkbox"/>            | da solo permette di produrre una copia forense                                  | ✗ |
| <input type="checkbox"/>            | garantisce la non alterazione del disco sorgente                                | ✗ |
| <input checked="" type="checkbox"/> | esegue una copia bit a bit di un supporto di memoria generando un file immagine | ✓ |
| <input checked="" type="checkbox"/> | permette di eseguire una copia di un solo file                                  | ✓ |

# Copia Forense

## comando «*DD*»

### ▶ Eseguiamo la copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

IF = input file [*disco sorgente «sda»*]

OF = output file [*file immagine «sda.dd»*]

BS = block size in byte (default 512) [*dimensione del blocco di lettura «2048 byte»*]

CONV = esegue l'elaborazione in base ai parametri indicati

noerror = continua ad elaborare in caso di errore di lettura

sync = sostituisce i blocchi di memoria non letti nella destinazione con NULs (mantiene sincronizzata la dimensione della destinazione con quella della sorgente)

# Domanda nr. 09



Per eseguire una copia forense il seguente comando: dd if=/dev/sda bs=2048 | tee mnt/dd\_image/sda.dd | md5sum > mnt/dd\_image/sda.hash

- produce una immagine divisa in parti da 2048MB ✗
- non è corretto ✗
- è corretto ✓
- esegue la copia forense della sorgente "sda" ✓
- esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd" ✗

# Copia Forense comando «DD»

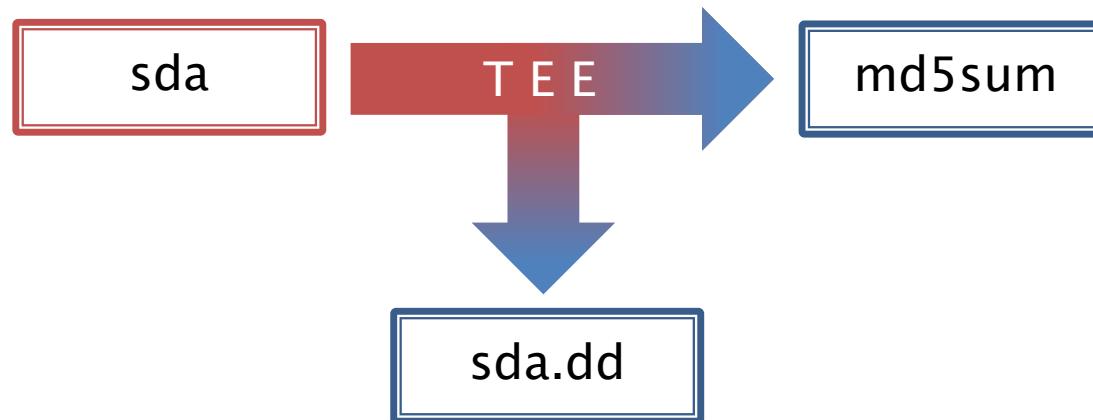
## Calcolare l'Hash

### ▶ Metodo nr. 2:

- Calcoliamo l'hash durante l'elaborazione della copia

```
root@caine:/# dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |  
md5sum > /mnt/dest/dd_image/ sda.hash
```

TEE = biforca\duplica lo stream [una viene utilizzata per generare il file immagine, l'altra viene trasmesso al comando successivo «md5sum»]



# Domanda nr. 10

Per eseguire una copia forense, il seguente comando: dd if=/mnt/sda.dd of=/dev/sda conv=noerror, sync

- è errato in quanto non è stato specificato il "blocksize" ✗
- è corretto ✗
- non è completo, in quanto manca il calcolo dell'hash ✗
- non è corretto poiché le opzioni "noerror" e "sync" non andrebbero combinate ✗
- non è corretto per altri motivi ✓



# Copia Forense

## comando «*DD*»

### ▶ Eseguiamo la copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

IF = input file [*disco sorgente «sda»*]

OF = output file [*file immagine «sda.dd»*]

BS = block size in byte (default 512) [*dimensione del blocco di lettura «2048 byte»*]

CONV = esegue l'elaborazione in base ai parametri indicati

noerror = continua ad elaborare in caso di errore di lettura

sync = sostituisce i blocchi di memoria non letti nella destinazione con NULs (mantiene sincronizzata la dimensione della destinazione con quella della sorgente)

# Domanda nr. 11



il formato DD/RAW:

- |                                     |  |   |
|-------------------------------------|--|---|
| <input type="checkbox"/>            | conserva solo il calcolo dell'hash MD5       | ✗ |
| <input checked="" type="checkbox"/> | non conserva i metadati del reperto sorgente | ✓ |
| <input checked="" type="checkbox"/> | non esegue compressione                      | ✓ |
| <input checked="" type="checkbox"/> | contiene la copia di un solo file            | ✓ |

# Disk Image: *formato DD/RAW*

Formato semplice: è un container dello stream

## ▶ Problematiche:

- Non conserva metadati dell'evidence: *modello, seriale, dimensione, etc.*
- Non conserva hash calcolati;
- Non esegue compressione;
- Non può contenere più di un file/stream;



# Domanda nr. 12

E' un formato disk image:

<input checked="" type="checkbox"/> ISO	✓
<input checked="" type="checkbox"/> .bin/.cue	✓
<input checked="" type="checkbox"/> Smart (.s01, .s02, ...)	✓
<input checked="" type="checkbox"/> DD	✓
<input type="checkbox"/> EnCase L01 (.L01, .L02, ...)	✗



# Disk Image: *Encase L01 Logical (Famiglia EWF)*

- ▶ Acquisizione di file logici.
- ▶ Segmentazione dell'immagine: *.l01, .l02, etc.*
- ▶ Impiega nr. 15 sezioni (+ 2 al formato E01):
  - Ltree section
  - Ltypes section



# Domanda nr. 13

Guymager

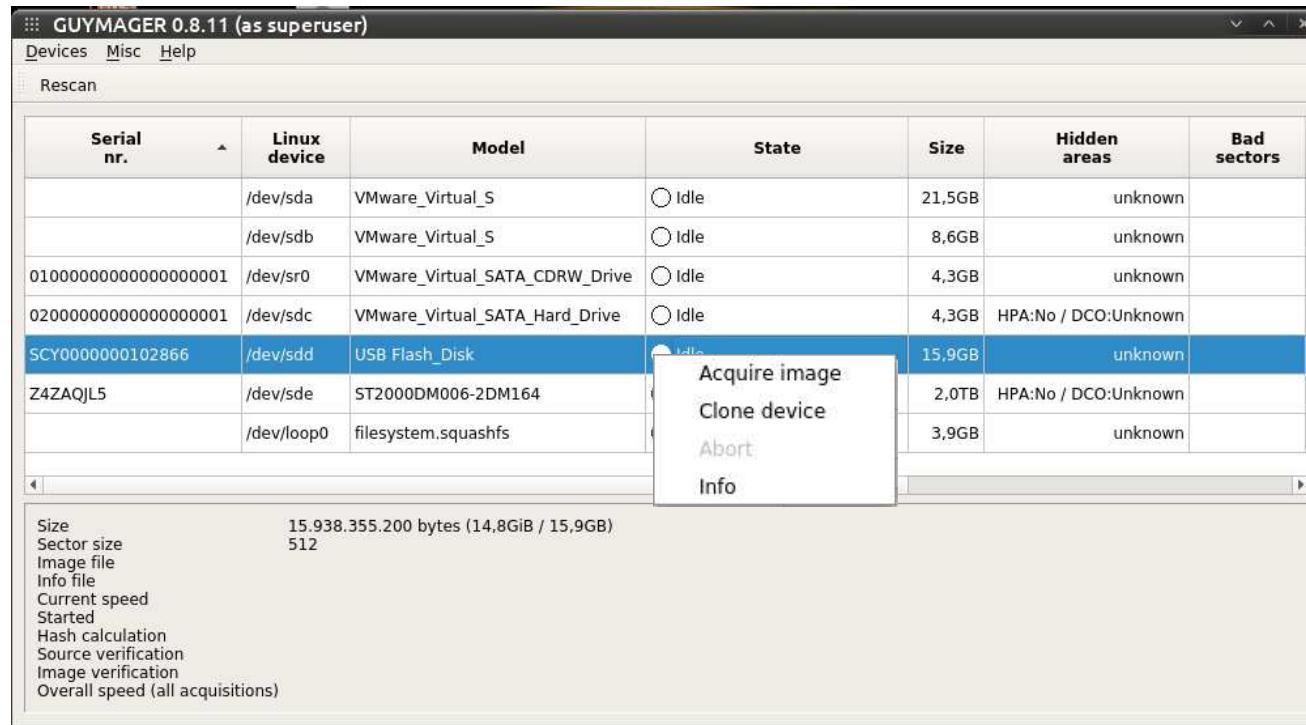
<input checked="" type="checkbox"/>	è uno strumento per elaborare copie forensi	✓
<input type="checkbox"/>	non fa uso dell'hashing on-the-fly	✗
<input type="checkbox"/>	non permette di segmentare/splittare l'immagine	✗
<input checked="" type="checkbox"/>	permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256	✓
<input checked="" type="checkbox"/>	esegue copie forensi solo di tipo "full disk"	✓



# Tool di acquisizione

## *Guymager: Disk Image*

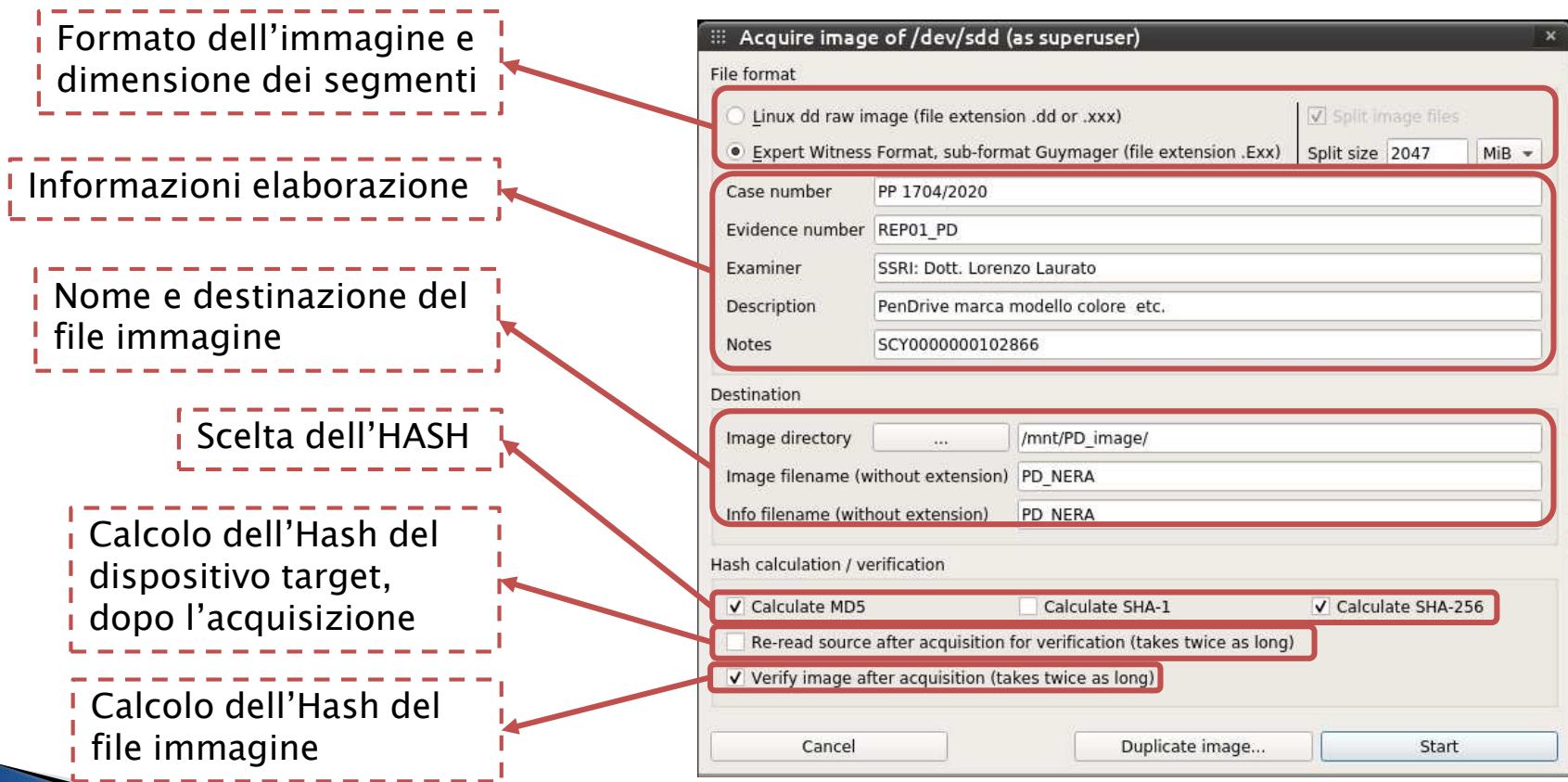
- ▶ scelta del dispositivo da acquisire (*/dev/sdd - USB Flash\_Disk*)



# Tool di acquisizione

## *Guymager: Disk Image*

### ▶ Settaggio dell'elaborazione



# Domanda nr. 14

## FTK Imager

- |                                     |  |   |
|-------------------------------------|--|---|
| <input checked="" type="checkbox"/> | è uno strumento per elaborare copie forensi                    | ✓ |
| <input type="checkbox"/>            | esegue copie forensi solo di tipo "full disk"                  | ✗ |
| <input type="checkbox"/>            | permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256 | ✗ |
| <input checked="" type="checkbox"/> | può eseguire una copia della memoria volatile                  | ✓ |



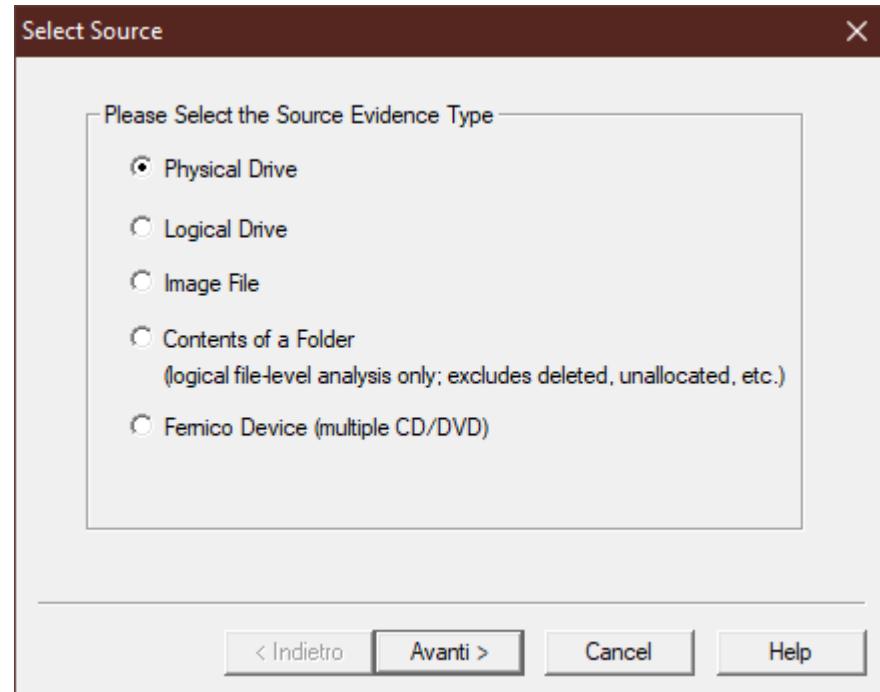
# Tool di acquisizione

## *FTK Imager*

- ▶ File>Create Disk Image...

- ▶ Tipi di acquisizioni:

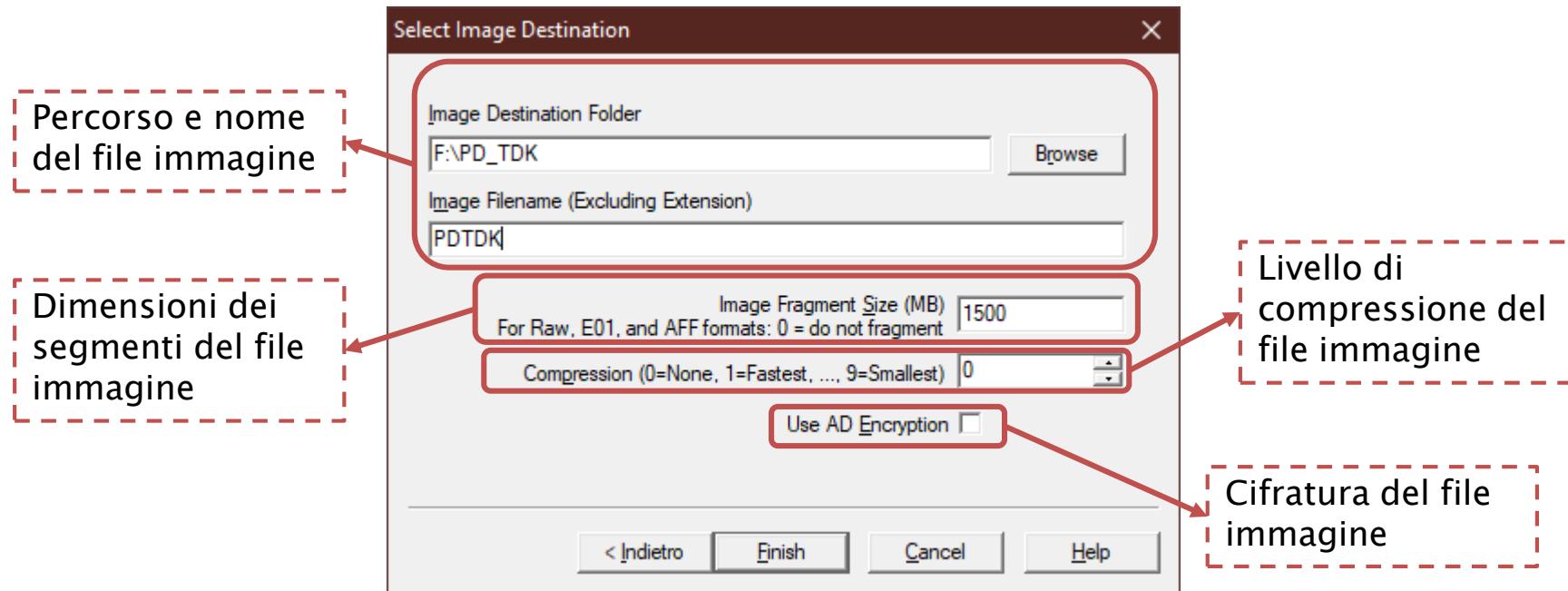
- Physical Drive
- Logical Drive
- Image File
- Content of folder
- Fenico Device



# Tool di acquisizione

## *FTK Imager: Physical Drive*

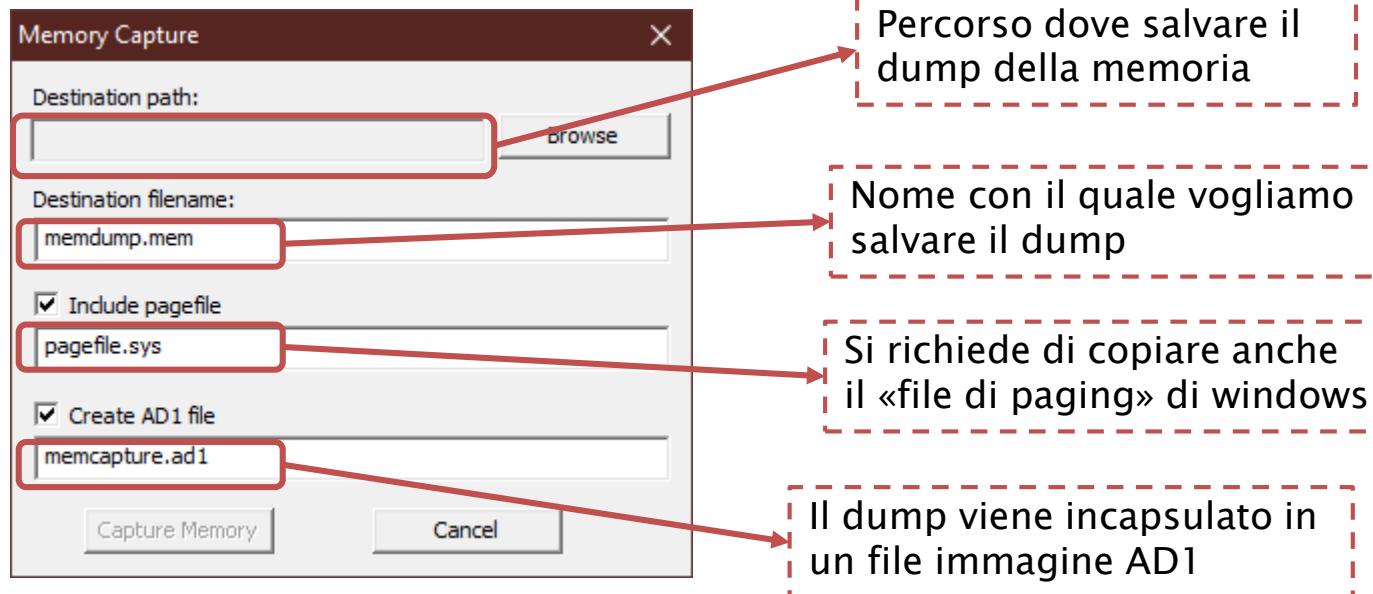
### ▶ Definizione del file immagine



# Tool di acquisizione

## *FTK Imager: dump memoria volatile*

### ▶ File>Capture Memory



# Domanda nr. 15

## L'algoritmo di Hash MD5

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> processa il messaggio in blocchi di 512bit  | ✓ |
| <input type="checkbox"/> è costituito da 4 round e 3 funzioni logiche           | ✗ |
| <input checked="" type="checkbox"/> rispetto a MD4 fa uso di 62 costanti in più | ✓ |
| <input type="checkbox"/> l'output è un digest a 160bit                          | ✗ |



# Funzione Hash

## *MD4/MD5: padding del messaggio*

- ▶ **MD4/MD5** processa il messaggio in blocchi di 512 bit
  - Ogni blocco consta di 16 parole di 32 bit
- ▶ **M'** sarà costituito da:
  - messaggio originario **M**
  - *p bit* di padding
  - *b bit* di rappresentazione della lunghezza di M (*max*  $2^{64}$ )

$$M' = M \underbrace{100\dots0}_{p} \underbrace{b}_{64bit}$$

$$p \mid (p+M) \bmod_{512} 448 \iff 512 - [(M+b) \bmod_{512}]$$

- ▶ **M'** consta di un numero di bit multiplo di 512, ovvero di un numero *L blocchi* di 512 bit
  - Ovvero di N parole con N multiplo di 16:
    - $L=N/16$  blocchi di 512 bit

# Funzione Hash

## *MD4/MD5: funzioni*

### ▶ Funzioni definite su parole di 32 bit:

- round 1:  $F(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$  [if X then Y else Z]
- round 2:  $G(X,Y,Z) = (X \wedge Z) \vee ((Y \wedge (\neg Z))$  [MD5] [if Z then X else Y]
- round 2:  $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge Z) \vee (X \wedge Y)$  [MD4] [2 su 3]
- round 3:  $H(X,Y,Z) = X \oplus Y \oplus Z$  [bit di parità]
- round 4:  $I(X,Y,Z) = Y \oplus (X \vee (\neg Z))$  [MD5]

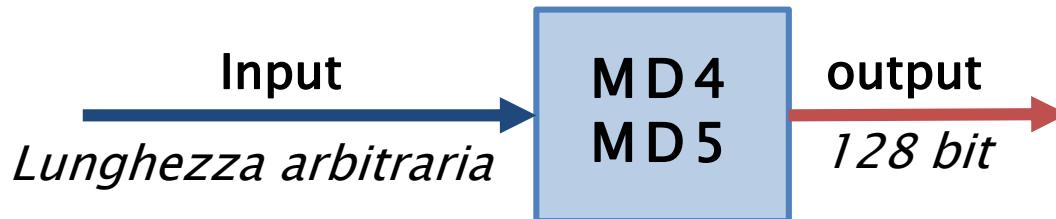
X	Y	Z	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

# Funzione Hash

## *MD4/MD5*

MD = Message Digest

- ▶ MD4: Progettata nel 1990 da Ron Rivest
- ▶ MD5: Progettata nel 1991
- ▶ Operazioni efficienti su architetture 32 bit little-endian



# Funzione Hash

## *MD5/MD4: differenze*

MD5	MD4
▶ 4 round = $4 \cdot 16$ operazioni	▶ 3 round = $3 \cdot 16$ operazioni
▶ 4 funzioni logiche	▶ 3 funzioni logiche
▶ 64 costanti additive	▶ 2 costanti additive
▶ ogni passo aggiunge il risultato del passo precedente	

# Domanda nr. 16



Nell'algoritmo di SHA-1 se il messaggio di input  $M$  è di 968bit, dopo il padding avremo che  $M'$  sarà costituito da :

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> 3 blocchi da 512bit       | ✓ |
| <input type="checkbox"/> 60bit per la lunghezza del messaggio | ✗ |
| <input checked="" type="checkbox"/> un bit a "1" al 969° bit  | ✓ |
| <input type="checkbox"/> nessun bit di padding                | ✗ |
| <input checked="" type="checkbox"/> 1536bit                   | ✓ |

# Funzione Hash

## *SHA: padding del messaggio*

- ▶ SHA processa il messaggio in blocchi di 512 bit
  - Ogni blocco consta di 16 parole di 32 bit
- ▶ M' sarà costituito da:
  - messaggio originario M
  - *p bit* di padding
  - *b bit* di rappresentazione della lunghezza di M (*max*  $2^{64}$ )

$$M' = M \underbrace{100\dots0}_{p} \underbrace{b}_{64bit}$$

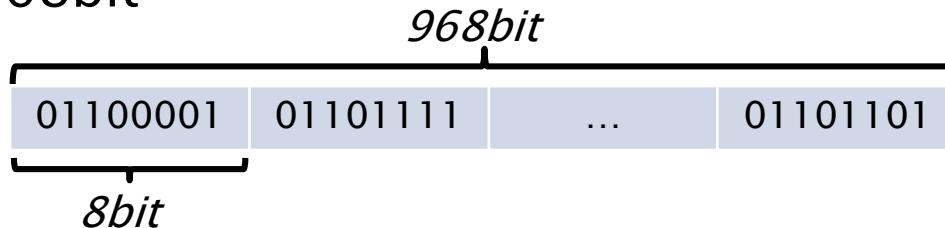
$$p \mid (p+M) \bmod_{512} 448 \iff 512 - [(M+b) \bmod_{512}]$$

- ▶ M' consta di un numero di bit multiplo di 512, ovvero di un numero *L blocchi* di 512 bit
  - Ovvero di N parole con N multiplo di 16:
    - $L=N/16$  blocchi di 512 bit

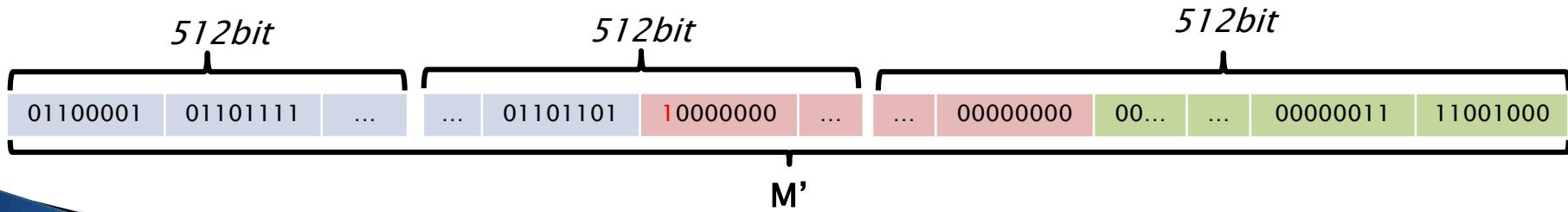
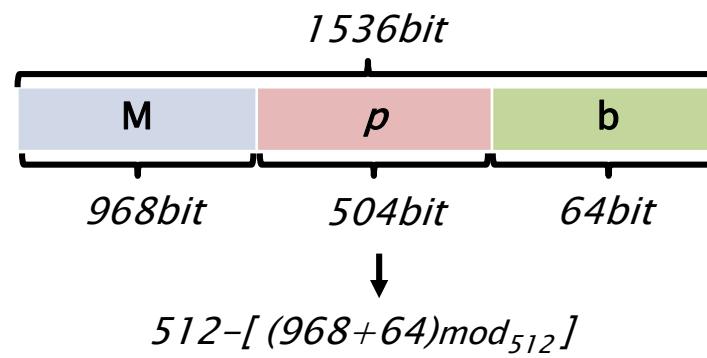
# Funzione Hash

## *padding del messaggio*

- ▶  $|M|=968\text{bit}$



- ▶  $M' = M \ p \ b$





## SSRI Lorenzo Laurato s.r.l.



Via Coroglio nr. 57/D (BIC- Città della Scienza)  
80124 Napoli



Tel. 335.54.56.550 - 081.19804755



Fax 081.19576037

[lorenzo.laurato@ssrilab.com](mailto:lorenzo.laurato@ssrilab.com) - [info@ssrilab.com](mailto:info@ssrilab.com)  
[ssri@legalmail.it](mailto:ssri@legalmail.it)

# Lezione 12: L'Analisi *gli strumenti* *(parte 1)*



A.A. 2019/20

Dott. Lorenzo LAURATO



# Nelle puntate precedenti...

Accertamento tecnico  
ripetibile



Accertamento tecnico  
irripetibile



# Fasi

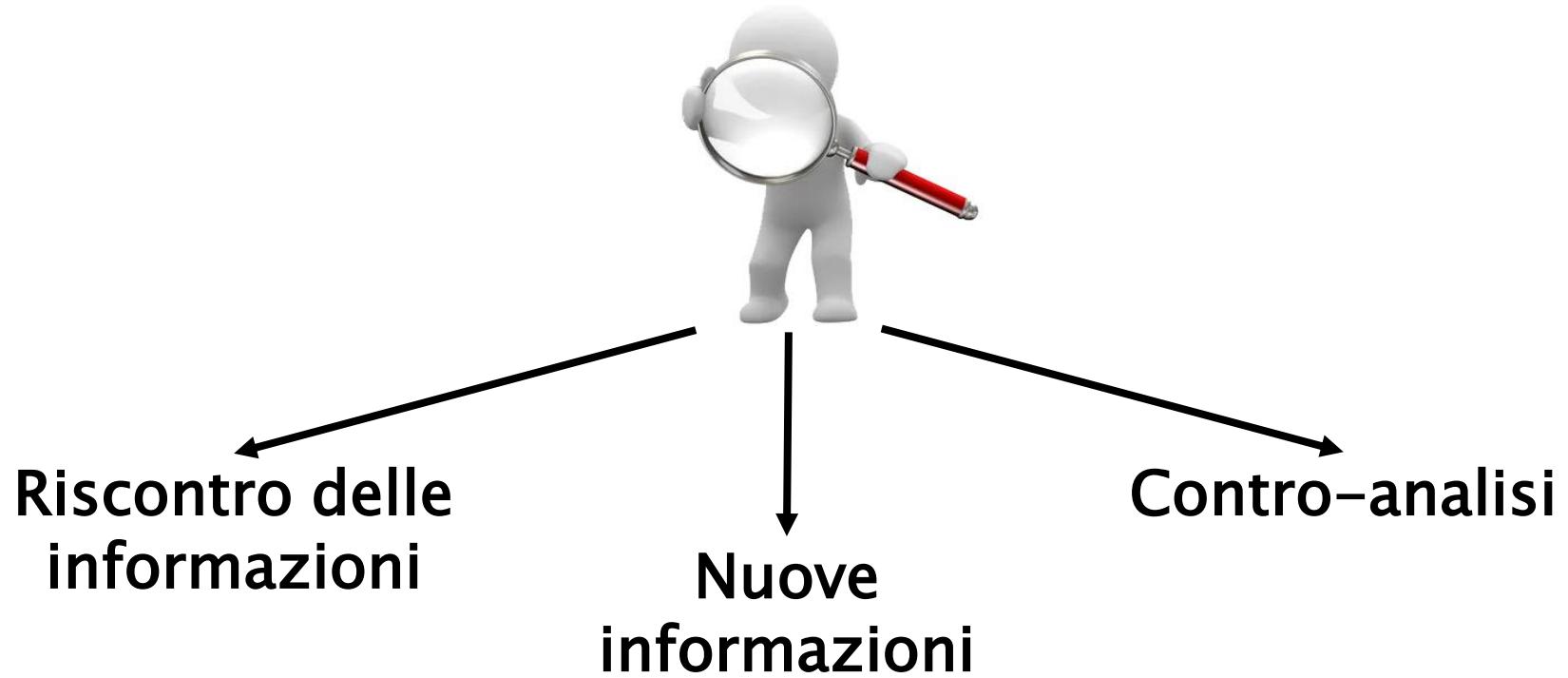


# L'analisi

- ▶ Va eseguita su una copia
- ▶ Riproducibilità
- ▶ Stesso risultato ottenibile da diverse operazioni/strumenti di analisi
- ▶ Ricostruzione di eventi passati mediante la lettura di dati digitali

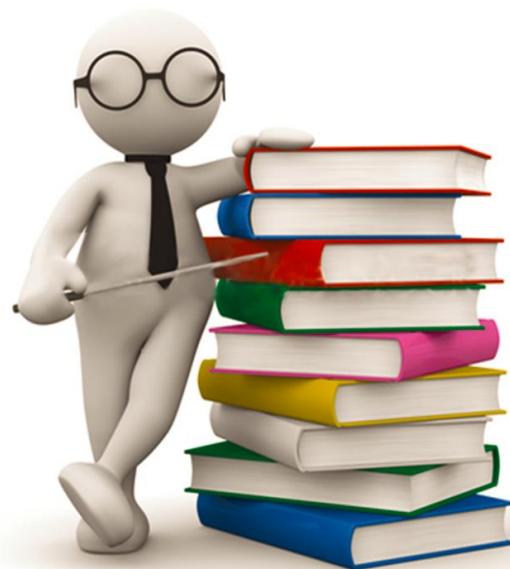


# L'analisi



# L'analisi

- ▶ Il primo strumento di analisi è il proprio bagaglio di conoscenze informatiche.



# L'Analisi

» montare un file immagine



# L'Analisi

## *montare un file immagine: linux*

### ► Analizziamo il file immagine

```
root@caine:/# fdisk -l /mnt/dest/dd_image/sda.dd

Disk /mnt/dest/dd_image/sda.dd: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c

Device            Boot   Start     End Sectors Size Id Type
/mnt/dest/dd_image/sda.ddp1      2048 2099199 2097152  1G  b W95 FAT32
/mnt/dest/dd_image/sda.ddp2 2099200 8388607 6289408  3G  b W95 FAT32
```

Il file immagine rappresenta una memoria con due partizioni: p1 e p2

# L'Analisi

## *montare un file immagine: linux*

- ▶ montiamo la partizione p2

Device	Boot	Start	End	Sectors	Size	Id	Type
/mnt/dest/dd_image/sda.ddp1		2048	2099199	2097152	1G	b	W95 FAT32
/mnt/dest/dd_image/sda.ddp2	2099200	8388607	6289408	3G	b	W95 FAT32	

```
root@caine:/# mount -o ro,loop,offset=1074790400 /mnt/dest/dd_image/sda.dd /mnt/sda_dd
```

- ▶ **ro**: read-only
- ▶ **loop**: crea un *virtual block device* da un file (*character device*)
- ▶ **offset=byte**: punto di inizio della partizione da montare (*2099200 · 512*)

**Solo immagini DD/Raw non segmentate**

# L'Analisi

## *montare un file immagine: linux*

- ▶ merge immagine segmentata DD\RAW (AFFLIBv3)

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194308
-rwxrwxrwx 1 root root 2147483648 apr  8 01:16 sda.000
-rwxrwxrwx 1 root root 2147483648 apr  8 01:23 sda.001
-rwxrwxrwx 1 root root      823 apr  8 01:23 sda.log
```

```
root@caine:/# affuse /mnt/dest/dd_image/sda.000 /mnt/sda_fuse
```

```
root@caine:/# ls -l /mnt/sda_fuse/
total 0
-r--r--r-- 1 root root 4294967296 gen  1 1970 sda.000.raw
```

```
root@caine:/# fdisk -l /mnt/sda_fuse/sda.000.raw
Disk /mnt/sda_fuse/sda.000.raw: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device          Boot  Start    End Sectors Size Id Type
/mnt/sda_fuse/sda.000.raw1            2048 2099199 2097152   1G  b W95 FAT32
/mnt/sda_fuse/sda.000.raw2        2099200 8388607 6289408   3G  b W95 FAT32
```

# L'Analisi

## *montare un file immagine: linux*

- ▶ merge immagine segmentata EWF (libewf)

```
root@caine:/# ls -l /mnt/dest/e01_image/
total 235526
-rw-r--r-- 1 root root 104857600 apr  8 02:26 sda.E01
-rw-r--r-- 1 root root 104857600 apr  8 02:28 sda.E02
-rw-r--r-- 1 root root  31457280 apr  8 02:29 sda.E03
-rw-r--r-- 1 root root      7161 apr  8 02:29 sda.info
```

```
root@caine:/# ewfmount /mnt/dest/e01_image/sda.E01 /mnt/sda_fuse
```

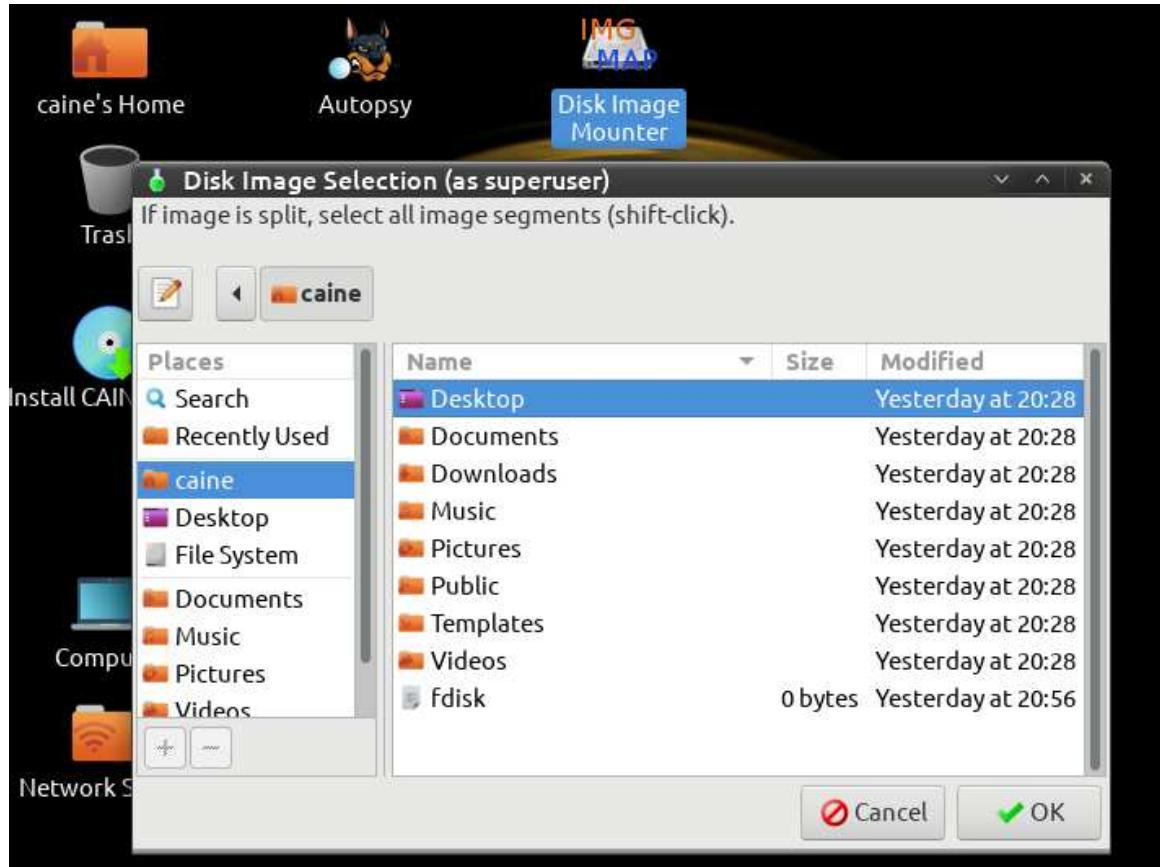
```
root@caine:/# ls -l /mnt/sda_fuse/
total 0
-r--r--r-- 1 root root 4294967296 apr  8 02:31 ewf1
```

