



UNIVERSITÀ DI PISA

in collaborazione con

Master Universitario di I Livello in Cybersecurity

Digital Forensics

Arianna Del Soldato, Maurizio Martinelli

Istituto di Informatica e Telematica - CNR
Unità Tecnologica Innovazione Digitale

arianna.delsoldato@iit.cnr.it, maurizio.martinelli@iit.cnr.it

Programma del Corso

- Breve descrizione IIT
- Introduzione alla Digital Forensics
- Cyber Crime
- La figura dell'Investigatore Digitale
- I requisiti per la gestione dell'evidenza digitale
- Le fasi principali della Digital Forensics
 - Identificazione della prova
 - Ricerca delle fonti di prova e riconoscimento
 - Acquisizione e Conservazione
 - Analisi
 - Presentazione e Valutazione
- Norme applicabili e Best practice
- Analisi forense di sistemi di file sharing
- Cloud Forensics
- Vehicle Forensics
- Anti-forensics
- Esercitazione

Sommario

- Breve descrizione IIT
- Introduzione alla Digital Forensics
- Cyber Crime
- La figura dell'Investigatore Digitale
- I requisiti per la gestione dell'evidenza digitale

BREVE DESCRIZIONE IIT

L'Istituto di Informatica e telematica

- È dislocato presso l'Area della Ricerca del CNR di Pisa
 - La più grande Area di Ricerca in Italia
 - 12 Istituti per un totale di oltre 1500 persone
- Conta quasi 200 persone, tra ricercatori, tecnologi, assegnisti di ricerca, tecnici, amministrativi e borsisti
- Principali tematiche di ricerca e servizi
 - Algoritmi e matematica computazionale
 - Trustworthy and Secure Future Internet
 - Ubiquitous Internet
 - **Innovazione Digitale**
 - **Registro.it**



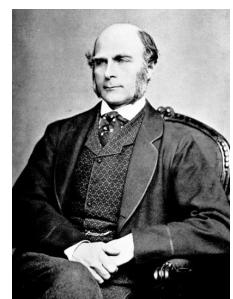
Unità Innovazione Digitale: Missione

- Pianificare, progettare e realizzare servizi e applicazioni innovative per:
 - L'Istituto e il CNR
 - Il Registro.it
 - La Pubblica Amministrazione italiana
- Principali settori di competenza: DNS, PE, DB, Web, CMS, gestione di data-center, sistemi di registrazione dei domini, sistemi di monitoraggio del traffico di rete e dei servizi, architetture di rete, sistemi di crawling e analisi dei dati, ecc.
- Attività di R&D
- Tirocini, tesi, ecc.
- L'Unità Tecnologica è costituita da 7 Unità Operative per un totale di quasi 30 persone

INTRODUZIONE ALLA DIGITAL FORENSICS

Forensics: un po' di storia

- **Forensic** letteralmente significa “forense”, cioè che concerne il foro e, quindi, l’attività giudiziaria
- Più in generale assume il significato di “utilizzo della scienza nei casi legali” e quindi di “indagini della polizia scientifica”
- Ha origini antiche: l’esploratore e antropologo britannico **Francis Galton** (1822-1911) fece moltissimi studi sulle impronte digitali degli individui e ideò un sistema per la loro classificazione, favorendone l’effettiva adozione nelle aule giudiziarie



Forensics: un po' di storia

- **Leone Lattes** (1887–1954), lo scienziato italiano pioniere nello studio della **Forensic Serology** che nel 1916 scoprì i diversi gruppi sanguigni
 - **Case #1**
A guy returned home from a trip and had blood on his shirt. His wife accused him of cheating but the man said he didn't cheat it was either his own blood or blood from the meat shop. Lattes tested the blood and found out that the blood was human and it was type O which was the guy's blood type
 - **Case #2**
A guy was accused of homicide because he had lots of blood on his coat. Lattes tested the blood from the guy's coat and the victim. He found out that the blood on the coat was type O while the victim's blood was type A. Therefore the guy was safe and wasn't accused of possible homicide

Forensics: un po' di storia

- **Calvin Goddard** (1891-1955), lo scienziato di Baltimora pioniere nella **Forensic ballistics** e, in particolare, nel confronto scientifico, al microscopio, tra le armi e i relativi proiettili
 - Fu il responsabile del primo laboratorio indipendente di criminologia degli USA (1925)
 - Il primo laboratorio di Forensics dell'FBI è del 1932
- **Hans Gross** (1847-1915), il criminologo austriaco considerato tuttora il padre della scienza dell'indagine criminale
- E poi ancora **Albert Osborn** (1858–1946), il padre della **Questioned document examination (QDE)**, cioè la scienza forense che si occupa di stabilire se un documento è originale, autentico, è stato alterato, ecc.



E la Digital Forensics?

- La **Digital Forensics** (o **Computer Forensics**) è un processo investigativo che fa uso di tecniche informatiche per **identificare, acquisire, conservare e analizzare** indizi o fonti di prova digitali
 - In altre parole, è la scienza che studia:
 - **Identificazione**
 - **Acquisizione e conservazione**
 - **Analisi**
 - **Documentazione**
- di un **dato informatico** per essere valutato in un processo giuridico*

Obiettivi della Digital Forensics

- Le investigazioni digitali hanno assunto un ruolo molto importante ai giorni d'oggi
- Il numero di attacchi informatici è in continuo aumento e Internet è considerato un canale "sicuro" per la criminalità
- L'identità "digitale" di una persona è ormai molto più complessa e ricca di informazioni di quella "reale"
- L'esame della "digital evidence" è entrato di diritto nell'analisi dei fatti, delle prove e degli alibi che ruotano intorno ad un "evento criminale"
 - Un "forensic/digital investigator" deve essere in grado di:
 - Determinare la natura e gli eventi relativi ad un crimine
 - Seguire una procedura investigativa rigorosa al fine di individuare il potenziale colpevole

Che cos'è la Digital Evidence?

- Non esiste una definizione "formalizzata" di **digital evidence**
 - Può essere definita come **qualsiasi informazione avente valore probatorio che sia memorizzata o trasmessa in forma digitale**
- Una digital evidence può quindi essere ricavata da:
 - Un **dispositivo di memorizzazione digitale**
 - PC, notebook, HD esterno, NAS, nastro, CD/DVD, memory card, USB drive, ecc.....
 - Cellulari, Smartphone, Smartwatch, Tablet, Navigatori, ecc...
 - Una **rete** (Intranet/Internet)
 - Traffico di rete
 - Email (client/server)
 - Web (client/server)
 - Social network
 - Chat/IM
 - Cloud
 - ...

La Digital Evidence

- Una digital evidence è **fragile per natura**, ovvero facilmente modificabile
 - Se il dispositivo che contiene le informazioni di interesse **viene spento**, i dati che non sono stati salvati possono andare definitivamente persi
 - Se il dispositivo viene rivenuto spento, **l'accensione comporta modifiche al sistema e/o ai dati in esso contenuti**
 - Se il dispositivo è connesso ad Internet o ad una rete aziendale, **possono avvenire accessi dall'esterno con l'obiettivo di cancellare le informazioni**
 - Se la digital evidence si trova su Internet (sito web, profilo di social network, ecc.), **può essere modificata e/o rimossa dall'owner della pagina**

La Digital Evidence (cont)

- I dati digitali possono essere divisi in due categorie principali:
 - **Dati volatili**
 - Sono dati facilmente alterabili/persi in caso di spegnimento del dispositivo che li conserva
 - Utenti connessi in un determinato istante
 - File aperti
 - Software e servizi in esecuzione
 - Contenuto della RAM
 - Applicazioni aperte in uno smartphone/tablet
 - Contenuti di alcune tipologie di sistemi di chat e videoconferenze
 - **Dati non volatili**
 - Dati conservati generalmente su memorie di massa e che non sono cancellati in caso di spegnimento del dispositivo che li conserva
 - File personali (documenti, fogli di calcolo, archivio immagini, ecc.)
 - Sistema Operativo
 - File di configurazione e di utilizzo da parte degli applicativi
 - Database
 - Sistemi di backup (online, offline, remoto, cloud, ecc.)

IL CYBER CRIME

Il Cyber Crime

- Il **cyber crime**, o computer crime, può essere definito come «qualsiasi reato o comportamento delittuoso svolto nell'ambito delle tecnologie informatiche»
- Può essere suddiviso in due categorie principali:
 - Crimini il cui scopo è **attaccare una risorsa di rete**
 - Virus, malware, attacchi mirati, DoS, DDoS, ecc.
 - Crimini che vengono perpetrati utilizzando i computer in rete per effettuare **frodi online, furti d'identità, furti della proprietà intellettuale, cyberbullismo, cyberstalking, cyberwarfare**, ecc.
- Attori principali:
 - **Il soggetto che commette il crimine**
 - **Tool** per commettere il crimine
 - **Target** del crimine (vittima)
 - **Materiale** (informazione) potenzialmente appetibile

Chi sono i cyber criminali

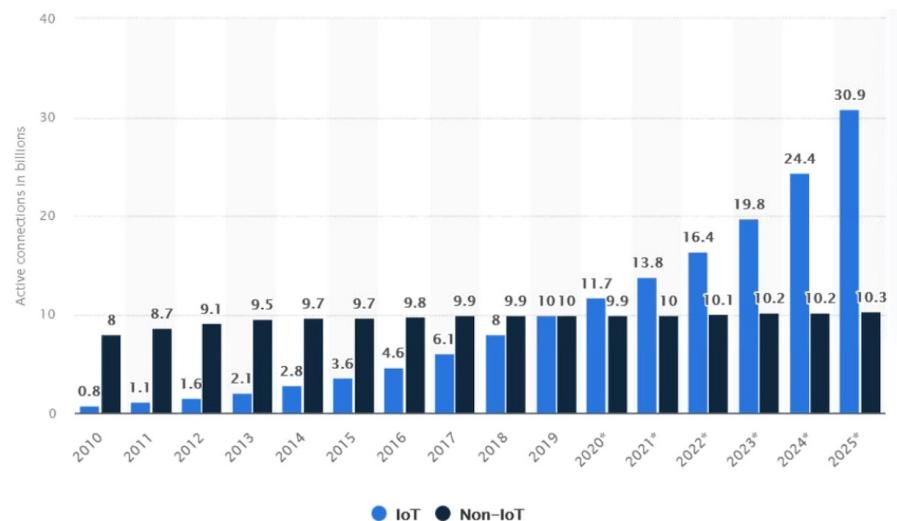
- **Criminali singoli o organizzati**
 - Spesso privi di particolari competenze tecniche
- **Obiettivi**
 - **Ottener dati**, quali credenziali, numeri di carte di credito, elenchi di contatti, database
 - **Inibire un servizio** o un applicativo (Distributed Denial of Service - DDoS)
- Alcune motivazioni:
 - **Sfide** (generalmente tra giovani)
 - **Attacchi su commissione** (competitor, vendetta, scopi commerciali...)
 - **Spionaggio industriale**, politico, ...
 - A scopo remunerativo
 - **Estorcere**
 - **Impersonificare** (furto d'identità)
- La proliferazione dei computer e della rete, la disponibilità di tool gratuiti per sferrare attacchi, di botnet (reti controllate da un botmaster e composta da dispositivi infettati da malware specializzato, detti bot o zombie), l'anonimizzazione che la rete offre, rendono il **Cyber Crime** un'attività relativamente semplice e **profittevole...**

Chi sono i cyber criminali (cont)

- L'hacker è sempre cattivo?
- **White Hat** (hacker etico)
 - usa le sue vaste competenze tecniche per scoprire e segnalare vulnerabilità dei sistemi e dei software informatici, affinché possano essere risolte tempestivamente
- **Black Hat** (cracker, pirati informatici) sfrutta le vulnerabilità o inganna gli utenti della rete con intenti criminali

Superficie di attacco

- Superficie di attacco: insieme di vulnerabilità, percorsi o metodi che gli hacker possono utilizzare per ottenere accessi non autorizzati a reti, sistemi e dati, o per compiere un attacco informatico
 - Più utenti
 - Più traffico
 - Più dati
 - Più dispositivi
 - Più smartphone
 - IoT



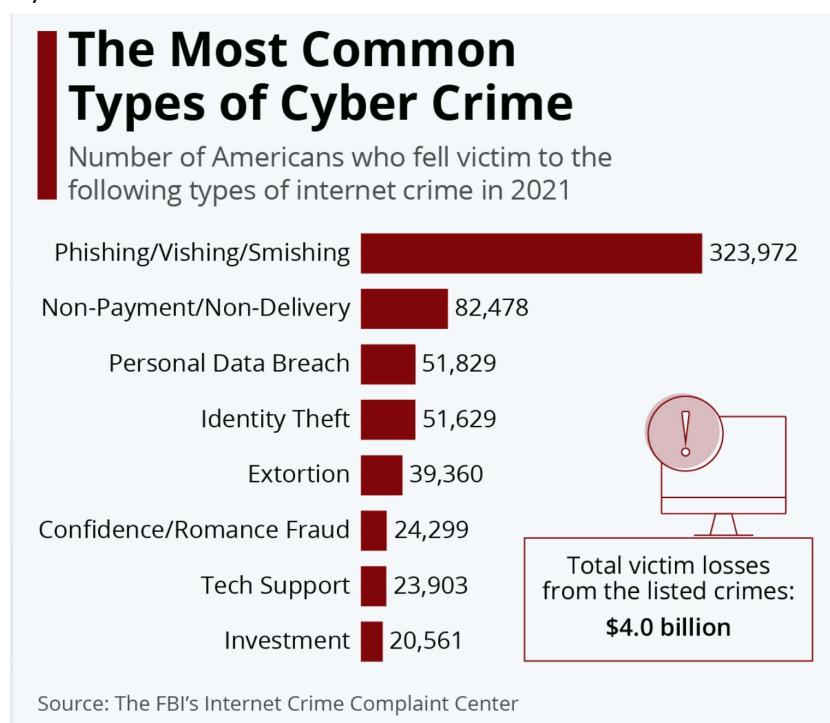
Cyber Crime: un po' di dati

- Le aziende americane hanno subito, negli ultimi anni, perdite pari a oltre 500 milioni/anno a causa del cybercrime
 - la maggior parte di attacchi sono imputabili a attacchi di tipo DoS/ DDoS e generati da codice malevolo
- Lloyd's Assicurazioni ha stimato i danni causati da attacchi informatici in circa **450 miliardi di dollari** all'anno (include sia i crash di sistema che i costi di ripristino)
- Juniper Networks valuta che il costo mondiale per la perdita di dati sensibili di aziende e cittadini si attesta su una cifra superiore a **1,2 trilioni di dollari**

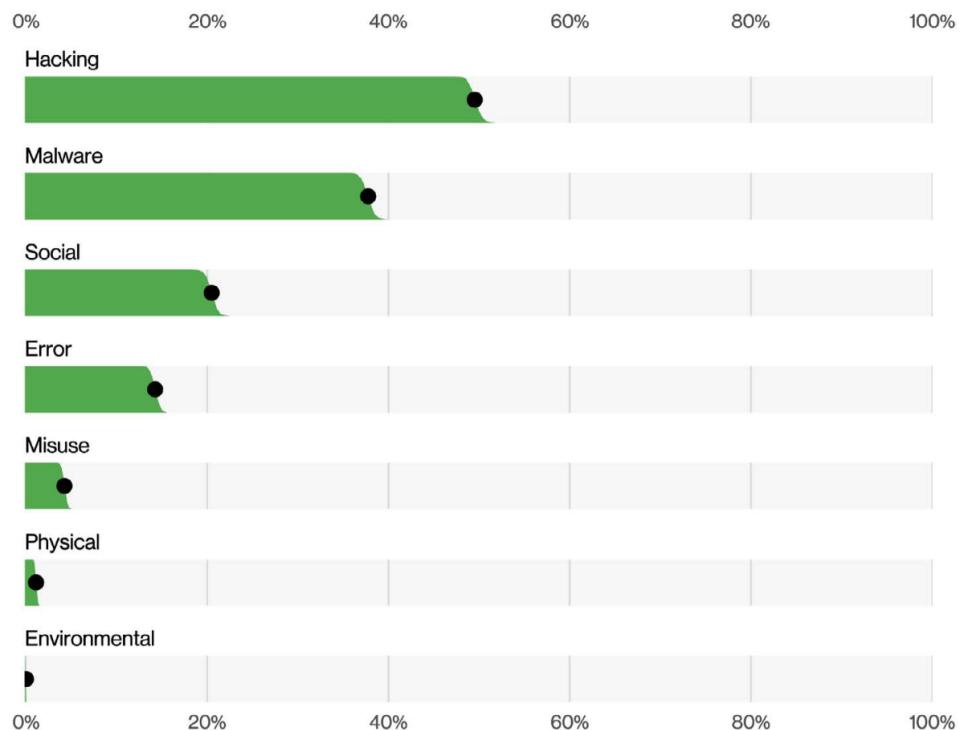
www.statista.com

Cyber Crime: un po' di dati (cont)

- Dati dell'Internet Crime Complaint Center (IC3), che fa parte del Federal Bureau of Investigation (FBI):



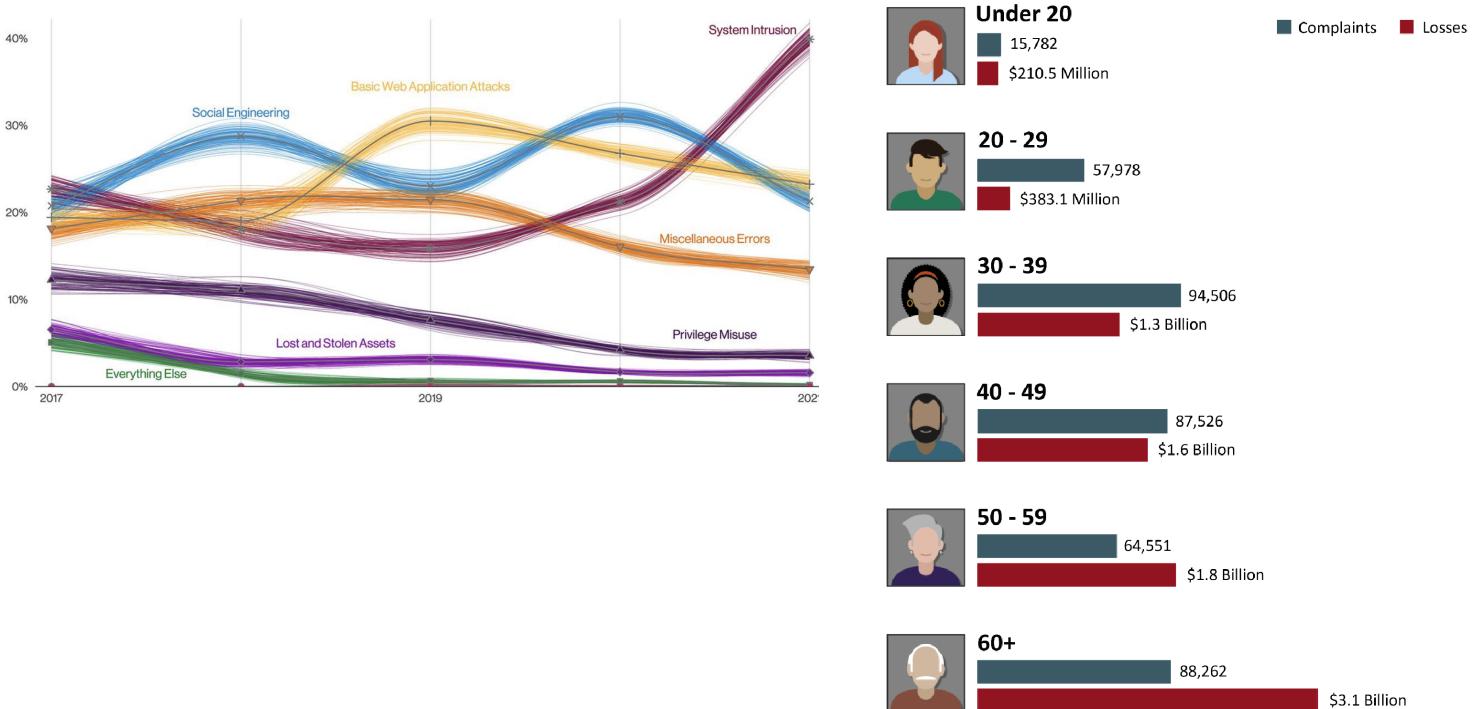
Principali azioni che hanno comportato un data breach (2008-2022)



<https://www.verizon.com/business/resources/T793/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>

Data breaches

2022 - VICTIMS BY AGE GROUP¹⁷

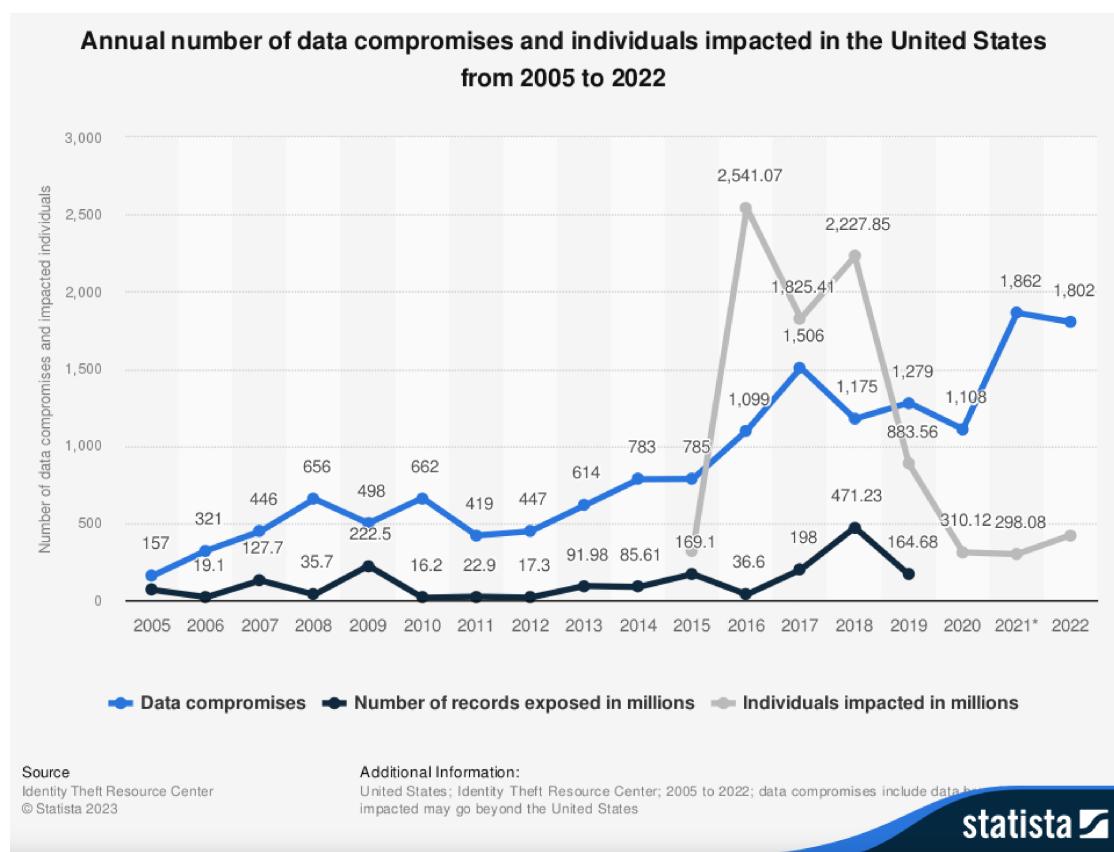


a.a. 2022/2023

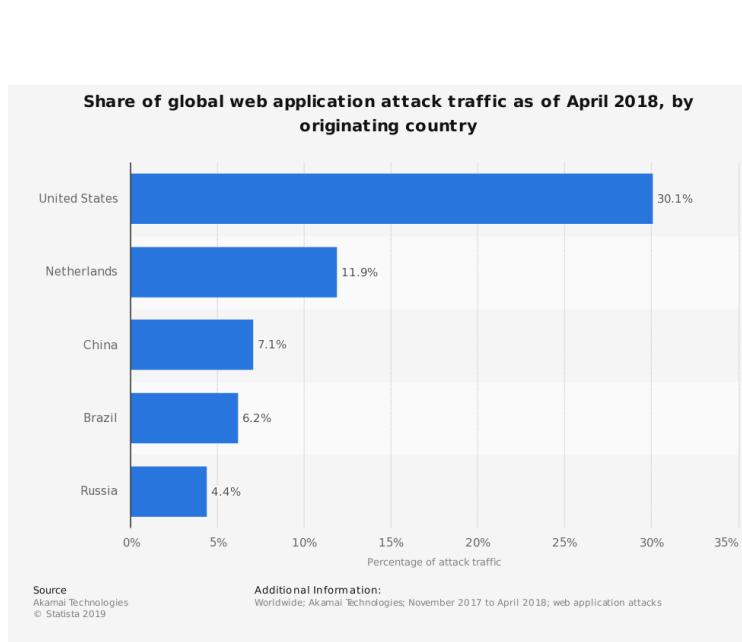
Digital Forensics

24

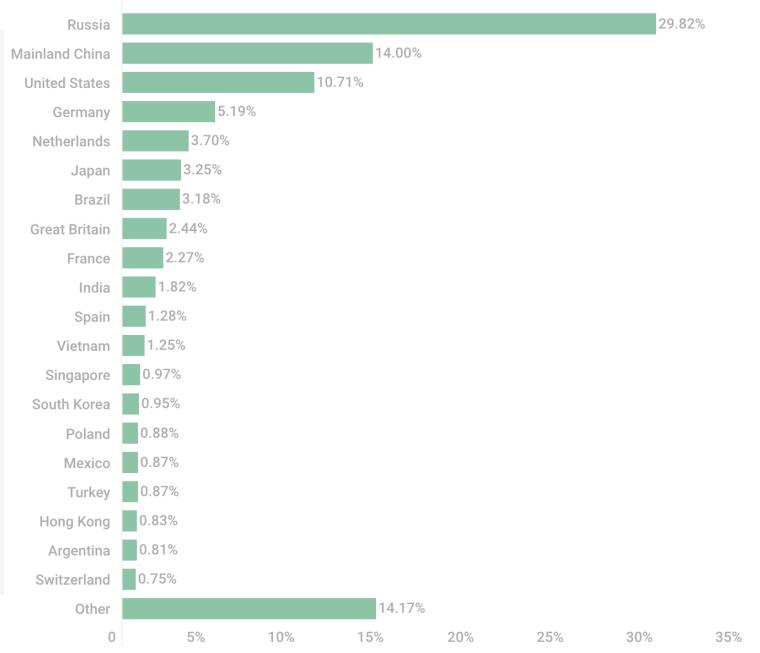
Andamento data breaches negli USA



Paesi di origine degli attacchi e spam



TOP 20 countries — sources of spam, 2022



kaspersky

Ingegneria sociale

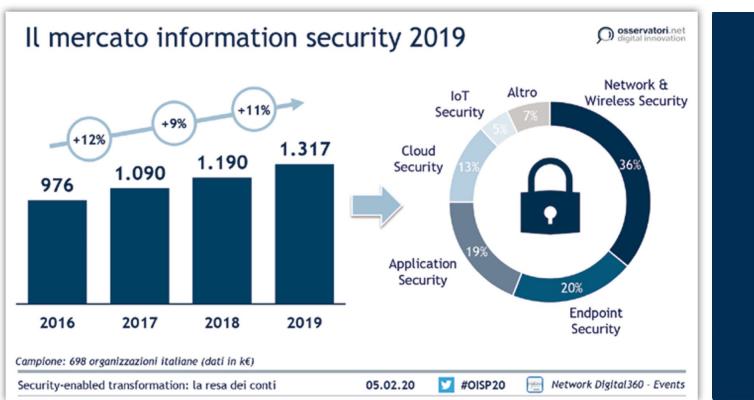
- Si affida alla natura umana, piuttosto che all'hacking tecnico, per **indurre con l'inganno le persone a compromettere la sicurezza personale o aziendale (hacking umano)**
- L'attaccante manipola le emozioni e gli impulsi delle vittime per indurle a compiere azioni contrarie ai loro interessi
- Può costituire il **primo stadio di un attacco più ampio**
 - ottenendo accesso a reti, dispositivi e account aziendali

Ingegneria sociale: le tattiche

- **Phishing**
 - fingersi ente o persona affidabile
 - il veicolo principale è l'e-mail, ma si sta diffondendo anche via SMS (smishing), whatsapp, FB messenger e per telefono (vishing)
- **Adescamento**
 - tramite beni o servizi desiderabili (regalo/vincita)
 - tipico esempio: truffa del principe nigeriano
 - anche musica o software gratuiti
 - programmi che promettono di sbloccare opzioni nei giochi (vittime spesso i ragazzi)
 - programmi crackati
 - unità USB abbandonate!
- **Scareware**
 - avviso dalle forze dell'ordine con accusa di un crimine (es. possesso di materiale pedopornografico)
 - avviso da parte del supporto tecnico di presenza di malware
 - minaccia di diffondere video compromettenti
- **Tailgating**
 - caso fisico: seguire una persona autorizzata attraverso una porta aperta
 - caso digitale: accedere ad un computer lasciato incustodito con account aperti

E in Italia?

