EUWEB
EU-WESTERN BALKANS
Cooperation on Justice and Home Affairs

Transnational Cybercrime and Digital Forensics

Raffaele Pizzolante
Dipartimento di Informatica
Università degli Studi di Salerno
Fisciano (SA), Italia

With the support of the Erasmus+ Programme of the European Union

UNIVERSITÀ DEGLI STUDI DI SALERNO

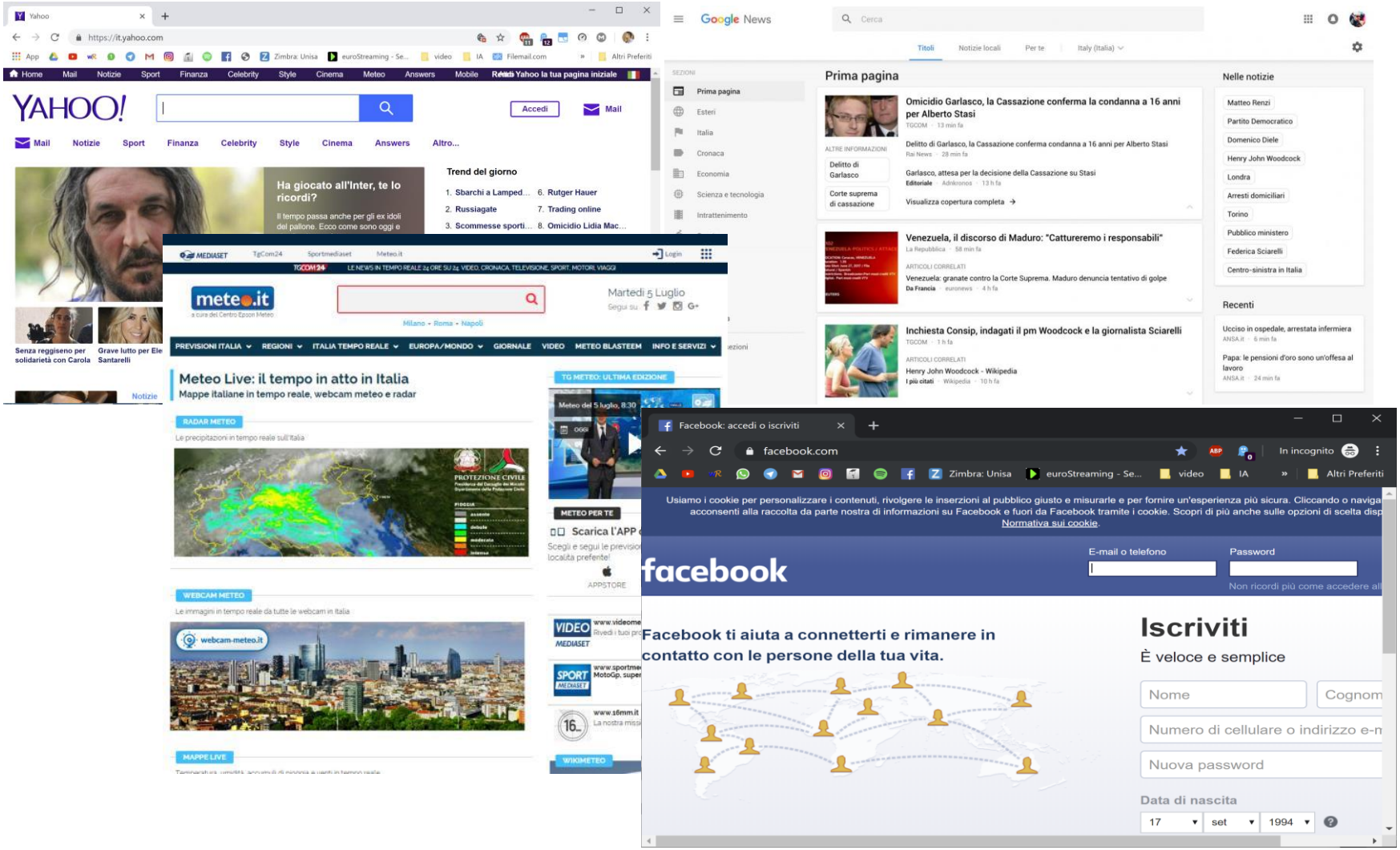
Outline

- Introduzione
- Transnational Cybercrime
- Digital Forensics e Digital Evidence
- Workflow della Digital Forensics
- Fasi del Processo di Investigazione
- Un Caso di Studio: Drone Forensics
- Conclusioni

Outline

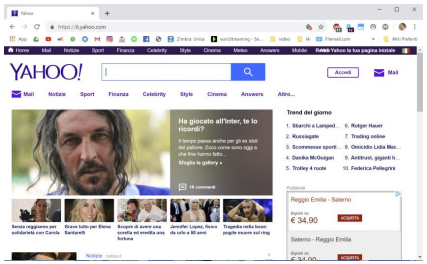
- **Introduzione**
- Transnational Cybercrime
- Digital Forensics e Digital Evidence
- Workflow della Digital Forensics
- Fasi del Processo di Investigazione
- Un Caso di Studio: Drone Forensics
- Conclusioni

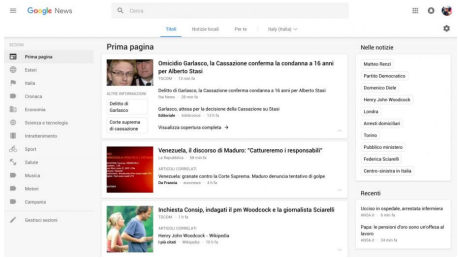
Internet che conosciamo!

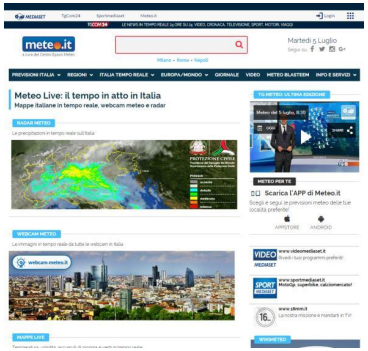


Ma…

Quello che usiamo quotidianamente è
solo la **punta dell'iceberg**







4%

Surface Web

Surface Web

Facebook, Twitter, Instagram

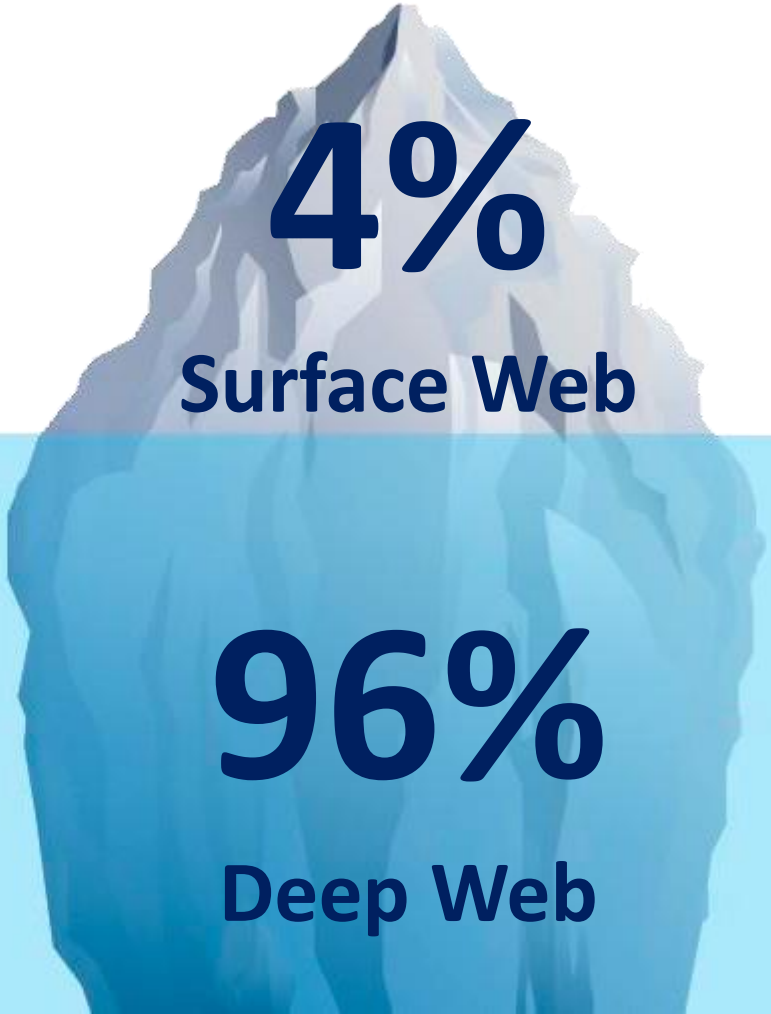
Motori di Ricerca (Google, Bing, ecc.)

Wikipedia, Netflix, Twitch

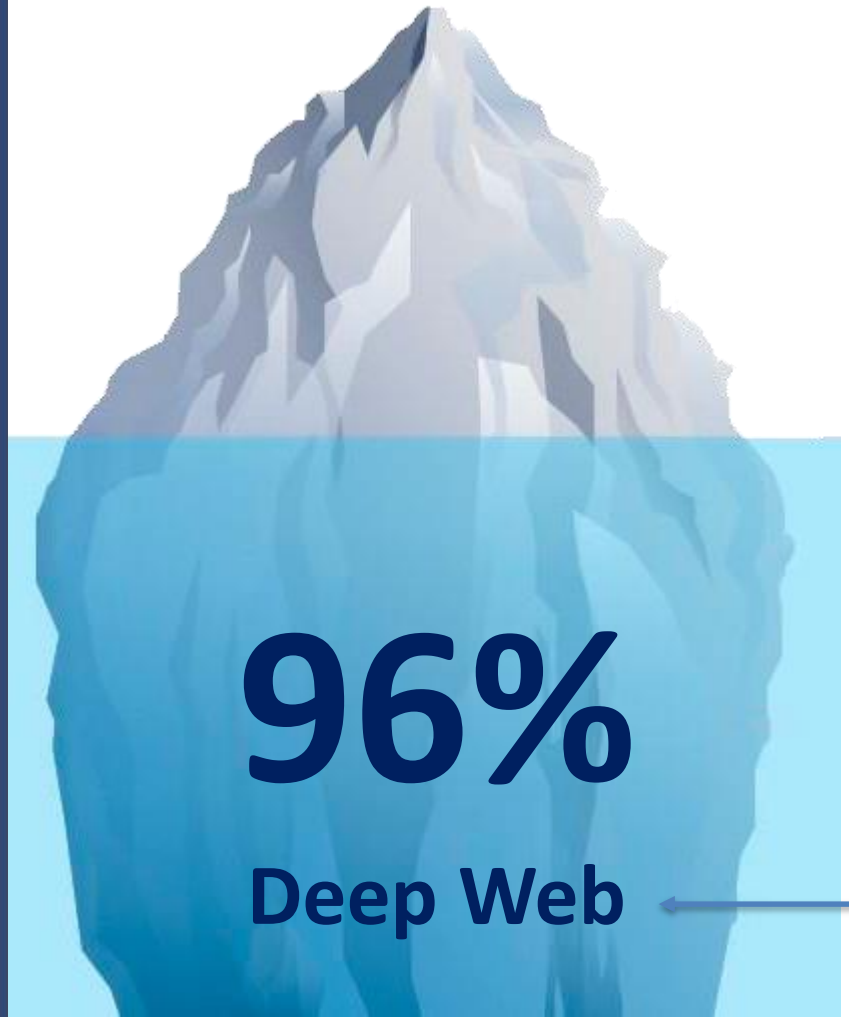
4%

Surface Web

Oltre il Surface Web…

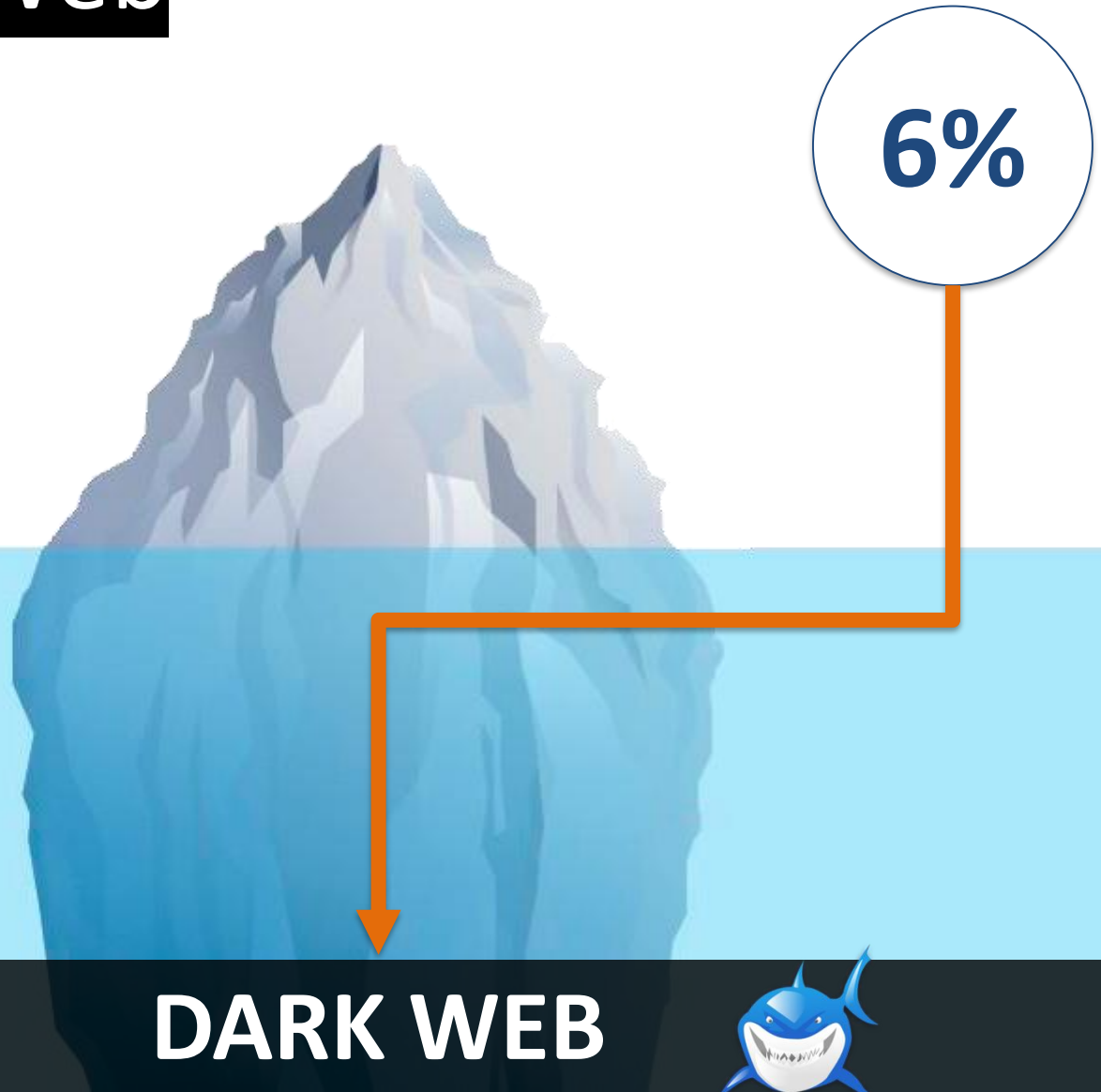


Deep Web



- Articoli Accademici
- Risorse Governative
- Documenti Legali
- Documenti Finanziari
- Documenti Medici
- Documenti di Organizzazioni