```
root@caine:/# fdisk -l /mnt/sda_fuse/ewf1
Disk /mnt/sda_fuse/ewf1: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device          Boot   Start     End Sectors Size Id Type
/mnt/sda_fuse/ewf1p1            2048 2099199 2097152   1G  b W95 FAT32
/mnt/sda_fuse/ewf1p2        2099200 8388607 6289408   3G  b W95 FAT32
```

# L'Analisi

## *montare un file immagine: linux*

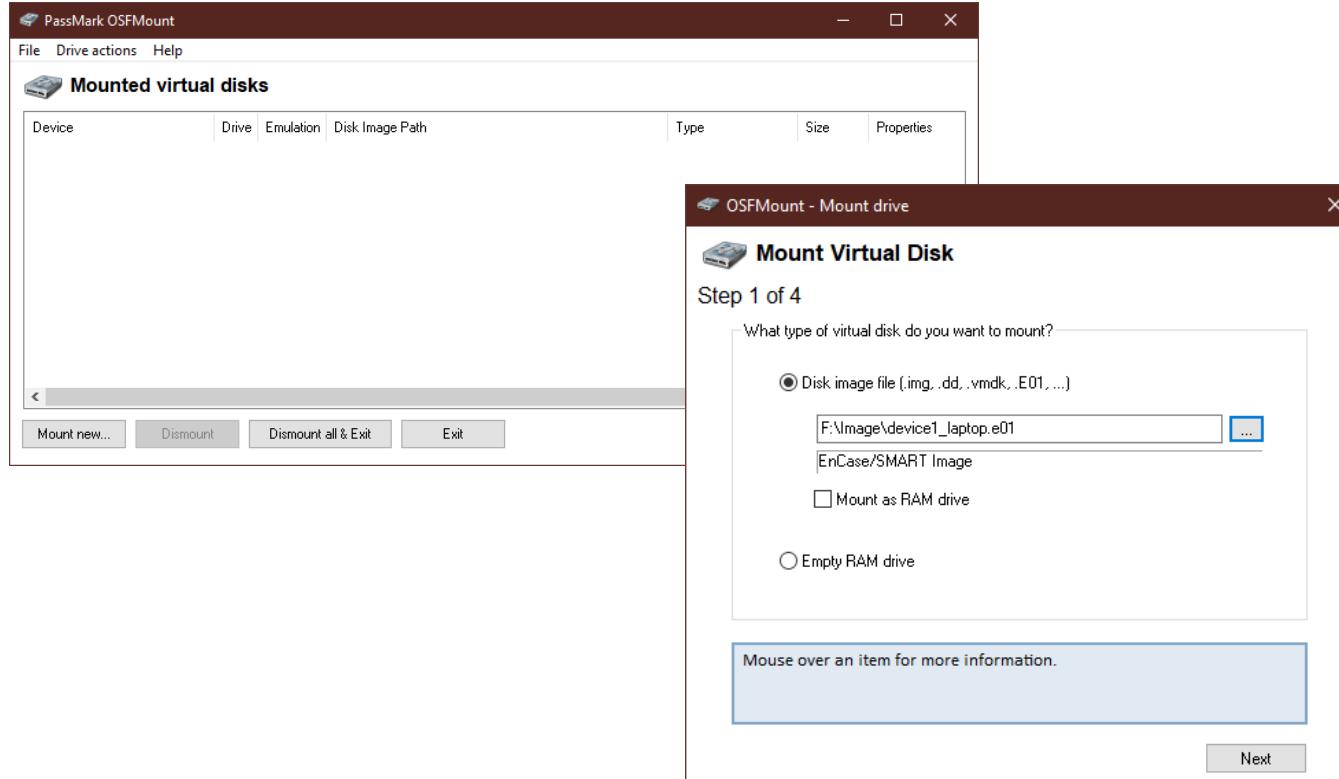
- ▶ tramite GUI: tool «IMG\_MAP»



# L'Analisi

## *montare un file immagine: windows*

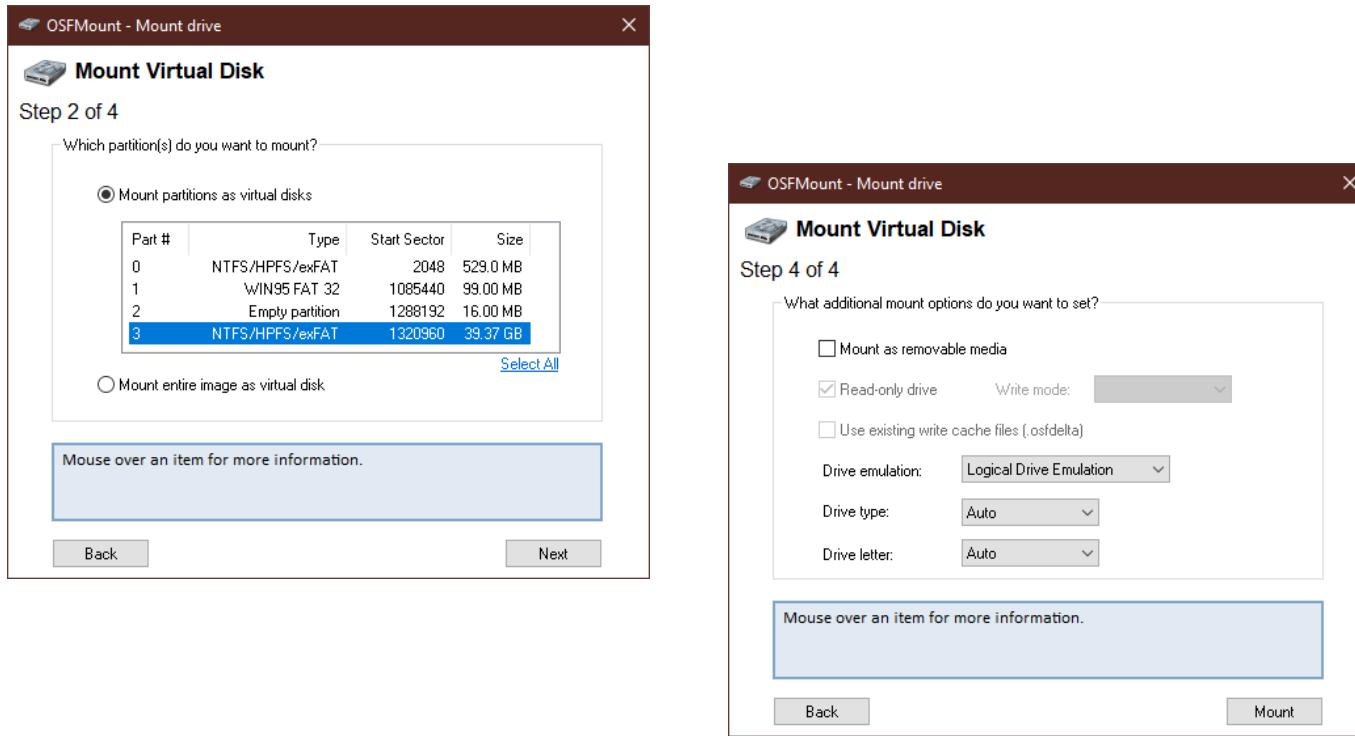
### PassMark OFSMount



# L'Analisi

## *montare un file immagine: windows*

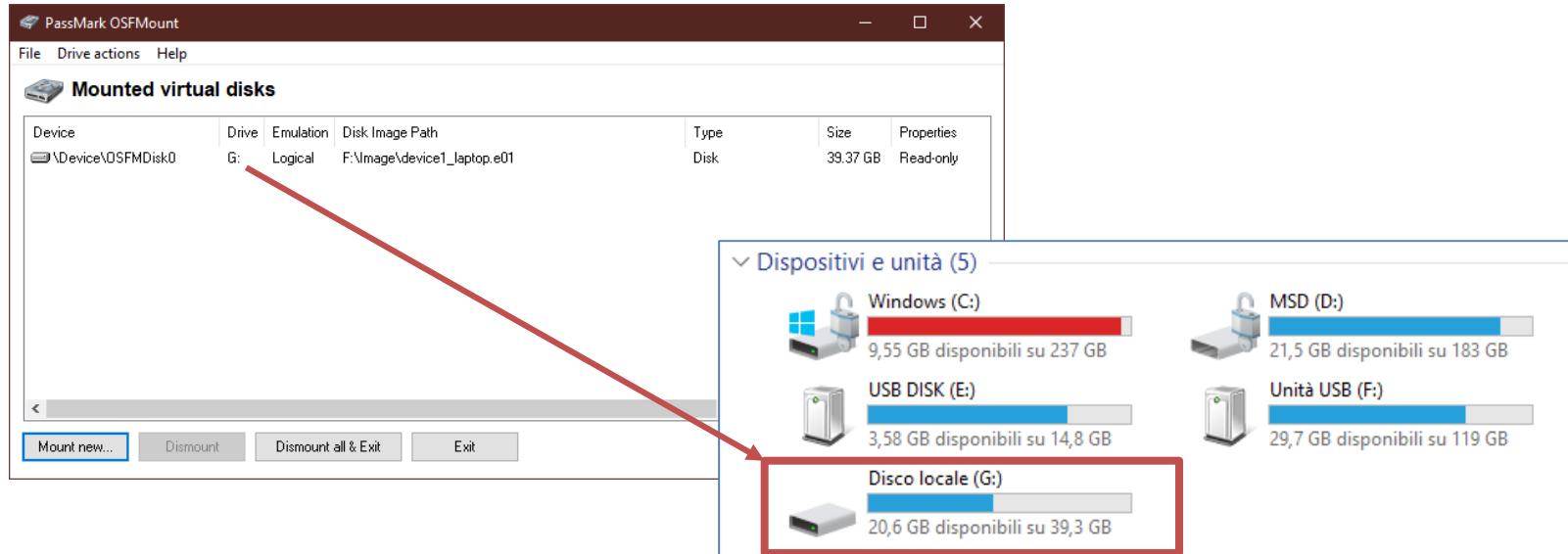
### PassMark OFSMount



# L'Analisi

## *montare un file immagine: windows*

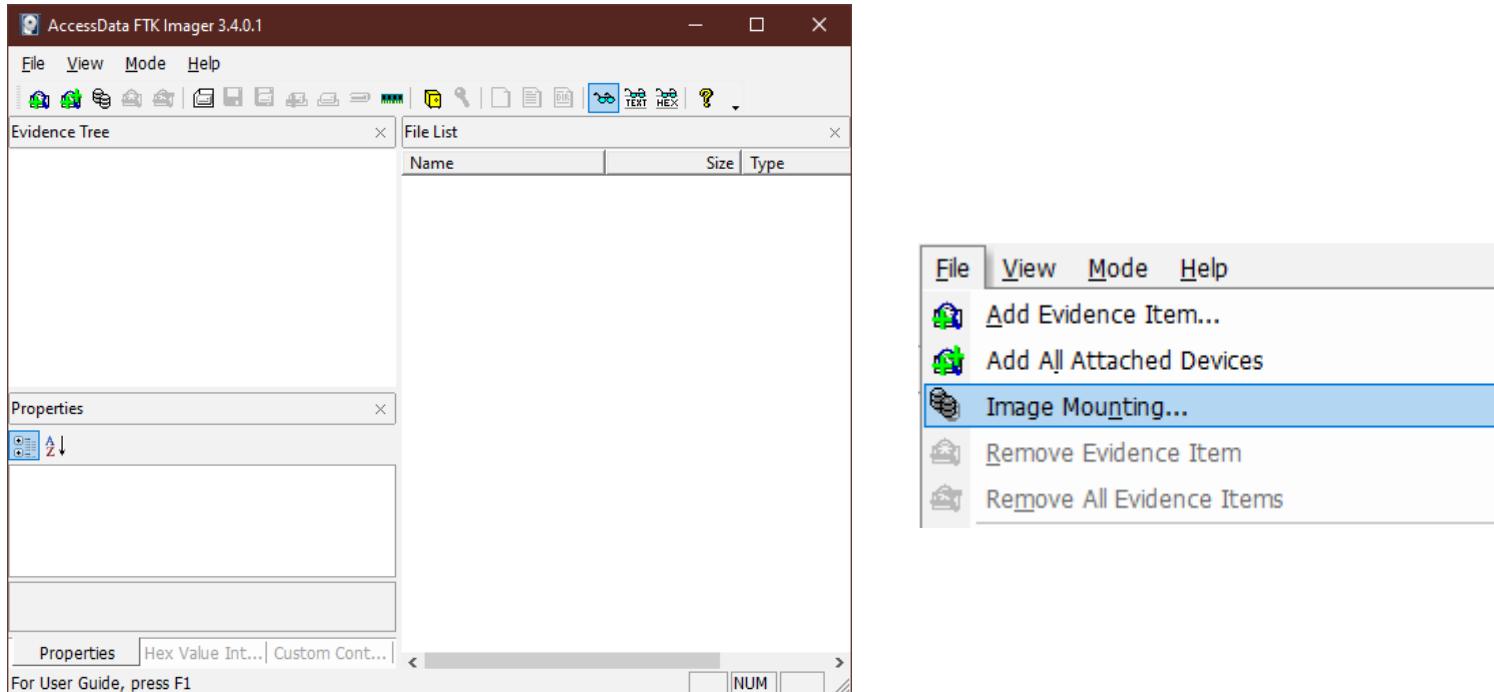
### PassMark OFSMount



# L'Analisi

## *montare un file immagine: windows*

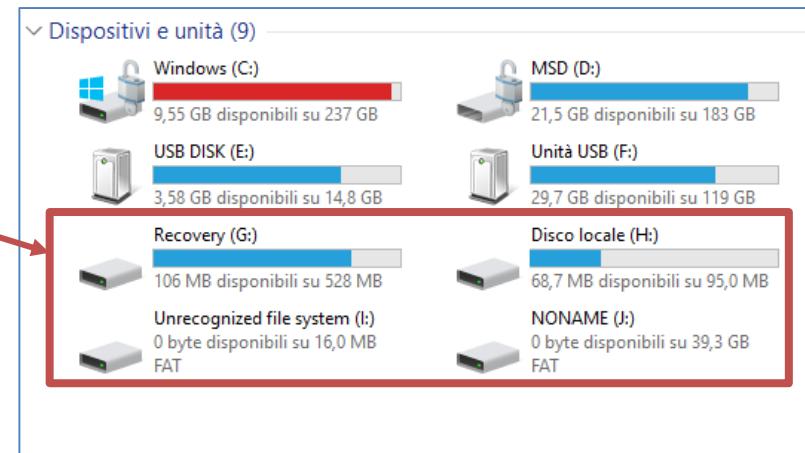
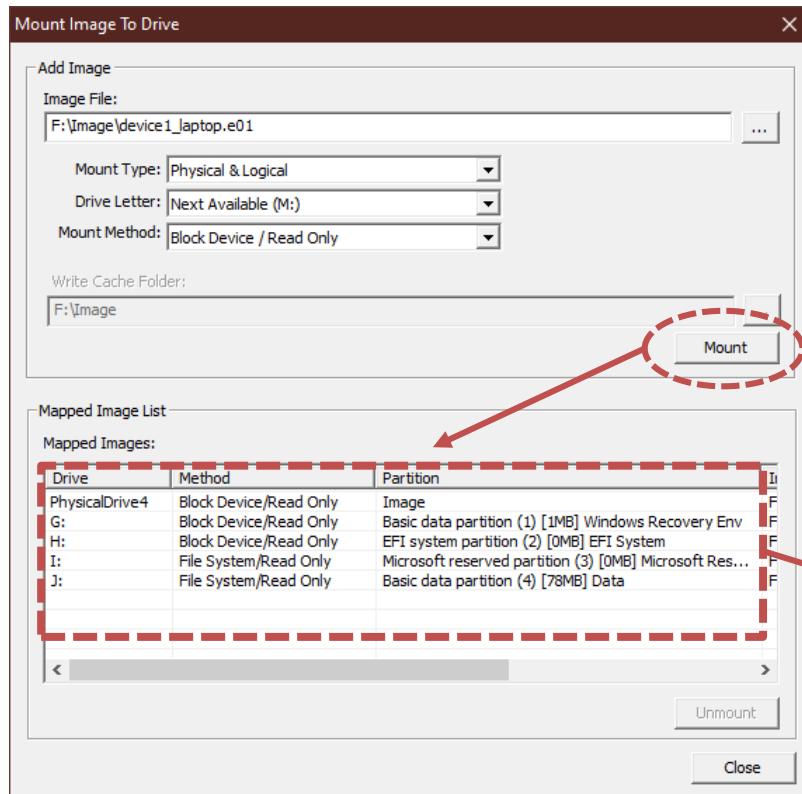
### *AccessData FTK Imager*



# L'Analisi

## *montare un file immagine: windows*

### *AccessData FTK Imager*



# L'Analisi

## *montare un file immagine*

### Pro

- ▶ veloce per operazioni semplici
- ▶ Utilizzo di tool non forensic oriented

### Contro

- ▶ Farraginoso
- ▶ Solo file residenti
- ▶ Riconoscimento del FileSystem dell'immagine demandata al nostro S.O.

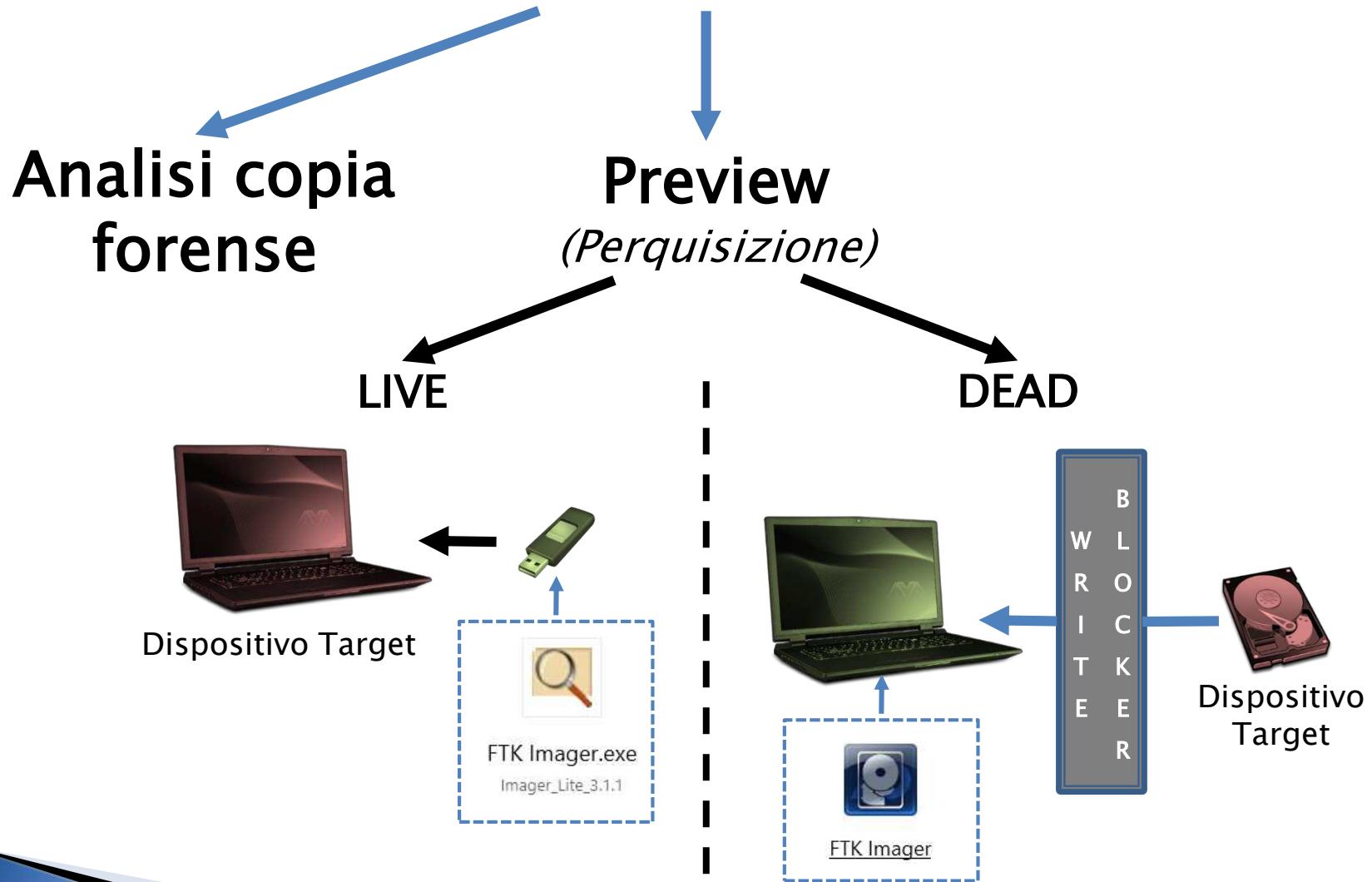
**Solo per specifiche analisi**

# L'Analisi

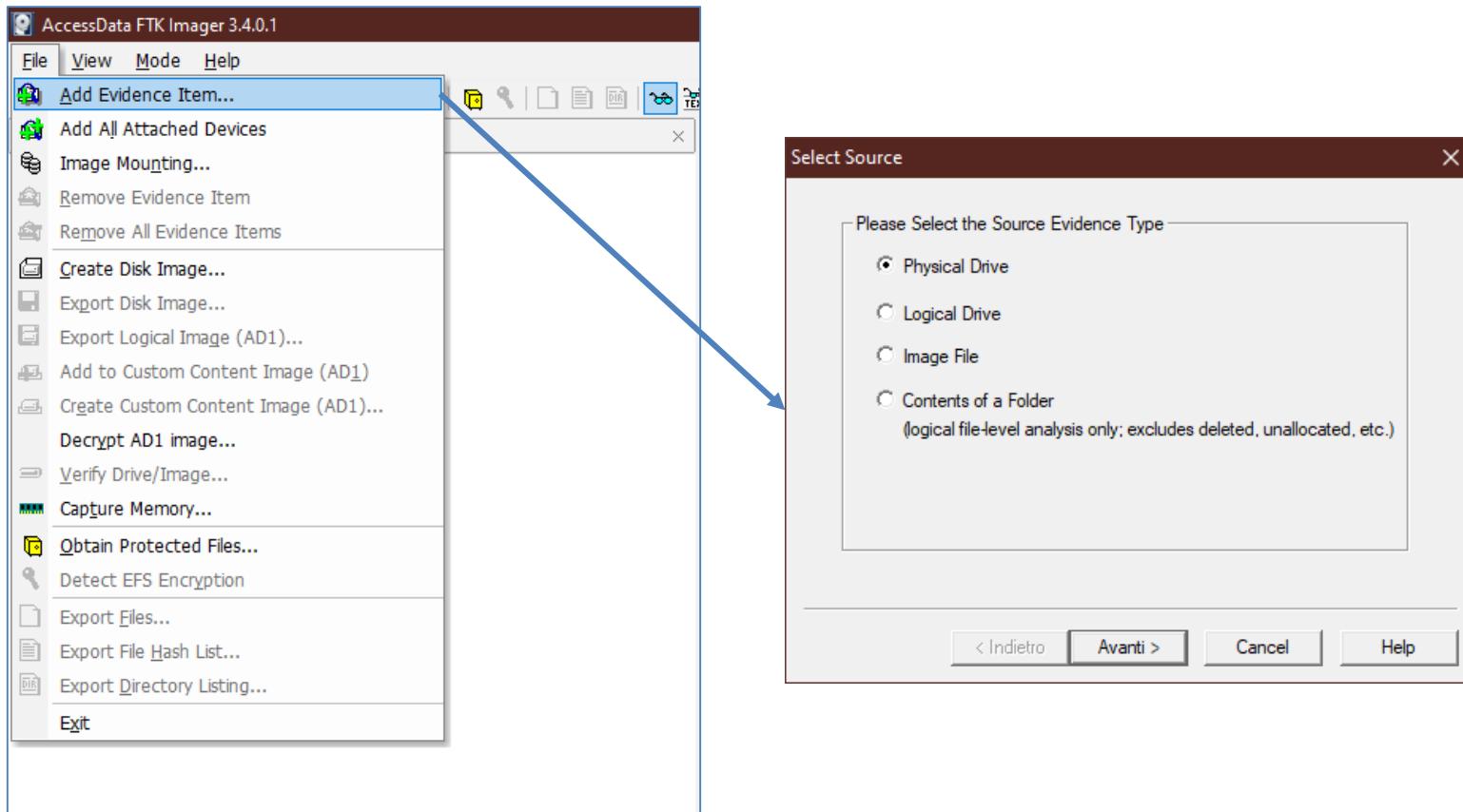
» FTK Imager



# FTK Imager



# FTK Imager



# FTK Imager

## Hard Disk Image Formats

The following table lists AccessData Imager-identified and analyzed hard disk image formats:

### Identified and Analyzed Hard Disk Image Formats

- |                                  |                                   |
|----------------------------------|-----------------------------------|
| • Encase, including 6.12         | • SnapBack                        |
| • Safeback 2.0 and under         | • Expert Witness                  |
| • Linux DD                       | • ICS                             |
| • Ghost (forensic images only)   | • SMART                           |
| • AccessData Logical Image (AD1) | • Advanced Forensics Format (AFF) |



# FTK Imager

## CD and DVD Image Formats

The following table lists AccessData Imager-identified and analyzed CD and DVD image formats:

### Identified and Analyzed CD and DVD File Systems and Formats

• Alcohol (*.mds)	• IsoBuster CUE
• PlexTools (*.pxi)	• CloneCD (*.ccd)
• Nero (*.nrg)	• Roxio (*.cif)
• ISO	• Pinnacle (*.pdi)
• Virtual CD (*.vc4)	• CD-RW,
• VCD	• CD-ROM
• DVD+MRW	• DVCD
• DVD-RW	• DVD-VFR
• DVD+RW Dual Layer	• DVD-VR
• BD-R SRM-POW	• BD-R DL
• BD-R SRM	• CloneCD (*.ccd)
• HD DVD-R	• HD DVD-RW DL
• SVCD	• HD DVD

# FTK Imager

## File Systems

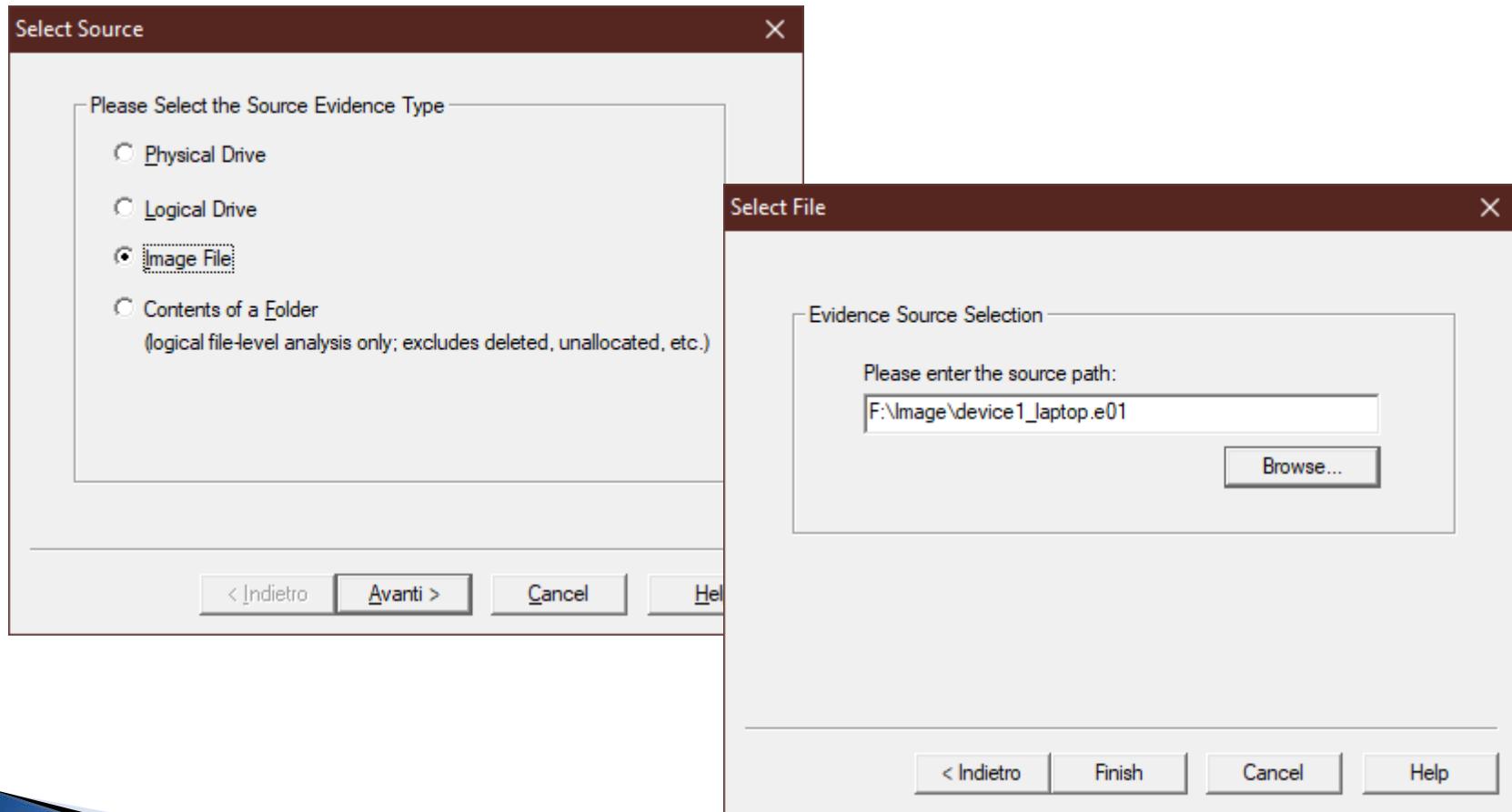
The following table lists AccessData Imager-identified and analyzed file systems:

### Identified and Analyzed File Systems

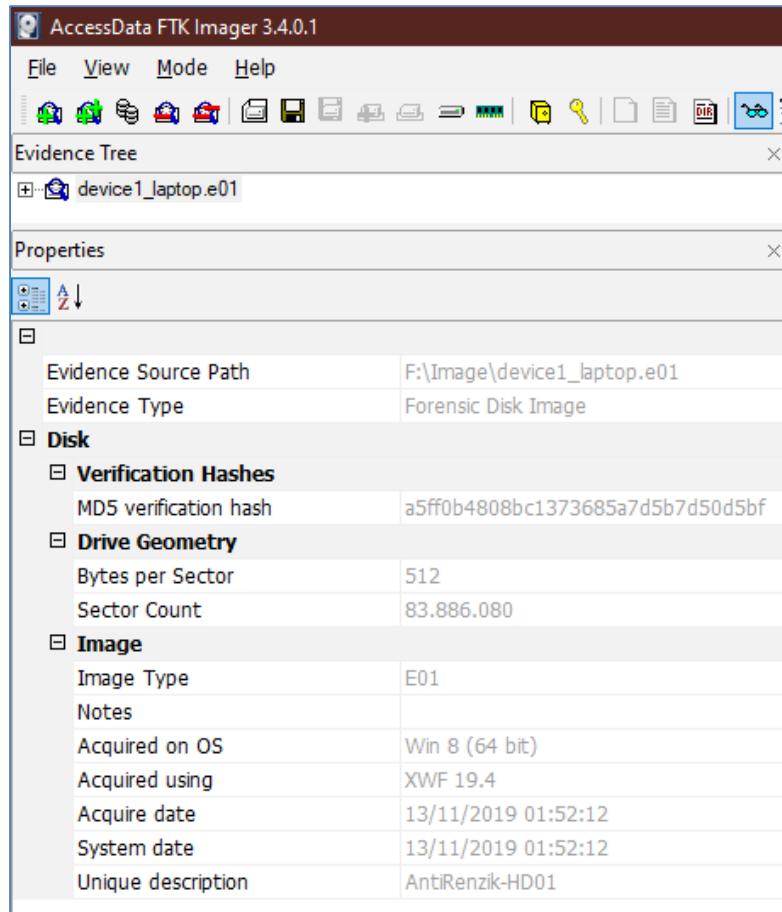
- |                       |             |
|-----------------------|-------------|
| • APFS                | • HFS       |
| • CDFS                | • HFS+      |
| • exFAT               | • NTFS      |
| • Ext2FS              | • ReiserFS3 |
| • Ext3FS              | • VXFS      |
| • Ext4FS              | • XFS       |
| • FAT12, FAT16, FAT32 |             |

# FTK Imager:

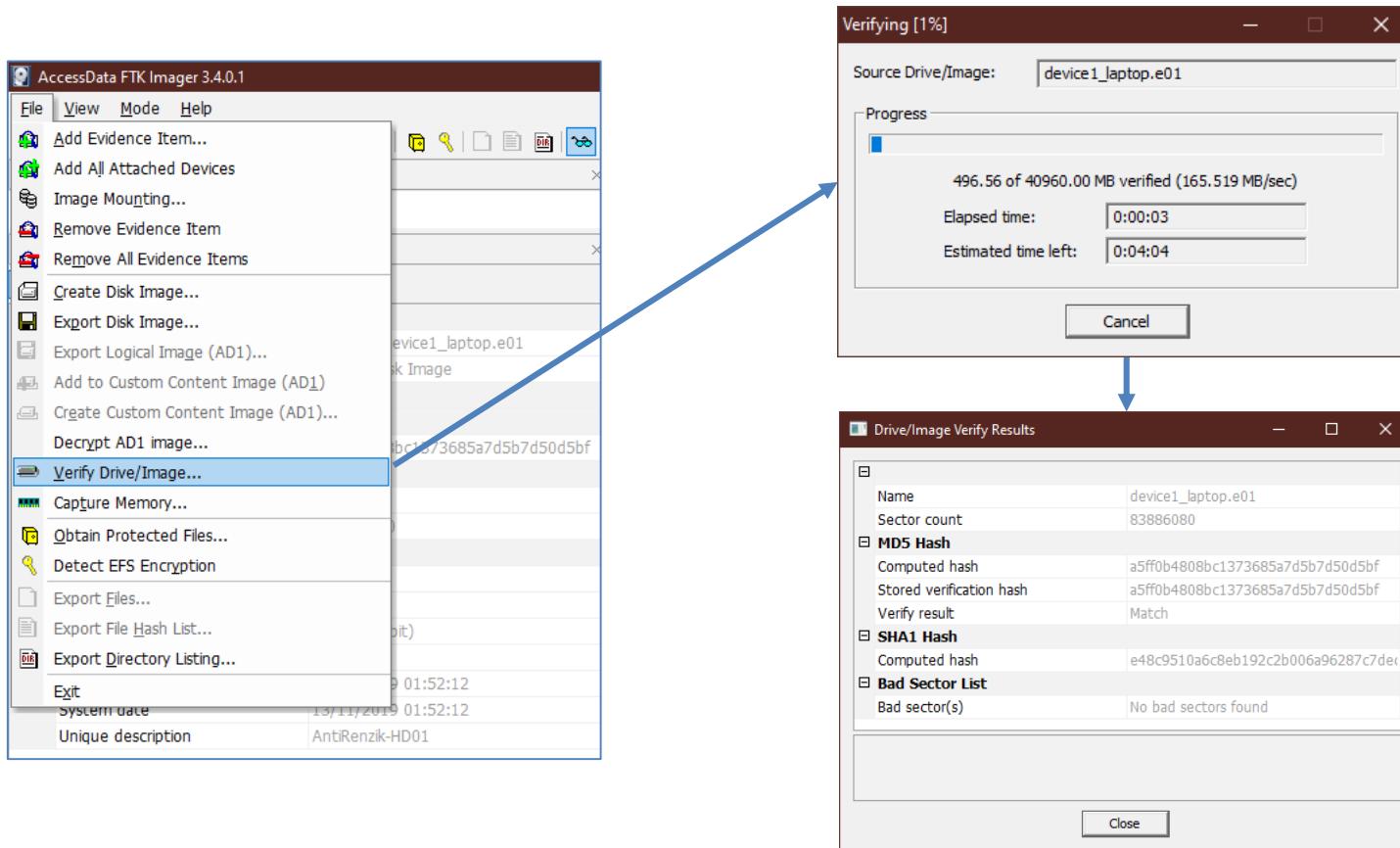
## *analisi file immagine*



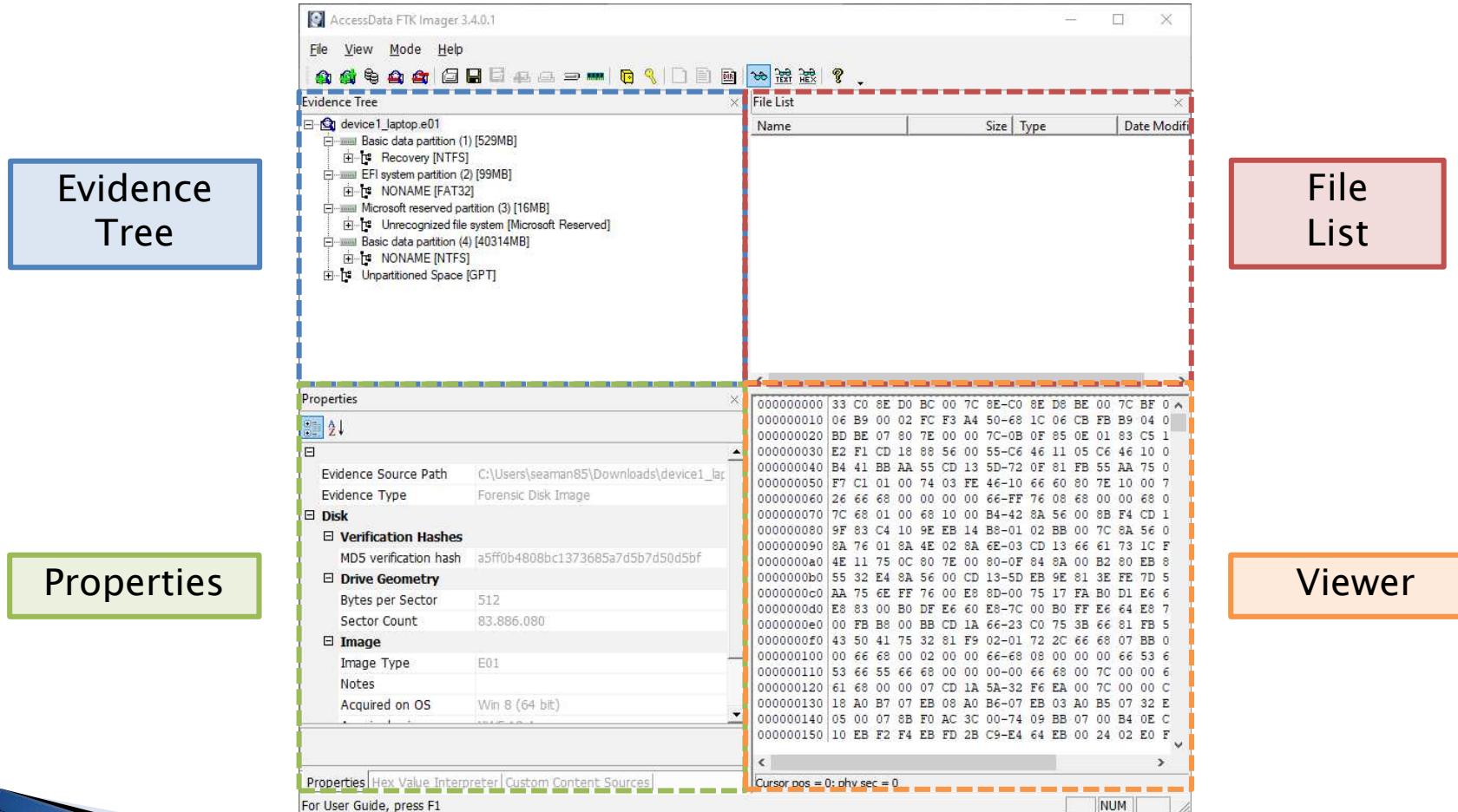
# FTK Imager: *analisi file immagine: header info*



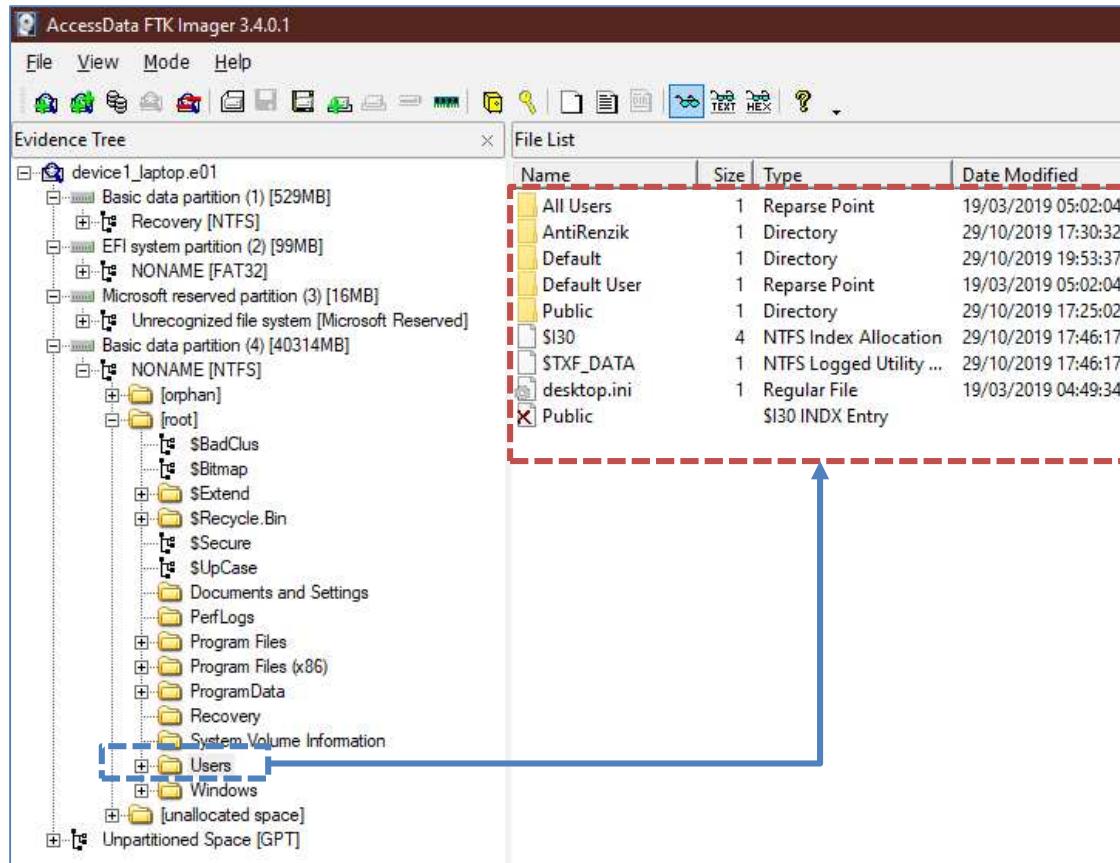
# FTK Imager: *analisi file immagine: verifica*



# FTK Imager: *analisi file immagine: GUI*



# FTK Imager: *analisi file immagine: GUI*



# FTK Imager: *analisi file immagine: GUI*

The screenshot shows the FTK Imager interface with the following details:

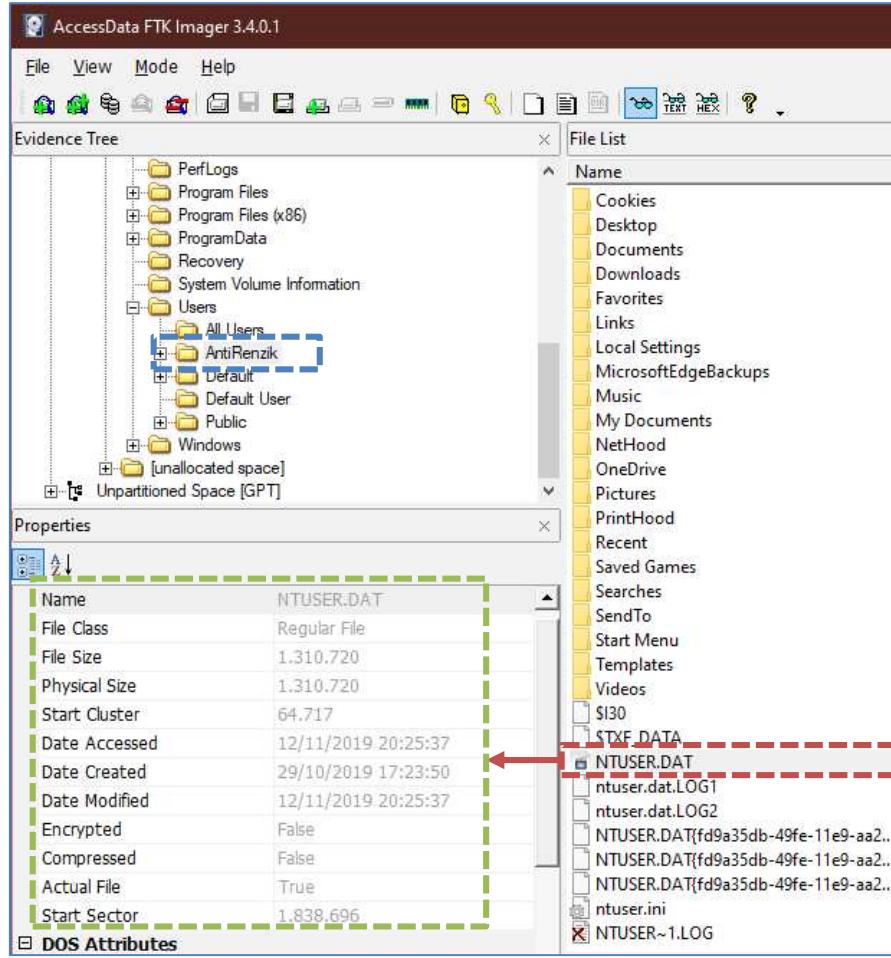
**Evidence Tree:** The left pane displays the evidence structure for "device1\_laptop.e01". It includes:

- Basic data partition (1) [529MB]:
  - Recovery [NTFS]
- EFI system partition (2) [99MB]:
  - NONAME [FAT32]
- Microsoft reserved partition (3) [16MB]:
  - Unrecognized file system [Microsoft Reserved]
- Basic data partition (4) [40314MB]:
  - NONAME [TEST1]:
    - [orphan]
    - [root]:
      - \$BadClus
      - \$Bitmap
      - \$Extend
      - \$Recycle.Bin
      - \$Secure
      - \$UpCase
      - Documents and Settings
      - PerfLogs
      - Program Files
      - Program Files (x86)
      - ProgramData
      - Recovery
      - System Volume Information
      - Users
      - Windows
    - [unallocated space]
  - Unpartitioned Space [GPT]

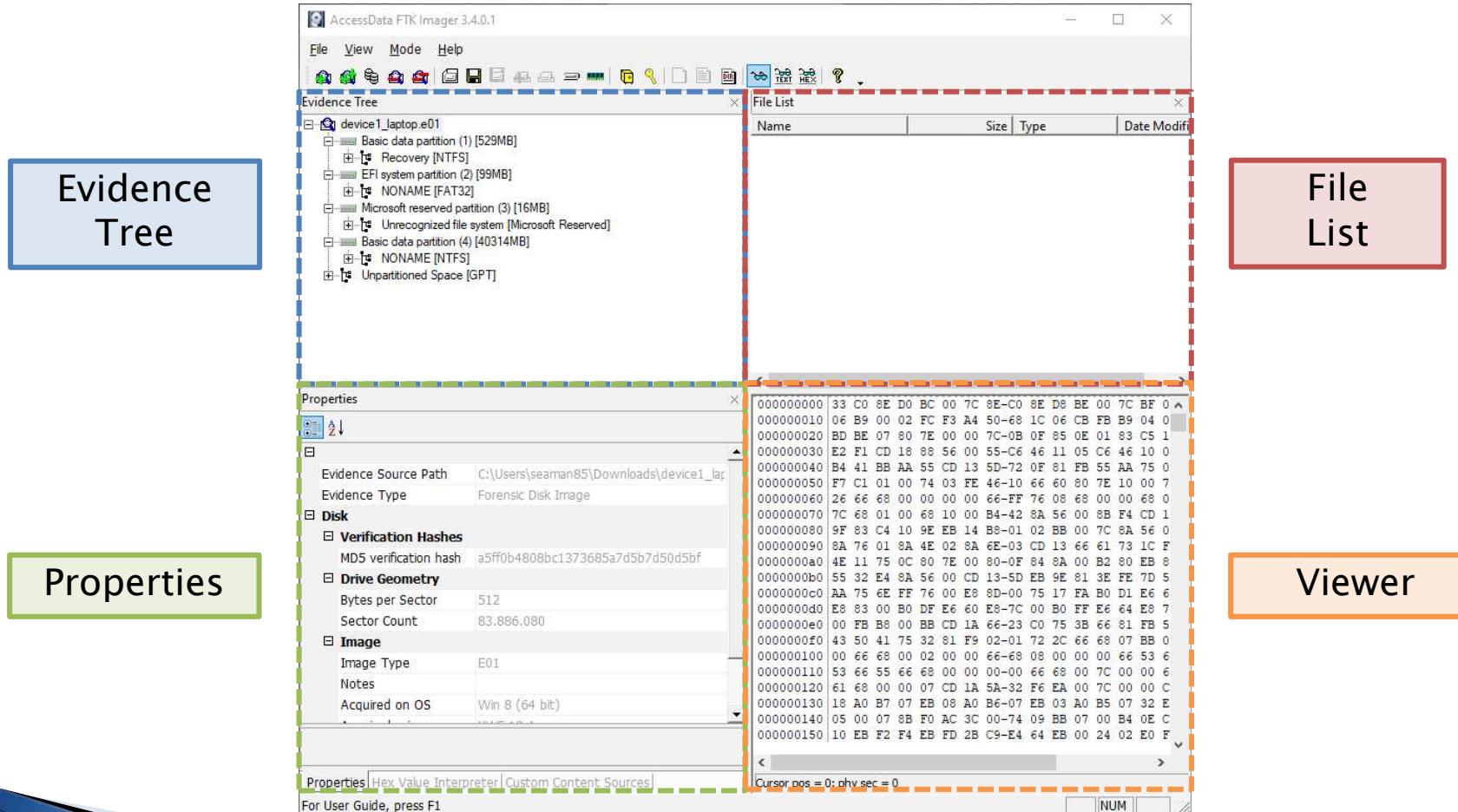
**File List:** The right pane displays a list of files found in the selected directory. A red dashed box highlights the list.

Name	Size	Type	Date Modified
AppxMetadata	1	Directory	12/11/2019 20:47:22
AppxMetadata	1	Directory	12/11/2019 20:47:22
microsoft.system.package.metadata	1	Directory	12/11/2019 20:47:22
microsoft.system.package.metadata	1	Directory	05/11/2019 00:10:29
microsoft.system.package.metadata	1	Directory	05/11/2019 00:02:46
0.0.filtertrie.intermediate.txt	34	Regular File	05/11/2019 00:06:18
0.1.filtertrie.intermediate.txt	1	Regular File	05/11/2019 00:06:18
0.2.filtertrie.intermediate.txt	1	Regular File	05/11/2019 00:06:18
All mail Including Spam and Trash.m...	27....	Regular File	12/11/2019 20:20:50
All mail Including Spam and Trash.m...	3	File Slack	
Apps.ft	45	Regular File	05/11/2019 00:06:18
Apps.index	1.0...	Regular File	05/11/2019 00:06:19
AppxBlockMap.xml	6	Reparse Point	05/11/2019 00:10:29
AppxBlockMap.xml	1	Regular File	05/11/2019 00:10:29
AppxBlockMap.xml	1	Regular File	05/11/2019 00:02:45
AppxManifest.xml	59	File Slack	
AppxManifest.xml.FileSlack	4	File Slack	
AppxManifest.xml.FileSlack	5	Reparse Point	05/11/2019 00:10:29
AppxSignature.p7x	60	File Slack	
AppxSignature.p7x	12	Regular File	05/11/2019 00:10:30
AppxSignature.p7x	11	Regular File	05/11/2019 00:10:29
AppxSignature.p7x	11	Regular File	05/11/2019 00:02:45
CodelIntegrity.cat	12	Regular File	05/11/2019 00:10:29
GameBar.exe	193	Reparse Point	05/11/2019 00:10:30
GameBar.exe.FileSlack	63	File Slack	

# FTK Imager: *analisi file immagine: GUI*

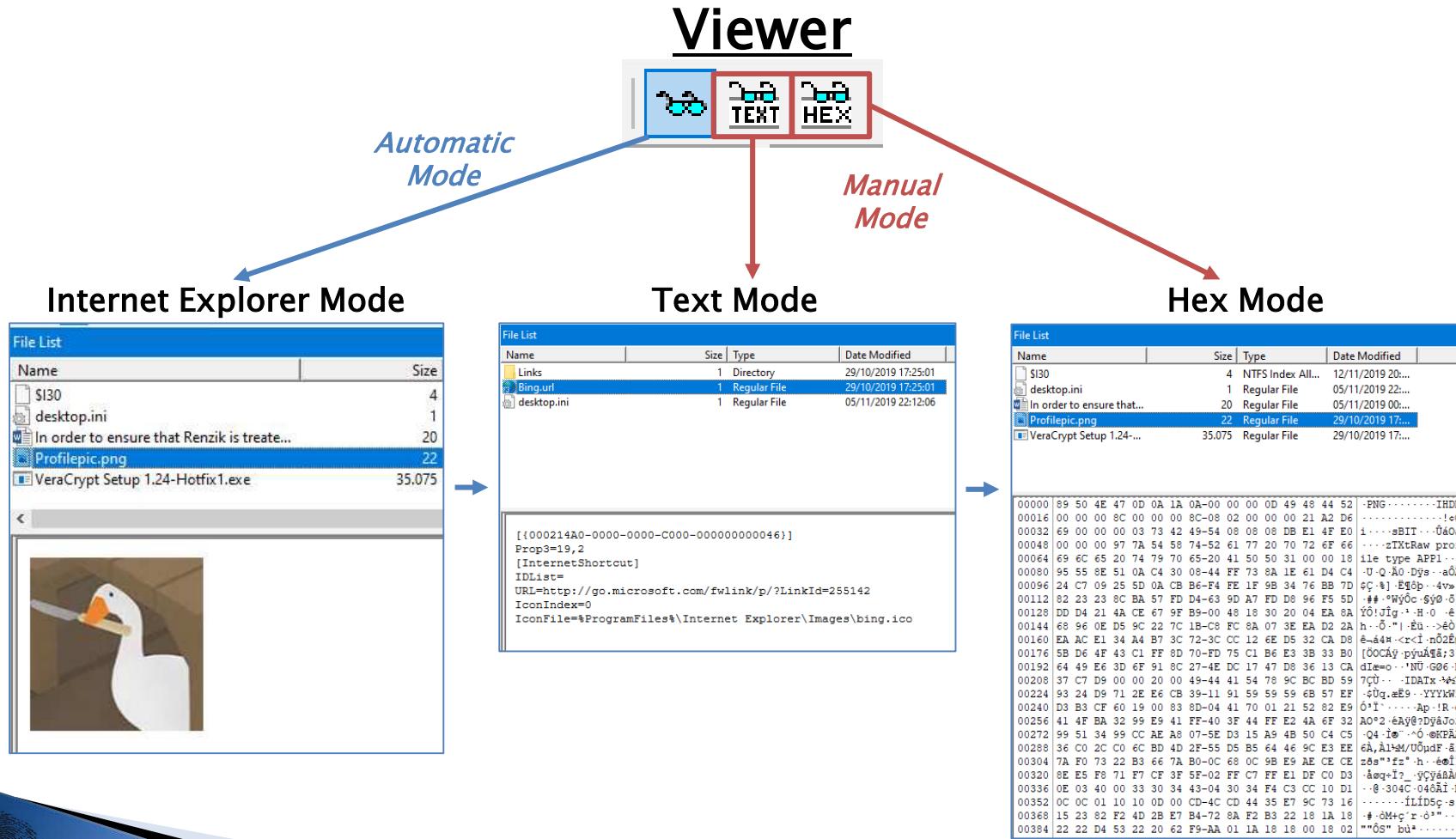


# FTK Imager: *analisi file immagine: GUI*



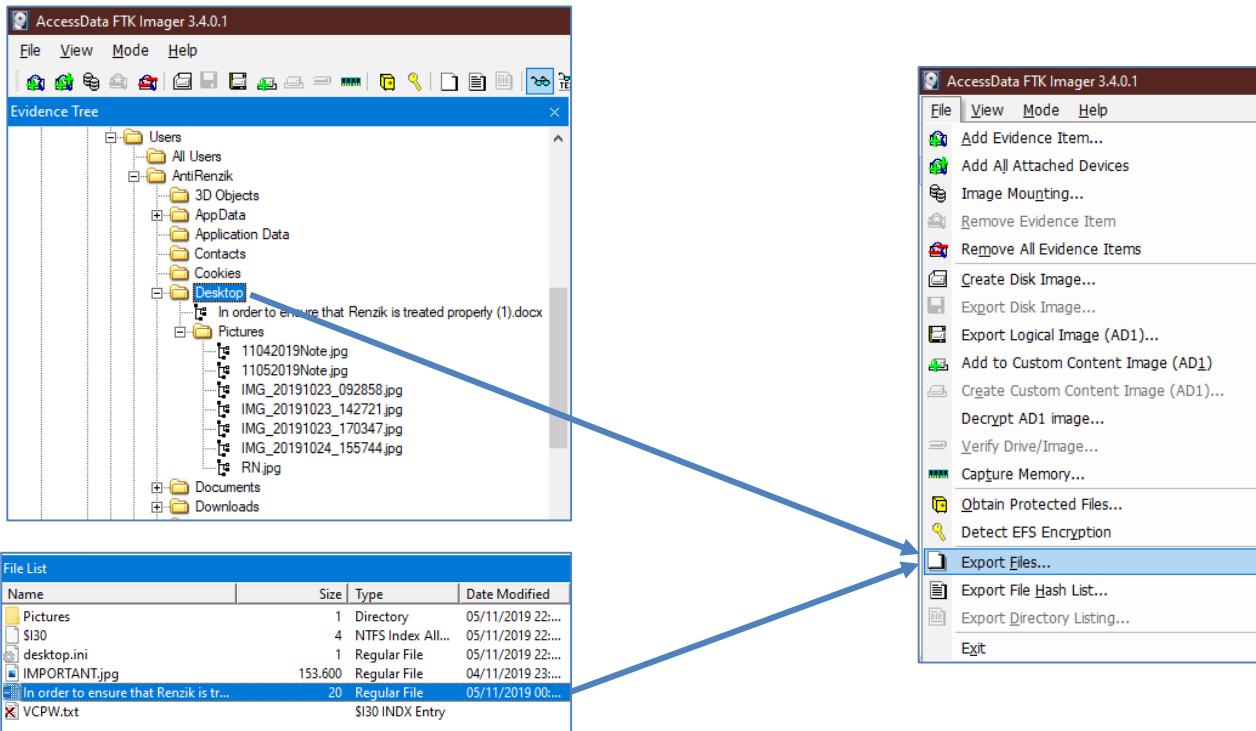
# FTK Imager:

## *analisi file immagine: GUI*



# FTK Imager: *analisi file immagine: Export* Export Files

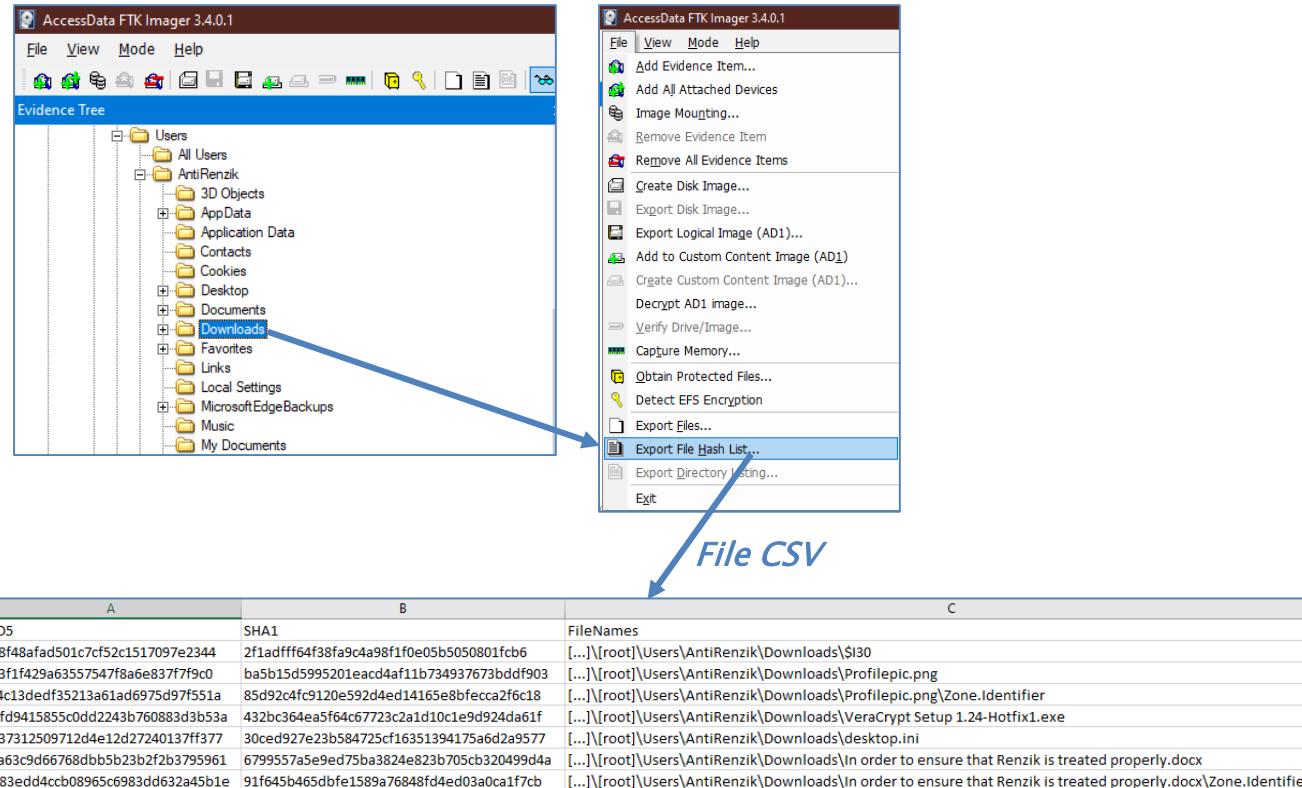
- ▶ Esportazione di un file o di un nodo di cartelle



# FTK Imager: *analisi file immagine: Export*

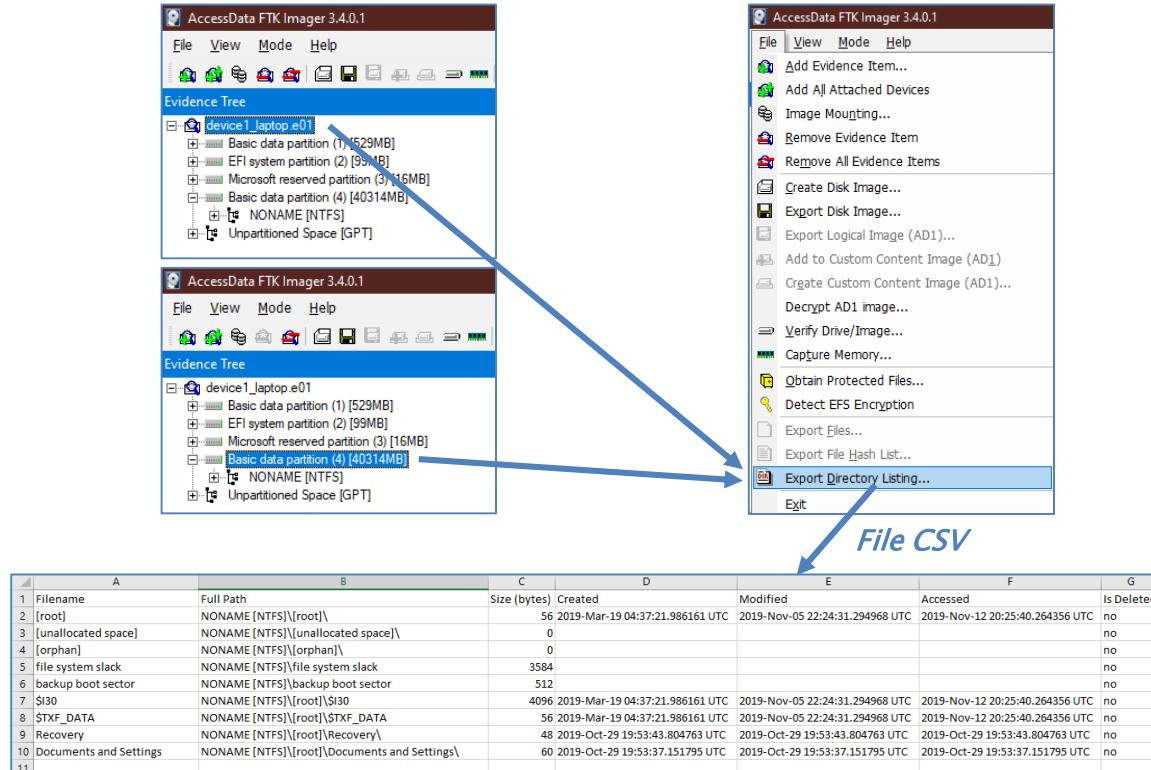
## Export File Hash List

- ▶ Esportazione del calcolo Hash (*MD5/SHA1*) di un file o di un nodo di cartelle



# FTK Imager: *analisi file immagine: Export Export Directory Listing*

- ▶ Esportazione dell'elenco di file e cartelle presenti nell'interno dispositivo/partizione



# L'Analisi

» Strumenti Software



# L'Analisi

## strumenti software

### Toolkit

- ▶ Supporto all'intera fase di analisi

Es.:

- AccessData FTK
- Autopsy
- Encase Forensics
- BlackLight
- X-Ways Forensics
- PassMark OS Forensics

### Tools Forensic Oriented

- ▶ Esecuzione di un specifico task

Es.:

- Internet Evidence Finder
- Amped Five
- Log2Timeline

### Tool Generici

- ▶ Non progettati per la C.F.

Es.:

- USBdeview
- Diff-PDF
- VMWare

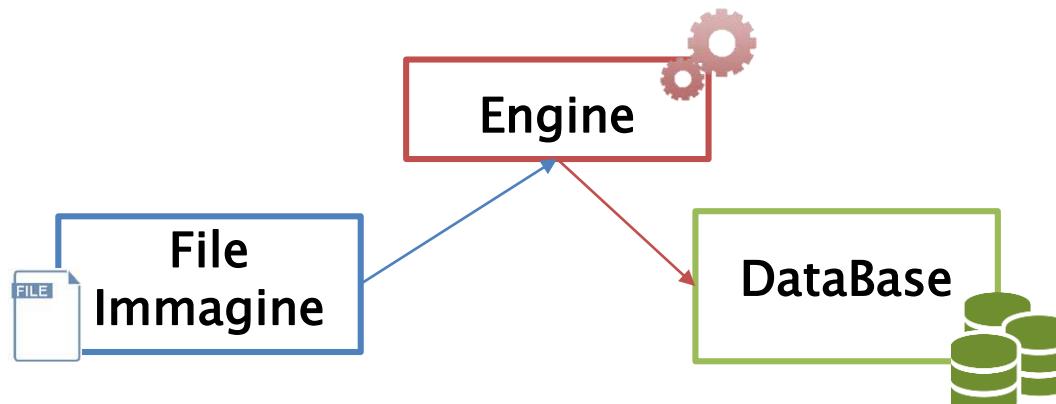
# I Toolkit: overview

## Forensic ToolKit (FTK)

- ▶ Commerciale
- ▶ Microsoft Windows

## Autopsy

- ▶ Free e OpenSource
- ▶ Multiplataforma



Multi-utente / Scalabile

# Fine prima parte...



## SSRI Lorenzo Laurato s.r.l.



Via Coroglio nr. 57/D (BIC- Città della Scienza)  
80124 Napoli



Tel. 335.54.56.550 - 081.19804755



Fax 081.19576037

[lorenzo.laurato@ssrilab.com](mailto:lorenzo.laurato@ssrilab.com) - [info@ssrilab.com](mailto:info@ssrilab.com)  
[ssri@legalmail.it](mailto:ssri@legalmail.it)

# COMPUTER FORENSICS

## Lezione 13: L'Analisi *gli strumenti* *(2<sup>a</sup> parte)*



A.A. 2021/22

Dott. Lorenzo LAURATO



# L'Analisi

## strumenti software

### Toolkit

- ▶ Supporto all'intera fase di analisi

Es.:

- [AccessData FTK](#)
- [Autopsy](#)
- Encase Forensics
- BlackLight
- X-Ways Forensics
- PassMark OS Forensics

### Tools Forensic Oriented

- ▶ Esecuzione di un specifico task

Es.:

- Internet Evidence Finder
- Amped Five
- Log2Timeline

### Tool Generici

- ▶ Non progettati per la C.F.

Es.:

- USBdeview
- Diff-PDF
- VMWare

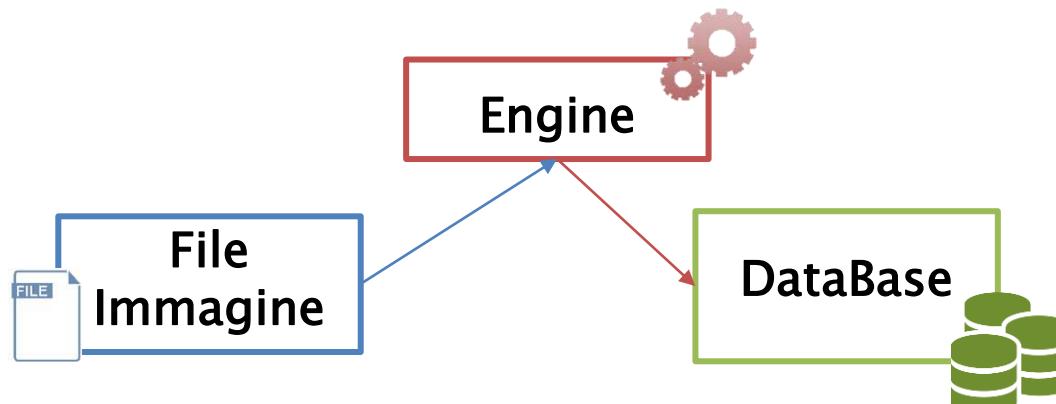
# I Toolkit: overview

## Forensic ToolKit (FTK)

- ▶ Commerciale
- ▶ Microsoft Windows

## Autopsy

- ▶ Free e OpenSource
- ▶ Multiplataforma



Multi-utente / Scalabile

# I Toolkit

## Formati File Immagine

### Forensic ToolKit (FTK)

- ▶ Encase E01
- ▶ Encase L01 Logical Image
- ▶ Expert Witness
- ▶ SnapBack
- ▶ Safeback 2.0 and under
- ▶ ICS
- ▶ Linux DD
- ▶ SMART
- ▶ Ghost (forensic images only)
- ▶ MSVHD (MS Virtual Hard Disk)
- ▶ AccessData Logical Image (AD1)
- ▶ Lx0, Lx01
- ▶ DMG (Mac)
- ▶ VMDK (VmWare Disk)

### Autopsy

- ▶ Encase E01
- ▶ Raw (DD, BIN, IMG)
- ▶ Virtual Disk (VMDK, VHD)

# I Toolkit File System

## Forensic ToolKit (FTK)

- ▶ FAT
- ▶ exFAT
- ▶ NTFS
- ▶ Ext2FS
- ▶ Ext3FS
- ▶ Ext4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ CDFS
- ▶ ReiserFS 3
- ▶ VxFS (Veritas File System)

## Autopsy

- ▶ FAT
- ▶ ExFAT
- ▶ NTFS
- ▶ EXT2FS
- ▶ EXT3FS
- ▶ EXT4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ YAFFS2

# I Toolkit

## Le Viste

Offrono più visualizzazioni delle informazioni contenute nella copia forense

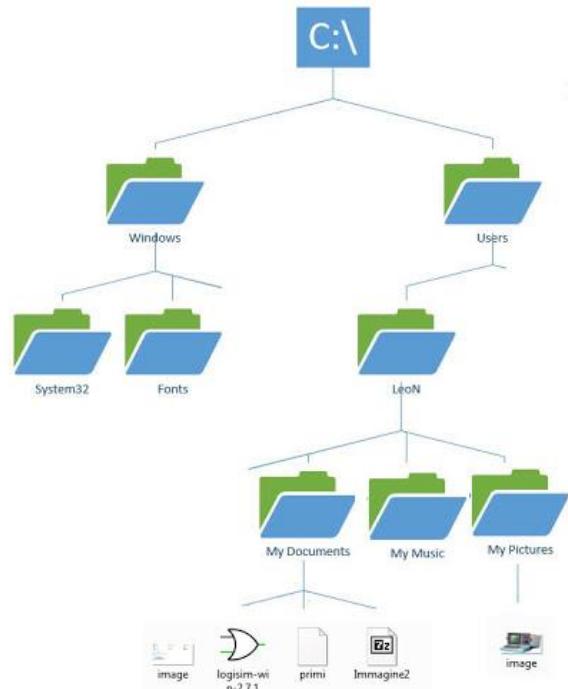


Elaborazione di file e artefatti

# I Toolkit

## Le Viste

### Albero



Rappresentazione gerarchica dei file

# I Toolkit

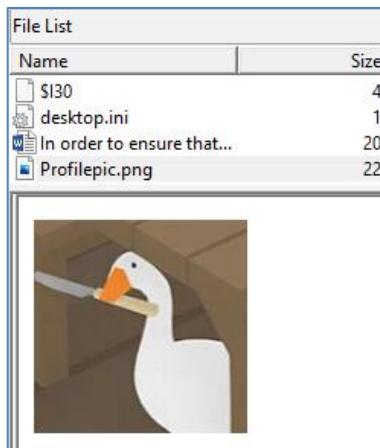
## Le Viste

### File Type

- ▶ **Catalogazione:** analisi dei file per
  - ***estensione*:** suffisso del file
    - .docx, .jpg, .pdf, .zip, etc.
  - ***signature (magic number)*:** sequenza di bit posta in punto ben preciso del file (offset), normalmente prima della sequenza di dati, che serve per definire il formato in cui i dati sono memorizzati.

# I Toolkit Le Viste Signature

Hex signature	89 50 4E 47 0D 0A 1A 0A
ASCII	.PNG....
Offset	0
Ext	PNG



File List				
Name	Size	Type	Date Modified	
\$I30	4	NTFS Index All...	12/11/2019 20...	
desktop.ini	1	Regular File	05/11/2019 22...	
In order to ensure that...	20	Regular File	05/11/2019 00...	
Profilepic.png	22	Regular File	29/10/2019 17...	

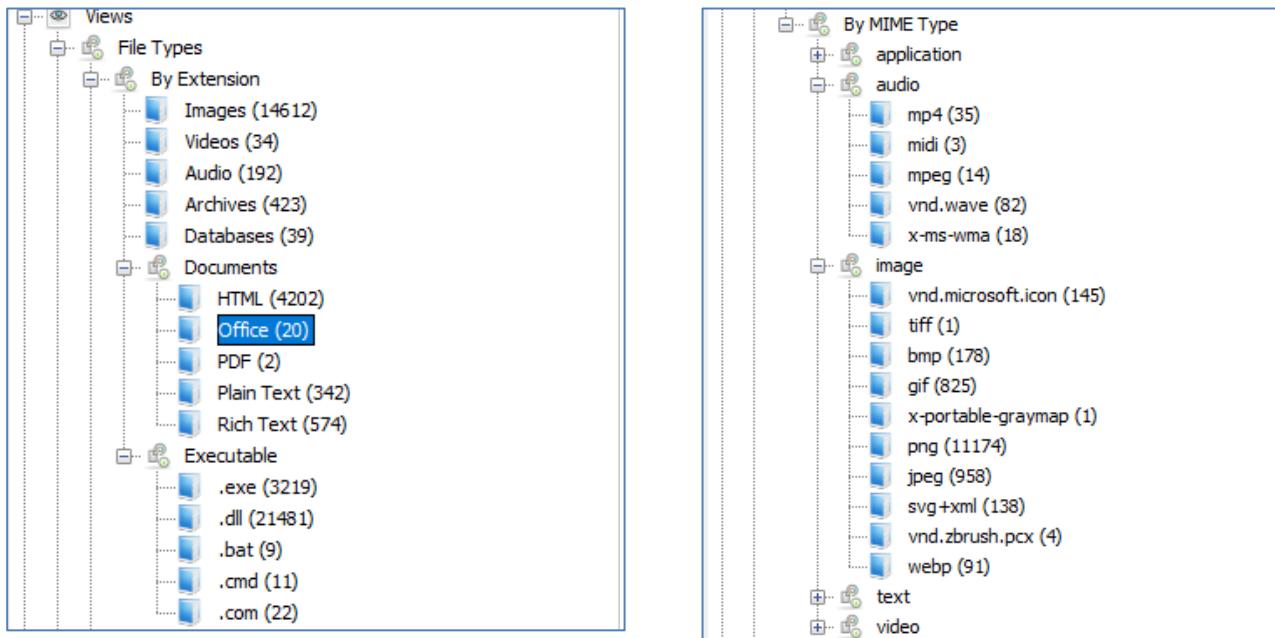
  

0000	89 50 4E 47 0D 0A 1A 0A-100 00 00 00 0D 49 48 44 52	-PNG-	IHDR
0010	00 00 00 8C 00 00 00 8C-08 02 00 00 00 21 A2 D6	.....	!Ö
0020	69 00 00 00 03 73 42 49-54 08 08 08 DB E1 4F E0	i...sBIT	ÚÁÒà
0030	00 00 00 97 7A 54 58 74-52 61 77 20 70 72 6F 66	....zTxtRaw prof	
0040	69 6C 65 20 74 79 70 65-20 41 50 50 31 00 00 18	ile type APPL	

# I Toolkit

## Le Viste

### File Type Autopsy

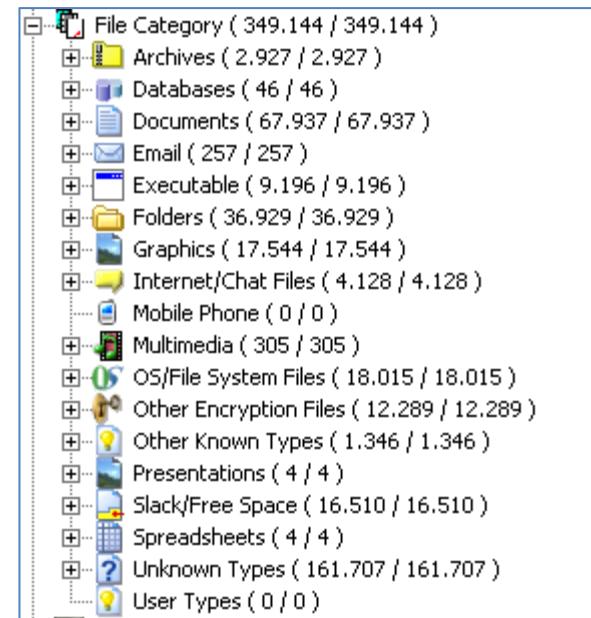
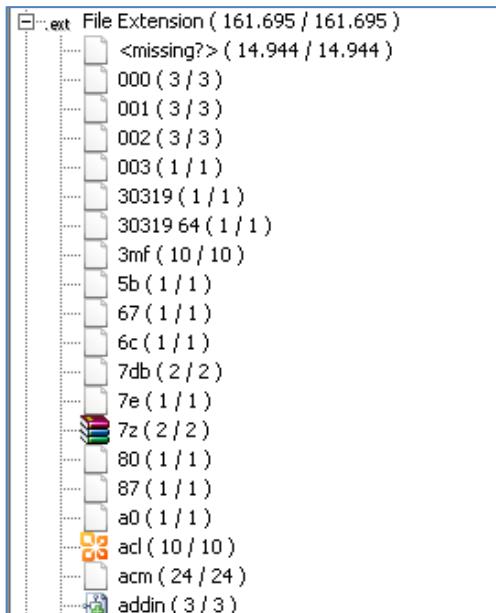


# I Toolkit

## Le Viste

### File Type

FTK

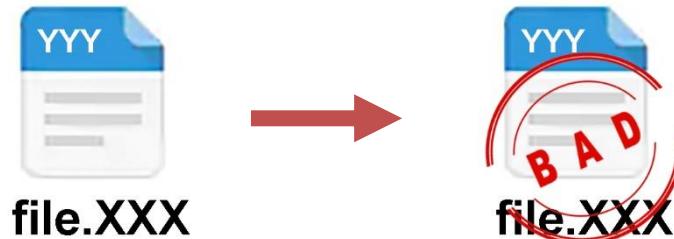


# I Toolkit

## Le Viste

### File Type

- ▶ **Classificazione:** i file vengono analizzati ed arricchiti di alcuni attributi:
  - **Bad Extension:** estensione vs signature



- **Delete file:** file marcati come cancellati dal file system

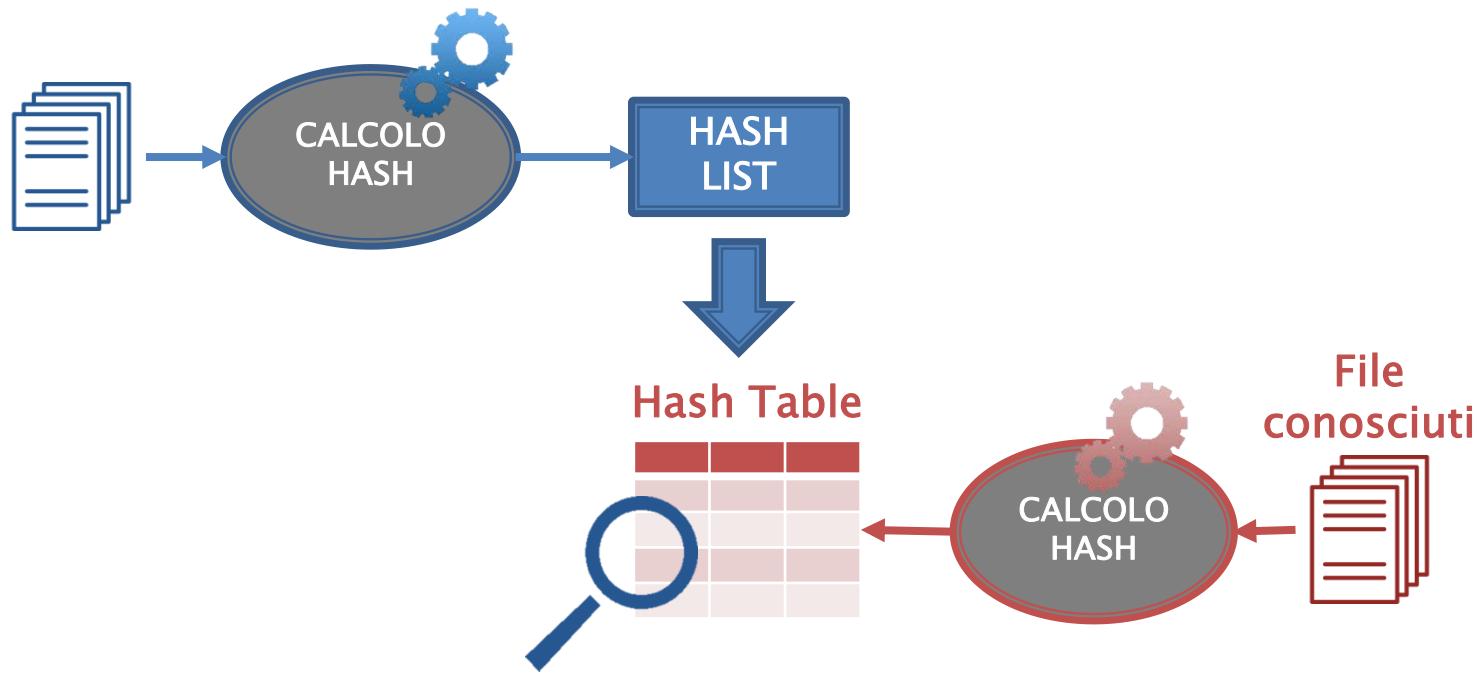


# I Toolkit

## Le Viste

### Known File

- ▶ Riconoscimento del file basato sull'HASH



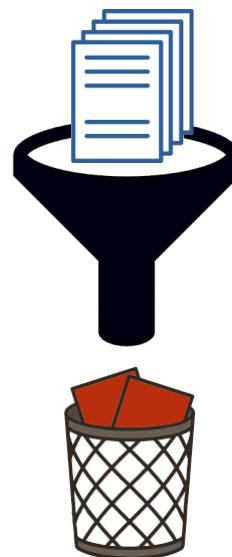
Ignorable File / Notable File

# I Toolkit

## Le Viste

### Known File: *Ignorable File*

- ▶ File conosciuti come di non interesse:
  - Sottrazione di migliaia di File dall'analisi
  - Es: file di sistema/programmi (National Software Reference Library)



# I Toolkit

## Le Viste

### Known File: *Notable File*

- ▶ File conosciuti come di notevole interesse:
  - Ricerca mirata di determinati file
  - Es: Pedopornografia (Project VIC)

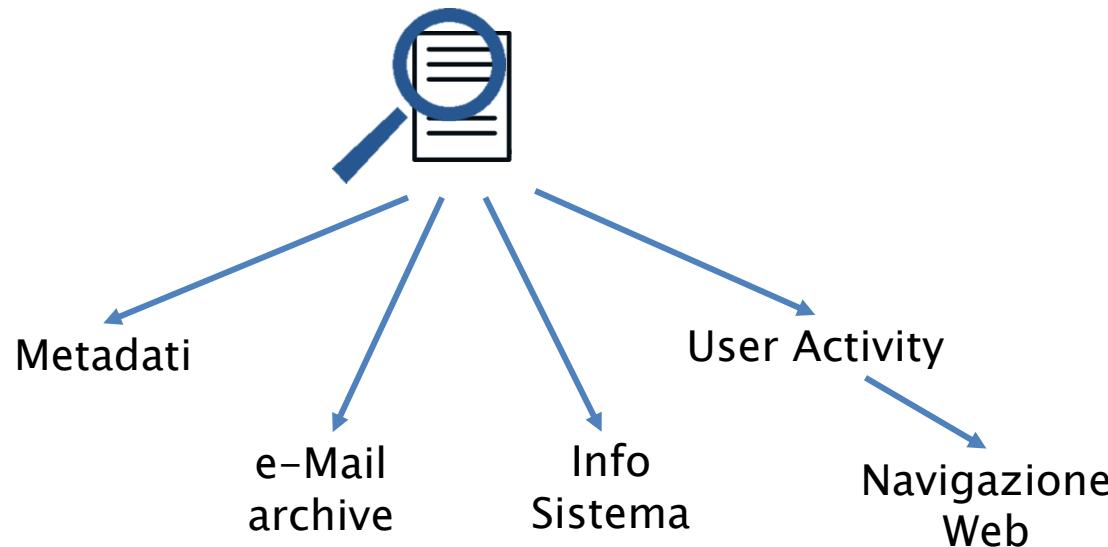


# I Toolkit

## Le Viste

### Artefatti

- ▶ Analisi del contenuto del file:
  - Estrazione ed elaborazione delle informazioni presenti in uno o più file



# I Toolkit

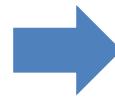
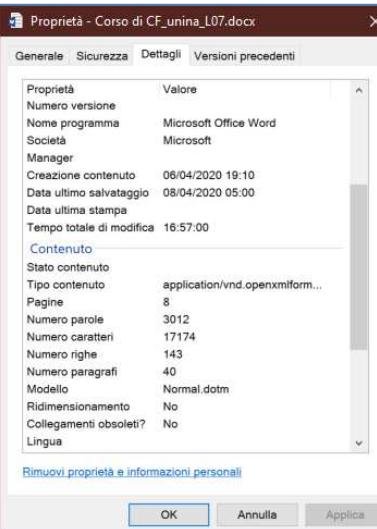
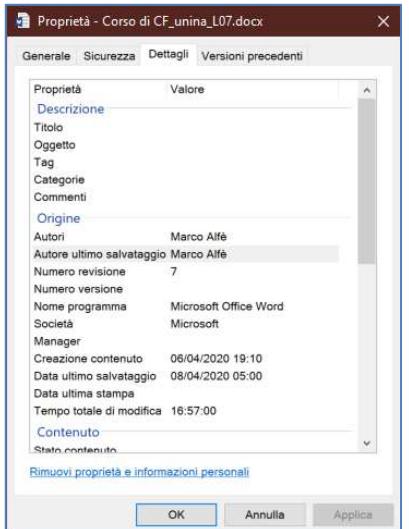
## Le Viste

### Artefatti: *Metadati*

- ▶ dati strutturati contenenti informazioni aggiuntive sul file

Documenti  
(Office, PDF, etc)

FTK



Properties	
Name	Corso di CF_unina_L07.docx
Item Number	351001
File Type	Microsoft Word 2016 XML
Path	Corso di CF_unina_L07.docx
General Info	
Microsoft Office Metadata	
Author	Marco Alfè
Template	Normal.dotm
Last saved by	Marco Alfè
Revision number	7
Total editing time	16 minutes 57 seconds
Create time	06/04/2020 19:10:00 (2020-04-06 17:10:00 UTC)
Last saved time	08/04/2020 05:00:00 (2020-04-08 03:00:00 UTC)
Number of pages	8
Number of words	3.012
Number of characters	17.174
Creating application	Microsoft Office Word
Security	0
Line Count	143
Paragraphs	40
Crop or Scale	False
Document Sections Count	Titolo=1
Company	Microsoft

# I Toolkit

## Le Viste

### Artefatti: *Metadati*

Exif: informazioni sulla fotografia  
(JPEG, TIFF, RIFF)



IMG\_20191023\_170347.jpg

Autopsy

Type	Value
Date Created	2019-10-23 17:03:47
Latitude	29.950344083333334
Longitude	-90.06626891666666
Altitude	10.0
Device Model	BLU R1 HD
Device Make	BLU

FTK

EXIF Entries:	
Exif.Image.Make	BLU
Exif.Image.Model	BLU R1 HD
Exif.Image.Orientation	1
Exif.Image.XResolution	72/1
Exif.Image.YResolution	72/1
Exif.Image.ResolutionUnit	2
Exif.Image.Software	MediaTek Camera Application
Exif.Image.DateTime	2019:10:23 17:03:47
Exif.Image.YCbCrPositioning	2
Exif.Image.ExifTag	426
Exif.Image.GPSTag	812
Exif.Photo.ExposureTime	2327/1000000
Exif.Photo.FNumber	20/10
Exif.Photo.ExposureProgram	0
Exif.Photo.ISOSpeedRatings	106
Exif.Photo.ExifVersion	48 50 50 48
Exif.Photo.DateTimeOriginal	2019:10:23 17:03:47
Exif.Photo.DateTimeDigitized	2019:10:23 17:03:47
Exif.Photo.ComponentsConfiguration	1 2 3 0
Exif.Photo.ExposureBiasValue	0/10
Exif.GPSInfo.GPSVersionID	2 2 0 0
Exif.GPSInfo.GPSLatitudeRef	N
Exif.GPSInfo.Latitude	29/1 57/1 12387/10000
Exif.GPSInfo.LongitudeRef	W
Exif.GPSInfo.Longitude	90/1 3/1 585681/10000
Exif.GPSInfo.AltitudeRef	0
Exif.GPSInfo.Altitude	10/1
Exif.GPSInfo.GPSTimeStamp	22/1 3/1 20/1
Exif.GPSInfo.GPSProcessingMethod	65 83 67 73 73 0 0 0 78 69 84 87 79 82 75
Exif.GPSInfo.GPSDateStamp	2019:10:23

# I Toolkit

## Le Viste

### Artefatti: *e-Mail Archive*

#### ▶ Analisi degli archivi/database e-Mail:

- Visualizzazione delle e-Mail
- Estrazione degli allegati



The screenshot shows the Autopsy Forensic Browser interface. On the left, a 'File List' pane displays a list of files, including various emails and attachments. A specific email from 'Goose Honkerson' to 'We Have Renzik' is selected. A large blue arrow points from this selected email to the right-hand analysis panes. The 'File Content' pane shows the raw email message, which includes the recipient's name and a threatening message. The 'Email Attachments' pane shows two attachments: 'RN.jpg' and 'IMG\_20191023\_092858.jpg'. The bottom right corner of the slide features the text 'Autopsy ≡ FTK' in red.

File List

Subject	Submit Time	From	To
Photos	01/11/2019 21:12:46 ...	PeacockLeprechaun <peacockleprechaun@gmail.com>	antrenzik@gmail.com
ARG questions	01/11/2019 21:24:57 ...	PeacockLeprechaun <peacockleprechaun@gmail.com>	Goose Honkerson <antrenzik@gmail.com>
Undelivered Mail Returned to Sender	01/11/2019 21:30:43 ...	MAILER-DAEMON@mailstream-east.mxrecord.io (<...>)	antrenzik@gmail.com
Fareed: The Middle East Is Still Fertile Ground for Terror Groups	01/11/2019 23:20:49 ...	Fareed's Global Briefing <GlobalBriefing@cnn.com>	<antrenzik@gmail.com>
We Have Renzik	01/11/2019 23:27:26 ...	Goose Honkerson <antrenzik@gmail.com>	PeacockLeprechaun <peacockleprechaun@gmail.com>
Re: ARG questions	01/11/2019 23:30:33 ...	Goose Honkerson <antrenzik@gmail.com>	briancarrier@basistech.com
Re: ARG questions	01/11/2019 23:32:01 ...	Goose Honkerson <antrenzik@gmail.com>	PeacockLeprechaun <peacockleprechaun@gmail.com>
The Point: The impeachment vote had no tricks -- and no treats	01/11/2019 23:32:56 ...	Chris Cillizza <ccilliza@cnn.com>	<antrenzik@gmail.com>
We Have Renzik	01/11/2019 23:33:11 ...	Goose Honkerson <antrenzik@gmail.com>	info@basistech.com
Re: ARG questions	01/11/2019 23:35:10 ...	Goose Honkerson <antrenzik@gmail.com>	PeacockLeprechaun <peacockleprechaun@gmail.com>
225 days; McHenry and Fox; Deadspin's future; Warzel's remin...	02/11/2019 02:22:57 ...	Brian Stelter <brian.stelter@cnn.com>	<antrenzik@gmail.com>
What happens when dreams come true?	02/11/2019 13:08:50 ...	CNN's Good Stuff <TheGoodStuff@cnn.com>	
Day 9 - What The Heck Is Mining?	02/11/2019 19:32:29 ...	"The Bitcoin.com Team" <team@bitcoin.com>	

File Content

From: Goose Honkerson <antrenzik@gmail.com>  
Sent: 01/11/2019 15:33:11 -0700  
To: info@basistech.com  
Subject: We Have Renzik  
Attachments: RN.jpg; IMG\_20191023\_092858.jpg

My dearest Mr Carrier,

We have Renzik, and we have had him for a few days. Do not try to find him, we have specifically ensured that he is safely hidden. You will hear from us in 24 hours with more details.

All Hail Hash

Email Attachments

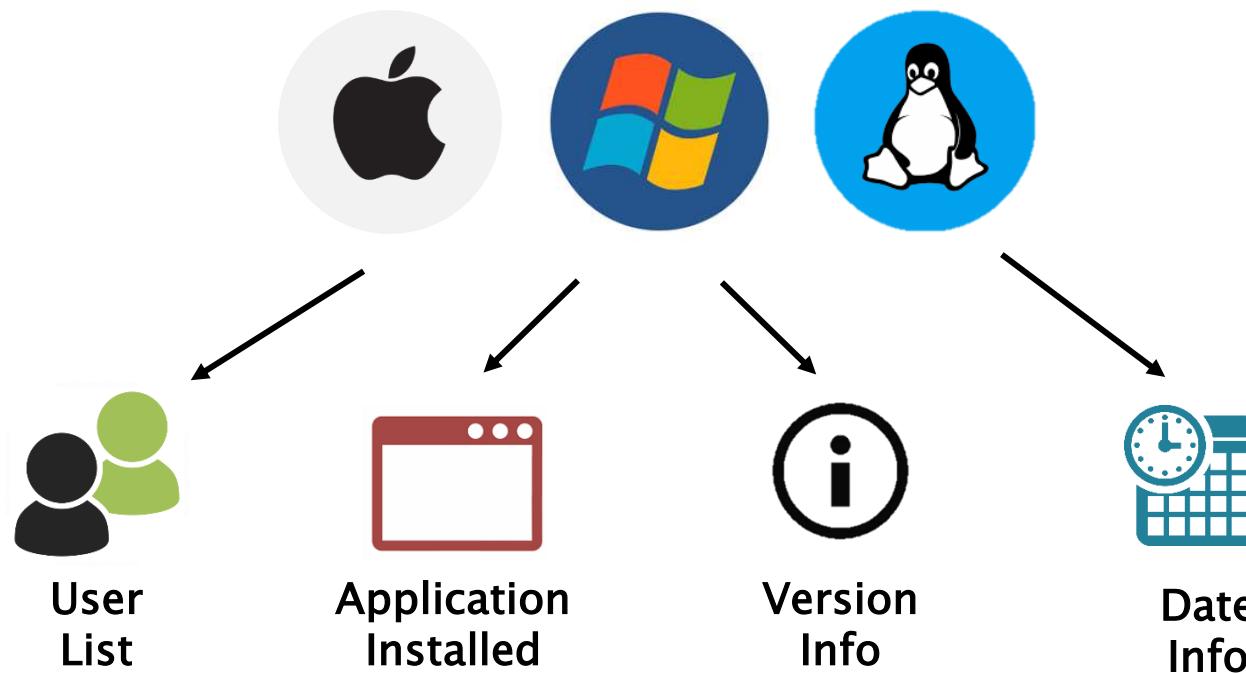
- entry #23494986.eml
- RN.jpg
- IMG\_20191023\_092858.jpg

# I Toolkit

## Le Viste

### Artefatti: *System Information*

- ▶ Estrazione delle informazioni dell'ambiente di lavoro

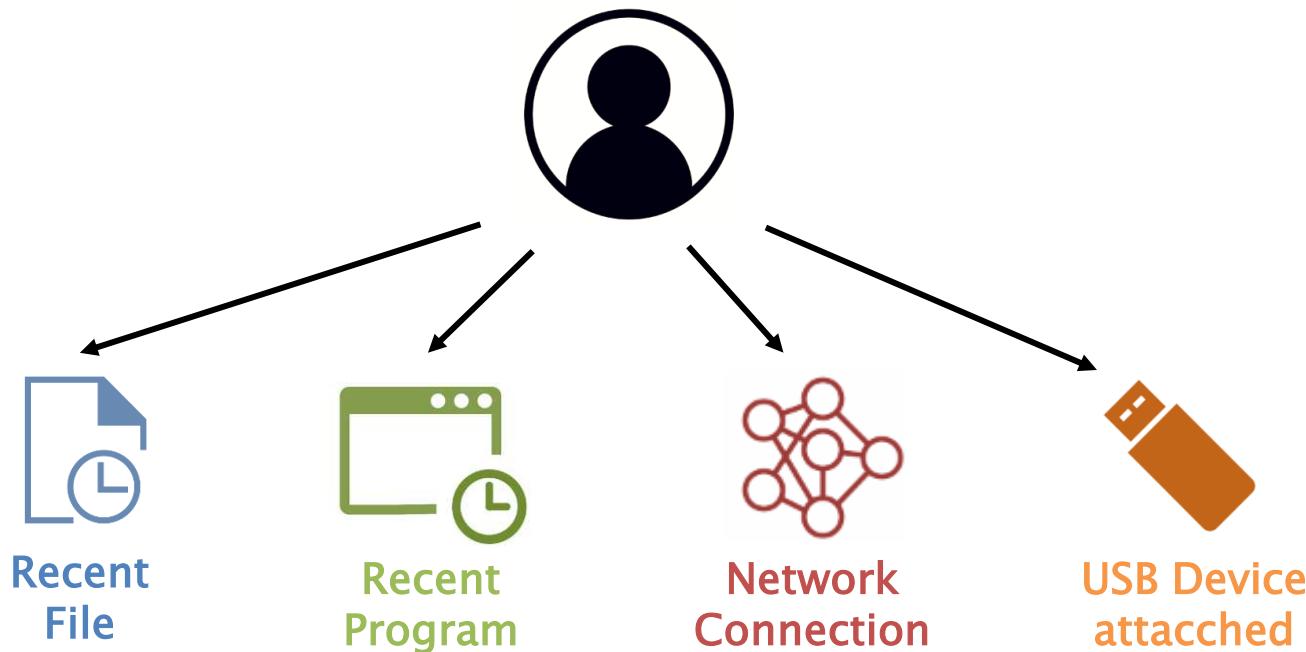


# I Toolkit

## Le Viste

### Artefatti: *User Activity*

- ▶ Analisi delle attività eseguite dall'utente: *File di registro, log, etc.*

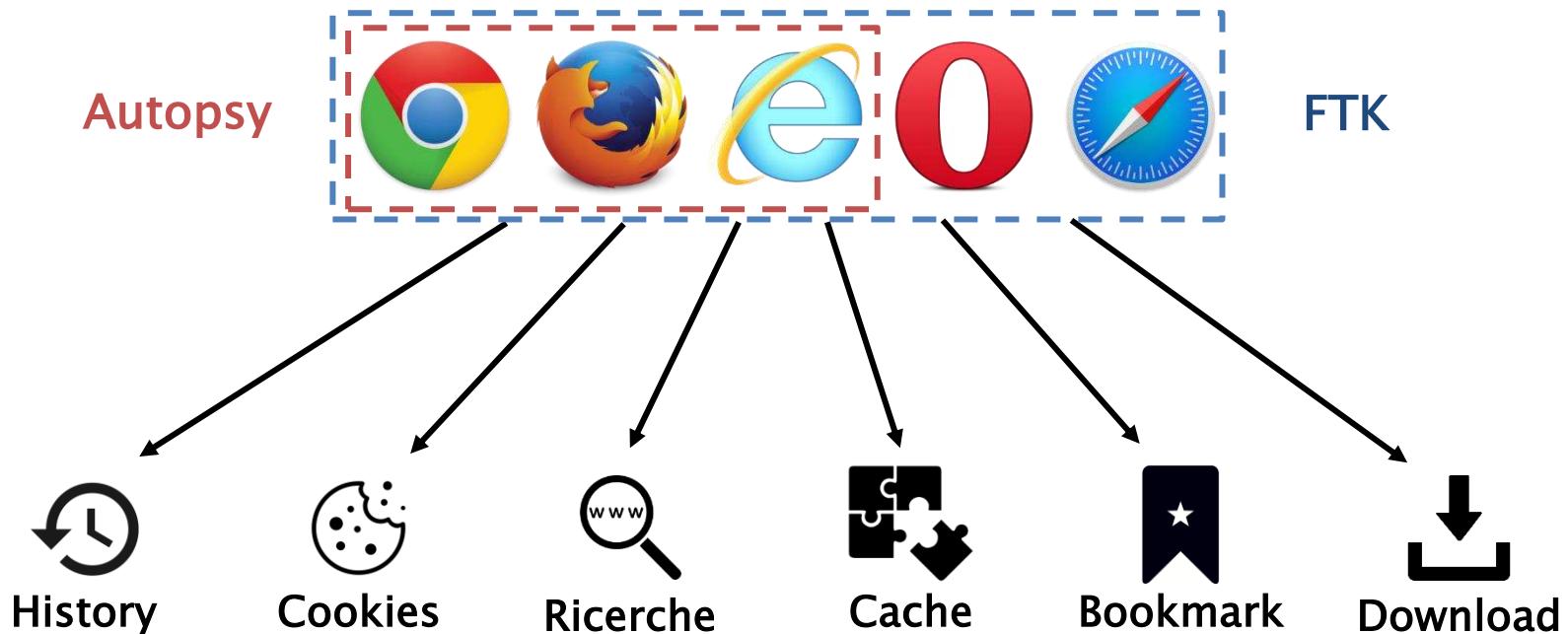


# I Toolkit

## Le Viste

### Artefatti: *Navigazione WEB*

- ▶ Analisi dei file dei browser web: *history, cookies, cache, download, search, autofill.*



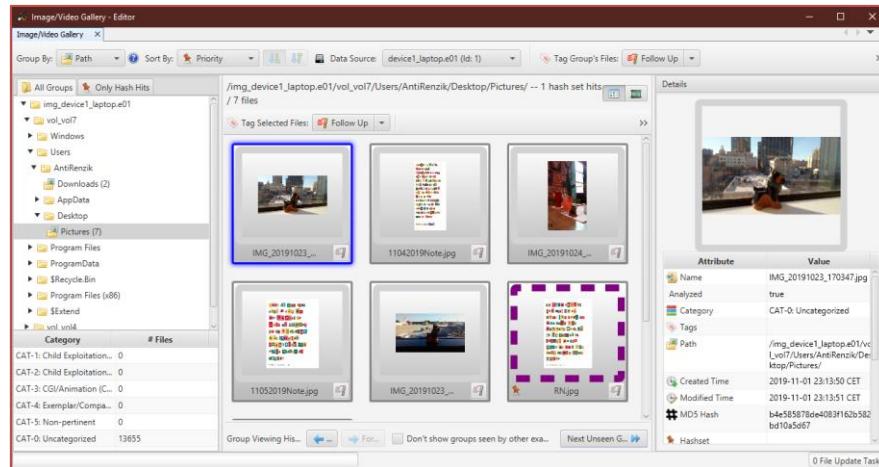
# I Toolkit

## Le viste specializzate

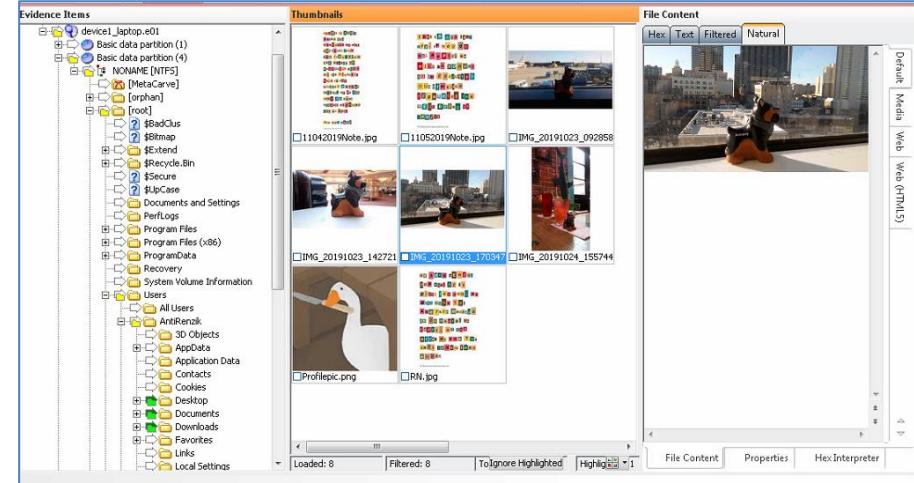
### Image Gallery

- ▶ Generazione e visualizzazione di *thumbnail* dei file grafici

### Autopsy



### FTK



# I Toolkit

## Le viste specializzate

### Video Gallery

- ▶ Processo di elaborazione per l'estrazione e la visualizzazione di frame dai video:
  - Ogni valore % del video (*5%, 10%, etc.*)
  - Ogni intervallo di tempo (*1min, 5min, etc.*)

The screenshot shows a timeline of video frames from a file named "Photos\_FRE\_Carousel\_Explore\_620x252.mp4". The timeline is displayed in a grid format, with each row representing a second from 00:00:00 to 00:00:07. Each frame thumbnail shows a scene with a smartphone, a laptop, and a potted plant. The interface includes a header with file metadata and a navigation bar with tabs like Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, and Video Triage.

Autopsy

The screenshot shows the FTK software interface with a "Video Thumbnails" view. On the left, there is a tree view of multimedia files, including 256 images, 186 audios, 0 RIFF files, 70 videos, and 69 WMP playlists. To the right, a grid of video thumbnails is displayed, showing various frames from different video clips. Some thumbnails have text overlays such as "YOU ARE A SECRET ADVENTURE" and "I VOTED". At the bottom, there are status bars for loaded, filtered, total, highlighted, checked, and total Lsize.

SSRI

SICUREZZA SISTEMI  
RETI INFORMATICHE

UNIVERSITÀ DEGLI STUDI DI  
NAPOLI FEDERICO II

a.a. 2021/22

# I Toolkit

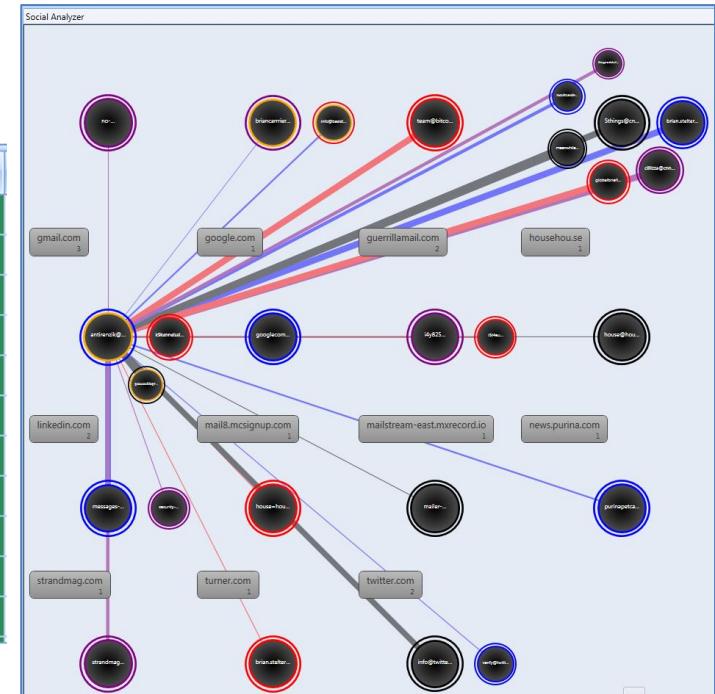
## Le viste specializzate

### Social Analyzer

- ▶ Visualizzazione delle relazioni/connesioni avvenute tra i diversi soggetti (*eMail*)

FTK

Display Name	Email Address	Traffic Count	Sent	Received
(mail delivery system)		1	1	0
good morning from cnn	5things@cnn.com	13	13	0
	antrenzik@gmail.com	139	12	127
brian stelter	brian.stelter@cnn.com	12	12	0
brian stelter	brian.stelter@turner.com	1	1	0
	briancarrier@basistech.com	1	0	1
chris cillizza	cillizza@cnn.com	13	13	0
cnn's global briefing	globalbriefing@cnn.com	13	13	0
google community team	googlecommunityteam-noreply@google.com	1	1	0
house house	house@househou.se	1	1	0
house house	house=househou.se@mail8.mcsignup.com	1	1	0



# I Toolkit

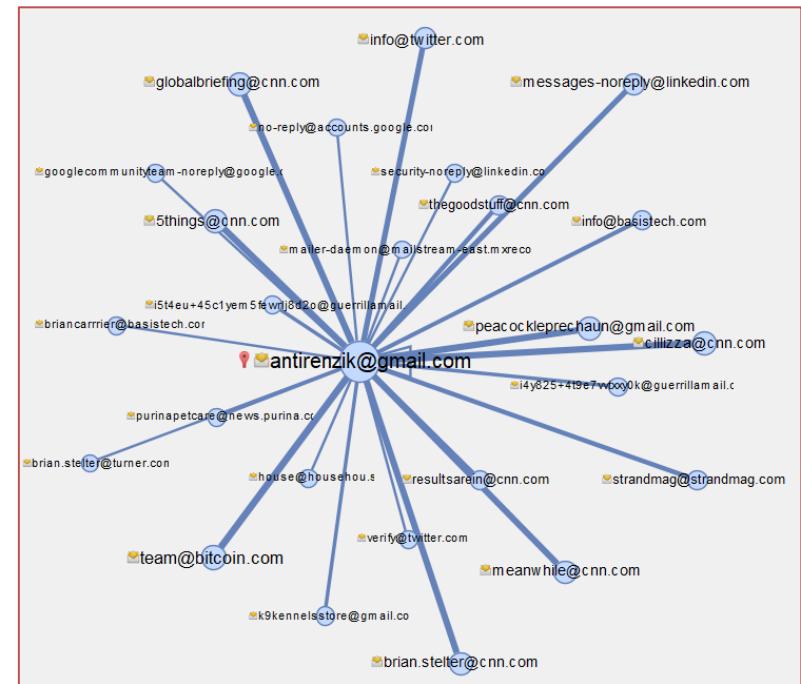
## Le viste specializzate

### Social Analyzer

- ▶ Visualizzazione delle relazioni/connesioni avvenute tra i diversi soggetti (*eMail*)

Account	Device	Type	Items
<a href="#">antrenzik@gmail.com</a>	device1_laptop.e01	Email	276
<a href="#">team@bitcoin.com</a>	device1_laptop.e01	Email	34
<a href="#">5things@cnn.com</a>	device1_laptop.e01	Email	26
<a href="#">peacockleprechaun@gmail.com</a>	device1_laptop.e01	Email	26
<a href="#">globalbriefing@cnn.com</a>	device1_laptop.e01	Email	26
<a href="#">cillizza@cnn.com</a>	device1_laptop.e01	Email	26
<a href="#">brian.stelter@cnn.com</a>	device1_laptop.e01	Email	24
<a href="#">meanwhile@cnn.com</a>	device1_laptop.e01	Email	22
<a href="#">messages-noreply@linkedin.com</a>	device1_laptop.e01	Email	14
<a href="#">info@twitter.com</a>	device1_laptop.e01	Email	14

Autopsy



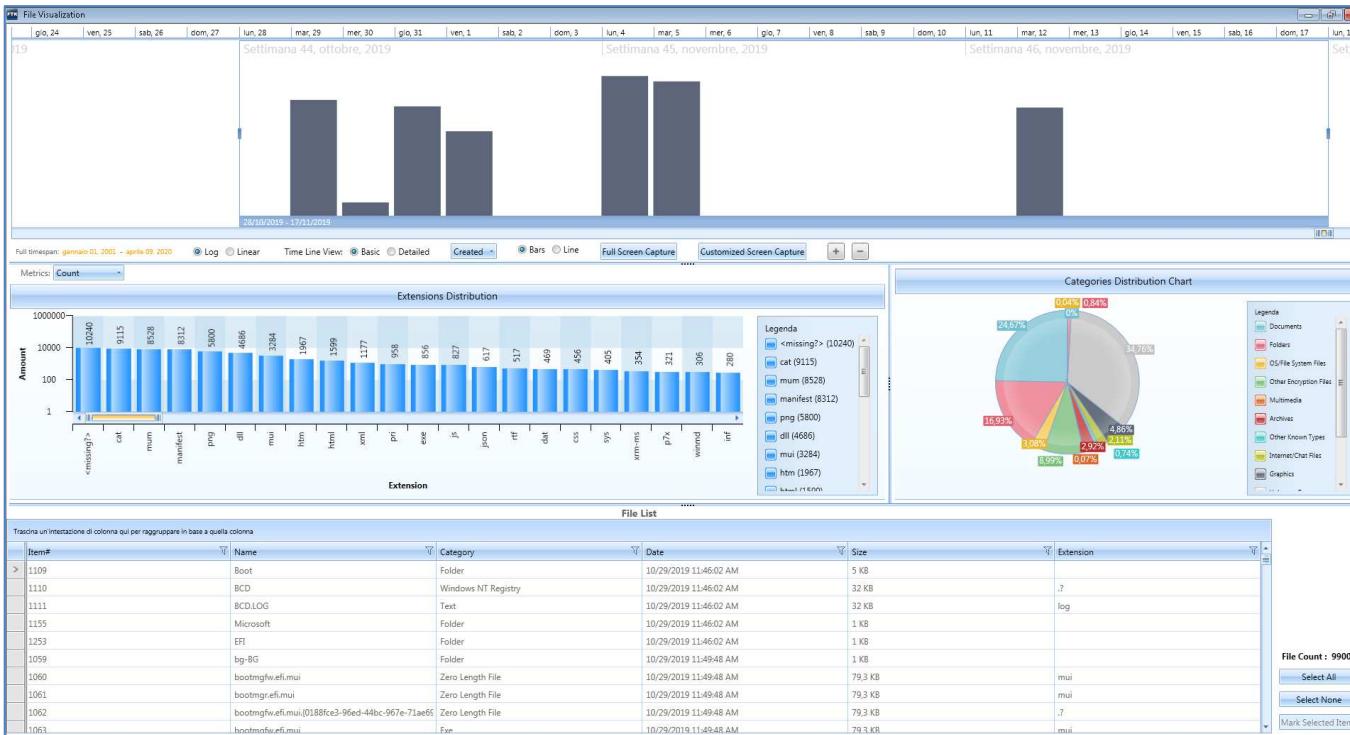
# I Toolkit

## Le viste specializzate

### TimeLine

- ▶ Visualizzazione temporale dei file

### FTK

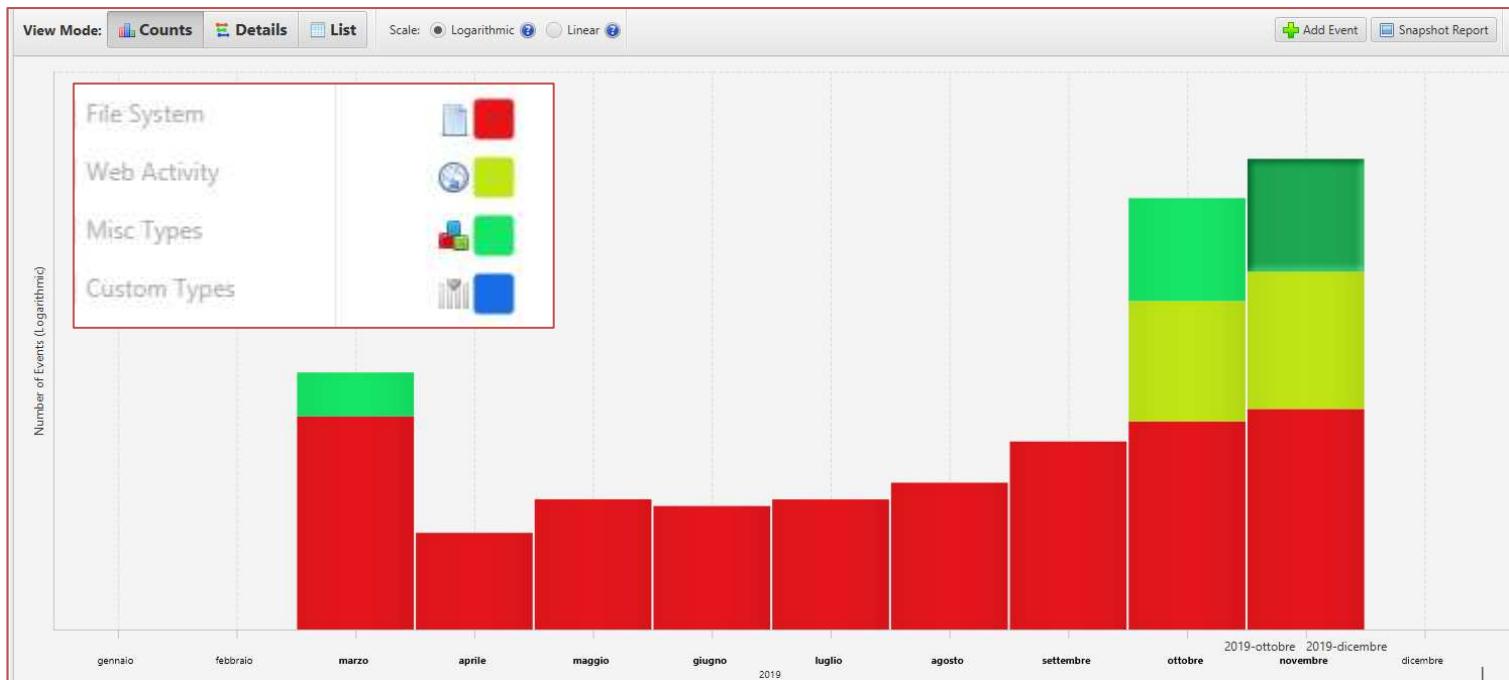


# I Toolkit

## Le viste specializzate

### TimeLine

- ▶ Visualizzazione temporale dei file
- Autopsy

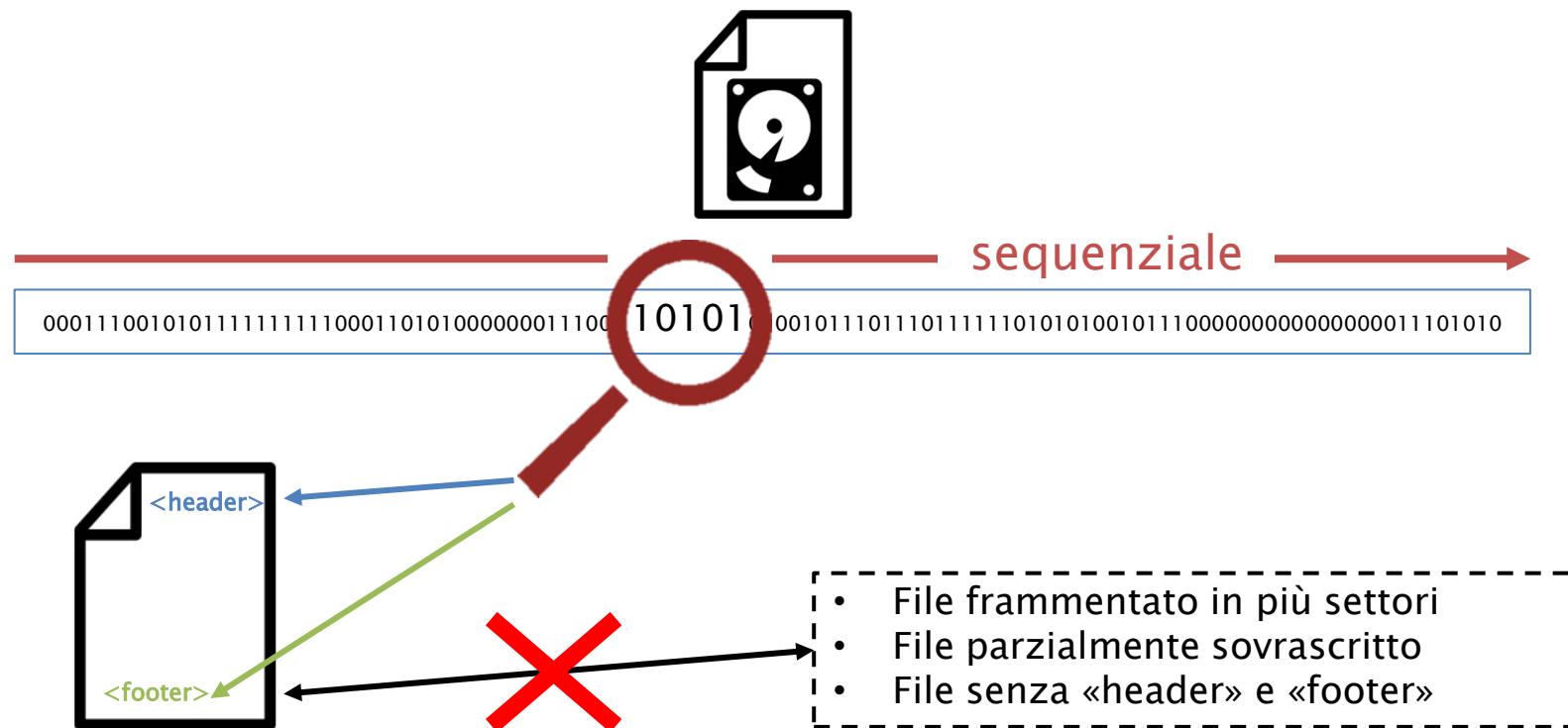


# I Toolkit

## Altri strumenti

# File Carving

- ▶ Recupero dei file non più residenti nel file system



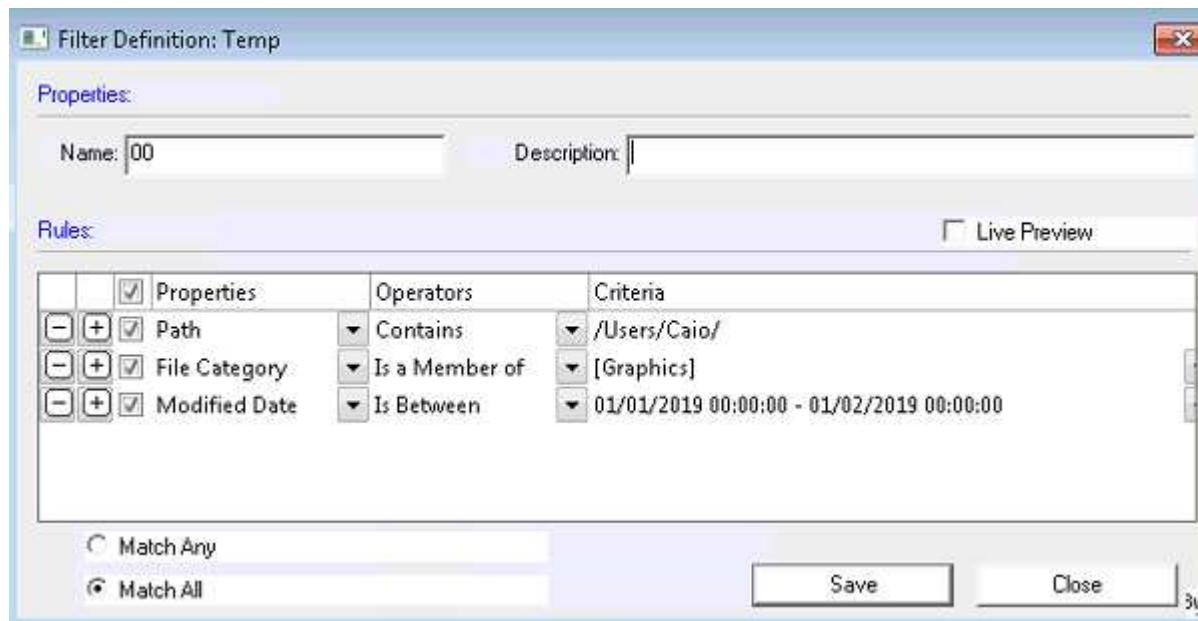
# I Toolkit

## Altri strumenti

### Ricerche semi manuali

#### ▶ Ricerca tramite attributi

- Es.: immagini presenti nel profilo utente di CAIO che si riferiscono al periodo gennaio 2019.



# I Toolkit

## Altri strumenti

### Ricerche semi manuali

- ▶ **Document Content:** estrazione di determinate informazioni mediante regular expression



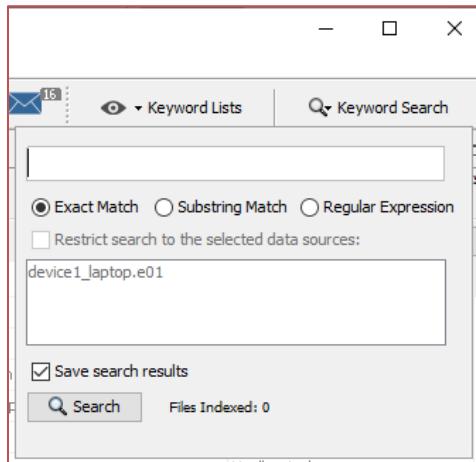
# I Toolkit

## Altri strumenti

Ricerche semi manuali

- ▶ **Indexing:** ricerche di determinate parole chiave

Autopsy



FTK

dtSearch®



Search Index	
Terms	
Indexed Words	Total Hits
prova	46
provacsettingindex	278
provadefogo	2
provadofazendeiro	2
provalertlistener	15
provando	2
provar	58
provare	11
provàrà	1
provate	1

# I Toolkit

## Altri strumenti



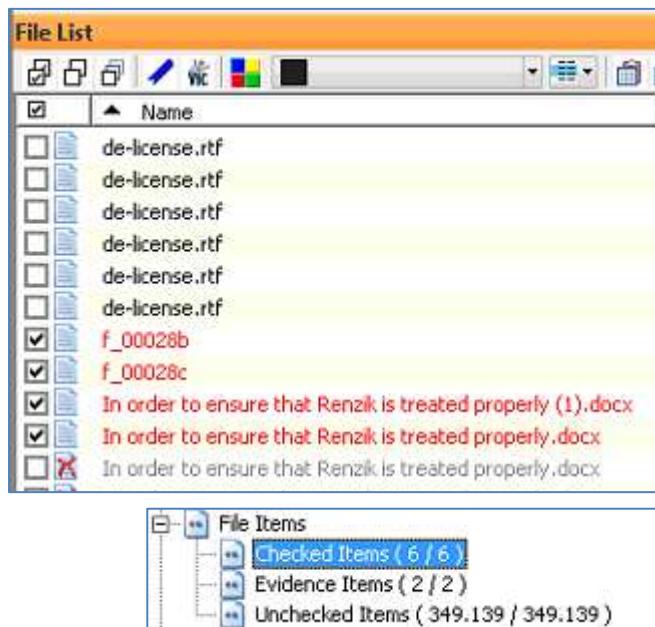
- ▶ Decrypt
- ▶ Malware Analysis
- ▶ Processing Image:
  - PhotoDNA
  - Riconoscimento Immagine/Viso
- ▶ Traduttore

# I Toolkit Export/Report

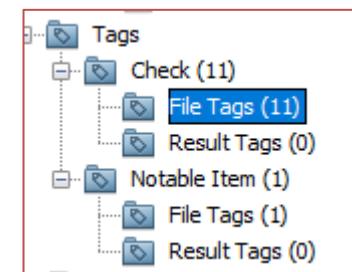
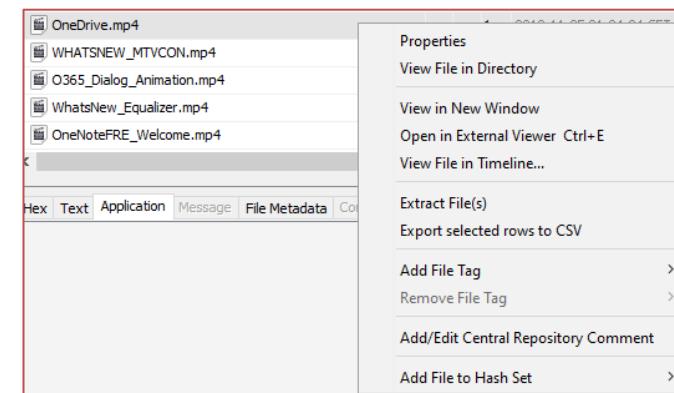
## ▶ Esportare i file di interesse:

- Etichette/Tag
- Checkbox

FTK



Autopsy



# I Toolkit

## Export/Report

### Autopsy

**Report Navigation**

- Case Summary
- Hashset Hits (0)
- Keyword Hits (0)
- Tagged Files (11)
- Tagged Images (11)
- Tagged Results (0)

**Autopsy Forensic Report**

HTML Report Generated on 2020/05/08 02:06:05

Case: Case1  
Number of Images: 3  
Examiner: Marco

**Image Information:**  
device1\_laptop.e01

**FTK CASE REPORT**

**Case Summary**

- Case Information
- File Overview
- Evidence List

**Bookmarks**

**Graphics**

**Videos**

- Page 1

**File Paths**

- Checked Items

**File Properties**

- Checked Items

**Selected Registry Types**

**Case Information**

Time zone for display: ora legale Europa occidentale

Version	AccessData Forensic Toolkit Version: 7.2.0.4127
Case Owner	AD-SSRILAB\FTK
Case Name	case1
Case Reference	
Case Description	
Report Created	08/05/2020 02:05:59
Agency/Company	
Investigator's Name	
Address	
Phone	
Fax	
Email	
Comments	

AccessData Forensic Toolkit®

FTK

**SSRI**  
SICUREZZA SISTEMI  
RETI INFORMATICHE

UNIVERSITÀ DEGLI STUDI DI  
NAPOLI FEDERICO II  
a.a. 2021/22

# Fine seconda parte...



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 14: L'Analisi *Autopsy* (1<sup>a</sup> parte)



A.A. 2021/22

Dott. Lorenzo LAURATO



# Autopsy

»» Configurazione



# Autopsy

## *download*

- ▶ Risorsa: *<https://www.autopsy.com/download/>*

### Download Autopsy

VERSION 4.19.3 FOR WINDOWS

[DOWNLOAD 64-BIT >](#)

### DOWNLOAD FOR LINUX AND OS X

Autopsy 4 will run on Linux and OS X. To do so:

- Download the Autopsy [ZIP file](#) (NOTE: This is not the latest version)
- Linux will need The Sleuth Kit [Java .deb Debian package](#)
- Follow the [instructions](#) to install other dependencies

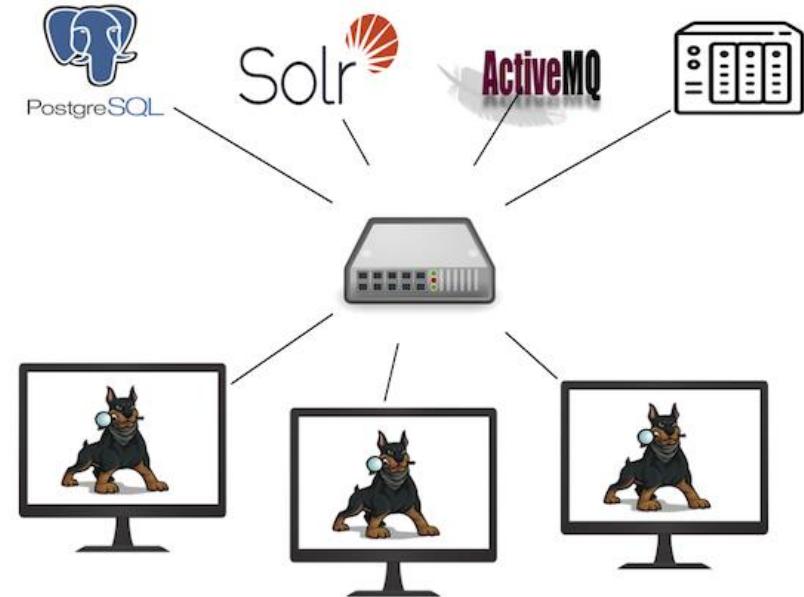
# Autopsy

## *configurazione*

**Single User**



**Multi User**



# Autopsy

## *configurazione*

### *Central Repository*

- ▶ Database in cui vengono memorizzate le informazioni di casi precedentemente analizzati:
  - Conoscere se un file è già stato rinvenuto;
  - Evidenziare automaticamente un file come di notevole interesse (*notable file*);
  - Case DB più leggero;

# Autopsy

## configurazione

### Central Repository

The screenshot shows the Autopsy interface with the 'Central Repository' module selected in the top navigation bar. The main window displays configuration options for the Central Repository, including:

- Database Configuration:** Type: Disabled, Name: (empty), Location: (empty). A checkbox labeled "Use a Central Repository" is checked.
- Correlation Properties:** A link to "Manage Correlation Properties".
- Organizations:** A link to "Manage Organizations".
- Case Details:** A link to "Manage Cases".
- Note:** "Configure the database to enable this module."

A blue arrow points from the "Manage Correlation Properties" button in the main window to the "Manage Correlation Properties" dialog box. This dialog box contains the following text and table:

Enable one or more correlation properties to use for correlation during ingest. Note, these properties are global and impact all users of the Central Repository.

Correlation Properties	Enable
Files	<input checked="" type="checkbox"/>
Domains	<input checked="" type="checkbox"/>
Email Addresses	<input checked="" type="checkbox"/>
Phone Numbers	<input checked="" type="checkbox"/>
USB Devices	<input checked="" type="checkbox"/>
Wireless Networks	<input checked="" type="checkbox"/>
MAC Addresses	<input checked="" type="checkbox"/>
IMEI Number	<input checked="" type="checkbox"/>
IMSI Number	<input checked="" type="checkbox"/>
ICCID Number	<input checked="" type="checkbox"/>

Buttons at the bottom of the dialog box include "OK" and "Cancel".

# Autopsy

## *creazione del caso*

The screenshot shows the Autopsy 4.14.0 interface. On the left, the main menu bar includes Case, View, Tools, Window, Help, and a highlighted New Case option with the keyboard shortcut Ctrl+N. A red box and arrow point from the New Case menu item to the first step of the 'New Case Information' dialog. The 'Case Information' tab is selected in the dialog, which contains fields for Case Name (CaseTest), Base Directory (C:\Cases\), and Case Type (Single-user). Below this, a note states 'Case data will be stored in the following directory:' followed by the path C:\Cases\CaseTest. A second red box and arrow point from the 'Optional Information' link in the 'Steps' section of the dialog to the second step of the dialog, which is titled 'Optional Information'. This step includes fields for Case Number (0705-2020), Examiner Name (Marco), and Organization analysis settings.

Autopsy 4.14.0

Case View Tools Window Help

New Case **Ctrl+N**

Open Recent Case

Open Case **Ctrl+O**

Unpack and Open Portable Case

Close Case

Delete Case

Add Data Source

Case Details

Data Source Summary

Exit

New Case Information

Steps

1. Case Information  
2. Optional Information

Case Information

Case Name: CaseTest

Base Directory: C:\Cases\

Case Type:  Single-user  Multi-user

Case data will be stored in the following directory:  
C:\Cases\CaseTest

New Case Information

Steps

1. Case Information  
2. **Optional Information**

Optional Information

Case

Number: 0705-2020

Examiner

Name: Marco

Phone:

Email:

Notes:

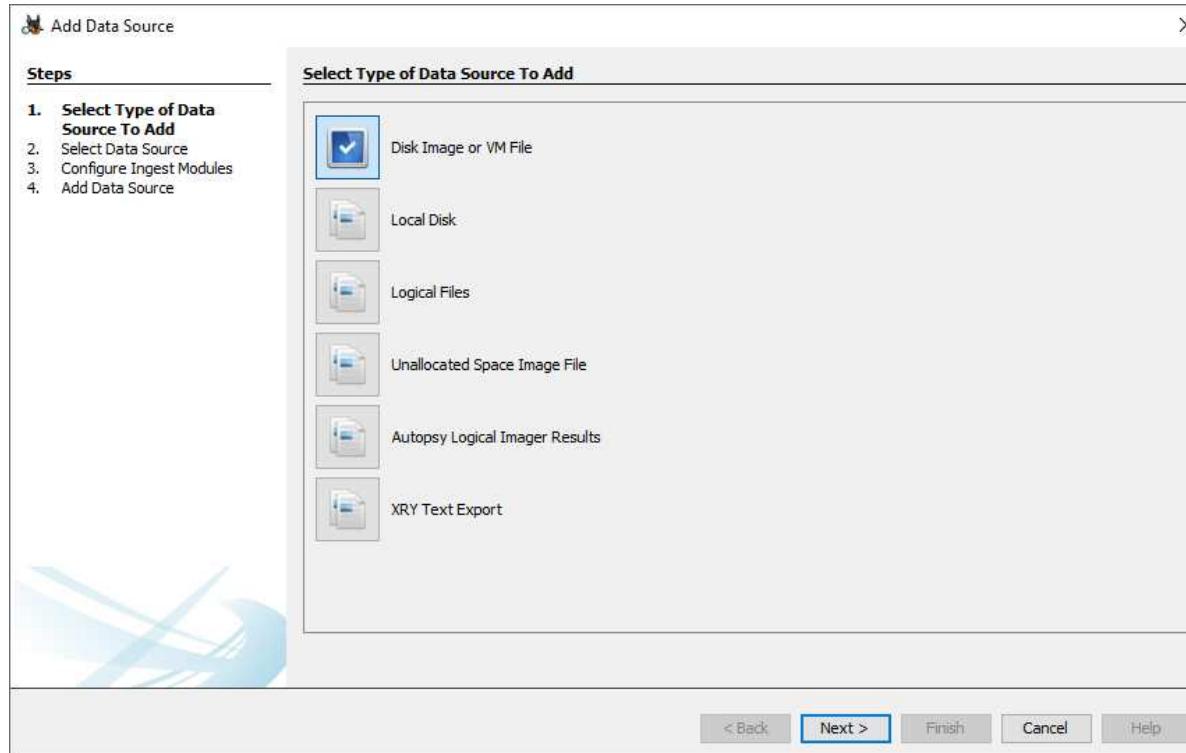
Organization

Organization analysis is being done for: Not Specified

< Back

# Autopsy

## *creazione del caso*



# Autopsy

## *configurazione*

 Add Data Source

**Steps**

1. Select Type of Data Source To Add
- 2. Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

**Select Data Source**

Path: C:\autopsy\device1\_laptop.e01

Ignore orphan files in FAT file systems

Time zone: (GMT +1:00) Europe/Berlin

Sector size: Auto Detect

Hash Values (optional):

MDS:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

# Autopsy

## Formati supportati

### Disk Image:

- ▶ Encase E01
- ▶ Raw (DD, BIN, IMG)
- ▶ Virtual Disk (VMDK, VHD)

### Volume:

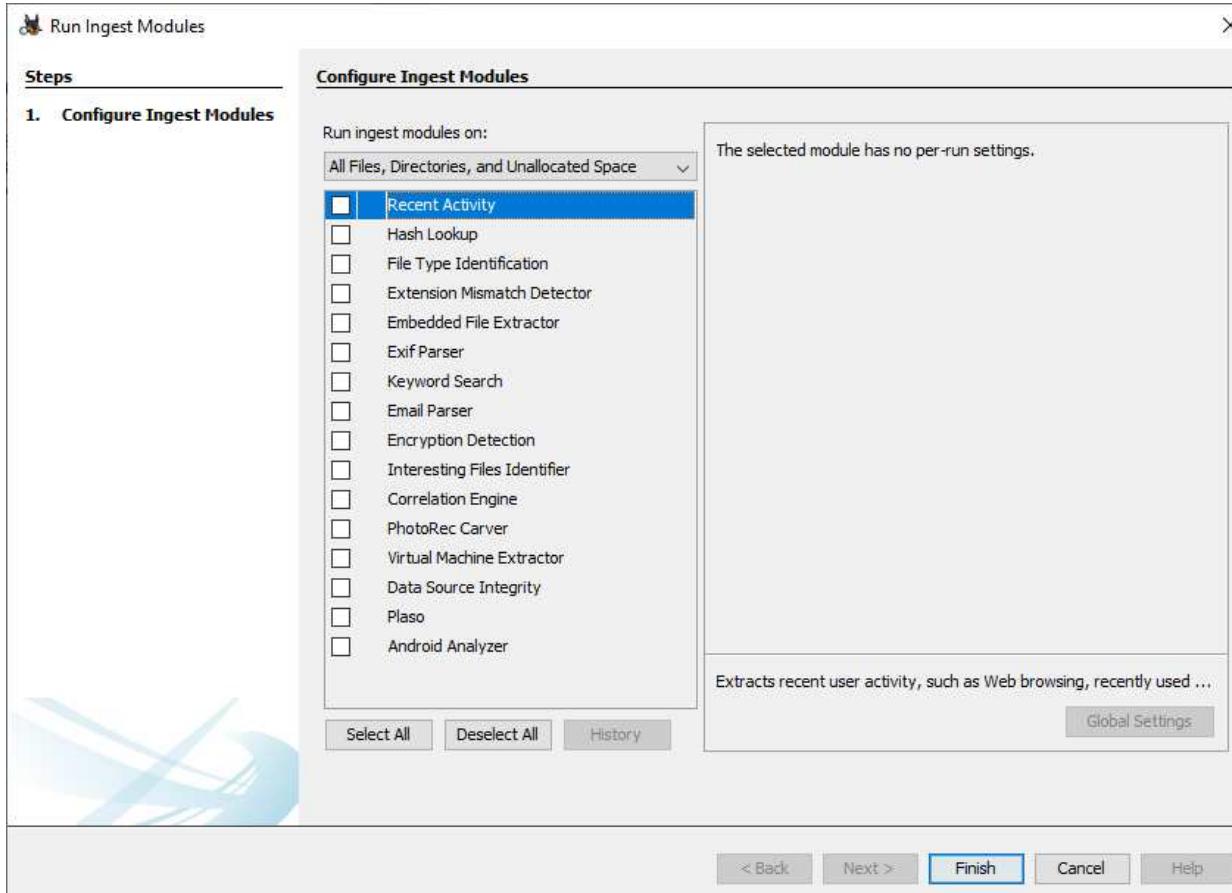
- ▶ DOS
- ▶ GPR
- ▶ MAC
- ▶ BSD
- ▶ Solaris

### File System:

- ▶ FAT
- ▶ ExFAT
- ▶ NTFS
- ▶ EXT2FS
- ▶ EXT3FS
- ▶ EXT4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ YAFFS2

# Autopsy

## *creazione del caso*



# Autopsy

» Graphical User Interface

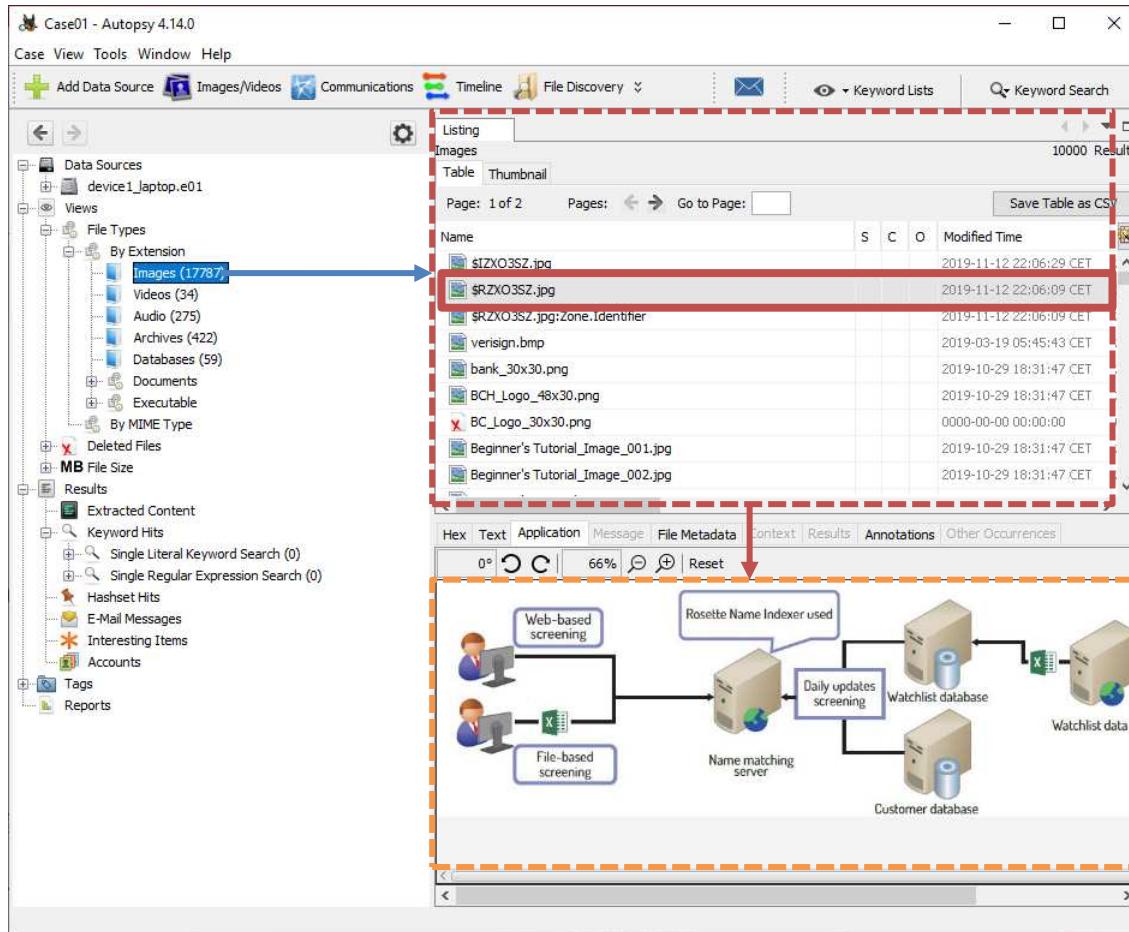


# Autopsy GUI

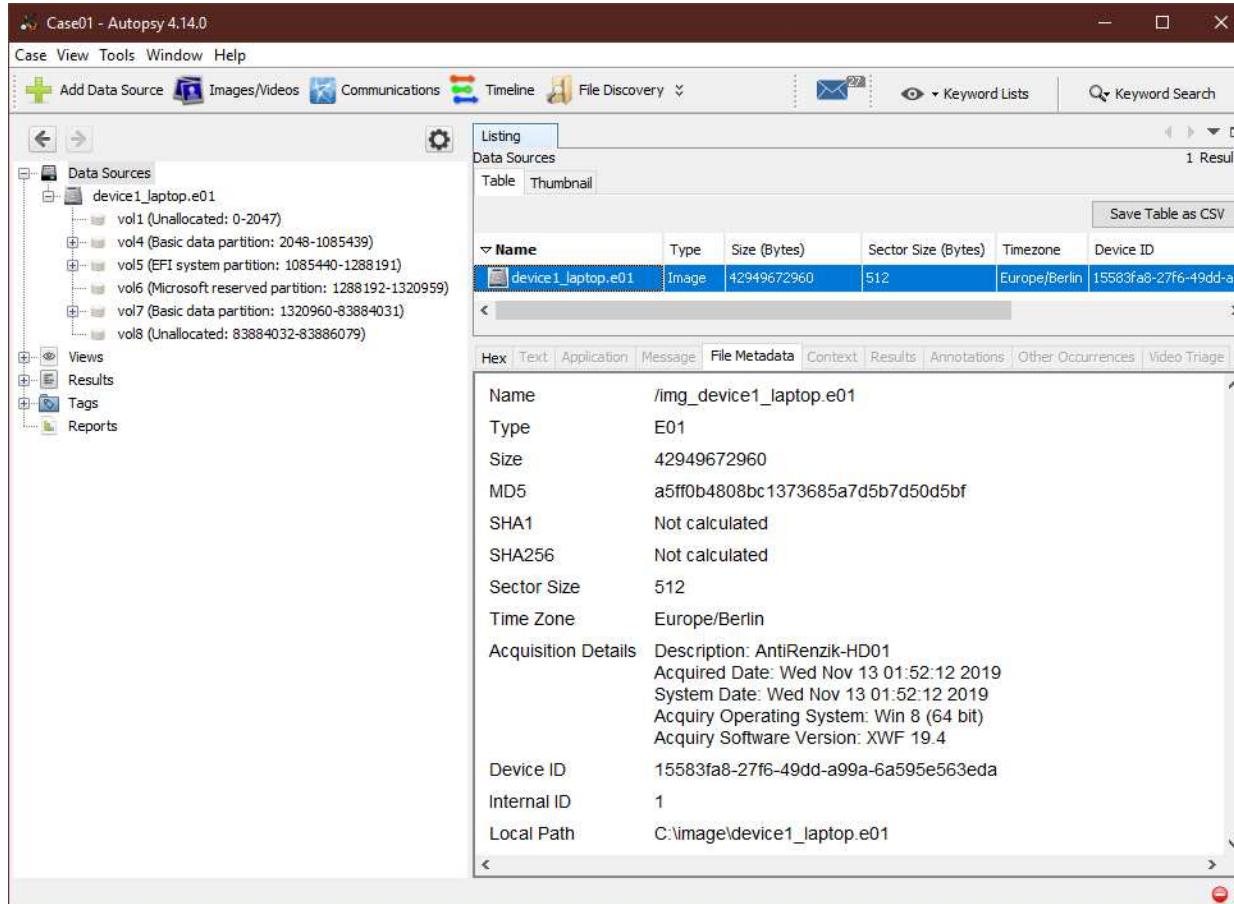
The screenshot shows the Autopsy 4.14.0 interface with several panes:

- Evidence Tree**: Shows the file system structure of the evidence source "device\_1\_laptop.e01". It includes partitions vol1 through vol8, various folders like \$OrphanFiles, \$Extend, \$Recycle.Bin, and \$Unalloc, and specific files like desktop.ini.
- Views**: A sidebar with options like File Types, Deleted Files, and MB File Size.
- Results**: A sidebar with results from keyword searches, regular expressions, and hashset hits.
- Tags**: A sidebar with options for Tags and Reports.
- File List**: A table view showing the contents of the "/img\_device1\_laptop.e01/vol7/Users" directory. The table has columns for Name, S, C, O, Modified Time, Change Time, and Access. One row is highlighted with a red border.
- Viewer**: A detailed view pane showing file metadata for a selected file, including Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, Strings, Indexed Text, and Translation tabs. The "Text" tab displays the content of "desktop.ini".

# Autopsy GUI

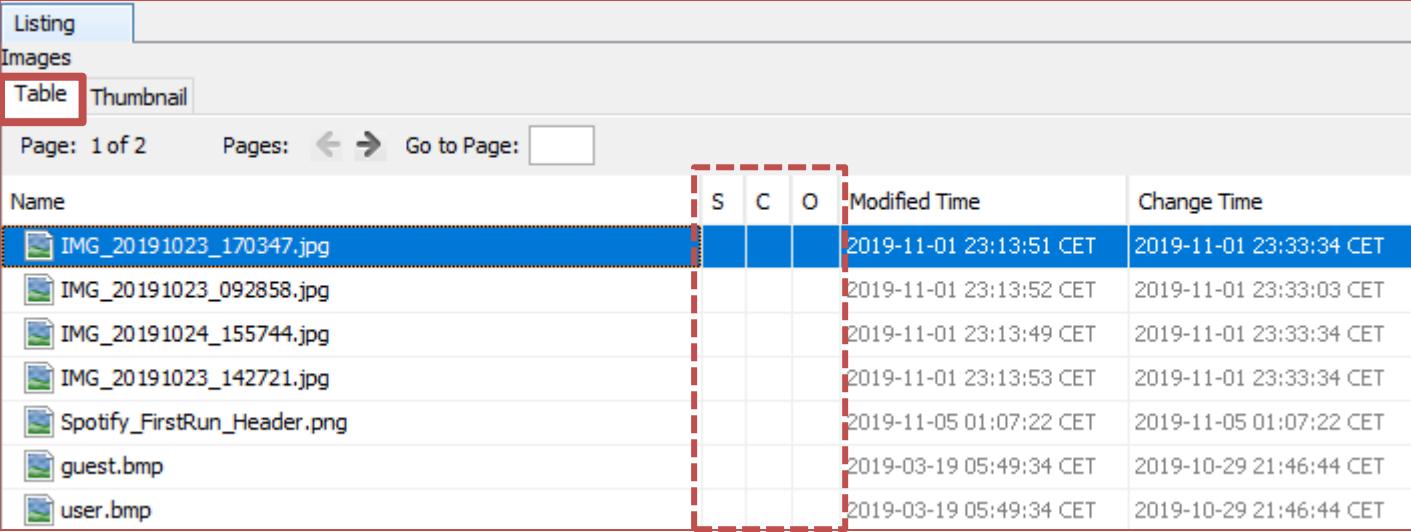


# Autopsy GUI



# Autopsy

## GUI



The screenshot shows the Autopsy GUI interface. At the top, there are tabs: Listing, Images, Table (which is selected and highlighted in red), and Thumbnail. Below the tabs, there are buttons for Page navigation (Page: 1 of 2, Pages: < >, Go to Page: [ ]). The main area displays a table of files:

Name	S	C	O	Modified Time	Change Time
IMG_20191023_170347.jpg				2019-11-01 23:13:51 CET	2019-11-01 23:33:34 CET
IMG_20191023_092858.jpg				2019-11-01 23:13:52 CET	2019-11-01 23:33:03 CET
IMG_20191024_155744.jpg				2019-11-01 23:13:49 CET	2019-11-01 23:33:34 CET
IMG_20191023_142721.jpg				2019-11-01 23:13:53 CET	2019-11-01 23:33:34 CET
Spotify_FirstRun_Header.png				2019-11-05 01:07:22 CET	2019-11-05 01:07:22 CET
guest.bmp				2019-03-19 05:49:34 CET	2019-10-29 21:46:44 CET
user.bmp				2019-03-19 05:49:34 CET	2019-10-29 21:46:44 CET

- ▶ **S (score):** indica se l'elemento è notevolmente importante  (*notable file*) oppure se è interessante. 
- ▶ **C (comments):** indica se l'elemento è stato commentato, anche in un precedente caso. 
- ▶ **O (occurrences):** indica quante volte l'elemento è stato già rinvenuto in altri reperti

# Autopsy

## GUI

Listing  
Images  
Table **Thumbnail**

Page: 1 of 50 Pages: [◀](#) [▶](#) Go to Page:  Images: 1-200 Medium Thumbnails ▾ Sort Sorted by: 1. Size ▾

Background_Safe...	Pattern_Doodles...	Background_Room...	LockScreen___10...	Background_Forw...	Background_Room...
Background_Room...	Background_Forw...	SaturationGradi...	Background_Room...	Background_Room...	Background_Room...
MotionControlle...	11042019Note.jpg	Pattern_Adventu...	hero-still-imag...	bg7.jpg	NoSearchResult.png

# Autopsy

## GUI



- Pictures
- Video
- SQLite
- HTML
- Registry
- Binary PList

Hex	Text	Application	Message	File Metadata	Context	Results	Annotations	Other Occurrences	Video Triage
				<p>Name /img_device1_laptop.e01/vol_vo1/ProgramData/Microsoft/Windows NT/MSScan/WelcomeScan.jpg</p> <p>Type File System</p> <p>MIME Type image/jpeg</p> <p>Size 516424</p> <p>File Name Allocation Allocated</p> <p>Metadata Allocation Allocated</p> <p>Modified 2019-03-19 05:46:56 CET</p> <p>Accessed 2019-03-19 05:46:56 CET</p> <p>Created 2019-03-19 05:46:56 CET</p> <p>Changed 2019-10-29 21:46:44 CET</p>					

# Autopsy

## GUI

The screenshot shows the Autopsy Forensic Browser interface. The top navigation bar includes tabs for Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, and Video Triage. The 'Hex' tab is currently selected.

The main pane displays a hex dump of a file. The left column shows memory addresses (e.g., 0x00000000, 0x00000010, etc.) and the right column shows the corresponding ASCII characters and byte values. Some strings are partially visible, such as 'JFIF.....', 'kDucky...', and 'Natphotos/Digital Vision/Getty Images'.

A second window or pane is overlaid at the bottom right, also titled 'Text'. This pane shows the decoded text from the hex dump. It includes the same strings: 'JFIF', 'kDucky', '(c) Natphotos/Digital Vision/Getty Images', 'XICC\_PROFILE', 'HLino', 'mntrRGB XYZ', 'acspMSFT', 'IEC sRGB', and several other short entries like '-HP', 'cppt', '3desc', 'lwptt', 'bkpt', 'rXYZ', 'gXYZ', 'bXYZ', 'dmnd', 'pdmdd', 'vued', and 'view'.

# Autopsy

» Moduli di elaborazione



# Autopsy

## *Ingest Modules*

- ▶ Plug-in responsabili di analizzare i dati presenti all'interno del file immagine:
  - Hashing
  - Identificazione del File Type:
    - Bad extension
  - User Activity:
    - Analisi dei registri
    - Web activity
  - Indexing
  - File Carving
  - etc...

# Autopsy

## *Ingest Modules*

- ▶ Ingest Manager esegue i processi di analisi in background:
  - File vengono processati in base alla seguente priorità:
    - Cartelle utenti
    - Program Files e altre cartelle nella root
    - Cartella di Windows
    - Spazio non allocato
  - Esecuzione parallela di più file immagine.
- ▶ I risultati sono visualizzabili nella sezione «result»

# Autopsy Ingest Modules

The image shows the Autopsy 4.14.0 interface with a red arrow pointing from the 'Run Ingest Modules' option in the context menu of a selected file type ('Recent Activity') to the 'Configure Ingest Modules' dialog.

**Autopsy 4.14.0 Interface:**

- Case01 - Autopsy 4.14.0
- Case View Tools Window Help
- Add Data Source Images/Videos Communications Timeline
- Data Sources: device1\_laptop.e01
- Views: device1\_laptop.e01
- File Types:
  - By Extension
    - Images (11)
    - Videos (34)
    - Audio (114)
    - Archives (2)
    - Databases
    - Documents
      - HTML (10)
      - Office (7)
- Properties
- Extract Unallocated Space to Single Files
- Open File Search by Attributes
- View Summary Information
- Run Ingest Modules** (highlighted with a blue box)
- View in New Window
- Remove Data Source
- Collapse All

**Configure Ingest Modules Dialog:**

- Run ingest modules on: All Files, Directories, and Unallocated Space
- Selected module: Recent Activity
- Module details:
  - Extracts recent user activity, such as Web browsing, recently used ...
  - Global Settings
- Available modules (list):
  - Recent Activity (selected)
  - Hash Lookup
  - File Type Identification
  - Extension Mismatch Detector
  - Embedded File Extractor
  - Exif Parser
  - Keyword Search
  - Email Parser
  - Encryption Detection
  - Interesting Files Identifier
  - Correlation Engine
  - PhotoRec Carver
  - Virtual Machine Extractor
  - Data Source Integrity
  - Plaso
  - Android Analyzer
- Buttons: Select All, Deselect All, History, Back, Next, Finish (highlighted with a blue box), Cancel, Help

# Autopsy

## *Ingest Modules: Hash Lookup*

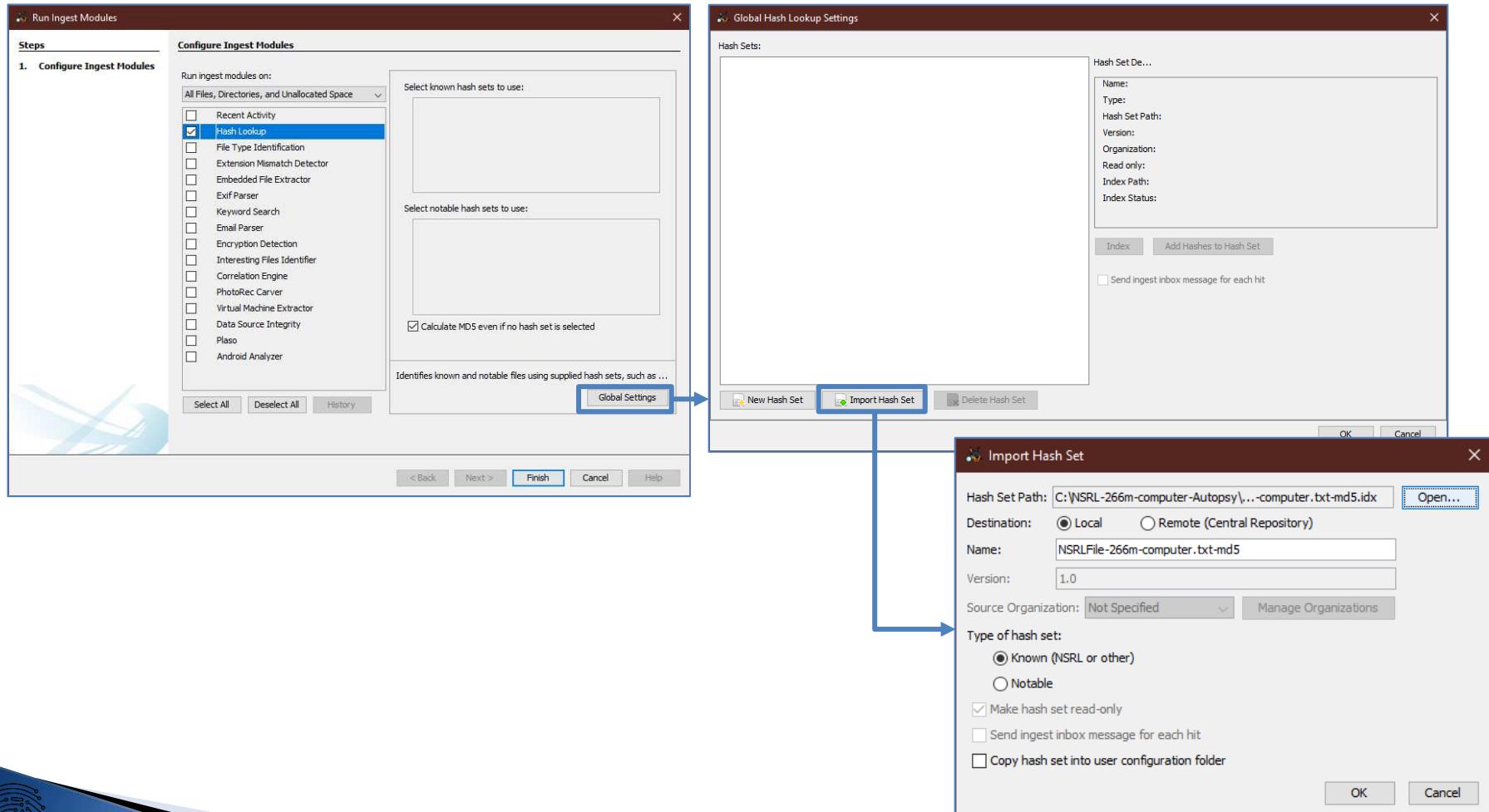
- 1) Calcola l'hash MD5 per ogni file
- 2) Memorizza gli Hash nel Case DB
- 3) Ricerca gli hash calcolati all'interno di una lista di «Known Hash»:
  - Known as Ignorable File (NSLR)
  - Known as Notable File

Ogni file nel caso ha tre valori di «Known Status»:

- **Unknown** (*default*)
- **Known** (*ignorable*)
- **Notable** (*Known bad*)

# Autopsy

## Ingest Modules: Hash Lookup



# Autopsy

## *Ingest Modules: Hash Lookup*

### Known (Ignorable File)

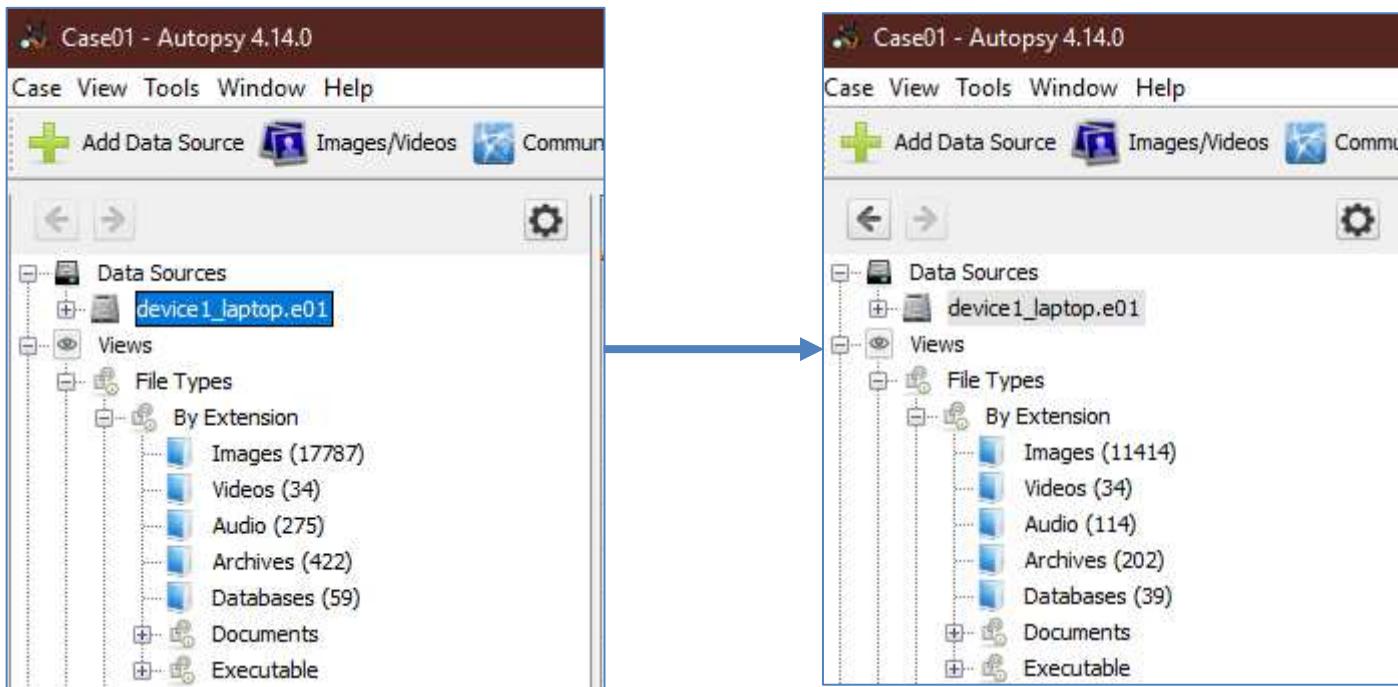
- ▶ Possono essere ignorati anche dagli altri moduli
- ▶ Possono essere nascosti dalla «views» area (*default*)
- ▶ Possono essere nascosti dalla vista ad albero (*not default*)

Velocizza notevolmente l'analisi

# Autopsy

## *Ingest Modules: Hash Lookup*

### Known (*Ignorable File*)



# Autopsy

## Ingest Modules: Hash Lookup

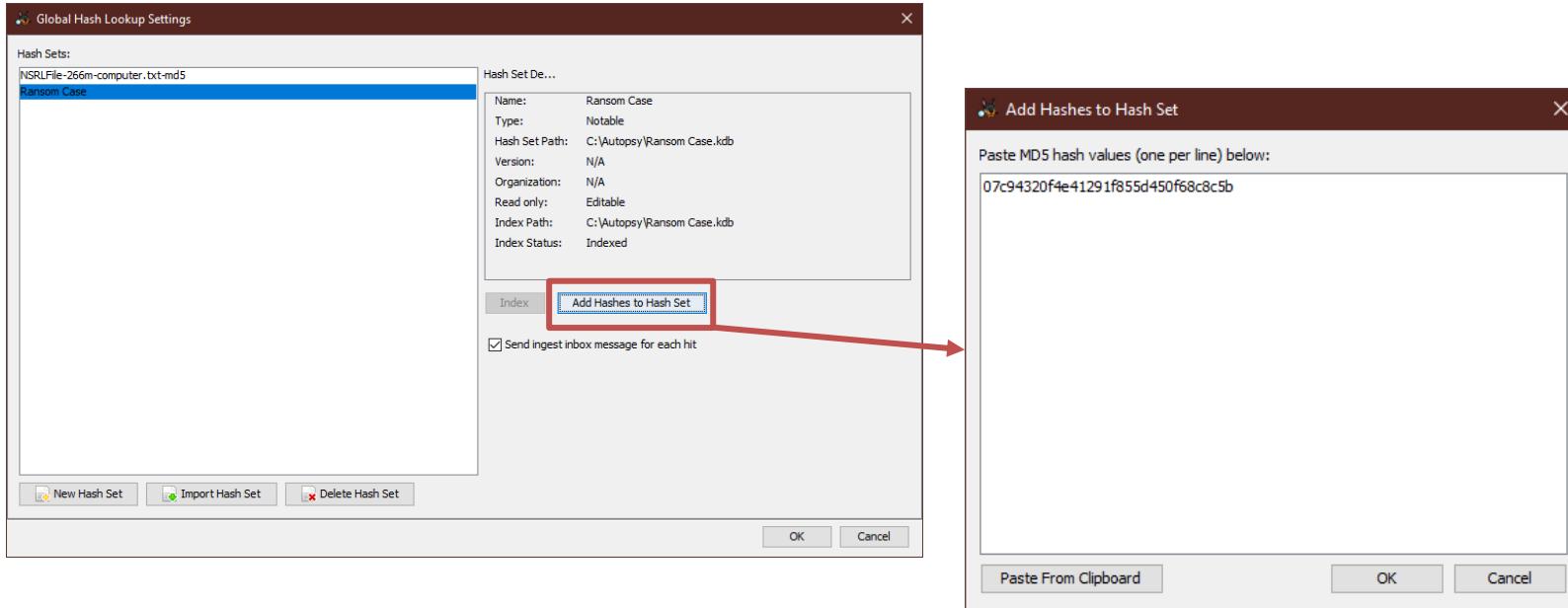
The image shows three windows from the Autopsy software:

- Configure Ingest Modules**: A dialog where "Hash Lookup" is selected under "Run ingest modules on: All Files, Directories, and Unallocated Space".
  - Select known hash sets to use:** An empty list.
  - Select notable hash sets to use:** An empty list.
  - Calculate MD5 even if no hash set is selected**: A checked checkbox.
  - Identifies known and notable files using supplied hash sets, such as ...**: A note.
  - Global Settings**: A button.
- Global Hash Lookup Settings**: A dialog showing a "Hash Sets:" list which is currently empty.
  - Hash Set De...**: A panel with fields for Name, Type, Hash Set Path, Version, Organization, Read only, Index Path, and Index Status.
  - Index** and **Add Hashes to Hash Set** buttons.
  - Send ingest inbox message for each hit**: A checked checkbox.
  - OK** and **Cancel** buttons.
- Create Hash Set**: A dialog for creating a new hash set.
  - Destination:**  Local,  Remote (Central Repository).
  - Name:** Ransom Case.
  - Hash Set Path:** C:\Autopsy\Ransom Case.kdb, with a **Save As...** button.
  - Source Organization:** Not Specified, with a Manage Organizations button.
  - Type:**  Known,  Notable.
  - Send ingest inbox messages for each hit**: A checked checkbox.
  - OK** and **Cancel** buttons.

A red arrow points from the "New Hash Set" button in the Global Hash Lookup Settings dialog to the "Create Hash Set" dialog.

# Autopsy

## Ingest Modules: Hash Lookup



HASH: 07c94320f4e41291f855d450f68c8c5b

# Autopsy

## Ingest Modules: Hash Lookup

### Notable File (Bad File)

The screenshot shows the Autopsy interface. On the left, a table lists two files: 'RN.jpg' and 'f\_000239'. Both files have an MD5 hash of '07c94320f4e41291f855d450f68c8c5b'. A red arrow points from the 'Results' tab in the top navigation bar of the main pane to the right-hand details panel.

**Main Pane (Left):**

Source File	S	C	O	MD5 Hash	Comment	File Path
RN.jpg	!	0		07c94320f4e41291f855d450f68c8c5b		/img_device1_laptop.e01/vol_vo17/Users/AntiRenzik/Desktop/Pictures/RN.jpg
f_000239	!	0		07c94320f4e41291f855d450f68c8c5b		/img_device1_laptop.e01/vol_vo17/Users/AntiRenzik/AppData/Local/Google/Chro...

**Details Panel (Right):**

Type	Value	Source(s)
Set Name	Ransom Case	Hash Lookup
MD5 Hash	07c94320f4e41291f855d450f68c8c5b	Hash Lookup
Comment		Hash Lookup
Source File Path	/img_device1_laptop.e01/vol_vo17/Users/AntiRenzik/Desktop/Pictures/RN.jpg	
Artifact ID	-9223372036854775807	

# Autopsy

## *Ingest Modules: Hash Lookup*

### Notable File (*Bad File*)

Name	S	C	O	Modified Time	Change Time	Access Time
In order to ensure that Renzik is treated properly (1).docx	0	2019-11-05 01:23:09 CET	2019-11-05 01:23:32 CET	2019-11-05		
In order to ensure that Renzik is treated properly (1).docx:Zone.Ident				Properties	01:23:32 CET	2019-11-05
In order to ensure that Renzik is treated properly.docx				View File in Directory	01:23:02 CET	2019-11-05
In order to ensure that Renzik is treated properly.docx:Zone.Iden				View in New Window	01:23:02 CET	2019-11-05
WDAGPlaceholder.docx				Open in External Viewer Ctrl+E	21:48:56 CET	2019-03-19
WDAGPlaceholder.pptx				View File in Timeline...	21:48:56 CET	2019-03-19
WDAGPlaceholder.xlsx				Extract File(s)	21:48:56 CET	2019-03-19
				Export selected rows to CSV		
				Add File Tag >		
				Remove File Tag >		
				Add/Edit Central Repository Comment		
				Add File to Hash Set >		
				Show only rows where >		

# Autopsy

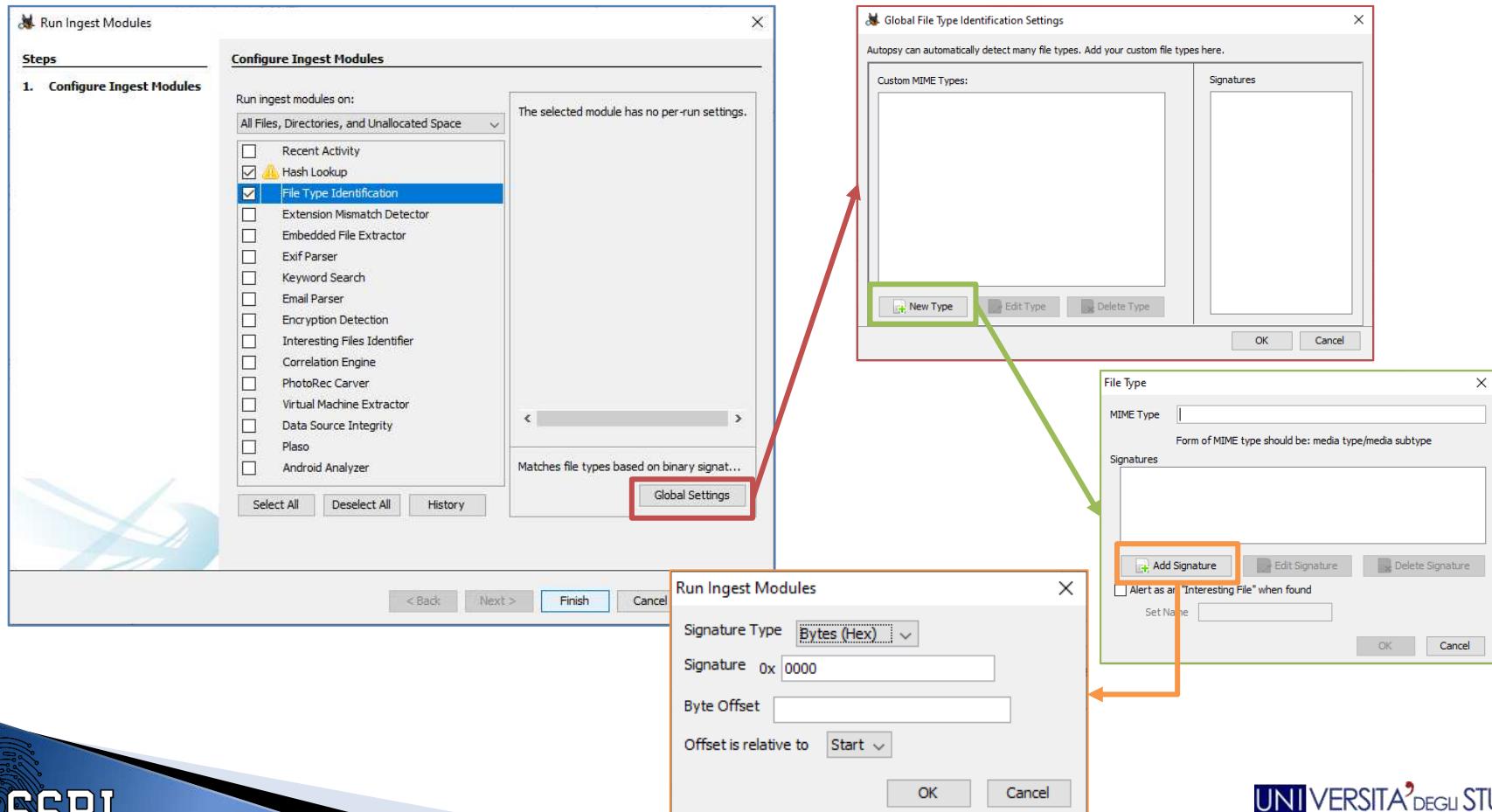
## *Ingest Modules: File Type*

- ▶ Determina la tipologia del file analizzando la signature:
  - Es: 0xffd8 => JPEG File
  - Modo più accurato per definire il tipo di file
- ▶ Il file type viene conservato nel Case DB
  - Molti moduli dipendono da queste informazioni
- ▶ Basato sulla libreria Tika (*open source*) :
  - Viene impiegato la catalogazione MIME type:
    - application/zip
    - audio/mpeg
    - Image/jpeg
    - ...
    - application/octet-stream (*unknown type*)

# Autopsy

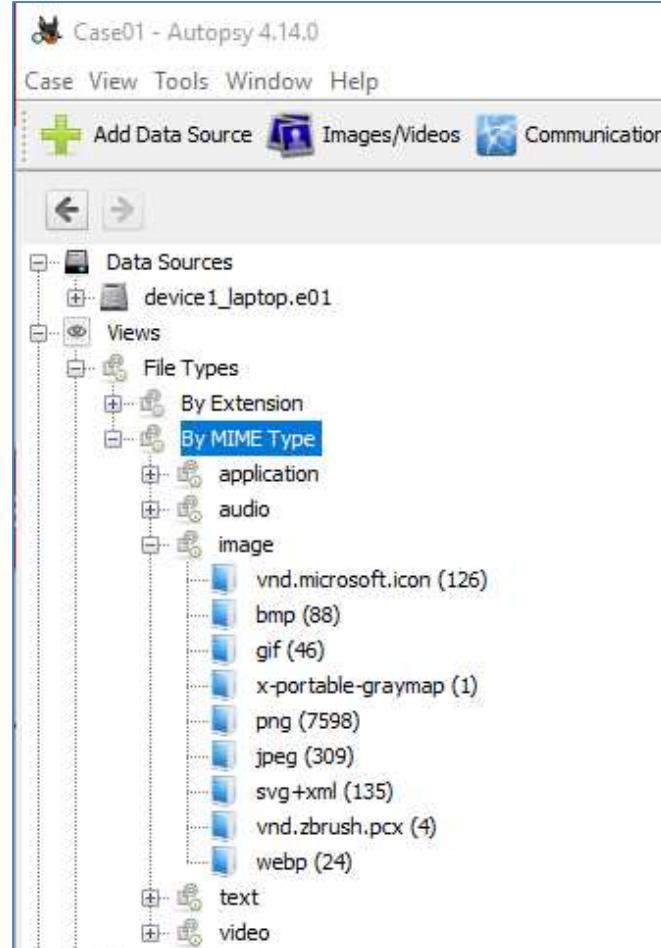
## Ingest Modules: File Type

- ▶ Può essere ampliato aggiungendo ulteriori tipi:



# Autopsy

## *Ingest Modules: File Type*



# Autopsy

## *Ingest Modules: File Extension Mismatch*

- ▶ Per ciascun file confronta l'estensione (.doc, .jpeg, etc.) con la propria categoria:
  - Se le informazioni non sono coerenti viene etichettato
- ▶ Dipende dal modulo «File Type»

**Obiettivo:** trovare i file che l'utente ha provato a nascondere

# Autopsy

## Ingest Modules: File Extension Mismatch

The image shows the Autopsy software interface. On the left, a sidebar titled "Run Ingest Modules" lists "Steps" and "1. Configure Ingest Modules". The main window displays the "Configure Ingest Modules" dialog. Under "Run ingest modules on:", "All Files, Directories, and Unallocated Space" is selected. A list of modules is shown, with "Extension Mismatch Detector" highlighted and checked. To the right, configuration options include radio buttons for "Check all file types", "Check all file types except text files", and "Check only multimedia and executable files" (which is selected). There are also checkboxes for "Skip files without extensions" and "Skip known files". A note at the bottom states "Flags files that have a non-standard extension...". A red box highlights the "Global Settings" button, which has a red arrow pointing to the "Global File Extension Mismatch Identification Settings" dialog on the right. This dialog lists "File Types:" (including ".") and "Allowed Extensions for image/jpeg:" (listing gif, jfi, jif, jpe, jpeg, jpg, jpg:ms-thumbnail, png, tif). Buttons for "New Type" and "Delete Type" are at the bottom. Another red arrow points from the "Global Settings" button in the main dialog to the "New Type" button in the settings dialog.

# Autopsy

## Ingest Modules: File Extension Mismatch

The screenshot shows the Autopsy 4.14.0 interface. The left sidebar displays a tree view of data sources, views, file types (including image, audio, and video), deleted files, MB file size, and results (extracted content, keyword hits, search results, and hashset hits). A message in the results section indicates "Extension Mismatch Detected (113)". The main pane is titled "Listing" and "Extension Mismatch Detected". It contains two tabs: "Table" (selected) and "Thumbnail". The "Table" tab displays a table with columns: Source File, S, C, O, Extension, MIME Type, and Data Source. The data shows numerous entries for files like ".rsrc", "00000\_impact\_metal\_icon.bytes", and various ".icon.bytes" files, all categorized under "image" type and "bytes" extension, with "image/png" as the MIME type and "device1\_laptop.e01" as the data source.

Source File	S	C	O	Extension	MIME Type	Data Source
8.rsrc	0			rsrc	image/png	device1_laptop.e01
9.rsrc	0			rsrc	image/png	device1_laptop.e01
00000_impact_metal_icon.bytes	0			bytes	image/png	device1_laptop.e01
00000_impact_sand_icon.bytes	0			bytes	image/png	device1_laptop.e01
00000_impact_stone_icon.bytes	0			bytes	image/png	device1_laptop.e01
10162_scifi_portal_icon.bytes	0			bytes	image/png	device1_laptop.e01
10164_explosion_icon.bytes	0			bytes	image/png	device1_laptop.e01
10165_powerup_wall_icon.bytes	0			bytes	image/png	device1_laptop.e01
10169_muzzleflash_icon.bytes	0			bytes	image/png	device1_laptop.e01
10170_neonsphere_icon.bytes	0			bytes	image/png	device1_laptop.e01
10171_rain_icon.bytes	0			bytes	image/png	device1_laptop.e01
10172_smoke_icon.bytes	0			bytes	image/png	device1_laptop.e01
10173_sparking_electricity_icon.bytes	0			bytes	image/png	device1_laptop.e01
10174_underwater_icon.bytes	0			bytes	image/png	device1_laptop.e01
10175_upward_dust_explosion_icon.bytes	0			bytes	image/png	device1_laptop.e01
10234_laserbeam_icon.bytes	0			bytes	image/png	device1_laptop.e01
10247_ray_of_light_icon.bytes	0			bytes	image/png	device1_laptop.e01
10249_glow_icon.bytes	0			bytes	image/png	device1_laptop.e01
10250_sparkle_glitter_icon.bytes	0			bytes	image/png	device1_laptop.e01
10251_files_icon.bytes	0			bytes	image/png	device1_laptop.e01

*Molti falsi positivi*

# Autopsy

## *Ingest Modules: Exif parser*

- ▶ Estraie i **metadati Exif** dai file JPEG memorizzandoli nella sezione «Result»:
  - Identificazione della fotocamera;
  - Identificazione del *timestamp* dello scatto;
  - Geolocalizzazione del luogo dello scatto;

# Autopsy

## Ingest Modules: Exif parser

The screenshot shows the Autopsy digital forensics tool. On the left, a sidebar titled 'Run Ingest Modules' contains a 'Steps' section and a 'Configure Ingest Modules' section. Under 'Configure Ingest Modules', a list of modules is shown with checkboxes. Several modules are checked, including Hash Lookup, File Type Identification, Extension Mismatch Detector, and Exif Parser. A red arrow points from the 'Exif Parser' checkbox in the configuration dialog down to the 'EXIF Metadata' table in the main case view window.

**Configure Ingest Modules**

Run ingest modules on:

- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Correlation Engine
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- Plaso
- Android Analyzer

Select All   Deselect All   History

**Case01 - Autopsy 4.14.0**

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline File Discovery Close Case Generate Report

**Listing**

EXIF Metadata

Source File	S	C	O	Date Created	Device Model	Device Make	Latitude	Longitude
IMG_20191023_142721.jpg	0	2019-10-23 14:27:21 CEST	BLU R1 HD	BLU				
IMG_20191023_092858.jpg	0	2019-10-23 09:28:58 CEST	BLU R1 HD	BLU	39.17767333333333	-76.66690825		
IMG_20191023_170347.jpg	0	2019-10-23 17:03:47 CEST	BLU R1 HD	BLU	29.950344083333334	-90.06626891666666		
IMG_20191024_155744.jpg	0	2019-10-24 15:57:45 CEST	BLU R1 HD	BLU	29.946456888888889	-90.06748961111111		
