Studio Informatica Forense

POLITECNICO MILANO

Forenser Digital Investigations

DIGITAL FORENSICS

CASI PRATICI, LE INDAGINI IN MATERIA DI REATI INFORMATICI

Paolo Dal Checco

Consulente Informatico Forense

Chi sono

- PhD @UniTO nel gruppo di **Sicurezza** delle Reti e degli Elaboratori
- Passato di R&D su **crittografia** e sicurezza delle comunicazioni
- Piccole collaborazioni di docenza con **Università** degli Studi di Torino, Milano e Genova
- Consulente Informatico Forense, Perizie Informatiche per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- **Albo CTU e Periti del Tribunale di Torino**, Periti ed Esperti CCIAA TO
- Tra i fondatori e nel direttivo dell'**ONIF**, Osservatorio Nazionale d'Informatica Forense (www.onif.it)
- **Socio** IISFA, Tech & Law, Clusit, LAB4INT, Assob.It, AIP, Persone & Privacy
- www.dalchecco.it, www.ransomware.it, www.bitcoinforensics.it, www.osintbook.it
- paolo@dalchecco.it, @forensico

Cosa è l'informatica forense?

- Ricerca, identificazione, raccolta, preservazione, acquisizione, analisi, presentazione e valutazione dei dati informatici a fini probatori
- Regolata in Italia dalla Legge 48 del 2008
- Non esistono al momento altre normative o certificazioni

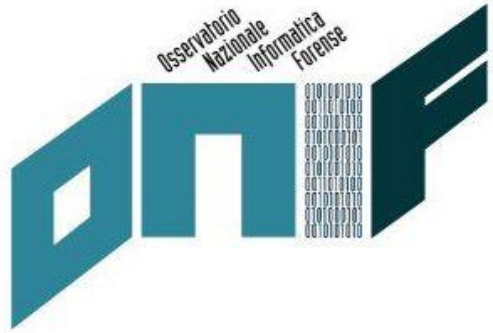
- Alcuni esempi di reati in azienda:
  - **Furto** credenziali
  - **Accesso abusivo** a dati o sistemi
  - **Violazione di Corrispondenza**
  - **Danneggiamento**
  - **Diffamazione** su internet
  - **Concorrenza sleale** e dipendente infedele
  - **Ransomware** (accesso abusivo, danneggiamento, estorsione)
  - **Phishing** (truffa, sostituzione di persona, accesso abusivo)

Chi si avvale dell'Informatica forense?

- Giudici
  - CTU in procedimenti civili
  - Perito in procedimenti penali
- Pubblici Ministeri
  - Consulente Tecnico del PM
- Avvocati
  - Consulente Tecnico di Parte
  - Perizie stragiudiziali
- Aziende
  - Investigazioni difensive
  - Gestione di incidenti di sicurezza
- Società di investigazione
- Privati

Chi è l'informatico forense?

