
ITIS
LEONARDO DA VINCI
Via Toscana, 10 - 43122 PARMA - Tel 0521266511 - Fax 0521266550 - e-mail itis@itis.pr.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)

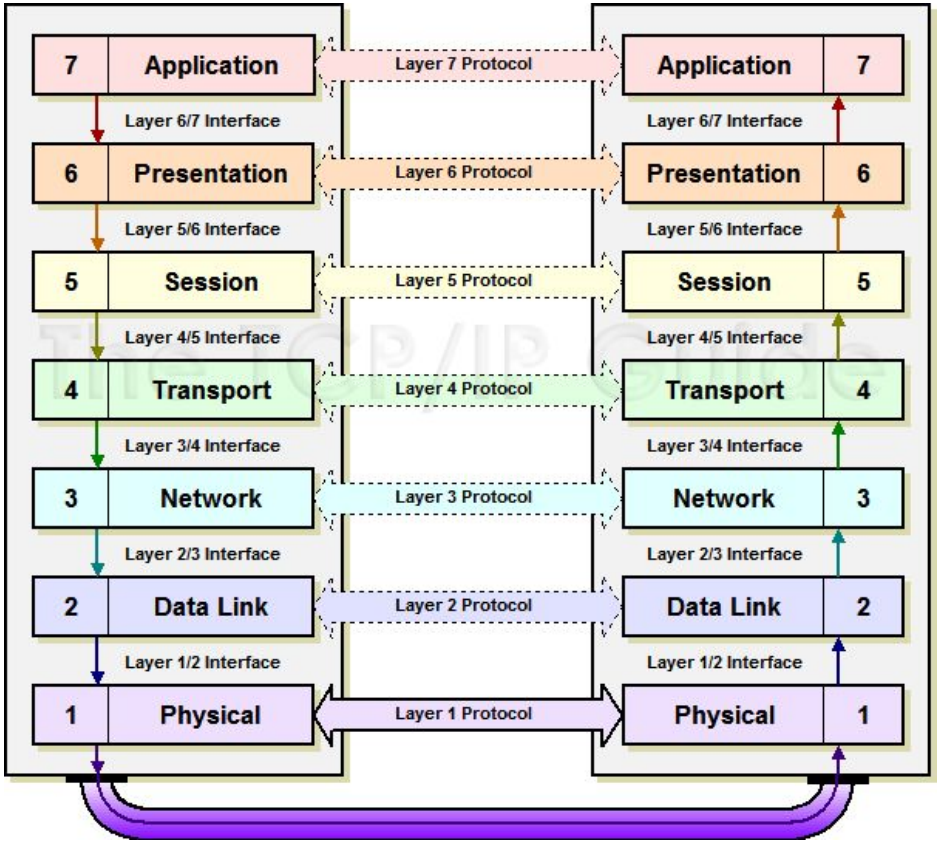
- networking
- Indirizzamento IPv4
- Funzioni ricorsive
- Operatori bitwise
- Calcolo combinatorio
- Probabilità
- Logica

Cosa faremo Oggi: Misc

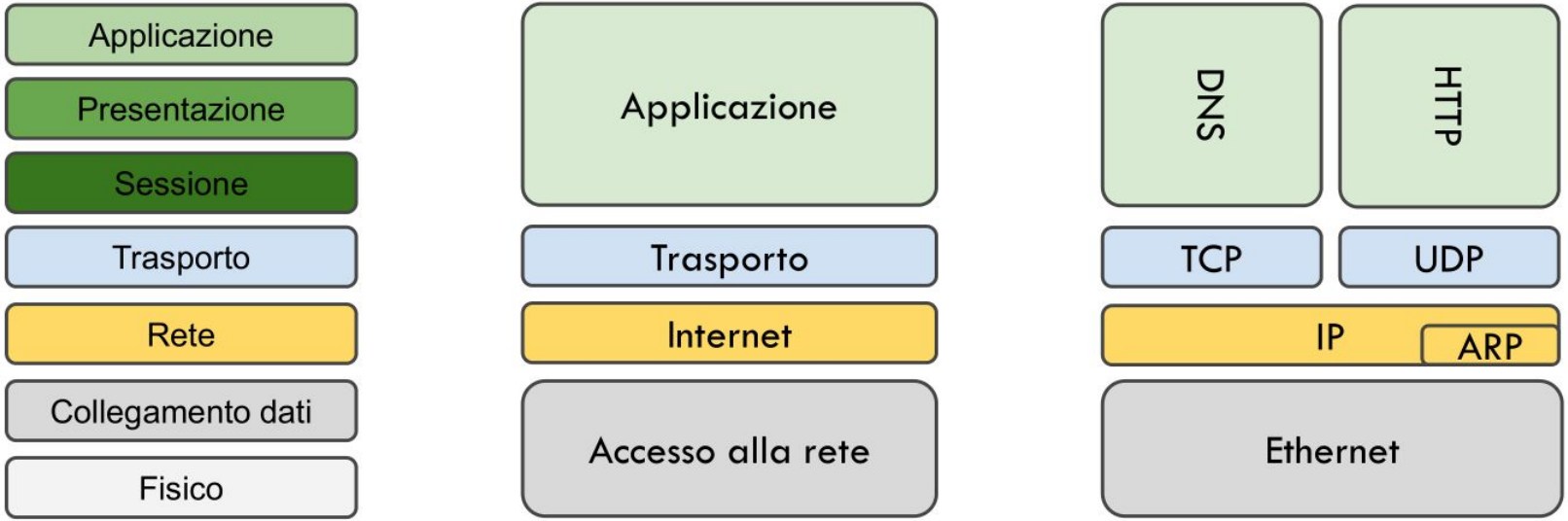
1. Fondamentali: modello ISO/OSI e TCP/IP
2. Netcat e PownTools
3. Misc
    a. Magic Bytes
    b. Metadati
    c. Steganografia