f_0000c1	0	2019-03-13 12:26:26 CET	Canon EOS-1D X	Canon				
f_000198	0	2018-04-09 21:08:12 CEST	ILCE-7M3	SONY				
f_0001a4	0	2014-12-09 08:53:56 CET	Canon EOS-1D X	Canon				
f_0001c9	0	2017-09-17 16:28:25 CEST	iPhone 7 Plus	Apple				
f_0001d9	0	2019-03-13 09:30:38 CET	Canon EOS-1D X Mark II	Canon				
f_00022e	0	2019-10-24 15:57:45 CEST	BLU R1 HD	BLU	29.946456888888889	-90.06748961111111		
f_00022f	0	2019-10-23 17:03:47 CEST	BLU R1 HD	BLU	29.950344083333334	-90.06626891666666		
f_000230	0	2019-10-23 09:28:58 CEST	BLU R1 HD	BLU	39.17767333333333	-76.66690825		
f_000233	0	2019-10-23 14:27:21 CEST	BLU R1 HD	BLU				
f_000350	0	2017-10-14 11:30:33 CEST	Nikon D750	Nikon Corporation				
f_000403	0	2019-10-17 09:05:44 CEST	Nikon D5	Nikon Corporation				
bg1a_thumb.png	0	2017-09-27 16:05:12 CEST						

# Autopsy

## *Ingest Modules: Embedded File Extractor*

- ▶ Estrae i file incapsulati in altri file:
  - Archive File: Zip, Rar, etc.
  - File grafici da Documenti Office/PDF
- ▶ I File estratti vengono salvati nel Case Folder:
  - risultati sono visionabili nella «tree view»
- ▶ Vengono etichettati se protetti da password

# Autopsy

## Ingest Modules: Embedded File Extractor

The screenshot shows the Autopsy digital forensics tool. On the left, a modal window titled "Configure Ingest Modules" is open, listing various modules. The "Embedded File Extractor" module is selected and highlighted with a blue arrow pointing from the list to its description area. The main window shows a file tree for a case named "Case01 - Autopsy 4.14.0". A file named "S1L1DWH.zip" is selected in the tree, and its contents are listed in a table below, showing a single entry for "Takeout".

Run Ingest Modules

**Steps**

1. Configure Ingest Modules

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

The selected module has no per-run settings.

Recent Activity

Hash Lookup

File Type Identification

Extension Mismatch Detector

**Embedded File Extractor**

Exif Parser

Keyword Search

Email Parser

Encryption Detection

Interesting Files Identifier

Correlation Engine

PhotoRec Carver

Virtual Machine Extractor

Data Source Integrity

Plaso

Android Analyzer

Select All Deselect All History

Extracts embed

< Back Next >

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline File Discovery Close Case Generate Report

Case01 - Autopsy 4.14.0

Data Sources

- device1\_laptop.e01
  - vol1 (Unallocated: 0-2047)
  - vol4 (Basic data partition: 2048-1085439)
  - vol5 (EFI system partition: 1085540-1288191)
  - vol6 (Microsoft reserved partition: 1288192-1320959)
  - vol7 (Basic data partition: 1320960-83884031)
    - \$OrphanFiles (0)
    - \$Extend (9)
    - \$Recycle.Bin (5)
      - S-1-5-18 (3)
      - S-1-5-21-2274644105-2924306947-3431561117-1000 (3)
      - S-1-5-21-2274644105-2924306947-3431561117-1001 (13)
        - S1L1DWH.zip (1)
          - Takeout (2)
      - \$Unalloc (29)
      - Documents and Settings (2)
      - PerfLogs (2)
    - Program Files (20)
      - Program Files (x86) (17)
      - ProgramData (15)
    - Recovery (2)
    - System Volume Information (5)
    - Users (8)
    - Windows (105)
  - vol8 (Unallocated: 83884032-83886079)

Listing /img\_device1\_laptop.e01/vol7/\$Recycle.Bin/S-1-5-21-2274644105-2924306947-3431561117-1001

Name S C O Modified Time Change Time

Takeout 0000-00-00 00:00:00 0000-00-00 00:00:00

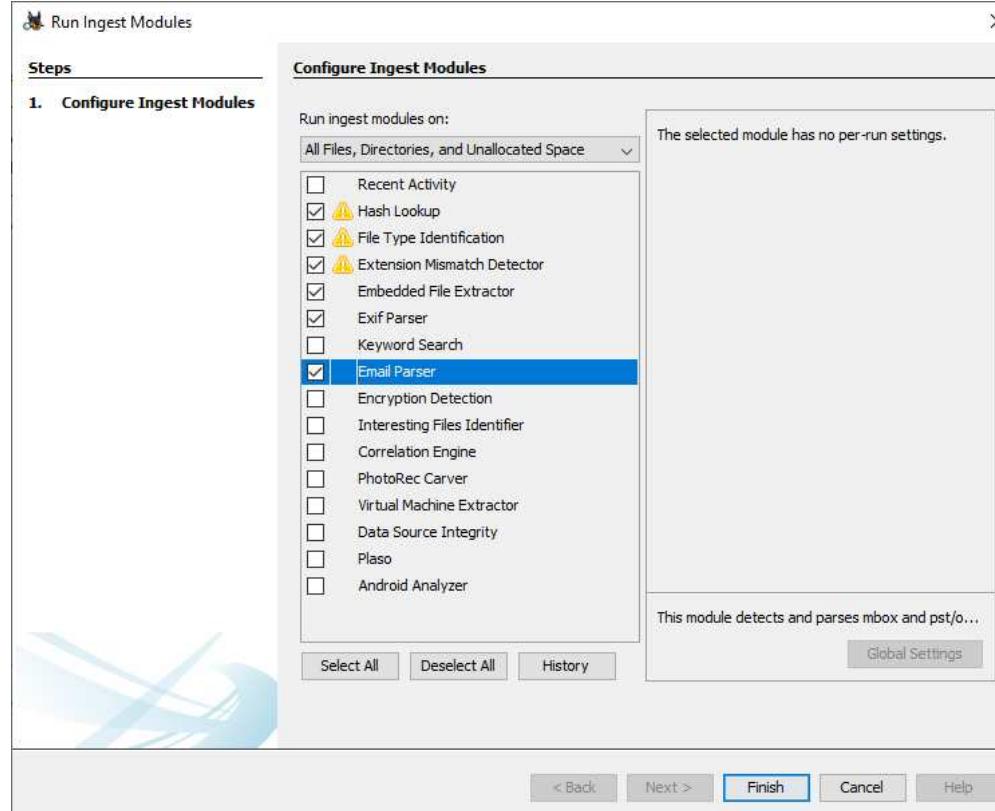
# Autopsy

## *Ingest Modules: Email parser*

- ▶ Ricerca ed analizza archivi di posta:
  - Mbox, PST e EML File
- ▶ I risultati sono visualizzabili nella sezione «result» nella categoria «E-Mail Messages»:
  - Gli allegati sono trattati come figli del messaggio
  - Sono raggruppati in *threads*
- ▶ E' possibile analizzarli dettagliatamente attraverso la vista «Communications»

# Autopsy

## *Ingest Modules: Email parser*



# Autopsy

## Ingest Modules: Email parser

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help, and several icons for adding data sources, generating reports, and closing cases.

The left sidebar displays a tree view of the case structure:

- Data Sources: device1\_laptop.e01
- Views:
  - File Types: By Extension, By MIME Type, Deleted Files, MB File Size
  - Results:
    - Extracted Content: EXIF Metadata (23), Extension Mismatch Detected (339), User Content Suspected (23)
    - Keyword Hits: Single Literal Keyword Search (0), Single Regular Expression Search (0)
    - Hashset Hits: Ransom Case (6), E-Mail Messages, Default ((Default)), Default (138)
    - Interesting Items: Accounts, Email
    - Tags
    - Reports

The main pane shows a table titled "Listing" with 138 results. The columns are Source File, S, C, O, E-Mail From, E-Mail To, and Subject. The table lists various email messages from addresses like 5things@cnn.com, bean@bitcoin.com, team@bitcoin.com, messages-noreply@linkedin.com, briant.stelter@turner.com, 15t4eu+45c1yem5fewrlj8d2o@guerrillamail.com, antirenzik@gmail.com, and peacockleprechaun@gmail.com. The subjects include "Chicago is breathing a sigh of relief today", "Bitcoin halving: to panic, or not to panic?", "Welcome to Bitcoin.com!", "Goose, be recognizable on LinkedIn", "Day 4 - What Is A Bitcoin Wallet?", "Welcome to CNN's Reliable Sources Newsletter", "Reminder", and "Re: Meetup?".

Below the table, a preview pane shows the content of an email message:

From: peacockleprechaun@gmail.com;  
To: antirenzik@gmail.com;  
CC:  
Subject: Re: Meetup?

Headers: Text, HTML, RTF, Attachments (0)  
Download Images

The message body contains:

That works for me. Although I have some news, this morning after giving him food, Renzik bit me. The bleeding has mostly stopped. Do you know what kind of d

On Tue, Nov 12, 2019, 12:03 PM Goose Honkerson <antirenzik@gmail.com> wrote:  
Yes, I arrived, although a few days later than I had initially planned. I assume that everything is going well with Renzik still. Haven't seen anything from Basis, in inbox.

Lets plan on meeting up later today, how about Jackson Park at about 4? Then I can take Renzik and hold onto him until Basis responds to us

Jackson Square, 701 Decatur St, New Orleans, LA 70116

On Tue, Nov 12, 2019 at 4:41 AM Peacock Leprechaun <peacockleprechaun@gmail.com> wrote:  
It's been a few days since you said you were going to be down here, but I've not heard anything. Did you make it down yet? If so, what's the plan boss?

# Autopsy

## *Ingest Modules: Interesting Files*

- ▶ Etichetta file e cartelle che si pensa essere «interessanti» (*interesting items*)
  - Viene notificato il rinvenimento di tali oggetti.
  - Es.:
    - iPhone Backup
    - VMware image
    - BitCoin wallets
    - Cloude storage client
    - etc.

# Autopsy

## Ingest Modules: Interesting Files

The screenshot illustrates the configuration of Autopsy's ingest modules, specifically focusing on the "Interesting Files Identifier".

**Main Interface (Configure Ingest Modules):**

- Run Ingest Modules:** A button to start the analysis.
- Steps:** A navigation bar with the current step being "Configure Ingest Modules".
- 1. Configure Ingest Modules:** A sub-step for selecting modules.
- Run ingest modules on:** Set to "All Files, Directories, and Unallocated Space".
- Select interesting files sets to:** A dropdown menu.
- Module List:** A list of available modules with checkboxes:
  - Recent Activity
  - Hash Lookup (checked)
  - File Type Identification (checked)
  - Extension Mismatch Detector (checked)
  - Embedded File Extractor (checked)
  - Exif Parser (checked)
  - Keyword Search
  - Email Parser (checked)
  - Encryption Detection
  - Interesting Files Identifier (checked)** (highlighted in blue)
  - Correlation Engine
  - PhotoRec Carver
  - Virtual Machine Extractor
  - Data Source Integrity
  - Plaso
  - Android Analyzer
- Buttons:** Select All, Deselect All, History, < Back, Next >, Finish, Cancel, Help.

**Global Interesting Items Settings (Top Right):**

- Set Details:** Description: [empty]
- Rule Sets:** A list of sets with buttons: New Set (highlighted with a green box), Edit Set, Delete Set, Copy Set, Import Set, Export Set.
- Rules:** Buttons: New Rule, Edit Rule, Delete Rule.
- Rule Details:** File Type: Radio buttons for Files (selected), Directories, All. Name: [empty]. Path Substring: [empty] (with Regex checkbox). MIME Type: [empty]. File Size: [empty] (with Kilobytes dropdown).

**Interesting Files Set Rule (Bottom Right):**

- Set Name:** Encryption (highlighted with a green box).
- Description:** [empty]
- Ignore Known Files:** Checkbox (unchecked).
- Buttons:** OK (highlighted with a green box), Annulla.

A red arrow points from the "Global Settings" button in the main interface to the "New Set" button in the Global Interesting Items Settings dialog. A green box highlights the "New Set" button in both dialogs.

# Autopsy

## Ingest Modules: Interesting Files

The screenshot shows the Autopsy Global Interesting Items Settings interface. On the left, under 'Rule Sets', 'Encryption' is selected. A red box highlights the 'New Set' button. In the center, a 'Set Details' dialog is open, also with a red box around the 'New Rule' button. An orange arrow points from the 'New Rule' button in the main interface to the 'New Rule' button in the dialog. The dialog has a title 'Set Details' and a 'Description:' text area. Below it is a 'Rules:' section containing a 'New Rule' button, which is also highlighted with a red box. At the bottom are 'OK' and 'Cancel' buttons.

**Global Interesting Items Settings**

This module allows you to find files that match specified criteria. Each set has a list of rules, which will match on their chosen file characteristics. A file need only match one rule to be found.

Rule Sets:

- Encryption

New Set Edit Set Delete Set

Copy Set Import Set Export Set

**Set Details**

Description:

Ignore Known Files

**Rules:**

**New Rule** Edit Rule Delete Rule

**Rule Details**

File Type:  Files  Directories  All

Name:

Full Name  Extension Only  Substring / Regex

Path Substring:   
 Regex

MIME Type:

File Size:   Kilobytes

Modified Within:  day(s)

OK Cancel

**Interesting Files Set Rule**

Enter information about files that you want to find.

Type:  Files  Directories  All

Name:  truecrypt.exe  
 Full Name  Extension Only  Substring / Regex

Folder Name:   
 Regex  Folder must be in parent path. Use '/' to give consecutive names

MIME Type:

File Size:   Kilobytes

Modified Within:  day(s)

Rule Name (Optional):

OK Cancel

**Interesting Files Set Rule**

Enter information about files that you want to find.

Type:  Files  Directories  All

Name:  veracrypt.exe  
 Full Name  Extension Only  Substring / Regex

Folder Name:   
 Regex  Folder must be in parent path. Use '/' to give consecutive names

MIME Type:

File Size:   Kilobytes

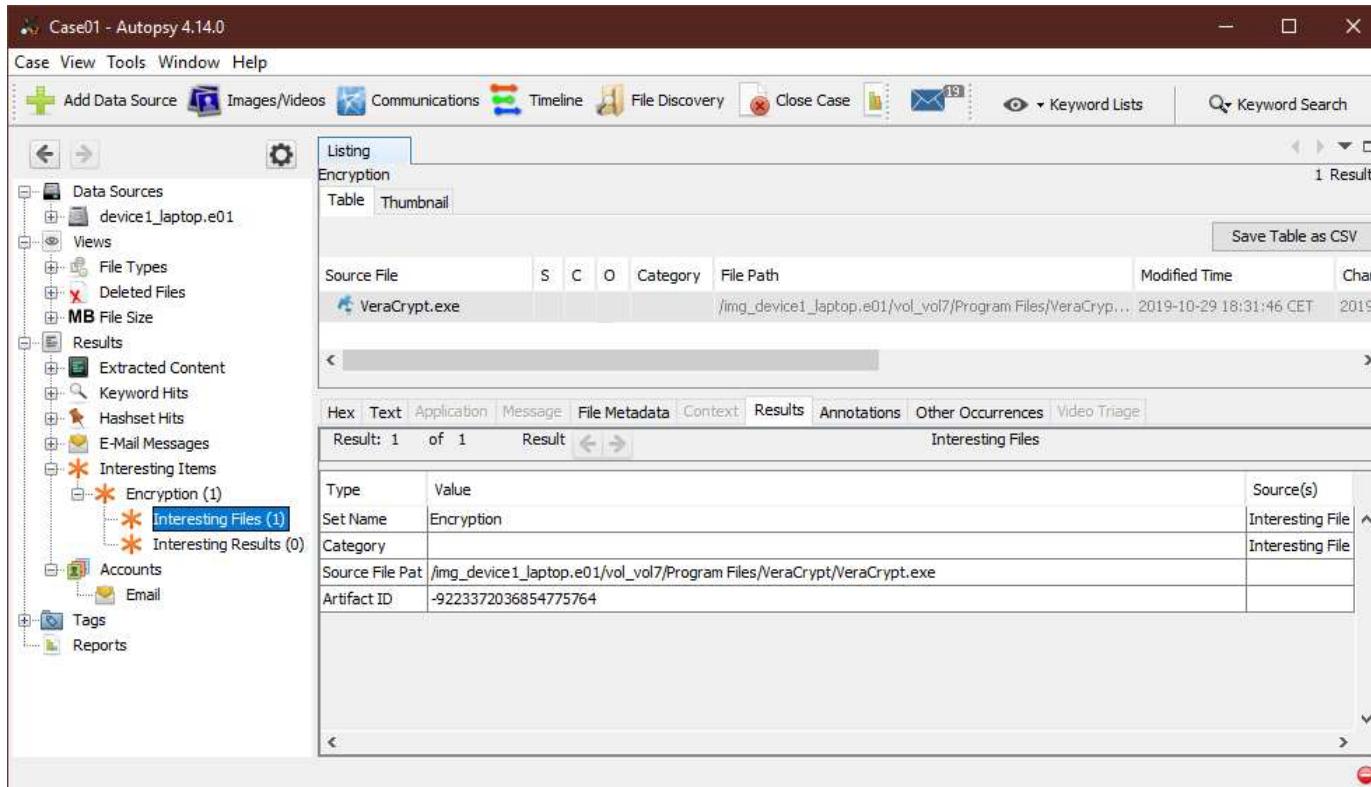
Modified Within:  day(s)

Rule Name (Optional):

OK Cancel

# Autopsy

## Ingest Modules: Interesting Files



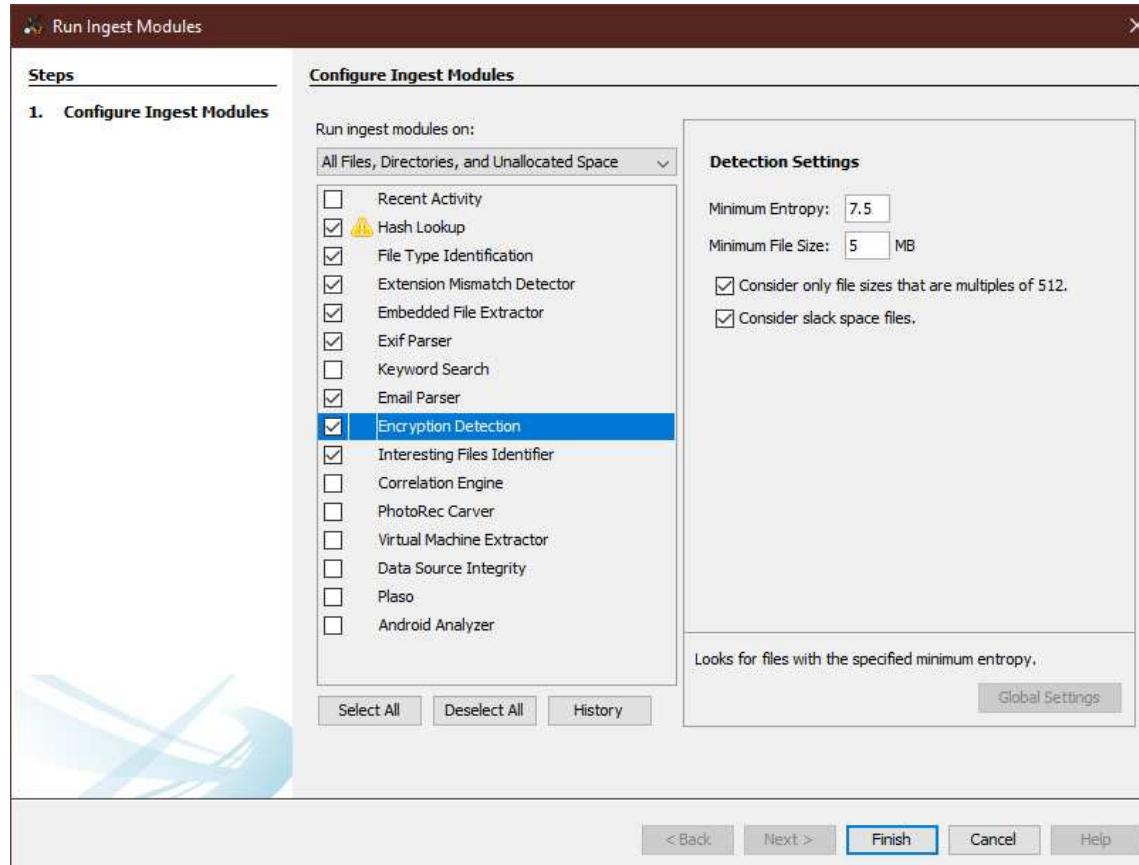
# Autopsy

## *Ingest Modules: Encryption Detection*

- ▶ Etichetta file e volumi che sono\potrebbero essere cifrati:
  - Documenti Office/PDF e Access DB protetti da password
  - Possibili file o volumi con cifratura basato su:
    - High Entropy
    - Dimensione: multiplo di 512byte
    - Tipo di file: sconosciuto

# Autopsy

## *Ingest Modules: Encryption Detection*



# Autopsy

## Ingest Modules: Encryption Detection

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help, and several icons for adding data sources, generating reports, and keyword searching. The left sidebar contains a tree view of data sources, views, results (including extracted content like EXIF metadata, encryption detection, and extension mismatch), keyword hits, and interesting items related to encryption. The main pane displays a table titled "Encryption Detected" with 6 results. The table has columns for Source File, S, C, O, Comment, and Data Source. The first result is highlighted with a blue selection bar. The table content is as follows:

Source File	S	C	O	Comment	Data Source
In order to ensure that Renzik is treated properly (1).docx				Password protection detected.	device1_laptop.e01
In order to ensure that Renzik is treated properly.docx				Password protection detected.	device1_laptop.e01
f_00028b				Password protection detected.	device1_laptop.e01
f_00028c				Password protection detected.	device1_laptop.e01
In order to ensure that Renzik is treated properly.docx				Password protection detected.	device1_laptop.e01
In order to ensure that Renzik is treated properly.docx				Password protection detected.	device1_laptop.e01

Below the table, there is a detailed view of the selected result (the second row from the table). It shows the Type (Comment), Value (Password protection detected.), and Source(s) (Encryption Detect). The Source File Path is listed as /img\_device1\_laptop.e01/vol\_vol7/Users/AntiRenzik/Downloads/In order to ensure that Renzik is treated properly.docx and the Artifact ID is -9223372036854775803.

# Autopsy

## Ingest Modules: Encryption Detection

The screenshot shows the Autopsy 4.14.0 interface with the title bar "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, and Help. The toolbar features icons for Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Generate Report, Keyword Lists, and Keyword Search.

The left sidebar navigation tree includes:

- Data Sources: device1\_laptop.e01
- Views
- File Types
- Deleted Files
- MB File Size
- Results
  - Extracted Content
    - EXIF Metadata (23)
    - Encryption Detected (6)
    - Encryption Suspected (4)
    - Extension Mismatch Detected (113)
    - User Content Suspected (23)
  - Keyword Hits
  - Hashset Hits
  - E-Mail Messages
    - Interesting Items
      - Encryption (1)
        - Interesting Files (1)
        - Interesting Results (0)
    - Accounts
      - Email
  - Tags
  - Reports

The main content area displays a "Listing" titled "Encryption Suspected". It shows a table with 4 results, with "Thumbnail" selected as the view mode. The table has columns: Source File, S, C, O, Comment, and Data Source. The results are:

Source File	S	C	O	Comment	Data Source
IMPORTANT.jpg				Suspected encryption due to high entropy (7,999999).	device1_laptop.e01
mpenginedb.db				Suspected encryption due to high entropy (7,986163).	device1_laptop.e01
SOFTWARE.LOG1-slack				Suspected encryption due to high entropy (7,944463).	device1_laptop.e01
FontCache-S-1-5-21-2274644105-2924306947-3431561117-1001.dat-slack				Suspected encryption due to high entropy (7,597646).	device1_laptop.e01

Below the table, a detailed view for the first result ("IMPORTANT.jpg") is shown in a tabular format:

Type	Value	Source(s)
Comment	Suspected encryption due to high entropy (7,999999).	Encryption Detec
Source File Path	/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/Desktop/IMPORTANT.jpg	
Artifact ID	-9223372036854775802	

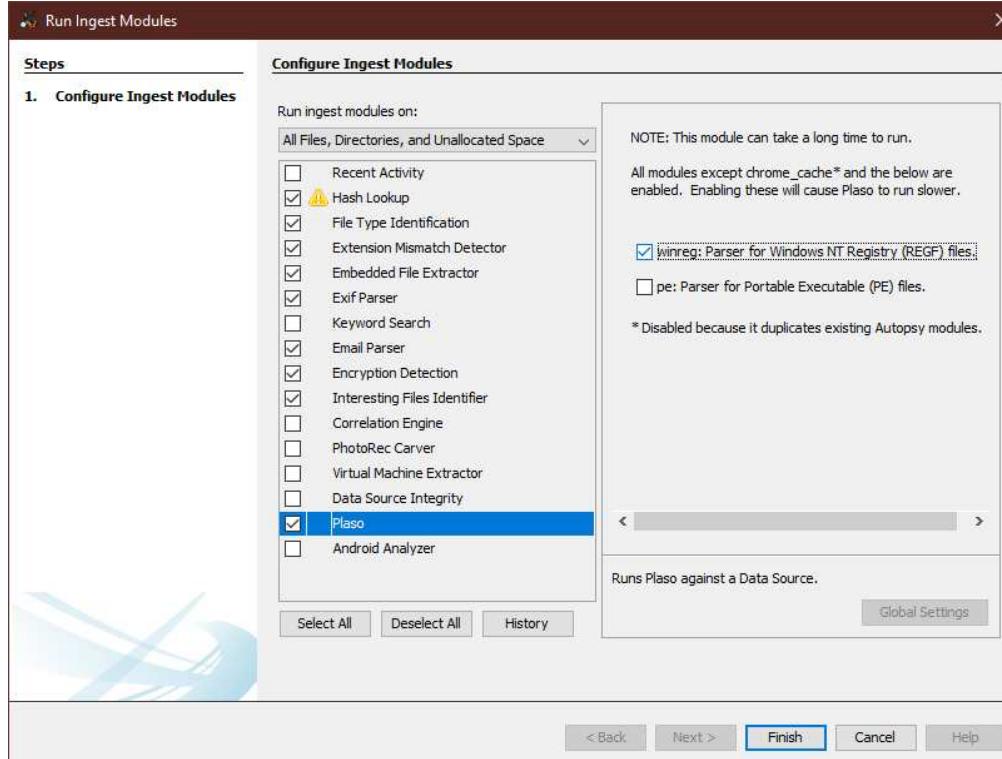
# Autopsy

## *Ingest Modules: Plaso*

- ▶ Tool open source che esegue il *parsing* di file log e altri tipi di file per estrarre i **timestamp**:
  - Estraе quanti più *timestamp* possibili per l'elaborazione di una **timeline**;
  - Operazione molto lunga

# Autopsy

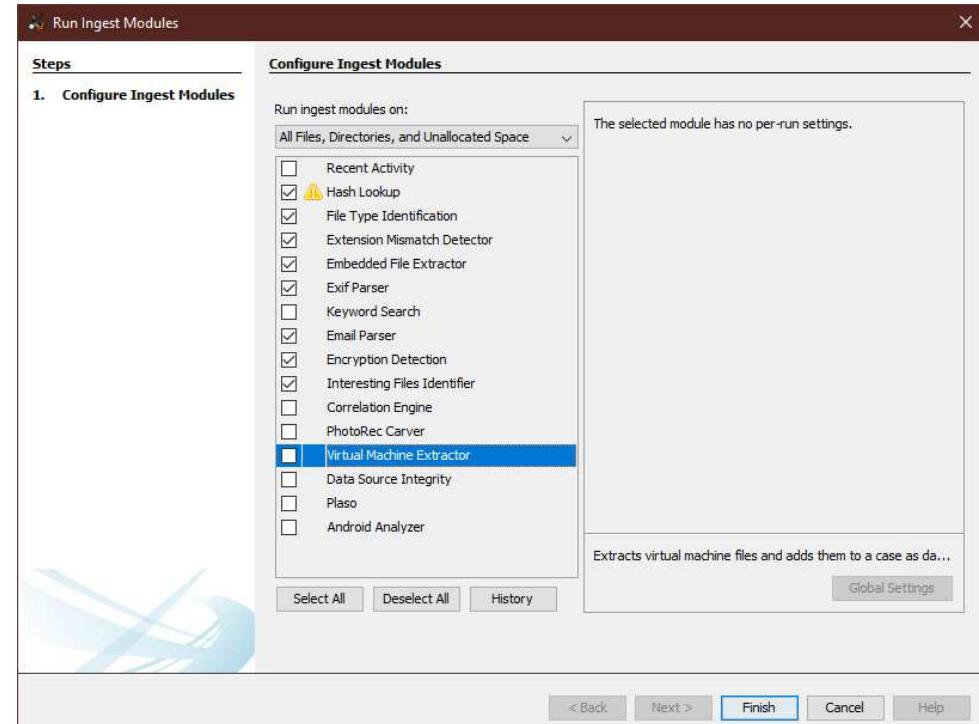
## *Ingest Modules: Plaso*



# Autopsy

## *Ingest Modules: Virtual Machine Extractor*

- ▶ Analizza le *Virtual Machine* presenti all'interno del reperto:
  1. Ricerca i file VMDK e VHD
  2. Crea una copia locale
  3. Vengono inseriti in *datasources*



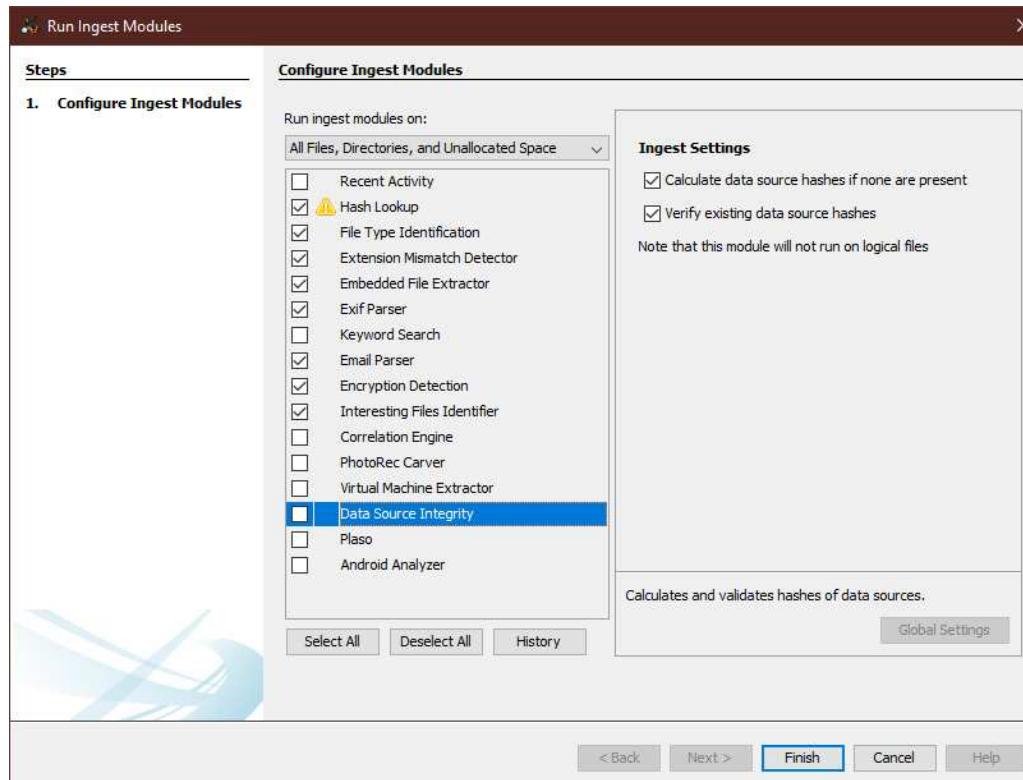
# Autopsy

## *Ingest Modules: Data Source Integrity*

- ▶ Calcola e valida l'hash del reperto
  - Assicura l'integrità dell'evidence
  
- 1. Recupera l'hash dai metadati del disk image oppure da quelli inseriti dal CF.
- 2. Calcola l'hash del disk image
- 3. Invia un alert se la validazione fallisce

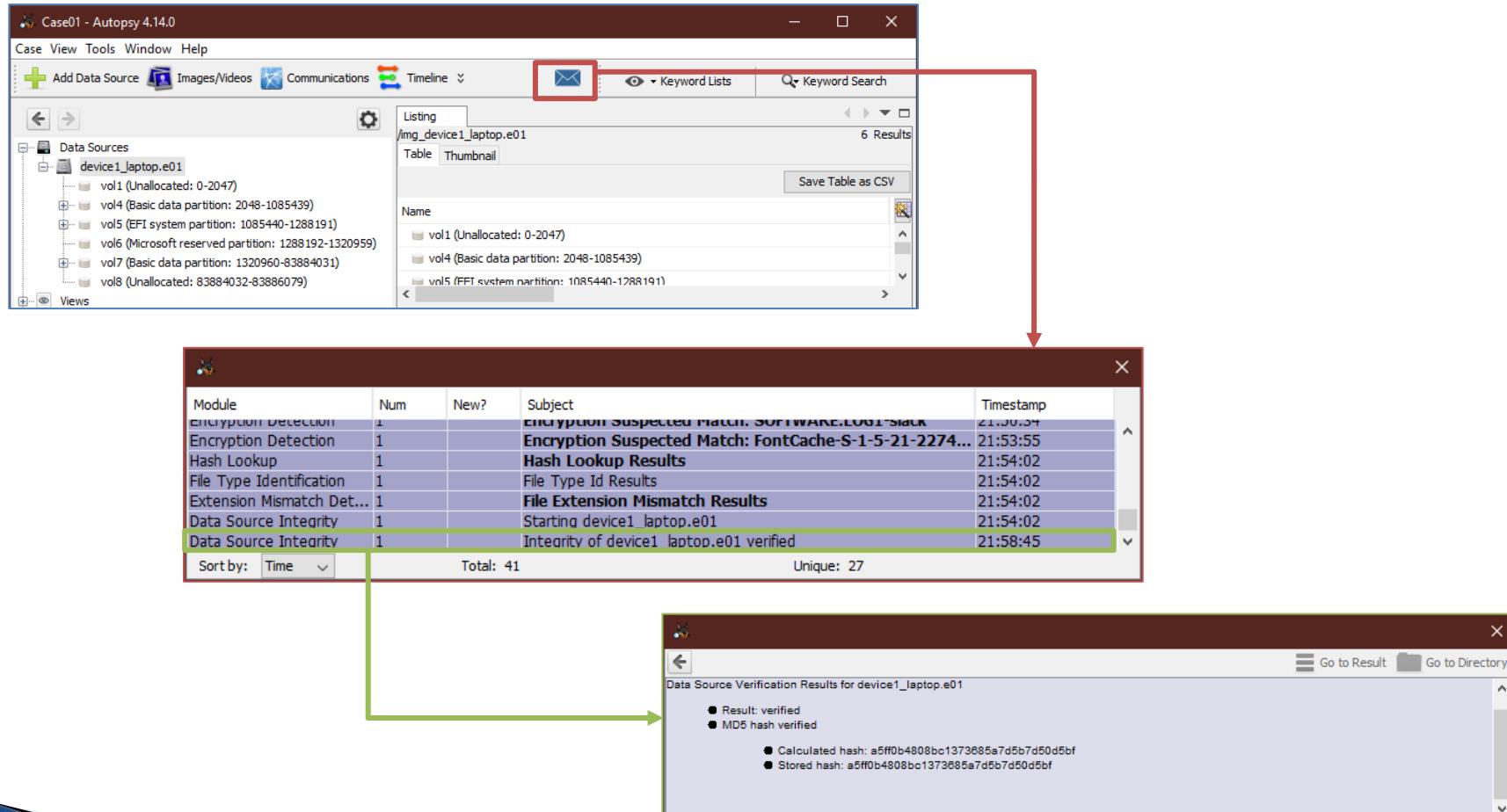
# Autopsy

## *Ingest Modules: Data Source Integrity*



# Autopsy

## Ingest Modules: Data Source Integrity



# Fine prima parte...



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 15: L'Analisi *Autopsy* (2<sup>a</sup> parte)

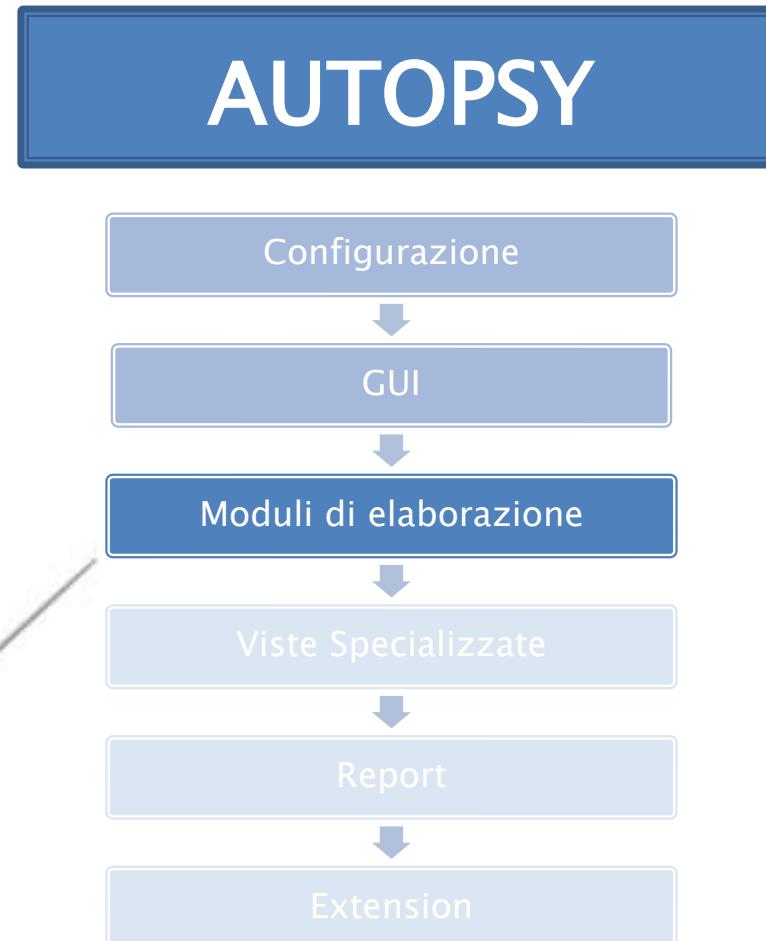


A.A. 2021/22

Dott. Lorenzo LAURATO



# Nella puntata precedente...



# Nella puntata precedente...



- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Correlation Engine
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- Plaso
- Android Analyzer

# Autopsy

» Moduli di elaborazione



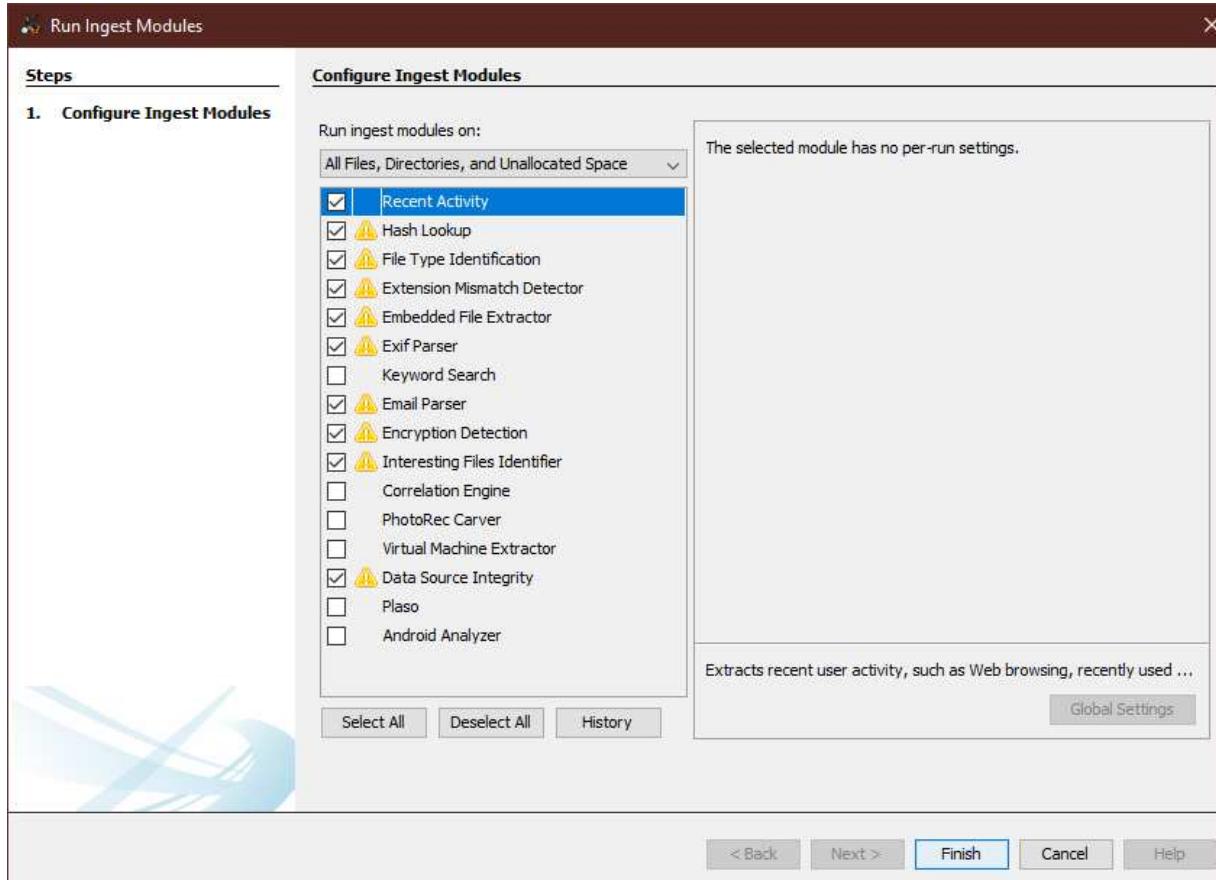
# Autopsy

## *Ingest Modules: Recent Activity*

- ▶ Estrae le attività recenti dell'utente:
  - Analisi dei Web Browser (*History, cookies, download, etc.*)
  - Analisi dei registri:
    - Dispositivi USB
    - Lista utenti
    - Programmi installati
    - Programmi eseguiti
  - Analisi del «Cestino»
- ▶ I risultati vengono inseriti in «*Extracted Content*»

# Autopsy

## *Ingest Modules: Recent Activity*



# Autopsy

## *Ingest Modules: Recent Activity*

### Artefatti WEB

	History	Cookie	Bookmark	Download	Cache	Auto Fill
Chrome	X	X	X	X	X	X
Firefox	X	X	X	X	-	X
IE/Edge	X	X	X	-	-	-
Safari	X	X	X	X	-	-

*I risultati dei differenti browser vengo uniti*

# Autopsy

## Ingest Modules: Recent Activity

### Artefatti WEB

The screenshot shows the Autopsy 4.14.0 interface. The left sidebar displays a tree view of extracted content, with a red box highlighting the 'Web Bookmarks (5)' node under 'Extracted Content'. The main pane shows a table titled 'Listing' for 'Web Bookmarks'. The table has columns: Source File, S, C, O, URL, Title, Program Name, and Date Created. The data is as follows:

Source File	S	C	O	URL	Title	Program Name	Date Created
Bookmarks	0			https://mail.google.com/mail/u/0/#inbox	Gmail	Chrome	2019-10-29 18:32:37 CET
Bookmarks	0			https://www.linkedin.com/feed/?trk=guest_homepage-basic_sign-in-submit	LinkedIn	Chrome	2019-10-31 04:25:13 CET
Bookmarks	0			http://www.ransomizer.com/	Ransom Note Generator	Chrome	2019-11-01 23:27:53 CET
Bookmarks	0			https://twitter.com/home	Twitter	Chrome	2019-11-05 23:25:39 CET
Bing.url	0			http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	Internet Explorer	2019-10-29 18:25:01 CET

Below the table are tabs for Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, and Video Triage.

# Autopsy

## Ingest Modules: Recent Activity

### Artefatti WEB

The screenshot shows the Autopsy 4.14.0 interface with the following details:

**Case01 - Autopsy 4.14.0**

**Case View Tools Window Help**

**Listing** Web Downloads

**Table** **Thumbnail** **Save Table as CSV**

**Source File** **S** **C** **O** **Path** **URL** **Date Accessed**

Source File	S	C	O	Path	URL	Date Accessed
History				C:\Users\AntiRenzik\Downloads\IMG_20191023_170347.jpg	about:blank	2019-11-01 23:13:50 CET
History		0		C:\Users\AntiRenzik\Downloads\IMG_20191023_170347.jpg	https://mail.google.com/mail/u/0/?ui=2&ik=ef83645ed2&a...	2019-11-01 23:13:50 CET
History		0		C:\Users\AntiRenzik\Downloads\IMG_20191023_092858.jpg	https://mail-attachment.googleusercontent.com/attachme...	2019-11-01 23:13:50 CET
History		0		C:\Users\AntiRenzik\Downloads\IMG_20191023_092858.jpg	about:blank	2019-11-01 23:13:51 CET
History		0		C:\Users\AntiRenzik\Downloads\IMG_20191023_092858.jpg	https://mail.google.com/mail/u/0/?ui=2&ik=ef83645ed2&a...	2019-11-01 23:13:51 CET
History		0		C:\Users\AntiRenzik\Downloads\IMG_20191023_092858.jpg	https://mail-attachment.googleusercontent.com/attachme...	2019-11-01 23:13:51 CET

**Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Video Triage**

**Result: 379 of 521** **Result** **Web Downloads**

**Type** **Value** **Source(s)**

Type	Value	Source(s)
Path	C:\Users\AntiRenzik\Downloads\IMG_20191023_170347.jpg	Recent Activity
URL	https://mail.google.com/mail/u/0/?ui=2&ik=ef83645ed2&attid=0.2&permmsgid=msg-f:1649031702406491793&th=16e28998ad4be e91&view=att&disp=safe&realattid=16e289940d7aa98d69c2	Recent Activity
Date Accessed	2019-11-01 23:13:50	Recent Activity
Domain	mail.google.com	Recent Activity
Program Name	Chrome	Recent Activity
Source File Path	/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/History	
Artifact ID	-9223372036854774034	

**Extracted Content** (54 Results)

- Accounts (2)
- EXIF Metadata (46)
- Encryption Detected (26)
- Encryption Suspected (12)
- Extension Mismatch Detected (339)
- Operating System Information (2)
- Recent Documents (24)
- Recycle Bin (3)
- Shell Bags (26)
- USB Device Attached (14)
- User Content Suspected (46)
- Web Bookmarks (5)
- Web Cache (6411)
- Web Cookies (780)
- Web Downloads (54) **(highlighted)**
- Web Form Autofill (3)
- Web History (401)
- Web Search (117)

**Keyword Hits** **Hashset Hits** **E-Mail Messages** **Interesting Items** **Encryption (1)**

# Autopsy

## Ingest Modules: Recent Activity

### Artefatti WEB

The screenshot shows the Autopsy 4.14.0 interface with the following details:

**Case01 - Autopsy 4.14.0**

**Case View Tools Window Help**

**Listing** Web History Table | Thumbnail 401 Results Save Table as CSV

**Data Sources**: device1\_laptop.e01

**Results**:

- Extracted Content
  - Accounts (2)
  - EXIF Metadata (46)
  - Encryption Detected (26)
  - Encryption Suspected (12)
  - Extension Mismatch Detected (339)
  - Operating System Information (2)
  - Recent Documents (24)
  - Recycle Bin (3)
  - Shell Bags (26)
  - USB Device Attached (14)
  - User Content Suspected (46)
  - Web Bookmarks (5)
  - Web Cache (641)
  - Web Cookies (780)
  - Web Downloads (54)
  - Web Form Autofill (3)
  - Web History (401) **(highlighted with a red box)**
  - Web Search (117)
- Keyword Hits
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
    - Encryption (1)
  - Accounts
    - Email
  - Tags
  - Reports

**Table Headers:** Source File, S, C, O, URL, Date Accessed, Referrer URL

**Table Data (partial):**

Source File	S	C	O	URL	Date Accessed	Referrer URL
History	0			http://www.ransomizer.com/	2019-11-05 23:30:15 CET	http://www.ransomizer.com/
History	0			http://www.ransomizer.com/	2019-11-05 23:30:15 CET	http://www.ransomizer.com/
History	0			http://www.ransomizer.com/	2019-11-05 23:30:15 CET	http://www.ransomizer.com/
History	0			http://www.ransomizer.com/	2019-11-05 23:30:15 CET	http://www.ransomizer.com/
History	0			http://www.ransomizer.com/	2019-11-05 23:30:15 CET	http://www.ransomizer.com/
History	0			http://www.ransomizer.com/	2019-11-05 23:30:15 CET	http://www.ransomizer.com/
History	0			http://yahoo.com/	2019-10-29 18:33:05 CET	http://yahoo.com/
History	0			https://accounts.google.com/CheckCookie?hl=en&checked... l	2019-11-12 21:18:51 CET	https://accounts.google.com/CheckCookie?hl=en&checked... l
History	0			https://accounts.google.com/CheckCookie?hl=en&checked... l	2019-10-29 18:29:56 CET	https://accounts.google.com/CheckCookie?hl=en&checked... l
History	0			https://accounts.google.com/ServiceLogin?continue=https://... t	2019-10-29 18:29:56 CET	https://accounts.google.com/ServiceLogin?continue=https://... t
History	0			https://accounts.google.com/ServiceLogin?passive=12096... t	2019-11-12 21:12:43 CET	https://accounts.google.com/ServiceLogin?passive=12096... t
History	0			https://accounts.google.com/ServiceLogin?passive=12096... t	2019-11-12 21:18:00 CET	https://accounts.google.com/ServiceLogin?passive=12096... t

**Details Panel:**

Type	Value	Source(s)
URL	https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://takeout.google.com/settings/takeout&followup=https://takeout.google.com/settings/takeout	Recent Activity
Date Accessed	2019-11-12 21:12:43	Recent Activity
Referrer URL	https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://takeout.google.com/settings/takeout&followup=https://takeout.google.com/settings/takeout	Recent Activity
Title	Download your data	Recent Activity
Program Name	Chrome	Recent Activity
Domain	accounts.google.com	Recent Activity
Source File Path	/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/History	
Artifact ID	-9223372036854774775	

# Autopsy

## Ingest Modules: Recent Activity

### Artefatti WEB

Source File	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				www.google.com	veracrypt	Chrome	2019-10-29 18:30:58 CET	device1_laptop.e01
History				www.google.com	veracrypt	Chrome	2019-10-29 18:30:58 CET	device1_laptop.e01
History				www.google.com	gmail	Chrome	2019-10-29 18:32:09 CET	device1_laptop.e01
History				www.google.com	gmail	Chrome	2019-10-29 18:32:09 CET	device1_laptop.e01
History				www.google.com	linkedin	Chrome	2019-10-31 04:22:32 CET	device1_laptop.e01
History				www.google.com	linkedin	Chrome	2019-10-31 04:22:32 CET	device1_laptop.e01
History				www.google.com	new orleans saints	Chrome	2019-10-31 04:26:31 CET	device1_laptop.e01
History				www.google.com	new orleans saints	Chrome	2019-10-31 04:26:31 CET	device1_laptop.e01
History				www.google.com	new orleans saints	Chrome	2019-10-31 04:26:31 CET	device1_laptop.e01

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Video Triage

Result: 407 of 521 Web Search

Type	Value	Source(s)
Domain	www.google.com	Recent Activity
Text	veracrypt	Recent Activity
Program Name	Chrome	Recent Activity
Date Accessed	2019-10-29 18:30:58	Recent Activity
Source File Path	/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/History	
Artifact ID	-9223372036854760542	

### Web Search: Analisi degli url

# Autopsy

## Ingest Modules: Recent Activity

### Artefatti WEB

The screenshot shows the Autopsy 4.14.0 interface with the following details:

- Case View:** Case01 - Autopsy 4.14.0
- Toolbar:** Case, View, Tools, Window, Help; Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Generate Report, Keyword Lists, Keyword Search.
- Left Sidebar:** Data Sources (device1\_laptop.e01), Views, Results (Extracted Content, Accounts (2), EXIF Metadata (46), Encryption Detected (26), Encryption Suspected (12), Extension Mismatch Detected (339), Operating System Information (2), Recent Documents (24), Recycle Bin (3), Shell Bags (26), USB Device Attached (14), User Generated Content (12), Web Bookmarks (5), Web Cache (6411) **(highlighted with a red box)**, Web Cookies (780), Web Downloads (54), Web Form Autofill (3), Web History (401), Web Search (117), Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items (Encryption (1)), Accounts (Email), Tags, Reports.
- Central Area:** Listing (Web Cache). Table view showing results. Headers: Source File, S, C, O, URL, Date Created, Headers. A table row for 'data\_1' is shown with the following details:

data_1				https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu... https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu... https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu... https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu... https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu... https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu... https://clients1.google.com/tbproxy/af/query?q=Chc2LjEu...	2019-10-29 18:28:49 CET 2019-10-29 18:28:51 CET 2019-10-29 18:28:51 CET 2019-10-29 18:28:51 CET 2019-10-29 18:28:51 CET 2019-10-29 18:28:51 CET 2019-10-29 18:28:51 CET	date : Tue, 29 Oct 2019 10:09:13 GMT content. date : Tue, 29 Oct 2019 03:30:17 GMT server. date : Mon, 28 Oct 2019 17:29:07 GMT content. date : Mon, 28 Oct 2019 17:29:07 GMT content.
--------	--	--	--	--	---	--
- Bottom Navigation:** Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, Video Triage. Result: 3... of 6411.
- Details Panel:** Web Cache. Shows Type, Value, and Source(s) for URL, Date Created, and Headers.

# Autopsy

## Ingest Modules: Recent Activity

### Artefatti WEB

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The main window displays a file tree on the left under "User Data (32)" and a detailed listing table on the right.

**File Tree:**

- User Data (32)
  - BrowserMetrics (3)
  - CertificateRevocation (4)
  - Crashpad (5)
  - Default (83)
    - Accounts (3)
    - AutofillStrikeDatabase (8)
    - blob\_storage (3)
    - BudgetDatabase (8)
    - Cache (1437)
      - data\_1 (2652)
      - data\_2 (1328)
      - data\_3 (1240)
      - f\_000004 (1)
      - f\_000005 (1)
      - f\_000008 (1)
      - f\_000009 (1)
      - f\_00000b (1)
      - f\_000016 (1)
      - f\_000017 (1)
      - f\_000018 (1)
      - f\_000019 (1)
      - f\_00001a (1)
      - f\_00001b (1)
      - f\_00001c (1)
      - f\_00001d (1)
      - f\_00001e (1)
      - f\_000020 (1)
      - f\_000021 (1)
      - f\_000022 (1)
      - f\_000023 (1)
      - f\_000024 (1)

# Autopsy

## *Ingest Modules: Recent Activity*

### Analisi Registri

- ▶ Analisi delle chiavi di registro mediante **RegRipper**:
  - Tool OpenSource
  - Analizza il contenuto del registro e visualizza i risultati:
    - Non è un tool interattivo
- ▶ Registri: *System, Software, Security, SAM, NTUSER*
- ▶ Produzione di artefatti:
  - Dispositivi USB connessi
  - Programmi installati e eseguiti
  - Informazioni di sistema e dell'utente

# Autopsy

## Ingest Modules: Recent Activity

### Registro

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The main window displays a table titled "Listing" with 14 results for "USB Device Attached". The table columns include Source File, S, C, O, Date/Time, Device Make, Device Model, Device ID, and Data Source. The results show various system files from a VMware virtual machine, including several entries for "SYSTEM" files with dates ranging from November 5, 2019, to November 12, 2019. The "Device Make" column shows "VMware, Inc." and "Virtual USB Hub" or "Virtual USB". The "Data Source" column shows "device1\_laptop.e01" and "device1\_laptop.e01".

The left sidebar shows a tree view of "Data Sources" and "Results". The "Results" section is expanded, showing categories like "Extracted Content", "Operating System Information", "Recent Documents", "Recycle Bin", "Shell Bags", "USB Device Attached", and "User Content Suspected". The "USB Device Attached" category is highlighted with a red box. Other categories like "Web Cache" and "Web Cookies" are also visible.

At the bottom, there is a detailed table for the selected "USB Device Attached" entry, showing fields such as Type, Value, and Source(s). The Type column includes "Date/Time", "Device Make", "Device Model", "Device ID", "Source File Pat", and "Artifact ID". The Value column contains specific details like "2019-11-05 01:31:33", "PNY", "Product: 009F", "AFA27H33YD35000553", "/img\_device1\_laptop.e01/vol\_vol7/Windows/System32/config/SYSTEM", and "-9223372036854761205". The Source(s) column indicates "Recent Activity" for most fields.

# Autopsy

## Ingest Modules: Recent Activity

### Registro

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help. The toolbar has icons for Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Keyword Lists, and Keyword Search. The left sidebar shows a tree view of Data Sources, Views, File Types, Deleted Files, MB File Size, Results, Extracted Content (Accounts, EXIF Metadata, Encryption Detected, Encryption Suspected, Extension Mismatch Detected, Operating System Information, Recent Documents, Recycle Bin, Shell Bags, USB Device Attached, User Content Suspected, Web Bookmarks, Web Cache, Web Cookies, Web Downloads, Web Form Autofill, Web History, Web Search), Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, and Reports. The main area is titled "Listing" and shows a table of "Report Name" entries, each preceded by a "RecentActivity" icon. The table has columns for "Source Module Name" and "Report Name". The "Report Name" column contains the following entries:

Source Module Name	Report Name
RecentActivity	RegRipper /img_device1_laptop.e01/vol_volt7/Users/AntiRenzik/AppData/Local/Microsoft/Windows/UserClass.dat
RecentActivity	RegRipper /img_device1_laptop.e01/vol_volt7/Users/AntiRenzik/NTUSER.DAT
RecentActivity	RegRipper /img_device1_laptop.e01/vol_volt7/Users/Default/NTUSER.DAT
RecentActivity	RegRipper /img_device1_laptop.e01/vol_volt7/Windows/ServiceProfiles/LocalService/NTUSER.DAT
RecentActivity	RegRipper /img_device1_laptop.e01/vol_volt7/Windows/ServiceProfiles/NetworkService/NTUSER.DAT
RecentActivity	RegRipper /img_device1_laptop.e01/vol_volt7/Windows/System32/config/SYSTEM

# Autopsy

## *Ingest Modules: Recent Activity*

### Recycle Bin

- ▶ Analisi del file cancellati ed ancora presenti nel «*cestino*»
  - Cambio del filename:
    - ≥ Windows 7: \$R+[random numbers/letters] (Es.:\$R3F5245.doc)
    - < Windows 7: D+[drive letter] +[random numbers/letters]  
(Es.:DC8FXD2.doc)
    - \* se viene eliminata un'intera cartella solo il suo nome cambia.
  - Analisi dei «file manifest» associati ai file:
    - \$I+[*newnamefile*]
    - Conserva l'originale *namefile* e *path*

# Autopsy

## Ingest Modules: Recent Activity

### Recycle Bin

- ▶ Risultato: artefatto «Recycle Bin»

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, and Help. The toolbar features Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Keyword Lists, and Keyword Search. The left sidebar displays Data Sources (device1\_laptop.e01), Views, and Results. Under Results, Extracted Content is expanded, showing Accounts (2), EXIF Metadata (25), Encryption Detected (6), Encryption Suspected (4), Extension Mismatch Detected (113), Operating System Information (2), Percent Documents (24), Recycle Bin (3), Shell Bags (26), USB Device Attached (14), User Content Suspected (25), Web Bookmarks (5), Web Cache (641), Web Cookies (780), Web Downloads (54), Web Form Autofill (3), Web History (401), and Web Search (117). A red box highlights the "Recycle Bin (3)" item. The main pane shows a "Listing" view for the Recycle Bin with 3 Results. It lists three files: \$RFC5YC5.txt, \$RL1DWH.zip, and \$RZXO3SZ.jpg. Below this is a detailed table with columns for Type, Value, and Source(s). The table entries are:

Type	Value	Source(s)
Path	C:\Users\AntiRenzik\Desktop\VCPW.txt	Recycle Bin
Time Deleted	2019-11-12 22:06:29	Recycle Bin
Username		Recycle Bin
Source File Path	/img_device1_laptop.e01/vol_vol7/\$Recycle.Bin/S-1-5-21-2274644105-2924306947-3431561117-1001 /\$RZXO3SZ.jpg	
Artifact ID	-9223372036854761159	

# Autopsy

## Ingest Modules: Recent Activity

### Recycle Bin

- ▶ Risultato: creazione di un «delete file» nella vista ad albero (*data sources*)

The screenshot shows the Autopsy 4.14.0 interface with the title bar "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help, and several icons for Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Keyword Lists, and Keyword Search.

The main window displays the "Listing" view for the path "/img\_device1\_laptop.e01/vol\_vol7/Users/AntiRenzik/Downloads". The results table shows 10 items:

Name	S	C	O	Modified Time	Change Time
In order to ensure that Renzik is treated properly.docx	0			2019-11-05 01:23:02 CET	2019-11-05 01:23:02
In order to ensure that Renzik is treated properly.docx:Zone.Identifier	0			2019-11-05 01:23:02 CET	2019-11-05 01:23:02
Profilepic.png	0			2019-10-29 18:42:01 CET	2019-11-05 23:23:01
Profilepic.png:Zone.Identifier	0			2019-10-29 18:42:01 CET	2019-11-05 23:23:01
VeraCrypt Setup 1.24-Hotfix1.exe	0			2019-10-29 18:31:21 CET	2019-10-29 18:31:28
[current folder]				2019-11-12 21:21:50 CET	2019-11-12 21:21:50
[parent folder]				2019-10-29 18:30:32 CET	2019-10-29 18:30:32
desktop.ini	0			2019-11-05 23:12:06 CET	2019-11-05 23:12:06
takeout-20191112T181254Z-001.zip				2019-11-12 21:21:50 CET	2019-11-12 21:21:50

The left sidebar shows the "Data Sources" tree, with the "Downloads (10)" folder highlighted in red. The bottom panel displays detailed file metadata for "unnamed.jpg":

Name	/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/Downloads/unnamed.jpg
Type	File System
MIME Type	image/jpeg
Size	48095
File Name Allocation	Unallocated
Metadata Allocation	Unallocated

# Autopsy

## *Ingest Modules: Keyword Search*

- ▶ Genera/aggiorna un «text index»:
  - Abilità la ricerca testuale
  - 1. Si estraе ogni word da ogni file
  - 2. Se la word non esiste viene aggiunta
  - 3. Associa la word all'ID del file
- ▶ Uso di Apache Solr:
  - Indice memorizzato all'interno del «case folder»
  - contiene:
    - File name
    - Testo estratto dal contenuto del file
    - Testo estratto dagli artefatti

# Autopsy

## *Ingest Modules: Keyword Search*

- ▶ Uso di *Apache Tika* per l'estrazione del contenuto dei file e dei metadati:
  - Per file non riconosciuti o corrotti: *string extractor*
    - Ricerca per byte (encoding, languages)
- ▶ Uso di un proprio «*HTML Text extractor*»:
  - Estrazione anche di «commenti» e «java script»
- ▶ Normalizzazione
  - Ricerche case insensitive
  - Unicode (Es.: nessuna differenza di accenti)

# Autopsy

## Ingest Modules: Keyword Search

The image shows two windows from the Autopsy forensic analysis tool.

**Run Ingest Modules Window:**

- Steps:** 1. Configure Ingest Modules
- Configure Ingest Modules:**
  - Run ingest modules on:** All Files, Directories, and Unallocated Space
  - Select keyword lists to enable during ingest:** A list of checkboxes for various modules, with "Keyword Search" checked and highlighted in blue.
  - Scripts enabled for string extraction from unknown file types:** A list of checkboxes for modules like Email Parser, Encryption Detection, Interesting Files Identifier, etc.
  - Encodings:** UTF8, UTF16
  - Performing file indexing and periodic search using keywords and regular expressions in lists:** A section with a "Global Settings" button.

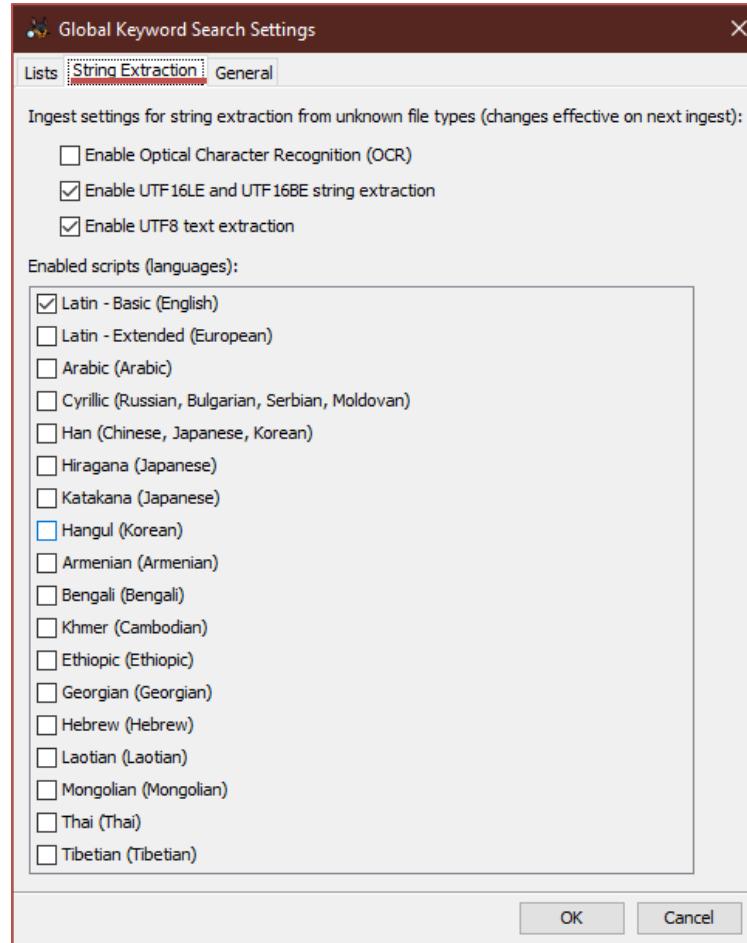
**Global Keyword Search Settings Window:**

- General Tab:**
  - Settings:**
    - Do not add files in NSRL (known files) to keyword index during ingest
    - Show Keyword Preview in Keyword Search Results (will result in longer search times)
  - Results update frequency during ingest:** A group of radio buttons for 20 minutes, 10 minutes, 5 minutes (selected), 1 minute, and No periodic searches.
  - Information:** Files in keyword index: 14552, Chunks in keyword index: 14818
- Buttons:** OK, Cancel

A red arrow points from the "Global Settings" button in the Run Ingest Modules window to the Global Keyword Search Settings window, indicating they are related.

# Autopsy

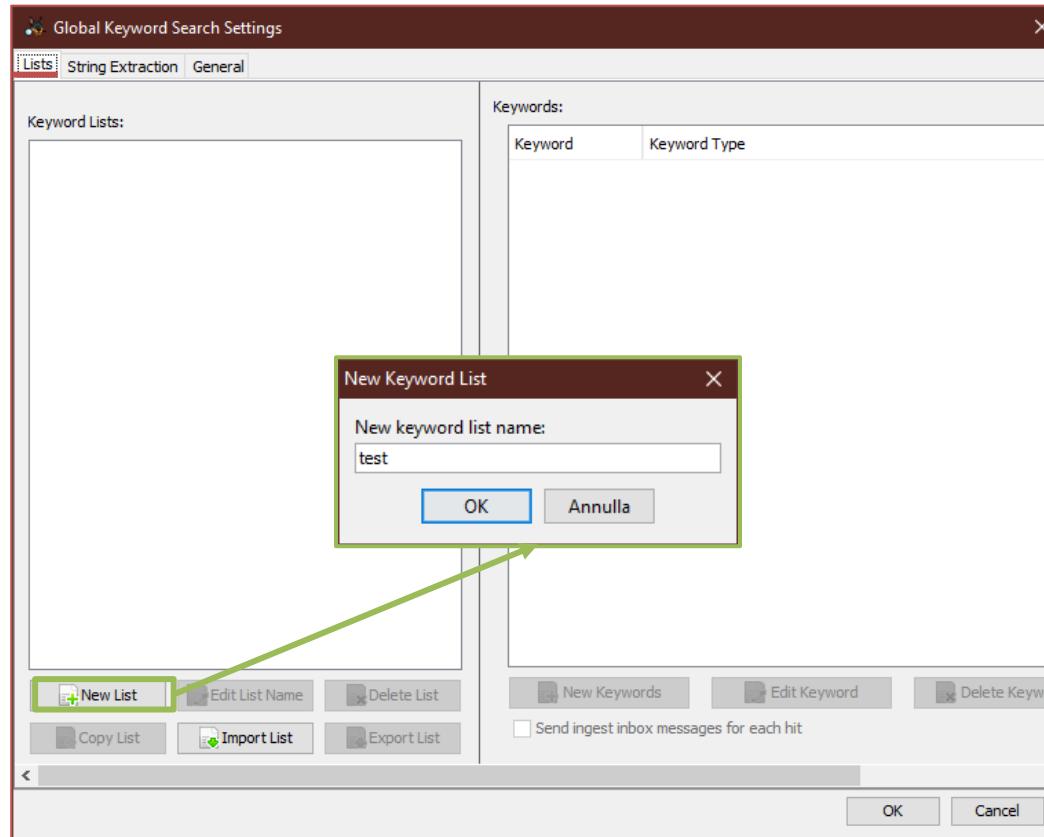
## Ingest Modules: Keyword Search



# Autopsy

## *Ingest Modules: Keyword Search*

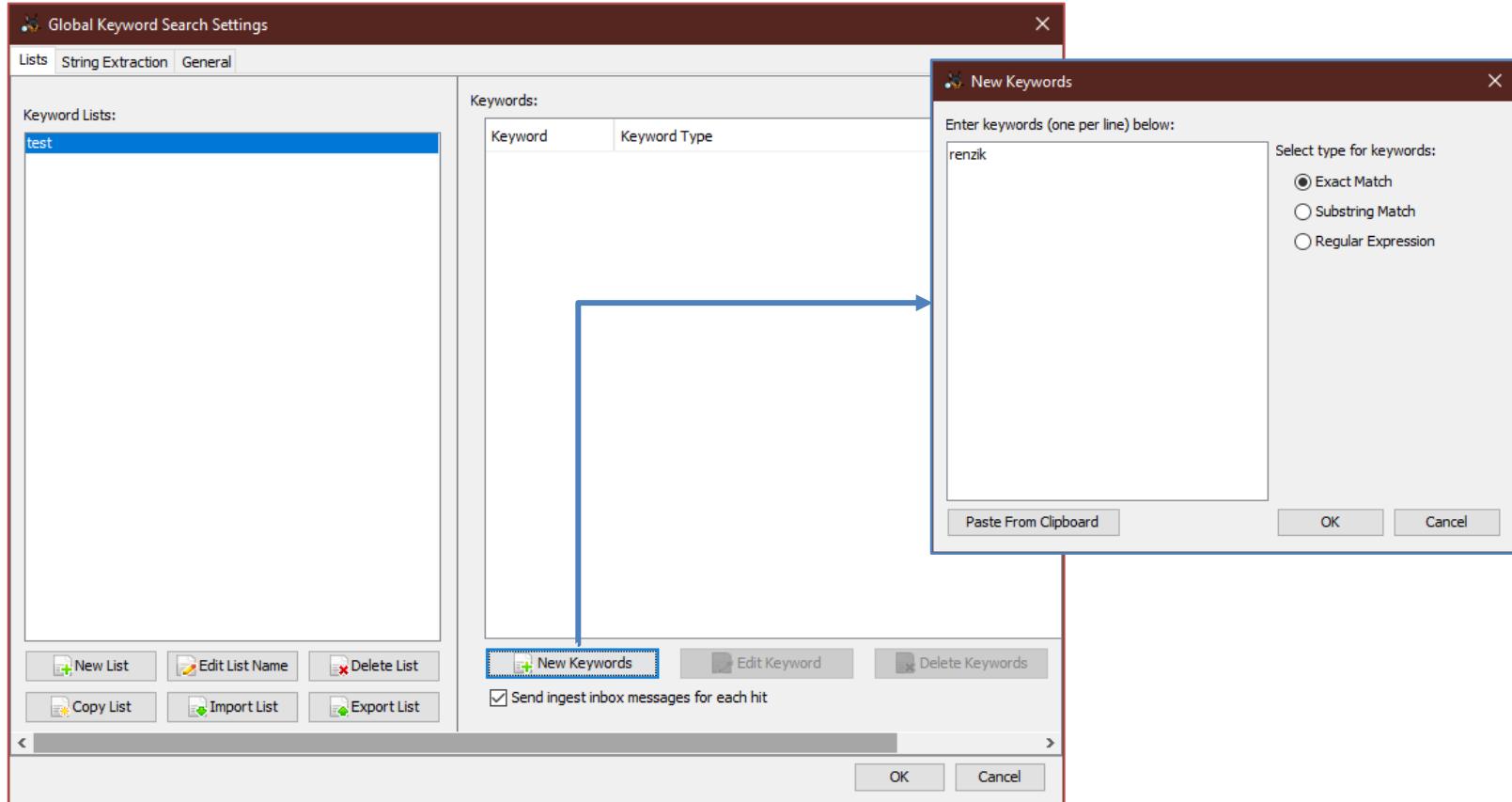
- ▶ Creazione di una lista di keyword



# Autopsy

## *Ingest Modules: Keyword Search*

- ▶ Creazione di una lista di keyword



# Autopsy

## Ingest Modules: Keyword Search

The screenshot shows the Autopsy 4.14.0 interface. On the left, the sidebar includes 'Data Sources' (device1\_laptop.e01 selected), 'Results' (Extracted Content, Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, Reports), and a progress bar at the bottom indicating 'Analyzing files from device1\_laptop.e01' at 22%.

The main pane displays a 'Listing' of results for 'device1\_laptop.e01'. A green box highlights the 'Thumbnail' view. A red arrow points from the 'Keyword Search' button in the top right of the main window to a detailed search configuration dialog.

The 'Keyword Search' dialog is shown in two instances. The top instance has 'Exact Match' selected, a search term 'word', and a table listing partitions (vol1 to vol7). The bottom instance shows 'test' selected in a dropdown under 'Phone Numbers' and 'Email Addresses'.

Name	ID
vol1 (Unallocated: 0-2047)	1
vol4 (Basic data partition: 2048-185439)	4
vol5 (EFI system partition: 10854-0-1288191)	5
vol6 (Microsoft reserved partition: 1288192-1320959)	6
vol7 (Basic data partition: 12000-0-0-0-0-0-0-0)	7

Phone Numbers	Name	Keyword Type
<input type="checkbox"/> IP Addresses	renzik	Exact Match
<input checked="" type="checkbox"/> Email Addresses		
<input type="checkbox"/> URLs		
<input type="checkbox"/> Credit Card Numbers		
<input checked="" type="checkbox"/> test		

# Autopsy

## Ingest Modules: Keyword Search

The screenshot shows the Autopsy 4.14.0 interface with the following details:

- Toolbar:** Case, View, Tools, Window, Help.
- Menu Bar:** Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Keyword Lists, Keyword Search.
- Left Sidebar:** Data Sources (device1\_laptop.e01), Views, Results, Extracted Content (highlighted with a red box). Under Extracted Content, there are sections for Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, and Reports.
- Central Area:** Listing view for the keyword "renzik". The table shows results for "Source File" and "Keyword Preview".

S	C	O	Keyword Preview	Keyword
0	0	is a test of the Anti «Renzik» Broadcasting Network.	renzik	
0	0	(Plaintext) : So, we've had «Renzik» for a few days and no	renzik	
0	0	: what kind of dog is «renzik» Program Name : Chrome	renzik	
0	0	: what kind of dog is «renzik» Program Name : Chrome	renzik	
0	0	Honkerson (Top Goose at Anti «Renzik» Group).Learn why ...	renzik	
0	0	; what kind of dog is «renzik» Program Name : Chrome	renzik	
0	0	Honkerson (Top Goose at Anti «Renzik» Group).Learn why ...	renzik	
0	0	Honkerson (Top Goose at Anti «Renzik» Group).Learn why ...	renzik	
0	0	Honkerson (Top Goose at Anti «Renzik» Group).Learn why ...	renzik	
0	0	In order to ensure that «Renzik» is treated properly (1)	renzik	
0	0	:"Leader of the Anti «Renzik» Group", "entities": {"d	renzik	
0	0	regarding the we\$of «renzik», 35,[362,39],{"du":"!"	renzik	
0	0	regarding the we\$of «renzik»+is+our+8+if+you+do+not+	renzik	
- Bottom Panel:** Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, Video Triage. The Text tab is selected. It shows matches for "renzik" in the file "device1\_laptop.e01/vol/vol7/Users/AntiRenzik/NT/af47be93e4c33dc6\_0".

Domain : www.google.com  
Text : what kind of dog is **renzik**  
Program Name : Chrome  
Date Accessed : 2019-11-12 21:11:56 CET

# Autopsy

## *File Search by Attributes (1)*

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, and Help. The toolbar features icons for Add Data Source, Images/Videos, Communications, Timeline, Keyword Lists, and Keyword Search.

The left sidebar displays a tree view of the case structure:

- device1\_laptop.e01
  - Data Source Files
  - Views
  - File Types
    - By Extension
      - Images (11442)
      - Videos (34)
      - Audio (118)
      - Archives (223)
      - Databases (40)
      - Documents
      - Executable
    - By MIME Type
    - Deleted Files
  - MB File Size
  - Results
    - Extracted Content
    - Keyword Hits
    - Hashset Hits
    - E-Mail Messages
    - Interesting Items
    - Accounts
  - Tags- device2\_mediocard.e01
- Reports

The main pane shows a table titled "Listing" under "Images". It has two tabs: "Table" (selected) and "Thumbnail". The table header includes columns for Name, S, C, O, and Modified Time. The results list several image files:

Name	S	C	O	Modified Time
IC_WelcomeBanner.scale-200.png	1			2019-03-19 07:24:38
IC_WelcomeBanner.scale-400.png	1			2019-03-19 07:24:38
IMG_20191023_092858.jpg	2			2019-11-01 23:13:52
IMG_20191023_092858.jpg	2			0000-00-00 00:00:00
IMG_20191023_092858.jpg	2			0000-00-00 00:00:00

A search bar at the bottom of the table contains the text "IMG". A dropdown menu titled "Match Case" is open, listing various attributes to search in:

- Name
- S
- C
- O
- Modified Time
- Change Time
- Access Time
- Created Time
- Size
- Flags(Dir)
- Flags(Meta)
- Known
- Location
- MD5 Hash
- MIME Type
- Extension

Below the table, a thumbnail preview shows a landscape photograph of a bridge over water.

# Autopsy

## File Search by Attributes (2)

The screenshot illustrates the process of performing a file search by attributes in the Autopsy Forensic Browser. A blue arrow points from the 'File Search by Attributes' menu item in the top-left navigation bar to the 'File Search by Attributes' dialog box. Another blue arrow points from the 'Search' button in the dialog box to the 'File Search Results 1' table on the right.

**File Search by Attributes Dialog:**

- Name:**
- Date:**  to   
Empty fields mean "No Limit". The date format is mm/dd/yyyy.
- Timezone:** (GMT+1:00) Europe/Berlin
- Modified:**
- Accessed:**
- Created:**
- Changed:**
- Size:**  equal to  Byte(s)
- Known Status:**
  - Unknown
  - Known (NSRL or other)
  - Notable
- MIME Type:**    
A dropdown menu lists several image MIME types: image/ief, image/jp2, image/jpeg, image/jpm, and image/jpx.
- Data Source:**    
A dropdown menu lists a single source: device1\_laptop.e01.
- MD5:**

**Search**

**File Search Results 1**

Name	S	C	O	Modified Time	Change Time
IMG_20191023_092858.jpg	2			2019-11-01 23:13:52 CET	2019-11-01
IMG_20191023_142721.jpg	2			2019-11-01 23:13:53 CET	2019-11-01
IMG_20191023_170347.jpg		!	I	2019-11-01 23:13:51 CET	2019-11-01
IMG_20191024_155744.jpg	2			2019-11-01 23:13:49 CET	2019-11-01
img0_1024x768.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_1200x1920.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_1366x768.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_1600x2560.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_2160x3840.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_2560x1600.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_3840x2160.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_768x1024.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img0_768x1366.jpg	1			2019-03-19 05:45:56 CET	2019-10-29
img100.jpg	0			2019-03-19 05:43:45 CET	2019-10-29
img101.png	0			2019-03-19 05:43:45 CET	2019-10-29

**Save Table as CSV**

# Autopsy

## Search All Cases

The screenshot shows the Autopsy software interface. On the left is a vertical menu bar with the following options:

- Tools
- Window
- Help
- Images/Videos
- Communications
- Geolocation
- Timeline
- File Discovery
- File Search by Attributes
- Search All Cases** (highlighted with a blue selection bar)
- Find Common Properties
- Run Ingest Modules >
- Generate Report
- Plugins
- Python Plugins
- Options
- Make Live Triage Drive
- Open Case Folder
- Create Logical Imager

In the center, a modal dialog box titled "Search All Cases" is displayed. It contains the following text:  
"Search the Central Repository for correlation properties with a specified value. The search is case insensitive."  
Below this is a "Correlation Property Type:" dropdown menu with "Files" selected. To its right is a "Correlation Property Value:" input field containing the placeholder "Example: "f0e1d2c3b4a5968778695a4b3c2d1e0f"".  
At the bottom of the dialog, it says "The current Central Repository contains 1 case(s)." and has a "Search" button.

