Security Summit Milano 2026

Associazione **Digital Forensics Alumni**

Digital forensics per la gestione degli incidenti

19 marzo 2026

Digital Forensics Alumni

L’attività di analisi

Andrea Ferraresso

Dalla teoria alla pratica

Digital Forensics Alumni

→ In questo intervento **non parliamo di normative**.

→ Entriamo nel dettaglio “pratico” della questione.

→ Senza per troppi tecnicismi (nb: ci saranno semplificazioni volute).

Un’integrazione possibile?

Digital Forensics Alumni

→ **Incident response**

- contenere
- eliminare
- ripristinare.

→ **Digital forensics**

- preservare
- ricostruire
- attribuire
- documentare.

Il “classico” conflitto

Digital Forensics Alumni

→ **Business continuity** (ripristinare subito)

vs

→ **Digital forensics** (fermare tutto per analizzare).

(e in genere vince il primo… 😭)

Una storia vera

Digital Forensics Alumni

→ Ipotizziamo di aver subito un **attacco informatico** (incidente informatico intenzionale).

→ Già definirlo potrebbe non essere facile.

→ Perché è **più facile definire gli effetti che le cause**.

Apriamo una piccola parentesi…

Una situazione ricorrente

Digital Forensics Alumni

→ I nostri utenti/clienti ci dicono «Il vostro **sito web** è **irraggiungibile**».

→ Questa informazione come ci arriva? Per quale canale?

→ Ecco il punto: abbiamo creato un **sistema per ricevere** questo tipo di **segnalazioni** in tempo reale o quasi? E perché arrivino alla persona giusta?

Monitorare

Digital Forensics Alumni

→ Prima ancora di capire cosa succede, dobbiamo chiederci: chi lo sa per primo? Se lo scopriamo dai social o dal call center, abbiamo un **problema di monitoraggio**.

→ Questo vale anche per altri tipi di incidenti informatici, ovviamente.

Chiusa parentesi.

«Il vostro sito web è irraggiungibile»

Digital Forensics Alumni

→ Questa è un’**informazione sugli effetti**.

→ Non è una diagnosi. Non è una causa. Non è ancora un incidente informatico.

→ Abbiamo almeno tre possibili scenari (completamente diversi).

Tre possibili scenari (tra i tanti)

Digital Forensics Alumni

→ **A. Malfunzionamento hardware**, es. guasto del server fisico oppure assenza di alimentazione ecc.

→ **B. Malfunzionamento applicativo**, es. nel web server o in uno degli altri componenti che servono a rendere fruibile il nostro sito web (v. aggiornamento non riuscito…).

→ **C. Attacco DDoS**, in cui le risorse del nostro server vengono consumate da troppe richieste “inutili”.

Agire con metodo

Digital Forensics Alumni

→ La **segnalazione** deve arrivare **contemporaneamente** a chi deve “riparare” e a chi deve “analizzare”.

→ Se arriva solo ai sistemisti, il rischio di sovrascrivere prove vitali (log, dump di memoria…) per la fretta di ripartire è alto (sicuramente saranno sotto pressione per ripartire in fretta!).

Torniamo ai tre scenari

Digital Forensics Alumni

→ **A. Malfunzionamento hardware.** Es. se il server è morto, la forensics si concentra sull'integrità degli hard disk.

→ **B. Malfunzionamento applicativo.** Qui bisogna capire se si tratta di un aggiornamento fallito o un database corrotto… La forensics ci serve per escludere che il "malfunzionamento" sia in realtà un sabotaggio o l'esito di una web shell.

→ **C. Attacco DDoS.** Qui ci serve un'analisi dei log in tempo reale o quasi. Dobbiamo capire se è veramente una botnet.

Possibili azioni

Digital Forensics Alumni

→ **Acquisizione “live”** (prima di spegnere o riavviare cancellando la memoria volatile).

→ **Analisi dei log e “timeline”**, ovvero significa “unire” i log del web server con quelli del firewall, ad esempio. Se vediamo 10 mondo richieste al secondo da IP sparsi nel globo, è un DDoS. Se vediamo una singola query SQL anomala che ha mandato in crash il DB, è una SQL injection. ecc.

Possibili risultati

Digital Forensics Alumni

→ Se era un **guasto**, siamo certi che non ci sono stati accessi abusivi e abbiamo attivato il disaster recovery.

→ Se era un **errore applicativo**, abbiamo identificato il bug (o quantomeno che era un bug).

→ Se era un **attacco**, abbiamo i log integri per capire da dove sono entrati, cosa hanno visto…, dati utili per la relazione tecnica (che servirà poi per la compliance).

Dagli effetti alla causa

Digital Forensics Alumni

→ Da che **cosa è successo**

→ a **come è stato possibile**.

→ Per evitare un loop di reinfezione (es. quando un malware si “nasconde” in una stampante multifunzione).

