



ITIS
LEONARDO DA VINCI

Via Toscana, 10 - 43122 PARMA - Tel 0521266511 - Fax 0521266550 - e-mail itis@itis.prit.it - cf.80007330345 - PRTF010006



CORSO DI **CYBER SECURITY**

Incontro #05 - Mar 26 Nov 24

Prof. Ugolotti 2023-2024

Obiettivi del corso:



OLIMPIADI
ITALIANE DI
CYBERSICUREZZA



CYBER
CHALLENGE.IT

Selezione scolastica
18/01/2025



Preselezione
? Febbraio 2024




Non dimenticate il primo obiettivo...

<https://olicyber.it/materiale>

La Selezione scolastica (18 Gen 2025)

- networking
- Indirizzamento IPv4
- Funzioni ricorsive
- Operatori bitwise
- Calcolo combinatorio
- Probabilità
- Logica



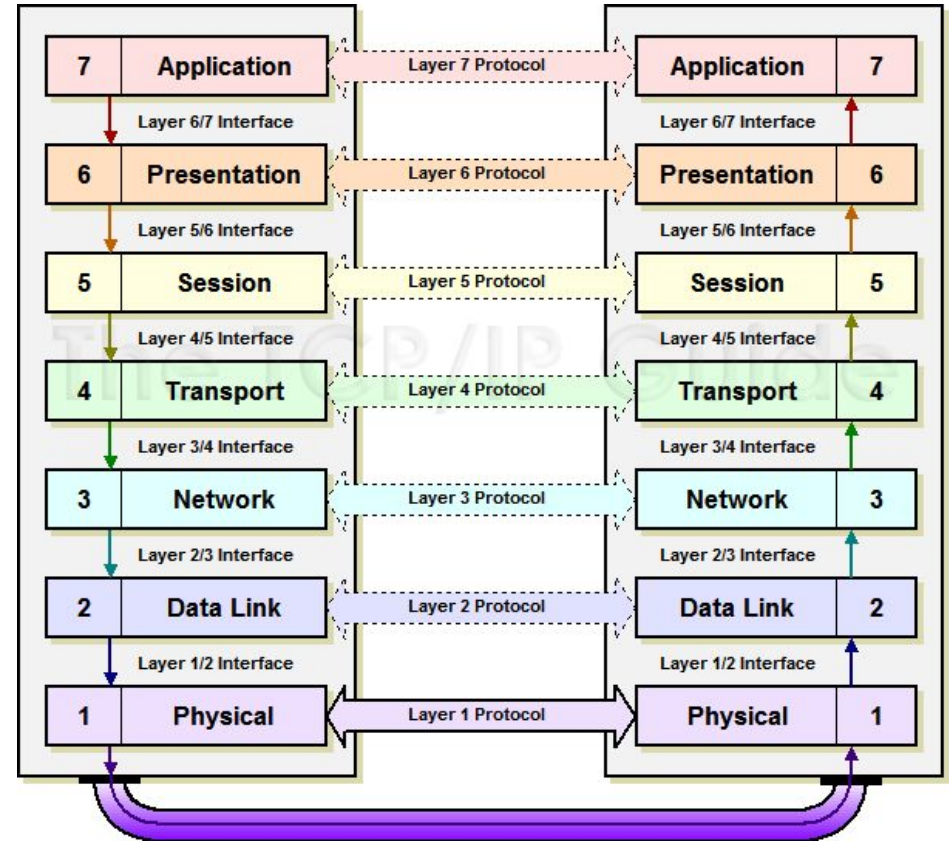
The screenshot shows the Olicyber website interface. At the top, there is a navigation bar with the Olicyber logo (a white horse head on a blue background) and the text 'OLICYBER' and 'CIBER INNOVATION & CERTIFICAZIONE'. To the right of the logo are buttons for 'REGISTRATI' and 'ACCEDI'. Below the navigation bar, the main content area features a red icon of a school building and the heading 'Materiale didattico'. Underneath, there is a paragraph of text: 'In questa pagina trovi puntatori e riferimenti a tutto il materiale didattico disponibile dalle precedenti edizioni del progetto che puoi usare per prepararti alla nuova edizione.' Below this, there are two columns of content. The left column is titled 'Lezioni teoriche' and contains a list of video lessons: 'Lezione di Network Security', 'Lezione di Web Security 1', 'Lezione di Web Security 2', 'Lezione di Cryptography 1', 'Lezione di Cryptography 2', 'Lezione di Software Security 1', 'Lezione di Software Security 2', and 'Lezioni dai Training Camp'. The right column is titled 'Selezione scolastica' and contains a paragraph: 'La selezione scolastica consiste in un breve quiz a risposta multipla con domande relative a logica, matematica, informatica e sicurezza di base. I migliori iscritti di ogni istituto vengono selezionati per partecipare alla successiva selezione territoriale. Esercitati con le precedenti selezioni scolastiche:'. Below this paragraph are three buttons: 'Selezione scolastica 2021', 'Selezione scolastica 2022', and 'Selezione scolastica 2023'. Below these buttons is the text 'Soluzioni commentate:' followed by three buttons: 'Soluzioni commentate selezione scolastica 2021', 'Soluzioni commentate selezione scolastica 2022', and 'Soluzioni commentate selezione scolastica 2023'. At the bottom of the screenshot, there are two more sections: 'Selezione territoriale' and 'Competizione nazionale', each with a brief description of the respective activity.