- Il mercato della sicurezza informatica sta crescendo e nel 2021 ha raggiunto circa 1,55 miliardi di euro, secondo i dati 2022 dell'Osservatorio Information Security & Privacy, in parte come conseguenza dell'aumento della consapevolezza indotta dalla regolamentazione GDPR



- Secondo SANS (Sysadmin, Audit, Networking and Security), State of ICS Security Survey, il 42% delle minacce ai sistemi provengono dall'interno delle organizzazioni
 - Intenzionali o sabotaggi (10%)
 - Errori dovuti a scarsa competenza (15%)
 - Malfunzionamenti e/o scarsa integrazione con gli altri sistemi (10%)
 - Altro (7%)

Costo medio di un attacco in Italia



Italy	2020	2019
Average cost of a breach	\$3.19M	\$3.52M
Average time to identify & contain	268 days	283 days
Security automation deployed	56% of orgs.	49% of orgs.
Highest average cost industry	Financial	Financial
Cost of a Data Breach Report 2020	IBM Security	

SHARE OF PHISHING ATTACKS IN THE BANKING SECTOR IN ITALY IN 2019

33.7%

SHARE OF PHISHING ATTACKS IN THE E-COMMERCE SECTOR IN ITALY IN 2019

4.8%

SHARE OF PHISHING ATTACKS IN THE FINANCE SECTOR IN ITALY IN 2019

17.6%

Ogni violazione dei dati costa poco meno di **3 milioni di euro**, per riparare i sistemi, pagare le spese legali, ripristinare la produttività e il buon nome dell'azienda colpita. Il costo medio relativo al furto o alla perdita di **ogni singolo dato** è invece di **125 euro**



Have I Been Pwned?

- <https://haveibeenpwned.com>
- Consente di verificare se i propri dati sono stati violati



'--have i been pwned?'

Check if your email or phone is in a data breach

email or phone (international format)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords



Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



Exploit.in (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.in". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Compromised data: Email addresses, Passwords



Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames



LinkedIn Scrapped Data: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data



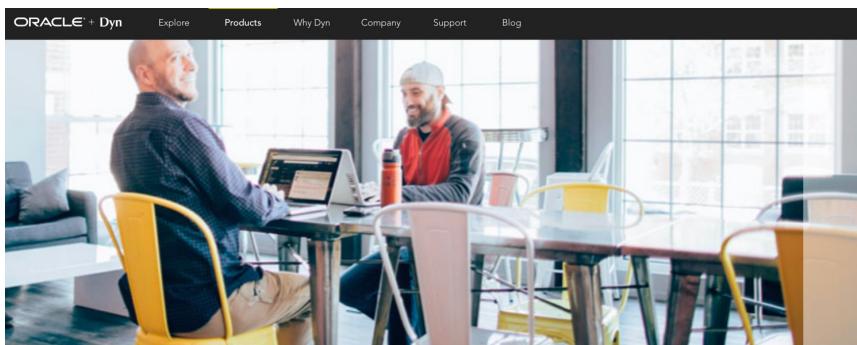
Phishing quiz

- Riusciamo a riconoscere le mail fraudolente?

<https://phishingquiz.withgoogle.com/>



Cyber Crime - 2 attacchi importanti: Dyn e Wanna Cry



ORACLE + Dyn Explore Products Why Dyn Company Support Blog SIGN IN CONTACT

The Dyn Difference

- Industry-leading DNS response times worldwide (<30ms)
- Industry-leading DNS propagation times (<30s)
- Hundreds of sensors collecting 240 billion data elements daily
- Highly resilient network with four tier-1 transit providers per PoP
- Battle-proven DDoS mitigated expertise built in at no extra cost
- Continuously improving geolocation accuracy
- Deep industry involvement and strong relationships throughout the DNS community

The unique value of DNS from Dyn



Consistent, high resiliency and performance Our diversified network allows us to offer world-renowned service—consistently and reliably.	Advanced DDoS attack process Our DDoS mitigation is battle-proven, and is built in at no extra cost.	Optimized transit connections at each POP Multiple tier 1 & 2 transit providers at each POP for redundancy and performance optimization.
DNS propagation time <1	Superior geolocation	Extreme industry expertise

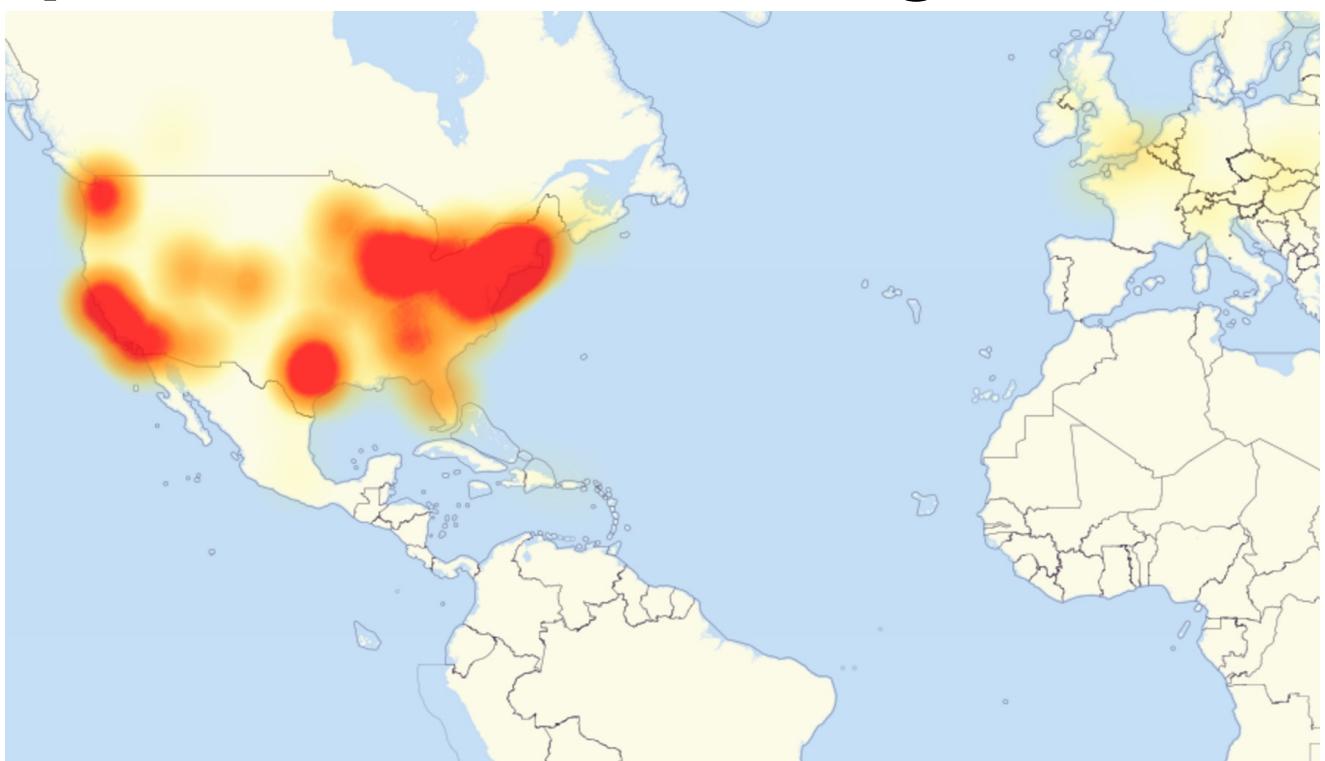
Clara Snowball, Christiana Oliver, Eric Dwinell
How can we help you? We're here for you!

Type your message...
We're  by Drift 

Cyber Crime: Dyn attack

- Dyn nasce nel 2001 a Manchester come società di tipo DNS Provider
 - Diventa Registrar nel 2004
 - Dal 2009 inizia ad acquisire grossi clienti, come Twitter, Netflix, Microsoft, Amazon, Time Warner, BBC, CNN, PayPal, ecc.
 - Dal 2010 al 2014 si lancia anche nei servizi Email, di monitoraggio e analisi dei dati
 - Nel 2016 viene acquistata da Oracle
- Il 21 ottobre 2016 il servizio di DNS viene attaccato per ben 3 volte
 - Attacco di tipo DDoS
 - Utilizzato il botnet Mirai
 - **Mirai** è un malware che trasforma i sistemi informatici in botnet controllabili da remoto, che possono essere utilizzate in attacchi informatici su larga scala
 - La maggior parte dei dispositivi utilizzati appartengono al mondo IoT (telecamere, DVR, router domestici, ecc.)
 - Impiegati nell'attacco oltre 100.000 device
 - Uno scan effettuato nel 2019 da una società americana (Flashpoint) ha riscontrato la presenza di oltre 550.000 device vulnerabili

Dyn attack: main outages



L'attacco non ha risparmiato grossi carrier e fornitori di servizi, come Level 3 (oggi CenturyLink-Lumen), Amazon, PlayStation Network, PayPal, Netflix, ecc.

Dyn attack: Mirai IoT password

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/kv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/kv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.formuse-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdpic	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcaadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root</none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.irongulls.com/2016/02/hack-and-patch-your-zte-f660-routers.html

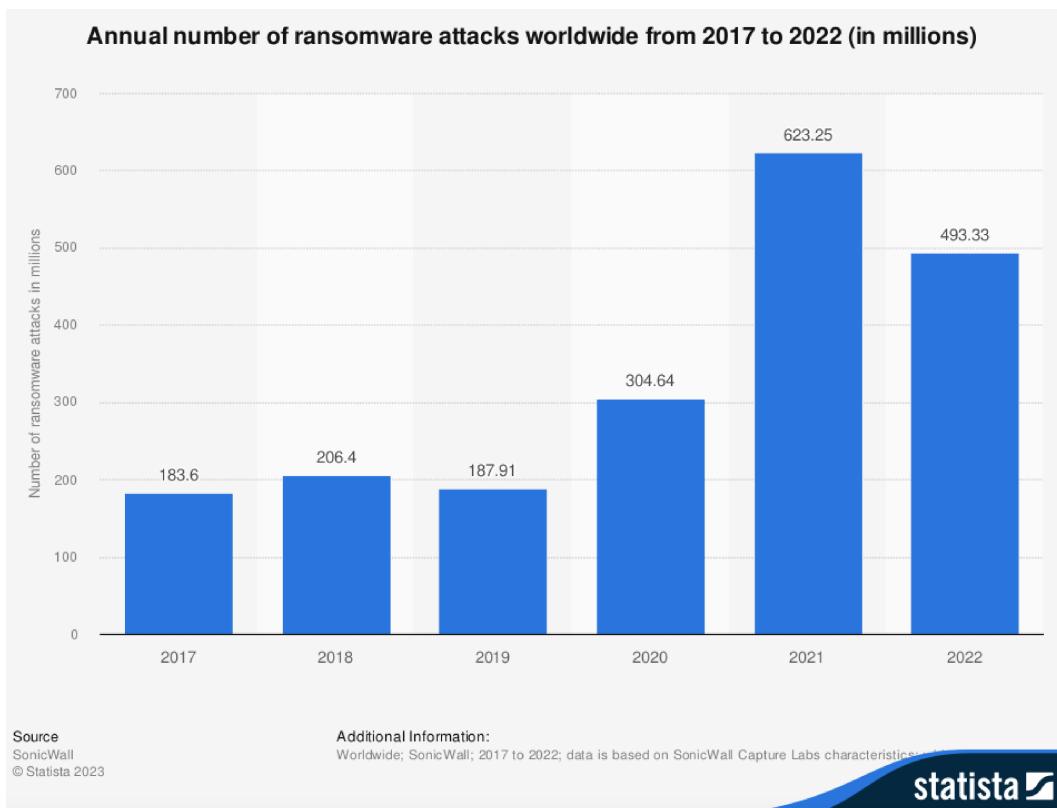
Cyber Crime: *Wanna Cry attack*

- **Ransomware Wanna Cry**
 - Classe di malware (MAlicious softWARE) che rendono inaccessibili, mediante cifratura, i dati dei computer infettati e dove viene chiesto il pagamento di un riscatto (ransom) per ripristinarli, tipicamente in bitcoin
 - Nati in Russia, si sono diffusi rapidamente in tutto il mondo (cryptolocker, la sua evoluzione cryptowall, ecc.)
 - Appartiene al settore della Cryptovirology, la crittografia applicata ai virus
 - la vittima vede i propri file cambiare estensione e icona e diventare inaccessibili
 - Possono individuare e crittografare anche file e backup accessibili in rete
- Attacco worldwide iniziato il 12 maggio 2017
 - Ha infettato oltre 230.000 computer e 150 Paesi
 - Target: sistemi Windows
 - Si è propagato usando **EternalBlue**, una vulnerabilità del protocollo SMB (Samba) appositamente creata dall'NSA e rivelata da un gruppo di hacker (gli Shadow Brokers) il 14 aprile 2017

Cyber Crime: Wanna Cry attack(*cont*)



Diffusione degli attacchi ransomware



a.a. 2022/2023

Digital Forensics

39

L'INVESTIGATORE DIGITALE

La figura dell'investigatore digitale o dell'informatico forense



- Quali sono le caratteristiche ideali dell'informatico forense?
- La valutazione è basata su 3 criteri:
 - Formazione
 - Competenze tecniche
 - Esperienza professionale

La figura dell'informatico forense: Formazione

- In Italia non era presente, fino a pochi anni fa, un percorso di studi specifico
- Materia assolutamente interdisciplinare
- Iter formativo suggerito:
 - Laurea in ingegneria informatica o in informatica (o anche altre equivalenti quali, ad es. matematica, fisica, ingegneria telecomunicazioni, elettronica, ecc.)
 - Laurea magistrale in cybersecurity, master, corsi specifici e/o di perfezionamento universitario
 - Formazione continua attraverso la partecipazione a convegni, seminari e eventi formativi
 - Formazione “on the job”

La figura dell'informatico forense: Competenze



La figura dell'informatico forense: Competenze (cont)

- Competenze tecniche e giuridiche
- Da un punto di vista tecnico:
 - Competenze trasversali in informatica
 - Sistemistiche
 - Programmazione
 - Networking
 - Sicurezza
 - device mobili, audio, video, IoT, ecc.
- Da un punto di vista giuridico:
 - Conoscenza di base del codice penale, civile, della Convenzione di Budapest del 2001 sulla criminalità informatica e della legge 48/2008 che la recepisce
 - Conoscenza del CAD, del D. Lgs 196/2003 e del Reg. 2016/679/UE (GDPR)
- Buona padronanza della lingua italiana (scritta e orale) e buona comprensione della lingua inglese (almeno livello B1 del CEFR - Common European Framework of Reference for Languages)

La figura dell'informatico forense: Esperienza e attività

- L'esperienza professionale cresce con il numero dei casi seguiti e la loro eterogeneità
- Principali attività e ambiti lavorativi:
 - Consulente Tecnico del PM o del Giudice;
 - Consulente Tecnico di parte dell'imputato/indagato, delle parti civili, delle parti offese
 - Ausiliario di PG durante l'attività di perquisizione e sequestro e/o successivamente ad essa
 - Esperto in cybersecurity
- Per i ruoli svolti per conto del PM o di un Giudice, presso i Tribunali sono istituiti gli albi dei Consulenti Tecnici (ambito civile) e dei Periti (ambito penale)
- Oltre all'ambito giudiziario, l'informatico forense svolge attività anche in ambito aziendale per prevenzione e/o gestione di incidenti informatici

Possibilità di avvalersi di consulenti tecnici

- **Art. 359 CPP - Consulenti tecnici del Pubblico Ministero**

1. Il Pubblico Ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di **consulenti**, che non possono rifiutare la loro opera
2. Il consulente può essere autorizzato dal Pubblico Ministero ad assistere a singoli atti di indagine

- **Art. 360 CPP - Accertamenti tecnici non ripetibili**

1. Quando gli **accertamenti** previsti dall'art. 359 riguardano persone, cose o luoghi, **il cui stato è soggetto a modificazione**, il PM avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici



Esempio di istanza per l'iscrizione all'albo dei Consulenti Tecnici di Ufficio (CTU)

https://www.giustizia.it/giustizia/it/mg_3_4_1.page

ISCRIZIONE ALL'ALBO DEI C.T.U.

DA PRESENTARE ALL'UFFICIO C.T.U. VIA LEPANTO, 4, ascensore 6, p. 3°
CANCELLERIE TEL. 06 32398433- 06 32398304 - DIRIGENTE 06/32398547

dal lunedì al venerdì ore 09-13

- 1) **domanda di iscrizione all'Albo redatta dall'aspirante C.T.U. in forma libera, in bollo da € 16,00** indirizzata al Presidente del Tribunale, con indicazione specifica delle materie richieste (non più di quattro; l'elenco delle materie è disponibile per la consultazione presso l'Ufficio C.T.U.);
- 2) **fotocopia del documento di identità personale aggiornato; (l'aspirante deve avere residenza, o il domicilio prof., e iscrizione Ordine nel circondario del Tribunale di Roma ;**
- 3) **fotocopia del codice fiscale e copia attestato di Laurea quinquennale.**
- 4) solo per i medici non specialisti: certificato di esami sostenuti e laurea (fotocopia);
- 5) autocertificazione su modello predisposto dall'Ufficio C.T.U. ai sensi degli artt. 1-2-3 legge 15 maggio 1999 n. 127, sulla base di documenti di identità personale aggiornato nei dati e non scaduto; (da ritirare e compilare, al momento della presentazione della domanda, davanti al funzionario). Chi non volesse avvalersi dell'autocertificazione dovrà presentare il certificato di nascita (in carta libera), certificato di residenza (in bollo) e certificato Ordine o Collegio Professionale (in bollo); Non verranno prese in considerazione le domande con un'anzianità di iscrizione all'Ordine o Collegio professionale inferiore ai 5 anni.
- 6) **curriculum professionale, corredato** da titoli e documenti dimostranti l'effettivo svolgimento dell'attività professionale e la speciale competenza tecnica in possesso dell'aspirante (in fotocopia) (es. fatture , contratti, collaborazioni, pubblicazioni ecc....);
- 7) attestazione comprovante l'avvenuto pagamento della tassa di concessione governativa di € 168,00 sul c/c postale n.8003, intestato a "Ufficio Registro Tasse di Roma, Concessioni Governative". (Usare gli appositi moduli reperibili presso gli Uffici Postali ed indicare sul retro la causale del versamento n. 8617). **Il versamento verrà effettuato immediatamente dopo l'avvenuta iscrizione all'Albo;**
- 8) solo per interpreti e traduttori: Titolo di studio in bollo (laurea o diploma Scuola Interp. e Tradutt.); per gli stranieri è necessario l'attestato scuola italiana (in bollo) e permesso di soggiorno.
- 9) se dipendente pubblico: autorizzazione allo svolgimento dell'attività di C.T.U. rilasciata dall'Amministrazione cui il dipendente appartiene (ex art. 53 d. lgs. 30.03.2001, n. 165)
- 10) In caso di iscrizione, a conclusione di tutto l'iter, il Consulente dovrà presentare un curriculum informatico secondo il modello fornito telematicamente da questo ufficio.

Il possesso del requisito della speciale competenza **sarà verificato** dalla Commissione competente che effettuerà la valutazione della documentazione esibita dall'interessato in base ai seguenti criteri:

- (a) dimostrata esecuzione di prestazioni professionali di particolare complessità;
- (b) pubblicazione di monografie su temi inerenti le materie per le quali si chiede l'iscrizione;
- (c) pubblicazione di saggi brevi, articoli, note, inerenti le materie per le quali si chiede l'iscrizione;
- (d) dimostrato svolgimento di attività professionale intensa e continua.

Entro 6 mesi dalla definizione dell'istanza di iscrizione dovranno essere ritirati tutti gli allegati di curricula prodotti, che saranno altrimenti smaltiti per inderogabili problemi logistici.
SI RICHIENDE SPECCHIATA MORALITA'
I tempi tecnici di istruzione delle istanze (richiesta di informative) sono di circa tre mesi.

La figura dell'informatico forense: Caratteristiche

- Professionalità
- Correttezza e trasparenza di rapporti con tutte le parti coinvolte in un caso
- Capacità di interloquire con le altre parti processuali
- Riservatezza dei dati e delle informazioni di cui si viene a conoscenza durante le fasi di analisi
- Aggiornamento continuo
- Applicazione di metodi scientifici, verificati e verificabili per l'analisi e l'interpretazione dei dati e utilizzo di tecniche e strumenti riconosciuti dalla comunità scientifica internazionale
- Capacità di gestire situazioni per le quali non sono state ancora definite metodologie e tecniche consolidate (acquisizione di dispositivi non tradizionali, dati su Internet/cloud, ecc.)

Cosa/Chi non è il consulente di informatica forense

- Elenco semiserio... ☺
 - “Ho la passione per i computer”
 - “Sono laureato in informatica, ma non so cosa sia una copia forense...”
 - “Non sono laureato in informatica, ma ho l’ECDL!”
 - “Conosco un giudice che abita nel mio quartiere e una volta gli ho sistemato il PC...”
 - “Faccio da una vita trascrizioni di audio forense”
 - “Sono un ottimo programmatore Python”
 - “Faccio siti web da una vita!”

REQUISITI PER LA GESTIONE DELL'EVIDENZA DIGITALE

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE

- **Rilevanza**: "Deve essere possibile dimostrare che il **materiale acquisito è rilevante** per l'inchiesta"
- **Sufficienza**: "Deve essere raccolto abbastanza materiale per consentire lo svolgimento di una corretta **indagine**"

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE (cont)

- **Verificabilità:** “Le attività svolte devono poter essere valutate da parte di una terza persona indipendente o da altre parti interessate autorizzate”
- **Giustificabilità:** “Le azioni e i metodi utilizzati per gestire le potenziali prove digitali devono poter essere tutte giustificare”

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE (cont)

- **Ripetibilità:** quando vengono prodotti i medesimi risultati di prova nelle seguenti condizioni:
 - Sono prodotti nello stesso luogo e dallo stesso operatore
 - Utilizzando la stessa procedura e metodo di misura
 - Utilizzando gli stessi strumenti e nelle stesse condizioni di utilizzo
 - Può essere ripetuto in qualsiasi momento dopo il test originale

Art. 359 c.p.p. e Art. 360 c.p.p.