.

Immancabile citazione dell’IA

Digital Forensics Alumni

Al di là di agenti di monitoraggio che sappiano fare “micro-dump” dei dati ecc. ...

→ Come possiamo sfruttare l’IA per aiutarci in questi compiti?

→ Ad esempio, potremmo dare in pasto i file di log all’IA generativa, ma la privacy?

→ (C’è molta confusione tra IA e IA generativa).

IA “classica” (ML/statistica)

Digital Forensics Alumni

→ In generale l’IA “classica” lavora bene su grandi volumi strutturati o almeno semi-strutturati.

→ E in ogni caso i dati prima puliti, resi omogenei ecc.

→ L’IA generativa può aiutare, ad esempio, a generare il codice Python/Go/Rust…. per leggere un file di log con 20 milioni di righe, estrarre i vari dati utili, inserirli in un database e creare anche le query SQL per trovare gli IP maggiormente coinvolti in un attacco DDoS.

Altri svantaggi dell’uso dell’IA generativa

Digital Forensics Alumni

→ Privacy (già detto).

→ Costi (possiamo “bypassare” l’interfaccia chat di questi sistemi e collegarci direttamente ai server, aumentando le nostre possibilità. Ovviamente aumentano anche i costi.

→ La sua natura intrinseca la porta a generare risposte che possono essere sensibilmente diverse a fronte di richieste identiche.

Un altro “meta” utilizzo dell’IA generativa

Digital Forensics Alumni

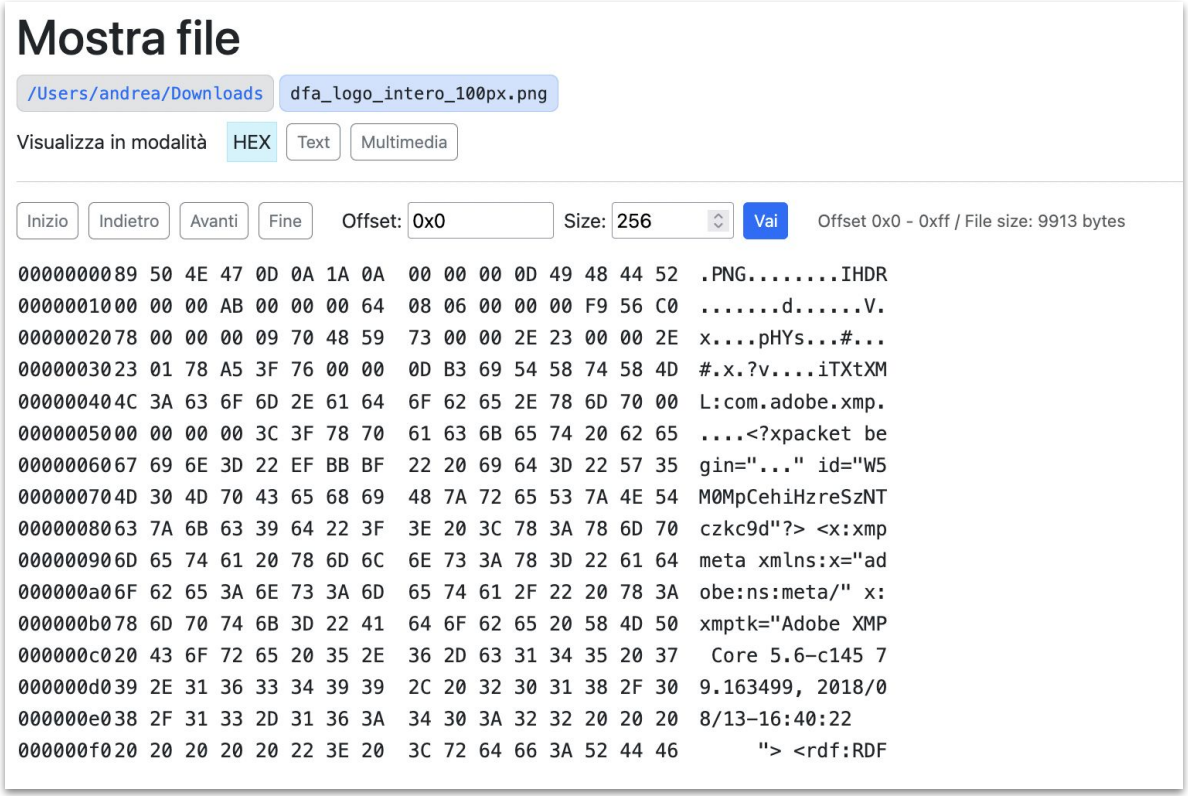
Posto che è sicuramente possibile usare l’IA generativa per creare degli script personalizzati per leggere log ecc.

→ In generale, è possibile crearsi dei tool per l’analisi forense che aiutino a integrare digital forensics e gestione degli incidenti?

