INTERNET FORENSICS

Acquisizione Forense di Evidenze in Rete

INDAGINI ONLINE

AGENDA

- Acquisizione a distanza
  - Architettura dei Servizi Internet
  - Tipologie di dati online
  - Identificazione
  - Acquisizione classica e a distanza
  - Acquisizione dei contenuti: «*On-the-fly*», «*Full*», «*Paranoid*»
  - Casi di studio: pagina web, contenuti multimediali, streaming, cloud computing, web app, mail
- Presentazione dei risultati – Reporting
  - Esempio di Report
- Conclusioni – Quesiti

Acquisizione a distanza

Architettura dei Servizi Internet

Ispezione – Perquisizione – Acquisizione

INDAGINI ONLINE

Problema

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 determinati reati quali:

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

Inoltre, 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).

Esempio

Come alterare un contenuto online prima dell'acquisizione

INDAGINI ONLINE

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).

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

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

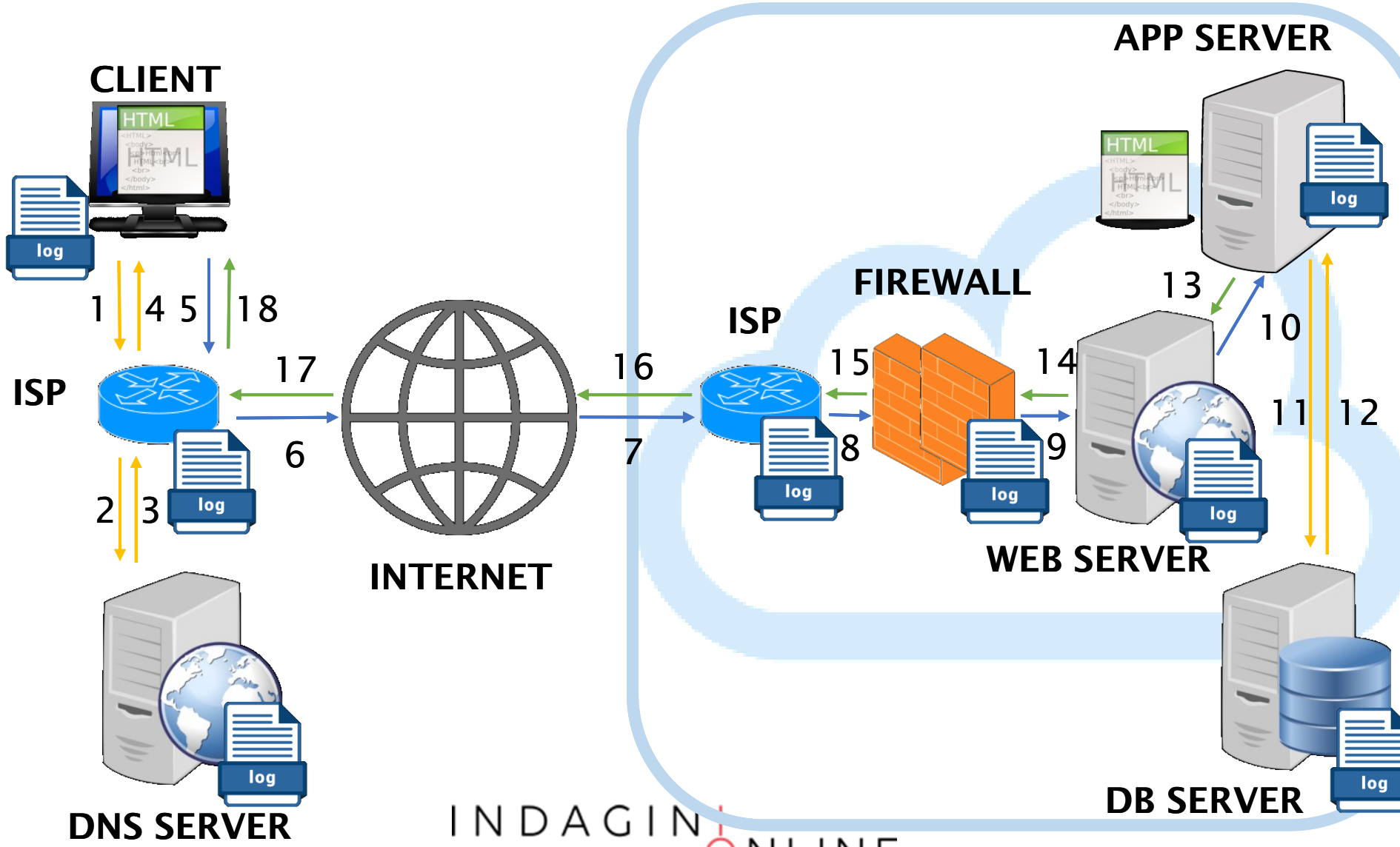
Dopo aver identificato i contenuti è necessario decidere la strategia di acquisizione / sequestro.

