Project Work

DACA TRACEY

Indice

Guida Utente - DACA TRACEY

Versione del Software: 1.0.3 - disponibile per ora solo su windows

Data e revisione del manuale: 29/10/2025

Prefazione: La nostra visione è quella di combinare la potenza del **packet sniffing**.
per offrire un ambiente in cui l'utente possa dialogare con una chat box implementata con un **AI** e ricevere risposte/diagnosi sul traffico qualitativo e quantitativo in tempo reale.
Abbiamo voluto che il sistema fosse accessibile, efficiente e sicuro, pur mantenendo flessibilità per usi avanzati.
Questo manuale nasce con l'obiettivo di accompagnare l'utente dallo step iniziale fino alle funzionalità più complesse in un percorso di scoperta e utilizzo dell'applicazione. I principi, le scelte di design e le motivazioni che ci hanno guidato nel progettare questo strumento. A chiunque decida di esplorarlo, speriamo che diventi un compagno affidabile nel controllo e nell'analisi delle reti.

Pubblico a cui si rivolge: DACA TRACEY si rivolge a professionisti IT che necessitano di strumenti avanzati per l'analisi del traffico di rete.

Amministratori di Rete: Monitorano costantemente le performance della rete aziendale, diagnosticano problemi di connettività e ottimizzano il **flusso dei dati**. L'AI li supporta nell'identificare anomalie in tempo reale o caricando un file di rete all' interno, riducendo drasticamente i tempi di troubleshooting.

Analisti di Sicurezza Informatica: Sono in prima linea nella difesa contro minacce cyber. L'applicazione analizza il traffico per individuare pattern sospetti, tentativi di intrusione, **malware** e violazioni delle policy di sicurezza, fornendo **alert** intelligenti e contestualizzati.

DevOps e Sviluppatori: Durante lo sviluppo e il **debug** di applicazioni di rete, hanno bisogno di comprendere nel dettaglio il comportamento delle loro soluzioni. L'analisi AI dei pacchetti accelera l'identificazione di bug, problemi di protocollo e inefficienze nelle comunicazioni client-server.

Security Operations Center (SOC): I team **SOC** utilizzano lo strumento per la correlazione avanzata di eventi, l'analisi forense post-incident e il threat hunting proattivo, sfruttando l'AI per processare grandi volumi di traffico e identificare minacce sofisticate.

GUIDA PER L'INSTALLAZIONE DELL'AI
https://ollam.com/download/windows
mandare in esecuzione OllamaSetup.exe
finita la configurazione aprire la cmd ed eseguire il seguente comadno => ollama pull llama3.2

Schema Generale dell'Applicazione:
Il **Traffic Network Analyzer** segue uno schema di funzionamento chiaro e strutturato, suddiviso in tre fasi principali:
1. Sniffing dei pacchetti – In questa fase l'applicazione cattura il **traffico di rete** in tempo reale e visualizza i pacchetti rilevati direttamente all'interno dell'interfaccia grafica.

2. Analisi tramite intelligenza artificiale – I pacchetti acquisiti vengono successivamente elaborati e analizzati dall'IA, che fornisce informazioni dettagliate sul loro contenuto, sul **protocollo** utilizzato e sulla loro funzione all'interno della rete.

3. Interazione con l'utente – L'utente può consultare i pacchetti sniffati, salvare i dati raccolti e interagire con l'intelligenza artificiale per ottenere chiarimenti, spiegazioni o approfondimenti relativi ai pacchetti visualizzati.

PACCHETTI CHE PUOI ANALIZZARE:
la nostra applicazione sniffa questi tipi di pacchetti :
TCP – Base di quasi tutto il traffico Internet (HTTP, HTTPS, FTP, SSH, ecc.).

HTTPS – Standard per la navigazione web sicura, usato nella maggior parte dei siti moderni.

HTTP – Ancora utilizzato, ma sempre più sostituito da HTTPS.

DNS – Fondamentale per la risoluzione dei nomi di dominio.

UDP – Usato in molte applicazioni in tempo reale (streaming, VoIP, giochi online).

DHCP – Essenziale per l'assegnazione automatica degli **indirizzi IP** in rete.

ICMP – Cruciale per diagnostica e controllo della rete (es. ping, traceroute).

ARP – Necessario per la comunicazione locale tra dispositivi nella stessa rete.

SSH – Importante per accesso remoto sicuro e amministrazione di sistemi.

FTP – Usato per trasferimenti di file, ma in declino per motivi di sicurezza.

RTP – Fondamentale per trasmissioni audio/video in tempo reale (VoIP, streaming).

SNMP – Usato per la gestione e il monitoraggio delle reti, soprattutto in ambito enterprise.

NTP – Sincronizza gli orologi dei dispositivi, utile ma con impatto limitato sul traffico generale.