To the right of the dialog, a sidebar titled "Files" lists various correlation property types. The "Domains" option is currently selected, highlighted with a blue background. Other listed items include:

- Domains
- Email Addresses
- Phone Numbers
- USB Devices
- Wireless Networks
- MAC Addresses
- IMEI Number

# Autopsy

## *Ingest Modules: Correlation Engine*

- ▶ Ricerca dei file del caso all'interno del «Central Repository»:
  - Correlare il Caso corrente con i Casi passati:
    - Evidenzia i file\item che erano stati etichettati come «Notable» nei Casi precedenti.
- ▶ Aggiorna il «Central Repository» con i file del Caso corrente:
  - Consente di correlare nuovi Casi al Caso corrente.

# Autopsy

## *Ingest Modules: Correlation Engine*

- ▶ «Central Repository» conserva:
  - Valore (*Hash, Phone Numbers, eMail address, etc*)
  - Caso
  - Data Source
  - File Path
  - Commento del CF
  - Notable Status

# Autopsy

## Ingest Modules: Correlation Engine

Case01 - Autopsy 4.14.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Keyword Lists Keyword Search

Listing img\_device1\_laptop.e01/vol\_vol7/Users/AntiRenzik/Desktop/Pictures 16 Results

Name S C O Modified Time

Save Table as CSV

Properties

View in New Window

Open in External Viewer Ctrl+E

View File in Timeline...

Extract File(s)

Export selected rows to CSV

Add File Tag

Remove File Tag

Add/Edit Central Repository Comment

Add File to Hash Set

Bookmark Ctrl+B

CAT-0: Uncategorized

CAT-1: Child Exploitation (Illegal) (Notable)

CAT-2: Child Exploitation (Non-Illegal/Age Difficult) (Notable)

CAT-3: CGI/Animation (Child Exploitive) (Notable)

CAT-4: Exemplar/Comparison (Internal Use Only)

CAT-5: Non-pertinent

Follow Up

Notable Item (Notable)

Tag and Comment...

New Tag...

a.a. 2021/22

# Autopsy

## Ingest Modules: Correlation Engine

Run Ingest Modules

Steps

1. Configure Ingest Modules

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Correlation Engine
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- Plaso
- Android Analyzer

Select All   Deselect All   History

Ingest Settings

Save items to the Central Repository

Flag items previously tagged as notable

Flag devices previously seen in other cases

Saves properties to the central repository for later correlation

Global Settings

Manage Correlation Properties

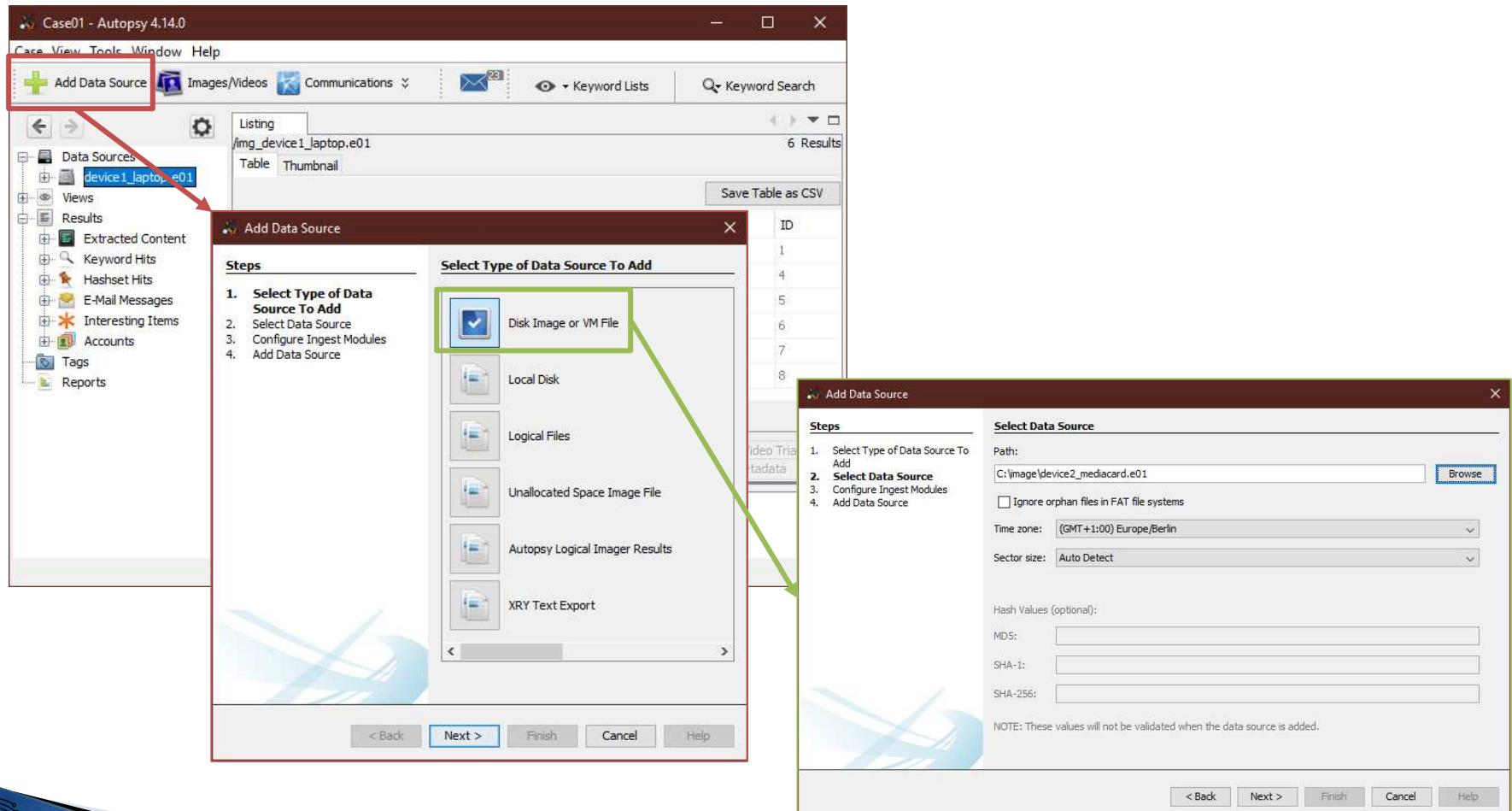
Enable one or more correlation properties to use for correlation during ingest. Note, these properties are global and impact all users of the Central Repository.

Correlation Properties	Enable
Files	<input checked="" type="checkbox"/>
Domains	<input checked="" type="checkbox"/>
Email Addresses	<input checked="" type="checkbox"/>
Phone Numbers	<input checked="" type="checkbox"/>
USB Devices	<input checked="" type="checkbox"/>
Wireless Networks	<input checked="" type="checkbox"/>
MAC Addresses	<input checked="" type="checkbox"/>
IMEI Number	<input checked="" type="checkbox"/>
IMSI Number	<input checked="" type="checkbox"/>
ICCID Number	<input checked="" type="checkbox"/>

< Back   Next >   Finish   Cancel   Help

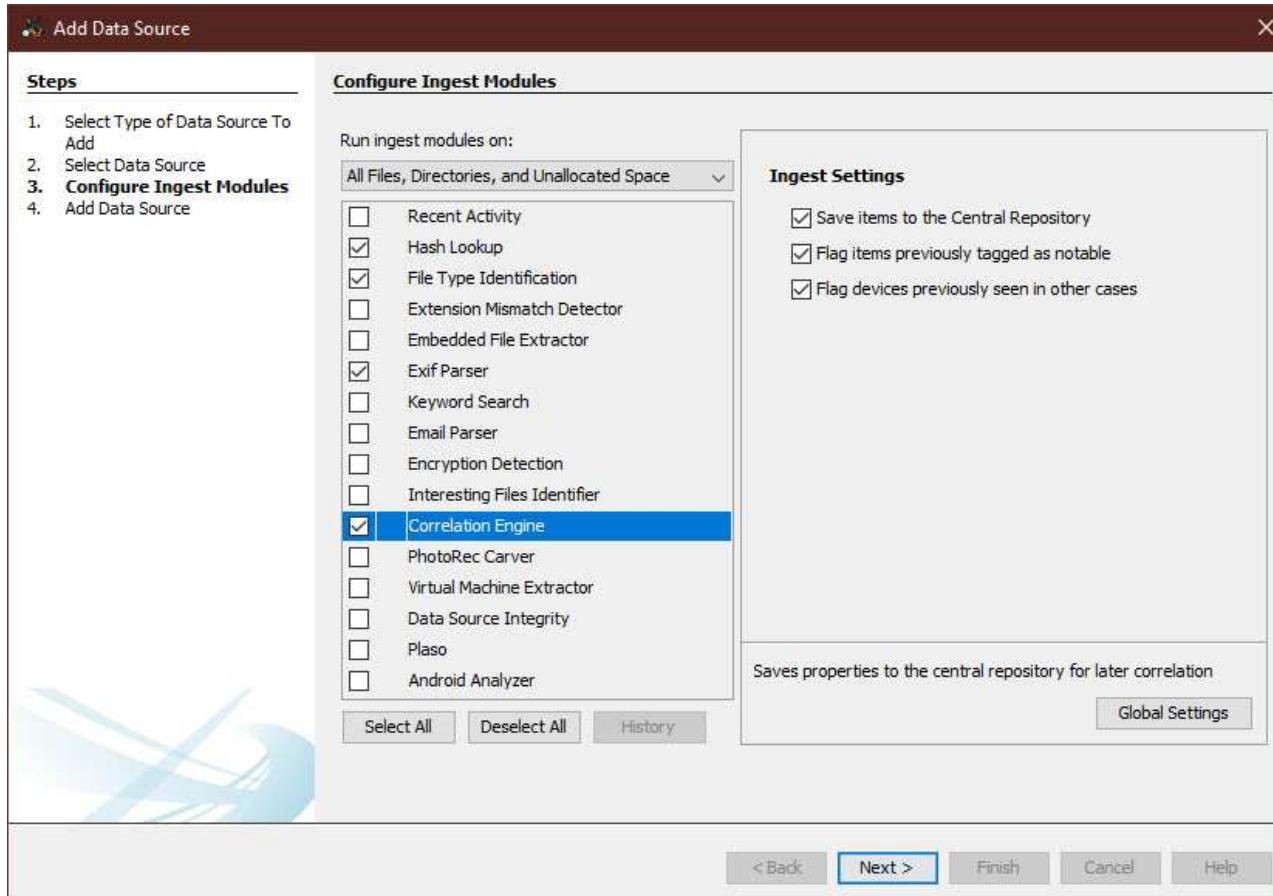
# Autopsy

## *new evidence*



# Autopsy

## *Ingest Modules: Correlation Engine*



# Autopsy

## Option Panel View

The image shows the Autopsy Option Panel View. On the left, there is a sidebar with various options like Data Sources, Views, File Types, Deleted Files, MB File Size, Results, Extracted Content, and Reports. A blue arrow points from the 'Views' icon in the sidebar to a central 'Global Settings' dialog box. The 'Global Settings' dialog contains several configuration options:

- Hide known files (i.e. those in the NIST NSRL) in the:
  - Data Sources area (the directory hierarchy)
  - Views area
- When selecting a file:
  - Change to the most specific file viewer
  - Stay on the same file viewer
- Hide slack files in the:
  - Data Sources area (the directory hierarchy)
  - Views area
- When displaying times:
  - Use local time zone
  - Use another time zone
- Hide other users' tags in the:
  - Tags area in the tree
- Do not add columns for:
  - S(core), C(omments), and O(ccurrences) to reduce loading times
- Translate text:
  - Add column in result viewer for file name translation
- Maximum number of Results to show in table:

Below the settings, there are sections for Current Case Settings and Current Session Settings, each containing a checkbox. In the Current Case Settings section, the checkbox 'Group by data source' is highlighted with a red border.

On the right, there is a comparison between two file tree structures. The left tree is for 'device1\_laptop.e01' and the right tree is for 'device2\_mediocard.e01'. The right tree shows the results of applying the 'Group by data source' setting, where items under 'Extracted Content' are grouped together. A large red arrow points from the 'Current Case Settings' section towards the right tree.

# Autopsy

## Ingest Modules: Correlation Engine

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help, and several icons for Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Generate Report, Keyword Lists, and Keyword Search.

The left sidebar displays a tree view of data sources:

- device1\_laptop.e01
- device2\_mediocard.e01
- Data Source Files
- Views
- File Types
- Deleted Files
- MB File Size** (highlighted)
- Results
  - Extracted Content
    - EXIF Metadata (5)
    - User Content Suspected (5)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
    - Previously Tagged As Notable (Central Repository) (1)
      - Interesting Files (1)
      - Interesting Results (0)
  - Accounts
- Tags
- Reports

The main pane shows the "Listing" results for "Previously Tagged As Notable (Central Repository)". The table has columns: Source File, S, C, O, Comment, File Path, and Modified Time. One result is listed:

Source File	S	C	O	Comment	File Path	Modified Time
IMG_20191023_170347.jpg	2			Previous Case: Case01	/img_device2_mediocard.e01/vol_vol2/DCIM/Camera/IMG...	2019-10-23 16:03:46 CEST

The "Data Content" tab is selected, showing a table with columns: Case, Data Source Name, File Name, and Common Properties. The "Common Properties" section details:

- Type: Files
- Value: b4e585878de4083f162b582bd10a5d67
- Known Status: notable

The "File Details" section shows the File Path: /users/antrenzic/desktop/pictures/img\_20191023\_170347.

The "Data Source Details" section shows the Name: device1\_laptop.e01.

The "Case Details" section shows the Name: Case01 and Created Date: 2020/05/12 13:25:22 (CEST).

At the bottom, it says Central Repository Starting Date: 2020/05/12 13:25:22 (CEST) and Found 3 instances in 1 cases and 1 data sources.

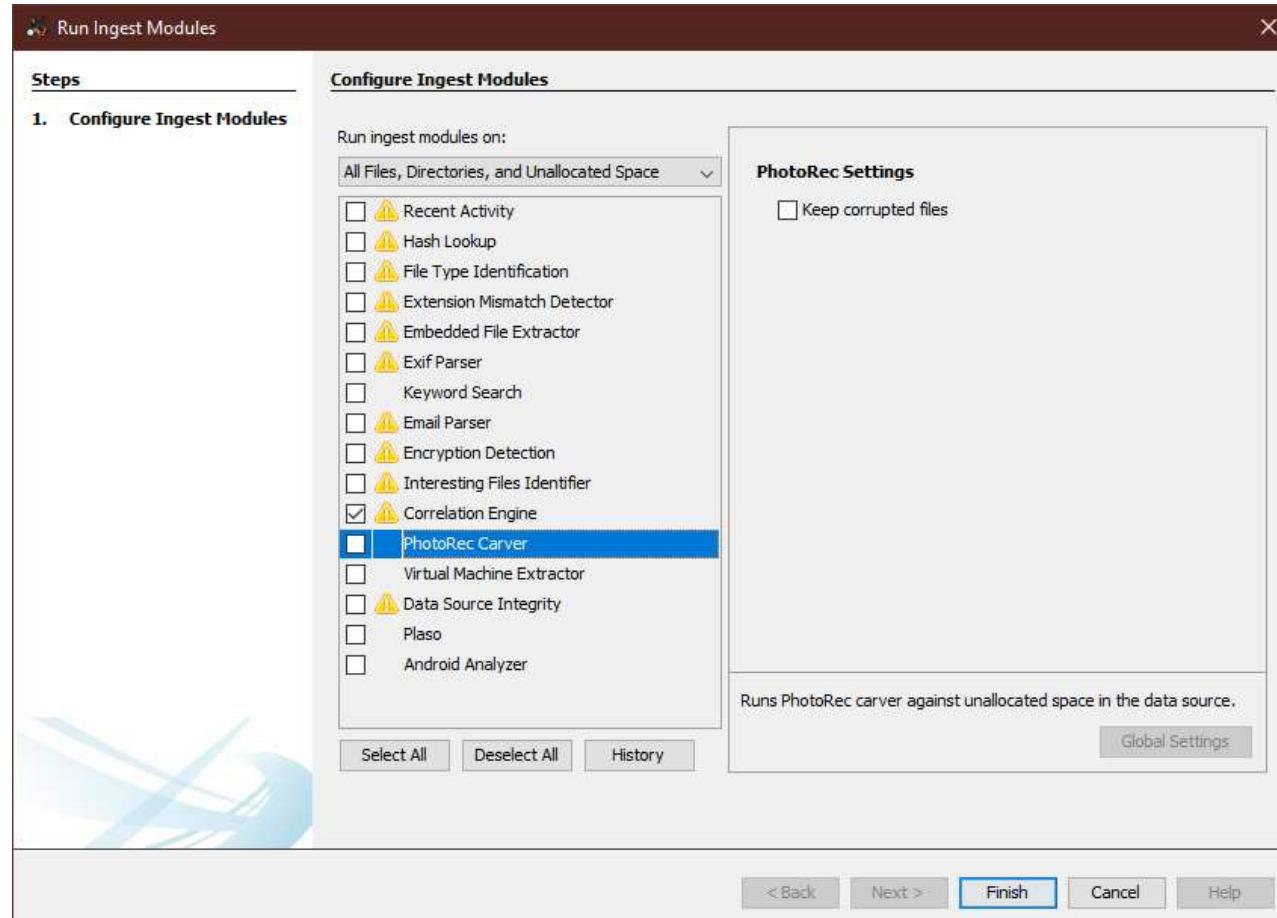
# Autopsy

## *Ingest Modules: PhotoRec Carver*

- ▶ Recupero dei file cancellati mediante «PhotoRec»:
  - OpenSource Tool
  - Data Carving
  - lavora su «unallocated space»
  
- ▶ Risultati:
  - nella vista ad albero «\$CarvedFile»

# Autopsy

## *Ingest Modules: PhotoRec Carver*



# Autopsy

## Ingest Modules: PhotoRec Carver

### Unallocated Space

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Keyword Lists, and Keyword Search. The main window displays a file tree on the left and a listing table on the right.

**File Tree:**

- device1\_laptop.e01
  - Data Source Files
    - device1\_laptop.e01
      - vol1 (Unallocated: 0-2047) (highlighted)
      - vol4 (basic data partition: 2048-1085459)
      - vol5 (EFI system partition: 1085440-1288191)
      - vol6 (Microsoft reserved partition: 1288192-1320959)
      - vol7 (Basic data partition: 1320960-83884031)
        - \$OrphanFiles (0)
        - \$Extend (9)
        - \$Recycle.Bin (5)
        - Unalloc (29) (highlighted)
      - Documents and Settings (2)
      - Perflogs (2)
      - Program Files (20)
      - Program Files (x86) (17)
      - ProgramData (15)
      - Recovery (2)
      - System Volume Information (6)
      - Users (8)
      - Windows (105)
    - vol8 (Unallocated: 83884032-83886079) (highlighted)

**Listing Table:**

Name	S	C	O	Modified Time	Change Time	Action
Unalloc_390291_12144484352_13048868864				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_13067730944_16573267968				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_16805244928_17878986752				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_17878986752_18952728576				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_18952728576_20026470400				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_20026470400_21100212224				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_21100212224_22173954048				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_22173954048_23247695872				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_23247695872_24321437696				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_24321437696_25395179520				0000-00-00 00:00:00	0000-00-00 00:00:00	
Unalloc_390291_25395179520_26468921344				0000-00-00 00:00:00	0000-00-00 00:00:00	

Below the table, there are tabs for Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, and Video Triage. The status bar at the bottom indicates "Analyzing files from device1\_laptop.e01" and "9%".

*Unalloc\_ParentID\_StartByte\_EndByte*

# Autopsy

## Ingest Modules: PhotoRec Carver

### \$CarvedFiles

The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The menu bar includes Case, View, Tools, Window, Help, and several icons for Add Data Source, Images/Videos, Communications, Timeline, File Discovery, Close Case, Generate Report, Keyword Lists, and Keyword Search.

The left sidebar displays the file system structure of "device1\_laptop.e01":

- device1\_laptop.e01
  - vol1 (Unallocated: 0-2047)
  - vol4 (Basic data partition: 2048-1085439)
  - vol5 (EFI system partition: 1085440-1288191)
  - vol6 (Microsoft reserved partition: 1288192-1320959)
  - vol7 (Basic data partition: 1320960-83884031)
    - \$OrphanFiles (0)
    - \$CarvedFiles (818) **(highlighted)**
    - sextendo (9)
    - \$Recycle.Bin (5)
    - \$Unalloc (29)
    - Documents and Settings (2)
    - Perflogs (2)
    - Program Files (20)
    - Program Files (x86) (17)
    - ProgramData (15)
    - Recovery (2)
    - System Volume Information (6)
    - Users (8)
    - Windows (105)
  - vol8 (Unallocated: 83884032-83886079)
- Views
  - File Types
  - By Extension
  - By MIME Type
  - Deleted Files
  - MB File Size** **(highlighted)**
  - Results
    - Extracted Content
      - Accounts (2)
      - EVKML.L1 (2)

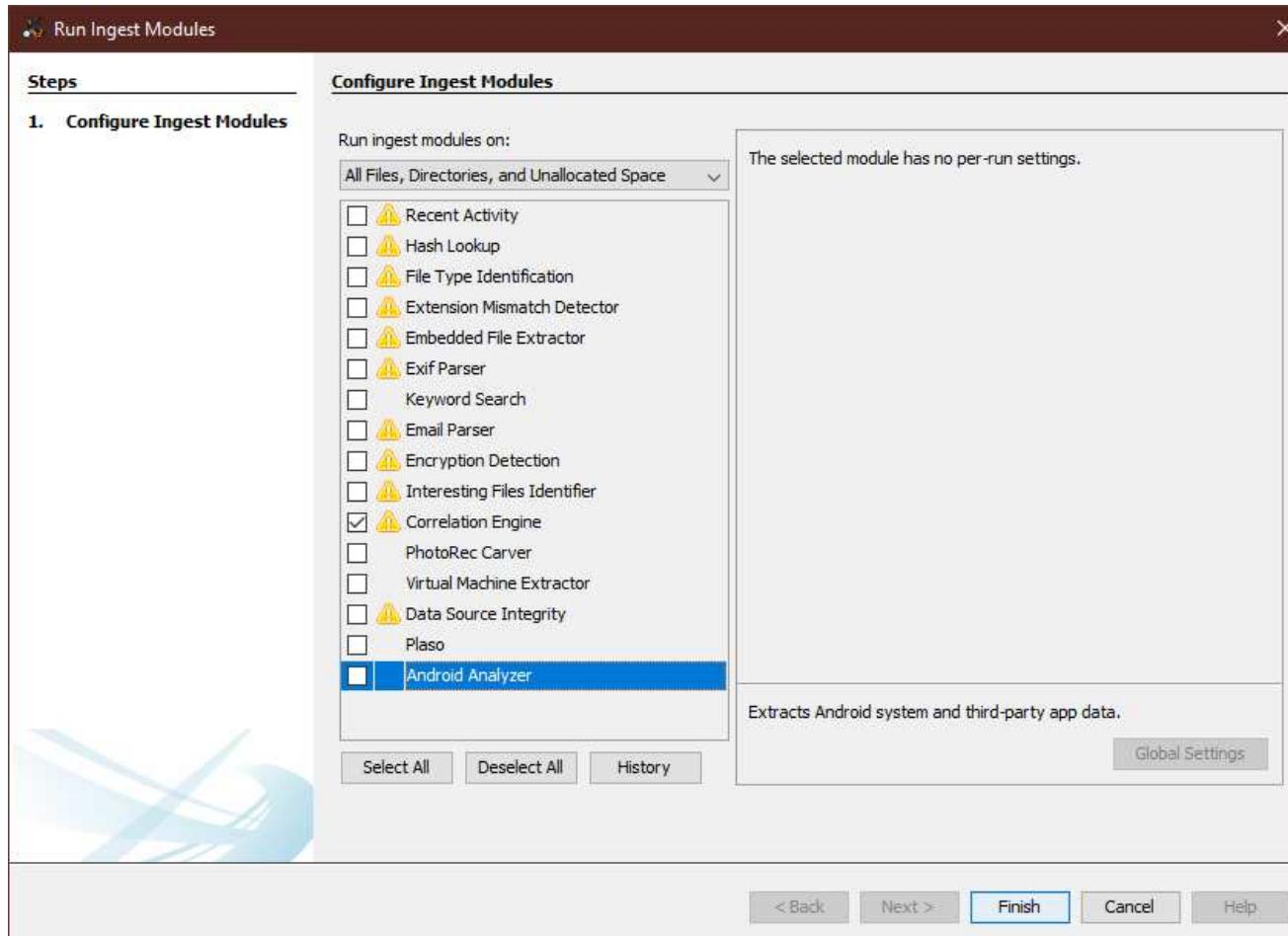
# Autopsy

## *Ingest Modules: Android Analyzer*

- ▶ Analizza i dispositivi Android:
  - Database di Android e App di terze parti;
  - Acquisizione fatta mediante altri strumenti;
  
- ▶ Estrae:
  - Registro Chiamate
  - Contatti
  - Messaggistica (SMS, WhatsApp, Facebook Messenger, etc.)
  - Browser
  - Geolocation
  - ...

# Autopsy

## *Ingest Modules: Android Analyzer*



# Autopsy

» Viste specializzate



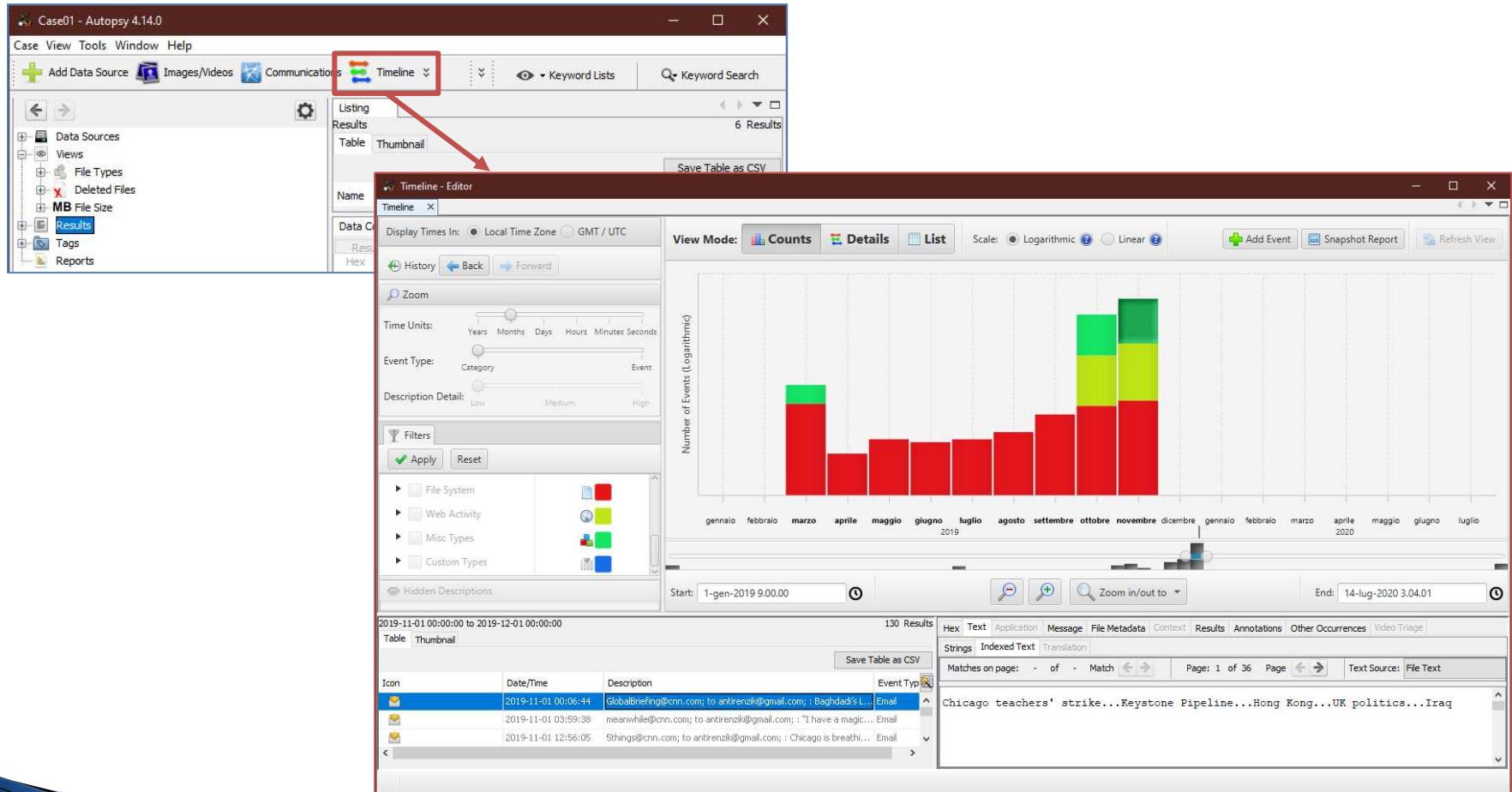
# Autopsy

## *TimeLine Graphic Interface*

- ▶ Consente di visualizzare graficamente le attività del sistema ordinate temporalmente:
  - File Time estratti dal «File System»
  - Web activity estratti dal «Recent Activity»
  - Exif
  - Plaso
  - Etc.
- ▶ Obiettivo:
  - *Quando è stato usato il sistema?*
  - *Cosa è accaduto in un certo tempo?*
  - *Cosa è accaduto prima e dopo a certi eventi?*

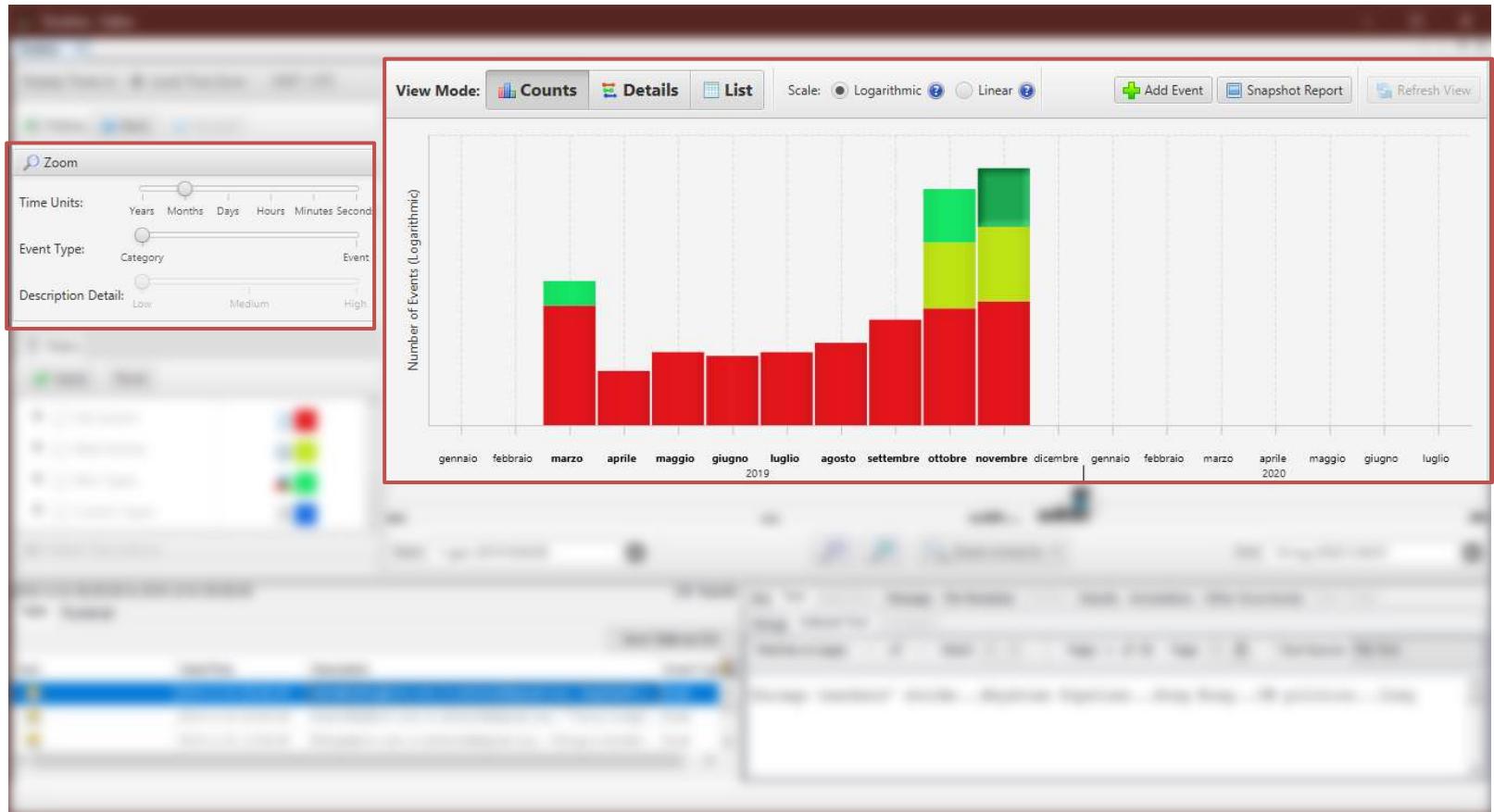
# Autopsy

## TimeLine Graphic Interface



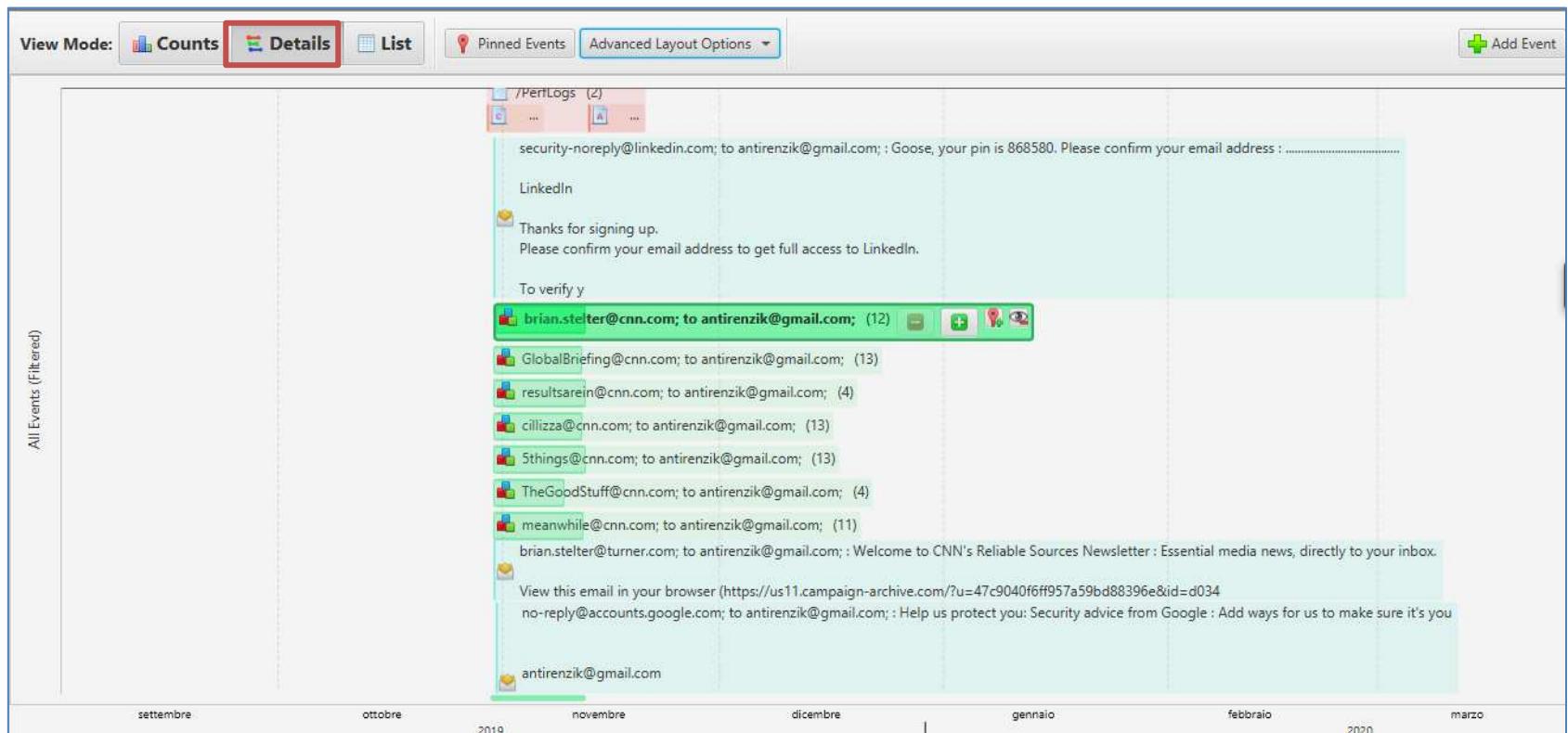
# Autopsy

## *TimeLine Graphic Interface*



# Autopsy

## TimeLine Graphic Interface



# Autopsy

## TimeLine Graphic Interface

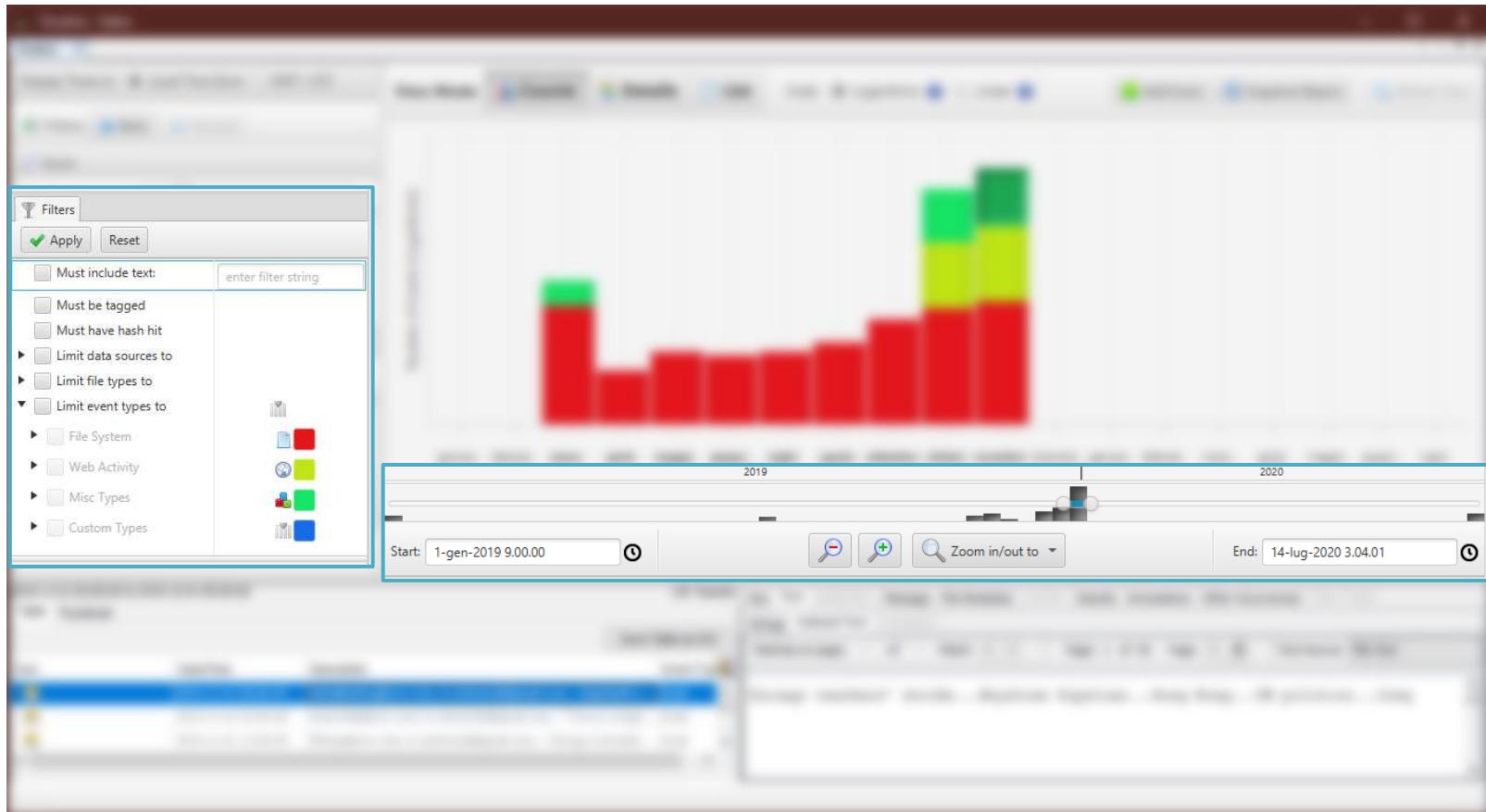
View Mode: **Counts** **Details** **List** List Add Event Snapshot Report Refresh View

395.651 events

Date/Time	Event Type	Description	Tagged	Hash Hit	+
2019-09-16 17:49:30	M__	/Users/AntiRenzik/AppData/Local/Google/Chrome/Us ... Cache/data_1/data_1_a10107f4/data_1_a10107f4/0			
2019-09-18 18:21:36	M__	/Users/AntiRenzik/AppData/Local/Google/Chrome/Use ... efault/Cache/data_3/data_3_c10306a8/optanon.css			
2019-09-20 06:14:04	M__	/Windows/WinSxS/x86_microsoft-windows-servicing ... 0.0.18362.411_none_03353754a072182b/poqexec.exe			
2019-09-20 06:14:04	M__	/Windows/SysWOW64/poqexec.exe			
2019-09-20 06:29:50	M__	/Windows/WinSxS/x86_microsoft-windows-s..gstack-b ... .18362.411_none_4f9cf9dd49a2a582/fveupdateai.dll			
2019-09-20 06:29:57	M__	/Windows/WinSxS/x86_microsoft-windows-s..ck-mof- ... .0.18362.411_none_1397bf66083d7047/wbemcore.dll			
2019-09-20 06:29:57	M__	/Windows/WinSxS/x86_microsoft-windows-servicings ... 8362.411_none_03353754a072182b/TiFileFetcher.exe			
2019-09-20 06:29:58	M__	/Windows/WinSxS/x86_microsoft-windows-s..install ... 18362.411_none_e592469f7e8e080b/wmicmplugin.dll			
2019-09-20 06:29:58	M__	/Windows/WinSxS/x86_microsoft-windows-s..install ... 362.411_none_e592469f7e8e080b/NetSetupEngine.dll			
2019-09-20 06:29:58	M__	/Windows/WinSxS/x86_microsoft-windows-servicings ... 0.0.18362.411_none_03353754a072182b/CbsCore.dll			
2019-09-20 06:29:59	M__	/Windows/WinSxS/x86_microsoft-windows-s..gstack-b ... 18362.411_none_4f9cf9dd49a2a582/securebootai.dll			
2019-09-20 06:30:01	M__	/Windows/WinSxS/x86_microsoft-windows-servicings ... 18362.411_none_03353754a072182b/updateagent.dll			
2019-09-20 06:30:02	M__	/Windows/WinSxS/x86_microsoft-windows-servicings ... 35_10.0.18362.411_none_03353754a072182b/dpx.dll			
2019-09-20 06:30:04	M__	/Windows/WinSxS/x86_microsoft-windows-servicings ... 35_10.0.18362.411_none_03353754a072182b/wcp.dll			
2019-09-20 06:30:14	M__	/Windows/WinSxS/x86_microsoft-windows-servicings ... 0.18362.411_none_03353754a072182b/smiengine.dll			
2019-09-20 06:36:27	M__	/Windows/System32/poqexec.exe			
2019-09-20 06:36:27	M__	/Windows/WinSxS/amd64_microsoft-windows-servici ... 0.0.18362.411_none_5f53d2d858cf8961/poqexec.exe			

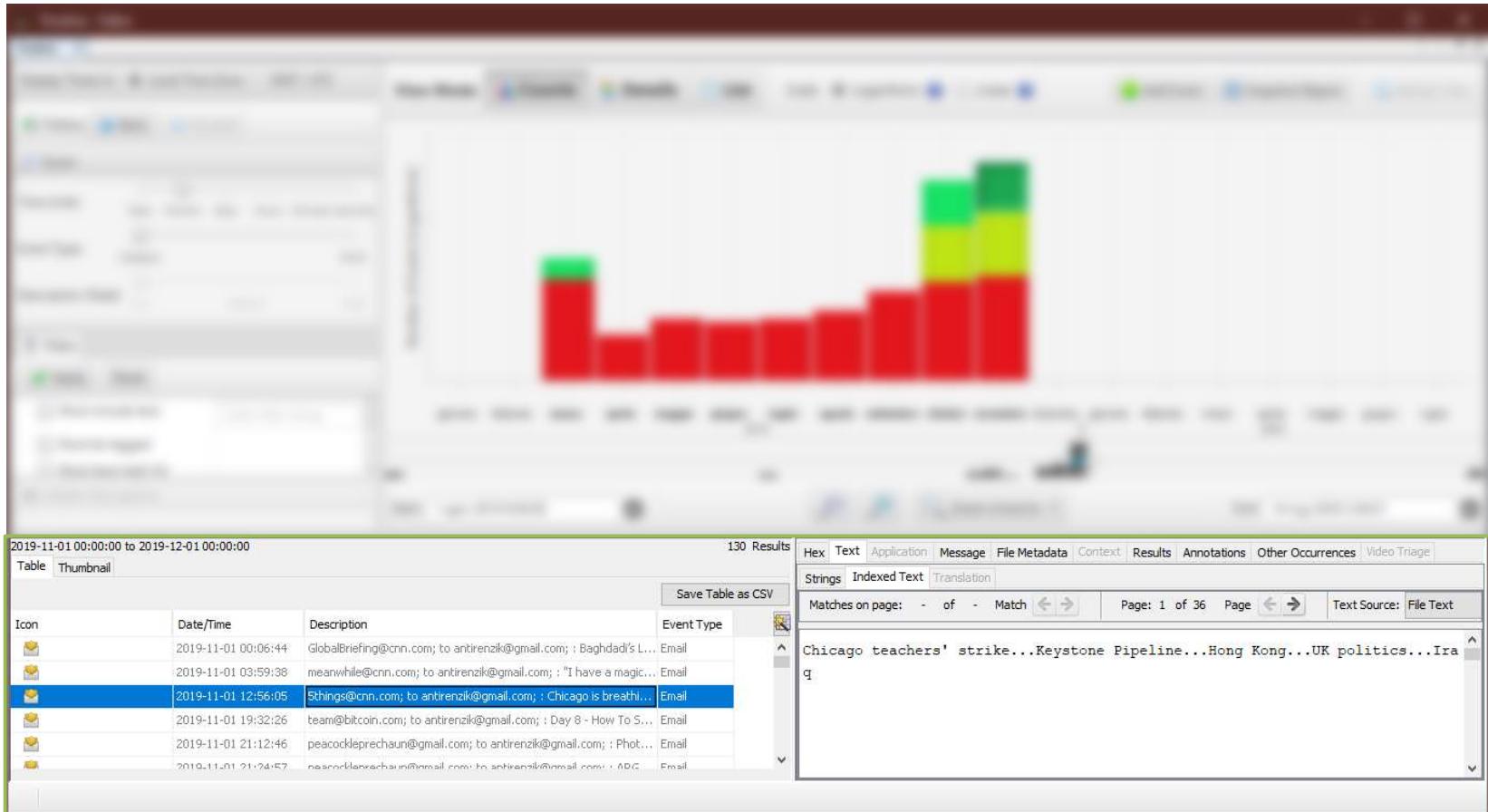
# Autopsy

## *TimeLine Graphic Interface*



# Autopsy

## *TimeLine Graphic Interface*



# Autopsy

## *Image Gallery*

- ▶ Consente di visualizzare velocemente un insieme di immagini e video:
  - materiale pedopornografico
  - materiale Revenge Porn
  - documenti scansionati
- ▶ Viene visualizzato il contenuto di una cartella alla volta:
  - Priorità:
    - Numero di risultati positivi sull'hash
    - Numero di immagini\video

# Autopsy Image Gallery

The screenshot shows the Autopsy 4.14.0 interface with the 'Images/Videos' tab selected. A red arrow points from the 'Images/Videos' tab in the main menu bar to the 'Image/Video Gallery - Editor' window.

**Main Menu Bar:** Case01 - Autopsy 4.14.0, Case, View, Tools, Window, Help.

**Toolbar:** Add Data Source, Images/Videos (highlighted with a red box), Communications, Timeline, Keyword Lists, Keyword Search.

**Left Sidebar:** Data Sources, Views, File Types, Deleted Files, MB File Size, Results (highlighted with a blue box), Tags, Reports.

**Image/Video Gallery - Editor Window:**

- Left Panel:** Shows file structures and categories:
  - All Groups
  - img\_device2\_mediocard.e01
  - vol.vol2
  - DCIM
    - Camera (5)
  - img\_device1\_laptop.e01
  - vol.vol7
  - vol.vol4
- Center Panel:** Displays five image thumbnails from the 'Camera' folder. One thumbnail is highlighted with a blue border.
- Right Panel:** Details view for the selected file 'IMG\_20191023\_142721.jpg'.

Attribute	Value
Name	IMG_20191023_142721.jpg
Analyzed	true
Category	CAT-0: Uncategorized
Tags	
Path	/img_device2_mediocard.e01/vol.vol2/DCIM/Camera/
Created Time	2019-10-23 13:27:22 CEST
Modified Time	2019-10-23 13:27:22 CEST
MD5 Hash	2e119a3a56cf810206eba2f8c56a4c0a

# Autopsy

## *Image Gallery*

The screenshot shows the Autopsy Image/Video Gallery - Editor window. On the left, a red box highlights the **Folder Tree** containing a list of groups and their contents. Below it is a table showing the number of files per category. In the center, a green box highlights the **Group view**, which displays a grid of image thumbnails. One thumbnail is selected and highlighted with a blue border. On the right, an orange box highlights the **Details** panel, which provides a detailed table of file attributes for the selected image.

**Folder Tree**

**Category**

Category	# Files
CAT-1: Child Exploitation...	0
CAT-2: Child Exploitation...	0
CAT-3: CGI/Animation (C...	0
CAT-4: Exemplar/Compa...	0
CAT-5: Non-pertinent	0
CAT-0: Uncategorized	9961

**Group view**

**Details**

Attribute	Value
Name	IMG_20191023_142721.jpg
Analyzed	true
Category	CAT-0: Uncategorized
Tags	
Path	/img_device2_mediocard.e01/vol_vol2/DCIM/Camera/
Created Time	2019-10-23 13:27:22 CEST
Modified Time	2019-10-23 13:27:22 CEST
MD5 Hash	2e119a3a56cf810206eba2f8c56a4c0a

Category

Group view

Details

# Autopsy

## *Image Gallery*

### Bordi



Immagine categorizzata/etichettata

1	CAT-1: Child Exploitation (Illegal)	1
2	CAT-2: Child Exploitation (Non-Illegal/Age Difficult)	2
3	CAT-3: CGI/Animation (Child Exploitive)	3
4	CAT-4: Exemplar/Comparison (Internal Use Only)	4
5	CAT-5: Non-pertinent	5
0	CAT-0: Uncategorized	0



Immagine positiva all'hash

# Autopsy

## *Communication interface*

- ▶ Visualizza i dati delle comunicazioni in modo differente:
  - E-Mail Parser
  - Android Analyzer
- ▶ È orientato intorno agli account:
  - vengono visualizzate tutte le attività associate
  - vengono visualizzate le relazioni con gli altri account:

# Autopsy

## Communication interface

The screenshot shows the Autopsy 4.14.0 interface with a red box highlighting the 'Communications' tab in the top navigation bar. A red arrow points from the 'Communications' tab to the 'Communications Visualization - Editor' window.

**Communications Visualization - Editor**

**Browse Visualize**

Account	Device	Type	It...
antirenzik@gmail.com	device1_laptop.e01	Email	138
team@bitcoin.com	device1_laptop.e01	Email	17
Sthings@cnn.com	device1_laptop.e01	Email	13
peacockleprechaun@gmail.com	device1_laptop.e01	Email	13
globalbriefing@cnn.com	device1_laptop.e01	Email	13
lilizza@cnn.com	device1_laptop.e01	Email	13
brian.stelter@cnn.com	device1_laptop.e01	Email	12
meanwhile@cnn.com	device1_laptop.e01	Email	11
messages-noreply@linkedin.com	device1_laptop.e01	Email	7
info@twitter.com	device1_laptop.e01	Email	7
thegoodstuff@cnn.com	device1_laptop.e01	Email	4
resultsarein@cnn.com	device1_laptop.e01	Email	4
strandmag@strandmag.com	device1_laptop.e01	Email	4
info@basistech.com	device1_laptop.e01	Email	3
i5Heu+45c1yem5fewrlj8d2o@guerrillamail.cc	device1_laptop.e01	Email	2
purinapetcare@news.purina.com	device1_laptop.e01	Email	2
k9kennelstore@gmail.com	device1_laptop.e01	Email	2
14y825+4t9e7vvbxxy0k@guerrillamail.com	device1_laptop.e01	Email	2
brian.stelter@turner.com	device1_laptop.e01	Email	1
mailer-daemon@mailstream-east.mxrecord.io	device1_laptop.e01	Email	1
briancarrier@basistech.com	device1_laptop.e01	Email	1
security-noreply@linkedin.com	device1_laptop.e01	Email	1
googlecommunityteam-noreply@google.com	device1_laptop.e01	Email	1
house@househou.se	device1_laptop.e01	Email	1
no-reply@accounts.google.com	device1_laptop.e01	Email	1

**Contacts**  
antirenzik@gmail.com  
This account was referenced by a device in the case.

**Communications**  
Messages: 138  
Call Logs: 0  
Media Attachments: 13  
Total Attachments: 16

**Account Contacts**  
Book Entries: 0  
Communication References: 0

**File References in Current Case**  
Path: /img\_device1\_laptop.e01/vol\_vol7/\$Recycle.Bin/

**Other Occurrences**  
Case Name Creation Date

# Autopsy

## Communication interface

Communications Visualization - Editor

Communications Visualization

Filters  Apply  Refresh

Account Types:

Device  Email

Uncheck All Check All

Devices:

device1\_laptop.e01  device2\_mediocard.e01

Uncheck All Check All

Date Range (Europe/Berlin): < >

Browse Visualize

Account	Device	Type	It...
antrenzik@gmail.com	device1_la...	Email	138
team@bitcoin.com	device1_la...	Email	17
5things@cnn.com	device1_la...	Email	13
peacockleprechaun@gmail.com	device1_la...	Email	13
globalbriefing@cnn.com	device1_la...	Email	13
cilizza@cnn.com	device1_la...	Email	13
brian.stelter@cnn.com	device1_la...	Email	12
meanwhile@cnn.com	device1_la...	Email	11
messages-noreply@linkedin.com	device1_la...	Email	7
info@twitter.com	device1_la...	Email	7
thegoodstuff@cnn.com	device1_la...	Email	4
resultsarein@cnn.com	device1_la...	Email	4
strandmag@strandmag.com	device1_la...	Email	4
info@basistech.com	device1_la...	Email	3
i5t4eu+45c1yem5fewrlj8d2o@guerrillamail.cc	device1_la...	Email	2
purinapetcare@news.purina.com	device1_la...	Email	2
k9kennelsstore@gmail.com	device1_la...	Email	2
i4y825+4t9e7vbxy0k@guerrillamail.com	device1_la...	Email	2
brian.stelter@turner.com	device1_la...	Email	1
mailer-daemon@mailstream-east.mxrecord.io	device1_la...	Email	1
briancarrier@basistech.com	device1_la...	Email	1
security-noreply@linkedin.com	device1_la...	Email	1
googlecommunityteam-noreply@google.com	device1_la...	Email	1
house@househou.se	device1_la...	Email	1
no-reply@accounts.google.com	device1_la...	Email	1

Contacts Summary Media Attachments

Messages Call Logs

antrenzik@gmail.com

This account was referenced by a device in the case.

Communications

Messages: 138  
Call Logs: 0  
Media Attachments: 13  
Total Attachments: 16

Account Contacts

Book Entries: 0  
Communication References: 0

File References in Current Case

Path: /img\_device1\_laptop.e01/vol\_vol7/\$Recycle.Bin/

Other Occurrences

Case Name	Creation Date
-----------	---------------

# Autopsy

## Communication interface

Communications Visualization - Editor

Communications Visualization

Filters  Apply Refresh

Account Types:  Device  Email

Uncheck All Check All

Devices:  device1\_laptop.e01  device2\_mediocard.e01

Uncheck All Check All

Date Range (Europe/Berlin): < >

Browse Visualize

Account

Account	Device	Type	Items
antirenzik@gmail.com		Email	13
team@bitcoin.com	device1_laptop.e01	Email	13
5things@cnn.com	device1_laptop.e01	Email	12
peacockleprechaun@gmail.com	device1_laptop.e01	Email	11
globalbriefing@cnn.com	device1_laptop.e01	Email	7
cilizza@cnn.com	device1_laptop.e01	Email	4
brian.stelter@cnn.com	device1_laptop.e01	Email	4
meanwhile@cnn.com	device1_laptop.e01	Email	4
messages-noreply@linkedin.com	device1_laptop.e01	Email	3
info@twitter.com	device1_laptop.e01	Email	2
thegoodstuff@cnn.com	device1_laptop.e01	Email	2
resultsarein@cnn.com	device1_laptop.e01	Email	1
strandmag@strandmag.com	device1_laptop.e01	Email	1
info@basistech.com	device1_laptop.e01	Email	1
i5t4eu+45c1yem5fewrlj8d20@guerrilla	device1_laptop.e01	Email	1
purinapetcare@news.purina.com	device1_laptop.e01	Email	1
k9kennelsstore@gmail.com	device1_laptop.e01	Email	1
i4y825++4t9e7vtxxylk@guerrillama	device1_laptop.e01	Email	1
brian.stelter@turner.com	device1_laptop.e01	Email	1
mailer-daemon@mailstream-east.mx	device1_laptop.e01	Email	1
briancarrier@basistech.com	device1_laptop.e01	Email	1
security-noreply@linkedin.com	device1_laptop.e01	Email	1
googlecommunityteam-noreply@google.com	device1_laptop.e01	Email	1
house@househou.se	device1_laptop.e01	Email	1
no-reply@accounts.google.com	device1_laptop.e01	Email	1

Add Selected Account to Visualization  
Visualize Only Selected Account

Contacts Summary Media Attachments  
Messages Call Logs

antirenzik@gmail.com

This account was referenced by a device in the case.

Communications

Messages:	138
Call Logs:	0
Media Attachments:	13
Total Attachments:	16

Account Contacts

Book Entries:	0
Communication References:	0

File References in Current Case

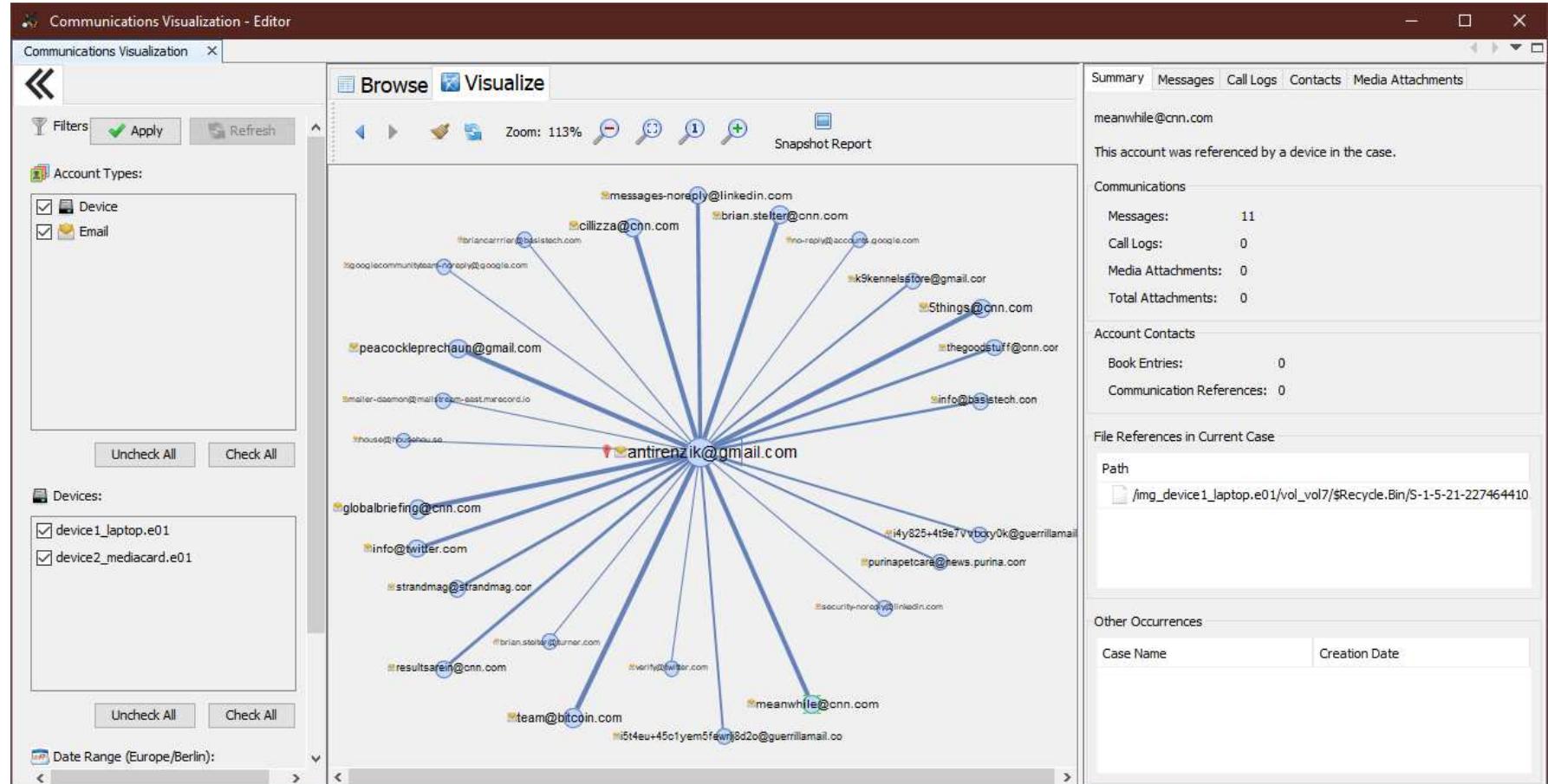
Path: /img\_device1\_laptop.e01/vol\_vol7/\$Recycle.Bin/

Other Occurrences

Case Name	Creation Date
-----------	---------------

# Autopsy

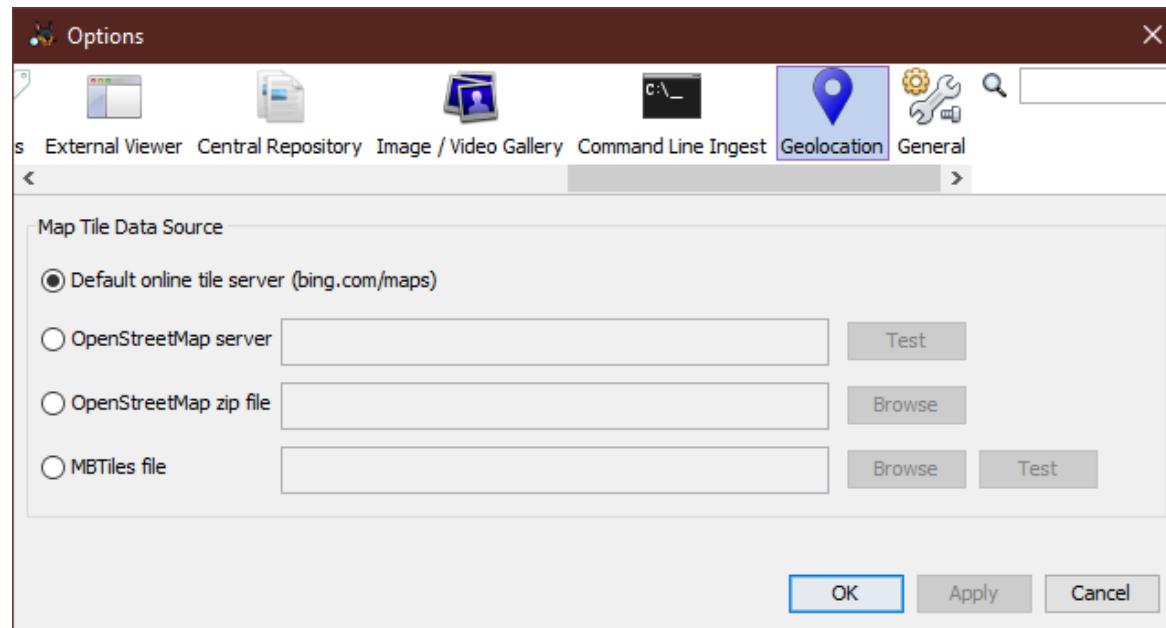
## Communication interface



# Autopsy

## *Geolocation*

- ▶ Riepiloga tutti gli artefatti in cui sono state estratte le informazioni sulle posizioni:
  - Exif Parser



# Autopsy Geolocation

Case01 - Autopsy 4.14.0

Case View Tools Window Help

Add D

Images/Videos

Communications

**Geolocation**

Timeline

File Discovery

File Search by Attributes

Search All Cases

Find Common Properties

Run Ingest Modules >

Generate Report

Plugins

Python Plugins

Options

Make Live Triage Drive

Open Case Folder

Create Logical Imager

Geolocation - Editor

Waypoints

Show All

Show only last 10 days of activity

Include waypoints with no time stamps

Data Sources

device1\_laptop.e01

device2\_mediocard.e01

Apply

Filters

Uncheck All Check All

[85.04176086898546, -179.9344253540039]

KML Report

# Autopsy

» Tag & Report



# Autopsy

## *Tagging*

- ▶ Creare un riferimento ad un file\item di interesse:
  - Consente di commentarlo
  - Consente di etichettare solo una parte di una immagine
- ▶ Sono associati all'esaminatore:
  - Conoscere chi li ha etichettati
  - Possono essere nascoste le etichette degli altri esinatori
- ▶ Obiettivo:
  - Ritrovare facilmente il/i file di interesse
  - Evidenziarlo/i ed esportarlo/i nel Report

# Autopsy Tagging

The screenshot shows the Autopsy 4.14.0 interface. On the left, the案卷树 (Case Tree) displays devices and their contents. The main area shows a listing of source files, including EXIF metadata. A context menu is open over a file, with the 'Add File Tag' and 'Add Result Tag' options highlighted with a red box. To the right, a 'Create Tag' dialog is open, showing pre-existing tag names like 'Bookmark' and 'CAT-0: Uncategorized'. A new tag named 'Check' is being created. A green box highlights the 'New Tag' section, and a green arrow points from the 'New Tag' input field to the 'OK' button. A red box highlights the 'Ctrl+B' keyboard shortcut for adding a tag.

Case01 - Autopsy 4.14.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline File Discovery Close Case Generate Report Keyword Lists Keyword Search

device1\_laptop.e01 device2\_mediocard.e01

Data Source Files device2\_mediocard.e01

Views File Types Deleted Files MB File Size

Results Extracted Content EXIF Metadata (5) User Content Suspected (5)

Keyword Hits Single Literal Keyword Search (0) Single Regular Expression Search (0)

Hashset Hits E-Mail Messages

Interesting Items Previously Tagged As Notable (Central Repository) Interesting Files (1) Interesting Results (0)

Accounts Tags Reports

Properties

View Result in Timeline... View Source File in Timeline... View Source File in Directory View in New Window Open in External Viewer Ctrl+E Extract File(s) Export selected rows to CSV

Add File Tag Add Result Tag Remove File Tag Remove Result Tag Add/Edit Central Repository Comment Add File to Hash Set

Bookmark CAT-0: Uncategorized CAT-1: Child Exploitation (Illegal) CAT-2: Child Exploitation (Non-Illegal/Age Difficult) CAT-3: CGI/Animation (Child Exploitive) CAT-4: Exemplar/Comparison (Internal Use Only) CAT-5: Non-pertinent Follow Up Notable Item

New Tag

Tag Name: Check Description:   Tag indicates item is notable.

OK Cancel

Ctrl+B

# Autopsy Tagging

The screenshot shows the Autopsy 4.14.0 interface. The left sidebar contains a tree view of case files and analysis results. The main area displays a table of EXIF metadata for several images. One specific file, 'IMG\_20191023\_142956.jpg', is selected and highlighted with a red border. The right panel provides details about the selected source file, including its tags.

**EXIF Metadata Listing:**

Source File	S	C	O	Date Created	Latitude	Longitude	Altitude	Device
IMG_20191023_092858.jpg	2			2019-10-23 09:28:58 CEST	39.17767333333333	-76.66690825	15.0	BLU R1 HD
IMG_20191023_142721.jpg	2			2019-10-23 14:27:21 CEST				BLU R1 HD
IMG_20191023_142956.jpg	1			2019-10-23 13:29:56 CEST	29.986032472222224	-90.25782011111112	4.294967275E9	BLU R1 HD
IMG_20191023_170347.jpg	2			2019-10-23 17:03:47 CEST	29.95034408333334	-90.06626891666666	10.0	BLU R1 HD
IMG_20191024_155744.jpg	2			2019-10-24 15:57:45 CEST	29.94645688888889	-90.06748961111111	4.294967274E9	BLU R1 HD

**Selected Item:**  
There are no tags for the selected artifact.

**Source File:**

Tag: Check  
Tag User: seaman85  
Comment:

# Autopsy Tagging

Case01 - Autopsy 4.14.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline File Discovery Close Case Generate Report Keyword Lists Keyword Search

device1\_laptop.e01  
device2\_mediocard.e01  
Data Source Files  
Views  
File Types  
Deleted Files  
MB File Size  
Results  
Extracted Content  
EXIF Metadata (5)  
User Content Suspected (5)  
Keyword Hits  
Single Literal Keyword Search (0)  
Single Regular Expression Search (0)  
Hashset Hits  
E-Mail Messages  
Interesting Items  
Previously Tagged As Notable (Central R)  
Accounts  
Tags  
Check (1)  
File Tags (1)  
Result Tags (0)  
Reports

Listing  
EXIF Metadata  
Table Thumbnail  
Save Table as CSV

Source File S C O Date Created Latitude Longitude Altitude Device Model  
IMG\_20191023\_092858.jpg 2 2019-10-23 09:28:58 CEST 39.17767333333333 -76.66690825 15.0 BLU R1 HD  
IMG\_20191023\_142721.jpg 2 2019-10-23 14:27:21 CEST 39.17767333333333 -76.66690825 15.0 BLU R1 HD  
IMG\_20191023\_142956.jpg 1 2019-10-23 13:29:56 CEST 29.986032472222224 -90.25780211111112 4.294967275E9 BLU R1 HD  
IMG\_20191023\_170347.jpg 2 2019-10-23 17:03:47 CEST 29.950344083333334 -90.06626891666666 10.0 BLU R1 HD  
IMG\_20191024\_155744.jpg 2 2019-10-24 15:57:45 CEST 29.946456888888889 -90.06748961111111 4.294967274E9 BLU R1 HD

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Video Triage  
0° C C | 13% | Reset

Tags Menu  
Create  
Delete  
Hide  
Export

Source File	S	C	O	Date Created	Latitude	Longitude	Altitude	Device Model
IMG_20191023_092858.jpg	2			2019-10-23 09:28:58 CEST	39.17767333333333	-76.66690825	15.0	BLU R1 HD
IMG_20191023_142721.jpg	2			2019-10-23 14:27:21 CEST	39.17767333333333	-76.66690825	15.0	BLU R1 HD
IMG_20191023_142956.jpg	1			2019-10-23 13:29:56 CEST	29.986032472222224	-90.25780211111112	4.294967275E9	BLU R1 HD
IMG_20191023_170347.jpg	2			2019-10-23 17:03:47 CEST	29.950344083333334	-90.06626891666666	10.0	BLU R1 HD
IMG_20191024_155744.jpg	2			2019-10-24 15:57:45 CEST	29.946456888888889	-90.06748961111111	4.294967274E9	BLU R1 HD

# Autopsy Tagging

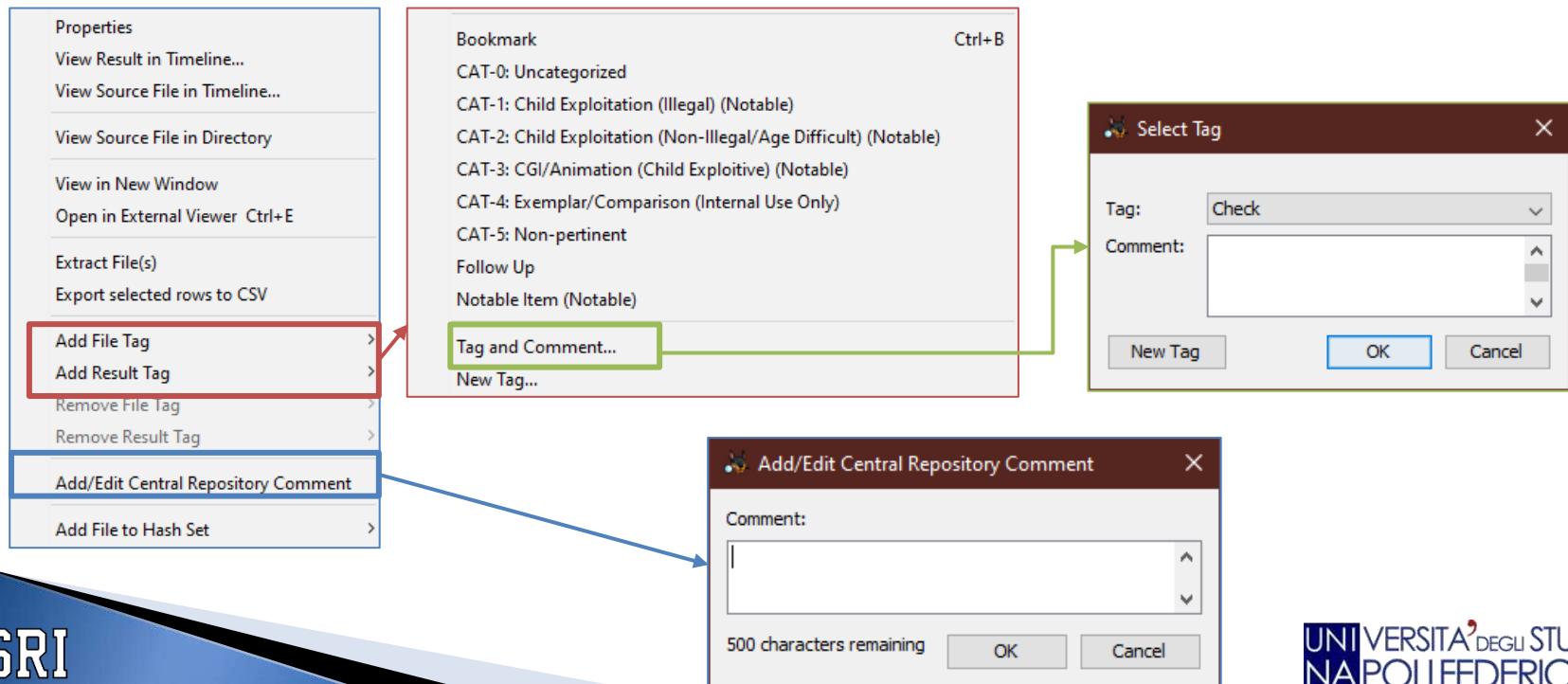
The screenshot shows the Autopsy 4.14.0 interface with the title "Case01 - Autopsy 4.14.0". The main window displays a table of source files, including EXIF metadata for several photographs. A specific image, "IMG\_20191023\_142956.jpg", is selected and highlighted with a red box. A modal dialog titled "Select Tag" is open over the image, showing the "Check" tag selected with a comment "USA Flag". The left sidebar shows the case structure with various data sources and analysis results.

Source File	S	C	O	Date Created	Latitude	Longitude	Altitude	Device Model
IMG_20191023_092858.jpg		▼	2	2019-10-23 09:28:58 CEST	39.17767333333333	-76.66690825	15.0	BLU R1 HD
IMG_20191023_142721.jpg			2	2019-10-23 14:27:21 CEST				BLU R1 HD
IMG_20191023_142956.jpg		▼	1	2019-10-23 13:29:56 CEST	29.98603247222224	-90.25782011111112	4.294967275E9	BLU R1 HD
IMG_20191023_170347.jpg			2	2019-10-23 17:03:47 CEST	29.950344083333334	-90.06626891666666	10.0	BLU R1 HD
IMG_20191024_155744.jpg			2	2019-10-24 15:57:45 CEST	29.94645688888889	-90.06748961111111	4.294967274E9	BLU R1 HD

# Autopsy

## Comments

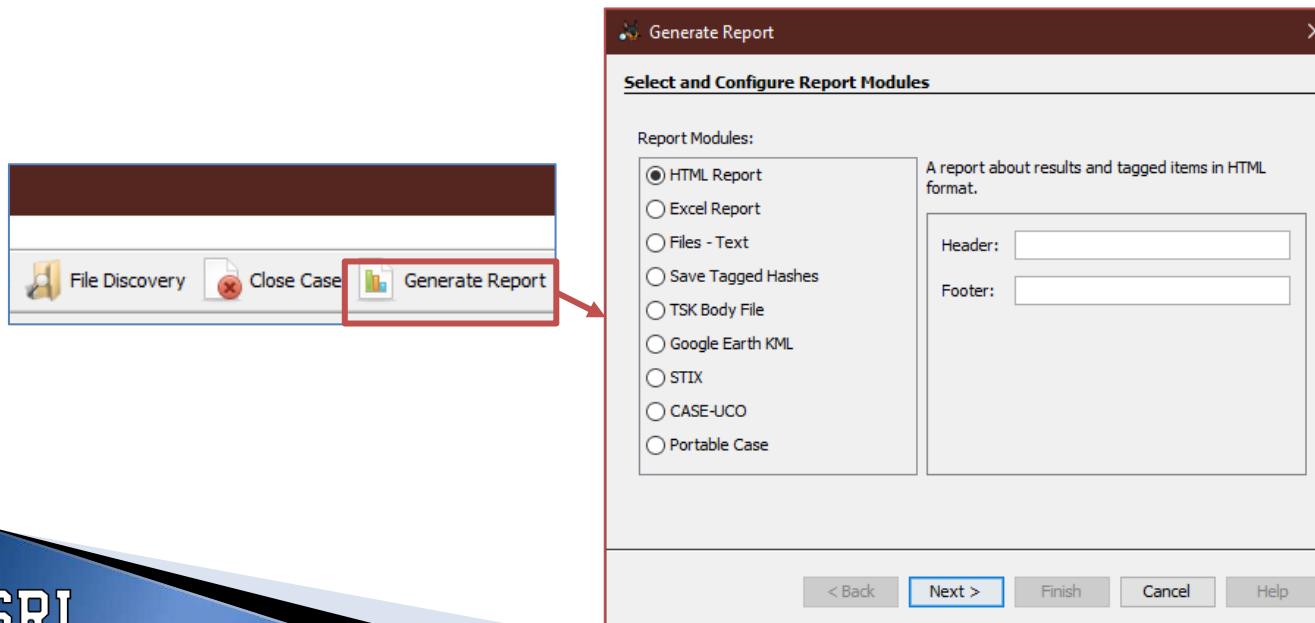
- ▶ Consente di annotare il motivo dell'interesse di un file\item:
  - Verrà visualizzato nel Report
  - Può essere salvato nel «Central Repository»



# Autopsy

## Reporting

- ▶ Generare un report per:
  - Esportare e condividere i risultati dell'analisi
  - Unirlo ad altri report
- ▶ Salvato nella sezione «Reports»:
  - Può essere elaborato da ulteriori «ingest module»



# Autopsy

## Reporting

### HTML Report

The image shows two windows from the Autopsy software:

- Generate Report** window:
  - Configure Report** section: "Select which data to report on".
    - All Results
    - All Tagged Results
    - Specific Tagged Results
  - Result Types** button (highlighted with a red box and arrow)
  - Buttons at the bottom: < Back, Next >, Finish (highlighted with a blue border), Cancel, Help

A red arrow points from the "Result Types" button in the first window to the "Result Type Selection" dialog.

- Result Type Selection** dialog:
  - "Select which result types you would like to report on:"
  - Checklist of result types, all checked:
    - Accounts
    - Data Source Usage
    - E-Mail Messages
    - EXIF Metadata
    - Encryption Detected
    - Encryption Suspected
    - Extension Mismatch Detected
    - Hashset Hits
    - Interesting Files
    - Keyword Hits
    - Operating System Information
  - Buttons: Select All, Deselect All, OK

# Autopsy

## Reporting

### HTML Report

The screenshot shows a web browser displaying the 'Autopsy Forensic Report for case' page. The URL in the address bar is file:///C:/Autopsy/Case01/Reports/Case01 HTML Report 05. The page has a dark header bar with the title and a search bar labeled 'Cerca'. Below the header is a 'Report Navigation' sidebar on the left containing a list of forensic findings with icons and counts: Case Summary (1), Accounts (2), Accounts: Email (26), Data Source Usage (1), E-Mail Messages (138), EXIF Metadata (30), Encryption Detected (6), Encryption Suspected (4), Extension Mismatch Detected (113), HashSet Hits (6), Interesting Files (6), Keyword Hits (218), Operating System Information (2), Recent Documents (24), and Recycle Bin (3). The main content area is titled 'Autopsy Forensic Report' and includes a timestamp 'HTML Report Generated on 2020/05/14 21:35:38'. It lists case details: Case: Case01, Case Number: 0705-2020, Number of Images: 2, and Examiner: Marco. Below this is a section titled 'Image Information:' with entries for 'device1\_laptop.e01' (Timezone: Europe/Berlin, Path: C:\image\device1\_laptop.e01) and 'device2\_mediocard.e01' (Timezone: Europe/Berlin, Path: C:\image\device2\_mediocard.e01). A final section titled 'Software Information:' is present.

Report Navigation

- Case Summary
- Accounts (2)
- Accounts: Email (26)
- Data Source Usage (1)
- E-Mail Messages (138)
- EXIF Metadata (30)
- Encryption Detected (6)
- Encryption Suspected (4)
- Extension Mismatch Detected (113)
- HashSet Hits (6)
- Interesting Files (6)
- Keyword Hits (218)
- Operating System Information (2)
- Recent Documents (24)
- Recycle Bin (3)

Autopsy Forensic Report

HTML Report Generated on 2020/05/14 21:35:38

Case: Case01  
Case Number: 0705-2020  
Number of Images: 2  
Examiner: Marco

Image Information:

device1\_laptop.e01

Timezone: Europe/Berlin  
Path: C:\image\device1\_laptop.e01

device2\_mediocard.e01

Timezone: Europe/Berlin  
Path: C:\image\device2\_mediocard.e01

Software Information:

# Autopsy

## *Reporting*

### Portable Case

- ▶ Versione più piccola del Caso originale:
  - Solo i file etichettati (*tagged file*)
  - Solo i file presenti nella categoria «Interesting Item»
- ▶ Ha un proprio DataBase SQLite
- ▶ I file sono esportati nel CaseFolder

# Autopsy

## Reporting

### Portable Case

The image shows two screenshots of the Autopsy Generate Report interface. A red arrow points from the first screenshot to the second, indicating a progression from module selection to configuration.

**Screenshot 1: Select and Configure Report Modules**

Report Modules:

- HTML Report
- Excel Report
- Files - Text
- Save Tagged Hashes
- TSK Body File
- Google Earth KML
- STIX
- CASE-UCO
- Portable Case

Copies selected items to a new single-user case that can be easily shared

*This report will be configured on the next screen.*

**Screenshot 2: Choose Portable Case settings**

Include the following tags:

All Tagged Results

Notable Item (1)

Check (2)

Select All Deselect All

Include Interesting Items from these sets:

All Interesting Items

Encryption (1)

Previously Tagged As Notable (Central Repository) (5)

Select All Deselect All

< Back Next > Finish Cancel Help

# Autopsy

» Extensible



# Autopsy

## *Extensible*

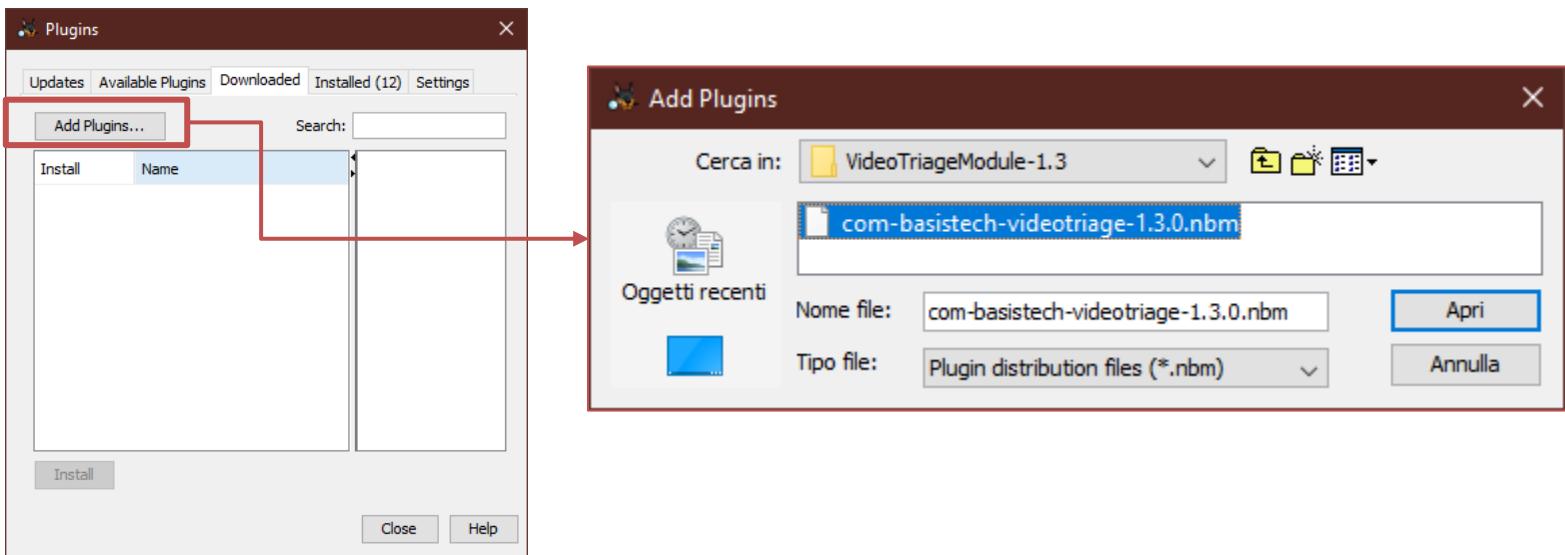
- ▶ Autopsy è costituito da moduli «plug-in»:
  - DataSource Processor
  - Ingest Module
  - Content viewer
  - Machine Translation
  - Report Module
  - Etc...
- ▶ Gli utenti possono creare e pubblicare dei propri plug-in:
  - GitHub Repo: [https://github.com/sleuthkit/autopsy\\_addon\\_modules](https://github.com/sleuthkit/autopsy_addon_modules)
- ▶ Linguaggio:
  - Java
  - Python

# Autopsy

## *Extensible*

### Java Module

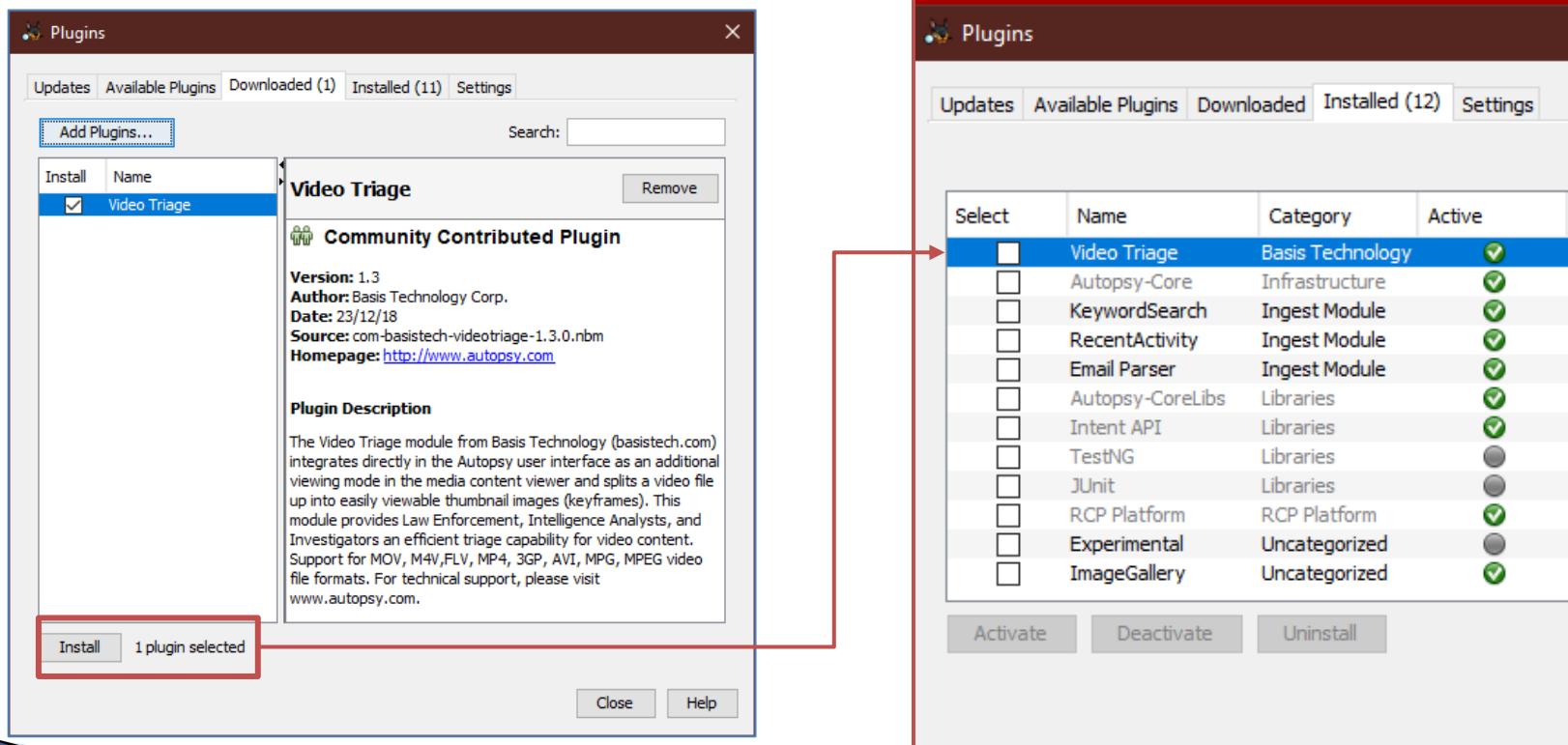
- ▶ Sono file con estensione «.nbt»:
  - Possono contenere più moduli
  - NetBeans consente di auto-aggiornarli e scaricarli
- ▶ Tools->Plugins



# Autopsy

## *Extensible*

### Java Module

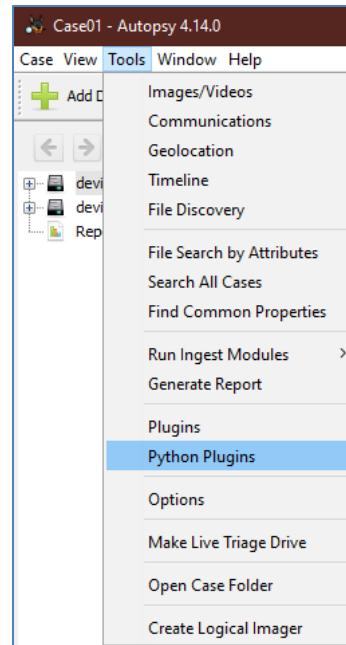


# Autopsy

## *Extensible*

### Python Module

- ▶ Sono cartelle che contengono file con estensione «.py»:
  - Copia manuale delle cartelle in una specifica directory:
    - [%USER\_PATH%]\AppData\Roaming\autopsy\python\_modules
  - Possono essere solo «Ingest Module» e «Report Module»





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 17: L'Analisi *i File System*

(1<sup>a</sup> parte)



A.A. 2021/22

Dott. Lorenzo LAURATO



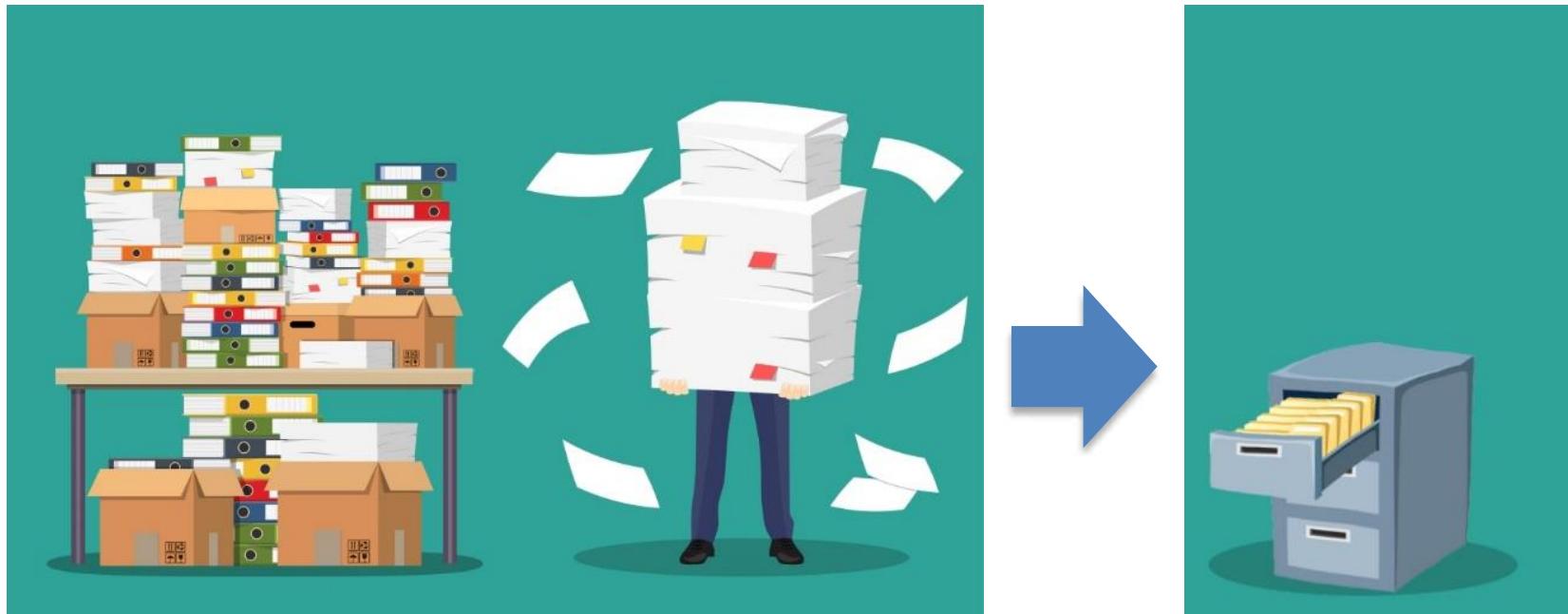
# File System

» Overview

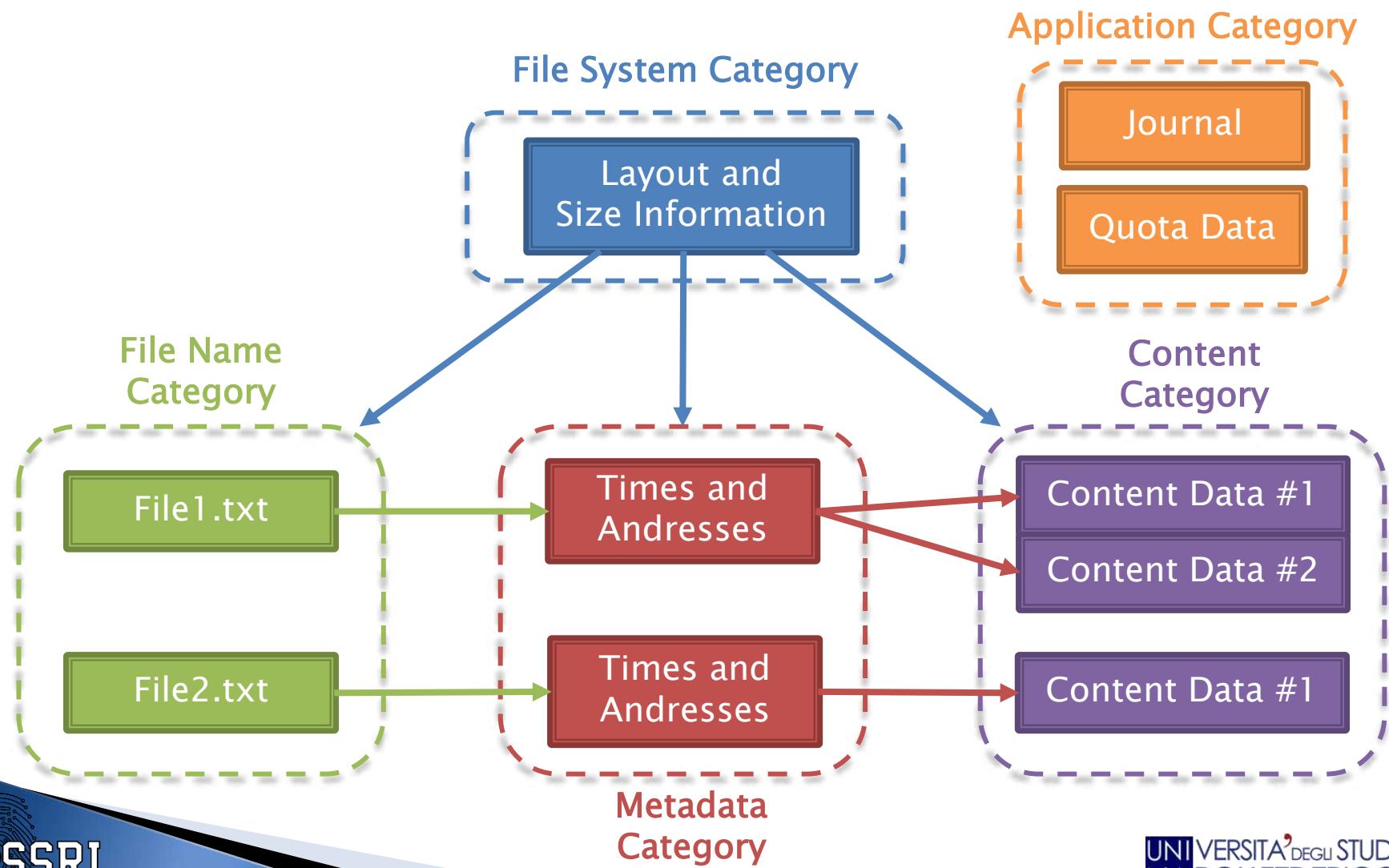


# File System

- ▶ Sistema che permette la memorizzazione dei dati, organizzandoli gerarchicamente in file e directory, in modo tale da ritrovarli velocemente.



# File System



# File System

## Dati Essenziali

- ▶ Dati che se modificati/alterati causano il malfunzionamento del sistema:
  - Indirizzamento del contenuto del file
  - Nome del File
  - Dimensione del file

TRUSTED DATA

## Dati Non Essenziali

- ▶ Informazioni accessorie
  - Dati temporali
  - Permessi utente

UNTRUSTED DATA

# File System:

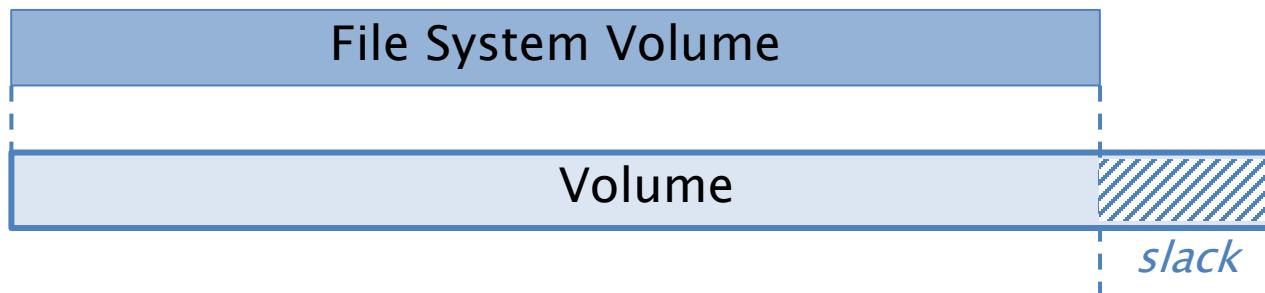
## *File System Category*

### ▶ Informazioni generali sul File System:

- Solitamente posizionati nel primo settore
- Essenziali: informazioni sul layout dei dati

### ▶ Analisi:

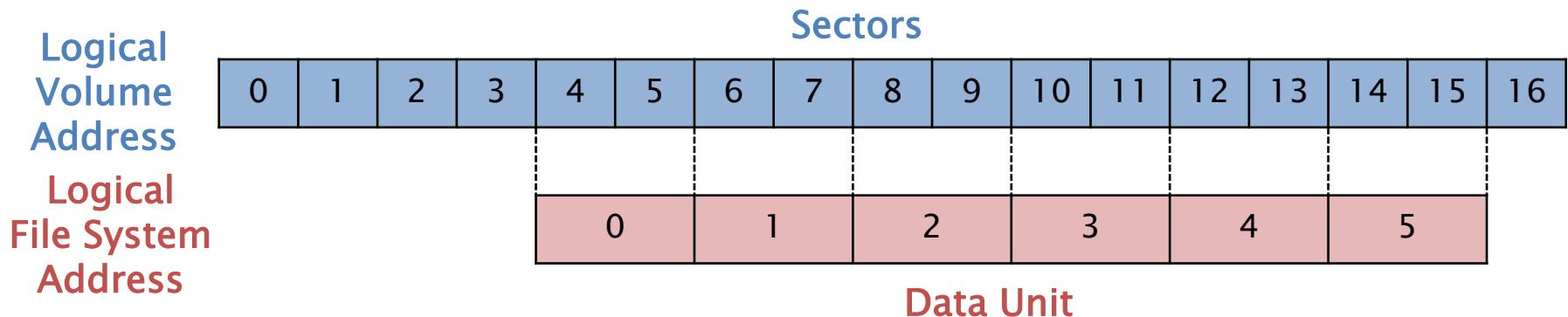
- Informazioni sulla generazione del File System
- Informazioni sul layout
- Controllo di consistenza: *volume slack*



# File System:

## *Content Category*

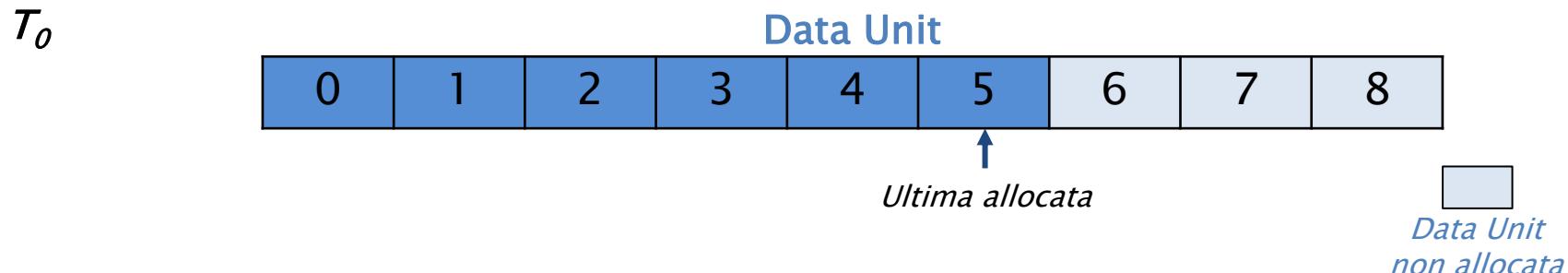
- ▶ Locazioni di memoria impiegate per la memorizzazioni del contenuto dei file:
  - **Data Unit:** *raggruppamento di più settori*
    - STATO: allocato e non allocato
    - Logical File System address



# File System: *Content Category* *strategie di allocazione*

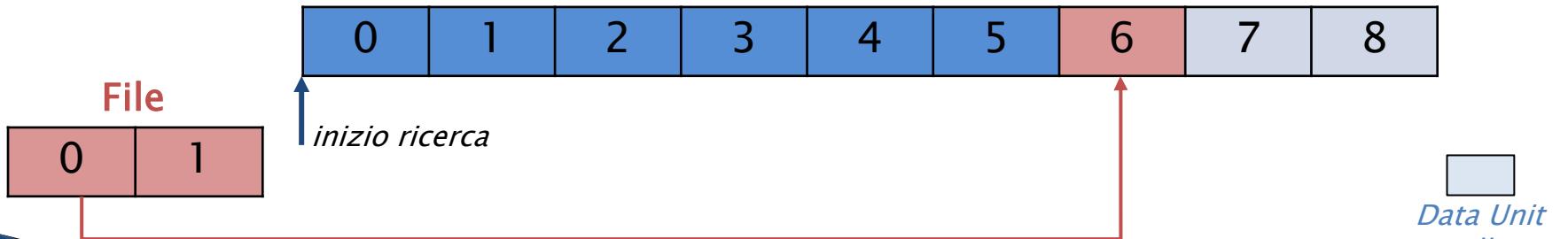
## ▶ Strategia del primo disponibile:

- Si cerca una «data unit» libera ogni volta partendo dall'inizio del file system.



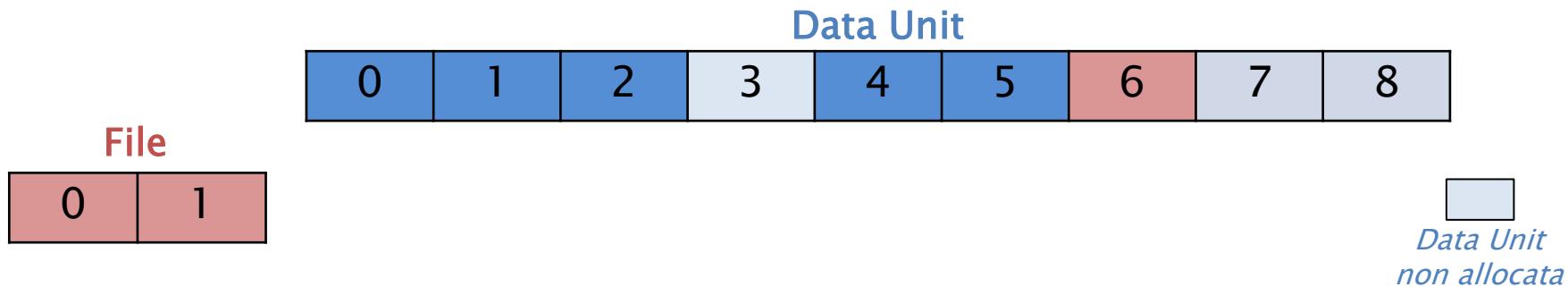
$T_1$

Data Unit

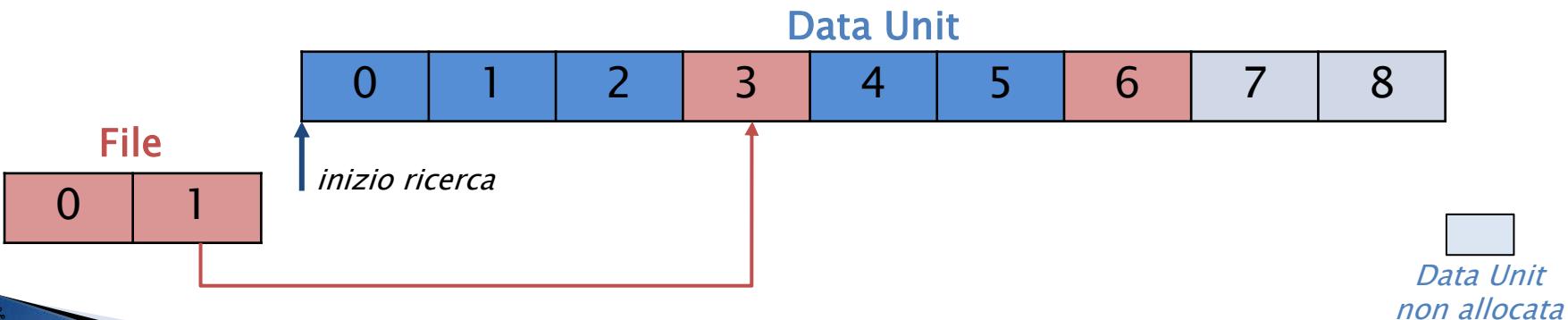


# File System: *Content Category* *strategie di allocazione*

$T_2$



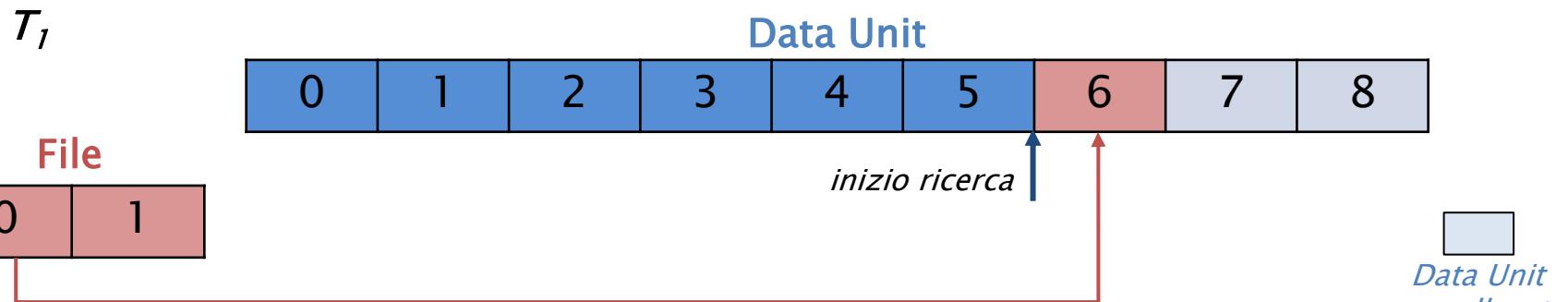
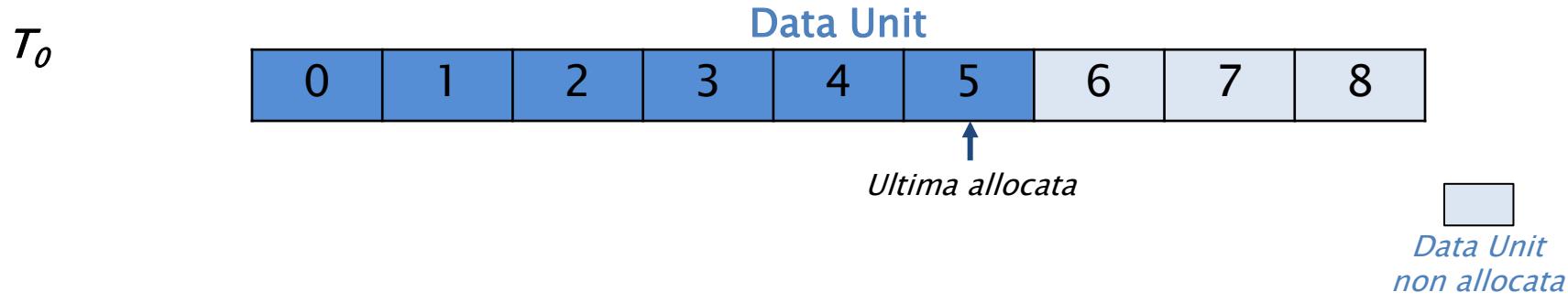
$T_3$



# File System: *Content Category* *strategie di allocazione*

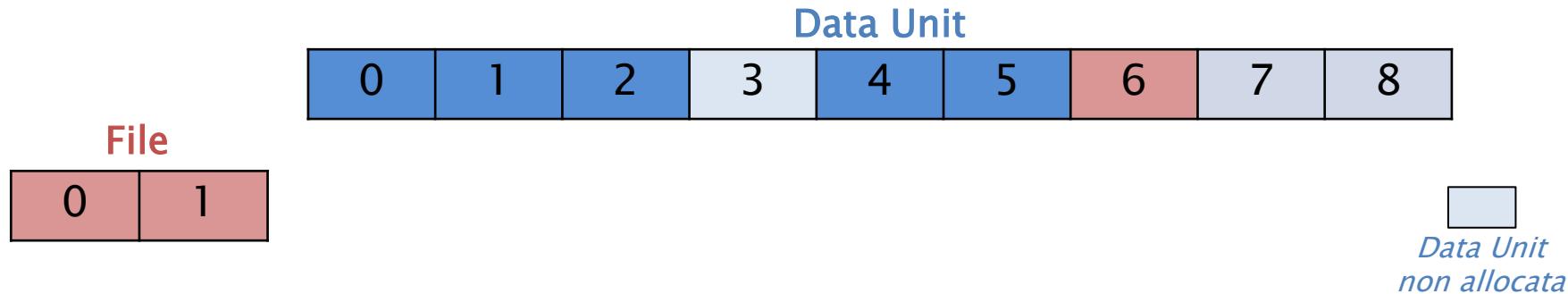
## ▶ Strategia del prossimo disponibile:

- Si cerca una «data unit» libera partendo dall'ultima locazione allocata

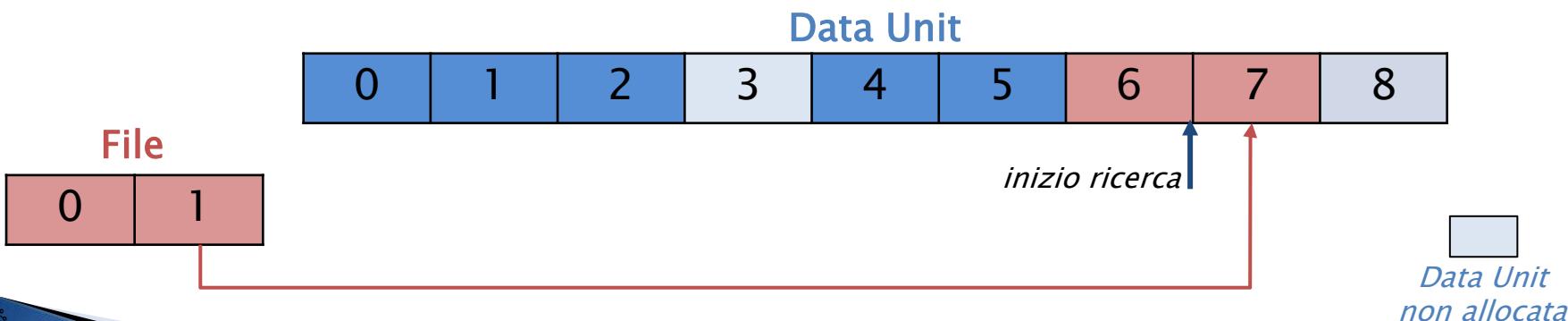


# File System: *Content Category* *strategie di allocazione*

$T_2$



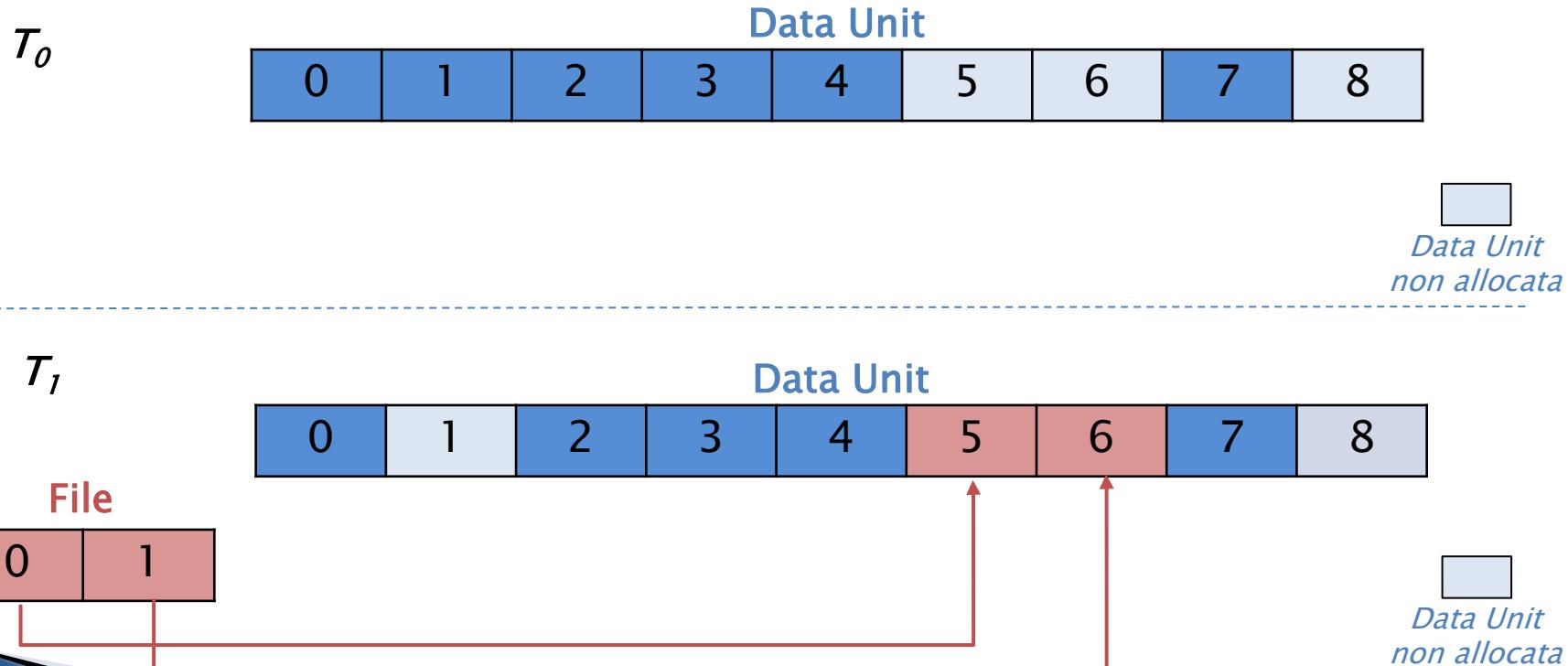
$T_3$



# File System: *Content Category* *strategie di allocazione*

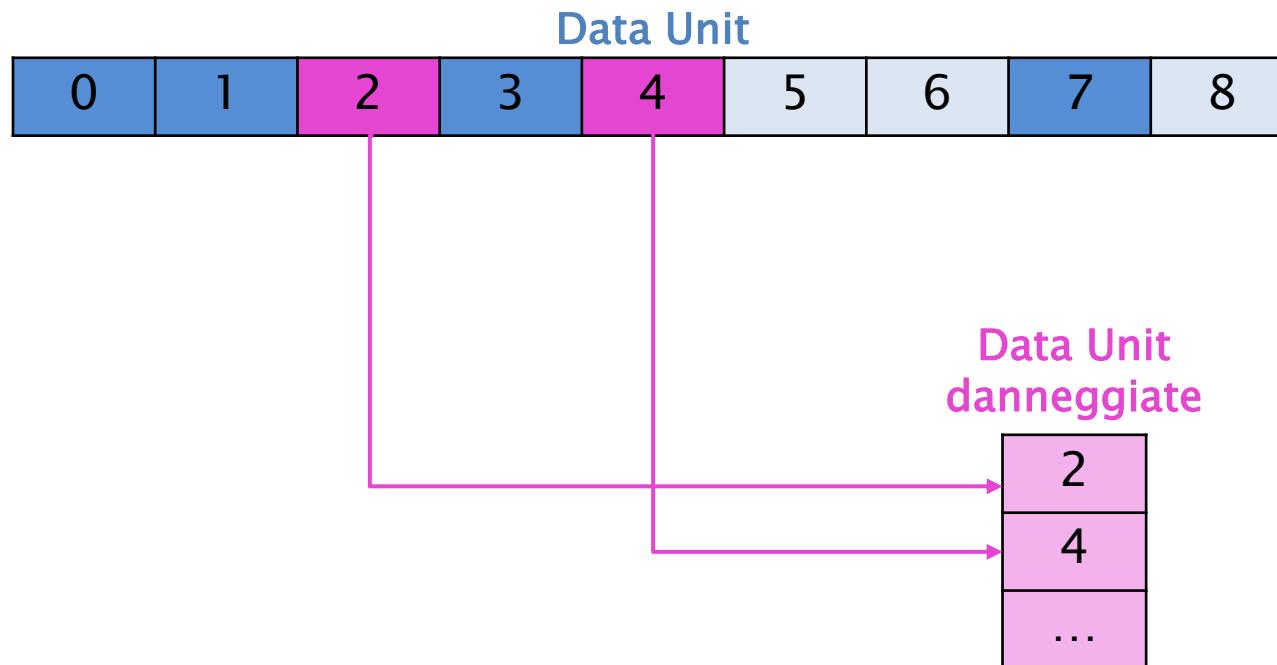
## ► Strategia del più adatto:

- Si cercano «data unit» libere che possano contenere consecutivamente il file



# File System: *Content Category*

## *data unit danneggiate*



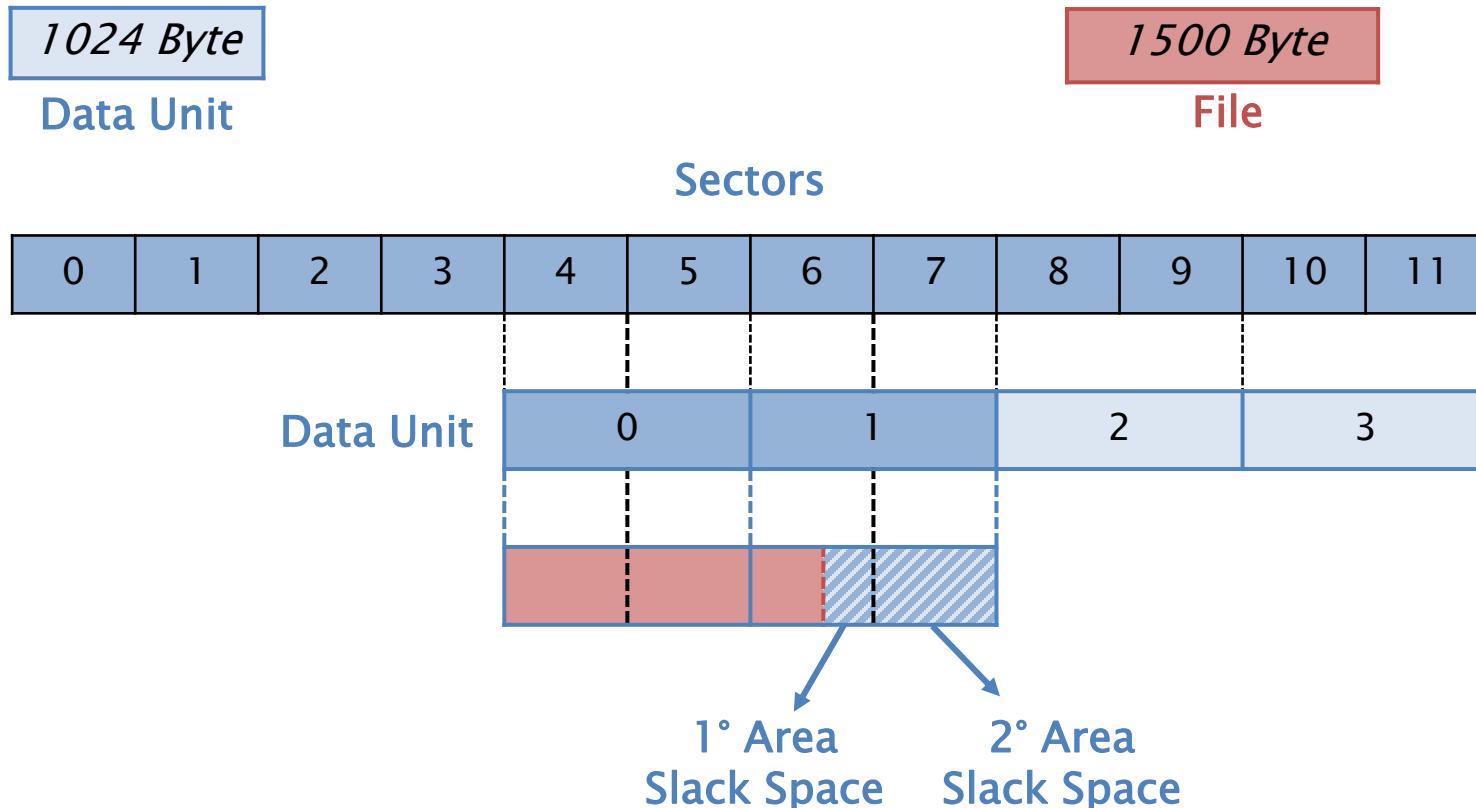
# File System: *Content Category analisi*

- 1) **Data Unit View:** ricerca di *settori* noti del File System
- 2) **Logical File System Searching:** ricerca la presenza di un contenuto specifico nei *data unit*
- 3) **Data Unit Allocation Status:** ricerca nei *data unit* non allocati
- 4) **Consistency Check:** ricerca di Data Unit non referenziati in «metadata category» (*Orphan Data Unit*)

# File System

## *Slack Space*

- ▶ Parte non usata di una Data Unit allocata



Data Unit  
non allocata

# File System

## *Slack Space*

1024 Byte

Data Unit

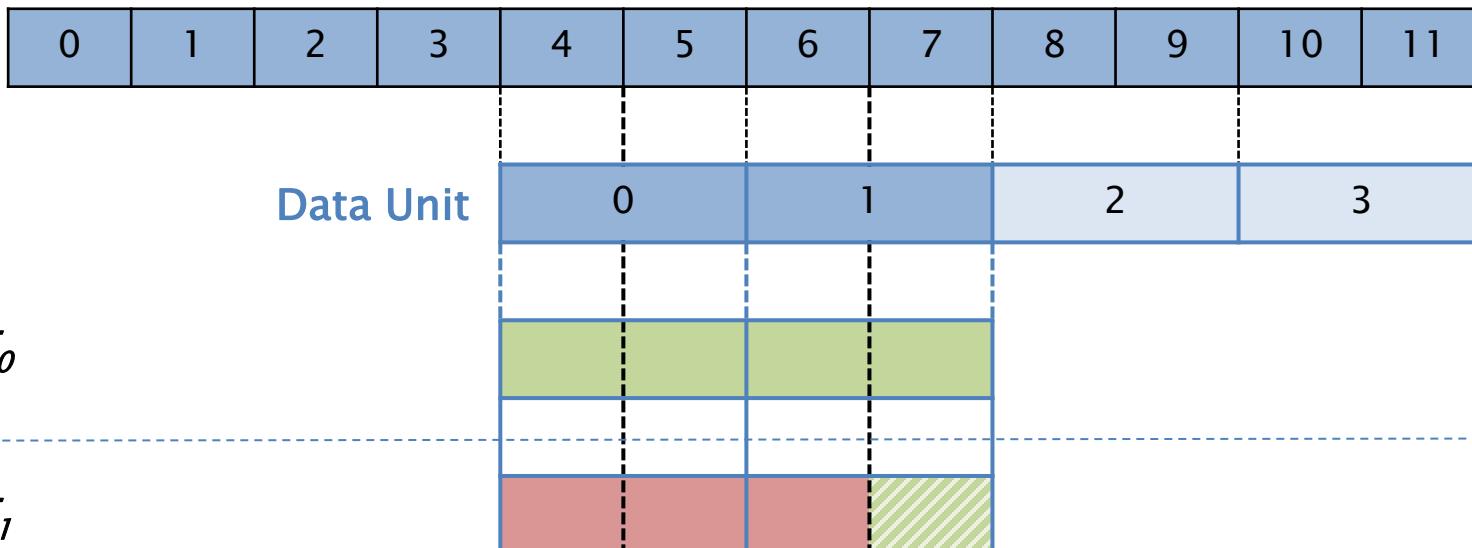
2048 Byte

File 01

1536 Byte

File 02

Sectors



# File System:

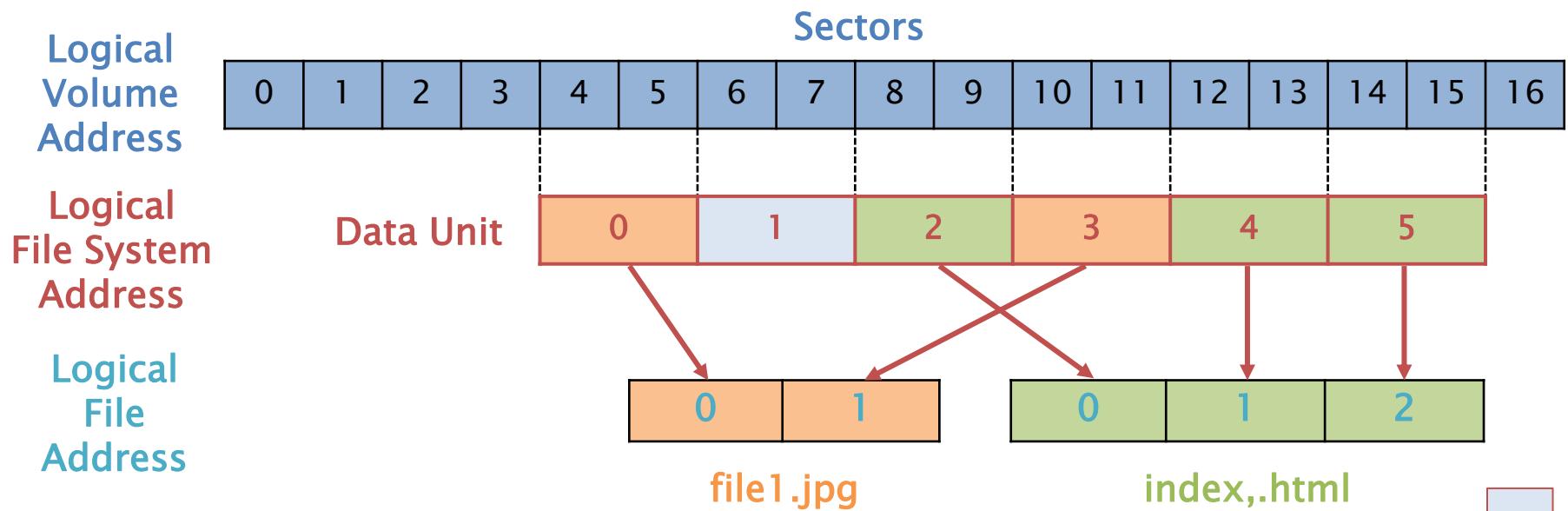
## *Metadata Category*

- ▶ Descrivono i file presenti in «content category»:
  - Informazioni temporali: *data di creazione/accesso/modifica*
  - Indirizzo delle Data Unit allocate per il File
- ▶ Analisi:
  - Ricerca di maggiori informazioni su di un file
  - Ricerca di file in base agli attributi descritti in questa categoria:
    - *es.: file creati dopo il 01/01/20*

# File System: *Metadata Category*

## *Logical File Address*

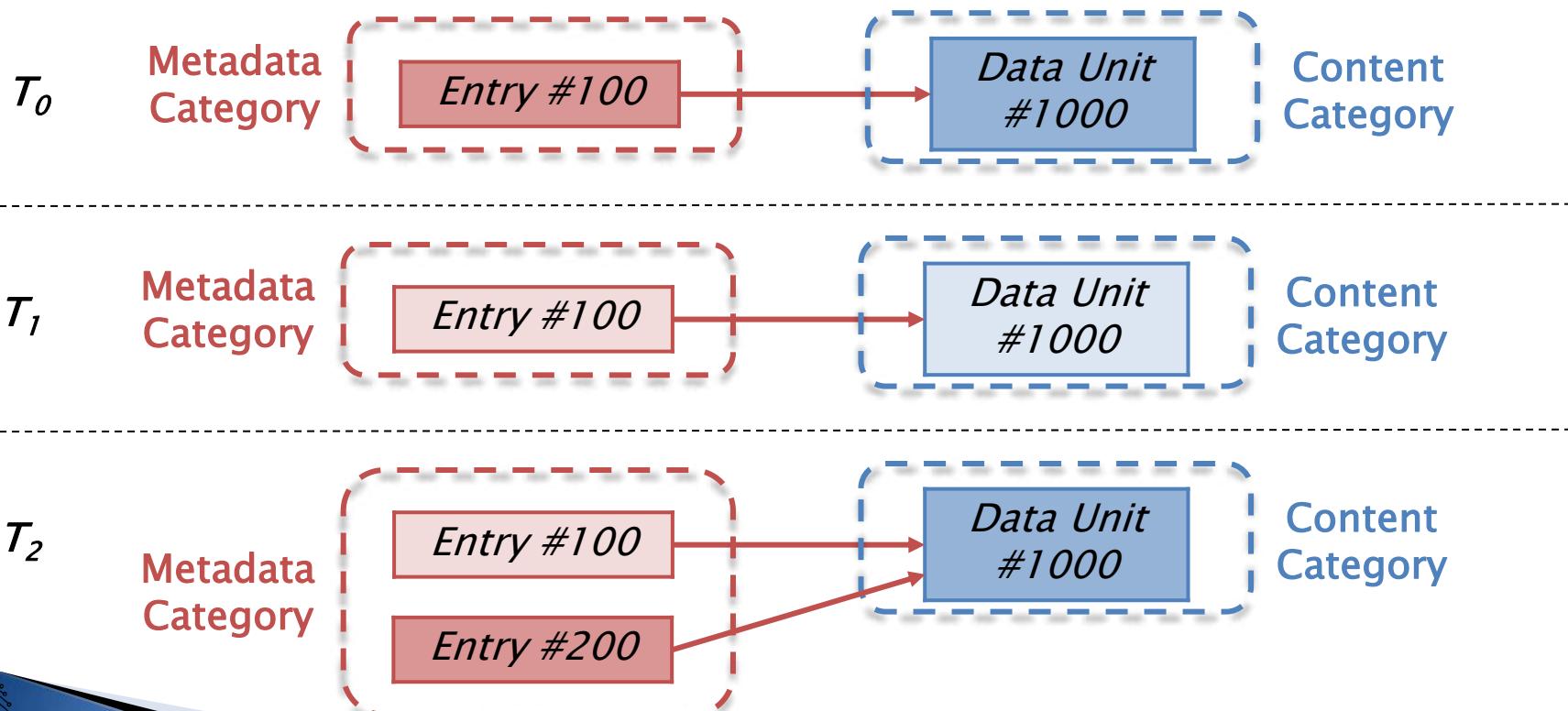
- ▶ Indirizzo di parte del file allocata nella data unit:
  - È contenuto nella data unit



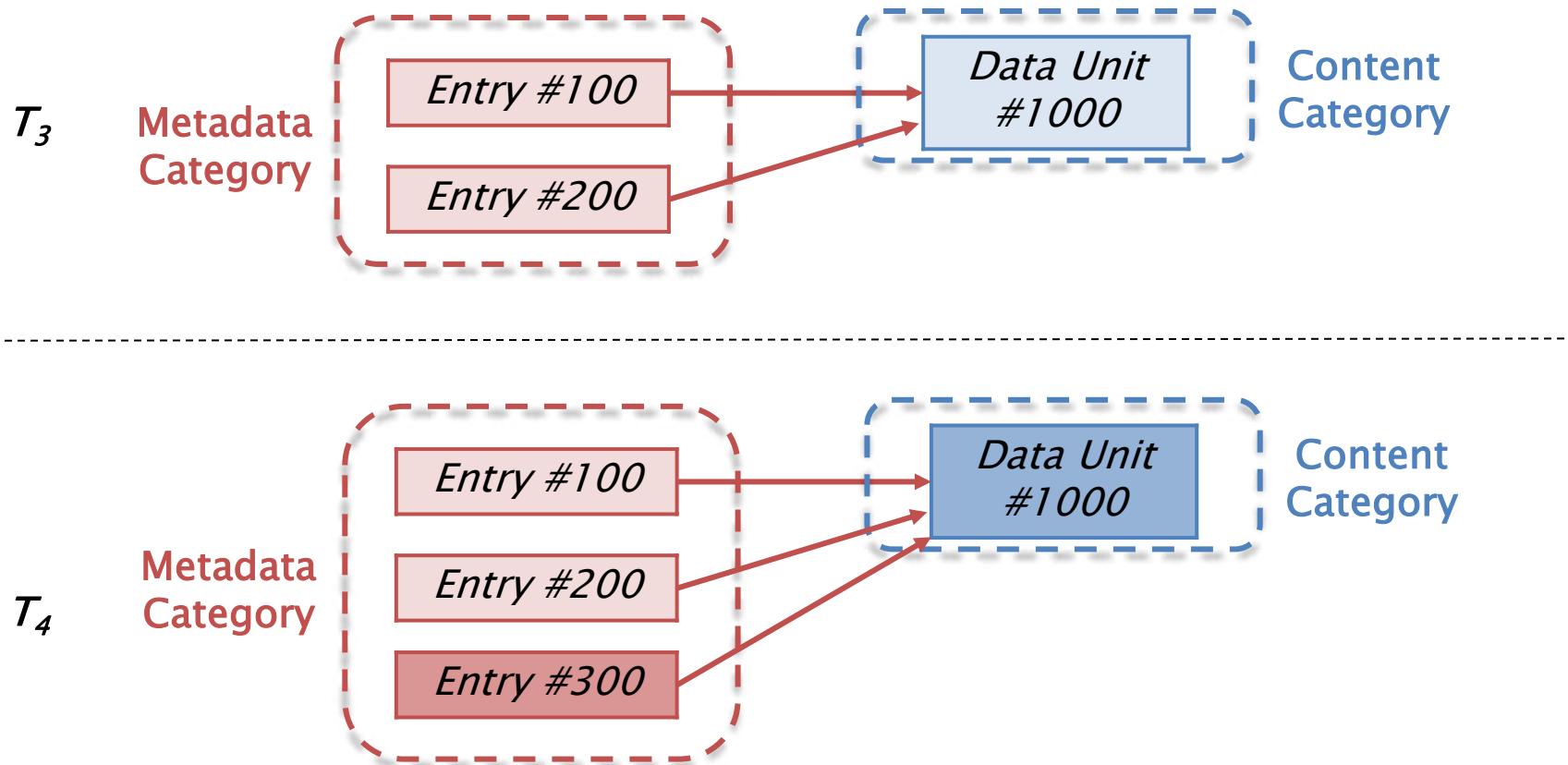
Data Unit  
non allocata

# File System: *Metadata Category* *File Recovery*

- ▶ Recupero dei file cancellati analizzando le entry in «metadata category» con lo stato non allocato.

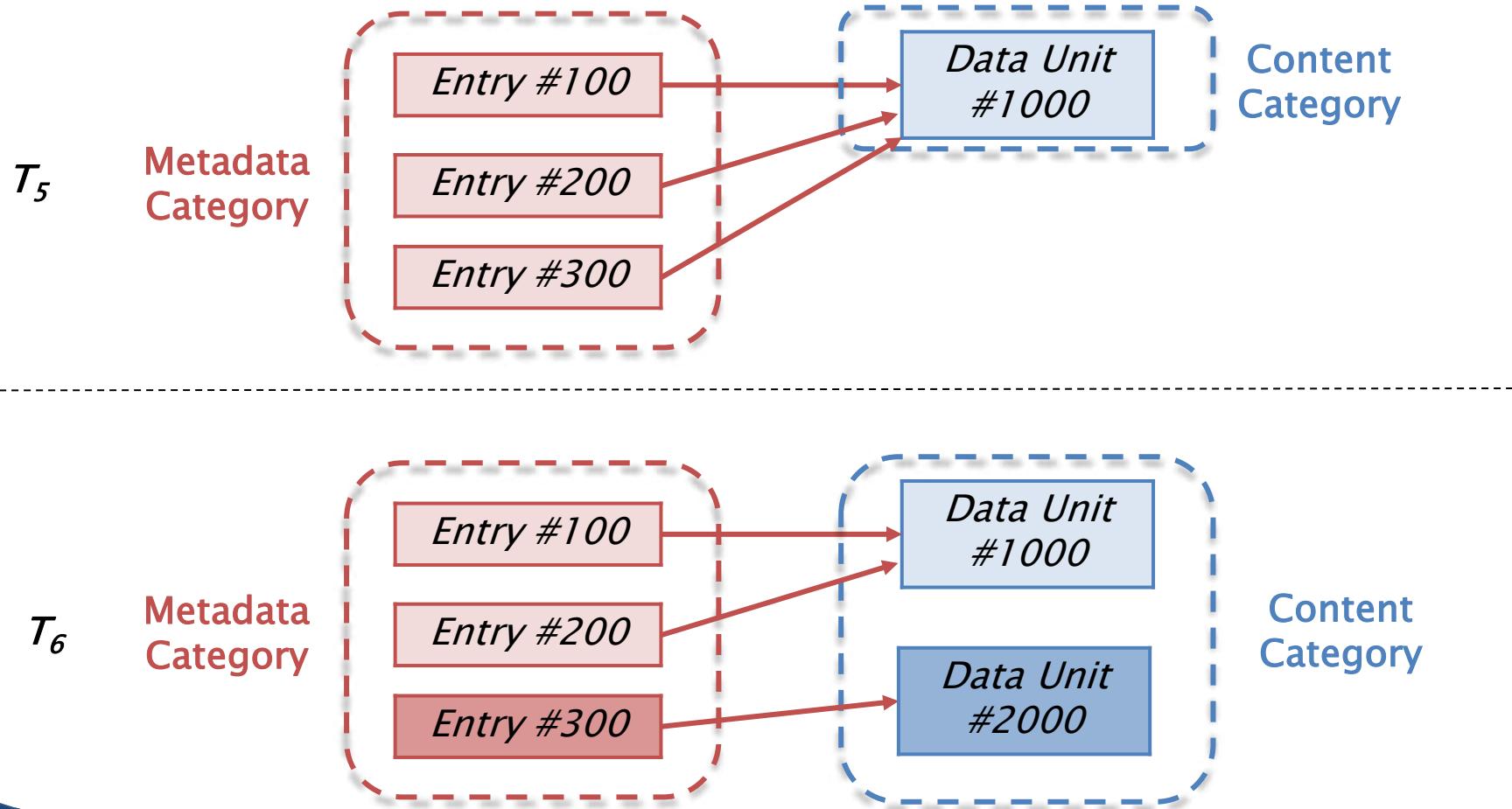


# File System: *Metadata Category* *File Recovery*



# File System: *Metadata Category*

## *File Recovery*



# File System

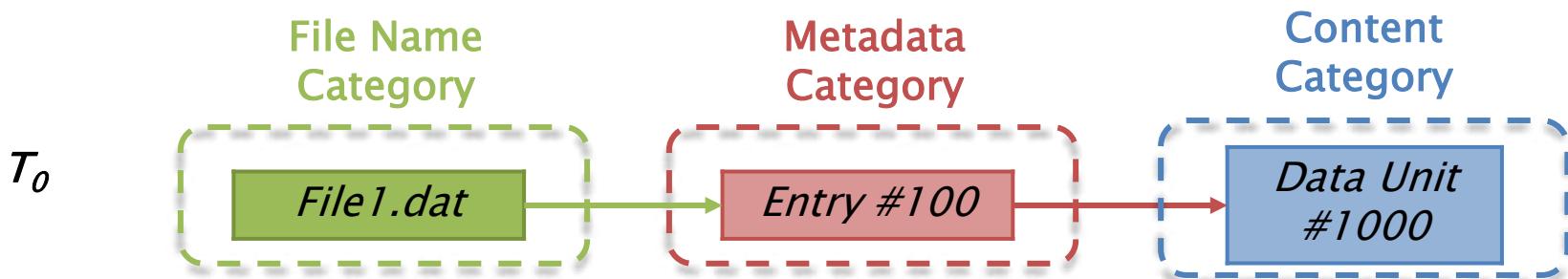
## *Compressed File*

- ▶ Memorizzare i dati in un formato compresso occupano meno Data Unit
- ▶ Tre livelli di compressione:
  - Compressione dei soli dati all'interno del file (*es.: JPEG, mp3, etc.*)
  - Compressione di tutto il file: creazione di un nuovo file.  
*(Es.: zip, rar, etc.)*
  - *Compressione eseguita dal File System: invisibile lato applicativo e utente*

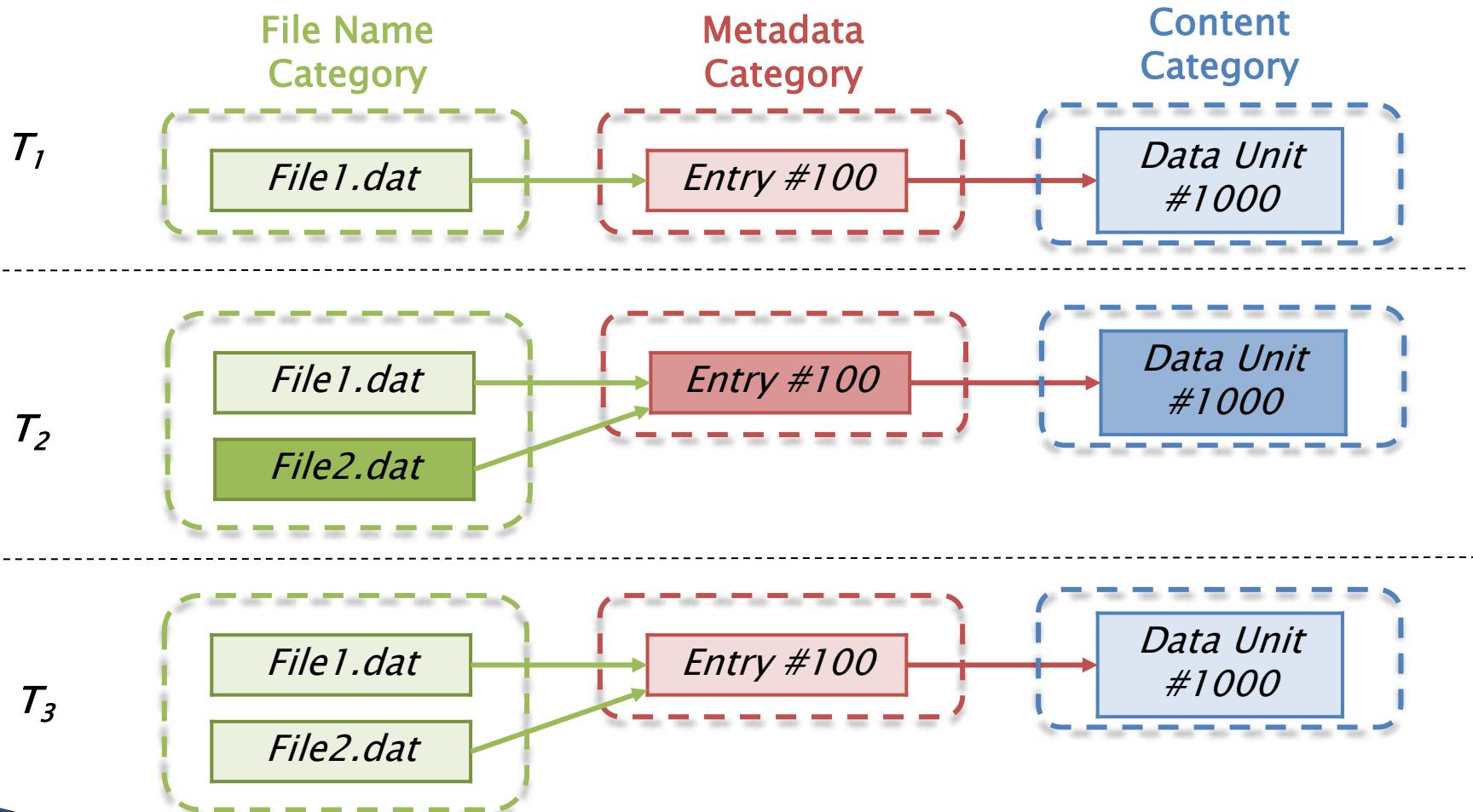
# File System:

## *File Name Category*

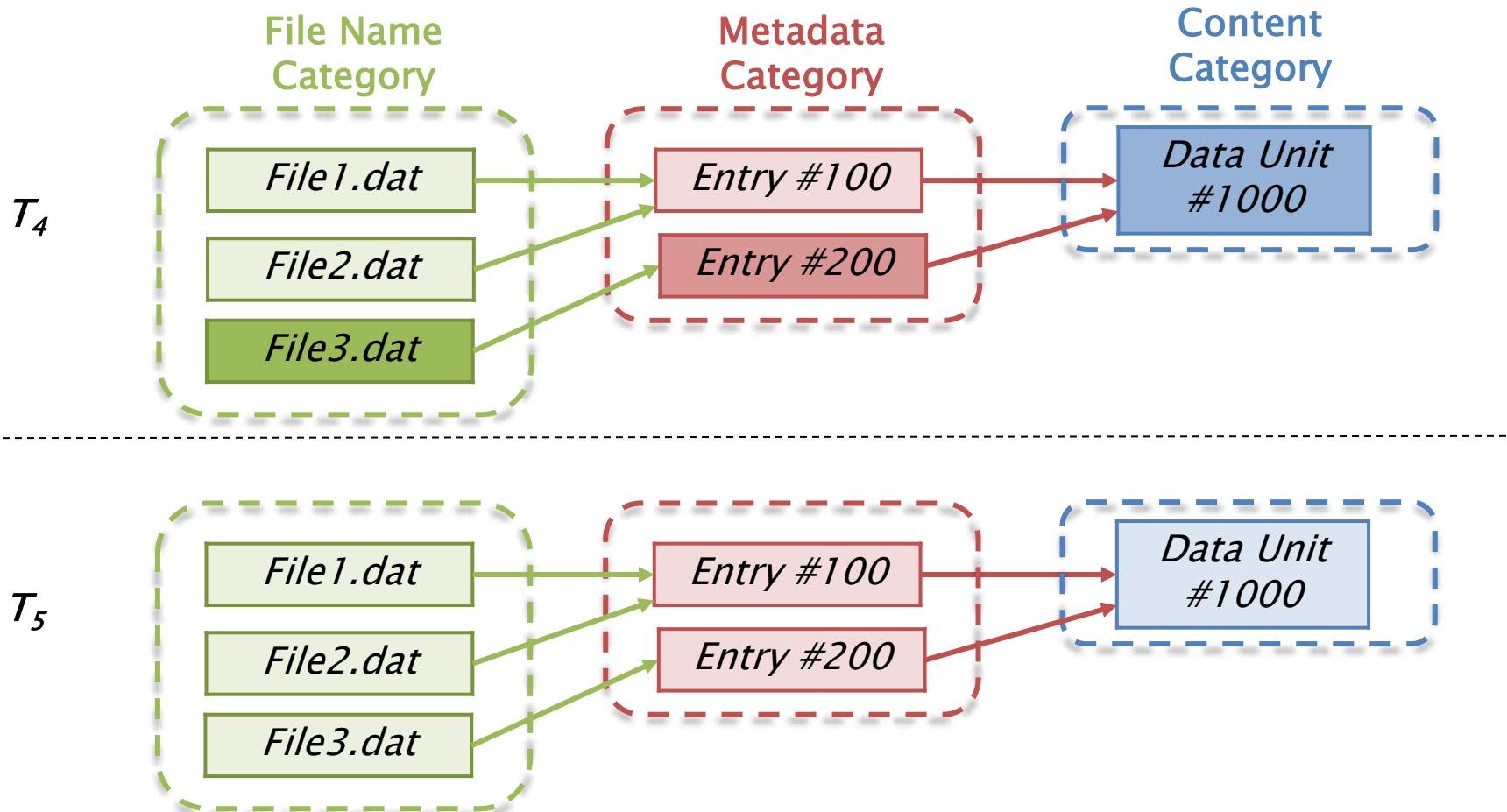
- ▶ Nome assegnato a ciascun file:
  - *Nome del file* – Indirizzo della struttura metadato.
- ▶ *File Recovery*:
  - Recupero dei file cancellati ricercando i «File Name» con lo stato non allocato:
    - Analisi della struttura metadati indirizzata



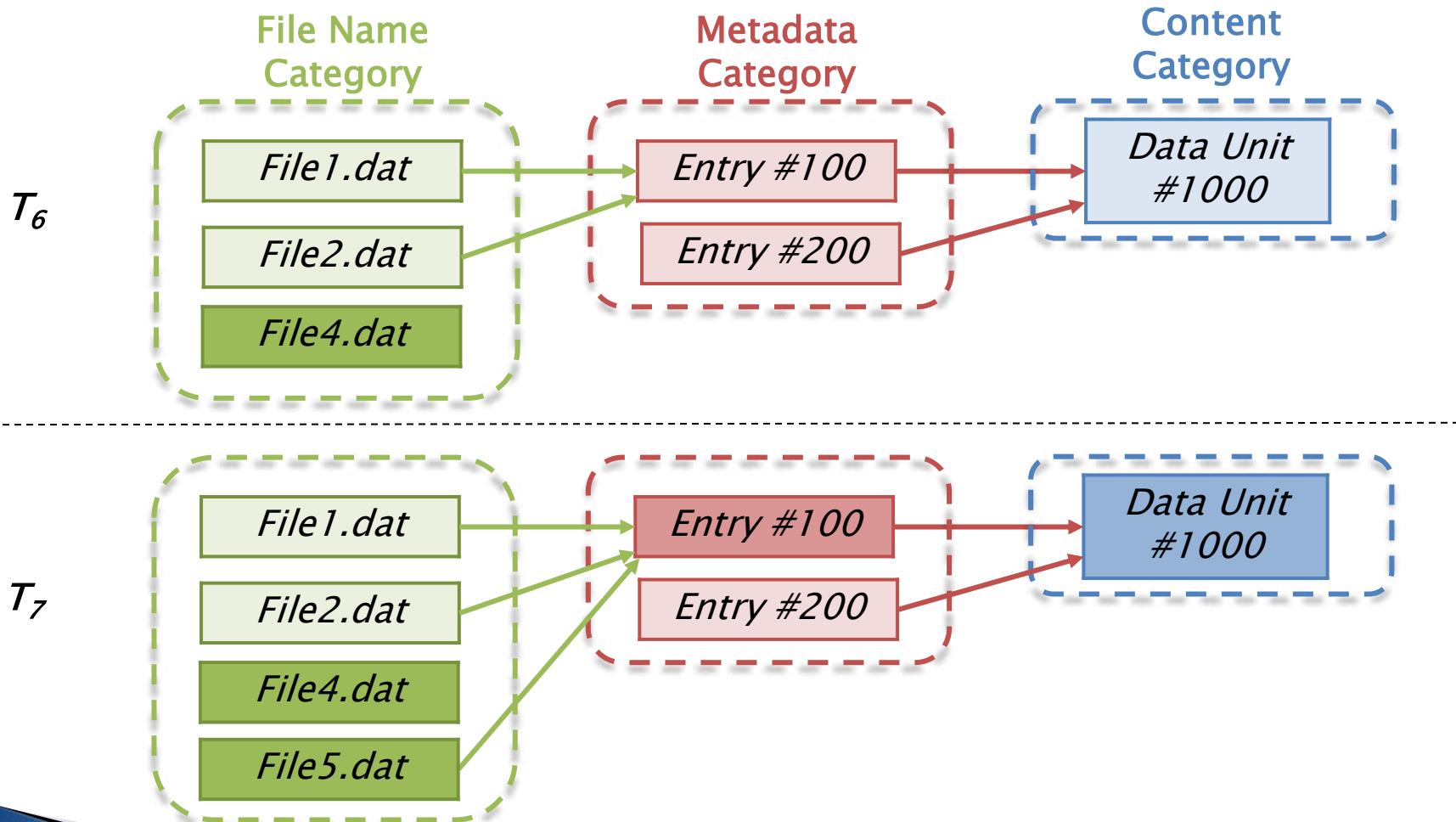
# File System: *File Name Category* *File Recovery*



# File System: *File Name Category* *File Recovery*

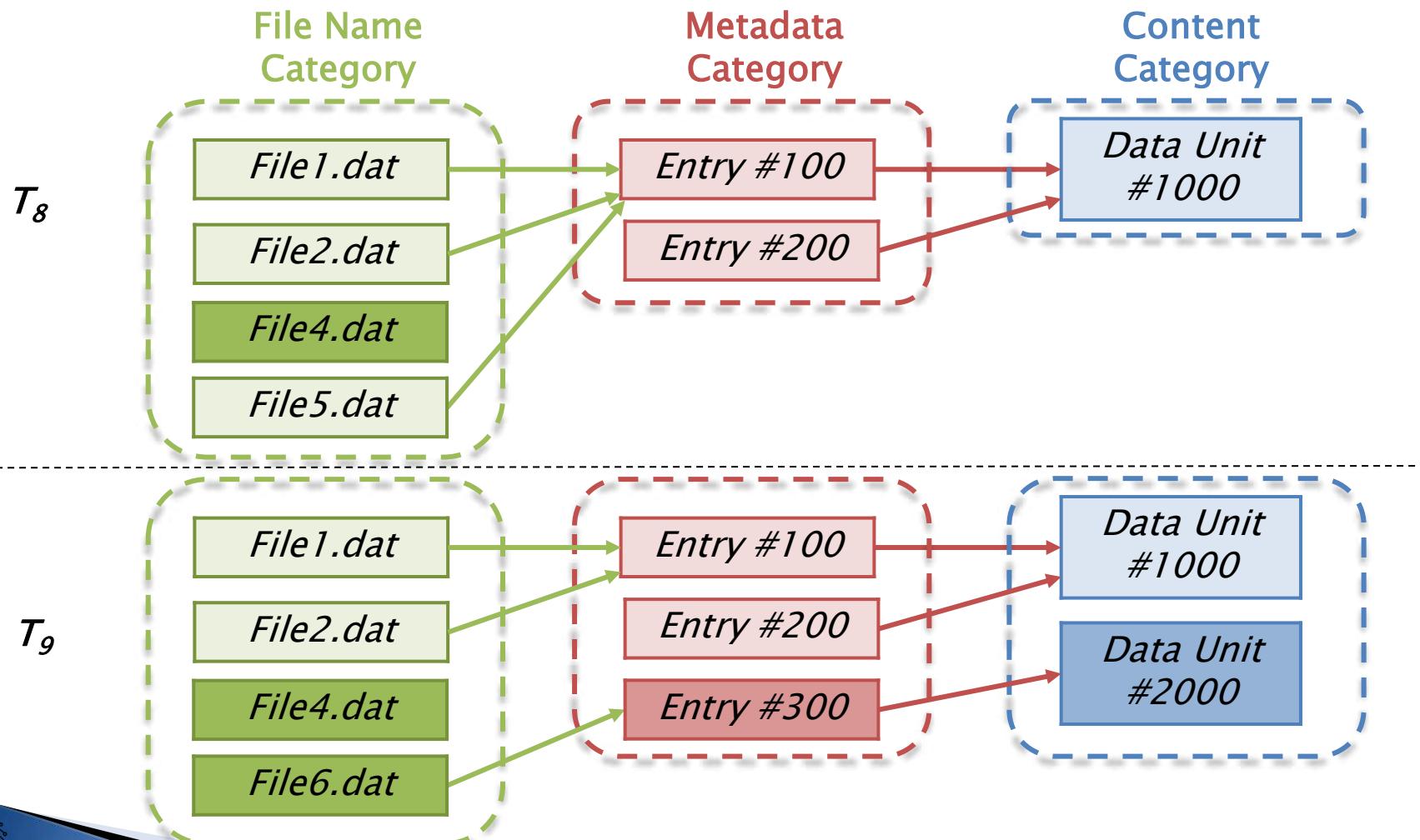


# File System: *File Name Category* *File Recovery*



# File System: *File Name Category*

## *File Recovery*



# File System: *Application Category*

- ▶ Dati non essenziali al File System:
  - Sono più efficienti se conservati nel File System.
  - *Es: Spazio occupato, Journaling.*
- ▶ *Journaling*
  - Conservazione delle modifiche da effettuare ed effettuate sui metadati:
    - Evitare l'inconsistenza:
      - *Completamento delle operazioni di modifica*
      - *Ripristino dei dati a prime delle modifiche (rollback)*
  - Analisi: ricostruire eventi di un incidente recente.



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 18: L'Analisi *i File System*

(2<sup>a</sup> parte)



A.A. 2021/22

Dott. Lorenzo LAURATO

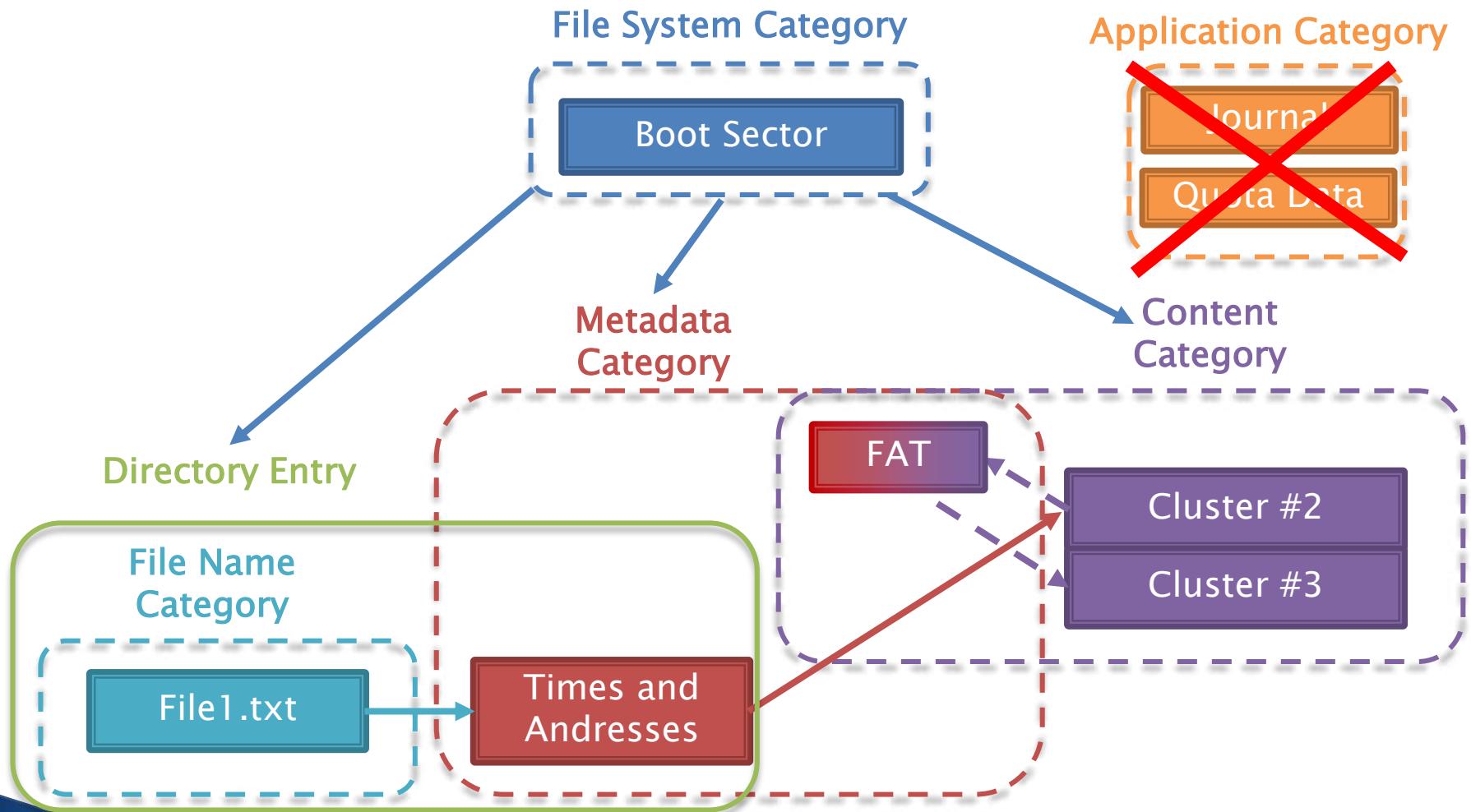


# File System

» FAT File System

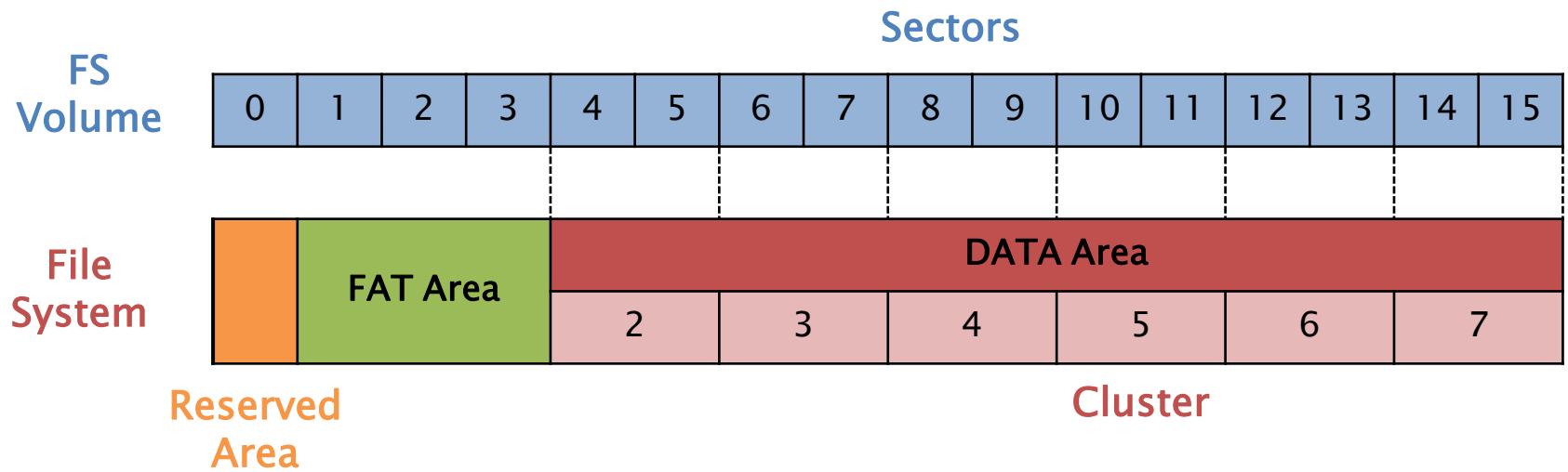


# FAT File System



# FAT File System

## *Physical Layout*



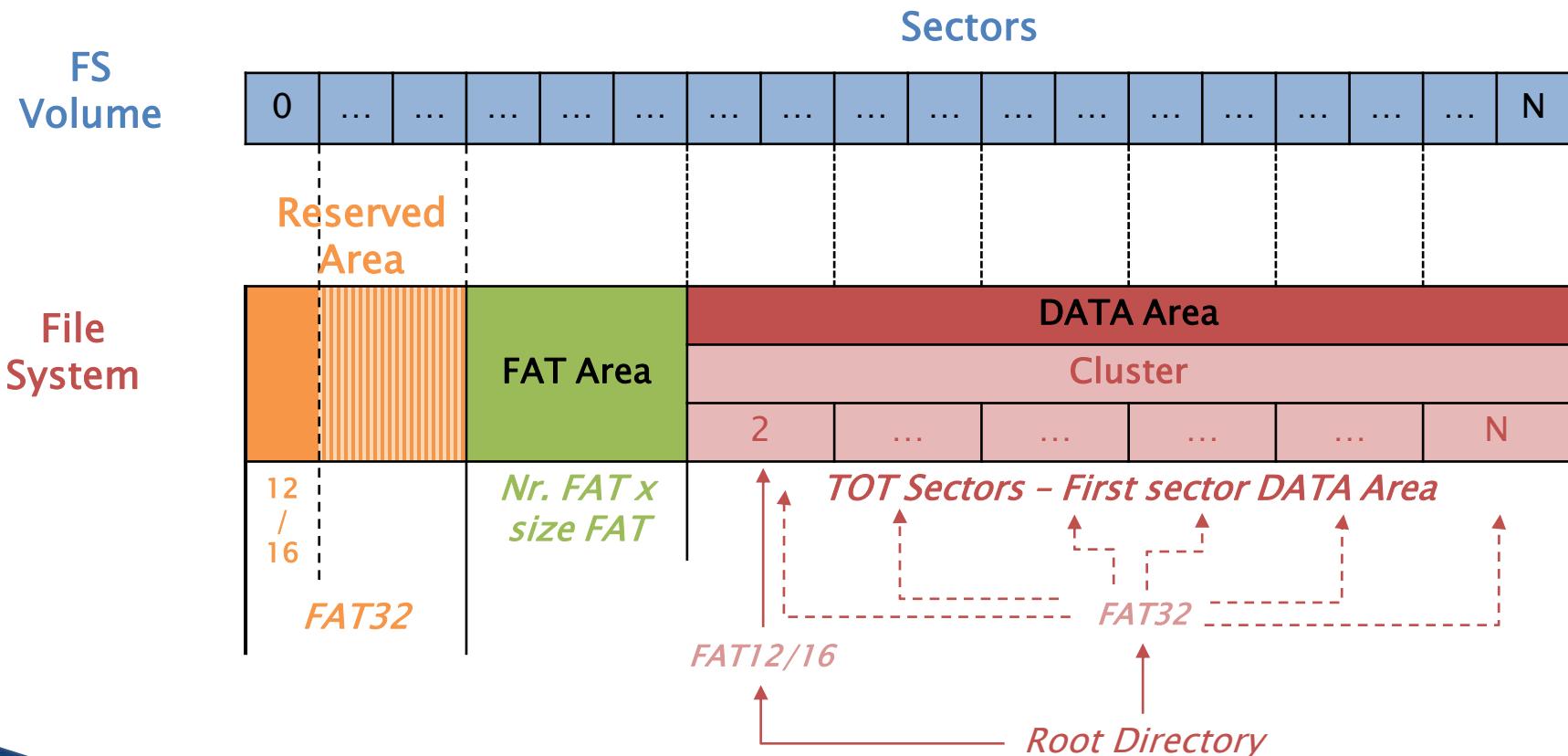
# FAT File System

## *File System Category*

- ▶ **FSINFO(FAT32): Reserved Area (*BootSector*)**
  - Cluster liberi
  - Prossimo Cluster libero
- ▶ **Boot Sector:** primo settore (*Reserved Area*)
  - *Physical Layout (Essential Data):*
    - **Reserved Area:** *settore 0*
      - FAT12/16: Dimensione 1 Settore
      - FAT32: Dimensione variabile
    - **FAT Area:** *dopo la «Reserved Area»*
      - Dimensione: Nr. FAT x Size FAT
    - **Data Area:** *dopo la «FAT Area»*
      - Dimensione: tot. settori - Inizio Area
      - Dimensione Cluster
      - Root directory:
        - Posizione (FAT32)
        - Dimensione (FAT12/16)

# FAT File System

## *Physical Layout*



# FAT File System

## *File System Category*

- ▶ **Boot Sector:** primo settore (*Reserved Area*)
  - *NO Essential Data:*
  - **OEM Name:** info strumento creazione del FS
  - **Volume Serial Number:** data di creazione (Microsoft)
  - **File System Label:** *FAT, FAT12, FAT16, FAT32*

# FAT File System

## Boot Sector

Byte	Description	Es.
0-2	Istruzioni assembly per saltare al bootcode	NO
3-10	OEM Name (ASCII)	NO
11-12	Dimensione settore (Byte)	SI
13	Dimensione Cluster (Settori) [ $x^2$ max 32kb]	SI
14-15	Dimensione Reserved Area (Settori)	SI
16	Nr. di FAT [solitamente 2]	SI
17-18	Max nr. File in root directory [FAT12/16] 0 (ZERO) [FAT32] => Byte 36-39	SI
19-20	Tot. settori FS [se > 65.536 => 0; usare Byte 32-35]	SI
21	Media Type [f8 - dischi fissi, f0 - disp. removibili]	NO
22-23	Dimensione FAT (settori) [FAT12/16] 0 (ZERO) [FAT32]	SI
24-25	Nr. settori per traccia INT.13h	NO
26-27	Nr. Head dispositivo INT.13h	NO
28-31	Nr. settori prima dell'inizio della partizione	NO
32-35	Tot. settori FS [se < 65.536 => 0; usare Byte 19-20]	NO

# FAT File System

## *Boot Sector (FAT12/16)*

Byte	Description	Es.
36	BIOS INT.13h	NO
37	Non usato	NO
38	Extended boot signature: identifica se i successivi tre valori sono validi [29]	NO
39–42	Volume Serial Number [Windows lo genera utilizzando la data di creazione]	NO
43–53	Etichetta Volume (ASCII) [scelto dall'utente\tool al momento della creazione del FS]	NO
54–61	File System type (ASCII) [FAT, FAT12, FAT16]	NO
62–509	Non usato [boot code]	NO
510–511	Signature [AA55]	NO

# FAT File System

## *Boot Sector (FAT32)*

Byte	Description	Es.
36-39	Dimensione della FAT (settori)	SI
40-41	Nr. di FAT [se bit[7]=1 solo una delle FAT bit[0-3] è attiva, altrimenti mirror]	SI
42-43	Nr. di versione	SI
44-47	Posizione root directory (cluster)	SI
48-49	Posizione della struttura FSINFO (settori)	NO
50-51	Copia di backup del Boot Sector (settori) [6]	NO
52-63	Riservati	NO
64	BIOS INT.	NO
65	Non usato	NO
66	Extended boot signature: identifica se i successivi tre valori sono validi [29]	NO
67-70	Volume SN [Windows lo genera utilizzando la data di creazione]	NO
71-81	Etichetta Volume (ASCII)	NO
82-89	File System type (ASCII) [FAT32]	NO
90-509	Non usato [boot code]	NO
510-511	Signature [AA55]	NO

# FAT File System

## *Boot Sector: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 0 | xxd
0000000: eb58 904d 5344 4f53 352e 3000 0202 2600 .X.MSDOS5.0...&.
0000016: 0200 0000 00f8 0000 3f00 4000 c089 0100 .....?@.....
0000032: 4023 0300 1d03 0000 0000 0000 0200 0000 @#.....[...]
```

