MODULO 1

ASPETTI SOSTANZIALI E PROCESSUALI DEI REATI INFORMATICI E DELLE PROBLEMATICHE INFORMATICHE DELL'INVESTIGAZIONE

Procuratore Aggiunto della Repubblica presso il Tribunale di Benevento **Dott. Gianfranco Scarfò**

REATI INFORMATICI E REATI SU INTERNET

INFORMATICA ED INDAGINI PENALI

DISTINZIONE FRA REATI INFORMATICI E REATI COMMESSI CON UTILIZZO DI SISTEMI INFORMATICI OVVERO SU INTERNET

LE CONDOTTE COSTITUENTI REATO COMMESSE CON STRUMENTI INFORMATICI OVVERO SULLA RETE SONO SEMPRE PIÙ DIFFUSI MA SI DIFFERENZIANO DAI REATI INFORMATICI IN SENSO STRETTO.

GLI STRUMENTI DI INVESTIGAZIONE INFORMATICA, OVVERO SU SUPPORTI INFORMATICI INVECE RIGUARDANO L'INTERO SPETTRO DELLE INVESTIGAZIONI PERCHÉ VIRTUALMENTE OGNI REATO «INCORPORA» ELEMENTI INFORMATICI ANCHE SOLO SOTTO IL PROFILO DELLA PROVA DELLO STESSO (SI PENSI ALLE COMUNICAZIONI INTERPERSONALI VIA MESSAGGISTICA O CHAT)

REATI INFORMATICI IN SENSO STRETTO

La distinzione fra reati informatici e reati commessi su rete o con strumenti informatici si coglie a pieno con l'esempio della truffa.

La maggior parte delle truffe *on line* non sono frodi informatiche in senso stretto posto che gli artifizi e raggiri che costituiscono l'elemento principale della truffa semplicemente avvengono su e mediante internet o altri strumenti anche social della rete

ART. 640 CP

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032....)

ART. 640 TER CP

Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema (6).

ART. 640 TER CP

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età

CRITERI DISTINTIVI

SECONDO LA GIURISPRUDENZA VI E' UN RAPPORTO DI SPECIALITA'

La fattispecie della frode informatica è posta a tutela sia della riservatezza e della regolarità dei sistemi informatici che del patrimonio altrui; l'evento consiste nel conseguimento da parte del soggetto attivo di un ingiusto profitto con altrui danno;

condotta consistente nell'alterazione del funzionamento del sistema informatico o telematico, ovvero in un intervento non autorizzato (PARIMENTI ALL'IPOTESI DI CUI AL 615 TER)

Nella frode informatica l'attività fraudolenta dell'agente non investe il soggetto passivo, di cui manca l'induzione in errore, ma il sistema informatico di pertinenza della stessa persona offesa che viene manipolato al fine di ottenere una penetrazione

CRITERI DISTINTIVI

QUEL CHE CONTA PERTANTO E' L'INTROMISSIONE O INTERVENTO NON AUTORIZZATO NEL SISTEMA INFORMATICO ALTRUI ED IL CONSEGUIMENTO DI PROFITTO.

SE AL FINE DI INTROMETTERSI NEL SISTEMA ALTRUI VI E' STATA CONCRETAMENTE UNA INDUZIONE IN ERRORE DI UN ESSERE UMANO, CIO' NON MUTA LA QUALIFICAZIONE GIURIDICA (da ultimo sul punto anche alcune recenti decisioni della Procura Generale presso la Corte d'Appello di Napoli)

LA CASISTICA INFATTI MUTA DALLA INTROMISSIONE ALL'INSAPUTA DEL TITOLARE OVVERO ALL'ACQUISIZIONE CON MEZZI INSIDIOSI LE «CHIAVI» DEL SISTEMA INFORMATICO; A LORO VOLTA I MEZZI POSSONO ESSERE PURAMENTE INFORMATICI (SMS - SMISHING, LINK – PHISHING,) OVVERO PARZIALMENTE «UMANI» (LA TELEFONATA – VISHING - SIMULANDO DI ESSERE OPERATORI ED INDUCENDO ALLA RIVELAZIONE DI PASSWORD)

IDENTITÀ DIGITALE

AGGRAVANTE DELLA FRODE INFORMATICA

se il fatto è commesso con furto o indebito utilizzo dell'identità digitale

Il legislatore non ha fornito alcuna definizione dell'"identità digitale«.

CASS 40862/2022

In tema di frode informatica, la nozione di "identità digitale", che integra l'aggravante di cui all'art. 640-ter, comma terzo, cod. pen., non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati. (Fattispecie in cui è stata ritenuta l'aggravante in un caso di accesso abusivo a un servizio di "home banking")

LA FRODE INFORMATICA; LE CONDOTTE

FORNITORE DEL CONTO RICETTORE DEL PROFILI

DIFFICOLTÀ DI INDIVIDUAZIONE DELL'AUTORE DELLA CONDOTTA DI INTROMISSIONE.

RELATIVA MAGGIORE FACILITÀ DI INDIVIDUAZIONE DI CHI HA FORNITO IL CONTO O POSIZIONE DI « *ARRIVO*» o «*PASSAGGIO*» DEL PROFITTO.

QUEST'ULTIMO SOLO CON UNA PROVA RIGOROSA PUO' ESSERE RITENUTO CONCORRENTE EX 110 CP NEL 640 TER

LA FRODE INFORMATICA; LE CONDOTTE

FORNITORE DEL CONTO RICETTORE DEL PROFITTO

PIÙ AGEVOLE (E COMUNE IN GIURISPRUDENZA) LA QUALIFICAZIONE COME<u>RICICLAGGIO EX</u> ART. 648 BIS CP

CASS 19125/23

Integra il delitto di riciclaggio la condotta di chi, senza aver concorso nel delitto presupposto, metta a disposizione il proprio conto corrente per ostacolare l'accertamento della delittuosa provenienza delle somme da altri ricavate mediante frode informatica, consentendone il versamento su di esso e provvedendo, di seguito, al loro incasso. (Fattispecie in cui l'imputato, a seguito dell'abusivo accesso effettuato da altri nella "home banking" della persona offesa, ricevuti due bonifici con accredito delle somme illecitamente prelevate, aveva richiesto, nello stesso giorno, l'emissione di due vaglia postali, incassando il denaro provento del delitto di cui all'art. 640-ter cod. pen.).

LE SINGOLE CONDOTTE

FORNITORE DEL CONTO DI ARRIVO DEL PROFITTO

INDICI DI RESPONSABILITÀ

- Titolarità del conto di ricezione
- Mancanza di denuncia di smarrimento dei documenti ovvero dello strumento per monetizzazione (carta di credito, postepay
- Vicinanza temporale fra attivazione conto ed operazione illecita
- Rinvenimento materiale (ad es con perquisizione) del titolo legittimante del conto

LA FATTISPECIE EX ART. 493 ter CP

SI APPLICA AI SOLI CASI DI MANCANZA DI INTROMISSIONE NEL SISTEMA INFORMATICO

MERO UTILIZZO - NON AUTORIZZATO -MATERIALE DELLA CARTA (C/O NEGOZI O ATM) DI CUI SI E' ENTRATI IN POSSESSO (ANCHE MEDIANTE REATI CONTRO IL PATRIMONIO CHE CONCORRONO)

CASS 2019

Integra il delitto di indebita utilizzazione di carte di credito di cui all'art. 55, comma 9, d.lgs. 21 novembre 2007, n. 231 (oggi art. 493-bis cod. pen.), e non quello di frode informatica ex art. 640-ter cod. pen., la condotta di colui che, ottenuti, senza realizzare frodi informatiche, i dati relativi ad una carta di debito o di credito, unitamente alla stessa tessera elettronica, la utilizzi indebitamente per effettuare prelievi di denaro. (Fattispecie relativa ad indebito utilizzo di una carta bancomat sottratta dall'imputato alla fidanzata in uno al codice PIN).

ART. 615 TER C.P.

«chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo, è punito con la reclusione fino a tre anni»

RILEVANZA DELLE AGGRAVANTI (c. 2 e 3)

DA UN PUNTO VISTA SOGGETTIVO – FATTO COMMESSO da pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema

Tema controverso con più interventi delle Sezioni Unite

Cass 17551/23

integra il delitto previsto dall'art. 615-ter, comma terzo, cod. pen. la condotta dell'ufficiale di polizia giudiziaria che acceda alla banca dati interforze in violazione delle procedure interne di carattere autorizzativo e per finalità meramente esplorative, onde acquisire informazioni su colleghi e personaggi pubblici in assenza anche solo di un qualificato sospetto idoneo a stimolare l'attività di iniziativa della polizia giudiziaria.

ART. 615 TER C.P.

DA UN PUNTO DI VISTA OGGETTIVO – FATTO COMMESSO SU SISTEMA DI INTERESSE PUBBLICO

CASS 24576/21

In tema di accesso abusivo ad un sistema informatico, ai fini della configurabilità dell'aggravante di cui all'art. 615-ter, comma terzo, cod. pen., sono "di interesse pubblico" solo i sistemi informatici o telematici di pubblica utilità, ossia destinati al servizio di una collettività indifferenziata e indeterminata di soggetti, e non anche quelli a vario titolo riconducibili all'esercizio di diritti, pur di rilevanza collettiva, costituzionalmente tutelati. (Fattispecie in cui la Corte ha escluso la sussistenza dell'aggravante nel caso di accesso abusivo al sito del fondatore di un movimento politico di livello nazionale utilizzato per la divulgazione delle idee di detto movimento)

ART. 617 SEXIES C.P.

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

CASS 39678/17

La fattispecie incriminatrice di cui all'art. 617-sexies cod. pen. configura un peculiare reato di falso che si caratterizza per il dolo specifico del fine di procurare a sé o ad altri un vantaggio, non necessariamente patrimoniale, o di arrecare ad altri un danno, nonché per la particolare natura dell'oggetto materiale, costituito dal contenuto di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. (Nella specie, la Corte di cassazione ha ravvisato la sussistenza del reato "de quo" nel caso della falsificazione della notifica di avvenuta lettura di una e-mail di convocazione per una procedura concorsuale indetta da un ente locale).

617 QUATER CP

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma

CASS 17814/23

In tema di installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, sussiste la circostanza aggravante di cui al combinato disposto degli artt. 617-quinquies, comma secondo, e 617-quater, comma quarto, n. 1, cod. pen., nel caso di apposizione, presso il "bancomat" di un istituto di credito, di un dispositivo (cd. "skimmer") finalizzato ad intercettare comunicazioni di dati, posto che l'attività bancaria di raccolta del risparmio costituisce, ai sensi dell'art. 359, n. 2, cod. pen., servizio di pubblica necessità, in quanto, pur avendo natura privatistica, siccome esercitata in forma di impresa da soggetti privati quali gli istituti di credito, corrisponde ad un interesse pubblico e il suo esercizio è subordinato ad autorizzazione ed è sottoposto a controllo da parte delle competenti Autorità amministrative.

ART. 635 BIS CP

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni

CASS 54715/16

Il reato di frode informatica si differenzia da quello di danneggiamento di dati informatici, di cui agli artt. 635 bis e ss. cod. pen., perché, nel primo, il sistema informatico continua a funzionare, benché in modo alterato rispetto a quello programmato, mentre nel secondo l'elemento materiale è costituito dal mero danneggiamento del sistema informatico o telematico, e, quindi, da una condotta finalizzata ad impedire che il sistema funzioni

ART. 635 TER CP

- 1. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
- 2. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni

Non si rinvengono decisioni della Cassazione.

ART. 635 QUATER CP

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni

CASS 4470/20

Ai fini della configurabilità del reato di cui all'art. 635-quater cod. pen., per "sistemi informatici o telematici", oggetto materiale della condotta di danneggiamento, deve intendersi un complesso di dispositivi interconnessi o collegati con unità periferiche o dispositivi esterni (componenti "hardware") mediante l'installazione di un "software" contenente le istruzioni e le procedure che consentono il funzionamento delle apparecchiature e l'esecuzione delle attività per le quali sono state programmate. (Fattispecie relativa alla distruzione, al fine di perpetrare un furto, di due telecamere esterne dell'area di accesso ad una casa di cura, che la Corte ha riconosciuto come componenti periferiche di un "sistema informatico" di videosorveglianza, in quanto strumenti di ripresa e trasmissione di immagini e dati ad unità centrali per la registrazione e memorizzazione).

AGGRAVANTE OPERATORE DEL SISTEMA

COMUNE A MOLTE FATTISPECIE (ANCHE AI FINI DELLA PROCEDIBILITÀ D'UFFICIO) E L'AGGRAVANTE DELL'OPERATORE DEL SISTEMA

DEFINIZIONE AMPIA IN GIURISPRUDENZA

CASS 7775/22

In tema di accesso abusivo a un sistema informatico, ai fini dell'integrazione della circostanza aggravante di abuso della qualità di operatore del sistema, riveste siffatta qualifica non solo il titolare di poteri decisori sulla gestione dei contenuti o sulla configurazione del sistema, ma anche colui che, pur se destinato a svolgere compiti meramente esecutivi, sia comunque abilitato a operare sul sistema, modificandone i contenuti o la struttura.

CASS 17318/19

In tema di frode informatica, l'installatore di "slot machine" che provveda all'inserimento di schede informatiche dallo stesso predisposte, e tali da alterare il sistema informatico così da eludere il pagamento delle imposte previste con conseguente ingiusto profitto, assume la qualifica di operatore di sistema, rilevante ai fini dell'integrazione della circostanza aggravante prevista dall'art. 640-ter, secondo comma, cod. pen

LE NORME IN MATERIA DI COMPETENZA

Secondo l'art. 51 cpp i delitti informatici sono di competenza per le indagini e l'esercizio dell'azione penale della Procura distrettuale e non delle Procure circondariali

3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414-bis, 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 609-undecies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente

PROBLEMATICA PERSISTENTE NECESSITÀ DI TALE NORMA

- DIFFICOLTÀ (SOPRATTUTTO PER IL NUMERO DI PROCEDIMENTI) DI INVESTIGAZIONE ED ACCERTAMENTO PER LE PROCURE DISTRETTUALI
- AMPIA DIFFUSIONE DEI MEZZI INVESTIGATIVI E DELLE CONOSCENZE TECNICHÉ A LIVELLO NON SOLO DISTRETTUALE

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

DISTINZIONE – ALLO STATO – FRA ACQUISIZIONE DI DATI PREESISTENTI E STATICI E DATI DINAMICI.

MENTRE PER L'ACQUISIZIONE DEI SECONDI SI PROCEDE A MEZZO INTERCETTAZIONE TELEMATICA OVVERO PER CAPTATORE (CON AUTORIZZAZIONE DEL GIUDICE), PER I SECONDI SI PROCEDE A MEZZO DI PERQUISIZIONE E SEQUESTRO CON ATTO DEL PM (OVVERO DELLA PG SOGGETTO A CONVALIDA DEL PM) RIENTRANDO TALE RICERCA NELL'AMBITO DELLA PROVA DOCUMENTALE.

Fino a pochi mesi fa era granitica la giurisprudenza di legittimità nel senso di ricondurre l'acquisizione di simili comunicazioni scritte nell'alveo della prova documentale ex art. 234 c.p.p. e, quindi, di non ravvisare la necessità per la loro acquisizione in fase di indagini di un provvedimento del P.M. e men che meno del magistrato giudicante.

Fra le tante

- Cass., Sez. 6 - , Sentenza n. 12975 del 06/02/2020 Ud. (dep. 27/04/2020), Ceriani, Rv. 278808 – 02 "In tema di mezzi di prova, i messaggi di posta elettronica memorizzati nell'account o nel computer del mittente ovvero del destinatario hanno natura di documenti informatici, sicché la loro acquisizione processuale non soggiace alla disciplina delle intercettazioni di cui all'art. 266-bis cod. proc. pen., che postula la captazione di un flusso di comunicazioni in atto, ma avviene ai sensi dell'art. 234 cod. proc. pen.";

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

Il quadro è mutato con la citata sentenza costituzionale n. 170/2023 che, nel risolvere un conflitto di attribuzioni ex artt. 68, comma 3, e 134 Cost. tra il Senato della Repubblica e la Procura della Repubblica presso il Tribunale di Firenze ha ricondotto le e-mail e le chat whatsapp (e simili) nella nozione di "corrispondenza" e "comunicazione" rilevante ex art. 15 Cost. (oltre che ex art. 68, comma 3, Cost).