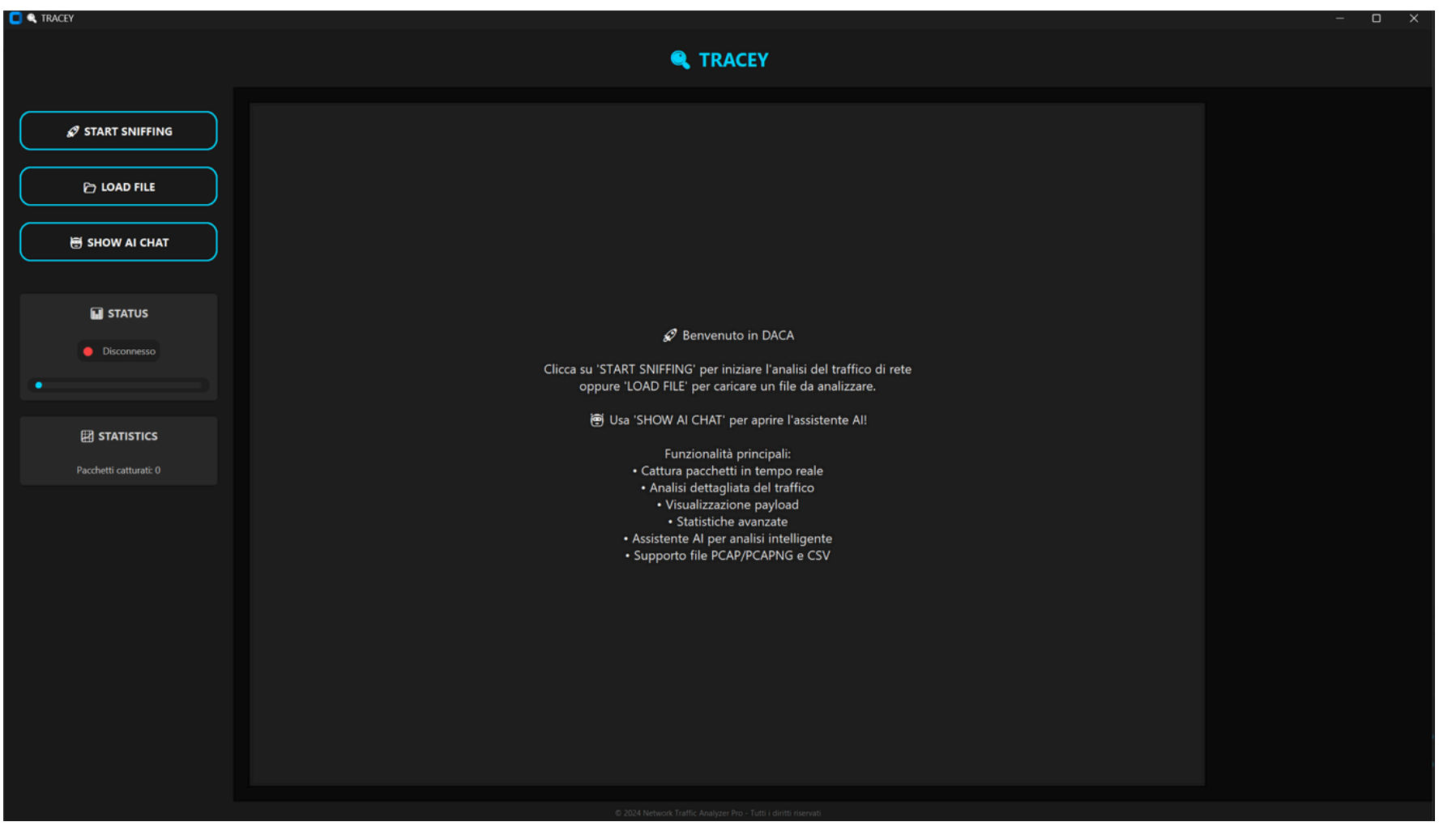
Analisi con algoritmi di intelligenza artificiale: L'analisi dei pacchetti viene effettuata tramite un sistema di AI basato sul **servizio Ollama**, al quale ci colleghiamo utilizzando il modello llama 3:2.
I pacchetti catturati vengono prima elaborati e salvati da un apposito algoritmo di lettura, che si occupa di estrarre e organizzare le informazioni necessarie. Successivamente, tali dati vengono inviati alla nostra AI, che li analizza in modo approfondito.
Grazie a questa analisi, l'intelligenza artificiale è in grado di fornire numerose informazioni sui pacchetti esaminati. Ad esempio, può spiegare il protocollo utilizzato, descrivere la funzione del **pacchetto** e fornire dettagli tecnici specifici relativi al suo contenuto o al suo comportamento nella rete.
In questo modo, la nostra AI si comporta a tutti gli effetti come un assistente intelligente, in grado di guidare l'utente nella comprensione dei pacchetti sniffati e di rispondere a qualsiasi dubbio o curiosità riguardante le informazioni acquisite.