Dark Web



Cosa si trova al suo interno…

DARK WEB

CYBERCRIMINI INTERNAZIONALI e INTERCONTINENTALI

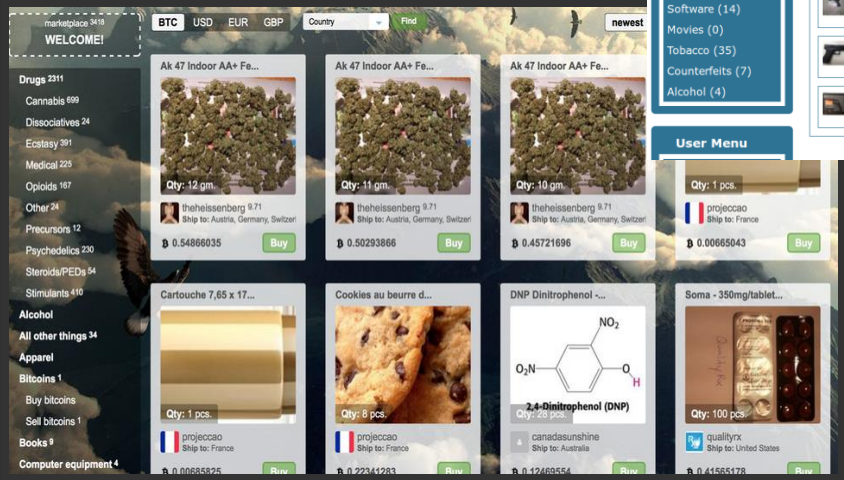
TERRORISMO e WARFARE

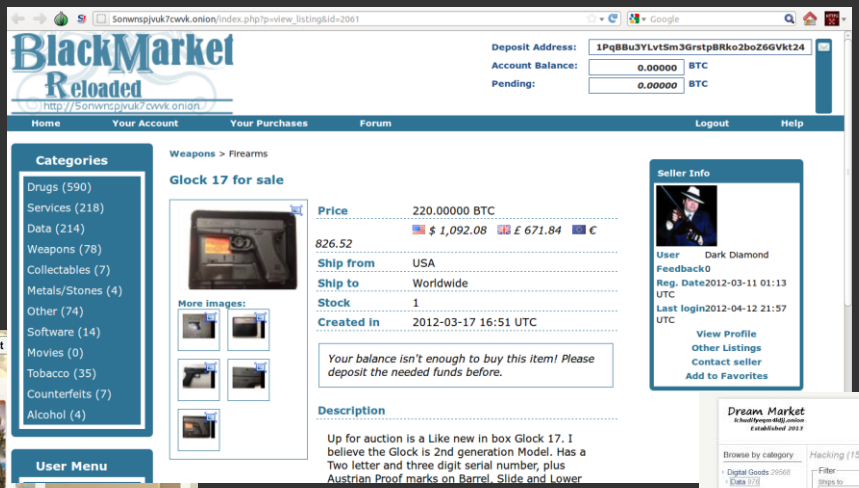
VENDITA ARMI e RICICLAGGIO

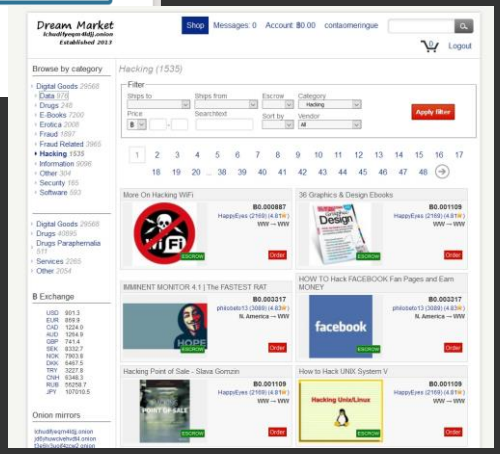
FURTI DI IDENTITÀ

Cosa si trova al suo interno…

DARK WEB

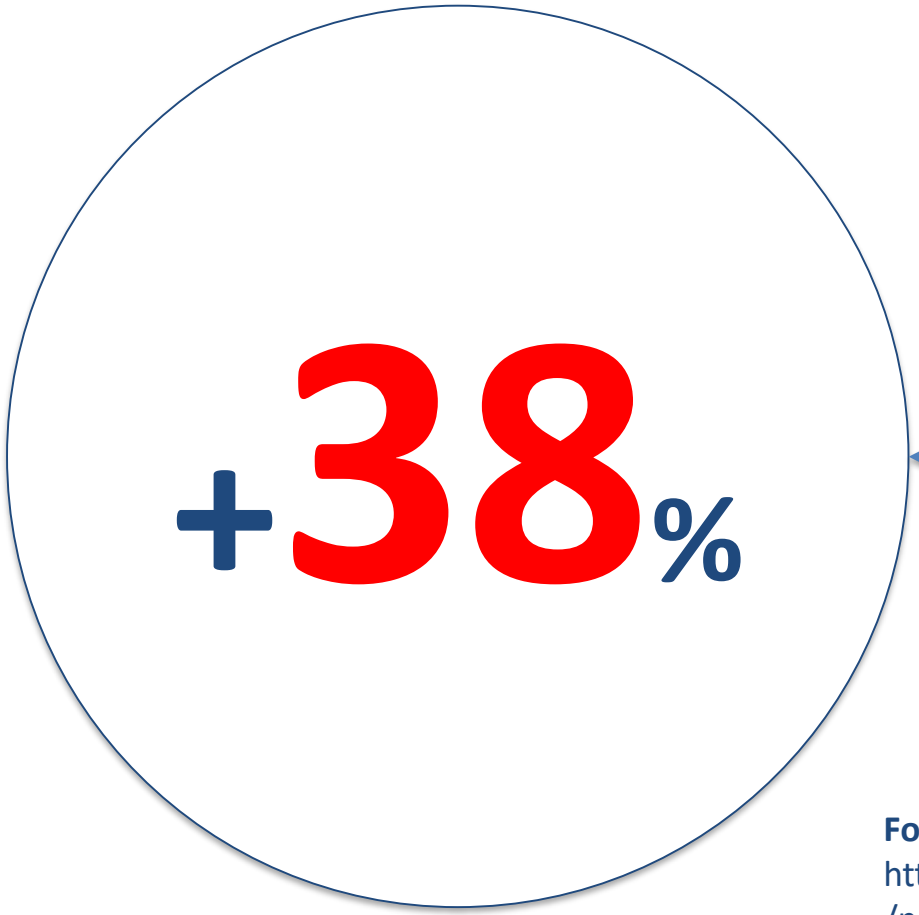






Cybercrime – 1/2

Incremento dei Cybercrimini nel 2018, rispetto al 2017



Fonte:
https://www.repubblica.it/tecnologia/sicurezza/2019/02/21/news/nel_2018_piu_38_di_cyber_attacchi_nel_mondo_sono_raddoppiati_nella_sanita_-219722787/

Cybercrime – 2/2

Un Cybercrime è un atto criminale compiuto utilizzando un **dispositivo informatico** e/o **tramite internet**.

Questo atto **trascende i confini nazionali** e **internazionali** e solleva diversi problemi giurisdizionali, che una Nazione, da sola, non può mitigare.

Definizione adattata da [1]

Il Mattino > Primo Piano > Politica

Cyber-terrorismo e Jihad, nuovo allarme dei Servizi italiani

Police arrest three

Hans News Service | 20 Aug 2019 11:56 PM IST

HIGHLIGHTS

The Cyber Crime Police of Rachakonda on Tuesday arrested three cyber stalkers from Ankushapur village under Ghatkesar police station limits for harassing a woman by posting obscene pictures and videos on her Facebook account.

Cyberbullismo: nell'ultimo anno colpito il 6% dei ragazzi

BimbiSaniBelli - 5 set 2019

Il 19%, invece, ha assistito a episodi di **cyberbullismo**. In questo **c** arrabbiano e si rattristano, ma non fanno nulla per difendere i ...

IL REPORT

Cybercrim
ai dispositi

Home › News › Truffe Unicredit e Intesa Sanpaolo: nuove email infestano le caselle postali

Truffe Unicredit e Intesa Sanpaolo: nuove email infestano le caselle postali

Unicre

Cyberstalking in Sicilia, un ammonimento ci ricorda come

Rapporto Clusit su cybercrimine: “Sorveglianza d massa e furto di se E' di

VENE

I numeri del

Statistiche, vicende e lc

Il cybercrime usa la dogana come esca per nuovi attacchi in Italia

23 Agosto 2019 Francesco Bussoletti Cyber, Difesa e Sicurezza

delinquenza

GIUSEPPE CHINA
@Ciussy88

cchi in Italia per

pirata

diffondere Urshi

6 Settembre 2019 Francesco Bussoletti Cyber, Difesa e Sicurezza

ARTICOLI E COMMENT

Cyberter problematici d

Articolo, 06/09/2018

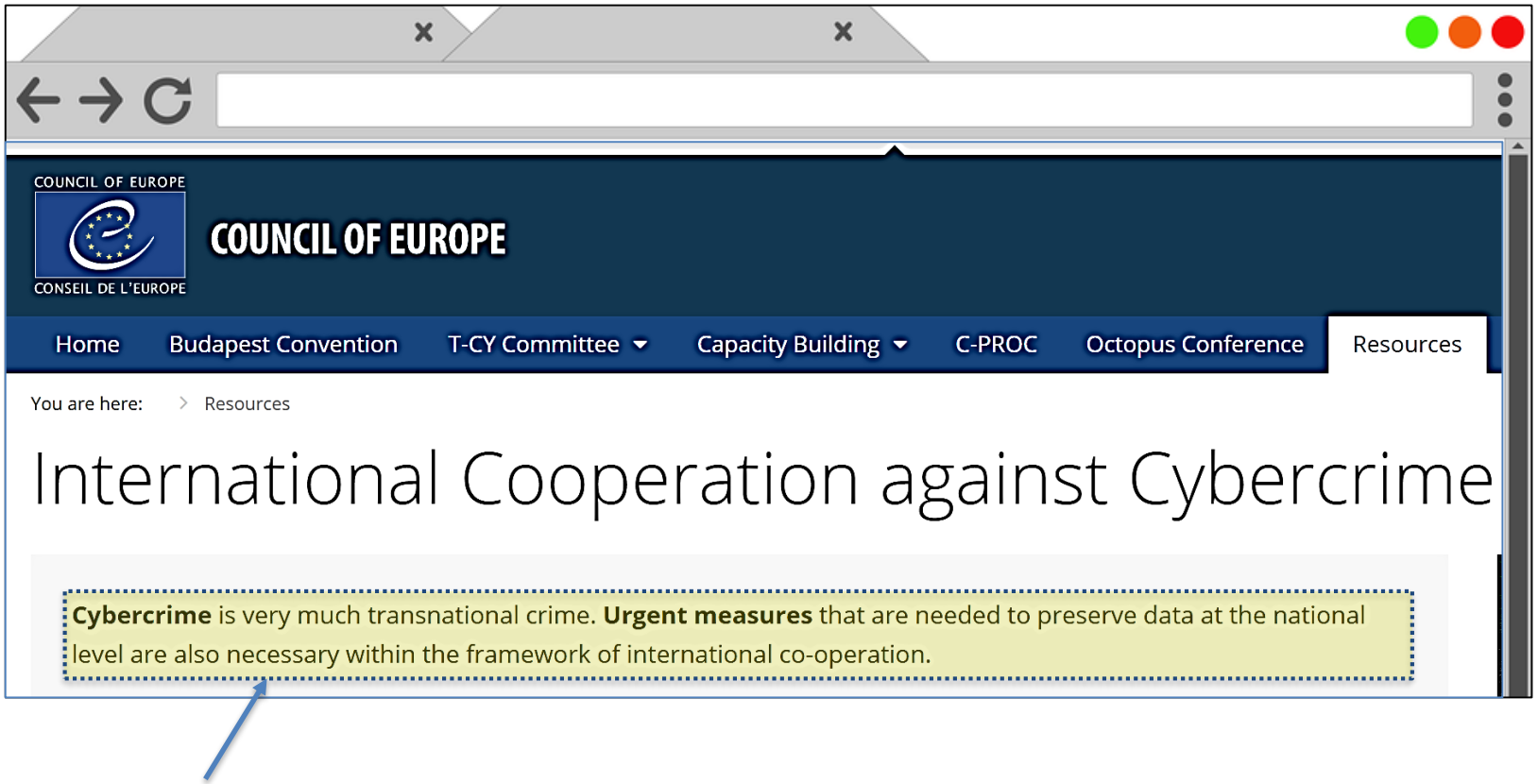
Tecnologia 16 Settembre 2019

Cyberbullismo: casi in aumento sia negli ambienti virtuali sia all’interno delle scuole!