Byte	Description	Value
3-10	OEM Name (ASCII)	MSDOS5.0
11-12	Dim. settore (Byte)	0200 (512)
13	Dim. Cluster (Settori)	2
14-15	Dim. Reserved Area (Settori)	0026 (38)
16	Nr. di FAT	2
17-18	Max nr. File in root directory	0
19-20	Tot. settori FS	0
21	Media Type	f8(disco fisso)
22-23	Dim. FAT (settori)	0
28-31	Nr. settori prima dell'inizio della partizione	000189c0 (100.800)
32-35	Tot. settori FS	00032340 (205.632)

# FAT File System

## *Boot Sector: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 0 | xxd
[...]
0000032: 4023 0300 1d03 0000 0000 0000 0200 0000 @#.....
0000048: 0100 0600 0000 0000 0000 0000 0000 0000 .....
0000064: 8000 2903 4619 4c4e 4f20 4e41 4d45 2020 ..).F.LNO NAME
0000080: 2020 4641 5433 3220 2020 33c9 8ed1 bcf4  FAT32  3....
[...]
0000496: 7274 0d0a 0000 0000 00ac cbd8 0000 55aa rt.....U.
```

Byte	Description	Value
36-39	Dimensione della FAT (settori)	00031d (797)
44-47	Posizione root directory (cluster)	00000002 (2)
48-49	Posizione della struttura FSINFO (settori)	0001 (1)
50-51	Copia di backup del Boot Sector (settori)	0006 (6)
67-70	Volume SN	4c194603
71-81	Etichetta Volume (ASCII)	«NO NAME »
82-89	File System type (ASCII) [FAT32]	«FAT32 »
510-511	Signature	AA55

# FAT File System

## *FSINFO*

Byte	Description	Es.
0-3	Signature [41615252]	NO
4-483	Non usato	NO
484-487	Signature [61417272]	NO
488-491	Nr. di Cluster liberi	NO
492-495	Prossimo Cluster libero	NO
496-507	Non usato	NO
508-511	Signature [AA550000]	NO

# FAT File System

## *FSINFO: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 1 | xxd
```

```
0000000: 5252 6141 0000 0000 0000 0000 0000 0000 RRaA.....  
0000016: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
              [...]  
0000464: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000480: 0000 0000 7272 4161 1e8e 0100 4b00 0000 .....rrAa....K..  
0000496: 0000 0000 0000 0000 0000 0000 55aa .....U.
```

Byte	Description	Value
0-3	Signature	41615252
484-487	Signature	61417272
488-491	Nr. di Cluster liberi	00018e1e (101.918)
492-495	Prossimo Cluster libero	0000004b (75)
508-511	Signature	AA550000

# FAT File System

## *Boot Sector: analisi*

```
root@caine:/# fsstat -f fat fat-4.dd
FILE SYSTEM INFORMATION
-----
File System Type: FAT
OEM Name: MSDOS5.0
Volume ID: 0x4c194603
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FAT DISK
File System Type Label: FAT32

Backup Boot Sector Location: 6
FS Info Sector Location: 1
Next Free Sector (FS Info): 1778
Free Sector Count (FS Info): 203836
Sectors before file system: 100800
```

File System Layout (in sectors)  
Total Range: 0 - 205631  
\* Reserved: 0 - 37  
\*\* Boot Sector: 0  
\*\* FS Info Sector: 1  
\*\* Backup Boot Sector: 6  
\* FAT 0: 38 - 834  
\* FAT 1: 835 - 1631  
\* Data Area: 1632 - 205631  
\*\* Cluster Area: 1632 - 205631  
\*\*\* Root Directory: 1632 - 1635

### CONTENT-DATA INFORMATION

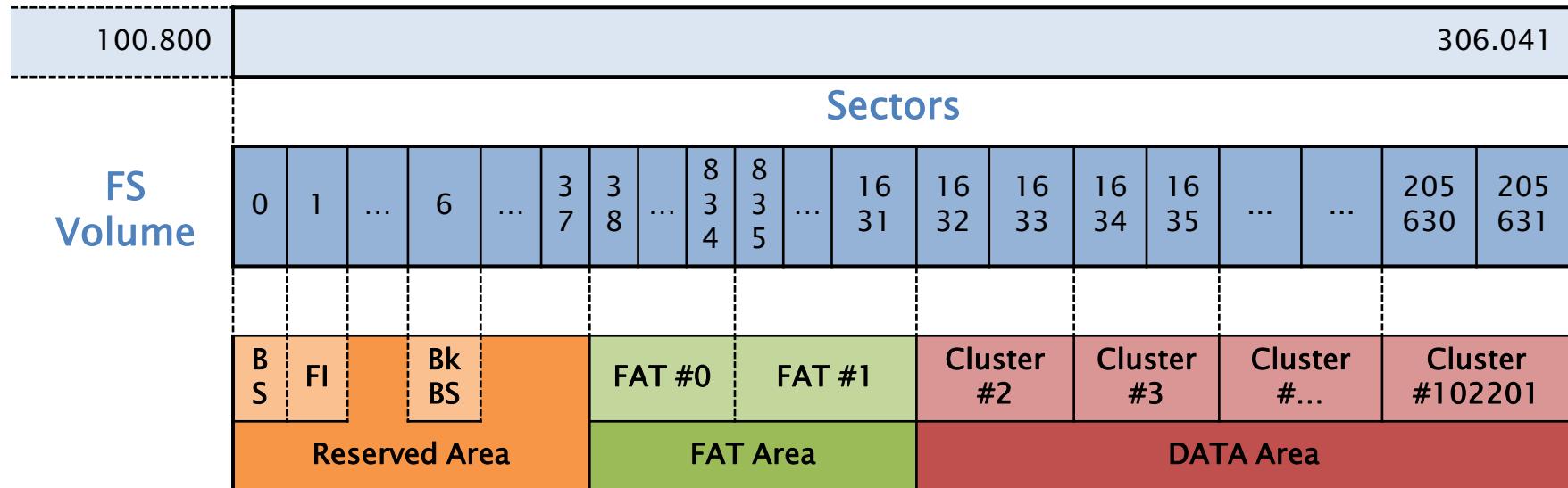
---

Sector Size: 512  
Cluster Size: 1024  
Total Cluster Range: 2 - 102001  
[...]