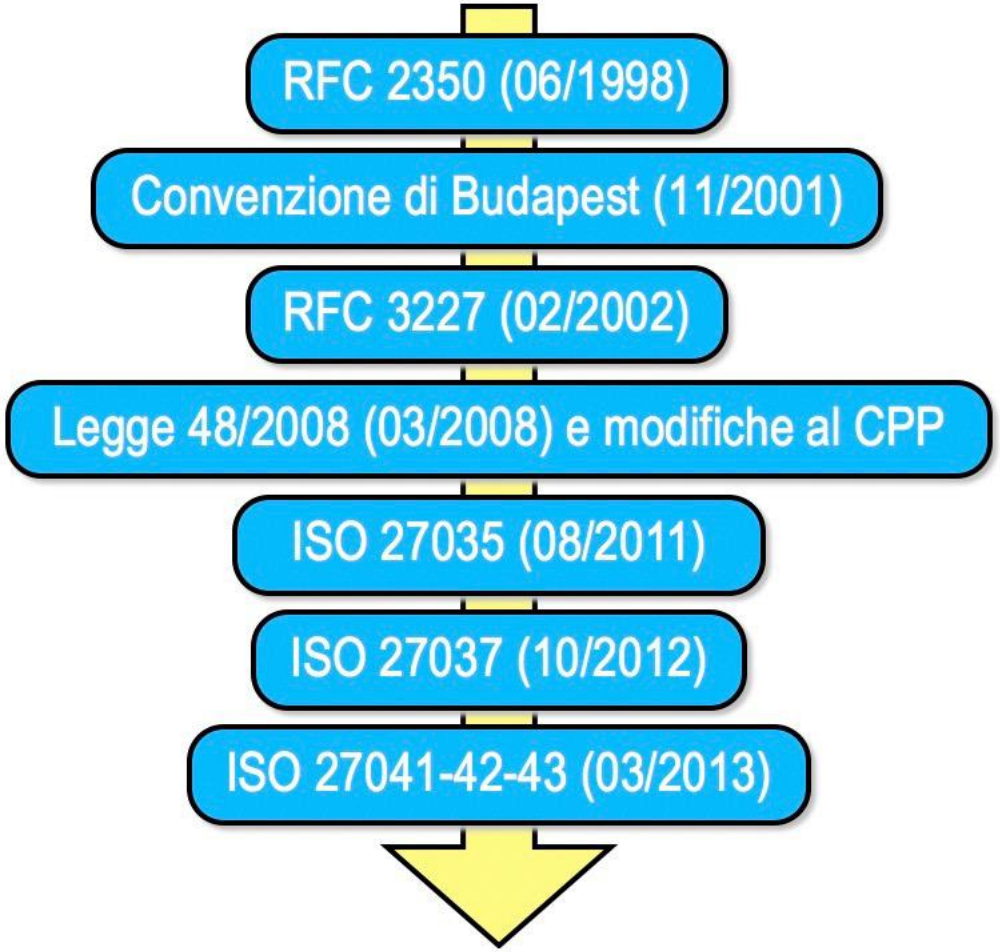
- Figura altamente tecnica ma con conoscenze delle normative da rispettare
- Conoscenze orizzontali su diversi fronti (computer, smartphone, reti, immagini, audio, criptomonete, etc…)
- Utilizzo di apparecchiature specifiche di acquisizione e software di analisi
- Impiego di metodologie che garantiscono la conservazione dei dati
- Comprensione del suo ruolo nella scala delle decisioni
- Autonomia
- Chiarezza espositiva
- Etica
- Non è un investigatore, ma lo supporta
- Non è un legale, ma lo supporta



Indagini difensive e digital forensics

- La digital forensics è un elemento strategico in ambito d'indagini difensive
- Può esser svolta direttamente da Agenzie Investigative oppure tramite Informatico Forense
- L'informatico Forense viene nominato dal cliente, oppure dallo Studio Legale o dall'Agenzia Investigativa
- Frequenti in ambito lavorativo (es. dipendente infedele), coniugale, in presenza di violenze, stalking, accesso abusivo, etc… per la raccolta di evidenze e analisi tecniche delle prove digitali

Basi tecniche e normative della digital forensics



Legge 48/2008

- Art. 244 CPP “Casi e forme delle ispezioni”
- «L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359), anche in relazione a sistemi informatici o telematici, adottando **misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione**».

Legge 48/2008

- Art. 247 CPP “Casi e forme delle perquisizioni”
- «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**».

Legge 48/2008

- Art. 254-bis: Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni)

- 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che **la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità**. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. (l., n. 48 del 2008)

Legge 48/2008

- Art. 259 CPP “Custodia delle cose sequestrate”
- «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**».

Legge 48/2008

- Art. 260 “Apposizione dei sigilli alle cose sequestrate. Cose deperibili”
- «anche di carattere elettronico o informatico»
- «Quando si tratta di dati, di informazioni o di programmi informatici, **la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità**; in tali casi, **la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria**»

Legge 48/2008

- Art. 352 Perquisizioni
- 1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, **adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi. (l., n. 48 del 2008)

Legge 48/2008

- Art. 354 - Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro
- 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 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 [253, 356; disp. att. 113] [1]. (l., n. 48 del 2008)

Legge 48/2008

- I tre punti chiave per l'informatica forense che emergono dalla Legge 48/2008 sono:
  - 1) Lasciare inalterato l'originale (write blocker)
  - 2) Copia identica all'originale (confronto)
  - 3) Copia inalterabile nel tempo (verbalizzazione hash + data certa)

- Art. 244 CPP "Casi e forme delle ispezioni"
- «L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359), anche in relazione a sistemi informatici o telematici, adottando **misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**».

