Linux Day

26 – ottobre - 2024

Le Comunicazioni Nascoste

Tecniche di Occultamento Dati

Francesco Ressa

LINUX DAY 2024

Cosa faremo oggi ?!

Nasconderemo un messaggio di testo in un'immagine.

Utilizzeremo la tecnica “Analisi del rumore” per fare steganalisi.

Inseriremo un testo nascosto in un file audio usando la steganografia su spettrogramma.

Nasconderemo un file dentro più contenitori.

Inseriremo un'esca in un file steganografato utilizzando dati finti. (Steganografia negabile)

Inseriremo un malware all'interno di un file, evitando il rilevamento da parte dell’antivirus.

Steganografia

<stéganos> “nascosto”

<gràfein> “scrittura”

Il punto forte

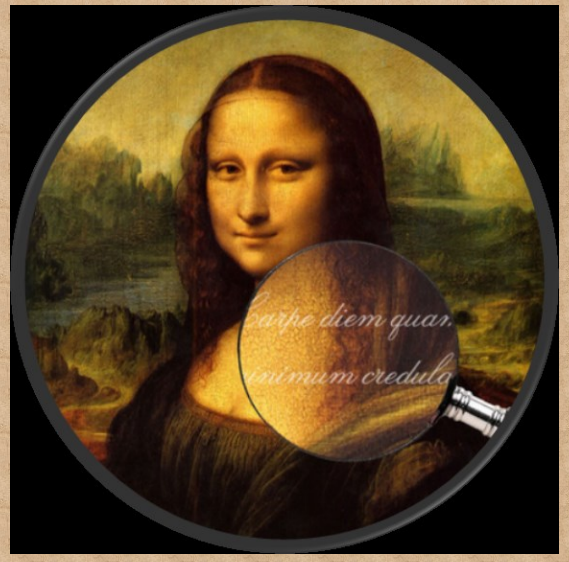
La Steganografia mira a far sembrare tutto assolutamente normale.

Steganografia classica

È l’arte di nascondere messaggi o informazioni all'interno di supporti ordinari.

Steganografia digitale

È la tecnica usata per nascondere un messaggio (o un file) all’interno di uno o più file (contenitori)

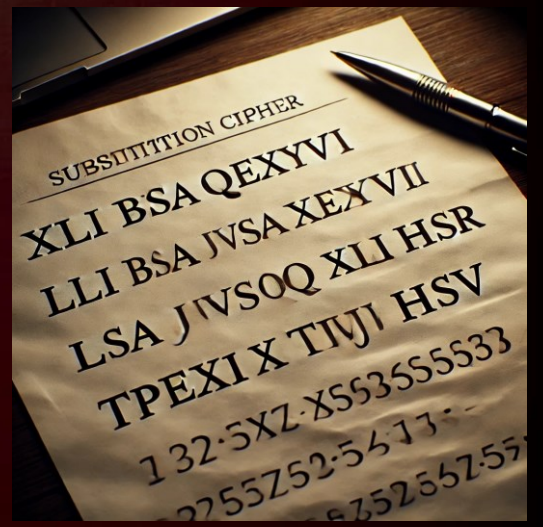


Le prime Steganografie della storia 499 A.C.