Modulo Interfaccia Utente: Il modulo di interfaccia utente della nostra applicazione offre un **ambiente grafico** intuitivo e facilmente utilizzabile.
Attraverso questa interfaccia è possibile visualizzare in tempo reale il flusso dei pacchetti di rete catturati dal sistema.
L'utente ha inoltre la possibilità di caricare un flusso di pacchetti precedentemente registrato per analizzarlo in un secondo momento.
I dati visualizzati possono essere esportati e salvati e letti in formato **CSV**, consentendo così ulteriori elaborazioni o archiviazione.
Infine, l'interfaccia permette di interagire direttamente con l'intelligenza artificiale integrata, ponendo domande sui pacchetti che transitano in tempo reale o su quelli salvati, ottenendo spiegazioni e approfondimenti immediati.

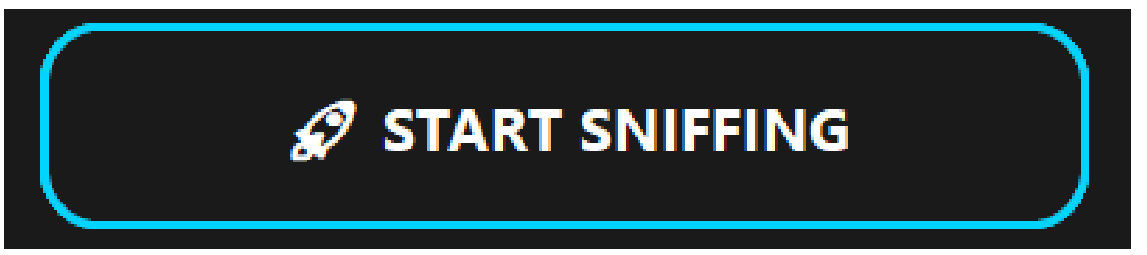
Uso dell'applicazione: guida operativa Navigazione dell'interfaccia (menu, dashboard, opzioni)

La navigazione consente all'utente di spostarsi tra le diverse sezioni dell'applicazione per accedere alle varie funzioni disponibili.
Questa sezione descrive come spostarsi tra le diverse aree dell'interfaccia dell'applicazione. Imparerai a utilizzare il menu principale, le barre di strumenti e i pulsanti di navigazione per accedere alle funzioni disponibili

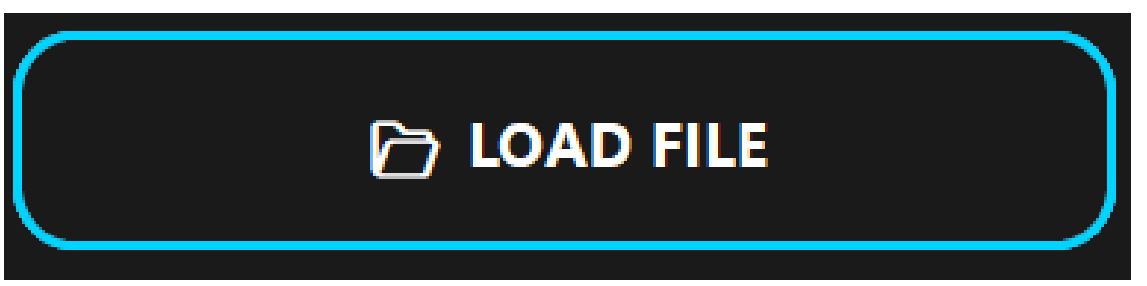
Interfaccia principale:



E’ composto da un menu laterale che consente di accedere alle varie sezioni del programma