La perizia informatica

- Deve contenere il risultato di un'attività d'informatica forense
- Esempio di suddivisione:
  - Frontpage
  - Incarico
  - Introduzione
  - Profilo autori (anche in fondo)
  - Catena di conservazione dei reperti o delle informazioni
  - Acquisizione dei reperti
  - Analisi tecnica
  - Conclusioni (la parte più importante)

La perizia informatica

- Legenda delle immagini (c'è chi la utilizza)
- Riferimenti bibliografici
- Eventuale asseverazione
- Allegati (c'è chi allega anche manuali degli strumenti usati…)

- Attenzione alla documentazione di ciò che viene analizzato e utilizzato (hash, data certa, cristallizzazione pagine web)
- Attenzione a non sforare nella diffamazione
- Suggerimento: spiegare le risultanze delle proprie analisi fornendo riferimenti precisi (anche se non esaustivi) a come le si sono ottenute

La raccolta delle prove

- RFC **3227**: “Guidelines for Evidence Collection and Archiving”
- Procedere metodicamente
- Catturare un’immagine completa del sistema
- Minimizzare le modifiche ai dati
- Isolare se necessario il sistema
- Prima si raccoglie, poi si analizza
- Procedere in ordine di volatilità
- Garantire la catena di custodia

La raccolta delle prove

- ISO **27037**: ““Guidelines for identification, collection, acquisition and preservation of digital evidence”
- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica, non arriva all’analisi, non si occupa di aspetti legali, strumenti, reportistica, trattamento dei dati
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio

- Si occupa di trattamento del reperto informatico e **identifica 4 fasi**:
  - 1)Identificazione (ispezione),
  - 2) Raccolta (sequestro)
  - 3) Acquisizione (copia o sequestro virtuale)
  - 4) Conservazione (conservazione e sigillo)

La raccolta delle prove

49016-17

In caso di diffusione del presente provvedimento omettere le generalità e gli altri dati identificativi, a norma dell'art. 52 d.lgs. 196/03 in quanto:
☐ disposto d'ufficio
☐ a richiesta di parte
☐ imposto dalla legge

REPUBBLICA ITALIANA
In nome del Popolo Italiano
LA CORTE SUPREMA DI CASSAZIONE
QUINTA SEZIONE PENALE

Composta da:

PUBBLICA UDIENZA
DEL 19/06/2017

MARIA VESSICHELLI - Presidente -
CATERINA MAZZITELLI
SERGIO GORJAN
GIUSEPPE DE MARZO
IRENE SCORDAMAGLIA - Rel. Consigliere -

Sent. n. sez.
1660/2017

REGISTRO GENERALE
N.9109/2017

http://www.processopenaleegiustizia.it/materiali/49016.pdf

La raccolta delle prove

2. Va giudicata ineccepibile la decisione della Corte territoriale di non acquisire la trascrizione delle conversazioni svoltesi sul canale informatico denominato '*whatsapp*', tra l'imputato e la parte offesa il 2 gennaio 2014, che la difesa dell'imputato avrebbe voluto versare agli atti del processo a riprova della inattendibilità della persona offesa, che aveva sostenuto che la relazione con l'imputato si era interrotta nell'ottobre 2013.

Deve, infatti, osservarsi che, per quanto la registrazione di tali conversazioni, operata da uno degli interlocutori, costituisca una forma di memorizzazione di un fatto storico, della quale si può certamente disporre legittimamente ai fini probatori, trattandosi di una prova documentale, atteso

La raccolta delle prove

che l'art. 234, comma 1, cod. proc. pen. prevede espressamente la possibilità di acquisire documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo (in tema di registrazione fonica cfr. Sez. 1, n. 6339 del 22/01/2013, Pagliaro, Rv. 254814; Sez. 6, n. 16986 del 24/02/2009, Abis, Rv. 243256), l'utilizzabilità della stessa è, tuttavia, condizionata dall'acquisizione del supporto – telematico o figurativo - contenente la menzionata registrazione, svolgendo la relativa trascrizione una funzione meramente riproduttiva del contenuto della principale prova documentale (Sez. 2, n. 50986 del 06/10/2016, Rv. 268730; Sez. 5, n. 4287 del 29/09/2015 – dep. 2/02/2016, Pepi, Rv. 265624): tanto perché occorre controllare l'affidabilità della prova medesima mediante l'esame diretto del supporto onde verificare con certezza sia la paternità delle registrazioni sia l'attendibilità di quanto da esse documentato.

