INTERNET FORENSICS

Acquisizione Forense di Evidenze in Rete

INDAGINI ONLINE

About me

Ho studiato Ingegneria Informatica (La Sapienza) e Sicurezza Informatica (UniMI).

Successivamente, mi sono «perfezionato» in Data Protection & Data Governance (UniMI), Criminalità Informatica & Investigazioni Digitali e Big Data & Artificial Intelligence (UniMI)

Ho conseguito l'Advanced Cybersecurity Graduate Certificate alla Stanford University, il CERT Certification in Digital Forensics alla Carnegie Mellon University, l'European Certificate on Cybercrime and E-Evidence (ECCE) rilasciato dall'European Commission's Directorate General Justice, Freedom and Security.

Dal 1992 Referente Informatico e Funzionario alla Sicurezza c/o Ministero dell'Interno.

Dal 2004 Information Security Engineering: mi occupo della risoluzione delle problematiche connesse alla sicurezza delle informazioni ed alla tutela dei dati personali

Dal 2005 Consulente di Informatica Forense: esercito l'attività di consulenza tecnica in procedimenti giudiziari che hanno ad oggetto i reati informatici o che vengono attuati tramite l'information & communication technology

Dal 2017 Professore a contratto di Tecnologie per la Sicurezza Informatica c/o Università

Dal 2018 Trainer sulle tematiche della Cyber Security e Digital Forensics (Indagini Online)

Autore di alcuni articoli e saggi

INDAGINI ONLINE

Punto di partenza

La maggior parte delle azioni umane sono svolte interagendo, direttamente o indirettamente, con gli strumenti dell'ICT.

Anche i reati hanno questa peculiarità? **SI**

Distinguiamo **i reati**:

- tipicamente informatici
- aventi ad oggetto gli strumenti dell'ICT
- perpetrati attraverso l'uso di strumenti dell'ICT
- che lasciano tracce sugli strumenti dell'ICT

e gli altri **illeciti**? **SI**

- procedimenti civili
- procedimenti aventi ad oggetto il diritto del lavoro
- procedimenti amministrativi
- procedimenti in materia tributaria

Problema

Inoltre, la nascita del c.d. Web 2.0 e la crescente pervasività delle tecnologie ha favorito la proliferazione di diversi servizi Internet (**Newsgroup, Blog, Chat, Social network**), utilizzati per la diffusione delle informazioni, spesso non regolamentati e coperti dall'anonimato.

Ciò ha incrementato il numero di specifici reati legati al mondo digitale:

la diffamazione, lo stalking (cyber-stalking), l'hate-speech, l'adescamento telematico (grooming), la pedopornografia, il reverge porn, il sextortion, il furto d'identità digitale, la sostituzione di persona, la violazione di copyright e l'utilizzo illecito di marchi, il furto dei dati, il phishing, le truffe online, l'accesso abusivo ad una banca dati, la violazione della privacy, il controllo a distanza illecito, l'assenza di tutela legale, l'intercettazione abusiva, gli attacchi denial of service, il danneggiamento degli apparati di telecomunicazione, ecc.

Soluzione

In base alle caratteristiche di alcuni dei predetti servizi,
le informazioni oggetto di reato possono essere volatili e, quindi, facilmente **manipolabili o rimovibili**.

Quindi abbiamo la necessità di acquisire in maniera certa e sicura le evidenze presenti online da diversi fonti e servizi diversi.

La soluzione consiste nel realizzare una acquisizione forense e certificata del contenuto che si contesta così come è consultabile, che diventerà evidenza, prima che possa scomparire.

Tipologie di dati online

- siti web, forum, gruppi di discussione
- posta elettronica e mailing list
- dati di geolocalizzazione
- profili, pagine, gruppi su social network
- file sharing
- streaming audio/video
- servizi o app web per dispositivi desktop e mobile
- chat, gruppi, supergruppi, canali e bot
- messaggi delle piattaforme di messagistica
- informazioni sui conti delle cripto valute

Acquisizione di una pagina web

La stampa in PDF o su carta può essere utilizzata come prova?

Le stampe o gli screenshot difficilmente sono ammessi in un procedimento giudiziario come prova perchè non godono dell'**integrità** delle evidenze informatiche raccolte con strumentazione adeguata e metodi scientifici.

Anche la fotografia dello schermo del PC non ha pienamente valore probatorio, o meglio, può essere facilmente essere contestata dalla controparte, poiché per quanto possa avere una storicità temporale (l'ora esatta potrebbe essere contenuta nell'immagine, ovvero il sistema che l'ha generata si sincronizza automaticamente con l'ora esatta e salva le immagini in modo incrementale) ritrae qualcosa che può facilmente essere **artefatto** (lo schermo).

Acquisizione di una pagina web

La stampa in PDF o su carta può essere utilizzata come prova?