- **Riproducibilità:** quando vengono prodotti i medesimi risultati di prova cambiando una o più condizioni di misura:
 - Luogo o operatore
 - Procedura o metodo di misura
 - Strumenti o condizioni di utilizzo
 - Può essere riprodotto in qualsiasi momento dopo il test originale



UNIVERSITÀ DI PISA

in collaborazione con

Master Universitario di I Livello in Cybersecurity

Digital Forensics

Arianna Del Soldato, Maurizio Martinelli

Istituto di Informatica e Telematica - CNR
Unità Tecnologica Innovazione Digitale

arianna.delsoldato@iit.cnr.it, maurizio.martinelli@iit.cnr.it



UNIVERSITÀ DI PISA

in collaborazione con

Master Universitario di I Livello in Cybersecurity

Digital Forensics

Arianna Del Soldato, Maurizio Martinelli

Istituto di Informatica e Telematica - CNR
Unità Tecnologica Innovazione Digitale

arianna.delsoldato@iit.cnr.it, maurizio.martinelli@iit.cnr.it



UNIVERSITÀ DI PISA

in collaborazione con

Master Universitario di I Livello in Cybersecurity

Digital Forensics

Arianna Del Soldato, Maurizio Martinelli

Istituto di Informatica e Telematica - CNR
Unità Tecnologica Innovazione Digitale

arianna.delsoldato@iit.cnr.it, maurizio.martinelli@iit.cnr.it

Sommario

- I requisiti per la gestione dell'evidenza digitale
- Le Best Practice
- Le fasi principali della Digital Forensics
 - Identificazione della prova
 - Analisi preliminare
 - Ricerca delle fonti e riconoscimento
 - Acquisizione e Conservazione
 - Acquisizione della prova
 - Intercettazione e Sequestro
 - Considerazioni sulla privacy
 -
 - Conservazione e Protezione

REQUISITI PER LA GESTIONE DELL'EVIDENZA DIGITALE

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE

- **Rilevanza**: "Deve essere possibile dimostrare che **il materiale acquisito è rilevante per l'inchiesta**"
- **Sufficienza**: "Deve essere raccolto **abbastanza materiale per consentire lo svolgimento di una corretta indagine**"

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE (cont)

- **Verificabilità:** “Le attività svolte devono poter essere valutate da parte di una terza persona indipendente o da altre parti interessate autorizzate”
- **Giustificabilità:** “Le azioni e i metodi utilizzati per gestire le potenziali prove digitali devono poter essere tutte giustificate”

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE (cont)

- **Ripetibilità:** quando vengono prodotti i medesimi risultati di prova nelle seguenti condizioni:
 - Sono prodotti nello stesso luogo e dallo stesso operatore
 - Utilizzando la stessa procedura e metodo di misura
 - Utilizzando gli stessi strumenti e nelle stesse condizioni di utilizzo
 - Può essere ripetuto in qualsiasi momento dopo il test originale

Art. 359 c.p.p. e Art. 360 c.p.p.

- **Riproducibilità:** quando vengono prodotti i medesimi risultati di prova cambiando una o più condizioni di misura:
 - Luogo o operatore
 - Procedura o metodo di misura
 - Strumenti o condizioni di utilizzo
 - Può essere riprodotto in qualsiasi momento dopo il test originale

LE BEST PRACTICE

Le Best practice

- Il **legislatore non specifica quali debbano essere le procedure** da seguire che consentono alla digital evidence di avere un valore probatorio
- Una **risposta** in tal senso è fornita dalle cosiddette "**Best practices**"
 - Linee guida, procedure e metodologie per approcciare la prova digitale nella maniera più corretta

Le Best practice

- **Protocolli sviluppati da agenzie di controllo** con riferimento al quadro normativo del singolo paese, Esempio:
 - Best Practices for Seizing Electronic Evidence – US Department of Homeland Security in collaborazione con United State Secret Service (<http://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf>)
 - Good Practice Guide for Digital Evidence - Association of Chief UK Police Officer (https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)
- **Protocolli elaborati da associazioni di categoria** che forniscono una certificazione sulle metodologie proposte e promuovono un codice di condotta condiviso:
 - DFA Digital Forensics Association
 - IISFA International Information System Computer Association IACIS International Association of Computer Investigative Specialists
- **Standard di matrice più propriamente tecnica**, sviluppati da organismi di standardizzazione nazionale che forniscono procedure tecniche indipendenti dal contesto normativo:
 - RFC 3227, IETF feb 2002 - Guidelines for Evidence Collection and Archiving
 - ISO/IEC 27037:2012, ISO/IEC 27041:2015, ISO/IEC 27042:2015, ISO/IEC 27043:2015, ISO/IEC 27050:2019

Le Best practice: RFC 3227 Guidelines for Evidence Collection and Archiving

- Fornisce le **procedure tecniche universalmente riconosciute** ed applicabili a prescindere del contesto normativo della singola nazione.
- Il documento è diviso in tre sezioni:
 1. Principi guida da seguire durante il reperimento/acquisizione dell'evidenza (cosa fare e non fare, considerazioni sulla privacy e legali)
 2. La procedura per l'acquisizione (trasparenza e riproducibilità della procedura)
 3. La procedura di archiviazione (catena di custodia, archiviazione, strumenti utilizzabili)

Le Best practice: norme ISO/IEC 27k

- Gli standard **ISO / IEC** (International Electrotechnical Commission) **27037, 27041, 27042, 27043 e 27050** promuovono i metodi e i processi di *best practice* per l'identificazione, la raccolta, l'acquisizione e la conservazione delle evidenze digitali
- **Scopo:** facilitarne lo scambio fra più Paesi utilizzando protocolli metodologici comuni
- Lo standard è **applicabile in qualsiasi ambito** (civile, penale, stragiudiziale), senza riferimenti a specifici ordinamenti o a norme giuridiche

Le Best practice: norme ISO/IEC 27k (cont)

- **ISO/IEC 27037 — Security techniques Guidelines for identification, collection, acquisition, and preservation of digital evidence**
 - Individua figure specifiche in funzione delle competenze e dei momenti di interazione con l'evidenza (**Digital Evidence First Responder, Digital Evidence Specialist, Incident Responder Specialist , Forensics Laboratory Manager**)
 - **SI OCCUPA:** documentazione, tracciabilità, priorità di intervento, imballaggio e trasporto dei reperti, catena di custodia,
 - **NON SI OCCUPA:** aspetti legali, analisi, strumenti tecnici, redazione dei report e presentazione

Le Best practice: norme ISO/IEC 27k (cont)

- **ISO/IEC 27042 — Guidelines for the analysis and interpretation of digital evidence**
 - Offre una guida sul processo di analisi ed interpretazione delle prove digitali
 - Fornisce indicazioni sui meccanismi per dimostrare le competenze del gruppo investigativo
- **ISO/IEC 27041 — Guidance on assuring suitability and adequacy of incident investigative methods**
 - Descrive i metodi attraverso i quali tutte le fasi del processo di indagine possono essere dimostrate appropriate (rispetto dei requisiti di credibilità, affidabilità e integrità)

Le Best practice: norme ISO/IEC 27k (cont)

- **ISO/IEC 27043 — Incident investigation principles and processes**
 - Fornisce le linee guida per i processi di indagine applicabili alle più comuni tipologie di indagine attraverso diversi scenari
- **ISO/IEC 27050 (4 parti)— Electronic discovery**
 - Fornisce una panoramica del processo che consente di scoprire le informazioni memorizzate elettronicamente (ESI) coinvolte in un'indagine o in un contenzioso
 - Delinea i requisiti e raccomandazioni sulle attività di identificazione, conservazione, raccolta, elaborazione, revisione, analisi e produzione di informazioni delle ESI

LE FASI PRINCIPALI DELLA DIGITAL FORENSICS

Digital Forensics: Fasi principali

- La Digital Forensics prevede le seguenti fasi:



Ciclo di vita della Digital Forensics



ANALISI PRELIMINARE



Analisi preliminare

- È il **processo investigativo** sempre necessario
- Viene svolta una **valutazione del caso** (perizia) al fine di **identificare il crimine** e **dove potrebbe essere localizzata la prova**
- Le **investigazioni** sono condotte su due **tipologie di sistemi**:
 - Quelli utilizzati **per commettere il crimine**
 - Quelli eventualmente **bersaglio del crimine**

Analisi preliminare (cont)

- Solitamente inizia con un **incontro preliminare con la Polizia Giudiziaria e/o il PM**
- Aiuta a **capire la natura e l'entità dell'indagine**
- **Definisce gli Obiettivi:**
 - Perseguire qualcuno?
 - Interrompere un rapporto di lavoro?
 - Scoprire come e perché è accaduto l'incidente a scopo preventivo futuro?
 - Cercare di recuperare delle risorse perse o rubate?
 - Una combinazione di una o più di queste cose

Esempi di quesiti



«**Esaminati gli atti del fascicolo processuale** e presa visione di tutto il materiale in sequestro, previa **esecuzione di una “bit-stream image”** degli hard disk e dei supporti informatici sequestrati all’indagato, in modo da **consentirne la ripetibilità di eventuali ulteriori accertamenti tecnici** e di **non pregiudicare la genuinità delle tracce informatiche**, analizzi il materiale informatico **anche ricercando file cancellati**; indichi il consulente la natura e il contenuto dello stesso **specificando il numero delle immagini o filmati pedopornografici eventualmente rinvenuti, effettuandone la stampa ovvero la duplicazione su supporto**. Accerti la condotta posta in essere, precisandone **le date, in particolare le modalità di accesso a sistemi informatici e/o telematici**, la frequenza degli accessi accertati, i collegamenti con altri soggetti, precisando i siti da cui ha effettuato il download. **Verifichi operazioni di invio file e tracce di invii verso altri utenti. Accerti gli elementi identificativi dell’utilizzatore»**

Esempi di quesiti (cont)

- «Proceda il CT ad estrarre **copia forense** del computer portatile sequestrato in data 24/1/2023 all'indagato “Paolino Paperino” e di **analizzarne il contenuto** con particolare riferimento ai **documenti ed alle comunicazioni attraverso Internet**»



Esempi di quesiti (cont)

- «Proceda il consulente all'analisi forense del materiale informatico sequestrato a “*Paolino Paperino*” ... e comunque **quant'altro rilevante ai fini di giustizia secondo le emergenze conseguenti all'analisi**»
- **Rilevante?**



Analisi preliminare: *Fasi principali*

- L'investigatore è interessato a **capiere l'entità dell'incidente**
- L'analisi è costituita da **4 fasi principali:**
 1. Definizione della **struttura organizzativa** dell'indagato
 2. Pianificazione e **allocazione delle risorse**
 3. Stesura del **contratto** di ingaggio
 4. Preparazione di una **lista di testimoni/sospetti**

Analisi preliminare:

1. Definizione della struttura organizzativa

- Comprende:

Le **relazioni tra le persone**

Il **sistema di sicurezza**

La **natura del business** / specificità della **persona**

I **sistemi ICT** in uso

I **numero di persone** coinvolte

La **complessità delle operazioni** all'interno dell'organizzazione

Le possibili **connessioni esterne**

Analisi preliminare:

2. Pianificazione e allocazione delle risorse

- Allocazione del **personale** e degli **strumenti necessari**:



Determinare il **numero** di **personale** da assegnare ai vari compiti



Assegnare **attrezzature** e strumenti adeguati



Individuare **gli esperti forensi** digitali



Determinare i **compensi** da destinare ad ogni squadra

Analisi preliminare:

3. Stesura del contratto di ingaggio

- Stabilisce un **compenso** sulla base del servizio offerto
- Implica un **accordo su:**
 - L'**obiettivo** della richiesta
 - Le **tempistiche** e la **remunerazione**
 - La persona o l'**autorità** a cui far **riferimento**
 - La **revisione della relazione** prima della stesura del report finale
 - Eventuali **costi aggiuntivi** relativi ad ulteriori richieste o eventuali indagini aggiuntive
- Non deve mai garantire risultati specifici



Analisi preliminare:

4. *Preparazione di una lista di testimoni*

- La **lista** deve essere **in parte fornita dal cliente e in parte individuata dall'esperto forense stesso**



RICERCA DELLE FONTI DI PROVA E RICONOSCIMENTO



Ricerca delle fonti di prova e Riconoscimento

- Deve essere **identificata la fonte di prova** tra un insieme di fonti informative potenzialmente utili
- È fondamentale **individuare tutto quello che può essere utile**
- È di primaria importanza in vista della **cristallizzazione**

Ricerca delle fonti di prova: *Elementi in grado di memorizzare dati*

- Non esistono **strumenti per l'identificazione di queste fonti di prova**
- Sta **nell'esperienza e meticolosità dell'investigatore** far emergere le casistiche

Elementi in grado di memorizzare dati: *Supporti magnetici e ottici*



Elementi in grado di memorizzare dati: Altri dispositivi



Elementi in grado di memorizzare dati: *Altri dispositivi (cont)*



Elementi in grado di memorizzare dati: *Altri dispositivi (cont)*



Elementi in grado di memorizzare dati: *Altre fonti*



Elementi in grado di memorizzare dati: ... e non sono sempre facili da individuare



Riconoscimento della prova: *Dove cercare?*

- Devo prendere in considerazione i **diversi elementi** che concorrono al funzionamento del **Sistema Informatico**:
 1. Tipologia del **Sistema Informatico**
 2. Tipologia del **Sistema Operativo**
 3. Tipologia del **file system**
 4. Tipologia di **file**
 5. Presenza e **tipologia di interfacce**

Dove cercare?

1. Tipologia del Sistema Informatico

- Due categorie di utilizzo, **due approcci:**
 - a. **Destinati agli utenti per attività ludica o lavorativa** 
 - Non contengono servizi critici
 - È consentito lo spegnimento, l'estrazione del disco e la cristallizzazione dell'intero supporto
 - b. **Destinati all'erogazione di servizi critici o a supporto del business o dell'infrastruttura informatica** 
 - Lo spegnimento non è effettuabile
 - La duplicazione potrebbe essere gravosa => acquisisco solo i dati che potrebbero essere fonte di prova a sistema acceso

Dove cercare?

2. Tipologia del Sistema Operativo

- È il cuore del Sistema Informatico e determina il tipo e il formato di file gestiti. Permette di:
 - Identificare le **zone di memoria** dove cercare i dati
 - Tracciare l'uso del computer da parte dei **diversi utenti** ivi definiti
 - Le **periferiche** che sono state collegate
 - Individuare l'elenco dei **file stampati** e su quale stampante
 - Identificare le **reti** (tradizionali o Wi-Fi) cui il computer è stato collegato
 - Ecc.

Dove cercare?

3. **File System**

- Determina **come sono organizzati i dati e li ospita**
- Alcuni tipi:
 - ISO 9660 / JOILET / CDFS (supporti ottici come i CD-ROM)
 - UDF (DVD)
 - FAT 16/32 (MP3 Player, USB, vecchi SO Microsoft, telecamere digitali)
 - NTFS (Microsoft NT, 2000/2003, XP, 10, ecc.)
 - EXT / ReiseFS (UNIX, Linux)
 - HFS+ (Mac OS)
 - QNX (Sistemi embedded)

Dove cercare?

4. Tipologie di file

- Esistono diverse tipologie di file che possono essere utili ai fini forensi:
 - **Documenti** – realizzati ed utilizzati dagli utenti (file multimediali, immagini, documenti office)
 - **File di configurazione** – memorizzazione delle impostazioni degli utenti, configurazioni di sistema
 - **File di log** – utilizzati per salvare le informazioni generate da applicazioni attive sul sistema
 - **File a supporto del SO** – utilizzati dal SO per svolgere le proprie attività
 - **Eseguibili e librerie** – possono essere avviati da SO (es: file .dll nel mondo Windows)
 - **File cifrati** – documenti cifrati successivamente mediante altri programmi o da funzionalità intrinseche dell'applicazione associata al documento

Dove cercare?

Altre fonti di dati

- **Area di swap** del SO
- **Memory Dump**: indicazioni delle informazioni elaborate dal sistema
- **Hibernation file di Windows (hiberfil.sys)**: conserva copia dei dati al momento della sospensione
- **Registri di Windows**: configurazione dei programmi installati
- **Slack Space e settori non utilizzati**: possono contenere dati utili non ancora sovrascritti

ACQUISIZIONE DEL DATO DAL SISTEMA



Acquisizione del dato dal sistema

- **Attività delicata** dal punto di vista della ripetibilità/irripetibilità delle attività
- L'approccio al sistema dipende dalla **tipologia di dispositivo** e/o sua **localizzazione**:
 - **Intercettazione**, se il dato viene trasferito tra sistemi
 - **Sequestro del dispositivo o duplicazione forense** del dato, se il dato è all'interno del sistema
 - **Acquisizione parziale** del dato, se il sistema contiene troppi dati, solo alcuni casi sono rilevanti, solo alcuni dati possono essere acquisiti per vincoli legali
- L'approccio dipende anche dallo **stato in cui viene ritrovato il sistema**
 - Sistema **spento** (**Post Mortem Forensics**)
 - Sistema **acceso** (**Live Forensics**)

Acquisizione del dato: **Intercettazione**

- **Generalmente vietata** e necessita di **apposite "coperture giuridiche"**
 - **Tutela della riservatezza** dei dati personali
- Vengono **utilizzate delle sonde**
 - in grado di **memorizzare le comunicazioni** che avvengono **col** il sistema sospetto
 - collegate a specifici punti della rete ed **interfacciate con diversi tipi di canali di comunicazione**
 - LAN, rete wireless, WAN, modem ADSL/isdn, ponte radio, ecc.
 - Le **tecniche di intercettazione** sono **strettamente legate al mezzo utilizzato per la comunicazione**
- Vengono installati **Captatori Informatici /Spyware**
 - consentono il **controllo delle apparecchiature da remoto**

Acquisizione del dato: **Sequestro**

- È una attività di Polizia Giudiziaria
- Il consulente tecnico deve supportare per superare le difficoltà tecniche e per la realizzazione della catena di custodia
- Le fasi successive devono essere svolte operando su una “copia forense” del reperto sequestrato

Acquisizione del dato: *Considerazioni sulla privacy*

- Le Best Practices sull'acquisizione e l'archiviazione dell'evidenza includono anche delle considerazioni sulla privacy:
 - **Rispettare le regole e le linee guida sulla privacy** e della giurisdizione di competenza
 - **Non intromettersi nella privacy delle persone** almeno che non ci siano forti giustificazioni
 - Quando si intraprendono le azioni per raccogliere la prova di un incidente, assicurarsi di verificare le eventuali procedure “interne”



UNIVERSITÀ DI PISA

in collaborazione con

Master Universitario di I Livello in Cybersecurity

Digital Forensics

Arianna Del Soldato, Maurizio Martinelli

Istituto di Informatica e Telematica - CNR
Unità Tecnologica Innovazione Digitale

arianna.delsoldato@iit.cnr.it, maurizio.martinelli@iit.cnr.it

Sommario

- Le fasi principali della Digital Forensics
 - Acquisizione e Conservazione
 - Acquisizione della prova
 - Intercettazione e Sequestro
 - Considerazioni sulla privacy
 - Live e post-mortem
 - Copia forense
 - Funzioni di hash
 - Conservazione e Protezione
 - Analisi e Valutazione
 - Catena di custodia
 - Redazione dei verbali
- Analisi forense di sistemi di file sharing
- Demo CAINE

Acquisizione del dato: Considerazioni sulla privacy

- Le **Best Practices** sull'acquisizione e l'archiviazione dell'evidenza **includono** anche delle **considerazioni sulla privacy**:
 - **Rispettare le regole e le linee guida sulla privacy** e della giurisdizione di competenza
 - **Non intromettersi nella privacy delle persone** almeno che non ci siano forti giustificazioni
 - Quando si intraprendono le azioni per raccogliere la prova di un incidente, assicurarsi di **verificare le eventuali procedure “interne”**

Acquisizione del dato: *Attività live e post mortem*

- Quando ci si trova davanti a un computer, nel caso in cui questo sia acceso si deve effettuare una scelta:
 - Esaminarlo mentre è **in esecuzione**
 - Analisi **live**
 - **Spegnerlo subito** per effettuare una copia forense
 - Analisi **post-mortem**
- La scelta dipende da vari fattori:
 - Competenza e/o conoscenza dello specifico sistema
 - Strumenti disponibili
 - Rilevanza dei dati rispetto all'indagine

NO LIVE
↑

Acquisizione del dato e priorità

- **Valore della sorgente** del dato in campo probatorio
 - prima quelle che potrebbero contenere **dati più importanti** poi le altre
- **L'ordine di volatilità** del dato (secondo RFC 3227 o la più recente ISO/IEC 27037) è:
 - 1. cache
 - 2. tabelle di routing, arp cache, process table, kernel statistics, memory
 - 3. file system temporanei
 - 4. dischi
 - 5. file di log remoti e dati di monitoraggio rilevanti per il sistema
 - 6. configurazioni, topologia della rete
 - 7. archivio dei media

Locali

Remoti

Acquisizione del dato: *Live Forensics*

- Un **intervento di live forensics** si rende comunque **necessario** quando:
 - Il **sistema non è fisicamente rimovibile** e/o **non può essere spento**
 - Sistemi militari
 - Videosorveglianza
 - Strumenti medicali
 - Servizi/sistemi/database condivisi
 - Server in hosting
 - Ecc.
 - Le **informazioni “volatili”** possono risultare **rilevanti per le indagini:**
 - chat/download in corso, informazioni nella memoria, nei cookies, cache, routing table, arp cache, process table, temporary file systems, remote logging, ecc.
 - Siamo in presenza di **volumi/partizioni/file cifrati** (FileVault, BitLocker, TrueCrypt, ecc.)

Acquisizione del dato: Live Forensics (cont)

- Le tecniche di “live forensics” hanno come contro:
 - Il sistema viene alterato
 - Le modifiche apportate sono note?
 - Le modifiche apportate sono documentabili?
 - Le modifiche apportate intaccano significativamente il risultato dell’analisi?
 - Ogni modifica apportata può distruggere altri dati significativi
 - Gli accertamenti svolti su sistemi “accesi” non saranno ripetibili

Acquisizione del dato: Live Forensics (cont)

- Stand-by o acceso:
 - Accessibile:
 - Accedo con login o senza
 - Verifico la presenza di processi attivi e dischi cifrati "montati"
 - Estraggo i dati dal disco prima che venga spento
 - Acquisisco dati relativi allo stato del sistema e degli utenti mentre le attività sono in corso
 - Posso fare *memory dump* per salvare le info contenute in memoria
 - NON accessibile:
 - Utilizzare tecniche di «hacking» per ottenere l'accesso
 - Se possibile, spegnere il sistema rimuovendo la fonte di alimentazione elettrica da parte del dispositivo → Freeze del Sistema

Acquisizione del dato: *Post Mortem*

- **Mettere in sicurezza** la scena
- **Allontanare** le persone presenti **dai dispositivi digitali**
- **Fotografare** o fare una ripresa video della **scena del crimine**
- **Assicurarsi** che il computer sia **effettivamente spento**
- **NON ACCENDERE IL COMPUTER PER NESSUN MOTIVO!!**

Acquisizione del dato: *Post Mortem* (cont)

- **Rimuovere** la batteria
- **Scollegare** l'alimentazione
- **Etichettare** le porte e i cavi
- Assicurarsi che tutte gli **oggetti** siano stati **sigillati e siglati**
- Identificare eventuali **indicazioni del modello** e del **numero di serie** presenti
- **Compilare un report** di sequestro per ogni oggetto
- **Prendere nota dettagliata di tutte le operazioni compiute** in relazione ai dispositivi informatici

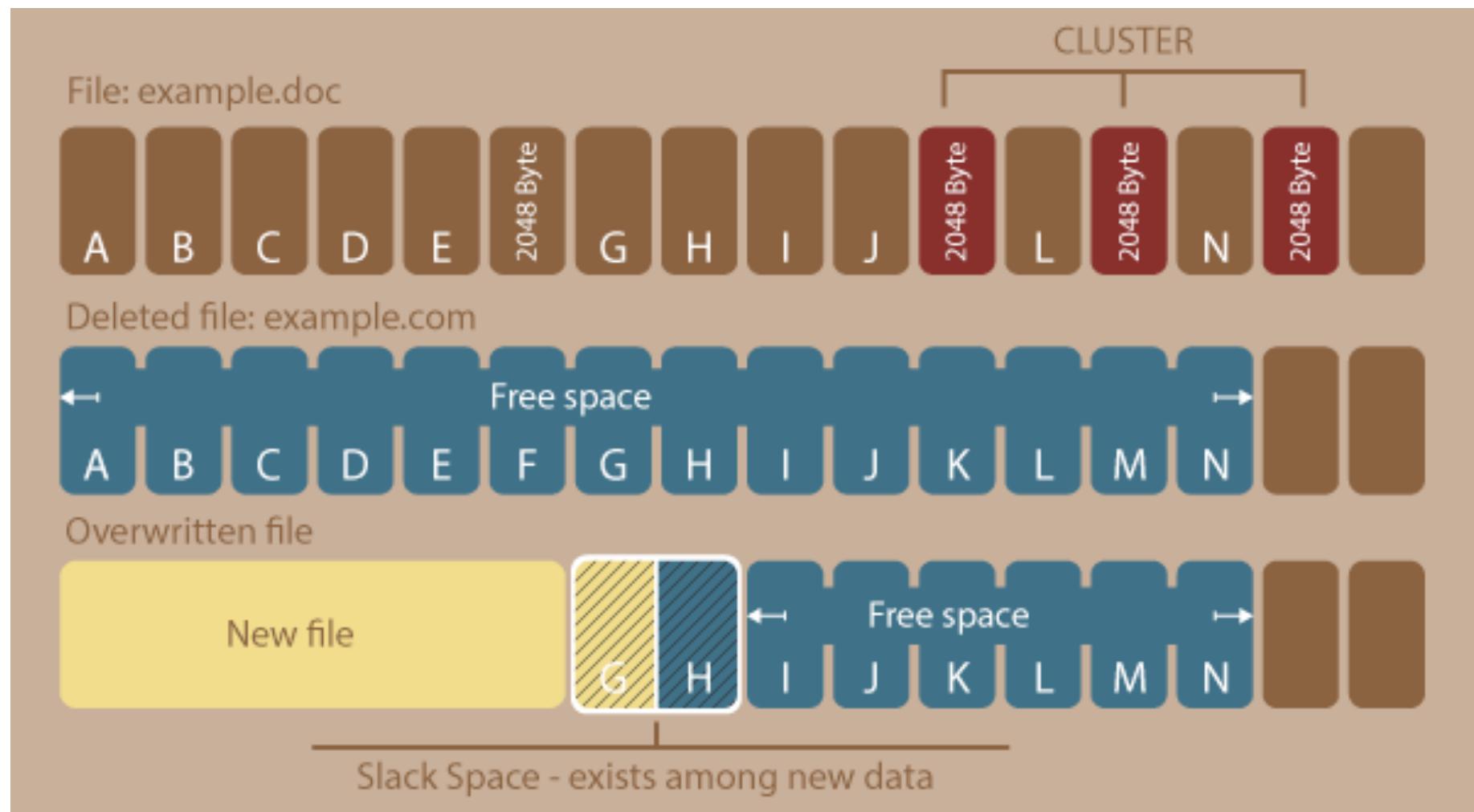
Acquisizione del dato: *Attività live e post mortem*



Acquisizione del dato: Copia forense

- Dopo aver svolto la perizia, l'investigatore deve procedere all'acquisizione dei dati che costituiscono la prova
- Regola fondamentale: **preservare l'originale!**
 - Devono essere estratti solo i dati effettivamente rilevanti
 - L'originale **non deve mai essere utilizzato** per l'analisi dei dati
 - Per effettuare l'acquisizione dei dati, è necessario (ove possibile) effettuare una copia a basso livello del supporto originale (bit-stream image)
 - Operazione diversa dalla semplice copia o backup dei dati che tralascia i file cancellati, lo slack space, lo spazio non allocato, ecc.
 - Necessità di prevenire qualsiasi scrittura sul supporto originale
 - Uso di software tool, come DD (Data Duplicator), EnCase (commerciale), ProDiscover Forensics (commerciale), TSURUGI Linux, CAINE, ecc.
 - dd if=/dev/hda6 of=/mnt/sda4/mystery.img bs=4096
 - Uso di Duplicatori HDD e/o dispositivi di Write Blocker

Slack space



Copia Forense

Duplicatori e Write Blocker



Acquisizione del dato: Buone norme

- Pulizia del supporto utilizzato per la copia (data wiping)
- Validazione della copia e verifica di integrità (hashing)
- Aspetti temporali
 - **Timestamp**: data nella quale è stata effettuata l'operazione
 - **Timeline**: sequenza con cui le singole azioni, di cui si è trovata traccia, si sono verificate
 - **Scostamento temporale** con gli orologi informatici (ora attuale, ora del BIOS, ora del SO)
 - **Time server**: presenza di configurazioni che facciano riferimento alla sincronizzazione con i Time Server
 - Differenze di unità di misura nei vari componenti e di zona oraria

Verifica dell'integrità della copia

- Come posso verificare la conformità e la successiva integrità della copia?
- Usando funzioni di hash!

