

Acquisizione e trattamento dati informatici in Rete (social, web, email)



Prof. Sebastiano Battiato

A.A. 2023/2024

Corso di Laurea in Informatica
Università di Catania
Dipartimento di Matematica e Informatica



1

Diffamazione in Rete

La sempre maggiore diffusione di **mezzi di comunicazione** di massa, tra cui anche quelli telematici, pongono il problema della **individuazione** del ruolo dell'informazione e dei limiti di liceità della stessa, ove potenzialmente lesive della altrui reputazione.



Digital Forensics



2

Diffamazione in Rete

A differenza di quanto avviene per i media tradizionali, in Rete le notizie ed i commenti **non sono**, di norma, frutto dell'attività di professionisti e non sono soggetti ad un **regime di controlli professionali interni**.

Ciò spesso si traduce anche in una minore autorevolezza e credibilità dei contenuti esposti.



Digital Forensics



3



Diffamazione in Rete

I **social network** sono diventati l'ambiente virtuale dove ogni giorno milioni di persone interagiscono con gli altri, scambiandosi **opinioni**, **foto**, **commenti** e **informazioni**.

L'azione più semplice di tutte, cioè l'esprimere un proprio pensiero o una propria opinione, racchiude però **insidie** e **conseguenze**, anche di natura penale, che a volte vengono ignorate.



Buon senso e la padronanza intrinseca del mezzo di comunicazione potrebbero aiutare



Digital Forensics



4

Diffamazione

L'art. 595 comma terzo cod. pen. punisce ogni **“offesa recata col mezzo della stampa o qualsiasi altro mezzo di pubblicità...”**; rientrano, quindi, nella previsione della norma anche altre forme di offesa come quelle realizzate attraverso Internet o altri mezzi di comunicazione.

La pena è della reclusione da **sei mesi a tre anni** o della multa non inferiore a **cinquecentosedici euro**

La giurisprudenza ha costruito tre fondamentali ipotesi di limiti a tutela della persona umana:

- **il limite dell'onore, della riservatezza, dell'identità personale**

Accanto a questi è il **limite della reputazione.**



Digital Forensics



5

Requisiti del Reato di Diffamazione

Assenza dell'offeso (se è presente sussisterà il reato di ingiuria)

Offesa all'altrui reputazione.

La persona diffamata non deve essere necessariamente indicata nominativamente ma tuttavia **deve essere individuabile** agevolmente e con certezza. In sostanza è sufficiente che l'offeso possa essere individuato per esclusione, o in via deduttiva.

Comunicazione a più persone.

Non sussiste quindi il reato di diffamazione nella lesione della reputazione comunicata ad una persona solamente, pur potendo essere ciò sufficiente per richiedere il risarcimento del danno in via civile. Con riguardo alla diffamazione a mezzo Internet la sussistenza della comunicazione a più persone si presume nel momento stesso in cui il messaggio offensivo viene inserito su un sito Internet che, per sua natura, è destinato ad essere visitato da un numero indeterminato di persone in breve tempo.



Digital Forensics



6

Diffamazione in Rete

La diffamazione via web o tramite piattaforma social è diventata ormai una pratica diffusa

Sindrome dell'abitacolo

Cosa fare in caso di diffamazione via Facebook, ma anche su siti web, forum o social network come Twitter, LinkedIn, Google Plus o chat di gruppo su Facebook Messenger?.



Digital Forensics



7

Diffamazione in Rete

La diffamazione a mezzo Facebook, in particolare con riferimento a post diffamatori, può verificarsi in **due generali ipotesi**:

- a) La prima è quella della **pubblicazione su pagine personali**, alle quali, per accedere, è necessario il consenso del titolare, ove si deve ritenere la comunicazione non potenzialmente diffusiva e pubblica, in quanto, attraverso Facebook si attua una conversazione virtuale privata con destinatari selezionati che hanno chiesto previamente al presunto offensore di poter accedere ai contenuti delle pagine dallo stesso gestite;



Digital Forensics



8

Diffamazione in Rete

- b) La seconda è caratterizzata dalla **pubblicazione di post, commenti** o **quant'altro** su pagine nelle quali l'utente non sceglie direttamente i propri interlocutori.



Digital Forensics



9



Diffamazione in Rete

Presupposti per la **diffamazione a mezzo Facebook** sono:

- la precisa individualità del destinatario delle manifestazioni ingiuriose;
- la comunicazione con più persone alla luce del carattere pubblico dello spazio virtuale e la possibile sua incontrollata diffusione;
- la coscienza e volontà di usare espressioni oggettivamente idonee a recare offesa al decoro, onore e reputazione del soggetto passivo.



Digital Forensics



10



Diffamazione in Rete

La **Cassazione** ha espressamente riconosciuto la possibilità che il reato di diffamazione possa essere commesso a mezzo internet, configurando la propagazione tramite **Facebook** un'ipotesi che integra quale aggravata quella di cui al terzo comma del menzionato articolo.

Il legislatore si è interessato, pertanto, ad un'analisi della condotta protesa a postare un commento offensivo sulla bacheca, in rapporto alla pubblicazione e alla diffusione di essa, e cioè volta a comunicare con terzi quale gruppo di persone apprezzabile dal punto di vista numerico (Cassazione penale, sez. I, 28/04/2015, n. 24431).



11



Digital Forensics



Diffamazione in Rete

La certificazione di una presunta diffamazione via Facebook, su siti web o social network deve necessariamente includere la **fase di acquisizione delle prove informatiche, certificazione dell'integrità** dei dati raccolti oltre che la **stesura di una relazione tecnica** che possa diventare Consulenza Tecnica di Parte da allegare a eventuale denuncia/querela per diffamazione.



Digital Forensics



12



Diffamazione in Rete

Una raccolta delle prove di diffamazione non corretta può :

- evitare al diffamatore di essere **identificato**
- permettere al diffamatore di **cancellare le prove** prima che si arrivi in fase di giudizio
- consentire al diffamatore di attribuire ad altri l'azione di diffamazione (ad esempio sostenendo la tesi del **furto dell'account**)



13

Diffamazione in Rete

La diffamazione e l'offesa che avviene su in Rete (anche in gruppi chiusi) è punibile a seguito di **querela** della parte offesa che diventa più efficace se riporta anche una Consulenza tecnica circa l'avvenuta diffamazione e **l'acquisizione forense e certificata del contenuto diffamatorio** che si contesta, che diventerà poi prova nel processo penale o civile in Tribunale.

Prove che potrebbero anche scomparire prima di avere il tempo di sporgere querela, rischiando quindi che le evidenze digitali della diffamazione scompaiano e sia poi decisamente più complesso ottenerle, se non tramite **Rogatoria Internazionale** (MLAT) in genere utilizzata in casi di rilevanza penale maggiore rispetto alla diffamazione, seppur a mezzo Stampa o a mezzo Internet e Facebook.



14

Diffamazione in Rete

La perizia/consulenza finalizzata a **documentare** tramite **prove informatiche** la diffamazione e l'offesa o l'ingiuria avvenuta in Rete può essere estesa tramite indagini e ricerche OSINT alla **ricerca** e **acquisizione** dei dati relativi ai proprietari o agli utilizzatori dei profili, gruppi o pagine Facebook su cui vengono pubblicati i messaggi diffamatori.

Spesso i profili utilizzati per la diffamazione su Facebook o in generale a mezzo Internet, ma anche le **pagine** o talvolta i **gruppi**, **vengono chiusi** dopo aver commesso il reato proprio per rendere più complesse le indagini. Lo stesso tipo di cristallizzazione della prova e analisi forense e investigativa è fattibile tecnicamente anche in caso di diffamazione su canali diversi, sempre a mezzo Internet, come diffamazione su siti web, portali, forum, gruppi di discussione, post di blog, commenti a blog, tweet su Twitter, post e pagine su LinkedIn o Instagram.



15

Acquisizione (artigianale)



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

Le stampe o screenshot difficilmente vengono ammesse in Tribunale come prova perché non godono dell'**integrità** delle prove informatiche raccolte con strumentazione adeguata e metodi scientifici.

Anche la fotografia dello schermo del PC non ha pienamente valore legale o meglio, può facilmente essere contestata dalla controparte, poiché per quanto possa avere una storicità temporale (i cellulari si sincronizzano automaticamente con l'ora esatta e salvano le immagini in modo incrementale) ritrae qualcosa che può facilmente essere **artefatto** (lo schermo).



16

Acquisizione (2): Notaio

La stampa del profilo Facebook **certificata da un Notaio** o da un **Pubblico Ufficiale** è certamente un'alternativa migliore ma può non essere sufficiente a identificare il proprietario del profilo o della pagina utilizzata per la diffamazione, poiché 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.

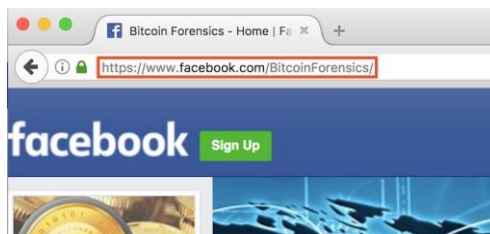


Digital Forensics



17

Facebook: Identificazione del profilo



Per quanto sia importante, non è sufficiente prendere nota del **nome del profilo** o della **pagina**, neanche copiando la URL, cioè l'indirizzo che compare nella barra degli indirizzi del browser

Per poter eseguire una consulenza Informatica su un profilo, pagina o gruppo Facebook è necessario, in realtà, identificare il codice **ID** che lo **identifica univocamente**.

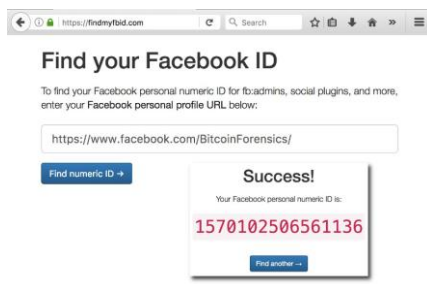
Il nome del profilo infatti può essere modificato dal proprietario, così come l'indirizzo che compare nella barra delle URL del browser.



Digital Forensics



18



Per individuare il codice **ID** del profilo o della pagina da cui proviene la diffamazione, è possibile utilizzare un sito come **Find My FB ID** (findmyfbid.com), incollando l'indirizzo del profilo o della pagina nel campo di testo e premendo il pulsante "Find numeric ID".

Si otterrà un numero da ricopiare o stampare, per "**congelare**" l'identificativo univoco che permetterà di ritrovare il profilo o pagina anche in caso di cambio nome o URL e all'Autorità Giudiziaria di richiedere a Facebook eventuali file di log o contenuti diffamatori.

La raccolta delle prove per uso legale in caso di diffamazione su Facebook, partendo dal codice ID del profilo o della pagina, è molto più efficace.



Digital Forensics



19

Facebook: Come trovare il riferimento univoco del post o del commento diffamatorio?

Identificato l'User **ID** del proprietario del profilo da cui è avvenuta la diffamazione o il Page ID della pagina che contiene il testo diffamatorio, si deve "**congelare**" anche il post o il commento stesso per utilizzarlo poi come prova informatica della diffamazione.

La **data del post** incriminato contiene un link all'indirizzo o URL che identifica il post stesso, che si aprirà nel browser.



Digital Forensics



20

Facebook: Come trovare il riferimento univoco del post o del commento diffamatorio?

Esempio:

www.facebook.com/nome.profilo/posts/10213357451991856

Per identificare un commento specifico per “congelarlo” come prova di una diffamazione, così da poter poi redigere una consulenza tecnica che ne documenti in modo oggettivo il contenuto, andrà fatta una cosa simile, cliccando però questa volta sulla data e ora sotto il commento stesso, dopo il link “Mi Piace”.



Digital Forensics

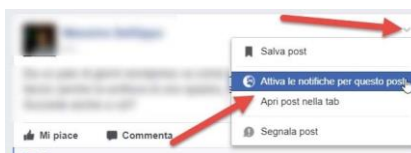


21

Notifiche sui post diffamatori

Per attivare le notifiche su un post diffamatorio di Facebook, cliccare sulla freccia con punta in basso posizionata in alto a destra nel post e poi sulla voce di menù “Attiva le notifiche per questo post”. Si riceveranno così email a ogni nuovo commento al post, che potranno essere utilizzate dal perito informatico per certificare o rintracciare i commenti anche nel caso in cui – come spesso accade – dovessero essere rimossi poco dopo la pubblicazione.

Ovviamente le email devono essere mantenute nella casella di posta e non cancellate, così da permettere successivamente una analisi sulla posta elettronica che ne certifichi l'originalità e la presenza sul server per un utilizzo in Tribunale.



22

OSINT

- La Open Source INTelligence, acronimo **OSINT** (in italiano: "Intelligence delle fonti libere"), è l'attività di raccolta d'informazioni mediante la consultazione di fonti di pubblico accesso.
- L'OSINT si distingue dalla ricerca perché applica un processo di gestione delle informazioni con lo scopo di creare una specifica conoscenza in supporto di una specifica decisione di un individuo o gruppo.