La stampa di un pagina web **certificata da un Notaio** o da un **Pubblico Ufficiale** è certamente un'alternativa migliore, ma può non essere sufficiente a identificare l'autore del reato, per esempio nel caso di un post diffamatorio pubblicato su un social network è necessario acquisire anche ulteriori dati come il codice identificativo univoco che permette di ritrovare il profilo o la pagina diffamatoria anche in caso di cambio del nome o dell'indirizzo.

Fatto salvo **il principio del libero convincimento del giudice** che gli consente di valutare la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati (c.p.p. art. 192, comma I).

Digital Evidence

Definizione

La fonte di prova digitale o digital evidence è ***«qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale»***

Distinguiamo:

- La prova creata dall'uomo
- La prova creata autonomamente dal computer
- La prova creata sia dall'essere umano che dal computer

Caratteristiche

Le peculiarità che contraddistinguono la fonte di prova digitale, che non possono essere ignorate, consistono in:

- **Immaterialità**: la prova digitale è il contenuto e non il supporto su cui è memorizzata;
- **Dispersione**: la prova digitale può essere dislocata su più dispositivi molto distanti tra loro,
- **Promiscuità**: la prova digitale può trovarsi all'interno di dispositivi che contengono altre informazioni non attinenti all'indagine,
- **Congenita modificabilità**: la prova digitale è estremamente alterabile.

Digital Forensics: perché?

Il tema della prova è centrale all'interno del processo, costituendo il campo più critico entro il quale si dispiega l'attività degli operatori del diritto e che oggi non può prescindere dall'informatica, dalla **volatilità** e **fragilità** del **dato informatico**, dall'importanza della corretta acquisizione e gestione dei bit, dalla fonte di prova digitale.

La giurisprudenza, pertanto, incoraggia l'utilizzo delle tecniche di informatica forense, affinché siano estratti contenuti in copia dei dati presenti, cristallizzati in **copie forensi** consentendo la produzione di **elementi giudiziali certi**, in relazione ad **integrità** dei dati, **non manipolazione, riconducibilità all'autore** e **certezza temporale**, rendendo la copia forense prodotta **immodificabile** e tendenzialmente vincolante per il giudicante.

Scopo: Digital Forensics

Lo scopo dell'informatica forense si esplicita nelle seguenti prerogative: **identificare, conservare, acquisire, documentare e interpretare** i dati presenti su una memoria digitale.

L'ordinamento Italiano, dopo l'approvazione della Legge 48 del 2008 di ratifica della Convenzione sul Cybercrime di Budapest, **ha stabilito che**, nel processo penale, **tutte le attività probatorie che hanno ad oggetto le prove digitali devono essere disposte attraverso tecniche idonee ad assicurare la conservazione dei dati originali ed impedirne l'alterazione**.

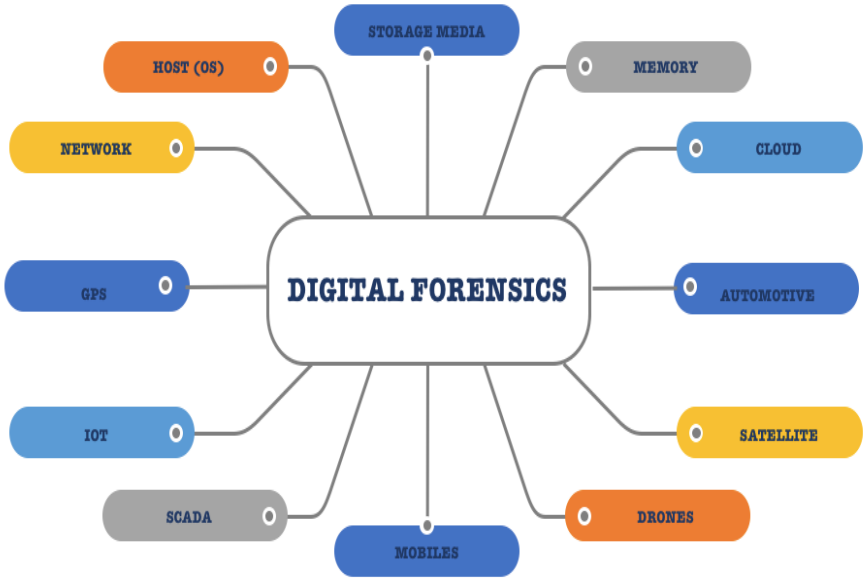
Pertanto, è necessario che anche **le metodologie utilizzate per il trattamento delle evidenze digitali abbiano la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle parti processuali in ordine alla loro verificabilità, ripetibilità, riproducibilità e giustificabilità.**