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
-



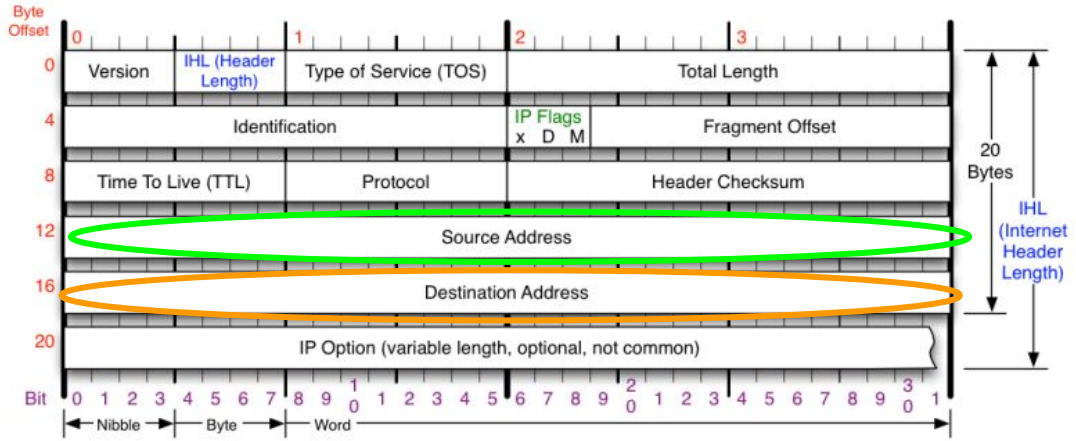
Modello TCP/IP



© CINI – 2021 Rel. 22.03.2021

Protocollo IPv4

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



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

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

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

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.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

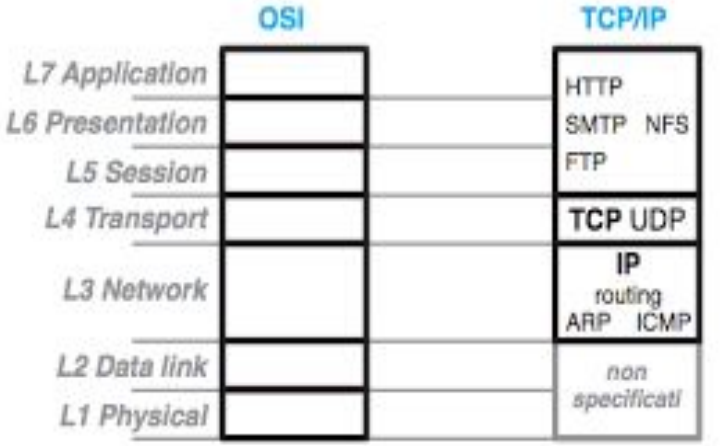
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