Digital Forensics



23

OSINT (2): fonti

- **Mezzi di comunicazione:** giornali, riviste, televisione, radio e siti web.
- **Dati pubblici:** rapporti dei governi, piani finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi, avvisi aeronautici e marittimi.
- **Osservazioni dirette:** fotografie di piloti amatoriali, ascolto di conversazioni radio e osservazione di fotografie satellitari. La diffusione di fotografie satellitari, spesso in alta risoluzione, sulla rete (ad esempio Google Earth) ha esteso la possibilità di Open source intelligence anche per aree che prima erano disponibili solo alle maggiori agenzie di spionaggio.
- **Professionisti e studiosi:** conferenze, simposi, lezioni universitarie, associazioni professionali e pubblicazioni scientifiche

La maggior parte delle informazioni sono georeferenziate. Non tutti i dati open source sono testo senza struttura. Alcuni esempi di open source georeferenziati spaziali sono: copie materiali o digitali di mappe, atlanti, repertori geografici, progetti di porto, dati gravitazionali, aeronautici, nautici, geodetici, geo-antropici, ambientali, di iconografia commerciale, lidar, iper- e multi-spettrali, foto aeree, di web services di mash-up, di database.



Digital Forensics



24

OSINT e Facebook

- Anche sulle piattaforme Social è possibile ricavare informazioni senza per forza far riferimento a software del settore.
- Facebook è una di quelle piattaforme che meglio si prestaVA alla raccolta d'informazioni.



Digital Forensics



25

Manipolazione URL (valide fino al 7/6/2019)

- Queste tecniche permettono di scoprire informazioni su persone, gusti, mi piace, recensioni, luoghi visitati e tutte quelle informazioni che non sono reperibili dal profilo dell'utente stesso.
- Il primo passo è quello di cercare il codice numerico dell'utente Facebook, per poterlo poi inserire in specifiche posizioni di una URL.
- Le URL che utilizzeremo sono così composte:
URL statica
ID Utente
Termine di ricerca

| URL statica | ID utente | Variabile di ricerca |
<https://www.facebook.com/search/000000/photos-liked>



Digital Forensics



26

Esempi (valide fino al 7/6/2019)

- **Places Visited / Luoghi visitati**
[https://facebook.com/search/\[User ID\]/places-visited](https://facebook.com/search/[User ID]/places-visited)
- **Recent Places Visited / Luoghi visitati di recente**
[https://facebook.com/search/\[User ID\]/recent-places-visited](https://facebook.com/search/[User ID]/recent-places-visited)
- **Places Checked/In / Luoghi in cui ci si è registrati**
[https://facebook.com/search/\[User ID\]/places-checked-in](https://facebook.com/search/[User ID]/places-checked-in)
- **Places Liked / “Mi Piace” ai luoghi**
[https://facebook.com/search/\[User ID\]/places-liked](https://facebook.com/search/[User ID]/places-liked)
- **Pages Liked / “Mi Piace” alle pagine**
[https://facebook.com/search/\[User ID\]/pages-liked](https://facebook.com/search/[User ID]/pages-liked)
- **Photos By User / Foto dell'utente**
[https://facebook.com/search/\[User ID\]/photos-by](https://facebook.com/search/[User ID]/photos-by)
- **Photos Liked / “Mi Piace” alle foto**
[https://facebook.com/search/\[User ID\]/photos-liked](https://facebook.com/search/[User ID]/photos-liked)



Digital Forensics



27

Esempi (valide fino al 7/6/2019)

- **Photos Of /Tagged / Foto in cui l'utente è stato taggato**
[https://facebook.com/search/\[User ID\]/photos-of](https://facebook.com/search/[User ID]/photos-of)
- **Photos Comments / Commenti alle foto**
[https://facebook.com/search/\[User ID\]/photos-commented](https://facebook.com/search/[User ID]/photos-commented)
- **Photos Interacted / Interazioni con foto**
[https://facebook.com/search/\[User ID\]/photos-interacted](https://facebook.com/search/[User ID]/photos-interacted)
- **Photos Interested / Foto di interessi**
[https://facebook.com/search/\[User ID\]/photos-interested](https://facebook.com/search/[User ID]/photos-interested)
- **Photos Recommended / Foto raccomandate**
[https://facebook.com/search/\[User ID\]/photos-recommended-for](https://facebook.com/search/[User ID]/photos-recommended-for)
- **Apps Used / App in uso**
[https://facebook.com/search/\[User ID\]/apps-used](https://facebook.com/search/[User ID]/apps-used)
- **Videos / Video**
[https://facebook.com/search/\[User ID\]/videos](https://facebook.com/search/[User ID]/videos)



Digital Forensics



28

Esempi (valide fino al 7/6/2019)

- **Videos Of User / Video dell'utente**
[https://facebook.com/search/\[User ID\]/videos-of](https://facebook.com/search/[User ID]/videos-of)
- **Videos Tagged / Video con Tag**
[https://facebook.com/search/\[User ID\]/videos-tagged](https://facebook.com/search/[User ID]/videos-tagged)
- **Videos By User / Video per l'utente**
[https://facebook.com/search/\[User ID\]/videos-by](https://facebook.com/search/[User ID]/videos-by)
- **Videos Liked / "Mi Piace" ai video**
[https://facebook.com/search/\[User ID\]/videos-liked](https://facebook.com/search/[User ID]/videos-liked)
- **Video Comments / Commenti ai video**
[https://facebook.com/search/\[User ID\]/videos-commented](https://facebook.com/search/[User ID]/videos-commented)
- **Future Event Invitations / Inviti agli eventi futuri**
[https://facebook.com/search/\[User ID\]/events](https://facebook.com/search/[User ID]/events)



Digital Forensics



29

Esempi (valide fino al 7/6/2019)

- **Events Year / Eventi per anno (da specificare)**
[https://facebook.com/search/str/\[User ID\]/events/\[Year\]/date/events/intersect/](https://facebook.com/search/str/[User ID]/events/[Year]/date/events/intersect/)
- **Events Created Year / Eventi creati dall'utente in un anno specifico (da indicare)**
[https://facebook.com/search/str/\[User ID\]/events-created/\[Year\]/date/events/intersect/](https://facebook.com/search/str/[User ID]/events-created/[Year]/date/events/intersect/)
- **Events Invited Year / Inviti agli eventi in un anno specifico (da indicare)**
[https://facebook.com/search/str/\[User ID\]/events-invited/\[Year\]/date/events/intersect/](https://facebook.com/search/str/[User ID]/events-invited/[Year]/date/events/intersect/)
- **Events Joined Year / "PartecipoMi interessa" agli eventi in un anno specifico (da indicare)**
[https://facebook.com/search/str/\[User ID\]/events-joined/\[Year\]/date/events/intersect/](https://facebook.com/search/str/[User ID]/events-joined/[Year]/date/events/intersect/)
- **Posts by User / Post dell'utente**
[https://facebook.com/search/\[User ID\]/stories-by](https://facebook.com/search/[User ID]/stories-by)
- **Posts by Year / Post dell'utente per anno (da specificare)**
[https://facebook.com/search/\[User ID\]/stories-by/\[Year\]/date/stories/intersect/](https://facebook.com/search/[User ID]/stories-by/[Year]/date/stories/intersect/)
- **Posts Tagged / Post con Tag**
[https://facebook.com/search/\[User ID\]/stories-tagged](https://facebook.com/search/[User ID]/stories-tagged)
- **Posts Liked / "Mi Piace" ai Post**
[https://facebook.com/search/\[User ID\]/stories-liked](https://facebook.com/search/[User ID]/stories-liked)



Digital Forensics



30

Esempi (valide fino al 7/6/2019)

- **Posts Commented / Commenti ai post**
[https://facebook.com/search/\[User ID\]/stories-commented](https://facebook.com/search/[User ID]/stories-commented)
- **Employers / Luogo di lavoro\Datore di lavoro\Azienda**
[https://facebook.com/search/\[User ID\]/employers](https://facebook.com/search/[User ID]/employers)
- **Reviews / Recensioni**
[https://facebook.com/\[User ID\]/reviews](https://facebook.com/[User ID]/reviews)
- **Groups / Gruppi**
[https://facebook.com/search/str/\[User ID\]/groups](https://facebook.com/search/str/[User ID]/groups)
- **Co/Workers / Colleghi\Collaboratori**
[https://facebook.com/search/\[User ID\]/employees](https://facebook.com/search/[User ID]/employees)
- **Friends / Amici**
[https://facebook.com/search/\[User ID\]/friends](https://facebook.com/search/[User ID]/friends)
- **Followers / Followers**
[https://facebook.com/search/\[User ID\]/followers](https://facebook.com/search/[User ID]/followers)
- **Relatives / Parenti**
[https://facebook.com/search/\[User ID\]/relatives](https://facebook.com/search/[User ID]/relatives)
- **Friends' Likes / "Mi Piace" degli amici alle pagine**
[https://facebook.com/search/\[User ID\]/friends/pages-liked](https://facebook.com/search/[User ID]/friends/pages-liked)



31

Commenti

- Non si tratta di un bug o altro; le limitazioni alla privacy sono decise da ogni singolo utente che interagisce con la piattaforma.
- Un profilo che utilizza tutti gli accorgimenti di privacy possibili, interagendo con un altro utente che non le utilizza, deve “sottostare” alle impostazioni di quest’ultimo.
- Riassumendo, nelle interazioni, chi ha il livello di privacy più basso, decide la visibilità o meno delle informazioni.



Digital Forensics



32

Risorse (valide fino al 7/6/2019)

- Source:
<https://www.ictsecuritymagazine.com/articoli/facebook-osint-come-ricavare-le-informazioni-tramite-specifiche-query/>



Digital Forensics



33

Tool on line e altre risorse

- <https://inteltechniques.com/book1.html>
- <https://stalkscan.com/> (NON più ATTIVO)
- <https://securitytrails.com/blog/osint-facebook-tools>
- <https://plessas.net/facebookmatrix>
- <https://osintcurio.us/2019/08/22/the-new-facebook-graph-search-part-1/>
- <https://osintcurio.us/2019/08/22/the-new-facebook-graph-search-part-2/>
- <http://www.subliminalhacking.net/2012/12/27/osint-tools-recommendations-list/>
- <https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools>



Digital Forensics



34

The new Facebook Graph Search

Most recent popular content

```
1 JSON: {"rp_chrono_sort":{"name":"chronosort"},"a
2 Base64: eyJycF9jaHJvbm9fc29ydCI6IntcIm5hbWVcIjpcImNoc
```

Most popular public content

```
1 JSON: {"rp_author":{"name":"merged_public_posts\"
2 Base64: eyJycF9hdXRob3IiOiJ7XCJucyYw1lXCI6XCJtZXJnZWRFc
```

Most popular content posted from your own profile

```
1 JSON: {"rp_author":{"name":"author_me"},"args\"
2 Base64: eyJycF9hdXRob3IiOiJ7XCJucyYw1lXCI6XCJhdXRob3Jfb
```

Most popular content viewed by your profile

```
1 JSON: {"interacted_posts":{"name":"interacted_pos
2 Base64: eyJpbmRlcmFjdGVkX3Bvc3RzIjoie1wibmFtZVwiOlwia
```



35

Altre fonti?

- Esistono siti che uniscono più ricerche contemporaneamente. Ad esempio, [All-io](#) permette ricerche su Google, Twitter, Youtube e molti altri, mentre [Qwant](#) ha un'opzione in base a ciò che si vuole cercare.



Sicurezza, privacy e nessuna tracciabilità. [Scopri di più >>](#)

Accedi  



Che cosa stai cercando?



36

Acquisizione/cristallizzazione pagine WEB (e non solo)

Anche per premunirsi in caso di cancellazione è comunque necessario iniziare al più presto la fase di “**cristallizzazione**” utilizzando alcuni accorgimenti, come ad esempio il software gratuito **FAW (Forensic Acquisition of Websites)** che permette di acquisire in maniera **forense** pagine web o profili di social network con alcune garanzie sull'originalità del dato acquisito.

Esistono poi servizi web che permettono di scaricare una **copia autentica** di pagine o post Facebook a patto che questi siano pubblici e non privati.

Esempio

- Perma.cc
- Archive.is



37

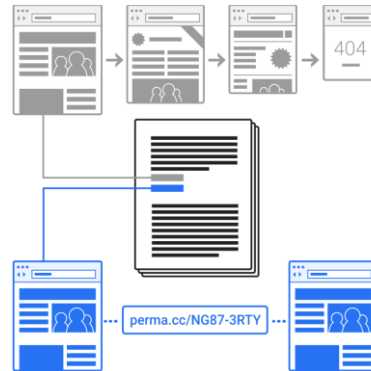
Acquisizione: problematiche tecniche

L'**acquisizione forense con cristallizzazione** della prova online su Internet per tutelare i propri diritti può includere ad esempio anche i file robots.txt, i certificati SSL, le sitemap, i metadati RSS o dei documenti presenti sul sito, il filmato dell'acquisizione forense, le sitemap, eventuali codici di errore, indirizzi IP, record DNS, un dump del traffico di rete realizzato tra il browser/client e il server web che ospita il sito, incluse le chiavi SSL necessarie poi per decriptare il traffico e verificarne la consistenza.