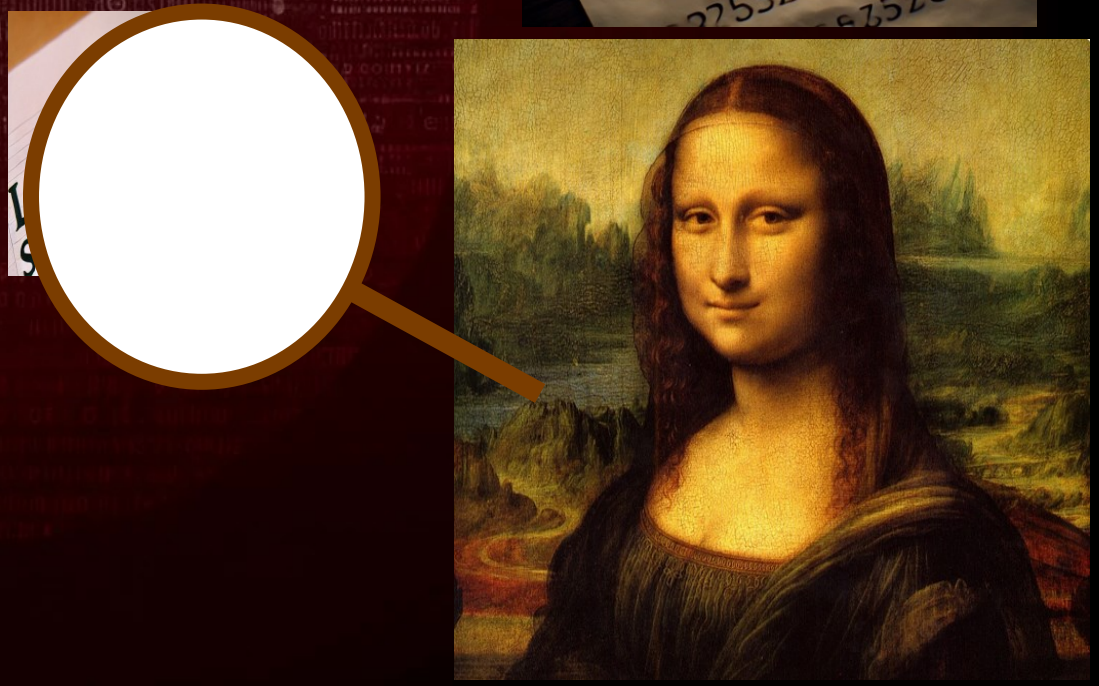
La Steganografia nella seconda guerra mondiale

Steganografia vs Crittografia

Crittografia: il messaggio è visibile, ma non comprensibile.



Steganografia: il messaggio è completamente invisibile, nascosto all'interno di un altro contenuto.



Perché BMP a 24 bit?

I file BMP non comprimono l'immagine, quindi:

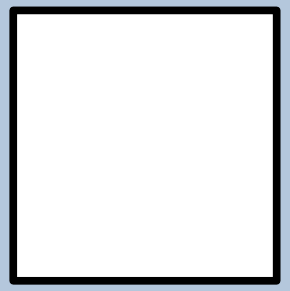
non si hanno perdite di qualità

si ha più spazio per incorporare dati nascosti senza destare sospetti

si riduce il rischio di rilevamento

è facile modificare i bit meno significativi LSB (Least Significant Bit) senza alterare la qualità dell'immagine.

Perché BMP a 24 bit?



PIXEL

R	G	B
8 bit	8 bit	8 bit

$2^{8=}$ 256

ARANCIONE =

R	G	B
255	165	0

Perché BMP a 24 bit?