Copia forense di un dispositivo

- E’ pratica ormai consolidata la creazione di **copia bit-a-bit** (o **bit-stream** o **copia forense** o **copia conforme** o **immagine**) del supporto originale
- L’acquisizione viene solitamente effettuata leggendo ogni bit del supporto originale (prevenendo qualsiasi possibile scrittura) e scrivendo un file “immagine” su un supporto esterno
- **Il disco originale non deve mai essere utilizzato per lanalisi dei dati**.
- Il formato “immagine” più utilizzato è il **formato RAW/DD oppure EWF (Encase Witness Format – formato proprietario di Encase)**
- Duplicazione effettuata via **software** o via **hardware**
- Indispensabile **calcolare valore hash** (una sorta di “impronta”) del file e verbalizzarlo, se possibile apporre data certa (PEC, firma digitale, raccomanata, data certa in posta)
- Essenziale non accendere il PC dopo la copia, sia che venga depositato sia che rimanga in mano alla parte per futuro deposito su richiesta

Copia forense di un disco

- Proteggere integrità dei dati da alterazioni naturali, colpose o dolose
- Utilizzare metodologia per dimostrare che non si sono verificate alterazioni
- Proteggere anche la riservatezza dei dati
- Descrivere la catena di custodia
- Utilizzare imballaggi opportuni (es. per i supporti magnetici, imballaggi antistatici) che non danneggino il supporto

Recupero dati

- Necessario avere accesso «physical»
  - Copia forense
  - Administrator
  - Chip-ff/Jtag/Flasher Box
- Aree non allocate
  - Carving
  - Magic Numbers
- Mirror dei dati in aree divers
- Cloud
- Wipe? [CCleaner, Privazer, etc…]

Strumenti per la copia: Live CD/USB

- Live CD/DVD/USB disponibili online gratuitamente e a pagamento
- DEFT, Tsurugi, Caine, Helix, Paladin, Raptor (Linux) ma anche WinFE WinPE (Win)
- Cosa si può fare:
  - Preview
  - Copie forensi
  - Hash e verifica
  - Recupero ed estrazione dati
  - Ripristino di sistemi o accesso ai dati su disco
  - Analisi forensi (meglio versione installabile)

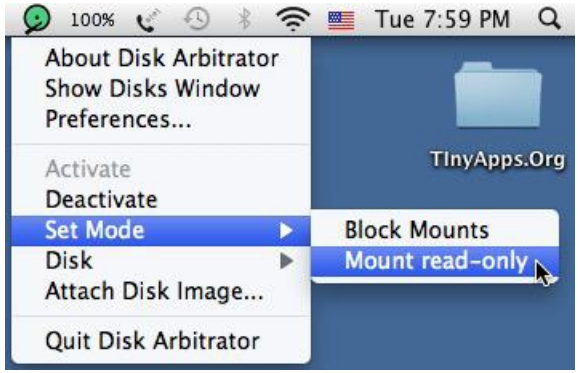
Strumenti per la copia: Hardware

Strumenti per la copia: Software

- Linux (OS con modifiche su automount)

- Windows (chiave di registro - M2CFG)

- Mac OS (Disk Arbitrator)



Copia forense di un cellulare

- Acquisizione e analisi di dispositivi mobili: “Mobile forenscs”
- Acquisizione tramite:
  - un **software di acquisizione** installato su un personal computer
  - un **dispositivo hardware** dedicato all’estrazione dei dati
  - Estrazione del chip di memoria flash e acquisizione (**chip-off**)
  - Acquisizione tramite **Flasher box** o **JTAG**
- Problematiche relative all **ripetibilità**: per diversi modelli è necessario avviare il cellulare tramite il suo sistema operativo
- Recentemente, si verifica sempre più spesso l’esigenza di **acquisizione via Cloud** (i documenti non sono sul dispositivo ma altrove (o anche altrove, come iCloud o Dropbox) → Art. 234 Prova documentale.)