38

Perma.cc offre 10 acquisizioni gratuite al mese per ogni account registrato e ha il vantaggio che è possibile acquisire una pagina creandone una “copia” che poi può essere resa privata, così da evitare che venga trovata tramite ricerche su web. Una volta registrati e creata la copia certificata della pagina web, ricordarsi di modificarne le proprietà rendendola “privata”, così da non renderla accessibile a Google ma poterla fornire poi al consulente informatico nominato per la perizia sulla diffamazione a mezzo stampa o internet via Facebook.



Digital Forensics



39

Archive.is non richiede registrazione ma va tenuto presente che qualunque cosa gli si faccia acquisire, verrà pubblicata su Internet e farà parte dei risultati di ricerca di Google e dei vari motori: un messaggio diffamatorio su Facebook, quindi, sarà poi presente due volte, una su Facebook e una su Archive.is.

Voglio archiviare il contenuto di una pagina web

Archive.is is a time capsule for web pages!

It takes a 'snapshot' of a webpage that will always be online even if the original page disappears.

It saves a text and a graphical copy of the page for better accuracy and provides a short and reliable link to an unalterable record of any web page including those from Web 2.0 sites:

- <http://archive.is/2013.05.01/http://nickaishu.github.io/ds-is/>
- <http://archive.is/2014.06.26/https://www.google.com/maps/>

This can be useful if you want to take a 'snapshot' a page which could change soon: price list, job offer, real estate listing, drunk blog post, ...

Saved pages will have no active elements and no scripts, so they keep you safe as they cannot have any popups or malware!

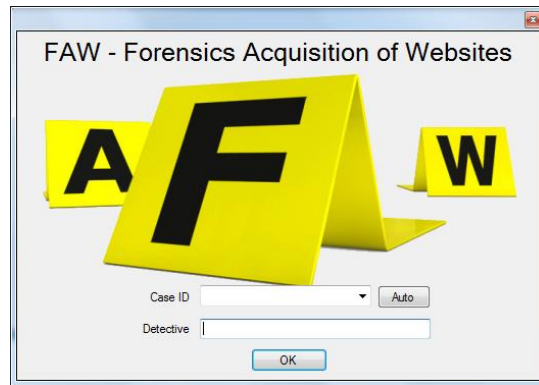


Digital Forensics



40

Forensics Acquisition of Websites



<https://it.fawproject.com/>



Digital Forensics



41

FAW (Manuale utente)

https://www.fawproject.com/manuals/manuale_faw_2023_it.pdf

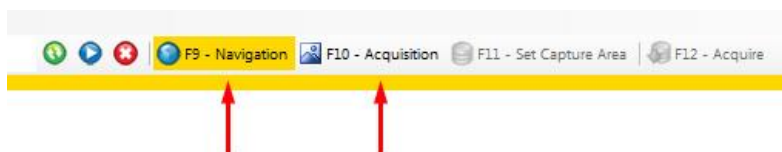


Digital Forensics



42

Dalla barra del menu è possibile settare le preferenze del programma scegliendo: la pagina iniziale, la cartella in cui salvare le acquisizioni e lo user-agent da utilizzare. FAW utilizza due modalità operative: Navigazione e Acquisizione attivabili cliccando sul rispettivo pulsante oppure tramite i tasti funzioni F10 e F11.



La modalità Navigazione imposta FAW come un normale browser e permette di navigare tra le pagine web utilizzando i controlli classici: barra dell'indirizzo, pulsanti avanti e indietro, pulsanti vai, stop e ricarica. Cliccando sul pulsante [Acquisizione], FAW inizia ad acquisire il traffico sulla rete e salva gli eventi di windows generati da questo momento fino alla fine dell'acquisizione; in questa modalità è possibile navigare normalmente, effettuare login e ogni altra operazione fino ad arrivare alla pagina Web che si intende acquisire.



Digital Forensics



43

Acquisizione pagina Web

Raggiunta la pagina web da acquisire si deve premere il pulsante [Set Capture Area] in questo modo verrà bloccata la navigazione e i relativi controlli, e sarà possibile regolare l'altezza dell'area delimitata in giallo denominata "Gold Box" per acquisire l'intera pagina Web.



Il Gold Box si può estendere verso il basso con la funzione di resize semplicemente andandoci sopra con il puntatore del mouse nella parte destra apparirà la barra di scorrimento verticale della Gold Box che non deve essere confusa con la barra di scorrimento della pagina web.

Il concetto base per l'acquisizione grafica di una pagina web è: **tutto ciò che si trova all'interno della Gold Box viene acquisito.**



Digital Forensics



44

Acquisizione pagina Web

Per iniziare l'acquisizione della pagina Web si deve cliccare sul pulsante [Acquire]



FAW inizierà ad acquisire l'immagine della pagina Web facendola scorrere, poi acquisirà gli headers e il codice HTML di tutta la pagina (non solo dell'area selezionata) e gli eventuali oggetti contenuti nella pagina (se selezionati nel menu Configuration).

Al termine delle operazioni si aprirà la finestra della cartella dove sono stati acquisiti i vari file.



Digital Forensics



45

- **Acquisition.log:** è il file che contiene l'elenco delle operazioni eseguite con il software FAW
- **Acquisition.txt:** è un file di testo che contiene tutti i riferimenti dell'acquisizione
- **Acquisition.xml:** è un file in formato xml che contiene tutti i riferimenti dell'acquisizione secondo lo standard DFXML
- **Checking.faw:** è il file che contiene un codice di controllo che permette di verificare se i file Acquisition.txt e Acquisition.xml non sono stati alterati
- **Code.htm:** è un file htm che contiene tutto il codice HTML della pagina web
- **CodeFrame{nomeframe}.htm:** sono file che contengono il codice HTML del frame {nomeframe} se presente
- **Headers.txt:** è un file di testo che contiene gli headers inviati al browser dalla pagina web
- **Hosts:** è la copia del file hosts di windows al momento dell'acquisizione della pagina Web



Digital Forensics



46

- **Image.png:** è il file che contiene l'immagine della pagina web delimitata dalla Gold Box in formato png a 24bit
- **Image{numero}.png:** sono file immagine con i ritagli dell'immagine completa della pagina Web acquisita con aspect-ratio 1,41 adatte ad essere stampate a pagina intera su fogli A4
- **SystemLogEvents.txt:** è il file in cui vengono registrati tutti gli eventi di windows avvenuti durante l'acquisizione della pagina Web
- **screenCapture.wmv:** è il file video acquisito da VLC con la cattura dell'intero schermo del computer dall'inizio dell'acquisizione fino alla fine
- **Wireshark_{mac-address-network-interface}.pcap:** è il file acquisito da WireShark con il traffico di rete avvenuto durante l'acquisizione della pagina Web
- **Cartella Objects:** è la cartella che contiene tutti gli elementi della pagina Web acquisiti numerati progressivamente con il formato [nnnnn]filename.ext

Ogni acquisizione viene inserita in una sottocartella numerata sequenzialmente (esempio: 0001, 0002, 0003, 000n) della cartella con nome del Case ID scelta dall'utente.



Digital Forensics



47

Fasi Finali

Per rendere l'acquisizione della pagina web valida a fini legali si può firmare digitalmente il solo file **Acquisition.txt** oppure il file **Acquisition.xml** ricordandosi di apporvi anche una marca temporale che certifica la data dell'acquisizione.

Salvataggio dei dati dell'acquisizione su server FAW

Al termine dell'acquisizione FAW chiede se si vuole salvare i dati dell'acquisizione nel database del server FAW; i dati che verranno salvati sono i seguenti: checking code, data inizio e fine acquisizione, URL acquisito e l'indirizzo IP del client che ha eseguito l'acquisizione.

Se l'utente acconsente all'invio di questi dati gli stessi saranno memorizzati nel database del server FAW e saranno disponibili per eseguire verifiche on-line dell'integrità dell'acquisizione.



Digital Forensics



48

Marca Temporale



Trattasi di tecniche per la **generazione**, **apposizione** e **verifica** della validazione temporale dei documenti informatici, mediante generazione e applicazione di una **marca temporale**. Queste marche temporali sono generate da un apposito sistema di validazione temporale che deve contenere almeno le seguenti informazioni:

- Identificativo dell'emittente;
- Numero di serie della marca temporale;
- Algoritmo di sottoscrizione della marca temporale;
- Identificativo del certificato relativo alla chiave di verifica della marca temporale;
- Riferimento temporale della generazione della marca temporale;
- Identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- Valore dell'impronta dell'evidenza informatica.



Digital Forensics



49

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 Codice dell'Amministrazione Digitale Dlgs 82/2005)

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



Digital Forensics



50

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.

Apporre una Marca Temporale ad un documento firmato digitalmente pertanto fa sì che la **Firma Digitale risulti sempre e comunque valida** anche nel caso in cui il relativo Certificato risulti scaduto, sospeso o revocato, purché la Marca sia stata apposta in un momento precedente alla scadenza, revoca o sospensione del Certificato di Firma stessa.

Come sancito **dall'articolo 49 del Dpcm del 30/03/2009**, le Marche Temporal emesse devono essere conservate in appositi archivi per un periodo non inferiore a 20 anni. **L'apposizione di una Marca Temporale a un documento firmato digitalmente, quindi, ne garantisce la validità nel tempo.**



Digital Forensics



51



Il software di riferimento per l'acquisizione forense di pagine web. Riconosciuto dalle comunità forensi in tutto il mondo come uno strumento prezioso per cristallizzare pagine web.



Acquisisce le pagine web presenti sul Darkweb attraverso la rete TOR.



Inizia l'acquisizione di pagine web e le termina manualmente, consentendo all'operatore di catturare nel suo complesso il comportamento di pagine e contenuti multimediali (audio/video).



Consente di programmare l'acquisizione di una pagina web, in modo da poter catturare il contenuto della stessa in diversi momenti della giornata.



È un vero e proprio crawler che cerca tutte le pagine web collegate alla pagina principale, estraendone l'URL e l'hash per creare un indice da cui può essere successivamente acquisito automaticamente. Permette inoltre di eseguire ricerche su siti web con aree protette da login, come i social network.



FAW in versione multipagina, consente la cattura automatica di un elenco di pagine web. Perfetto per catturare interi siti web in modo rapido e automatico.



Questo strumento consente di catturare interi siti Web in modalità FTP e SFTP senza modificare metadati di file copiati.



Con questo strumento è possibile creare un report dettagliato di tutte le attività svolte con la suite FAW; importa automaticamente tutti i riferimenti delle acquisizioni.



Digital Forensics



52

Faw x VirtualBOX



E' scaricabile dalla sezione download del sito ufficiale FAW una macchina virtuale preconfigurata per VirtualBox (ma utilizzabile anche su VMWare, dato che il disco virtuale è in formato VMDK) contenente una versione di valutazione di Windows 7 Enterprise all'interno della quale è stato preinstallato FAW, il software per acquisizione certificata e cristallizzazione di siti e pagine web a fini probatori per uso legale in Tribunale. Il tool gratuito FAW è installato nella VM in versione 5.1.6.4 ed è integrato con VLC e Wireshark, necessari per arricchire l'acquisizione probatoria con filmati video e registrazione del traffico di rete.

<https://www.dalchecco.it/acquisizione-forense-siti-web-faw-virtualbox/>



Digital Forensics



53

Tools

VLC media player

Lettore multimediale

VLC media player è un lettore multimediale gratuito open source multiplatforma, in grado di riprodurre file audio e video in diversi formati e su vari dispositivi, sviluppato dal progetto VideoLAN. [Wikipedia](#)

VirtualBox

Software

Oracle VM VirtualBox, è un software open source per l'esecuzione di macchine virtuali per architettura x86 e 64bit che supporta Windows, GNU/Linux e macOS come sistemi operativi host, ed è in grado di ... [Wikipedia](#)

Wireshark

Software

In informatica e telecomunicazioni Wireshark è un software per analisi di protocollo o packet sniffer utilizzato per la soluzione di problemi di rete, per l'analisi e lo sviluppo di protocolli o di software di comunicazione e per la didattica. [Wikipedia](#)



Digital Forensics



54

Legal Eye™ Pro è un servizio in cloud. Semplice, sicuro, garantito.

Acquistato il servizio, Legal Eye™ Pro è subito pronto per registrare automaticamente tutte le prove per te.

Legal Eye™ registra anche i download dei documenti che effettui mentre navighi.

Data certa (e certificata) dei documenti che scarichi.

L'acquisizione genera un archivio certificato criptato della prova digitale valido per sempre.

L'acquisizione genera un archivio certificato criptato della prova digitale valido per sempre.

Puoi ripetere l'acquisizione per confermarla solo quando la ritieni soddisfacente.