R 255 → 11111111

G 165 → 10100101

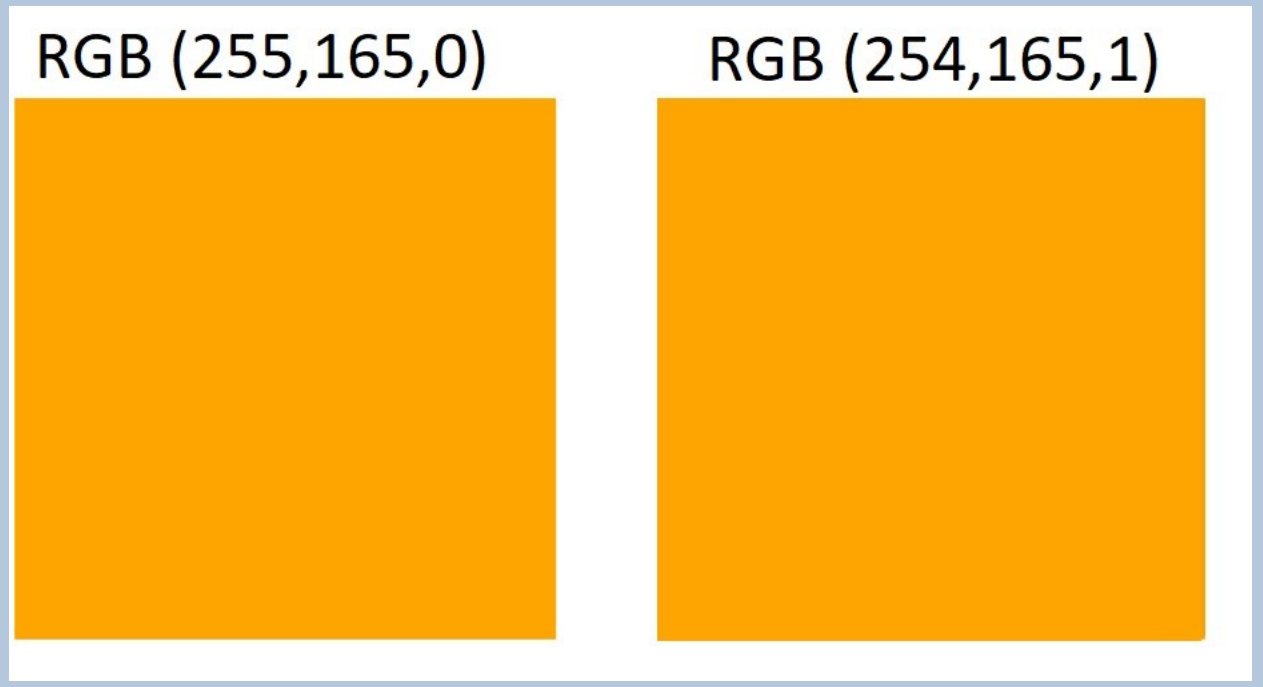
B 0 → 00000000

R 254 → 11111110

G 165 → 10100101

B 1 → 00000001

3 = 011 (binario)



Steganalisi

L'obiettivo della steganalisi è identificare la presenza di un messaggio nascosto all'interno di un mezzo o file, senza necessariamente decodificarne il contenuto.

Analisi del Rumore e dei bit LSB (Least Significant bit)

Confrontando l'immagine sospetta con una versione originale senza dati nascosti, è possibile esaminare le variazioni di rumore e la distribuzione dei bit che potrebbero indicare la presenza di steganografia.

