

26 Maggio 2023

Digital Forensics

Esame: 3 domande aperte scritte

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.

- Leone Lattes (1887–1954), lo scienziato italiano pioniere nello studio della Forensic Serology che nel 1916 scoprì i diversi gruppi sanguigni
 1. 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

2. 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

- 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:

1. Un dispositivo di memorizzazione digitale
 - a. PC, notebook, HD esterno, NAS, nastro, CD/DVD, memory card, USB drive, ecc.....
 - b. Cellulari, Smartphone, Smartwatch, Tablet, Navigatori, ecc...
2. Una rete (Intranet/Internet)
 - a. Traffico di rete
 - b. Email (client/server)
 - c. Web (client/server)
 - d. Social network
 - e. Chat/IM
 - f. 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 rinvenuto spento, l'accensione comporta modifiche al sistema e/o ai dati in esso contenuti
- Se il dispositivo è connesso a Internet o a 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

I dati digitali possono essere divisi in due categorie principali:

1. 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
2. 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.)

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:

1. Crimini il cui scopo è attaccare una risorsa di rete
 - Virus, malware, attacchi mirati, DoS, DDoS, ecc.
2. Crimini che vengono perpetrati utilizzando i computer in rete per effettuare frodi online, furti d'identità, furti della proprietà intellettuale, cyberbullismo, cyberstalking, cyberwarfare, ecc.

Gli attori principali sono:

- Il soggetto che commette il crimine
- Tool per commettere il crimine
- Target del crimine (vittima)
- Materiale (informazione) potenzialmente appetibile

Chi sono i cyber criminali

Sono criminali singoli o organizzati spesso privi di particolari competenze tecniche.

Gli obiettivi sono:

- Ottenere 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'anonymizzazione che la rete offre, rendono il Cyber Crime un'attività relativamente semplice e profittevole...

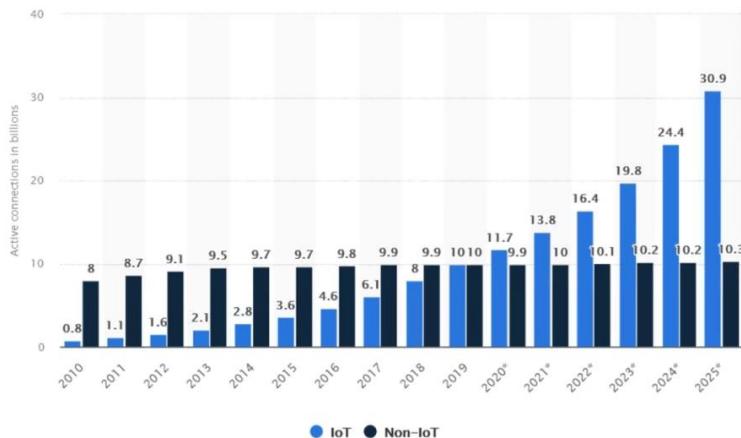
L'hacker è sempre cattivo?

- **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

E' un 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.

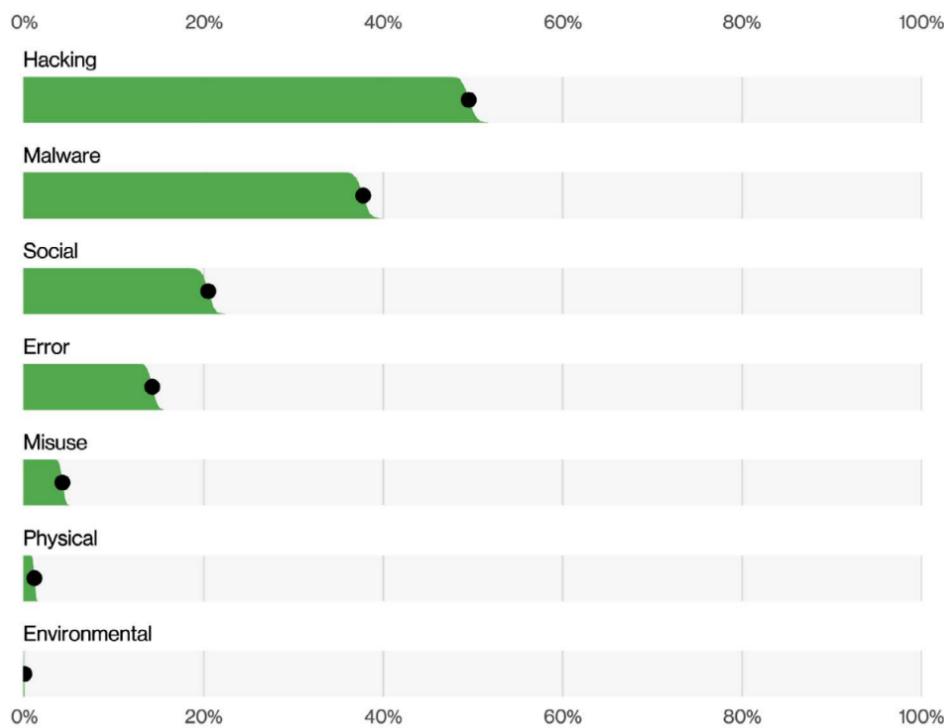
- Lloyd's Assicurazioni ha stimato i danni causati da attacchi informatici in circa 450 miliardi di dollari all'anno (include sia i crash di sistema che i costi di ripristino).
- Juniper Networks valuta che il costo mondiale per la perdita di dati sensibili di aziende e cittadini si attesta su una cifra superiore a 1,2 trilioni di dollari.

È possibile visualizzare tali dati sul sito www.statista.com

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

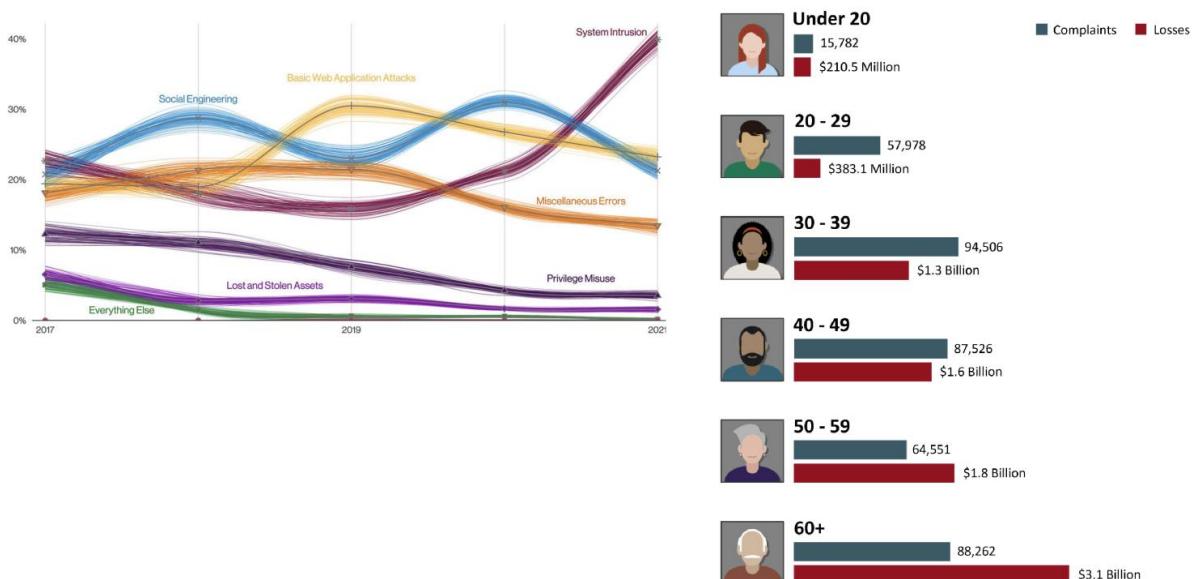


Principali azioni che hanno comportato un data breach (2008-2022)

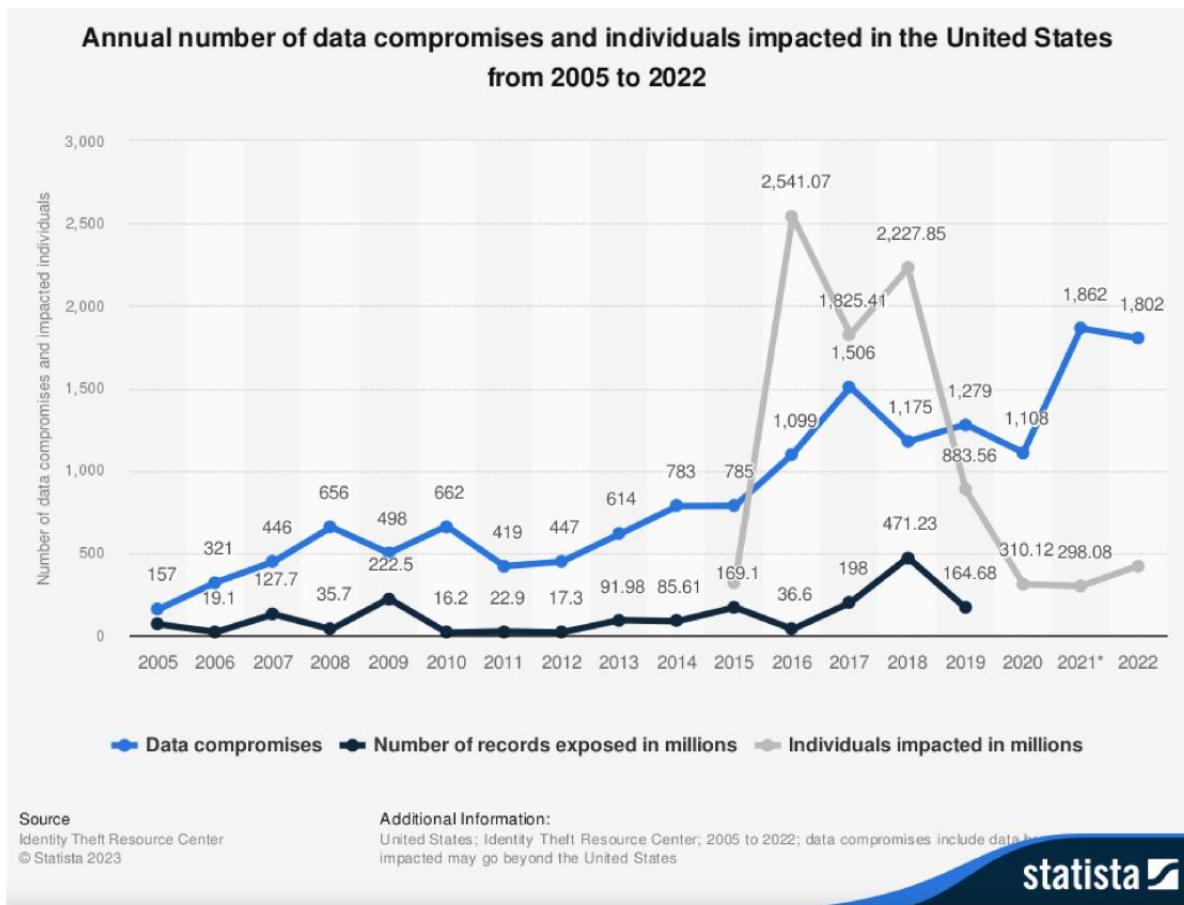


Data breaches (violazione dei dati)

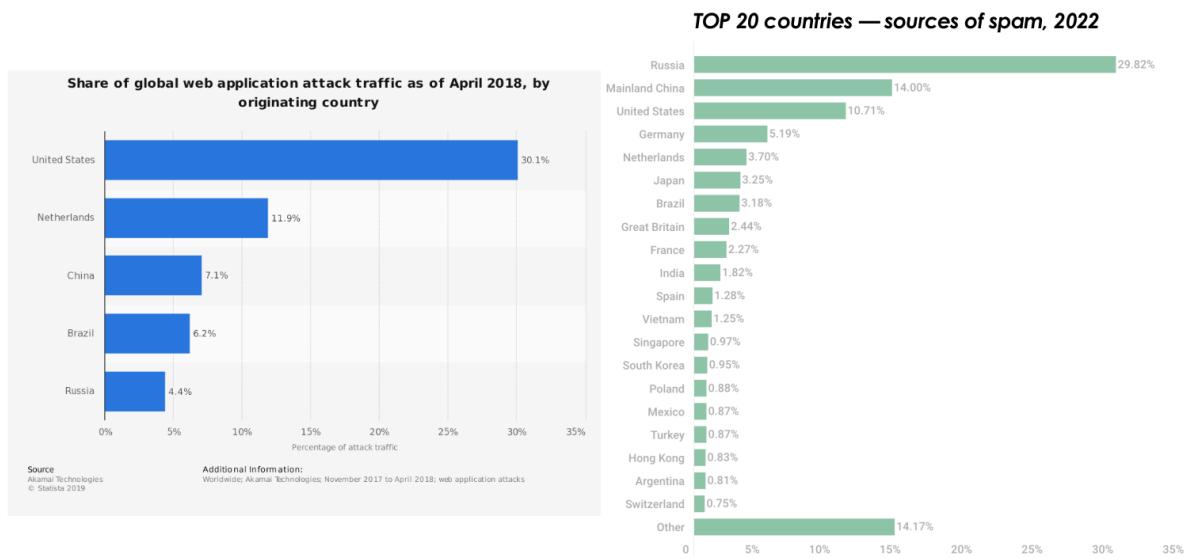
2022 - VICTIMS BY AGE GROUP¹⁷



Andamento data breaches negli USA



Paesi di origine degli attacchi e spam



Ingegneria sociale

L'ingegneria sociale è utilizzata in maniera malevola per indurre la vittima a condividere informazioni private.

L'ingegneria sociale è utilizzata per cercare di manipolare una persona, al fine di instaurare un rapporto di fiducia e indurla a condividere le sue informazioni private. Si rischia di diventare vittima dell'ingegneria sociale tutte le volte che apriamo un link all'interno delle e-mail che riceviamo senza controllare attentamente il nome del mittente; oppure quando divulgiamo le nostre informazioni personali nelle e-mail.

L'ingegneria sociale consiste nell'utilizzo di metodi "non tecnici" da parte di un malintenzionato per ingannare una potenziale vittima, facendole condividere informazioni personali quali, per esempio, password, dati relativi al conto bancario e altre informazioni personali.

L'ingegneria sociale è una forma di hacking che si rivolge alle persone sfruttando la natura umana e le debolezze nel prendere decisioni. Gli ingegneri sociali utilizzano la manipolazione per ottenere l'accesso ai vostri dati e alle vostre risorse.