Hai 3 mesi di backup gratuito della prova digitale in cloud.

Su richiesta, puoi ricevere la tua acquisizione digitale su DVD.

Digital Forensics

55



- L'acquisizione viene effettuata in modalità simile alla semplice navigazione in Internet. Tramite il browser dell'utente, viene reso disponibile un "browser virtuale", con il quale è possibile accedere a qualunque sito web pubblico o privato.
- Tutta la navigazione è registrata ed è possibile archiviare qualunque materiale presente in rete. Tutto quanto scaricato - compreso il video dell'intera navigazione - sarà automaticamente reso disponibile all'interno di un archivio cifrato, pochi attimi dopo il termine dell'acquisizione.
- <https://www.legaleye.cloud/public>

Digital Forensics

JUNCE PROCESSING LABORATORY


56

<https://www.kopjra.com/>

Kopjra

STORE

Benvenuti nello store digitale di Kopjra



WEB INTELLIGENCE
Gestione di investigazioni su Internet


Suite di soluzioni per la gestione di approfondite investigazioni su Internet e in particolare per l'individuazione e rimozione tempestiva di violazioni della reputazione, della proprietà intellettuale e industriale su clear, deep e dark web.

A PARTIRE DA
50 €/MESE

CONFIGURA E ACQUISTA

PROVA GRATIS

[Accedi a Web Intelligence](#)




WEB FORENSICS
Acquisizione forense di prove su Internet

Soluzione per l'acquisizione di pagine web da produrre come prove nei giudici, rispettando le best practice internazionali dell'informatica forense, ovvero lo standard ISO/IEC 27037:2012.

A PARTIRE DA
75 €

CONFIGURA E ACQUISTA

[Accedi a Web Forensics](#)



WEB SIGN
Firma elettronica di documenti

Piattaforma in cloud brevettata per la gestione di complessi flussi di firma a partire da documenti e modelli in formato PDF, prima in assoluto a seguire i principi dell'informatica forense.

A PARTIRE DA
15 €/MESE

CONFIGURA E ACQUISTA

PROVA GRATIS

[Accedi a Web Sign](#)



Digital Forensics



57



WEB FORENSICS

LA PROVA DIGITALE



Digital Forensics



58

Credits/Link

<http://www.altalex.com/documents/news/2016/06/27/diffamazione-a-mezzo-internet-nei-piu-recenti-orientamenti-giurisprudenziali>

<http://www.altalex.com/documents/news/2017/07/21/diffamazione-via-facebook>

<https://www.studiocataldi.it/articoli/24051-la-diffamazione-a-mezzo-internet.asp>

Diffamazione on-line Tecniche d'investigazione sui social media, reperimento delle fonti di prova, criteri per il risarcimento del danno Autori: Di Stefano Michelangelo, Ferrazzano Michele, Fiammella Bruno 2023



Digital Forensics



59

Social Network (def. Treccani)



social network. Con l'espressione social network si identifica un servizio informatico on line che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro. Generalmente i s.n. prevedono una registrazione mediante la creazione di un profilo personale protetto da password e la possibilità di effettuare ricerche nel database della struttura informatica per localizzare altri utenti e organizzarli in gruppi e liste di contatti. Le informazioni condivise variano da servizio a servizio e possono includere dati personali, sensibili (credo religioso, opinioni politiche, inclinazioni sessuali ecc.) e professionali. Sui s.n. gli utenti non sono solo fruitori, ma anche creatori di contenuti.

60

Social Network

- Instagram
- Twitter
- LinkedIn
- TIKTOK
- YouTube
- Pinterest
- Google Plus+
- Tumblr
- Reddit
- Vkontakte
- Flickr
- Meetup
- Ask.fm
- Classmates



<https://socialmedialist.org/elenco-dei-social-network-nel-mondo.html>



61



La Posta Elettronica



64



Il servizio di posta elettronica

Il servizio di posta elettronica, chiamato anche "**e-mail**" (**electronic mail**) consente a ogni utente che abbia accesso ad un computer e che possa connettersi ad Internet di inviare "messaggi" (testi ma anche, più in generale, "oggetti" memorizzati in formato elettronico, sotto forma di file, come programmi, immagini, suoni, ecc.) ad un qualsiasi altro utente che disponga di un indirizzo di posta elettronica e che lavori su un qualsiasi altro computer, ovunque collocato, purché raggiungibile tramite connessioni in rete.



Digital Forensics



65

Il servizio di posta elettronica

I computer dei due corrispondenti non debbono essere contemporaneamente o permanentemente connessi alla rete; i messaggi infatti vengono recapitati su caselle di posta elettronica ospitate da appositi server (**comunicazione asincrona**)

L'utente che vuole verificare l'arrivo di messaggi a lui indirizzati potrà **contattare il server** e solamente nell'intervallo in cui avviene la transazione tra il computer dell'utente ed il server è necessario che la connessione di rete sia attiva.

Un primo evidente vantaggio che l'utilizzo della posta elettronica comporta è la velocità: anche tra i sistemi più distanti tra loro, purché in qualche modo comunicanti, i messaggi possono essere recapitati nel giro di poche ore (il più delle volte sono comunque sufficienti pochi minuti).



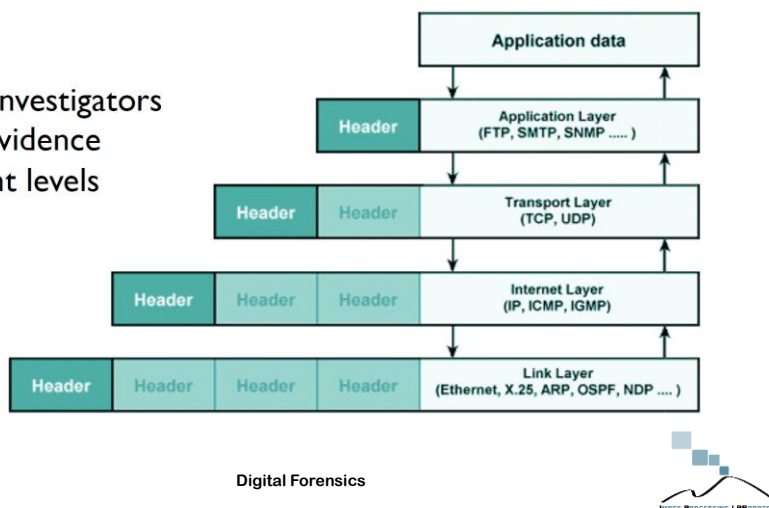
Digital Forensics



66

TCP/IP Protocolli e Layer

Forensic investigators
may get evidence
at different levels



67

Il servizio di posta elettronica



La disponibilità di un indirizzo di e-mail è un prerequisite indispensabile per utilizzare il servizio di posta elettronica, dal momento che serve per individuare sulla rete mittenti e destinatari dei messaggi. Gli indirizzi di posta elettronica hanno la forma:

utente@indirizzo

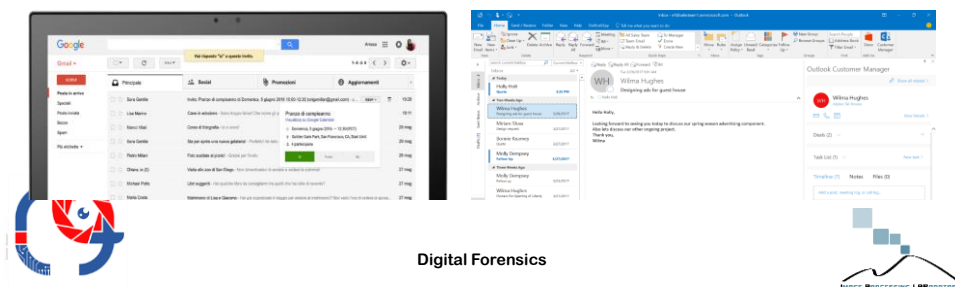
dove la parte a sinistra del simbolo @, detto anche "chiocciola" e normalmente letto come "at" (presso), **identifica l'utente in maniera univoca all'interno del server che lo ospita**; la parte di indirizzo a destra del simbolo @ identifica invece in maniera univoca, all'interno della rete Internet, **il sistema informatico presso il quale l'utente è ospitato** e corrisponde appunto al "nome" del server, normalmente espresso come un insieme di parole (o più in generale di stringhe di caratteri alfanumerici) separate da punti.

68

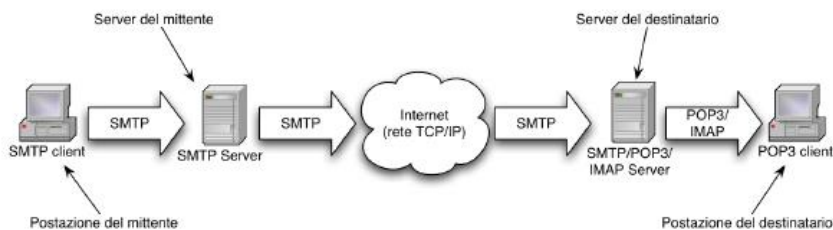
Sistemi di posta elettronica

Ogni Internet Service Provider (ISP) o altri fornitori di servizi online permettono agli utenti privati e di pubbliche imprese di aprirsi una propria casella di posta elettronica dove poter inviare e ricevere messaggi, anche allegati. La posta elettronica è consultabile:

- attraverso il sito internet di riferimento ([webmail](#))
- attraverso un programma client di posta elettronica che, settato opportunamente, scarica da internet la posta di uno o più account.



69

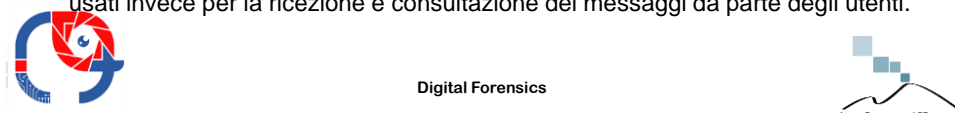


I sistemi di posta elettronica sono composti da due sottosistemi:

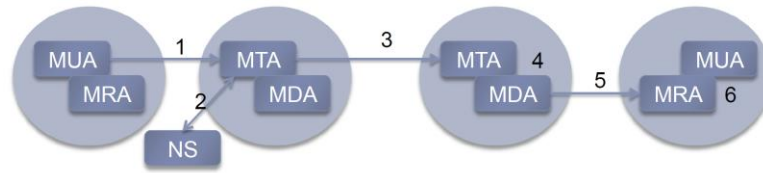
- **agenti utente o client**, ovvero programmi che consentono alle persone di leggere e inviare la posta elettronica (webmail o programma client).
- **server**, si occupano dello spostamento dei messaggi dall'origine alla destinazione attraverso l'utilizzo di determinati protocolli.

I protocolli tipicamente impiegati per lo scambio di e-mail sono:

- **SMTP (Simple Mail Transfer Protocol)**, usato per l'invio, la ricezione e l'inoltro dei messaggi tra server (nonché per il solo invio da parte dei client).
- **POP3 (Post Office Protocol)** e **IMAP (Internet Message Access Protocol)** usati invece per la ricezione e consultazione dei messaggi da parte degli utenti.



70



- ▶ MUA – Mail User Agent
 - ▶ E.g. thunderbird, outlook
 - ▶ MTA – Mail Transfer Agent
 - ▶ E.g. sendmail, qmail
 - ▶ MDA – Mail Delivery Agent
 - ▶ E.g. procmail
 - ▶ MRA – Mail Retrieval Agent
 - ▶ POP/IMAP client
 - ▶ NS – Name Server
 - ▶ DNS server
1. MUA implements smtp client to smtp server
 2. MTA solves address using MX record in NS
 3. MTA contacts MTA though SMTP
 4. Receiving MTA delivers the email to MDA
 5. MRA uses IMAP/POP/MAPI to retrieve from MDA
 6. MUA presents mail to user



Digital Forensics



71

SMTP tramite telnet

```

C: telnet server8.engr.scu.edu 25
S: 220 server8.engr.scu.edu ESMTP Sendmail 8.12.10/8.12.10; Tue, 23 Dec 2003 16:32:07
-0800 (PST)
C: helo 129.210.16.8
S: 250 server8.engr.scu.edu Hello dhcp-19-198.engr.scu.edu [129.210.19.198], pleased to
meet you
C: mail from: jholliday@engr.scu.edu
S: 250 2.1.0 jholliday@engr.scu.edu... Sender ok
C: rcpt to: tschwarz
S: 250 2.1.5 tschwarz... Recipient ok
C: data
S: 354 Enter mail, end with "." on a line by itself
C: This is a spoofed message.
C: .
S: 250 2.0.0 hB00W76P002752 Message accepted for delivery
C: quit
S: 221 2.0.0 server8.engr.scu.edu closing connection
  
```

Senza accedere all'account di terzi è possibile stabilire una connessione con l'e-mail server (ad esempio mediante [telnet](#)) e scrivere direttamente i comandi relativi a mittente e destinatario, ai parametri aggiuntivi e creare il corpo della mail



Digital Forensics



72

Sistemi di posta elettronica

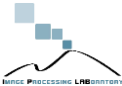
Un aspetto importante nei sistemi di posta elettronica è la distinzione tra **l'involucro** e il suo **contenuto**.