Poi sono intervenute sentenze della VI sezione n. 44154/2023 "laria" e n. 44155/2023 "Kolgjokaj" in materia di acquisizione di CHAT (SKY ECC) di sistema criptato dalla Francia che – in alcuni passaggi – sembrano quasi « evocare» la necessità di un'autorizzazione giudiziale per l'acquisizione della messaggistica chat

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

<u>MA:</u>

La questione delle sentenze « gemelle» è di fatto rimessa alle Sezioni Unite con quesito che esula dalla problematica della perquisizione e del sequestro

- 1) se, in tema di mezzi di prova, la acquisizione mediante O.E.I. di messaggi su chat di gruppo presso A.G. straniera che ne ha eseguito la decrittazione costituisca o meno acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-bis cod. proc. pen.
- 2) se, inoltre, tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della A.G. nazionale.

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

2. La Cassazione con altra sentenza ha ribadito i vecchi principi (cass 46482/23)

Le norme che disciplinano la ricerca dei dati informatici (anche costituenti corrispondenza), quindi, sono: - art. 244 cod. proc. pen. (nella parte in cui fa riferimento alla ispezione informatica); art. 247, comma 1-bis, cod. proc. pen. In tema di perquisizione informatica, art. 254-bis cod. proc. pen. in tema di sequestro di dati informatici presso fornitori di servizi, art. 352, comma 1-bis, cod. proc. pen., per le medesime attività compiute di iniziativa dalla polizia giudiziaria alle date condizioni.

In tutti questi casi, le regole applicabili, invero, sono sostanzialmente prescrizioni mirate all'utilizzo di protocolli di sicur<mark>ezza per la</mark> non dispersione dei dati e la garanzia di conformità dei dati acquisiti.

In tale ambito, invece, mancano del tutto disposizioni che siano sanzionate con nullità o inutilizzabilità: il mancato rispetto delle regole di protezione dei dati potrà essere valutato, sul piano processuale, per valutare la affidabilità della prova raccolta ma non per espungerla dal processo.

In tutti questi casi, quindi, è agevole anche concludere (con riferimento a quanto in questa sede assume rilievo) che l'attività di acquisizione della documentazione nella fase delle indagini spetta al Pubblico ministero senza necessità di provvedimento del giudice.

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

SI TRATTA PERTANTO DI ARGOMENTO MOLTO DELICATO E SUSCETTIBILE DI RIFORME LEGISLATIVE. PERALTRO OCCORRE PRENDERE ATTO CHE IL SISTEMA NORMATIVA ORA PREVEDE CAUTELE PER L'ACQUISIZIONE DEI DATI COMUNICATIVI DA INTERCETTAZIONE E <u>NULLA PREVEDE PER I DATI CONTENUTI SU SUPPORTI INFORMATICI</u> ACQUISITI NELLE INDAGINI CHE CONTENGONO NORMALMENTE DATI BEN PIU' LESIVI DELLA PRIVACY DEI SOGGETTI COINVOLTI.

IN TAL SENSO SI E' MOSSA INFATTI LA GIURISPRUDENZA DELLA CASSAZIONE CHE HA INTERPOSTO LÌMITI DI PROPORZIONE ALL"ACQUISIZIONE, ANALISI ED UTILIZZAZIONE DI TALI DATI.

perché allorquando l'individuazione degli elementi necessari ai fini dell'accertamento dei fatti non sia immediata, ma presupponga operazioni non eseguibili dagli operanti incaricati dell'esecuzione del sequestro, quali un'analisi tècnica (ad esempio, da parte di esperti informatici) ovvero il vaglio di ampia mole di dati, il principio di proporzionalità del sequestro non può prescindere dall'apprezzamento del dato temporale; l'autorità giudiziaria, quindi, può disporre un sequestro dai contenuti molto estesi, provvedendo, tuttavia, nel rispetto del principio di proporzionalità ed adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti (ex multis Cass 2018, n. 4857)

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

IN OSSEQUIO A TALE IMPOSTAZIONE MOLTE PROCURE FRA CUI QUELLA DI BENEVENTO HANNO EMESSO DIRETTIVE VOLTE ALLA;

- 1) Celere estrazione di copia forense con restituzione dell'apparecchio subito dopo il completamento di tale operazione;
- 2) selezione, estrazione e riversamento agli atti del procedimento dei soli dati rilevanti ai fini dell'accertamento dei reati per i quali si procede, salva separata comunicazione di ogni notizia di reato diverso acquisita;
- 3) restituzione all'avente diritto della copia forense e di ogni altra copia dei dati estratti dal dispositivo o distruzione della copia dei dati riprodotti su qualsiasi supporto informatico diverso dalla copia forense, al più tardi prima del deposito degli atti ex art 415 bis cp o dell'esercizio dell'azione penale allorché tale deposito non sia previsto;
- 4) alle richieste cautelari vanno allegati solo i dati ritenuti rilevanti, in nessun caso la copia forense integrale, comprendete anche la parte ritenuta irrilevante, può essere allegata agli atti nella fase cautelare sia pure in forma di annotazione e/o copia cartacea;

L'ACQUISIZIONE DEI DATI INVESTIGATIVI INFORMATICI

ALCUNE PRONUNCE RECENTI DELLA CASSAZIONE

CASS 3591/22

E' legittima l'acquisizione di un "file" in corso di redazione su "personal computer" mediante "screenshot" eseguito da un captatore informatico, trattandosi di mera constatazione del dato informatico in corso di realizzazione, oggetto di "comportamento comunicativo", suscettibile di intercettazione ed anche di videoregistrazione ai sensi dell'art. 266-bis cod. proc. pen., e non di perquisizione informatica diretta alla ricerca ed estrapolazione di dati preesistenti

Cass 25667/18

Non configura un provvedimento di sequestro di dati informatici, neppure implicito, l'annotazione nel verbale di perquisizione di informazioni visionate dagli operanti di polizia giudiziaria ed estrapolate direttamente dal telefono nel corso della perquisizione, senza effettuare alcuna copia dei dati stessi.

GRAZIE PER L'ATTENZIONE

MODULO 2

LE TUTELE NEGLI ACCERTAMENTI RISORSE

Maresciallo Ordinario Emiliano Batori
GRUPPO BENEVENTO - GUARDIA DI FINANZA

LE TUTELE NEGLI ACCERTAMENTI

MISURE MINIME DI SICUREZZA DA OSSERVARE PER LA NAVIGAZIONE SUL WEB

PROTEGGERE IL PROPRIO INDIRIZZO IP

Nelle successive slide verrà evidenziata l'importanza, per l'operatore, di adottare delle attenzioni finalizzate a mantenere riservato e non conoscibile il proprio <u>indirizzo ip</u> durante la navigazione sulla rete Internet.

L'obiettivo è quello di neutralizzare azioni di profiling generali o mirate che possano esporre e/o palesare il binomio informativo, delicato e sensibile, composto da OPERATORE AG/PG e INFORMAZIONE GIUDIZIARIA.

In ragione dei numerosi scenari, talvolta imprevedibili, a cui si è esposti durante la navigazione nel web nonché alle eventuali conseguenze derivanti da una raccolta dati di varia natura effettuata dai sistemi informatici, laddove possibile, l'utilizzo di VPN per la navigazione su internet può contribuire ad una tutela efficace.

IP LOGGER

MISURE MINIME DI SICUREZZA DA OSSERVARE PER LA NAVIGAZIONE SUL WEB

A titolo di esempio, per evidenziare l'opportunità dell'adozione di accorgimenti volti alla sicurezza dei dispositivi utilizzati per le attività di ricerca online di informazioni connesse ad attività giudiziarie, si segnalano gli IP LOGGER.

Servizi disponibili sulla rete o software facilmente reperibili finalizzati all'individuazione e conoscibilità di un indirizzo IP di un dispositivo attraverso una interazione di varia natura, all'esito della quale, il dispositivo fornisce le informazioni attese senza la consapevolezza del proprietario.

Unitamente all'INDIRIZZO IP si acquisiscono altre informazioni che possono aiutare e contribuire ad una azione di profilazione finalizzata ad altre specifiche attività sul dispositivo.

IP LOGGER

MANTENERE RISERVATO IL PROPRIO INDIRIZZO IP

1. Attraverso un servizio online si genera facilmente un payload da nascondere in un link esistente qualsiasi, magari calibrato sul destinatario (articoli di news, immagini, ...)



2. Il nuovo link generato viene inviato al destinatario via SMS, chat, ...



3. Si attende che il bersaglio apra il link per visualizzare le informazioni specifiche del dispositivo



VPN - Virtual Private Network

MANTENERE RISERVATO IL PROPRIO INDIRIZZO IP

COSA E'?

Una VPN è servizio/software che, in estrema sintesi, permette di "coprire/sostituire" il proprio indirizzo IP durante la navigazione su Internet con un altro indirizzo IP e con una georeferenziazione diversa dalla propria

PERCHÉ USARE UNA VPN DURANTE LE INDAGINI?

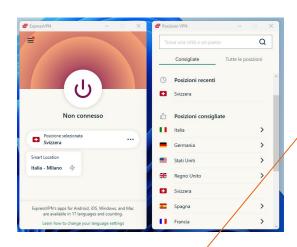
In caso di profilazione dei navigatori che accedono ad un sito o all'azione di un IP Logger, l'IP utilizzato dagli operatori di PG sarà quello della VPN e non quello proprio o istituzionale (potenzialmente censito e quindi "riconosciuto" oppure esposto ad eventuali contromisure)

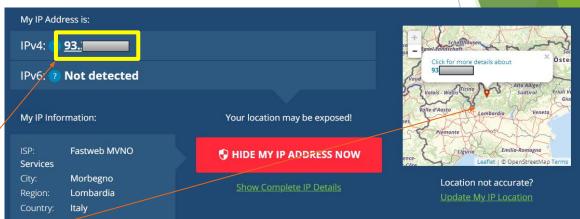
Alcuni siti web/sistemi informatici o telematici possono mostrare/nascondere contenuti in funzione dell'IP dei navigatori (es: un contenuto non visibile per un navigatore italiano può essere invece accessibile per un navigatore francese)

→ E' POSSIBILE UTILIZZARE VPN GRATUITE (LIMITATE) OPPURE VPN A PAGAMENTO

VPN - Virtual Private Network

ESEMPIO DI NAVIGAZIONE "IN CHIARO" SENZA VPN

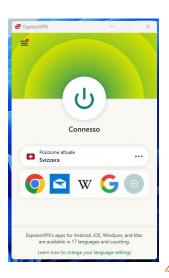


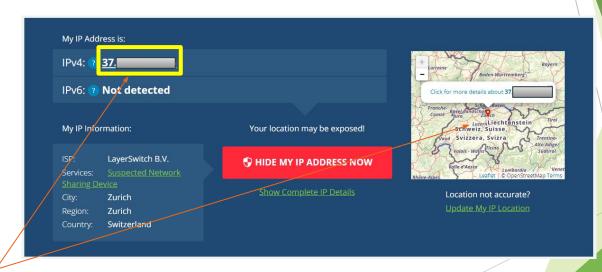


Il nostro vero INDIRIZZO IP trasmesso durante la navigazione senza l'utilizzo di una VPN e la connessa posizione geografica

VPN - Virtual Private Network

ESEMPIO DI NAVIGAZIONE CON "VPN"





L'INDIRIZZO IP trasmesso durante la navigazione con l'utilizzo di una VPN e la connessa posizione geografica

RIDURRE L'ESPOSIZIONE DEI DATI

I RISCHI DELLE RICERCHE SULLE "FONTI APERTE"

La ricerca dell'User ID di un utenza Facebook

PREMESSE:

- a) Spesso è necessario cercare delle informazioni, riconducibili ad un procedimento, su internet;
- a) Spesso non si utilizza una VPN per cui il proprio indirizzo IP è palesato a numerosi server/servizi informatici rendendo pertanto possibile geolocalizzare il navigatore/operatore;
- Spesso si cercano le informazioni all'interno di portali web, non necessariamente istituzionali (anche destinati
 esplicitamente a PM, PG e Consulenti e previa registrazione con email istituzionale), per effettuare, ad
 esempio, la ricerca dell'USER ID di un'utenza Facebook, magari con un software installato sul proprio PC.

CONSEGUENZE:

→ Ciò determina, di fatto, <u>una piena condivisione a terzi</u> di obiettivi di interesse inve<mark>stigativo e/o</mark> giudiziario unitamente alla PG operante ed al luogo di attivazione della stessa per gli obiettivi oramai palesati.

RIDURRE L'ESPOSIZIONE DEI DATI

I RISCHI DELLE RICERCHE SULLE "FONTI APERTE"

Esempio: il sito web riceve il link con il nome utente di Facebook e restituisce il relativo User ID

Facebook profile, page or group link https://www.facebook.com/commentpicker/ Find Facebook profile link. Find Facebook profile link. Find Facebook profile link. Find Facebook profile link. Find Facebook group link. SOLVE SUM 7-7= Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.	FACEBOOK SETTINGS -FACEBOOK LINK	YOUR FACEBOOK ID		
FACEBOOK ID Find Facebook profile link. Find Facebook page link. Find Facebook group link. SOLVE SUM 7-7-2 Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.				
Find Facebook page link Find Facebook page link Find Facebook page link Find Facebook group link SHARE OR COPY FACEBOOK ID Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.	https://www.facebook.com/le			
• Find Facebook page link. • Find Facebook group link. SOLVE SUM— 7+7= SHARE OR COPY FACEBOOK ID Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.	E.g. https://facebook.com/Commentpicker/	FACEBOOK ID		
• Find Facebook group link -SOLVE SUM 7+72 SHARE OR COPY FACEBOOK ID Whote Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.	Find Facebook profile link.			
SHARE OR COPY FACEBOOK ID Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.	Find Facebook page link.	100000693		
SHARE OR COPY FACEBOOK ID Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.	Find Facebook group link.			
Note: Loading your Facebook ID may take time. Please wait until we have found your Facebook ID. You might need to try multiple times after failure.		SHARE OR COPY FACEBOOK ID		
	7+7=			
GET PACEBOOK ID	GET FACEBOOK ID			

https://commentpicker.com/find-facebook-id.php

RIDURRE L'ESPOSIZIONE DEI DATI

I RISCHI DELLE RICERCHE SULLE "FONTI APERTE"

Unitamente a quello che direttamente trasmettiamo al sito, <u>la nostra ricerca</u>, l'Al di Google ci conferma che indirettamente il nostro browser sta trasmettendo altre informazioni



PROTEZIONE DEI DATI

I RISCHI DELLE RICERCHE SULLE "FONTI APERTE"

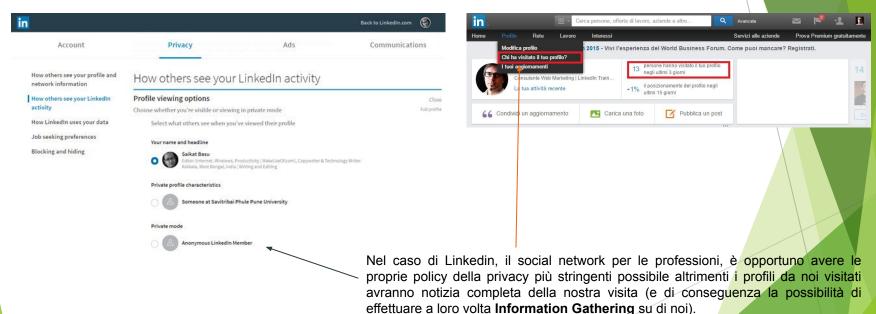
L'operazione di ricerca dell'USER ID dell'utenza Facebook può, spesso, essere fatta direttamente sulla pagina web dello stesso social network del nostro bersaglio, **senza la condivisione di dati con altri "intermediari"**, cercando nel codice sorgente della pagina il valore della stringa **"owning_profile_id"**

```
The second content of the second content of
```

```
Q==","owning_profile_id":"1000006______3","__modu
```

PROTEZIONE DEGLI ACCOUNT

PRIVACY DEI PROFILI SOCIAL





RISORSE

STRUMENTI DI SUPPORTO PER LE ATTIVITÀ DI INDAGINE

HASHING

CALCOLARE L'HASH

PERCHÉ CALCOLARE L'HASH

Garantire l'integrità dei dati: L'hashing può essere utilizzato per verificare che i dati non siano stati modificati. Ad esempio, se si invia un file a un destinatario, è possibile calcolare l'hash del file prima dell'invio e inviare anche l'hash al destinatario. Il destinatario può quindi calcolare l'hash del file ricevuto e confrontarlo con l'hash originale. Se i due hash coincidono, i dati non sono stati modificati. Se i due hash non coincidono, i dati sono stati modificati.