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



INDAGIN 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

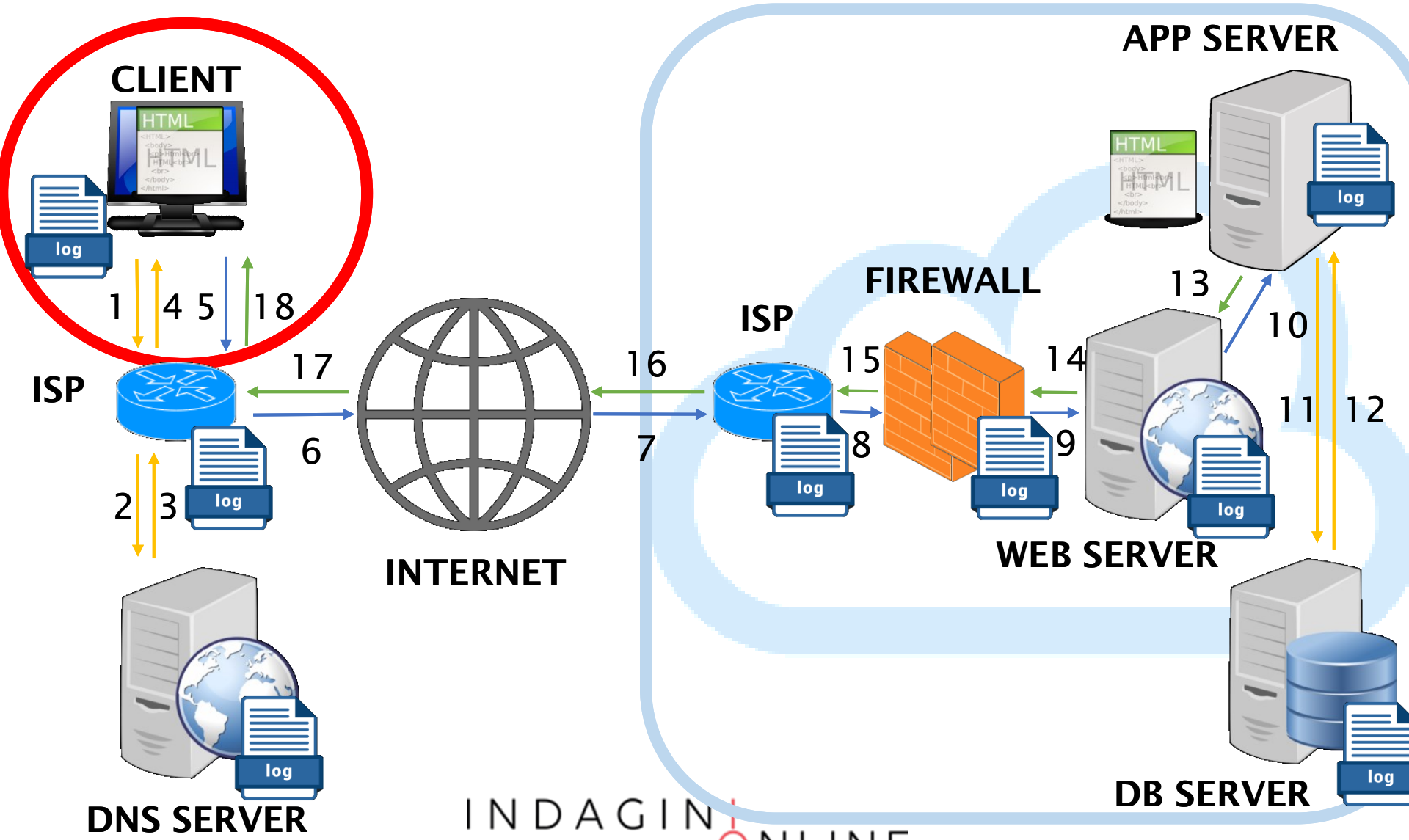
Acquisizione off-premise

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:

- il nodo/server non è agevolmente identificabile e raggiungibile. Si pensi, ad esempio, alle infrastrutture dei grandi Social Media o degli Operatori OTT - Over-The-Top ,
- 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;
- il server si trova in uno stato estero per cui è necessaria una rogatoria internazionale di difficile attuazione;
- 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;
- 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:

- l'operatore ha compiuto le operazioni corrette
- l'ambiente di acquisizione è idoneo (p.e. VM)
- la connessione tra il client e il server è affidabile
- 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:

- I comandi eseguiti dall'operatore
- Il log del traffico di rete generato
- Le richieste effettuate al servizio web
- Le risposte ricevute dal servizio web
- Gli oggetti ipertestuali, multimediali o di altro formato digitale ricevuti dal servizio web
- Altre informazioni a latere utili a dimostrare la validità delle informazioni (data e ora certa, id utente)
- 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.

MIME HTML Format (RFC 2557)

È un formato di archiviazione dei dati pensato per il salvataggio di pagine web e documenti ipertestuali. Consente di riunire in un unico file sia il codice HTML che gli altri elementi richiamati dal documento come ad esempio immagini, file audio, applet Java o animazioni Flash.

MHTML non è attualmente considerato uno standard, per quanto già dal 1999 ne sia stata proposta la standardizzazione (RFC 2557), ma è implementato dai principali browser web.

In particolar modo, i browser Chromium based sfruttano la libreria Blink (Rendering Engine) (https://www.chromium.org/blink).

Web ARChive: ISO28500 File Format

Target Websites and Social Media

WARC ISO 28500 File

```
WARC/1.0
WARC-Type: response
WARC-Record-ID: <urn:uuid:7004e5fd-3f87-f10f-0539-
e116845021fe>
WARC-Date: 2011-11-01T18:12:33Z
WARC-Target-URI: http://news.bbc.co.uk/
WARC-Concurrent-To: <urn:uuid:58c7c6ab-458e-008a-
cda5-41ccda1ce188>
X-Hanzo-Page-Id: <bbc.warc>
X-Hanzo-Page-Uri: http://news.bbc.co.uk
X-Remote-Host: 212.58.246.82:80
X-Hanzo-Record-Id: 875a0395-c82e-46b4-a251-0f910535a344
WARC-IP-Address: 212.58.246.82
Content-Type: application/http;msgtype=response
Content-Length: 939
WARC-Block-Digest:
sha256:1c5006cbd371f39a25f3bbae6ee30c853b60
1bf9bb69579f

HTTP/1.1 301 Moved Permanently
Date: Tue, 01 Nov 2011 18:12:33 GMT
Server: Apache
Set-Cookie: BBC-
UID=44ae0be013563901a7a39e9291faeaa9f756127670a0c1ffd299c6b
4a41f72f60Mozilla%2f5%2e0%20%28Macintosh%3b%20U%3b%20Intel
%20Mac%20OS%20X%2010%5f6%5f5%3b%20de%2dde%29%20AppleWebKit
%2f534%2e15%2b%20%28KHTML%2c%20like
Location: http://www.bbc.co.uk/news/
Cache-Control: max-age=0
Expires: Tue, 01 Nov 2011 18:12:33 GMT
X-Original-Content-Length: 234
Keep-Alive: timeout=5, max=693
X-Original-Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
Content-Length: 234

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://www.bbc.co.uk/
news/">here</a>.</p>
</body></html>
```

Metadata

Hash

Headers

Original Native Format Content

INDAGINI ONLINE

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.

Esempio

Acquisizione in modalità «*on-the-fly*»

INDAGINI ONLINE

Esercizio

Acquisizione di una pagina statica

INDAGINI ONLINE

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. **Sincronizzare la data e l'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

Esempio

Acquisizione in modalità «*Full*»

INDAGINI ONLINE

Esercizio

Acquisizione dei contenuti da un social network

INDAGINI ONLINE

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

Esempio

Acquisizione in modalità «*Paranoid*»

INDAGINI ONLINE

Download contenuti multimediali

Nel caso in cui è necessario acquisire separatamente file digitali presenti sul web oppure tramite altre applicazioni web come:

Documento	**Immagine**	**File compresso**
Foglio di calcolo	**Foto**	**Programma**
Presentazione	**Video**	**File generico**

È utile:

- Acquisire la pagina di origine
- Documentare l'Url dell'evidenza e il protocollo di trasmissione
- Effettuare il download del file

Se il contenuto da acquisire è raggiungibile solo attraverso una determinata applicazione, diversa da un browser, occorre utilizzare la stessa applicazione, effettuando degli screenshot e documentare il protocollo di trasmissione.