L'involucro incapsula il messaggio e contiene tutte le informazioni necessarie per il trasporto dei messaggi: come **l'indirizzo di destinazione**, la **priorità** e il **livello di protezione**, che sono distinte dal messaggio stesso. Gli agenti di trasporto dei messaggi utilizzano l'involucro per l'instradamento e trasferire il messaggio al destinatario, così come gli uffici postali tradizionali utilizzano le buste.

Il messaggio all'interno dell'involucro consiste di due parti: **l'intestazione** (**header**) e il **corpo**. L'intestazione contiene le informazioni di controllo per gli agenti utente ed il corpo è dedicato interamente al destinatario umano.



Digital Forensics

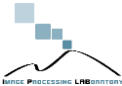


73

Posta elettronica vs Posta cartacea



Digital Forensics



74

Posta elettronica vs Posta cartacea

L'informazione trasmessa attraverso un messaggio di posta elettronica giunge normalmente al destinatario nella stessa forma in cui era sul computer "mittente" ma è suscettibile ad elaborazioni da parte del destinatario sul proprio computer (**manipolazione**, **copiatura**, **"ritaglio"**, **completamento**, ecc.), senza passaggi intermedi.

Nel caso di un messaggio "cartaceo" invece, l'informazione non può essere alterata se non attraverso una complicata procedura che prevede la riproduzione in formato elettronico del documento e l'elaborazione digitale del testo o delle immagini ecc.



Protocolli

Inizialmente il protocollo per la rappresentazione dei documenti di posta elettronica era definito nel documento [RFC 822](#), del 1982; in cui veniva specificato il formato per i messaggi di posta e ci si limitava a messaggi esclusivamente di tipo testuale, senza alcun riferimento a messaggi di altro tipo (ad esempio file multimediali).

Intestazione	Significato
To:	gli indirizzi di posta elettronica dei destinatari primari
Cc:	gli indirizzi di posta elettronica dei destinatari secondari
Bcc:	gli indirizzi di posta elettronica per le copie per conoscenza nascoste
From:	la persona che ha creato il messaggio
Sender:	l'indirizzo di posta elettronica del mittente vero e proprio
Received:	la riga aggiunta da ogni agente di trasferimento lungo il percorso
Return-path:	può essere utilizzato per identificare un percorso di ritorno al mittente



Protocolli

L'affermarsi dei servizi di posta elettronica e la conseguente necessità di far fronte alle limitazioni dettate da RFC 822, ha portato nel giugno 1992 alla presentazione di un nuovo documento, l'[RFC 1341](#), in cui viene descritto lo standard **MIME (Multipurpose Internet Mail Extensions)**. In particolare in RFC 1341 vengono specificati i meccanismi per definire il formato sia di messaggi testuali (ASCII e non) sia di messaggi multimediali (cioè contenenti video, suono, immagini, ecc.). Tale documento si concretizza con la definizione di cinque nuove intestazioni dei messaggi

Intestazione	Significato
MIME-version:	identifica la versione di MIME
Content-description:	stringa leggibile che comunica che cosa contiene il messaggio
Content-id:	identificatore univoco
Content-transfer-encoding:	indica come il corpo del messaggio è stato preparato per la trasmissione
Content-type:	il tipo e il formato del documento



Digital Forensics



77

E-mail: Analisi forense

Webmail

Accesso server (consenso, pwd, ecc.)



Software di gestione di posta elettronica

Nel secondo caso, in cui l'utente utilizza software di gestione di posta elettronica, tutto o parte dell'archivio di posta viene scaricato sul computer (o sul dispositivo) al momento della configurazione dell'account. Periodicamente il client di posta effettua controlli per verificare la presenza di nuovi messaggi in arrivo. In questo caso la **Computer Forensics** può intervenire attraverso l'analisi sugli archivi, cercando di estrapolare la maggior parte dei dati possibile.

Una volta entrato in possesso dei file contenenti le e-mail, l'esperto forense può intraprendere la fase d'analisi analizzando tutti i campi relativi all'intestazione e al corpo del messaggio stesso.



Digital Forensics



78

Analisi e-mail: Intestazioni/headers

Identificazione mittente

- Phishing
- Malware
- Ecc.

```

Received-SPF: pass (google.com: domain of chris@example.com
66.171.248.166 as permitted sender) client-ip=66.171.248.166;
Authentication-Results: mx.google.com; spf=pass (google.com:
chris@example.com designates 66.171.248.166 as permitted
smtp.mailfrom=chris@example.com
Received: from [192.168.1.122] (192.168.1.1) by mail.google.com
ESMTP (EIMS X 3.3.9) for <joe.user@example.com>; Tue, 12 Jun 2010
13:40:34 -0700
From: Chris <chris@example.com>
Content-Type: multipart/alternative;
boundary="Apple-Mail=3EEF9FAD-3853-6BCF-8509-825622338383"

```



Digital Forensics



79

```

Delivered-To: mariorossi@gmail.com
Received: by 10.218.111.222 with SMTP id m78zs52525wei; Wed, 16 Jun 2010 10:39:19 -0700 (PDT)
Received: by 10.216.91.7 with SMTP id g7mr996235wef.93.1276709959223; Wed, 16 Jun 2010 10:39:19 -0700 (PDT)
Return-Path: <rosario.verdi@tiscali.it>
Received: from mrqout1.tiscali.it (mrqout1-sorbs.tiscali.it [195.115.228.3]) by mx.google.com with ESMTP id x45si7853472weq.196.2010.06.16.10.39.18; Wed, 16 Jun 2010 10:39:19 -0700 (PDT)
Received-SPF: pass (google.com: domain of rosario.verdi@tiscali.it designates 195.145.188.7as permitted sender) client-ip=195.115.228.3;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of rosario.verdi@tiscali.it designates 195.145.188.7as permitted sender) smtp.mail=rosario.verdi@tiscali.it
Received: from [10.23.116.88] by mrq-1 with esmtp (Exim) id 1OOWLh-0002ki-My; Wed, 16 Jun 2010 19:24:25 +0200
Received: from ps23 (10.39.75.93) by mail-8.mail.tiscali.sys (8.0.031) id 3CF3B10F009F2F83 for mariorossi@gmail.com; Wed, 16 Jun 2010 19:24:25 +0200
Message-ID: <13163784.4962237656166810.JavaMail.defaultUser@defaultHost>
Date: Wed, 16 Jun 2010 19:24:22 +0200 (CEST)
From: rosario.verdi@tiscali.it
Reply-To: rosario.verdi@tiscali.it
To: mariorossi@gmail.com
Cc: <go_sc@yahoo.net>
Subject: I: Riepilogo situazione aziendale MIME-Version: 1.0 Content-Type: multipart/mixed;
boundary="-----_Part_3112_30806331.1276709062485
xOriginalSenderIP: 95.226.11.23
X-Priority: 1
X-MSMail-Priority:
High X-Mailer: Microsoft Outlook Express 6.00.2900.5843 Disposition-Notification-To: rosario.verdi@tiscali.it rosario.verdi@tiscali.it
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5579

```



Analisi e-mail: headers

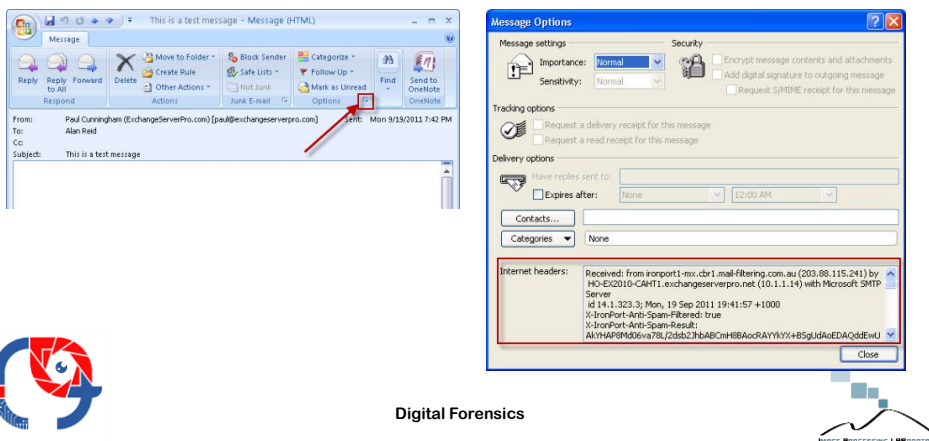
Digital Forensics



80

Analisi e-mail: estrazione headers

I client di posta elettronica rendono disponibile questi tipi di informazione relativamente ad ogni e-mail ricevuta. Le modalità d'accesso a tali dati dipendono dallo specifico client.



81

Headers

Gli headers vanno letti dal **basso** verso **l'alto**. Partendo dalle informazioni principali, risalendo verso la cima dell'headers è quindi possibile ricostruire tutto il percorso fatto dalla mail prima di giungere al destinatario.

Le righe che evidenziano questo percorso sono quelle che iniziano con la parola chiave **Received**. Tale elemento viene aggiunto da ciascun server **SMTP** che ha trattato il messaggio indicando tra parentesi tonde () e quadre [] gli indirizzi IP da cui è stato ricevuto il messaggio ed ulteriori informazioni sulle locazioni geografiche del computer/server.



82

Headers (2)

Dopo il blocco di informazioni contrassegnate dalla parola “**Received**” sono presenti altri campi:

- **Subject** - oggetto del messaggio.
- **From** - fornisce l'informazione della casella di posta del mittente.
- **To** - indica il destinatario.
- **Cc** - destinatari in copia carbone [per conoscenza].
- **Bcc** - destinatari in copia carbone nascosta.
- **Date** - data ed ora al momento dell'invio.
- **Message id** - contiene un codice costruito dal primo server da cui il messaggio è stato spedito, e che dovrebbe permettere di identificare univocamente il messaggio sui server attraversati.
- **Importance** o **X-priority** - priorità del messaggio [se c'è il valore 1 ! alta priorità, 2 ! media priorità, 3 ! normale priorità].
- **X-Mailer** - programma usato per inviare la mail (se si usa una webmail questo campo non è presente).



Digital Forensics



83

Headers (3)

Altra riga da tenere in considerazione è quella preceduta dalla parola Mime.

Il **Mime** (**Multipurpose Internet Mail Extensions**) è un protocollo definito per il trasferimento e l'interpretazione dei dati non codificati in ASCII. Il Mime si occupa anche del trasferimento di allegati in qualsiasi formato, ad esempio file **audio**, file **video**, file **testo** di qualsiasi formato.

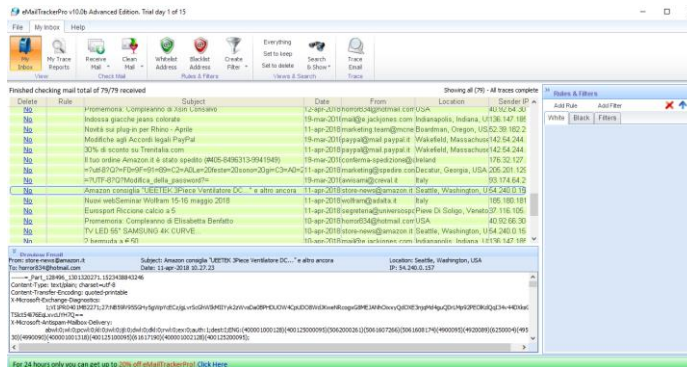


Digital Forensics



84

Tools: Email Tracker



- Estrae automaticamente gli header
- Effettua diversi tipi di analisi
- Traccia attraverso gli IP negli headers il percorso fatto dalla mail
- Genera un report

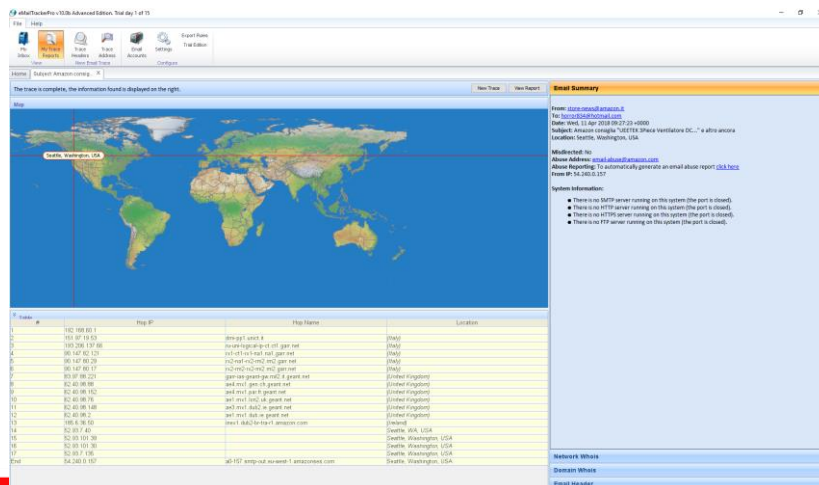


Digital Forensics



85

Tools: Email Tracker



Digital Forensics



86

E-mail: Autenticazione Mittente

Dall'analisi degli header è possibile ricostruire la storia/percorso che una mail compie prima di arrivare a destinazione. La domanda che spesso ci si pone è se tale tipo di analisi basti ad **autenticare** il mittente della mail inviata, ovvero se è possibile in maniera univoca affermare che la casella di posta da cui è partita la mail (nel caso d'esempio identificata dal campo From rosario.verdi@tiscali.it) sia veramente stata utilizzata per l'invio della stessa.