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

- **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 (baiting), 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), Lo scam nigeriano è una classica truffa già nota negli anni '90 nella quale un sedicente principe nigeriano (da qui il nome) contatta via posta delle persone a caso affermando di avere la necessità di spostare grandi quantità di denaro all'estero, facendolo però in maniera discreta. Si chiede quindi di potersi appoggiare al conto in cambio di una grossa percentuale sul denaro spostato, che è solitamente nell'ordine dei milioni di euro. Cosa succede agli sprovveduti che abboccano? I truffatori iniziano a chiedere denaro per fantomatiche parcelli di avvocati, di notai, e proseguono sino a che la vittima smette di pagare o si rende conto di essere stata truffata.
 - programmi crackati
 - unità USB abbandonate!
- **Scareware:** individua una classe di software dannosi o comunque di limitata utilità la cui installazione viene suggerita agli utenti attraverso tecniche di marketing scorretto o mediante i metodi dell'ingegneria sociale. Oggi vengono più comunemente riuniti sotto la classe di malware nota come Rogueware o FraudTool.
 - avviso dalle forze dell'ordine con accusa di un crimine (es. possesso di materiale pedopornografico)
 - avviso da parte del supporto tecnico di presenza di minaccia malware 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

Cyber Crime - 2 attacchi importanti: Dyn e Wanna Cry

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

Cyber Crime: Dyn attack

Dyn nasce nel 2001 a Manchester come società di tipo DNS Provider. Il 21 ottobre 2016 il servizio di DNS viene attaccato per ben 3 volte

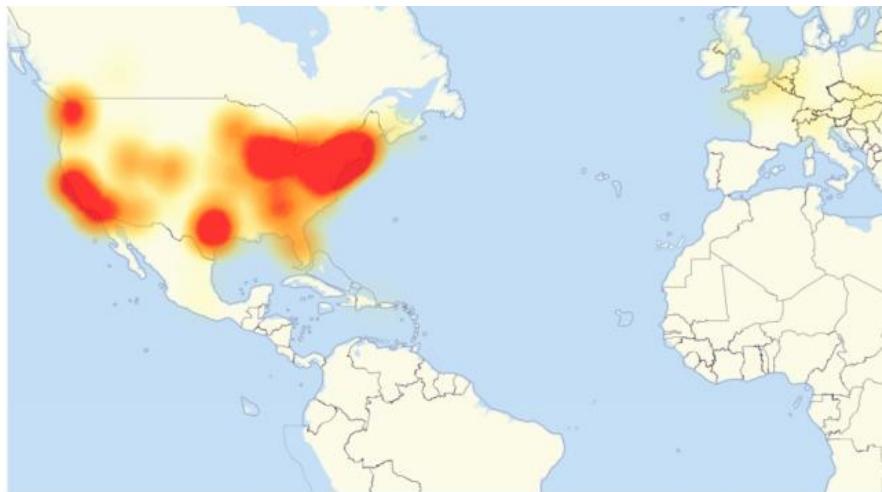
- Diventa Registrar nel 2004 e dal 2009 inizia ad acquisire grossi clienti, come Twitter, Netflix, Microsoft, Amazon, Time Warner, BBC, CNN, PayPal, ecc.
- Dal 2010 al 2014 si lancia anche nei servizi Email, di monitoraggio e analisi dei dati
- Nel 2016 viene acquistata da Oracle
- Sempre nel 2016 ha subito un 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.)

Sono stati 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/rakko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleanccs.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=9386.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9386.0
666666/666666	Dahua IP Camera	http://www.cleanccs.com/router-default/Dahua/DH-IPC-HD7V4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forum/threads/reset-root-password-plugin.101148/
root/zfix	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/hc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/h3518	HiSilicon IP Camera	https://acasias.wordpress.com/2014/08/10/got-a-new-h3518-ip-camera-module/
root/kiv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd6bab4773ff047356198c781f27d
root/kiv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd6bab4773ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd6bab4773ff047356198c781f27d
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/mesmism	Mobotix Network Camera	http://www.forum.usenet.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:Wt1phozQ7URUJ.community.freepbx.org/t/voip-atlas-phones/4111
root/000000000	Panasonic Printer	https://www.experts-exchange.com/questions/28194355/Default-User-Password-for-Panasonic-CP-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/B00EB6ENDI
admin/smcaadmin	SMC Routers	http://www.cleanccs.com/router-default/SMC/ROUTER
root/kwb	Toshiba Network Camera	http://aq.surefiredynsupport.com/index.php?action=article&cat=4&id=8&lang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-mfh/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.ironbugs.com/2015/02/hack-and-patch-your-zte-f660-routers.html

Cyber Crime: Wanna Cry attack

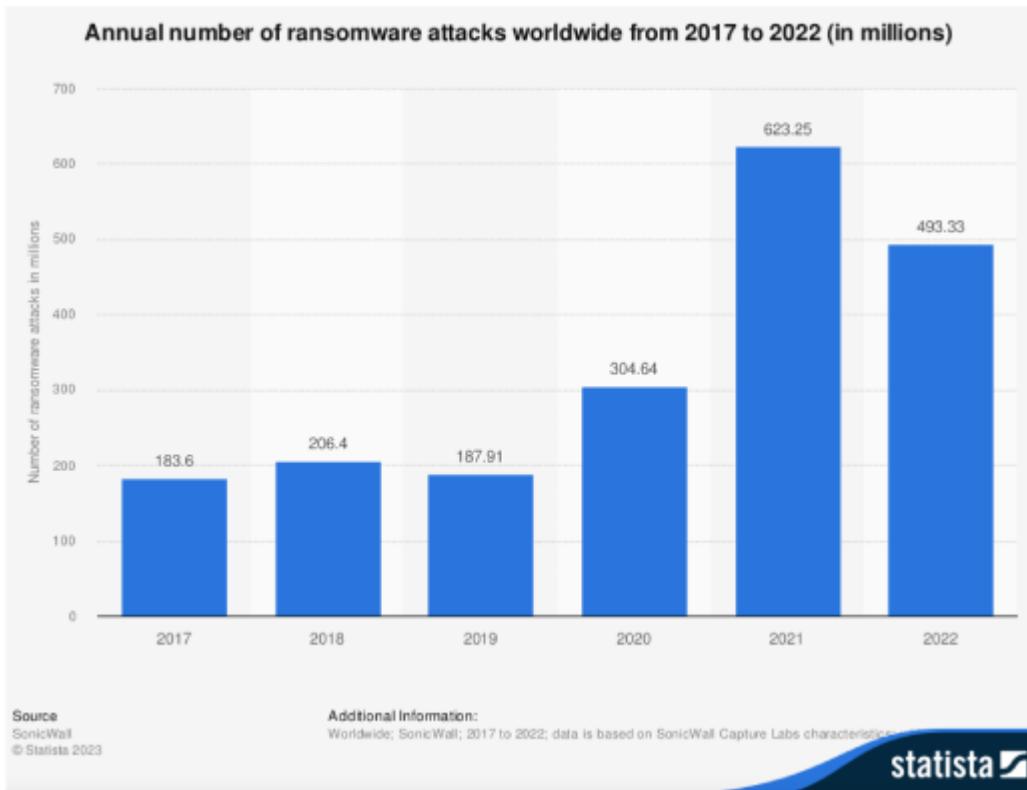
- **Ransomware Wanna Cry**
 - **Classe di malware** (MALicious softWARE) che rendono inaccessibili, mediante cifratura, i dati dei computer infettati e dove viene richiesto il pagamento di un riscatto (ransom) per ripristinarli, tipicamente in bitcoin
 - Nati in Russia, si sono diffusi rapidamente in 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 cifrare 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

Diffusione degli attacchi ransomware



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, era una materia assolutamente interdisciplinare.

Iter formativo suggerito:

- Laurea in ingegneria informatica o in informatica (o anche altre equivalenti quali, p. 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

- 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
 - a. 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.
 - b. Il consulente può essere autorizzato dal Pubblico Ministero ad assistere a singoli atti di indagine.
- Art. 360 CPP - Accertamenti tecnici non ripetibili
 - c. 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

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!”

9 Giugno 2023

REQUISITI PER LA GESTIONE DELL'EVIDENZA DIGITALE

Requisiti per la gestione dell'evidenza digitale: PAROLE CHIAVE

Il valore della prova digitale è la sua capacità di resistere alle contestazioni del giudice e della controparte.

Per avere valore probatorio, la prova digitale deve soddisfare 6 requisiti.

- **Rilevanza:** “Deve essere possibile dimostrare che il materiale acquisito è rilevante per l'inchiesta”, la prova deve fornire al giudice le informazioni che permetteranno al giudice di decidere la colpevolezza o l'innocenza.
- **Sufficienza:** “Deve essere raccolto abbastanza materiale per consentire lo svolgimento di una corretta indagine”, ma il materiale non deve essere superfluo.
- **Verificabilità:** “Le attività svolte nell'investigazione 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”. È necessario poter dimostrare che le scelte fatte nella gestione della prova nelle varie fasi sono state le migliori possibili.

- **Ripetibilità:** se uno stesso analista, ripetendo in tempi diversi lo stesso processo di elaborazione dati, ottiene lo stesso risultato. Quindi è ripetibile 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
- **Irripetibilità quando:**
 - indifferenziabilità [?] (nel caso di inerzia, la prova va perduta - per esempio dei dati che passano sulla rete, o li prendo in quel momento o non li prendo più);
 - non reiterabilità, cioè l'attività che si va a fare sulla prova comporta una modifica della prova e quindi non è più la stessa (prendo un campione di sangue sull'asfalto mentre piove)
-

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

- **Riproducibilità:** se un altro individuo con adeguate competenze tecniche è in grado di ottenere lo stesso risultato, anche cambiando una o più condizioni di misura. Cioè 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

In questo caso non viene richiesto che il risultato sia uguale bit a bit (se cambio software, per esempio, possono esserci differenze implementative, tipo il formato della data). L'importante è che l'informazione trasmessa sia la stessa.

Queste due criteri influiscono anche sulle tecniche di acquisizione e analisi:

- **Live Forensics** quando la prova non è ripetibile;
- **Post Mortem** quando la prova è ripetibile e quindi la Cassazione ha deciso che l'attività può essere fatta all'estrazione di un dato.

Le best practices

- 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”, cioè le buone pratiche che l'esperto deve seguire durante l'indagine affinché l'evidenza digitale mantenga i criteri di cui sopra.
 - Linee guida, procedure e metodologie per approcciare la prova digitale nella maniera più corretta
 - Un insieme di comportamenti non necessariamente formalizzati, ma che secondo la comunità scientifica sono il modo più corretto di operare.

Le best practice si dividono in 3 categorie.

- **Protocolli sviluppati da agenzie di controllo** —> hanno l'obiettivo di coniugare il 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 dagli associati:
 - 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 (siccome lo IETF sviluppa protocolli, è quasi obbligatorio seguirne le RFC)
 - 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 e applicabili a prescindere dal contesto normativo della singola nazione.
- Il documento è diviso in tre sezioni:
 - a. Principi guida da seguire durante il reperimento/acquisizione dell'evidenza (cosa fare e non fare, considerazioni sulla privacy e legali)
 - b. La procedura per l'acquisizione (trasparenza e riproducibilità della procedura)
 - c. La procedura di archiviazione (catena di custodia, archiviazione, strumenti utilizzabili)
- Le RFC sono pubbliche

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
- Sono a pagamento.
- **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
- **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
- **ISO/IEC 27042 — Guidelines for the analysis and interpretation of digital evidence**
 - Offre una guida sul processo di analisi e interpretazione delle prove digitali
 - Fornisce indicazione 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)
- **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

La Digital Forensics prevede le seguenti fasi:



1. Identificazione: l'investigatore cerca di ottenere le info di base per capire l'entità dell'incidente. Si esaminano le aree di interesse del crimine, dove potrebbero essere contenute prove. Si identifica quali dati e informazioni possano costituire la [...].
2. Acquisizione e conservazione del materiale necessario all'indagine, che sarà messo al sicuro in previsione delle fasi successive.
3. Analisi, in cui i fatti vengono correlati tra loro per dimostrare o meno la veridicità dei fatti.

4. Presentazione e valutazione delle prove e dell'evidenza digitale, da fare al giudice o a chi commissionato l'indagine. Comporta la compilazione dei report.

Ciclo di vita della Digital Forensics —> le macroattività che costituiscono tutto il ciclo di vita del dato nell'ambito dell'analisi forense.



La cristallizzazione è il processo più delicato, che congela i dati contenuti nel sistema esaminato, in modo che vi possano essere attribuiti quanto più possibile le caratteristiche richieste dalle norme internazionali.

Il processo di cristallizzazione deve essere affiancato da:

- catena di custodia, che indica in ogni momento chi sta gestendo il dato;
- reportistica in cui sono dettagliate le attività svolte (per assicurarne la verificabilità e la giustificabilità).

Analisi preliminare

È il processo investigativo sempre necessario, per qualsiasi indagine. Viene svolta una valutazione del caso (**perizia**) al fine di identificare il crimine e dove potrebbe essere localizzata la prova.

Deve essere svolta in modo sistematico, per rilevare tutte le evidenze a supporto o discapito della tesi.

Le investigazioni sono condotte su due tipologie di sistemi:

- Quelli utilizzati per commettere il crimine
- Quelli eventualmente bersaglio del crimine

Soltanamente inizia con un incontro preliminare con la Polizia Giudiziaria e/o il PM, aiuta a capire la natura e l'entità dell'indagine e 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»

Questo è molto chiaro come quesiti, i seguenti invece non lo sono.

- «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**»
- «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 capire 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

1. Definizione della struttura organizzativa



2. Pianificazione e allocazione delle risorse

Allocazione del personale e degli strumenti necessari:



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



Individuare **gli esperti forensi** digitali



Assegnare **attrezzature** e strumenti adeguati



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

3. Stesura del contratto di ingaggio

- Stabilisce un compenso sulla base del servizio offerto
- Implica un accordo su:
 - L'obiettivo della richiesta
 - Le tempistiche (non può superare i 18 mesi - 2 anni, per i reati gravi) 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

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**. Bisogna ridurre la possibilità di compromissione.

Una fase tecnica, non semplice e importante.

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

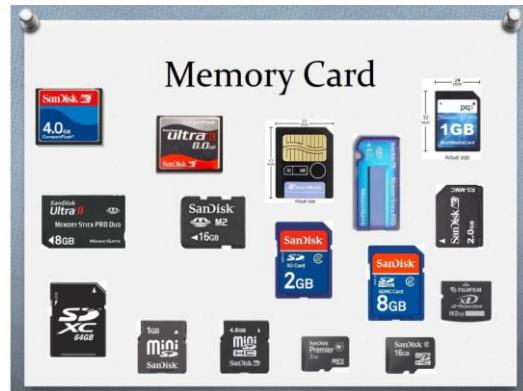
- Non esistono **strumenti per l'identificazione di queste fonti di prova**
- Sta **nell'esperienza e meticolosità dell'investigatore** far emergere le casistiche
- Stanno inoltre emergendo figure nuove, di esperti specifici in mobile forensics, cloud forensics... via via che si evolvono le tecnologie di storage dei dati.