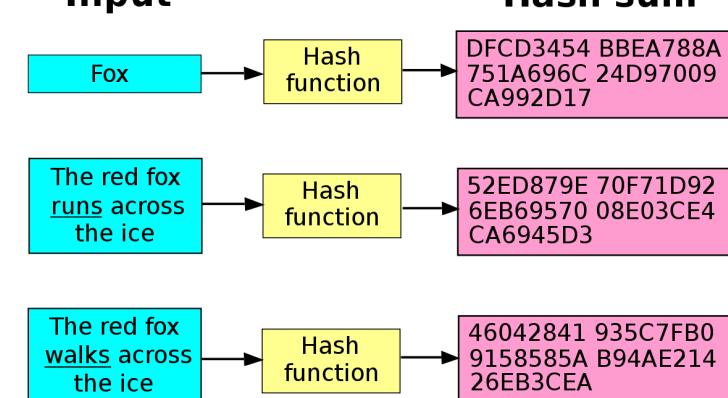
Funzioni di hash

- Una funzione crittografica di hash **trasforma** dei **dati di lunghezza arbitraria** (una sequenza di bit) in una **stringa di dimensione fissa** chiamata **valore di hash** o **checksum**
- I checksum vengono usati spesso sulla rete per garantire che i dati scaricati siano corretti e autentici
 - I distributori di sw open-source spesso pubblicano anche il suo digest, che può essere utilizzato dall'utente per verificare l'integrità dei dati
- Algoritmi **unidirezionali** e non invertibili
- Utilizzati in applicazioni quali:
 - **Firma digitale**
 - **Autenticazione** tramite algoritmi TSIG (Transaction SIGnature)
 - **Verifica delle password** degli utenti
 - Identificazione di file in applicazioni che hanno la necessità di gestire grandi quantitativi di dati e file come le reti peer-to-peer
 - Ecc...

Funzioni di hash (cont)

- Una funzione di hash deve avere le seguenti proprietà fondamentali:
 - Deve essere semplice da calcolare su qualsiasi tipo di dato
 - Deve essere deterministica, nel senso che per uno stesso «messaggio» deve essere generato sempre lo stesso digest;
 - Deve essere estremamente difficile (o infinitamente oneroso in termini di calcolo) risalire al dato originario
 - Qualsiasi piccola variazione nel dato originario si deve tradurre in una grande variazione del risultato
 - Deve essere estremamente improbabile che due dati, anche se simili, restituiscano il medesimo risultato (**collisioni**)
 - Minore è la probabilità di collisioni e migliore è la qualità dell'algoritmo di hash e quindi la sicurezza nell'integrità dei dati

- Le funzioni di hash più diffuse e utilizzate sono:
 - MD5 (128 bit)
 - SHA-1 (160 bit)
 - SHA-256 (256 bit)
 - SHA-512 (512 bit)



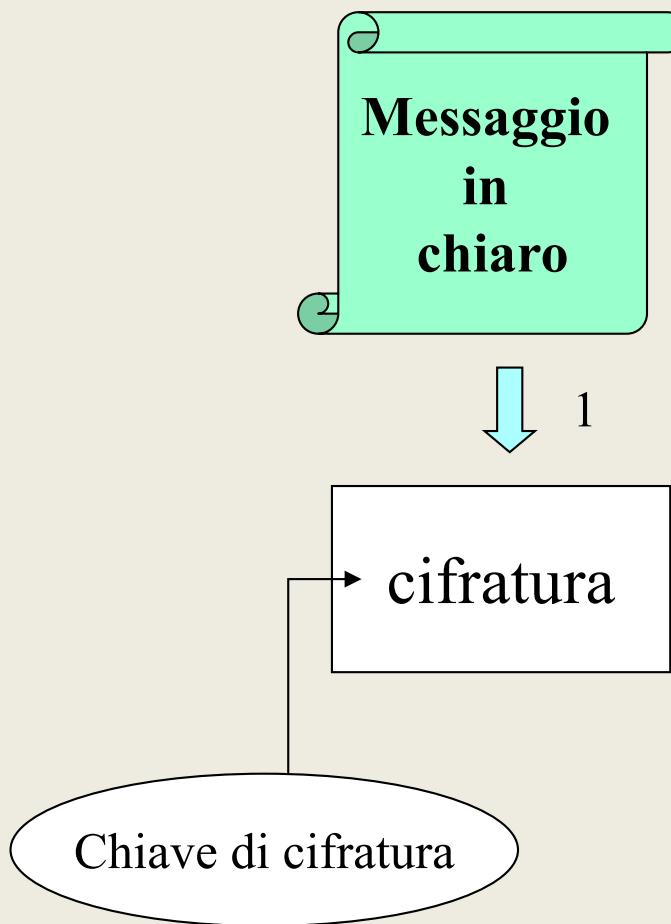
- Gli strumenti di acquisizione (hardware o software) calcolano l'hash del supporto originale e dell'immagine ottenuta, per verificare la correttezza del processo di copia

Alcuni concetti di crittografia

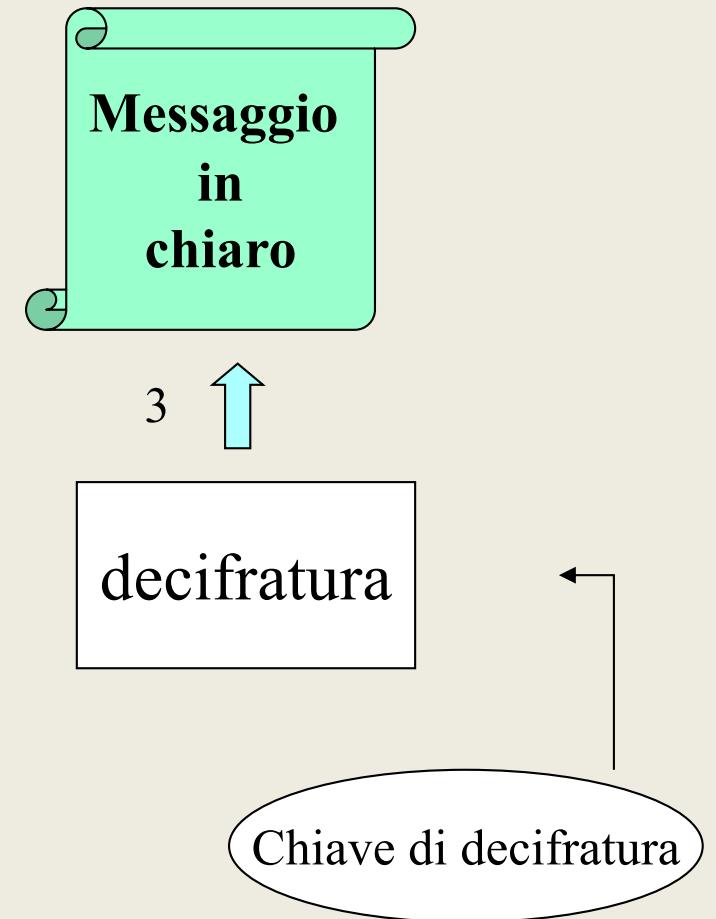
- **Cifratura:** trasformazione di un **testo in chiaro** in un **testo cifrato**
- **Decifratura:** trasformazione di un **testo cifrato** in un **testo in chiaro**
- **Trasformazione basata** in genere su:
 - **chiave**
 - **algoritmo** (procedimento preciso e ben definito)
- Nella **crittografia moderna** l'**algoritmo è pubblico**
- **La sicurezza si basa su:**
 - **segretezza della chiave**
 - **robustezza dell'algoritmo**

Cifratura e decifratura

Mittente



Destinatario



Cosa garantisce la crittografia

- la **riservatezza** del contenuto (analogamente alla busta in un sistema postale convenzionale)
- l'**integrità** del contenuto del documento trasmesso
- l'effettiva provenienza da colui che si dichiara mittente (**autenticità**)
- il **non ripudio**: chi trasmette non può negare di avere spedito il messaggio

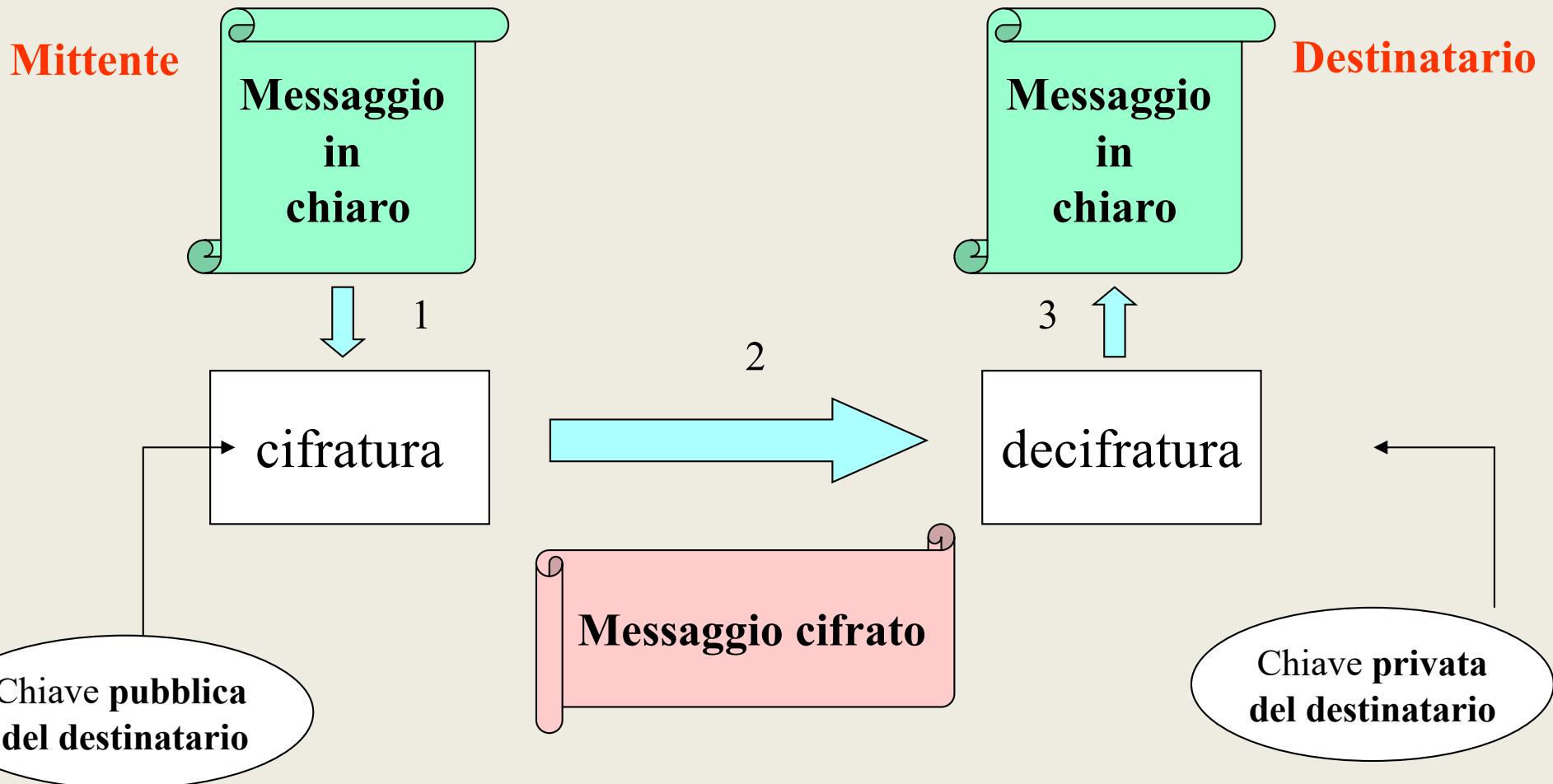
Algoritmi a chiavi simmetriche

- Chiave di cifratura e chiave di decifratura uguali
- Riservatezza, integrità, autenticità garantite dalla segretezza della chiave
- *Vantaggi:*
 - Gli algoritmi più diffusi (DES, 3DES, AES) impiegano chiavi di 32-512 bit e sono molto veloci
 - AES 128 è ritenuto sufficiente a proteggere informazioni governative classificate fino al livello “secret”, mentre le informazioni cosiddette “top secret” richiedono chiavi con lunghezza pari a 192 o 256 bit (AES-192 e AES-256)
- *Svantaggi:*
 - Scambiarsi la chiave segreta col destinatario in modo sicuro risulta spesso non agevole
 - Per una comunità di n utenti sono necessarie $2n$ chiavi
- Esempi di applicazioni che utilizzano algoritmi a chiavi simmetriche (**TSIG**):
 - NSUPDATE
 - Autenticazione tra nameserver
 -

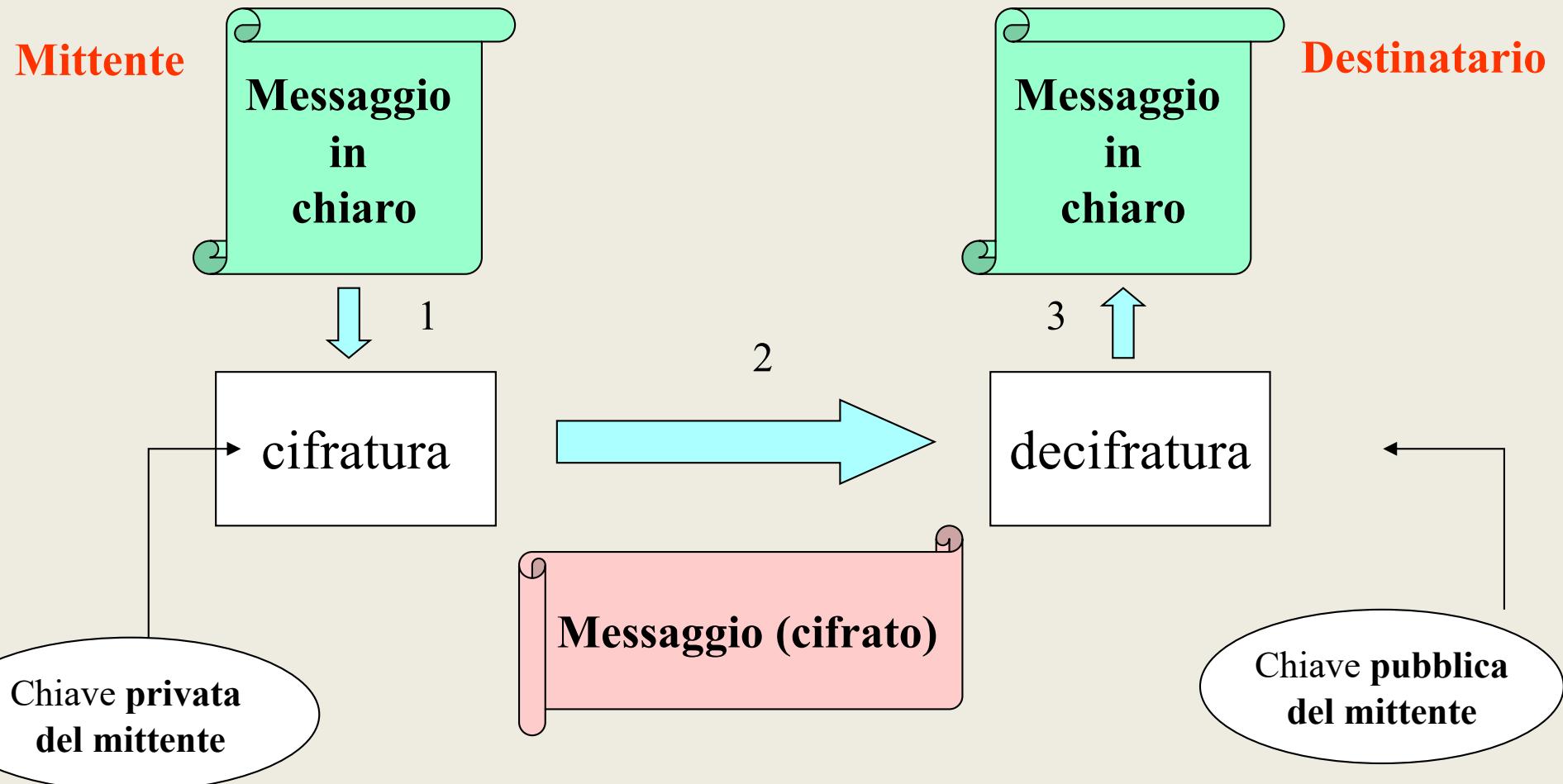
Algoritmi a chiavi asimmetriche

- Chiave di cifratura diversa da chiave di decifratura
- Ogni soggetto dispone una coppia di chiavi
 - Chiave privata: segreto da custodire
 - Chiave pubblica: informazione da diffondere
- *Vantaggi:*
 - Flessibilità: Riservatezza, integrità, autenticità garantite da un uso opportuno della coppia di chiavi
- *Algoritmi più diffusi:*
 - RSA e DSA che utilizzano chiavi di 1024-2048-4096 bit
 - Elliptic Curve Cryptography (ECCDSA, ECC-GOST,)
- Esempi di applicazioni che utilizzano algoritmi a chiavi asimmetriche:
 - PGP (OpenPGP)
 - SSH (per autenticazione basata su chiavi)
 - DNSSEC
 -