# FAT File System

## *Physical Layout*

Disk Volume



# FAT File System

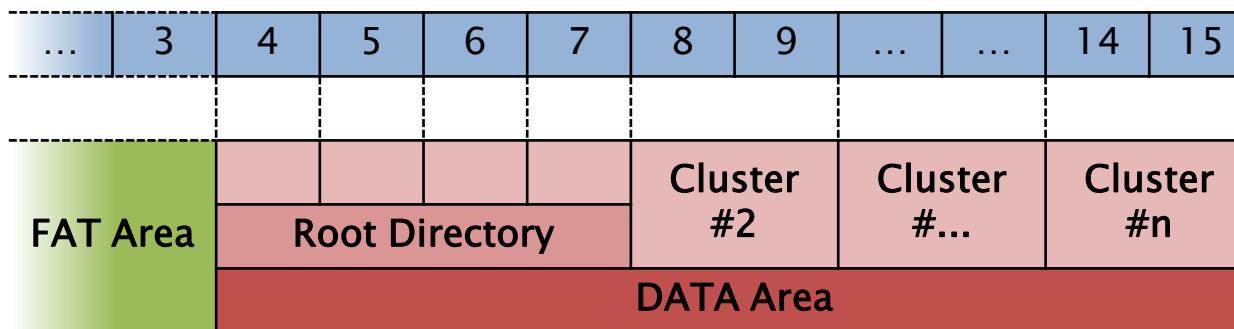
## *File System Category: analisi*

- ▶ Recuperare informazioni sul layout
- ▶ Controllare possibili dati nascosti:
  - Bootcode
  - Settori in Reserved Area:
    - FSINFO
  - Volume slack
- ▶ Confronto tra il Boot Sector ed il backup del Boot Sector

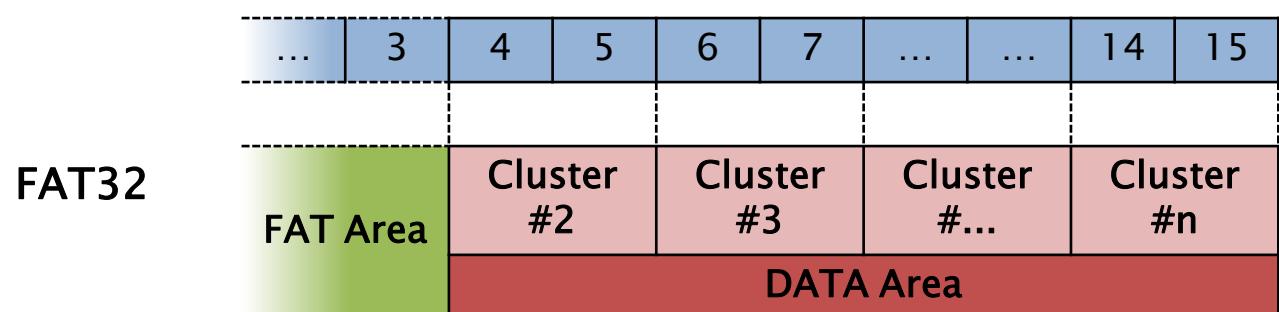
# FAT File System

## *Content Category*

- ▶ Contenuto di File e Directory
- ▶ Cluster:  $2^x$  settori (*max 32KB*)
  - Primo Cluster: indirizzo 2
  - Solo in Data Area



FAT12/16



FAT32

# FAT File System

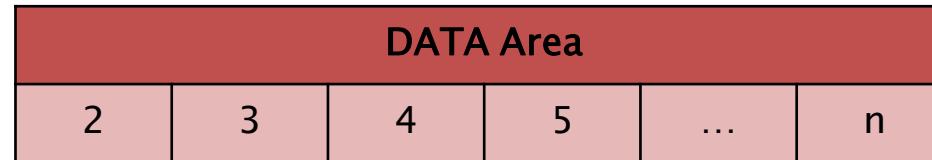
## FAT

- ▶ Identificare lo stato di allocazione dei Cluster
- ▶ Successivo Cluster del file: *Cluster Chain*
- ▶ Layout: *Boot Sector*
- ▶ Entry di ugual dimensione: FAT12: 12bit, FAT16: 16bit, FAT32: 32bit
  - Indirizzamento diretto:
    - La prima entry ha indirizzo 0 ZERO
    - Indirizzo entry = Indirizzo Cluster: *Es. Entry[10]=Cluster[10]*
      - Entry[0]: informazione del media
      - Entry[1]: dirty status
      - Entry[2] -> Cluster[2]
      - Entry[n] -> Cluster[n]

# FAT File System

## FAT

### ▶ Contenuto delle Entry:



FAT	
0	<i>Info Media</i>
1	<i>Dirty status</i>
2	
3	
4	
5	
...	
n	

- 
- A green arrow points from the empty entry at index 3 in the FAT table to the list of cluster states.
- Cluster non allocato: 0 (Zero)
  - Cluster allocato:
    - Prossimo cluster (*Cluster Chain*)
    - EOF:
      - 0xff8 [FAT12]
      - 0xffff8 [FAT16]
      - 0x0fff fff8 [FAT32]
  - Cluster danneggiato:
    - 0xff7 [FAT12]
    - 0xffff7 [FAT16]
    - 0x0fff fff7 [FAT32]

# FAT File System

## *FAT: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 38 | xxd
[...]
0000288: 4900 0000 4a00 0000 4c00 0000 0000 0000 I...J...L.....
0000304: 4d00 0000 ffff ff0f 4f00 0000 ffff ff0f M.....0.....
0000320: 5100 0000 5200 0000 ffff ff0f ffff ff0f Q...R.....
0000336: ffff ff0f 0000 0000 0000 0000 0000 0000 ..... .
0000352: 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

Entry: 32Byte  
(Offset/4)

Entry #	Byte	Valore
72	288-291	00000049 (73)
73	292-295	0000004a (74)
74	296-299	0000004c (76)
75	300-303	00000000 (0)
76	304-307	0000004d (77)
...	...	...
85	340-343	00000000 (0)

# FAT File System

## *FAT*

## ▶ Indirizzamento:



## Es.: Cluster 75:

$$(75 - 2) \times 2 + \text{Sect\_Cluster\_2}$$

$$38 + 1594 = 1632$$

(Dim\_ReservedArea) (Dim\_FATArea)

$$(75 - 2) \times 2 + 1632 => 1778$$

# FAT File System

## *FAT*

### ▶ Indirizzamento:

- Cluster => Settore ?

```
root@caine:/# blkstat -f fat fat-4.dd 1778
```

Sector: 1778

Not Allocated

Cluster: 75

# FAT File System

## *Metadata Category*

- ▶ Informazioni su file e directory
  - Indirizzo del primo cluster
- ▶ Parent Directory:
  - Directory Entry: 32KB
    - File
    - Directory
  - Posizionata nella Data Area (Cluster)
  - File Name Category:
    - Nome File (8 caratteri) + Estensione (3 caratteri)
    - > Long File Name Directory Entry

# FAT File System

## *Directory Entries*

Byte	Description	Es.
0	- Primo carattere del filename (ASCII) - 0xe5 o 0x00 [non allocato]	SI
1-10	Caratteri da 2 a 11 del filename (ASCII)	SI
11	<b>Attributo File</b>	SI
12	Riservato	NO
13	Ora di creazione (decimi di secondo)	NO
14-15	Ora di creazione (ora, minuti, secondi)	NO
16-17	Data di Creazione	NO
18-19	Data di Accesso	NO
20-21	- Indirizzo del primo cluster (High Byte) - 0 (ZERO) [FAT12/16]	SI
22-23	Ora di Modifica (ora, minuti, secondi)	NO
24-25	Data di Modifica	
26-27	Indirizzo del primo cluster (Low Byte)	SI
28-31	- Dimensione del file - 0 (ZERO) per le directory	SI

# FAT File System

## *Directory Entries: attributes*

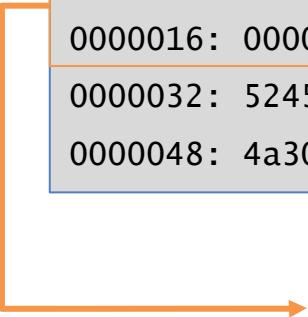
Attributo File [Byte 11]		
Flag Value bit	Description	Es.
0000 0001 (01)	Sola lettura	NO
0000 0010 (02)	File nascosto	NO
0000 0100 (04)	File di sistema	NO
0000 1000 (08)	Etichetta volume	SI
0000 1111 (0f)	Long File name	SI
0001 0000 (10)	Directory	SI
0010 0000 (20)	Archive	NO

# FAT File System

## *Directory Entries: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 1632 | xxd
```

```
0000000: 4641 5420 4449 534b 2020 2008 0000 0000 FAT DISK .....
0000016: 0000 0000 0000 874d 252b 0000 0000 0000 .....M%+.....
0000032: 5245 5355 4d45 2d31 5254 4620 00a3 347e RESUME-1RTF ..4~
0000048: 4a30 8830 0000 4a33 7830 0900 f121 0000 .0.0....0....!..
```



Byte	Description	Value
0	Fila Name – Primo carattere	F
1-10	Fila Name – Dieci caratteri	«AT DISK »
11	Attributo File	08 (0000 1000) [Etichetta Volume]
22-23	Ora di Modifica	4d87
24-25	Data di Modifica	2b25

# FAT File System

## *Directory Entries: analisi*

Byte	Description														Value				
22-23	Ora di Modifica														4d87				
24-25	Data di Modifica														2b25				
0	0	1	0	1	0	1	1	0	0	1	0	0	1	0	1	0	0	1	1
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0				
Anno (0-127) + 1980							Mese (1-12)							Giorno (1-31)					
2001							9							5					
0	1	0	0	1	1	0	1	1	0	0	0	0	1	1	1	1	1	1	
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0				
Ora (0-23)							Minuti (0-59)							Secondi (0-29) x 2					
9							44							14					

# FAT File System

## *Directory Entries: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 1632 | xxd
0000000: 4641 5420 4449 534b 2020 2008 0000 0000 FAT DISK .....
0000016: 0000 0000 0000 874d 252b 0000 0000 0000 .....M%+.....
0000032: 5245 5355 4d45 2d31 5254 4620 00a3 347e RESUME-1RTF ..4~
0000048: 4a30 8830 0000 4a33 7830 0900 f121 0000 .0.0.....0...!..
```

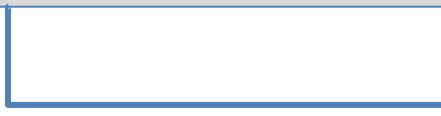


Byte	Description	Value
0	Fila Name – Primo carattere	R
1-10	Fila Name – Dieci caratteri	«ESUME-1.RTF»
11	Attributo File	20 (0010 0000) [Archive]
13	Ora di Creazione (decimi s)	a3 (163)
14-15	Ora di Creazione	7e34 (15:49:40)
16-17	Data di Creazione	304a (10/02/2004)
20-21 26-27	Indirizzo Primo cluster File	0000 0009 (9)
28-31	Dimensione del file	000021f1 (8.689)

# FAT File System

## *FAT: analisi*

```
root@caine:/# blkcat -f fat fat-4.dd 38 | xxd
[...]
0000032: ffff ff0f 0a00 0000 0b00 0000 0c00 0000 .....
0000048: 0d00 0000 0e00 0000 0f00 0000 1000 0000 .....
0000064: 1100 0000 ffff ff0f 1300 0000 1400 0000 .....
```



Entry #	Byte	Valore
9	36-39	0000000a (10)
10	40-43	0000000b (11)
11	44-47	0000000c (12)
12	48-51	0000000d (13)
13	52-55	0000000e (14)
14	56-59	0000000f (15)
15	60-63	00000010 (16)
16	64-67	00000011 (17)
17	68-71	0fffffff (EOF)

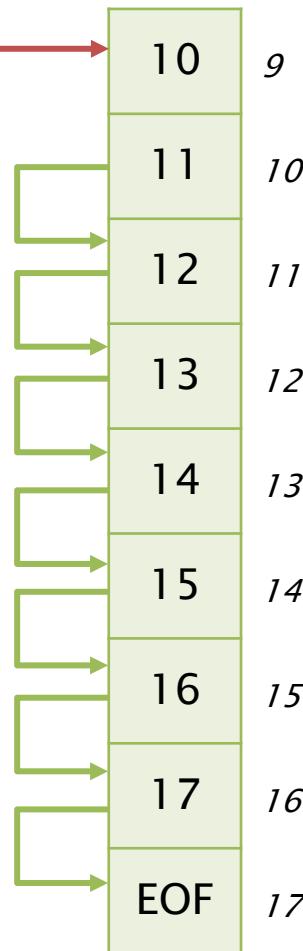
# FAT File System

## *FAT: cluster chain*

Directory Entry

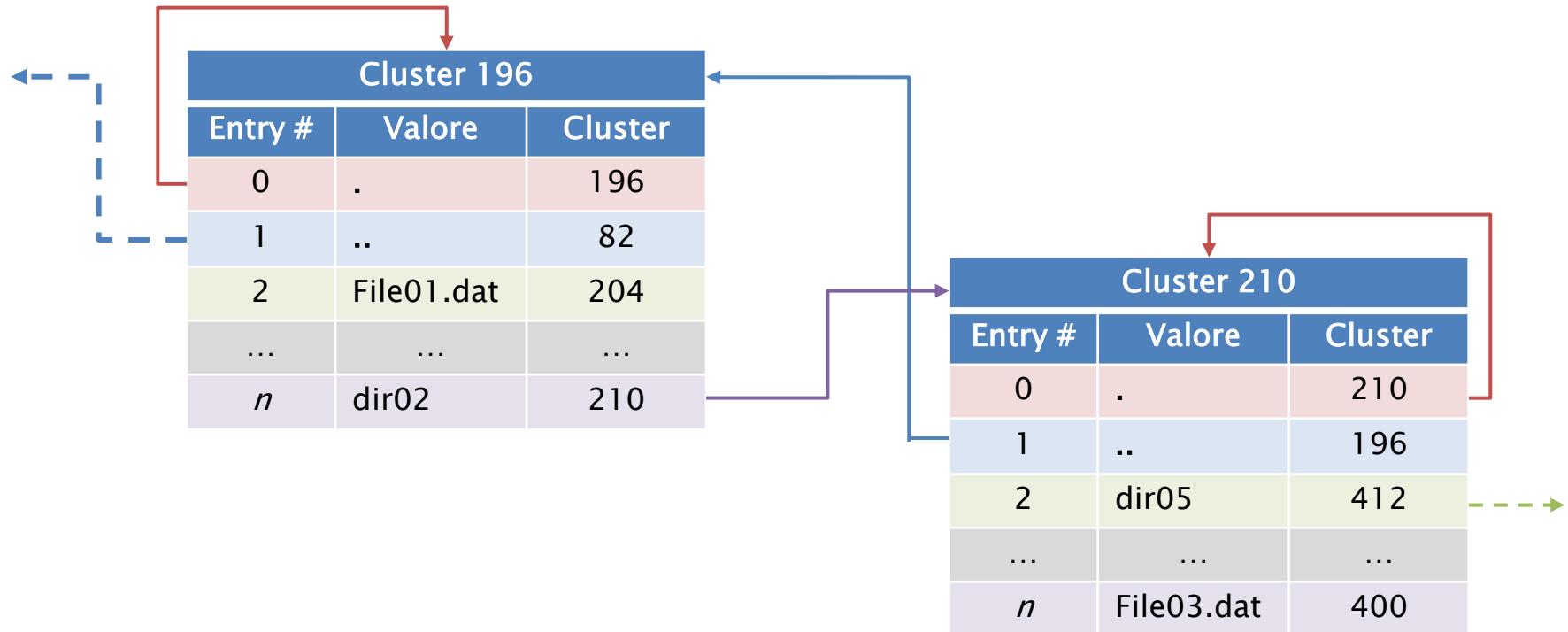
File Name	Start	Dimensione
RESUME-1.RTF	9	8.689

FAT



# FAT File System

## *Metadata Category: Directory*



# FAT File System

## *Metadata Category*

- ▶ **Informazioni temporali (*non essential data*)**
  - Data di creazione (Windows)
    - Nuovo File/Copia File => Nuova data
    - Sposto/Rinomino => copia della data
  - Data di Modifica (Windows): modifica del contenuto
    - Copia/Sposto/Rinomino File => copia della data
  - Data di Accesso (Windows):
    - Modificata anche visualizzando le proprietà

# FAT File System

## *File Name Category*

- ▶ Mappare le strutture «Metadata» con un etichetta: **Filename**
- ▶ Directory Entry: insieme ai «Metadata Catergory»
  - FileName 11 caratteri
  - Long File Name (LFN) directory entry: +13 caratteri

Cluster 196		
Entry #	Valore	Cluster
0	.	196
1	..	82
2	FileSys.TXT	204
3	TextFileFAT	204
4	TE021F~1.TXT	204
...	...	...

# FAT File System

## *File Name Category*

Byte	Description	Es.
0	Nr. sequenza (bit)	SI
1-10	Nome File [caratteri da 1 a 5]	SI
11	Attributo file [0f]	SI
12	Reserved	NO
13	Checksum	SI
14-25	Nome File [caratteri da 6 a 11]	SI
26-27	Reserved	NO
28-31	Nome File [caratteri da 12 a 13]	SI



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 19: L'Analisi *i File System*

(3<sup>a</sup> parte)



A.A. 2021/22

Dott. Lorenzo LAURATO



# File System

» NT File System



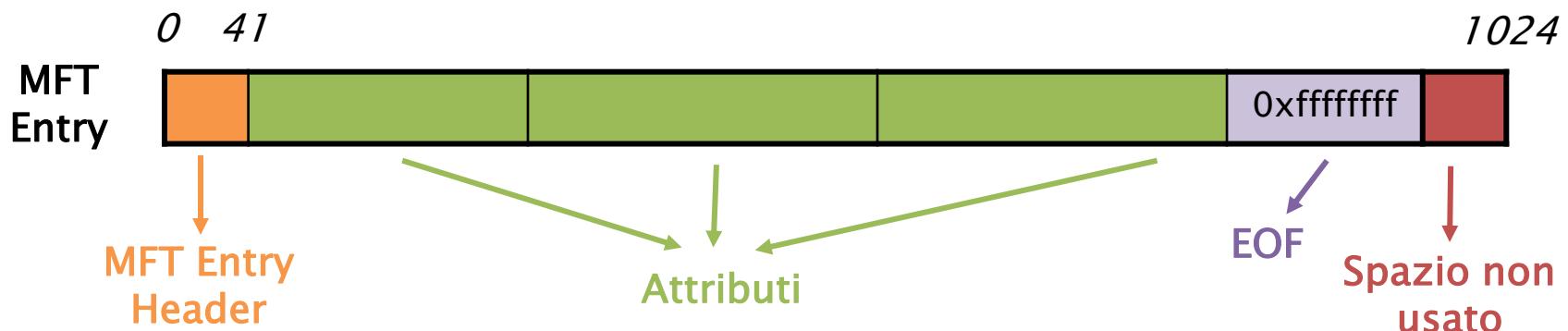
# NT File System

- ▶ New Technologies File System (NTFS)
  - Microsoft 1993
- ▶ Ogni cosa è un file:
  - \$MFT: *Master File Table*
  - \$MFTMirr: *backup della MFT*
  - \$Boot: *boot sector*
  - \$Volume: *informazioni del volume*
  - \$Bitmap: *stato di allocazione dei cluster*
  - \$AttDef: *definizione degli attributi*
  - \$BadClus: *elenco dei cluster danneggiati*
  - \$Secure: *descrittore di sicurezza*
  - \$I30: *Index*
  - ...

# NT File System

## Master File Table (\$MFT)

- ▶ Contiene informazioni sul file e directory:
  - Ogni file/directory ha almeno una entry (*File Record*)
    - 1024 byte (*boot sector*)
  - Entry[0]: \$MFT
- ▶ Starter Cluster (*Boot Sector*)



# NT File System

## Master File Table (\$MFT)

### MFT Entry

- ▶ Dimensione 1024 Byte:
  - Header: 42byte
  - Attributi: *strutture dati*
- ▶ Signature: «FILE» / «BAAD»
- ▶ Stato di allocazione: attributo **\$BITMAP** nella *entry[0]* \$MFT
- ▶ Indirizzo sequenziale: 48bit (*File Number*)
- ▶ Numero sequenziale: 16bit (*contatore allocazione*)

File Reference Address

MFT			
	[...]	Nr. Seq	
312	[...]	0x0003	0003 0000 0000 0312
313	[...]	0x0001	0001 0000 0000 0313
...	[...]	...	[...]

# NT File System

## *Master File Table (\$MFT)*

Byte	Description	Es.
0-3	Signature (ASCII) [FILE BAAD]	NO
4-5	Offset to fixup array	YES
6-7	Number of entries in fixup array	YES
8-15	\$LogFile Sequence Number	NO
16-17	Sequence value	NO
18-19	Link count	NO
20-21	Offset to first attribute	YES
22-23	Flags [01:in use   02:directory]	YES
24-27	Used size of MFT entry	YES
28-31	Allocated size of MFT entry	YES
32-39	File reference to base record	NO
40-41	Next attribute ID	NO
42-1023	Attributes and fixup values	YES

# NT File System

## *Master File Table (\$MFT)*

```
root@caine:/# icat -f ntfs ntfs1.dd 0-128 | xxd
0000000: 4649 4c45 3000 0300 4ba7 6401 0000 0000 FILE0...K.d....
0000016: 0100 0100 3800 0100 b801 0000 0004 0000 ....8.....
0000032: 0000 0000 0000 0000 0600 0000 0000 0000 .....
0000048: 5800 0000 0000 0000 1000 0000 6000 0000 X.....
[...]
0000496: 3101 b43a 0500 0000 ffff ffff 0000 5800 1.....X.
0000512: 0000 0000 0000 0000 0000 0000 0000 0000 .....
[...]
0001008: 0000 0000 0000 0000 0000 0000 5800 .....X.
```

Byte	Description	Value
0-3	Signature (ASCII)	«FILE»
16-17	Sequence value	0001 (1)
18-19	Link count	0001 (1)
20-21	Offset to first attribute	0038 (56)
22-23	Flags [01:in use   02:directory]	0001 (1)
32-39	File reference to base record	0
40-41	Next attribute id	0006 (1)
42-1023	Attributes and fixup values	

# NT File System

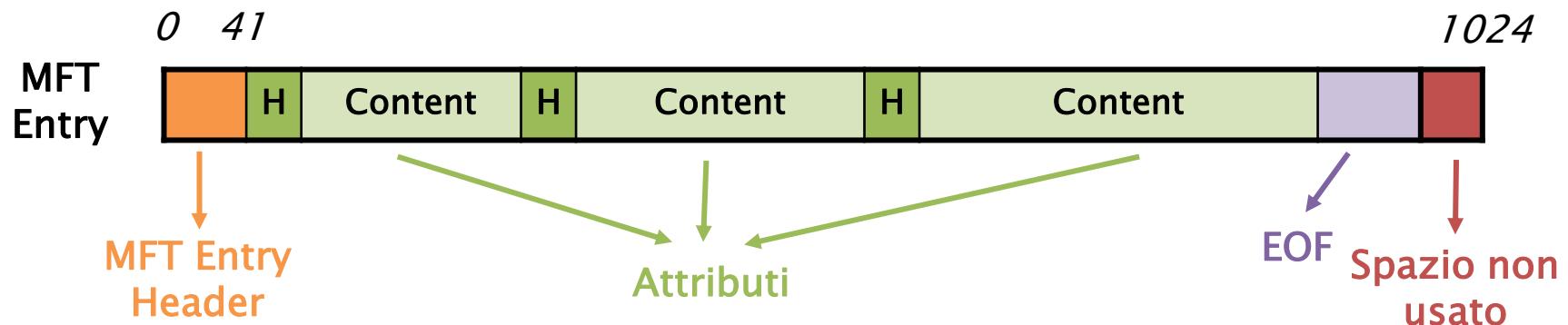
## *File System Metadata*

- ▶ File contenenti dati per l'amministrazione del FS
- ▶ Prime 12 entry MFT

0	\$MFT	MFT Entry
1	\$MFTMirr	MFT Backup
2	\$LogFile	Journal
3	\$Volume	Volume Info
4	\$AttrDef	Attribute info
5	.	Root directory
6	\$Bitmap	Allocation status
7	\$Boot	Boot Sector, BootCode
8	\$BadClus	Cluster that have bad sector
9	\$Secure	Security Info
10	\$Upcase	Uppercase version of every Unicode character
11	\$Extend	Application category

# NT File System

## Attributes



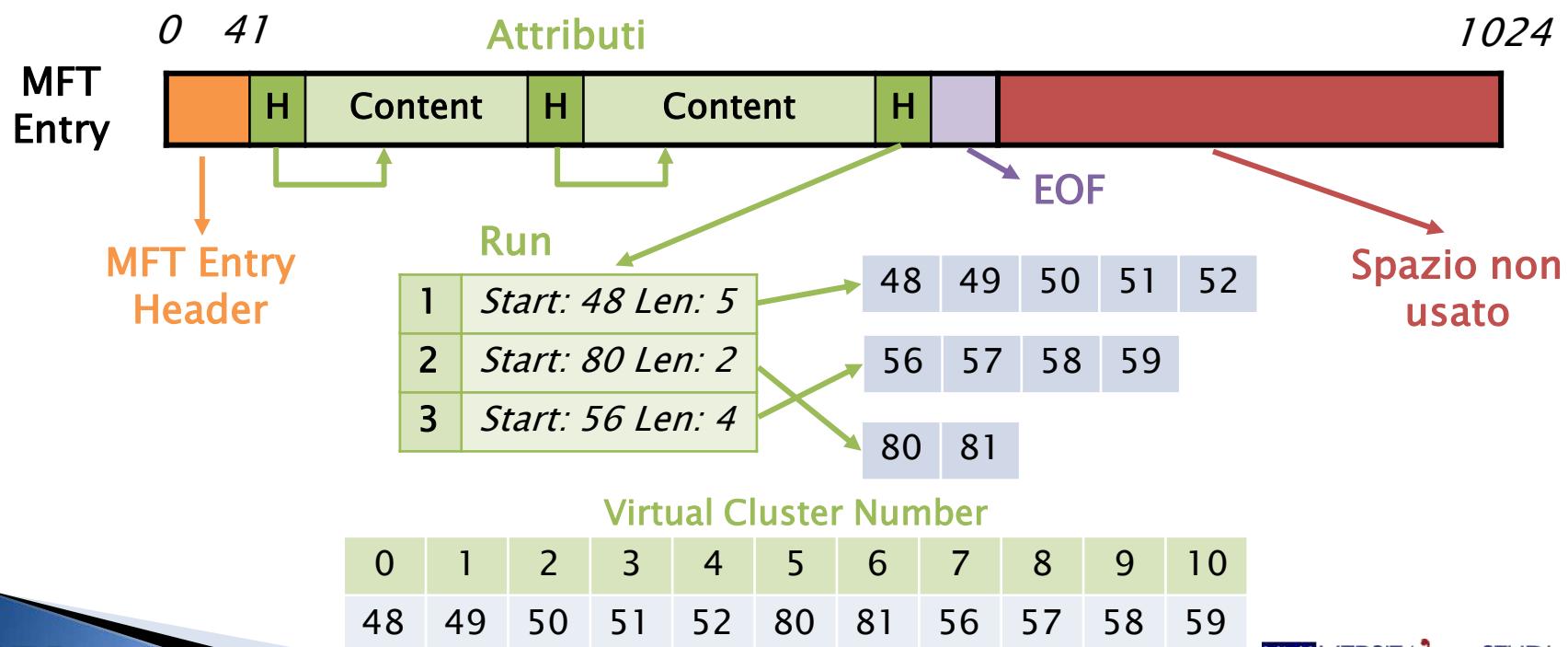
- ▶ **Attribute Header:** descrive l'attributo (*tipo, dimensione, nome*)
  - ID: identificatore univoco nell'entry (16 bit)
  - Type ID: identificatore tipo attributo
  - OFFSet attribute Content

# NT File System

## Attributes

### Attribute Content:

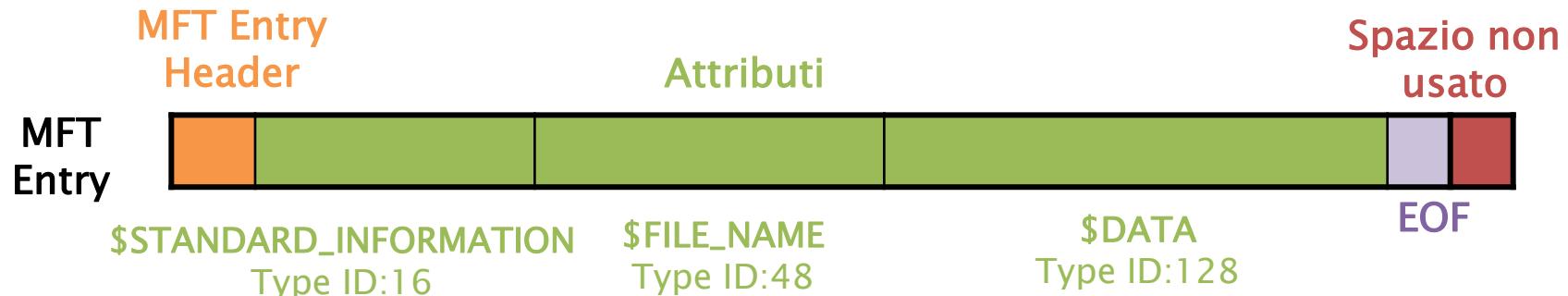
- Residente: viene posizionato all'interno della stessa entry
- Non residente: viene posizionato in cluster esterni
  - *cluster run*: cluster consecutivi



# NT File System

## Standard Attribute Types

- ▶ Definiti nel FS Metadata *\$AttrDef*



16	\$STANDARD_INFORMATION	<i>General information, such as flags; the last accessed, written, and created times; and the owner and security ID</i>
32	\$ATTRIBUTE_LIST	<i>List where other attributes for file can be found</i>
48	\$FILE_NAME	<i>File name, in Unicode, and the last accessed, written, and created times</i>
64	\$VOLUME_VERSION	<i>Volume information</i>
64	\$OBJECT_ID	<i>A 16-byte unique identifier for the file or directory</i>

# NT File System

## *Standard Attribute Types*

80	\$SECURITY_DESCRIPTOR	<i>The access control and security properties of the file</i>
96	\$VOLUME_NAME	<i>Volume name</i>
112	\$VOLUME_INFORMATION	<i>File system version and other flags</i>
128	\$DATA	<i>File contents</i>
144	\$INDEX_ROOT	<i>Root node of an index tree</i>
160	\$INDEX_ALLOCATION	<i>Nodes of an index tree rooted in \$INDEX_ROOT attribute</i>
176	\$BITMAP	<i>A bitmap for the \$MFT file and for indexes</i>
192	\$SYMBOLIC_LINK	<i>Soft link information</i>
192	\$REPARSE_POINT	<i>Contains data about a reparse point</i>
208	\$EA_INFORMATION	<i>Used for backward compatibility with OS/2 applications (HPFS)</i>
224	\$EA	<i>Used for backward compatibility with OS/2 applications (HPFS)</i>
256	\$LOGGED.Utility_Stream	<i>Contains keys and information about encrypted attributes</i>

# NT File System

## *Base/Non-Base MFT Entry*

- ▶ Quando una entry riesce a contenere\descrivere tutti gli attributi per uno specifico file

**Base  
MFT Entry**



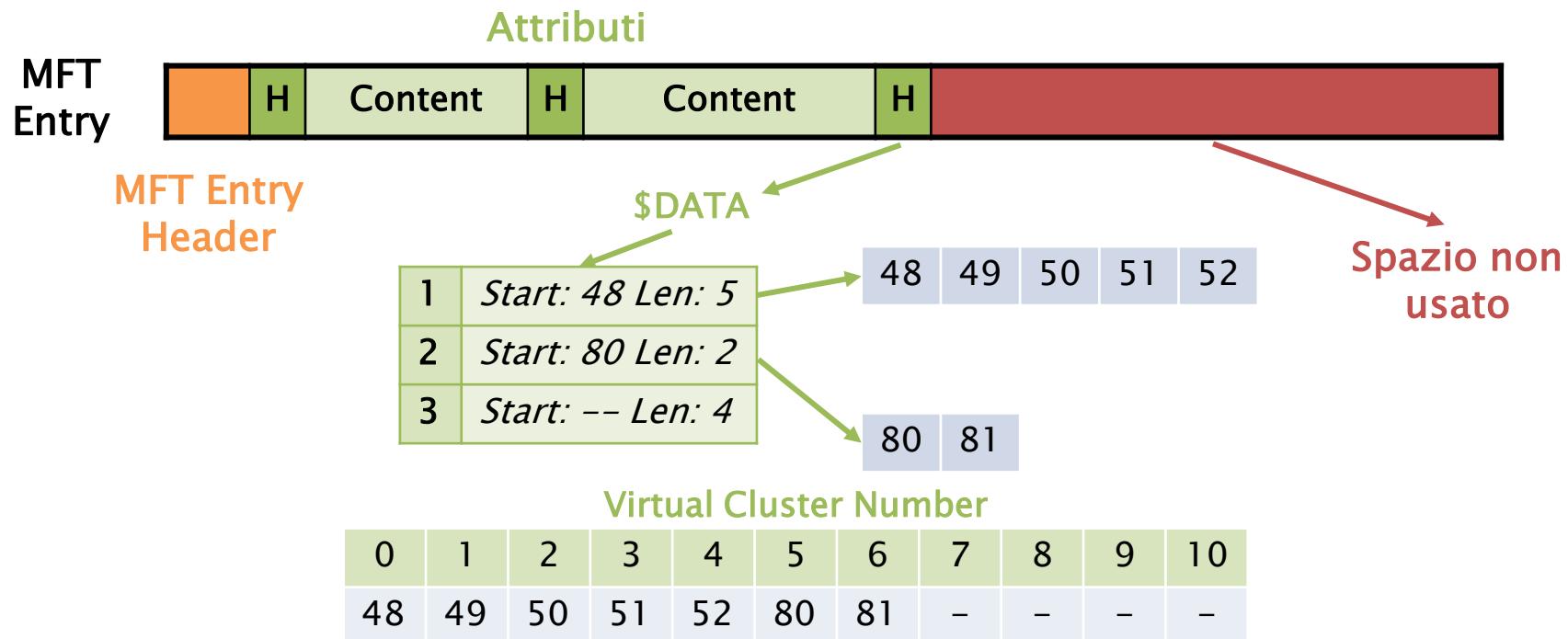
**Non-Base  
MFT Entry**



# NT File System

## *Sparse Attributes*

- ▶ Risparmiare di allocare cluster ZERO per l'attributo \$DATA



# NT File System

## *altre caratteristiche*

- ▶ **Compressione:** gli attributi non residenti \$DATA
- ▶ **Indicizzazione:** collezione di attributi memorizzata in maniera ordinata (B-Tree)

# NT File System

## Attribute Header

Byte	Description	Es.
0-3	Attribute type ID	YES
4-7	Length of attribute	YES
8	Non-resident flag	YES
9	Length of name	YES
10-11	Offset to name	YES
12-13	Flags	YES
14-15	Attribute identifier	YES
16-19	Size of content	YES
20-21	Offset to content	YES

Flags	
0x0001	compressed
0x4000	encrypted
0x8000	sparse



Resident Attribute

# NT File System

## *Resident Attribute Header*

### ▶ Starter Byte 56:

```
0000000: 1000 0000 6000 0000 0000 1800 0000 0000 . . . . .  
0000016: 4800 0000 1800 0000 305a 7a1f f63b c301 H. . . . 0Zz. . .
```

Byte	Description	Value
0-3	Attribute type ID	00000010 (16) \$STANDARD_INFORMATION
4-7	Length of attribute	00000060 (96)
8	Non-resident flag	00 (0)
9	Length of name	00 (0)
12-13	Flags	0000 (0)
14-15	Attribute ID	0000 (0)
16-19	Size of content	00000048 (72)
20-21	Offset to content	0018 (24)

# NT File System

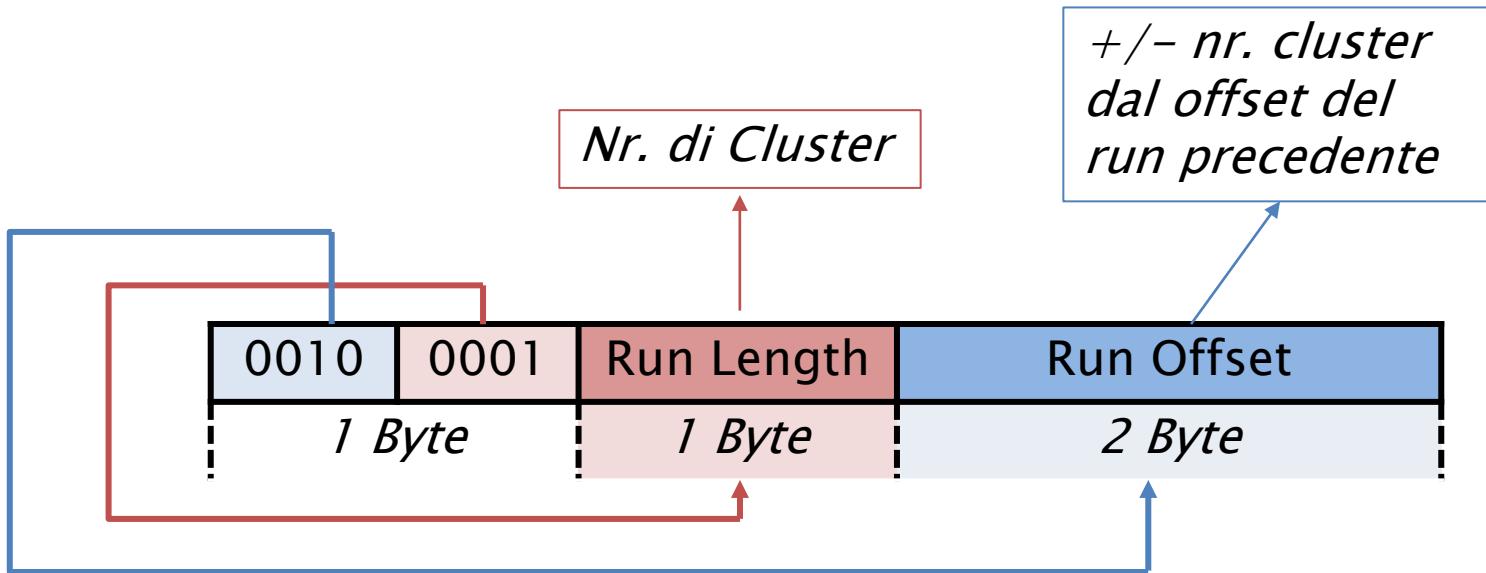
## *Attribute Header*

Byte	Description	Es.
0-15	General Header	YES
16-23	Starting Virtual Cluster Number (VCN) of the runlist	YES
24-31	Ending VCN of the runlist	YES
32-33	Offset to the runlist	YES
34-35	Compression unit size	YES
36-39	Unused	NO
40-47	Allocated size of attribute content	NO
48-55	Actual size of attribute content	YES
56-63	Initialized size of attribute content	NO

Non-Resident  
Attribute

# NT File System

## Run



# NT File System

## *Non-Residente Attribute Header*

### ▶ Attributo \$DATA:

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 .....`.....@.....
0000016: 0000 0000 0000 0000 ef20 0000 0000 0000 .....`.....@.....
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @.....`.....@.....
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 .....`.....@.....
0000064: 32c0 1eb5 3a05 2170 1b1f 2290 015f 7e31 2.....!p..!"...~1
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v..!.....n.HD~.
```

Byte	Description	Value
0-3	Attribute type ID	00000080 (128) \$DATA
4-7	Length of attribute	00000060 (96)
8	Non-resident flag	01 (1)
9	Length of name	00 (0)
12-13	Flags	0000 (0)
14-15	Attribute identifier	0001 (1)
16-23	Starting VCN runlist	0
24-31	Ending VCN runlist	20ef (8.431)

# NT File System

## *Non-Residente Attribute Header*

### ▶ Attributo \$DATA:

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 ....`.....@.....
0000016: 0000 0000 0000 0000 ef20 0000 0000 0000 ..... .
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @.....
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 ..... .
0000064: 32c0 1eb5 3a05 2170 1b1f 2290 015f 7e31 2...!:p..!"...~1
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v..!....n.HD~.
```

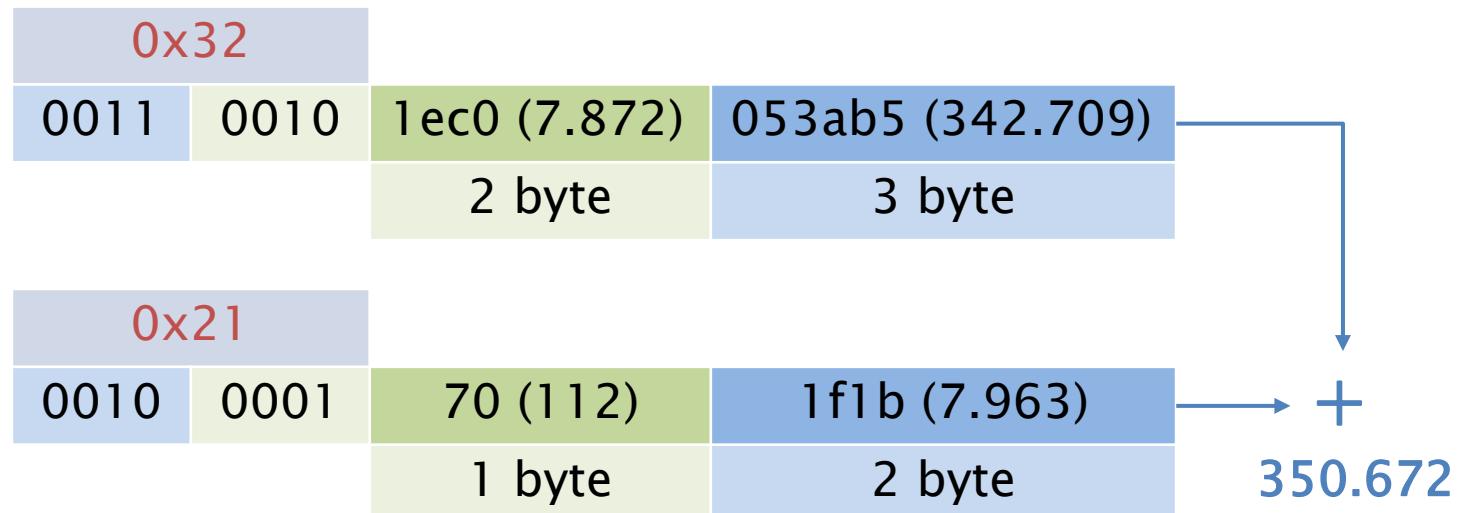
Byte	Description	Value
32-33	Offset to the runlist	0040 (64)
40-47	Allocated size of attribute content	0083c000 (8.634.368)
48-55	Actual size of attribute content	0083c000 (8.634.368)
56-63	Initialized size of attribute content	0083c000 (8.634.368)

# NT File System

## *Non-Residente Attribute Header*

### ▶ Run List:

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 ....`.....@....  
0000016: 0000 0000 0000 0000 ef20 0000 0000 0000 ..... . ....  
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @..... . ....  
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 ..... . ....  
0000064: 32c0 1eb5 3a05 2170 1b1f 2290 015f 7e31 2....!p..!"...~1  
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v..!....n.HD~.
```



# NT File System

## *File System Category*

### File System Metadata \$MFT File

- ▶ contiene la Master File Table
  - Cluster Iniziale: Boot Sector
- ▶ Layout:
  - ≥ Windows 7: cluster 786432 (0x0C0000)
- ▶ Entry[0] di MFT
  - \$DATA: cluster usati
  - \$BITMAP: stato di allocazione delle entry

# NT File System

## *File System Category*

### File System Metadata \$MFT File

```
root@caine:/# istat -f ntfs ntfs1.dd 0

        [...]
$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0 Security ID: 256
Created: Thu Jun 26 10:17:57 2003
File Modified: Thu Jun 26 10:17:57 2003
MFT Modified: Thu Jun 26 10:17:57 2003
Accessed: Thu Jun 26 10:17:57 2003
        [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 74
Type: $DATA (128-1) Name: $Data Non-Resident size: 8634368
342709 342710 342711 342712 342713 342714 342715 342716
342717 342718 342719 342720 342721 342722 342723 342724
        [...]
443956 443957 443958 443959 443960 443961 443962 443963

Type: $BITMAP (176-5) Name: N/A Non-Resident size: 1056
342708 414477 414478 414479
```

# NT File System

## *File System Category*

### File System Metadata \$MFTMirr File

- ▶ Copia di backup della Master File Table
  - Prime 4 entry: *\$MFT, \$MFTMirr, \$LogFile, \$Volume*
- ▶ Entry[1] di MFT
- ▶ Layout:
  - ≥ Windows 7: dopo il Boot Sector (16° settore)
  - < Windows 7: a metà del File System

# NT File System

## *File System Category*

### File System Metadata \$MFTMirr File

```
root@caine:/# istat -f ntfs ntfs1.dd 1
```

```
[...]
```

Attributes:

```
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
```

```
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
```

```
Type: $DATA (128-1) Name: $Data Non-Resident size: 4096
```

```
514064 514065 514066 514067
```

# NT File System

## *File System Category*

### File System Metadata \$Boot File

- ▶ **Boot Sector**
  - Dimensione dei cluster
  - Nr. settori del File System
  - Layout MFT
    - Cluster iniziale
    - Dimensione entry
- ▶ **Entry[7] di MFT**
- ▶ **Layout:** primi 16 settori del File System
  - Signature: *0xAA55*

# NT File System

## \$Boot File

Byte	Description	Es.
0-2	Istruzioni assembly per saltare al bootcode	NO
3-10	OEM Name (ASCII)	NO
11-12	Dimensione settore (Byte)	YES
13	Dimensione Cluster (Settori)	YES
14-15	Settori riservati	NO
16-20	Non usati	NO
21	Descrizione Media	NO
22-23	Non usati	NO
24-31	Non usati	NO
32-35	Non usati	NO
36-39	Non usati	NO
40-47	Tot. settori FS	YES
48-55	Indirizzo del cluster iniziale di MFT	YES
56-63	Indirizzo del cluster iniziale di MFT Mirror	NO

# NT File System

## \$Boot File

Byte	Description	Es.
64	Dimensione delle entry MFT	YES
65-67	Non usati	NO
68	Dimensione dei record dell'index	YES
69-71	Non usati	NO
72-79	Serial Number	NO
80-83	Non usati	NO
84-509	Boot Code	NO
510-511	Signature (0xaa55)	NO

# NT File System

## *File System Category*

### File System Metadata \$Boot File

```
root@caine:/# istat -f ntfs ntfs1.dd 7
```

```
[...]
```

Attributes:

Type: \$STANDARD\_INFORMATION (16-0) Name: N/A Resident size: 48

Type: \$FILE\_NAME (48-2) Name: N/A Resident size: 76

Type: \$SECURITY\_DESCRIPTOR (80-3) Name: N/A Resident size: 104

Type: \$DATA (128-1) Name: \$Data Non-Resident size: 8192

0 1 2 3 4 5 6 7

# NT File System

## *File System Category*

### File System Metadata \$Volume File

- ▶ **Informazioni sul volume:**
  - etichetta
  - versione
- ▶ **Entry[3] di MFT:**
  - \$VOLUME\_NAME: nome in UNICode del volume
    - ID Type: 96
  - \$VOLUME\_INFORMATION:
    - versione di NTFS
    - dirty status
  - \$DATA: 0 Byte

# NT File System

## *\$VOLUME\_INFORMATION Attribute*

Type ID 112

Byte	Description	Es.
0-7	Unused	NO
8	Major version	YES
9	Minor version	YES
10-11	Flags	NO

Flags	
0x0001	Dirty
0x0002	Resize \$LogFile
0x0004	Upgrade volume next time
0x0008	Mounted in NT
0x0010	Deleting change journal
0x0020	Repair object IDs
0x8000	Modified by chkdsk

# NT File System

## *File System Category*

### File System Metadata \$Volume File

```
root@caine:/# istat -f ntfs ntfs1.dd 3
```

```
[...]
```

Attributes:

```
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-1) Name: N/A Resident size: 80
Type: $OBJECT_ID (64-6) Name: N/A Resident size: 16
Type: $SECURITY_DESCRIPTOR (80-2) Name: N/A Resident size: 104
Type: $VOLUME_NAME (96-4) Name: N/A Resident size: 22
Type: $VOLUME_INFORMATION (112-5) Name: N/A Resident size: 12
Type: $DATA (128-3) Name: $Data Resident size: 0
```

# NT File System

## *File System Category*

### File System Metadata \$AttrDef File

- ▶ definisce gli attributi:
  - Nomi
  - Type ID
- ▶ Entry[4] di MFT

# NT File System

## \$AttrDef File

Byte	Description	Es.
0-127	Name of attribute	YES
128-131	Type identifier	YES
132-135	Display rule	NO
136-139	Collation rule	NO
140-143	Flags	YES
144-151	Minimum size	NO
152-159	Maximum size	NO

Flags	
0x02	Attribute can be used in an index
0x04	Attribute is always resident
0x08	Attribute can be non-resident

# NT File System

## *File System Category*

### File System Metadata \$AttrDef File

```
root@caine:/# istrat -f ntfs ntfs1.dd 4
```

```
[...]
```

Attributes:

```
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
```

```
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
```

```
Type: $SECURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 104
```

```
Type: $DATA (128-4) Name: $Data Non-Resident size: 2560
```

```
342701 342702 342703
```

# NT File System

## *File System Category: Analisi*

- 1) Processare il primo settore del File System: Boot Sector
  - Layout MFT
- 2) Processare la MFT[0]:
  - \$MFTMirr
- 3) Processare \$Volume
- 4) Processare \$AttrDef
- 5) Processare le altre entry MFT

# NT File System

## *Content Category*

- ▶ Contenuto degli attributi:
  - Residenti: all'interno delle entry MFT
  - Non Residenti: cluster esterni
- ▶ Cluster:
  - Cluster[0] = settore[0] del File System
    - Settore= Cluster x Settori\_Cluster

# NT File System

## *Content Category*

### File System Metadata \$Bitmap File

- ▶ Informazioni sullo stato di allocazione dei cluster
  - Bit[x]=cluster[x]
    - Bit[x]=1 cluster x è allocato
    - Bit[x]=0: cluster x non è allocato
- ▶ Entry[6] di MFT

# NT File System

## *Content Category*

### File System Metadata \$Bitmap File

```
root@caine:/# istat -f ntfs ntfs1.dd 6
[...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 80
Type: $DATA (128-1) Name: $Data Non-Resident size: 128520
514113 514114 514115 514116 514117 514118 514119 514120
514121 514122 514123 514124 514125 514126 514127 514128
[...]
```

# NT File System

## *Content Category*

### File System Metadata \$BadClus File

- ▶ traccia i cluster con settori danneggiati
- ▶ Entry[8] di MFT
  - \$DATA= «\$Bad»
    - Flag = Sparse
    - Size = File System

# NT File System

## *Content Category*

### File System Metadata \$BadClus File

```
root@caine:/# istat -f ntfs ntfs1.dd 8
```

```
[...]
```

Attributes:

```
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 82
Type: $DATA (128-2) Name: $Data Resident size: 0
Type: $DATA (128-1) Name: $Bad Non-Resident size: 1052803072
```

# NT File System

## *Content Category: Layout*

- ▶ Diverso a seconda della versione NTFS
- ▶ Zona MFT
  - Settori consecutivi riservati per MTF:
    - 12,5% del File System
- ▶ Boot Sector: primo settore
  - File System Metadata File dopo il Boot Sector



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 20: L'Analisi *i File System*

(4<sup>a</sup> parte)



A.A. 2021/22

Dott. Lorenzo LAURATO



# File System

» NT File System



# Nella lezione precedente...

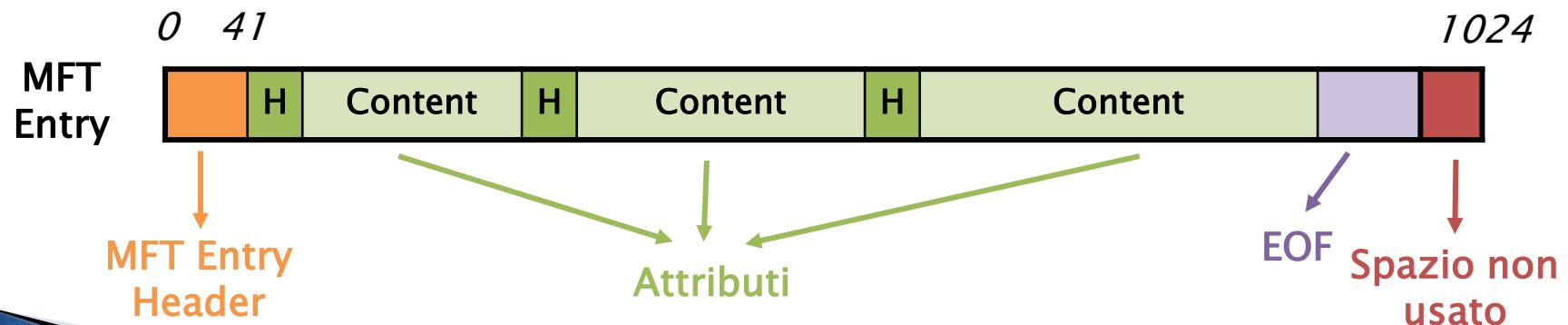
- ▶ NTFS gestisce tutto con i file
- ▶ Master File Table (MFT):
  - prime 12 entry:

0	<b>\$MFT</b>	MFT Entry
1	<b>\$MFTMirr</b>	MFT Backup
2	<b>\$LogFile</b>	Journal
3	<b>\$Volume</b>	Volume Info
4	<b>\$AttrDef</b>	Attribute info
5	.	Root directory
6	<b>\$Bitmap</b>	Allocation status
7	<b>\$Boot</b>	Boot Sector, BootCode
8	<b>\$BadClus</b>	Cluster that have bad sector
9	<b>\$Secure</b>	Security Info
10	<b>\$Upcase</b>	Uppercase version of every Unicode character
11	<b>\$Extend</b>	Application category

# Nella lezione precedente...

## ▶ Entry MFT:

- Header MFT: 42byte
- Attributi:
  - *Header*
  - *Content:*
    - *Residente*
    - *Non residente: Cluster Run*



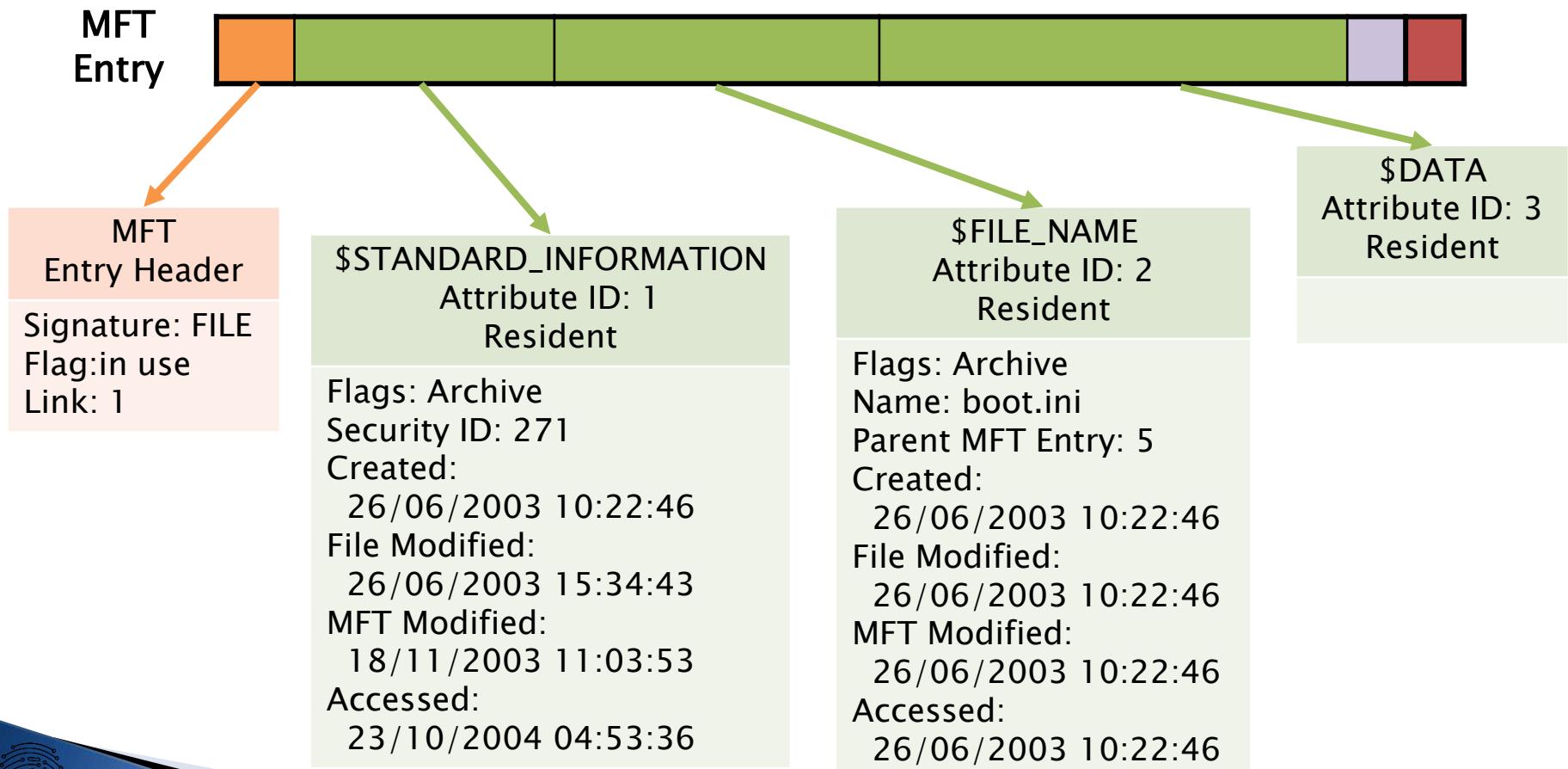
# Nella lezione precedente...

- ▶ File System Category:
  - File System Metadata File:
    - \$MFTMirr
    - \$BootFile:
    - \$Volume
    - \$AttrDef
- ▶ Content Category
  - Attributo \$Data
  - FS Metadata File:
    - \$BitMap
    - \$BadClus

# NT File System

## *Metadata Category*

- ▶ Reperibili dagli attributi:



# NT File System

## *Metadata Category*

### \$STANDARD\_INFORMATION Attribute

- ▶ Esiste per ogni file e directory
- ▶ Contiene i metadati principali:
  - Informazioni temporali
  - Proprietà
  - Sicurezza e quota
- ▶ Type ID: 16

# NT File System

## *\$STANDARD\_INFORMATION Attribute*

Byte	Description	Es.
0–7	Creation time	NO
8–15	File altered time	NO
16–23	MFT altered time	NO
24–31	File accessed time	NO
32–35	Flags	NO
36–39	Maximum number of versions	NO
40–43	Version number	NO
44–47	Class ID	NO
48–51	Owner ID	NO
52–55	Security ID	NO
56–63	Quota Charged	NO
64–71	Update Sequence Number (USN)	NO

# NT File System

## *Metadata Category*

### \$STANDARD\_INFORMATION Attribute

- ▶ Quattro valori temporali (timestamp):
  - Data di creazione: creazione del file
  - Data di ultima modifica: modifica del contenuto degli attributi \$DATA e \$INDEX
  - Data di ultima modifica MFT: modifica dei metadati del file
  - Data di ultimo accesso: accesso al contenuto del file

# NT File System

## *\$STANDARD\_INFORMATION Attribute*

Byte	Description	Es.
0-7	Creation time	NO
8-15	File altered time	NO
16-23	MFT altered time	NO
24-31	File accessed time	NO
32-35	Flags	NO
36-39	Maximum number of versions	NO
40-43	Version number	NO
44-47	Class ID	NO
48-51	Owner ID	NO
52-55	Security ID	NO
56-63	Quota Charged	NO
64-71	Update Sequence Number (USN)	NO

Flags	
0x0001	Read Only
0x0002	Hidden
0x0004	System
0x0020	Archive
0x0040	Device
0x0080	#Normal
0x0100	Temporary
0x0200	Sparse file
0x0400	Reparse point
0x0800	Compressed
0x1000	Offline
0x2000	Content is not being indexed for faster searches
0x4000	Encrypted

# NT File System

## *Metadata Category*

### **\$FILE\_NAME Attribute**

- ▶ Ogni file e directory ha almeno un attributo \$FILE\_NAME
- ▶ Dimensione: 66byte + lunghezza nome
- ▶ Type ID: 48
- ▶ Riferimento al Parent Directory

# NT File System

## *\$FILE\_NAME Attribute*

Namespace	
0	POSIX: The name is case sensitive and allows all Unicode characters except for '/' and NULL.
1	Win32: The name is case insensitive and allows most Unicode characters except for special values such as '/', '\', ':', '>', '<', and '?'.
2	DOS: The name is case insensitive, upper case, and no special characters. The name must have eight or fewer characters in the name and three or less in the extension
3	Win32 & DOS: Used when the original name already fits in the DOS namespace and two names are not needed.

# NT File System

## *\$FILE\_NAME Attribute*

Byte	Description	Es.
0-7	File reference of parent directory	NO
8-15	File creation time	NO
16-23	File modification time	NO
24-31	MFT modification time	NO
32-39	File accessed time	NO
40-47	Allocated size of file	NO
48-55	Real size of file	NO
56-59	Flags	NO
60-63	Reparse value	NO
64	Length of name	NO
65	Namespace	NO
66+	Name	NO

Flags	
0x0001	Read Only
0x0002	Hidden
0x0004	System
0x0020	Archive
0x0040	Device
0x0080	#Normal
0x0100	Temporary
0x0200	Sparse file
0x0400	Reparse point
0x0800	Compressed
0x1000	Offline
0x2000	Content is not being indexed for faster searches
0x4000	Encrypted

# NT File System

## *Metadata Category*

### \$DATA Attribute

- ▶ Impiegato per memorizzare qualsiasi forma di dati:
  - Non ha formato e valori definiti
- ▶ Dimensione:  $\geq 0$  Byte
  - >700Byte: non residente
- ▶ Type ID: 128
- ▶ Alternative Data Stream (ADS): attributi \$DATA aggiuntivi
  - Es.: C:\> echo «Ciao a tutti»>file.txt:pippo

# NT File System

## *Metadata Category*

### \$ATTRIBUTE\_LIST Attribute

- ▶ Lista degli attributi nella entry:
  - Quando un file/directory necessita di più entry per gli attributi
  - Tipo di attributo->Posizione della entry che lo contiene
- ▶ Type ID: 32

# NT File System

## *\$ATTRIBUTE\_LIST Attribute*

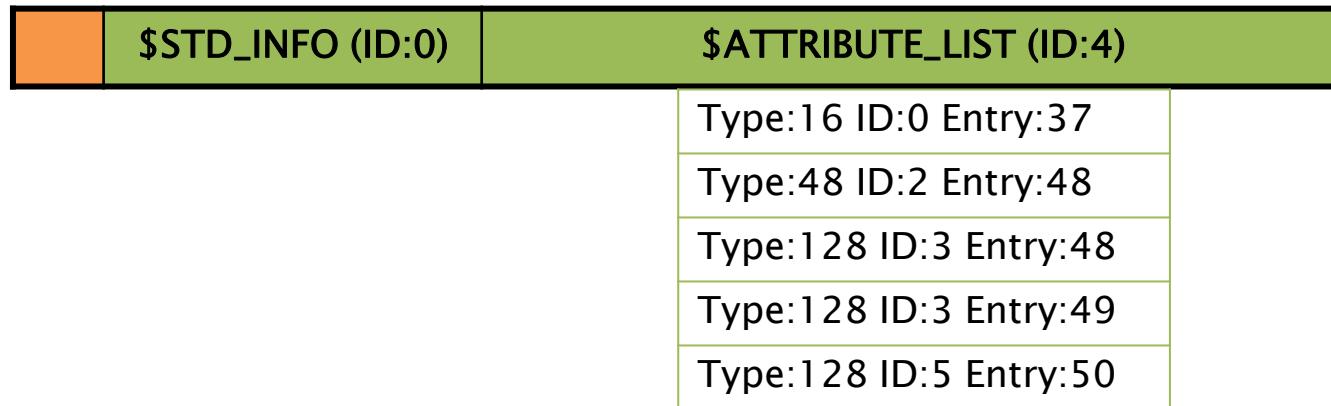
Byte	Description	Es.
0–3	Attribute type	YES
4–5	Length of this entry	YES
6	Length of name	YES
7	Offset to name (relative to start of this entry)	YES
8–15	Starting VCN in attribute	YES
16–23	File reference where attribute is located	YES
24	Attribute ID	YES

# NT File System

## *Metadata Category*

### \$ATTRIBUTE\_LIST Attribute

37



48



49



50



# NT File System

## *Metadata Category*

### \$SECURITY\_DESCRIPTOR Attribute

- ▶ descrive i criteri di controllo dell'accesso che devono essere applicati a un file o una directory
- ▶ Type ID: 80

Solo versioni NTFS < 3.0

# NT File System

## *Metadata Category*

### File System Metadata \$Secure File

- ▶ descrive i criteri di controllo dell'accesso che devono essere applicati a un file o una directory
- ▶ Entry[9] di MFT
  - Indice \$SDH
  - Indice \$SII
  - attributo \$DATA (\$SDS).
- ▶ Ogni File\Directory
  - \$STANDARD\_INFORMATION:
    - Security ID: Indice nel \$Secure File

Solo versioni NTFS  $\geq 3.0$

# NT File System

## *Metadata Category*

### Algoritmi di allocazione

- ▶ Allocazione delle Entry MFT:
  - Strategia del primo disponibile: dalla entry 24
  - Allocato->Non allocato: cambio della flag «in uso»
  - Non Allocato->Allocato: pulizia della entry
- ▶ Allocazione degli attributi:
  - riduzione dell'ultimo attributo (\$DATA)
  - Crescita dell'attributo: residente->non residente

# NT File System

## *Metadata Category*

### Aggiornamento informazioni temporali

▶ **\$FILE\_NAME:**

- Aggiornamento creazione/spostamento file

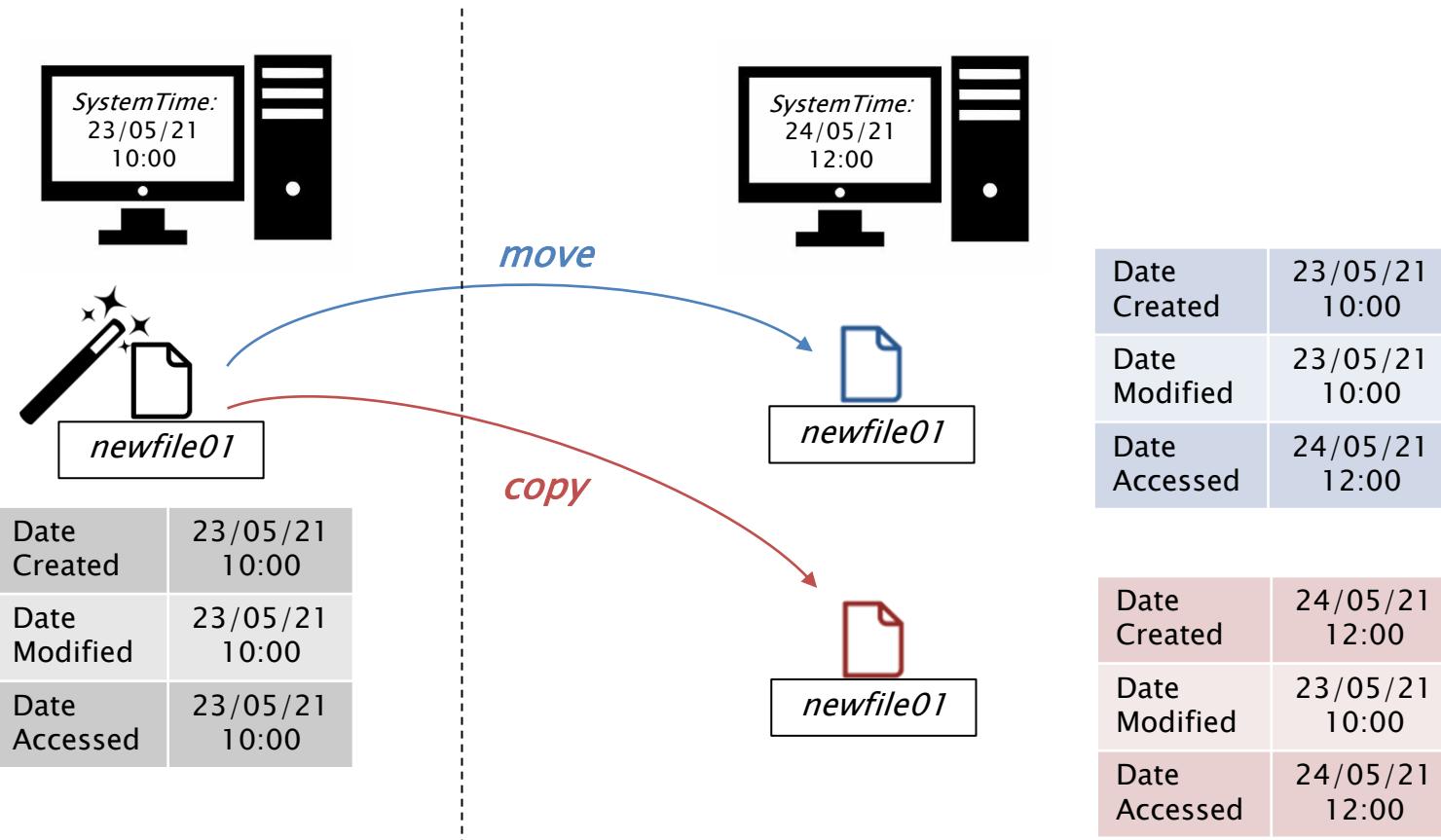
▶ **\$STANDARD\_INFORMATION:**

- Data di creazione: creazione nuovo file o copia
- Data di ultima modifica: variazione degli attributi DATA, \$INDEX\_ROOT o \$ INDEX\_ALLOCATION
- Data di ultima modifica MFT: modifica degli attributi
- Data di accesso: viene fatto accesso alla entry (metadati o contenuto)

# NT File System

## *Metadata Category*

### Aggiornamento informazioni temporali



# NT File System

## *Metadata Category: Analisi*

### 1) Individuazione di una entry MFT:

- individuare la MFT tramite il boot sector

### 2) elaborazione del contenuto della entry:

- Elaborazione degli attributi:
  - STANDARD\_INFORMATION
  - \$DATA:
    - NON RESIDENTE: Processare la RUNLIST
  - \$FILE\_NAME
- Elaborazione delle possibili entry secondarie:
  - \$ATTRIBUTE\_LIST

# NT File System

## *File Name Category*

- ▶ Correlazione dei nomi: indici
  - Raccolta di strutture dati ordinate per chiave
- ▶ Struttura B-Tree:
  - Nodi:
    - \$INDEX\_ROOT: radice dell'albero
    - \$INDEX\_ALLOCATION: indici utilizzati

# NT File System

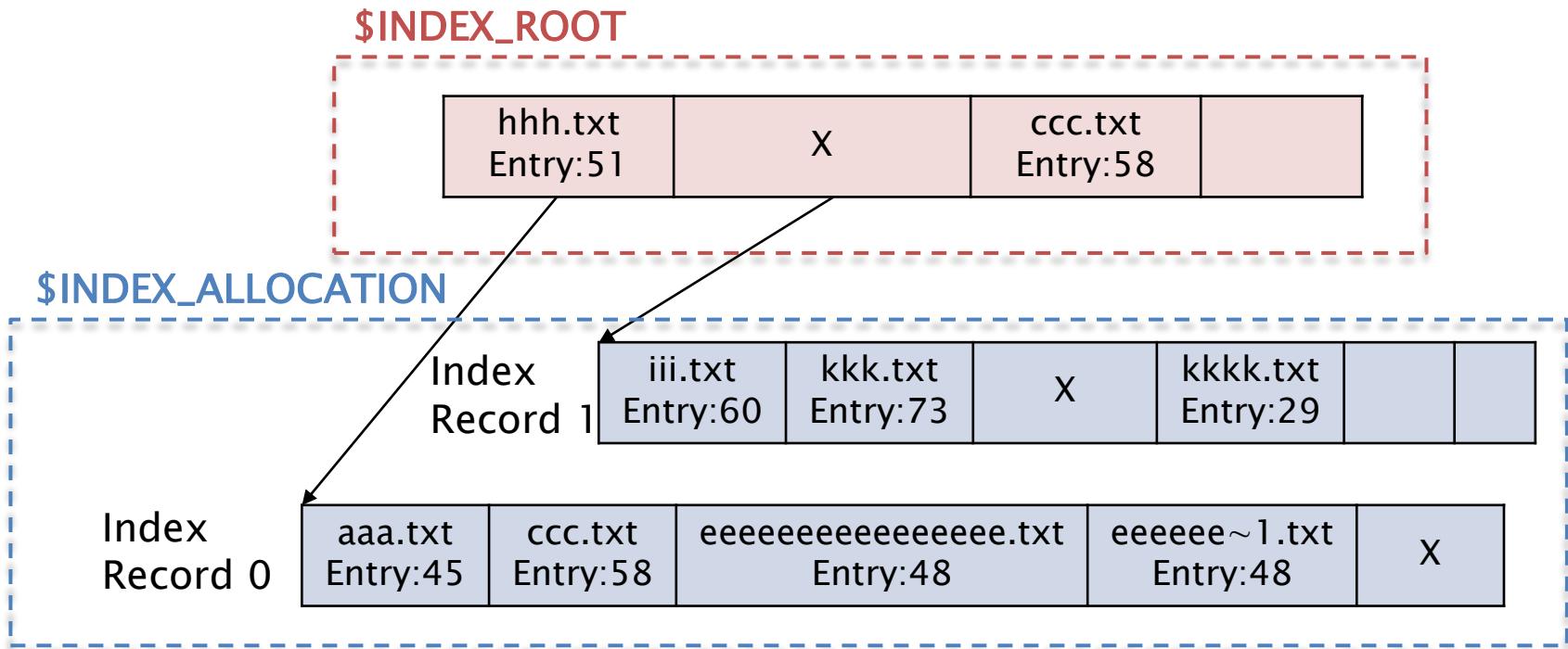
## *Directory Index Entry Data Structure*

Byte	Description	Es.
0–7	MFT file reference for file name	YES
8–9	Length of this entry	YES
10–11	Length of \$FILE_NAME attribute	NO
12–15	Flags	YES
16+	\$FILE_NAME Attribute	YES
Last 8	VCN of child node in \$INDEX_ALLOCATION	YES

# NT File System

## *File Name Category*

### Directory Indexes



# NT File System

## *File Name Category*

### Root directory

- ▶ ENTRY[5] di MFT
  - Nome: « . »
- ▶ risiedono tutti i «File System Metadata File»

# NT File System

## *Application Category*

### Disk Quotas (\$Quota)

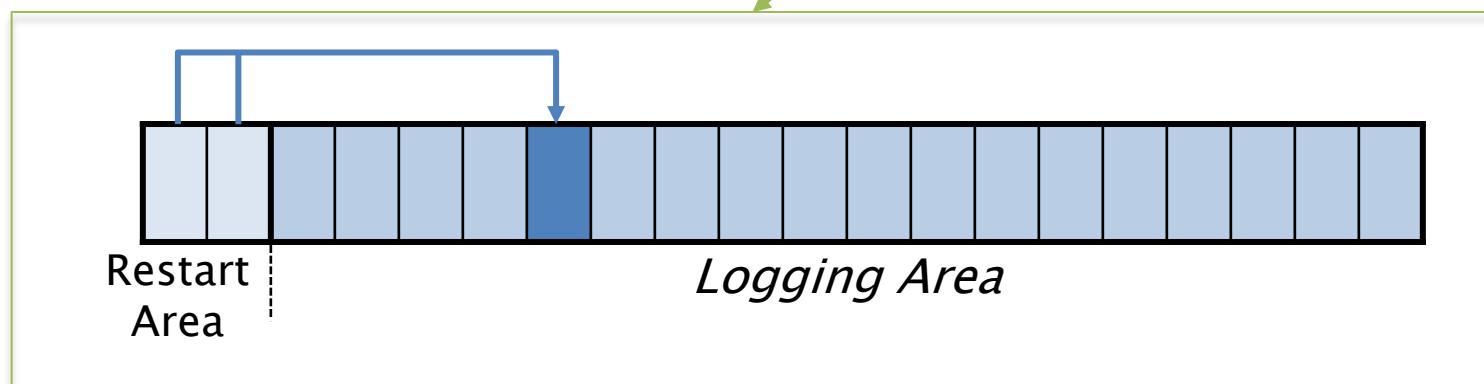
- ▶ Supporto alle quote di spazio su disco:
  - Limitare lo spazio allocata ad un utente
- ▶ Dati nel File System:
  - NTFS vers. < 3.0: Entry[9] di MFT
    - \\$Quota
  - NTFS vers.  $\geq 3.0$ : qualsiasi posizione di MFT
    - \\$Extend directory
- ▶ Registro di Windows

# NT File System

## *Application Category*

### Logging/Journaling (\$LogFile)

- ▶ Consente di mantenere il File System in uno stato di consistenza
- ▶ Entry[2] di MFT



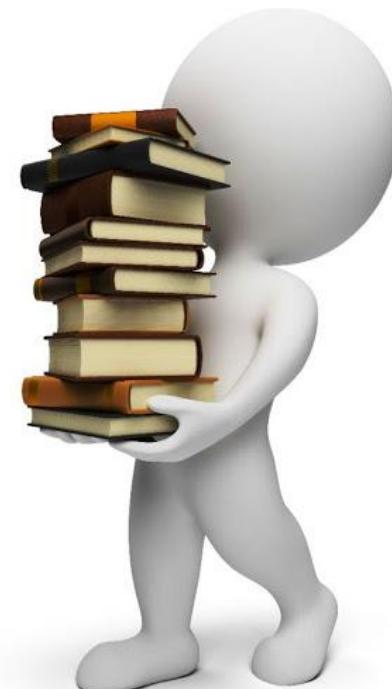
# NT File System

## Analisi: *File Recovery*

- ▶ Eliminazione file:
  - File name eliminato dall'index directory
  - Recupero entry MFT: attributo \$FILE\_NAME (Parent Directory)
  - Controllare la presenza di ulteriori \$DATA (ADS)

# Bibliografia

- ▶  **File System Forensics Analysis**  
Brian Carrier – (2005)  
Addison Wesley Professional





## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 21: L'Analisi *i sistemi operativi*



A.A. 2021/22

Dott. Lorenzo LAURATO



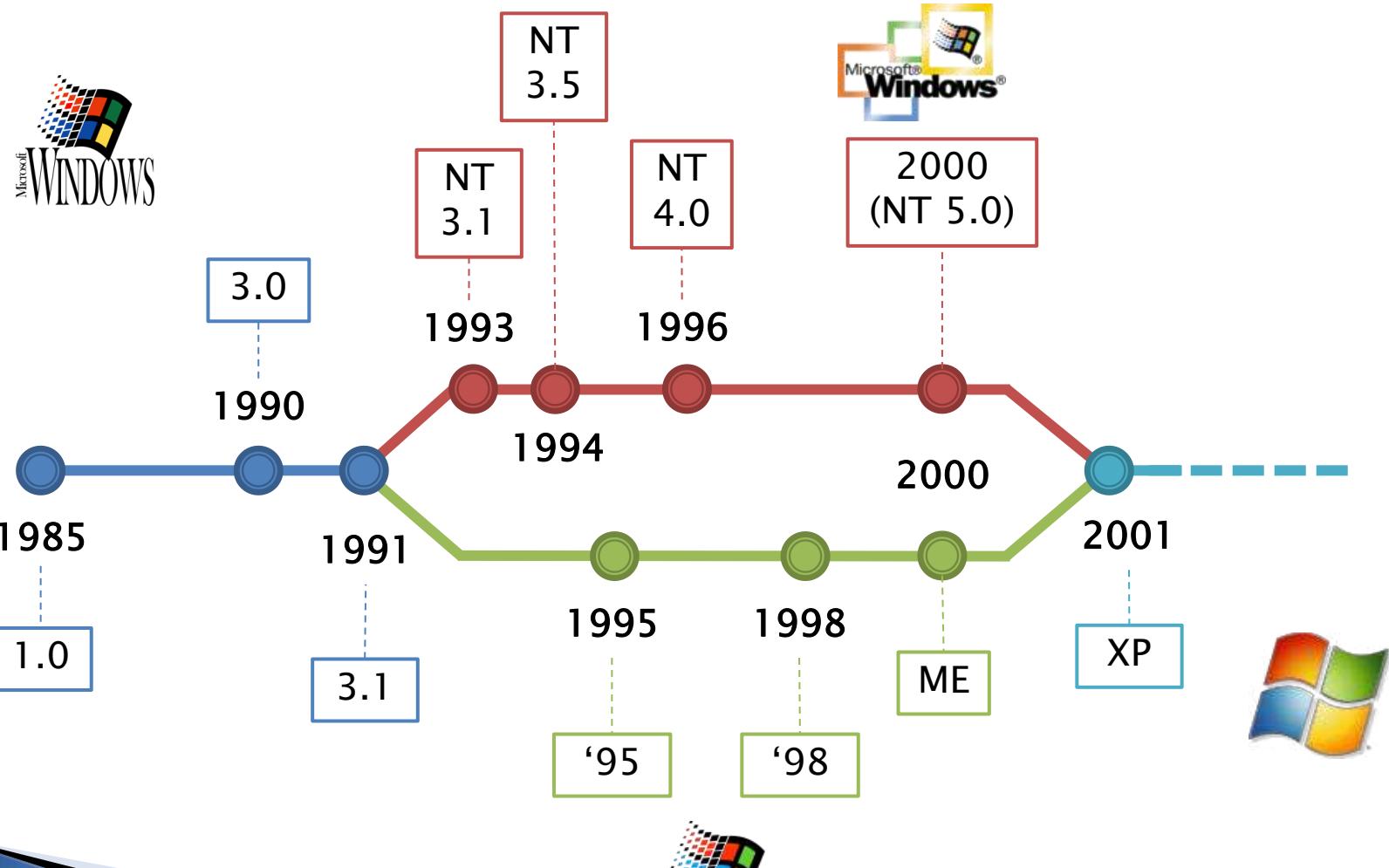
# Sistemi Operativi

» Microsoft Windows



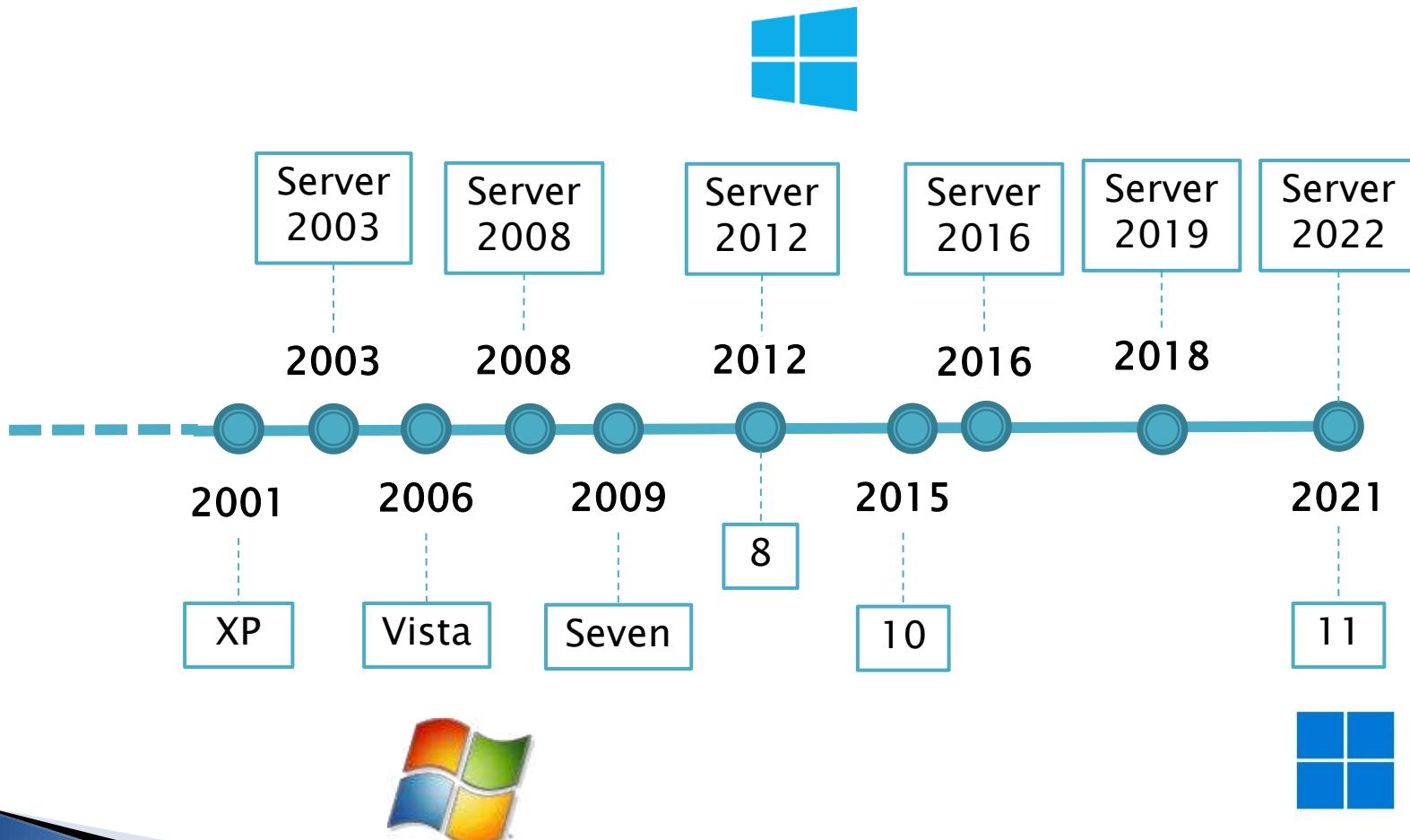
# Microsoft Windows

## *storia*



# Microsoft Windows

## *storia*



# Microsoft Windows

## *users*



### ▶ Account locali:

- accesso al singolo sistema
- autenticazione locale

### ▶ Account di dominio:

- accesso a tutti sistemi attestati
- autenticazione tramite Domain Controller

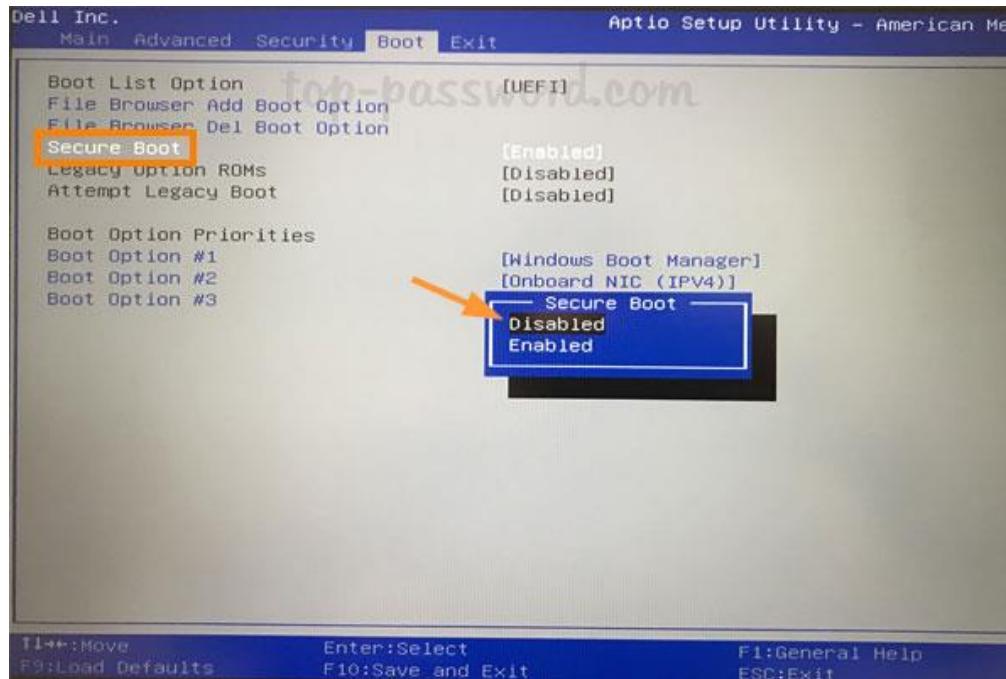
### ▶ Account online:

- accesso a tutti i sistemi attestati
- autenticazione tramite account Microsoft

# Microsoft Windows

## *secure boot*

- ▶ UEFI
- ▶ Avvio solo di S.O. Microsoft
  - è *disabilitabile*



# Microsoft Windows

## *Registro di Sistema*



- ▶ *Impostazioni del S.O. e di Programmi installati.*
- ▶ **Windows 95/98:**
  - User.dat:
    - \Windows
    - \Windows\Profiles\[user\_name]
  - System.dat:
    - \Windows
- ▶ **Windows ≥ XP:**
  - Software, System, SAM, Security, Default:
    - \Windows\system32\config
  - NTuser.dat:
    - \Documents and Settings\[user\_name] (*Windows XP*)
    - \Users\[user\_name] (*Windows ≥ Vista*)

# Microsoft Windows

## *Registro di Sistema*



- ▶ Struttura ad albero con cinque sotto-alberi principali (**hive**):
  - HKEY\_CLASSES\_ROOT:
    - Associazione: estensione file – applicazione

The screenshot shows the Windows Registry Editor window. The title bar reads "Editor del Registro di sistema". The menu bar includes File, Modifica, Visualizza, Preferiti, and ?.

The left pane displays a tree view of registry keys under "Computer\HKEY\_CLASSES\_ROOT\.3gp". The keys listed are: \*, .001, .264, .265, .386, .3ds, .3fr, .3g2, .3ga, .3gp (which is selected and highlighted in blue), .3gp2, .3gpp, and .3mf.

The right pane is a table with columns: Nome, Tipo, and Dati. It lists five entries:

Nome	Tipo	Dati
(Predefinito)	REG_SZ	FormatPlayer.3gp
Content Type	REG_SZ	video/3gpp
FormatPlayer.bak	REG_SZ	VLC.3gp
PerceivedType	REG_SZ	video
VLC.backup	REG_SZ	WMP11.AssocFile.3GP

# Microsoft Windows

## Registro di Sistema



- **HKEY\_USERS:**

- impostazioni di tutti profili utenti configurati nel sistema (*NTuser.dat*)

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
APPDATA	REG_SZ	C:\Users\marco\AppData\Roaming
HOMEDRIVE	REG_SZ	C:
HOMEPATH	REG_SZ	\Users\marco
LOCALAPPDATA	REG_SZ	C:\Users\marco\AppData\Local
LOGONSERVER	REG_SZ	\DC
USERDNSDOMAIN	REG_SZ	AD.SSRILAB.COM
USERDOMAIN	REG_SZ	AD-SSRILAB
USERDOMAIN_ROAMINGPROFILE	REG_SZ	AD-SSRILAB
USERNAME	REG_SZ	marco
USERPROFILE	REG_SZ	C:\Users\marco

# Microsoft Windows

## Registro di Sistema



- **HKEY\_CURRENT\_USER:**

- puntatore al profilo utente presente in “HKEY\_USERS”, loggato nel sistema

The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer\HKEY\_CURRENT\_USER\Volatile Environment'. The right pane is a table showing various registry entries with their names, types, and values.

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
APPDATA	REG_SZ	C:\Users\marco\AppData\Roaming
HOMEDRIVE	REG_SZ	C:
HOMEPATH	REG_SZ	\Users\marco
LOCALAPPDATA	REG_SZ	C:\Users\marco\AppData\Local
LOGONSERVER	REG_SZ	\DC
USERDNSDOMAIN	REG_SZ	AD.SSRILAB.COM
USERDOMAIN	REG_SZ	AD-SSRILAB
USERDOMAIN_ROAMINGPROFILE	REG_SZ	AD-SSRILAB
USERNAME	REG_SZ	marco
USERPROFILE	REG_SZ	C:\Users\marco

# Microsoft Windows

## *Registro di Sistema*



- **HKEY\_LOCAL\_MACHINE:**
  - configurazione del computer

Editor del Registro di sistema

File Modifica Visualizza Preferiti ?

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control

	Nome	Tipo	Dati
ab	(Predefinito)	REG_SZ	(valore non impostato)
ab	BootDriverFlags	REG_DWORD	0x0000001c (28)
ab	CurrentUser	REG_SZ	USERNAME
ab	DirtyShutdownCount	REG_DWORD	0x00000002 (2)
ab	EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure SystemEventsE
ab	FirmwareBootDevice	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)
ab	LastBootShutdown	REG_DWORD	0x00000000 (0)
ab	LastBootSucceeded	REG_DWORD	0x00000001 (1)
ab	PreshutdownOrder	REG_MULTI_SZ	DeviceInstall UsoSvc gpsvc trustedinstaller
ab	SvcHostSplitThresholdInKB	REG_DWORD	0x00380000 (3670016)
ab	SystemBootDevice	REG_SZ	multi(0)disk(0)rdisk(0)partition(2)
ab	SystemStartOptions	REG_SZ	NOEXECUTE=OPTIN
ab	WaitToKillServiceTimeout	REG_SZ	5000

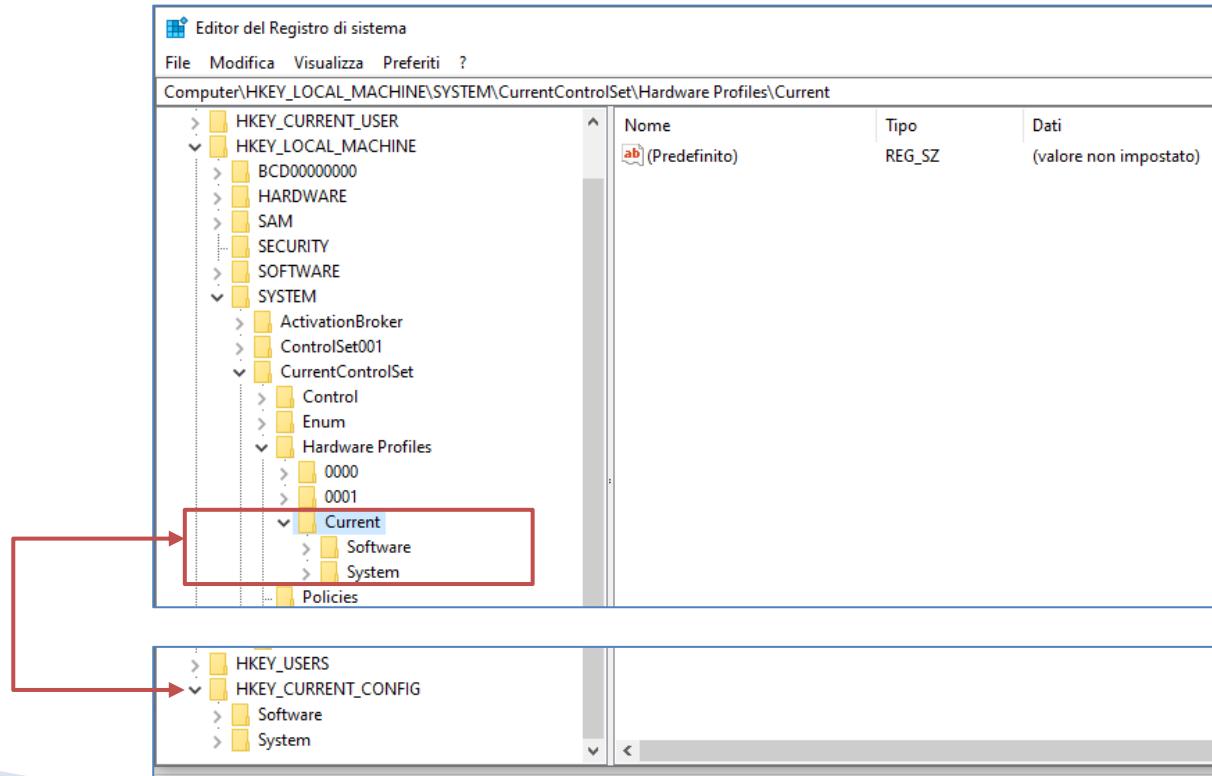
# Microsoft Windows

## Registro di Sistema



### ◦ HKEY\_CURRENT\_CONFIG:

- puntatore alla corrente configurazione situata in «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current»



# Microsoft Windows

## *Registro di Sistema*



- ▶ Ogni nodo dell'albero:
  - Chiave: coppia di valori (*NomeChiave–Valore*)
  - Sottochiavi

Tipi di chiavi	
Tipo	Descrizione
REG_SZ	NUL-terminated string
REG_EXPAND_SZ	NUL-terminated string (variabili di ambiente)
REG_BINARY	Dati binari
REG_DWORD/ REG_DWORD_LITTLE_ENDIAN	4Byte (intero senza segno) [little endian]
REG_DWORD_BIG_ENDIAN	4Byte (intero senza segno) [big endian]
REG_LINK	Collegamento ad un'altra chiave
REG_MULTI_SZ	Array di NUL-terminated string

# Microsoft Windows

## *Registro di Sistema*



Tipi di chiavi	
Tipo	Descrizione
REG_RESOURCE_LIST	Elenco di risorse per un driver
REG_FULL_RESOURCE_DESCRIPTOR	Un descrittore di risorsa utilizzata da un driver
REG_RESOURCE_REQUIREMENTS_LIST	Un elenco requisiti delle risorse di un driver
REG_QWORD / REG_QWORD_LITTLE_ENDIAN	8Byte (intero senza segno) [little endian]
REG_NONE	Nessun tipo

# Microsoft Windows

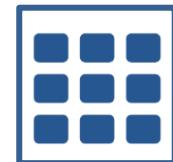
## *Registro di Sistema: Analisi*



- ▶ Configurazioni dell'utente
- ▶ Dispositivi USB: *pendrive, dischi esterni, etc.*
- ▶ Informazioni temporali: data di ultima modifica delle chiavi
- ▶ Strumenti:
  - RegEdit (*Windows*)
  - Windows Registry Recovery (*Mitec*)
  - Registry Viewer (*Access Data*)

# Microsoft Windows

## Thumbnails



- ▶ *miniature delle immagini presenti nelle cartelle*



# Microsoft Windows

## *Thumbnails*



- ▶ **Windows 98 – XP:**
  - Thumbs.db:
    - In ogni cartella in cui sono\erano presenti immagini
- ▶ **Windows ≥ Vista:**
  - Database centralizzato thumbcache\_[NUM].db  
*[NUM]: dimensioni delle anteprime: 96, 256, 1024*
    - %userprofile%\AppData\Local\Microsoft\Windows\Explorer
- ▶ **ANALISI**: miniature di immagini non più presenti
  - Thumbs Viewer
  - Thumbcache Viewer

# Microsoft Windows

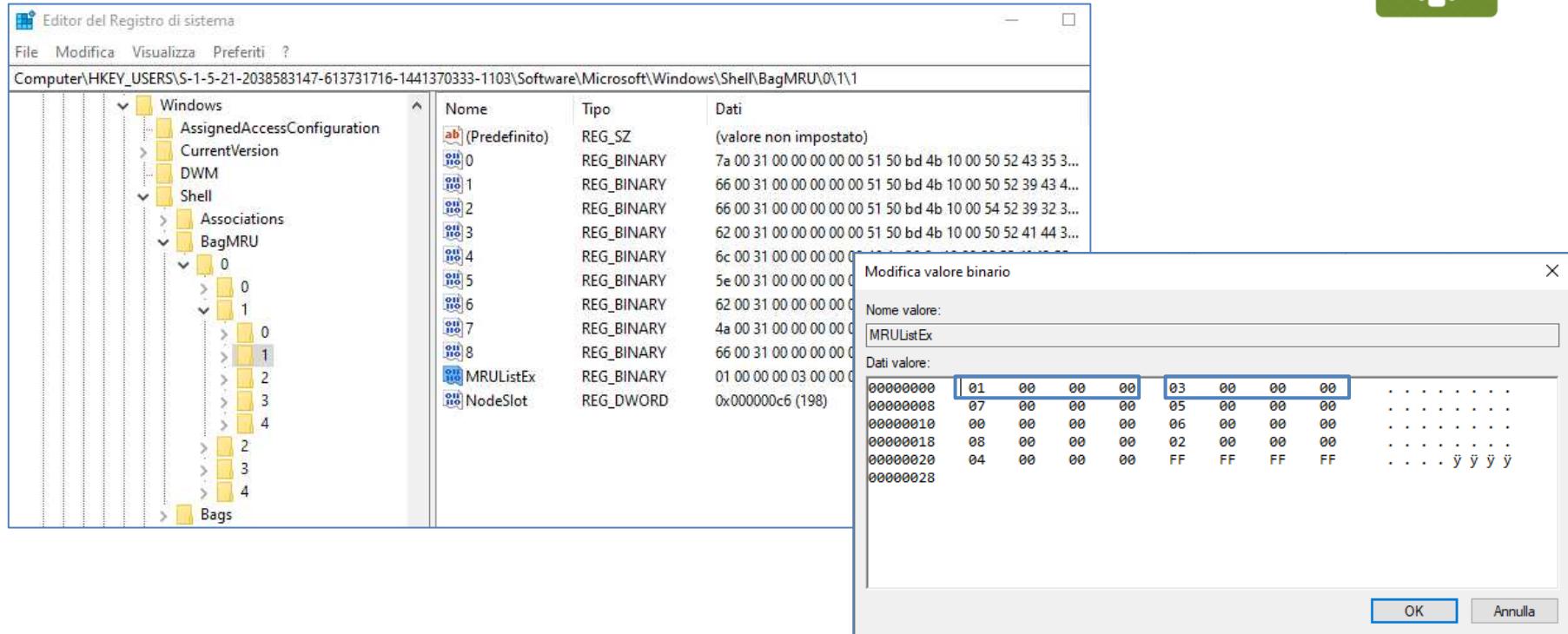
## *ShellBag*



- ▶ *Personalizzazioni utente delle visualizzazione del contenuto delle cartelle*
- ▶ **Chiavi di registro**
  - HKEY\_USERS\ <USERID>\Software\Microsoft\Windows\Shell\
  - HKEY\_USERS \ <USERID>\Software\Microsoft\Windows\ShellNoRoam (*Windows < Vista*)
  - HKEY\_USERS \ <USERID>\ Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell\ (*Windows ≥ Vista*)

# Microsoft Windows

## *ShellBag*



The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer\HKEY\_USERS\S-1-5-21-2038583147-613731716-1441370333-1103\Software\Microsoft\Windows\Shell\BagMRU\0\1\1'. The right pane shows a table with columns 'Nome', 'Tipo', and 'Dati'. Several binary values are listed, such as 0, 1, 2, 3, 4, 5, 6, 7, 8, and NodeSlot. A context menu is open over the '0' entry, and a sub-menu 'Modifica valore binario' is displayed, showing fields for 'Nome valore:' (MRUIListEx) and 'Dati valore:' (binary data). The binary data for NodeSlot is shown as 0x000000c6 (198).

- ▶ **BagMRU:** storico di tutte le cartelle visualizzate dall'utente
- ▶ **Bags:** impostazioni di visualizzazione delle cartelle contenute in BagMRU

# Microsoft Windows

## *ShellBag: analisi*



- 1) Si segue la lista delle cartelle presenti in MRUListEx (*Esempio: Procura Napoli*)
  - o Si seleziona visualizza il valore della chiave relativa: nome cartella (*Esempio: Procura Napoli*)

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under 'Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell\BagMRU\0\1\1'. The right pane shows a table with columns 'Nome', 'Tipo', and 'Dati'. One entry, 'MRUListEx', is selected and highlighted. A context menu is open over this entry, with a submenu titled 'Modifica valore binario'. This submenu contains a single input field with the value '1'. At the bottom of the submenu, there are 'OK' and 'Annulla' buttons.

Nome	Tipo	Dati
0	REG_SZ	ab (Predefinito)
0	REG_BINARY	0
1	REG_BINARY	1
0	REG_BINARY	2
1	REG_BINARY	3
2	REG_BINARY	4
3	REG_BINARY	5
4	REG_BINARY	6
2	REG_BINARY	7
3	REG_BINARY	8
4	REG_BINARY	MRUListEx
Bags	REG_BINARY	
TabletPC	REG_DWORD	
Windows Error Reporting	REG_DWORD	

# Microsoft Windows

## *ShellBag: analisi*



- 2) Si segue la sottochiave della cartella (Es.:)
- Si visualizza la chiave MRUListEx e si continua ricorsivamente la sua esplorazione

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under 'Computer\HKEY\_USERS\S-1-5-21-2038583147-613731716-1441370333-1103\Software\Microsoft\Windows\Shell\BagMRU\0\1\1\1'. A red box highlights the 'MRUListEx' value under key '1'. A context menu is open over this value, with 'Modifica' selected. A 'Modifica valore binario' dialog box is overlaid on the editor, showing the binary value of 'MRUListEx' as 0x00000000000000000000000000000000. The dialog also shows the current value data as 0x00000000000000000000000000000000.

# Microsoft Windows

## *ShellBag: analisi*



- ▶ Informazioni ottenibili:
  - **Bag Number:** la sottochiave Bags che contiene le preferenze dell'utente (Nodeslot).
  - **Registry key last write time:** data di primo accesso o di ultima modifica della cartella.
  - **Folder name:** nome della cartella.
- ▶ Tool: ShellBagsView (*NirSoft*)

# Microsoft Windows

## *Event Viewer*



- ▶ Sistema di *logging* standard (EVT/EVTX)

Nome	Tipo	Numero di eventi	Dimensione
Applicazione	Amministrativo	14.125	9,07 MB
Sicurezza	Amministrativo	30.071	20,00 MB
Installazione	Operativo	53	68 KB
Sistema	Amministrativo	19.876	10,07 MB
Eventi inoltrati	Operativo	0	0 byte

# Microsoft Windows

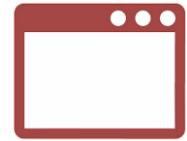
## *Event Viewer*



ID Evento ≥ Vista	ID Evento < Vista	Descrizione
1102	517	Log di audit cancellato
4624	528/540	Accesso di un account completato
4625	529/537	Accesso non riuscito per un account
4634	538	Un account è stato disconnesso
4674	578	Operazione eseguita con privilegi elevati
4704	608	Assegnazione di un diritto per un utente
4719	612	Cambiamento nelle politiche di audit
4720	624	Aggiunta di un nuovo account
4722	626	Un account utente è stato abilitato
4726	630	Un account utente è stato eliminato
4732	636	Un account utente è stato aggiunto ad un gruppo locale
4738	642	Un account utente è stato modificato
4739	643	Cambiamento nelle policy di dominio.

# Microsoft Windows

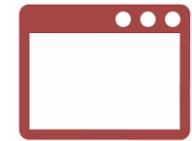
## *Application Data*



- ▶ *impostazioni dei programmi utilizzati dall'utente e file temporanei*
  
- ▶ **Windows XP:**
  - \Documents and Settings\[nome\_utente]\
    - Dati Applicazioni
    - Impostazioni Locali
  
- ▶ **Windows ≥ Vista:**
  - \Users\[nome\_utente]\AppData

# Microsoft Windows

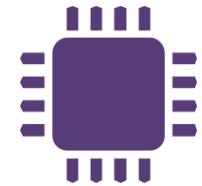
## *Application Data: Analisi*



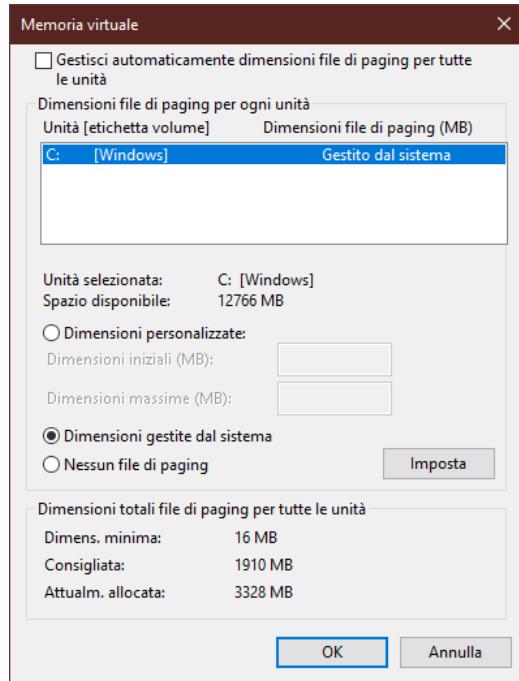
- ▶ quadro complessivo dell'utilizzo del computer da parte di un utente:
  - Posta elettronica
  - Cache
  - Cronologia
  - Log
  - Configurazioni

# Microsoft Windows

## *File Swap*



- ▶ *Estensione della memoria volatile (RAM)*
  - **Pagefile.sys**



- ▶ **Hiberfil.sys:** congelamento della memoria RAM in fase di sospensione\ibernazione

# Microsoft Windows

## *Analisi*



### *Vantaggi*

- ▶ Diffuso
- ▶ Documentato
- ▶ Supportato

### *Svantaggi*

- ▶ Pochi log
- ▶ Presenza di antivirus che possono compromettere una timeline
- ▶ Sistema commerciale

# Sistemi Operativi

» Apple OS X/macOS

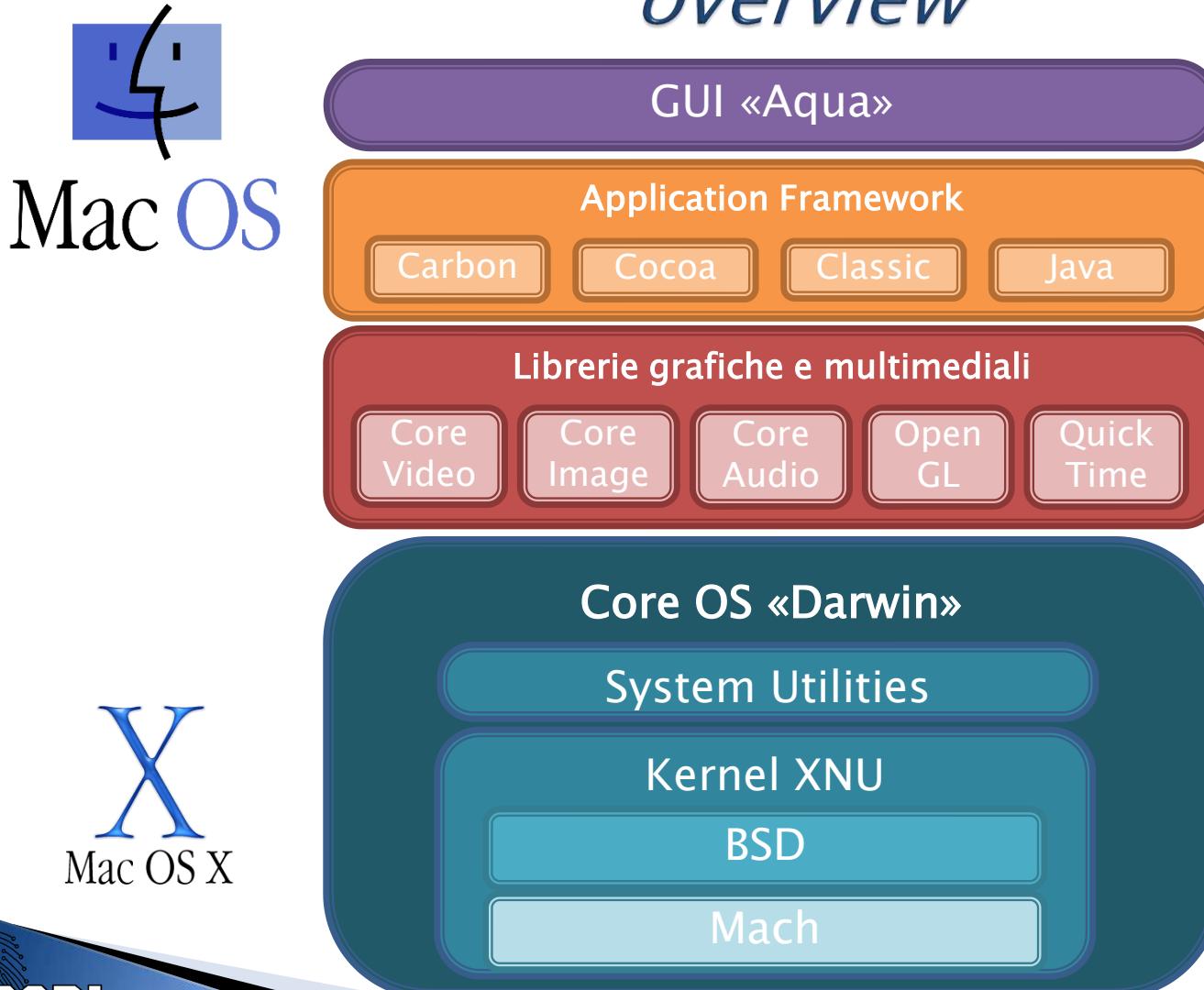


# Apple OS X/macOS

## *overview*



Mac OS



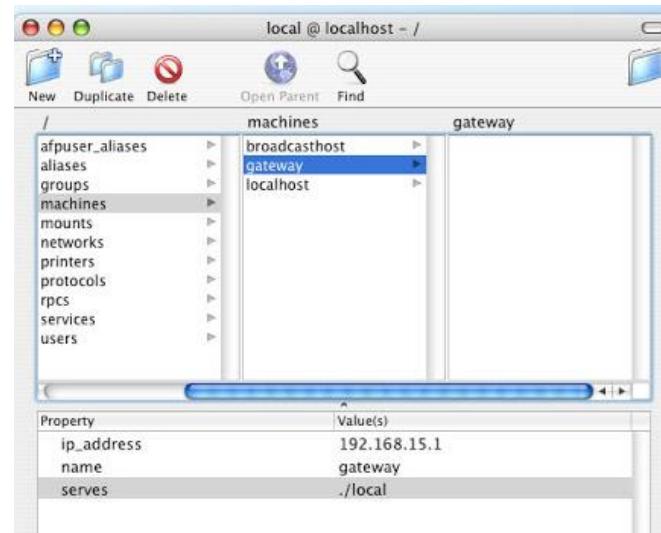
# Apple OS X/macOS

## *configurazione*



- ▶ NetInfo (DB ad oggetti)
  - Controlla diverse configurazioni del S.O.
    - Entry statiche di rete (file hosts)
    - Definizione di tutti gli utenti
- ▶ Gestione NetInfo:
  - /Application/Utility (OS X ≤ 10.4)
  - /Application/Utility/Utility Directory (OS X >10.4)

*Fino alla versione  
Mac OS X 10.5*



# Apple OS X/macOS

## *configurazione server*

- ▶ Open Directory (Mac OS X Server 10.4)
  - Servizio di directory
  - Gestione delle autenticazioni

Tool	Descrizione
dscl	Manipolazione e gestione dei servizi di directory
dsconfigldap	manipolazione degli alberi LDAP
dsconfigad	manipolazione dei sistemi Active Directory
dseditgroup	gestione di gruppi di utenti
dsenableroot	abilita/disabilita l'utente root in OpenDirectory
dscacheutil	regola le cache relative a OpenDirectory
dsmemberutil	Gestisce i gruppi di appartenenza di un oggetto OpenDirectory
dsexport	esporta oggetti da un albero OpenDirectory
dsimport	importa oggetti in un albero OpenDirectory

# Apple OS X/macOS

## *cifratura*



- ▶ **FileVault**
  - Cifratura della home directory (/Users/[nome\_utente])
- ▶ **FileVault 2 (OS X  $\geq 10.7$ )**
  - Full disk encryption

# Apple OS X/macOS

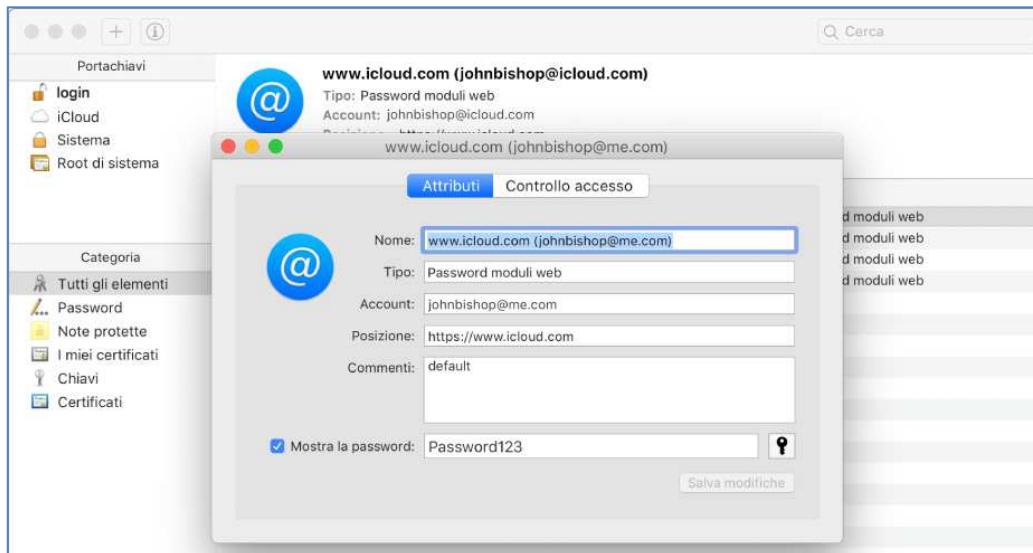
## *file swap*

- ▶ Estensione della memoria volatile (RAM)
  - */private/var/vm/swapfile\**
- ▶ congelamento della memoria RAM in fase di sospensione:
  - */private/var/vm/sleepimage*

# Apple OS X/macOS

## *portachiavi*

- ▶ Accentramento delle credenziali utente
  - Accesso tramite API
  - Cifratura AES-128
- ▶ OS X ≥ 10.9
  - Integrazione servizio Apple iCloud



# Apple OS X/macOS

## *analisi*

- ▶ Elevato numero di tecnologie proprietarie
  - Uso di un sistema OS X per l'analisi
- ▶ Strumenti:
  - *BlackBag Technologies*
    - Blacklight: toolkit forense
    - MacQuisition: tool di acquisizione forense
  - Mac Forensics Lab (*SubRosaSoft*)
  - Apple hdiutil: *tool da riga di comando*
    - Apple DMG
      - Copia FullDisk
      - Copia Logica

# Apple OS X/macOS

## *analisi*

### ▶ Home Directory Utente

- La granparte dei file dell'utente
- Dati delle applicazioni: */Users/[nome\_utente]/Library*



# Sistemi Operativi

» Linux



# Linux

## *overview*

- ▶ Distribuzioni basate su kernel GNU/Linux
- ▶ Linux Standard Base (LSB)
  - Standardizzazione delle diverse distribuzioni
- ▶ Componenti:
  - Kernel
  - Librerie di sistema
  - Tool di base



# Linux

## *overview*

### ▶ Distribuzioni commerciali:

- Red Hat Enterprise
  - Fedora
  - CentOS: versione libera senza supporto
  - Scientific Linux
- SUSE Linux Enterprise
  - openSUSE



### ▶ Distribuzioni gratuite:

- Debian: distribuzione ufficiale della Free Software Foundation
- Ubuntu



# Linux

## *sistema*

- ▶ Multiutente e Multitasking
- ▶ Struttura rigida del file system:

Directory	Contenuto
/bin	Binari d'uso comune nel sistema.
/boot	Kernel e file necessari al boot
/dev	device fisici e logici collegati al computer
/etc	File di configurazione del sistema
/home	File degli utenti
/lib	Librerie di sistema
/mnt	Punto di montaggio per media esterni
/opt	Punto dove sono installati programmi che richiedono complesse alberature per il loro funzionamento
/root	Home directory dell'utente root

# Linux

## *sistema*

Directory	Contenuto
/sbin	Binari riservati all'uso di root
/srv	File di dati per alcuni servizi server come web e server FTP
/tmp	Locazione generale per i file temporanei
/usr	Contiene programmi non indispensabili al sistema
/usr/local	Locazione per i programmi compilati dagli utenti
/usr/src	Sorgenti del kernel e dei vari pacchetti
/var	Parte variabile dei programmi. Contiene log, mail, spool di stampa, database e quanto può essere utile a un programma da tenere in una directory scrivibile

# Linux

## *sistema*

Device /dev	Contenuto
/hda	Disco ATA master collegato al canale primario
/hdd	Disco ATA slave collegato al canale secondario
/sda	Disco SCSI con l'ID più basso collegato alla catena
/hda1	Prima partizione del disco ATA master collegato al canale primario
/loop0	Loop device. Permette visualizzare un file immagine come se fosse realmente agganciato
/eth0	Prima scheda di rete collegata al sistema
/md0	RAID software generato da Linux

# Linux

## *sistema*



### ▶ Sistema di permessi di file e directory:

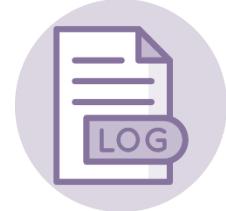
- r: permesso di lettura
- w: permesso di scrittura
- x: *file* permesso di esecuzione | *directory* permesso di accesso

r	w	x	r	w	x	r	w	x
owner	group	public						

- Utente root: *nessun limite*

# Linux

## Log



- ▶ **Syslog:** sistema di gestione Log
  - **syslogd:** daemon (*servizio*)
  - **configurazione:** /etc/syslog.conf

Facility code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon

# Linux

## *Log*



Facility code	Keyword	Description
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16–23	local0 – local7	Locally used facilities

Severity Value	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant conditions
6	Informational	Informational messages
7	Debug	Debug-level messages

# Linux

## *Log*



- ▶ Posizione dei log: */var/log*
  - **messages**: eventi relativi alla macchina
  - **wtmp**: registrazione degli accessi
- ▶ **Logfinder**: ricerca di tutti i file log

# Linux

## *configurazioni*



- ▶ posizione:
  - /etc (*configurazione di default*)
    - Inittab: file di configurazione di boot
    - passwd: elenco degli utenti
    - shadow: password degli utenti
  - File nascosti nella home directory utente (*configurazioni personalizzate*)
- ▶ Nome\_programma.conf (*Esempio: apache.conf*)

## *swap*

- ▶ Partizione:
  - *FAT*
  - *0x83 (marcatore)*

# Linux

## *home directory*



### ▶ Tipi di utente:

- root: amministratore di sistema (*sys-admin*)
- utente comune

### ▶ Directory disponibili all'utente:

- /usr/local/bin: file dei programmi utilizzabili dall'utente
- /tmp: file temporanei
- /home/[*nome\_utente*]: directory principale dell'utente
  - *Dati dell'utente*: la gran parte dei file creati\gestiti dall'utente
  - *Shell history*: lista dei comandi impiegati dall'utente
  - *Cache*
  - *File di configurazione*: configurazioni personalizzate di programmi

# Linux

## */var*

- ▶ Contiene di dati cambiano/variano durante la normale esecuzione del sistema
  - Specifico per ogni sistema
- ▶ Dati:
  - log di sistema;
  - spool di stampa;
  - mail in transito e code;
  - tablespace degli RDBM;
  - cache di sistema;
  - configurazione dei vari tool;
  - database dei pacchetti installati;
  - file di bind;
  - database di LDAP;
  - database di sistema di AFS;
  - database di Kerberos.

# Linux

## *analisi*



- ▶ /home
- ▶ /etc
- ▶ /var
  
- ▶ Analisi live:
  - 1) **inittab/systemd**: controllare tutti i servizi (deamon) eseguiti in fase di boot
  - 2) **Autenticazione**: verificare la configurazione PAM, kerberos e openLDAP
  - 3) \etc\fstab: verificare il montaggio dei file system all'avvio



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 22: Mobile Forensics *acquisizione e analisi*



A.A. 2021/22

Dott. Lorenzo LAURATO

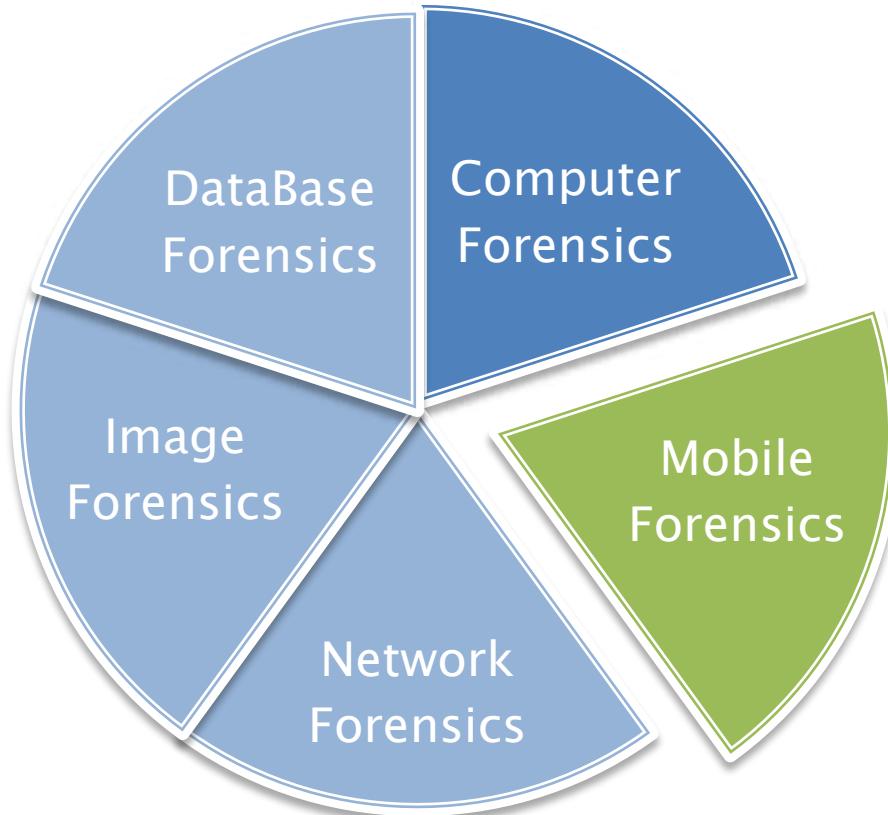


# Mobile Forensics

» Overview

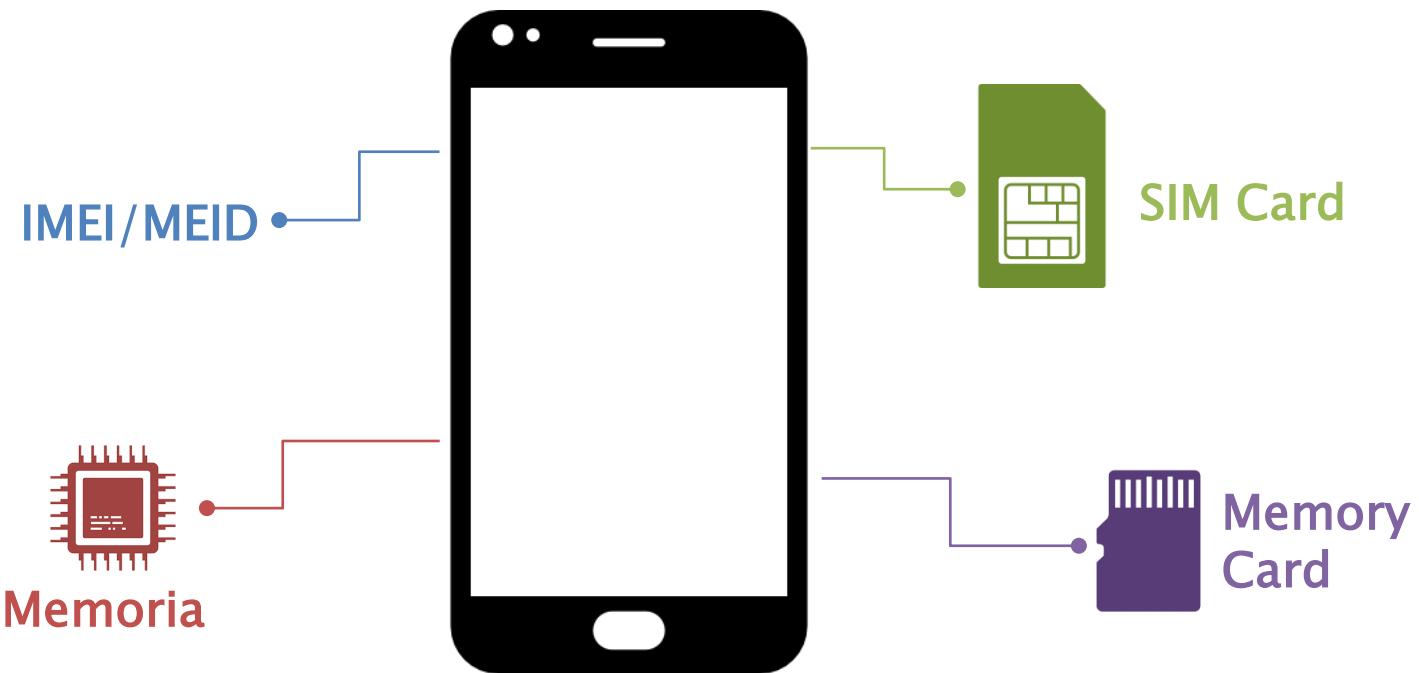


# Digital Forensics



# Mobile Forensics

## *evidence*



# Mobile Forensics

## GSM/CDMA

### GSM

*Global System for Mobile communications*

- ▶ **IMEI** (*International Mobile Equipment Identity*): codice univoco del dispositivo all'interno della rete mobile
- ▶ **SIM Card** (*Subscriber Identity Module*):
  - ICCID (*Integrated Circuit Card ID*): nr. seriale 19/20 cifre
  - IMSI (*International Mobile Subscriber Identity*): identificativo nella rete mobile dell'operatore

### CDMA

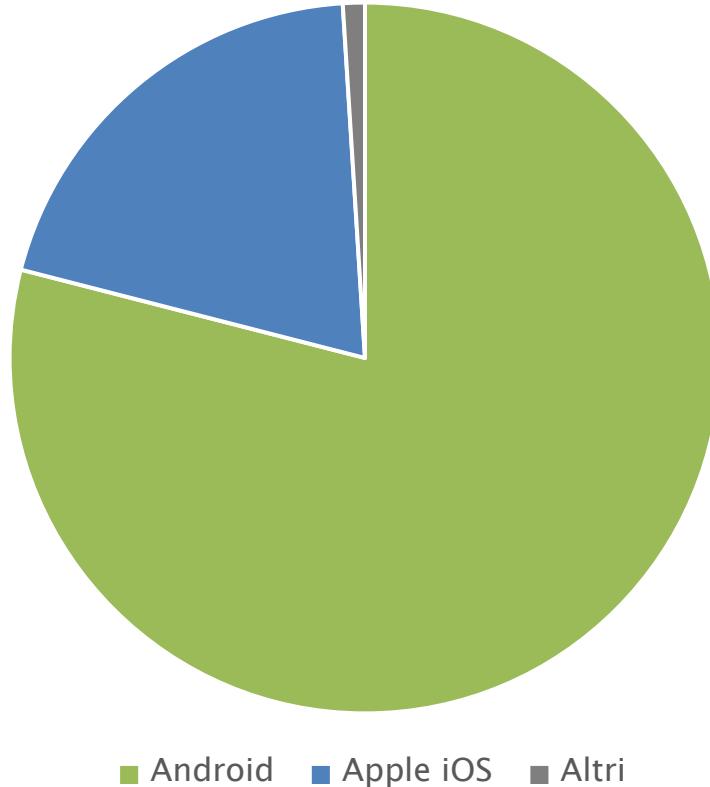
*Code Division Multiple Access*

- ▶ **MEID** (*mobile equipment identifier*): codice univoco del dispositivo all'interno della rete mobile
- ▶ **NO SIM Card**

# Mobile Forensics

## *dispositivi*

O.S.



■ Android ■ Apple iOS ■ Altri

# Mobile Forensics

## *la raccolta*

- 1) Disabilitare tutte le connessioni:
  - OFF Line Mode/Airplane Mode
  - Faraday Bag
  - L'obiettivo è evitare:
    - Remote Wipe
    - Sovrascrittura di informazioni presenti



# Mobile Forensics

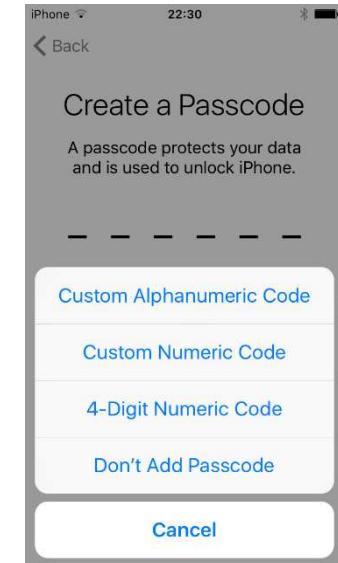
## *la raccolta*

### 2) Sbloccare il dispositivo:

- Apple iOS:

- PassCode a 4 cifre
- PassCode a 6 cifre (default)
- PassCode > 6 cifre
- Password alfanumerica
- *Face ID/ Touch ID*

Max 10 tentativi



# Mobile Forensics

## *la raccolta*

2) Sbloccare il dispositivo:

- Android OS:

- PassCode  $\geq$  4 cifre
- Password alfanumerica
- Pattern
- *Face ID/ Touch ID*
- *Password di avvio*

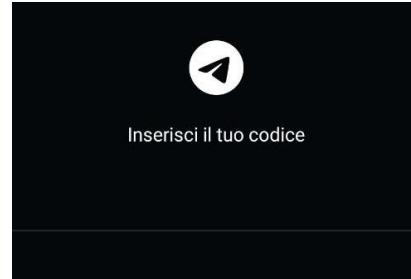


Max ? Tentativi

# Mobile Forensics

## *la raccolta*

- 2) Sbloccare il dispositivo:
  - Protezione implementata dalle app



- *Applicazione di sicurezza*

# Mobile Forensics

## *la raccolta*



### 2) Sbloccare il dispositivo:

- SIM Card:
  - PassCode 4 cifre (PIN)
    - Max 3 tentativi
  - PUK: recovery code
    - 8 cifre
    - Max 10 tentativi

# Mobile Forensics

## *la raccolta*



- 3) Spegnere il dispositivo:
  - Alcuni dispositivi richiedono lo sblocco

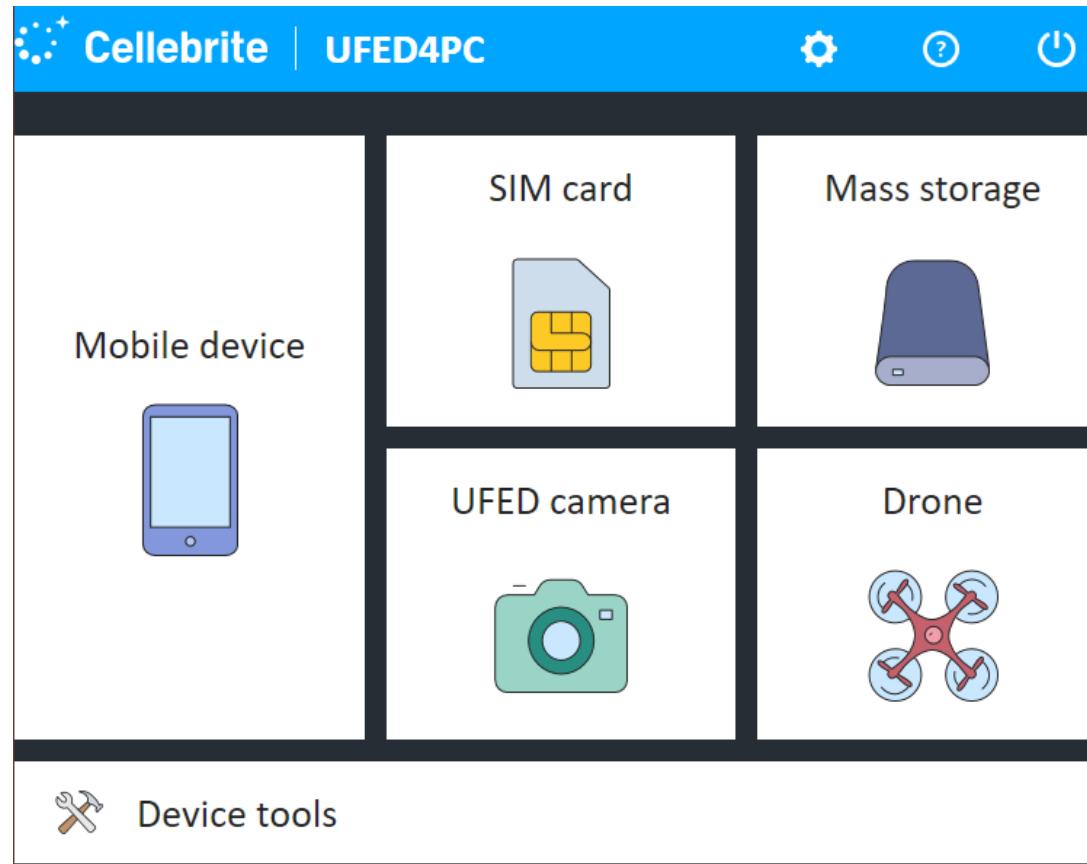
# Mobile Forensics

» Acquisizione



# Mobile Forensics: acquisizione strumenti

- ▶ *Cellebrite UFED (Universal Forensic Extraction Device)*



# Mobile Forensics: acquisizione strumenti

- ▶ *Cellebrite UFED (Universal Forensic Extraction Device)*



# Mobile Forensics: acquisizione *memory card*



- ▶ *Micro SD, MiniSD, etc.*
  - ..., 16GB, 32GB, 64GB, 128GB, etc.
  - Foto, Video, Musica
  - Applicazioni
  - Backup
  - ...
- ▶ E' la prima cosa da acquisire:
  - writeblock hardware/software

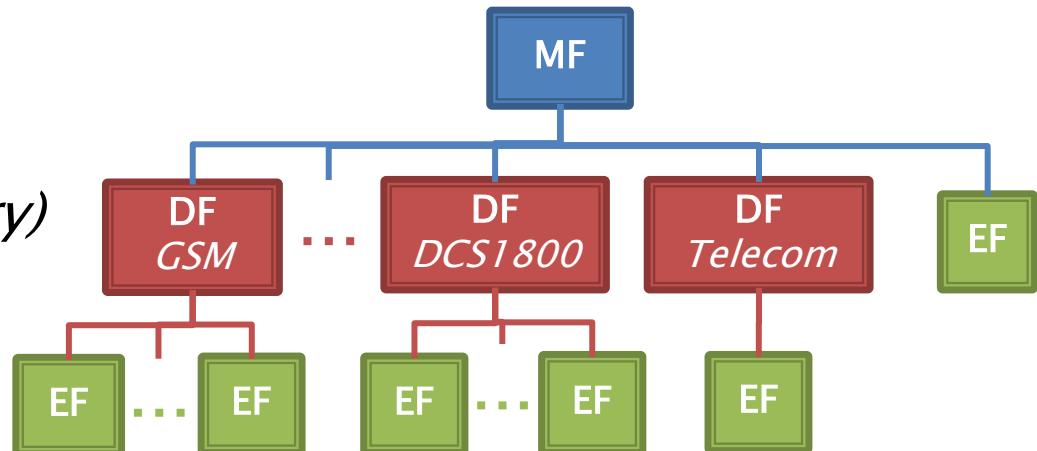
# Mobile Forensics: acquisizione

## *SIM card*



- ▶ (Mini) SIM, Micro SIM, Nano SIM
  - 16KB, 32KB, 64KB, 128KB, etc.
  - Rubrica
  - SMS
  - Identificativi: ICCID, IMSI

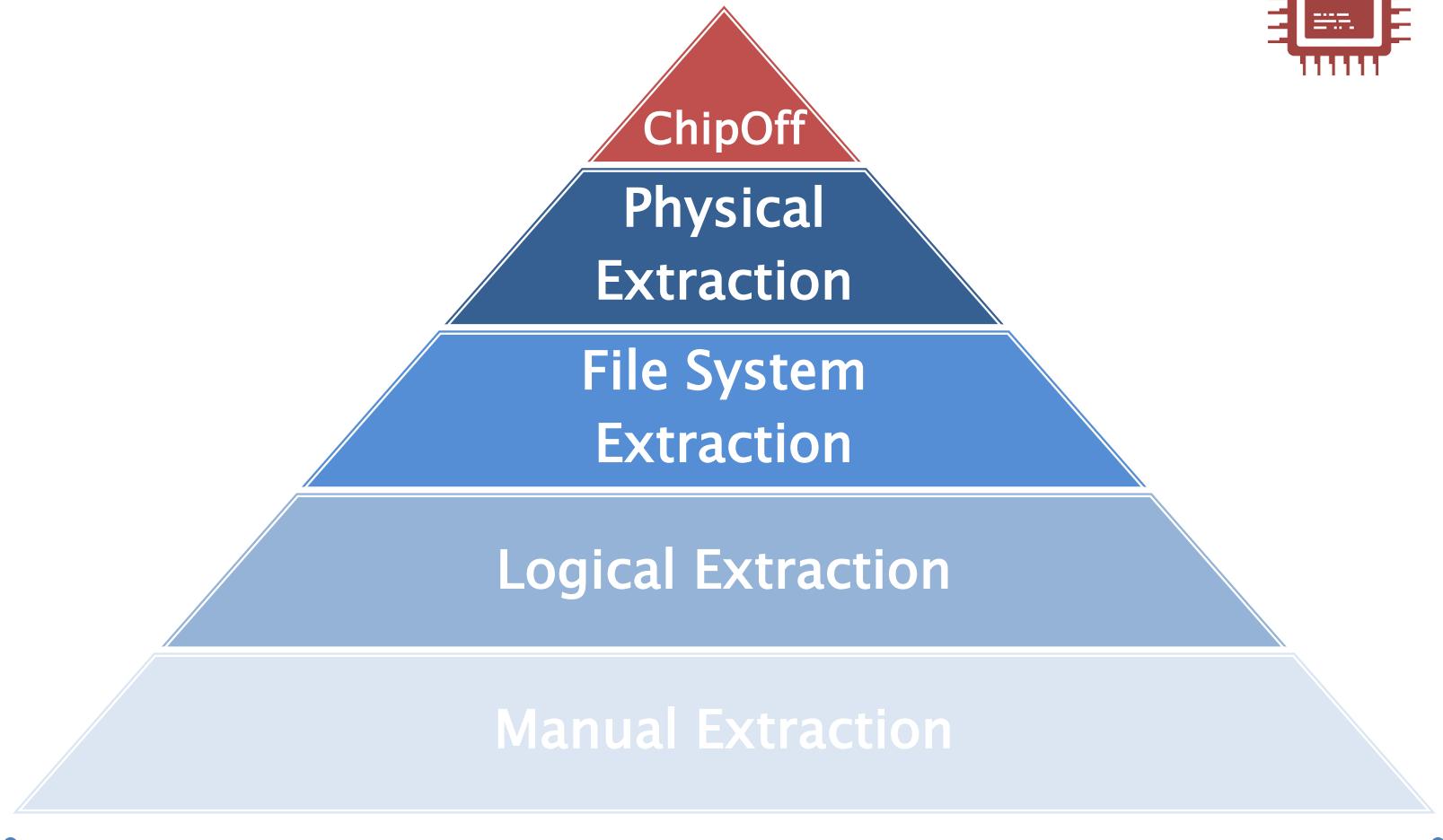
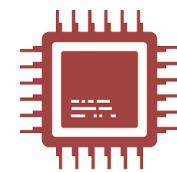
- ▶ Struttura:
  - Master File (*root*)
  - Dedicated File (*directory*)
  - Elementary File (*file*)



- ▶ Acquisizione:
  - *Lettore di SIM Card*

# Mobile Forensics: acquisizione

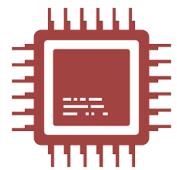
*tipi*



*Nr. di dispositivi supportati*

# Mobile Forensics: acquisizione

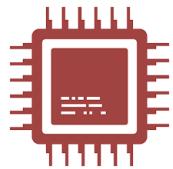
## *tipi*



All	Vendors	Generic profiles	Recently used
Sony (SonyEricsson)	Sunup	Swisstone	Tablets
			
TCL	TEC	Tecno	Telit
			
Texet	TIM	T-Mobile	TomTom
			

# Mobile Forensics: acquisizione

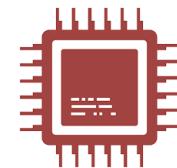
## *tipi*



Sony (SonyEricsson) D5833 Xperia Z3 Compact 	Sony (SonyEricsson) D6503 Xperia Z2 	Sony (SonyEricsson) D6603 Xperia Z3 	Sony (SonyEricsson) D6616 Xperia Z3 
Sony (SonyEricsson) D6643 Xperia Z3 TV 	Sony (SonyEricsson) D6653 Xperia Z3 	Sony (SonyEricsson) D6708 Xperia Z3v 	Sony (SonyEricsson) D750i 
Sony (SonyEricsson) E2006 Xperia E4g 	Sony (SonyEricsson) E2104 Xperia E4 	Sony (SonyEricsson) E2105 Xperia E4 	Sony (SonyEricsson) E2303 Xperia M4 Aqua 

# Mobile Forensics: acquisizione

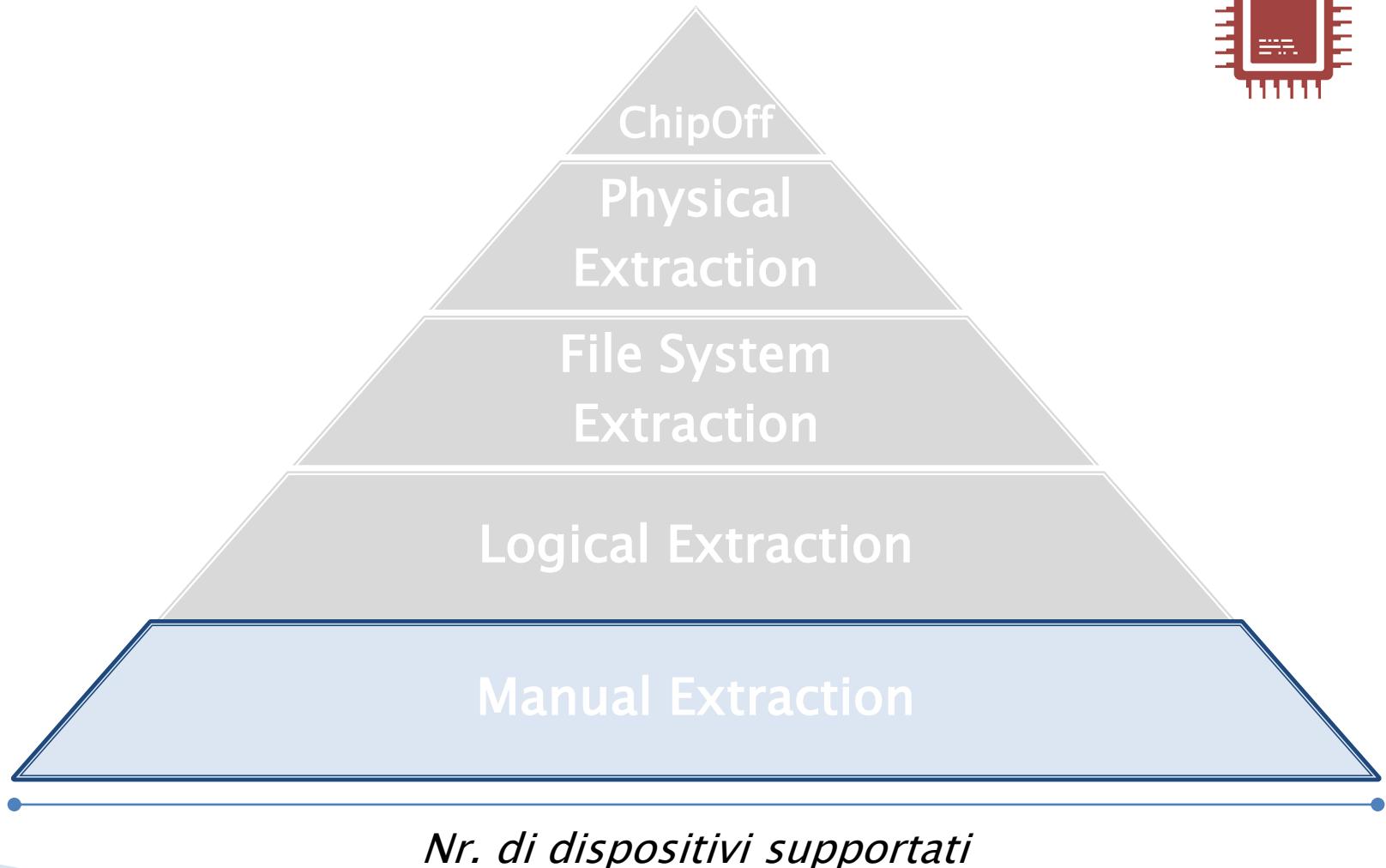
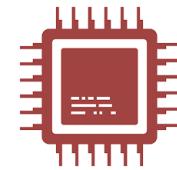
## *tipi*



Sony (SonyEricsson) D6603 Xperia Z3  
Cable A with black tip T-100

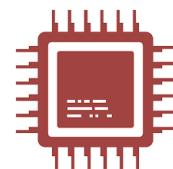
Advanced Logical 	Disable/Re-Enable User Lock  Lock Bypass	File system 	Physical 
Camera 	Screenshot 		

# Mobile Forensics: acquisizione

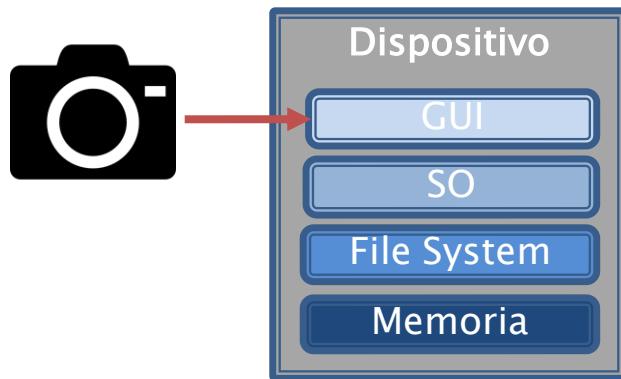


# Mobile Forensics: acquisizione

## *Manual Extraction*

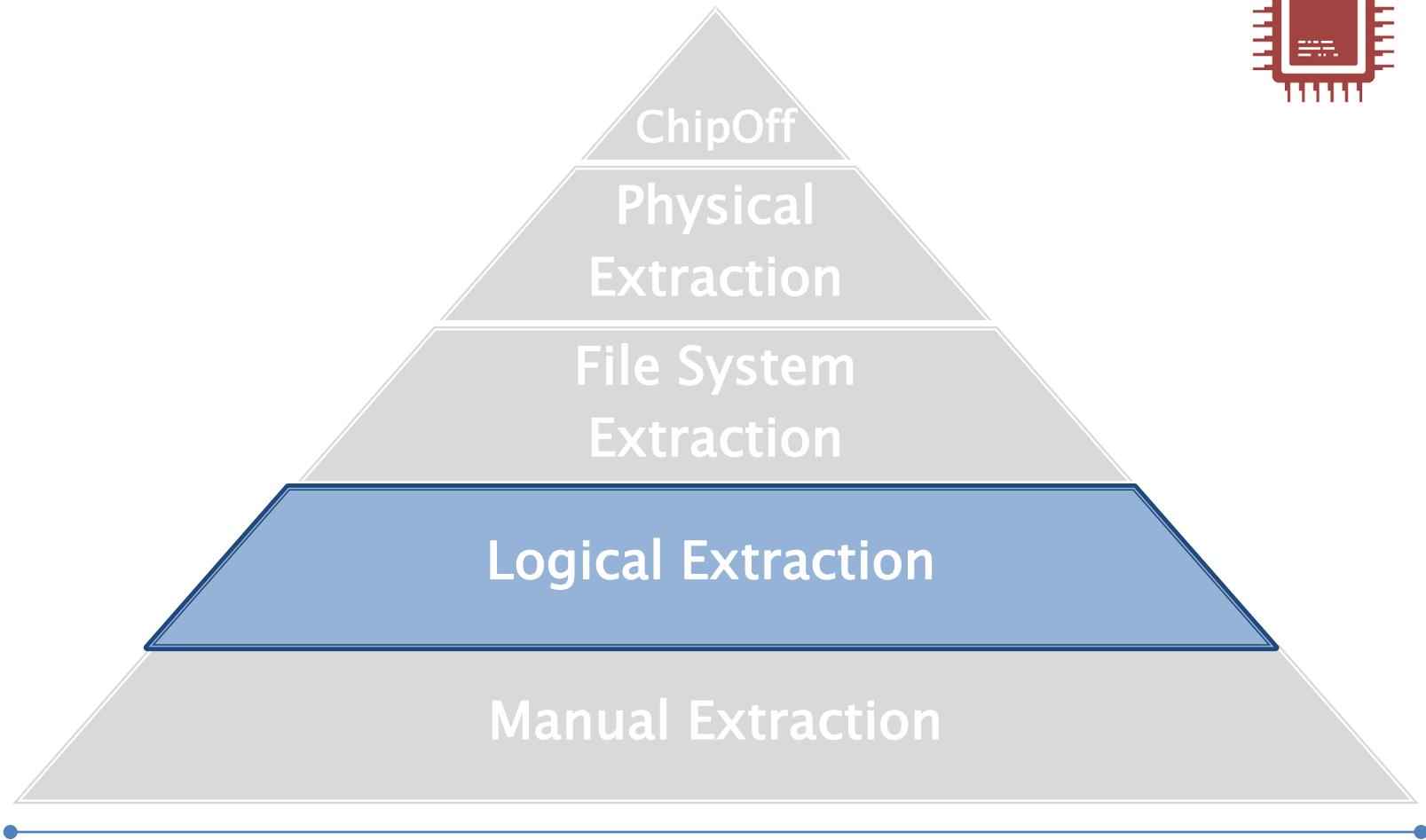
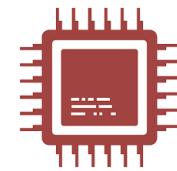


- ▶ repertazione fotografica del contenuto
  - *Interagire con la GUI*



- ▶ **Svantaggi:**
  - Processo lungo
  - Rischio modifica/cancellazione dei dati
  - Visualizzazione limitata delle informazioni
- ▶ **Limiti:**
  - Display non funzionante
  - Codice di sblocco

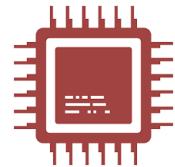
# Mobile Forensics: acquisizione



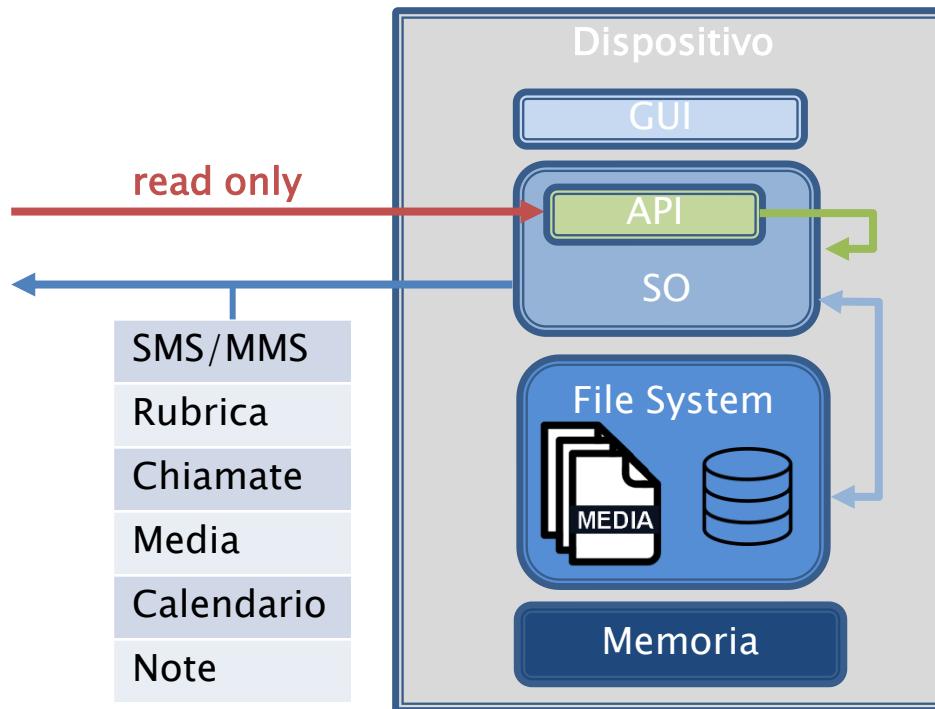
*Nr. di dispositivi supportati*

# Mobile Forensics: acquisizione

## *Logical Extraction*

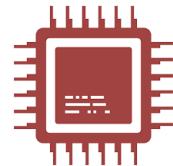


- ▶ Estrazione dei dati tramite API del dispositivo



# Mobile Forensics: acquisizione

## *Logical Extraction*

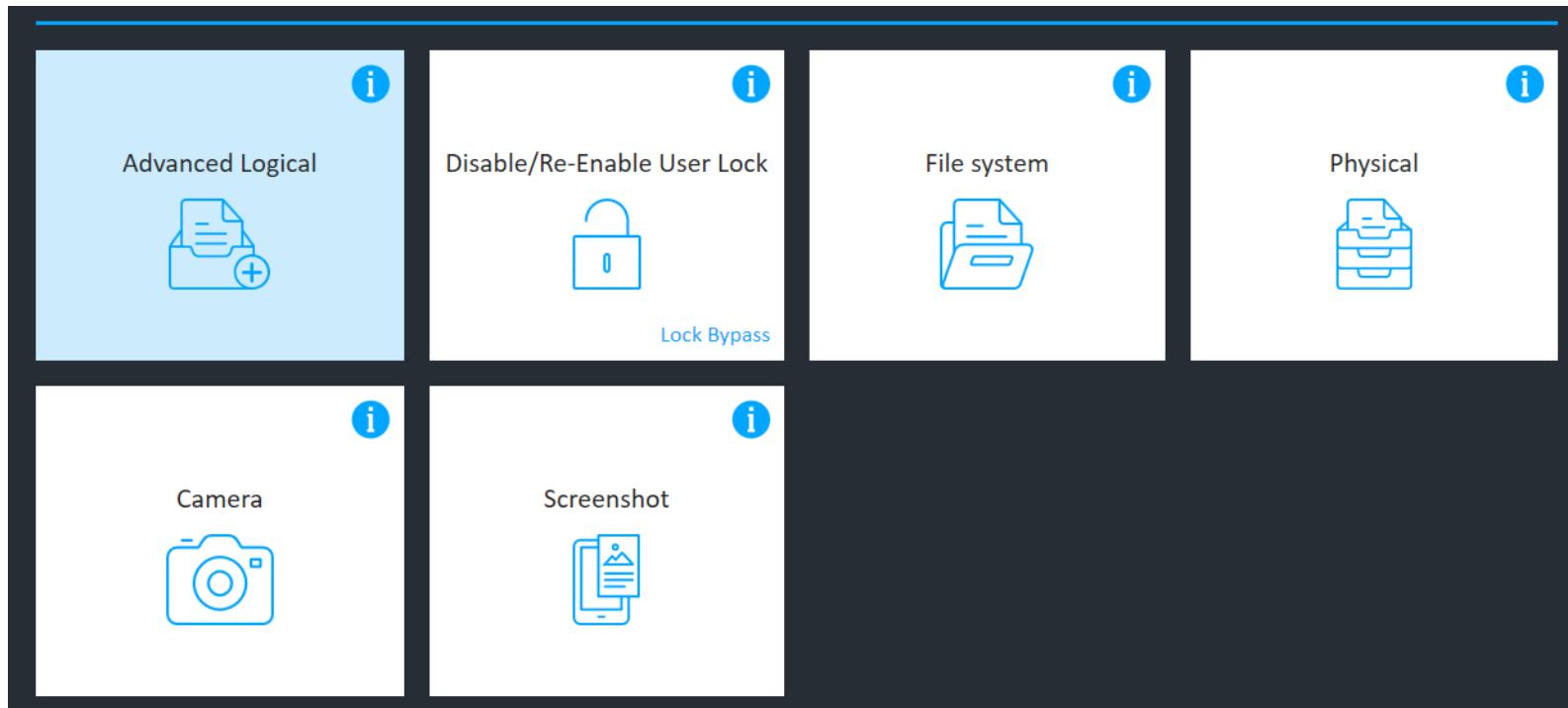
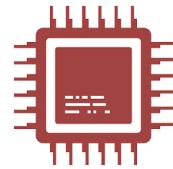


### ▶ Limiti:

- I risultati dipendono dall'API
  - Parziali:
    - solo alcune informazioni di un dato
    - solo alcuni dati: nessun dato di app di terze parti
- Codice di sblocco

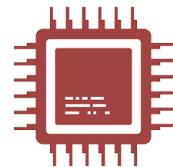
# Mobile Forensics: acquisizione

## *Logical Extraction*



# Mobile Forensics: acquisizione

## *Logical Extraction*



Sony (SonyEricsson) D6603 Xperia Z3  
Cable A with black tip T-100

---

Extract from

Device     SIM     Memory Card

---

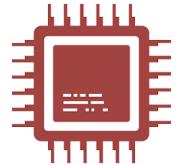
Choose data types to extract

All

<input type="checkbox"/> Contacts	<input type="checkbox"/> SMS	<input type="checkbox"/> MMS	<input type="checkbox"/> Calendar
<input type="checkbox"/> Pictures	<input type="checkbox"/> Audio/Music	<input type="checkbox"/> Videos	<input type="checkbox"/> Ringtones
<input type="checkbox"/> Call Logs	<input type="checkbox"/> Files	<input type="checkbox"/> Email	<input type="checkbox"/> IM
<input type="checkbox"/> Browsing Data	<input type="checkbox"/> User Dictionary		

# Mobile Forensics: acquisizione

## *Logical Extraction*

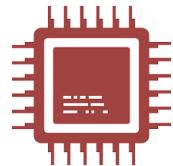


- 📁 Attachments
- 📁 Audio
- 📁 Images
- 📁 Ringtones
- 📄 Backup 2016\_05\_20 (001).cal
- 📄 Backup 2016\_05\_20 (001).clog
- 📄 Backup 2016\_05\_20 (001).MMS
- 📄 Backup 2016\_05\_20 (001).PBB
- 📄 **Backup 2016\_05\_20 (001).SMS**
- PA Logical.udf
- Report.html
- Report.xml
- Report\_AudioSection.html
- Report\_CalendarSection.html
- Report\_CallLogsSection.html
- Report\_ContactsSection.html
- Report\_DatabasesSection.html
- Report\_ImagesSection.html
- Report\_MMSSection.html
- Report\_RingtonesSection.html
- Report\_SMSSection.html
- Report\_VideoSection.html

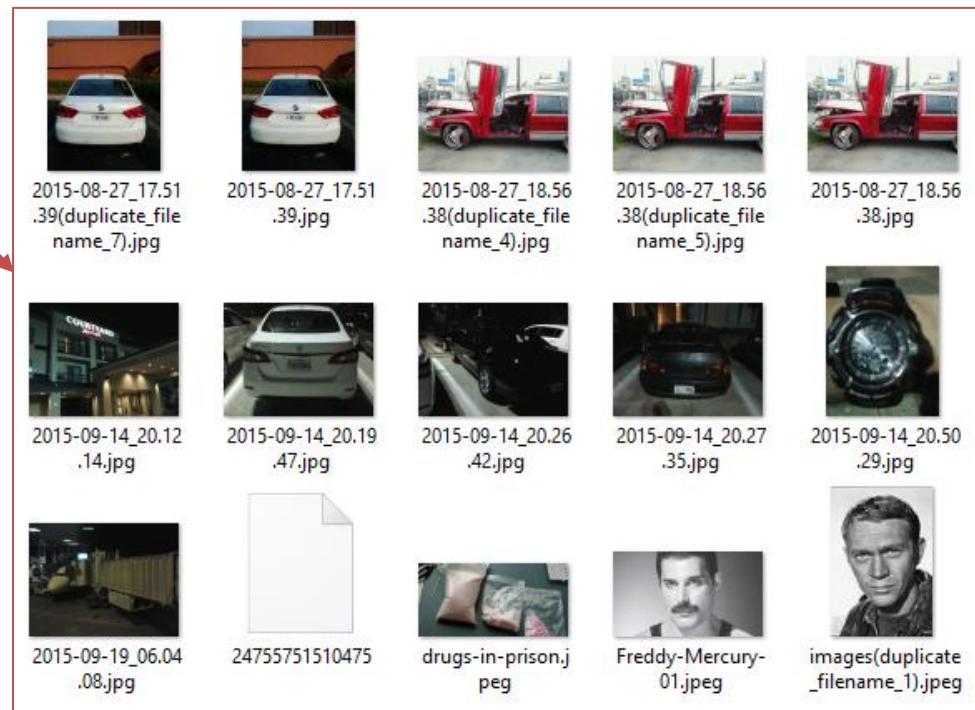
```
Type(1)=0
Source(1)=1
Folder(1)=1
SMSC(12)=+12063130057
Number(12)=+14782279373
Date(6)=150826
Time(6)=100039
Body(261)=Señor El Chappo, The new lab is up and running. The U.S. Coast Guard
intercepted the last shipment on our submarine. We only lost 10,000 kilos. This will
not interfere with our profit margin. The U.S. Economy is supports our business model
very well!! Jorge
Status(1)=1
GmtOffset(4)=-300
Name(12)=Valio Jorge
#
Type(1)=0
Source(1)=1
Folder(1)=1
SMSC(12)=+12063130055
Number(12)=+14782279373
Date(6)=150826
Time(6)=103400
Body(65)=Señor El Chapo, We are preparing the weapons for your escape.
Status(1)=1
GmtOffset(4)=-300
Name(12)=Valio Jorge
```

# Mobile Forensics: acquisizione

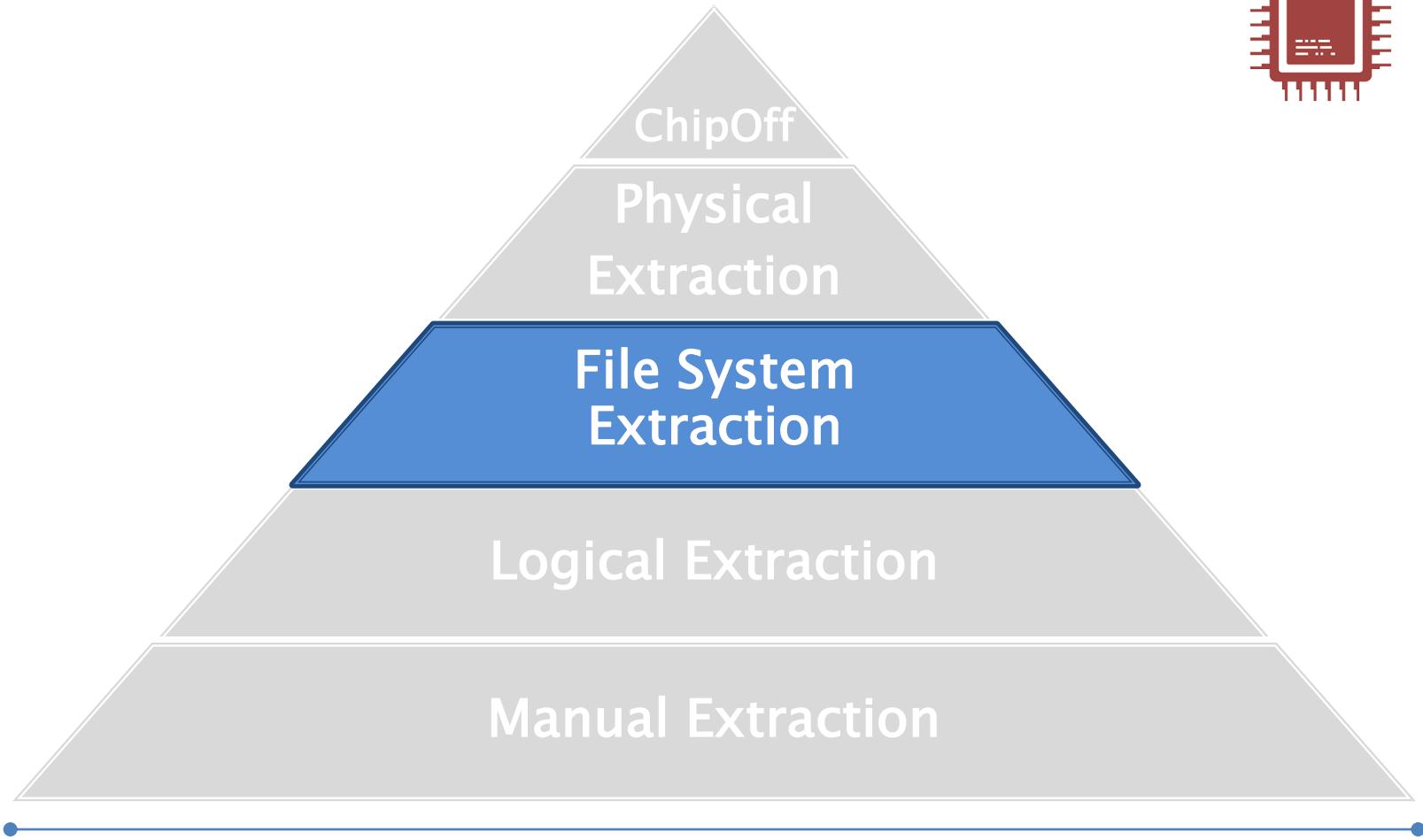
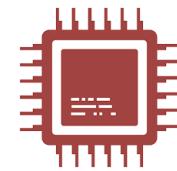
## *Logical Extraction*



- Attachments
- Audio
- Images
- Ringtones
  
- Backup 2016\_05\_20 (001).cal
- Backup 2016\_05\_20 (001).clog
- Backup 2016\_05\_20 (001).MMS
- Backup 2016\_05\_20 (001).PBB
- Backup 2016\_05\_20 (001).SMS
  
- Logical.udf
- Report.html
- Report.xml
- Report\_AudioSection.html
- Report\_CalendarSection.html
- Report\_CallLogsSection.html
- Report\_ContactsSection.html
- Report\_DatabasesSection.html
- Report\_ImagesSection.html
- Report\_MMSSection.html
- Report\_RingtonesSection.html
- Report\_SMSSection.html
- Report\_VideoSection.html

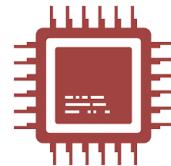


# Mobile Forensics: acquisizione

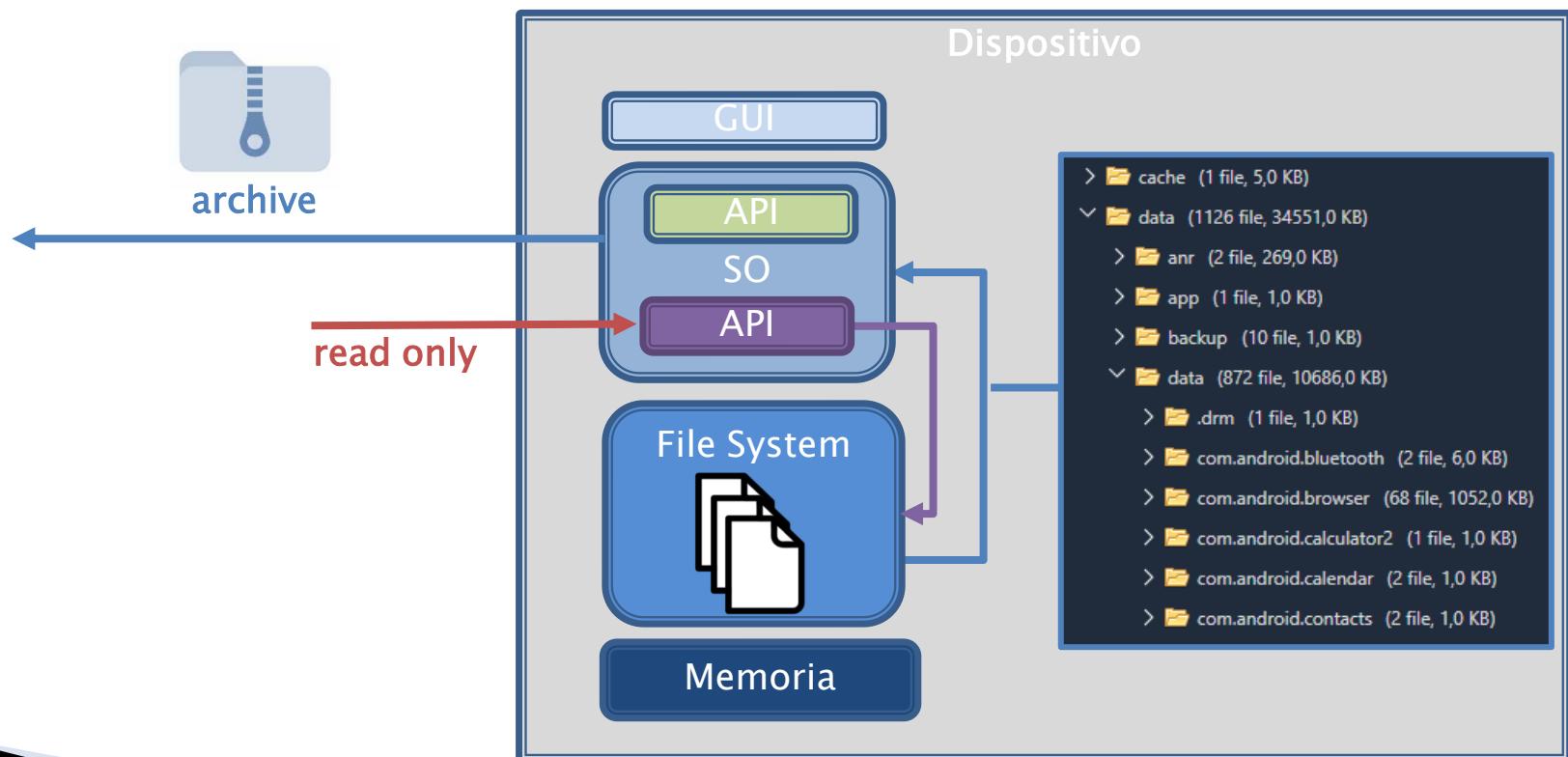


# Mobile Forensics: acquisizione

## *File System Extraction*

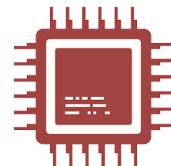


- ▶ Estrazione dei file tramite API del dispositivo



# Mobile Forensics: acquisizione

## *File System Extraction*



### ▶ Risultato:

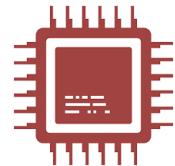
- L'output va processato per visualizzare i dati contenuti:
  - I dati sono contenuti in DB SQLite
  - Possibilità di visualizzare dati cancellati (entry dei DB)

### ▶ Limiti:

- I risultati dipendono dai permessi con cui vengono fatte le richieste:
  - File System Completo: tutta la struttura della live partition.
  - File System Parziale: solo determinate porzioni

# Mobile Forensics: acquisizione

## *File System Extraction*



Smart Phones/PDAs Android

USB cable Original Cable

i

Android Backup

i

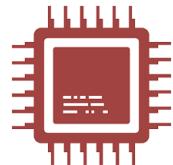
Android Backup APK  
Downgrade

i

FS + App. Sys. files

# Mobile Forensics: acquisizione

## *File System Extraction*



Smart Phones/PDAs Android

USB cable Original Cable

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

**Android:**

**Important:**

Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode.

This method is supported for devices running Android version 4.1 and above and with Developer options enabled.

To enable the Developer options, go to Menu → Settings → About (information) → tap the "Build number" 7 times until it's enabled.

Under Developer options → enable the Android/USB debugging and Stay awake (if available).

**Notice:**

After pressing "Continue" the extraction will start automatically, DO NOT press anything.

If the extraction does not start you will be prompted to select "Back up my data" on the device.

**Note:**

On some devices the "Back up my data" button may be disabled.

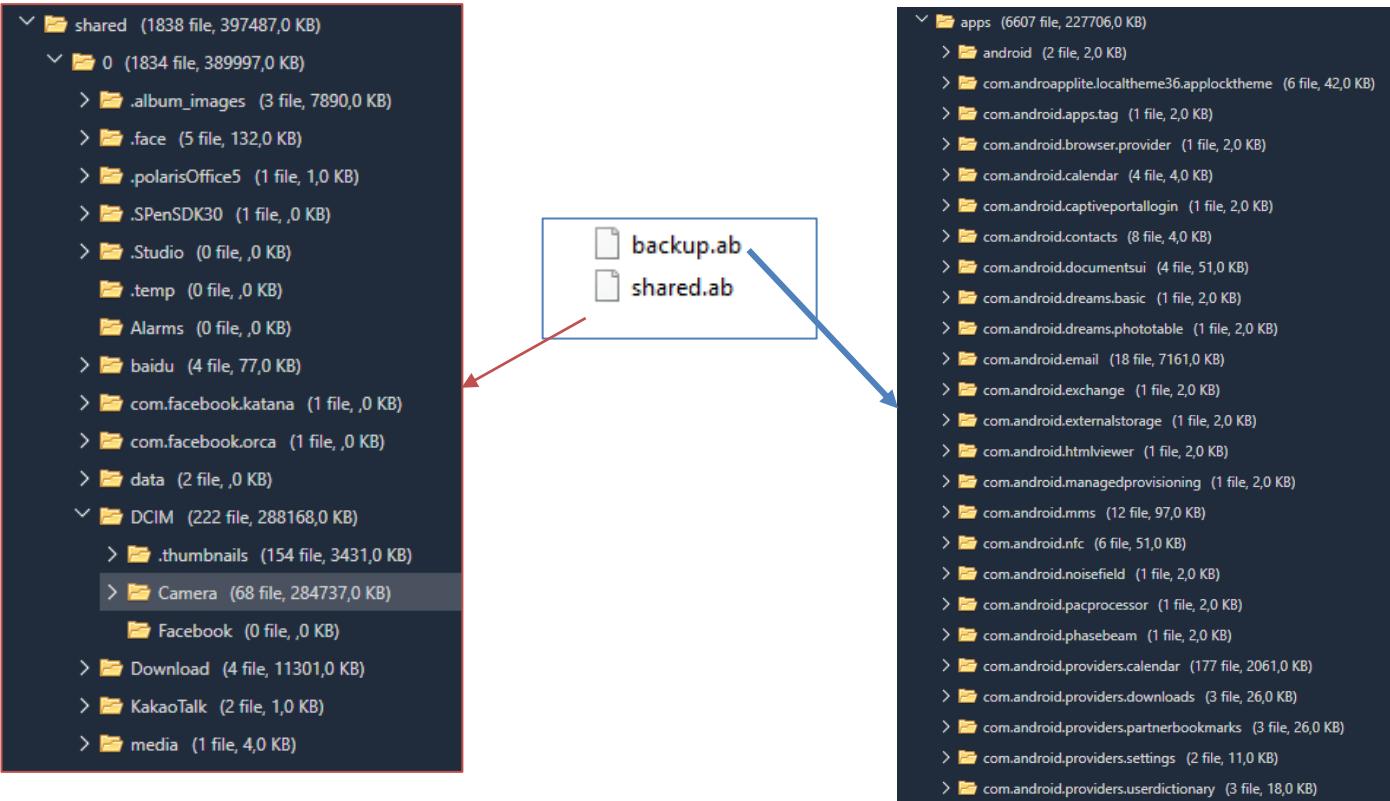
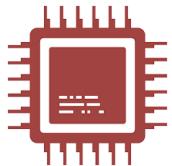
To enable it, enter a password and then press the "Back up my data" button.

To decode the extraction, this password will also be required in Physical Analyzer.

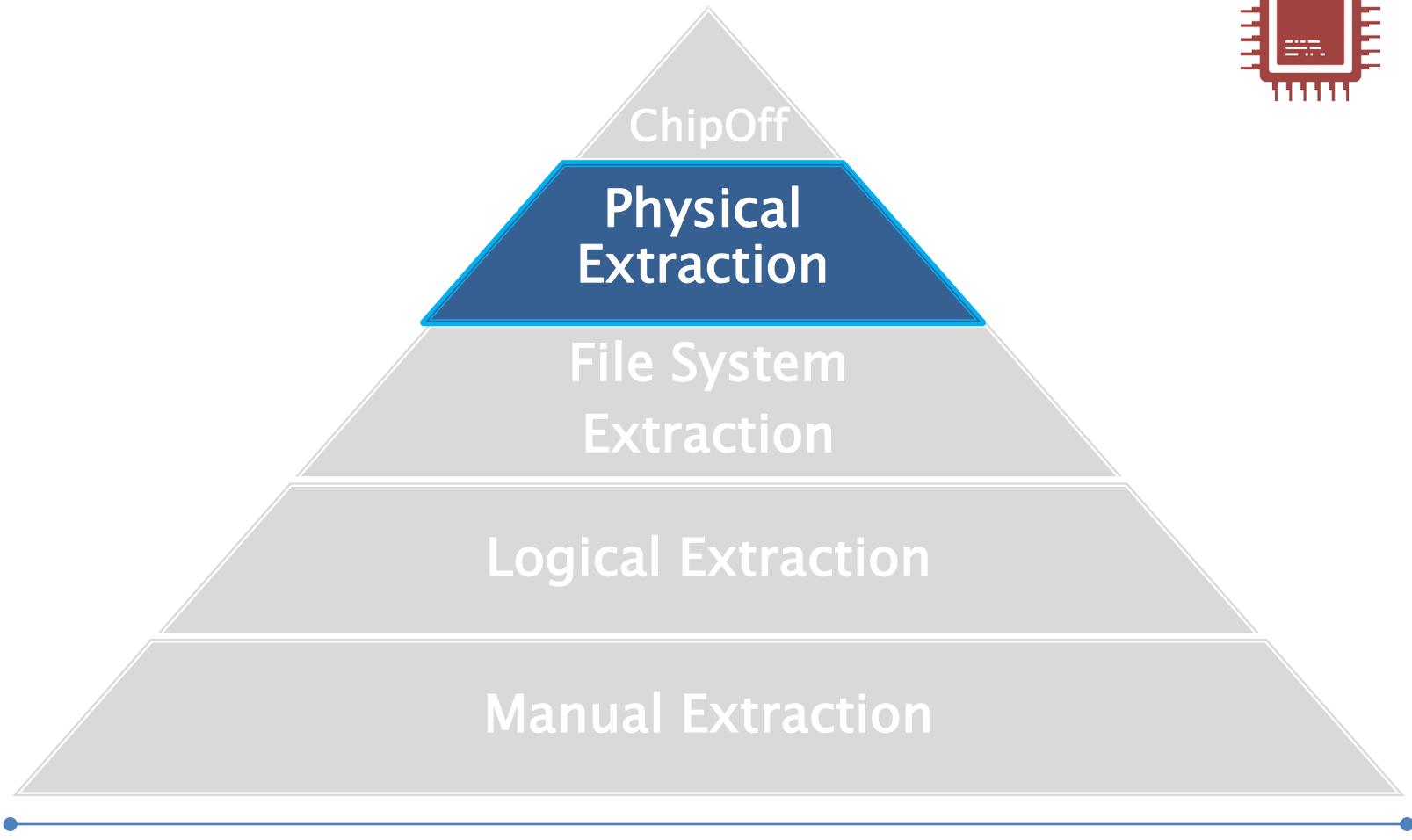
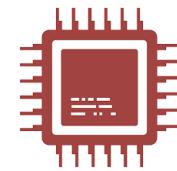
On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue.

# Mobile Forensics: acquisizione

## *File System Extraction*

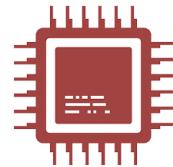


# Mobile Forensics: acquisizione

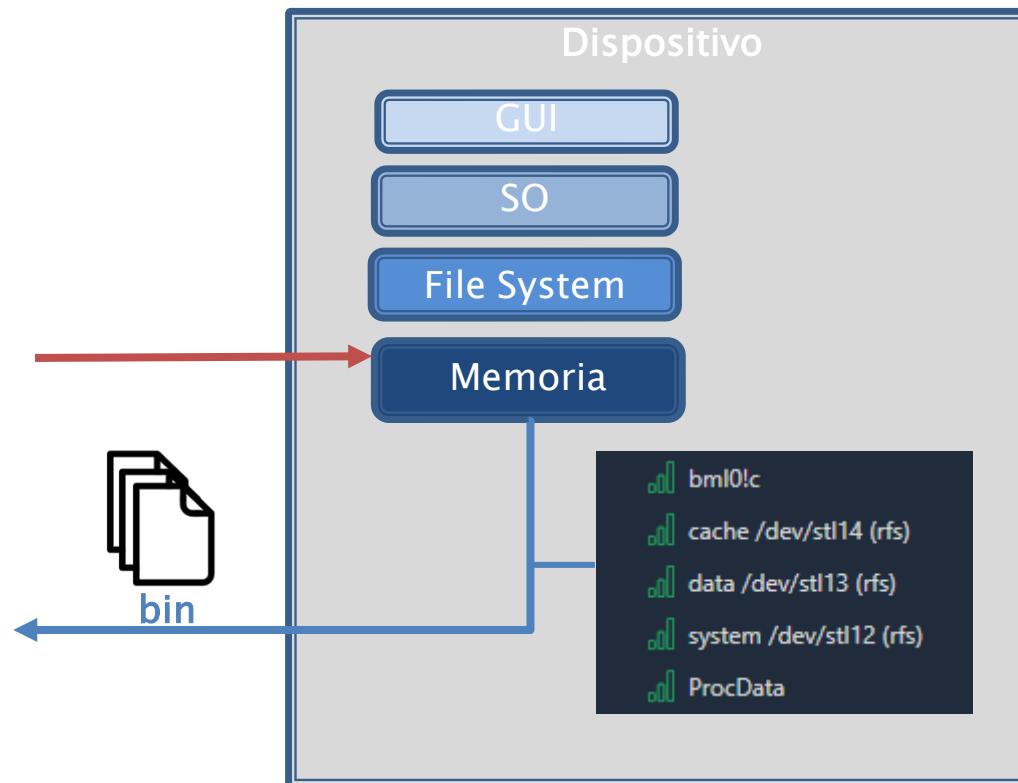


# Mobile Forensics: acquisizione

## *Physical Extraction*

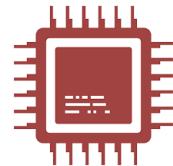


- ▶ Copia bit-a-bit della memoria del dispositivo

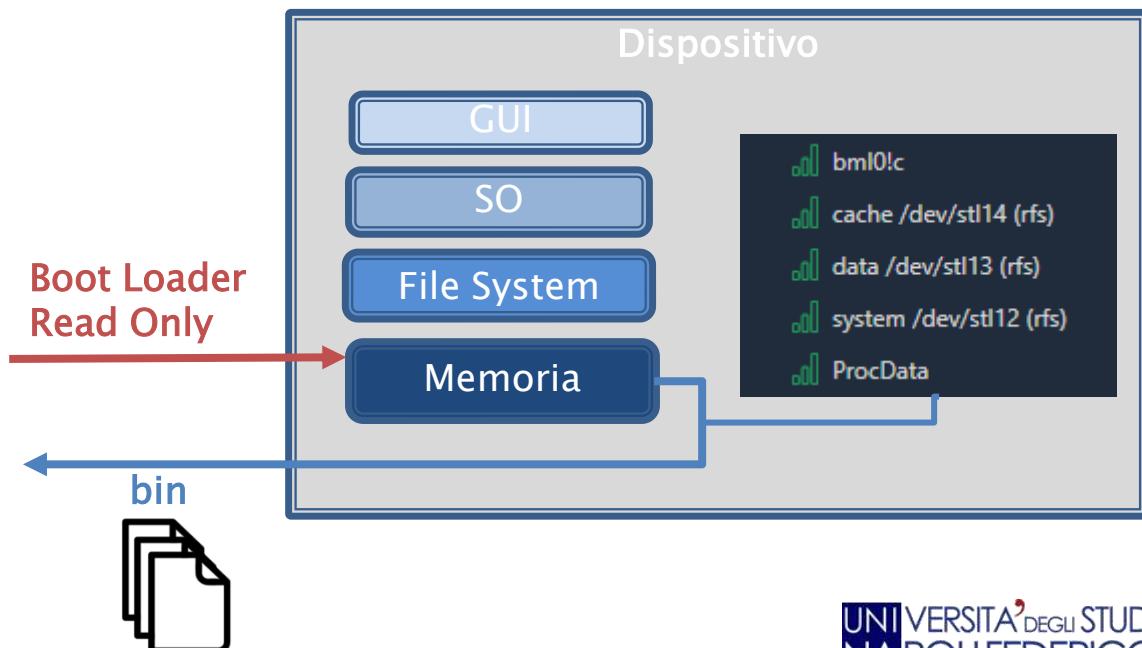


# Mobile Forensics: acquisizione

## *Physical Extraction*

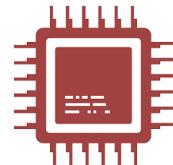


- ▶ Copia bit-a-bit della memoria del dispositivo:
  - Boot loader: codice immesso nella fase di avvio del dispositivo per avviare l'estrazione dati
    - Bug del firmware\Chipset

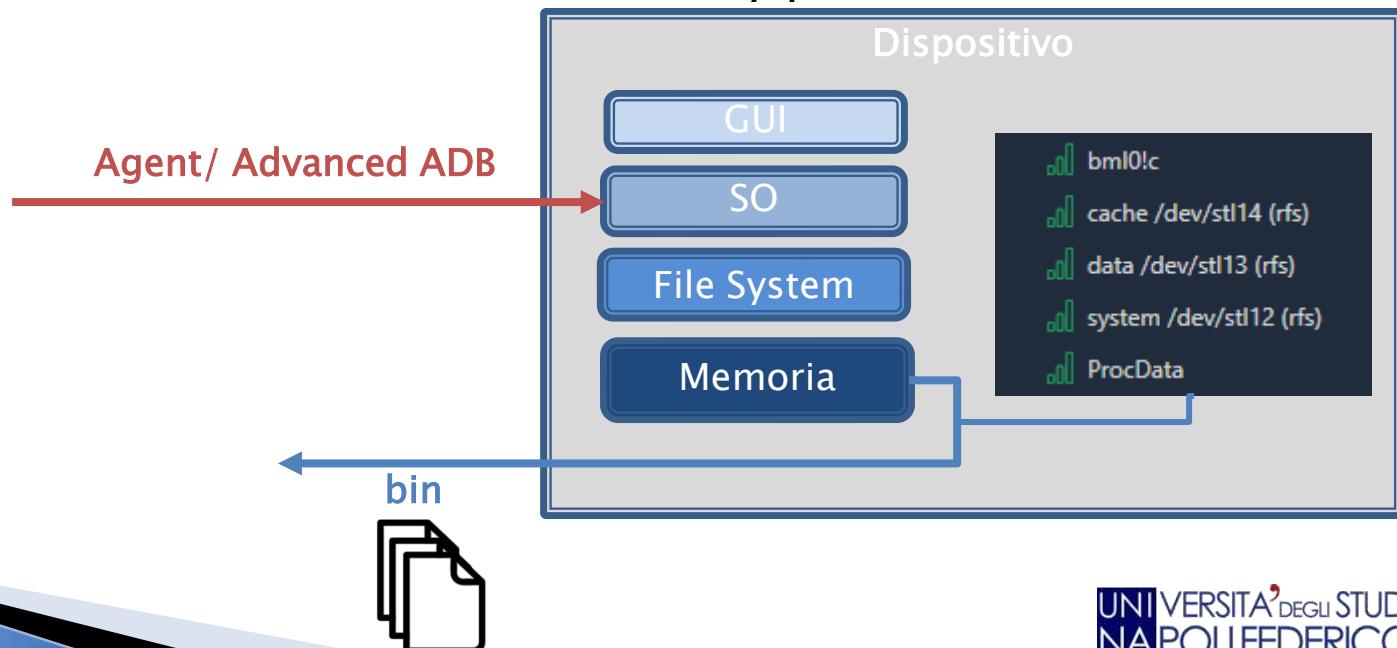


# Mobile Forensics: acquisizione

## *Physical Extraction*

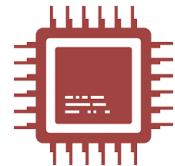


- ▶ Copia bit-a-bit della memoria del dispositivo:
  - Agent: tool installato nel S.O.
    - Bug nel S.O.
  - Advanced ADB(*Android Debug Bridge*):
    - Bug nel S.O. (Android  $\leq$  7.1 & security patch  $\leq$  11/2016)



# Mobile Forensics: acquisizione

## *Physical Extraction*



### ▶ Risultato:

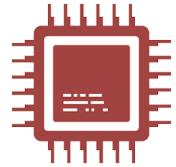
- L'output va processato per visualizzare i dati contenuti
- Recupero di file cancellati (carving)

### ▶ Limiti:

- Produttore del dispositivo
- Chipset
- Versione del S.O.
- Patch di sicurezza

# Mobile Forensics: acquisizione

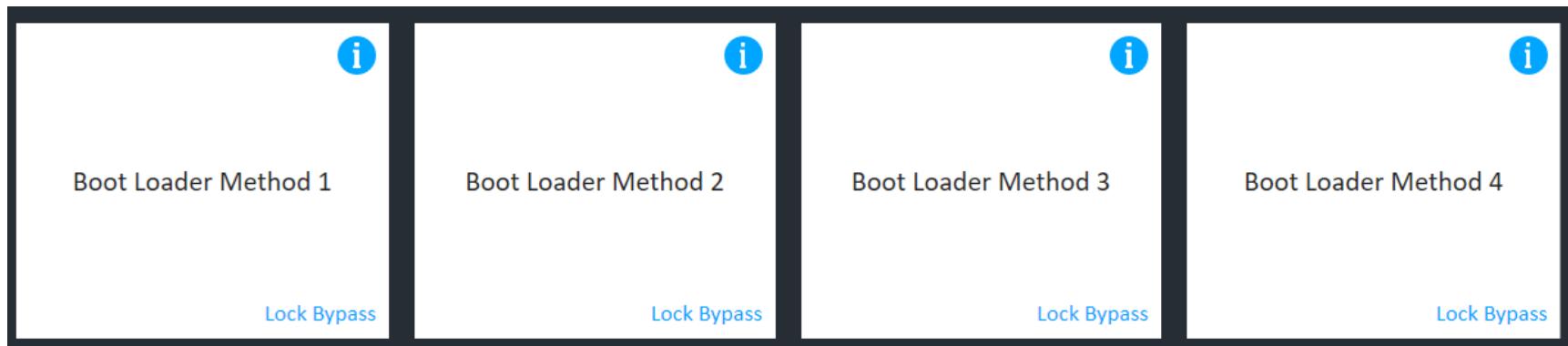
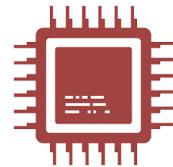
## *Physical Extraction*



All	Vendors	Generic profiles	Recently used
Android 	Qualcomm 	Decrypting Qualcomm 	MTK 
Decrypting MTK 	Decrypting LG MTK 	MTK Live 	Android Bluetooth 

# Mobile Forensics: acquisizione

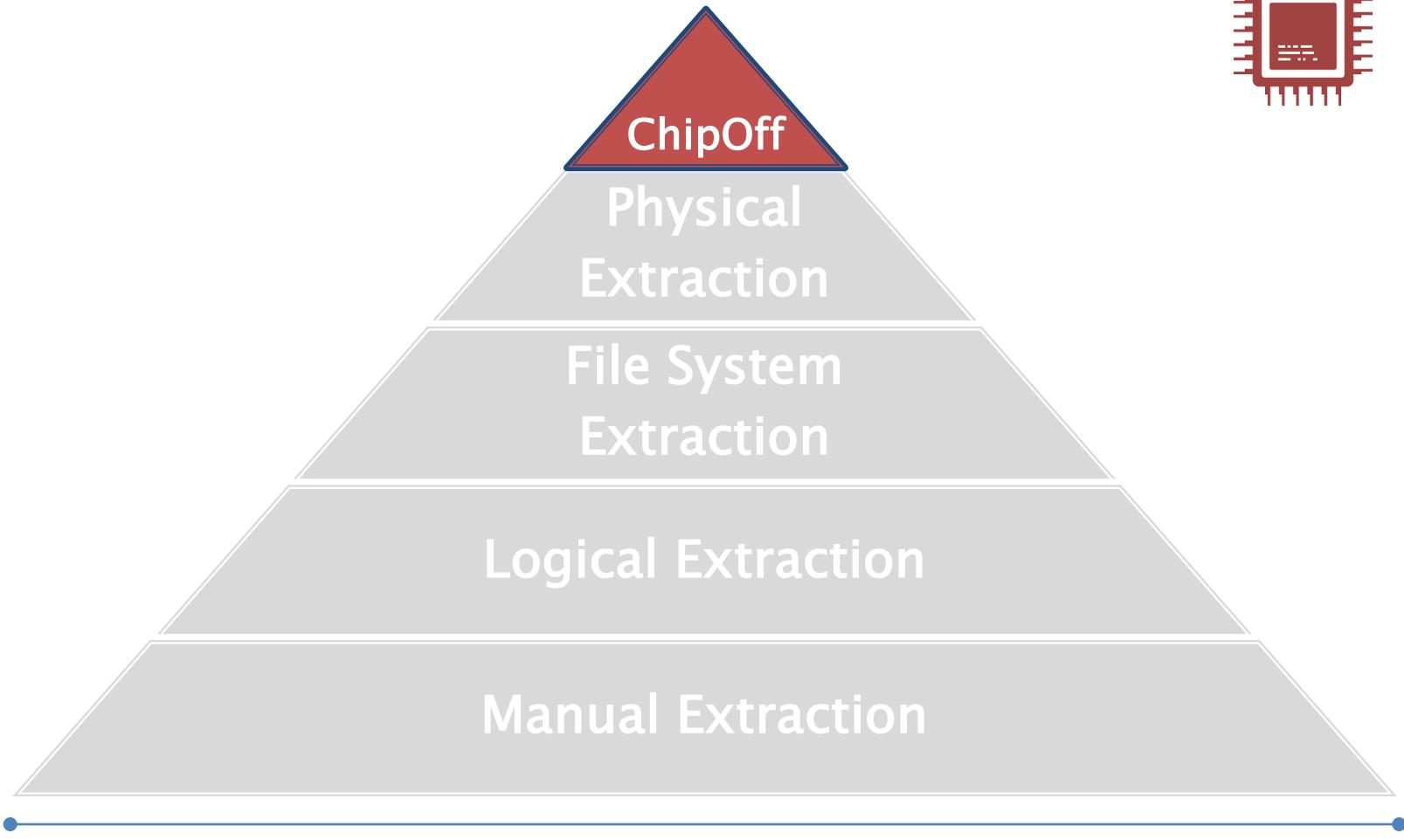
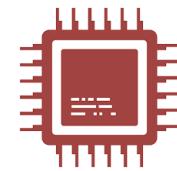
## *Physical Extraction*



A list of extracted data files, each with a small blue icon to its left:

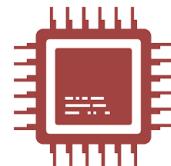
- blk0\_bml0\_c.bin
- blk12\_stl12.bin
- blk13\_stl13.bin
- blk14\_stl14.bin
- log.txt
- proedata.zip

# Mobile Forensics: acquisizione



# Mobile Forensics: acquisizione

## *Chip Off*



- ▶ Estrazione fisica del chip dalla scheda madre
  - Distruzione del dispositivo
- ▶ Limiti:
  - Dispositivo cifrato

# Mobile Forensics

» Analisi



# Mobile Forensics: analisi *i sistemi operativi*

## ▶ O.S. Android:

- Migliaia di produttori e modelli
- Kernel linux: OpenSource
- App

## ▶ Apple iOS:

- Pochi modelli
- Closed
- App

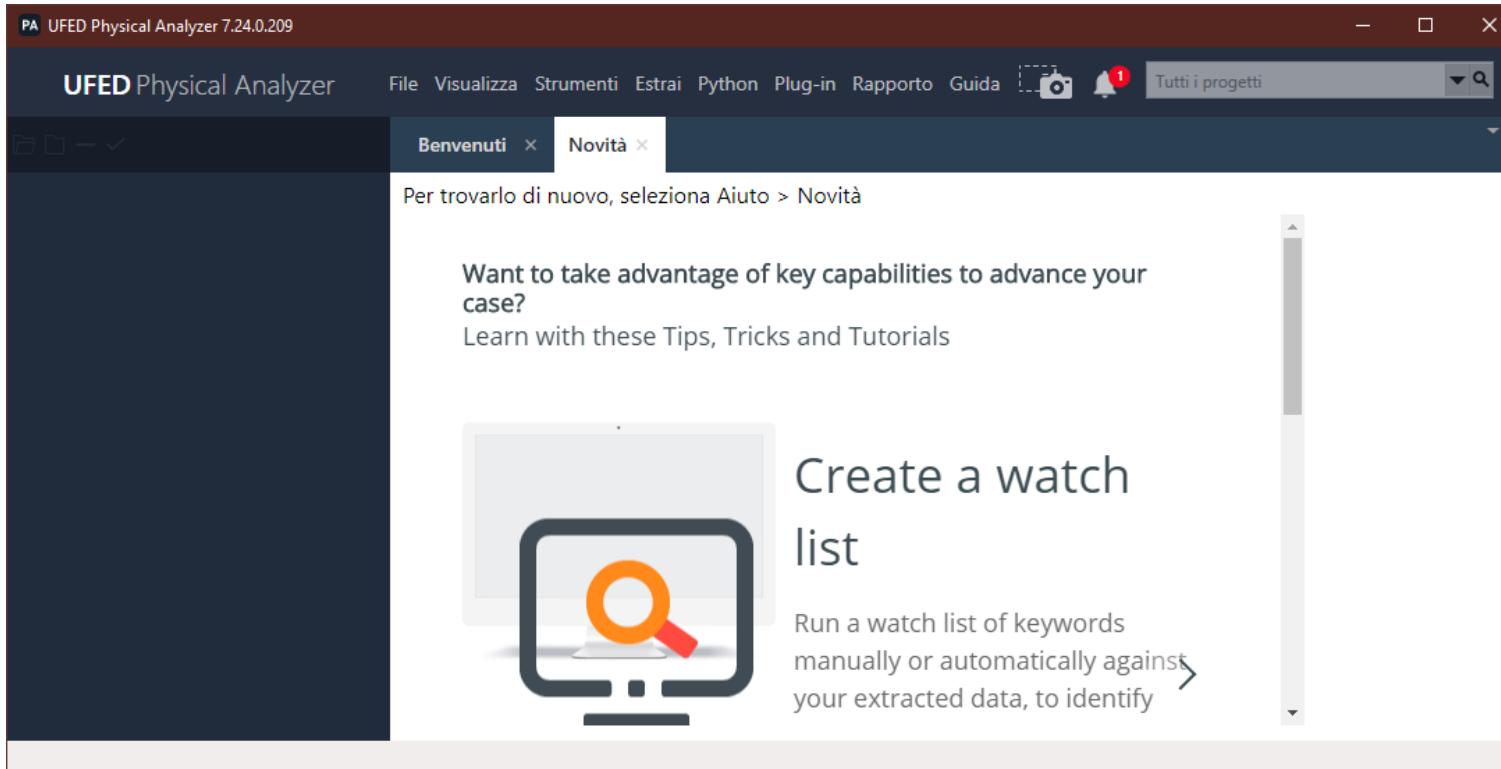
# Mobile Forensics: analisi *App*

- ▶ Estendono la funzionalità del S.O.
- ▶ Rappresentano le principali interazioni con l'utente:
  - Produzione di dati
- ▶ Hanno un proprio dominio

# Mobile Forensics: analisi

## *Strumenti*

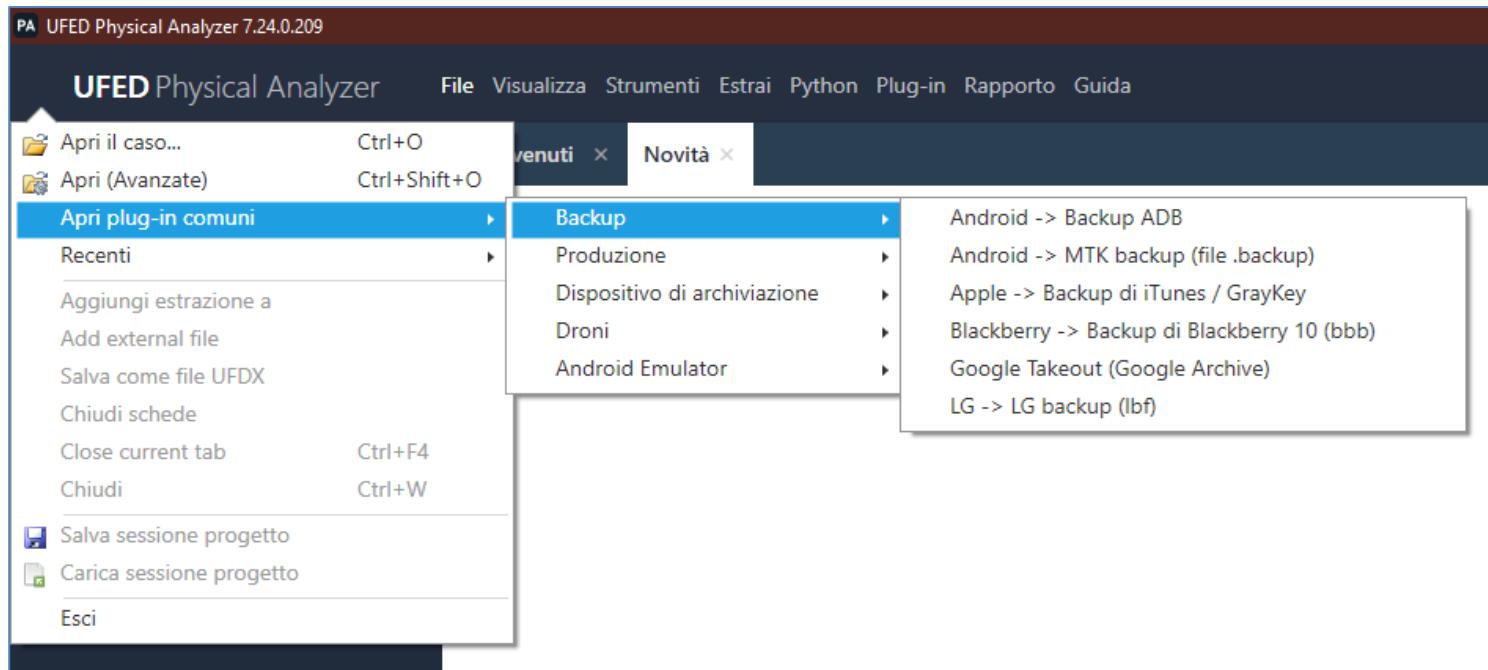
### ► UFED Physical Analyzer



# Mobile Forensics: analisi

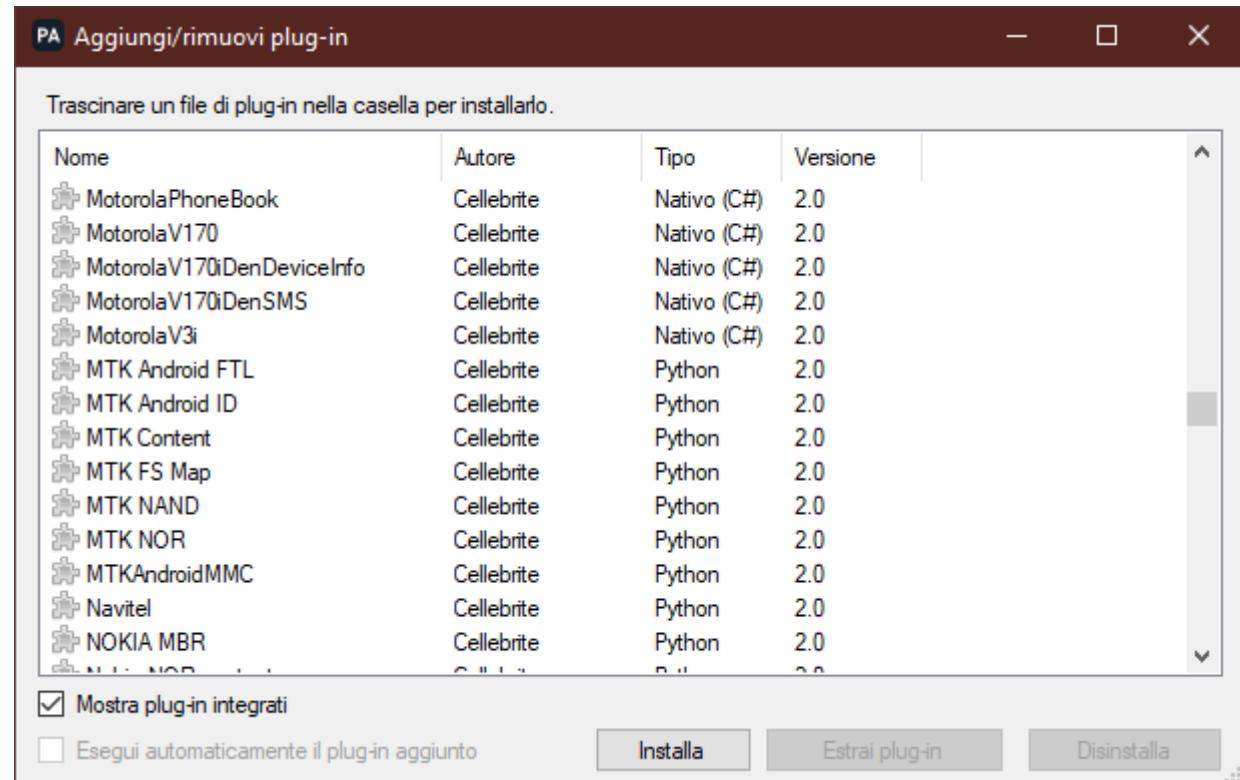
## *Strumenti*

### ► Analisi di backup

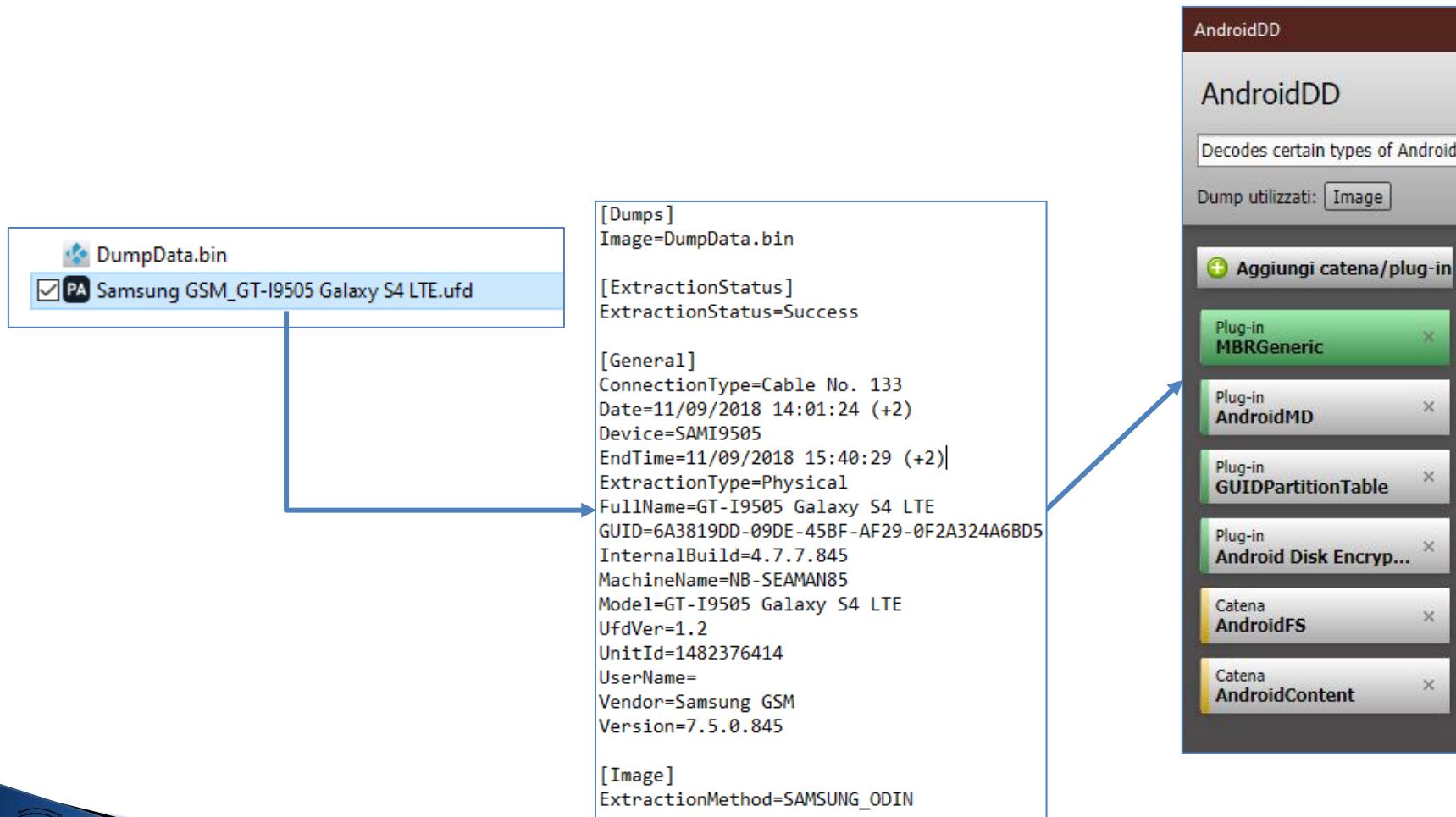


# Mobile Forensics: analisi *plugin*

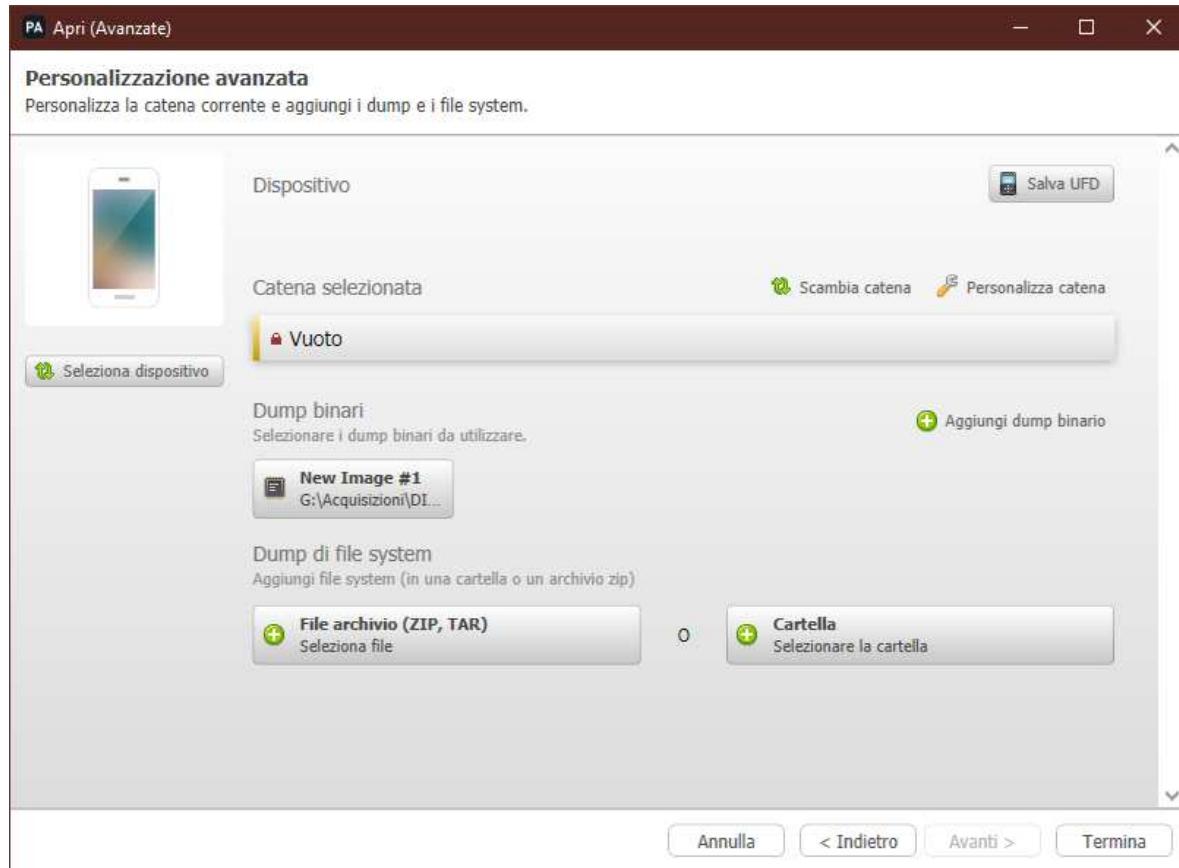
## ► Modulare: plugin



# Mobile Forensics: analisi *plugin*



# Mobile Forensics: analisi *plugin*



PA Apri (Avanzate)

Personalizzazione avanzata

Personalizza la catena corrente e aggiungi i dump e i file system.

Dispositivo

Catena selezionata

Vuoto

Scambia catena Personalizza catena

Selezione dispositivo

Dump binari

Selezionare i dump binari da utilizzare.

New Image #1  
G:\Acquisizioni\DI...

Aggiungi dump binario

Dump di file system

Aggiungi file system (in una cartella o un archivio zip)

File archivio (ZIP, TAR)  
Selezione file

Cartella  
Selezione la cartella

0

Annula < Indietro Avanti > Termina

DumpData

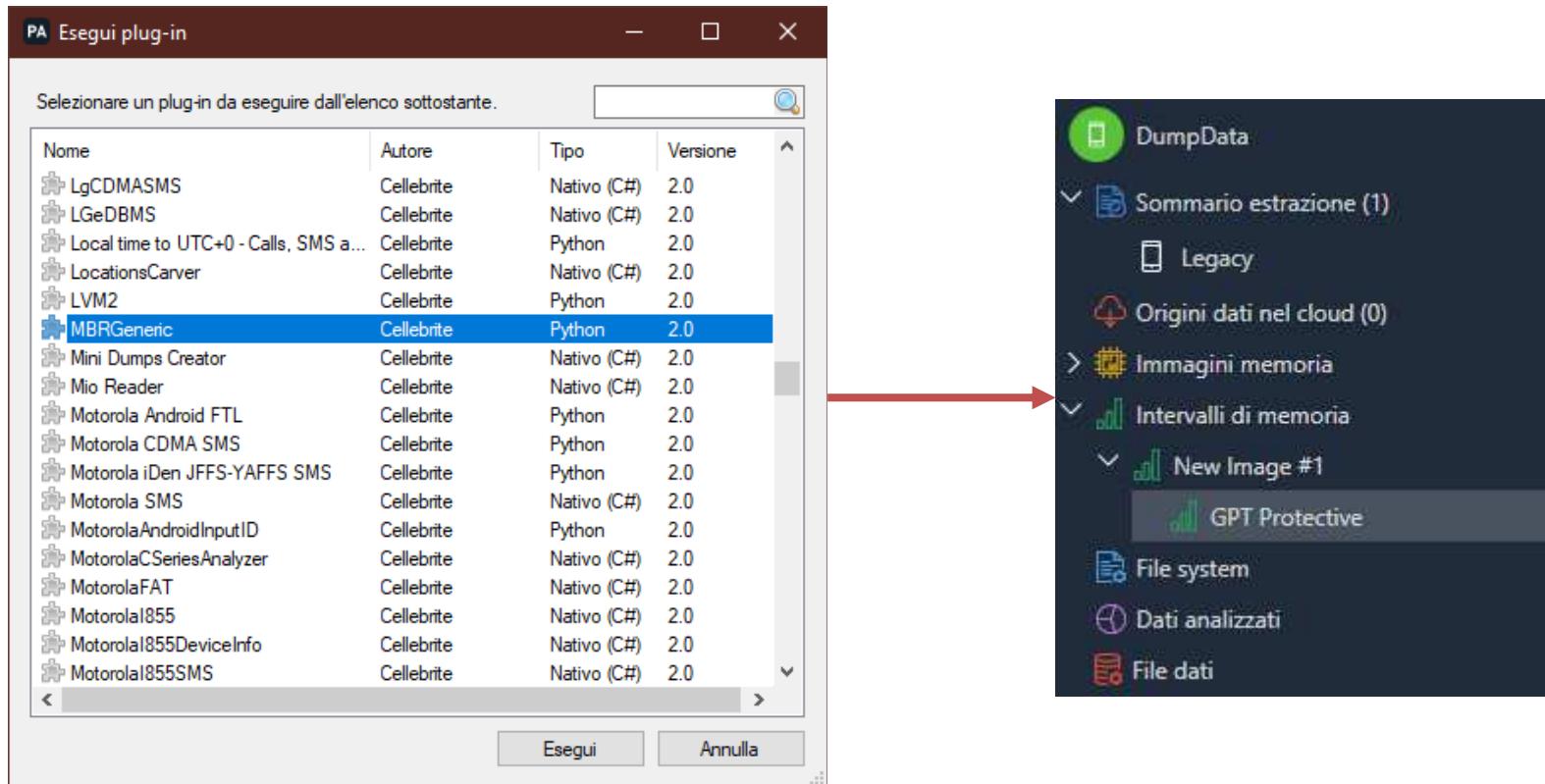
Sommaario estrazione (1)

- Legacy
- Origin dati nel cloud (0)
- Immagini memoria

Intervalli di memoria

- New Image #1
- File system
- Dati analizzati
- File dati

# Mobile Forensics: analisi *plugin*



The image shows a screenshot of a mobile forensic tool's interface. On the left, a dialog box titled "PA Esegui plug-in" lists available plugins. The "MBRGeneric" plugin is selected and highlighted in blue. On the right, the main analysis interface displays a hierarchical tree of extracted data. A red arrow points from the "MBRGeneric" selection in the dialog to the corresponding node in the tree.

PA Esegui plug-in

Selezionare un plug-in da eseguire dall'elenco sottostante.

Nome	Autore	Tipo	Versione
LgCDMASMS	Cellebrite	Nativo (C#)	2.0
LGedbMS	Cellebrite	Nativo (C#)	2.0
Local time to UTC+0 - Calls, SMS a...	Cellebrite	Python	2.0
LocationsCarver	Cellebrite	Nativo (C#)	2.0
LVM2	Cellebrite	Python	2.0
<b>MBRGeneric</b>	<b>Cellebrite</b>	<b>Python</b>	<b>2.0</b>
Mini Dumps Creator	Cellebrite	Nativo (C#)	2.0
Mio Reader	Cellebrite	Nativo (C#)	2.0
Motorola Android FTL	Cellebrite	Python	2.0
Motorola CDMA SMS	Cellebrite	Python	2.0
Motorola iDen JFFS-YAFFS SMS	Cellebrite	Python	2.0
Motorola SMS	Cellebrite	Nativo (C#)	2.0
MotorolaAndroidInputID	Cellebrite	Python	2.0
MotorolaCSeriesAnalyzer	Cellebrite	Nativo (C#)	2.0
MotorolaFAT	Cellebrite	Nativo (C#)	2.0
MotorolaI855	Cellebrite	Nativo (C#)	2.0
MotorolaI855DeviceInfo	Cellebrite	Nativo (C#)	2.0
MotorolaI855SMS	Cellebrite	Nativo (C#)	2.0

Esegui Annulla

DumpData

Sommario estrazione (1)

Legacy

Origini dati nel cloud (0)

Immagini memoria

Intervalli di memoria

New Image #1

GPT Protective

File system

Dati analizzati

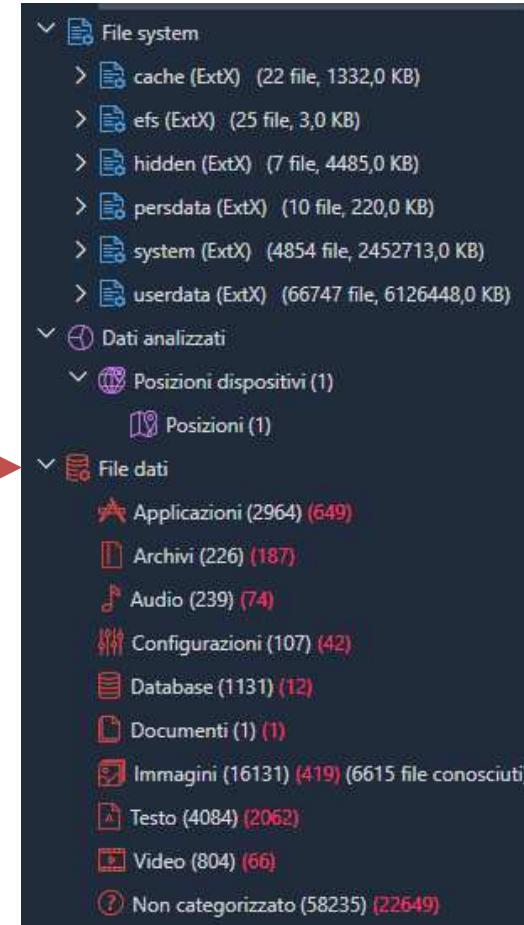
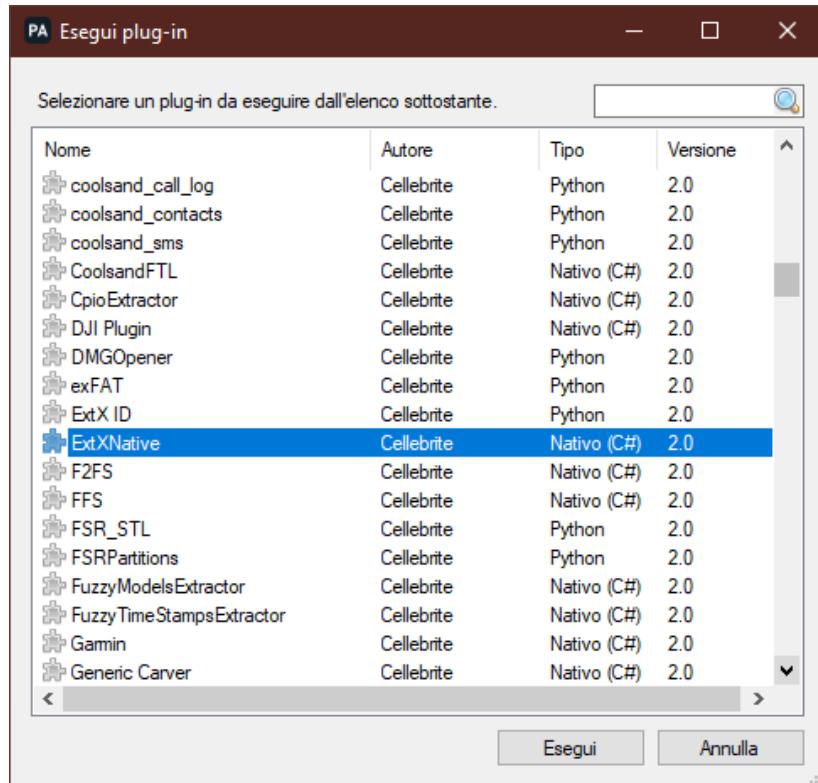
File dati

# Mobile Forensics: analisi *plugin*

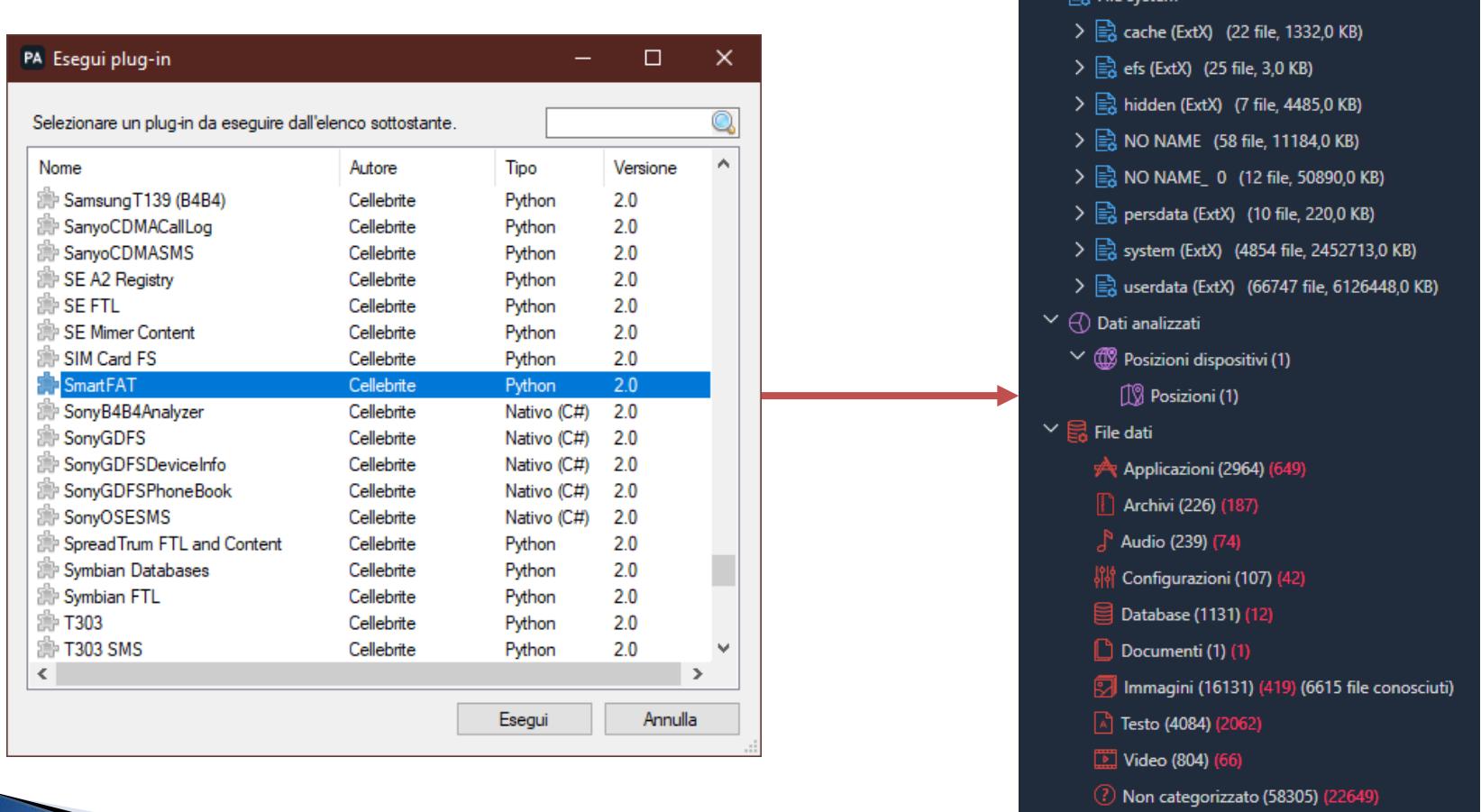
The image shows a screenshot of a mobile forensics tool's interface. On the left, a window titled "Esegui plug-in" displays a list of available plugins. The "GUIDPartitionTable" plugin by Cellebrite, which is selected and highlighted in blue, is shown in the list. The list includes various other plugins such as ExtX ID, ExtXNative, F2FS, FFS, FSR\_STL, FSRPartitions, FuzzyModelsExtractor, FuzzyTime Stamps Extractor, Garmin, Generic Carver, Google Takeout Databases, HFS, iCloudBackupFS, iCloudBackupFS for UFED Cloud, iDenAndroidRearrange, iDenYaffs2, and Image Rename. At the bottom of this window are two buttons: "Esegui" (Execute) and "Annulla" (Cancel). A red arrow points from the "GUIDPartitionTable" entry in the plugin list to the right-hand extraction summary window.

The right-hand window is titled "Sommario estrazione (1)". It shows a hierarchical tree view of the extraction process. The root node is "Legacy". Under "Legacy", there is a node for "Origini dati nel cloud (0)". Below "Legacy" is a node for "Immagini memoria". Under "Immagini memoria", there is a node for "Intervalli di memoria". Under "Intervalli di memoria", there is a node for "Image". Under "Image", there is a node for "GPT Protective". Under "GPT Protective", there is a list of file system components: "aboot", "apnholos", "backup", "boot", "cache", "carrier", "efs", "fota", "fsg", "hidden", "m9kefs1", "m9kefs2", "m9kefs3", and "mdm". To the right of this tree view, there is a vertical list of file system components: "mdm", "modemst1", "modemst2", "pad", "param", "persdata", "persist", "recovery", "rpm", "sbl1", "sbl2", "sbl3", "ssd", "system", "tz", and "userdata". At the bottom of the right-hand window, there are three icons: "File system" (blue folder), "Dati analizzati" (purple circular arrow), and "File dati" (green document).

# Mobile Forensics: analisi *plugin*



# Mobile Forensics: analisi *plugin*



The image shows a screenshot of a mobile forensics application interface. On the left, a window titled "Esegui plug-in" displays a list of available plugins. The list includes various devices and file types, such as SamsungT139 (B4B4), SanyoCDMACallLog, SanyoCDMASMS, SE A2 Registry, SE FTL, SE Mimer Content, SIM Card FS, SmartFAT, SonyB4B4Analyzer, SonyGDFS, SonyGDFSDeviceInfo, SonyGDFSPhoneBook, SonyOSESMS, SpreadTrum FTL and Content, Symbian Databases, Symbian FTL, T303, and T303 SMS. The "SmartFAT" plugin is selected and highlighted with a blue background. On the right, a detailed analysis tree is shown, indicating the structure of the device's file system and the count of files found in various categories like Applications, Archives, Audio, Configurations, Databases, Documents, Images, Text, and Video.

Nome	Autore	Tipo	Versione
SamsungT139 (B4B4)	Cellebrite	Python	2.0
SanyoCDMACallLog	Cellebrite	Python	2.0
SanyoCDMASMS	Cellebrite	Python	2.0
SE A2 Registry	Cellebrite	Python	2.0
SE FTL	Cellebrite	Python	2.0
SE Mimer Content	Cellebrite	Python	2.0
SIM Card FS	Cellebrite	Python	2.0
<b>SmartFAT</b>	<b>Cellebrite</b>	<b>Python</b>	<b>2.0</b>
SonyB4B4Analyzer	Cellebrite	Nativo (C#)	2.0
SonyGDFS	Cellebrite	Nativo (C#)	2.0
SonyGDFSDeviceInfo	Cellebrite	Nativo (C#)	2.0
SonyGDFSPhoneBook	Cellebrite	Nativo (C#)	2.0
SonyOSESMS	Cellebrite	Nativo (C#)	2.0
SpreadTrum FTL and Content	Cellebrite	Python	2.0
Symbian Databases	Cellebrite	Python	2.0
Symbian FTL	Cellebrite	Python	2.0
T303	Cellebrite	Python	2.0
T303 SMS	Cellebrite	Python	2.0

Selezionare un plug-in da eseguire dall'elenco sottostante.

File system

- cache (ExtX) (22 file, 1332,0 KB)
- efs (ExtX) (25 file, 3,0 KB)
- hidden (ExtX) (7 file, 4485,0 KB)
- NO NAME (58 file, 11184,0 KB)
- NO NAME\_0 (12 file, 50890,0 KB)
- persdata (ExtX) (10 file, 220,0 KB)
- system (ExtX) (4854 file, 2452713,0 KB)
- userdata (ExtX) (66747 file, 6126448,0 KB)

Dati analizzati

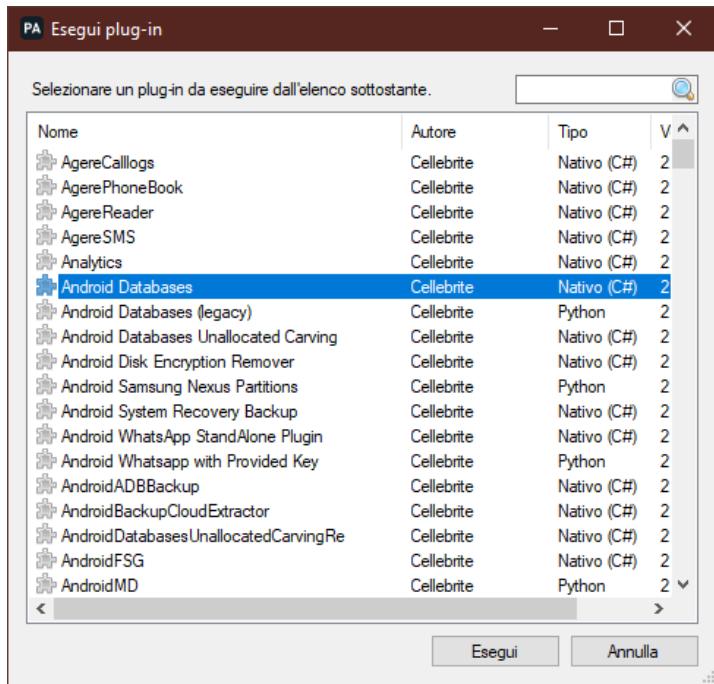
Posizioni dispositivi (1)

- Posizioni (1)

File dati

- Applicazioni (2964) (649)
- Archivi (226) (187)
- Audio (239) (74)
- Configurazioni (107) (42)
- Database (1131) (12)
- Documenti (1) (1)
- Immagini (16131) (419) (6615 file conosciuti)
- Testo (4084) (2062)
- Video (804) (66)
- Non categorizzato (58305) (22649)

# Mobile Forensics: analisi *plugin*



A red arrow points from the "Android Databases" plugin entry in the first screenshot to the corresponding log entry in the second screenshot.

The second screenshot shows a tree view of analyzed data items:

- Dati analizzati
  - Account utenti (43)
  - Calendario (1)
  - Chat (109) (10)
    - Facebook Messenger (47) (576 messaggi)
    - imo (2) (2 messaggi)
    - WhatsApp (60) (10) (842 messaggi)
  - Contatti (763) (125)
  - Cookie (4286) (8)
  - Cronologia Web (2458) (8)
  - Dizionario utente (3613)
  - Downloads (112)
  - Elementi ricercati (365) (17)
  - E-mail (694)
  - Eventi del dispositivo (8)
  - Info sulle app
  - Messaggi MMS (3)
  - Messaggi SMS (368)
  - Notifiche del dispositivo (6) (5)
    - Password (832)
  - Posizioni dispositivi (4699) (42)
  - Reg. chiam (1010) (140)
    - Reti wireless (4092) (13)
  - Riempimento automatico (55)
  - Ripetitori cellulari (657) (29)
  - Utenti dispositivo (1)

Log entries for the "Android Databases" plugin are listed in a red-bordered box:

- 04:16 Running plugin Android Databases (debug=False)
- 04:16 Parsing GooglePlay
- 04:16 Parsing Permissions
- 04:16 Parsing App Usage
- 04:16 Parsing App Usage
- 04:16 Parsing AndroidID
- 04:16 Parsing Build Prop
- 04:16 Parsing Keystore
- 04:16 Parsing ChatOn\_3.5.839
- 04:16 Parsing Calendar
- 04:16 Parsing providers\_settings
- 04:16 Parsing S Note
- 04:16 Parsing Google+\_6.5.0.104456905
- 04:16 Parsing DropBox\_102.2.2
- 04:16 Parsing AnalyzeMedia
- 04:16 Parsing WiFi
- 04:16 Parsing WiFi\_12.8.74 (020308-204998136)
- 04:16 Parsing Accounts

# Mobile Forensics: analisi *plugin*

- ✓ Chat (109) (10)
  - Facebook Messenger (47) (576 messaggi)
  - imo (2) (2 messaggi)
  - WhatsApp (60) (10) (842 messaggi)



#					Partecipanti	Ora inizio	Ultima attività	
40			4	2	491725 [REDACTED]@s.whatsapp.net 491521 [REDACTED]7@s.whatsapp.net Habib [REDACTED] (proprietario)	19/11/2016 20:04(UTC+0)	19/11/2016 22:11(UTC+0)	
41			7	1	491521 [REDACTED]@s.whatsapp.net Habib [REDACTED] (proprietario)	06/09/2016 21:41(UTC+0)	21/11/2016 23:57(UTC+0)	
42			5	8	4915739 [REDACTED]@s.whatsapp.net 4915210 [REDACTED]@s.whatsapp.net kanistafa [REDACTED] Habib [REDACTED] (proprietario)	28/08/2016 17:19(UTC+0)	14/10/2016 19:20(UTC+0)	
43			16	28	2	4915731 [REDACTED]@s.whatsapp.net 4915210 [REDACTED]@s.whatsapp.net ☺ Habib [REDACTED] (proprietario)	24/08/2016 18:19(UTC+0)	27/12/2016 22:22(UTC+0)
44			46	49	2	4915214 [REDACTED]@s.whatsapp.net 49152103 [REDACTED]@s.whatsapp.net +491521 [REDACTED] Habib [REDACTED] (proprietario)	22/08/2016 16:11(UTC+0)	04/10/2017 20:29(UTC+0)
45			6	1	4915210 [REDACTED]@s.whatsapp.net [REDACTED] F [REDACTED] (proprietario)	12/08/2016 11:24(UTC+0)	15/08/2016 16:49(UTC+0)	
46			2	9	2	447481 [REDACTED]@s.whatsapp.net Rafi [REDACTED] 49152103 [REDACTED]7@s.whatsapp.net Habib [REDACTED] (proprietario)	10/08/2016 07:44(UTC+0)	23/05/2017 19:39(UTC+0)
47			27	2	2	4915788 [REDACTED]@s.whatsapp.net Queen [REDACTED] 4915210 [REDACTED]@s.whatsapp.net Habib [REDACTED] (proprietario)	08/08/2016 12:10(UTC+0)	15/08/2016 16:52(UTC+0)

# Mobile Forensics: analisi *plugin*

Numero righe	Nome
1	_jobqueue-WhatsAppJobManager.db
1948	axolotl.db
6	chatsettings.db
0	chatsettingsbackup.db
3	Cookies
7713	emojidictionary.db
1	google_app_measurement_v2.db
1	hsmpacks.db
1	location.db
2	media.db
1206	msgstore.db
399	wa.db
3	Web Data
0	web_sessions.db



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)

# COMPUTER FORENSICS

## Lezione 23: Fase Finale *la Relazione Tecnica*



A.A. 2021/22

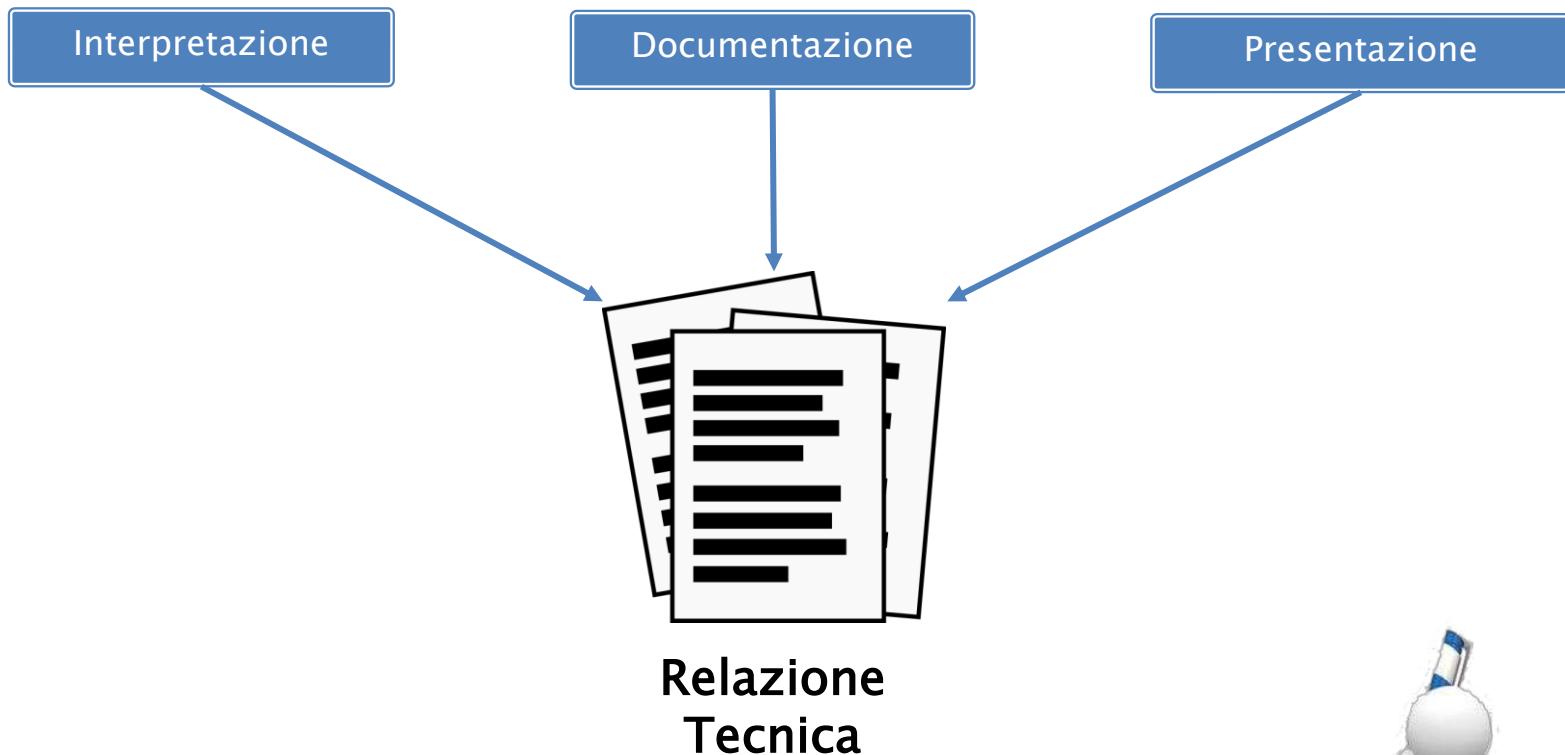
Dott. Lorenzo LAURATO



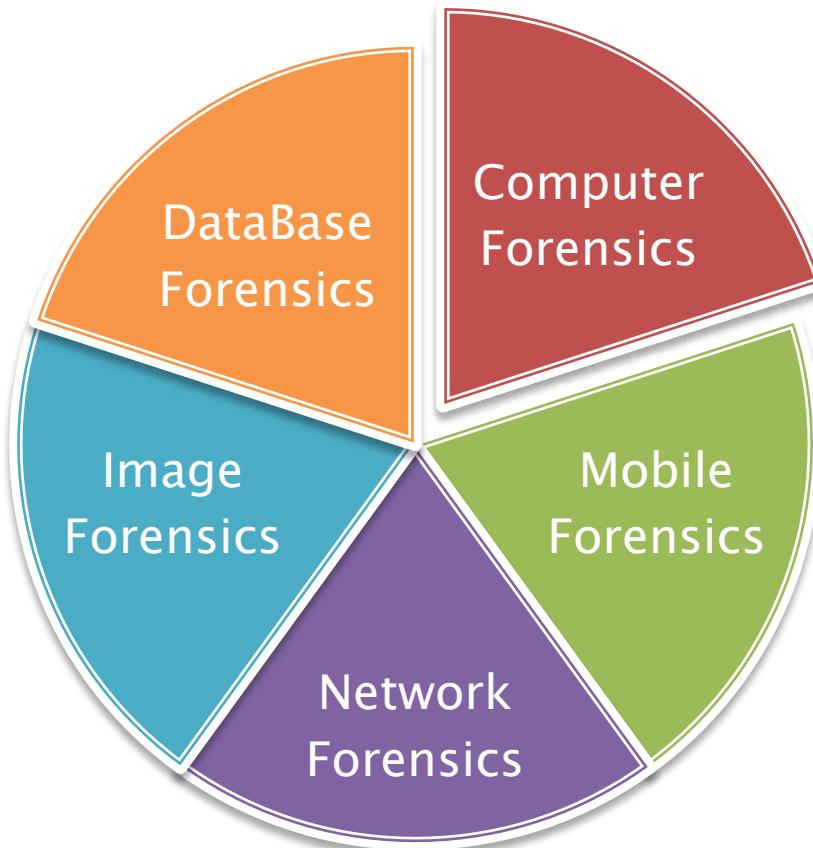
# Fasi



# Fasi



# Digital Forensics



# La prova digitale

## ▶ CONTRO:

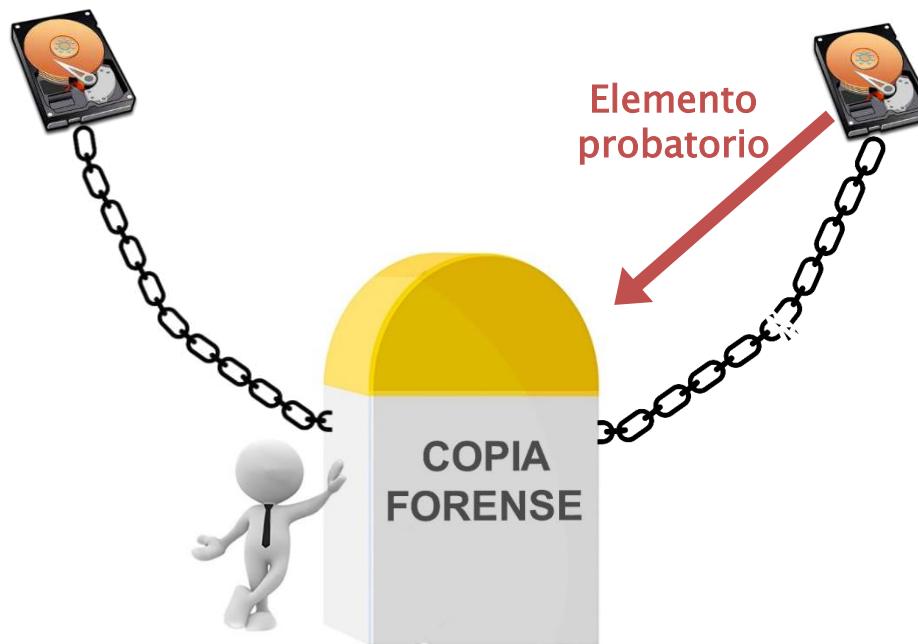
- Facilmente corruttibile

## ▶ PRO:

- Duplicazione

# Accertamenti...

Accertamento tecnico ripetibile



Accertamento tecnico irripetibile

Accertamento  
tecnico ripetibile

# L'accertamento ripetibile

- ▶ Agire in modo da non alterare la prova
- ▶ Agire in modo da documentare ogni azione compiuta su di essa
- ▶ Porre la controparte in condizione di replicare quanto fatto

# La relazione tecnica

- ▶ Base di partenza: quesito
- ▶ Descrizione degli strumenti Hardware e Software impiegati
- ▶ Descrizione delle azioni che hanno portato/non portato risultati
- ▶ Scopo: chiunque deve poter giungere alle medesime conclusioni

# La relazione tecnica

ESEMPIO: *indagine di pedopornografia*

1. Ricerca di immagini residenti
2. Ricerca di immagini in archivi compressi e posta elettronica
3. Ricerca di programmi P2P (*Es.: eDonkey, BitTorrent, etc.*)
  - a) Diffusione?
4. Ricerca file cancellati
5. Ricerca di periferiche di archiviazione agganciate
6. Analisi steganografica

# La relazione tecnica

- ▶ Descrizione dettagliata di hardware e software impiegato

deft



Autopsy®  
BASIS  
TECHNOLOGY



Eric Zimmerman's  
TOOLS



ACCESSDATA®  
Forensic Toolkit (FTK)



# La relazione tecnica

## Descrizione e valutazioni

- ▶ Parte Descrittiva: dettagliata ed accurata:
  - Documentazione fotografica
- ▶ Parte valutativa:
  - Motivazioni
  - Descrizione dell'iter logico
  - *Giuridicamente non è vincolante*

# La relazione tecnica

## Forma

- ▶ Quattro parti:
  - Parte Epigrafica: *indicazione degli estremi del P.P., P.M., Giudice, descrizione dell'incarico, parti presenti ad un accertamento, etc.*
  - Parte Descrittiva: *illustrazione degli accertamenti e/o ricostruzioni compiuti*
  - Parte Valutativa: *risposta ai quesiti con motivazione esaustiva delle conclusioni*
  - Parte Riassuntiva: *esposizione sintetica della risposta ad ogni quesito*
- ▶ Chiara ed intellegibile:
  - Impiego di grafici, illustrazioni, tavelle, etc.

# La relazione tecnica

## Forma

1) Parte Epigrafica: *indicazione degli estremi del P.P., P.M., Giudice, descrizione dell'incarico, parti presenti ad un accertamento, etc.*

<p>Procedimento Penale Nr. 8800/20xx R.G.N.R.</p> <p>Procura della Repubblica presso il Tribunale di Napoli</p> <p>Consulenza Informatica Forense</p> <p>Pubblico Ministero Dott.ssa ....</p> <p>Consulente Tecnico del PM Dott. Lorenzo LAURATO</p>	<p>CONSULENZA INFORMATICA R.G.N.R. 8800/20xx</p> <p><b>PREMESSA</b></p> <p>Con verbale datato 25/05/20xx, alle ore 14.00, negli Uffici della Procura della Repubblica presso il Tribunale di Napoli, la SVI conferiva al sottoscritto Dott. Lorenzo Laurato, mandato di consulenza tecnica informatica, nell'ambito del Procedimento Penale n. 8800/20xx R.G.N.R.</p> <p>Quesito dell'incarico:</p> <p><b>"Proceda il c.t. ad effettuare analisi preliminare di primo livello su tutti i supporti informatici che saranno rinvenuti nel corso dell'attività di perquisizione di cui a separato provvedimento;</b></p> <p><b>Proceda altresì ad effettuare copia forense ed analisi del contenuto del materiale informatico che sarà eventualmente sottoposto a sequestro."</b></p>
--	--

# La relazione tecnica

## Forma

### 2) Parte Descrittiva: *illustrazione degli accertamenti e/o ricostruzioni compiuti*

CONSULENZA INFORMATICA  
R.G.N.R. 8800/20xx

Le acquisizioni dei supporti di memoria da analizzare vengono effettuate impiegando, a seconda del caso:

- il "Forensic Quest" e/o il "Forensic Dossier", prodotti dalla "Logicube" e/o il "Forensic Duplicator TD1" della "Tableau", dispositivi hardware autonomi, con sistema operativo Linux based embedded, concepiti per la realizzazione di copie forensi di qualsiasi tipo di hard disk: le modalità di funzionamento degli strumenti impediscono qualsiasi tipo di scrittura, anche accidentale, sul supporto di origine, preservandone il contenuto.

CONSULENZA INFORMATICA  
R.G.N.R. 8800/20xx

**Tecnica**

**L'analisi**

L'analisi delle immagini prodotte dal dispositivo mobile è stata eseguita impiegando lo strumento della Cellebrite Ltd denominato "**UFED Physical Analyzer 5.1**".



Il reperto catalogato "CELSAM", relativo al dispositivo Cellulare Samsung SM-G357FZ Galaxy Ace 4, è stato acquisito impiegando lo strumento denominato Cellebrite UFED, così come specificato nei paragrafi iniziali della presente relazione.

Tale acquisizione non ha permesso di estrarre i dati delle applicazioni presenti sul dispositivo e nella fattispecie, l'applicazione di messaggistica istantanea denominata "WhatsApp".

Per tale motivo solo per l'estrazione dei database dell'applicazione "WhatsApp" è stato impiegato lo strumento software denominato "**WhatsApp Xtract 2.5.8**".

# La relazione tecnica

## Forma

### 3) Parte Valutativa: *risposta ai quesiti con motivazione esaustiva delle conclusioni*

Una prima analisi sulla memoria del dispositivo è stata eseguita allo scopo di determinare la presenza del reato di "stalking" compiuto ai danni della p.o. "**Maria ROSSI**". Da tale analisi si evidenziano i seguenti riscontri:

La ricerca all'interno della rubrica del dispositivo cellulare in oggetto eseguita mediante il nominativo e l'utenza telefonica della p.o. "Maria ROSSI" ha avuto esito negativo.

Successivamente è stata eseguita una ricerca, mediante l'utenza telefonica della p.o., nell'intero contenuto del dispositivo: ciò ha evidenziato la presenza di nr. 2 elementi all'interno del registro chiamate:

From: +3	[REDACTED]	Scricciolo	22/12/2015 17:24:19(UTC+0)	00:01:10	Incoming
To: +393	[REDACTED]	Scricciolo	22/12/2015 17:23:40(UTC+0)	00:00:00	Outgoing

Da tale evidenza inoltre si può presumere che precedentemente l'utenza telefonica della p.o. era rubricata all'interno del dispositivo cellulare con il nominativo "**Scricciolo**".

# La relazione tecnica

## Forma

- 4) **Parte Riassuntiva:** *esposizione sintetica della risposta ad ogni quesito*

CONSULENZA INFORMATICA  
R.G.N.R. 8800/20xx

### CONCLUSIONI

**"Proceda il c.t. ad effettuare analisi preliminare di primo livello su tutti i supporti informatici che saranno rinvenuti nel corso dell'attività di perquisizione di cui a separato provvedimento;**

**Proceda altresì ad effettuare copia forense ed analisi del contenuto del materiale informatico che sarà eventualmente sottoposto a sequestro."**

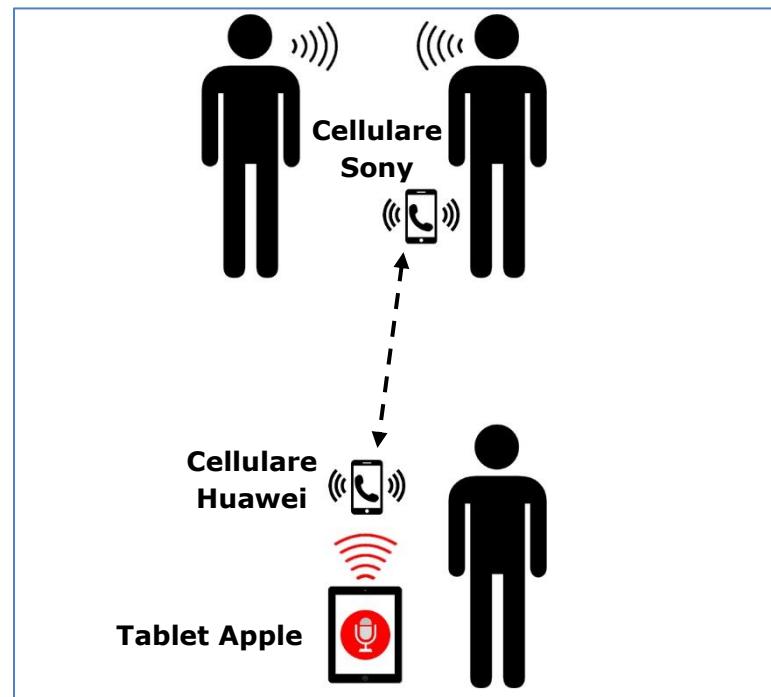
Tutto il restante materiale informatico sottoposto a sequestro e consegnato al sottoscritto CTU, è stato clonato attraverso tecniche di computer forensics, adottando tutte le procedure e le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

L'acquisizione forense è avvenuta rispettando le "**Best Practices**" riconosciute a livello internazionale dallo "*IACIS (International Association of Computer Investigative Specialists)*".

# La relazione tecnica

## Forma

- ▶ Chiara ed intellegibile:
  - Impiego di grafici, illustrazioni, tavole, etc.



# Digital Forensics

»» Un caso di Computer Forensics



# PREMESSA

**Il quesito del PM recita testualmente:**

- a) identifichi l'autore del software installato sui pc in sequestro e che consentiva di non inviare le giocate al concessionario FiveBet;
- b) spieghi il meccanismo di funzionamento di quel programma;
- c) accerti, attraverso l'analisi della memoria, l'esistenza di dati che consentano di individuare altre persone che erano connesse con i PC condividendo il programma e determini il numero di giocate gestite con tale programma;
- d) riferisca quant'altro utile ai fini delle indagini;

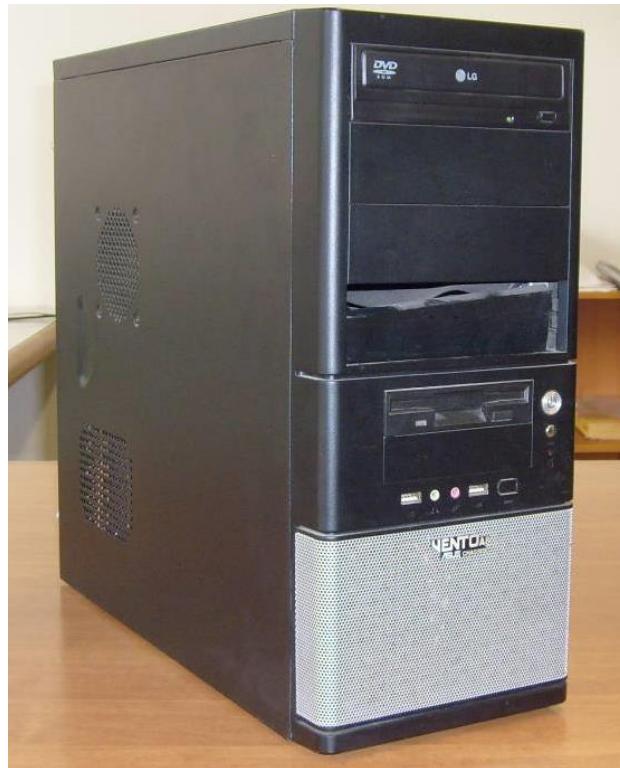
# LA COPIA FORENSE



02/03/2009 12:58

# LA COPIA FORENSE

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049



02/03/2009 13:04

# LA COPIA FORENSE

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049



# LA COPIA FORENSE

## *descrizione degli strumenti*

- **Tableau T15 Forensic SATA:**
  - **Write Block:** strumento che impedisce qualsiasi scrittura, anche accidentale, sul supporto di origine
- **AccessData FTK Imager 2.5.3.14:** software forense utilizzato per la generazione della copia forese.
  - **Hash MD5 e SHA1:** Il software *certifica* digitalmente la copia forense calcolando l'hash del disco origine e della copia generata.
  - **File LOG:** riassumono l'attività di clonazione effettuata, con le indicazioni dei file generati e la verifica, conclusa con esito positivo, del calcolo degli algoritmi di Hash .

# LA COPIA FORENSE

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049



Calcolo Hash MD5:  
**ad75597184687bbe223eac94e9406792**

Calcolo Hash SHA1:  
**cbe75bf8ead1daa38250ed6f54e7c65dc1ed9a01**

# L'ANALISI

## *preliminare*

Analisi del file system mediante lo strumento  
**AccessData FTK 3.3**

- Prime informazioni sul profilo dell’utente e sui software installati

# L'ANALISI

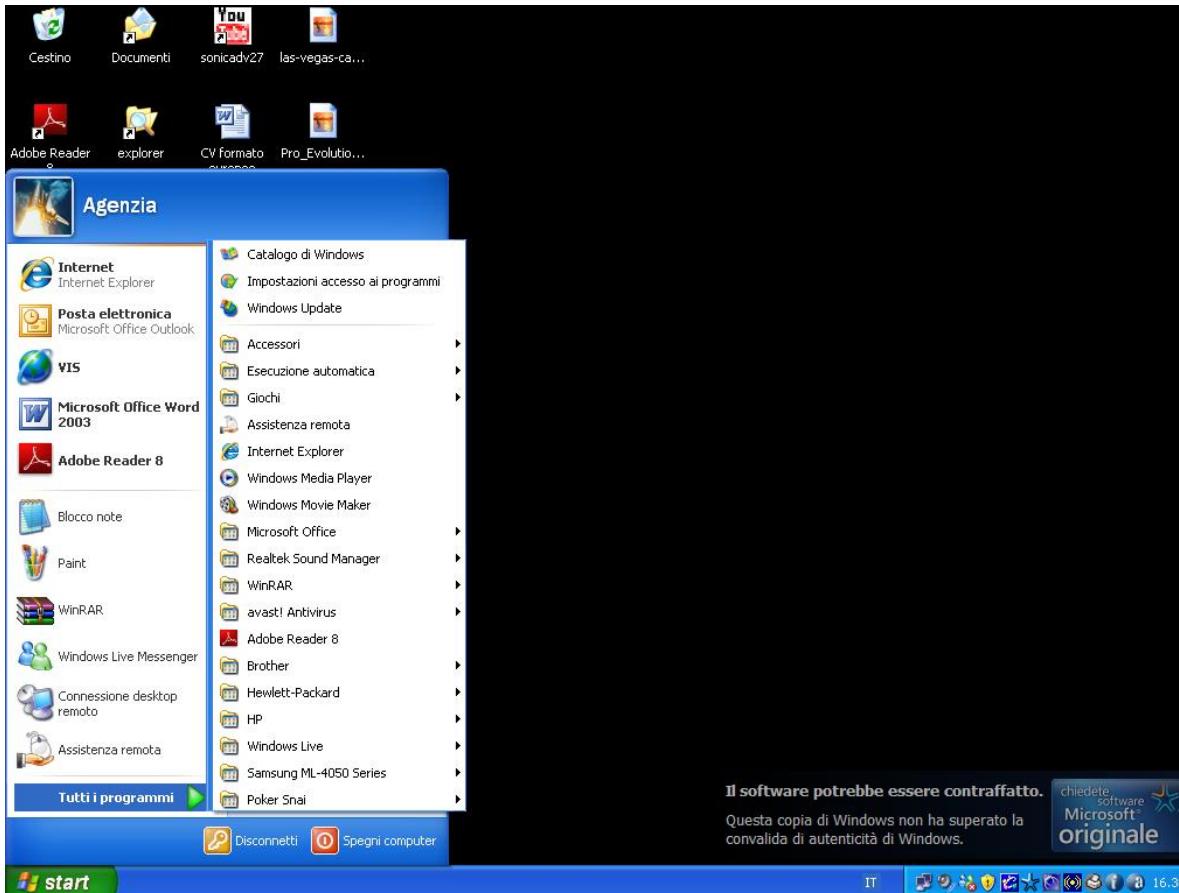
## *la virtualizzazione*

- La “*virtualizzazione*” delle immagini “DD”, in pratica il clone del personal computer, da la possibilità di avviare il personal computer come macchina virtuale all’interno del proprio sistema operativo, tale visione è utile per meglio definire l’utilizzo della macchina analizzata e per un’analisi di primo livello delle informazioni da recuperare;
- Consente di ottenere a livello di utente una vista dell’ambiente da esaminare, il tutto senza modificare l’immagine, poiché tutte le modifiche apportate sono scritte in un file separato;
- E’ avvenuta utilizzando il software open source, **LiveView vers. 0.6**: è uno strumento forense che crea una macchina virtuale “**VMware**” a partire da un’immagine disco o da un disco fisico.

# L'ANALISI

## *la virtualizzazione*

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

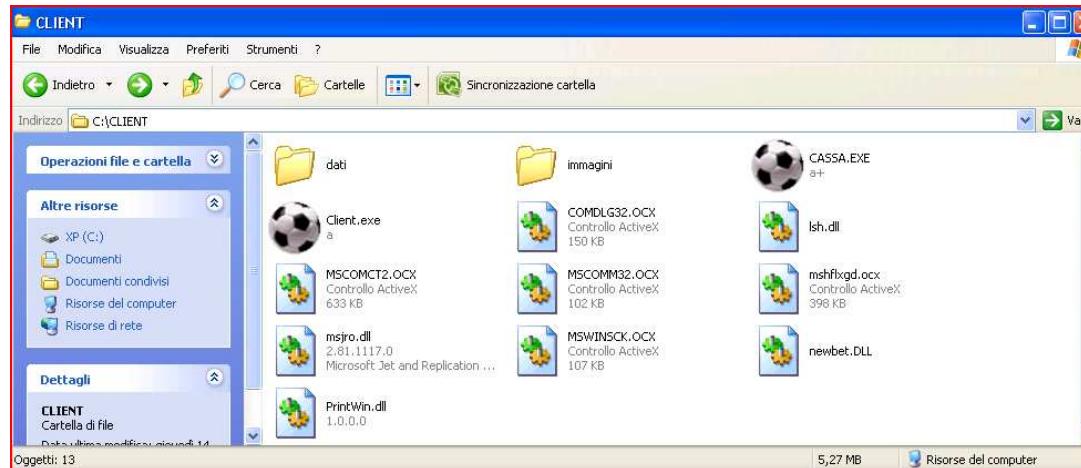


# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

Avendo necessità di individuare software utili alla gestione delle scommesse sportive telematiche tramite internet di eventi sportivi, si è passati alla analisi del contenuto del PC in maniera approfondita.

Le icone presenti sul desktop, evidenziano la presenza di due icone di interesse, denominate rispettivamente “**VIS**” e “**Client**”, le quali “*puntano*” ad una cartella comune, individuata nella directory principale “**C:**”, denominata “**Client**”:

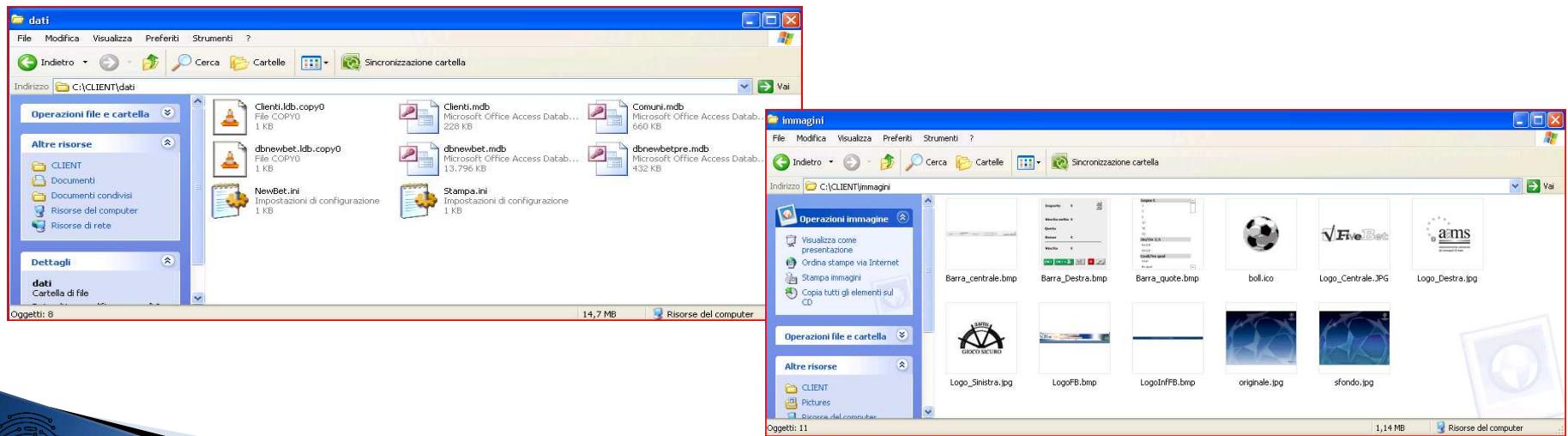


# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

Nella cartella sono presenti due file eseguibili, “Client.exe” e “CASSA.EXE” individuati dal collegamento delle due icone precedentemente citate, oltre una serie di file a supporto delle due applicazioni.

Le sottocartelle “dati” e “immagini” contengono rispettivamente una serie di archivi mdb (Access) e una serie di immagini.



# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

Il primo tentativo è stato quello di “lanciare” il file eseguibile denominato “**Client.exe**”, l’esito è stato negativo, un messaggio di errore blocca l’esecuzione del programma ed impedisce la corretta esecuzione, un secondo tentativo di esecuzione del programma denominato “**Cassa.exe**” restituiva il medesimo risultato negativo:



Probabilmente qualche tipo di protezione, evita la normale esecuzione del software, non restava che analizzare le “*chiamate al sistema*” utilizzate dal software in questione, per fare ciò si utilizzava il programma denominato “**Filemon**”.

# L'ANALISI

## FILEMON:

E' un programma che mostra informazione sui file che si stanno eseguendo nel sistema operativo, effettua un monitoraggio e mostra le informazioni in tempo reale sull'attività del sistema di file di un computer.

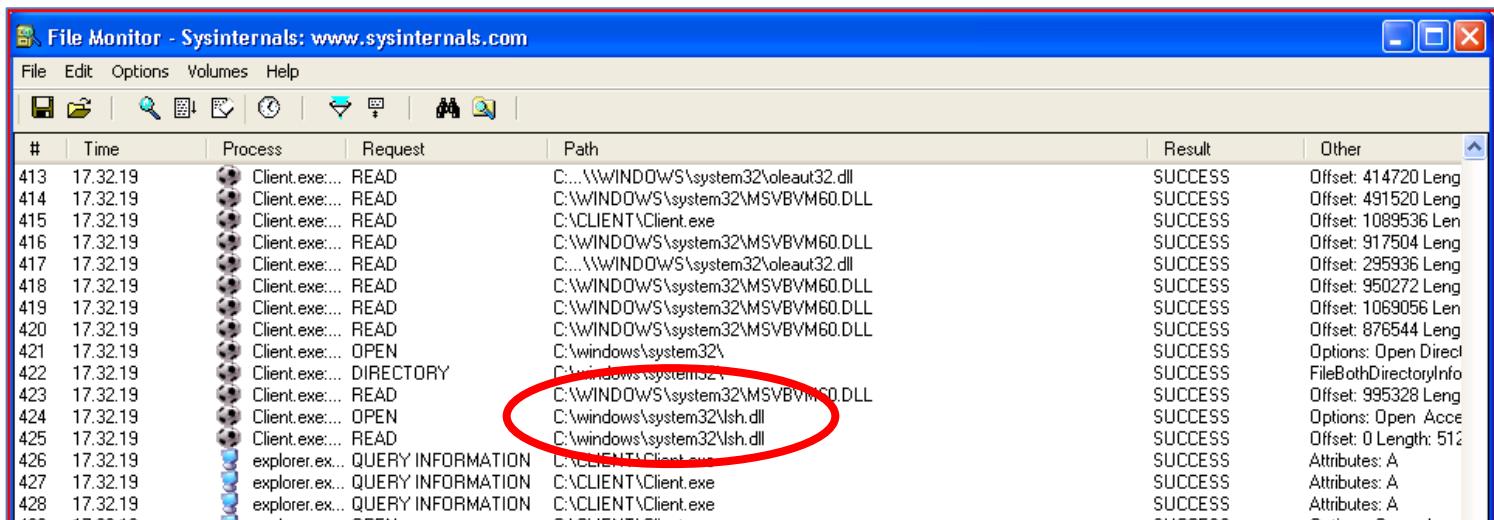
Le sue avanzate capacità fanno di FileMon un poteroso strumento per osservare la maniera in cui lavora Windows, scrutando come le applicazioni usano i file e le DLL, e facendo un inseguimento dei problemi del sistema o dei file di configurazione delle applicazioni.

# L'ANALISI

## Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

Opportunamente configurato e filtrato di tutte le procedure non utili alle indagini in corso, si è focalizzato l'interesse sul comportamento del sistema operativo e del programma “**Client.exe**”;

nel momento in cui viene tentata l'esecuzione, oltre alle comuni chiamate a file di configurazione e a dll di sistema, indispensabili per il funzionamento del sistema operativo di windows, si notavano alcune anomalie su file non noti in ambiente Windows:

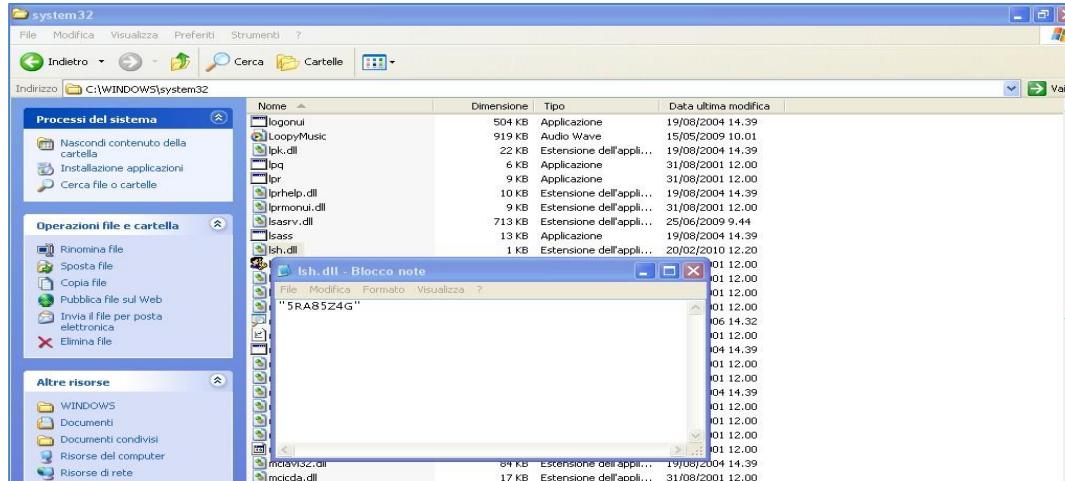


#	Time	Process	Request	Path	Result	Other
413	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Offset: 414720 Leng
414	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\MSVBVM60.DLL	SUCCESS	Offset: 491520 Leng
415	17.32.19	Client.exe....	READ	C:\CLIENT\Client.exe	SUCCESS	Offset: 1089536 Len
416	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\MSVBVM60.DLL	SUCCESS	Offset: 917504 Leng
417	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Offset: 295936 Leng
418	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\MSVBVM60.DLL	SUCCESS	Offset: 950272 Leng
419	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\MSVBVM60.DLL	SUCCESS	Offset: 1069056 Leng
420	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\MSVBVM60.DLL	SUCCESS	Offset: 876544 Leng
421	17.32.19	Client.exe....	OPEN	C:\windows\system32\	SUCCESS	Options: Open Direct
422	17.32.19	Client.exe....	DIRECTORY	C:\windows\system32\	SUCCESS	FileBothDirectoryInfo
423	17.32.19	Client.exe....	READ	C:\WINDOWS\system32\MSVBVM60.DLL	SUCCESS	Offset: 995328 Leng
424	17.32.19	Client.exe....	OPEN	C:\windows\system32\lsh.dll	SUCCESS	Options: Open Acce
425	17.32.19	Client.exe....	READ	C:\windows\system32\lsh.dll	SUCCESS	Offset: 0 Length: 512
426	17.32.19	explorer.ex...	QUERY INFORMATION	C:\CLIENT\Client.exe	SUCCESS	Attributes: A
427	17.32.19	explorer.ex...	QUERY INFORMATION	C:\CLIENT\Client.exe	SUCCESS	Attributes: A
428	17.32.19	explorer.ex...	QUERY INFORMATION	C:\CLIENT\Client.exe	SUCCESS	Attributes: A
429	17.32.19		OPEN	C:\CLIENT\lsh.dll	SUCCESS	

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

Una dll denominata “**Ish.dll**”, appariva tra i file in uso al software, tale dll non rappresenta un file conosciuto in ambiente windows, e grazie a *filemon*, è stato possibile individuare la posizione all'interno del file system.

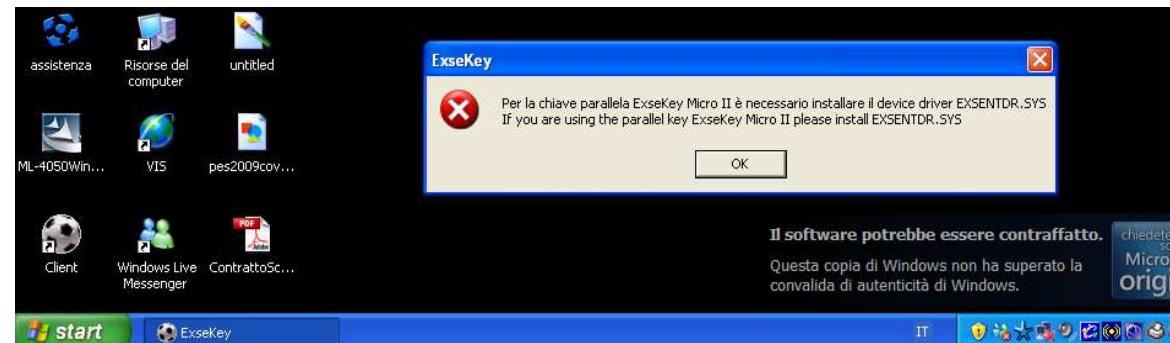


In pratica all'interno del file è presente un semplice codice alfanumerico, che altro non è che il serial number del disco rigido installato sul PC.

# L'ANALISI

**Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049**

A questo punto si è immediatamente provveduto a recuperare il numero seriale del disco clonato, lo si è sostituito all'interno del file “**Ish.dll**” e si è tentato di rilanciare il programma “**client.exe**”:



# L'ANALISI

## ExseKey

La chiave **ExseKey**, è una chiave hardware installata probabilmente su porta parallela (porta delle stampanti), la quale impedisce l'utilizzo del software in sua assenza, è stata fatta una rapida ricerca tramite internet per verificare la bontà di tale sistema di protezione;

la chiave oltre ad essere di tipo parallela, potrebbe essere celata in una chiavetta USB, ed inoltre potrebbe essere rappresentata da uno unico sistema che configura la protezione tramite rete Lan, unitamente alla presenza fisica di uno dei due dispositivi:



# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

Non potendo eseguire il programma, nonostante tutti i tentativi finora descritti, si è passati alla analisi degli archivi individuati nel percorso “C:\Client\Dati”:

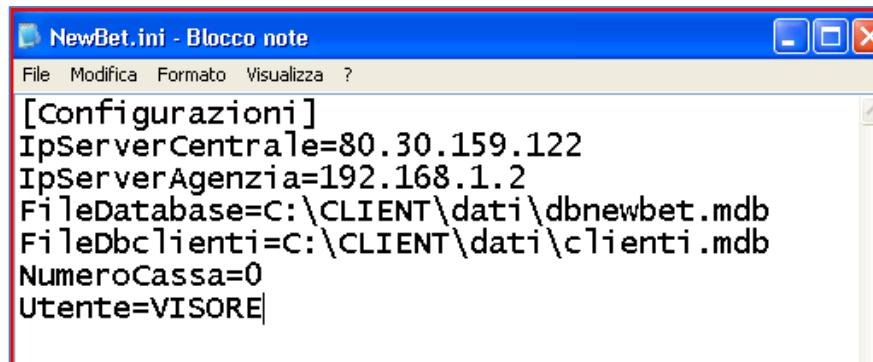
Nome	Dimensione	Tipo
dbnewbet.mdb	13.796 KB	Microsoft Office Access Database
Comuni.mdb	736 KB	Microsoft Office Access Database
dbnewbetpre.mdb	432 KB	Microsoft Office Access Database
Clienti.mdb	228 KB	Microsoft Office Access Database
dbnewbet.ldb.copy0	1 KB	File COPY0
NewBet.ini	1 KB	Impostazioni di configurazione
Stampa.ini	1 KB	Impostazioni di configurazione
Clienti.ldb.copy0	1 KB	File COPY0

Oltre agli archivi sono presenti due file di configurazione denominati “NewBet.ini” e “Stampa.ini”

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## NewBet.ini