QUANDO CALCOLARE L'HASH

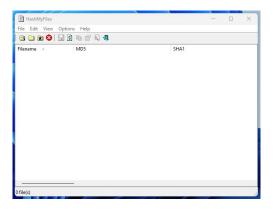
Quando si individuano file da estrarre, ad esempio su un dispositivo della p.o. ovvero su un dispositivo che non verrà sottoposto a sequestro ma interessato da attività di perquisizione, è opportuno calcolare e riportare in atti l'hash dei file affinché una volta estratti ed entrati nella disponibilità dell'operatore si possa confermare l'integrità dei dati estratti mediante ulteriore calcolo dell'hash

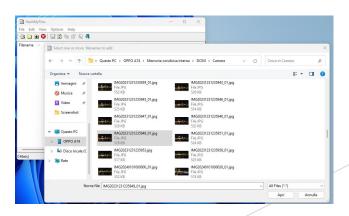
esempio di una stringa hash (*digest*) calcolata su un file con algoritmo sha1: bf7206323c6340aa269e75f7231544886611d59b

HASHING

COME CALCOLARE L'HASH DI UN FILE SU UN DISPOSITIVO MOBILE

- Disporre del software installato su un proprio pc/notebook
 (es: HashMyFiles: https://www.nirsoft.net/utils/hash_my_files.html)
- Collegare il dispositivo (possibilmente in sola lettura) con un cavo usb al proprio pc/notebook e individuare il/i file di interesse attraverso il software

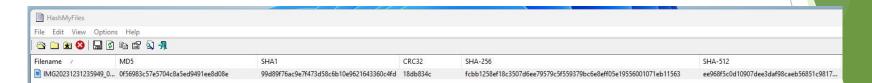




HASHING

COME CALCOLARE L'HASH DI UN FILE SU UN DISPOSITIVO MOBILE

3. Copiare la stringa di interesse prodotta (es: SHA-256 o SHA-512)



INDIRIZZI IP COME LOCALIZZARE UN INDIRIZZO IP

Esistono diversi modi per localizzare un indirizzo IP. Un modo è utilizzare un servizio di localizzazione IP online. Questi servizi utilizzano una base di dati di indirizzi IP e posizioni per determinare la posizione approssimativa di un indirizzo IP. Alcuni esempi di servizi di localizzazione IP online includono:

- Whatismyipaddress.com
- WhatIsMyIP.com
- IPI ocation net
- GeolP.com
- Whois.com

È importante notare che la localizzazione di un indirizzo IP può essere imprecisa. La precisione dipende da una serie di fattori, tra cui la qualità della base di dati di indirizzi IP utilizzata dal servizio di localizzazione, la tecnica utilizzata per determinare la posizione e la disponibilità di informazioni sulla posizione

E' opportuno inoltre comprendere se l'IP in argomento possa essere attribuito ad una VPN

INDIRIZZI IP COME LOCALIZZARE UN INDIRIZZO IP

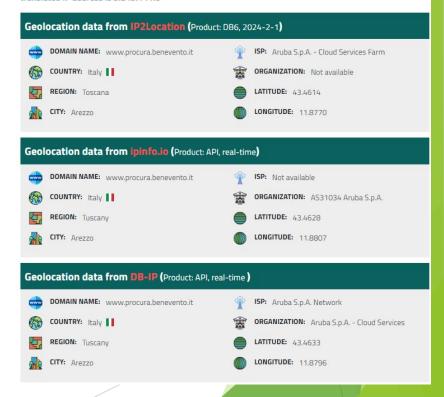
Esempio di Domain Lookup (ricerca del dominio)

IP Location Finder

https://www.procura.benevento.it/

IP Lookup

You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is 5.249.141.8



SITI WEB

COME INDIVIDUARE UN INTESTATARIO DI UN SITO WEB

L'intestatario di un dominio web è la persona o l'organizzazione che possiede il dominio. L'intestatario del dominio è responsabile del pagamento delle tasse di registrazione del dominio e della manutenzione del sito web associato al dominio.

Esistono due tipi di intestatari di domini: intestatari privati e intestatari aziendali.

Intestatari privati sono persone fisiche che possiedono un dominio per uso personale o professionale.

Intestatari aziendali sono organizzazioni che possiedono un dominio per uso commerciale

Per trovare l'intestatario di un dominio web, è possibile utilizzare un servizio di ricerca del dominio. Questi servizi utilizzano il database WHOIS per recuperare le informazioni di contatto dell'intestatario del dominio.

Esistono molti servizi di ricerca del dominio disponibili online. Alcuni esempi includono:

- Whois.com
- DomainTools.com
- Namecheap.com

procura.benevento.it

* Please note that the following result could be a subgroup of *

* the data contained in the database. *

* Additional information can be visualized at: *

* http://web-whois.nic.it *

Domain: procura benevento it

Status: ok Signed: no

Created: 2017-05-02 11:25:11 Last Update: 2023-05-18 00:52:03

Expire Date: 2024-05-02

Registrant

Organization: Procura della Repubblica presso il Tribunale di Benevento

Admin Contact Name: hidden

Organization: hidden

Technical Contacts Name: hidden

Organization: hidden

Registrar

Organization: Aruba s.p.a. Name: ARUBA-REG

Web: http://www.aruba.it

DNSSEC: yes

Nameservers

dns.technorail.com

dns2.technorail.com dns3.arubadns.net

dns4.arubadns.cz



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

IBAN

COME VERIFICARE UN BAN - HTTPS://IT.IBANCALCULATOR.COM/

Verifica un codice IBAN

Se il controllo ha dato un codice IBAN corretto e vi servono informazioni aggiuntive cliccate qui

IBAN:

Controlla il codice IBAN



Convalida un altro codice IBAN

IMMAGINI

LE RICERCHE SU IMMAGINI - TINEYE

Permette di verificare se una immagine, rappresentativa di un profilo social o di un oggetto pubblicizzato in un annuncio di vendita online, sia stata già utilizzata precedentemente o contestualmente in altri profili/annunci

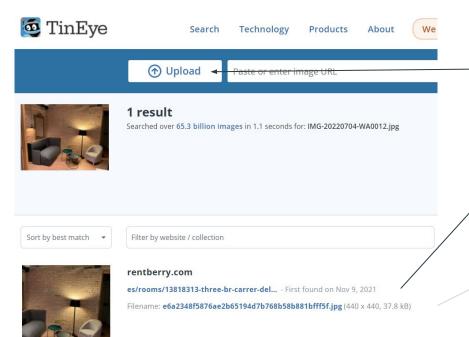


IMMAGINI

LE RICERCHE SU IMMAGINI - TINEYE

Fotografia inviata alla p.o. relativa ad un annuncio immobiliare proposto all'interno di un gruppo facebook Erasmus per la città di Vienna, in Austria, nel 2022





La fotografia viene caricata nel sito TinEye

Il portale web rivela che la stessa immagine, il 05 novembre 2021, è stata utilizzata con un altro filename, per un annuncio di locazione immobiliare nella città di Barcellona, in Spagna

WAYBACK MACHINE L'ARCHIVIO DI INTERNET

Permette di verificare le varie o eventuali versioni dello stesso sito web nel tempo nonché di individuare, nelle varie versioni delle pagine trovate i relativi contenuti, tra cui riferimenti a indirizzi email, telefonici o altro e rimossi nella versione attuale del sito web



Explore more than 863 billion web pages saved over time

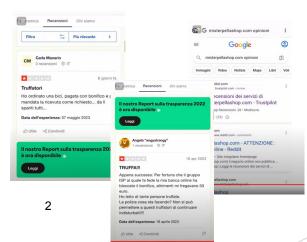
Enter a URL or words related to a site's home page

WAYBACK MACHINE L'ARCHIVIO DI INTERNET

SCENARIO DI UNA TRUFFA ONLINE PER LA VENDITA DI PELLET

- 1) Offerta vantaggiosa su canali "social" e siti web allestiti appositamente
- 2) Segnalazioni e denunce
- I siti web, predisposti per la vendita, vengono "svuotati"





STATO POST TRUFFE DEL DOMINIO

C. Percel Infest

Q. Percel Infest

Q. Percel Infest

Q. Serramenti. s. Infest

D. Serramenti. s

1

WAYBACK MACHINE

L'ARCHIVIO DI INTERNET



ACCESSO ALLE RISULTANZE Siamo un'azienda che vende articoli da giardinaggio professionale e accessori per il vostro giardino da noi il giardinaggio to fai con un Clad?

Puoi chiedere a la nostra assistenza clienti per le tue domande ti risponderanno subito

Se cerchi assistenza su prodotti o per altre richieste contatta l'assistenza clienti tramite whatsapo al numero 3512250125 oppure via mail assistenzaclienti@misterpallashop.com

Per saperne di



322082132/https://www.misterpellashop.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.misterpellashop.com%2F"/>
2/https://www.misterpellashop.com/wp-json/oembed/1.0/embed?url=https%3A%4F%2Fwww.misterpellashop.com%2F&amg;format=xml"/>

rg", "@type":"LocalBusiness", "address":("@type":"PostalAddress", "addressLocality":"Nappoli", "streetAddress":"Vico Carceri S. Felice, 3", "addressRegion":"NA"), "logo":"/
_e0Tz]LosYcJp8H_wYvV217"/><meta name="description" content="Rivendiamo prodotti per giardinaggio attrezzatura per potatura bricolage accessori per giardino "/>
_tent/themes/gox/public/fonts/NunitoSans-latin_latin-ext-regular.eot);src:local("NunitoSans Regular"),local("NunitoSans-Regular");src:url(/web/202303220821321m_/https

LBAR INSERT -->

MALTEGO

SOFTWARE PER OPEN SOURCE INTELLIGENCE

Maltego è un software di analisi dei collegamenti utilizzato per l'intelligence open source (OSINT), la medicina legale e altre indagini. Viene utilizzato per visualizzare e analizzare le relazioni tra persone, organizzazioni, infrastrutture e altre entità.

Maltego può essere utilizzato per una varietà di scopi, tra cui:

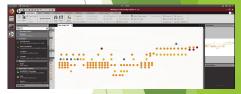
- Indagini su minacce informatiche
- Ricerca di frodi
- Intelligence competitiva
- Indagini investigative
- Ricerca di persone

Maltego è uno strumento potente che può essere utilizzato per comprendere meglio le relazioni tra persone, organizzazioni e altre entità. È uno strumento prezioso per chiunque sia coinvolto nell'intelligence, nelle indagini o nella ricerca.

Ecco alcuni esempi di come Maltego può essere utilizzato:

- Un analista della sicurezza informatica può utilizzare Maltego per mappare la rete di un'azienda e identificare potenziali vulnerabilità.
- Un investigatore finanziario può utilizzare Maltego per rintracciare i flussi di denaro in un caso di frode.
- Un giornalista investigativo può utilizzare Maltego per ricercare le connessioni tra persone e organizzazioni coinvolte in una storia.







AI - INTELLIGENZA ARTIFICIALE CONSIDERAZIONI, AMBITI DI UTILIZZO, ACCESSO E CASI PRATICI DI IMPIEGO

CONSIDERAZIONI

- occorre valutare le soluzioni proposte dall'Al
- essere consapevoli che si stanno condividendo dei dati che assumeranno profili di "sensibilità giudiziaria" con soggetti terzi (anche internazionali)
- è uno strumento molto pertinente ed utile sia per l'operatore esperto che può raffinare il proprio metodo sia per l'operatore poco esperto che per necessità può trovarsi a gestire dispositivi e dati in una condizione unica ed irripetibile

AMBITI DI UTILIZZO

L'intelligenza artificiale (Al) sta diventando sempre più importante nelle indagini informatiche. L'Al può essere utilizzata per:

- automatizzare compiti ripetitivi
- analizzare grandi quantità di dati
- identificare modelli e tendenze nascosti

Ecco alcuni esempi di come l'Al può essere utilizzata nelle indagini informatiche:

Automazione di attività ripetitive

L'Al può essere utilizzata per automatizzare attività ripetitive, come la raccolta di dati, la scansione dei registri e l'analisi dei file. Ciò può liberare tempo agli investigatori per concentrarsi su attività più complesse.

Analisi di grandi quantità di dati

L'Al può essere utilizzata per analizzare grandi quantità di dati, come i registri di rete, i file di log e i file di immagine. Ciò può aiutare gli investigatori a identificare modelli e tendenze nascosti che potrebbero essere altrimenti difficili da rilevare.

Identificazione di modelli e tendenze

L'Al può essere utilizzata per identificare modelli e tendenze nascosti nei dati. Ciò può aiutare gli investigatori a comprendere meglio la natura di un attacco informatico o a identificare i sospetti.

Ecco alcuni esempi specifici di come l'Al viene utilizzata nelle indagini informatiche oggi:

- L'Al può essere utilizzata per analizzare le e-mail in cerca di modelli comuni di e-mail di phishing. Ciò può aiutare gli investigatori a identificare e bloccare le e-mail di phishing prima che raggiungano gli utenti finali.
- L'Al viene utilizzata per identificare i malware
- L'Al può essere utilizzata per analizzare i file in cerca di segni di malware. Ciò può aiutare gli investigatori a identificare e rimuovere il malware dai sistemi compromessi.

Accesso

I due principali sistemi di intelligenza artificiali disponibili sono:

- Google Gemini
- Chat GPT OpenAl

Entrambi accessibili mediante collegamento ad un link ed eventuale registrazione



https://gemini.google.com/



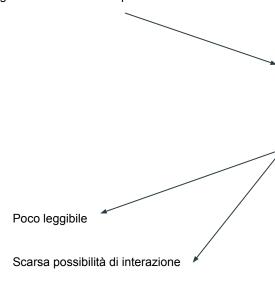
https://chat.openai.com/

CASI PRATICI DI IMPIEGO

E' possibile utilizzare questi sistemi, dal proprio dispositivo PC o SMARTPHONE, per trovare soluzioni - dirette, immediate e molto valide - a problematiche operative, nel caso specifico di natura informatica, sia durante le attività di indagine sia durante le attività di perquisizione.