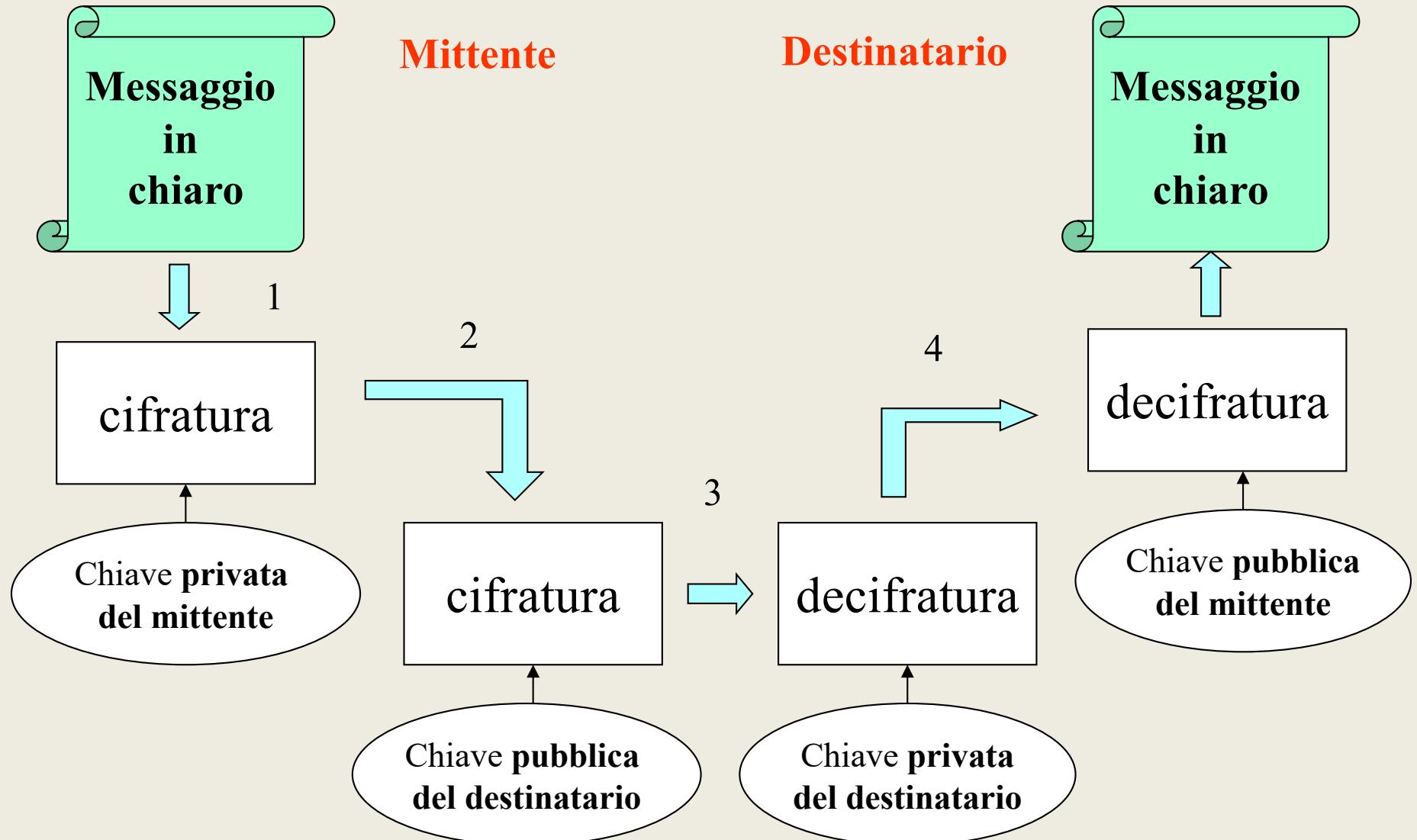
Riservatezza di un messaggio



Autenticità e integrità

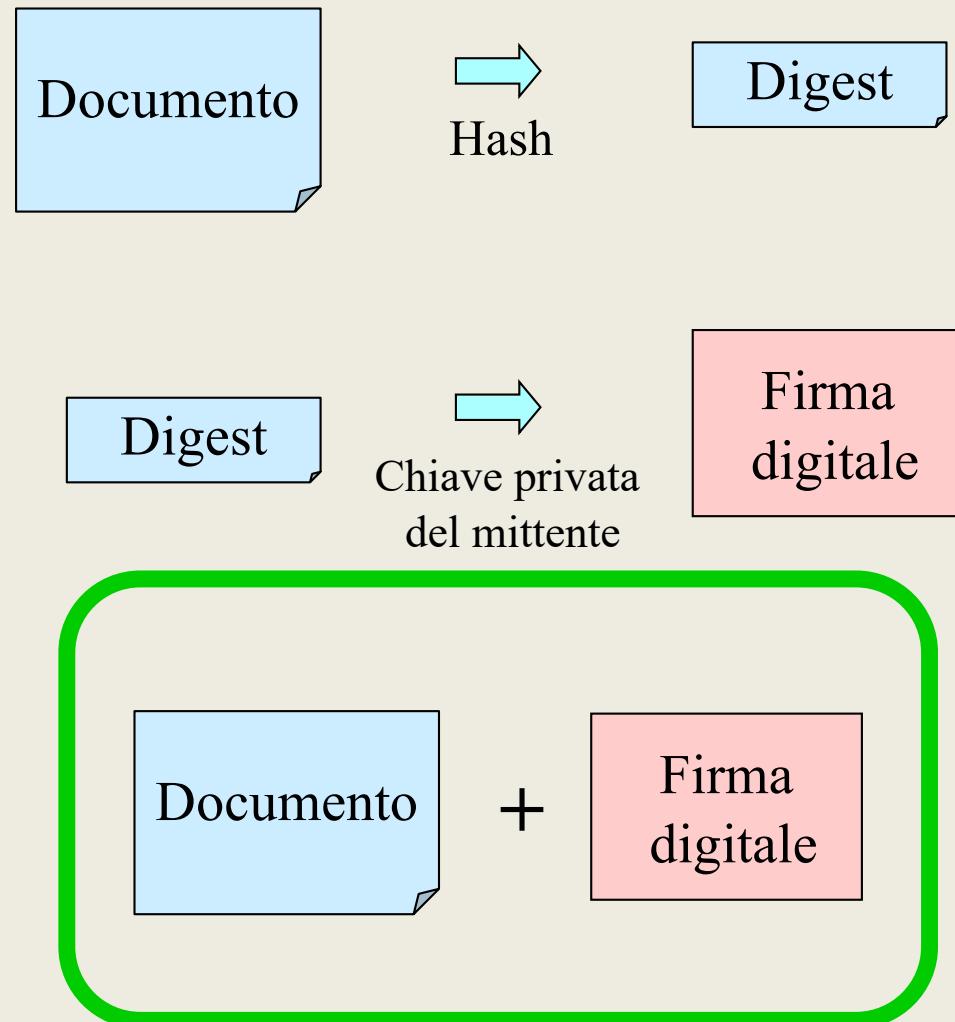


Autenticità e riservatezza



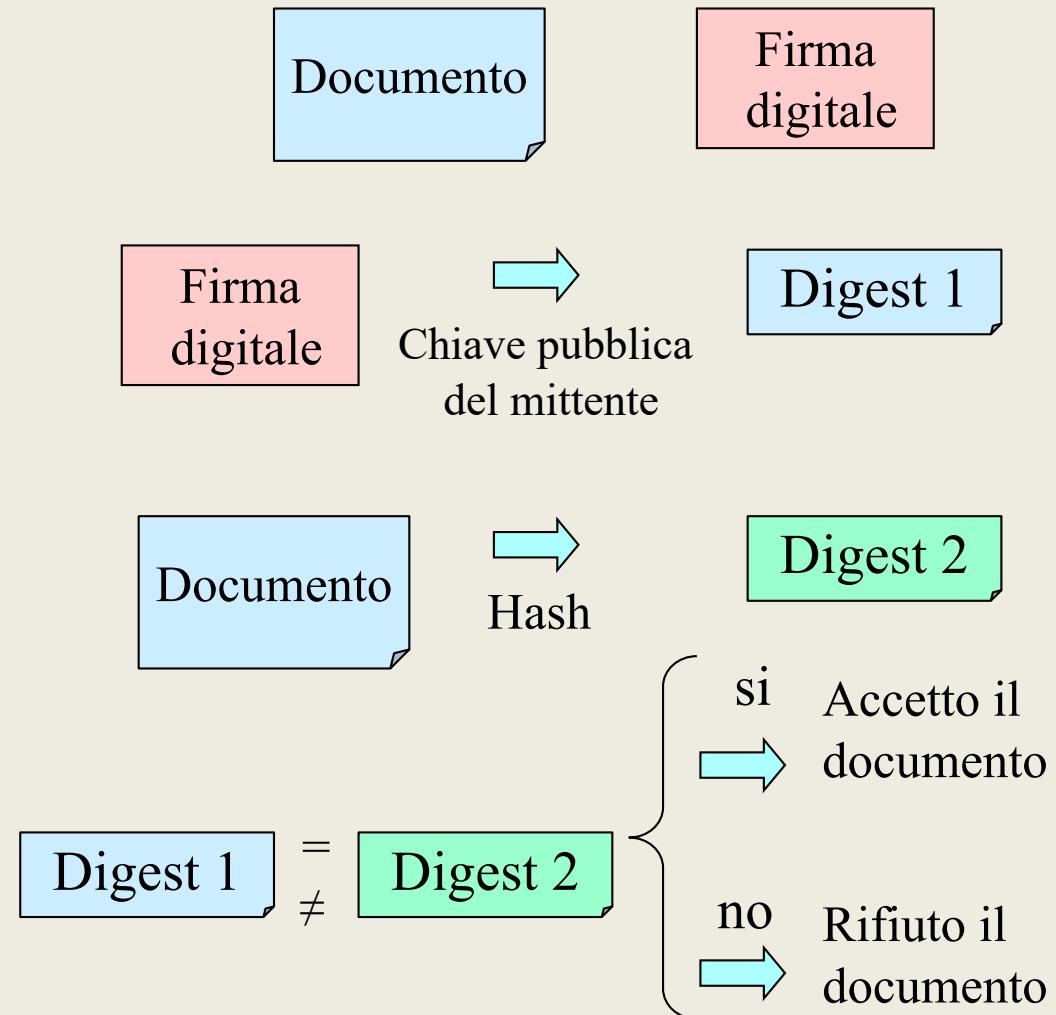
Generazione della firma

- Calcolare il **DIGEST** del documento
- **CIFRARE** il digest con la chiave privata del mittente (si ottiene così la firma elettronica)
- Aggiungere al documento originale la firma elettronica ottenuta al passo precedente e inviare la coppia (**messaggio, firma**)



Verifica della firma

- Separare il messaggio dalla firma
- Decifrare la firma usando la chiave pubblica del mittente
- Applicare al documento la funzione di Hash cioè calcolarsi il digest
- Verificare che i due risultati coincidano
 - si: accetto il documento
 - no: rifiuto il documento poiché è stato manomesso



La firma digitale

- Generata dal mittente (per uno specifico documento) utilizzando la sua chiave privata (**garanzia di autenticità e non ripudio**)
- Verificata dal destinatario tramite l'uguaglianza tra il digest ricevuto (decifrato utilizzando la chiave pubblica del mittente) e quello da lui generato dal documento ricevuto (**garanzia di integrità e autenticità**)
- Se è necessaria la **riservatezza**, il documento può venire cifrato:
 - con la chiave pubblica del destinatario
 - con una chiave simmetrica stabilita volta per volta tramite scambio di messaggi riservati

Conservazione e protezione della prova



Analisi e valutazione della prova



Analisi e valutazione della prova

- Segue la fase di acquisizione (Live/ Post mortem) e conservazione dei dati
- Anche questa fase dipende dal contesto in cui si opera:
 - Operazioni di accertamento per la polizia/autorità giudiziaria
 - Operazioni di accertamento in ambito aziendale
 - Contesto di Incident Response
- e consente di accettare:
 - Attività di sabotaggio
 - Diffusione di codice malevolo
 - Violazione delle politiche aziendali
 -

Analisi e valutazione della prova (cont)

- Comprende:
 - Identificazione del supporto contenente le informazioni
 - Recupero dei file e delle informazioni cancellate
 - Analisi del contenuto dei file
 - Documenti
 - Immagini
 - Video, audio,
 - Analisi dei principali software applicativi
 - Web browser
 - Verifica dell'account, cronologia, parole cercate, cookies, temporanei, ecc.
 - Posta elettronica
 - Client locale e/o webmail e relativi account

Analisi e valutazione della prova (cont)

- Chat e Video conferencing
 - messenger, whatsapp, telegram, sms, skype, zoom, gotomeeting, teams, ecc.
- Social network
 - Facebook, Instagram, Tik Tok, Twoo, Tinder, ecc.
- Utilizzo di sistemi di file sharing
 - eMule, BitTorrent, Kazaa, Limeware, ecc.
- Utilizzo di sistemi di cloud storage
 - Dropbox, Google Drive, OneDrive,
- Utilizzo di visualizzatori di immagini, player video, software di masterizzazione,
- Log di sistema e applicativi (locali e remoti)
- Registro chiamate (cellulare, centralino VoIP), contatti
- Generazione della **timeline** di utilizzo del computer/device

Strumenti di analisi

- Open-source vs proprietario
 - Utilizzare tool open-source se disponibili e efficienti
- Il **National Institute of Standards** and Technology (NIST – con HQ a Gaithersburg nel Maryland) ha attivo, ormai da anni, un progetto che effettua il **test e la validazione degli strumenti sw e hw di computer forensics**
 - <https://www.cftt.nist.gov>

Computer Forensics Tool Testing CFTT

NIST
Information Technology Laboratory / Software and Systems Division

SOFTWARE QUALITY GROUP

Computer Forensics Tool Testing Program (CFTT)

- CFTT General Information +
- CFTT Technical Information +
- Federated Testing Project
- CFReDS
- Computer Forensics Tool Catalog
- Useful Links

Computer Forensics Tool Testing (CFTT)

Welcome to the Computer Forensics Tool Testing (CFTT) Project Web Site.

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The NIST Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) has developed a methodology for testing computer forensic software tools by development of general tool test criteria, test sets, and test hardware. The results provide the information necessary for law enforcement agencies to make informed choices about acquiring and using computer forensics tools, and for international partners to evaluate their capabilities. A capability is required to ensure that forensic software tools consistently produce reliable results. Our approach for testing computer forensic tools is based on well-recognized international testing and quality testing.

The Computer Forensics Tool Testing Program is a project in The [Software and Systems Division](#) and the [Department of Homeland Security](#). Through the [Cyber Security](#) Department of Homeland Security's Science and Technology partners with the NIST CFTT project to provide reports to the public.

NEW: [Federated Testing](#) -- Guidance for common test methods & test report sharing via a central repository.



Forensic Science, Digital evidence, Software research and Software testing

Science and Technology

Research | Collaboration | Work with S&T | News & Events | About S&T



> [Science and Technology](#) > [Research](#) > [Cybersecurity](#)



Cybersecurity

[NIST Computer Forensic Tool Testing Reports](#)

National Institute of Standards and Technology (NIST) Computer Forensic Tool Testing (CFTT) Reports

Through the [Cyber Forensics](#) project, DHS S&T partners with the NIST CFTT project to provide forensic tool testing reports to the public. The CFTT project has established a methodology for testing computer forensic software tools utilizing tool specifications, test procedures, test criteria, test sets, and test hardware. Report results encourage developers to update and improve tools and provide end users with information on tool capabilities necessary for use and acquisition.

Reports, organized by tool category, can be accessed and downloaded via the links below. Reports within each category are organized by publication date (newest to oldest).

[Binary Image \(JTAG, Chip-Off\) Decoding and Analysis Tools](#)

[Deleted File Recovery and Active File Listing](#)

[Digital Data Acquisition](#)

[Disk Imaging](#)

[Forensic Media Preparation](#)

[Graphic File Carving](#)

[Hardware Write Block](#)

[Mobile Device Acquisition](#)

[String Search Tool](#)

[Software Write Block](#)

[Video File Carving](#)

[Write Protected Drive](#)

[Windows Registry Forensic Tool](#)

Toolkit Forense open source: **CAINE**

- CAINE (Computer Aided INvestigative Environment) è una distribuzione italiana Linux live
 - Distribuita con licenza GNU
 - Sviluppata e gestita da Giovanni Bassetti (NBS)
 - Esiste anche una release per Windows
 - <https://www.caine-live.net/>
- È utilizzata nei laboratori di Informatica Forense di alcune università italiane e straniere e in enti privati, oltre ad essere uno strumento impiegato da molte forze dell'ordine

Toolkit Forense CAINE (cont)

- CAINE integra sistemi e strumenti open source al fine di offrire un ambiente completo per l'analisi forense
- CAINE mira a garantire:
 - Un ambiente che possa supportare l'investigatore digitale durante le 4 fasi della Digital Forensics
 - Un'interfaccia grafica user-friendly
 - La disponibilità di strumenti user-friendly
- All'avvio, il sistema non utilizza le partizioni di swap presenti nel sistema sottoposto ad analisi
 - Tutti i device sono montati di default in read-only
 - Tutti i software di acquisizione di memorie di massa e di traffico su rete IP non alterano l'integrità del dato sottoposto ad acquisizione
- Si avvia tramite CD/DVD o penna USB

Toolkit Forense CAINE (cont)

- Alcuni principali tools:
 - Autopsy
 - Bulk Extractor
 - Ddrescue
 - Dcfldd
 - Log2Timeline
 - Disk utility
 - Iphonebackupanalyzer
 - Wireshark
 - Steghide
 - Dropbox reader
 - Nmap
 - Pdfcrack cracking tool
 - Pdf malware analysis
 - Midnight Commander (come file manager)
 - Testdisk per il recupero delle partizioni/file perse/cancellate
 - IE Cache View, History View e Cookies View (Opera, Mozilla, Chrome, Safari,)
 - AutoMacTC
 -

Esempi di Analisi forense: pedopornografia

- Chiunque **consapevolmente si procura o detiene** materiale pornografico realizzato utilizzando minori degli anni diciotto ... (600 quater cpp)
- Chiunque **consapevolmente cede ad altri**, anche a titolo gratuito, materiale pornografico realizzato utilizzando minori degli anni diciotto ... (600 ter cpp)
- Esempi di modalità di analisi:
 - Utilizzo di sistemi di **file sharing**
 - File scaricati
 - Parole chiave utilizzate
 - Condivisione dei file
 - **Navigazione su Internet**
 - Siti acceduti
 - Parole chiave ricercate

Esempi di Analisi forense: pedopornografia (cont)

- Posta elettronica
- Accesso a Social Network (Facebook, Badoo, Twoo,)
- Ricerca per keywords
- Utilizzo di sistemi di cloud storage (Dropbox, Google Drive, OneDrive, iCloud,)
- Utilizzo di visualizzatori di immagini e player video
- Utilizzo di software di masterizzazione
- Cestino: file ancora nella disponibilità dell'utente?
- File cancellati
-

Esempi di Analisi forense: **accesso abusivo**

- ????

La catena di custodia



Redazione dei verbali



ANALISI FORENSE DI SISTEMI DI FILE SHARING

Sistemi di File Sharing

- La tematica del file sharing è molto vasta e abbraccia una varietà enorme di applicazioni
- **File sharing**: condivisione di file e, quindi, di informazioni
- Alcuni esempi di file sharing:
 - Uso del protocollo **FTP**
 - Uso del protocollo **Netbios** su sistemi Windows
 - Uso del protocollo **Samba**
 - Uso del protocollo **NFS** e AFS
 - Uso del **Web sharing**
 - Uso dei **protocolli P2P**

I sistemi P2P

- Rappresentano, senza dubbio, una delle tecnologie più efficienti, veloci, scalabili e “sicure”, per condividere e scaricare file di qualsiasi natura e contenuto
- Sono utilizzati anche da applicazioni VoIP e di videconferenza (Skype, Hangout, ecc.), Instant Messaging (Mesh, Tox, Jami, ecc.)

I sistemi P2P (cont)

- Secondo alcune statistiche, l'occupazione di banda generata dal traffico P2P nell'area EMEA (Europa, Medio Oriente, Asia) raggiunge livelli superiori al 10% della banda totale
 - Questo traffico è generato principalmente dal protocollo BitTorrent durante le ore notturne
- I sistemi P2P consentono l'accesso al dato e all'informazione non tramite una specifica risorsa di rete (tipicamente un server) che la possiede, ma sulla base del contenuto che si sta cercando (concetto del **Content-Centric Networks** – CCN)
 - Un'informazione può essere recuperata da qualsiasi dispositivo di rete che la possegga e non necessariamente da una specifica locazione sulla rete

Architetture delle reti P2P

- In generale, le reti P2P si basano su una propria rete logica, detta di **overlay**, dove, nella maggior parte dei casi, non prevale il principio di server o gestore (controllore) centrale
 - Gli utenti mettono a disposizione le proprie informazioni condividendo parte della potenza computazionale, della capacità di storage e di banda del proprio computer e ricevendo, in cambio, servizi **content-centric**

Architetture delle reti P2P (cont)

- I nodi della rete sono “paritari” (**peer**) e contribuiscono tutti al mantenimento e alla crescita della rete, svolgendo sia la funzione di client che di server (**servent**, coniato appositamente per identificare il ruolo dei nodi delle reti P2P)
- Esistono tre architetture principali di reti P2P:
 - **Strutturate**
 - **Non strutturate**
 - **Gerarchiche**
- Le reti P2P “**Non strutturate**” sono quelle che meglio riflettono il comportamento di funzionamento delle reti P2P comunemente conosciute

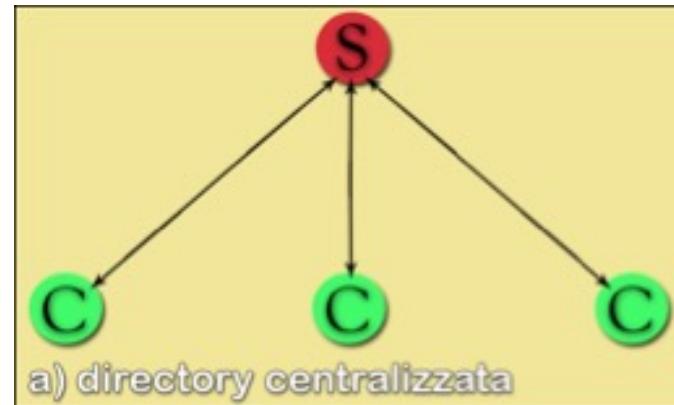
Le reti P2P non strutturate

- Non prevedono una struttura ben definita della rete di overlay
 - A parte alcuni casi specifici, possono essere considerate, a tutti gli effetti, delle reti **mesh**, con un'architettura completamente magliata e grafi casuali e non predibili
- Sono suddivise in 3 principali categorie:
 - **Ibride**
 - **Decentralizzate pure**
 - **Parzialmente decentralizzate**

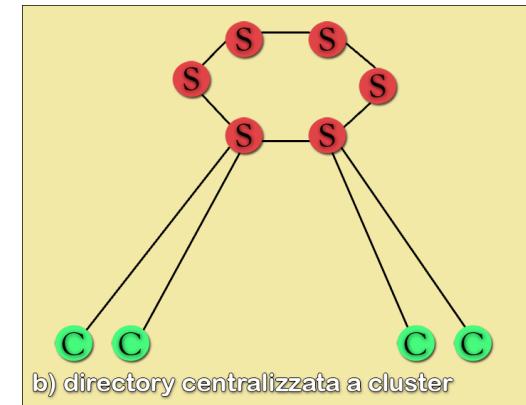
Le reti P2P ibride

- Sono state tra i primi modelli di reti non strutturate
 - Ogni peer mette a disposizione i propri contenuti, ma è necessario un **server centrale** (uno o più) che svolga la funzione di **indice dei contenuti** e fornisca il servizio di ricerca delle risorse
 - Tutti i peer interrogano il server per effettuare la ricerca del contenuto e, successivamente, stabiliscono una connessione (tipicamente TCP) con il peer che possiede il contenuto cercato
 - **Napster** è stato il primo sistema P2P di file sharing di massa ed era basato su tale modello

Le reti P2P ibride (cont)

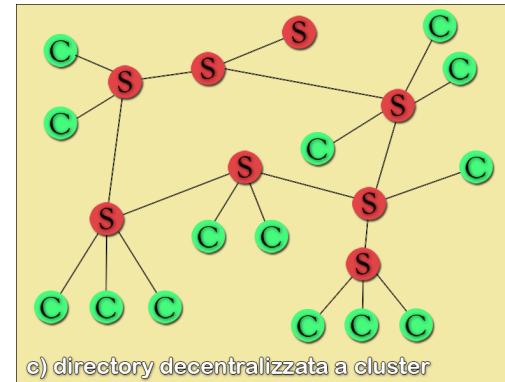


Directory centralizzata



**Directory centralizzata
a cluster**

- Gestione onerosa del server centrale
- Bottleneck costituito dal nodo centrale e, quindi, scalabilità limitata
- Single point of failure, sia dal punto di vista tecnico che legale



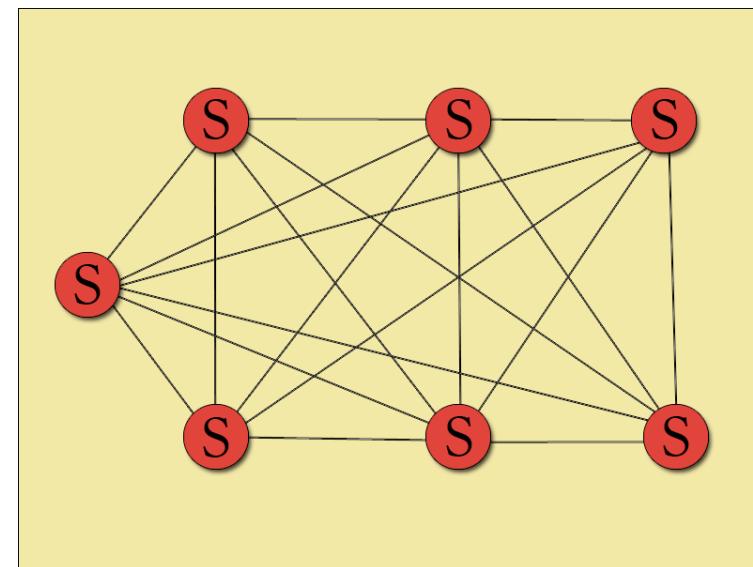
**Directory decentralizzata
a cluster**

Le reti P2P decentralizzate pure

- Costituiscono il **modello più collaborativo** delle reti P2P
- **Tutti i peer ricoprono lo stesso ruolo** e hanno le stesse responsabilità
- I nodi sono organizzati in una rete di overlay dove la **posizione assunta è casuale**
- Quando un **nuovo peer si connette alla rete** deve conoscere l'indirizzo IP di almeno un nodo (**bootstrap node**) che **lo accetta come neighbour**
 - Il nodo **stabilisce poi connessioni con gli altri peer attraverso un meccanismo di ping flooding**

Le reti P2P decentralizzate pure (cont)

- Il limite principale risiede nell'identificazione di un bootstrap node
- Approcci diversi:
 - **Bootstrap server** (server che memorizza una lista di peer attivi)
 - **Peer cache** (ogni peer mantiene la cache della lista di peer contattati precedentemente)
 - **Well known hosts** (non vi sono entità che registrano i peer attivi)



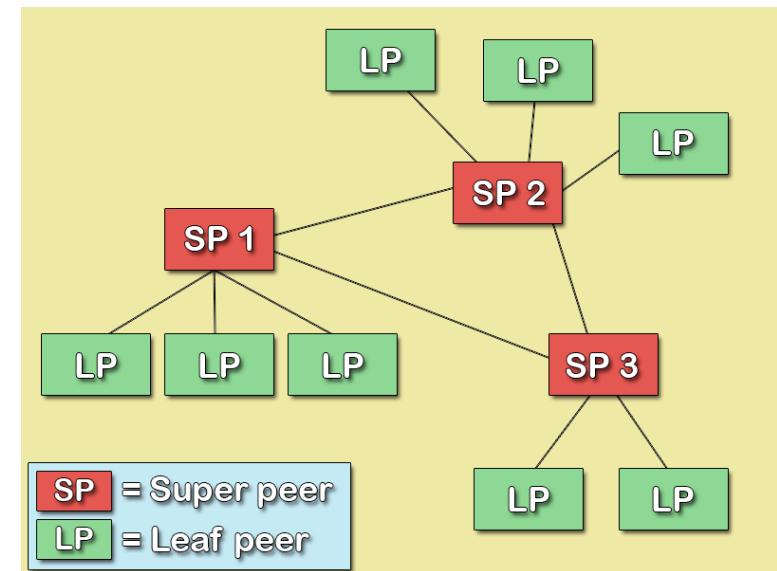
Reti P2P decentralizzate pure

Le reti P2P parzialmente centralizzate

- Suddividono i peer in due classi:
 - **Supernodi** (superpeer o ultrapeer)
 - **Nodi semplici** (ordinary peer o leaf peer)
- I superpeer sono nodi dotati di buona connettività e buona capacità computazionale
 - Formano, a loro volta, delle reti non strutturate dove essi agiscono come server locali
 - Mantengono l'indice delle risorse disponibili presenti nei leaf peer
 - Sono identificati dinamicamente tramite uno specifico algoritmo di elezione

Le reti P2P parzialmente centralizzate (cont)

- **Vantaggi:**
 - Riduzione del tempo di discovery delle risorse
 - Limitazione del ping flooding ai soli superpeer
 - Sfruttamento delle effettive potenzialità dei nodi peer partecipanti alla rete
- **Esempi:** Gnutella v0.6 e Skype



Analisi forense di sistemi P2P

- Le attuali regolamentazioni e linee guida non disciplinano esplicitamente le modalità di espletamento dell'analisi forense
- Sistemi con struttura e architettura complessa che vedono il coinvolgimento di molti attori:
 - Colui che effettua il download dell'informazione
 - Colui che mette a disposizione i dati
 - Gli Internet Service Provider e gli Access Provider coinvolti
 - La non chiara dislocazione geografica di dove sono situati gli host e l'informazione stessa
 - Ecc.
- Si deve cercare di seguire e applicare, per quanto possibile, le 4 fasi principali della Digital Forensics

Analisi forense di sistemi P2P (cont)