Outline

- Introduzione
- **Transnational Cybercrime**
- Digital Forensics e Digital Evidence
- Workflow della Digital Forensics
- Fasi del Processo di Investigazione
- Un Caso di Studio: Drone Forensics
- Conclusioni

Transnational Cybercrime



Fonte:
https://www.coe.int/en/web/cybercrime/international-cooperation

Stiamo diventando massicciamente **interconnessi**.

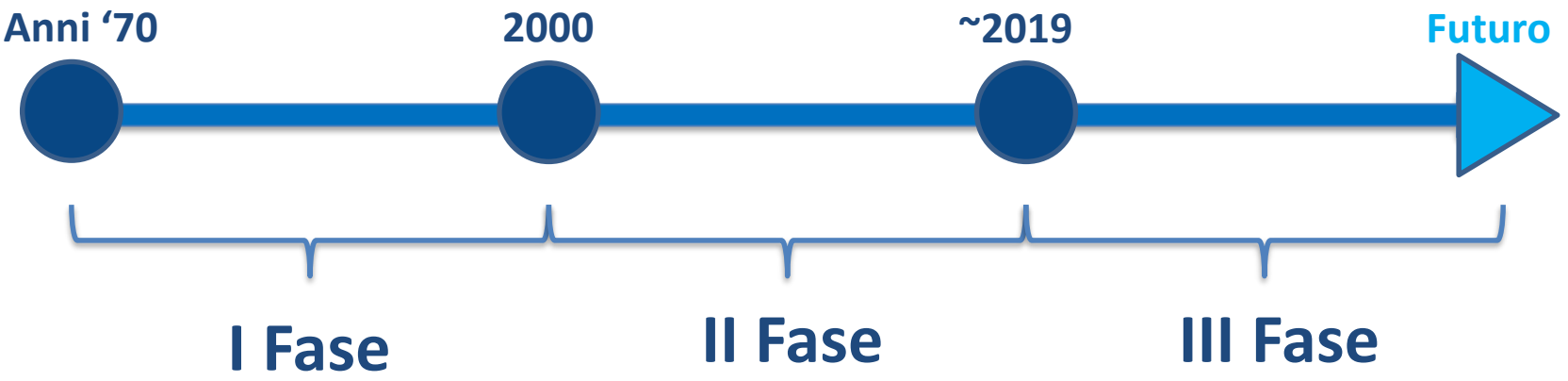
Che ci piaccia o no, dobbiamo coesistere con persone e **sistemi di affidabilità sconosciuta** e **non identificabile** (**comprese le parti ostili** non identificabili), all'interno degli Stati Uniti e altrove.

I nostri problemi sono diventati internazionali […] e non possono essere risolti solo a livello locale.

Estratto adattato dall'intervento "Information System Adversities and Risks" di Peter G. Neumann (principale scienzato al Computer Science Laboratory, SRI International) alla Stanford Conference, tenutasi alla Stanford University, Stanford, California (USA), 6 e 7 dicembre, 1999

Transnational Cybercrime

Evoluzione del Cybercrime



Transnational Cybercrime

Evoluzione del Cybercrime

I Fase

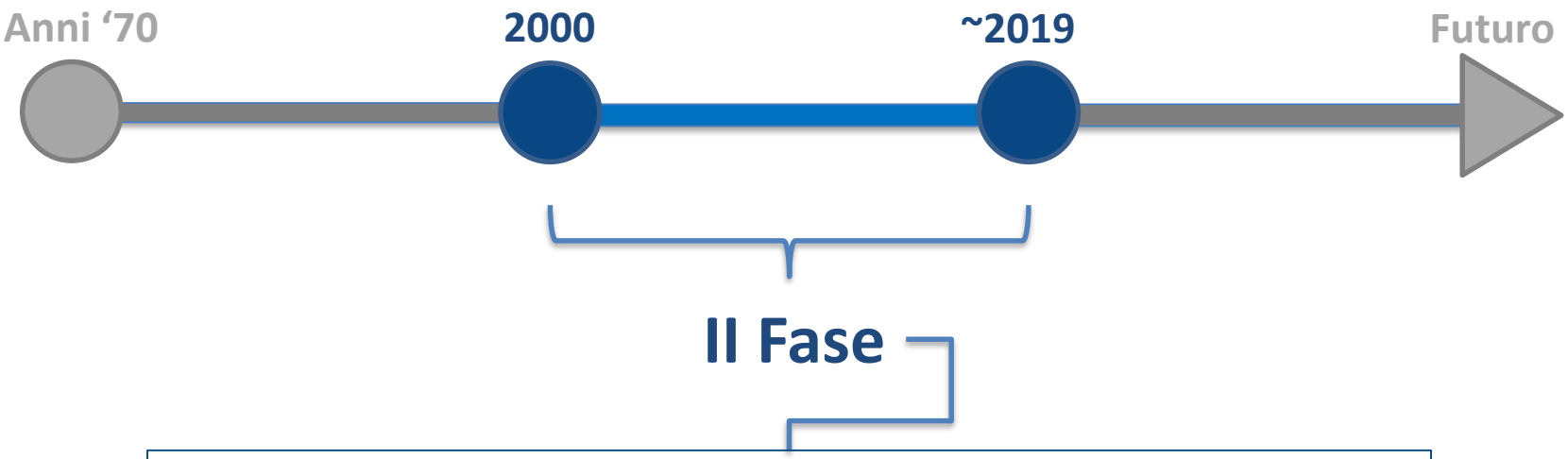
Caratterizzata da attacchi diretti contro sistemi e reti

Obiettivo: Sconfiggere le istituzioni causando il crash di sistemi o causando danni fisici

Vittime Tipiche: Hardware e istituzioni, **NON** individuali

Transnational Cybercrime

Evoluzione del Cybercrime



Sfrutta punti deboli (ad es., vulnerabilità) della sicurezza del sistema e delle reti

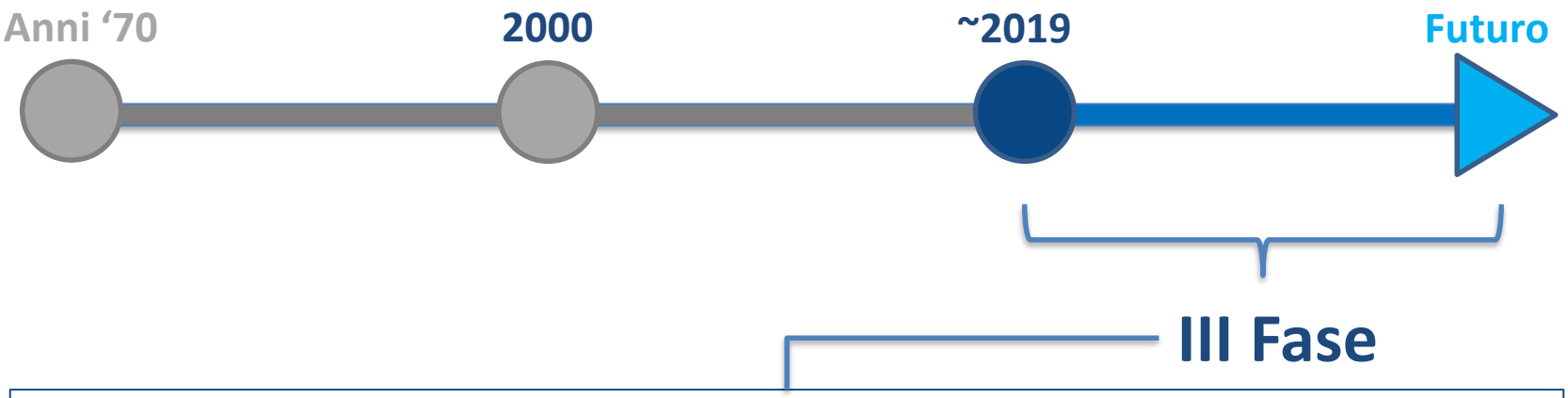
Obiettivi: Sfruttamento di individui specifici → Vittime Specifiche

Il cybercrime diventa profittevole

Esempi: Furti di identità, frodi con carte di credito, crimini finanziari, vendette verso persone specifiche, …

Transnational Cybercrime

Evoluzione del Cybercrime



Questa fase è caratterizzata dalla manipolazione dei social media e dal furto o dall'acquisto di dati personali

Accurata **selezione delle vittime** in base al loro orientamento politico, istruzione, opinioni e altri fattori che li rendono persuadibili e vulnerabili.

Diffusioni fake news, deep fake, fake social media → aumento dei disordini sociali, cambiamenti nella struttura del potere delle nazioni, …

Transnational cybercime: cybercrime finanziario, cyberwarfare, frodi online, …

Transnational Cybercrime

Evoluzione del Cybercrime

- In generale, le organizzazioni criminali transazionali (dette anche TOC da "**Transnational Organized Crime**") sono sempre più **coinvolte nei cybercrimini**
- Minacciano reti e infrastrutture informatiche sensibili delle **imprese** e del **governo** (mercati azionari, banche, ecc.)
  - Questo si traduce in **costi elevatissimi** per i consumatori
- **Esempio**
  - Ad esempio, le frodi online perpetrate dalle reti di cybercrime dell'Europa centrale hanno effettuato frodi a cittadini/entità statunitensi per un valore di circa **$1 miliardo in un solo anno**, secondo alcune stime
    - **Fonte:**
      - https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat

Outline

- Introduzione
- Transnational Cybercrime
- **Digital Forensics e Digital Evidence**
- Workflow della Digital Forensics
- Fasi del Processo di Investigazione
- Un Caso di Studio: Drone Forensics
- Conclusioni

Digital Forensics

- **Problema:** Come indagare su **cybercrimine**, **transnational cybercrime** e **crimini** che coinvolgono **dispositivi informatici**?

Digital Forensics – Definizione

- La **digital forensics** (***investigazione digitale forense***) consiste nell'uso di **metodi scientificamente provati**, per le attività di:
  - Raccolta e Conservazione
  - Convalida e Identificazione
  - Analisi e Interpretazione
  - Documentazione
  - Presentazione

  di **dati digitali**, derivanti da **dispositivi informatici** utilizzati per commettere azioni illegali, **cybercrime, transnational cybercrime** e **crimini**

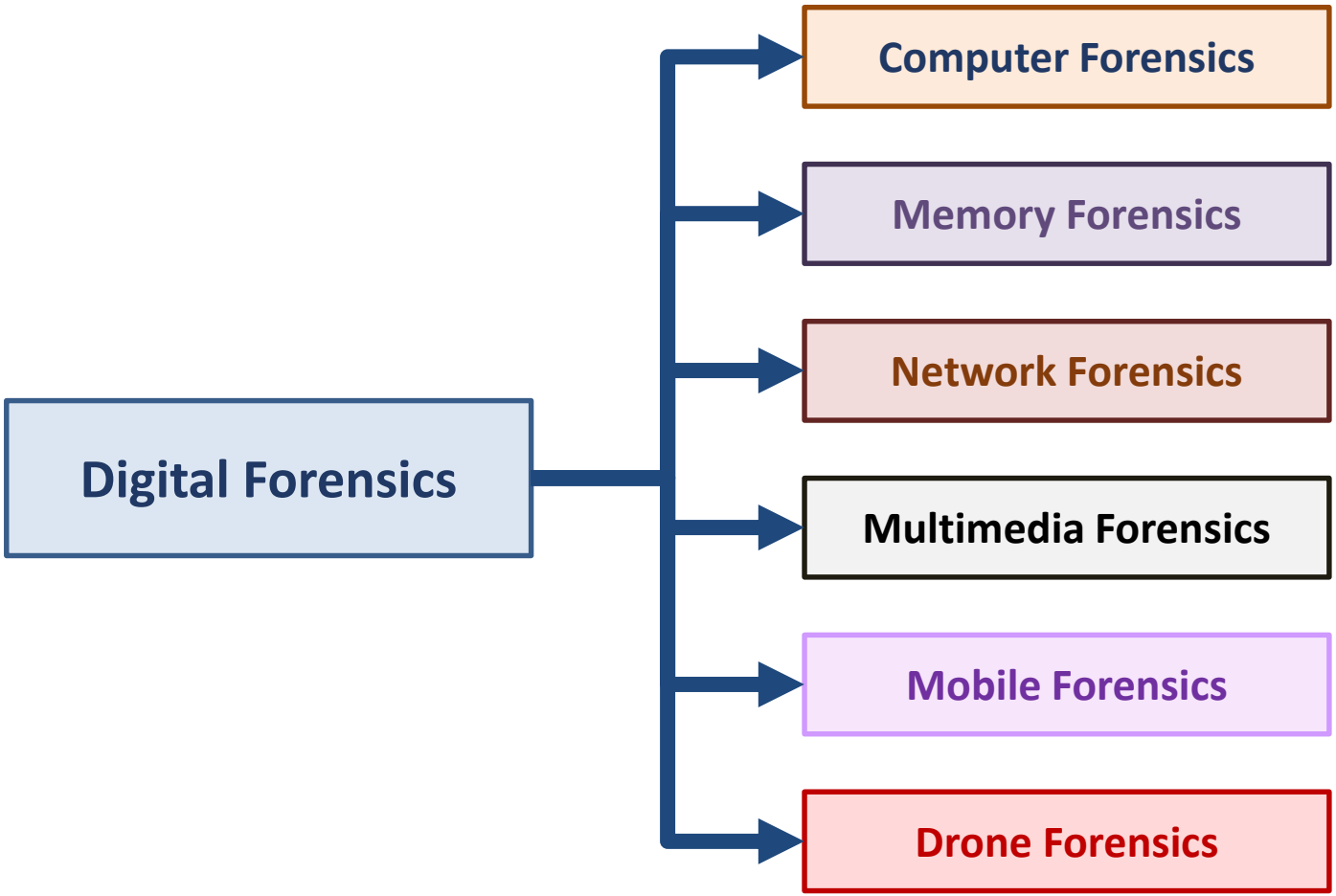
Definizione adattata e semplificata da [4]