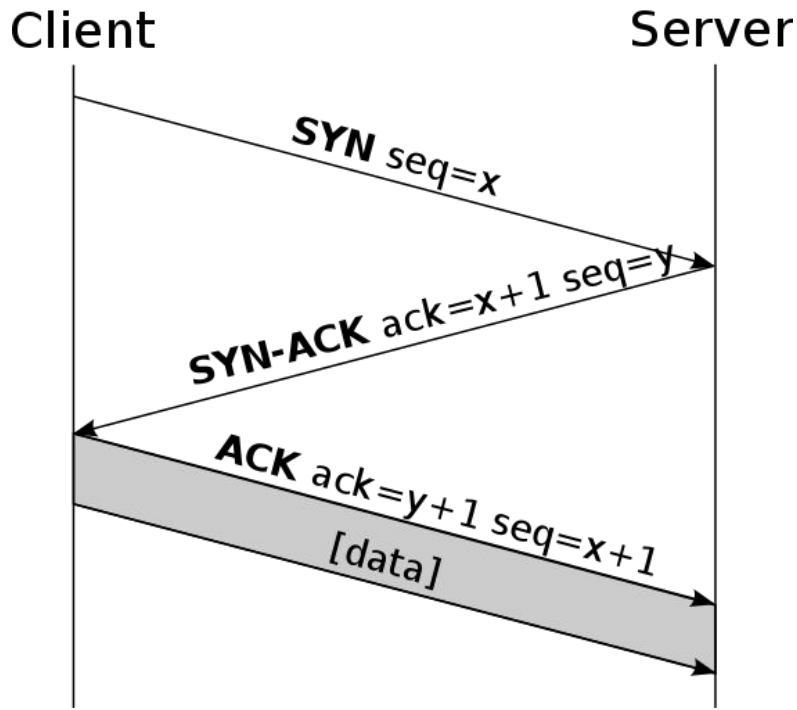
Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Protocollo TCP

