Ordine Avvocati di Torino, Commissione Scientifica
In Collaborazione con Fondazione Fulvio Croce

LE INVESTIGAZIONI DIGITALI

GLI STRUMENTI DI CUI PUÒ DISPORRE IL DIFENSORE E IL LORO UTILIZZO

Paolo Dal Checco, Consulente Informatico Forense
Forenser Srl

Forenser
Digital Investigations

CHI SONO

- Laurea e Ph.D. in Informatica, Università di Torino
- Consulente Informatico Forense (10+ anni, 2k+ casi)
- CTP, CTU, Esperto, Perito del Giudice, CT del PM, Ausiliario di PG
- Collaborazioni con UniTO (Docente a Contratto corso Sicurezza Informatica @SUISS), UniGE (Master), UniMI e PoliMI (Master e Corsi di Perfezionamento)
- Interessi in mobile forensics, OSINT, cryptocurrency forensics, web forensics…. in sostanza tutti gli aspetti della digital forensics

ARGOMENTI DELLA SECONDA PARTE DEL CORSO

- La cristallizzazione forense di pagine web, profili, post e commenti su Social Network finalizzata alla produzione nel processo;
- La verifica dell'integrità e la produzione in giudizio di messaggi di posta elettronica o PEC;
- Acquisizione forense di dati da Cloud (Google Drive, iCloud, Dropbox, OneDrive…).

CRISTALLIZZAZIONE FORENSE DI RISORSE WEB

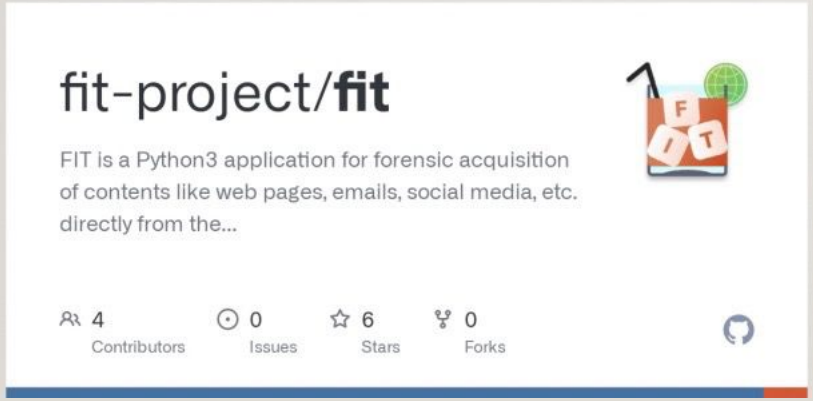
- Frequente richiesta di acquisire in maniera forense pagine web, siti, profili, post, commenti, video, etc..
- Facile alterare in locale prove acquisite online come pagine web [**DEMO**]
- Più difficile rispettare i 3 princìpi derivati dalla Legge 48/2008:
  - **Non alterare l'originale**; facile, ma si può correre il rischio (es. click su «mi piace» o visita profilo Linkedin);
  - **Copia identica all'originale**: difficile, troppi parametri variabili, necessario delineare perimetro (questioni legate a DNS, SSL, HTTP, HTML, traffico, video, audio, html5/ajax, etc…)
  - **Copia non modificabile e databile nel tempo**: facile, una volta salvata la copia, hash e marca temporale.