- Occorre tenere in considerazione che i sistemi P2P, per la natura delle informazioni scambiate e per l'utilizzo che spesso viene fatto di essi, sono molteplici, variegati e in continua evoluzione
- Lo sviluppo di sistemi di analisi forense che riescano a star dietro all'evoluzione della tecnologia in tale settore, costituisce un'impresa assai ardua
- Risulta indispensabile dotarsi di software specifici per l'analisi dei singoli applicativi e integrare tali software con altri tool che consentano di svolgere parti del processo di analisi che il software principale non consente di fare
- La stragrande maggioranza dei software per l'analisi dei sistemi P2P è di tipo commerciale

Un esempio di analisi forense di sistemi P2P: eMule

- eMule è stato uno dei client P2P più diffusi
 - Utilizza le reti P2P ed2k (eDonkey) e KAD (basata sul protocollo Kademlia)
 - Il client è open source (licenza GPL) e nel tempo ne sono state sviluppate varie versioni
 - L'architettura della rete ed2k è di tipo *ibrida*, costituita da client e server
 - La rete KAD, basata sul protocollo Kademlia, è invece una rete P2P priva di server e di tipo *decentralizzata pura*

Analisi forense di eMule

- L'ambiente di lavoro utilizzato ai fini dell'analisi forense di eMule prevede:
 - Un computer sul quale sia utilizzato il software P2P eMule
 - Sistema operativo Windows 7
 - Client **eMule 0.50a**
 - 2 tool specifici per l'analisi forense di eMule:
eMule Reader 1.0 e **eMule MET Viewer 1.1.2.0**

Analisi forense di eMule (cont)

- Di default eMule viene installato nella directory **C:\Programmi\emule**
 - Formata da 7 directory, ma ai fini dell'analisi sono rilevanti solo **Incoming** e **config**
 - Esiste anche una directory denominata **logs**, ma eMule non genera alcun file di log durante la sua attività e, pertanto, essa risulta irrilevante
 - **Incoming** contiene i file condivisi, cioè quelli scaricati dalla rete e quelli messi a disposizione di altri client P2P

Analisi forense di eMule (cont)

- La directory **config** contiene alcuni file fondamentali per il corretto funzionamento di eMule e un insieme di file che risultano determinanti per l'indagine investigativa:
 - File condivisi con altri utenti
 - Client che sono riusciti a scaricare file dal computer locale
 - Client con i quali il computer locale ha aperto una connessione ed ha scaricato file
 - L'identificativo del client locale nell'ambito della rete P2P, ecc.
 - Alcuni di questi file hanno l'estensione **.dat**, mentre altri hanno l'estensione **.met**

Analisi forense di eMule (cont)

- I file .dat sono leggibili tramite un qualsiasi editore di testo
- I file .met sono codificati secondo una struttura dati definita nel codice sorgente di eMule stesso
- Dal momento che il codice sorgente di eMule è open source, sono stati sviluppati tool ad hoc per decodifica
 - **eMule Reader™**
 - **eMule MET Viewer**

Analisi forense di eMule (cont)

- Bisogna capire se eMule è utilizzato in modalità condivisa tra gli utenti del computer sul quale è installato
 - Al momento dell'installazione, eMule chiede, tra le varie cose, se si desidera modificare il path di default di installazione e se si vuole rendere utilizzabile in maniera condivisa con gli altri utenti di Windows
 - È necessario analizzare alcune chiavi del registro di sistema di Windows
 - Uso di Regedit.exe

Analisi forense di eMule (cont)

- Verificare:

HKEY_CLASSES_ROOT\emule\DefaultIcon\shell\open\command

Fornisce il path di installazione di eMule e il nome dell'eseguibile

HKEY_CURRENT_USER\Software\emule

Fornisce:

- **Install path** (come l'altra)
- **Installer Language (1040)** corrisponde alla lingua italiana)
- **UsePublicUserDirectories**, che può assumere 3 valori:
 - **0** (ogni utente del computer ha una propria personalizzazione di eMule)
 - **1** (eMule è condiviso tra gli utenti del sistema e non utilizza la program directory per i file di configurazione e quelli condivisi)
 - **2** (eMule è condiviso tra gli utenti del sistema e utilizza la program directory per i file di configurazione e quelli condivisi)

Analisi forense di eMule: directory config

- Analisi dei file ritenuti più idonei allo scopo
- Utilizzo di eMule Reader™ per i file non leggibili con un editore di testo
 - Sviluppato dalla società statunitense Architecture Technology Corporation (ATC-NY), specializzata nella ricerca e sviluppo di prodotti per la computer e *digital forensics*, quali i prodotti commerciali P2P Marshal, Live Marshal, Mac Marshal, Mobile Marshal, ecc., utilizzati dalle forze dell'ordine americane
 - È costituito da dieci programmi

Programmi di eMule Reader™ e file analizzati

Programma eMule Reader	File analizzati
ParseCancelled.exe	cancelled.met
ParseClients.exe	clients.met
ParseKeyIndex.exe	key_index.dat
ParseKnown.exe	known.met, known2.met, known2_64.met
ParseLoadIndex.exe	load_index.dat
ParseNodes.exe	nodes.dat
ParsePartMet.exe	File con estensione .part.met
ParseServer.exe	server.met
ParseSourceIndex.exe	src_index.dat
ParseStoredSearches.exe	StoredSearches.met

NomeProgramma [-dh] -i <infile> -o <outfile>

Analisi forense di eMule: file analizzati

- ***cancelled.met***: contiene l'elenco dei file per i quali l'utente ha annullato il processo di download dalla rete
- ***known.met***: contiene l'elenco dei file scaricati e condivisi dall'utente. Per ogni file, sono indicati:
 - Il nome del file
 - La dimensione
 - La data di ultima modifica (che consente di ricavare, con una granularità che arriva ai secondi, quando è stato completato il download del file sul computer)
 - L'hash del file (che costituisce il suo identificatore sulla rete)
 - L'hash delle varie parti che lo compongono
 - La data di ultima condivisione sulla rete
 - Il numero di richieste di download del file da parte di client remoti
 - Il numero di richieste di download remoto effettivamente accettate
 - La velocità di trasferimento
 - Ecc.

Analisi forense di eMule: file known.met

- Esempio di visualizzazione tramite **ParseKnown.exe**

File Descriptor Values:

File Name: Phil Collins – Phill Collins – Sussudio.mp3

File Size: 4199916

Last Modified: Wed Mar 20 19:07:36 2013

Part Descriptor Values:

Part Name: 005.part

Hash Values:

AICH Master Hash: 1D AF E1 67 1E AE 23 3E B6 06
65 CA 87 FD 26 40 97 DA 08 9D

.....

eMule Met Viewer
consente di
visualizzare
graficamente le
informazioni
presenti nel file

Analisi forense di emule: file known.met (cont)

- known.met può essere analizzato anche tramite il tool eMule Met Viewer
 - Visualizzazione più chiara delle informazioni
 - Esportazione del contenuto in formato csv



Filename	File Size	Temporary Filename	Last Written (UTC)	Last Posted (UTC)	Last Shared (UTC)	Requests Total	Requests Accepted	Bytes Uploaded	Upload Priority	Artist	Album
Phil Collins - Phil Collins - Sussudio....	4.199.916	005.part	20/03/2013 18.07.36	20/03/2013 23.07.35	24/03/2013 12.00.03	1	1	184.320	Auto	Phil Collins	Testify (adv)
Phil Collins - Can't stop loving you....	4.120.576	001.part	20/03/2013 18.08.57	20/03/2013 23.08.57	24/03/2013 12.00.03	0	0	0	Auto	Phil Collins	Testify (adv)

0 / 2 selected | 2 records loaded successfully

Analisi forense di eMule: file clients.met e Preferences.dat

- **clients.met** contiene l'elenco dei computer con i quali si è svolta l'attività di scambio e condivisione delle informazioni, sia in download che in upload
- Per ognuno fornisce:
 - La chiave identificativa del client dal quale è stato trasferito un file o parte di esso (operazione di download)
 - La chiave identificativa del client che ha, invece, scaricato un file, o parte di esso, dal sistema locale (operazione di upload)
 - La data (con granularità fino ai secondi) di ultimo contatto con un client
 - Ecc.
- Il file serve, inoltre, a calcolare i crediti per la gestione locale della coda di upload
- **Preferences.dat** è un file di 16+1 byte che contiene l'hash dell'utente. Il valore di tale hash è calcolato, in maniera random, al momento del primo avvio di eMule sul sistema ed è utilizzato per identificare il client nella rete P2P

Esempio di file clients.met

Key: 49 1A 5F E8 CB 0E 1D 30 6D A6 F2 53 B9 88 6F D1

Uploaded: 0

Downloaded: 733958

Last Seen: Wed Mar 20 19:07:50 2013

Reserved: 0

.....

Secure Identity: 30 4A 30 0D 06 09 2A 86 48 86 F7 0D
01 01 01 05

Key: 5D 3A 0F CE 94 0E 50 7C 0C 0B 37 6D 3F 55 6F 14

Uploaded: 32529

Downloaded: 0

Last Seen: Wed Mar 20 19:37:50 2013

Reserved: 0

.....

Secure Identity: 30 4A 30 0D 06 09 2A 86 48 86 F7 0D
01 01 01 05

Demo del tool CAINE

Luca Vasarelli

Istituto di Informatica e Telematica - CNR
Unità Tecnologica Innovazione Digitale

luca.vasarelli@iit.cnr.it

CAINE

- **CAINE** (Computer Aided INvestigative Environment) è una distribuzione italiana live GNU/Linux per la digital forensics
- Principali caratteristiche:
 - Supporta l'investigatore digitale durante le 4 fasi della digital forensics
 - È dotata di un'interfaccia user-friendly
 - Integra molti tool sviluppati nell'ambito della DF
- <https://www.caine-live.net/>

DEMO LIVE

Ambiente di lavoro

- Windows 10 emulato tramite VirtualboxVM e GuestAdditions
- Immagine ISO Caine 13.0
- Utilizzo di device USB esterni per popolare di dati l'ambiente di lavoro e sperimentare il recupero di file cancellati dallo slack space, ecc.

Casi d'uso

1. L'investigatore ha recuperato un insieme di file e, tra questi, vi sono alcuni pdf protetti da pw
 - Utilizzo del tool **pdfcrack** per trovare le pw necessarie ad aprire e modificare i file
2. Tra i vari file recuperati sono presenti anche delle immagini
 - Tramite il tool **Stegosuite** verificheremo se tali immagini contengono dei messaggi e/o file segreti
 - Vedremo anche come è semplice nascondere un messaggio in un'immagine

Casi d'uso (cont)

3. L'investigatore ha trovato una penna USB dell'indagato e vuole verificare se sono state cancellate informazioni
 - Utilizzo dei tool **Photorec** e **TestDisk**
4. È stato ritrovato anche un portatile con S.O. Windows, i cui utenti sono però protetti da password
 - Utilizzeremo il tool **chntpw** per rimuovere la password associata ad un utente o promuoverlo amministratore



Master Universitario di I Livello in Cybersecurity

Digital Forensics

Arianna Del Soldato, Maurizio Martinelli

Istituto di Informatica e Telematica - CNR
Servizi Internet e Sviluppo Tecnologico

arianna.delsoldato@iit.cnr.it, maurizio.martinelli@iit.cnr.it

Sommario

- Le fasi principali della Digital Forensics
 -
 - Conservazione e protezione
 - Catena di custodia
 - Redazione dei verbali
 - Redazione del report e Presentazione
- Cloud Forensics
- Vehicle Forensics
 - I veicoli 'intelligenti'
 - Sfide da affrontare
 - Identificazione della fonte di prova
 - Acquisizione dei dati
 - Best practice
 -

Conservazione e protezione della prova



Conservazione e protezione della prova

- Come per la fase di acquisizione, **anche nel trasporto la fonte** di prova deve **rimanere integra**
- Aspetti da considerare:
 - **Sicurezza** nel **trasporto**
 - **Protezione fisica** dalle alterazioni
 - **Archiviazione sicura** e replica
 - **Restrizioni dell'accesso** al dato
- Riferimenti:
 - Best Practice RFC 3227 e norme ISO 27037
 - Legge 48 del 2008: art. 259 2° comma c.p.p e art. 260 1° e 2° comma c.p.p

Conservazione e protezione della prova: *Sicurezza nel trasporto*

- Preferibile trasporto fisico
 - Deve essere trasportata dall'investigatore o delegato
- Per garantire la catena di custodia, le fasi di imballaggio del trasporto e della conservazione devono essere adeguatamente registrate
 - Tutto deve essere etichettato e fotografato
- Sconsigliabile utilizzare Internet / reti
 - Difficoltà nel dimostrare l'integrità del dato nel trasferimento

Conservazione e protezione della prova: Protezione fisica dalle alterazioni

- È buona norma **sigillare** i supporti originali contenenti la **digital evidence**
 - Utilizzare un **imballaggio** che protegga il dispositivo
- Porre **attenzione**:
 - A forti **campi elettromagnetici** o **scariche elettrostatiche** che potrebbero cancellare la prova dal dispositivo
 - Ai **colpi** e alle **cadute** – scarsa resistenza all'urto delle parti motorizzate e componenti elettriche
 - **Umidità** o acqua, per i corto circuiti



Conservazione e protezione della prova: *Esempi di involucri*



ESD Bag
Sacchetto antistatico



**Patented wireless
strong bag**



Strong Hold Box
Gabbia di Faraday



Strong Hold tent
Gabbia di Faraday

Conservazione e protezione della prova: Archiviazione sicura e replica

- L'archiviazione della prova deve essere effettuata in luoghi che ne garantiscono la:
 - Protezione anti-incendio (allarme, estintori, divieto di fumare)
 - Temperatura ed umidità adeguata
 - Protezione contro i campi magnetici (es. lontano da dispositivi radio muniti di antenna direzionale)
 - Ecc.
- E' consigliata la duplicazione della fonte di prova e la conservazione in luoghi distinti

Conservazione e protezione della prova: *Restrizioni all'accesso del dato*

- La prova deve essere accessibile solo:
 - da personale fidato e dotato di adeguate autorizzazioni
 - per finalità strettamente legate all'indagine forense
- È possibile memorizzare la fonte di prova su appositi dischi o partizioni cifrate

La catena di custodia



La catena di custodia

- Ogni fonte di prova acquisita deve essere accompagnata da un documento che è **la catena di custodia**
- Necessario per la corretta **attribuzione** delle **responsabilità** in tutto il ciclo di vita della fonte di prova
 - Certifica l'**originalità**, l'**integralità** e le modalità in cui è stata trattata l'evidenza
 - Tutti i **passaggi di mano** dell'evidenza devono essere **tracciati** e ci deve essere un **responsabile**

La catena di custodia (cont)

- Contiene:
 - Intestazione con data e numero di protocollo associato al caso
 - Campi da compilare durante la fase di acquisizione
 - Campi da compilare per ogni aggiornamento
- Sono necessarie almeno tre sezioni relative a:
 - Caratteristiche del sistema
 - Caratteristiche della Digital Evidence
 - Dati relativi alla custodia e alla restituzione

La catena di custodia: **Caratteristiche del sistema**

- Sono un insieme di informazioni riguardanti il **sistema dal quale è stato acquisito il dato** o l'elemento fisico
- **Identifica** univocamente il/i sistema/i e **fornisce informazioni utili per l'analisi**

Id reperto	Sistema	Tipo	Marca	Modello	N. Serie	S.O.	Luogo del ritrovo	Data e ora
ADS/1	PC	Laptop	Apple	MacBook Air (Retina, 13-inch, 2020)	FVFCX1 85XXXX	macOS Big Sur V. 11.4	Stanza A23 IIT/CNR via G. Moruzzi 1 Pisa	26/06/23

La catena di custodia: ~~Caratteristiche dell'evidenza~~

- ~~Caratteristiche del dispositivo nel quale è cristallizzata la fonte di prova~~
- Se estratto dal sistema:

Id reperto	Driver	Produttore	Modello	Grandezza	N. Serie	HASH	Note aggiuntive
ADS/2	HardDisk	Maxdor	Seagate M3 HDD Esterno da 4TB	2TB	SN: XXXXXXXX	6e6bc4e4 9dd477eb c98ef4046 c067b5f....	

La catena di custodia: **Custodia e restituzione**

- Mantiene traccia di tutti i soggetti che vengono in contatto con la fonte di prova
- In ogni determinato istante temporale deve essere possibile risalire al responsabile della custodia

Id reperto	Data	Orario	Cedente Nominativo	Cedente Firma	Ricevente Nominativo	Ricevente Firma
ADS/2	05/06/2023	12:00	Paolino Paperino	<i>PaoPape</i>	Gastone	<i>Gastone</i>

- La sezione restituzione è analogo alla custodia e viene utilizzata nel momento di restituzione del dispositivo originale

Redazione dei verbali



Redazione dei Verbali

- I verbali sono i **primi documenti** legati alla catena di custodia e vi sono riportate le **attività relative all'acquisizione e all'analisi** della fonte di prova (titolo III del libro II c.p.p)
- Le **attività** svolte devono essere **dettagliate** e possibilmente supportate da foto
- Le **informazioni** contenute nel verbale devono rispettare i principi di **chiarezza, trasparenza e completezza**
- Devono essere in grado di resistere ai limiti e ai controlli della legge

Redazione dei Verbali (cont)

- Per le **attività di acquisizione** della fonte di prova, l'**investigatore** deve riportare:
 - La **descrizione** passo passo **della procedura** di estrazione della **Digital Evidence**, con **motivazione** e attività svolte
 - **Foto** del reperto, del sistema e di tutti gli elementi che certifichino le attività svolte
 - I **riferimenti temporali** delle **attività** e l'eventuale scostamento dall'ora riportata sul sistema
 - Riferimento a tutte le **persone intervenute**

Redazione dei Verbali (cont)

- Per le **attività di analisi** devono essere riportate:
 - Le **attività di laboratorio**,
 - le **analisi effettuate**,
 - gli **strumenti utilizzati e dati rilevati**

Redazione del report e presentazione



Redazione del report:

Passi per la preparazione

- 1. Raccolta dei dati/evidenze**
- 2. Analisi dei risultati** (COSA metto nel report)
- 3. Definizione della struttura del report** (COME presento le informazioni)
- 4. Stesura** e revisione della **bozza**
- 5. Stesura del report finale**
- 6. Diffusione** della relazione

Presentazione

- I **risultati e le conclusioni** dedotte devono essere presentate in **forma** facilmente **comprendibile**
 - L'esposizione deve **fornire prove** alla corte e **resistere alle opposizioni** dell'avversario
- **In tribunale:**
 - **Interrogatorio diretto:**
 - È **condotto dalla parte del mittente del lavoro**
 - Ha lo scopo di **fornire le prove per dimostrare il caso**
 - **Contraddittorio:**
 - È **condotto dall'opposizione**
 - Viene **valutata la validità della testimonianza**
 - Obiettivi della difesa:
 - Sminuire l'importanza della testimonianza diretta
 - Carpire dall'esperto delle testimonianze che siano a suo favore

CLOUD FORENSICS

Il Cloud

- È modello di elaborazione distribuito che **consente l'accesso condiviso** e su richiesta, mediante la rete, a risorse **delocalizzate** configurabili
- Ha cambiato radicalmente il modo di creare, erogare, accedere e gestire i servizi IT
- Ha portato benefici sia in ambito economico che sociale

I vari modelli di sistemi Cloud

- **Modelli di servizio:**
 - SaaS – Software as a Service
 - PaaS – Platform as a Service
 - IaaS – Infrastructure as a Service
- **Modelli di sviluppo:**
 - Cloud Privato
 - Cloud Pubblico
 - Cloud Comunitario
 - Cloud Ibrido

Caratteristiche del Cloud: PRO

1. Offerta di servizi «on-demand» a **basso costo**
2. **Semplicità di accesso alle risorse** via Internet tramite **interfaccia** offerta dal **Cloud Service Provider** (CSP)
3. **Storage illimitato di dati** o grandi quantità di spazio
4. **Condivisione di risorse delocalizzate** gestite dal CSP
5. **Elasticità dei servizi**

Caratteristiche del Cloud: CONTRO

- Problemi di riservatezza e sicurezza dei dati
- Creazione di grandi aggregazioni di dati digitali come obiettivi di criminali informatici
- Mancanza di controllo sui dati personali
 - Chi, dove e come vengono gestiti e processati
- Utilizzo delle tecnologie del Cloud per commettere crimini informatici

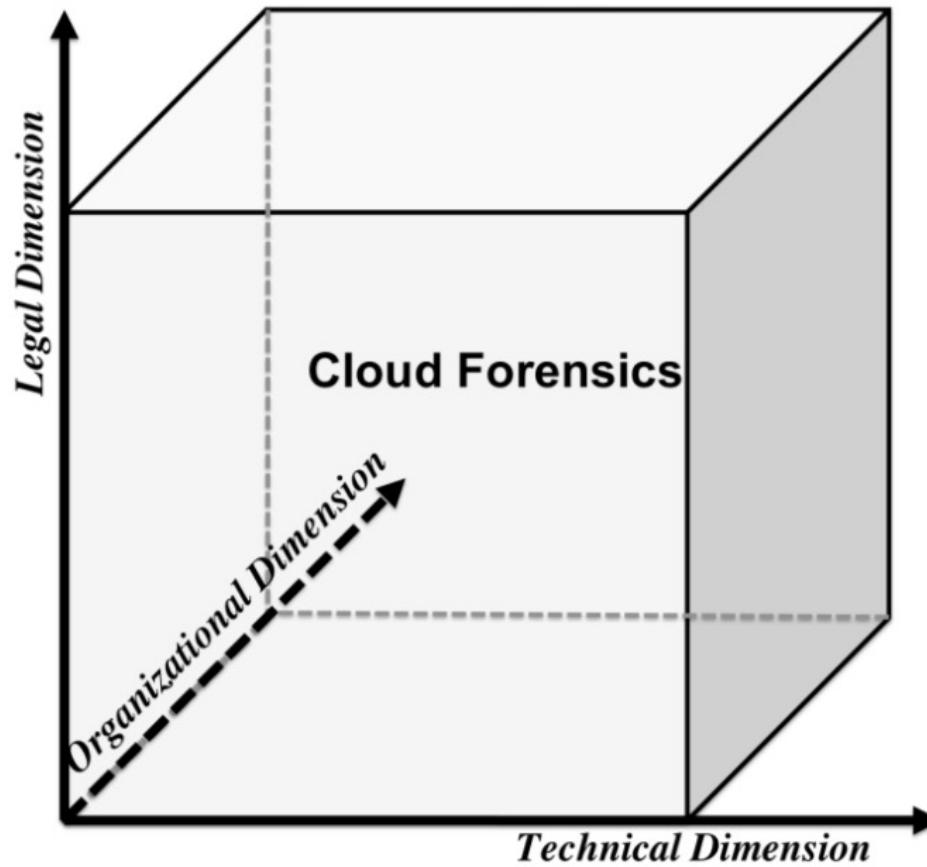
La Cloud Forensics

- Investigazioni digitali che coinvolgono l'ambiente di Cloud
- Le procedure forensi sul Cloud fanno riferimento alla Digital Forensics con le dovute integrazioni determinate dalla virtualizzazione e dalla distribuzione e duplicazione delle risorse
- Il Cloud può essere l'oggetto, il soggetto e lo strumento del crimine informatico

UNA DISCIPLINA MULTIDIMENSIONALE

Cloud Forensics

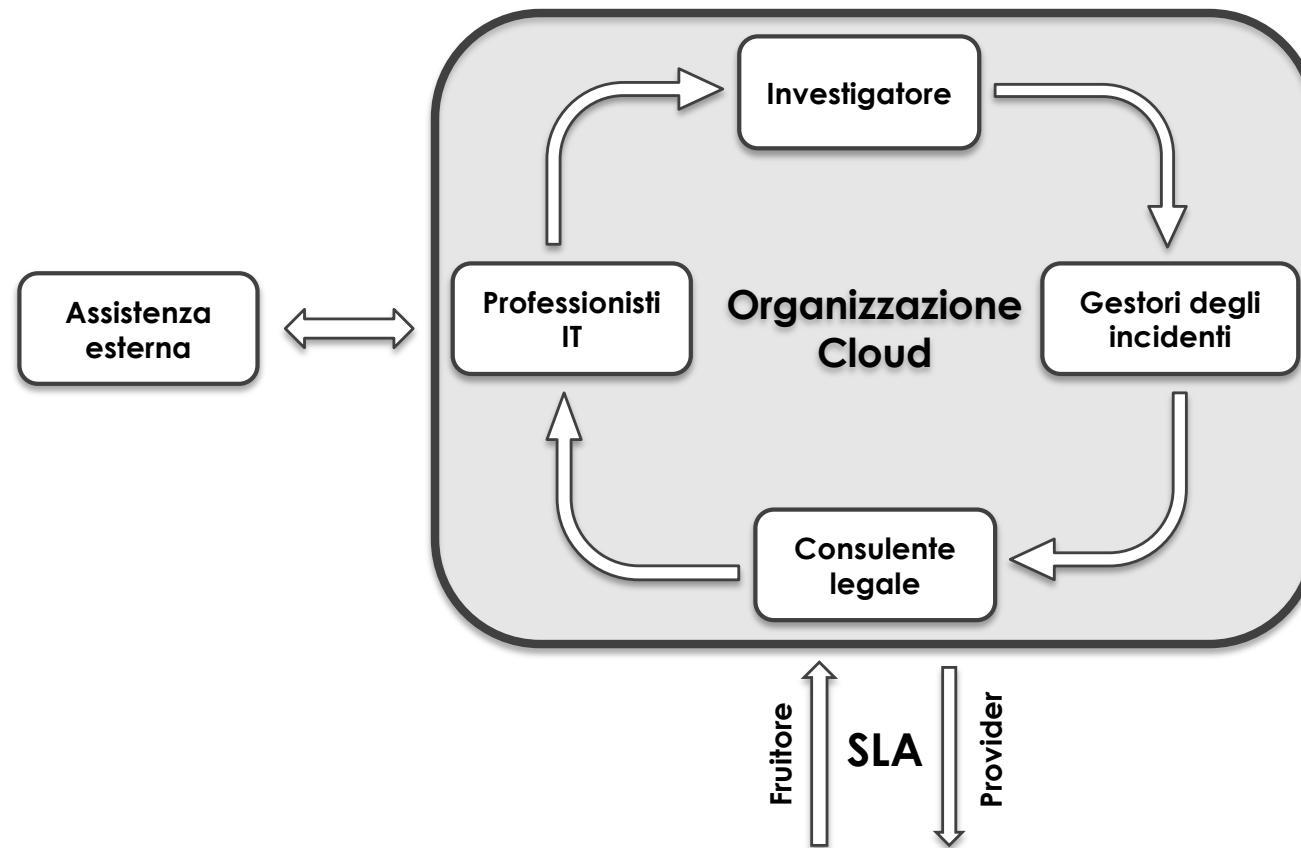
Cloud Forensics: una disciplina multidimensionale