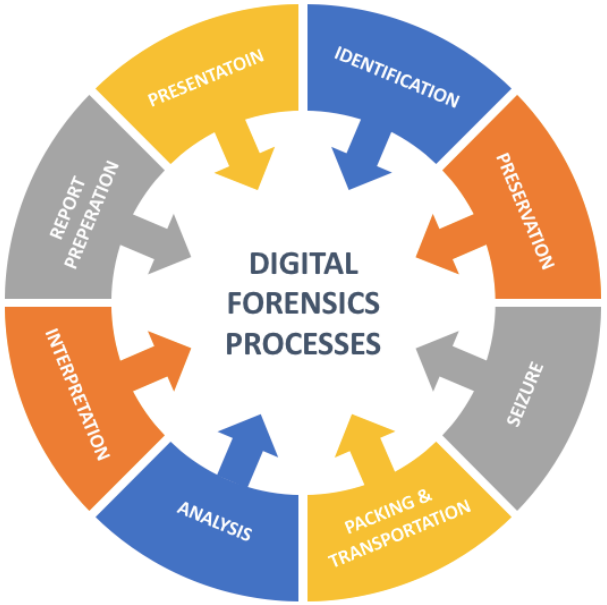
Per tale motivo è fortemente consigliato impiegare tecniche e standard ispirati al **metodo scientifico.**

Protocolli di Digital Forensics

Lo standard ISO/IEC 27037:2012 "**Guidelines for identification, collection, acquisition, and preservation of digital evidence**" fornisce delle linee guida relative alla gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di identificazione, raccolta, acquisizione e preservazione.

Lo standard ISO/IEC 27042:2015 «**Guidelines for the analysis and interpretation of digital evidence**" fornisce una guida sull'analisi e l'interpretazione delle prove digitali in grado di affrontare le questioni di continuità, validità, riproducibilità e ripetibilità.





Identificazione dei contenuti web

Iniziare a raccogliere le informazioni a latere:

- l'indirizzo del sito/servizio (whois)
- il proprietario del sito/servizio
- la tecnologia utilizzata per creare il sito/servizio
- l'autore dell'informazione (**ID user**)
- i dati identificativi dell'informazione (**ID del post, l'ora e la data**)
- **Creare la <u>storyboard</u> dei contenuti che occorre acquisire per**
  - **rappresentare l'informazione d'interesse**
  - **dimostrare l'autore della pubblicazione (profiling) e delle altre informazioni a latere che aiutano a rafforzare l'autenticità del dato**

OSINT

Vedasi Tabella 1 e Tabella 2

IDENTIFICATION SHEET

IDENTIFICATIVO CASO: | COMMITTENTE:

DATA E ORA: | COMPILATORE:

DESCRIZIONE:

Informazioni sul Target

NOME A DOMINIO:

INFO REGISTRANTE:

IP ADDRESSES: | NAMESERVERS:

LOCALIZZAZIONE: | DATA E ORA:

SERVIZI DISPOBINILI:

SERVIZI DI INTERESSE:

Informazioni sulla Connettività

INTERNET SERVICE PROVIDER:

LOCALIZZAZIONE: | DATA E ORA:

IP ADDRESS PUBLIC: | DNS SERVERS:

PROXY SERVER: NO | SI | URI: | PORT:

INDIRIZZO:

Informazioni sul Client di Acquisizione

SERVIZIO IN HOSTING: NO | SI | URI:

POSTAZIONE CLIENT: NO | SI | IN VIRTUAL MACHINE: NO | SI | IN CLOUD: NO | SI

LOCALIZZAZIONE: | DATA E ORA:

CONFIGURAZIONE DI RETE: INDIRIZZO IP | GATEWAY | DNS

SISTEMA OPERATIVO:

SOFTWARE UTILIZZATI:

NOTE:

INVESTIGATION PLANNING

IDENTIFICATIVO CASO: | COMMITTENTE:

DATA E ORA: | COMPILATORE:

DESCRIZIONE:

Caratteristiche del Target

FONTE APERTA (indicare [SI]/[NO]): SI / NO ---> indicare le modalità e le credenziali di accesso

ACCESSO DIRETTO: indicare l'url iniziale

ACCESSO INTERATTIVO: indicare le keys utilizzate per raggiungere l'evidenza

Storyboard

ID	EVIDENZA			
1	Descrizione			
	Autore	Data e ora pubbl.		
	URI da acquisire			
	FILE da acquisire			
	Note	Acquisita		
2	Descrizione			
	Autore	Data e ora pubbl.		
	URI da acquisire			
	FILE da acquisire			
	Note	Acquisita		
3	Descrizione			
	Autore	Data e ora pubbl.		
	URI da acquisire			
	FILE da acquisire			
	Note	Acquisita		
4	Descrizione			
	Autore	Data e ora pubbl.		
	URI da acquisire			
	FILE da acquisire			
	Note	Acquisita		
5	Descrizione			
	Autore	Data e ora pubbl.		
	URI da acquisire			
	FILE da acquisire			
	Note	Acquisita		

Identificazione tools

Per individuare le informazioni sul Target si suggerisce l'utilizzo di alcuni servizi web quali:

- DOMAINTOOLS (https://whois.domaintools.com/): un portale che ci consente di ottenere le informazioni sul nome di dominio, il proprietario, l'indirizzo del server, la localizzazione, ISP ed i suoi DNS di riferimento;
- IPINFO.IO (https://ipinfo.io/): consente di ottenere informazioni dettagliate sull'indirizzo IP;
- WAPPALYZER (https://www.wappalyzer.com/): rileva le tecnologie in uso sul server;
- SHODAN (https://www.shodan.io/): un motore di ricerca dedicato alla ricerca dei dispositivi collegati ad Internet e ci consente di scoprirne anche le tecnologie impiegate.