Copia forense di un cellulare: strumenti

- Closed source
  - Cellebrite UFED, Micro Systemation XRY, Oxygen Forensics, Praben Device Seizure, Lantern, MOBILedit

  - Libimobiledevice
  - Adb
  - Iphone Backup Analyzer
  - Sqlite Browser

deft SANTOKU

TSURUGI LINUX

GDPR e digital forensics

Prevenzione

- identificazione degli asset
- risk analysis
- messa in opera, formazione
- controlli e verifiche (audit, vulnerability assessment, penetration test, …)

Intervento

- gestione dell'emergenza (incident response)
- analisi dell'incidente (digital forensics)
- presentazione delle risultanze
- azioni correttive

regolamento generale
sulla protezione dei dati

Cosa è la «Forensic Readiness»

E’ la **capacità di far fronte** a problematiche interne informatiche, grazie a una predisposizione ragionata, gestendo l’incidente, ripristinando le attività e mantenendo la possibilità di rivalsa

- determinazione di scenari di rischio per i modelli di business adottati (*security assessment*, *risk analysis*, …) e loro verifica (*vulnerability assessment*)
- verifica e *hardening* dei sistemi informatici, dei processi e delle postazioni di lavoro dal punto di vista del livello di sicurezza figurato
- revisione e/o produzione di documenti aziendali per la miglior gestione del patrimonio informatico (stesura policy, moduli di presa in carico, uso e riconsegna di beni e servizi aziendali informatici da parte del personale dipendente e dei collaboratori/partner, …)
- formazione del personale per il corretto impiego degli strumenti informatici

- gestire l’incidente informatico (compromissione di sistema, trafugazione di dati, …) in funzione della *business continuity* e della collezione probatoria delle evidenze informatiche
- ricostruire le cause, determinare le origini, quantificare i danni e fornire gli elementi necessari per la tutela anche giudiziaria del patrimonio aziendale informatico
- definire e gestire un processo di rafforzamento delle difese e dei controlli a tutela dei dati

Preparare la forensic readiness

- Identificare le possibili fonti e i diversi tipi di evidenze digitali
- Determinare i requisiti tecnici e legali per la raccolta delle evidenze digitali
- Individuare e definire le risorse necessarie per la raccolta sicura e conforme alla legge di evidenze digitali
- Stabilire Policy e sistemi per gestione e conservazione sicura delle sorgenti di informazione:
  - Email, Log, Documenti
- Dotarsi di sistema di monitoraggio in grado di rilevare i principali incidenti
- Definire in quali circostanze si rende necessaria attivare una investigazione informatica completa
- Formare e sensibilizzare lo staff stabilire ruoli nella gestione delle prove
- Assicurare una revisione legale delle procedure per agevolare le azioni di risposta all'incidente
- Verificare i contratti e gli SLA con in fornitori

Alcuni mezzi per agevolare la forensic readiness

1. IDS/IPS
2. Proxy, VPN, Router, Firewall, Antivirus
3. Log applicativi, Log di Sistema (PC e Server)
4. Server/relay DNS e DHCP
5. Server di posta
6. Directory Server
7. Sistema gestione log (SIEM)
   - Raccolta
   - Parsing
   - Correlazione
   - Analisi Allarme
   - Storicizzazione Tamper Proof

Post incident

- Acquisizione (con firma digitale, hash e documentazione continua)
  - Identificazione del perimetro e isolamento dei sistemi
  - Dump di rete
  - Copia forense dei sistemi
  - Live Forensics, Data Recovery, eDiscovery
  - Avvio procedure per recupero log da SIEM
- Analisi:
  - Log
  - Copie forensi
  - Dati live
- Obiettivi da identificare con ricostruzione temporale:
  - Modalità d'ingresso (se possibile anche autori)
  - Durata del breach (sé è terminato)
  - Entità del danno (accesso ai dati, sistemi, etc…)

Post incident

- Strumenti hardware
  - Write Blocker
  - Copiatori forensi
- Strumenti software
  - TSURUGI, DEFT, CAINE, PALADIN, Raptor, SIFT
  - FTK, X-Ways, Axiom
  - Risorse varie
- Servizi
  - Timestamp digitale
  - AWS, Cloud
  - Decryption, Rainbow Table

Acqusizione chat Whatsapp/Telegram

- Sempre più spesso fonti di prova
- L'ideale è acquisirle da copia forense
- Quando non è possibile (es. Huawei, Telegram, etc…) si possono esportare
  - Download da App (funzionalità introdotta con GDPR)
  - Invio della chat via email, Airdrop, bluetooth, beam, Dropbox, etc…
  - Possibilità di acquisizione tramite Whatsapp Web o Telegram Desktop Client