Allo stato attuale la risposta è: dipende. Pensare di creare un tool di forensics con un prompt mi sembra utopistico. Sono però riuscito a ottenere buoni risultato “un passo alla volta”.

Esempio: editor binario/esadecimale

Digital Forensics Alumni



Esempio: visualizzatore rapido

Digital Forensics Alumni

Mostra file

/Users/andrea/Downloads | dfa_logo_intero_100px.png

Visualizza in modalità [Hex] [Text] MULTIMEDIA

Chiave	Valore
Name	dfa_logo_intero_100px.png
Path	/Users/andrea/Downloads/dfa_logo_intero_100px.png
Size	9.68 KB
Mime Type	image/png

Esempio: estrattore di metadati

Digital Forensics Alumni

`exif_full.go`

Go

```go
package imagemeta

import "encoding/binary"

func parseTIFFFull(tiff []byte) (*EXIFMetadata, error) {
    if len(tiff) < 8 {
        return nil, ErrInvalidTIFF
    }
```

Esempio: elaboratore di file di log

Digital Forensics Alumni

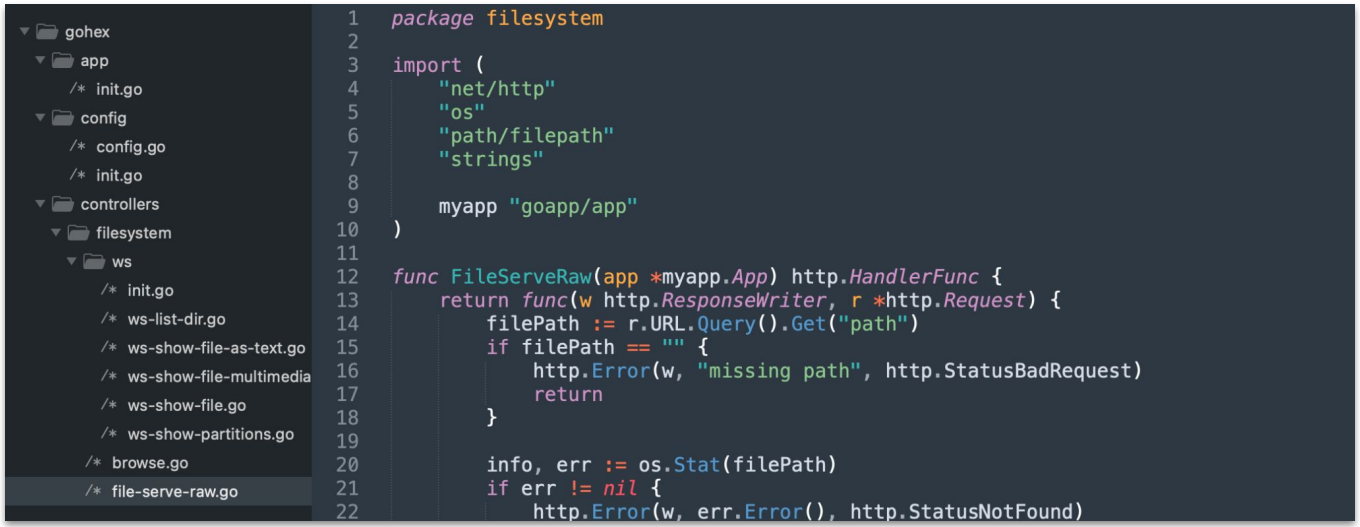
JSON

```
{
  "name": "generic_web_log",
  "description": "Formato personalizzato",
  "format_type": "regex",
  "line_pattern": "^(?P<ip>\\S+) - (?P<user>\\S+) \\[(?P<timestamp>[^\\]]+)\\] \"(?P<meth
  "time_format": "02/Jan/2006:15:04:05 -0700",
  "fields": [
    { "name": "ip", "type": "string", "indexed": true, "nullable": false },
    { "name": "user", "type": "string", "indexed": true, "nullable": true, "null_values":
    { "name": "timestamp", "type": "datetime", "indexed": true, "nullable": false },
    { "name": "method", "type": "string", "indexed": true, "nullable": false },
    { "name": "path", "type": "string", "indexed": true, "nullable": false },
    { "name": "protocol", "type": "string", "indexed": false, "nullable": true },
    { "name": "status", "type": "int", "indexed": true, "nullable": false },
    { "name": "bytes", "type": "int", "indexed": false, "nullable": true, "null_values":
  ],
  "options": {
    "ignore_empty_lines": true,
    "store_raw_line": true,
    "stop_on_error": false
  }
}
```

Ma non c’è la bacchetta magica

Digital Forensics Alumni

Il funzionamento del codice così prodotto va poi verificato e spesso integrato in codice già esistente…



Digital Forensics Alumni

Grazie per l’attenzione