Digital Evidence – Definizione

- Al centro di ogni investigazione digitale forense, vi sono sicuramente le **digital evidence** (***prove digitali*** o ***evidenze digitali***)
- Una **prova digitale** è qualsiasi dato digitale, contenente informazioni, utilizzabili per **supportare** o **confutare** ipotesi di un crimine

Definizione adattata e semplificata da [4]

Le Ramificazioni della Digital Forensics



Outline

- Introduzione
- Transnational Cybercrime
- Digital Forensics e Digital Evidence
- **Workflow della Digital Forensics**
- Fasi del Processo di Investigazione
- Un Caso di Studio: Drone Forensics
- Conclusioni

Workflow della Digital Forensics – 1/3

- **Denuncia** o **segnalazione**

L'innesco del workflow è la **denuncia** o **segnalazione** di un'attività illecita

Workflow della Digital Forensics – 2/3

- Denuncia o segnalazione
- **Processo di investigazione**

Segue un **processo di investigazione** che costituisce l'elemento fondamentale

Workflow della Digital Forensics – 3/3

- Denuncia o segnalazione
- Processo di investigazione
- **Dibattimento**

Il tutto culmina in un **dibattimento** in sede giudiziale

Processo di Investigazione

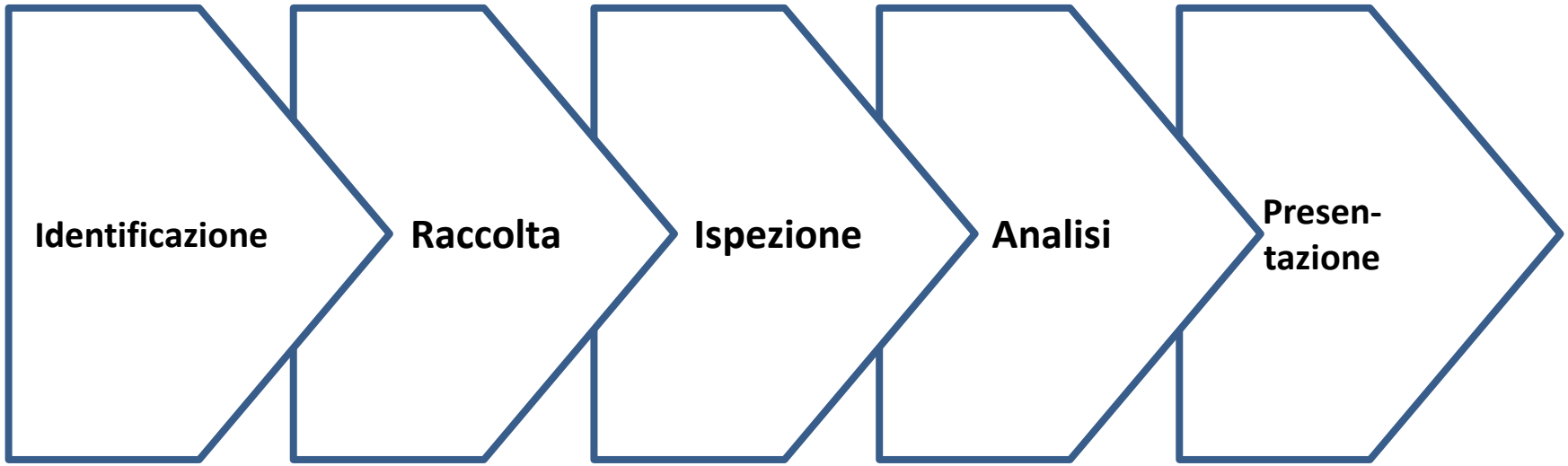
Outline

- Introduzione
- Transnational Cybercrime
- Digital Forensics e Digital Evidence
- Workflow della Digital Forensics
- **Fasi del Processo di Investigazione**
- Un Caso di Studio: Drone Forensics
- Conclusioni

Fasi del Processo di Investigazione

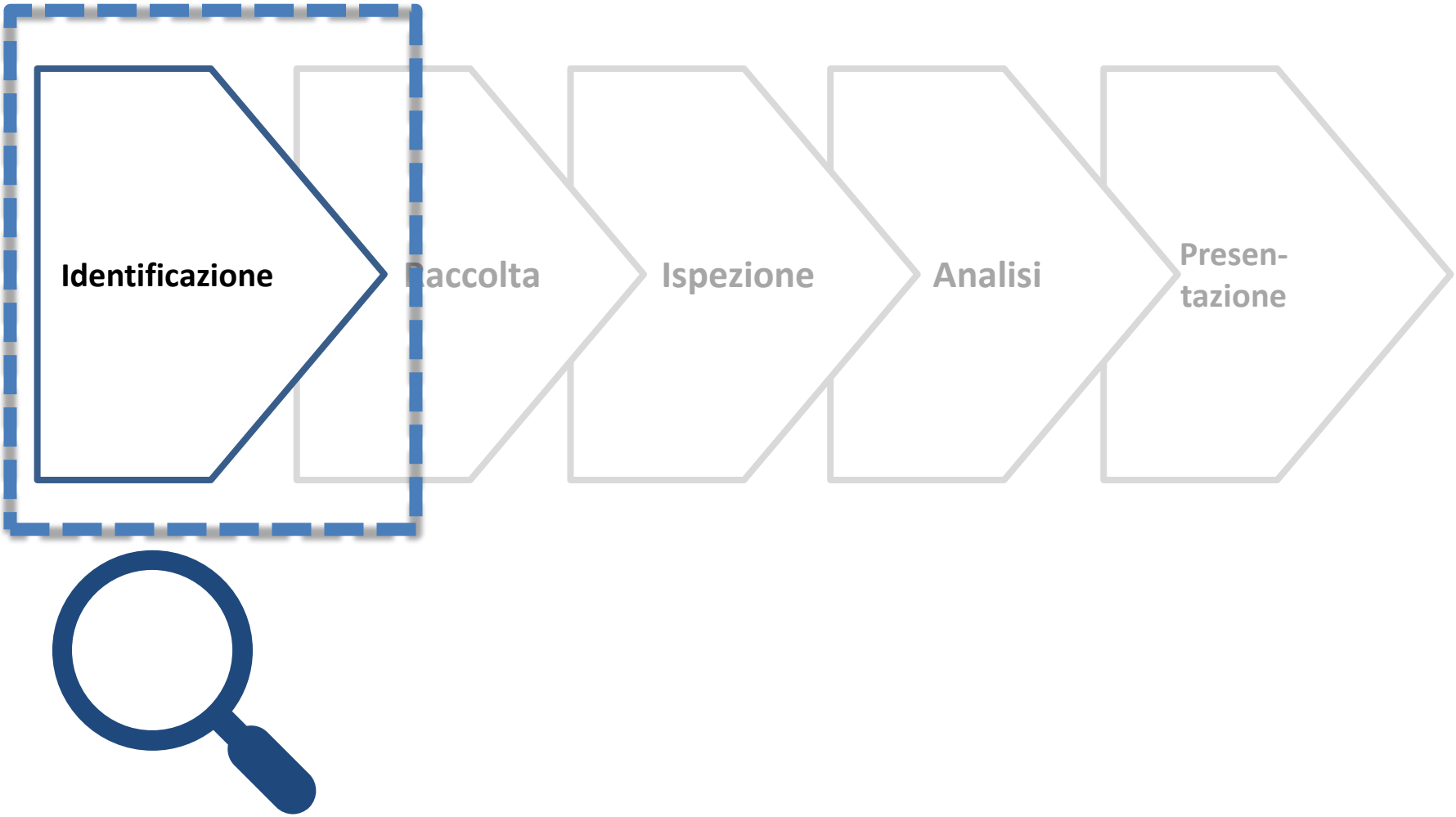
- Il **processo di investigazione** è articolato in cinque **fasi principali**:
  1. Identificazione
  2. Raccolta (o Acquisizione)
  3. Ispezione
  4. Analisi
  5. Presentazione

Fasi del Processo di Investigazione



Le fasi sono **consecutive**

Fasi del Processo di Investigazione



Identificazione – 1/3

- L'identificazione è una fase **estremamente importante**, poiché vengono **identificati dispositivi informatici** che potrebbero contenere **prove digitali**
  - Ad esempio:
    - Computer desktop
    - Laptop/Notebook/PC 2-in-1
    - Tablet e Smartphone
    - Penne USB, CD/DVD, ecc.
    - Dischi fissi interni, ecc.

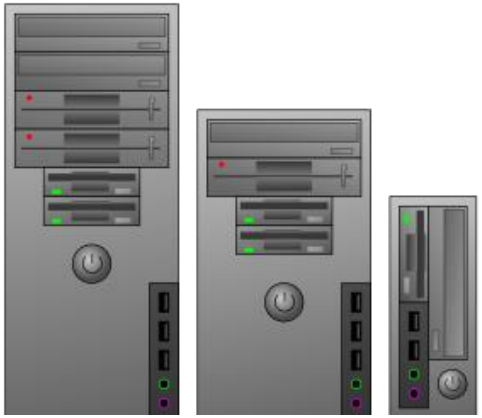
Identificazione – 2/3

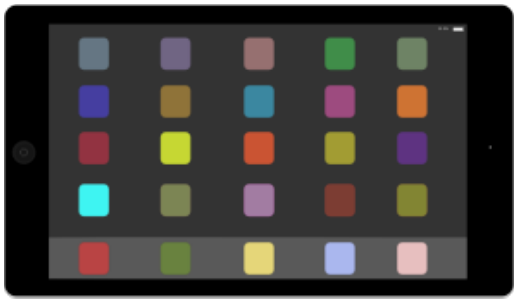
OSSERVAZIONE IMPORTANTE

I dispositivi informatici **NON** sono sempre facili da identificare

Identificazione – 3/3

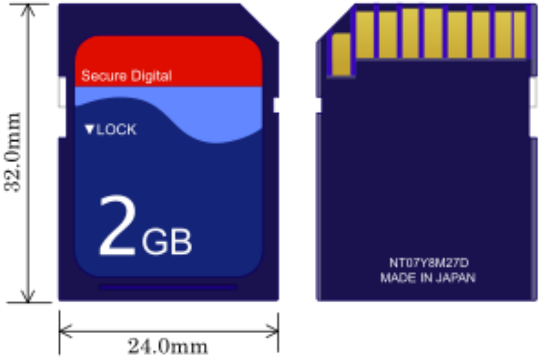
FACILE

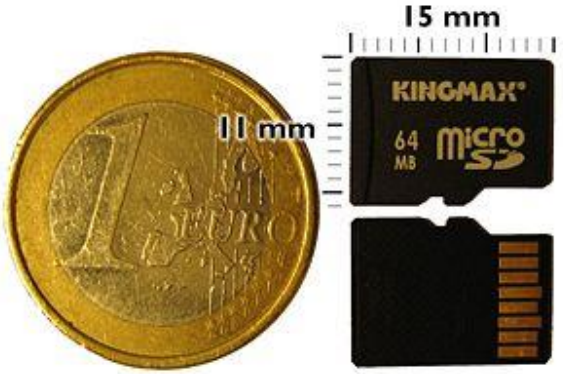


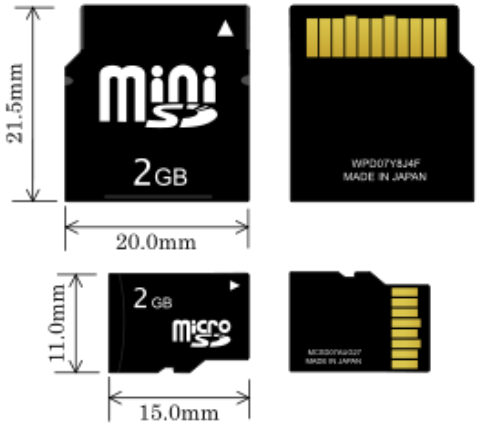


Identificazione – 3/3

MENO FACILE

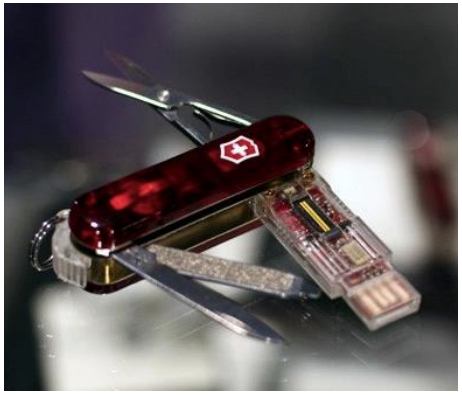






Identificazione – 3/3

DIFFICILE



Live System vs Dead System

Live Systems

Sistema in fase di attività

Dead Systems

Sistema NON in fase di attività

ALCUNE PROVE SONO CONTENUTE IN MEMORIE VOLATILI (SE SI SPEGNE IL SISTEMA, **POTREBBERO ESSERE PERSE**)

Live Analysis vs Post-Mortem Analysis

Live Systems

Sistema in fase di attività

→ **Live Analysis**

Dead Systems

Sistema NON in fase di attività

→ **Post-Mortem Analysis**

Conservazione delle Fonti di Prove Digitali

Fonte immagine:
https://upload.wikimedia.org/wikipedia/commons/6/6a/Mobiles.JPG

Fonti di Prove Digitali: Facili da Gestire?