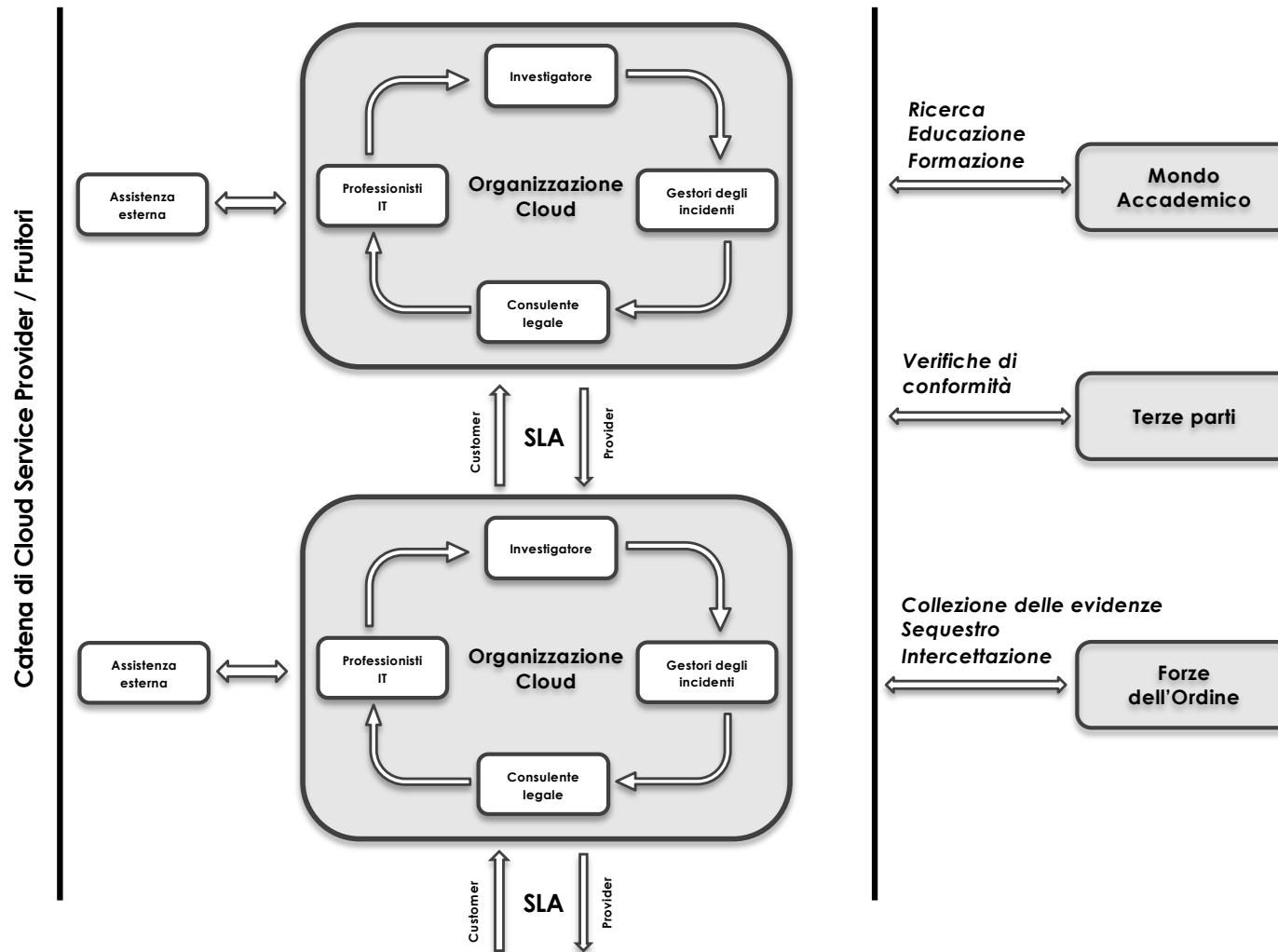
Technical Dimension: strumenti e procedure da adottare

- La **collezione dei dati dipendentemente dalla tipologia del Cloud**
 - Separo i ruoli del fruitore e del CSP, colleziono lato utente e CSP, rispetto dei requisiti che caratterizzano la prova digitale (autenticità e integrità), non violo le leggi e i regolamenti
- **Eseguo Elastic, Static e Live Forensics** nei processi di:
 - Acquisizione dei dati, recupero dei dati, analisi dell'evidenza, scelta di strumenti per collezionare i dati volatili
- **Separo le evidenze**
 - Ambienti Multi-tenant. Non violo la privacy di utenti che condividono la solita risorsa
- **Eseguo le investigazioni in ambiente virtualizzato**
 - Le sfide sono la perdita di dati, la localizzazione dei dati in un certo momento tenendo presente la giurisdizione e la locazione fisica
- **Attuazione di misure preventive**
 - Tool per la collezione di dati lato CSP e client, eseguire snapshot regolari di storage remoti

Organizational Dimension: *struttura proposta*



Organizational Dimension: struttura proposta (cont)



Legal Dimension

- Riguarda le sfide dovute alla multi-giurisdizione e al multi-tenancy
 - Devono essere rispettate le varie legislature, la riservatezza e la privacy dei fruitori dei servizi
- Definizione di Contratti di Servizio tra CSP e fruitori (SLA) definiscono:
 - I servizi, le tecniche forensi e l'accesso ai dati offerti dal CSP
 - I limiti, i ruoli e le responsabilità tra i contraenti
 - Le politiche adottate per garantire le indagini nel rispetto delle leggi e della privacy

LE SFIDE E LE OPPORTUNITÀ

Cloud forensics

Sfide: Le funzionalità easy-to-use

- L'accesso semplificato alle risorse di Cloud ha portato:
 - Creazione di grandi aggregazioni di dati digitali divenuti un obiettivo appetibile
 - Sistema di registrazione debole che facilita l'anonimato dei criminali
 - Una inconsapevolezza dell'utente della tecnologia utilizzata e dei rischi

Sfide: *Elastic, Static e Live forensics*

- La **sincronizzazione** dei timestamp
 - Tra infrastruttura del **CSP** e client Web remoti
 - Su più **macchine fisiche** distribuite su più aree **geografiche**
- L'**unificazione** o la **conversione** di diversi **formati** di log
 - formati proprietari nelle indagini congiunte
- **Recupero dei dati cancellati** e attribuzione della proprietà

Sfide: La separazione delle evidenze

- **Istanze diverse** della stessa macchina fisica sono logicamente isolate dall'Hypervisor ma **condividono le stesse risorse** fisiche
 - Il CSP e forze dell'ordine devono mantenere la stessa separazione delle evidenze durante il processo di indagine
 - Necessità di tecnologie di provisioning e de-provisioning degli utenti più accurate
- **Utilizzo della crittografia** per i dati sensibili dell'utente
 - Necessità di accordi per la gestione e l'accesso delle chiavi durante le fasi dell'Analisi Forense

Sfide: La virtualizzazione

- L'inaccessibilità delle risorse fisiche
 - Live forensics sulle MV, tecniche di acquisizione remota
- La compromissione dell'hypervisor è un grande punto di criticità e coinvolge tutte le risorse
 - Necessità di sviluppare politiche e procedure tecniche per facilitare le indagini a livello hypervisor
- Il mirroring dei dati, l'archiviazione in più giurisdizioni e la difficoltà di geolocalizzare real-time i dati possono ostacolare l'investigazione
 - Difficoltà per i CSP di fornire strumenti che consentano al cliente la tracciabilità fisica dei dati, in un certo periodo di tempo, in tutte le aree del Cloud
 - Necessita di collaborazioni internazionali tra forze dell'ordine (es: caso di confisca)

Sfide: **La formazione del personale interno**

- Stabilite una **struttura organizzativa interna** dedicata alla Cloud Forensics
 - Mancanza di esperienza legale pertinente
 - Lento progresso della disciplina della Forensics rispetto allo sviluppo della tecnologia
 - Lento progresso nello sviluppo di leggi e dei regolamenti internazionali

Sfide: *La catena di dipendenza*

- Identificare la **correlazione tra i CSP** che hanno rapporti di dipendenza
- **Coordinare le indagini** sulla catena di dipendenza che dipendono:
 - Dalle indagini di ciascuno dei suoi collegamenti
 - Dal livello di complessità della dipendenza
- **Stabilire** strumenti, procedure, politiche o **accordi** relativi alle indagini **cross-provider**

Sfide: I Service Level Agreement

- Assenza dei termini relativi alla Cloud Forensics nei SLA
 - Scarsa consapevolezza del cliente, la mancanza di trasparenza del CSP e dei regolamenti internazionali
- Dovrebbero **specificare le procedure** da seguire...
 - Servizi e Procedure per consentire l'accesso ai dati
 - La condotta da seguire nell'ambiente multi-giurisdizionale
 - I limiti delle responsabilità del CSP e del fruitore
- ...e le **misure tecniche e organizzative** adottate dal CSP:
 - La dislocazione delle strutture nel Cloud
 - Eventuali sub-fornitori
 - Paesi coinvolti
 - Politiche che regolano la *data redemption*
 - La completezza e l'affidabilità dei meccanismi di *logging*
 - La garanzia della legittimità dei trasferimenti transfrontalieri

Sfide: La Multi-giurisdizione e Multi-tenancy

- Le differenze tra le legislazioni in tutti i paesi (stati) in cui risiedono il Cloud e i suoi fruitori:
 - Quale **tipologia di dati** è possibile accedere e recuperare secondo la(le) giurisdizione(i) vigente(i) nel luogo in cui risiedono le macchine fisiche contenenti i dati?
 - Come conduco la fase di **repertamento delle prove senza violare la privacy** o i diritti degli utenti in base alle leggi e ai regolamenti in vigore dove risiedono i vari fruitori?
 - Quale tipo di **prova è ammissibile** al tribunale nella giurisdizione specifica?
 - Che tipo di **catena di custodia** è necessaria nella(e) giurisdizione(i) in cui i dati forensi sono passati durante un'indagine nel Cloud?
 - Quali sono i **meccanismi legislativi** nella collaborazione tra l'industria e le forze dell'ordine, in casi come il sequestro delle risorse, la confisca del Cloud, l'interscambio di dati tra paesi, ecc.?

Opportunità per la Forensics

- **Ridondanza dei dati**
 - Rende quasi impossibile la cancellazione totale dei dati
- **Servizi di clonazione** delle MV offerti da SaaS possono essere utilizzati per
 - creare un'immagine di una macchina da analizzare
 - Velocizzare le indagini con investigazioni parallele
- Il **versionamento** dei dati utilizzato dai CSP
 - Recuperare, ripristinare e conservare ogni versione di ogni oggetto memorizzato

Opportunità per la Forensics (cont)

- **Scalabilità e flessibilità del Cloud**
 - può offrire servizio di Cloud Forensics pay-per-use illimitato
 - Consente ai fruitori di predisporre dei server dedicati alla Forensics pronti da essere utilizzati se necessario
- **Forensics as a Service** (FaaS)
 - Sistema di analisi forense basato sul Cloud
- **Law as a Service** (LaaS)
 - Sistema di erogazione dei servizi legali ad uso degli avvocati e dei giuristi

LE FASI DELLA DIGITAL FORENSICS NEL CLOUD

Cloud Forensics

Identificazione

- Individuo il CSP e cerco di capire dove sono le strutture tecnologiche che contengono i dati
- Sfide:

Dislocazione
dei dati

Virtualizzazione

Limiti
giurisdizionali

Elasticità dei
servizi

Acquisizione e raccolta

- Eseguo:

Live Forensics sui client

Computer Forensics sulle MV

Network Forensics in ambiente virtualizzato

- Sfide:

Replicazione dei dati

Grandi quantità di dati

Catena di custodia

Volatilità delle risorse

Privacy dei fruitori del servizio

- Opportunità:

Ridondanza dei dati

Versionamento

Coservazione

- Garantire l'integrità dei dati originali memorizzati su un sistema *Cloud*
- Sfide:

Replicazione
dei dati

Volatilità
delle risorse

Segregazione
della prova

Analisi

- Data l'elasticità delle risorse, è difficile ottenere una fotografia del sistema in un determinato momento

- Sfide:



**Integrazione
delle prove**



Costruzione
della **timeline**



Cifratura
dei dati

- Opportunità:



**Servizi di
clonazione**



**Servizi
pay-per-use
illimitati**

Documentazione e presentazione

- Sfide:

Catena di custodia

Report fotografico

Comprensione dei concetti del Cloud Computing

VEHICLE FORENSICS

Perché l'analisi forense sui veicoli

- I **veicoli connessi** e a **guida autonoma**, così come le infrastrutture di supporto come le **città intelligenti** stanno diventando **sempre più comuni**
- **Memorizzano una grande quantità di informazioni** digitali, che possono essere **fonte di evidenze digitali in investigazioni** dove il **veicolo**
 - È **coinvolto nella scena del crimine**
 - È uno **strumento per commettere atti criminali**
- E' stata introdotta la **fattispecie di reato stradale** punito a titolo di colpa: Legge N. 41 del 23 marzo 2016
 - Omicidio colposo stradale (Art. 589-bis) e lesioni personali stradali gravi o gravissime ad una persona (Art. 590-bis)

I veicoli ‘intelligenti’

- Possono essere visti come un tipico **sistema informatico con diversi moduli elettronici** collegati e controllati da diversi dispositivi informatici
- In **ogni auto** connessa ci sono **circa 80 centraline**, 150 milioni di righe di codice e **25 GB** di dati per **ogni ora di funzionamento**
- L'**Internet of Vehicle** (IoV) prevede **comunicazioni**:
 - **V2V**: Vehicle-to-Vehicle, **V2I**: Vehicle-to-Infrastructure, **V2N**: Vehicle-to-Network, **V2P**: Vehicle-to-Pedestrian

Sfide da affrontare

- **Eterogeneità dei dati:**
 - Assenza di standard, problema della pertinenza
- **Catena di custodia:**
 - Rete delle componenti dinamica, assenza di riferimenti temporali
- **Acquisizione di prove valide:**
 - Componenti costruiti da diversi produttori, produttori e case automobilistiche di paesi diversi
- **Rispetto della privacy:**
 - Molti dati contengono informazioni personali

Identificazione della fonte di prova

- Identificare le tipologie di componenti elettronici e dispositivi:
 - Centraline legate ai sistemi di infotainment
 - Centraline con funzionalità EDR (Event Data Recorder)
 - Dati che provengono dalle scatole nere che montano le compagnie di assicurazione
- Conoscere quali informazioni memorizza ogni componente e dove
- Capire quali tipi di informazioni personali sono archiviate nei veicoli e come vengono archiviate (Es: cronologie delle chiamate e dati dei social media)
- Capire se c'è l'infrastruttura di supporto e come il veicolo interagisce con essa
 - semafori intelligenti e telecamere a circuito chiuso in una città intelligente
 - quali tipi di dati vengono archiviati, dove vengono archiviati e come possono essere recuperati

Acquisizione dei dati

- Utilizzando i **gateway** presenti nel veicolo tramite un connettore OBD (On Board Diagnostic) o porta USB
- Rimuovendo il **modulo** dal veicolo (senza danneggiare il modulo e/o alterare i dati)
 - Quali sono le implicazioni di una perdita di alimentazione sui dati memorizzata sul dispositivo?
 - I dati sono memorizzati su memorie RAM, flash, EPROM?
 - Vi sono altri dati volatili?
 - Vi sono dispositivi di archiviazione rimovibili (es: USB), ecc.?
 - Vi sono connessioni esterne?
 - Come mantengo la catena di custodia?
- Acquisizioni estreme e invasive
 - J-tag (standard IEEE 1149.1)
 - chip off



Acquisizione dei dati (cont)

- **Quali strumenti possono essere utilizzati** per acquisire in modo ufficiale/forense le prove dai vari componenti e dall'infrastruttura di supporto?
- **Difficoltà ad ottenere informazioni proprietarie** dai diversi produttori dei componenti del veicolo
 - Proprietà intellettuale
 - Moduli assemblati da diversi produttori ubicati in Paesi diversi
 - Rischi reputazionali
- **Difficoltà** dovute ai **Sistemi di sicurezza** sui componenti

Best practice

- Il veicolo dovrebbe essere custodito in un'area con scarsa o nessuna ricezione del segnale GPS.
 - Meglio una garage che funga da gabbia di faraday
- Non avviare l'auto, ove possibile, poiché alcune auto sovrascrivono o modificano i dati ad ogni giro della chiave di accensione
- Assicurarsi che l'unità di navigazione non si avvii per evitare modifiche alle informazioni (es. ultima posizione nota)
- Individuare qualsiasi dispositivo o veicolo nelle vicinanze con la funzione Bluetooth attivata e registrare i loro indirizzi MAC (es. Dispositivo Android e iOS, compresi i dispositivi del team investigativo)

I sistemi di Infotainment

Information + entertainment



Dati contenuti:

- **Info sul veicolo e sul sistema**
 - Numero di serie
 - Codice articolo
- **Dati delle applicazioni installate**
 - Meteo
 - Traffico
 - Social
- **Dispositivi connessi**
 - Telefoni e lettori multimediali
 - USB e SD card
 - Punti di accesso Wireless
- **Dati di navigazione**
 - Percorsi attivi e inattivi
 - Luoghi salvati
 - Destinazioni precedenti
- **Dati del cellulare**
 - ID del device
 - SMS e chiamate
 - Rubrica
 - Audio e Video
- **Eventi sul veicolo**
 - Lettore contachilometri
 - Indicazione marcia
 - Apertura/chiusura portiere
 - Accensione/spegnimento luci
 - Connessioni Bluetooth
 - Connessioni WI-FI
 - Sincronizzazioni ora GPS

Digital Forensics

Rita Rossi

Istituto di Informatica e Telematica del CNR

rita.rossi@iit.cnr.it

Digital Forensics

Principi generali in tema di prova e specificità della prova informatica

Argomenti

- Principi generali in tema di prova e specificità della prova informatica
- Ruolo e compiti dei consulenti informatici. Il regime di responsabilità.
- La Convenzione di Budapest sulla criminalità informatica e la legge nazionale di recepimento
- Le modifiche al codice di procedura penale e al codice privacy in materia di acquisizione e conservazione di documenti probatori inerenti i dati di traffico telefonico e telematico
- Giurisdizione e luogo di consumazione nei reati informatici

Principi generali in tema di prova
Art. 111 Costituzione

- *“La giurisdizione si attua mediante il giusto processo regolato dalla legge.*
- *Ogni processo si svolge nel contraddittorio tra le parti, in condizioni di parità, davanti a giudice terzo e imparziale. La legge ne assicura la ragionevole durata. “Omissis”*
- *Il processo penale è regolato dal principio del contraddittorio nella formazione della prova. “Omissis”.*

Il diritto alla prova

- Consiste nel **diritto di ricercare le fonti di prova**; chiedere l'ammissione del relativo mezzo; partecipare alla sua assunzione; **ottenere una valutazione del risultato al momento delle conclusioni**.
- E' sancito dall'art. 190, 1 c.p.p. secondo cui *Le prove sono ammesse a richiesta di parte. Il giudice provvede senza ritardo con ordinanza escludendo le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti.*
- Comprende il diritto di **partecipare all'assunzione del mezzo di prova attraverso la testimonianza**
- Vanno **considerate** le prove preconstituite, quali le **prove documentali** e quindi **l'accettazione nel processo del dato probatorio**
- Va tenuto conto dei poteri istruttori officiosi da parte del giudice per i quali "*Quando il giudice ritiene di non poter decidere allo stato degli atti assume, anche d'ufficio, gli elementi necessari ai fini della decisione*" che si esplicano in modo diverso a seconda della materia trattata

Peculiarità della prova informatica

- Il principio generale in materia di prova, secondo cui le prove si assumono in dibattimento, può soffrire eccezioni.
- I dati e le informazioni digitali presentano specifiche peculiarità poiché il dato digitale può presentarsi irripetibile e l'accesso stesso può portare al danneggiamento, alla distruzione o all'alterazione del contenuto probatorio, impedendo al giudice di valutare correttamente le informazioni.
- In alcuni casi, non si può attendere la fase del dibattimento e la prova deve essere “congelata” sin dalla fase delle indagini preliminari per essere portata integra (chain of custody e algoritmi di HASH) alla valutazione del giudice
- Il Codice di procedura penale prevede perciò specifiche indicazioni in materia di atti irripetibili per evitare che le prove urgenti vengano disperse e garantire il principio del contraddittorio.

Gli elementi della *Digital Forensics*

- Attraverso la *Digital Forensics* si persegue l'obiettivo di evidenziare il dato, giuridicamente rilevante, contenuto, memorizzato o trasmesso in qualsiasi sistema digitale, nell'ambito di procedimenti civili e penali, sebbene il termine sia più spesso utilizzato con riferimento ai fatti di criminalità informatica, ai quali peraltro, in queste brevi note faremo riferimento.

Digital Forensics

fasi di svolgimento

- La *Digital Forensics*, in quanto strumento per la ricerca delle prove digitali, è essenzialmente caratterizzata dalle seguenti azioni
 - Individuazione e Preservazione delle evidenze digitali
 - Acquisizione della prova informatica, garantendo l'inalterabilità di ciò che è analizzato
 - Analisi dei dati rinvenuti e correlazioni
 - Documentazione di quanto svolto nelle varie fasi
- Compito degli informatici forensi è quello di esaminare i media digitali e i sistemi tecnologici al fine di ricercare, individuare, estrarre, preservare e conservare gli elementi probatori da utilizzare nell'ambito di un procedimento legale

Peculiarità della prova informatica: indifferibilità e non reiterabilità

- L'attività investigativa relativa all'acquisizione della prova informatica presenta sovente i seguenti caratteri:
- **Indifferibilità**, ossia la prova deve essere assunta subito poiché diversamente andrebbe dispersa,
- **Non reiterabilità**: una volta compiuta l'attività investigativa di acquisizione della prova non è più possibile ripeterla

- Attività del Pubblico Ministero: articoli 359 e 360 del c.p.p.
 - 1. Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera.
 - 2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine (art. 359).
 - Quando gli accertamenti previsti dall'articolo 359 riguardano persone, cose o luoghi **il cui stato è soggetto a modificazione**, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici. Omissis (360 cpp).

Accertamenti tecnici non ripetibili e incidente probatorio

- **Accertamenti tecnici non ripetibili del difensore**
 - L'art. 391 decies disciplina gli **accertamenti tecnici non ripetibili compiuti dal difensore**. “3. Quando si tratta di **accertamenti tecnici non ripetibili**, **il difensore** deve darne avviso, senza ritardo, al pubblico ministero per l'esercizio delle facoltà previste, in quanto compatibili, dall'articolo 360.”
- **Incidente probatorio, Art. 392 c.p.p.** - 1. Nel corso delle indagini preliminari il pubblico ministero e la persona sottoposta alle indagini possono chiedere al giudice che si proceda con incidente probatorio: “Omissis”.
 - f) a una perizia o a un esperimento giudiziale, se la prova riguarda una persona, una cosa o un luogo il cui stato è soggetto a modificazione non evitabile; “Omissis”

Accertamenti tecnici indifferibili e non ripetibili

L'articolo 117 disp. att. c.p.p. relativo agli accertamenti tecnici che modificano lo stato dei luoghi, delle cose o delle persone stabilisce che:

*“Le disposizioni previste dall'articolo 360 del codice si applicano anche nei casi in cui l'accertamento tecnico determina modificazioni delle cose, dei luoghi o delle persone **tali da rendere l'atto non ripetibile.**”*

Tali articoli si applicano perciò sia ai casi di indifferibilità che di irripetibilità della prova”

Digital Forensics

**Mezzi di prova: documento informatico e perizia
Ruolo e compiti dei periti e consulenti tecnici**

Mezzi di prova e mezzi di ricerca della prova

- I **mezzi di prova** costituiscono gli **elementi** con i quali nel processo è possibile accettare direttamente i fatti oggetto del processo stesso. Costituiscono mezzi di prova: la testimonianza, l'esame delle parti, i confronti, gli esperimenti giudiziali, la perizia, i documenti.
- Si tratta di mezzi di prova “tipici”, previsti e disciplinati dal codice di procedura penale. E’ possibile, tuttavia, utilizzare anche mezzi di prova “atipici” ai sensi dell’art. 189 c.p.p. secondo cui: *“Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona”*
- I **mezzi di ricerca della prova**, quali le ispezioni, perquisizioni, sequestri, intercettazioni sono, invece, finalizzati a permettere l’acquisizione di tracce, notizie o dichiarazioni idonee ad assumere rilevanza probatoria.