Casi pratici di impiego: File di log

Esempio di una porzione di un file di log generato dal sistema operativo Windows 11



File Modifica Visualizza					
		16.0.11929.20606 16.0.11929.20606 Microsoft Corporation	16.0.11929.20606		
	Office 16 Click-to-Run Licensing Component 00006109F80000000000000000F01FEC Microsoft Corporation Oracle VM VirtualBox 7.0.12 09504E265C1F56440B017DBE31CCBBC0 Oracle and/or its affiliates 7.0.12 F1C5-4465-8010-07EB13CCBBC() Incomplete Library Complete Library C	16.0.11929.20606	C:\Windows\Installer\{62E4D590-		
	Microsoft Edge 0C423219299F6AC359FA87A6DFBD6460 Microsoft Corporation 120.0.2210.121 F992-3CA6-95AF-786AFDD84606}\icon.ico	C:\Windows\Inst	caller\{912324C0-		
	Microsoft .NET Host FX Resolver - 6.0.5 (x64) 14DCC6E369B6DB74E8E17D5B39EC9E67 Microsoft Corporation	ft Corporation 14.34.3	31931		
,	Teams Machine-Wide Installer 3180FA9387AF0684DAEB39982B419B41 Microsoft Corporation 1.3.0.362 McAfee Data Exchange Layer for MA 4566ACBDF124C354F94EE23893E09C82 McAfee LLC 6.0.241.0 (LDBCA6564-421F-453C-9FE4-2EB3390EC928)\{ProductIcon} ExpressyPN 5E3C985EC98822F49A954F48BA90287B3 ExpressyPN 12.70.0.10	C.\Mindous\Tastallon\(6	C:\Windows\Installer		
	F4889A2D783B}\app_icon.ico				
	Adobe Refresh Manager 68AB67CA408033019195008142548867 Adobe Systems Incorporated 1.8.0 C:\Windows\Installer\{AC76BA86-0804-1033-1959-001824458876}\ARPPRODUCTICON.exe	C:\Program Files (x86)\	Common Files\Adobe\ARM\1.0\		
	Adobe Acrobat Reader DC - Italiano 68AB67CA7DA704018744CAF070E41400 Adobe Systems Incorporated Reader DC\ C:\Windows\Installer\{AC76BA86-7AD7-1040-7844-AC0F074E4100}\SC Reader.ico	20.006.20042	C:\Program Files (x86)\Adobe\Acrobat		
	McAfee Agent 8100D7578E9FE6F49A80820EA942222 McAfee, Inc. 5.6.6.232 C:\Program File F9E8-4F6E-A908-28E0AA492222\ARPPRODUCTICON.exe	s\McAfee\Agent\	C:\Windows\Installer\{7E7D0018-		
	7-Zip 19.00 (x64 edition) 96F071321C0420729100000010000000 Igor Pavlov 19.00.00.0	ration 8.92.0.0 0665			
	Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.34.31931 D743C4FCE4593454882DCE710FF764F6 Microsoft Corporation 14.34.31931 Microsoft .NET Runtime - 6.0.5 (x64) D771A980EA8959141A51304C65318857 Microsoft Corporation 48.23.40665				
	Office 16 Click-to-Run Extensibility Component 00006109C800000000000000000000000000000000000		16.0.11929.20606		
	Office 16 Click-to-Run Licensing Component 00006109F800000000000000F01FEC Microsoft Corporation Opacle VM VirtualBox 7 0 12 09SD4F26SC1F5644DR8017DRF31CFBR0 Opacle and/op its affiliates 7 0 12	16.0.11929.20606	C:\Windows\Installer\{62F4D590=		

Casi pratici di impiego: File di log

Incollando nella Chat Box dell'Al in uso il contenuto del file di log

You

Office 16 Click-to-Run Licensing Component

00006109F8000000100000000F01FEC Microsoft Corporation 16.0:1929.20606

Oracle VM VirtualBox 7.0:12 095D4E265C1F5644DB017DBE31CCBBC0 Oracle and/or its affiliates 7.0:12 C:\Windows\Installer\(62E4D590-F1C5-4465-BD10-D7EB13CCBB0C\)\(con\VirtualBox\)

Microsoft Edge 0C423219299F6AC359FA87A6DFBD6460 Microsoft Corporation 120.0.2210.121 C:\Windows\Installer\{912324C0-F992-3CA6-95AF-

786AFDDB4606}\icon.ico

Microsoft .NET Host FX Resolver - 6.0.5 (x64)

14DCC6E369B6DB74E8E17D5B39EC9E67 Microsoft Corporation 48.23.40665

Microsoft Visual C++ 2022 X64 Additional Runtime - 14.34.31931

1B242EAE62A0A584FBBE2029EEF930BC Microsoft Corporation 14.34.31931

Microsoft Windows Desktop Runtime - 6.0.5 (x64)

23B875EDA4807E94E855F6853A57870C Microsoft Corporation 48.23.40699

Microsoft Update Health Tools 2C6A1CF1E675A984B9A4292DF1451263 Microsoft

Corporation 3.74.0.0

Teams Machine-Wide Installer 3180FA93B7AF0684DAEB399B2B419B41 Microsoft

Corporation 1.3.0.362

2EB3390EC928}\ProductIcon

ExpressVPN 5E3C9B5EC98822F49A954F8BA9D287B3 ExpressVPN 12.70.0.10 C:\Windows\Installer\{E5B9C3E5-889C-4F22-A959-F4B89A2D783B}\app_icon.ico

Casi pratici di impiego: File di log

L'Al immediatamente interpreta e rende le informazioni comprensibili anche all'operatore in pochi secondi

ChatGPT

Sembra che tu stia fornendo un elenco di programmi installati sulla tua macchina probabilmente estratto da un registro di installazione o da qualche altra fonte di informazioni sul software. Se hai domande specifiche su questi programmi o se c'è qualcosa di specifico che desideri fare o sapere, per favore fornisci ulteriori dettagli o chiedi in modo più specifico. Ecco alcune informazioni sulla lista che hai fornito

1. Office 16 Click-to-Run Licensing Component:

- Versione: 16.011929.20606
- . Fornitore: Microsoft Corporation

2. Oracle VM VirtualBox 7.0.12:

- Versione: 7.0.12
- Fornitore: Oracle and/or its affiliates
- Percorso di installazione: C:\Windows\Installer{62E4D590-F1C5-4465-BD10-D7FB13CCBB0C3\lconVirtualBox

3. Microsoft Edge:

- Versione: 120.0.2210.121
- . Fornitore: Microsoft Corporation
- Percorso di installazione: C:\Windows\Installer(912324C0-F992-3CA6-95AF-786AFDDB4606}\icon.ico

Microsoft .NET Host FX Resolver - 6.0.5 (x64):

- Versione: 48.23.40665
- . Fornitore: Microsoft Corporation

Microsoft Visual C++ 2022 X64 Additional Runtime - 14.34.31931:

- Versione: 14.34.31931
- Fornitore- Microsoft Corporation

6. Microsoft Windows Desktop Runtime - 6.0.5 (x64):

- Versione: 48 23 40699
- . Fornitore: Microsoft Corporation

Casi pratici di impiego: File di log

quali sono i fornitori? ChatGPT Nell'elenco che hai fornito, il termine "fornitore" si riferisce all'entità o all'azienda che ha sviluppato o distribuito il software. Ecco i fornitori associati a ciascun programma 1. Office 16 Click-to-Run Licensing Component: * Fornitore: Microsoft Corporation 2 Oracle VM VirtualBox 7.0.12: . Fornitore: Oracle and/or its affiliates 3. Microsoft Edge: Fornitore: Microsoft Corporation 4 Microsoft .NET Host FX Resolver - 6.0.5 (x64): . Fornitore: Microsoft Corporation Microsoft Visual C++ 2022 X64 Additional Runtime - 14,34,31931; * Fornitore: Microsoft Corporation Microsoft Windows Desktop Runtime - 6.0.5 (x64): . Fornitore: Microsoft Corporation 7. Microsoft Update Health Tools: Fornitore: Microsoft Corporation 8. Teams Machine-Wide Installer: Fornitore: Microsoft Corporation 9. McAfee Data Exchange Layer for MA: . Fornitore: McAfee LLC 10 ExpressVPN: Fornitore: ExpressVPN

Offrendo, peraltro, la possibilità di

interagire sugli stessi dati

Casi pratici di impiego: Hash di un file

Nel caso di una perquisizione informatica o di una ispezione/preview può essere necessario, nell'immediatezza, estrarre dei file dei quali, come detto, deve essere calcolato il relativo hash.

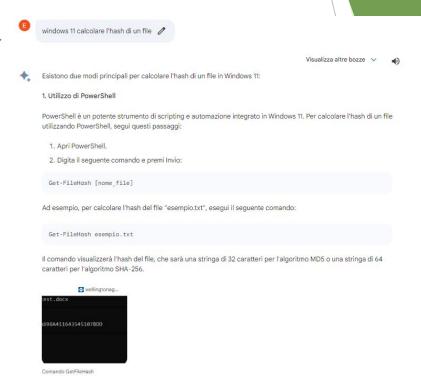
In assenza del Consulente informatico o di personale specializzato, l'Al può essere un utile strumento di riferimento per l'operatore.

Casi pratici di impiego: Hash di un file

Rivolgendo il quesito in modo chiaro e specifico nella chat box dell'Al:

"windows 11 calcolare l'hash di un file"

L'Al fornirà in modo chiaro e utile la sequenza delle operazioni da effettuare sul dispositivo in esame



Casi pratici di impiego: Log di sistema

Nel caso di una perquisizione informatica o di una ispezione/preview può essere necessario, nell'immediatezza, consultare ed eventualmente estrarre, ad esempio, alcuni file di log del sistema operativo.

In assenza del Consulente informatico o di personale specializzato, l'Al può essere un utile strumento operativo

Casi pratici di impiego: Log di sistema

Rivolgendo il quesito in modo chiaro e specifico nella chat box dell'Al:

"windows 11 come estrarre i log di sistema"

L'Al fornirà in modo chiaro e utile la sequenza delle operazioni da effettuare sul dispositivo in esame



ChatGPT

Per estrarre i log di sistema in Windows 11, puoi utilizzare l'applicazione "Registro eventi". Ecco come puoi accedervi e ottenere i log di sistema:

1. Apri il Registro eventi:

- * Premi 'Win + X' per aprire il menu di scelta rapida.
- . Seleziona "Gestione dispositivi" o "Gestione computer".
- * Nel menu a sinistra, espandi la voce "Registro eventi" e fai clic su "Log di sistema"

Filtrare i log:

- Puoi filtrare i log in base a vari criteri, come livello di gravità, origine, data e ora, ecc.
- Per fare ciò, fai clic con il pulsante destro del mouse su "Log di sistema" e scegli "Filtro corrente".

3. Esportare i log:

- · Dopo aver filtrato i log secondo le tue esigenze, puoi esportarli
- Fai clic con il pulsante destro del mouse su "Log di sistema" e scegli "Salva con nome"
- Seleziona il percorso in cui desideri salvare il file e specifica un nome per il file di log.

4. Usare il Prompt dei comandi (opzionale):

- · Puoi anche utilizzare il Prompt dei comandi per estrarre i log.
- Apri il Prompt dei comandi come amministratore (clic destro su Start, seleziona
- "Prompt dei comandi (Amministratore)" o "PowerShell (Amministratore)").
- * Digita il seguente comando per esportare i log di sistema in un file di testo:



Sostituisci "C:\percorso\del\tuo\file\log.txt" con il percorso e il nome del file desiderato.

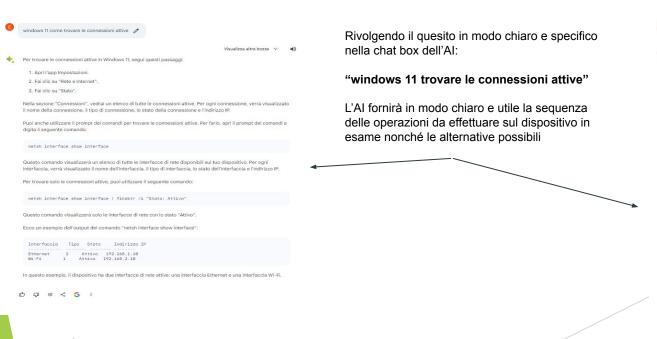
Questi passaggi ti consentiranno di estrarr og di sistema in Windows 11 sia attraverso l'interfaccia utente che utilizzando il Prompt dei comandi.

Casi pratici di impiego: Connessioni attive

Nel caso di una perquisizione informatica o di una ispezione può essere necessario individuare gli INDIRIZZI IP internet/lan al momento connessi con il dispositivo in esame.

In assenza del Consulente informatico o di personale specializzato, l'Al può essere un utile strumento operativo

CASI PRATICI DI IMPIEGO: CONNESSIONI ATTIVE





Casi pratici di impiego: Messaggi di posta elettronica

Nei primi accertamenti connessi alla ricezione di una denuncia-querela o durante l'analisi di contenuti di un dispositivo, può essere necessario analizzare un messaggio di posta elettronica (in particolare il suo header).

HEADER: L'header di un messaggio di posta elettronica è una serie di informazioni che accompagnano il messaggio stesso e ne forniscono dettagli sul mittente, il destinatario, la data e l'ora di invio, il percorso di consegna e altre informazioni tecniche. L'header viene aggiunto dal client di posta elettronica del mittente e da ogni server di posta elettronica (mail server) attraverso il quale il messaggio transita. Gli header sono composti da un insieme di campi, ciascuno dei quali contiene un'informazione specifica.

I campi più comuni sono:

From: contiene l'indirizzo email del mittente.

To: contiene l'indirizzo email del destinatario o dei destinatari.

Subject: contiene l'oggetto del messaggio.

Date: contiene la data e l'ora di invio del messaggio.

Return-Path: contiene l'indirizzo email a cui il messaggio verrà inviato in caso di mancata consegna.

X-Mailer: contiene il nome del software utilizzato per comporre il messaggio.

Received: contiene una serie di informazioni sul percorso di consegna del messaggio.

AI - INTELLIGENZA ARTIFICIALE

Casi pratici di impiego: Messaggi di posta elettronica

Gli header possono essere visualizzati in diversi modi, a seconda del client di posta elettronica utilizzato. In genere, è possibile visualizzarli selezionando il messaggio e quindi scegliendo l'opzione "Mostra header" o "Visualizza proprietà".

Gli header possono essere utili per diversi scopi, tra cui:

- Tracciare il percorso di consegna di un messaggio.
- Identificare il reale mittente di un messaggio.
- Verificare la sicurezza di un messaggio.
- Risoluzione dei problemi relativi alla consegna delle email.

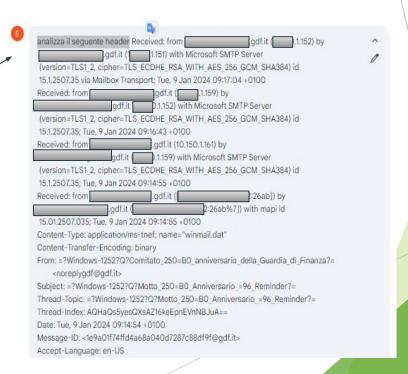
Ad esempio, se si riceve un messaggio da un mittente sconosciuto, è possibile visualizzare gli header per verificare se l'indirizzo email del mittente corrisponde al nome visualizzato. Se non corrisponde, è possibile che il messaggio sia stato falsificato.

AI - INTELLIGENZA ARTIFICIALE

Casi pratici di impiego: Messaggi di posta elettronica

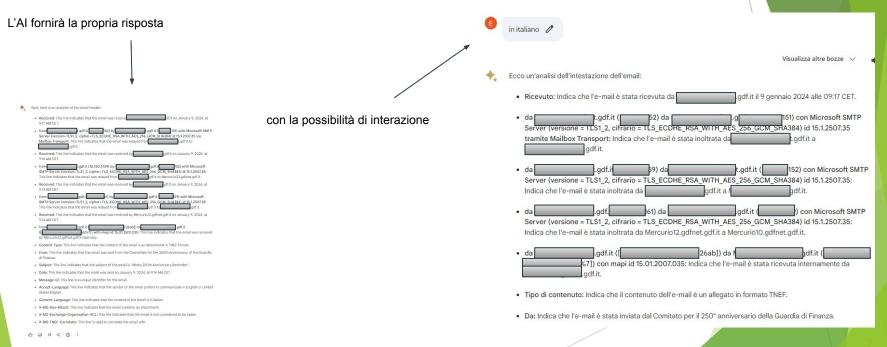
Incollando l'intero contenuto dell'header nella chat box dell'Al dopo aver inserito anche la richiesta:

"analizza il seguente header ..."



AI - INTELLIGENZA ARTIFICIALE

Casi pratici di impiego: Messaggi di posta elettronica



DATA RETENTION

...L'OBBLIGO DI CONSERVAZIONE IMPOSTO PER LEGGE AI FORNITORI DI SERVIZI DI COMUNICAZIONE ELETTRONICA ACCESSIBILI AL PUBBLICO O DI RETI PUBBLICHE DI COMUNICAZIONE DEI DAT (METADATI) DI TRAFFICO TELEFONICO E TELEMATICO DEI LORO UTENTI E/O ABBONATI.

D. Lgs. 196/2003, art. 132

- 24 mesi: periodo di conservazione dei dati relativi al traffico telefonico;
- 12 mesi: periodo di conservazione dei dati di traffico telematico (file di log);
- 30 giorni: periodo per le chiamate senza risposta.