```
[Configurazioni]
IpServerCentrale=80.30.159.122
IpServerAgenzia=192.168.1.2
FileDatabase=C:\CLIENT\dati\dbnewbet.mdb
FileDbclienti=C:\CLIENT\dati\clienti.mdb
NumeroCassa=0
Utente=VISORE
```

Dalle poche righe di configurazione presenti all'interno del file “NewBet.ini”, è possibile intuire come il programma utilizzi la rete locale per accedere al server locale, denominato “Server Agenzia”, con indirizzo IP 192.168.1.2.

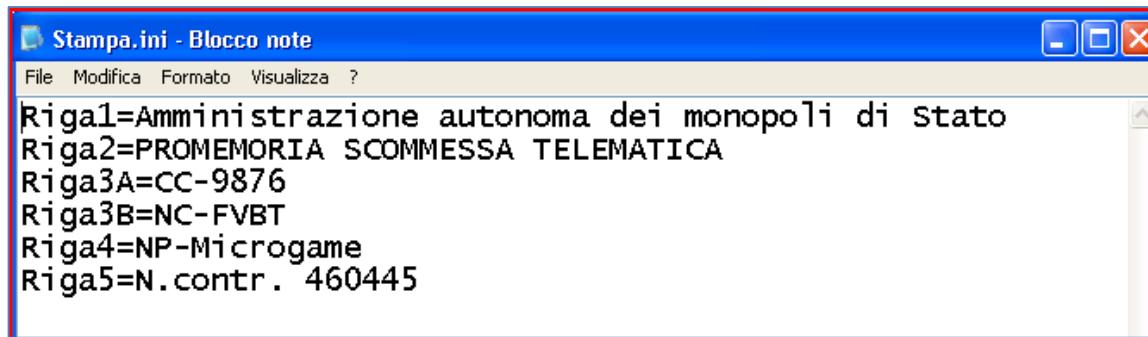
I file utilizzati come database, sono chiaramente i file individuati nel percorso già specificato in precedenza:

“C:\Client\dati\dbnewbet.mdb” e “C:\Client\dati\Clienti.mdb”.

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## Stampa.ini



Tale file appare evidentemente essere utilizzato per la configurazione di una intestazione di stampa, nella quale sono presenti le informazioni di riepilogo della scommessa telematica probabilmente effettuata.

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## dbnewbet.mdb

Nel tentativo di visualizzare il contenuto del primo archivio, veniva richiesta una password per l'accesso ai dati:



La password grazie al software “Elcom Recovery Password” è stata individuata in “**fracitumma**”, a questo punto è stato possibile accedere ai dati ivi contenuti.

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## dbnewbet.mdb

Sono presenti diverse tabelle, utili alla gestione del database:

- La tabella “**Utenti**” rappresenta evidentemente l’elenco delle persone abilitate all’accesso dei dati del programma.
- Le Tabelle “**Scommesse**” e “**ScommesseDettagliate**”, riportano l’elenco delle giocate caricate all’interno del sistema.

Tipo	Utente	Password	Abilitato
1	ADMIN	fracitumma	<input checked="" type="checkbox"/>
3	UTENTE1	1	<input checked="" type="checkbox"/>
3	UTENTE2	2	<input checked="" type="checkbox"/>
2	VISORE	vis	<input checked="" type="checkbox"/>
*			<input type="checkbox"/>

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

**Scommesse - Microsoft Access**

**Tabelle**

- Bonus
- Confettorecassa
- Impostazioni
- Margini
- Massimali
- Palinsesto
- Risultati
- Scommesse
- ScommesseDettagliate
- Utenti

Chiave IDElenc IdBolletta NumeroCas Palinsesto Bonus VincitaNett PotVincita Importo

230	14029	14029 VISORE	2023	L. 131,49	L. 876,63	L. 1.008,12	
230	14030	14030 VISORE	2023	L. 132,00	L. 879,99	L. 1.011,99	
230	14031	14031 VISORE	2023	L. 0,00	L. 150,50	L. 150,50	
230	14032	14032 VISORE	2023	L. 30,88	L. 205,85	L. 236,73	
230	14033	14033 VISORE	2023	L. 42,04	L. 525,48	L. 567,52	
230	14034	14034 VISORE	2023	L. 43,93	L. 292,85	L. 336,78	
230	14035	14035 VISORE	2023	L. 0,00	L. 299,40	L. 299,40	
230	14036	14036 VISORE	2023	L. 0,00	L. 209,80	L. 174,83	

Record: 1 di 2626 Nessun filtro Cerca

**ScommesseDettagliate - Microsoft Access**

**Tabelle**

- Bonus
- Confettorecassa
- Impostazioni
- Margini
- Massimali
- Palinsesto
- Risultati
- Scommesse
- ScommesseDettagliate
- Utenti

Scommessa Chiave IDElenc Inc IdBolletta Palinsesto Campionat Avvenimenti Squadra1 Squadra2

Over	230	97191	14029	2023	ScoCpSc	3785,10	Inverurie L.W.	M
Esito Finale 1	230	97192	14029	2023	ItaB	3768,14	Ancona	Tr
Esito Finale 1	230	97193	14029	2023	ItaD1b	3768,87	Pistoiese	Ps
Esito Finale 1	230	97194	14029	2023	IngLC	3790,12	Birmingham	D
Esito Finale 1	230	97195	14029	2023	IngLC	3790,18	Sheffield Utd	D
Esito Finale 1	230	97196	14029	2023	ItaA	3798,8	Milan	Ge
Esito Finale 1	230	97197	14029	2023	ItaA	3798,9	Roma	Ps
Esito Finale 1	230	97198	14029	2023	ItaA	3798,5	Catania	In
Esito Finale 1	230	97199	14029	2023	ItaA	3798,3	Atalanta	Bo
Under	230	97200	14030	2023	ScoCpSc	3785,10	Inverurie L.W.	M
Under	230	97201	14030	2023	ItaB	3768,14	Ancona	Tr
Under	230	97202	14030	2023	ItaD1b	3768,87	Pistoiese	Ps
Esito Finale 1	230	97203	14030	2023	IngLC	3790,12	Birmingham	D
Esito Finale 1	230	97204	14030	2023	IngLC	3790,18	Sheffield Utd	D
Esito Finale 1	230	97205	14030	2023	ItaA	3798,8	Milan	Ge
Esito Finale 1	230	97206	14030	2023	ItaA	3798,9	Roma	Ps

Record: 1 di 19117 Nessun filtro Cerca Visualizzazione Foglio dati

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## dbnewbet.mdb

Le due tabelle rappresentano l'insieme delle giocate effettuate dal 26/01/2009 al 18/02/2009.

La relazione tra le due tabelle, definita rapporto padre-figlio, (1->N), tabella “Scommesse”, archivio di testata, e tabella “ScommesseDettagliate”, definito archivio “figlio”, di dettaglio, rappresenta le giocate effettuate con il dettaglio della scommessa, per un totale di **2.626** scommesse e di **19.117** righe di dettaglio.

Ogni scommessa è composta da una giocata (testata) che può comprendere più partite o eventi (dettaglio) oggetto della stessa.

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## dbnewbet.mdb

Le tabelle “**Palinsesto**” e “**Risultati**” rappresentano gli archivi contenenti gli eventi sportivi sui quali è possibile scommettere, e i risultati degli stessi.

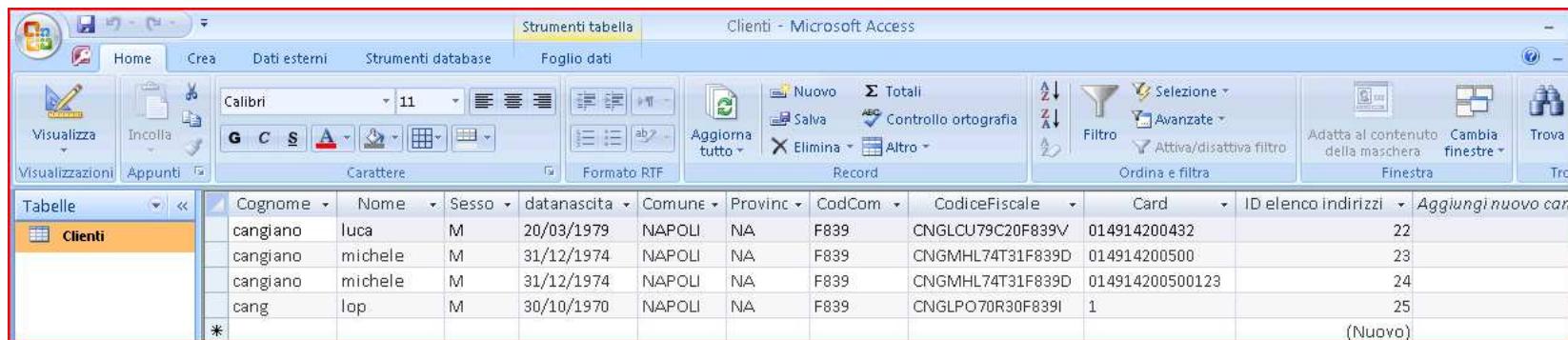
E’ evidente come il collegamento ad Internet del software, permette di scaricare in tempo reale, tutte le informazioni utili all’effettuazione delle giocate, quali i palinsesti con le singole quotazioni, successivamente i risultati servono a verificare le giocate vincenti.

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

**dbnewbet.mdb**

L'archivio “Clienti” registra alcuni nominativi:



The screenshot shows a Microsoft Access application window titled "Clienti - Microsoft Access". The ribbon tabs at the top include "Home", "Crea", "Dati esterni", "Strumenti database", and "Foglio dati". The "Strumenti tabella" tab is selected. The main area displays the "Clienti" table with the following data:

Cognome	Nome	Sesso	datanascita	Comune	Provinc	CodCom	CodiceFiscale	Card	ID elenco indirizzi	Aggiungi nuovo car
cangiano	luca	M	20/03/1979	NAPOLI	NA	F839	CNGLCU79C20F839V	014914200432	22	
cangiano	michele	M	31/12/1974	NAPOLI	NA	F839	CNGMHL74T31F839D	014914200500	23	
cangiano	michele	M	31/12/1974	NAPOLI	NA	F839	CNGMHL74T31F839D	014914200500123	24	
cang	lop	M	30/10/1970	NAPOLI	NA	F839	CNGLPO70R30F839I	1	25	(Nuovo)

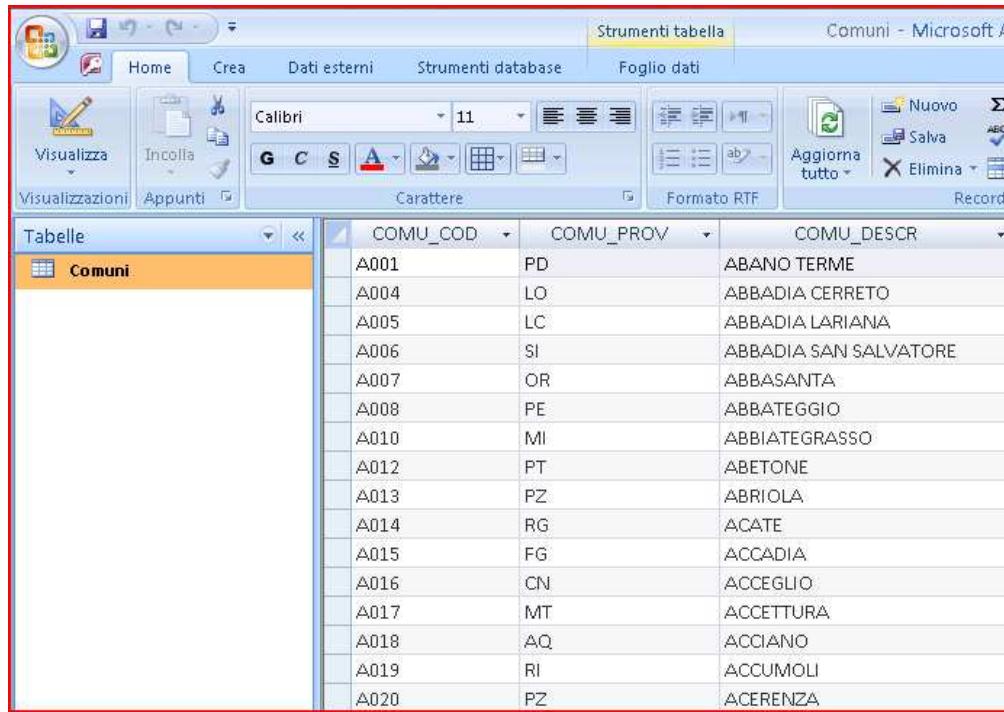
nominativi probabilmente utilizzati per le giocate, avendo un numero di Card associato all'anagrafica.

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## dbnewbet.mdb

L'archivio “Comuni” è un archivio contenente tutti i comuni d’Italia:



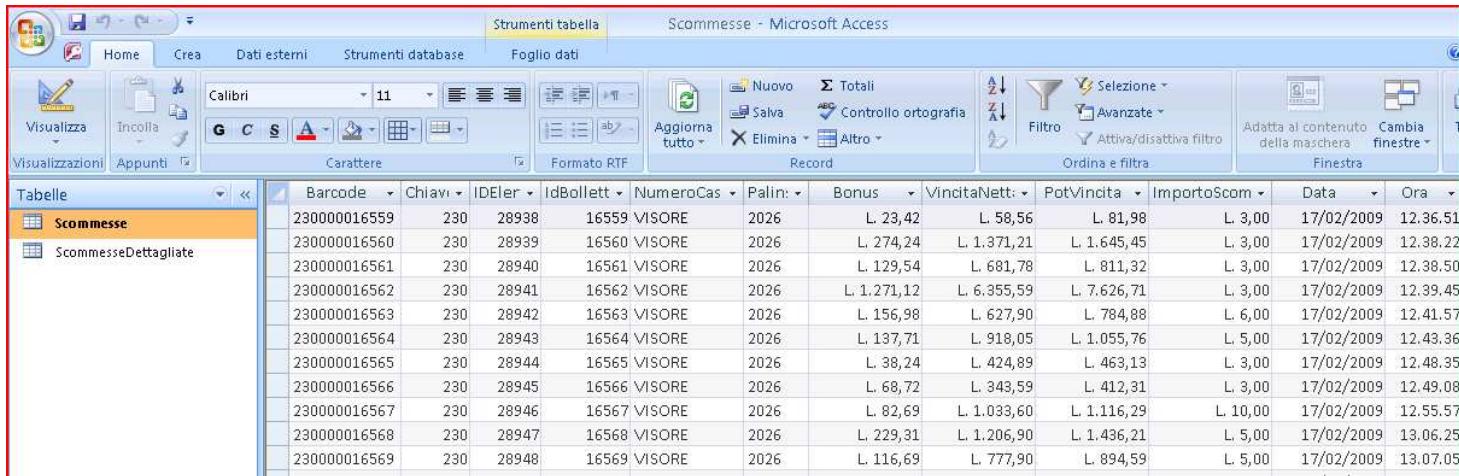
	COMU_COD	COMU_PROV	COMU_DESCR
A001	PD	ABANO TERME	
A004	LO	ABBADIA CERRETO	
A005	LC	ABBADIA LARIANA	
A006	SI	ABBADIA SAN SALVATORE	
A007	OR	ABBASANTA	
A008	PE	ABBATEGGIO	
A010	MI	ABBIATEGRASSO	
A012	PT	ABETONE	
A013	PZ	ABRIOLA	
A014	RG	ACATE	
A015	FG	ACCADIA	
A016	CN	ACCEGLIO	
A017	MT	ACCETTURA	
A018	AQ	ACCIANO	
A019	RI	ACCUMOLI	
A020	PZ	ACERENZA	

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

## DbNewBetPre.mdb

contiene una duplicazione delle tabelle “Scommesse” e “Dettaglio Scommesse”, analizzando il particolare è possibile verificare come in effetti tale archivio contenga le sole giocate del giorno “17/02/2009”, lasciando intuire una PREregistrazione delle scommesse che poi tramite software vengono ribaltate negli archivi principali.



The screenshot shows a Microsoft Access application window titled "Scommesse - Microsoft Access". The ribbon menu is visible at the top, and the "Home" tab is selected. The main area displays a table named "Scommesse" with the following data:

Barcode	Chiavi	IDElter	IdBollett	NumeroCas	Palin:	Bonus	VincitaNett:	PotVincita	ImportoScom	Data	Ora
230000016559	230	28938	16559	VISORE	2026		L. 23,42	L. 58,56	L. 81,98	L. 3,00	17/02/2009 12.36.51
230000016560	230	28939	16560	VISORE	2026		L. 274,24	L. 1.371,21	L. 1.645,45	L. 3,00	17/02/2009 12.38.22
230000016561	230	28940	16561	VISORE	2026		L. 129,54	L. 681,78	L. 811,32	L. 3,00	17/02/2009 12.38.50
230000016562	230	28941	16562	VISORE	2026		L. 1.271,12	L. 6.355,59	L. 7.626,71	L. 3,00	17/02/2009 12.39.45
230000016563	230	28942	16563	VISORE	2026		L. 156,98	L. 627,90	L. 784,88	L. 6,00	17/02/2009 12.41.57
230000016564	230	28943	16564	VISORE	2026		L. 137,71	L. 918,05	L. 1.055,76	L. 5,00	17/02/2009 12.43.36
230000016565	230	28944	16565	VISORE	2026		L. 38,24	L. 424,89	L. 463,13	L. 3,00	17/02/2009 12.48.35
230000016566	230	28945	16566	VISORE	2026		L. 68,72	L. 343,59	L. 412,31	L. 3,00	17/02/2009 12.49.08
230000016567	230	28946	16567	VISORE	2026		L. 82,69	L. 1.033,60	L. 1.116,29	L. 10,00	17/02/2009 12.55.57
230000016568	230	28947	16568	VISORE	2026		L. 229,31	L. 1.206,90	L. 1.436,21	L. 5,00	17/02/2009 13.06.25
230000016569	230	28948	16569	VISORE	2026		L. 116,69	L. 777,90	L. 894,59	L. 5,00	17/02/2009 13.07.05

# L'ANALISI

Personal Computer Assemblato S/N: 90-PL861AC004-530-79X350019049

La cartella immagini contiene alcuni file «bmp» utili alla gestione del software:



# RISPOSTA AI QUESITI

*identifichi l'autore del software installato sui pc in sequestro e che consentiva di non inviare le giocate al concessionario FiveBet;*

Tutte le opportune tecniche di indagine e di analisi sono state adottate al fine di individuare l'autore e/o la società produttrice del software utile alle giocate di scommesse sportive tramite Internet, evidentemente la progettazione, la stesura del codice, eventuali altre informazioni che potessero individuare gli autori del programma, sono state opportunamente omesse, in pratica risulta impossibile l'identificazione dell'autore del software installato sui PC in sequestro.

# RISPOSTA AI QUESITI

*spieghi il meccanismo di funzionamento di quel programma;*

Il software individuato sui PC in sequestro, utile alla effettuazione di scommesse su eventi sportivi è denominato “**Cassa.exe**” e “**Client.exe**”.

Il programma è protetto da chiave Hardware “**ExseKey-Micro II**”, in mancanza della quale si compromette il corretto andamento del software, pertanto non è stato possibile recuperare informazioni sul meccanismo di funzionamento del programma, tuttavia dall’analisi effettuata e dagli archivi rinvenuti, è possibile ipotizzare una gestione parallela delle scommesse sportive, integrata tramite il collegamento al sito [\*\*www.fivebet.it\*\*](http://www.fivebet.it), utile all’aggiornamento del palinsesto e dei risultati online aggiornati dalla società concessionaria AAMS.

# RISPOSTA AI QUESITI

*accerti, attraverso l'analisi della memoria, l'esistenza di dati che consentano di individuare altre persone che erano connesse con i PC condividendo il programma e determini il numero di giocate gestite con tale programma;*

I personal Computer analizzati sono configurati in una rete locale (LAN), collegati tra loro, cablati, tramite cavo di rete e connettori RJ45.

Non vi è una gestione centralizzata standard di Rete Informatica, tantoché non vi sono politiche di sicurezza ed accesso all'interno del sistema informatico individuato.

L'accesso ai personal computer è libero, non necessita di credenziali di autenticazione, pertanto non è possibile risalire a tutta una serie di eventi e di attività succedute sui PC.

# RISPOSTA AI QUESITI

*accerti, attraverso l'analisi della memoria, l'esistenza di dati che consentano di individuare altre persone che erano connesse con i PC condividendo il programma e determini il numero di giocate gestite con tale programma;*

Il Database “**Dbnewbet.mdb**” conserva nella tabella “Scommesse” le giocate effettuate a partire dal “26/01/2009” fino al “18/02/2009”, per un numero di record pari a “**2.626**” giocate.

Il totale dell’importo delle scommesse è pari a “**€ 17.858,00**”; tale risultato è dato dalla somma degli importi individuati nella colonna denominata “Importo Scommessa” all’interno dell’archivio “Scommesse”.

La colonna “**bolletta pagata**” riporta un totale di “**€ 6.572,57**”, corrispondente, presumibilmente, alle giocate vincenti pagate.



## SSRI Lorenzo Laurato s.r.l.



 Via Coroglio nr. 57/D (BIC- Città della Scienza)  
 80124 Napoli

 Tel. 081.19804755  
 Fax 081.19576037

 lorenzo.laurato@unina.it  
lorenzo.laurato@ssrilab.com

 [www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)  
[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)