Per reperire le informazioni concernenti la Connettività e la postazione Client è sufficiente eseguire interrogare il sito:

- IP Analyzer (https://ipalyzer.com/) (inserendo il proprio indirizzo ip visibile in homepage)
- Data e ora esatta
- ipconfig /all

Collection

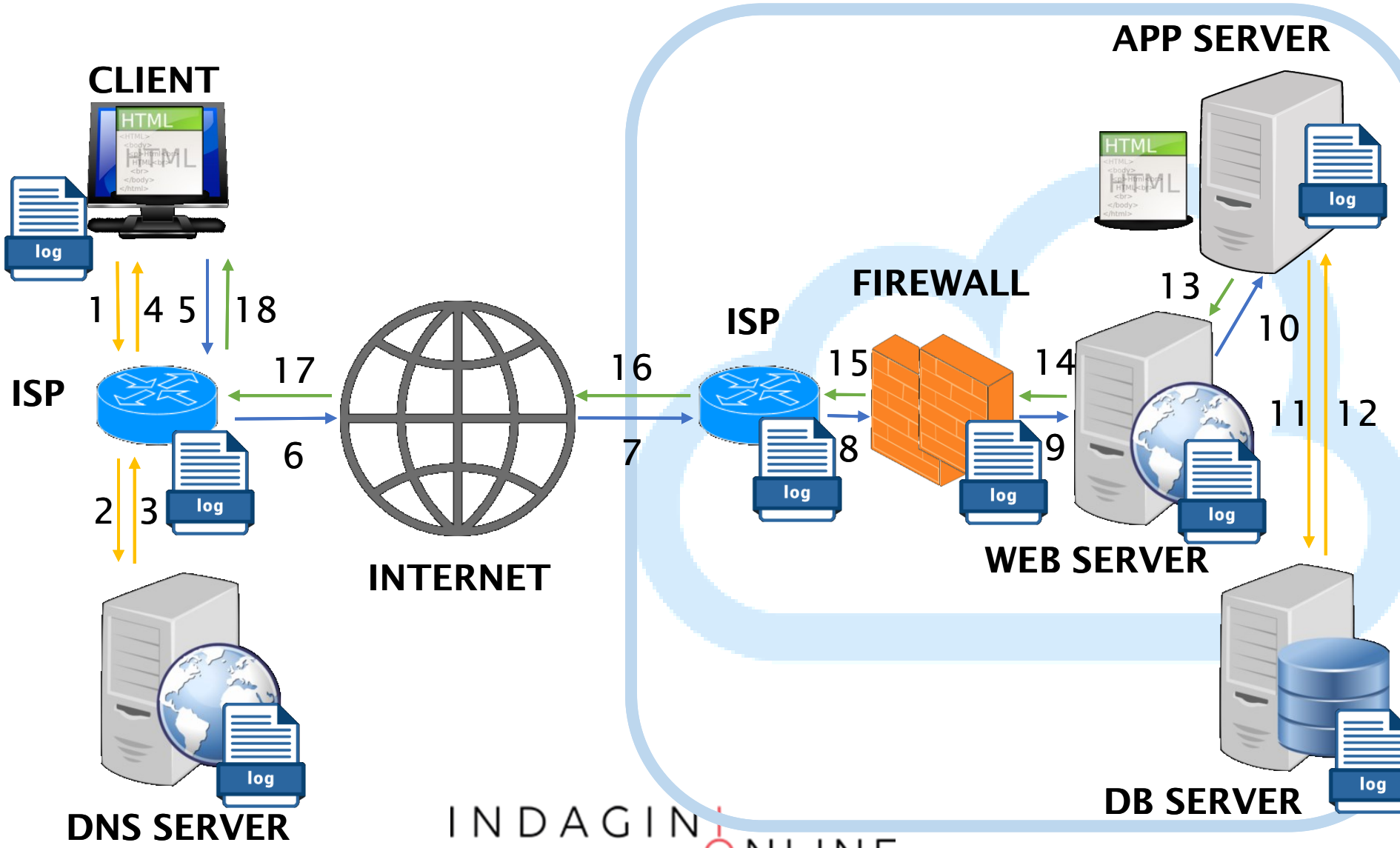
Dopo aver identificato i contenuti è necessario decidere la strategia di acquisizione / sequestro.