Elementi in grado di memorizzare dati:

Supporti magnetici e ottici



Altri dispositivi



... e non sono sempre facili da individuare



Riconoscimento della prova: Dove cercare?

Una volta individuato il supporto (o i supporti) occorre capire **dove** cercare.

Occorre prendere in considerazione i **diversi elementi** che concorrono al funzionamento del **Sistema Informatico**:

1. Tipologia del **Sistema Informatico** (definisce il principale utilizzo del dispositivo, che determina l'approccio da tenere nella ricerca).
 - 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
2. Tipologia del **Sistema Operativo**
 - È il cuore del Sistema Informatico e determina il tipo e il formato di file gestiti.
 - Il S.O., nel corso del suo funzionamento, registra diverse info in appositi file, salvati in posizioni note del filesystem.
 - Permette di:

- a. Identificare le **zone di memoria** dove cercare i dati
- b. Tracciare l'uso del computer da parte dei **diversi utenti** ivi definiti
- c. Le **periferiche** che sono state collegate
- d. Individuare l'elenco dei **file stampati** e su quale stampante
- e. Identificare **le reti** (tradizionali o Wi-Fi) cui il computer è stato collegato
- f. Ecc.

3. Tipologia del **file system**

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

4. Tipologia di **file**

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

5. Presenza e **tipologia di interfacce**

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



- Occorre materiale di supporto, in cui la digital evidence può esistere.
- **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", in particolare per la tutela della riservatezza dei dati personali, anche rispetto al trattamento del dato durante l'indagine e dall'autorità.
Le intercettazioni sono richieste dal PM e autorizzate dal GIP. Vengono effettuate dalla polizia giudiziaria. Teoricamente, salvo eccezionali ragioni, gli impianti per le intercettazioni devono essere installati negli uffici della procura della Repubblica.
- Oss: non è tanto la raccolta del dato a rappresentare un rischio per la riservatezza, quanto la violazione delle corrette regole di gestione del dato. Solo una corretta relazione tra raccolta, trattamento, utilizzo e finalità della raccolta garantiscono una garanzia della tutela di tutti gli interessi coinvolti.
- Attenzione in particolare ai dati sensibili, che non devono essere acquisiti.
- Vengono utilizzate delle **sonde**
 - in grado di memorizzare le comunicazioni che avvengono con il sistema sospetto
 - collegate a specifici punti della rete ed interfacciate con diversi tipi di canali di comunicazione

- TAP (Test Access Port), detti anche “rubinetto”, dispositivi HW inseriti a T nelle reti informatiche. Permettono il monitoraggio non invasivo del flusso dei dati, perché riceve lo stesso flusso dati del settore in cui è posto e lo copia su una terza porta.
 - Si connette in pochi secondi
 - È trasparente alla rete
 - Virtualmente invisibile a livello 2
 - Non ha indirizzo IP o MAC
 - Non introduce distorsioni o perdite
- 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 (anche microfoni, videocamere...)
- Attualmente, la convergenza sul protocollo IP fa sì che si possa usare la medesima architettura sia per le intercettazioni telefoniche sia per quelle informatiche.

Acquisizione del dato: Sequestro

- È una attività di Polizia Giudiziaria, disposto con decreto motivato. Quando non è possibile un intervento tempestivo della polizia giudiziaria, è consentito di sequestrare i beni, prima che si disperdano nell'attesa dell'intervento del PM.
- Ne esistono due tipi:
 - preventivo
 - conservativo
- Comportano un vincolo di indisponibilità dei sistemi, per evitare si possa pregiudicare il procedimento.
- Ciò viene messo sotto sequestro è il documento informatico contenuto nel dispositivo, non per esempio il pc, l'hard disk.
- Il sequestro deve protrarsi solo per il tempo necessario all'estrazione della copia dei dati (codice procedura penale).
- Nel caso di persone soggette a segreto d'ufficio non si può procedere al sequestro e in questo caso, quindi, il giudice chiede formalmente di consegnare il materiale al soggetto, che può scegliere i documenti con dati non rivelabili.
- Il sequestro si può fare anche presso fornitori di servizi informatici e telematici, per esempio tabulati IP, posta certifica, file di log, accessi a pagine web. Si fa attraverso copia su adeguato supporto.
- Il custode dei dati è informato dell'obbligo di impedire l'alterazione e l'accesso da parte di terzi, salvo diverse disposizioni da parte del giudice. Deve eventualmente avvisare il giudice in caso di situazioni di pericolo che possono occorrere.
- Il sigillo può essere foto, riproduzioni da mettere agli atti. Sul server una firma digitale, su una pagina web, la rimozione della rete.
- 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** a meno 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”

16 Giugno 2023

Acquisizione del dato: Attività live e post mortem

Le Best Practice contengono anche delle considerazioni sulla privacy: occorre rispettare i regolamenti e la giurisdizione di competenza sulla privacy e non intromettersi nella privacy delle persone (non acquisire informazioni personali non attinenti)

- 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 (se non lo si conosce, non si può effettuare un'analisi live, poiché si andrebbe a effettuare modifiche sul sistema.
Occorre quindi avere piena conoscenza di quello che si sta facendo.)
 - Strumenti disponibili
 - Rilevanza dei dati rispetto all'indagine

Acquisizione del dato e priorità

È necessario elaborare un piano di acquisizione dei dati, che tenga conto del valore dell'informazione in campo probatorio.

Per assegnare la priorità occorre tenere conto dei seguenti aspetti:

- **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

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. (che eventualmente devono essere analizzati prima di altri dati, come quelli sulla memoria del disco)
- Siamo in presenza di volumi/partizioni/file cifrati (FileVault, BitLocker, TrueCrypt, ecc.)

Le tecniche di “live forensics” hanno come contro:

- Il sistema viene alterato. Bisogna chiedersi:
 - 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

Nel caso in cui si effettui la Live Forensics, con un sistema in Stand-by o acceso.

- Se il sistema è accessibile:
 - Si accede, con login o senza
 - Si verifica la presenza di processi attivi e dischi cifrati “montati”
 - Si estraggono i dati dal disco prima che venga spento
 - Si acquisiscono dati relativi allo stato del sistema e degli utenti mentre le attività sono in corso
 - Si può fare memory dump per salvare le info contenute in memoria
- Se il sistema NON è accessibile:
 - Utilizzare tecniche di «hacking» per ottenere l’accesso
 - Se è necessario spegnere il sistema, lo si fa rimuovendo la fonte di alimentazione elettrica da parte del dispositivo

Acquisizione del dato: Post Mortem

- Mettere in sicurezza la scena (nessuno deve avvicinarsi ai dispositivi)
- Allontanare le persone presenti dai dispositivi digitali
- Fotografare o fare una ripresa video della scena del crimine
- Assicurarsi che il sistema da esaminare sia effettivamente spento
- **NON ACCENDERE IL COMPUTER PER NESSUN MOTIVO!!**
- Rimuovere la batteria
- Collegare l’alimentazione
- Etichettare le porte e i cavi
- Assicurarsi che tutti 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

Si possono fare entrambi i tipi di analisi.

Acquisizione del dato: Attività live e post mortem



a.a. 2022/2023

Digital Forensics

11

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)
- La copia bit a bit è un'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

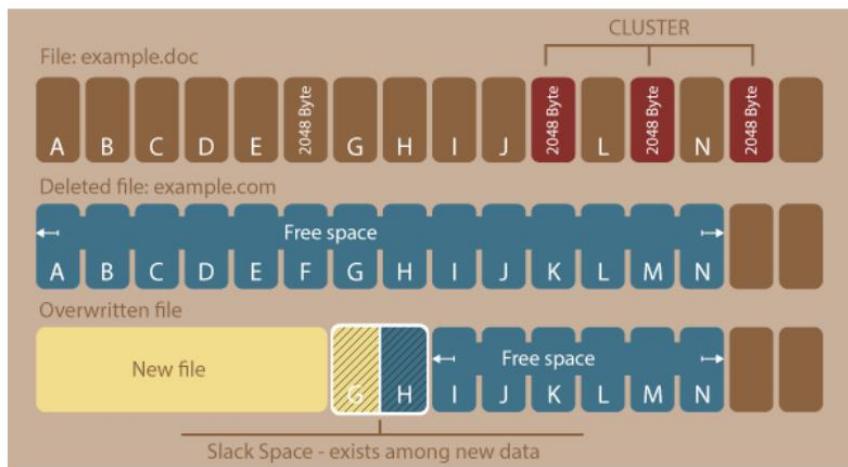
Slack space

Quando un file viene cancellato, non vengono davvero cancellati i dati, ma semplicemente non viene più referenziato dal sistema operativo.

Esempio in figura: il file example.doc si trova nei blocchi nell'immagine. Quando lo si cancella, il sistema rende quello spazio disponibile e quindi sovrascrivibile. Se viene scritto un nuovo file in quelle zone di memoria, che è più piccolo del cancellato, solo alcuni dei blocchi vecchi vengono sovrascritti.

Quindi è possibile individuare dei pezzi di informazioni (con un'analisi forense) che potrebbero essere disponibili sul disco. Potrebbero anche essere cose molto vecchie. Succede soprattutto ora che i dischi hanno una dimensione molto ampia. L'analisi dello slack space è una delle cose principali che va fatta nell'analisi forense.

Il pezzo del file "rimasto" ovviamente non si può aprire con word, al massimo con un editor di testo. Se il file è binario c'è bisogno di un tool per tradurlo.



Copia Forense Duplicatori e Write Blocker

I duplicatori servono a copiare i file a livello molto basso.



Acquisizione del dato: Buone norme

- Pulizia del supporto utilizzato per la copia (va effettuato il data wiping)
- Occorre validare la copia e verificarne l'integrità (hashing)
- Si tenga conto degli aspetti temporali
 - **Timestamp:** apporre una marca temporale della data nella quale è stata effettuata l'operazione

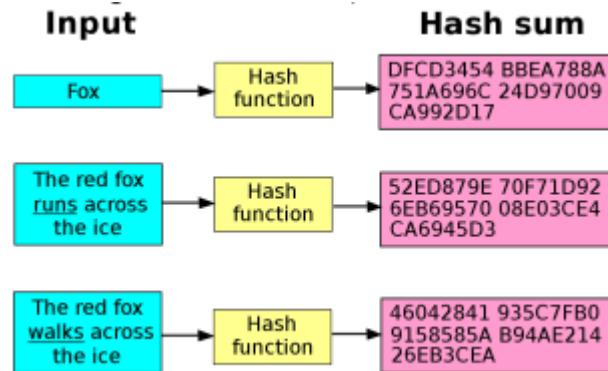
- **Timeline:** deve essere definita la sequenza in cui le azioni/eventi di cui si è trovata traccia si sono verificate
- **Scostamento temporale con gli orologi informatici:** verificare che il sistema esaminato abbia un orario congruo (verificare l'ora del BIOS, o del SO). In caso negativo, annotare lo scostamento
- **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:
 - 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...



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:

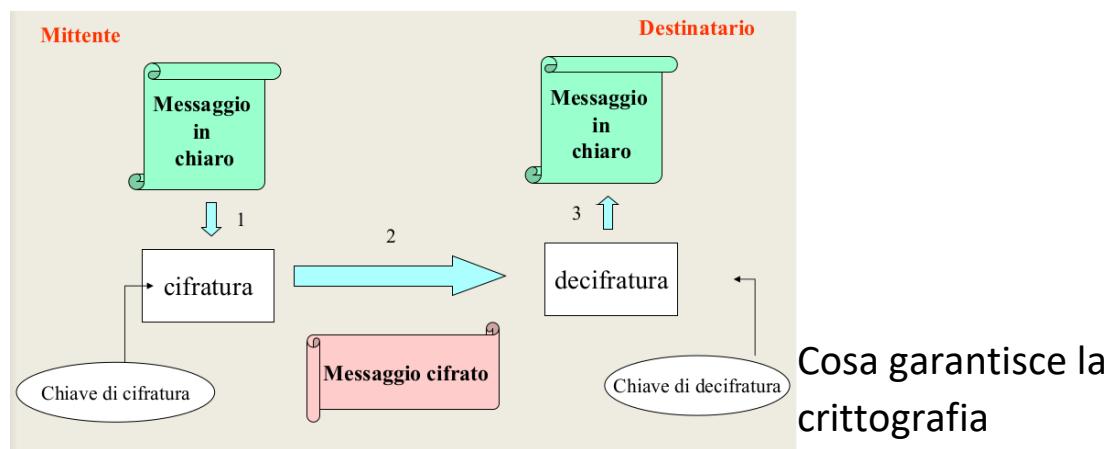
- MD5 (128 bit)
- SHA-1 (160 bit)
- SHA-256 (256 bit)
- SHA-512 (512 bit)

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



Algoritmi a chiavi simmetriche

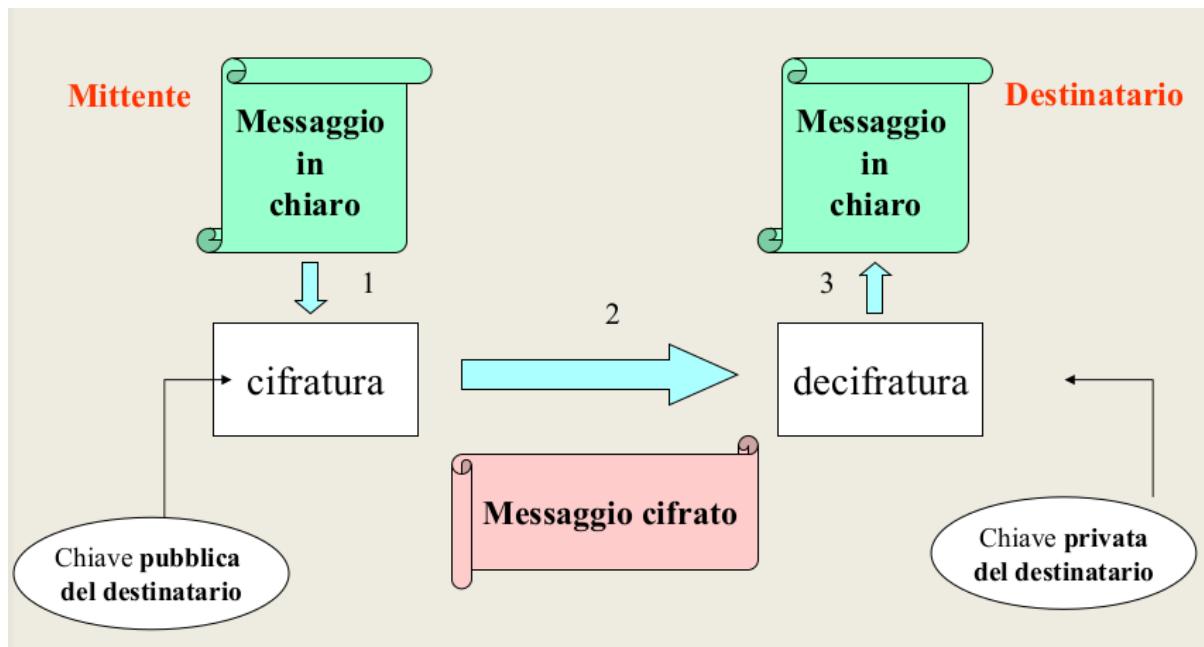
- Chiave di cifratura e chiave di decifratura uguali
- Riservatezza, integrità, autenticità garantite dalla segretezza della chiave
- Vantaggi:

- 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
 - ...