Esempio

Acquisizione di contenuti multimediali

INDAGINI ONLINE

Streaming dei contenuti multimediali

Se il contenuto da acquisire è disponibile in formato streaming (Youtube, Facebook Video, Instagram Video, ecc.)

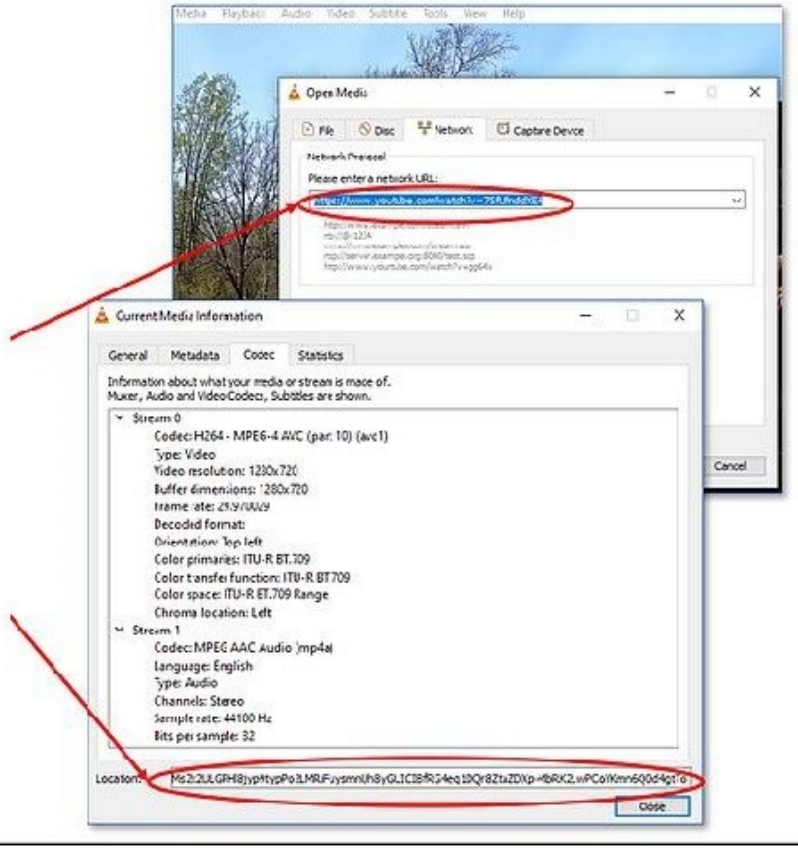
È necessario:

- Acquisire la pagine di origine
- Identificare l'Url dello streaming e scaricare il conternuto
- Utilizzare un servizio di recupero e download online:
  https://pastedownload.com (all platform)
  https://www.getfvid.com (Facebook)
  https://instadownloader.co (Instagram)
- Oppure Scaricare il contenuto con un software ad hoc:
  «Youtube downloader HD»
- In alternativa, effettuare la registrazione con il «video recorder» e documentare l'Url o la pagine web da cui è stato ricavato.

Streaming dei contenuti multimediali da Youtube

Come catturare un video da YOUTUBE

1. Selezionare l'URL della pagina Youtube che ospita il Video,
2. Aprire "VLC media player" e selezionare [Media > Apri flusso di rete],
3. Incollare l'URL nel campo [Inserisci un URL di rete:] e premere [Riproduci],
4. Durante la riproduzione, selezionare la voce [Menu Strumenti > Informazioni codificatore] e copiare l'URL visibile nel campo [Posizione],
5. Aprire l'URL copiato in una nuova scheda del browser Chrome,
6. Premere il tasto destro del mouse sul video e selezionare [Salva Video come…] per memorizzarlo nella Directory predefinita.