In realtà l'analisi dei campi finora descritti non può fornire tale garanzia riguardo il mittente, a meno che non sia presente un ulteriore campo **denominato DKIM (Domain Key Identified Mail)**.



Digital Forensics



87

E-mail: Autenticazione tramite DKIM:

Il campo DKIM-signature stabilisce che i gestori di un determinato dominio "firmatario" abbiano applicato una firma digitale certificando il contenuto e le intestazioni del messaggio.

Se la firma risulta valida si può quindi stabilire che la mail ricevuta sia "**certificata**" dal dominio che ha apposto la firma, permettendo al destinatario di verificare che il messaggio provenga veramente dal dominio dalla quale dichiara di provenire.

La specifica DKIM garantisce solo che la mail è stata inviata dal dominio firmatario.

```
Return-Path: <verdi@libero.it>
Received: from libero.it (10.248.25.164) by cpms54.iol.local (8.6.145)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=libero.it; s=s2014;
t=1473948239; bh=A7fkK40KPAjjoVRUKCXRscYLxFeSi83hQCriW514o=;
h=Date:From:Reply-To:To:Subject;
b=YSIRhn05SiZcsh1T1R6QehJUV0xiCXkaRGosjUQ0thY2dObgVhjM2gNBnXhW4zEA8
Uj5CZnj+GL1DcdT5e6FQoQ2gyvrmIXfbsbYEIZI5daRTjWC3DgYB/3q13rTS46BHIy
bMpSPe3e3GRt6g65Tx11xHbYA08ha80IFf5BF10xCL1FuVcQbRnN0T9TU74i6SuvE+
1Tju/r4uou030wZj34hQpBbf1zsj6u44Jd00IzgmhuXBH12KDH14Wfy973gYwrPvFf
z/W54te48frkyZAOeo9VaFf09kLaIJbxaWNNr6UwvPIAUvndBAMEIYgcmSd1huoSg8
S7P5Fv01odJPw==
```



Digital Forensics

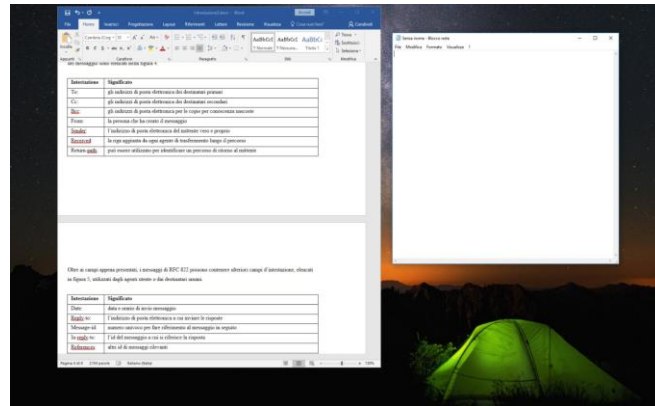


88

Fake e-mail

Cosa occorre:

- Un qualsiasi editor di testo
- Conoscere i campi degli header



Digital Forensics

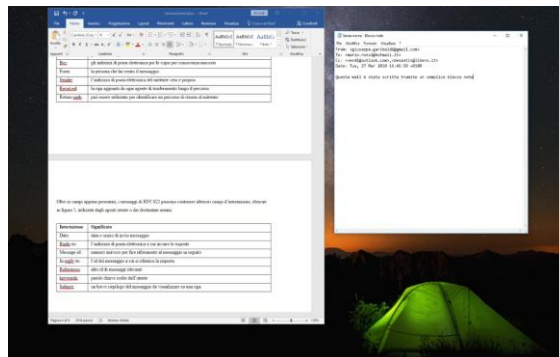


89

Fake e-mail

E' sufficiente inserire negli gli appositi campi i dati di interesse:

- **From** :giuseppe.garibaldi@gmail.com
- **To**: mario.rossi@hotmail.com
- **Cc**: verdi@outlook.com
- ...



Digital Forensics

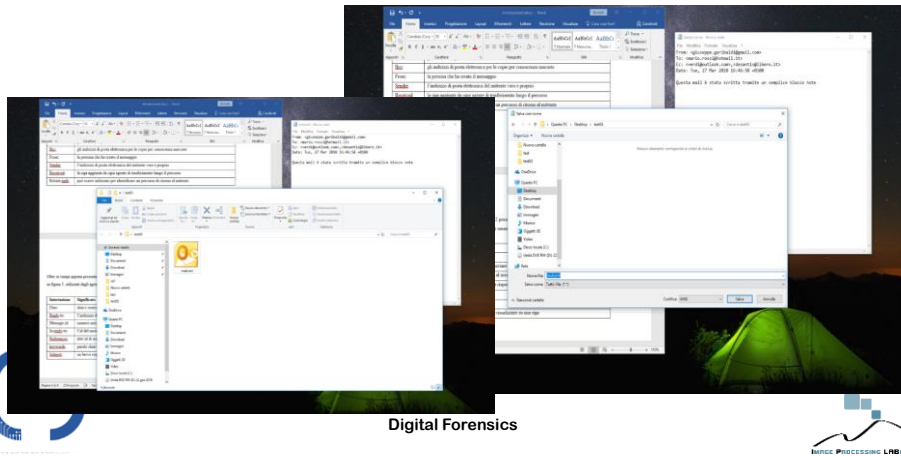


90

Fake e-mail

Cosa fare:

- Salvare il file di testo modificandone l'estensione in **.eml**.

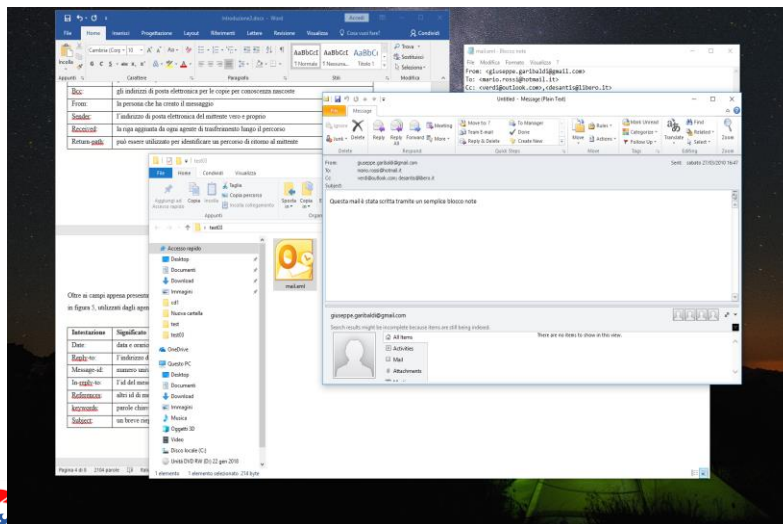


Digital Forensics



91

Fake e-mail



Digital Forensics



92

Fake e-mail: analisi

L'analisi identifica dei mittenti dei messaggi, destinatari, date e orari di invio.

L'assenza del campo **DKIM non permette** di certificare l'autenticità dei messaggi né tanto meno il reale invio degli stessi.

In conclusione non è possibile stabilire che i file presentati siano autentici e che siano stati realmente inviati ai destinatari indicati.



93

Anonymous e-mail

Le **webmail** consentono quasi sempre la registrazione senza una stretta verifica della veridicità dei dati personali forniti. Tuttavia, questi servizi in generale possono non essere completamente anonimi, nel senso che il fornitore impegna coerentemente con la normativa italiana sul data retention, a tracciare gli IP di connessione alla casella.



Tali informazioni sono disponibili per le autorità giudiziaria per un periodo normativo definito nella normativa in vigore.



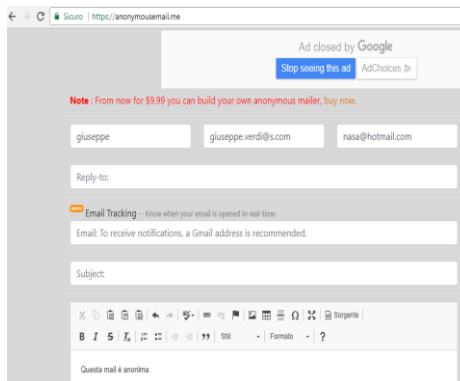
94

Anonymous e-mail

Esiste tuttavia la possibilità di utilizzare servizi **webmail** (a pagamento o free) **dichiaratamente anonimi**.

amonymusmail.me

- Consente l'invio di e-mail anonime
- Nessuna attività viene registrata
- Servizio erogato tramite dominio registrato ad Alexandria (Virginia)



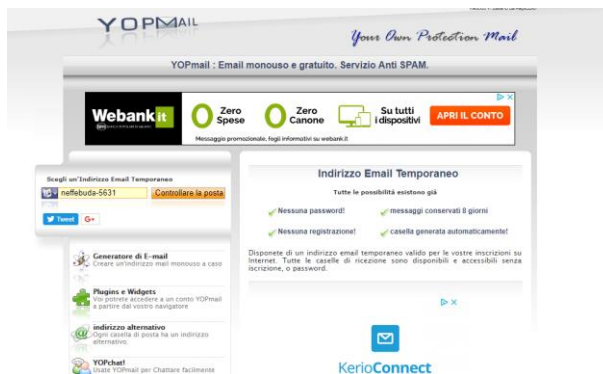
Digital Forensics



95

Anonymous e-mail: YOPmail

Nasce per contrastare le **mail spam** generando **indirizzi email monouso** per le iscrizioni, domande d'informazioni o di documentazioni su siti internet. Le mail inviate alla casella di posta vengono cancellati dopo **8 giorni**.



Digital Forensics



96

Valore giuridico delle e-mail

Un semplice messaggio di posta elettronica ha un qualche valore legale? Lo si può usare come prova in un vero processo. La normativa italiana lascia spazio all'interpretazione e concede margine di manovra al giudice, senza però dare uno strumento certo e definitivo sul tema.

Quale valore hanno le e-mail dal punto di vista giuridico?

Esse vengono utilizzate per una molteplicità di scopi, sia in ambito privato sia in ambito pubblico, ma una e-mail è equiparabile a un documento sottoscritto o non ha alcun valore? Può una semplice e-mail trasformarsi in una vera e propria prova?

Ci si chiede che valenza abbia una dichiarazione contenuta in un messaggio di posta elettronica, se quest'ultimo sia suscettibile di assurgere a **prova in un eventuale giudizio** e, prima ancora, cosa debba intendersi giuridicamente per e-mail.



Digital Forensics



97

Valore giuridico delle e-mail

I riferimenti normativi **L. n. 59/199** (riconoscimento regolamentazione della validità dei documenti formati e/o trasmessi con strumenti informatici), il **Codice dell'Amministrazione Digitale** (cd. CAD) di cui al D. Lgs. 82/2005 e successive modificazioni.

L'e-mail può essere ricondotta nella **categoria dei cd. documenti informatici**, in ragione della definizione che di essi viene fornita all'art. 1, 1° comma, lett. p) del suddetto Codice quale «*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*».



Digital Forensics



98

Valore giuridico delle e-mail

A tale riguardo occorre rilevare come siano rinvenibili **due orientamenti contrapposti**.

Da un lato, infatti, vi è chi ritiene che l'*e-mail* sia da considerarsi quale semplice documento informatico **privo di firma**, in considerazione della pressoché assenza di garanzie che consentano di attribuire allo stesso una **paternità certa**, a nulla rilevando il dispositivo di riconoscimento tramite *password* per l'accesso alla posta elettronica, poiché quest'ultimo sarebbe privo della necessaria connessione logica con i dati elettronici che costituiscono il messaggio.



Digital Forensics



99



Valore giuridico delle e-mail

Secondo tale orientamento, il valore probatorio dell'*e-mail* sarebbe da rinvenirsi nell'art. 2712 c.c. (così come modificato ex art. 23-*quater*, CAD) alla stregua del quale le riproduzioni informatiche, **«fanno piena prova dei fatti e delle cose rappresentate»** solo se colui contro il quale sono prodotte non **le contesta tempestivamente disconoscendone la conformità ai fatti o alle cose medesime**.



Digital Forensics



100



Valore giuridico delle e-mail



Art. 2712 c.c.

Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

Secondo questo primo orientamento la mail vale come prova solo se il mittente non afferma il contrario. Se ciò accade, il messaggio email non ha alcun valore legale – diviene ciò che comunemente chiamiamo “**carta straccia**”.