L. 20/11/2017 n. 167, per le finalità dell'accertamento e della repressione dei reati di cui agli art. 51 comma 3-quater, 407 comma 2 lettera a) c.p.p. o per delitti quali terrorismo, associazione a delinquere di stampo mafioso, omicidio, rapina, ... il termine di conservazione dei dati di traffico telefonico e telematico nonchè dei dati relativi alle chiamate senza risposta è stabilito in 72 mesi

ACQUISIZIONE FILE DI LOG

DATI TRAFFICO TELEFONICO/TELEMATICO/FILE DI LOG

FILE DI LOG: Sono file e quindi dati di registrazione sequenziale e cronologica di tutte le operazioni effettuate da un sistema informatico (server), dispositivo informatizzato, un programma o un'applicazione. Queste operazioni possono essere effettuate da un utente, oppure avvenire in modo totalmente automatizzato. Le registrazione di tali attività vengono conservate con una periodicità regolare.

PERCHÉ CHIEDERE I FILE DI LOG?

La presenza dei file di log è fondamentale per la Polizia Giudiziaria per individuare l'autore di una determinata connessione internet, in quanto il server in uso al fornitore del servizio (provider) conserva i relativi files di log che si identificano appunto nei dati relativi al traffico telematico.

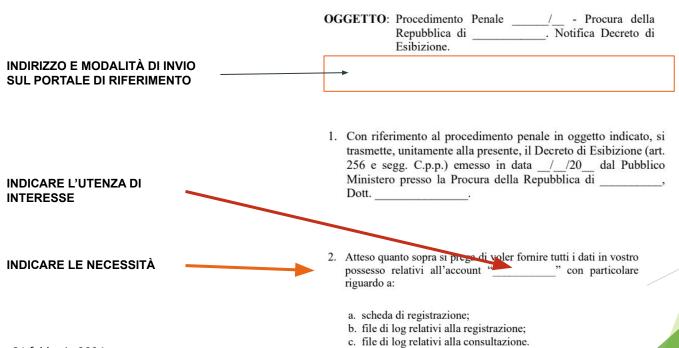
COME CHIEDERE I FILE DI LOG?

Per acquisire il traffico telematico è necessario un provvedimento di acquisizione dati del <u>P.M. ex art. 256 c.p.p.</u> da notificare al provider interessato, che dovrà contenere l'IP interessato, periodo di riferimento, fascia oraria. Peraltro l'acquisizione del traffico telematico potrebbe anche avvenire con le modalità di cui all'art. 254 bis del c.p.p. (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.), introdotto a seguito della L. 48/2008 di ratifica della Convenzione di Budapest "Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni".

ACQUISIZIONE FILE DI LOG

SI CONSIGLIA DI VERIFICARE NEL PORTALE WEB
DI INTERESSE LE SEZIONI DEDICATE ALLE FORZE
DELL'ORDINE / AUTORITÀ GIUDIZIARIA PER LE
MODALITA' DI COMPILAZIONE ED INVIO

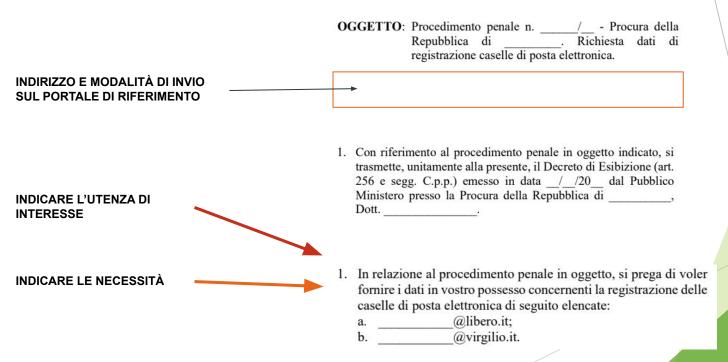
DATI TRAFFICO TELEFONICO/TELEMATICO/FILE DI LOG



SI CONSIGLIA DI VERIFICARE NEL PORTALE WEB
DI INTERESSE LE SEZIONI DEDICATE ALLE FORZE
DELL'ORDINE / AUTORITÀ GIUDIZIARIA PER LE
MODALITA' DI COMPILAZIONE ED INVIO

ACQUISIZIONE NOTIZIE

POSTA ELETTRONICA



CELLEBRITE READER

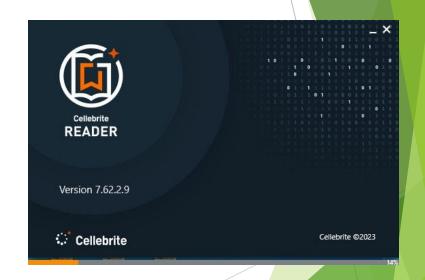
Cellebrite Reader è un'applicazione web gratuita che consente di visualizzare e analizzare i dati estratti dai dispositivi mobili utilizzando lo strumento di estrazione fisica UFED di Cellebrite.

Con Cellebrite Reader è possibile:

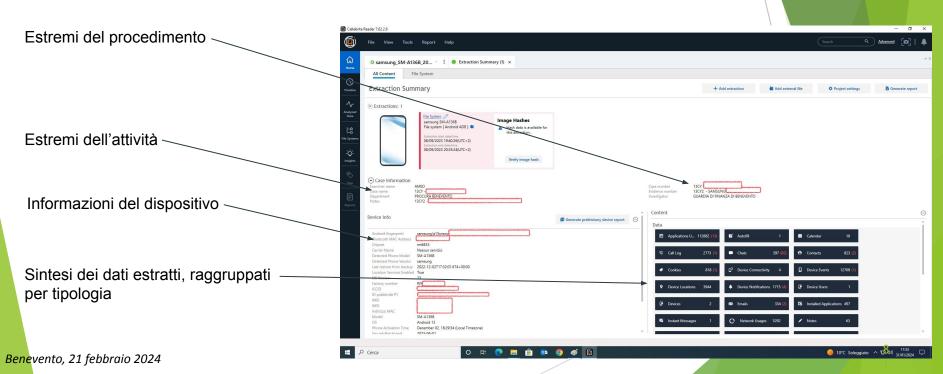
- Visualizzare e analizzare dati da vari dispositivi mobili, inclusi iPhone, dispositivi Android, BlackBerry e dispositivi Windows Mobile.
- Cerca parole chiave o frasi specifiche nel dati estratti.
- Tagga e evidenzia prove importanti per riferimento futuro.
- Genera report che riassumono i tuoi risultati.

Cellebrite Reader è uno strumento potente per investigatori e professionisti legali che necessitano di analizzare i dati dei dispositivi mobili.

È facile da usare e non richiede alcuna esperienza tecnica.



CELLEBRITE READER - ANTEPRIMA

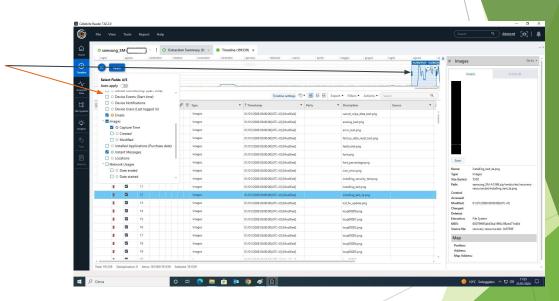




CELLEBRITE READER - TIMELINE

TIMELINE

Permette di filtrare alcuni eventi/dati presenti sul dispositivo in base ad un definito intervallo di tempo

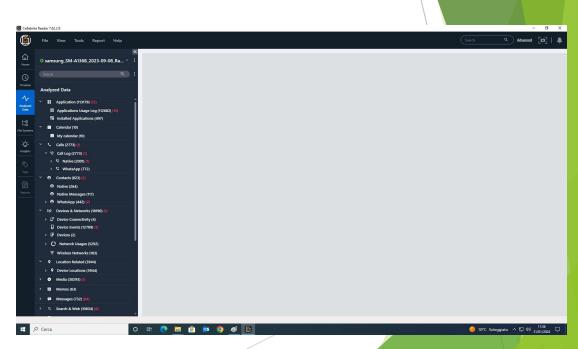


CELLEBRITE READER - ACCESSO AI DATI

DATI ANALIZZATI

Da qui è possibile accedere a tutti i dati estratti e catalogati in base alla propria tipologia e logica funzionale

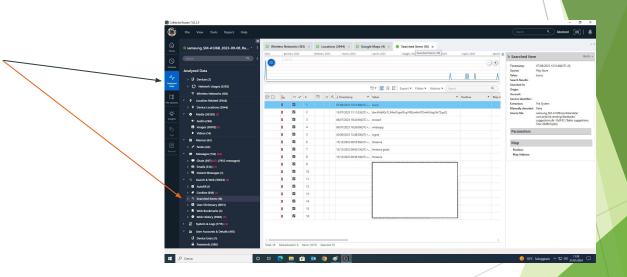
Quelli in rosso gli elementi cancellati e recuperati



CELLEBRITE READER - ACCESSI AI DATI

DATI ANALIZZATI

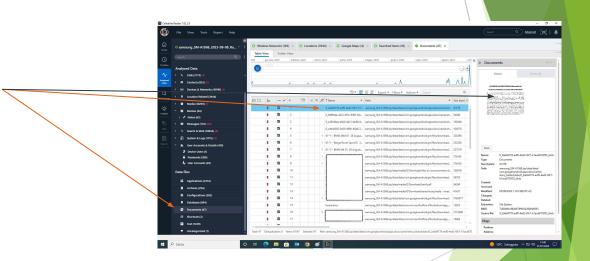
Selezionando ad esempio "Searched Items" è possibile accedere ai record relativi agli "Elementi ricercati" dall'utilizzatore del dispositivo e rilevati con l'acquisizione di Ufed



CELLEBRITE READER - ACCESSI AI DATI

L'accesso diretto ai DOCUMENTI disponibili sul dispositivo è consentito attraverso la voce "Documents".

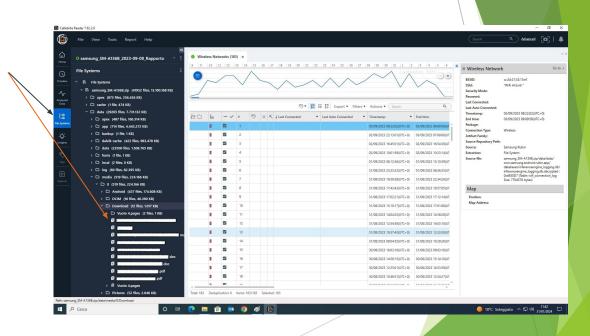
Selezionando con un click il singolo documento, si attiverà l'Anteprima; il doppio click permette la consultazione completa del file





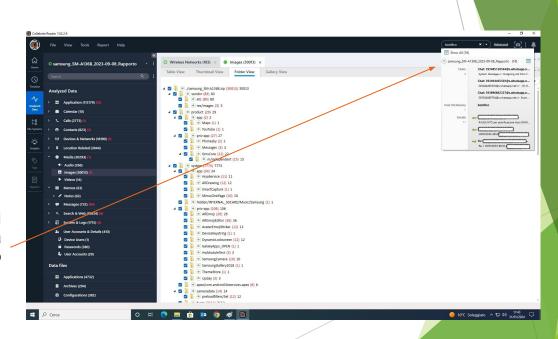
CELLEBRITE READER - ACCESSO AI DATI

La consultazione del materiale presente nel dispositivo è possibile anche attraverso la navigazione diretta del File System, sfogliando le singole cartelle e selezionando i file di interesse



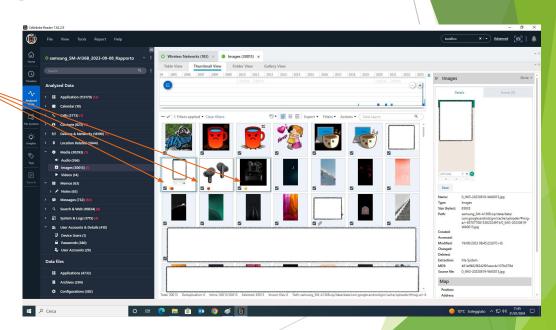
CELLEBRITE READER - RICERCA DEI DATI

Inserendo una parola chiave nel box di ricerca è possibile avere un'anteprima delle corrispondenze e della loro collocazione nel dispositivo



CELLEBRITE READER - TAG DEI DATI

In qualsiasi menù o visualizzazione è possibile attraverso i alcuni tasti funzione (F6, F7, F8, ...) impostare uno "stato di rilevanza" per il file (es: evidenza, importante, non utile, ...)



GRAZIE PER L'ATTENZIONE

MODULO 3

ISPEZIONE, PERQUISIZIONE E SEQUESTRO

Legge n. 48/2008 - Ratifica Convenzione di Budapest

MISURE DI SICUREZZA

PASSWORD E CREDENZIALI DI ACCESSO

"nemo tenetur se detegere" - Nessun obbligo di collaborazione può essere imposto all'indagato

La richiesta delle credenziali di accesso da parte della PG deve essere preceduta dall'avviso della facoltà di non rispondere di cui all'art. 64 comma 3 lett. B c.p.p. in virtù dell'art. 350 comma 1 c.p.p. per cui l'accesso agli apparati informatici sarebbe condizionato da una scelta difensiva dell'indagato.

Artt. 247 e 352 comma 1-bis c.p.p. prevedono, per la pg, nell'ambito delle perquisizioni informatiche, nonché delle perquisizioni in flagranza di reato oppure quando si debba procedere al fermo di una persona indiziata di delitto, il potere di perquisire sistemi informatici o telematici "ancorché protetti da misure di sicurezza"

Legge n. 48/2008 - Ratifica Convenzione di Budapest

EVIDENZE DIGITALI: FONTI DI PROVA MEMORIZZATE IN STRUMENTI INFORM

Il Legislatore ha stabilito la necessità di:

- a) adottare "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" (artt. 244 comma 2, 247 comma 1-bis, art 352 comma 1-bis, 354 comma 2 c.p.p.);
- b) il dato debba essere trattato con una procedura che assicuri "la conformità dei dati acquisiti a quelli originali e la loro immodificabilità" (artt. 254-bis, 354 comma 2 c.p.p.)

La TUTELA DELL'INTEGRITÀ' e la TUTELA DELL'AUTENTICITÀ' rappresentano l'obiettivo che deve guidare l'attività dei soggetti che interagiscono col dato digitale sin dal primo contatto:

- a) sia con riguardo alle attività urgenti d'iniziativa della polizia giudiziaria (art. 352 e ss)
- b) sia con riferimento ai mezzi di ricerca della prova disposti dal pm

PERQUISIZIONI

art 244 c.p.p. "casi e forme dell'ispezione"

consente all'AG, quando occorre accertare le tracce e gli altri effetti materiali del reato, di disporre "rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici"

art 247, comma 1-bis c.p.p.

"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"

art. 352 comma 1-bis c.p.p.

"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"

La perquisizione informatica deve essere eseguita ponendo attenzione a:

- acquisire la prova digitale (bit stream image/copia forense)
- applicazione di un sigillo elettronico (hash)
- garantire la ripetibilità

SEQUESTRO

art 260 c.p.p.

prevede la possibilità da parte delle autorità di assicurare le cose sequestrate attraverso l'apposizione di sigilli di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia

cd. Hash functions, certificazione fra copia e originale tramite procedure informatizzate, realizzata su adeguati supporti mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità

SEQUESTRO

art 354 c.p.p.

Accertamenti urgenti sui luoghi, sulle cose e sulle persone

Qualora tale attività sia compiuta in relazione a dato, informazioni, programmi informatici o sistemi informatici o telematici, dovranno essere adottate misure tecniche idonee ad assicurare la conservazione ed impedire l'alterazione del dato.

La PG deve provvedere all'immediata duplicazione dei dati informatici su adeguati supporti, attestando la conformità e l'immodificabilità.

L'immediata perquisizione dei sistemi nonché l'immediata duplicazione di quanto rinvenuto va ascritta alla natura volatile della digital evidence (che potrebbe essere persa dopo il riavvio o tramite procedure programmate).