Cosa faremo Oggi: Misc

1. Fondamentali: modello ISO/OSI e TCP/IP
2. Netcat e PownTools
3. Misc
 - a. Magic Bytes
 - b. Metadati
 - c. Steganografia

L'ultima volta...

- Protocollo: l'insieme di regole che consentono ai due medesimi livelli di comunicare
- Interfaccia: insieme di procedure per la comunicazione tra due livelli adiacenti
-

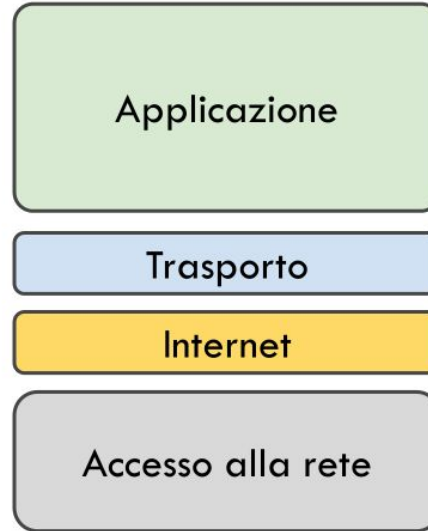


Modello TCP/IP

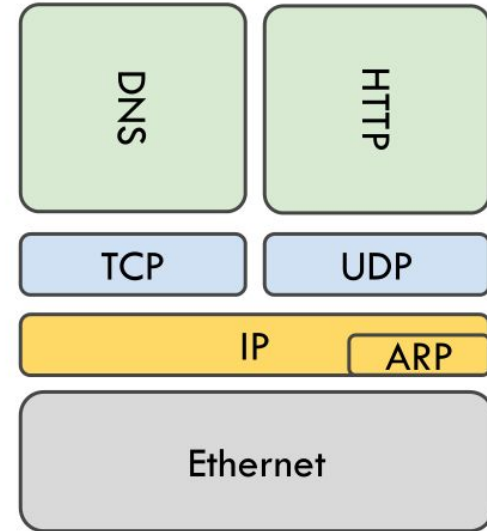
13



ISO/OSI



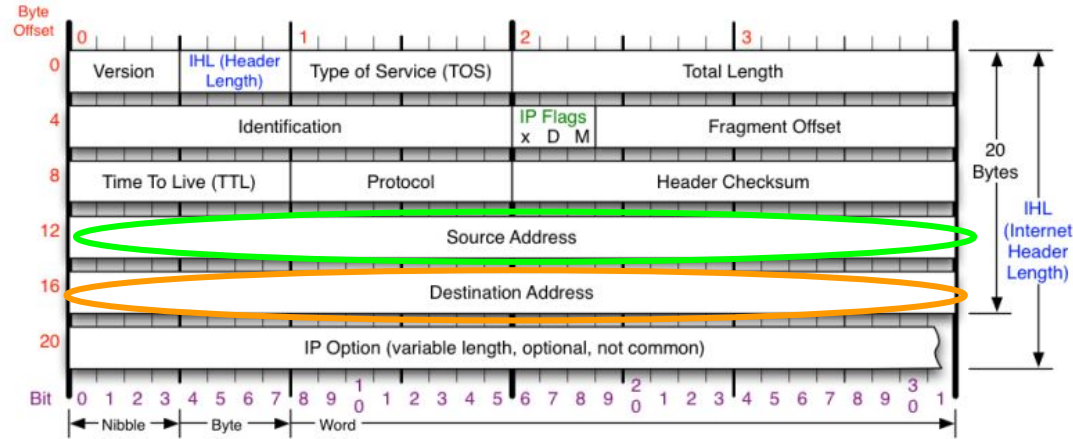
TCP/IP



Protocolli standard

Protocollo IPv4

- Protocollo di L3
- Fornisce l'instradamento su reti a maglia
- L'indirizzamento avviene mediante gli indirizzi IP (32bit) **mittente** e **destinatario**