- I dati e/o i dispositivi hardware potrebbe essere alterati o **danneggiati**

Intenzionalmente

Al fine di rendere difficile l'acquisizione agli investigatori

NON Intenzionalmente

Guasti meccanici (dovuti ad acqua, polvere, piccoli incendi, ecc.)

Fonti di Prove Digitali: Facili da Gestire?

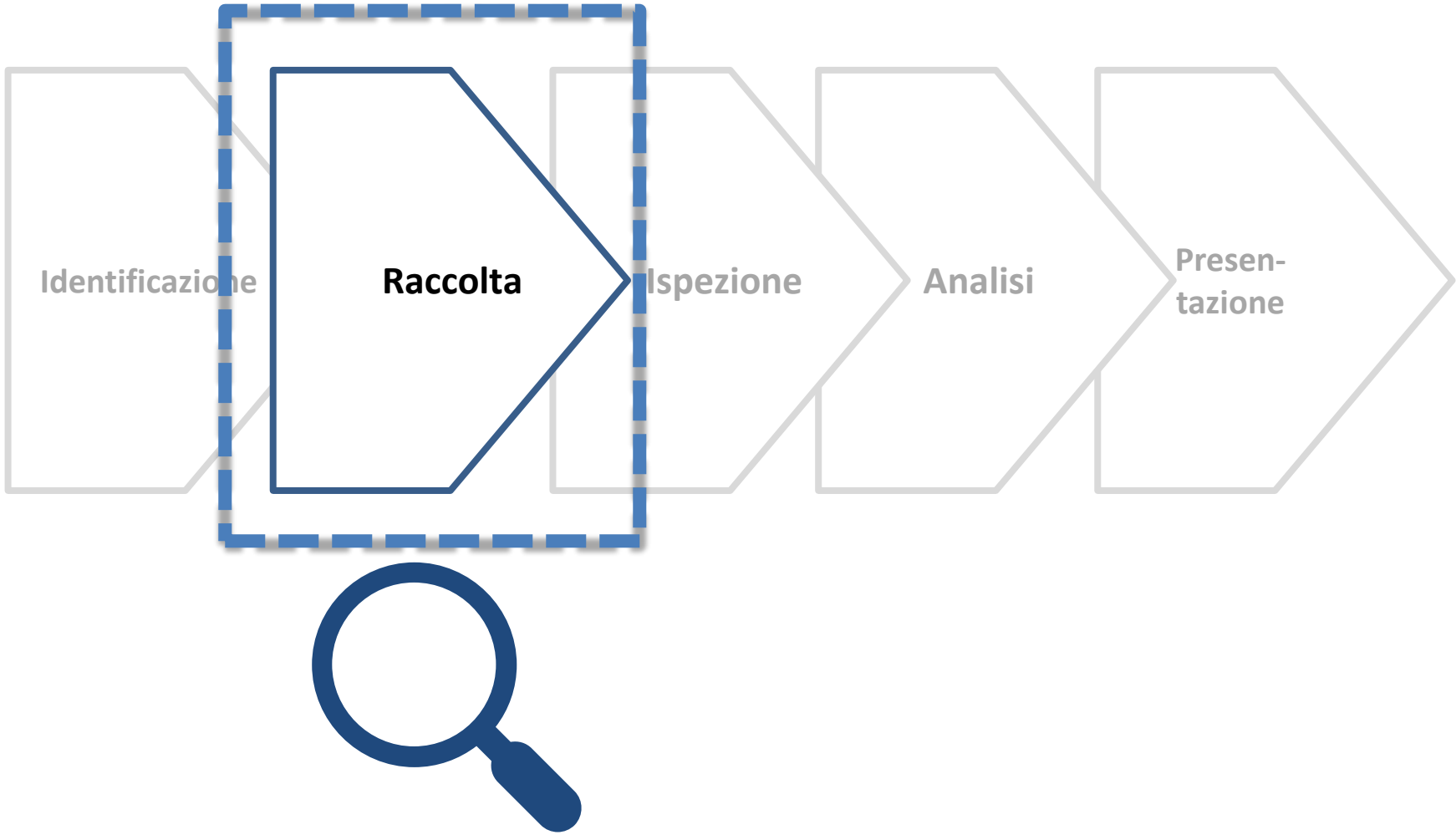
- **Problema:** In virtù dei possibili danni, talvolta, vi è quindi necessità di **ricostruire** dati appunto da **hardware/dati danneggiati**

Fonte immagine:
- https://upload.wikimedia.org/wikipedia/commons/3/39/Disassembled_HDD_and_SSD.JPG

Minacce: Dati «Cartacei» VS Dati Digitali

Alcune Minacce per i dati «cartacei»	Alcune Minacce per i dati digitali	
• Acqua • Fuoco e Umidità • Insetti • Età • Disastri naturali	• Errori Umani/Negligenze • Campi elettromagnetici e/o magnetici • Acqua • Umidità e Condensa • Polvere • Calore e Fuoco	• Fuoco • Impatti fisici • Voltaggio • Elettricità statica • Disastri naturali

Fasi del Processo di Investigazione



Raccolta – 1/3

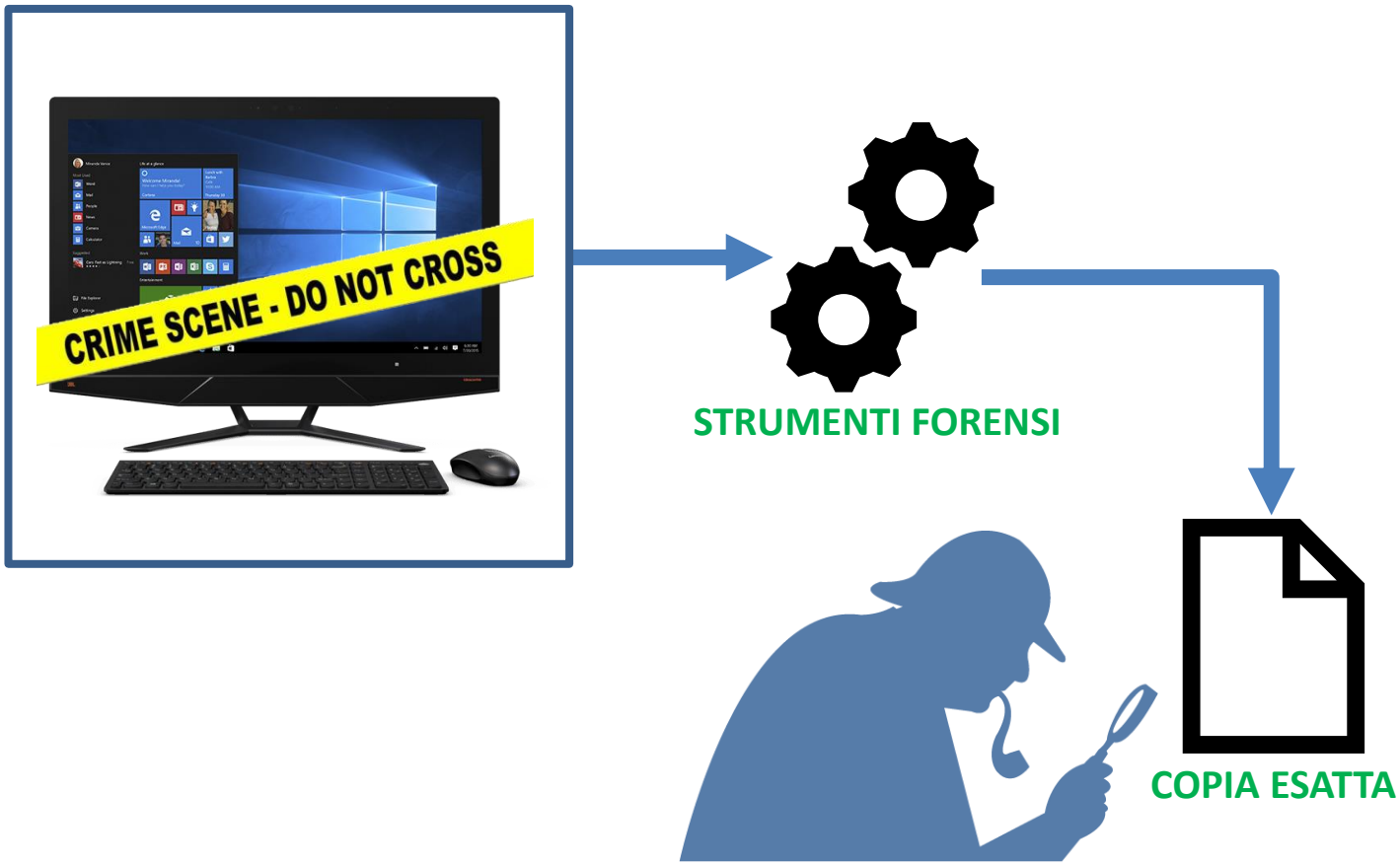
Raccolta – 2/3

PROCEDURA ERRATA

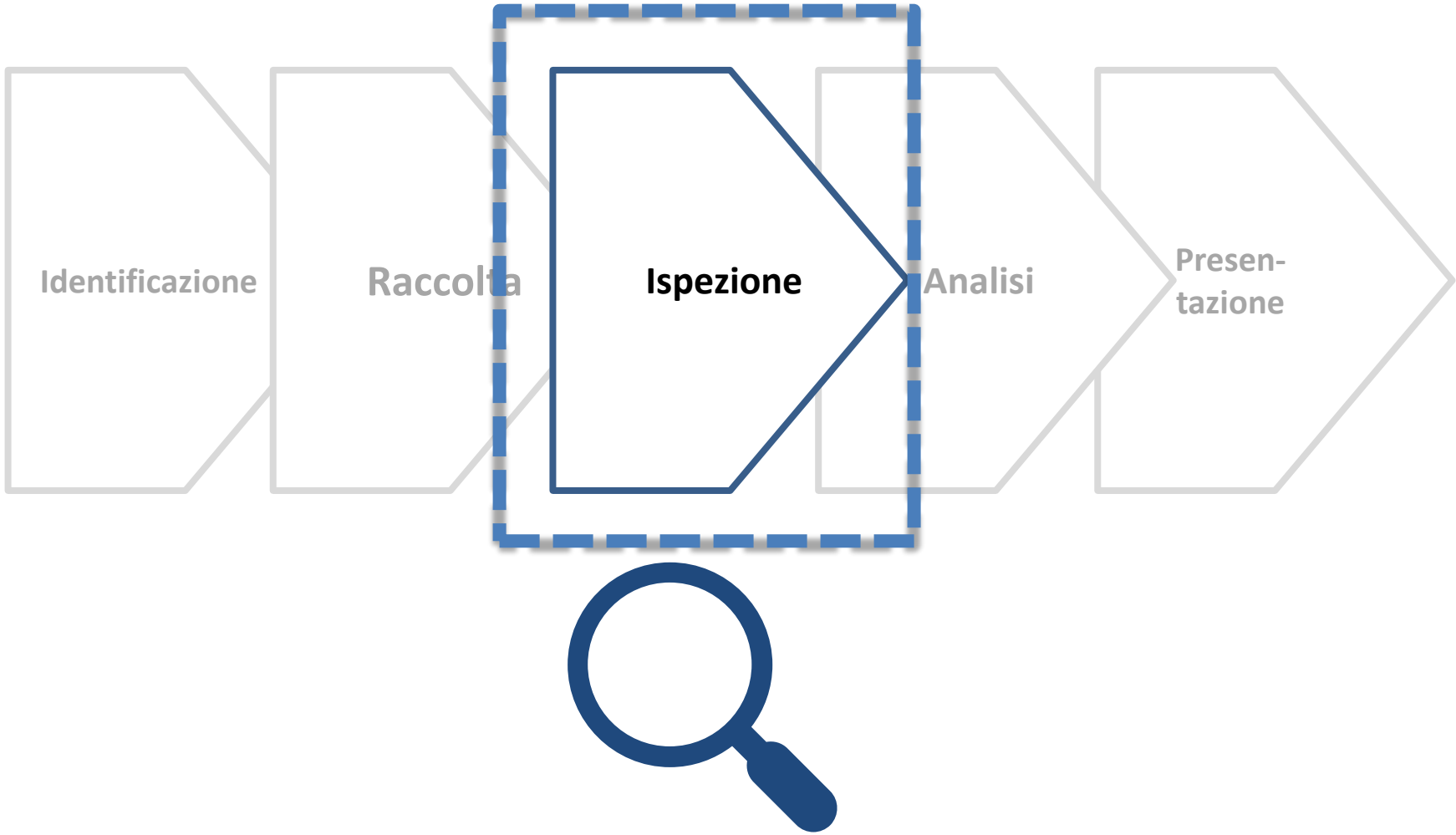
Per evitare **eventuali compromissioni** dei dati originali e, conseguentemente, compromettere le prove, è necessario lavorare **su delle copie «esatte» dei dati**