Acqusizione chat Facebook, Linkedin, Twitter, etc…

- Sempre più spesso fonti di prova
- L'ideale è acquisire intero profilo
  - Utilizzo funzione di esportazione del profilo, che grazie al GDPR stanno adottando tutti i provider
- Se non possibile esportare profilo, acquisire come risorsa web (es. FAW)
- Non esistono tabulati delle chiamate Messenger/Whatsapp/Telegram/Signal, sono solo sugli smartphone degli interlocutori

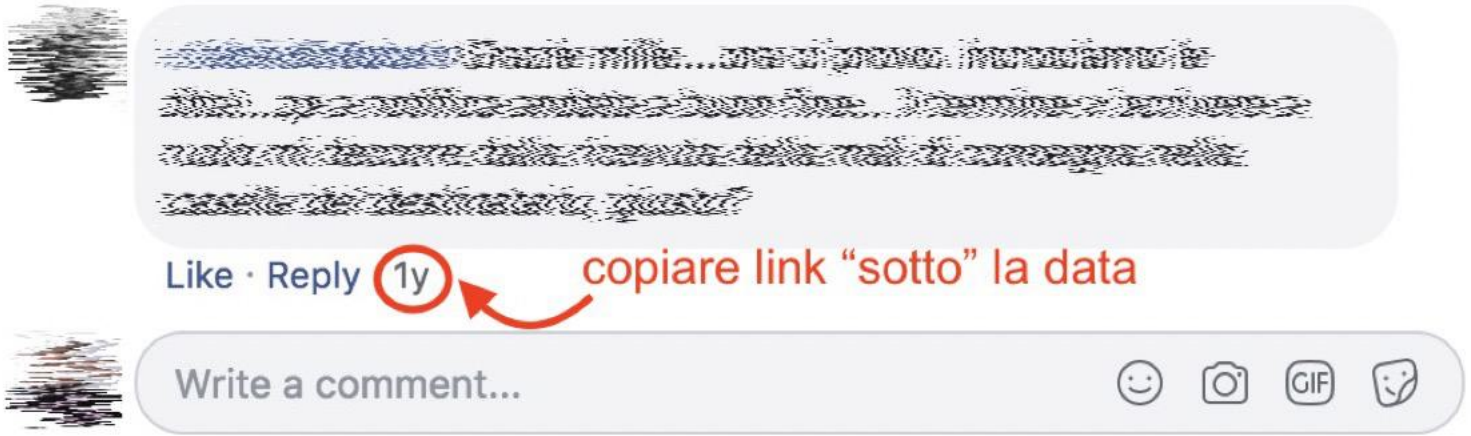
Acqusizione chat Facebook, Linkedin, Twitter, etc…

- Identificare correttamente il post/immagine/pagina da acquisire
- Fornire URL (indirizzo presente su barra del browsser)
- Se possibile, cercare il codice ID (es. **findmyfbid.com** per FB)

- Per i post su Facebook:

Acqusizione chat Facebook, Linkedin, Twitter, etc…

- Per i commenti su Facebook:



Acqusizione chat Facebook, Linkedin, Twitter, etc…

- Per i tweet:

Acqusizione tabulati telefonici/telematici

- L'utente può scaricare i suoi tabulati delle chiamate e SMS uscenti dal proprio profilo presso l'opeartore
- Per le chiamate/SMS entranti va fatta richiesta da parte di Legale (quasi mai soddisfatta) o da parte di PM
- Attenzione alla distinzione tra tabulati TELEFONICI e TELEMATICI
- Tabulati Telefonici (24 mesi):
  - Chiamate, chiamato, cella chiamate, cella chiamato (se stesso operatore), imsi, imei, tipo chiamata (solo di chiamate e SMS)
- Tabulati Telematici (12 mesi)
  - Inizio e fine navigazine, IP, cella
- Attenzione a chiedere sempre anche i tabulati telematici, poi (dopo 12 mesi) quando ci si accorge che servono gli IP/celle è troppo tardi
- Se presente intercettazione, allora si hanno anche i contenuti

Acqusizione registrazioni audio

- Sempre più spesso fonti di prova
- L'ideale è acquisirle da copia forense
- Se registrate e salvate direttamente su cloud (es. registrazioni telefoniche o ambientali) può essere una utile controprova
- Se provenienti da telefonate, valutare acquisizione anche del tabulato
- Quando non è possibile (es. Huawei, Telegram, etc…) si possono esportare:
  - Eseguire backup itunes/Android
  - Uso Ifunbox (per iOS) e accedo ai folder del recorder
  - Se possibile, acquisire anche tabulati con durata telefonate (uscenti, per quelle entranti è più complicato)
  - Usare funzioni di backup dei tool (es. Telegram «GDPR» Export, etc…)