Utilizzo di IA

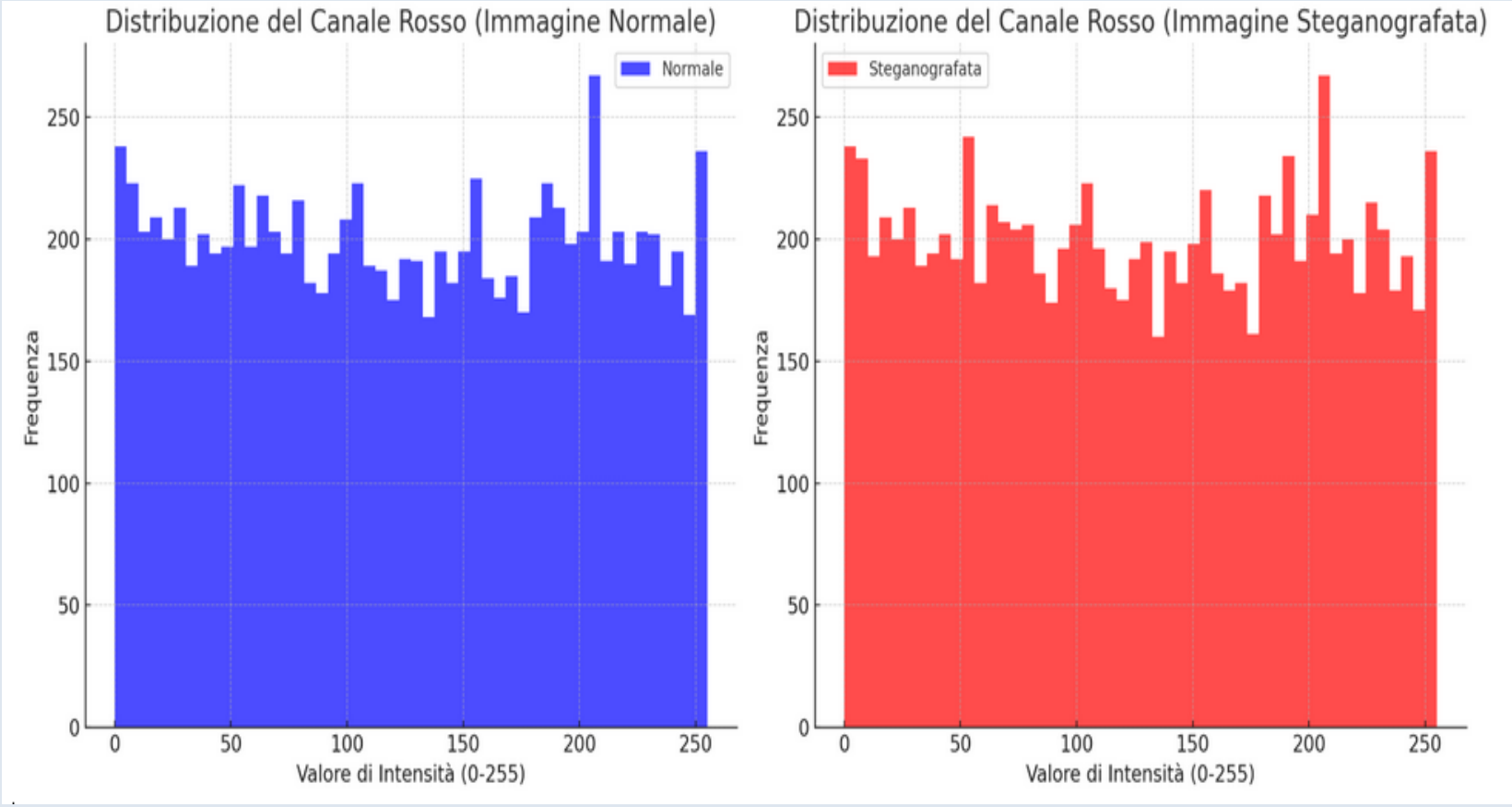
Impiego di algoritmi di apprendimento automatico per rilevare informazioni nascoste all'interno di file digitali, come immagini, video o audio.