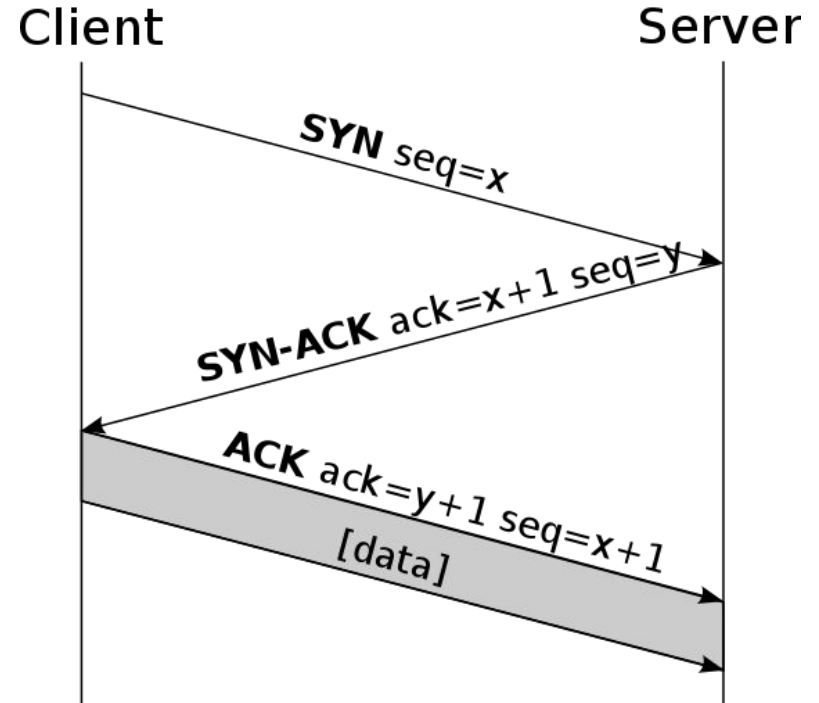
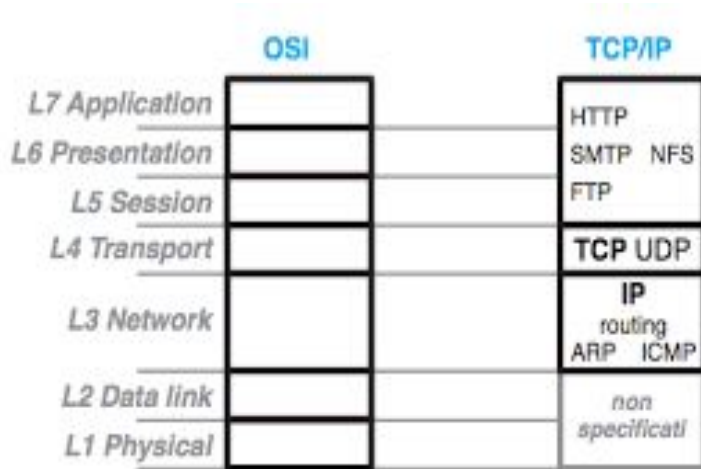


Version	Protocol	Fragment Offset	IP Flags
Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.	IP Protocol ID. Including (but not limited to): 1 ICMP 17 UDP 57 SKIP 2 IGMP 47 GRE 88 EIGRP 6 TCP 50 ESP 89 OSPF 9 IGRP 51 AH 115 L2TP	Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.	x D M x 0x80 reserved (evil bit) D 0x40 Do Not Fragment M 0x20 More Fragments follow
Header Length	Total Length	Header Checksum	RFC 791
Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.	Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.	Checksum of entire IP header	Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Protocollo TCP