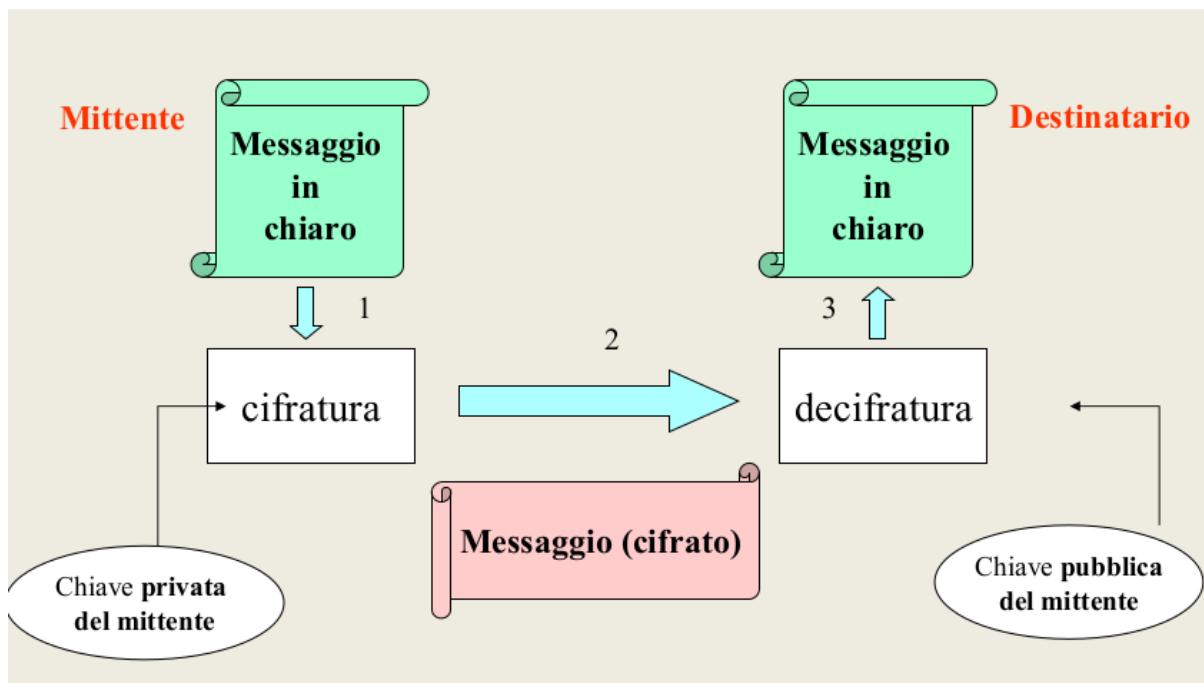
Algoritmi a chiavi asimmetriche

- 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

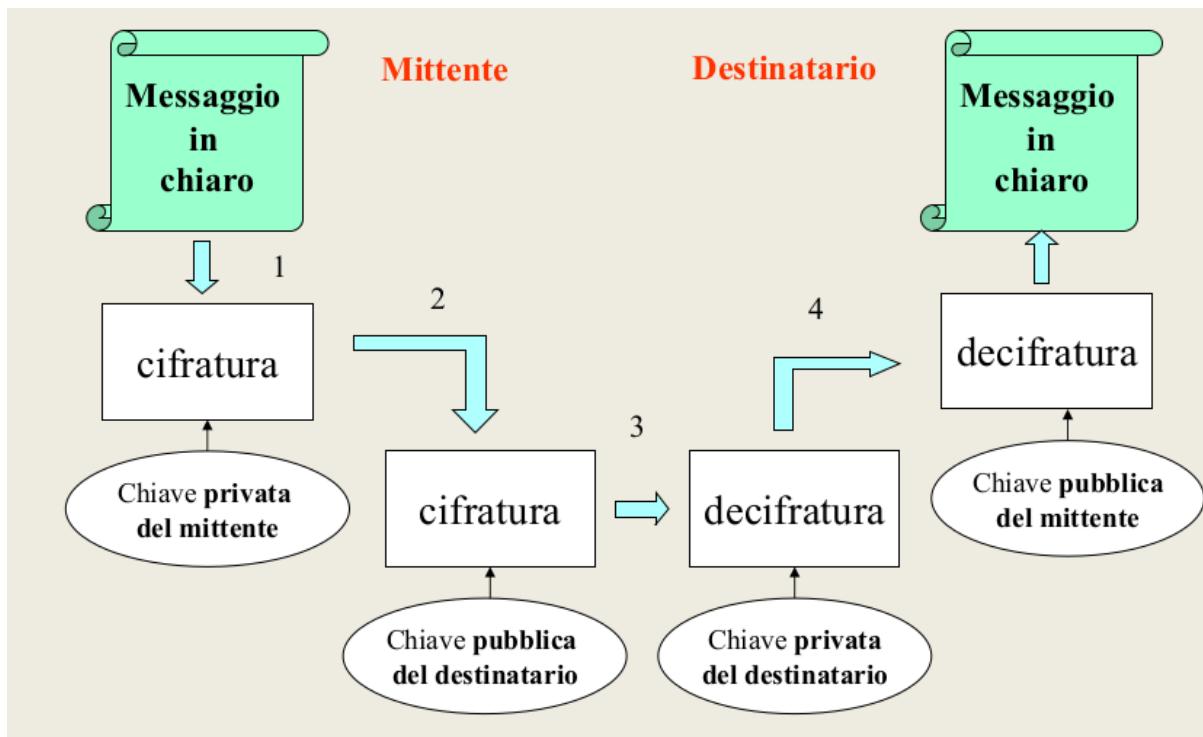
Riservatezza di un messaggio



Autenticità e integrità



Autenticità e riservatezza



Generazione della firma

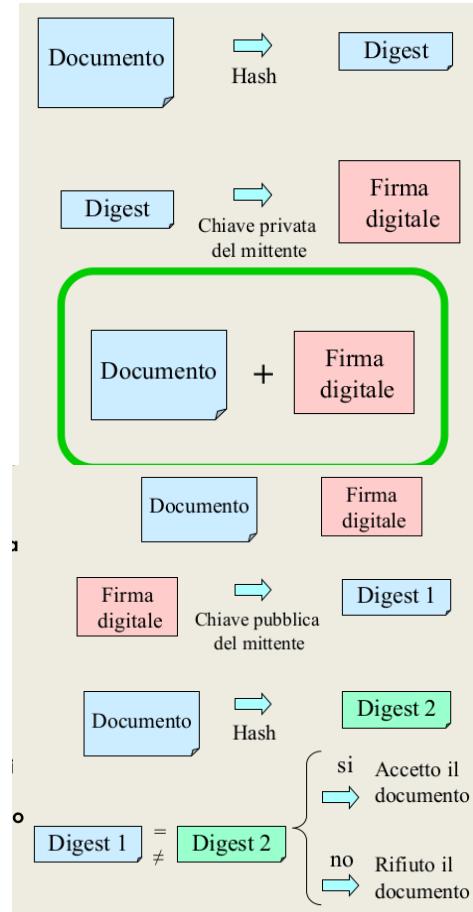
- Calcolare il DIGEST del documento
- CIFRARE il digest con la chiave privata del mittente (si ottiene così la firma elettronica)
- Aggiungere al documento originale la firma elettronica ottenuta al passo precedente e inviare la coppia (messaggio, firma)

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)

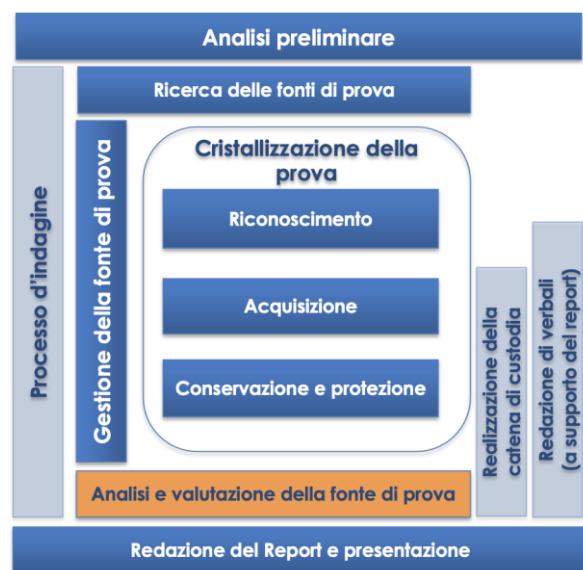


- Verificata dal destinatario tramite l'uguaglianza tra il digest ricevuto (decifrato utilizzando la chiave pubblica del mittente) e quello da lui generato dal documento ricevuto (garanzia di integrità e autenticità)
- Se è necessaria la riservatezza, il documento può venire cifrato:
 - con la chiave 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



- Segue la fase di acquisizione (Live/ Post mortem) e conservazione dei dati
- Anche questa fase dipende dal contesto in cui si opera e da cosa si deve accettare:
 - 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
 -
- 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
 - 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

The screenshot shows the homepage of the NIST Computer Forensics Tool Testing (CFTT) project. At the top, there's a navigation bar with links for 'Search NIST' and 'Menu'. Below it, a banner for 'Science and Technology' features the text 'National Institute of Standards and Technology (NIST) Computer Forensic Tool Testing (CFTT) Reports'. The main content area is titled 'Computer Forensics Tool Testing (CFTT)' and includes a sidebar with links for 'CFTT General Information', 'CFTT Technical Information', 'Federated Testing Project', 'CFIREDS', 'Computer Forensics Tool Catalog', and 'Useful Links'. The central text discusses the critical need for forensic tool testing and the methodology developed by the CFTT project. It also mentions the Cyber Forensics project and the availability of reports categorized by tool type.

Toolkit Forense open source: CAINE

- CAINE (Computer Aided INvestigative Environment) è una distribuzione italiana Linux live, creata da un uomo che fa questo mestiere da molti anni e che ha molta esperienza
 - 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
- CAINE integra sistemi e strumenti open source al fine di offrire un ambiente completo per l'analisi forense. Alcuni degli strumenti sono stati sviluppati da lui e dalla sua azienda, altri invece sono open source e sono stati validati e integrati
- 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

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** perché consentono un forte anonimato e quindi sono quelli maggiormente utilizzati in questo tipo di reato
 - File scaricati
 - Parole chiave utilizzate
 - Condivisione dei file
 - **Navigazione su Internet**
 - Siti acceduti
 - Parole chiave ricercate
 - **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

Supponiamo di dover verificare se c'è stato un accesso abusivo.

Verificare se si trova qualcosa nei log di sistema, log di dispositivi di rete. Si può analizzare la presenza di malware, rootkit ecc. Inoltre bisogna controllare i log di accesso al computer in locale o da remoto.

Una volta identificato l'ip possiamo dare questi comandi:

- dig -x {IP}
- whois {IP}
- geoIP database

Potremmo analizzare anche la traceroute per localizzare l'indirizzo IP.

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 (tipico dei sistemi Unix/IBM) per la condivisione di dischi
- 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
- Generalmente sono molto facili da usare
- Indipendenti da un server centralizzato
- Utilizzabili su macchine che non hanno elevate caratteristiche prestazionali
- Garantiscono un'elevata forma di anonimato e quindi sono stati utilizzati molto per la condivisione di materiale coperto da copyright e, anche, da soggetti atti a delinquere.
- Sono utilizzati anche da applicazioni VoIP e di videoconferenza (Skype, Hangout, ecc.), Instant Messaging (Mesh, Tox, Jami, ecc.)
- 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**).
 - Chi ha il dato lo condivide
 - 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**
- 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 (vengono detti anche **servent**, un termine 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

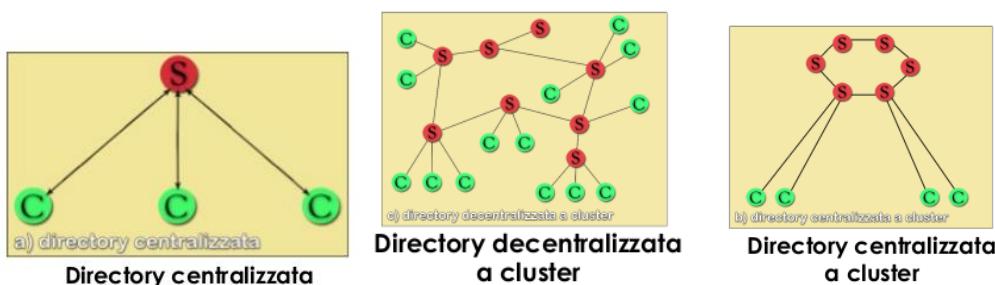
Le reti P2P non strutturate

- 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 prevedibili
- 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. Questo si occupa di reindirizzare ogni peer al nodo interessato
 - 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. Serviva principalmente per la condivisione di musica.
- 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

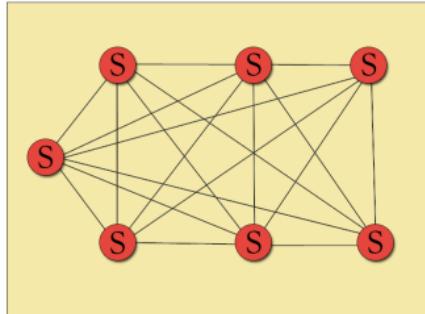
La prima immagine soffre di un collo di bottiglia perché c'è un unico server, ha una scalabilità limitata. Chi gestisce il server è facilmente individuabile.