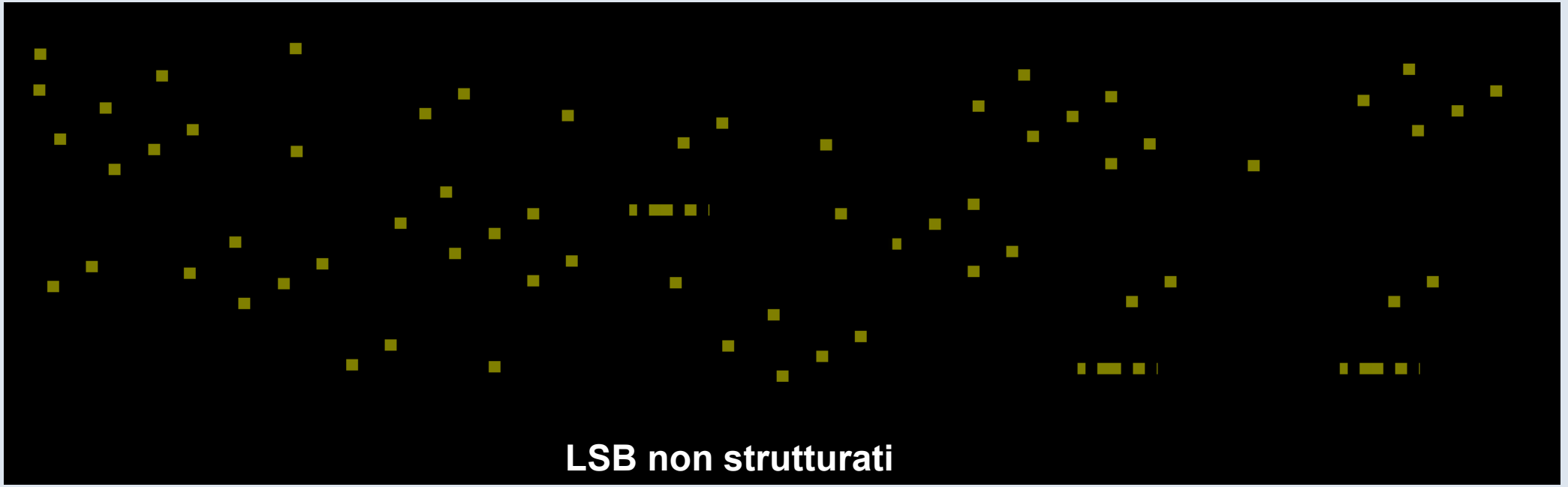
Steganalisi

L'obiettivo della steganalisi è identificare la presenza di un messaggio nascosto all'interno di un mezzo o file, senza necessariamente decodificarne il contenuto.

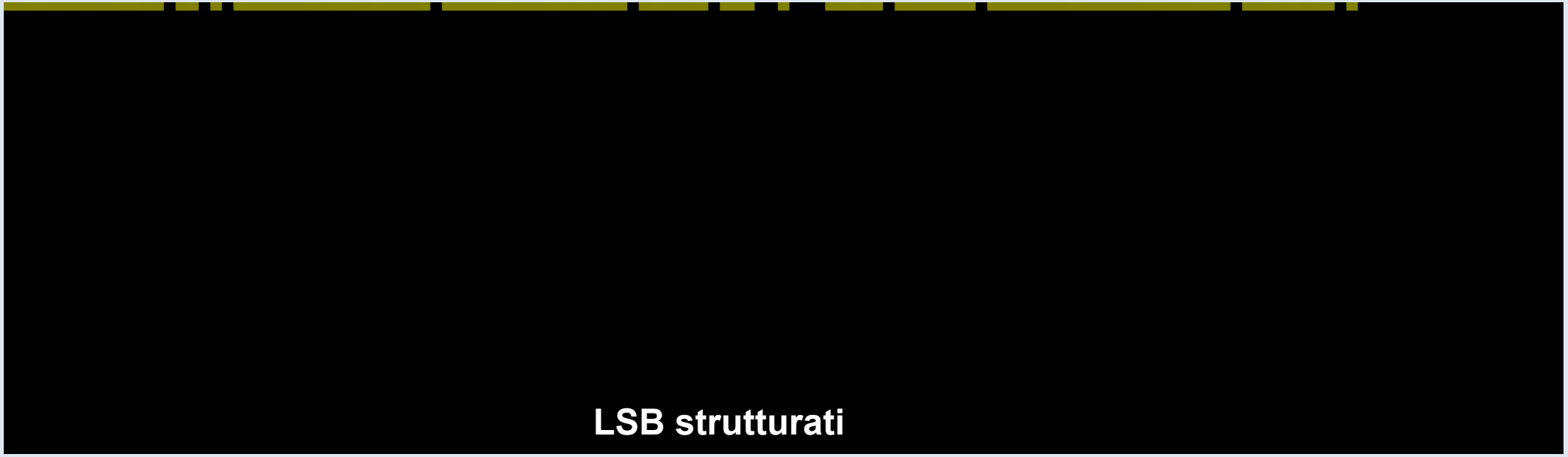
Steganalisi Statistica

In un'immagine digitale, i valori di colore dei pixel sono di solito distribuiti in modo naturale. Se un'immagine è stata alterata per nascondere informazioni, la distribuzione statistica potrebbe risultare anomala.