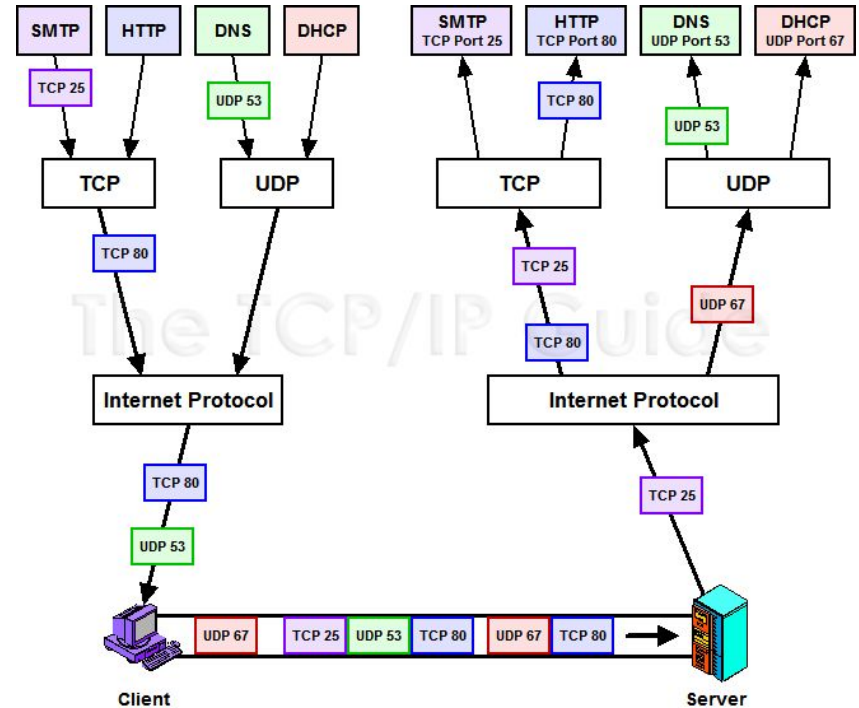
⇒ Protocollo connesso

⇒ Protocollo di L4



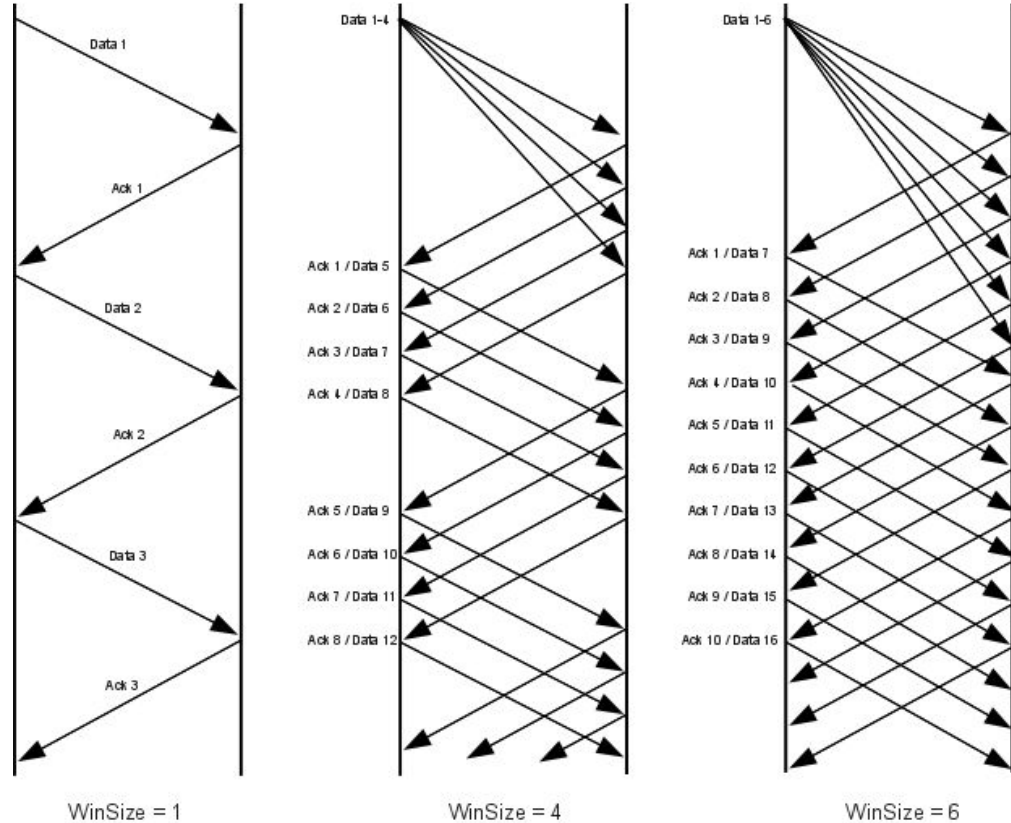
Protocollo TCP

- Protocollo di L4
- Protocollo connesso
- Indirizzamento con Porte fornisce multiplexing tra processi



Protocollo TCP

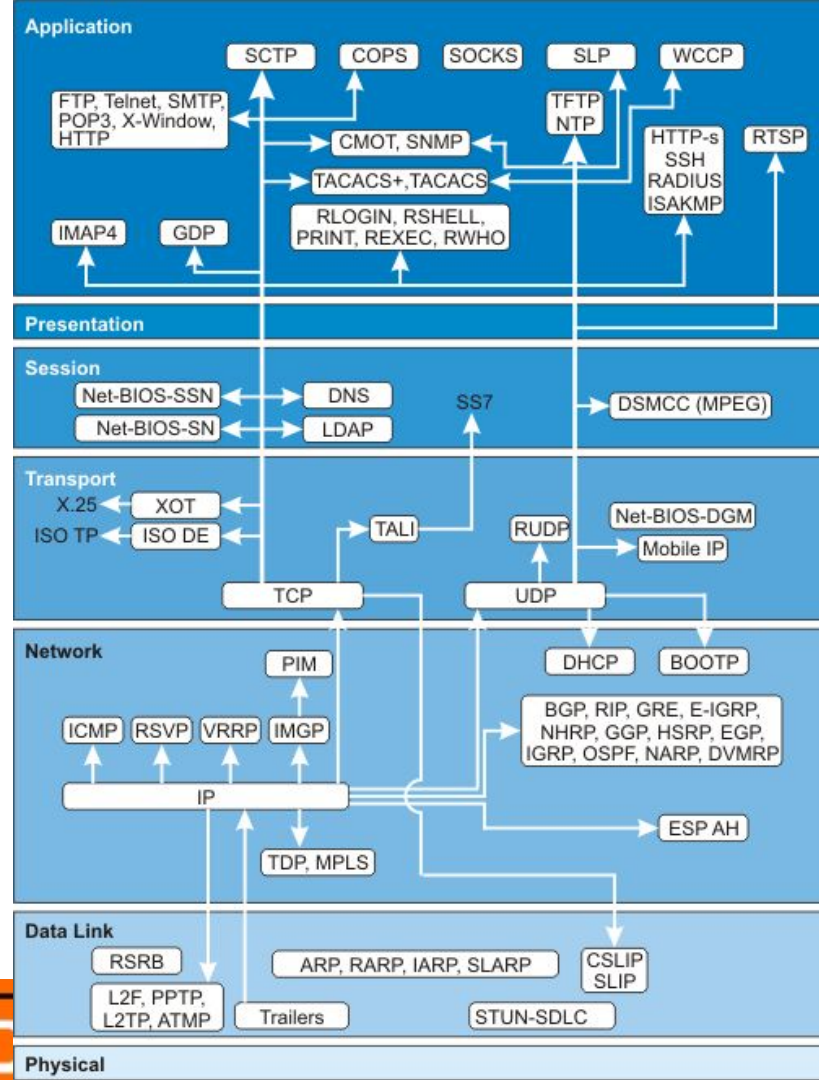
- Protocollo di L4
- Protocollo connesso
- Indirizzamento con Porte fornisce multiplexing tra processi
- Gestione del Flusso



Sliding Windows, bandwidth 6 packets/RTT

Una mappa dei protocolli

...alcuni



Challenge: Misc05

Misc 05 - Servizio tcp

4127 50

misc tcp

@ m1gnus

In aggiunta ai siti web, alcune challenge (tipicamente di categoria crypto o binary) potrebbero richiedere di interagire con servizi remoti da linea di comando, esposti tramite protocollo tcp.

Per questo tipo di challenge ti verrà fornito l'indirizzo del server e la porta su cui il servizio ascolta. Per interagire con tali servizi dovrai usare il comando `nc` del tuo terminale (`netcat`).