Inoltre, rileva anche il "vincolo pertinenziale" esistente tra dati digitali e supporti di memorizzazione, da considerare, al fine di evitare sequestri di materiale inutile o di dare luogo ad una acquisizione indiscriminata di informazioni e dati generando l'illegittimità del sequestro stesso.

SEQUESTRO - SITI WEB

art 321 c.p.p.

Sequestro preventivo di siti web

Se il dominio si trova in territorio nazionale (provider italiano o hardware in italia)

- l'AG emette un decreto di seguestro preventivo
- notifica da parte della pg presso la sede di pubblicazione del dominio sulle macchine preposte
- messa "off-line" del sito web
 - rimozione materiale dal server del materiale e download su 2 supporti magnetici/ottici
 - inserimento di una pagina web precompilata (o un redirect) dalla PG in sostituzione del materiale rimosso che "pubblicizzi" il seque<mark>stro</mark>

Se il dominio si trova <u>in territorio estero</u> (ospitato su server esteri)

- l'AG emette un decreto di sequestro preventivo, ex art. 521 c.p.p., attraverso la forma dell'inibizione/oscuramento (blocco IP/DNS)
- notifica del decreto agli Internet Service Provider nazionali
- Rogatoria

SEQUESTRO - CORRISPONDENZA TELEMATICA

art 254 comma 1 c.p.p.

estende l'ambito del sequestro di corrispondenza a "lettere, pieghi, pacchi, valori telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica"

Per trattarsi di "corrispondenza" è necessario che l'email, spedita dall'indagato o a lui diretta, sia in attesa dell'inoltro dal server di invio (Scenario 1).

Scenario 1: webmail, il messaggio si trova sui server del gestore di posta elettronica

Si applicano le garanzie difensive previste da art. 254 e 353 c.p.p., la corrispondenza deve essere trasmessa nel sistema di telecomunicazione e che, temporaneamente e prima dell'invio del destinatario, si trovi conservata e memorizzata presso il fornitore di servizio

Scenario 2: client di posta elettronica, il messaggio è scaricato sul dispositivo

In questo scenario, si esclude l'applicabilità dell'art. 254 c.p.p. quindi se durante perquisizione e sequestro si trovassero nei dispositivi elementi di corrispondenza telematica pertinenti all'indagine, se ne potrà liberamente prendere visione ed estrarne copia come per gli altri dati informatici

"i dati informatici acquisiti dalla memoria del telefono in uso all'indagato (sms, messaggi WhatsApp, messaggi di posta elettronica scaricati e/o conservati nella memoria dell'apparecchio cellulare) hanno natura di documenti ai sensi dell'art. 234 c.p.p."

Cass. Pen. Sez. V - 16/01/2018, n. 1822

Questo significa che quando non vi è certezza sul materiale prodotto è necessario acquisire il supporto su cui è presente il materiale depositato. Pertanto lo screenshot può costituire prova se e quando l'imputato conferma l'autenticità di quei messaggi o quando non vengono sollevate questioni o opposizioni.

DIGITAL FORENSICS

Acquisire, conservare, analizzare e documentare i reperti informatici

Consulente informatico

Dott. Alessandro Grimaldi

INDICE ARGOMENTI

- Breve introduzione al concetto di digital forensic
- La figura e le attività del "forenser"
- Acquisizione delle prove
- Come comportarsi in relazione al caso specifico e all'incarico assegnato
- Gli strumenti da utilizzare per il punto di cui sotto
- Esecuzione pratica di una copia forense (con strumenti software)
- Catena di custodia
- Verifica e conservazione della prova
- Sessione domande e risposte

Introduzione alla Digital Forensics

ATTIVITÀ DI COMPUTER E MOBILE FORENSIC

la Computer Forensics è una disciplina che si occupa della preservazione, dell'identificazione e analisi delle informazioni contenute all'interno di dispositivi di memorizzazione di massa, o nei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigativa prevalentemente di carattere giudiziario.

ATTIVITÀ DI COMPUTER E MOBILE FORENSIC

Tra le nuove figure professionali che si stanno sempre più affermando nell'ambito dell'Information Tecnology, sta acquisendo particolare importanza quella del Computer Forenser o Informatico Forense. Tale figura si occupa dell'esecuzione di indagini informatiche rispettando le norme di legge dello stato in cui si sta esercitando.



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

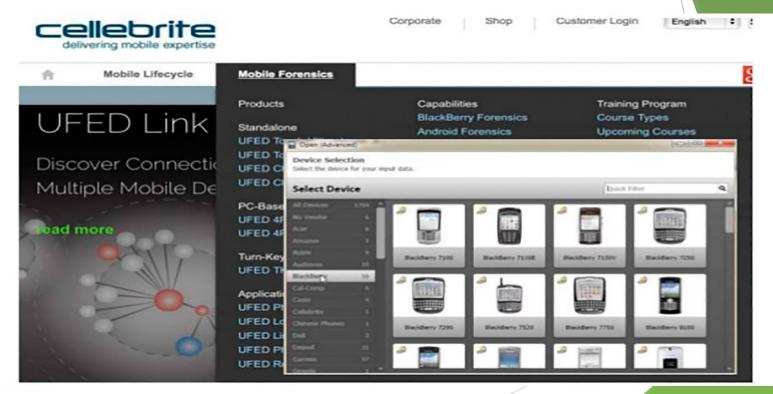
STRUMENTI



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

STRUMENTI





PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

STRUMENTI



ACQUISIZIONE DELLE PROVE

LA SCENA DEL CRIMINE

In qualunque scena del crimine, oggi pullulano di dispositivi high-tech.

Tra quest'ultimi, quelli di interesse per la computer forensics sono quelli in grado, in qualsiasi modo, di memorizzare informazioni.

Proprietà dell'evidenza digitale

- Per assumere valore probatorio, l'evidenza digitale deve soddisfare alcune proprietà:
 - ✓ Integrita': assenza di alterazioni
 - ✓ Completezza: analisi di tutti gli elementi utili
 - ✓ Autenticita': certezza della provenienza dei reperti
 - ✓ Veridicita': correttezza dell'interpretazione delle azioni
 che ne hanno determinato la comparsa delle prove

FRAGILITÀ DEI REPERTI

- Tutti i dispositivi oggetto di interesse (REPERTI) che si trovano nella scena del crimine vanno gestiti e controllati con i dovuti accorgimenti del caso.
- Non possono essere accesi e gestiti con leggerezza da parte dell'operatore.
- Fragilità della prova: data l'immaterialità della prova contenuta al suo interno, con estrema facilità può essere distrutta od alterata.



IL DATO

- Nel caso specifico ci occuperemo di ciò che riguarda la copia del dato (oggetto di indagine) = reperto informatico.
- Successivamente si passa alla fase di analisi e ricerca del dato.

Ma qual è il dato da ricercare?

L'aspetto più importante per un digital forenser è quello di seguire una metodologia investigativa standard e ben definita per la soluzione del problema forense che gli è stato sottoposto.



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

LA PROVA INFORMATICA/REPERTO



REGOLE DI INGAGGIO

- 1. Acquisire il reperto (usb pendrive)
- 2. Eseguire una copia forense:
 - 1. File immagine
 - 2. Clone di device
- 3. Verifica dei risultati
- 4. Consegna della prova per l'analisi



Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

Requisiti per la gestione della prova digitale

Verificabilità

- √ un terzo deve essere in grado di valutare le attività svolte
- √ documentazione di tutte le azioni svolte

Ripetibilità

✓ Le operazioni sono ripetibili sempre usando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni

Riproducibilità

✓ Le operazioni sono ripetibili sempre usando lo stesso metodo, strumenti diversi, sotto condizioni diverse

Giustificabilità

✓ Dimostrare che le scelte adoperate erano le migliori possibili

- La catena di custodia è un documento che contiene le informazioni di ciò che è stato fatto
 con la prova originale e con le copie forensi realizzate, a partire dall'acquisizione fino ad
 arrivare al giorno del processo.
- Tipiche informazioni che possono essere contenute inizialmente in questo documento sono:
 - ✓ Numero del caso
 - ✓ Società incaricata dell'investigazione
 - ✓ Investigatore assegnato al caso
 - ✓ Natura e breve descrizione del caso
 - ✓ Investigatore incaricato della duplicazione dei dati
 - ✓ Data e ora di inizio custodia
 - ✓ Luogo in cui il supporto è stato rinvenuto
 - ✓ Produttore del supporto
 - ✓ Modello del supporto
 - ✓ Numero di serie del supporto
- Ogni volta che i supporti oggetto di indagini vengono affidati ad un nuovo investigatore, nella catena di custodia, dovrà essere aggiunta un'informazione contenente:
 - ✓ Nome dell'incaricato all'analisi
 - ✓ Data e ora di presa in carico del supporto
 - ✓ Data e ora di restituzione del supporto



- •Terminata l'acquisizione procedere immediatamente alla custodia del disco originale.
- •Operazione fondamentale: creare in questa fase la Catena di Custodia



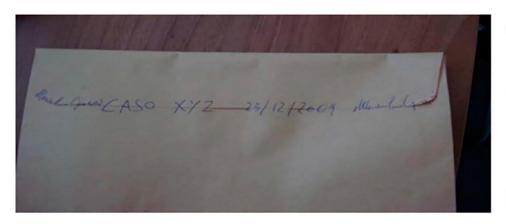
- Proteggere il supporto
- (esempio) inserire il supporto in una busta elettrostatica e poi avvolgerlo con un involucro antiurto





 Inserire tutto dentro una busta





 Porre le firme da coprire con nastro antieffrazione o ceralacca

RACCOLTA DELLA PROVA

- Terminata la fase di acquisizione delle informazioni, i device vengono rimossi dalla posizione originaria e trasportati in laboratorio per acquisizione e analisi.
- Le analisi possono anche essere eseguite sul posto o lasciando i device all'interno dei dispositivi. In questo caso occorre particolare cautela (modifica del BIOS)
- Talvolta rimuovere un supporto può essere rischioso, il device può trovarsi in due situazioni:
 - √acceso o spento

PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

Conservazione dei Device

ERRATO!





CORRETTO!



LA METODOLOGIA INVESTIGATIVA

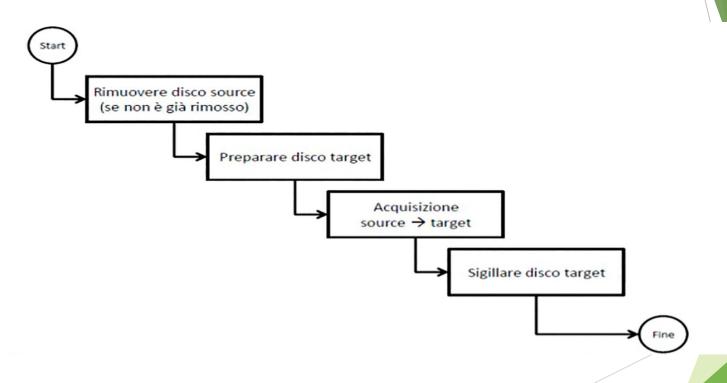
METODOLOGIA INVESTIGATIVA

- Profilo investigativo: determinazione dei passi operativi necessari allo svolgimento del caso, tenendo in considerazione il tempo necessario per ciascuno
- Determinazione delle risorse necessarie (hardware, software open source e professionali)
- Determinazione dei rischi e relativa predisposizione di una catena di custodia
- Analisi e recupero della prova digitale
- Stesura del report finale



Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

ACQUISIZIONE DISPOSITIVO SPENTO



PROCEDURE DI ACQUISIZIONE

PROCEDURE DI ACQUISIZIONE

- Individuazione del device da acquisire
- Assicurarsi di avere accesso in sola lettura al device
- Calcolo hash del device
- Acquisizione del device con creazione hash
- · Verifica degli hash calcolati
- Copia su un altro supporto dell'immagine acquisita con relativa verifica dell'hash (copia operativa)

NDIVIDUAZIONE DEL DEVICE DA ACQUISIRE

- Pendrive USB: DataTraveler 2GB
- Acquisizione delle info sul device (vedi es.con cat)



ALCUNE CONSIDERAZIONI PRIMA DI INIZIARE

- Non esiste un metodo o un software che si abbinano ad ogni singolo caso.
- Esistono programmi, distribuzioni su varie piattaforme dedicati alla forensics.
- Piccoli e banali tool di pochi kb a volte risolvono un caso.. (www.sleuthkit.org)

SOFTWARE E HARDWARE DA UTILIZZARE

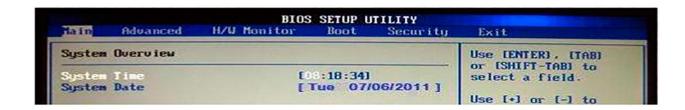
- Sul mercato sono disponibili diversi software che consentono di effettuare la copia bit-a-bit di un supporto di memoria:
 - ✓ Dispositivi HW ad hoc, con dei limiti:
 - o Tecnologia specifica;
 - Singoli dischi;
 - ✓ Software specializzati (es.dd, semplice e in grado si essere mostrato a livello di file sorgente);
- Ideale, dotarsi di una buona workstation forense con le interfacce più utilizzate sul mercato.

IMPORTANTE

Di pari passo alle attività tecniche dovranno essere eseguite, scrupolosamente, tutte le attività di reporting

SINCRONIZZAZIONE DI DATA E ORA

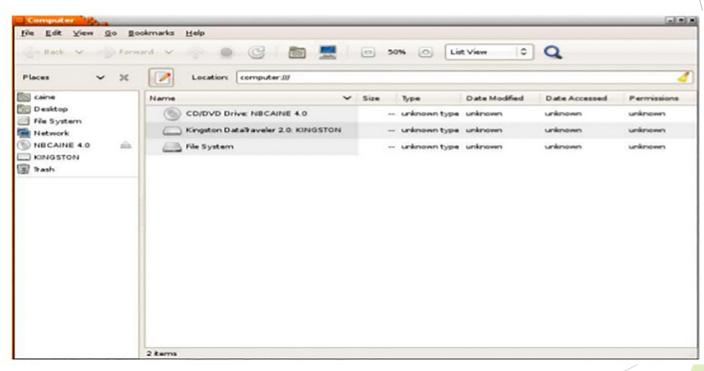
 Prima di addentrarci nella parte che riguarda la copia forense dell'hd, è opportuno sincronizzare la data e l'ora della macchina in esame, accedendo al bios.



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

COLLEGAMENTO DELLA PENDRIVE USB





WRITE BLOCKER

- Garantisce un blocco dell'accesso in scrittura per mantenere l'integrità della prova;
- Esistono due differenti metodologie per garantire il write blocking:
 - ✓ Write blocker software;
 - Agisce sull'operazione di mounting dell'hard disk da parte del sistema operativo.
 - ✓ Write blocker hardware;
 - o dispositivo fisico che viene posto tra l'hard disk e la macchina di acquisizione forense.