LSB non strutturati



LSB strutturati

Persistenza

È la capacità del contenuto di sopravvivere (quindi di permanere) alle modifiche del file contenitore.

Fotoritocco leggero:

Il contenuto può sopravvivere se le modifiche non sono troppo invasive.

Compressione:

JPEG: Alta probabilità di perdita del contenuto nascosto.

PNG, ZIP: Il contenuto sopravvive.

Invio via email o cloud (Google Drive, MEGA):

Se il file non viene modificato o compresso, il contenuto rimane.

Persistenza

È la capacità del contenuto di sopravvivere (quindi di permanere) alle modifiche del file contenitore.

Messaggistica (WhatsApp, Telegram):

Foto/video compressi: Il contenuto si perde.

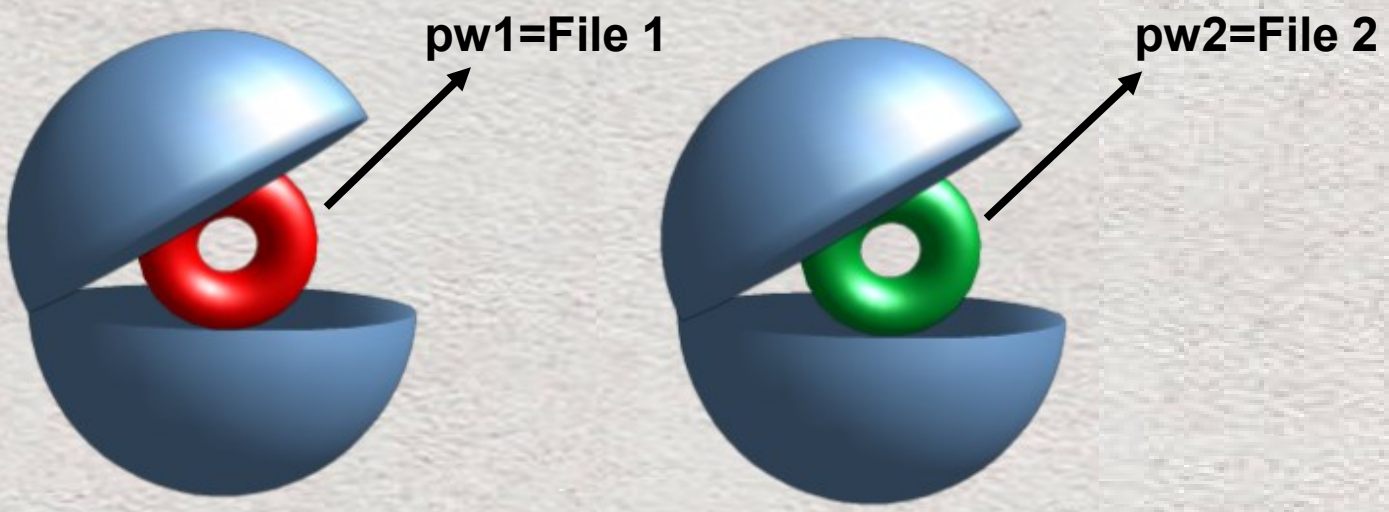
Documento: Il contenuto sopravvive.

Trasferimento tramite software di assistenza remota (Anydesk, TeamViewer):

Il file inviato direttamente mantiene il contenuto nascosto.

Steganografia «Negabile»

è un metodo per nascondere il vero contenuto mostrando qualcosa di finto se qualcuno ci obbliga a farlo. Si crea un contenuto falso convincente, così l'attaccante pensa che sia tutto e smette di cercare.



EICAR

European Institute for Computer Antivirus Research

https://www.eicar.org/download-anti-malware-testfile/

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Impiego della Steganografia

Legale

Comunicazioni Sicure.

Conservazione di Documenti Sensibili.

Trasmissione Sicura di Dati Riservati.

Leggermente meno legale

Distribuzione di Malware.

Commercio di Informazioni Rubate.

Distribuzione di Contenuti Illegali.

Spionaggio Industriale.


GRAZIE