Raccolta – 3/3

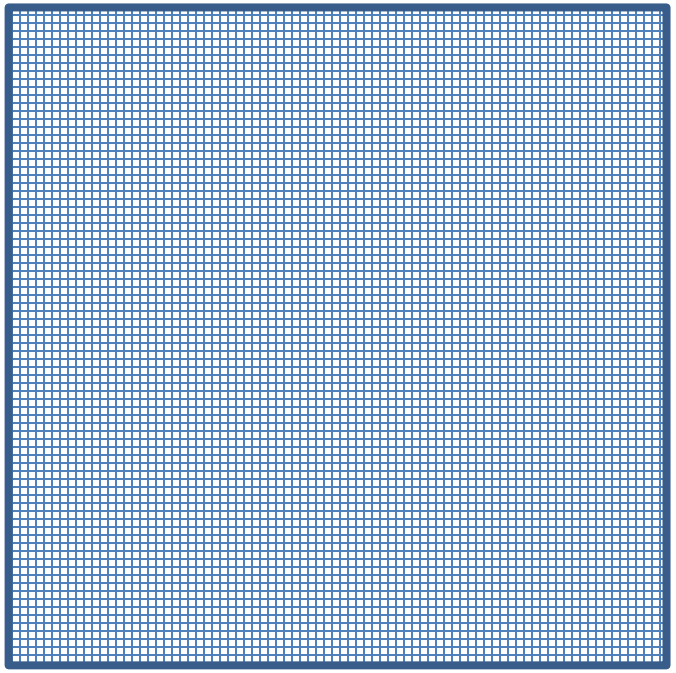
PROCEDURA CORRETTA



Fasi del Processo di Investigazione



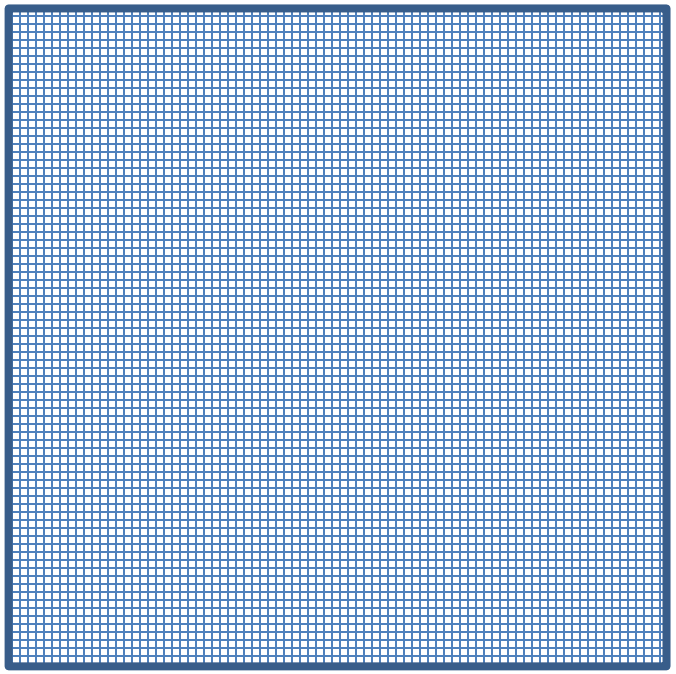
Ispezione – 1/3



COPIA ESATTA

Ispezione – 2/3

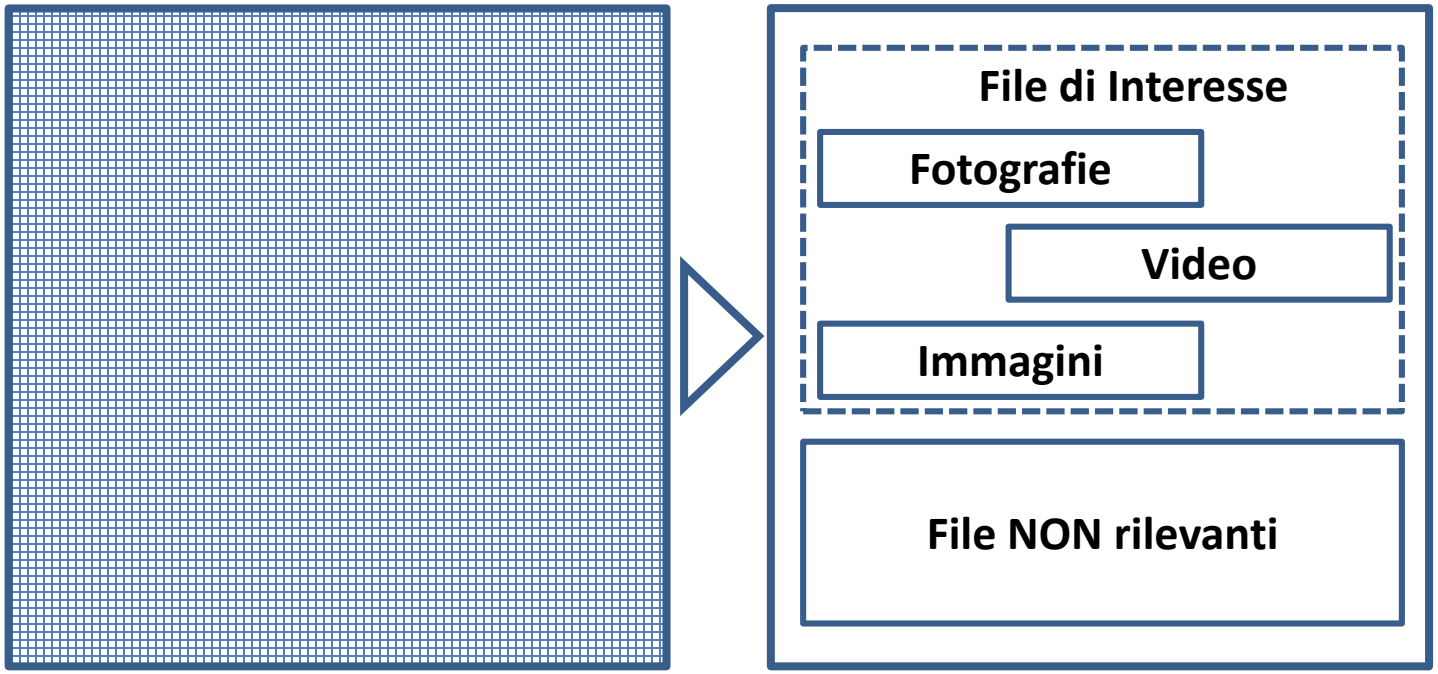
Riduzione e Filtraggio dei Dati Acquisiti



COPIA ESATTA

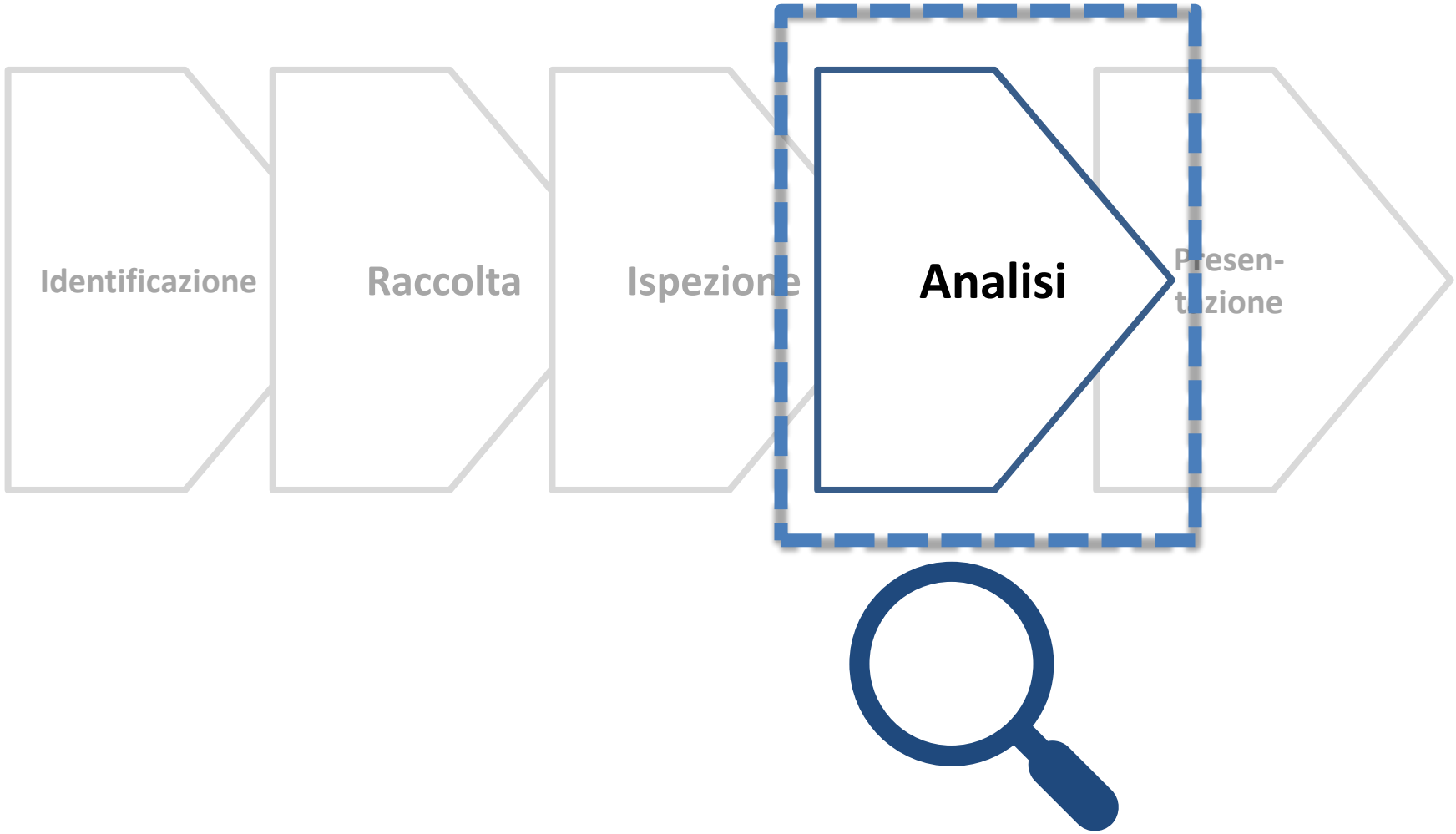
Ispezione – 3/3

Riduzione e Filtraggio dei Dati Acquisiti



COPIA ESATTA

Fasi del Processo di Investigazione



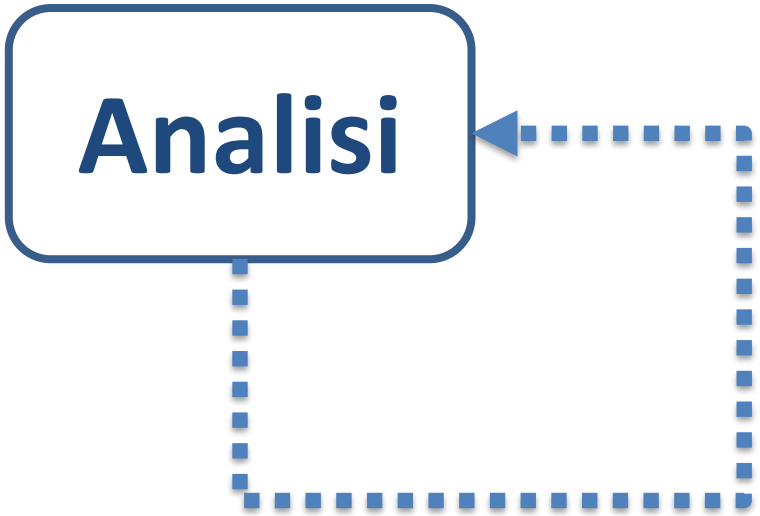
Analisi – 1/3

- I dati e/o i dispositivi hardware potrebbe essere alterati o **danneggiati**

OBIETTIVO

Determinare i ***fatti***, in relazione ad un **evento illecito**, e di determinare l'importanza e/o la **significatività di una prova** e **il/i soggetto/i responsabile/i**