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**
- 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)

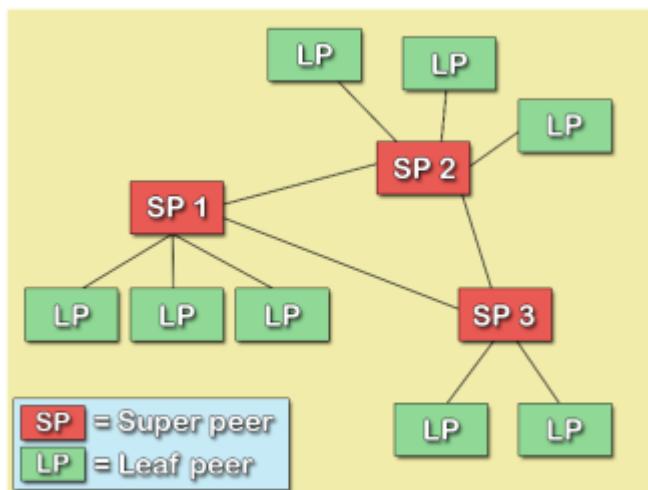
I superpeer sono nodi dotati di buona connettività e buona capacità computazionale

- 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

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
- 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 Kademia)
 - 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 Kademia, è invece una rete P2P priva di server e di tipo decentralizzata pura

Demo del tool CAINE

Simuliamo una macchina virtuale con windows. Faremo l'analisi forense di questo computer che è partito con la ISO di CAINE (come se avviassi il pc con una penna su cui c'è CAINE).

L'investigatore ha recuperato un insieme di file e tra questi vi sono alcuni pdf protetti da password. Si utilizza pdfcrack da riga di comando con attacco a forza bruta:

```
pdfcrack -n 4 -m 5 -u /media/sdb1/top-secret.pdf
```

dove abbiamo specificato 4 caratteri minimi e 5 al massimo. Il tool proverà molte password fin quando non trova quella giusta.

Dopo un po 'troverà la password.

Un altro modo è fare un attacco al dizionario specificando un dizionario contenente le password più utilizzate, ce ne sono diversi online. In base all'hardware su cui lavoriamo impiegherà più o meno tempo.

Nel caso di password complesse, con caratteri speciali, minuscole e maiuscole funziona allo stesso modo ma ovviamente ci vorrà più tempo. Sarebbe utile se sapessimo quali caratteri possiamo escludere, da quale lunghezza minima partire ecc.

Più informazioni conosciamo, meno tempo impiegherà.

Tra i file recuperati ci sono delle immagini, vogliamo vedere se ci sono informazioni nascoste. La steganografia a seconda del file riesce a nascondere delle informazioni. Per esempio per un'immagine, si potrebbe cambiare il bit meno significativo.

Stegosuite è un tool che ci aiuta in questo, che ci fornisce il file/testo o altro, nascosto dietro ad un file immagine, audio ecc.

L'investigatore ha trovato una penna USB dell'indagato e vuole verificare se sono state cancellate informazioni. Si utilizzano dei tool: Photorec e TestDisk. Con questi strumenti si possono leggere a basso livello i bit che sono su quella memoria, quindi capire se ci sono dei file o dei pezzi di dati che possono essere utili all'analisi forense.

In base all'ampiezza del disco impiegheranno più o meno tempo nella scansione della memoria. Possiamo scegliere di cercare solo delle tipologie di file oppure se li voglio vedere tutti. A questo punto posso vedere i file che prima erano sulla pennina e che poi sono stati eliminati ma non a basso livello. Tali pezzi di file non devono essere salvati sullo stesso dispositivo, ma da un'altra parte perché potrebbero essere compromessi. In questo caso sono stati recuperati tutti i file interi perché non sono stati sovrascritti.

Nonostante ciò però una delle immagini è danneggiata, ciò non toglie che con un certo tool non si possa recuperare completamente.

TestDisk è più evoluto di Photorec.

E' stato ritrovato un pc windows i cui utenti però sono protetti da password.

In questo caso CAINE deve essere impostato in modo che possiamo accedere al dispositivo su cui è montato in modalità scrivibile, perché di default ci fa vedere i file solo in modalità lettura per questioni di sicurezza in modo che non possiamo modificare le prove.

Usiamo MAC e possiamo vedere quali sono gli utenti del sistema e quali di loro sono admin. Prendo l'id di un utente e ci fa scegliere cosa vogliamo fare, per esempio eliminare la password. Possiamo anche promuovere un utente per renderlo admin. A questo punto riavviamo il pc senza la pennina CAINE in modo da poter accedere al computer dell'indagato. Supponiamo che il sistema non sia protetto da bitlocker (cifratura di file system), perché nel caso in cui ci sia bisogna avere le credenziali per montare il file system.

Prima di avviare il pc bisogna inserire la chiavetta con la ISO di CAINE installata sopra in modo che non venga avviato prima windows. Partirà quindi la pennina e il sistema andrà nella RAM.

CAINE può essere anche installata sul pc.

NB: il pc può essere acceso SOLO non facendo partire il sistema operativo originale, altrimenti si vanno a modificare delle cose.

30 Giugno 2023

Conservazione e protezione della prova

Fase tra acquisizione e analisi.

È la garanzia fondamentale attorno a cui ruota tutta la disciplina relativa al trattamento dell'evidenza digitale ed è rappresentata dal dovere di non alterare il dato originale. Una volta acquisite, le prove devono essere protette e mantenute integre, fino alla conclusione del processo (per la ripetibilità e riproducibilità).

Come per la fase di acquisizione, anche nel trasporto la fonte di prova deve rimanere integra. (Spesso deve essere spostata, dopo essere stata cristallizzata, per esempio per essere portata al laboratorio d'analisi).

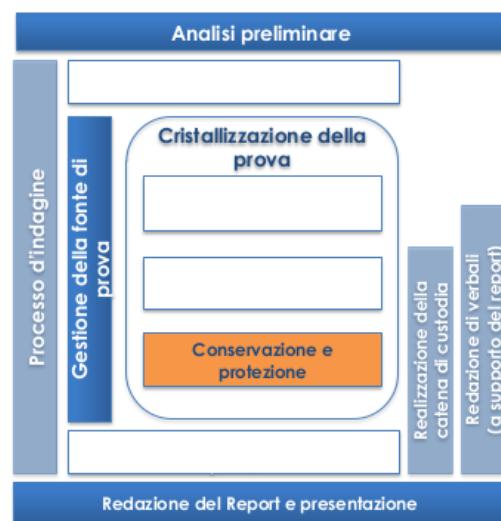
Occorre garantire

- genuinità (esatta corrispondenza tra copia e originale)
- conservazione (impedire alterazioni successive dell'originale o della copia)

Questo perché la prova potrebbe essere invalidata sia per degenerazione naturale del supporto di memorizzazione, sia per danneggiamento intenzionale della fonte di prova).

Aspetti da considerare per la protezione del supporto di memorizzazione:

- Sicurezza nel trasporto
- Protezione fisica dalle alterazioni
- Archiviazione sicura e replica
- Restrizioni dell'accesso al dato



Tutte le indicazioni sulle procedure da seguire sono date dalle best practice.

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 (sottolinea l'importanza di questa fase, per la salvaguardia dei dati e la necessità di adottare misure tecniche adeguate per la salvaguardia dei dati originali)

Conservazione e protezione della prova: Sicurezza nel trasporto

- Preferibile trasporto fisico
 - Deve essere trasportata dall'investigatore o delegato

- Si consiglia di usare guanti antistatici per maneggiare le prove
- 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
 - potrebbe indurre difficoltà nel processo di legittimazione della prova.

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
 - Si usano particolari imballaggi, che proteggono per esempio da campi elettromagnetici e dai fattori seguenti
- Porre attenzione:
 - A forti campi elettromagnetici o scariche elettrostatiche che potrebbero cancellare la prova dal dispositivo → si usano buste antistatiche (si usa anche scaricare l'elettricità scarica che si può avere)
 - Ai colpi e alle cadute – scarsa resistenza all'urto delle parti motorizzate e componenti elettriche
 - Umidità o acqua, per i corto circuiti
 - Luce, calore, raggi UV

Evitare polistirolo!

Non apporre etichette direttamente sul materiale, ma etichettare i contenitori.

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 avvenire garantendo al sicurezza della prova, dunque 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)
- Uso di armadi e cassaforte, ignifughi e accessibili solo a personale autorizzato..

È 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

Ogni altro accesso deve essere impedito con specifiche misure di sicurezza, legate anche alla specificità della prova.

Il laboratorio deve essere equipaggiato con sistemi di sicurezza.

La catena di custodia

- Durante le fasi di acquisizione, conservazione e analisi deve essere redatta la catena di custodia, per assicurare la verificabilità delle azioni eseguite e provare l'integrità dei dati.
- Ogni fonte di prova acquisita deve essere accompagnata da un documento che è la catena di custodia
- Il documento è 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
 - Tutti gli ulteriori accessi devono essere riportati nella catena di custodia
 - Si può documentare con foto

Contiene:

- Intestazione con data e numero di protocollo associato al caso
- Campi da compilare durante la fase di acquisizione, conservazione e analisi
- 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

Id → numero di riferimento univoco (quello riportato nell'etichetta apportata al momento dell'indagine)

Ci possono essere anche fotografie allegate.

La catena di custodia: Caratteristiche dell'evidenza

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

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: Custodia e restituzione

Terza fase.

- 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 analoga alla custodia e viene utilizzata nel momento di restituzione del dispositivo originale

Redazione dei verbali



I verbali delle operazioni affiancano le 3 fasi della catena di custodia, riconoscimento, acquisizione, conservazione e analisi.

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.).

Devono essere verbalizzati con cura i dati e gli eventi che avvengono durante le fasi. Verbalizzare con cura aiuta non solo a comprendere la situazione e individuare linee di indagine, ma fornisce anche una traccia degli eventi che può essere elaborata in seguito e usata per validare il processo informativo [?]

Le attività svolte devono essere dettagliate e possibilmente supportate da foto, che identificano le info chiave.

Le informazioni contenute nel verbale devono rispettare i principi di chiarezza, trasparenza e completezza e devono essere in grado di resistere ai limiti e ai controlli della legge.

I verbali sono anche legati al report finale.

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, in modo che tutto sia giustificabile (dalle best practice e se, non si fa fede a questo, bisogna giustificare scelte diverse)
- Per particolari atti come sequestri e intercettazioni occorre riferirsi alle deleghe dell'autorità giudiziaria.
- Screenshot, foto del reperto, del sistema e di tutti gli elementi che certifichino le attività svolte a patto che possano essere etichettate e validate.
- I riferimenti temporali delle attività e l'eventuale scostamento dall'ora riportata sul sistema
- Riferimento a tutte le persone intervenute

Per le attività di analisi devono essere riportate:

- Le attività di laboratorio,

- le analisi effettuate,
- gli strumenti utilizzati e dati rilevati

L'ideale è tenere in tempo reale durante l'indagine appunti.

Redazione del report e presentazione



Alla fine tutti i dati elaborati sono raccolti in un report finale, coronamento dell'attività.

Sarà di supporto alla presentazione in tribunale o da parte chi ha commissionato l'indagine

Passi per la preparazione

1. Raccolta dei dati/evidenze
2. Analisi dei risultati (COSA metto nel report) —> garantire coerenza; eliminare informazioni superflue e duplicate. Fase delicata.
3. Definizione della struttura del report (COME presento le informazioni). Il CTU si può aiutare con grafici o altri strumenti. Comprende:
 - parte epigrafica (il CTU indica gli estremi della causa e riassume le operazioni compiute)
 - parte descrittiva (per gli accertamenti o le ricostruzioni da lui compiute)
 - parte valutativa, in cui si risponde ai quesiti, motivando le scelte
 - parte riassuntive, in cui il CTU espone in forma sintetica le risposte ai quesiti
4. Stesura e revisione della bozza
5. Stesura del report finale
6. Diffusione della relazione

Presentazione

- La fase che segue la redazione del report. Presentazione nei confronti dell'organo giudicante (giudici, commissioni disciplinari, manager...)
- L'espositore deve fornire prove alla corte e resistere alle opposizioni dell'avversario. Occorre tradurre contesti tecnici, spesso complesso, in modo che siano comprensibili da tutti.
- Possono essere utilizzati supporti, sia per l'esposizione, sia come dimostrazione di quanto indagato.
- I risultati e le conclusioni dedotte devono essere presentate in forma facilmente comprensibile
 - L'esposizione deve fornire prove alla corte e resistere alle opposizioni dell'avversario
- In tribunale:

- Interrogatorio diretto:
 - È condotto dalla parte del committente del lavoro
 - Ha lo scopo di fornire le prove per dimostrare il caso
- Contraddittorio (consente di chiarire dei punti):
 - 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 un modello di elaborazione distribuito che consente l'accesso condiviso e su richiesta, mediante la rete, a risorse delocalizzate configurabili (offerti dai Cloud Service Provider). Ha cambiato radicalmente il modo di creare, erogare, accedere e gestire i servizi IT, sia per le persone, ma anche per le aziende, sollevandole dall'obbligo di acquistare e gestire delle infrastrutture tecniche IT per lo svolgimento delle attività, nonché per il costo di formazione). Ha portato benefici sia in ambito economico che sociale.

Ha identificato un nuovo modello di fruizione dei servizi IT. Ha ampliato il paradigma del servizio richiesto, prima modellato con client-server.

Il cloud ha avuto la sua espansione grazie ai progressi della tecnologia di virtualizzazione e alla diffusione della banda larga e dei dispositivi mobile e dell'IOT.

I vari modelli di sistemi Cloud

Progressivo spostamento di servizi, dati, applicazioni, infrastrutture che sono state ubicate verso soggetti terzi.

- Modelli di servizio (scopo di utilizzo, livello di astrazione e controllo dell'infrastruttura)
 - SaaS – Software as a Service → il fruitore usa le applicazioni del provider (minor grado di controllo da parte dell'utente, che non ha necessità di installazione e aggiornamento; costi ridotti di mantenimento)
 - PaaS – Platform as a Service → il provider fornisce una piattaforma di sviluppo preconfigurata (una rete, un server). Il fruitore può sviluppare e installare applicazioni. Il grado di controllo sulle risorse virtualizzate c'è, ma è limitato alle proprie applicazioni, mentre l'infrastruttura su cui sono sviluppate è sotto il controllo del provider. L'accesso ai dati del sistema richiede l'intervento del provider.
 - IaaS – Infrastructure as a Service → il provider offre infrastruttura e risorse computazionali (rete, server, storage). Il fruitore ha il controllo sui sistemi operativi e sullo storage. Ha il più alto grado di controllo sulle risorse virtualizzate e può accedere senza restrizioni a tutti i dati immagazzinati su tali risorse.
- Modelli di sviluppo (differiscono per la tipologia di gestione e la dislocazione delle risorse computazionali e tipologia di utenti):

- Cloud Privato → risorse e dati a disposizione di un'unica organizzazione.
L'infrastruttura può essere sia esterna sia interna all'organizzazione.
- Cloud Pubblico → le risorse sono accessibili da qualsiasi utente che ne faccia uso e sono di proprietà del provider.
- Cloud Comunitario → una via di mezzo tra pubblico e privato. Le infrastrutture sono messe a disposizione tra più organizzazioni.
- Cloud Ibrido → più sistemi di cloud, pubblici, privati o comunitari.