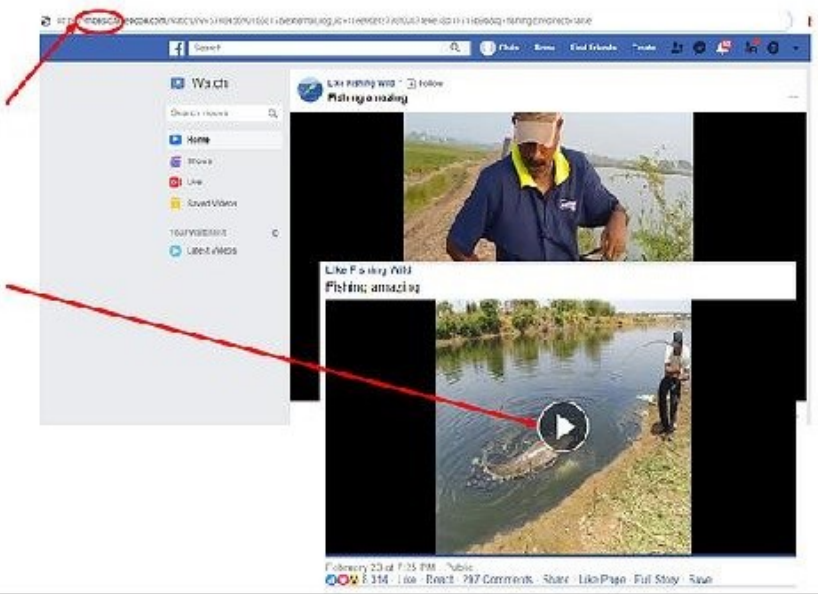


INDAGINI ONLINE

Streaming dei contenuti multimediali da Facebook

Come catturare un video da FACEBOOK

1. Individuare l'URL della pagina Facebook che ospita il Video,
2. Sostituire il prefisso "www" con "mbasic" nella URL del Video;
3. Aprire il nuovo URL, premere il testo del mouse sul video di interesse e selezionare [Apri link in un'altra scheda],
4. Nella nuova scheda premere il tasto destro del mouse sul video e selezionare la voce [Salva Video come…] per memorizzarlo nella Directory predefinita.

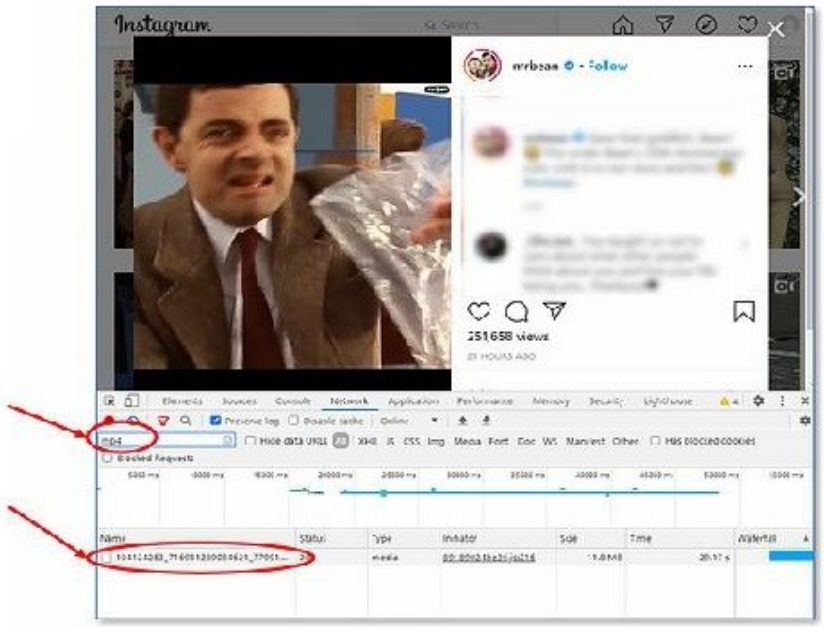


INDAGINI ONLINE

Streaming dei contenuti multimediali

Come catturare un video da INSTAGRAM, TWITTER, TIKTOK, SNAPCHAT e altri.

1. Aprire l'URL che ospita il Video Instagram,
2. Aprire gli [Strumenti per sviluppatore] (CTRL+SHIFT+I):
3. Andare nella [Network tab]
4. Inserire nel campo Filter "mp4"
5. Individuare il video di interesse
6. Fare doppio click sulla stringa nella colonna "Name"
7. premere il tasto destro del mouse sul video e selezionare la voce [Salva Video come…] per memorizzarlo nella Directory predefinita.