⇒ Protocollo di L4

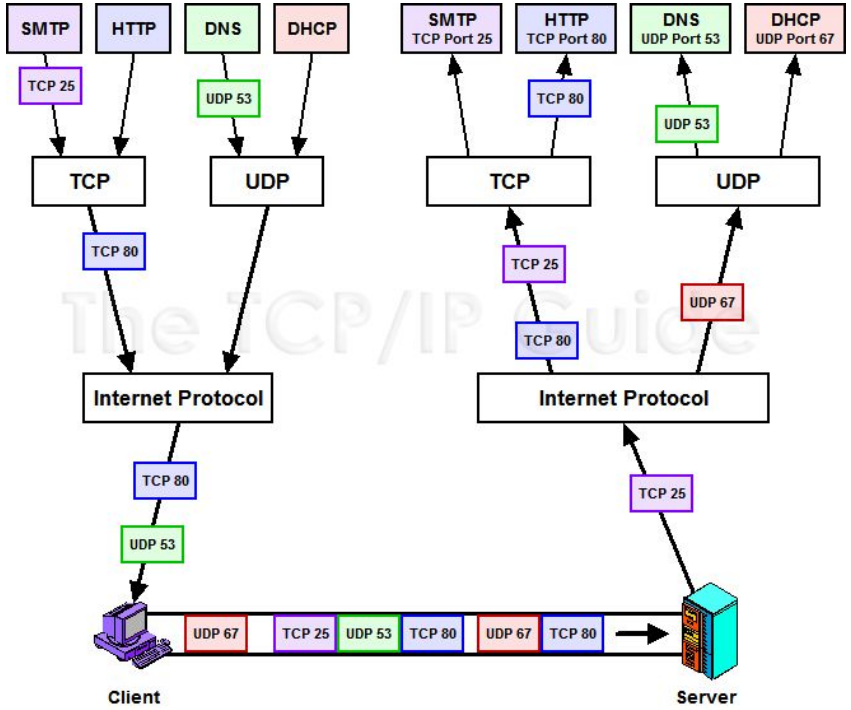


⇒ Protocollo connesso



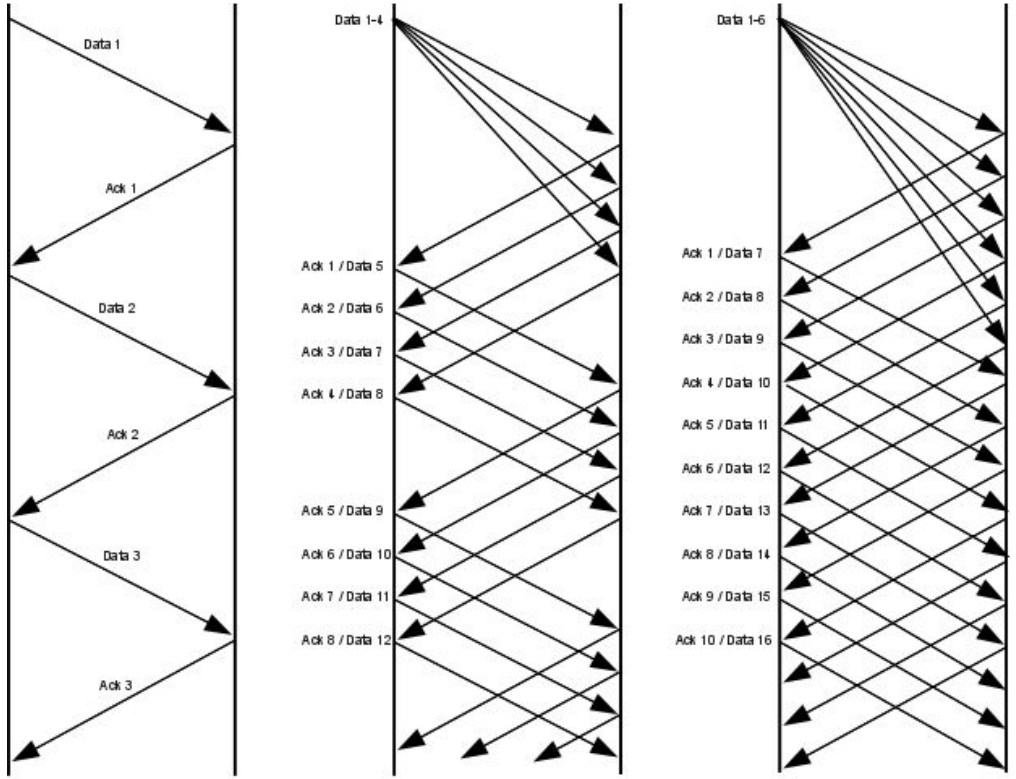
Protocollo TCP

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



Protocollo TCP

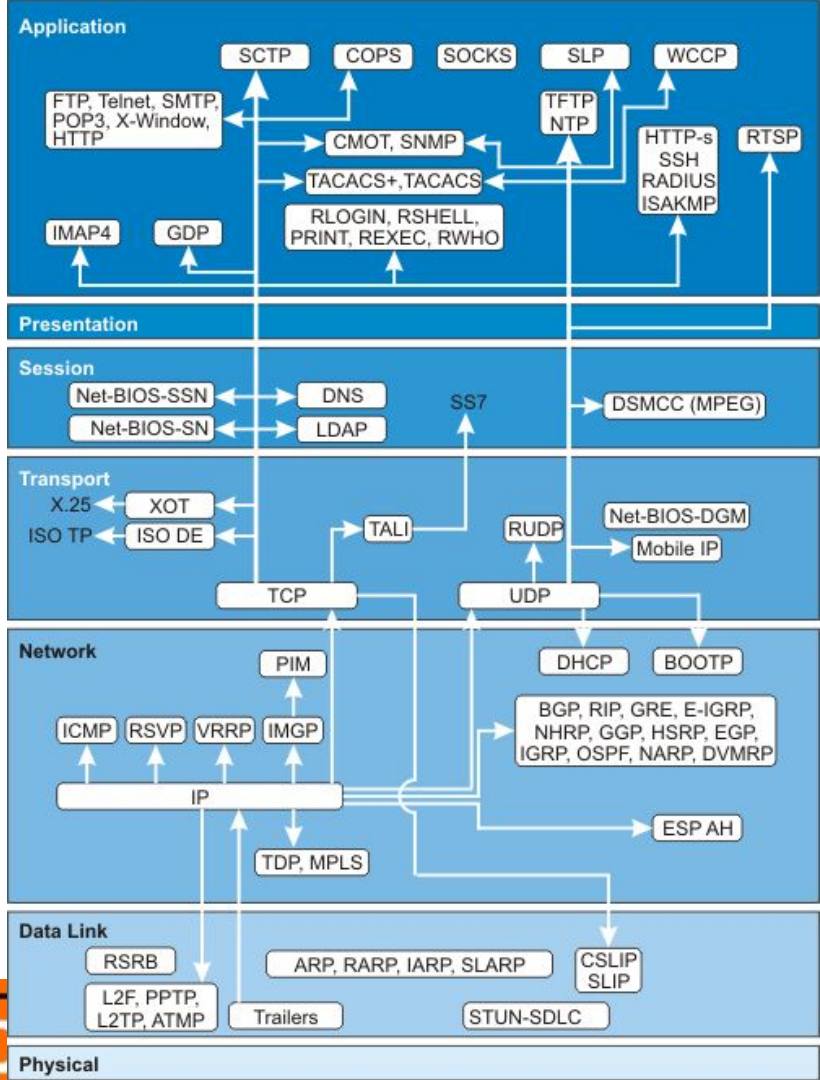
- Protocollo di L4
- Protocollo connesso
- Indirizzamento con Porte fornisce multiplexing tra processi
- Gestione del Flusso



Sliding Windows, bandwidth 6 packets/RTT

Una mappa dei protocolli

...alcuni



Challenge: Misc05

Tools per stabilire una connessione TCP:

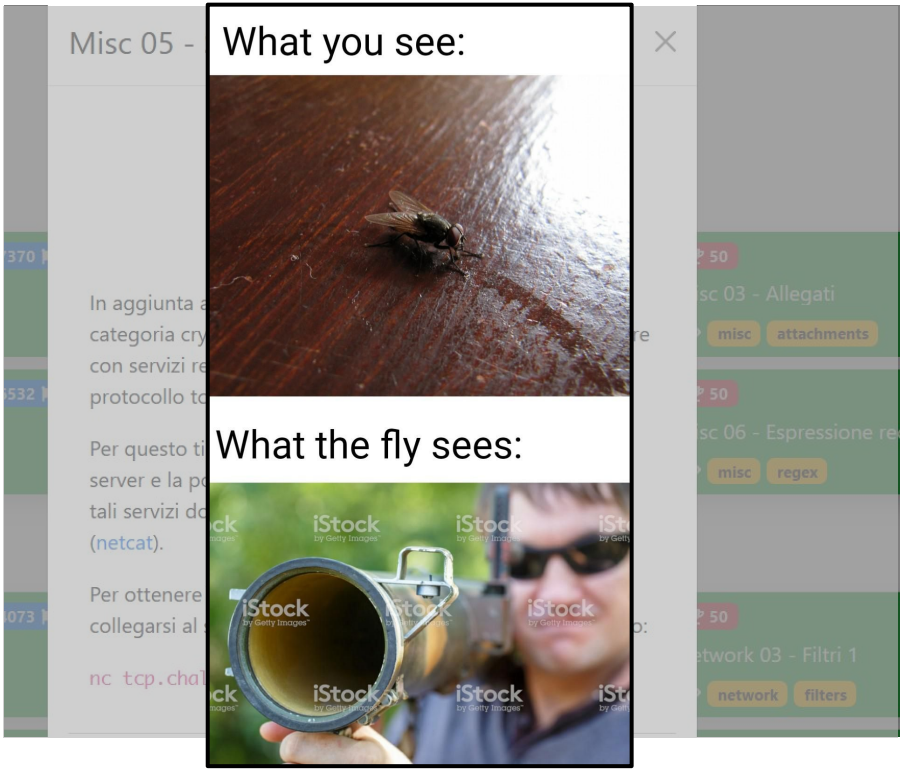
- **`telnet`** (putty)
- Netcat (**`nc`** / **`ncat`**)
- python (socket, powntools, ...)

Proviamo ad analizzare lo stream TCP della connessione con WireShark

Challenge: Misc05


```python
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.")
```