Per ottenere la flag di questa challenge è sufficiente collegarsi al servizio remoto da un terminale con il comando:

```
nc tcp.challs.olicyber.it 12210
```

Tools per stabilire una connessione TCP:

- **telnet** (putty)
- Netcat (**nc** / **ncat**)
- python (socket, powntools, ...)

Proviamo ad analizzare lo stream TCP della connessione con WireShark

Challenge: Misc05

Misc 05 - Servizio tcp

4127 50

misc tcp

@ m1gnus

In aggiunta ai siti web, alcune challenge (tipicamente di categoria crypto o binary) potrebbero richiedere di interagire con servizi remoti da linea di comando, esposti tramite protocollo tcp.

Per questo tipo di challenge ti verrà fornito l'indirizzo del server e la porta su cui il servizio ascolta. Per interagire con tali servizi dovrai usare il comando `nc` del tuo terminale (`netcat`).

Per ottenere la flag di questa challenge è sufficiente collegarsi al servizio remoto da un terminale con il comando:

```
nc tcp.challs.olicyber.it 12210
```

```
import socket
```

```
# End point
```

```
HOST = 'tcp.challs.olicyber.it' # Indirizzo IP del server
```

```
PORT = 12210 # Porta del server
```

```
# Dim buffer ricezione
```

```
BUFFER = 4096
```

```
# Creazione del socket
```

```
client_socket = socket.socket(socket.AF_INET,  
socket.SOCK_STREAM)
```

```
try:
```

```
# Connessione al server
```

```
client_socket.connect((HOST, PORT))
```

```
print(f"Connected to {HOST}:{PORT}")
```

```
# Ricezione della risposta
```

```
response = client_socket.recv(BUFFER)
```

```
print(f"Received: {response.decode()}")
```

```
except socket.error as e:
```

```
print(f"Socket error: {e}")
```

```
except Exception as e:
```

```
print(f"An error occurred: {e}")
```

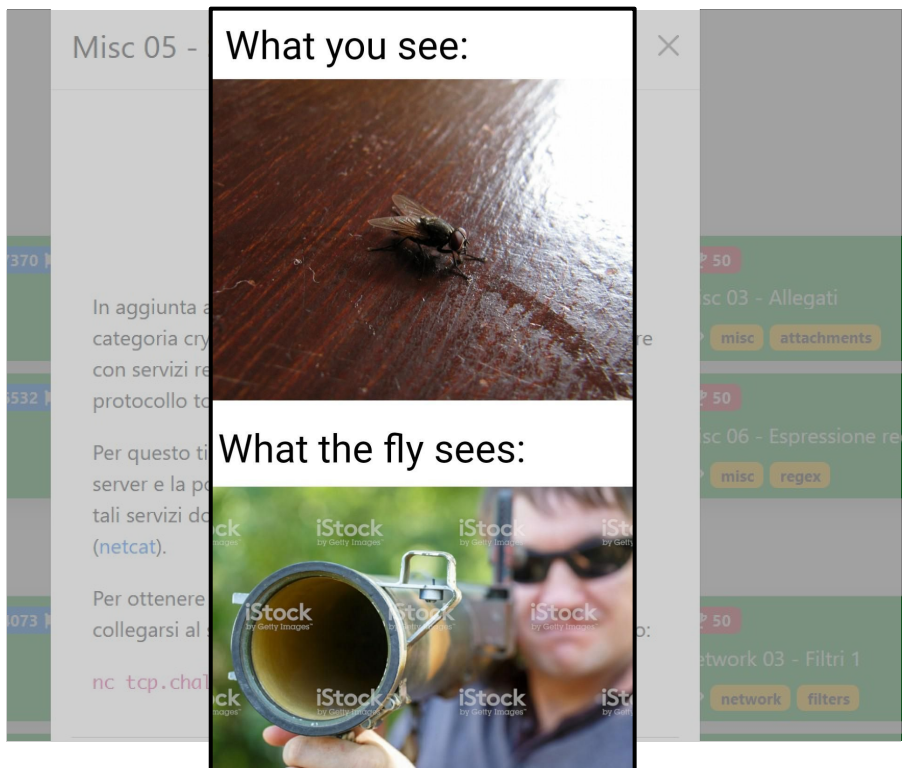
```
finally:
```

```
# Chiusura del socket
```

```
client_socket.close()
```

```
print("Connection closed.")
```


Challenge: Misc05



```
from pwn import remote
```

```
HOST = 'tcp.challs.olicyber.it'
```

```
PORT = 12210
```

```
conn = remote(HOST, PORT)
```

```
result = conn.recvline()
```

```
print(f"Server responded: {result.decode()}")
```

```
conn.close()
```

Provate voi: 2048

Olimpiadi Italiane di Cybersecurity (7/114)

2048

782 496

misc

@ stacchastacch

Status: **up**, last checked: 13 minutes ago

Gioca con me a 2048! In realtà me lo ricordavo diverso...