Alcune delle opzioni possibili sono le seguenti:

- Realizzare una copia forense presso il service provider
- Chiedere l'estrazione dei dati al service provider
- Sequestrare il contenuto presso il service provider
- Effettuare una copia forense a distanza

Pro e contro

Web architecture



INDAGINI ONLINE

Acquisizione on-premise

La modalità on-premise (in sede) consente di prelevare le evidenze direttamente dalla fonte e può prevedere la raccolta dei seguenti elementi:

- La copia forense della memoria dei servers (**anche parziale**)
- **I logs dei servers** (WEB, APP, DB)
- **I logs del traffico dell'ISP** che ospita i server
- **I logs del traffico dell'ISP** da cui è stata effettuata la connessione
- **I logs dei DNS server**
- **I logs del traffico telefonico** (per risalire all'utenza telefonica)
- **La copia forense del client** da cui è stato eseguito il reato

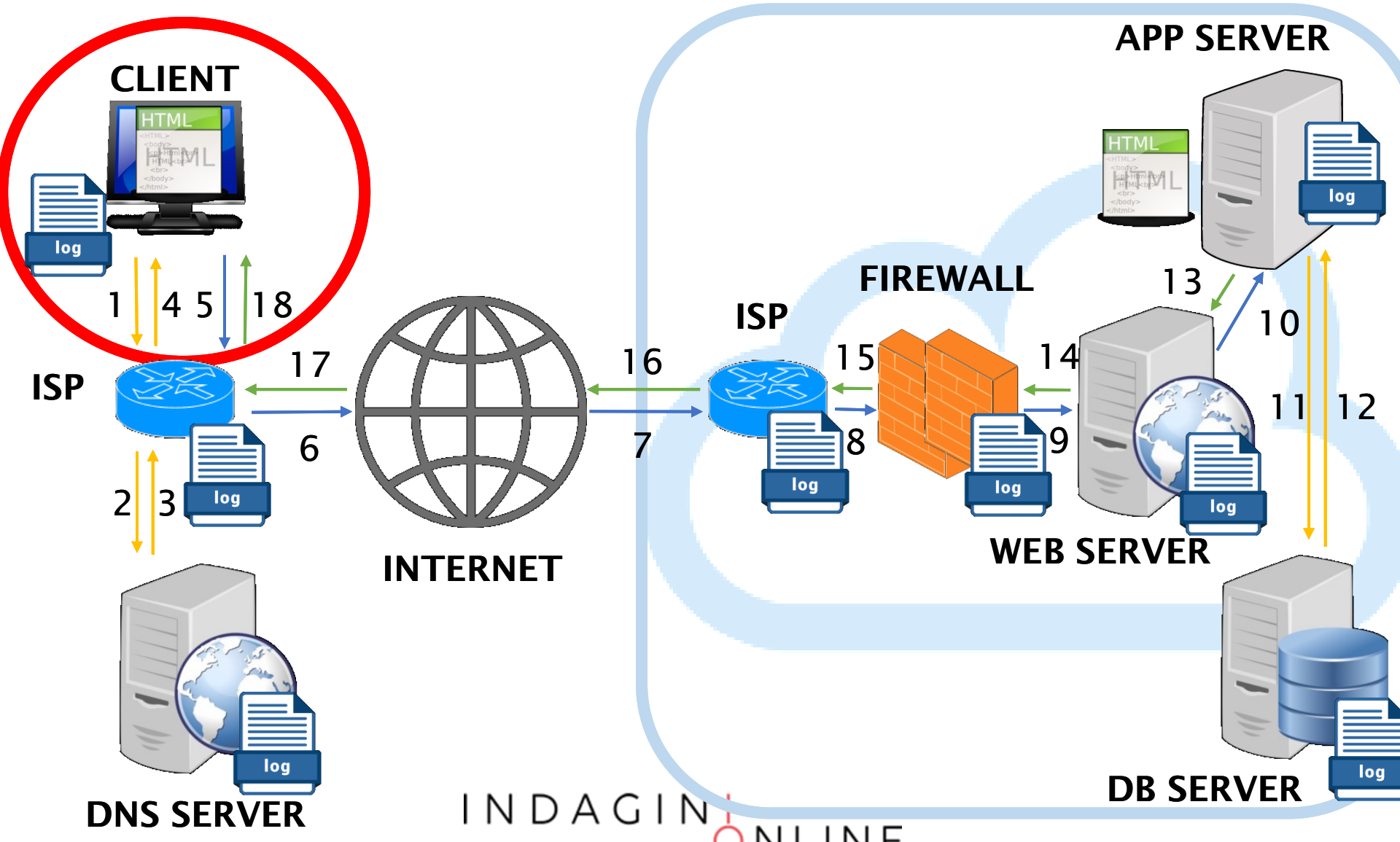
Acquisizione off-premise

È la tecnica utilizzata per realizzare una «preview» del dato e nei casi in cui non è possibile intervenire in presenza sui dispositivi su cui sono memorizzate le evidenze di interesse.