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

BITLOCKER: HARDWARE







VERIFICA INTEGRITÀ

- Garantisce che la copia del device sia inalterata ed identica all'originale
- Si utilizzano funzioni hash
 - ✓ Una funzione hash è un algoritmo che converte un input di grandezza qualunque in un output di grandezza prefissata chiamato "valore hash" tale che una qualsiasi modifica, accidentale o meno, nell'input originale generi con elevata probabilità un hash totalmente differente. L'hash rappresenta una firma digitale, un'impronta dell'input.
- · Gli algoritmi più utilizzati sono MD5 e SHA-1, ma ne esistono altri
- E' possibile ripetere la verifica sulle copie forensi o sui supporti originali in qualsiasi momento per dimostrare che i dati non sono stati alterati

ALGORITMI HASH

 MD5 (RFC 1321): Prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit (con lunghezza fissa di 32 valori esadecimali, indipendentemente dalla stringa di input)

√ md5sum <nome.file>

• SHA-1 (RFC 3174): Prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 160 bit (con lunghezza fissa di 40 valori esadecimali, indipendentemente dalla stringa di input)

√ sha1sum <nome.file>

CALCOLO DELL'HASH DEL DEVICE

```
caine@caine:~$ sudo su -
```

root@caine:~# md5sum /dev/sdb

2578836c63af173945200816bea039fa /dev/sdb

root@caine:~# sha1sum /dev/sdb

1b08156257acca064e815ecf949b0f1e837ab7cd /dev/sdb



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

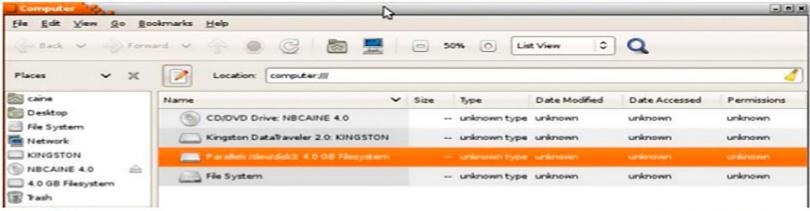
Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

PREPARAZIONE DISPOSITIVO

DI DESTINAZIONE









Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

COPIA



- PROVA ORIGINALE: pendrive USB Travel
 2GB = /dev/sdb
- DESTINAZIONE: SDHC card SanDisk 4GB = /dev/sdc

```
oot@caine:~# cat /proc/scsi/usb-storage/*
  Host scsi8: usb-storage
      Vendor: Kingston
     Product: DataTraveler 2.0
Serial Number: 899000000000000045B46334
    Protocol: Transparent SCSI
   Transport: Bulk
      Ouirks:
  Host scsi9: usb-storage
      Vendor: Parallels
     Product: APPLE SD Card Reader (disk3)
Serial Number: D83C66B2267F
    Protocol: Transparent SCSI
   Transport: Bulk
      Quirks:
oot@caine:~#
```

LA COPIA FORENSE

LA COPIA FORENSE

- Per copia forense (o bit-stream image) si intende l'acquisizione che genera una copia bit a bit di un dispositivo di memoria (ORIGINALE) su un altro dispositivo di memorizzazione (OPERATIVO)
- Deve essere quindi possibile ricreare un supporto perfettamente identico, a livello logico, all'originale
 - ✓ Un "copia e incolla" NON è una copia forense
 - ✓ Un "drag & drop" NON è una copia forense

PERCHÉ? Una copia forense include anche

- ✓ MBR
- ✓ File cancellati
- ✓ Slack space (Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per ultimo)
- ✓ Spazio libero

TIPOLOGIE DI COPIA

- CLONAZIONE: duplicazione di un dispositivo, comprendendo tutte le zone che non contengono alcun file direttamente visibile all'utente, definite tecnicamente aree non allocate.
- IMAGINE: copia del disco sorgente, comprendendo tutte le zone che non contengono alcun file direttamente visibile all'utente, in un file all'interno del filesystem del disco destinazione.



TIPOLOGIE DI COPIA

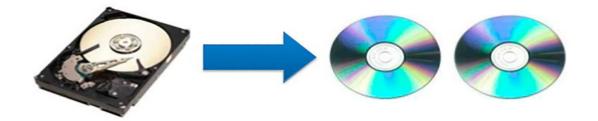
- RAW: il file sarà grande esattamente X poiché i bit saranno copiati uno ad uno senza alcuna compressione o organizzazione dei dati.
- EWF: (Expert Witness Format) è alla base dei formati immagine creati da EnCase ed altri tool.
- AFF: (Advanced Forensics Format) è un formato immagine sviluppato per essere estensibile ed aperto formato consiste in un gruppo di coppie nome-valore, chiamati segmenti. Alcuni segmenti contengono i dati ed altri contengono i metadati.

STRUMENTI NECESSARI ALL'ACQUISIZIONE

- GRUPPO DI CONTINUITA'
- WRITE BLOCKER (HW o SW)
- ADATATTORI
- SPAZIO DISCO
 - ✓ A causa delle limitazioni fisiche del supporto di destinazione (es. backup su DVD) oppure per motivi di compatibilità di filesystem (es. FAT32, nel caso in cui più periti debbano lavorare con sistemi eterogenei), l'immagine deve essere divisa in file più piccoli.
 - ✓ E' possibile dividerla direttamente in fase di acquisizione utilizzando il comando split.

LA COPIA DELLA COPIA

- Fare sempre un'ulteriore copia dell'immagine acquisita e verificarne l'integrità
- In particolar modo quando si lavora su file image e poter sempre fare un roll-back, evitando tutto il procedimento di riacquisizione



CONSERVAZIONE DEI DATI

- Proteggere integrità dei dati
 - ✓ Da alterazioni naturali, colpose o dolose
- · Normalmente, non dovrebbero esserci alterazioni
 - ✓ Utilizzare metodologia per dimostrare che non si sono verificate alterazioni
- Proteggere anche la riservatezza dei dati
- Utilizzare imballaggi opportuni
 - ✓ Es.: per i supporti magnetici, imballaggi antistatici
 - ✓ Non devono danneggiare il supporto

RELAZIONE TECNICA

- Sintetica: dato che non necessita di riportare eccessivi particolari tecnici dell'analisi ma solo ciò che interessa dal punto di vista giuridico;
- Semplificata: colui che legge e valuta l'esito è di principio un fruitore inesperto nel settore informatico e quindi, nell'ipotesi che sia possibile, bisogna eliminare terminologie non consuete e spiegare a livello elementare quanto rilevato;
- Asettica: non deve contenere giudizi personali dell'operatore né tanto meno valutazioni legali sulle informazioni rilevate a meno che tali considerazioni non siano state espressamente richieste.



CASO PRATICO PER IL SEQUESTRO DI MEMORIE MOBILE



DATI FASCICOLO		
Procedimento N / Mod.: RGNR		
Autorità Competente:		
Indagato:		
Bene in disponibilità di:		
N.:	DESCRIZIONE BENE	
Tipologia apparato	[] Telefono/Smartphone [] Tablet [] Smart w [] Altro :	
Marca		
Modello		
IMEI	1:2:	
SIM	ICCID: N.TEL:	PIN:
Memorie esterne	[] SD CARD Capacità: Marca:	
Stato dispositivo		
Supporti a corredo		
Rilievi fotografici		
Codici Accesso	PIN: (4 o 6 NUMERI) [] Riconoscimento Facciale [] Importate digitale	Annotare il pattern e la direzione

NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO

<u>Utilizzatore:</u> Nel caso si proceda al sequestro di un dispositivo utilizzato da conviventi, familiari dell'indagato, in quanto si sospetta che possano celare evidenze informatiche, specificare appositamente l'utilizzatore del dispositivo.

<u>Tipologia apparato</u>: specificare se il sistema mobile (in grado di connettersi a una rete cellulare senza utilizzo di cavi tipo Wi-Fi, Bluetooth etc..) sia un cellulare senza la disponibilità di servizi internet come la messaggistica istantanea (Whatsapp etc.), oppure sia uno smartphone fornito di tali servizi.

<u>Il modello</u>: Generalmente si trova nella scocca posteriore del dispositivo ed è contraddistinto da una sigla ad esempio SM-G960 (SAMSUNG) o A1337 (Apple).

<u>IMEI:</u> Per alcuni dispositivi, in particolare quelli più datati, è possibile rinvenire l'IMEI nella scocca posteriore del dispositivo (generalmente nei pressi della batteria), oppure sulla scatola di acquisto. Se il dispositivo è acceso e sbloccato digitare la sequenza *#06#, annotando il codice IMEI rilevato.

NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO

<u>SIM:</u> Specificare l'ICCID stampato sulla SIM generalmente sotto il logo del gestore in quanto è l'ICCID che identifica una SIM. In taluni casi impedire all'utente il riutilizzo dell'utenza associata alla SIM card potrebbe rivelarsi utile, per cui andrà richiesto all'A.G. apposito provvedimento d'inibizione da notificare al competente gestore. <u>Specificare marca della SIM e annotare anche il numero di utenza del telefono.</u>

<u>Memorie esterne:</u> Se il dispositivo oggetto di verifica è dotato di memorie esterne tipo sd card. Questa condizione si verifica per gli android e per alcuni telefoni di vecchia generazione.

<u>Stato:</u> Descrivere se il dispositivo sia stato rinvenuto acceso I spento, se presenta danni strutturali (rottura vetro, involucro esterno o altro. <u>Il dispositivo nel limite del possibile deve essere posto in modalità Aereo, Nel caso di incidenti stradali è utile rilevare se è abilitato il Bluetooth del dispositivo mobile, verificare lo stato del navigatore/radio a bordo del mezzo, se quest'ultimo è acceso o spento, ed infine accertare nel limite del possibile se il navigatore e il dispositivo mobile sono collegati.</u>

NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO

<u>Supporti a corredo:</u> Specificare se siano stati sequestrati anche scatolo, alimentatore cavi e quanto altro, specificando se si tratta di supporti originali. In alcuni casi taluni smartphone/cellulari utilizzano delle tipologie con standard proprietario difficilmente reperibili in commercio e fondamentali per l'estrazione dati per tanto è utile cercare sempre di recuperare i cavi originali.

Rilievi Fotografici: Cercare sempre di documentare, mediante fotografie lo stato del dispositivo all'atto del sequestro e non di meno il luogo ove è stato ritrovato, con descrizione analitica della scena sul verbale di sequestro.

PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO



NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO

Codici di Accesso: I codici di accesso al telefonino possono essere di varie tipologie:

- PIN (codice di accesso a 4 o 6 cifre numeriche)
- PASSWORD (codice di accesso complesso alfanumerico e di lunghezza non definita)
- Impronta digitale posta dietro al telefono o con nei più moderni con un micro sensore sul tasto accensione del telefono
- Riconoscimento facciale

NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO

Nel caso in cui l'interessato rifiuta di fornire i codici di accesso, oppure afferma di averle dimenticati, potrà essere reso edotto della possibilità che il superamento della password potrebbe comportare un "blocco" del dispositivo di sua proprietà.

Tuttavia con i nuovi strumenti a disposizione, in caso non sia fornito il PIN/PASSWORD non spegnere il dispositivo e tenerlo in corrente fino alla consegna di quest'ultimo al tecnico che dovrà operare la copia forense

PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

NOTIZIE UTILI PER LA COMPILAZIONE DEL VERBALE E L'ESECUZIONE DEL SEQUESTRO





Password alfanumerica

L'ACQUISIZIONE DEL DATO INFORMATICO

Consulente informatico **Dott. Odorisio Gallo**

L'ACQUISIZIONE DEL DATO INFORMATICO

Scopo della Digital Forensics è il dato, l'artefatto, l'evidenza digitale.

Che sia un file, un'immagine nascosta in un file, una foto pubblicata on-line, un post su facebook, ecc. le corrette modalità di acquisizione (e conservazione) sono fondamentali per la sua usabilità in giudizio

LE MODALITÀ DI ACQUISIZIONE

- Il dato può essere sequestrato, prendendo fisicamente il supporto che lo contiene: un PC, un telefono, una pen-drive, ecc.
- Il dato può essere copiato, dal supporto che lo contiene
- Il dato può essere intercettato, quando passa da un sistema ad un altro

DOVE CERCARE IL DATO

Stabilite le modalità di acquisizione, occorre sapere dove il dato risiede fisicamente. Ciascun dato infatti, ha due elementi di esistenza:

- fisico, il supporto che lo contiene (hard disk, una pendrive, uno smartphone, un NAS, un social network, il cloud, ecc.)
- digitale

IL SEQUESTRO

VANTAGGI

- Semplicità, sequestrando il contenitore del dato si evitano quelle attese (e preoccupazioni) legale alla duplicazione del dato e sua validazione tramite hash
- Velocità, individuato il contenitore del dato occorre solo prepararlo per il trasporto in laboratorio

IL SEQUESTRO

SVANTAGGI

- non è sempre possibile sequestrare
- I dati risiedono su sistemi distribuiti
- I dati risiedono su un'infrastruttura che non può essere spenta
- I dati risiedono in datacenter
- Il sistema su cui è presente il dato è virtuale

IL SEQUESTRO

CONSIDERAZIONI

Alla luce di queste considerazioni il sequestro, quindi, non è la soluzione definitiva per acquisire un dato anche se è indubbio che sia il metodo più veloce e pratico. L'Autorità Giudiziaria, inoltre, non ha la facoltà di disporre di un sequestro indiscriminato anche di materiale che non ha alcuna collegamento con il reato per il quale si sta procedendo per cui è bene considerare le accortezze da adottare al fine di procedere al sequestro nella maniera più corretta possibile in modo da evitare quegli errori che possano inficiare il buon esito dell'indagine.

LA PRESERVAZIONE DELLA PROVA: L 48/2008

...le modifiche apportate dalla L. 48/2008 il codice di procedura penale, con riferimento alle investigazioni informatiche, ha definitivamente accolto alcuni principi propri della Digital Forensics. Il legislatore tuttavia, ha ritenuto preferibile non specificare le metodologie da utilizzare limitandosi ad evidenziare quale sia il risultato che le stesse devono consentire di raggiungere. In sede di ispezione-perquisizione si dovranno adottare [...misure tecniche dirette ad assicurare la conservazione dei dati originali ed impedirne l'alterazione...], [...la copia deve essere realizzata su adeguati supporti mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità...]

LO SHUTDOWN

PRESERVARE LO STATO DELLA PROVA

Come comportarsi se in fase di perquisizione viene rinvenuto un PC acceso? La risposta è: dipende dal tipo di reato per cui si procede. In alcune circostanze, prima di spegnere la macchina con un regolare shutdown, potrebbe essere necessario:

- acquisire la memoria RAM (lo vedremo più avanti)
- effettuare una copia del supporto a livello cautelativo. E' il caso di computer molto datati dove uno spegnimento/riaccensione potrebbe stressare l'hardware che comporterebbero una mancata riaccensione del dispositivo o ancora il caso della presenza di volumi crittografati

. . .

LO SHUTDOWN

PRESERVARE LO STATO DELLA PROVA

L'ultima operazione da fare prima di uno shutdown, è annotare la data e l'ora corrente ed il loro scostamento rispetto all'ora esatta. Questo perché, specie se esaminato in un secondo momento, il computer potrebbe perdere l'impostazione corretta dell'orologio interno a causa ad esempio di una batteria tampone esaurita.

LA DUPLICAZIONE

L'ART. 254 BIS C.P.P.

Con l'introduzione del art. 254 c.p.p. il legislatore ha disciplinato il sequestro di dati informatici operato presso i fornitori di servizi telematici e delle telecomunicazioni prescrivendo la copia su adeguato supporto (e la sua immodificabilità) in modo da garantire la continuità del servizio. Per tutti gli altri scenari, la scelta tra sequestro del supporto e duplicazione, dovrà essere valutata caso per caso.

VALUTARE LA PRIORITÀ DEI DISPOSITIVI

In particolari scenari investigativi può risultare complesso se non impossibile procedere con l'esame delle possibili fonti di prova on-site. E' in queste circostanze che entra in gioco il c.d. Triage, vale a dire la capacità di valutare la priorità dei dispositivi utili alle indagini in modo da analizzare ed ordinare velocemente i dati in essi contenuti per individuare cosa sequestrare e attenzionare per ulteriori approfondimenti

STABILIRE LE PRIORITÀ

- Stabilire la priorità dei sistemi da attenzionare dipende da diversi fattori:
- lo stato delle macchine, quelle accese dovrebbero essere gestiti per prime
- volatilità del dato: un dato facilmente modificabile dovrebbe essere acquisito per primo rispetto ad uno non modificabile
- Il tipo di dispositivo

SCENARI POSSIBILI

- Moltitudine di dispositivi presenti sulla scena del crimine
- Tempo limitato per eseguire un'indagine approfondita
- Impossibilità a condurre un'analisi completa

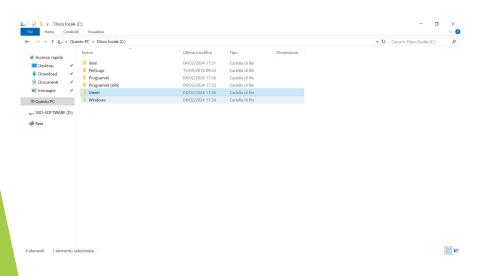
In questi ed altri scenari, è importante stabilire:

- Quali e quanti dispositivi contengono elementi utili
- Dove le evidenze digitali sono localizzate (quali sono i files e le cartelle da copiare)

VANTAGGI E SVANTAGGI

- Identificare la presenza di elementi utili alle indagini
- Identificare parole chiavi (keywords)
- non trattandosi di un'analisi completa occorre considerare ed accettare il rischio di perdere alcune evidenze utili alle indagini

DOVE CERCARE



\Users\%USERNAME%
, contiene il profillo
degli utenti loggati sul
sistema

JUMP LISTS

Le jumplists, sono un artefatto del sistema operativo Windows apparso per la prima volta in Windows 7 e presente nelle successive versioni di Windows. Le Jump Lists, consentono di accedere rapidamente ai file aperti di recente da un app presente nel menu 'Start' o nella 'Barra delle applicazioni'.