nc 2048.challs.olicyber.it 10007

Hints

Hint 1 -0pt

flag{...} Submit →

```
from pwn import remote

io = remote("2048.challs.olicyber.it", 10007)
io.recvlines(2) #salta le prime due righe

for _ in range(2048):
    operatore = io.recvuntil(b" ").strip().decode()
    x = int(io.recvuntil(b" ").strip().decode())
    y = int(io.recvuntil(b" ").strip().decode())

    print(_, operatore, x, y)

result = 0
match operatore:
    case "SOMMA":
        result = x+y
    case "DIFFERENZA":
        result = x-y
    case "PRODOTTO":
        result = x*y
    case "DIVISIONE_INTERA":
        result = x//y
    case "POTENZA":
        result = x**y

io.sendline(str(result).encode())

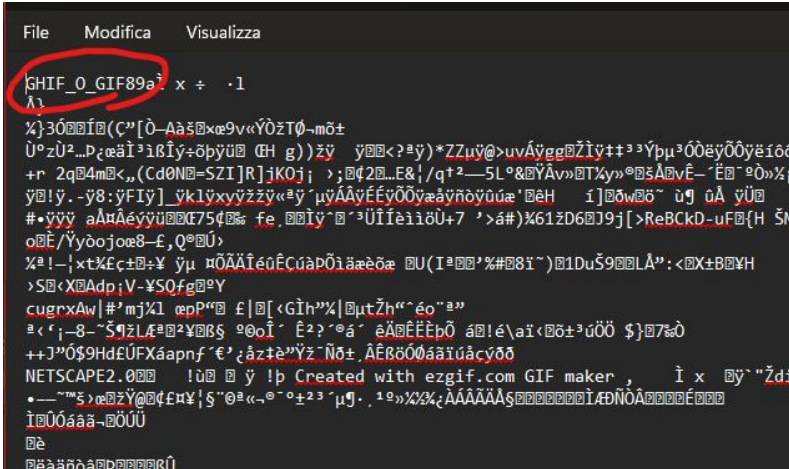
io.interactive()
```

Magic Bytes

→ Cosa definisce il formato di un file?

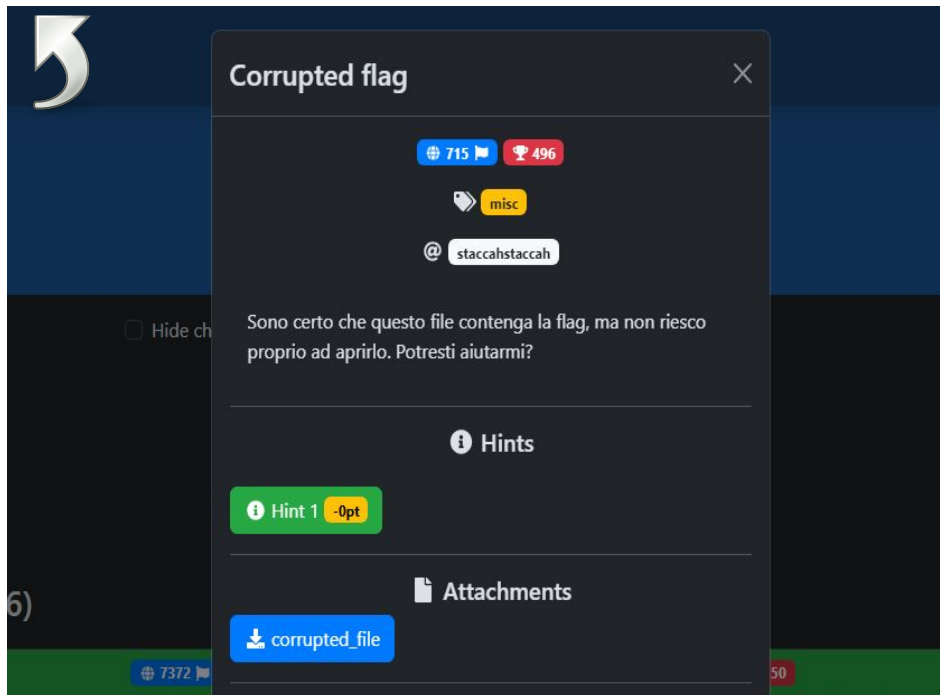
→ La sua estensione? 😞

✓ **I Magic Bytes** 🎉



Magic Bytes (Hex)	Estensione	ASCII	Descrizione
89 50 4E 47 0D 0A 1A 0A	.png	.PNG....	Immagine PNG
FF D8 FF	.jpg,.jpeg	ÿÿÿ	Immagine JPEG
47 49 46 38 39 61	.gif	GIF89a	Immagine GIF (GIF89a)
42 4D	.bmp	BM	Immagine Bitmap
25 50 44 46	.pdf	%PDF	Documento PDF
50 4B 03 04	.zip	PK..	Archivio ZIP
7F 45 4C 46	.elf	.ELF	File eseguibile Linux (ELF)
D0 CF 11 E0 A1 B1 1A E1	.doc, .xls, .ppt	Documenti Office (vecchio formato)
50 4B 03 04	.docx, .xlsx, .pptx	PK..	Documenti Office (nuovo formato, ZIP-based)
25 21 50 53	.ps	%!PS	PostScript
49 49 2A 00	.tif, .tiff	II*.	Immagine TIFF (Intel, LE)
4D 4D 00 2A	.tif, .tiff	MM.*	Immagine TIFF (Motorola, BE)
52 49 46 46	.wav, .avi	RIFF	File multimediale AVI/WAV
00 00 01 BA	.mpg, .mpeg	File video MPEG
1F 8B	.gz	..	Archivio GZIP
49 44 33	.mp3	ID3	File audio MP3
52 61 72 21 1A 07 00	.rar	Rar!...	Archivio RAR