Analisi – 2/3

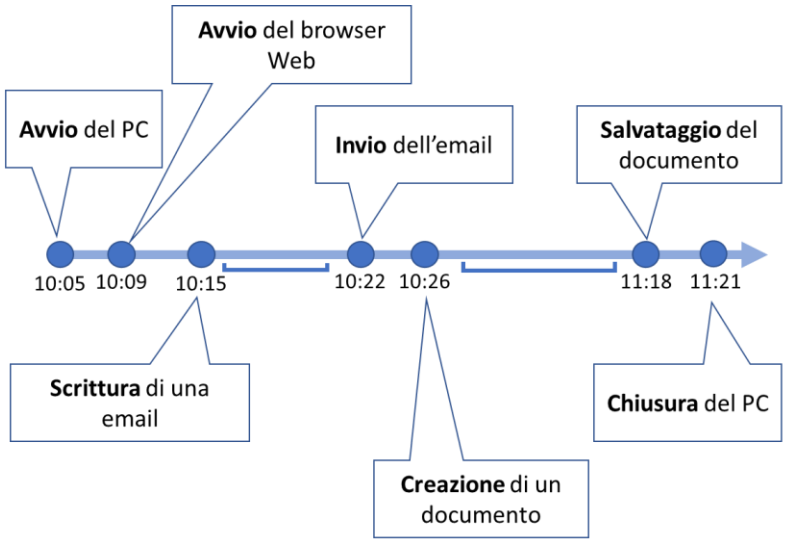


OSSERVAZIONE

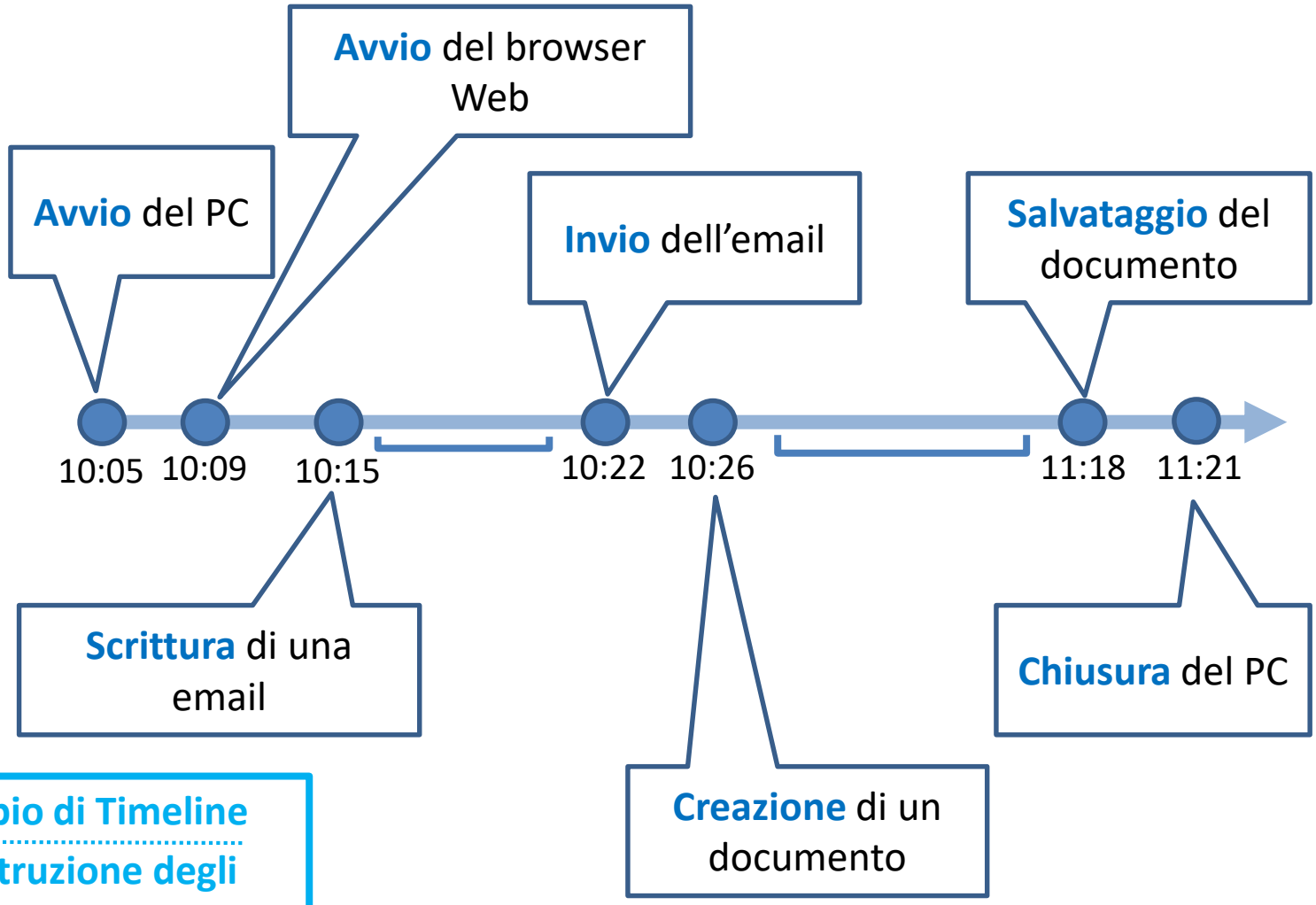
La fase di analisi è un essa stessa un **processo iterativo, in cui sono possibili raffinamenti successivi**

Analisi – 3/3

Un'attività della fase di analisi, è la ***redazione di una timeline*** che ricostruisca le attività di un cybercriminale in **ordine temporale**



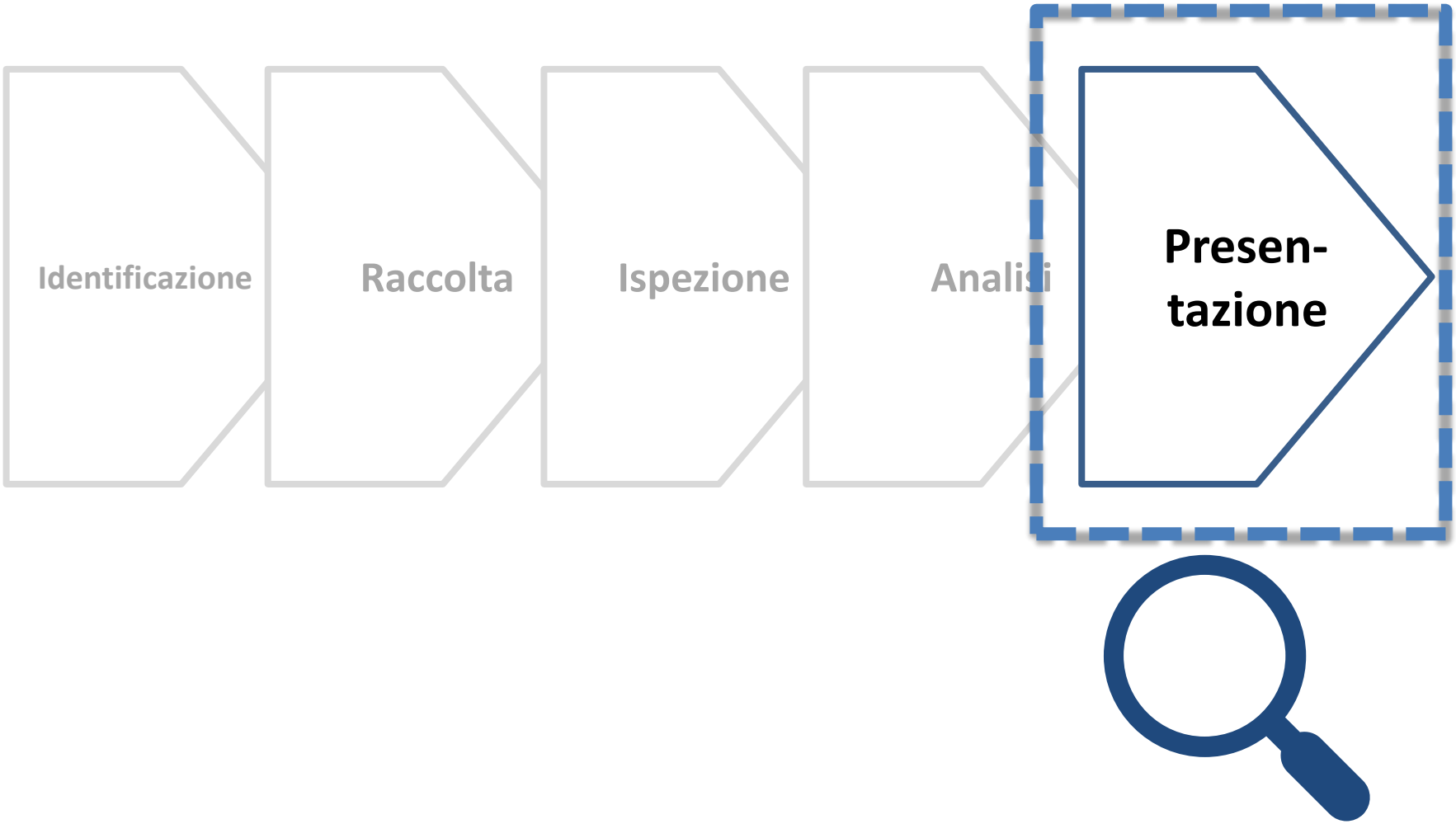
Analisi – 3/3



Esempio di Timeline

Ricostruzione degli Eventi e delle Attività

Fasi del Processo di Investigazione



Presentazione

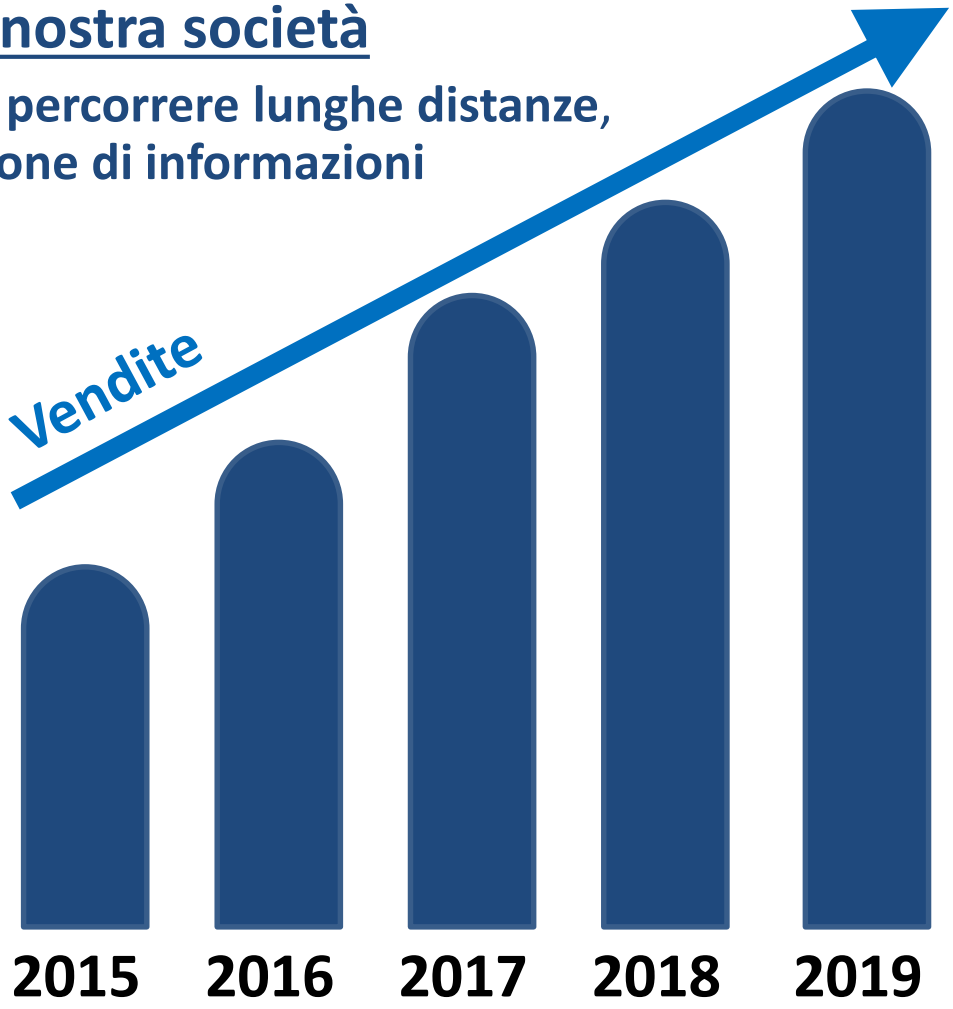
- La fase di **presentazione** è la fase in cui viene prodotta la documentazione finale relativa al risultato dell'investigazione
- Sarà presentata in **tribunale** o negli **uffici preposti**

Outline

- Introduzione
- Transnational Cybercrime
- Digital Forensics e Digital Evidence
- Workflow della Digital Forensics
- Fasi del Processo di Investigazione
- **Un Caso di Studio: Drone Forensics**
- Conclusioni

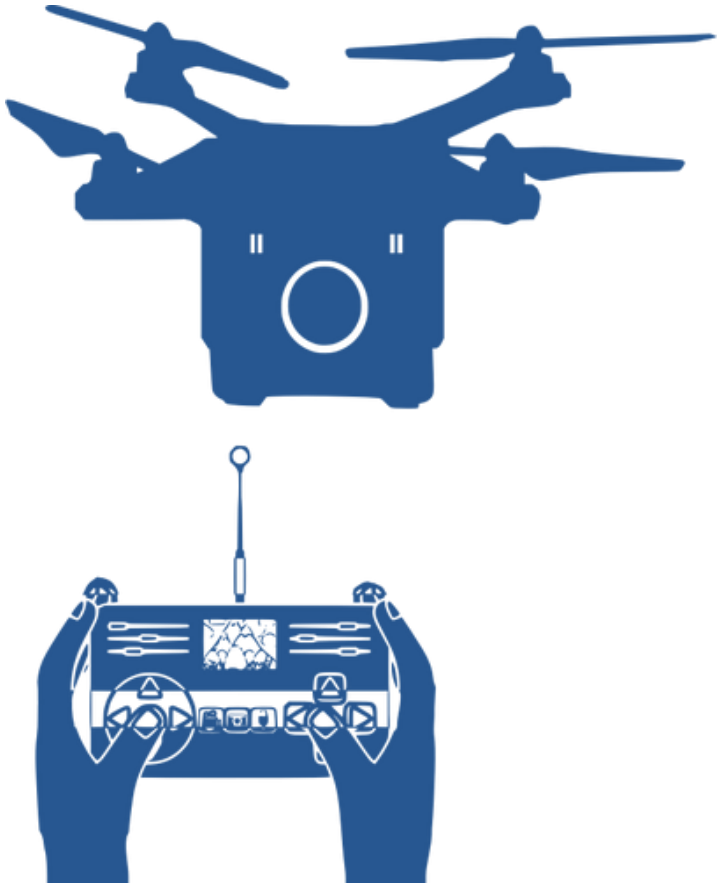
Introduzione – 1/3

- Negli ultimi anni, vi è stata una **<u>importante diffusione dei droni nella nostra società</u>**
  - Grazie alle loro **capacità di percorrere lunghe distanze**, **acquisizione** e di **elaborazione di informazioni**