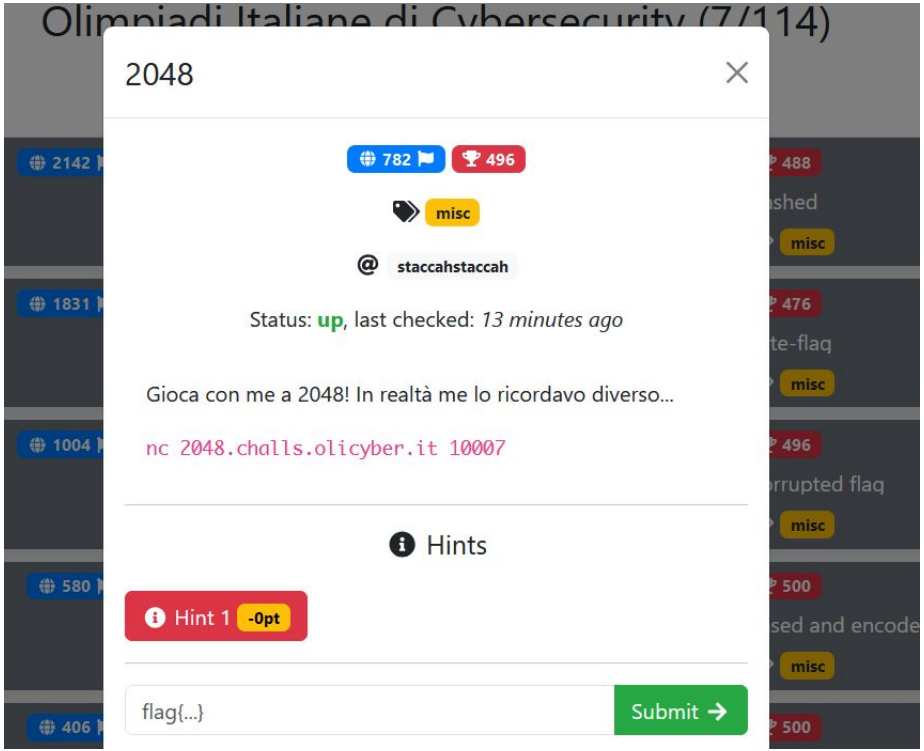
Challenge: Misc05



PWNTOOLS

```python
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



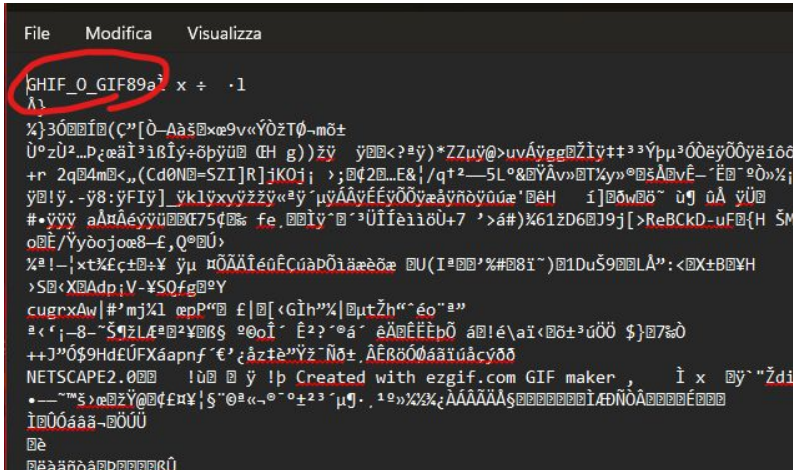

```python
from pwn import remote

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?

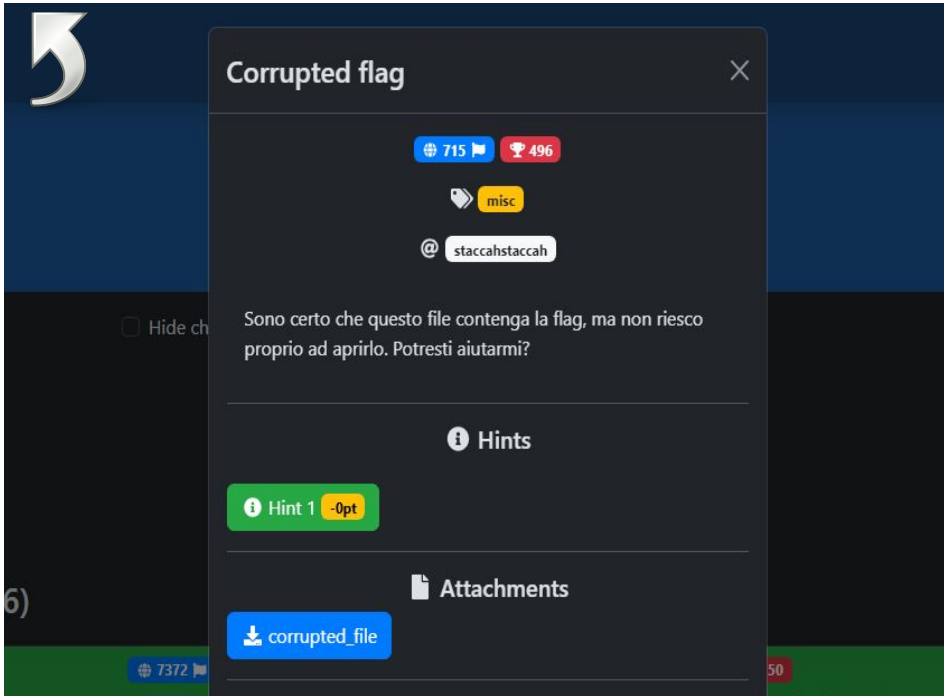
➔ La sua estensione? 😖

✓ ***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	ÿØÿ	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