Digital Forensics



101

Valore giuridico delle e-mail

Secondo un differente orientamento, invece, l'*e-mail* è da considerare, a tutti gli effetti, un documento informatico sottoscritto con **firma elettronica semplice**, come tale liberamente valutabile dal giudice sia in ordine all'idoneità della medesima a soddisfare il requisito della forma scritta, sia per ciò che concerne il suo valore probatorio, ai sensi degli artt. 20, comma 1-bis e 21, comma 1, D.Lgs. 82/2005.

Art. 20 comma 1-bis

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

Art. 21 comma 1

Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.



Digital Forensics



102

Valore giuridico delle e-mail

Si potrebbe obiettare, tuttavia, che sebbene l'accesso alla casella di posta elettronica comporti l'autenticazione dell'utente, ossia l'inserimento di uno **user id** e relativa **password**, potrebbe accadere che tali informazioni siano state in precedenza memorizzate in modo tale da consentirne l'accesso immediato. In tale eventualità, quindi, **la paternità del documento inviato non corrisponderebbe** al formale mittente del messaggio. Inoltre, sussiste la possibilità che il messaggio di posta elettronica ricevuto venga **modificato**, pregiudicandone l'integrità, o che un'e-mail mai venuta ad esistenza sia addirittura creata ad arte in modo tale da risultare tra i messaggi di posta ricevuti (o inviati).

In sintesi: il giudice può considerare una email come una **prova**, ma esistono diverse varianti da prendere in considerazione. Per sua natura, il messaggio elettronico è prone a modifiche che impediscono di considerarlo completamente attendibile.



Digital Forensics



103

Valore giuridico delle e-mail

È certamente condivisibile la preoccupazione delineata in relazione alla **limitata affidabilità** dell'e-mail tradizionale circa l'attribuzione di paternità del messaggio trasmesso e l'integrità di quest'ultimo, cionondimeno non può negarsi che si sia comunque in presenza di un documento elettronicamente firmato, seppur in forma non certificata.



Per tale motivo **è demandato al giudice il compito di valutare** nel caso concreto se l'e-mail prodotta in giudizio possa considerarsi attendibile, anche in relazione agli altri elementi probatori acquisiti.



Digital Forensics



104

Posta elettronica certificata (PEC)

La disciplina delle modalità di erogazione e utilizzo del servizio di **PEC** è contenuta nel DPR n. 68/2005 e nel DM 2 novembre 2005.

I soggetti del sistema PEC sono:

- Il mittente, che si avvale del servizio per l'invio di documenti prodotti attraverso l'utilizzo di strumenti informatici;
- Il destinatario, al quale viene recapitato il messaggio;
- Il gestore, soggetto pubblico o privato, che fornisce il servizio di PEC;
- Il DigitPA, l'amministrazione che cura l'iscrizione dei gestori in un apposito elenco pubblico e che svolge attività di vigilanza sul sistema.



Digital Forensics



105

Posta elettronica certificata (PEC)

- Il mittente e il destinatario che intendono fruire del servizio di PEC si avvalgono dei gestori inclusi nell'elenco pubblico tenuto dal DigitPA (art. 14, co. 1, DPR n. 68).
- I gestori devono possedere una serie di condizioni per poter essere accreditati presso tale elenco (art. 14, co. 3 e ss. DPR n. 68), di carattere soggettivo (forma societaria, requisiti di onorabilità, ecc.) e oggettivo (affidabilità organizzativa e tecnica, personale adeguato, certificazione di qualità, polizza assicurativa, ecc.).



Digital Forensics



106

Posta elettronica certificata (PEC)

Le principali caratteristiche della PEC:



Integrità del messaggio

L'utilizzo dei servizi di posta certificata avviene esclusivamente utilizzando protocolli sicuri, in modo da evitare qualsiasi manomissione del messaggio e degli eventuali allegati da parte di terzi. Infatti tutte le comunicazioni sono protette perché **crittografate** e **firmate digitalmente**.

Certificazione dell'invio

Quando si invia un messaggio da una casella PEC si riceve dal proprio provider di posta certificata una ricevuta di accettazione che attesta la **data** e **l'ora** della spedizione ed i destinatari.

Certificazione della consegna

Il provider del destinatario invia al mittente la ricevuta di consegna. Anche in questo caso si tratta di un messaggio e-mail che **attesta la consegna** con l'indicazione della data e ora e il contenuto consegnato



Digital Forensics



107

Posta elettronica certificata (PEC)



La Posta Elettronica Certificata (PEC) è l'equivalente informatico della "classica" **raccomandata con ricevuta di ritorno**.

Si tratta sostanzialmente di un messaggio di posta elettronica di cui vengono fornite le ricevute, aventi **valore legale**, di avvenuta spedizione e di avvenuta o mancata consegna.

Per poter usufruire delle funzionalità di PEC, non è sufficiente una casella di posta normale, ma bisogna acquisire una casella (di PEC appunto) da un gestore di **Posta Elettronica Certificata autorizzato**



Digital Forensics



108

Valore legale della PEC

Alla PEC è riconosciuto pieno valore legale e le **ricevute** possono essere usate come **prove dell'invio**, della ricezione ed anche del contenuto del messaggio inviato. Le principali informazioni riguardanti la trasmissione e la consegna vengono conservate per 30 mesi dal gestore e sono anch'esse opponibili a terzi.

Le ricevute hanno valore legale **solo se sia il mittente che il destinatario comunicano tramite email PEC.**

Il testo esplicativo redatto dal **CNIPA** è esplicito in proposito:

“ Da una casella di PEC è possibile inviare un messaggio certificato a chiunque abbia una casella di posta elettronica?

Sì, ma nel solo caso in cui il destinatario sia dotato di una casella di Posta Elettronica certificata, sia l'invio che la ricezione di un messaggio di PEC hanno valore legale. ”



Digital Forensics



109

Valore legale della PEC



Il mittente è garantito (ricevuta come prova)

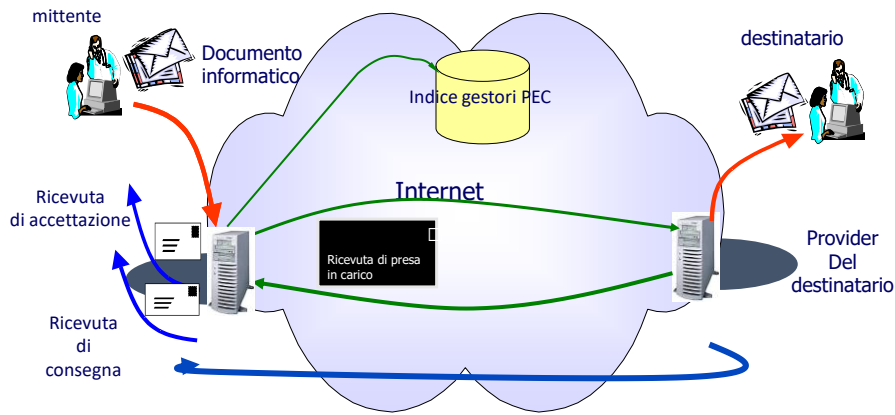
Il destinatario ha degli obblighi (non ripudiabilità, ecc.)



Digital Forensics



110



Digital Forensics



111

Tool Specializzati: Email forensics

- AccessData's Forensic Toolkit (**FTK**)
- ProDiscover Basic
- FINALeMAIL
- Sawmill-GroupWise
- DBXtract
- Fookes Aid4Mail and MailBag Assistant
- Paraben E-Mail Examiner
- Ontrack Easy Recovery EmailRepair
- R-Tools R-Mail



Digital Forensics



112

Credits/Link

<http://www.dirittodellinformatica.it/ict/valore-giuridico-delle-mail.html> - Dott.ssa Ilaria Mercuri

«La posta elettronica» Capitolo 7 – Computer Forensics e Indagini Digitali – Manuale tecnico-giuridico e casi pratici – Costabile, Mazzaraco, Cajani – Experta edizioni



Digital Forensics



113

Business Email Compromise



Falso IBAN << accesso IMAP >>



11/04/2020



114

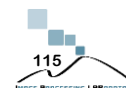
Caratteristiche dell'attacco

Truffa dei **bonifici devianti in modo fraudolento verso falsi IBAN** a fronte di mail modificate ad hoc da criminali che si sono insinuati nelle caselle di posta elettronica al fine di spiare le comunicazioni tra cliente e fornitore.

Queste truffe bancarie prendono il nome di “**Man in The Mail**” (variante di “Man in The Middle”), “**Business Email Compromise**”, o ancora “Bogus Invoice Scheme” o “Invoice Modification Scheme”.



115

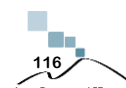


Caratteristiche dell'attacco

- Le **modalità** con le quali i criminali ottengono l'accesso ai dati riservati delle aziende, in particolare alla loro posta elettronica e alle loro fatture, **cambiano di volta in volta**, così come la tecnica utilizzata per alterare i codici IBAN all'interno delle fatture originali, così da deviare il bonifico verso conti spesso poco tracciabili o dai quali, in ogni caso, i fondi verranno rimossi non appena arrivati



116



Modalità dell'attacco

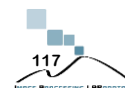
- Attacco alla casella di posta tramite **phishing, brute force o utilizzo di credenziali riciclate** su più account provenienti dai vari «leak» disponibili in rete, con conseguente monitoraggio della mailbox anche tramite forward delle mail



- Installazione di **trojan e spyware** sui PC o smartphone di chi esegue o riceve i bonifici o comunica con clienti e fornitori



117

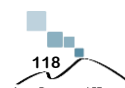


Modalità dell'attacco

- Attività di **social engineering** finalizzato a identificare le relazioni tra membri della società, così da poter inviare false mail con richieste di bonifici fraudolenti verso IBAN creati ad hoc
- **Registrazione di domini simili a quello della vittima o dei suoi fornitori**, utilizzando poi le caselle di posta per perpetrare la truffa dei trasferimenti deviati verso IBAN di terzi



118

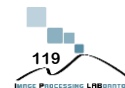


Modalità dell'attacco tramite IMAP

- Pur essendo il **phishing** il **metodo principale** con cui avviene da anni il “Man In The Mail” dei falsi IBAN, negli ultimi anni sono stati rilevati diversi casi perpetrati attraverso **l'accesso diretto alla casella di posta tramite protocollo IMAP** (una volta ottenute le credenziali di accesso)



119



Modalità dell'attacco tramite IMAP

- La compromissione delle mail **tramite IMAP** permette, utilizzando la funzione di **upload e modifica dei messaggi**, di **modificare testo o allegati direttamente nella casella di posta del destinatario** prima che questi ne scarichi il contenuto, rendendo così superfluo l'invio di posta da canali fraudolenti (**l'account del mittente non viene compromesso**)
- Una precauzione spesso presa dai truffatori è quella d'impostare un **inoltro su una casella esterna**, così da evitare che i proprietari possano leggere le email inviate dai reali clienti o fornitori prima della modifica



120



Strategie difensive

- La **miglior difesa è la formazione del personale** che deve essere ben consapevole che se un fornitore richiede un **repentino cambiamento del conto IBAN** sul quale versare il saldo indicato in fattura, è necessario eseguire adeguate verifiche tramite telefonate, fax o PEC
- Le email false, nel **caso di registrazione di domini simili a quello della vittima o dei suoi fornitori**, avranno una forte somiglianza con quelle originali, sia negli indirizzi sia nel contenuto, ma **spesso uno sguardo attento è sufficiente per capire se si tratta di un messaggio prodotto da terzi a fini di truffa e raggiro**



121

Strategie difensive

- Ben diverso è il **caso del falso IBAN tramite IMAP**, soprattutto se l'attacco viene portato al massimo della sofisticatezza, poiché **la mail originale viene alterata in minima parte (sostituzione dell'allegato a parte)**. Soprattutto in questo caso è il cambio di IBAN che deve mettere in guardia il destinatario

sostituzione #0



Giovanni Marotta <giorgion19@outlook.com> (giorgion19@outlook.com)

6/4/2020 17:34

A giorni.marotta@virgilio.it

Rispondi Rispondi a tutti Inoltra Elimina Altro ▼

1 allegato ▼ Vista Scarica Salva in Drive



21/04/2020



122

Digital Forensics

- Dal punto di vista dell'informatica forense, è essenziale **gestire l'acquisizione delle prove ricavabili dalle email**, dai file PDF con fatture, ordini o contabili bancarie, in modo tale da poter dimostrare l'eventuale estraneità dell'azienda vittima alla truffa
- **E' necessario acquisire correttamente le email in modo che contengano il formato RFC822**, tramite tecniche certificate a valore legale (**apposizione di hash e marche temporali alle mail acquisite**)