Challenge: Corrupted flag



The screenshot shows a challenge window with the following details:

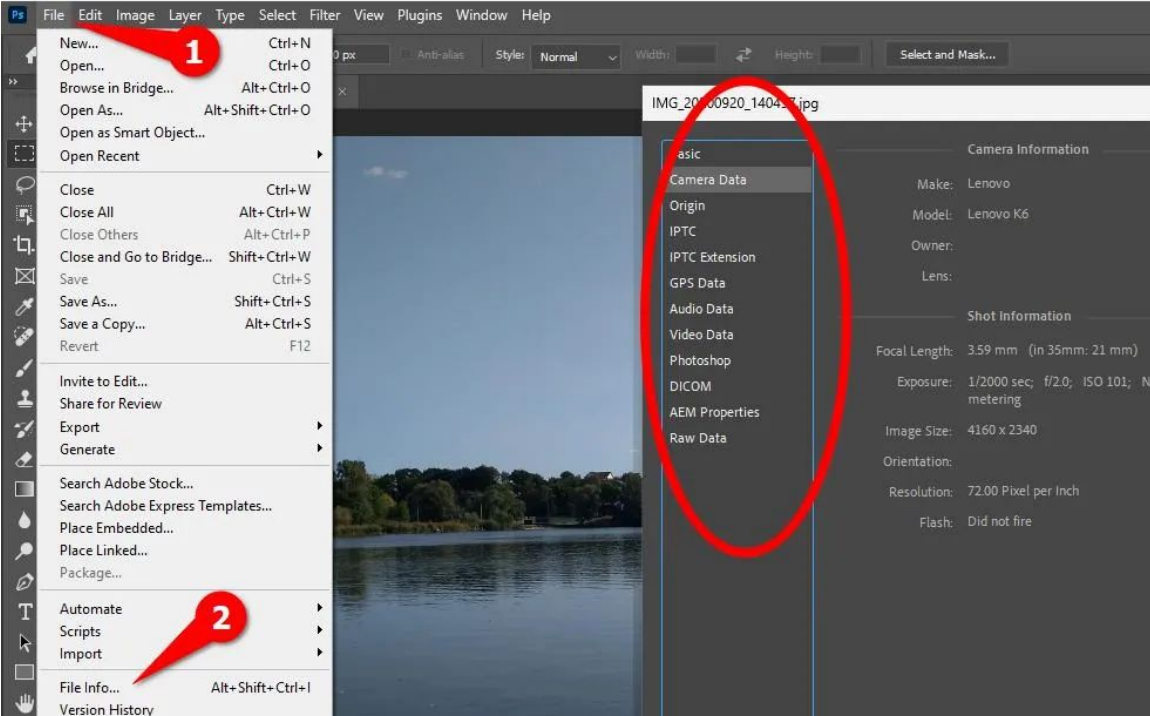
- Title:** Corrupted flag
- Stats:** 715 views, 496 attempts
- Category:** misc
- Author:** @stacchastacch
- Description:** Sono certo che questo file contenga la flag, ma non riesco proprio ad aprirlo. Potresti aiutarmi?
- Hints:** Hint 1 (-opt)
- Attachments:** corrupted_file

Tools utili:

- <https://hexed.it/>
- Editor Esadecimale
 - 010 Editor
 - HxD Hex Editor
 - Ultra Edit
- Linea di comando Linux
 - `xxd image.png | head`
 - `file -i 'nomefile'`
 - `hexedit`

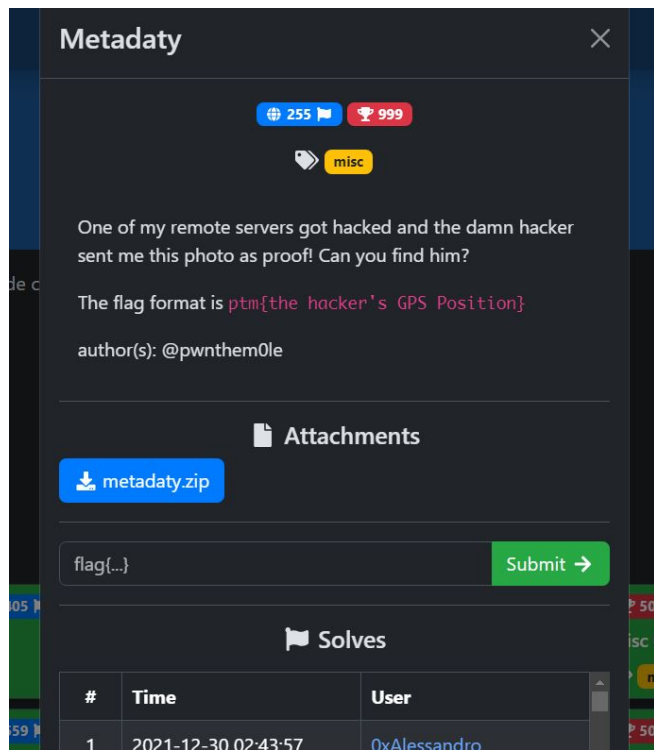
🗡️ “Do you believe in magic?” 🌐

Metadati



IT IS
LEONARDO DA VINCI

Challenge: **Metadaty**



Metadaty

255 999

misc

One of my remote servers got hacked and the damn hacker sent me this photo as proof! Can you find him?