Acquisizione risorse Internet

- Pagine web, profili social, gallerie Facebook, email, twitter, Forum, Blog, VoIP, P2P, Instagram
- Problemi con risorse web:
  - Non è facile comprendere **dove si trovino**
  - Possono trovarsi su **sistemi ubicati in Italia o all'estero**
  - Spesso è difficile procedere con un'acquisizione tradizionale per motivi **tecnici** (es. sistemi virtualizzati, database molto grandi, ecc.) e/o **procedurali** (es. sistemi ubicati all'estero)
  - Difficoltà nell'**identificare il proprietario**
  - Ancora più facile **alterare, nascondere o distruggere le informazioni**

Acquisizione risorse Internet

- Non possiamo utilizzare gli strumenti tipici della Computer Forensics
- **Non è sufficiente:**
  - Fare **screenshot** della pagina
  - Salvare la pagina in locale e **produrre stampa** (es. email visualizzata su webmail)
- E' quindi necessario individuare una procedura che garantisca:
  - Corrispondenza con loriginale
  - Riferibilità a un ben individuato momento

Acquisizione risorse Internet

- Email?
  - Header RDF 822
  - IMAP, POP3

- Cloud?
  - Uso client standard?
  - Software forensi?

Acquisizione risorse Internet

- Esempio di passi di un processo di acquisizione:
  - **Registrazione delle azioni** in corso sul PC (es. CamStudio)
  - **Registrazione del traffico di rete** generato e/o ricevuto (es. WireShark)
  - **Impostare il DNS di sistema** con un DNS pubblico noto (es. 8.8.8.8 – Google)
  - **Sincronizzare l'orologio** di sistema tramite un server NTP (es. Istituto Elettrotecnico Nazionale Galileo Ferraris – ntp.ien.it)
  - **Identificare lindirizzo IP** da cui si sta effettuando l'accesso e sul quale risiede la risorsa (es. "dig -t a www.dalchecco.it)
  - Se si tratta di mail, identificare dove si trova il server (es. **dig –t mx dalchecco.it**)
  - Avviare le operazioni di **mirroring, navigazione e/o download** della "digital evidence" che si vuole acquisire

Acquisizione risorse Internet

- Al termine delle operazioni di acquisizione:

  - **Interrompere il software di acquisizione** del traffico di rete
  - **Firmare digitalmente** (e possibilmente con marca temporale) il file con il traffico di rete
  - **Calcolare l'hash dei file scaricati**
  - Fare un unico archivio **contenente il traffico di rete e i file scaricati**
  - Firmare digitalmente il file ottenuto e calcolare l'hash
  - **Interrompere la registrazione** delle azioni a monitor

Acquisizione risorse Internet: FAW

- Soluzione all-in-one locale con possibilità di storage remoto
- Disponibile per WIN installabile e in macchina virtuale
- Esegue i vari passaggi “forensi” in automatico, video, dump di rete, etc…
- Versione gratuita e a pagamento

Acquisizione risorse Internet: OSIRT

- Gratuito e Open Source
- Non raggiunge il livello di FAW
- Buona base per acquisizione forense da integrare con altri strumenti o servizi
- Non acquisisce rete, chiavi SSL, etc…

Acquisizione risorse Internet: altre soluzioni commerciali

- Legaleye (legaleye.cloud)
- Cliens Prova Digitale (provadigitale.cliens.it)
- Legalizer (legalizer.it)
- Safe Stamper (www.safestamper.com)
- Kopjra (kopjra.com)
- PageFreezer (pagefreezer.com)

Acquisizione risorse Internet: altre soluzioni gratuite

- Acquisire anche con servizi terzi, gratuiti:
  - **Web.archive.org** (**attenzione**, rimane online, non indicizzato)
  - **Archive.is** (**attenzione attenzione**, rimane online, **indicizzato**, rimuovono su richiesta ma sono lenti), si può scaricare dump
  - **Perma.cc** (rimane online, anche in modo privato), si scarica dump
  - **webrecorder.io** (remote browser, si scarica dump)
    - github.com/webrecorder/webrecorderplayer-electron
  - **freezepage.com**

Grazie per l’attenzione!