L'acquisizione forense a distanza può essere eseguita quando si verifica uno della seguenti ipotesi:

1. il nodo/server non è agevolmente identificabile e raggiungibile. Si pensi, alle infrastrutture dei grandi Social Media o degli Operatori OTT (Over-the-Top)
2. non siamo nelle condizioni giuridiche per chiedere ad un terzo la copia forense di un dato, anche se è pubblico, perché siamo in una fase di precontenzioso
3. il server si trova in uno stato estero per cui è necessaria una rogatoria internazionale di difficile attuazione
4. il dato d'interesse ha un alto grado di volatilità, si pensi ad un post pubblicato su un portale social, e pertanto si rischia di non trovarlo più disponibile
5. il tempo concesso per svolgere l'indagine non è compatibile con le tempistiche scandite da questa modalità di acquisizione

Web architecture



INDAGINE ONLINE

Prerequisiti

Affinché l'acquisizione a distanza di un contenuto web sia corretta e provi l'esistenza di un dato elemento anche se l'elemento verrà cancellato, ovvero risponda ai requisiti di integrità, autenticità e disponibilità, è necessario garantire le seguenti condizioni:

1. l'operatore ha compiuto le operazioni corrette
2. l'ambiente di acquisizione è idoneo (p.e. VM)
3. la connessione tra il client e il server è affidabile
4. le attività sono riscontrabili all'interno dei logs

Raccolta (Sequestro)

La fase di raccolta (o sequestro) è un'attività posta in essere quando è necessario rimuovere o spostare la fonte di prova dal luogo di origine e, solitamente, viene disposta dall'Autorità Giudiziaria o da chi ne ha competenza.

Nella fattispecie di indagine che stiamo analizzando, ovvero le investigazioni a distanza, questa operazione non può essere realizzata fisicamente, ma, se necessario, può essere portata a termine in uno dei seguenti modi:

- Se la risorsa è pubblica: si ordina all'Internet Service Provider di metterla off-line
- Se la risorsa è protetta: si acquisiscono tutte le credenziali di accesso (dal proprietario o dall'ISP) e si modificano o disabilitano per renderla inaccessibile agli altri

Cosa acquisiamo?

Per rispondere ai predetti prerequisiti è utile acquisire:

1. i comandi eseguiti dall'operatore
2. il log del traffico di rete generato
3. le richieste effettuate al servizio web
4. le risposte ricevute dal servizio web
5. gli oggetti ipertestuali, multimediali o di altro formato digitale ricevuti dal servizio web
6. altre informazioni a latere utili a dimostrare la validità delle informazioni (data e ora certa, id utente)
7. se disponibile, anche i log (o similari) lato server

Come acquisiamo?

L'operatore incaricato di effettuare un'acquisizione di fonti prova online deve preliminarmente effettuare una serie di scelte tra le seguenti opzioni:

1. La modalità di acquisizione:
   automatica o interattiva
2. Il luogo da cui effettuare l'acquisizione:
   hosted o client
3. Gli strumenti e i comandi.

Acquisizione dei contenuti online

Alla luce delle **casistiche** *(pagina web, profilo sociale, mail, ecc.)*, del **contesto** *(evidenza principale o secondaria)* e della **volatilità del dato** possiamo distinguere tre modalità:

1. Acquisizione «***On-the-fly***» o «***Smart***»
2. Acquisizione «***Full***» o «***Rich***»
3. Acquisizione «***Paranoid***»

Gli elementi essenziali ed obbligatori, che rendono giuridicamente valida l'acquisizione, sono i seguenti:

- **Metodologia replicabile e verificabile**
- **Relazione dettagliata delle operazioni eseguite**
- **Firma digitale, con apposizione di una marca temporale, di tutti i contenuti digitali acquisiti**

Acquisizione «*On-the-fly*»

È la modalità più veloce per realizzare un'acquisizione di un contenuto web e può essere attuata anche con qualsiasi browser.

Questa modalità esegue un'istantanea del contenuto web ed è consigliata solo nei casi in cui si teme che l'informazione possa essere alterata o rimossa facilmente dalla rete.

Passi:

- Realizzare una copia attraverso uno dei seguenti servizi online:
  - **https://www.perma.cc (ISO 28500, private, esportabile)** *
  - **https://web.archive.org (ISO 28500, pubblico)** *
  - **https://archive.is (pubblico, non standard)** *
  - **https://conifer.rhizome.org/ (ISO 28500, private, esportabile)** **
  - **PageFrezeer, LegalEye, Hanzo, Cliens Prova Digitale (a pagamento)** **

**** Download non-interattivo*** ***** Download interattivo***

Acquisizione «*On-the-fly*»

Pro

- Velocità di acquisizione per evidenze altamente volatili (news, social network).
- Può essere realizzata con qualsiasi postazione connessa alla Rete Internet.
- L'acquisizione può essere utilizzata come elemento di complemento a quella «Full».
- Se effettuata online, risponde alle caratteristiche di imparzialità in quanto l'acquisizione è effettuata utilizzando servizi terzi.