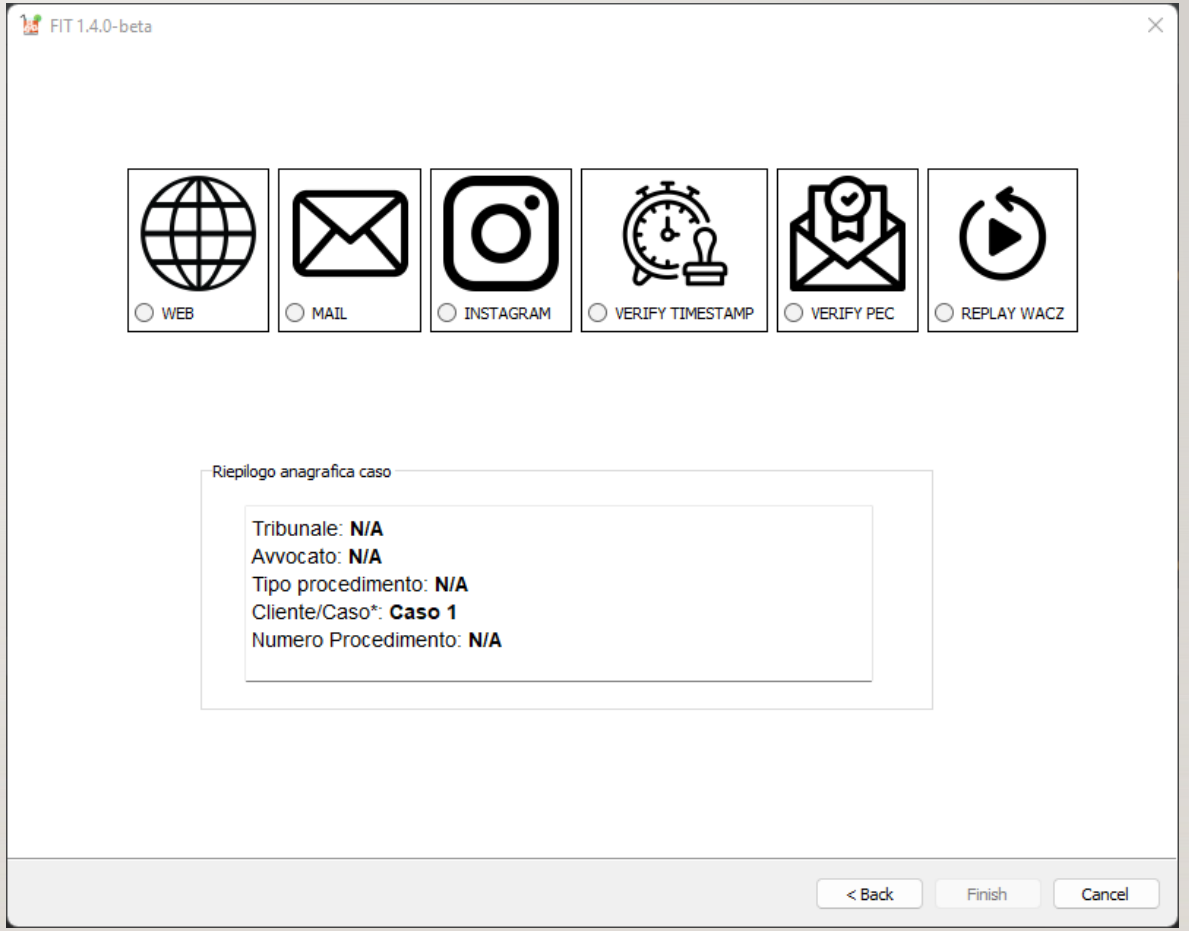
RISORSE GRATUITE

- Esistono risorse gratuite, online, oggettive ma limitate o con caveat:
  - Web Archive (http://web.archive.org/)
  - Perma.cc (https://perma.cc/)
  - Archive.is (https://archive.is/)
  - Conifer (https://conifer.rhizome.org/)
  - Archiveweb.page (https://archiveweb.page/)
  - Macchina Virtuale (https://www.dalchecco.it/forensic-acquisition-of-websites-and-webpages-osdfcon-2021/)

RISORSE GRATUITE

- FIT – Freezing Internet Tool
- Software da utilizzare/installare in locale per acquisizione forense risorse web
- Work in Progress, Python3, Open Source
- Basato su un progetto del Dott. Fabio Zito con collaborazione dei soci ONIF Dott. Nanni Bassetti, Ing Ugo Lopez, Dott. Andrea Lazzarotto + Studenti UniBA Francesca Policelli, Domenico Palmisano, Niccolò Santoro e Gino Laric