Caratteristiche del Cloud: PRO

1. Offerta di servizi «on-demand» a basso costo, che possono essere fruiti dall'utente in maniera indiretta e automatica.
2. Semplicità di accesso alle risorse via Internet tramite registrazione account interfaccia offerta dal Cloud Service Provider (CSP), raggiungibile da ovunque ci sia rete.
3. Storage illimitato di dati o grandi quantità di spazio
4. Condivisione di risorse delocalizzate gestite dal CSP, tra dispositivi dello stesso utente o tra utenti diversi
5. Elasticità dei servizi; risorse dinamicamente fruibili come servizi a consumo (pay per use). Così vengono garantite in ogni momento le qualità stabilite dal servizio. È il CSP che controlla e ottimizza i servizi come storage e larghezza della banda dipendentemente dall'impiego effettivo delle risorse.

Caratteristiche del Cloud: CONTRO

- Problemi di riservatezza e sicurezza dei dati
- Creazione di grandi aggregazioni di dati digitali, che sono soggetti a essere 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

Le caratteristiche devono essere tenute presenti quando ci si trova a eseguire un'analisi forense sul cloud.

L'investigatore deve essere in grado di effettuarvi un'analisi forense per determinare azioni effettuate su questi sistemi o tramite essi, le modalità in cui sono state compiute e il soggetto a cui sono riconducibile.

UNA DISCIPLINA MULTIDIMENSIONALE

Cloud Forensics: una disciplina multidimensionale

Non esiste ancora una best practice disegnata sul cloud, e quindi le procedure per il cloud fanno riferimento alle norme per la DF con le dovute integrazioni.

Queste procedure non sempre sono adatte al caso del cloud perché sono basate sul presupposto di poter sempre accedere senza restrizioni sia ai sistemi oggetto di analisi, sia ai dati generati relativi agli utenti. Questa ipotesi non vale per il cloud.

Il cloud può essere:

oggetto del crimine (per esempio se oggetto di un DOS);

soggetto se è l'ambiente in cui è compiuto il crimine (per esempio quando viene modificato o cancellato senza autorizzazione un dato residente nel cloud o un furto di identità);

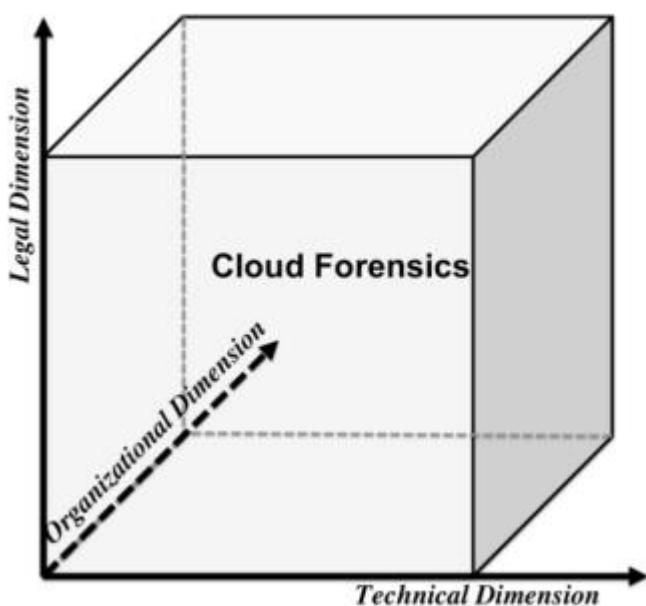
strumento (se è usato per condurre o pianificare un crimine o memorizzare delle prove del crimine o attaccare un altro cloud).

Non è una disciplina solo tecnica, ma multidimensionale:

dimensione legale → la parte più critica della Cloud Forensics, che si occupa delle diverse giurisdizioni e della condivisione delle (le principali sfide di questa investigazione);

dimensione organizzativa → coinvolge due tipi di attori, il CSP e il cliente, sempre. Quando il provider dà in outsource alcun servizi, la dimensione si allarga;

dimensione tecnica → coinvolge gli strumenti e procedure che consentono di portare avanti l'attività forense.



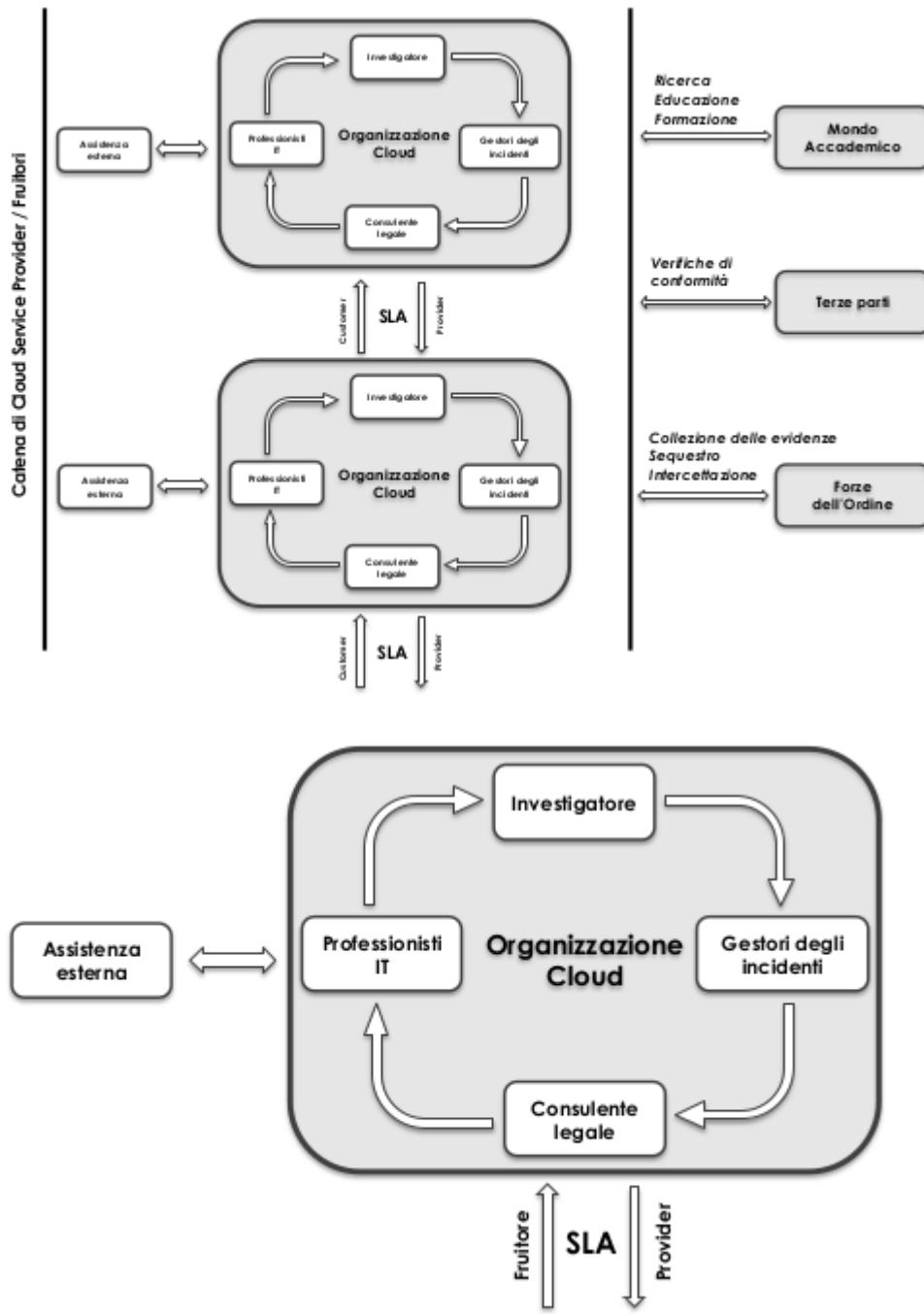
Technical Dimension: strumenti e procedure da adottare

La ripartizione dei ruoli e il livello di controllo che chi effettua l'indagine può effettuare dipende dal cloud e dal modello di sviluppo. Anche gli strumenti saranno diversi.

Bisogna sempre soddisfare i requisiti di autenticità e integrità e rispettare le norme giuridiche di dove sono collezionati i dati e non violare la privacy.

- 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 (uno stesso ambiente può essere condiviso da servizi riconducibili a soggetti diversi, che condividono magari dinamicamente le stesse risorse fisiche). La multi-tenance ha due problemi: da una parte i soggetti tendono a usare cifratura dei dati per maggiore privacy; inoltre può essere difficile stabilire a quale soggetto effettivamente appartengano i dati. Non violo la privacy di utenti che condividono la solita risorsa e che non sono coinvolte nell'indagine.
- Esegoo le investigazioni in ambiente virtualizzato, ma l'investigatore avrebbe bisogno di dati che stanno in postazioni fisiche, quindi le procedure devono essere in grado di individuare i dati in una posizione fisica a un certo timestamp o essere tracciati sullo stesso periodo. Si dovrebbe eseguire snapshot regolari sulle macchine in esecuzioni, che salvano i processi in esecuzione, i dati in memoria, gli utenti attivi collegati alla macchina virtuale e molti altri.
 - Le sfide sono la perdita di dati, la localizzazione dei dati in un certo momento tenendo presente la giurisdizione e la locazione fisica
- L'analisi potrà essere effettuata sui client usati per accedere al cloud, anche su dispositivi mobile (quindi applicazione di Computer Forensics e Cloud Forensics), sulle risorse virtualizzate che erogano i servizi (Server Forensics, virtuale o meno) e sulle risorse fisiche che ospitano le risorse virtualizzate e sulla rete che consente la loro interazione (fisiche e virtualizzate).
- Attuazione di misure preventive
 - Tool per la collezione di dati lato CSP e client, eseguire snapshot regolari di storage remoti

Organizational Dimension: struttura proposta



Viene proposta una struttura apposita. Ogni organizzazione coinvolta (cliente, CSP) è chiamata a definire al suo interno le persone che fanno parte della struttura.

Occorre collaborazione di provider del servizio e fruitore, con il supporto di un'assistenza tecnica esterna che stabilisca i ruoli.

Ci sarà un investigatore, responsabile delle investigazioni, che può collaborare con collaboratori esterni e forze dell'ordine.

I professionisti IT (amministratori di sistema, rete, esperti di sicurezza, staff tecnico) contribuiscono all'investigazione accedendo alla scena e collezionando i dati.

I gestori degli incidenti rispondono a specifici incidenti sul cloud (accesso non autorizzato, perdita dei dati, violazione della sicurezza, DOS, infezioni da malware). Sarebbe opportuno categorizzare gli incidenti.

Il consulente legale ha familiarità con le questioni multi-tenant e multi-giurisdizionali, in modo che non vengano violate le norme. Collabora eventualmente con le forze dell'ordine. Dovrebbe scrivere dei Service Level Agreement con le procedure da seguire in caso di investigazioni digitali.

La situazione si può complicare con una catena di dipendenze dinamiche con altri CSP.

In questi casi l'investigazione dipende da ogni legame e dalla complessità della dipendenza tra i nodi. Spesso sono necessarie ulteriori collaborazioni, per esempio con le forze dell'ordine (per trovare soluzioni ottimali per casi come il sequestro delle risorse).

Ci sono terze parti a stretto contatto negli auditing.

E tutto il mondo accademico e di ricerca, sia per contribuire alle conoscenze in Cloud Forensics, sia per formare il personale coinvolto, dedicato alla Cloud Forensics.

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

Il cloud pone di fronte a sfide da affrontare rispetto alle attività forensi tradizionali, ma offre anche opportunità che si possono sfruttare.

Sfide: Le funzionalità easy-to-use

- Una sfida per la raccolta delle evidenze digitali è data dalla proliferazione delle applicazioni mobile e delle interfacce web a disposizione degli utenti. Nel cloud ha fatto aumentare il numero di crimini e il carico di lavoro, proprio per la quantità di risorse legate al cloud.
- L'accesso semplificato alle risorse di Cloud ha portato:
 - Creazione di grandi aggregazioni di dati digitali divenuti risorse per aziende e primati, ma anche un obiettivo appetibile per i criminali
 - Sistema di registrazione debole che facilita l'anonimato dei criminali e rende difficile l'identificazione dei sospetti e quindi l'individuazione delle prove
 - Una inconsapevolezza dell'utente della tecnologia utilizzata e dei rischi e non sono a conoscenza dei potenziali problemi che potrebbero causare all'indagine. Addirittura non c'è consapevolezza su cosa succeda ai propri dati e su come agire in caso di abuso o perdita.

Sfide: Elastic, Static e Live forensics

- L'elasticità del Cloud causa un problema circa la sincronizzazione dei timestamp, che è sempre stata fondamentale per esempio nella Network Forensics (per esempio i log, che sono una prova fondamentale). In questo caso occorre fare una sincronizzazione sia tra:
 - tra infrastruttura del CSP e client Web remoti
 - sia su più macchine fisiche distribuite su più aree geografiche
- Un altro problema è l'unificazione o la conversione di diversi formati di log. Esisteva già nella Network Forensics, ma nel Cloud si è amplificata, anche perché nel Cloud si ha un'enorme mole di dati.
 - formati proprietari nelle indagini congiunte
- Il recupero dei dati cancellati (importante per la prova) → nel Cloud la cancellazione avviene insieme alla cancellazione del mapping con il dominio. Quindi l'accesso ai dati cancellati non è più possibile. I dati potrebbero essere ancora presenti, la sfida è come recuperarli.
- L'attribuzione della proprietà dei dati, per poterli usare come fonte di ricostruzione degli eventi.

Sfide: La separazione delle evidenze

- Istanze diverse della stessa macchina fisica sono logicamente isolate dall'Hypervisor ma condividono le stesse risorse fisiche. Le risorse delle macchine virtualizzate però non hanno accesso ai dischi fisici, ma a dischi virtualizzati. Quindi, per esempio, a livello fisico i log di sistema sono divisi tra più titolari.
 - Il CSP e forze dell'ordine devono mantenere la stessa separazione delle evidenze durante il processo di indagine, senza violare la riservatezza di clienti del cloud, estranei all'indagine.
 - Necessità di tecnologie di provisioning e de-provisioning degli utenti più accurate
- Nei casi di multi tenance, livelli adeguati di riservatezza sono talvolta soddisfatti mediante l'utilizzo della crittografia per i dati sensibili dell'utente. A volte è il provider del servizio a cifrare i dati e gestire le chiavi, in altri casi è l'utente, che li cifra prima di salvarli sul Cloud.
 - Necessità di accordi tra le Forze dell'Ordine, il cliente e il provider per la gestione e l'accesso delle chiavi durante le fasi dell'Analisi Forense.
- Sarebbe utile per l'indagine tracciare chi ha creato i dati e chi li ha modificati, ma potrebbe esserci un problema di sicurezza di queste informazioni, rischiando violazioni della privacy e della confidenzialità dell'informazione. Il provider per esempio potrebbe usare i log per generare una collezione didati utili all'indagine (funzionalità utilizzate, errori fatti da un certo fruitore, loggare le condizioni critiche che possono impattare su tutti gli utenti, cambi pwd, fallimenti di accesso, azioni eseguite in modalità privilegiata)

Sfide: La virtualizzazione

- La virtualizzazione è usata dal provider per implementare la ridondanza e la distribuzione delle risorse.
- Induce a un problema di inaccessibilità delle risorse fisiche
 - Live forensics con tecniche eseguite direttamente sulle MV in esecuzione e tecniche di acquisizione remota. Bisogna chiedere collaborazione al provider.