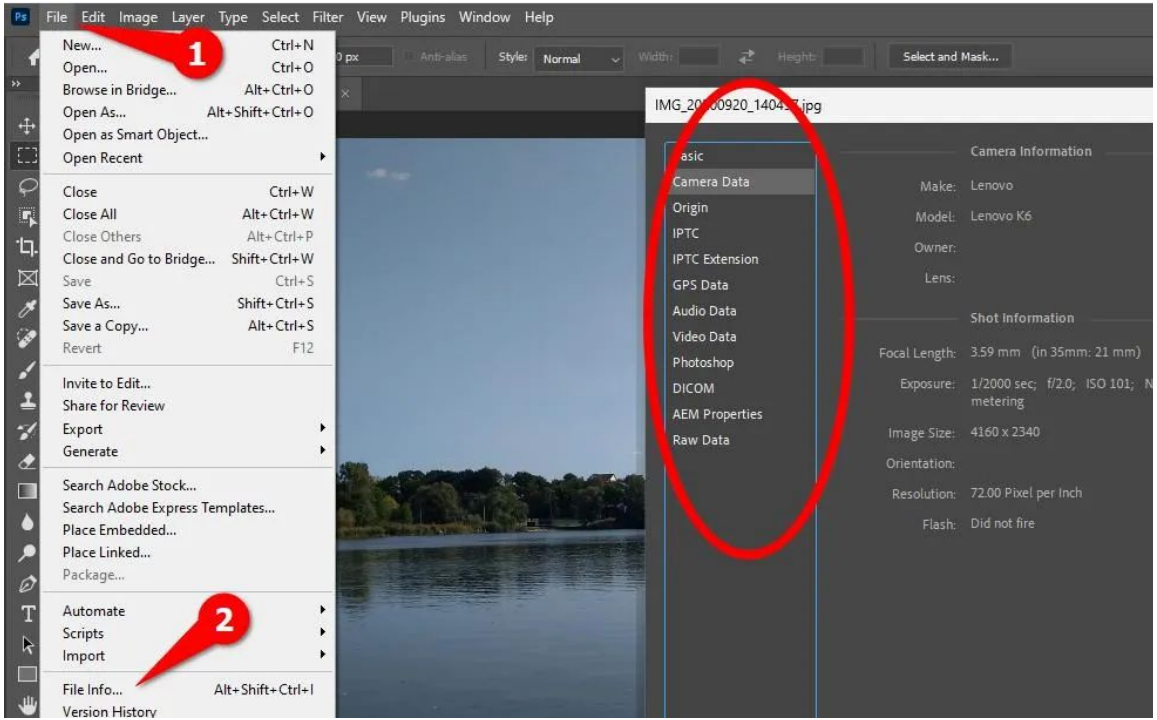


Tools utili:

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

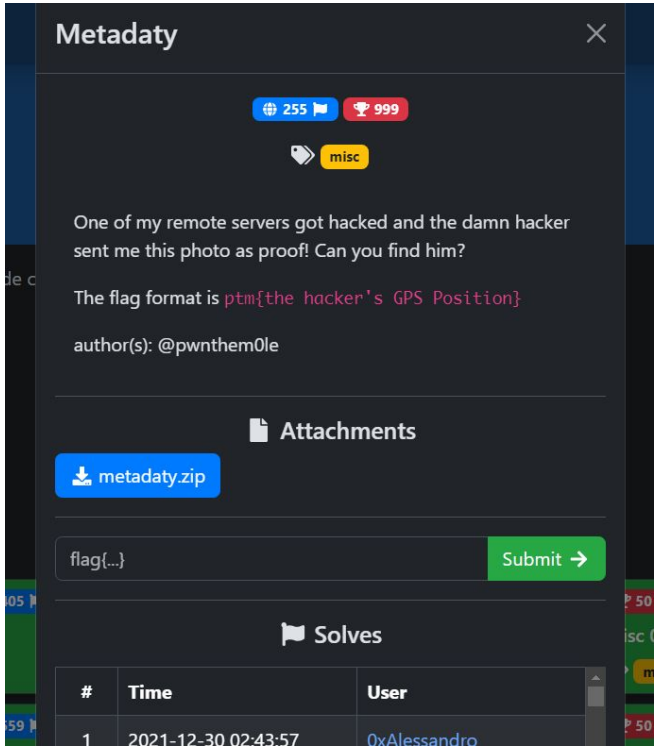
⚔️**"Do you believe in magic?"**🌎

Metadati


File Edit Image Layer Type Select Filter View Plugins Window Help
New... Ctrl+N
Open... Ctrl+O
Browse in Bridge... Alt+Ctrl+O
Open As... Alt+Shift+Ctrl+O
Open as Smart Object...
Open Recent
Close Ctrl+W
Close All Alt+Ctrl+W
Close Others Alt+Ctrl+P
Close and Go to Bridge... Shift+Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
Save a Copy... Alt+Ctrl+S
Revert F12
Invite to Edit...
Share for Review
Export
Generate
Search Adobe Stock...
Search Adobe Express Templates...
Place Embedded...
Place Linked...
Package...
Automate
Scripts
Import
File Info... Alt+Shift+Ctrl+I
Version History
1
2
Select and Mask...
Camera Data
Origin
IPTC
IPTC Extension
GPS Data
Audio Data
Video Data
Photoshop
DICOM
AEM Properties
Raw Data
Camera Information
Make: Lenovo
Model: Lenovo K6
Owner:
Lens:
Shot Information
Focal Length: 3.59 mm (in 35mm: 21 mm)
Exposure: 1/2000 sec; f/2.0; ISO 101;
metering
Image Size: 4160 x 2340
Orientation:
Resolution: 72.00 Pixel per Inch
Flash: Did not fire