To: Giovanni Marotta <gionnoig@gmail.com>
 From: Giovanni Marotta <giovanni-marotta@tiscali.it>
 Subject: pdf modificato da Thunderbird
 Message-ID: <054479f2-7106-d58e-36f2-04b270023641@tiscali.it>
 Date: Thu, 6 Feb 2020 11:28:27 +0100
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101
 Thunderbird/68.4.2
 MIME-Version: 1.0
 Content-Type: multipart/mixed;
 boundary="-----A184E8FD171CF18D5EC22990"



123

Digital Forensics

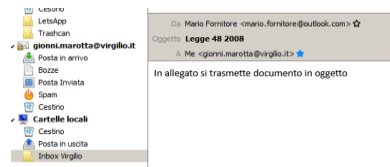
- Potrebbe essere necessario, nel caso del Falso IBAN tramite IMAP, **richiedere al provider del mittente l'originale del messaggio** (tramite Message-ID) per poter constatare la modifica presso il destinatario dal raffronto dei due sorgenti
- Allo stesso modo, eventuali telefonate, messaggi, SMS o comunicazioni con i presunti devono essere cristallizzate e preservate in modo da poterle portare come prova dell'attività di **Phishing o Social Engineering**



124

Esempi di attacco tramite IMAP /1

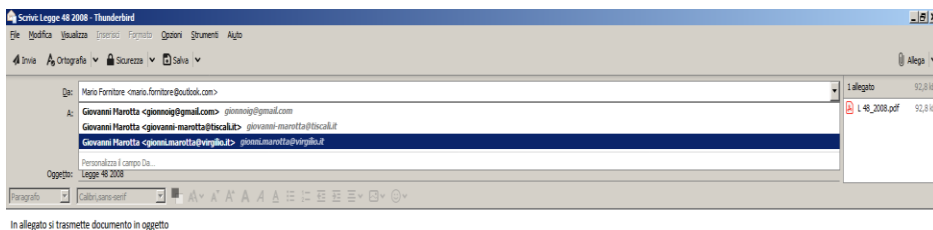
- In questi esempi supporremo di avere **accesso alla mailbox del destinatario** ed operare con degli strumenti che sfruttino le **potenzialità di modifica della posta in arrivo fornite dal protocollo IMAP**
- **Si può intercettare, ad es. su Thunderbird, la mail in arrivo con la vera fattura per spostarla in una cartella off-line locale:** quest'azione causerà la sua rimozione dalla mailbox del destinatario sul server
- Si può anche procedere alla **copia della mail su file .eml locale**, ma in questo caso bisogna rimuovere manualmente la mail dalla mailbox del



125

Esempi di attacco tramite IMAP /1

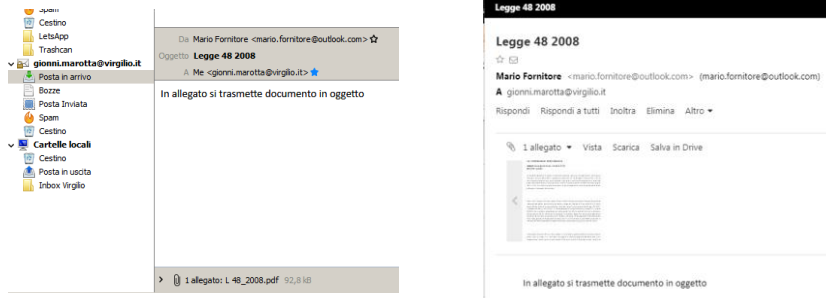
- Dalla cartella locale si può **creare una bozza su cui modificare il campo Da:** con un indirizzo mittente con nome ed **username simile o uguale al mittente** (la bozza viene creata a partire da una mailbox diversa da quella del mittente!) e **sostituire l'allegato** con quello modificato



126

Esempi di attacco tramite IMAP /1

- **Dalla cartella delle Bozze si può trasferire infine la mail modificata di nuovo alla Inbox del destinatario** (quest'azione mi permetterà di caricare di nuovo la mail in IMAP sulla mailbox del destinatario sul server)



127



Esempi di attacco tramite IMAP /1

- Questa modalità di attacco non richiede interventi molto più sofisticati, benché macchinosi, di quelli permessi da un client di posta elettronica quale Thunderbird
- **Benché ingannevole la visualizzazione della mail «fake» in formato RFC822 può rivelare alcuni indizi sulla manomissione (in giallo)**
- **Il From: è stato manomesso ma non viene evidenziato**
- **Anche l'orario è diverso da quello di partenza, ma il destinatario non può saperlo se non attraverso una indagine dei metadati IMAP attraverso strumenti specializzati**

```
X-Mozilla-Keys:
FCC: imap://gionnoig%40gmail.com/imap.gmail.com/[Gmail]/Posta inviata
X-Identity-Key: id1
X-Account-Key: account1
From: Mario Fornitore <mario.fornitore@outlook.com>
Subject: Legge 48 2008
To: "gionni.marotta@virgilio.it" <gionni.marotta@virgilio.it>
Message-ID:
<AM0PR04MB4244400D17C82A93F058E1A1D4C30@AM0PR04MB4244.eurprd04.prod.outlook>
Date: Tue, 7 Apr 2020 12:29:23 +0200
X-Mozilla-Draft-Info: internal/draft; vcard=0; receipt=0; DSN=0; uencode=0;
attachementreminder=0; deliveryformat=4
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101
Thunderbird/68.6.0
```

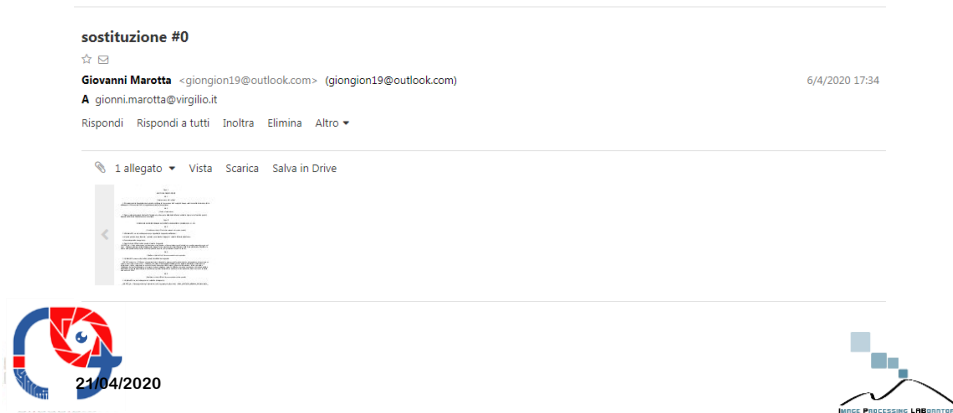


128



Esempi di attacco tramite IMAP /2

- **Mail con allegato sostituito:** la mail, così come visualizzata dal server, non rivela alcuna manomissione



131

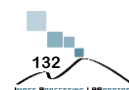
Esempi di attacco tramite IMAP /2

- In questa modalità di attacco **anche la visualizzazione della mail «fake» in formato RFC822 non è in grado di rivelare molti indizi sulla manomissione**, perché di fatto è stato sostituito solo l'allegato, non noto, a priori, dal ricevente
- **Tutte le intestazioni sono quelle del messaggio originale, compresi i controlli di sicurezza DKIM, SPF, DMARC che risultano «passati»**
- A parte una richiesta al provider del mittente del messaggio originale tramite il suo Message-ID, si deve **procedere alla ricerca di alcuni elementi non ricavabili dal sorgente RFC822**

```
X-Mozilla-Keys: nonjunk
Return-Path: <giongion19@outlook.com>
Delivered-To: gionni.marotta@virgilio.it
Received: from dcd-13 ([10.103.10.30])
  by dcbakend-01.iol.local with LMTP id cN62LPIL14/3QcA8zqZMg
  for <gionni.marotta@virgilio.it>; Mon, 06 Apr 2020 17:34:17 +0200
Received: from dcp-17.iol.local ([10.103.10.30])
  by dcd-13 with LMTP id YCmkLPIL16tQQAyAP63Q
  ; Mon, 06 Apr 2020 17:34:17 +0200
Received: from libero.it ([10.103.10.30])
  by dcp-17.iol.local with LMTP id aL3EEPIL16tQQAyAP63Q
  ; Mon, 06 Apr 2020 17:34:17 +0200
Received: from EUR04-VI1-obe.outbound.protection.outlook.com ([40.92.75.108])
  by smtp-30.iol.local with ESMTP
  id LTRJAI0okyOrLTIRjUEF; Mon, 06 Apr 2020 17:34:17 +0200
X-IOL-DMARC: pass con il dominio outlook.com
X-IOL-DKIM: pass con il dominio d=outlook.com
X-IOL-SPF: pass con l'IP 40.92.75.108:outlook.com
X-IOL-SEC: _SPFOK_DKIMOK_DMARCOK
```

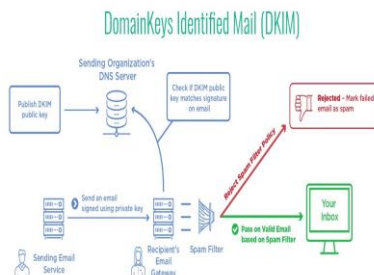


132



Esempi di attacco tramite IMAP /2

- In primo luogo si può installare ed attivare il **DKIM Verifier** su Thunderbird
- Il DKIM è una firma digitale del messaggio apposta dal server SMTP del mittente, utilizzando una chiave crittografica privata e viene utilizzato in ricezione dai filtri anti-spam del server di ricezione. Installare il DKIM Verifier comporta una **forzata del controllo del DKIM da parte del client di posta elettronica** che permette di individuare manipolazioni della mail in locale dopo la sua ricezione



133

Esempi di attacco tramite IMAP /2

- Poiché il **DKIM Verifier** agisce solo se il server SMTP appone il DKIM, a volte non si è in grado di ottenere riscontri utili
- C'è allora la possibilità di visualizzare il **numero d'ordine di ricezione della mail** che il server IMAP appone quando carica una mail, ma non viene visualizzato se non richiesto. Il numero d'ordine è un **metadato IMAP (UID)** che può essere facilmente visualizzato in Thunderbird
- Dal numero d'ordine di ricezione si può evincere (come dalla figura) che **l'ordine di ricezione non coincide con quello per data**, il che può essere un'evidenza del fatto che le mail evidenziate dalle frecce siano state poste off-line, probabilmente manipolate, e successivamente ricaricate sul server IMAP che ne ha aggiornato il numero d'ordine (rispetto a quello originale) ma non la data

Data	Ordine ricezione
02/06/2020, 13:11	1172
02/06/2020, 13:22	1171
01/06/2020, 17:13	1169
01/06/2020, 17:19	1168
01/06/2020, 12:31	1166
01/06/2020, 12:33	1163



134

Esempi di attacco tramite IMAP /2

- Un ultimo metadato IMAP che può tornare utile all'indagine è l'**INTERNAL DATE** che il server IMAP appone alla mail, per indicare la data e l'ora di caricamento nel server (=ricezione). Questo metadato differisce dalla data e dall'ora della mail, in quanto quest'ultimo viene, nella stragrande maggioranza dei casi, preso dal campo contenuto nella **ENVELOPE**, che invece viene creato dal primo server SMTP di transito della mail durante l'invio
- ***Se la mail è stata eliminata dal server IMAP e successivamente ricaricata, il metadato INTERNAL DATE sarà diverso da quello contenuto nella ENVELOPE a dimostrazione che la mail è stata posta per qualche tempo off-line***



135

Esempi di attacco tramite IMAP /2

- Ricavare l'INTERNAL DATE è possibile tramite il **comando «curl»**

```
C:\Users\Utente>curl --url "imaps://in.virgilio.it/INBOX" --user
«gionni.marotta@virgilio.it:mypassword" --request "fetch 1:* (UID FLAGS
INTERNALDATE ENVELOPE)"
```

- I metadati della seguente mail presentano **un valore di INTERNAL DATE decisamente successivo a quello contenuto nella ENVELOPE** (al netto della timezone della data), a riprova della sua possibile manipolazione:

```
* 14 FETCH (UID 1166 FLAGS (\Seen) INTERNALDATE "01-Jun-2020 15:22:34 +0200" ENV
ELOPE ("Mon, 1 Jun 2020 10:31:11 +0000" "mail con allegato sostituito" (("Giovann
ni Marotta" NIL "giongion19" "outlook.com"))) (("Giovanni Marotta" NIL "giongion1
9" "outlook.com"))) (("Giovanni Marotta" NIL "giongion19" "outlook.com"))) ("gion
ni.marotta@virgilio.it" NIL "gionni.marotta" "virgilio.it") NIL NIL NIL "<AMOP
R04MB42449C58B4097E5609F3388DD48A0@AM0PR04MB4244.eurprd04.prod.outlook.com>"))
```



136



Prof. Sebastiano Battiato
Dipartimento di Matematica e Informatica
University of Catania, Italy
www.dmi.unict.it/~battiato
battiato@dm.unict.it



Image Processing LAB – iplab.dmi.unict.it
iCTlab - www.ictlab.srl

Digital Forensics