Contro

- Non contiene tutti gli elementi di un'acquisizione completa (traffico di rete, elementi incorporati, ecc.).
- Deve comunque seguire un'acquisizione completa per estrarre il contenuto acquisito e consegnarlo al committente.
- Il risultato potrebbe risentire della localizzazione del server utilizzati e dello user-agent del browser.

Acquisizione «*Full*»

È la modalità completa perché consente di realizzare l'acquisizione del contenuto web e può essere attuata con più livelli di dettaglio.

Liv. 1: Registrare le uscite audio/video della postazione:

Permette di realizzare un filmato a testimonianza dei comandi e dei programmi adoperati per la realizzazione dell'estrazione.

Programmi utilizzabili:

- **OBS Studio** (obsproject.com free)
- **Icecream Screen Recorder** (icecreamapps.com free/pro)
- **Apowersoft** (apowersoft.it try/pro)

Acquisizione «*Full*»

Liv. 2: Catturare il traffico di rete:

Consente di memorizzare il traffico di rete generato durante l'interrogazione dei contenuti di interesse.

Programmi utilizzabili per catturare il traffico di rete:

- **Wireshark**
- **TCPDump**

Occorre fare attenzione al tipo di protocolli utilizzati e alla presenza della cifratura. In quest'ultimo caso è necessario catturare le chiavi concordate tra il server e il client durante la sessione di navigazione. In presenza di chiavi di cifratura (SSL/TLS) si può attivare la variabile temporanea SSLKEYLOGFILE:

set SSLKEYLOGFILE=%USERPROFILE%\Desktop\keylogfile.txt

Acquisizione «*Full*»

Liv. 3: Catturare il contenuto web:

Consente di memorizzare i contenuti web di interesse.

- Se il contenuto è pubblico o non richiede l'interazione dell'utente si può utilizzare:
  - **Wget (crawler open source) anche in formato *warc***
  - **Browser in formato *mhtml* (IE, Chrome, Firefox, Opera, ecc.) o *warc* (Safari)**

- Se la consultazione del contenuto di interesse richiede l'autenticazione o l'interazione dell'utente è necessario catturare l'intera sessione e si può utilizzare:
  - **Chrome (mhtml) + plugin opzionale (Hunchly)**
  - **Webrecorder (app, ISO 28500)**
  - **OSIRT - Open Source Internet Research Tool (formato proprietario)**
  - **FAW - Forensics Acquisition of Websites (formato html)**

Acquisizione «*Full*»

Passi:

1. **Avviare la capture dell'audio/video**
2. **Avviare la capture del traffico di rete (e delle chiavi SSL/TLS)**
3. **Verificare la sincronizzazione della data e ora**
4. **Controllare configurazione di rete / dns / proxy**
5. **Fare un tracert verso il target**
6. **Utilizzare il browser o il crawler per interrogare il target**
7. **Richiamare e memorizzare tutte le risorse web d'interesse**
8. **Chiudere la capture del traffico di rete**
9. **Chiudere la capture dell'audio/video**
10. **Apporre la Firma digitale con Marca temporale a tutto il materiale scaricato**
11. **Redigere una Relazione dettagliata dell'attività**

Acquisizione «*Full*»

Pro

- È memorizzato tutto il contenuto web scaricato dal client
- È memorizzato tutto il traffico trasmesso tra il client e il servizio web
- Il video aiuta a dimostrare che l'utente non ha manipolato o alterato i contenuti durante la consultazione degli stessi

Contro

- Richiede una postazione forense preconfigurata
- È consigliato effettuare acquisizione anche presso servizi terzi per corroborare la genuinità delle informazioni d'interesse

Acquisizione «*Paranoid*»

Tutti i passi realizzati nella modalità «*Full*» sono eseguii all'interno di una macchina virtuale «pulita» e preconfigurata che diventa anche il contenitore del materiale acquisito.