Il documento informatico

- La prova documentale costituisce un mezzo di prova
- «**documento informatico**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»; (Art. 1, DECRETO LEGISLATIVO 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale)
- Regolamento eIDAS: (REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE).
«**documento elettronico**», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;
- b. “**dati informatici**” indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione (Conv. Budapest sul Cybercrime);

Prova documentale Art. 234 c.p.p. e Art. 234 bis

- Il codice di procedura penale, agli articoli 234– 243 sotto il capo VII «Documenti» disciplina l'acquisizione della prova documentale riferita a documenti formati fuori dal processo e nel quale devono essere inseriti affinché possano acquisire efficacia probatoria.
- In ambito penale la nozione di documento assume una connotazione piuttosto ampia. L'art. 234 c.p.p dispone che: «*1. È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. 2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia. Omissis*
- È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare (Art. 234 bis).

Finalità e Oggetto della perizia

Art. 220 c.p.p

- La perizia costituisce un **mezzo di prova** indirizzato ad integrare le conoscenze del giudice con quelle di un esperto.
- “1. La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche.
- 2. Salvo quanto previsto ai fini dell'esecuzione della pena o della misura di sicurezza, non sono ammesse perizie per stabilire l'abitualità o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche indipendenti da cause patologiche.”

Consulenti Tecnici e Periti

Procedimento Civile e Penale

- Nel procedimento penale il consulente tecnico del giudice assume il nome di Perito (art. 221 c.p.p.).
- Nel procedimento civile il consulente tecnico del giudice assume il nome di Consulente Tecnico d'ufficio, CTU (Art. 61 c.p.c.).
- Sia nel procedimento civile che nel procedimento penale i consulenti delle parti assumono il nome di Consulente Tecnico di Parte, CTP (Art. 201 c.p.c. e Art. 225 c.p.p.)
- Il consulente tecnico del Pubblico Ministero è un Consulente Tecnico di parte, CTPM, art. 359 c.p.p.

Nomina del perito

- “1. **Il giudice nomina il perito scegliendolo tra gli iscritti negli appositi albi o tra persone fornite di particolare competenza nella specifica disciplina.** Quando la perizia è dichiarata nulla, il giudice cura, ove possibile, che il nuovo incarico sia affidato ad altro perito.
- 2. **Il giudice affida l'espletamento della perizia a più persone quando le indagini e le valutazioni risultano di notevole complessità** ovvero richiedono distinte conoscenze in differenti discipline.
- 3. **Il perito ha l'obbligo di prestare il suo ufficio,** salvo che ricorra uno dei motivi di astensione previsti dall'articolo 36”.

Nomina del perito

- Il consulente tecnico d'ufficio assume la qualifica di pubblico ufficiale.
- **Incompatibilità con l'ufficio di perito:** chi si trova nelle condizioni di cui all'art. 222, ovvero: (*minorenne, interdetto, inabilitato, chi è affetto da infermità di mente, chi è interdetto anche temporaneamente dai pubblici uffici, o è stato sospeso dall'esercizio di una professione o di un'arte, chi è sottoposto a misure di sicurezza personali o a misure di prevenzione, chi non può essere assunto come testimone o ha facoltà di astenersi dal testimoniare o chi è chiamato a prestare ufficio di testimone o di interprete, chi è stato nominato consulente tecnico nello stesso procedimento o in un procedimento connesso*

Consulenti Tecnici

- Articolo 225 c.p.p. Nomina del consulente tecnico

“1. Disposta la perizia, **il pubblico ministero e le parti private hanno facoltà di nominare propri consulenti tecnici in numero non superiore**, per ciascuna parte, a quello dei periti.

2. **Le parti private, nei casi e alle condizioni previste dalla legge sul patrocinio statale dei non abbienti, hanno diritto di farsi assistere da un consulente tecnico a spese dello Stato.**

- Valgono per il consulente tecnico le cause di incompatibilità di cui all'art. 222 cpp.

Attività del perito

- 1. **Il perito procede alle operazioni necessarie per rispondere ai quesiti.** A tal fine può essere autorizzato dal giudice a prendere visione degli atti, dei documenti e delle cose prodotti dalle parti dei quali la legge prevede l'acquisizione al fascicolo per il dibattimento.
- 2. Il perito può essere inoltre autorizzato ad assistere all'esame delle parti e all'assunzione di prove nonché a servirsi di ausiliari di sua fiducia per lo svolgimento di attività materiali non implicanti apprezzamenti e valutazioni.
- 3. Qualora, ai fini dello svolgimento dell'incarico, il perito richieda notizie all'imputato, alla persona offesa o ad altre persone, gli elementi in tal modo acquisiti possono essere utilizzati solo ai fini dell'accertamento peritale.
- 4. Quando le operazioni peritali si svolgono senza la presenza del giudice e sorgono questioni relative ai poteri del perito e ai limiti dell'incarico, la decisione è rimessa al giudice, senza che ciò importi sospensione delle operazioni stesse.

Comunicazioni relative alle operazioni peritali

- Articolo 229 c.p.p.
 1. Il perito indica il giorno, l'ora e il luogo in cui inizierà le operazioni peritali e il giudice ne fa dare atto nel verbale.
 2. Della eventuale continuazione delle operazioni peritali il perito dà comunicazione senza formalità alle parti presenti.

Attività dei consulenti tecnici

Art. 230 c.p.p.

- 1. I consulenti tecnici possono assistere al conferimento dell'incarico al perito e presentare al giudice richieste, osservazioni e riserve, delle quali è fatta menzione nel verbale.
- 2. Essi possono partecipare alle operazioni peritali, proponendo al perito specifiche indagini e formulando osservazioni e riserve, delle quali deve darsi atto nella relazione.
- 3. Se sono nominati dopo l'esaurimento delle operazioni peritali, i consulenti tecnici possono esaminare le relazioni e richiedere al giudice di essere autorizzati a esaminare la persona, la cosa e il luogo oggetto della perizia.
- 4. La nomina dei consulenti tecnici e lo svolgimento della loro attività non può ritardare l'esecuzione della perizia e il compimento delle altre attività processuali.

Consulenza tecnica fuori dei casi di perizia

- Attraverso la nomina di un consulente tecnico fuori dalla perizia ciascuna Parte ha il diritto di tentare di convincere il giudice applicando i principi scientifici che ritiene più adeguati, svolgendo le investigazioni difensive finalizzate a ricercare e individuare elementi di prova.
- Art. 233 c.p.p. “1. Quando non è stata disposta perizia, **ciascuna parte può nominare**, in numero non superiore a due, propri consulenti tecnici. Questi possono esporre al giudice il proprio parere.. Omissis”

Consulenti Tecnici del Pubblico Ministero

- Articolo 359 c.p.p.
 1. Il pubblico ministero, **quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze**, può nominare e **avvalersi di consulenti**, che non possono rifiutare la loro opera.
 2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.
- Il consulente del PM deve essere scelto, di regola, fra gli iscritti agli albi dei periti.

L'Informatico forense

- Costituisce una nuova professione suscettibile di sviluppi professionali interessanti nel nuovo contesto digitale in cui viviamo.
- Può operare come perito del giudice o consulente di parte, in procedimenti civili o penali.
- Si richiedono competenze principalmente tecniche, ma anche giuridiche; non esiste comunque preclusione se si è in possesso di altre competenze e conoscenze adeguate a svolgere tale professione
- L'Osservatorio Nazionale Informatica Forense (ONIF), come anche altre organizzazioni, svolge un'attività funzionale a far conoscere gli ambiti di questa professione anche attraverso appositi convegni e report. Interessanti informazioni sulla professione possono essere confrontate anche sul sito dedicato a: Albo Informatici Forensi Italiano»

L'attività di consulenza a fini giudiziari il consulente tecnico di parte. Il consulente del giudice

- L' attività di consulenza giudiziaria del professionista rientra nel novero delle c.d. prestazioni intellettuali
- Obbligazione di mezzo e non di risultato
- La prestazione deve essere svolta dal professionista con diligenza, prudenza e perizia
- l'errato o inesatto adempimento che cagioni un danno ingiusto, obbliga il professionista a risarcire il danno, indipendentemente dal fatto che abbia ricevuto l'incarico dal giudice o dalla parte privata.
- Responsabilità civile, disciplinare e penale propria di chi riveste il ruolo di CTU o perito.

L'attività di consulenza a fini giudiziari il consulente tecnico di parte. Il consulente del giudice

- La **responsabilità disciplinare** deriva dall'iscrizione all'ordine professionale cui normalmente afferisce il professionista e la sua condotta può integrare violazione dell'ordinamento professionale di appartenenza, nonché derivare dall'iscrizione nell'elenco dei relativi registri tenuti dal tribunale che prevedono il rispetto di specifiche previsioni deontologiche
- La **responsabilità civile** del CTU trova la sua fonte nell'art. art. 64 c.p.c. «*Si applicano al consulente tecnico le disposizioni del Codice penale relative ai periti. In ogni caso, il consulente tecnico che incorre in colpa grave nell'esecuzione degli atti che gli sono richiesti, è punito con l'arresto fino a un anno o con l'ammenda fino a diecimilatrecentoventinove euro. Si applica l'articolo 35 del Codice penale. In ogni caso è dovuto il risarcimento dei danni causati alle parti.*- Il Consulente tecnico di parte non è un pubblico ufficiale e non ha l'obbligo di accettare l'incarico, pertanto non è sottoposto al regime penalistico proprio dei pubblici ufficiali. La responsabilità professionale civile scaturisce dal contratto sottoscritto.

Digital Forensics

La Convenzione di Budapest e la legge nazionale di attuazione

La convenzione di Budapest sui reati informatici

- La Convenzione di Budapest del 23 novembre 2001 del Consiglio d'Europa sulla criminalità informatica rappresenta uno strumento internazionale vincolante per qualsiasi paese aderente ad essa al fine di sviluppare una legislazione nazionale completa contro la criminalità informatica
- E' stata attuata nel nostro ordinamento con la legge 28 marzo 2008 n. 48 con cui sono state introdotte modifiche al codice penale, al codice di procedura penale, al codice privacy e in materia di cooperazione internazionale
- Costituisce un quadro per la cooperazione internazionale tra Stati Parti del trattato sul funzionamento dell'Unione Europea, ed è completata da un protocollo sulla xenofobia e il razzismo commesso attraverso sistemi informatici.
- Il Secondo Protocollo addizionale sulla cooperazione internazionale potenziata e la raccolta di prove in formato elettronico è stato portato alla firma nel corso del mese di maggio 2022.

La Convenzione di Budapest sulla criminalità informatica

- La Convenzione sulla criminalità informatica, resa a Budapest il 23 novembre 2001,
 - **costituisce il primo accordo internazionale** riguardante i crimini commessi attraverso Internet
 - ha lo **scopo di rendere più efficienti le indagini** e l'azione penale su reati commessi in materia di sistemi informatici e **consentire la raccolta delle prove**

È divisa in **3 sezioni principali**:

1. **Definizione dei reati** per cui prendere provvedimenti a livello nazionale
2. **Disposizioni sull'acquisizione, la raccolta, e la conservazione** del dato digitale
3. **Principi generali** relativi alla **cooperazione internazionale** nelle indagini, nella raccolta di dati e nei procedimenti collegati ai reati informatici

La Convenzione di Budapest sulla criminalità informatica

Diritto penale sostanziale

1. Individuazione e contenuto dei reati da inserire negli ordinamenti nazionali:

- Accesso illegale ad un sistema informatico
- Intercettazione abusiva
- Attentato all'integrità dei dati e di un sistema informatico
- Abuso di apparecchiature
- Falsificazione informatica
- Frode informatica
- Reati relativi alla pornografia infantile
- Reati contro la proprietà intellettuale
- Tentativo e complicità nel commettere reato
- Responsabilità delle persone giuridiche

La Convenzione di Budapest sulla criminalità informatica

Diritto procedurale

2. Disposizioni sull'acquisizione, la raccolta, e la conservazione del dato informatico

La Convenzione obbliga ogni Stato aderente ad essa ad adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti il perseguimento e realizzazione di attività volte alla:

- **Conservazione** rapida di dati informatici immagazzinati
- **Conservazione e divulgazione** rapide di dati relativi al traffico
- **Ingiunzione di produrre** specifici dati
- **Perquisizione e sequestro** di sistemi informatici e di dati informatici immagazzinati
- **Raccolta in tempo reale** di dati sul traffico
- **Intercettazione** di dati relativi al contenuto

La Convenzione di Budapest sulla criminalità informatica

Cooperazione Internazionale

3. Principi generali relativi alla **cooperazione internazionale**

- **Estradizione** tra parti per i reati stabiliti
- **Mutua assistenza** tra le parti ai fini delle indagini
- Comunicazione di **informazioni spontanee**
- **Richiesta di conservazione** di dati informatici
- Accesso a dati pubblicamente disponibili
- Richiesta di raccolta di dati sul traffico
- Richiesta di intercettazione di dati
- Designazione di un punto di contatto 24/7

Digital Forensics

La legge 18 marzo 2008, n. 48 di attuazione della Convenzione di Budapest.

**Le modifiche al codice di procedura penale in materia di prova.
Le modifiche al codice privacy in materia di acquisizione e
conservazione di documenti probatori inerenti i dati di traffico
telefonico e telematico**

La legge 18 marzo 2008 n. 48

- La legge del 18 marzo 2008. n. 48, *Ratifica del esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno* ha comportato modifiche e aggiunte:
 - al codice penale e, segnatamente, nell'ambito dei cyber crimes introdotti con la legge 547/93;
 - al codice di procedura penale;
 - al decreto legislativo 30 giugno 2003 n. 196 (Codice privacy), oggi riformato per effetto del Reg. UE 679/2016 e del decreto legislativo 101/2018;
 - al decreto legislativo 231/2001 in materia di responsabilità delle persone giuridiche;
 - in tema di misure per il contrasto alla pedopornografia.

I mezzi di ricerca della prova informatica

La legge 48/2008 del 18 marzo 2008

- In relazione ai mezzi di ricerca della prova, la legge 48/2008 prevede le seguenti garanzie procedurali per la gestione dell'evidenza:
 1. Il dovere di conservare inalterato il dato originale **nella sua genuinità** e il dovere di impedire l'alterazione dell'originale.
 2. Il dovere di formare una copia che assicuri la conformità del dato acquisito rispetto a quello originale
 3. Il dovere di assicurare la non modificabilità dei dati acquisiti
 4. La garanzia della installazione di sigilli informatici sulle cose sequestrate
 5. L'ampliamento dello spettro esecutorio anche ai sistemi informatici o telematici, ancorché protetti da misure di sicurezza, mantenendo, anche in questo caso invariata, la disposizione dell'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione

I mezzi di ricerca della prova

- I mezzi di ricerca della prova sono strumenti procedurali che rendono possibile acquisire cose materiali, tracce o dichiarazioni dotate di attitudine probatoria.
- La legge n. 48/2008 riporta la perquisizione, l'ispezione e il sequestro di ogni sistema o supporto informatico nell'ambito dei **mezzi tipici di ricerca della prova**.
- Costituiscono mezzi di ricerca della prova:
 - Le ispezioni;
 - Le perquisizioni;
 - I sequestri;
 - Le intercettazioni di comunicazioni

Mezzi di ricerca della prova

Ispezioni

- **L'ispezione** (art. 244 c.p.p.) consiste nel **descrivere, osservare e accettare** sulle persone, nei luoghi o nelle cose le tracce e gli altri effetti materiali del reato.
- Il codice di procedura penale distingue fra *l'Ispezione personale* (art. 245 c.p.p.) e *l'Ispezione di luoghi o cose* (art. 246 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 accettare le tracce e gli altri effetti materiali del reato** [c.p.p. 354, 364].
- 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***

Mezzi di ricerca della prova

La perquisizione

- **La perquisizione** è un atto diretto a ricercare il corpo del reato o cose pertinenti al reato sulle persone ed in luoghi determinati, ovvero ad arrestare l'imputato o l'evaso.
- La perquisizione può essere personale o locale (art. 247 c.p.p.)

Perquisizione informatica

Art. 247, 1bis

- **1-bis.** 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.

Richiesta di consegna

art. 248 c.p.p.

- 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 presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. In caso di rifiuto, l'autorità giudiziaria procede a perquisizione.**

Mezzi di ricerca della prova

Il sequestro

- Sotto il profilo dei mezzi di ricerca della prova il sequestro del corpo del reato e delle cose pertinenti al reato costituisce uno **strumento probatorio** necessario per l'accertamento dei fatti (art. 253 e ss.c.p.p.).
- Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo. E' disposto con decreto motivato dell'autorità giudiziaria.

Sequestro di corrispondenza

Art. 254 c.p.p.

- 1. *Presso coloro che forniscono servizi postali, telegrafici, 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. “Omissis”

Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni

Art. 254bis c.p.p.

- *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.*

Dovere di esibizione e segreti

Art. 256 c.p.p

- 1. Le persone indicate negli articoli 200 (segreto professionale) e 201 (segreto d'ufficio) 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.

Custodia delle cose sequestrate

Art. 259 c.p.p.

- 1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. **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. 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. “Omissis.

Apposizione dei sigilli alle cose sequestrate.

Cose deperibili - Art. 260 c.p.p.

- 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.
- Omissis. *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.*
“Omissis”

Mezzi di ricerca della prova

Intercettazioni di conversazioni o comunicazioni

- L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazioni costituisce un mezzo di ricerca della prova che consente di acquisire copia del contenuto di comunicazioni fra due o più soggetti (artt. 266 e ss. c.p.p.).
- Essenziale il rispetto dei limiti oggettivi stabiliti dalla legge in osservanza dei diritti inviolabili di libertà e di segretezza della corrispondenza e di ogni altra forma di comunicazione stabiliti dall'art. 15 della Costituzione.

Intercettazioni di conversazioni o comunicazioni (2)

- Per il grado di invasività nella vita delle persone è ammessa solo per specifici reati, fra cui
 - delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore a cinque anni;
 - delitti contro la pubblica amministrazione per i quali è prevista la reclusione non inferiore nel massimo a cinque anni;
 - delitti concernenti sostanze stupefacenti o psicotrope;
 - delitti concernenti le armi e le sostanze esplosive;
 - delitti di contrabbando;
 - reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono;
 - delitti previsti dall'art. 600-ter terzo comma, c.p., relativi alla pornografia minorile, anche nella forma virtuale;
 - reati di commercio di sostanze alimentari nocive, reati in materia di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli o disegni, introduzione nello Stato e commercio di prodotti con segni falsi, frode nell'esercizio del commercio, vendita di sostanze alimentari non genuine, contraffazione di indicazioni geografiche o denominazione di origine di prodotti agroalimentari
 - Atti persecutori (stalking)
 - Associazioni criminali

Intercettazioni di conversazioni o comunicazioni

Le intercettazioni ambientali (3)

- Nei procedimenti relativi ai reati indicati all'art. 266, nonché a quelli commessi mediante l'**impiego di tecnologie informatiche o telematiche**, è consentita l'**intervento e l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici, ovvero intercorrente fra più sistemi** (art. 266 bis c.p.p.).
- L'intervento e l'intercettazione di comunicazioni fra presenti è consentita negli stessi casi in cui è consentita l'intervento e l'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazioni che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. (Art. 266 c.p.p.)
- Tuttavia, qualora queste avvengano nei luoghi indicati dall'art. 614 c.p., che tutela il domicilio e i luoghi in cui si svolge la vita privata della persona, l'intervento e l'intercettazione è consentita solo se vi è fondato motivo di ritenere che in quel luogo si stia svolgendo l'attività criminosa (Art. 266 c.p.p.), fatto salvo si proceda per gravi delitti compiuti da pubblici ufficiali.

Attività a iniziativa della polizia giudiziaria

Perquisizioni Art. 352 c.p.p.

- 1.Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.
- 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. "Omissis"**

Attività a iniziativa della polizia giudiziaria

Acquisizione di plichi o di corrispondenza

Art. 353 c.p.p.

- 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. (2)

Attività a iniziativa della polizia giudiziaria

Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro Art. 354 c.p.p.

- 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. (1) “Omissis”

Il Codice Privacy, le normative in materia di conservazione dei dati di traffico telefonico e telematico

- **Art. 132. Conservazione di dati di traffico per altre finalità**
 1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.
- **1-bis.** I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. Omissis

Art. 132 Codice privacy, le modifiche apportate dalla legge 48/2008

- 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, (...), **possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive** previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, **può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.**

Art. 132 Codice privacy, le modifiche apportate dalla legge 48/2008

- *4-quater.* Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter **deve ottemperarvi senza ritardo**, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. **Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità.** In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.
- *4-quinquies.* I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

Digital Forensics

Giurisdizione e luogo di consumazione nei reati informatici

Giurisdizione applicabile e luogo di consumazione dei reati informatici

- Il *locus commissi delicti* nei reati informatici costituisce un argomento altamente critico, essendo i reati informatici, per loro stessa natura, caratterizzati dalla delocalizzazione, dalla difficoltà di individuare dov'è stata realizzata la condotta e dove si è realizzato l'evento.
- Possono generarsi, infatti, conflitti di sovrapposizioni di giurisdizioni derivanti dalla difficoltà di individuare univocamente il luogo di consumazione del reato con conseguenti lungaggini nella concreta ed efficace perseguitabilità dei reati *on line*.
- Le tecnologie di cloud computing rendono ancora più problematici gli aspetti correlati all'individuazione univoca della giurisdizione applicabile

Giurisdizione applicabile e luogo di consumazione dei reati informatici

- Necessità di un coordinamento a livello nazionale e internazionale, compresa la previsione di strumenti di assistenza giudiziaria internazionale.
- La convenzione di Budapest stabilisce una serie di misure a livello investigativo intese a coordinare gli sforzi delle forze di polizia nel settore dei reati informatici.
- La convenzione di Budapest stabilisce che gli Stati interessati debbano avviare consultazioni “al fine di stabilire la competenza più appropriata per esercitare l’azione penale”
- Deve tenersi conto anche della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione

- 1. Gli Stati membri stabiliscono la propria competenza giurisdizionale relativamente ai reati di cui agli articoli da 3 a 8 (**Accesso illecito a sistemi di informazione, Interferenza illecita relativamente ai sistemi, Interferenza illecita relativamente ai dati, Intercettazione illecita, Strumenti utilizzati per commettere i reati, Istigazione, favoreggiamento, concorso e tentativo**) quando il reato sia stato commesso:
 - a) in tutto o in parte sul loro territorio; o
 - b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso.
- 2. Nello stabilire la propria competenza giurisdizionale conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora:
 - a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o
 - b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato.

La direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione - Articolo 12 Competenza giurisdizionale

- 3. Uno Stato membro informa la Commissione ove decida di stabilire la competenza giurisdizionale per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora:
 - a) l'autore del reato risieda abitualmente nel suo territorio; o
 - b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio.

Reati commessi nel territorio dello Stato

Principi di territorialità e di ubiquità

- Innanzitutto è necessario richiamare il nostro codice penale che all'art. 6 fissa, ai commi 1. e 2. i principi di territorialità e di ubiquità, stabilendo che:
- 1. comma "*Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana*"
- 2. comma "*Il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è verificato l'evento che è la conseguenza dell'azione od omissione*"
- Gli articoli 7 (*Reati commessi all'estero*), 8 (*Delitto comune dello straniero all'estero*) e 9 (*Delitto comune del cittadino all'estero*) indicano diversi criteri suppletivi che finiscono per temperare il principio della territorialità.

Luogo di consumazione del reato e cloud computing

- Le tecnologie di cloud computing, caratterizzate da condivisione, scalabilità delle risorse, delocalizzazione dei data center pongono rilevanti problemi in ordine all'intervento e alla perseguitabilità degli illeciti penali compiuti in ambiente cloud.
- L'offerta di grandi opportunità sotto il profilo produttivo, conoscitivo e informativo che il cloud offre, mostra, per contro e acuisce, aspetti critici con riferimento alla riservatezza, alla tutela dei dati personali, ai diritti di proprietà intellettuale, alla sicurezza dei dati e dei sistemi.
- il principio da cui partire non può che essere quello di territorialità, integrato dai criteri suppletivi e dal ricorso ad accordi internazionali

Luogo di consumazione del reato

Cass. SS.UU. sent. n. 17325/2015

- La condotta illecita compiuta in ambiente informatico assume specifiche peculiarità rispetto alla tradizionale nozione di ambiente fisico imponendo una rivalutazione che abbia riguardo all'ambiente virtuale nel quale la condotta criminale effettivamente si colloca.
- Non è agevole individuare con certezza una sfera spaziale suscettibile di tutela in un ambiente telematico, che opera e si connette ad altri terminali mediante reti e altri protocolli di comunicazione
- Deve essere superato il concetto classico di fisicità del luogo a favore della teoria basata sul funzionamento delocalizzato all'interno della rete di più sistemi informatici e telematici e su questa base valutare, quale luogo di consumazione del reato, quello in cui la condotta o l'omissione che costituisce il reato, si sono realizzate.

Luogo di consumazione del reato

- Sentenza Cassazione penale 26 marzo 2015 "il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente".
- Può costituire un valido criterio anche nell'ambito dei contratti di fornitura di servizi cloud.
- (Cassazione Penale, n. 10354 del 05.02.2020-17.03.2020, Sez. 2 - Reato di frode informatica: (Cassazione Penale, n. 10354 del 05.02.2020-17.03.2020, Sez. 2) »*Il collegio condivide la giurisprudenza secondo cui il reato di frode informatica (art. 640 ter cod. pen.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Anche la frode informatica si consuma, pertanto, nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui»*