The flag format is `ptm[the hacker's GPS Position]`

author(s): @pwnthem0le

Attachments

metadaty.zip

flag{...} Submit →

Solves

#	Time	User
1	2021-12-30.02:43:57	0xAlessandro

Tools utili:

- Linea di comando Linux
 - `exiftool`
 - `strings`

 “MetaMorph” 

Steganografia

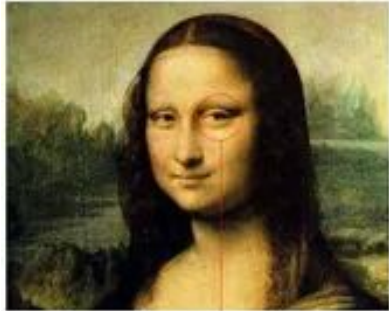
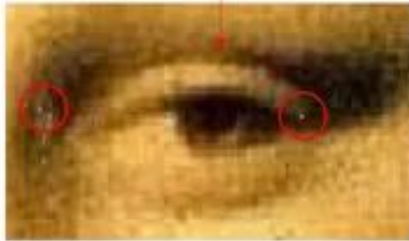
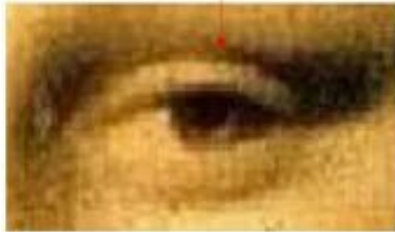


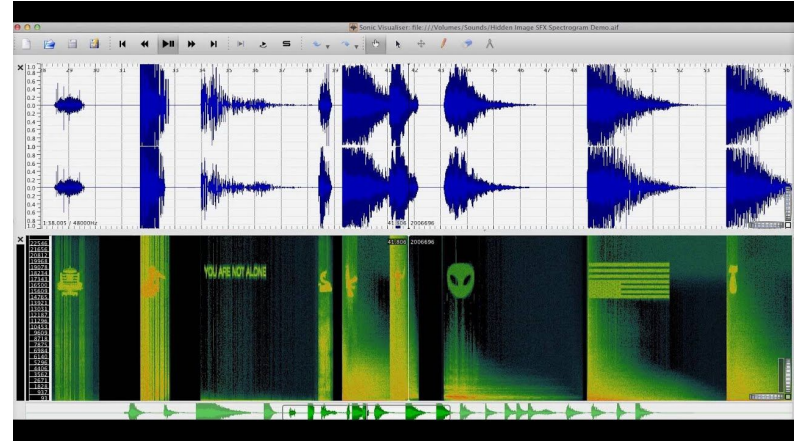
Immagine normale



Immagine Steganografata



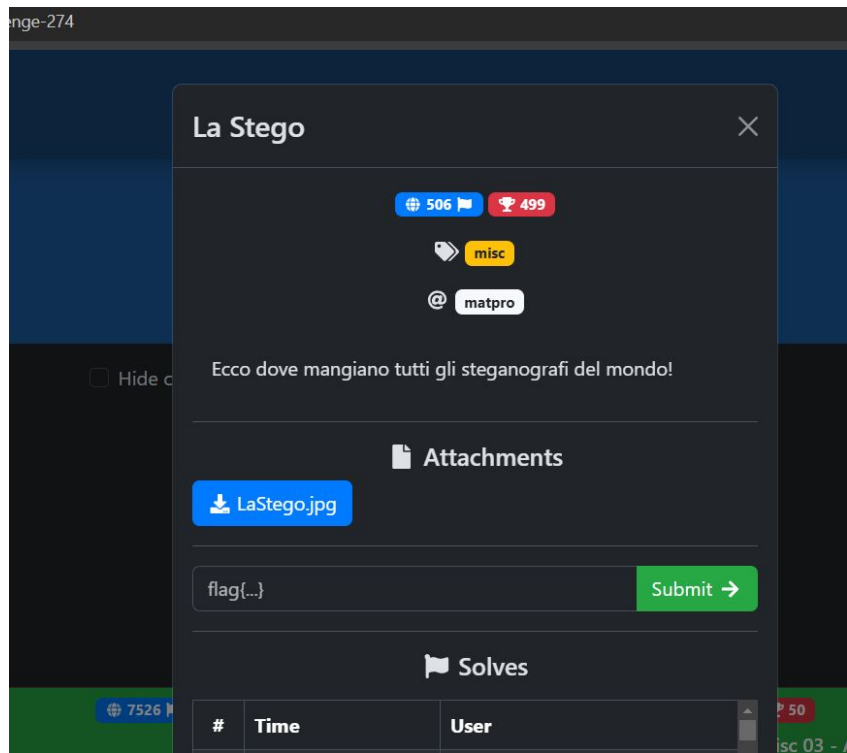
Dati in un'immagine



Immagini in un file audio

...in generale dati qualsiasi, nascosti in un media (foto, audio, video)

Challenge: “La stego”



La Stego

506 499

misc

@ matpro

Ecco dove mangiano tutti gli steganografi del mondo!

Attachments

LaStego.jpg

flag{...} Submit →

Solves

#	Time	User
---	------	------

Tools utili: Online:

- aperisolve.com
- <https://stylesuxx.github.io/steganography/>
- <https://manytools.org/hacker-tools/steganography-encode-text-into-image/>
- ...
- Linea di comando Linux
 - `steghide`
 - `stegcracker`
 - `stegsnow`
 - `stegolsb wavsteg`

 “f33linegCut3” 