METADATA IS DATA
ABOUT DATA
memegenerator.net

Challenge: Metadaty



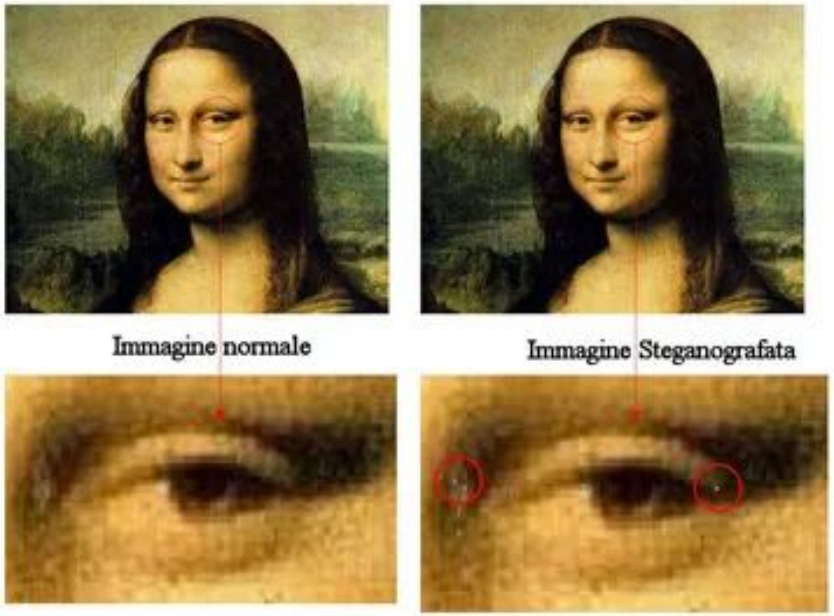
Tools utili:

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

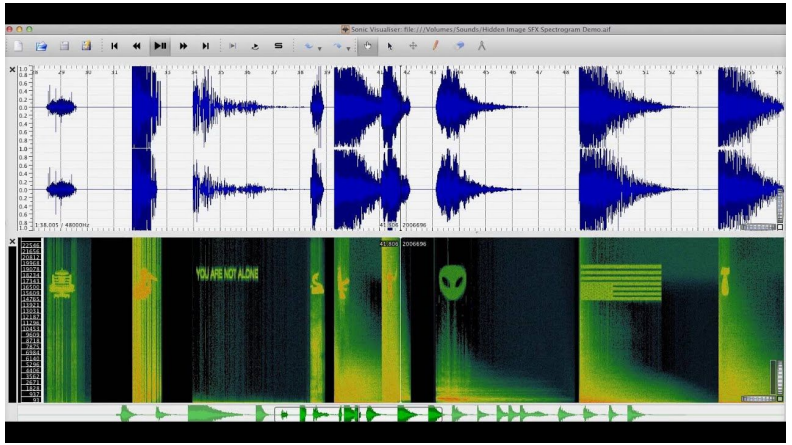
⚔️"MetaMorph"🌎

https://ctf101.org/forensics/overview/

Steganografia



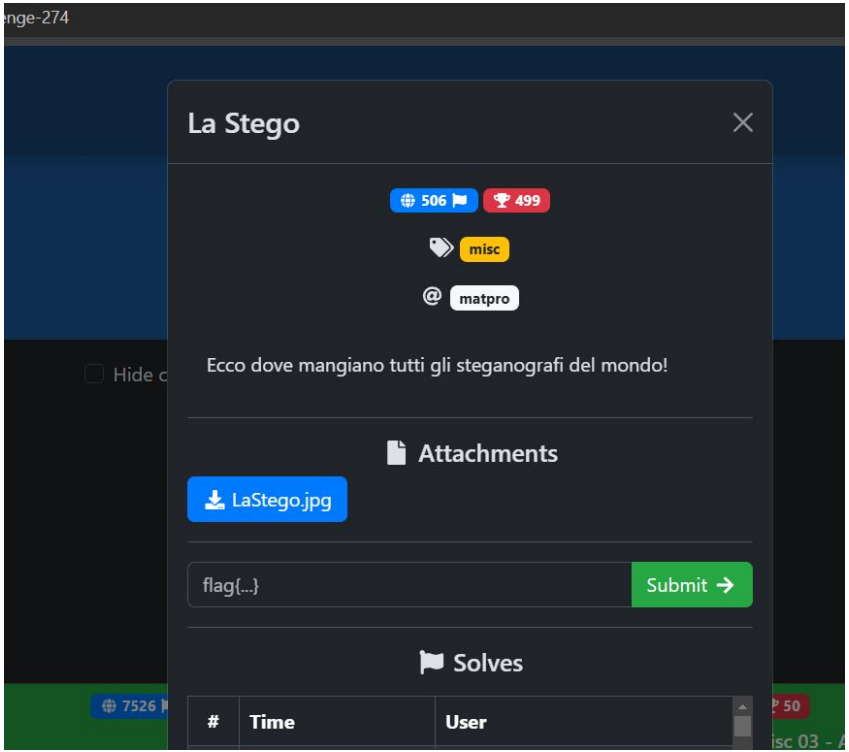
Dati in un'immagine



Immagini in un file audio

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

Challenge: “La stego”



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”🌎