INDAGINI ONLINE

Esempio

Acquisizione di contenuti in streaming

INDAGINI ONLINE

Esercizio

Acquisizione di un contenuto in streaming

INDAGINI ONLINE

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

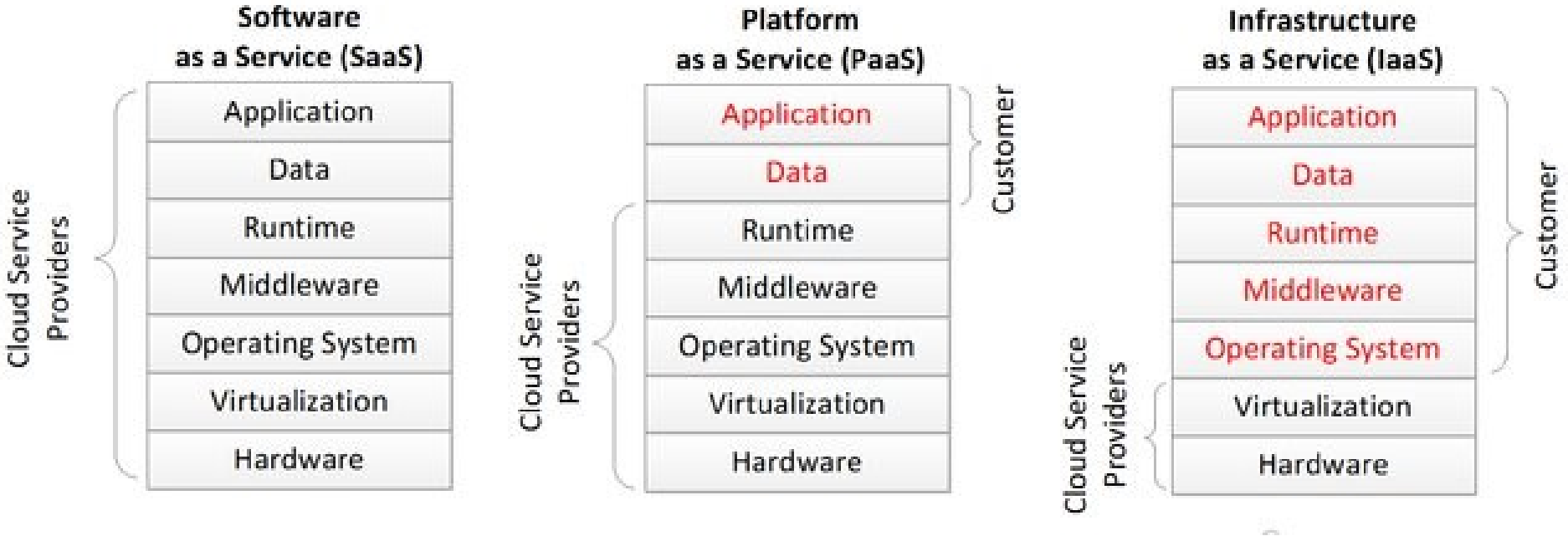
Esempio

Acquisizione di contenuti dalla cache

INDAGINI ONLINE

Cloud computing forensics

- Prima di acquisire le informazioni dal Cloud computing dobbiamo capire che tipologia di servizio stiamo analizzando poiché cambia l'oggetto su cui concentrare l'attività



INDAGINI ONLINE

Cloud computing: **SaaS**

Nell'ipotesi in cui si tratti il Cloud Service è configurato come Software as a Service (Web server, portale, ecc.) si procede come una qualsiasi acquisizione web:

- Procurarsi le credenziali di accesso all'area riservata
- Acquisire le pagine web interrogate, sia lato pubblico che privato, per visualizzare il contenuto oggetto di interesse
- Documentare, anche attraverso altra acquisizione, lo stato di configurazione e il registro degli eventi (se presente)
- Scaricare il contenuto e il backup dei dati (se disponibile)
- Se necessario, modificare la password di accesso per evitare manipolazione o cancellazioni

Cloud computing: **PaaS**

Nell'ipotesi in cui si tratti il Cloud Service è configurato come Platform as a Service (cloud storage, ecc.) e non abbiamo alcuna applicazione preconfigurata per accedervi direttamente dalla postazione è necessario:

- Acquisire le credenziali di accesso allo spazio virtuale
- Acquisire le pagine web interrogate per visualizzare il contenuto oggetto di interesse (sia lato pubblico che privato)
- Documentare, anche attraverso altra acquisizione, lo stato di configurazione e il registro degli eventi (se presente)
- Scaricare il contenuto o il backup (se disponibile)
- Se necessario, modificare la password di accesso per evitare manipolazione o cancellazioni

Cloud computing: **IaaS**

Nell'ipotesi in cui si tratti il Cloud Service è configurato come Infrastructure as a Service (Macchina virtuale, ecc.) e non abbiamo alcuna applicazione preconfigurata per accedervi direttamente dalla postazione è necessario:

- Acquisire le credenziali di accesso allo spazio virtuale
- Acquisire le pagine web interrogate per visualizzare l'interfaccia di amministrazione (sia lato pubblico che privato)
- Documentare, anche attraverso altra acquisizione, lo stato di configurazione e il registro degli eventi (se presente)
- Scaricare la macchina virtuale e farne una copia
- Se necessario, modificare la password di accesso per evitare manipolazione o cancellazioni

Esempio

Acquisizione di contenuti su cloud storage

INDAGINI ONLINE

App forensics

Le app presenti su device fissi o mobile memorizzano alcuni dati sulla memoria interna ed altre sul web.

Inoltre, spesso, le informazioni visionabili consultando il sito web riconducibile alla stessa app sono diverse da quelle mostrate sul device.

Pertanto, al fine di raccogliere più informazioni possibili, è necessario effettuare più acquisizioni:

- Effettuare una copia forense del device o della cartella che contiene l'app
- Acquisire gli screenshot delle videate significative dell'app
- (se presente) acquisire le stesse informazioni sul sito web afferente l'applicazione mobile

Esempio

Acquisizione di contenuti visibili dalla web app

INDAGINI ONLINE

Email forensics

Una casella di posta elettronica (ordinaria o pec) può essere consultata attraverso due modalità:

1. Portale «Webmail» (preferibile per acquisizioni di singole mail)
2. Client di posta elettronica (indicato per scaricare tutta la casella)

In entrambi casi, è necessario procurarsi gli indirizzi della casella, dei server e le credenziali di accesso.

Prima di procedere con l'acquisizione è utile conoscere i protocolli abilitati e i relativi port per l'accesso tramite client:

- Post Office Protocol version 3 (**POP3** / **POP3s**)
- Internet Message Access Protocol (**IMAP** / **IMAPs**)
- Simple Mail Transfer Protocol (**SMTP** / **SMTPs**)

Email forensics

Acquisizione tramite interfaccia web:

- Si accede con le credenziali fornite
- Si documenta la configurazione della casella, le impostazioni di ripristino, il log degli accessi (se presente) e lo stato delle cartelle visibili (Inbox, Sent, Draft, Trash, ecc.)
- Si acquisisce la pagine web che riporta l'elenco dei messaggi di interesse
- Si apre e si scarica il messaggio nel formato standard MIME RFC 5322 **(eml o msg) perché è quello che contiene anche gli header utili per l'analisi della mail**
- Se necessario, si modifica la password di accesso per bloccare l'accesso

Email forensics

Acquisizione tramite client di posta elettronica:

- Dopo aver appreso:
  - le credenziali di accesso (se necessario si modifica la password)
  - l'indirizzo del server di posta in entrata
  - i protocolli abilitati e i parametri necessari
- Si configura il client di posta elettronica per trasferire tutti i messaggi presenti nella casella lasciando sul server la copia originale
- Se possibile, utilizzare il protocollo IMAP perché riproduce la stessa struttura delle cartelle visibile tramite interfaccia web
- L'acquisizione tramite client consente di effettuare un analisi approfondita per verificare eventuali anomalie o manomissione dei messaggi

Esempio

Acquisizione mail da web e da client

INDAGINI ONLINE

Esercizio

Acquisizione di una mail dal web

INDAGINI ONLINE

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*)

Esempio

Decrittazione traffico SSL / TSL

INDAGINI ONLINE

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)

Esempio

Acquisizione attraverso soluzioni commerciali

INDAGINI ONLINE

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 dei risultati

Come creare un Report

Firma digitale e Marca temporale

INDAGINI ONLINE

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

Tipologia: La Perizia e la Consulenza tecnica

La perizia e la consulenza tecnica sono i due mezzi di prova attraverso i quali fa ingresso nel processo penale il sapere tecnico, scientifico e artistico.