- La compromissione dell'hypervisor (gestore delle risorse virtuali: gestisce le risorse fisiche dell'infrastruttura e le alloca dinamicamente in risorse virtuali; agisce come ponte tra dati fisici e l'utente) è un grande punto di criticità e coinvolge tutte le risorse, in quanto i criminali informatici possono indirizzare gli attacchi verso l'hypervisor, al cui compromissione fisica amplificherebbe qualsiasi attacco.
 - Necessità di sviluppare politiche e procedure tecniche per facilitare le indagini a livello hypervisor
- Il mirroring dei dati dà un problema sulla sincronizzazione delle copie (se la sincronizzazione è lenta, si possono perdere dati che non sono aggiornati, oppure se è veloce, li trovo aggiornati anche se volevo i dati precedenti. In questo caso potrebbe essere eseguito un Log Framework in cui il provider registra tutte le info riguardanti la memorizzazione dei dati, in modo che sia possibile identificare in modo preciso in quale risorsa il dato è memorizzato in un dato momento e ricostruire le operazioni fatte su esso.
- La natura distribuita del cloud porta alla
 - necessità di collaborazioni internazionali tra forze dell'ordine (es: caso di confisca del Cloud) e di Service Level Agreement che impongano dei vincoli sull'ubicazione geografica di dati e risorse
- L'archiviazione ridondante in più giurisdizioni e la difficoltà di geolocalizzare real-time i dati possono ostacolare l'investigazione (gli investigatori possono inavvertitamente violare le norme delle giurisdizioni competenti, non sapendo con esattezza l'area geografica in cui i dati risiedono in un dato momento)
 - 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

Sfide: La formazione del personale interno

- È necessario stabilire una struttura organizzativa interna dedicata alla Cloud Forensics
 - Spesso manca l'esperienza legale pertinente e le indagini vengono effettuate con metodologie della Forensics tradizionale oppure non viene affatto affrontato il problema
- 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

- Sono fondamentali per una corretta investigazioni.

- Dovrebbero essere corredati di documenti tecnici, perché spesso i provider non sono disposti a garantire la trasparenza ai clienti per quanto riguarda le indagini forensi (anche perché spesso loro stessi non sanno come indagare e temono che le tecniche che usano possano causare danni a loro volta)
- 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:
 - 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 fruttore (spesso nei contratti c'è uno squilibrio enorme tra provider e fornitore)
 - 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 sfide in questo ambito riguardano le differenze tra le legislazioni in tutti i paesi (stati) in cui risiedono il Cloud e i suoi fruttori.

- 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 fruttori?
- 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

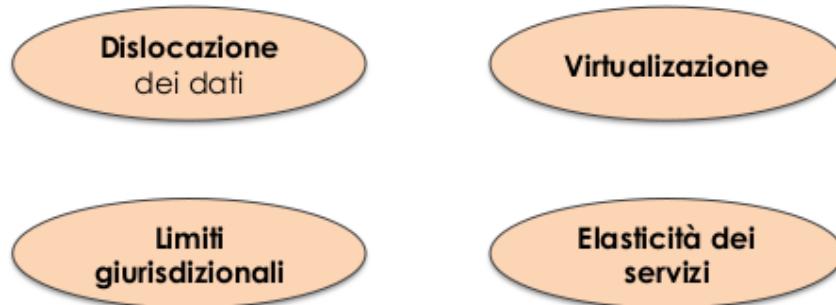
- Ridondanza dei dati
 - Rende quasi impossibile la cancellazione totale dei dati (che devono essere scovati)
- Servizi di clonazione delle MV offerti da SaaS possono essere utilizzati per
 - creare un'immagine di una macchina da analizzare
 - Velocizzare le indagini con investigazioni parallele, che non è possibile fare nella digital forensics tradizionale
- Il versionamento dei dati utilizzato dai CSP
 - Recuperare, ripristinare e conservare ogni versione di ogni oggetto memorizzato

- Scalabilità e flessibilità del Cloud
 - può offrire un servizio di Cloud Forensics pay-per-use illimitato
 - Consente ai fruitori di predisporre dei server dedicati alla Forensics pronti da essere utilizzati se necessario
- Si può creare un sistema di Forensics as a Service (FaaS)
 - Sistema di analisi forense basato sul Cloud, che ha dei vantaggi per esempio nei sistemi di storage su larga scala e fornisce potenza di calcolo, con gli ulteriori vantaggi di scalabilità, interattività, estensibilità, robustezza del sistema.
- Analogamente si può creare un sistema Law as a Service (LaaS)
 - Sistema di erogazione dei servizi legali ad uso degli avvocati e dei giuristi e quindi promuovere una collaborazione, semplificando il lavoro fuori sede e riducendo i costi dei piccoli uffici

LE FASI DELLA DIGITAL FORENSICS NEL CLOUD

Identificazione

- Individuo il CSP e cerco di capire dove sono le strutture tecnologiche che contengono i dati e che quindi sono possibili fonti di prova
- Sfide:
 - dati di dislocati su più risorse virtualizzate e dislocate in aree geografiche diverse, causando limiti giurisdizionali diversi
 - elasticità dei servizi (che può causare il problema dei dati cancellati visto prima)



Acquisizione e raccolta

- Eseguo:
 - Live Forensics sui client (che è predominante per esempio sui client usati per accedere alle risorse tramite interfacce web)
 - Computer Forensics sulle MV (che non può essere eseguita a macchine spente)
 - Network Forensics (tecniche classiche, ma in ambiente virtualizzato)
- Sfide:
 - Replicazione dei dati
 - Grandi quantità di dati a disposizione
 - Volatilità delle risorse
 - Privacy dei fruitori del servizio

- Catena di custodia (la raccolta dei dati, solitamente effettuata inviando esperti in loco, diventa difficile da gestire: gli investigatori non hanno accesso fisico alle risorse e occorre quindi fare riferimento al provider)
- Opportunità:
 - Ridondanza dei dati
 - Versionamento

CONSERVAZIONE

C'è il problema di garantire l'integrità dei dati originali memorizzati su un sistema Cloud. Nella forensics tradizionale l'integrità della prova è ottenuta mediante il rispetto della catena di custodia, nella Cloud Forensics ci sono problematiche caratterizzate da:

- Replicazione dei dati
- Volatilità delle risorse
- segregazione della prova

ANALISI

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

- Sfide:
 - integrazione delle prove (rendere convertibili i log)
 - costruzione della timeline (il CSP deve garantire la sincronizzazione dei server e delle apparecchiature che sono dislocate o che toccano il percorso logico dei dati)
 - cifratura dei dati
- Opportunità:
 - Servizi di clonazione, che possono facilitare nell'elaborazione dei dati
 - servizi pary-per-use illimitati

Documentazione e presentazione

- Sfide
 - Catena di custodia (difficile annotare tutte le persone entrate in contatto con le fonti di prova nelle varie fasi)
 - Report fotografico (dovrebbe essere effettuato da persone autorizzate, e invece potrebbe essere effettuato dal provider stesso)
 - Comprensione da parte della giuria e della corte 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 → la vehicle forensics sta emergendo come disciplina
- Memorizzano una grande quantità di informazioni digitali (del veicolo, sull'ambiente circostante, tracce del comportamento del conducente e degli altri passeggeri, destinazioni recenti, registri

- delle chiamate, contatti, guasti delle centraline, interazioni verso altri IoT - veicoli o reti cittadine), che possono essere fonte di evidenze digitali in investigazioni dove il veicolo
 - è coinvolto nella scena del crimine (rapina, sequestro, incidente stradale)
 - è uno strumento per commettere atti criminali
- L'analisi forense sul veicolo è diventata maggiormente importante in quanto è 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), con reclusione da 2 a 7 anni, e lesioni personali stradali gravi o gravissime ad una persona (Art. 590-bis)

I veicoli ‘intelligenti’

Dal punto di vista forense possono essere visti come un tipico sistema informatico con diversi moduli elettronici collegati e controllati da diversi dispositivi informatici e, come tali, vanno gestiti adeguatamente per non perdere i dati.

Ogni modulo genera, processa, trasmette e immagazzina dati digitali. In ogni auto connessa ci sono circa 80 centraline (freni, sterzo, airbag, infotainment), 150 milioni di righe di codice nei programmi di supporto (per le auto a guida assistita; per quelle a guida autonoma si parla di 300 milioni di righe di codice) e 25 GB di dati per ogni ora di funzionamento.

L'Internet of Vehicle (**IoV**) è un sistema dinamico che prevede comunicazioni:

– V2V: Vehicle-to-Vehicle, V2I: Vehicle-to- Infrastructure, V2N: Vehicle-to-Network, V2P: Vehicle-to-Pedestrian.

Rispetto ad altri sistemi IoT, l'IoV presenta strutture topologiche dinamiche, un'enorme scala di rete, nodi non distribuiti in maniera uniforme e la granularità dei dispositivi è complessa.

Sfide da affrontare

Eterogeneità dei dati: esistono parecchie fonti di dati sia a bordo, sia nell'infrastruttura. I dati a bordo sono archiviati in dispositivi diversi e formati diversi, generalmente non standardizzati (quindi devono essere modellati in modo da essere validi dal punto di vista forense).

Dal momento che ci sono molti enormi di dati, è essenziale individuare, raccogliere e analizzare solo quelli essenziali, in modo che possano essere presentati come prova in tribunale.

– Assenza di standard, problema della pertinenza

Catena di custodia:

– la rete delle componenti è dinamica nell'IoV e i nodi non sono distribuiti uniformemente; inoltre la maggior parte dei nodi non memorizza metadati, in particolare i dati temporali, che sono quindi assenti

- molti componenti sono assemblati all'estero, cosa che causa il problema nell'assegnazione della responsabilità e per la documentazione fotografica

Acquisizione di prove valide:

- i produttori spesso non sono disposti a fornire un accesso aperto ai dati immagazzinati nel veicolo
– Componenti costruiti da diversi produttori e case automobilistiche di paesi diversi, che comporta sfide dal punto di vista pratico e legale

– Molti dati contengono informazioni personali, anche di persone estranee

Identificazione della fonte di prova

Valgono i principi della Digital Forensics: occorre identificare le tipologie di componenti elettronici e dispositivi e quali possono essere fonti di prova:

- 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 ci sono, dove sono archiviate nei veicoli e come vengono archiviate (Es: cronologie delle chiamate e dati dei social media)

Capire se c'è un'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

Si può fare in tre modi:

- 1) Utilizzando i gateway presenti nel veicolo tramite un connettore OBD (On Board Diagnostic) o porta USB.
- 2) 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 memorizzati sul dispositivo (se ci sono dati volatili)?
 - 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?
- 3) Se non sono possibili i due modi precedenti, si procede ad acquisizioni estreme e invasive
 - J-tag (standard IEEE 1149.1 per la verifica dei progetti di collaudo dei circuiti stampati, che diventano mano a mano più complessi; si usa anche per leggere i dati della memoria). Occorre trovare la porta, poi bisogna avere un adattatore e un software di comunicazione, con un'interfaccia che permette di individuare lo spazio di memoria interessato e di caricarlo sul file. Alcuni produttori però adottano contromisure per rendere difficile l'uso di questa interfaccia, come l'offuscamento o la riconfigurazione e la disabilitazione dell'interfaccia
 - chipoff (ancora più invasivo: si identifica il chip di memoria sulla scheda madre, si toglie dissaldandolo con una pistola termica, per leggerlo sulla basetta a chiodi classica bit-a-bit. Anche qui ci sono metodi di sicurezza dei produttori, che vogliono impedire il trasferimento della centralina su un altro veicolo, che al distacco dei chip possono cancellare la memoria o bruciare il dispositivo).

Una volta stabilita la metodologia di acquisizione occorre capire quali strumenti possono essere utilizzati per acquisire in modo ufficiale/forense le prove dai vari componenti e dall'infrastruttura di supporto.

Spesso si hanno difficoltà a ottenere informazioni proprietarie dai diversi produttori dei componenti del veicolo poiché

- i produttori tendono a difendere la proprietà intellettuale
- i moduli sono assemblati da diversi produttori ubicati in Paesi diversi
- i produttori temono i rischi reputazionali (si possono trovare vulnerabilità sconosciute fino a quel momento)

Difficoltà dovute ai Sistemi di sicurezza sui componenti che iniziano a essere installati sui veicoli, che implementano politiche di protezione sulle porte o crittografia. L'accesso alla diagnostica viene fatto attraverso tool con accessi verificati.

Best practice

Per evitare perdita o modifica dei dati.

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. Se lo si deve fare, ogni modifica deve essere documentata e spiegata.

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)

Aspetti proprio del diritto processuale e come il diritto processuale è stato influenzato dagli aspetti relativi alla Digital Forensics.

Oggi la maggior parte dei crimini sono commessi attraverso strumenti tecnologici o gli strumenti sono l'oggetto stesso del crimine.

Informatici forensi = tecnici che nell'ambito del processo penale o civile svolgono la funzione ausiliaria delle parti o del giudice, affinché siano portati nel procedimento gli elementi probatori.

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 (hanno aderito una 70ina di paesi)
- 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 (la competenza del giudice è di tipo territoriale; la materia informatica inserisce nuovi termini).

L'aspetto relativo alla DF ha peraltro altre sfaccettature, in relazione alla natura della prova informatica (fragilità e immaterialità).

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”

I requisiti del giusto processo si basano su diversi principi fondamentali: necessità della presenza di un giudice terzo e imparziale, rispetto della parità tra accusa e difesa, il contraddittorio tra le parti, anche nella formazione della prova (elemento in cui entrano gli esperti informatici), ragionevole durata del processo...

Il processo penale è regolato dal principio del contraddittorio nella formazione della prova. “Omissis”.

Il ruolo dei consulenti informatici si svolge nel contraddittorio fra le posizioni dei diversi ausiliari tecnici.

Il diritto alla prova

Diritto fondamentale dell'indagato di cercare fonti di prova a discolpa.