Path:

- \Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- \Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

JUMP LISTS

Ogni applicazione è caratterizzata da un 'ApplD' (89b0d939f117f75c), una stringa alfanumerica, che permette di identificare l'applicazione.

E' possibile trovare un elenco delle app più comuni seguendo gli URL

- https://github.com/EricZimmerman/JumpList/blob/master/JumpList/Resources/AppIDs.txt
- https://gist.github.com/atilaromero/2146441

JUMP LISTS

- I dati archiviati in questi cataloghi possono contenere informazioni potenzialmente utili:
 - MRU (Most Recently Used)
 - la data e l'ora in cui l'applicazione è stata avviata la prima volta (Created UTC)
 - la data e l'ora di ultimo avvio dell'applicazione

IL TRIAGE .LNK FILES

Sono 'collegamenti' a file ed applicazioni, normalmente creati in automatico da Windows, quando si installa un programma. Tuttavia, possono essere creati anche dall'utente per un accesso rapido per velocizzare l'accesso a dati ed applicazioni.

Path:

- \Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recents Items
- \Users\%USERNAME%\Desktop

IL TRIAGE .LNK FILES

E' possibile individuare, file con estensione .lnk anche nei seguenti percorsi:

- \Users\%USERNAME%\AppData\Roaming\Microsoft\Office\Recent\
 (per documenti Microsoft Office su Windows da 7 a 10)
- \Users\%USERNAME%\Download

- - -

IL TRIAGE LNK FILES

La quantità di informazioni che può contenere un file con estensione .lnk varia in base al sistema operativo in uso. Ad esempio in Windows 10 sono presenti informazioni prima assenti nelle precedenti versioni del sistema operativo. Un file con estensione .lnk può contenere:

- percorso di origine di un file e relativi marcatori temporali (percorso completo del file destinazione, ora di creazione, di modifica e ora di accesso del file destinazione)
- dimensione del file di destinazione (espressa in byte)
- etichetta di volume e numero di serie dell'unità

. . .

THUMB NAILS

E' un file di database che memorizza piccole immagini in modo da velocizzarne la funzione di anteprima.

Path:

\Users\%USERNAME%\AppData\Local\Microsoft\Windows\Explorer

THUMB NAILS

Conservando un'anteprima delle immagini, potrebbero conservare artefatti relativi ad immagini non più presenti nel sistema, modificati o altro.

IL TRIAGE WINDOWS SEARCH HISTORY

Windows Search History, è una funzionalità di Windows che conserva gli elementi cercati e le keywords utilizzate dall'utente

Path:

\Users\%USERNAME%\APPDATA\LOCAL\MICROSOFT\WINDOWS\HISTORY

IL TRIAGE WINDOWS SEARCH HISTORY

La cronologia delle ricerche è un artefatto particolarmente importante di Windows. Potrebbe rivelare abitudini ed interessi del soggetto attraverso gli elementi ricercati per i quali viene indicato la data e l'ora in cui è stata eseguita la ricerca

IL CESTINO (RECYLE BIN)

Il cestino di Windows è il luogo in cui vengono conservati gli elementi cancellati fino alla lora definitiva eliminazione. Il cestino è un elemento nascosto del Sistema Operativo, può essere visualizzato da linea di comando o con l'ausilio di alcuni strumenti

Path:

C:\\$Recycle.bin\<**S**ecurity **ID**entifier>\

IL TRIAGE IL CESTINO (RECYLE BIN)

Nei moderni Sistemi Operativi, ogni file eliminato conserva due file:

- \$1, che contiene i metadati del file eliminato
- \$R, che contiene il file vero e proprio

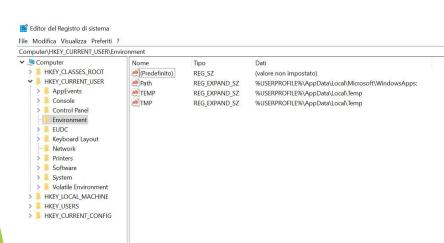
Se si elimina una cartella, \$R conterrà l'elenco dei nomi dei file eliminati in essa contenuti

IL REGISTRO DI WINDOWS

Il registro di Windows è un database strutturato che ospita la configurazione del Sistema Operativo di casa Microsoft e di numerose applicazioni. Sebbene l'utente standard ignori la sua esistenza, si trova spesso ad interagire con esso dal momento che l'installazione di un programma o l'utilizzo di un'applicazione registrano al suo interno preziose informazioni per gli investigatori forensi.

Tuttavia, non tutte le applicazioni memorizzano informazioni all'interno del registro di Windows per cui, anche se non vi è traccia di un'applicazione, non vuol dire che essa non sia stata utilizzata.

IL REGISTRO DI WINDOWS



In quanto database strutturato, il registro di Windows è diviso in hive.
Ad esempio l'hive
HKEY_CURRENT_USER archivia le impostazioni specifiche dell'utente attualmente connesso al sistema.

IL REGISTRO DI WINDOWS

Il Registro di Windows archivia i dati dell'hive HKEY_CURRENT_USER in un file denominato NTUSER. DAT

Path:

Users\%useraccount%\NTUSER.DAT

I dati contenuti in questo file vengono aggiornati ogni secondo per cui la sua copia del file è possibile solo quando l'utente non ha effettuato l'accesso al proprio account o con l'aiuto di software specializzati.

IL REGISTRO DI WINDOWS

Il registro di sistema di Windows è molto complesso tuttavia, avere la consapevolezza della sua esistenza aiuta a non trascurare un elemento così importante in occasione di un'indagine forense.

Di seguito alcune informazioni che possono essere estratte dal registro di sistema di Windows

- Time Zone, HKLM\SYSTEM\ControlSet###\Control\TimeZoneInformation
- Last User Logged In, SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
- USBSTOR, HKLM\SYSTEM\CONTROLSET00#\ENUM\USBSTOR

. . .

STRUMENTI UTILI

- Distribuzioni Linux Open Source (Caine, Deft, Kali...)
- FTK Imager
- Belkasoft Triage T
 - → è una soluzione c.d. portable che non richiede installazione
 - → è progettato per lasciare solo piccole tracce del suo utilizzo sul sistema target (ad esempio la cronologia degli storage collegati al dispositivo)
 - non necessità di altri supporti, vale a dire che è possibile copiare i risultati direttamente sul dispositivo da cui viene eseguito

FTK IMAGER

Uno strumento particolarmente versatile è FTK Imager sviluppato da Access Data. Il tool consente non solo di effettuare copie bit a bit ma anche di eseguire copie di singole cartelle, interi file system o share di rete includendo la copia in un contenitore logico con estensione .AD1 (tramite la funzione 'Add to Custom Content Image AD1').

Terminate le operazioni, l'immagine creata verrà automaticamente validata tramite gli algoritmi di hash MD5 e SHA1 da riportare nei verbali delle attività eseguite.

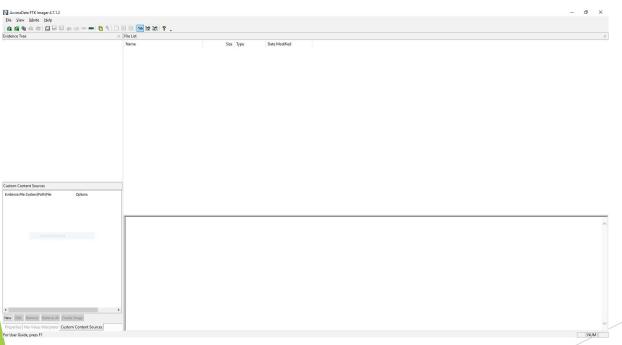


PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

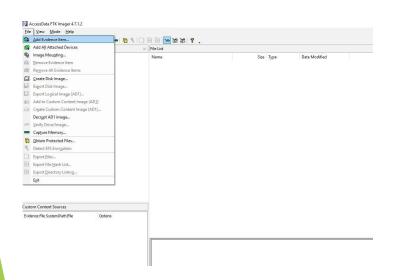
Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

IL TRIAGE

FTK IMAGER

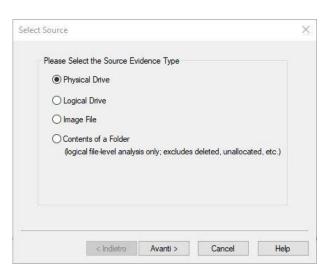


FTK IMAGER



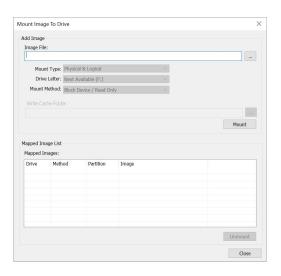
FTK Image consente di lavorare col più diffuso formato di imaging, ormai diventato uno standard, noto come Expert Witness Format o anche Encase (.e01). Il formato Encase, consente di ridurre di parecchio la dimensione dell'immagine di destinazione in quanto le aree non utilizzate del disco e contenenti zeri verranno compresse, così come i file con caratteristiche comprimibili quali testo e documenti.

FTK IMAGER



- FTK Image consente di lavorare con:
- Physical Drive, unità fisiche
- · Logical Drive, unità logiche
- Image File, file immagine
- Contents of a folder, le comuni cartelle

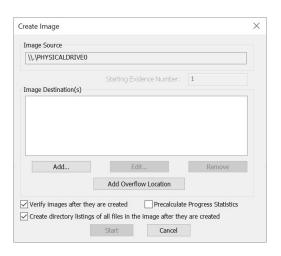
FTK IMAGER



La funzione Image Mounting, presente nel menu File, consente di 'montare' un'immagine in modo da sfogliarne il contenuto come se fosse fisicamente collegata al dispositivo.

Il mounting dell'immagine, come impostazione predefinita, avviene nella modalità Read Only (sola lettura). Questo consente di sfogliare il contenuto dell'unità in sicurezza senza alterare in alcun modo i dati in essa contenuti.

FTK IMAGER



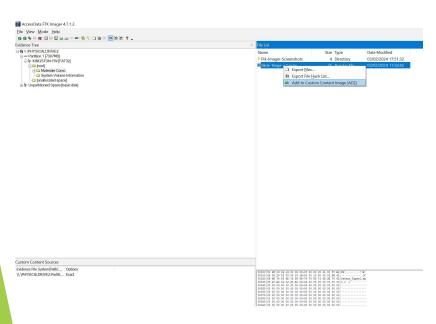
La funzione Create Disk Image, presente nel menu File, consente di creare un'immagine da una sorgente.

I formati immagine comunemente utilizzati sono:

- RAW (dd)
- E01

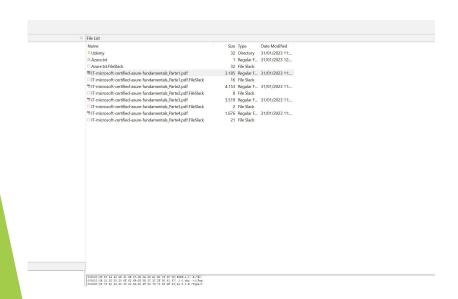
E' possibile verificare l'immagine al termine della sua creazione così come è possibile creare automaticamente un elenco di tutti i file in essa contenuti

FTK IMAGER



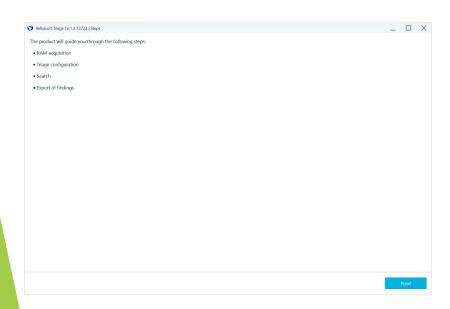
FTK Imager consente di aggiungere file e cartelle in un contenitore logico tramite la funzione Add to Custom Content Image (AD1). L'immagine creata verrà automaticamente valorizzata tramite le funzioni di hash MD5 e SHA1. I valori di hash, unitamente al nome del contenitore creato, possono essere immediatamente verbalizzati

FTK IMAGER



Lo Slack Space, visualizzato con estensione .FileSlack, è lo spazio inutilizzato nel blocco di archiviazione di un file. Questo spazio può essere utilizzato per celare dati del tipo testo, immagini, ecc.

BELKASOFT TRIAGE



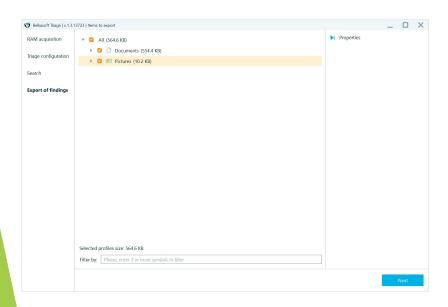
Belkasoft Triage consente, tramite un semplice wizard, di eseguire un triage efficace di un'unità o di una cartella. Il software consente inoltre l'acquisizione della memoria RAM ed una ricerca per hashset con pieno supporto NSRL (National Software Reference Library). Un Reference Data Set (RDS) contiene le firme di applicazioni considerate dannose ad esempio steganografia e script di hacking.

PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI BENEVENTO

Incontri Formativi per gli Organi Inquirenti in materia di Indagini Informatiche

IL TRIAGE

BELKASOFT TRIAGE



Al termine dell'analisi i risultati di interesse possono essere esportati in formato compresso .tar ed analizzati con i comuni software di analisi forense

MEMORY FORENSICS

- La RAM (Random Access Memory), è un particolare tipo di memoria utilizzata da un processo in esecuzione per l'archiviazione dei dati.
- Essendo una memoria ad accesso casuale (in contrapposizione a quella sequenziale), i programmi la utilizzano per leggere e scrivere le informazioni più velocemente.
- La memoria RAM è per sua natura una memoria volatile vale a dire che ad ogni riavvio del sistema il suo contenuto viene cancellato.

MEMORY FORENSICS

La memoria RAM è una fonte inestimabile di informazioni che non possono essere trovate altrove.

Essa può contenere:

- password dei volumi crittografati (BitLocker, VeraCrypt)
- credenziali di accesso dell'utente loggato
- cronologia della navigazione InPrivate
- dati di sessioni remote
- transazioni di criptovaluta

..

MEMORY FORENSICS: REQUISITI PER IL DUMPING

- portabilità, lo strumento utilizzato non può essere installato sulla macchina Host
- funzionalità in modalità Kernel
- low imprinting, lo strumento utilizzato deve avere un impatto minimo sul sistema:
 - non deve esportare il dump acquisito sulla macchina Host
 - o non deve utilizzare la cartella Temp di Windows
 - Il file eseguibile e le librerie che utilizza devono occupare il minor volume possibile di memoria RAM in modo da non sovrascrivere dati potenzialmente utili

MEMORY FORENSICS: ALCUNI STRUMENTI

Acquisizione della RAM

- FTK Imager
- Belkasoft Live RAM Capture
- Winpmem (https://winpmem.velocidex.com/)
 >.\winpmem_mini_x64_rc2.exe --output mem-dump.raw

..

Analisi della RAM

Volatility Framework (https://www.volatilityfoundation.org/releases/)

DOCUMENTARE

Dai sistemi più semplici a quelli più complessi, dove non può considerarsi l'associazione PC/memorie di massa, <u>la regola è documentare</u>

- in maniera minuziosa, magari supportata da foto, video o log le operazioni eseguite
- minimizzare il numero delle operazioni specificando le alterazioni che si stanno compiendo (ad esempio le date di ultimo accesso)
- cristallizzare i dati raccolti con una funzione di hash non soggetta a collisione (MD5 + SHA1) o solo SHA-2

GRAZIE PER L'ATTENZIONE