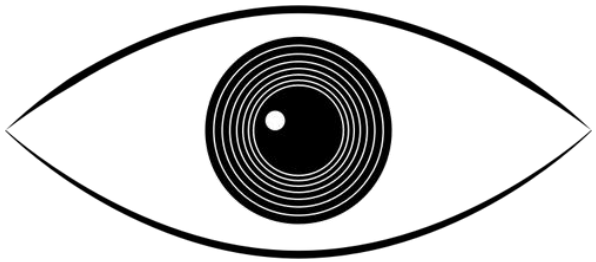
Introduzione – 2/3

- Tutte queste caratteristiche li rendono **adatti in diversi ambiti**:
  - Fotografia Aerea
  - Riprese video
  - Sicurezza e tracciamento
  - Monitoraggio ambientale
  - Monitoraggio architettonico
  - Ricerca dei dispersi
  - Telerilevamento



Introduzione – 3/3

- Oltre gli utilizzi leciti i droni vengono utilizzati anche per **attività illegali**:
  - Violazione della **privacy**
  - Spionaggio di individui
  - Spionaggio industriale
  - Spionaggio di enti governativi
  - Contrabbando



Proprio per questi motivi la drone forensics (branca della digital forensics) ha iniziato ad acquistare importanza

Attività Illegali e Drone Forensic

Esempio 1

- **Agosto 2016**
  - Un drone filmava **costantemente persone mentre prelevavano da un bancomat** a Templepatrick, nell'Irlanda del Nord
  - Probabilmente stava **cercando di registrare l'immissione dei loro PIN**

Attività Illegali e Drone Forensic

Esempio 2

- Un gruppo di criminali ha provato a **immettere droga** e un **cellulare** in una **prigione dell'Ohio**, tramite un drone

Fonte notizia:

- https://video.corriere.it/esteri/droga-cellulari-carcere-un-drone-ecco-come/f9fa7a94-df7c-11e9-aa5f-fbca0c81b7c9

Attività Illegali e Drone Forensic

Esempio 2bis

- **Ottobre 2018**

Salerno, usano il drone per consegnare la droga ai carcerati

Già nell'ottobre del 2018 l'analogo tentativo era fallito nel carcere di Taranto. Allora il velivolo precipitò nel cortile mentre trasportava due microtelefoni cellulari e dei wurstel imbottiti di stupefacenti

Sono ricorsi ai progressi della tecnologia per cercare di far entrare in **carcere** materiale proibito. È successo a **Fuorni**, in provincia di Salerno, dove invece di utilizzare i consueti nascondigli fantasiosi e i veloci passaggi di mano durante i colloqui, si è provato a far entrare la **droga** nella casa circondariale attraverso un **drone**.

Fonte notizia:

- http://www.ilgiornale.it/news/cronache/salerno-usano-drone-consegnare-droga-ai-carcerati-1659740.html

Attività Illegali e Drone Forensic

Esempio 2ter

- Il cartello messicano ha provato a **contrabbandare droga**, mediante droni

Fonte notizia e immagine:

- https://it.businessinsider.com/i-narcos-messicani-hanno-una-nuova-arma-i-droni/

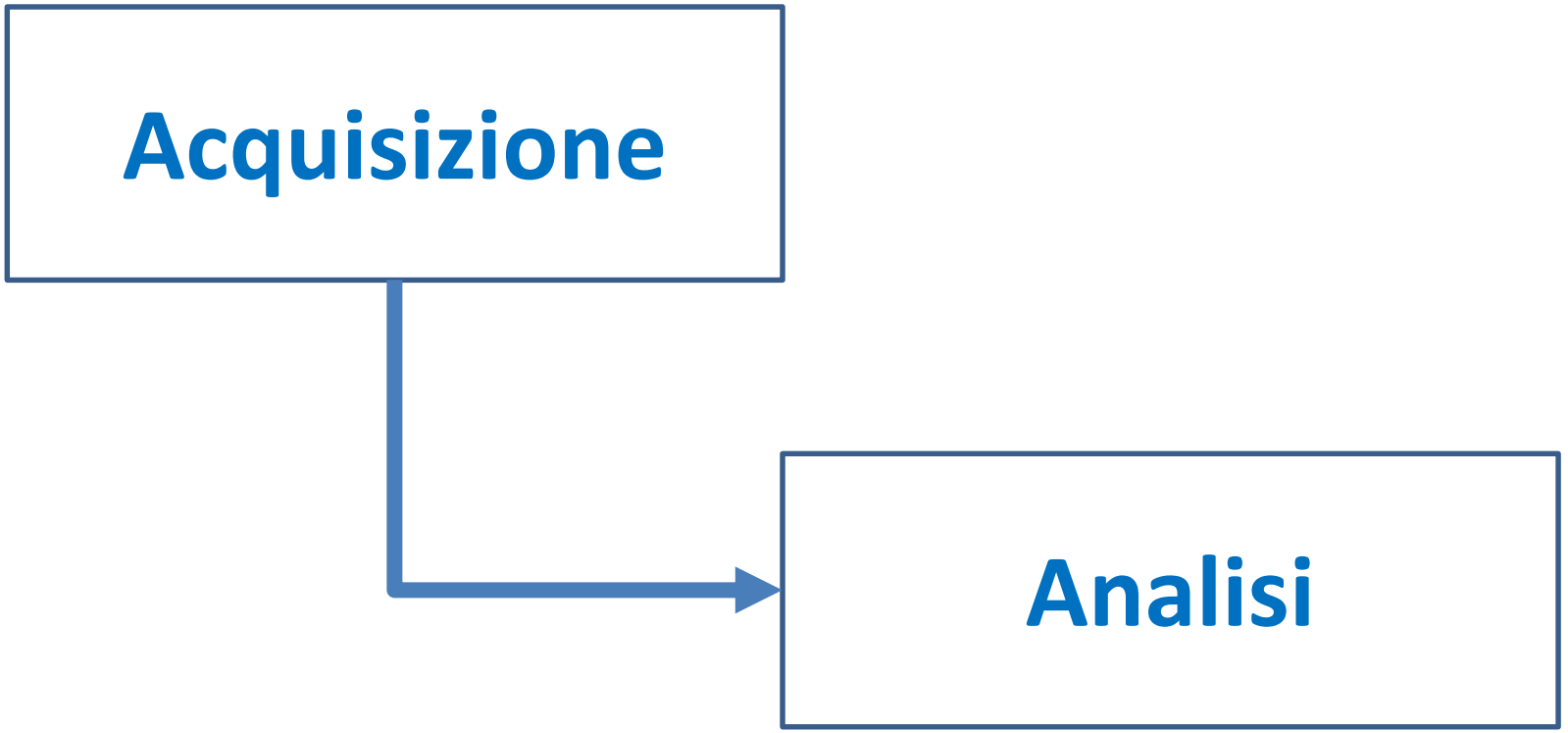
Attività Illegali e Drone Forensic

Esempio 3

- **Inizio 2017**
  - Una coppia nota un drone in «*hovering*» **fuori dalla finestra del bagno**
  - Evidente **violazione della privacy**

Un Esempio Pratico

Ci soffermeremo sulle fasi di:



Un Esempio Pratico

Ci soffermeremo sulle fasi di:

Acquisizione

Analisi

Esempio Pratico: Acquisizione

- Prevede il **sequestro dei supporti**:
  - Drone
  - Componenti (se possibile)
    - Controller, memorie rimovibili, ecc.
- Segnalazione di **eventuali modifiche** al drone
  - **Documentazione** attraverso **fotografie**
  - Segnalazione di eventuali **capacità del drone**
    - Video/foto/audio
    - Capacità di carico
    - Ecc.

Un Esempio Pratico

Ci soffermeremo sulle fasi di:

Acquisizione

Analisi

Esempio Pratico: Analisi (Cenni)

Dopo aver raccolto e analizzato le prove, vengono **ricostruiti gli eventi**

Esempio Pratico: Analisi (Cenni)

Analizzando la memoria del drone, ho ricostruito il tragitto!

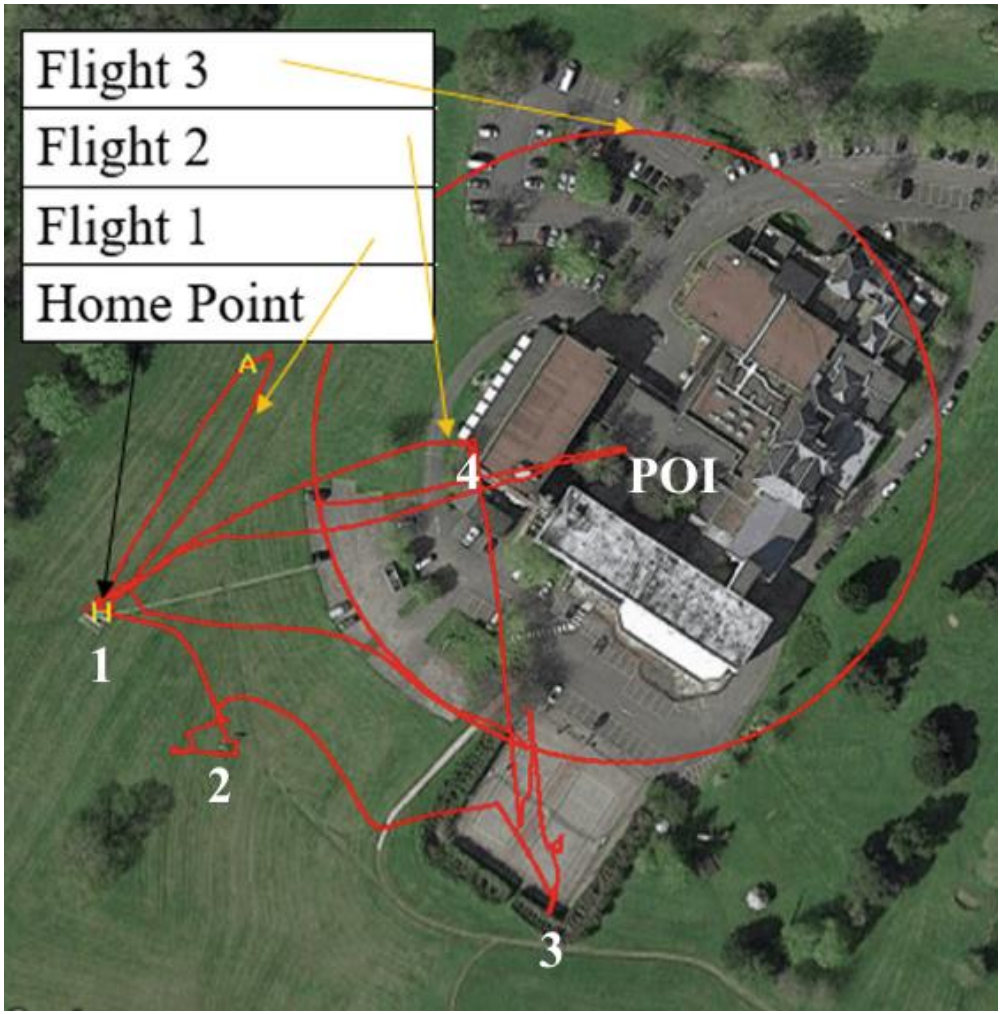


Immagine estratta da [6]

Outline

- Introduzione
- Transnational Cybercrime
- Digital Forensics e Digital Evidence
- Workflow della Digital Forensics
- Fasi del Processo di Investigazione
- Un Caso di Studio: Drone Forensics
- **Conclusioni**

Conclusioni

- **Cybercrime e transnational cybercrime** sono e in **continua evoluzione**
- Di conseguenza, la **digital forensics** svolge un ruolo chiave nell'individuazione di evidenze digitali, al fine di prevenire **cybercrimini** e punire i **cybercriminali**
  - Anch'essa è in continua **evoluzione** per contrastare al meglio il **cybercrime**
    - Perché la tecnologia si **evolve** e diventa sempre più usata nei **cybercrimini**

Riferimenti Bibliografici

1. Alexandrou, Alex. **"10 Cybercrime"**, *International and Transnational Crime and Justice* (2019): 61-66.
2. Faga, Hemen Philip. **"The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century"**, *Baltic Journal of Law & Politics* 10.1 (2017): 1-34
3. Choo, Kim-Kwang Raymond, and Russell G. Smith. **"Criminal exploitation of online systems by organised crime groups"**, *Asian journal of criminology* 3.1 (2008): 37-59
4. Årnes, André (Editor). **"*Digital forensics.*"** John Wiley & Sons, 2017 (Chapters 1, 2)
5. Garfinkel, Simson L. **"Digital forensics research: The next 10 years."** digital investigation 7 (2010): S64-S73.
6. Barton, Thomas Edward Allen, and MA Hannan Bin Azhar. **"Open source forensics for a multi-platform drone system."** *International Conference on Digital Forensics and Cyber Crime*. Springer, Cham, 2017.