Consiste nel diritto di ricercare le fonti di prova: è data la possibilità alla persona chiamata in causa di cercare elementi a sua discolpa, di chiedere l'ammissione del relativo mezzo; partecipare alla sua assunzione e ottenere una valutazione del risultato al momento delle conclusioni.

La libertà della prova consente la possibilità di ammettere nel procedimento anche elementi di carattere scientifico sempre nuovi e innovativi. In particolare la prova informatica ha caratteristiche di fragilità e immaterialità che richiedono competenze specifiche per essere portate integre e immodificate alla valutazione del giudice.

È 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 precostituite, 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

La prova informatica presenta peculiarità e quindi 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 per garantire il principio del contraddittorio. Queste indicazioni si sono nel tempo anche adattate alla specificità della prova informatica.

Gli elementi della Digital Forensics

Attraverso la Digital Forensics si persegue l'obiettivo di evidenziare il dato (evidenza digitale), 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

1. Individuazione e Preservazione delle evidenze digitali
2. Acquisizione della prova informatica, garantendo l'inalterabilità di ciò che è analizzato
3. Analisi dei dati rinvenuti e correlazioni
4. Documentazione di quanto svolto nelle varie fasi (elemento molto importante; si fa riferimento alle ISO, specialmente 27037)

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 o degradata alla fase di dibattimento;
- **Non reiterabilità**: una volta compiuta l'attività investigativa di acquisizione della prova non è più possibile ripeterla.

Alla luce di questi caratteri il cpp prevede particolari normative per l'assunzione della prova, non solo informatica, irripetibile

Prova informatica e accertamenti tecnici non ripetibili -

Attività del Pubblico Ministero: articoli 359 e 360 del c.p.p.

Art. 359

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: 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).

Il cpp prevede la possibilità di svolgere attività investigativa anche in fase di investigazioni preliminare quando si ritiene possa esserci una modifica dei luoghi o delle cose che possono essere oggetto di prova nell'ambito del processo.

[**Accertamenti tecnici non ripetibili e incidente probatorio**](#)

Ci sono anche gli 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 (la prova, anziché essere portata in dibattimento, viene anticipata nelle fasi delle indagini preliminari).

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 modifica 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** —> strumento attraverso cui il giudice immediatamente nel processo acquisisce le informazioni probatorie; è uno strumento diretto con cui il giudice esamina alcuni dati, che poi saranno discussi al dibattimento, ma consentono al giudice di arrivare immediatamente a un giudizio)

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 giudiziari, la perizia, i documenti.

Si tratta di mezzi di prova "tipici", previsti e disciplinati dal codice di procedura penale. In materia di prova vige il principio di libertà della forma: è possibile, quindi, 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, invece, non offrono un'immediata visione al giudice, ma sono finalizzati a permettere l'acquisizione di tracce, notizie o dichiarazioni idonee ad assumere rilevanza probatoria. Sono strumenti per arrivare ad assumere informazioni. Le perizie e i documenti, invece, forniscono immediatamente determinate informazioni, che saranno poi oggetto di contraddittorio.

Il documento informatico

La prova documentale costituisce un mezzo di prova

Definito in più atti legislativi

Ambito civile

«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).

Il CAD definisce il valore probatorio del documento d'indagine, dipendentemente dalla firma digitale o elettronica apposta. Un documento con firma digitale o firma elettronica avanzata fa piena prova fino a querela di falso, mentre un documento con firma elettronica deve essere rimesso al giudice la decisione sul valore probatorio.

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; Allarga il concetto di documento informatico.

Ambito penale

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). Ancora più ampia.

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

Nell'ambito penale, l'approccio al documento informatico è più ampio rispetto all'ambito civile. La parte relativa alla prova documentale nell'ambito del procedimento penale (quindi nel c.p.p.) comporta diversi articoli: da 234 al 243.

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).

Questo è un cenno alla prova documentale come mezzo di prova.

[Finalità e Oggetto della perizia - Art. 220 c.p.p](#)

La perizia, come il documento, costituisce un mezzo di prova indirizzato a 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.”

Per quanto riguarda l’ambito informatico, con lo sviluppo della tecnologia è un’attività sempre maggiormente richiesta.

[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.

Principio di giusto processo è la parità delle parti nel processo: entrambi PM e avvocato possono accedere al CT.

[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”.

Il consulente tecnico d'ufficio assume la qualifica di pubblico ufficiale. Quindi è sottoposto alle le normative anche di carattere penale che riguardano i pubblici ufficiali e che poi vedremo

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](#)

Sono i consulenti delle parti (pubblica accusa e indagato/imputato)
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 - Art. 228](#)

1. Il perito procede alle operazioni necessarie per rispondere ai quesiti che gli sono sottoposti dal giudice. 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. Il perito è tenuto a rispondere entro un certo tempo tecnico.
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 implicant 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. Spesso nei processi può esserci un contraddirittorio tra i periti, specialmente se i temi tecnici costituiscono il cuore del dibattimento.
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. (→ non ci può essere un atteggiamento dilatorio)

C'è proprio un'interazione tra le attività del perito e le attività dei CT di parte.

Consulenza tecnica fuori dei casi di perizia

Attraverso la nomina di un consulente tecnico fuori dalla perizia (cioè quando il giudice non ha disposto perizia) ciascuna Parte ha comunque 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

Una figura che diventa sempre più importante in ambito processuale (civile e penale) per quanto riguarda la formazione della prova.

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 cosiddette prestazioni intellettuali, rispetto alla quali si suole fare distinzione tra obbligazione di mezzo e non di risultato (cioè il professionista deve rendere al cliente o a chi ha commissionato l'attività un mezzo, non un risultato).

La prestazione deve essere svolta dal professionista con diligenza, prudenza e perizia, in modo che il cliente sia supportato nel raggiungere l'obiettivo che intende perseguire. Nel tempo questa distinzione è diventata più sfumata.

Nell'adempimento delle obbligazioni inerenti a un'attività professionale, la diligenza deve valutarsi con riguardo alla natura e alla correttezza dell'attività.

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. 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.»

È una forma di responsabilità extracontrattuale da fatto illecito che può essere fatta valere solo nell'ipotesi in cui il consulente incorra in colpa grave nell'esecuzione dei suoi compiti. Essendo un pubblico ufficiale, si applica anche tutta la specifica normativa in materia penale.

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. In questo caso la responsabilità professionale civile scaturisce dal contratto sottoscritto.

Per attribuire la responsabilità del tecnico occorre dimostrare che la condotta e l'errata consulenza sono stati rilevanti nella decisione del giudice; deve essere verificato un rapporto di causa ed effetto.

Digital Forensics

La Convenzione di Budapest e la legge nazionale di attuazione

La convenzione di Budapest sui reati informatici

La Convenzione di Budapest costituisce una pietra miliare nell'ambito della Computer Forensics e sia dei reati informatici, sia delle procedure, che sono state aggiornate.

Fissa 3 principi:

1. la raccolta non deve alterare alla fonteM
2. deve garantire la corrispondenza tra il dato acquisito e quello originale
3. deve essere garantita l'immodificabilità del dato informatico nel tempo.

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 (oggi sono una 70ina), al fine di sviluppare una legislazione nazionale completa contro la criminalità informatica, che sta procurando lesioni a diritti personali, politici.

Dal momento che i reati informatici non conoscono confini, è essenziale un quadro normativo comune che consenta ai vari di paese di perseguire le attività criminali in questo settore.

È stata (parzialmente) 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, anche per quanto riguarda il diritto di autore e la normativa in materia di pedopornografia.

Costituisce un quadro per la cooperazione internazionale tra Stati Parti del trattato sul funzionamento dell'Unione Europea, ed è completata da un primo protocollo addizionale 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. Stabilisce tutta una serie di modalità per ottenere prove ed evidenze digitali, affinché la perseguitabilità dei reati sia più veloce. Diventerà efficace quando almeno 5 stati lo avranno attuato nel proprio ordinamento.

[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 di consentire la raccolta delle prove

Non tutto di questa convenzione è stato attuato dal nostro ordinamento. È stata attuata parzialmente.

È divisa in 3 sezioni principali:

- 1.Definizione dei reati per cui prendere provvedimenti a livello nazionale (diritto penale sostanziale).
- 2.Disposizioni sull'acquisizione, la raccolta, e la conservazione del dato digitale (prima non rispondevano a criteri specifici, ma venivano effettuate con modalità tecniche lasciate alla capacità del singolo)
- 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](#)

Differenza tra codice e codice di procedura.

Codice (penale e civile): descrive il reato, la condotta criminale, la cui realizzazione comporta reato

Codice di procedura: descrive le norme con cui funziona il processo

La convenzione opera sia sul diritto penale sostanziale sia sul codice di procedura penale.

In base alla legge 547 del '93, che aggiornava il nostro codice penale, erano già stati sanzionati in materia informatica/telematica, sia nell'ipotesi in cui fosse il sistema informatico o telematico l'oggetto dell'atto criminale sia nell'ipotesi in cui il sistema fosse il mezzo di realizzazione dell'atto.

Accosta alle tradizionali figure di reato, quelle che andavano formandosi a fronte dello sviluppo della tecnologia.

Per esempio accanto al reato di violazione del domicilio fisico (art. 614) si ha l'articolo 615ter - Violazione del domicilio informatico.

L'attuazione della convenzione di Budapest impone delle modifiche al codice penale, che sono quelle che seguono.

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 va a modificare il nostro codice penale, già aggiornato con le modifiche della legge 547/93.

[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. Si stabiliscono i seguenti 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 cybercrimes 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 (attuazione del GDPR);
- al decreto legislativo 231/2001 in materia di responsabilità delle persone giuridiche (Comporta responsabilità amministrative per le spa, laddove i crimini commessi dai dirigenti apicali o del personale su indicazione dei dirigenti abbiano comportato vantaggi economici per la società);
- in tema di misure per il contrasto alla pedopornografia.

I mezzi di ricerca della prova informatica - La legge 48/2008 del 18 marzo 2008

La legge 48/2008 ha aggiornato tutta questa la parte della metodologia di ricerca della prova (ispezioni, perquisizioni, sequestri, intercettazioni delle comunicazioni, attività di apposizione dei sigilli) sulla base dei principi della Convenzione.

In relazione ai mezzi di ricerca della prova, la legge 48/2008 prevede le seguenti garanzie procedurali per la gestione dell'evidenza:

- Il dovere di conservare inalterato il dato originale nella sua genuinità e il dovere di impedire l'alterazione dell'originale.
- Il dovere di formare una copia che assicuri la conformità del dato acquisito rispetto a quello originale
- Il dovere di assicurare la non modificabilità dei dati acquisiti
- La garanzia della installazione di sigilli informatici sulle cose sequestrate (al fine dell'inalterabilità della prova)
- 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.

La legge 48 acquisisce i principi e li spalma in tutte le occasioni in cui è necessario lavorare sulle prove informatiche o in generale su sistemi informatici.

I mezzi di ricerca della prova

I mezzi di ricerca della prova sono strumenti procedurali che rendono possibile acquisire cose materiali, tracce o dichiarazioni inerenti il processo e 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, fissando le modalità procedurali corrette per assicurare il materiale probatorio.

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 accertare sulle persone, nei luoghi o nelle cose le tracce e gli altri effetti materiali del reato.

Si distingue dalla perquisizione.

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 accertare 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. (—> Questa è la prassi normale con cui l'autorità giudiziaria opera in caso di ispezioni.)

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 a impedirne l'alterazione. (—> questa è la previsione trasversale a tutti gli altri mezzi di ricerca della prova, in tutte le fasi. Il legislatore non si addentra nello specificare quali sono le misure tecniche specifiche più idonee; si è infine deciso di prevedere un'espressione di carattere generale. In questo modo ci si può sempre riferire allo stato dell'arte della conoscenza e della tecnologia.)

[Mezzi di ricerca della prova - La perquisizione](#)

La perquisizione, a differenza dell'ispezione che si concretizza nell'osservare e descrivere, è diretta a frugare per trovare elementi legati al reato.

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. È 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.](#)

Articolo nuovo, che attua il principio di garanzia dell'integrità del dato e della conformità all'originale stabilito dalla Convenzione di Budapest.

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 inerente al loro ufficio o professione.

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 inerente 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, salva, 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.

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'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici, ovvero intercorrente fra più sistemi (art. 266 bis c.p.p.).

L'intercettazione di comunicazioni fra presenti è consentita negli stessi casi in cui è consentita 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'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.**](#)

Le attenzione in ordine alle modalità con cui deve svolgersi l'acquisizione del dato informatico a fini probatori riguarda anche le attività a iniziativa della polizia giudiziaria.

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"

NB: La correttezza delle modalità di acquisizione dei dati può essere contestata nel contraddittorio.

[**Attività a iniziativa della polizia giudiziaria - Acquisizione di plichi o di corrispondenza - Art. 353 c.p.p.**](#)

Anche in questo ambito sono stati fatti degli aggiornamenti, estendendo le previsioni al contesto elettronico e telematico.

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 principio fondamentale della conformità del dato all'originale e la sua immodificabilità attraversa sia l'acquisizione dei mezzi di ricerca della prova, sia le attività della polizia giudiziaria, sia le attività del PM.

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

Ci sono stati adeguamenti anche nel Codice Privacy.

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.

(Una previsione contenuta nella Convenzione di Budapest, per la quale si richiede di agire nei confronti dei provider laddove si individui la necessità di svolgere indagini preventive.)

[Art. 132 Codice privacy, le modifiche apportate dalla legge 48/2008 \[saltato\]](#)

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. Non individuabile il concetto tradizionale di luogo di esecuzione del reato.

Inizialmente la corte di Cassazione ha disposto che la competenza in materia di reati informatici fosse il giudice del luogo in cui risiede il server attaccato. Nel tempo, la Cassazione è andata a modificare la sua posizione sulla giurisdizione dei reati informatici, partendo dal presupposto che al dato informatico si può accedere da più posti contemporaneamente. Si passa alla teoria del funzionamento delocalizzato dei sistemi informatici e su questa base definire il giudice competente.

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

[**La direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione - Articolo 12 Competenza giurisdizionale \[saltato\]**](#)

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 \[saltato\]**](#)

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 [saltato]

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 [saltato]

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".

Un'impiegata della motorizzazione di Napoli, insieme a un soggetto che aveva un'agenzia di motorizzazione, accedeva ai sistemi del Ministero dei Trasporti acquisendo dati che servivano per scopi loro personali.

Il Giudice di Napoli rimette la questione al Giudice di Roma, ritenendolo competente perché i server sono quelli del Ministro. Il Giudice di Roma si ritiene incompetente a sua volta.

La Corte di Cassazione stabilisce che il luogo di consumazione del reato è quello in cui il soggetto ha effettivamente compiuto l'azione criminale.

La competenza è pertanto del giudice di Napoli

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»