Entrambe si sostanziano, alternativamente o cumulativamente, nello svolgimento di indagini, nell'acquisizione di dati o nell'effettuazione di valutazioni che richiedono per la loro natura particolari competenze tecniche, scientifiche o artistiche.

La perizia (artt. 220 e ss.c.p.p.) costituisce mezzo di prova "neutro" (essendone affidato l'espletamento ad un soggetto terzo, quindi imparziale, nominato dal giudice) ed essenzialmente discrezionale (essendo rimessa al giudice la valutazione sul requisito della sua "occorrenza"). Oltre che a richiesta di parte, può essere disposta anche d'ufficio.

La consulenza tecnica, invece, può esperirsi: nell'ambito di una perizia già disposta, concedendo alle parti facoltà di nominare propri consulenti che possono partecipare alle operazioni peritali al fine di realizzare il contraddittorio nella formazione della prova (art. 225 c.p.p.).

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*

Esempio

Report di acquisizione

INDAGINI ONLINE

Firma digitale

La firma che consente di scambiare in rete documenti con piena validità legale.

CAD Art. 24. Firma digitale

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

Marca temporale

La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 CAD)

Il servizio di Marcatura Temporale può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida.

Sui documenti informatici sui quali è stata apposta una Firma Digitale, **la Marca Temporale attesta il preciso momento in cui il documento è stato creato, trasmesso o archiviato**.

Esempio

Firma e marca temporale

INDAGINI ONLINE

Esercizio

Redazione di un report

INDAGINI ONLINE

Conclusioni

Note giuridiche

Quesiti

INDAGINI ONLINE

Quadro normativo: ispezioni

La **Legge 48 del 18/3/20018** *«Ratifica ed esecuzione della Convenzione del Consiglio d´Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell´ordinamento interno»* ha introdotto alcune novità nel codice di procedura penale:

Art. 244 c.p.p. Ispezioni - Casi e forme delle ispezioni

1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.

2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. **L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**.

Modus operandi: ispezione

È un mezzo di ricerca della prova disposto quando occorre accertare le tracce e gli altri effetti materiali del reato, ovvero descrivere lo stato dei luoghi.

Se dovessimo realizzare **un'ispezione** ci limiteremo ad un'osservazione del sistema attraverso la descrizione del suo status, anche con l'ausilio di immagini, e l'annotazione della eventuale presenza di software attivi, nonché periferiche e connessioni, con la conseguenza che all'attività di osservazione, **descritta nel verbale contestualmente redatto, non può seguire quindi alcuna forma di apprensione delle informazioni** eventualmente individuate all'interno del sistema: l'ispezione del sistema, infatti, rappresenta un'attività preliminare rispetto al contesto dell'indagine informatica, usualmente deputata all'estrazione di dati digitali, pur nelle forme della legal imaging generalmente condivisa.

Quadro normativo: perquisizione

Art. 247 c.p.p. Perquisizioni - Casi e forme delle perquisizioni

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

2. La perquisizione è disposta con decreto motivato.

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

Modus operandi: perquisizione

La perquisizione è un Mezzo di ricerca della prova adottato nel processo penale qualora si ritenga che determinate cose pertinenti al reato afferiscano o si occultino.

Pertanto, assumono rilevanza **le modalità di perquisizione dell'elaboratore elettronico**, dettate dal comma 1-bis dell'art. 247 c.p.p., cui fa da pendant l'art. 352, comma 1-bis, c.p.p.

In tale ipotesi, oltre a redigere un dettagliato verbale, l'operatore dovrà acquisire le informazioni d'interesse «adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

Modus operandi: consigli

Valutare il rispetto della tutela dei diritti (privacy, proprietà intellettuale, immagine, minori, ecc.)

In caso di informazioni accessibili attraverso aree riservate: farsi autorizzare e consegnare le credenziali in maniera formale

In considerazione dell'elevato grado di modificabilità dei contenuti web e della predisposizione all'anonimato che contraddistingue gli utenti in rete, è sempre consigliato acquisire:

- Le informazioni a latere per rendere un'indagine più robusta
- I log file dai service provider per corroborare le attività online

Contatti

info@vincenzocalabro.it

Linkedin vincenzocalabro

INDAGINI ONLINE