RISORSE COMMERCIALI

- Esistono tool o servizi commerciali
  - Legaleye
  - Cliens Prova Digitale
  - Kopjra Web Forensics [**DEMO**]
  - CRIO
  - FAW
  - X1 Social Discovery

TAKEOUT

- Quando l'acquisizione riguarda un profilo social network (es. Facebook, Instagram, Linkedin, Twitter, etc…) esiste una soluzione ottimale: takeout
- Necessario autenticarsi sul profilo (quindi no profili di terzi)
- Richiede a volte ore/giorni
- Fornisce non solo contenuti ma anche indirizzi IP, user agent, marca/modello dispositivi connessi
- Contiene anche chat/comunicazioni tra profili/utenti

POSTA ELETTRONICA: ACQUISIZIONE/PRODUZIONE

- No stampa/pdf
- Facile alterare in locale prove acquisite online come messaggi di posta [**DEMO**]
- Se possibile, salvare messaggio integrale (RFC822) come EML/TXT o MSG (Outlook)
- L'ideale, per l'acquisizione, è estrapolare copia forense/export integrale:
  - FEC (Forensic Email Collector)
  - IMAP Downloader di SecurCube
  - Thunderbird/Outlook
  - **Takeout** (es. Gmail)
- Hash/Marca temporale (possibile utilizzare PEC per invio Mail o Hash)

POSTA ELETTRONICA: VALIDAZIONE

- I messaggi in formato sorgente possono contenere l'indirizzo IP del mittente
- Il miglior metodo di validazione è quello di verificare la firma DKIM [**DEMO**]
- Alternative: verificare i metadati IMAP (visibili solo fino a che la mail rimane nella mailbox o acquisibili tramite tool d'informatica forense)
- Per la validazione, varie possibilità:
  - https://mxtoolbox.com/EmailHeaders.aspx
  - Thunderbird DKIM Verifier (plugin)

PEC: VALIDAZIONE

- Una PEC non è altro che un «normale» messaggio di posta elettronica firmato con la chiave privata del certificatore, che firma l'accettazione e la consegna
- La validazione di un messaggio PEC quindi è semplice: bisogna verificare se la firma del certificatore è valida, è sufficiente aprire il messaggio con un programma di posta
- Alternativa «geek/nerd»:
  - Verifica: openssl smime -in msg.eml –verify
  - Estrai certificato: cat PEC/PEC\ Forenser\ 2023.eml | openssl smime -pk7out | openssl pkcs7 -print_certs | openssl x509 -text -noout
- Si può fare solo con messaggio salvato integralmente (EML/MSG) e non pdf(daticert.xml/postacert.eml
- Firma non valida?
  - Modifiche al contenuto;
  - Certificato scaduto → portare l'orario del PC al periodo di validità.

PEC: VALIDAZIONE

- Possibilità di richiedere i file di log, contenenti mittente, destinatario, oggetto e conferma di consegna/ricezione
- Alcuni provider forniscono pagina di download dei log direttamente sul portale

CLOUD

- Acquisizione forense di dati da Cloud (Google Drive, iCloud, Dropbox, OneDrive…)
- Il cloud si può spesso vedere come un sito web su un server esterno
- Acquisizione possibile come per un sito web (accesso al cloud via web, acquisizione con tool)
- Anche per il cloud, ove possibile utilizzate il Takeout;
- Hash/Marca temporale (possibile utilizzare PEC per invio Mail o Hash)

CONCLUSIONI

- **Acquisizione risorse web:** facile per singola pagina non autenticata, più difficile per siti/pagine dietro autenticazione/dinamiche/video
- **Acquisizione e validazione mail/PEC**: salvare come minimo mail integrale, se possibile intera mailbox con tool forense o exoprt completo, verifica integrità via DKIM o firma certificato PEC
- **Cloud**: ricondurlo a una acquisizione web