- Si configura una macchina virtuale (eventualmente in cloud)
- Si installano i programmi necessari al compimento dell'attività
- Si procede all'acquisizione dei contenuti di interesse
- Dopo aver realizzato l'acquisizione, seguendo i passi citati in precedenza, si chiude la macchina virtuale
- Si appone la Firma digitale con Marca temporale alla cartella contenente la macchina virtuale
- Si redige una Relazione dettagliata dell'attività

Acquisizione «*Paranoid*»

Pro

- Alle evidenze precedentemente elencate, aggiungiamo tutto il sistema operativo, i software utilizzati, le configurazione impostate, i logs di sistema e delle applicazioni, la cache del browser, ecc.
  per avvalorare l'integrità del dato acquisito

Contro

- Richiede una postazione forense preconfigurata
- È consigliato effettuare acquisizione anche presso servizi terzi per corroborare la genuinità delle informazioni d'interesse

Carving

L'acquisizione può riguardare anche informazioni cancellate o rimosse. Per tentare di effettuare il recupero di tali informazioni occorre spostare il target di acquisizione:

- Google Cache
  - Cliccando sulla freccia verso il basso dell'URL per visionare la SERP di Google.
  - Utilizzando l'operatore "cache:", seguito dall'URL della pagina desiderata. (p.e. scrivere su Google "cache: www.repubblica.it")
  - Sfruttando i plugin ad-hoc che consentono di visualizzare la cache e la storia di una determinata pagina.
- Wayback Machine
- Controllando i file robot.txt o sitemap.xml

Problematiche

- Sistemi di autenticazione / Area riservate
- Cifratura del traffico (SSL/TLS)
- Ambiente di acquisizione non verificato (*macchina condivisa*)
- Canale di comunicazione non affidabile (*connessione condivisa*)
- Caratteristiche della postazione forense (*s.o., software*)
- Localizzazione della postazione forense (*nazione o regione*)
- Lingua della postazione forense
- Versione del browser utilizzato (*user agent*)
- Contenuti dinamici (*HTML5 o AJAX*)

Soluzioni alternative e/o complementari

Servizi on demand:

- Legaleye (legaleye.cloud)
- Safe Stamper (www.safestamper.com)
- Pagefreezer (www.pagefreezer.com)
- Aleph Archive (aleph-archives.com)
- RAY (ray-webarchiving.com)
- KEN (ken-webarchiving.com)
- HANZO (www.hanzo.co)

Software commerciali:

- Forensics Acquisition Web browser (it.fawproject.com)
- X1 Social Discovery (www.x1.com)
- Oxygen Forensics (www.oxygen-forensic.com)

Analisi

L'attività di analisi può servire ad identificare e recuperare le informazioni d'interesse che, nell'ambito dell'Internet Forensics, possono riguardare le seguenti fattispecie:

1. l'identità e/o l'autenticità dell'identità dell'autore della fonte di prova
2. la datazione della fonte di prova e/o la sua attendibilità
3. l'estrazione dei backup
4. l'estrazione dei metadati e/o di ulteriori informazioni correlate alla fonte di prova
5. la semplice estrazione dei dati
6. la validazione dell'integrità dei dati
7. la verifica di modifiche o manomissioni
8. la comparazione con altre evidenze

Presentazione

Dopo aver completato le fasi tecniche, occorre predisporre una sintesi dell'intero processo tramite l'esposizione, entro i limiti concordati, delle informazioni fattuali ricavate dalle prove e dall'insieme di esami ed analisi che hanno costituito l'indagine. Questo obiettivo si concretizza attraverso la redazione di un elaborato o report da cui sia possibile ricavare:

- l'origine delle fonti di prova digitale,
- la metodologia utilizzata per la gestione delle fonti di prova,
- la tecnologia adoperata per il trattamento delle fonti di prova,
- la procedura eseguita per giungere ai risultati conseguiti,
- i risultati ottenuti (anche sottoforma di allegati multimediali),
- la risposta al quesito.

Presentazione

Un metodo suggerito per la stesura della relazione finale consiste nello sviluppare e strutturare la presentazione seguendo lo stesso ordine delle fasi ISO descritte nei paragrafi precedenti.

La presentazione dei risultati è l'elemento con cui si valuta tutta l'attività svolta. Per cui, durante la stesura, è fortemente consigliato tener conto delle seguenti indicazioni:

- occorre essere semplici e chiari,
- i risultati devono essere esposti in una forma facilmente comprensibile a tutti,
- i destinatari non hanno di solito competenze informatiche,
- molto probabilmente la relazione sarà esaminata da un tecnico della controparte,
- non bisogna essere approssimativi o esprimere giudizi che non siano corroborati dai dati.

Report

Parti essenziali:

- **Premessa**
  - *Curriculum del consulente*
  - **Oggetto dell'Incarico**
  - **Quesiti formulati**
  - *Breve descrizioni dei Fatti*
- **Fasi dell'Attività**
  - *Documenti e/o Evidenze forniti ed analizzati*
  - *Metodologia applicata*
  - **Strumenti (hardware e software) utilizzati**
  - **Descrizione dettagliata delle operazioni eseguite (anche foto e video)**
- **Risultati**
  - **Risposte ai quesiti**
  - **Conclusioni**
  - *Elenco Allegati*

Contatti

vincenzo@calabro.eu

Linkedin vincenzocalabro

INDAGINI ONLINE