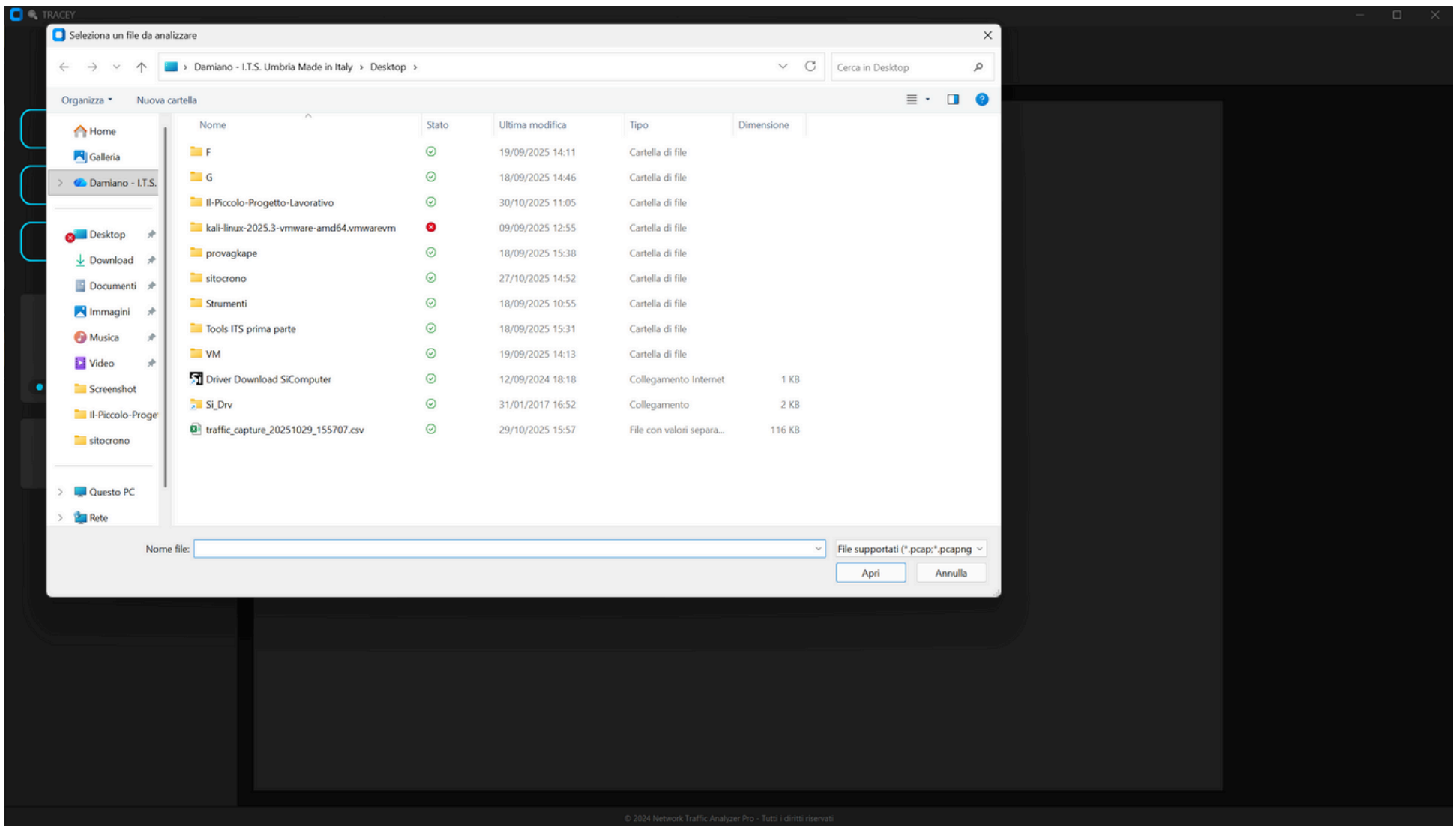


Premendo **Start Sniffing** l’applicazione avvia la **cattura e l’analisi del traffico di rete** sull’interfaccia selezionata. Vengono acquisiti i pacchetti che transitano e presentati per ispezione (protocollo, indirizzi IP, porte, **payload** parziale, ecc.)



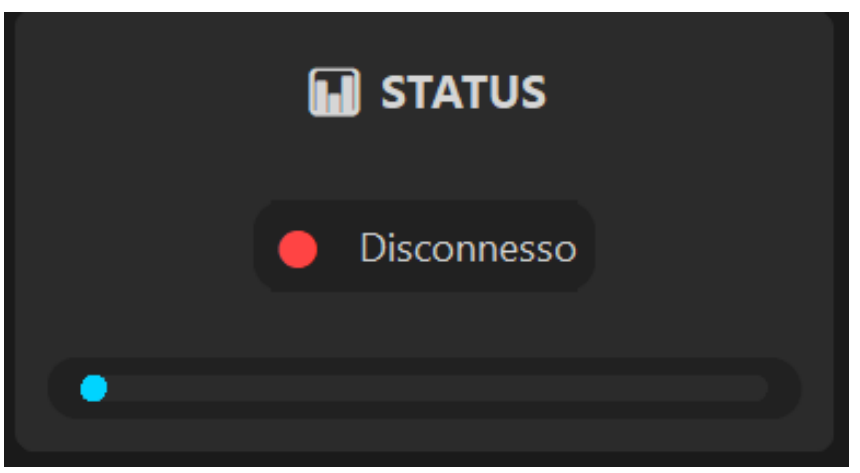
Load File permette di **caricare un file esistente nel pc** all’interno dell’applicazione.
È utilizzata per aprire e visualizzare dati precedentemente salvati o acquisiti di tipo **pcap**-**pcapng**-csv (con determinata nomenclatura), in modo da poterli analizzare, modificare o elaborare

Esempio di caricamento File:



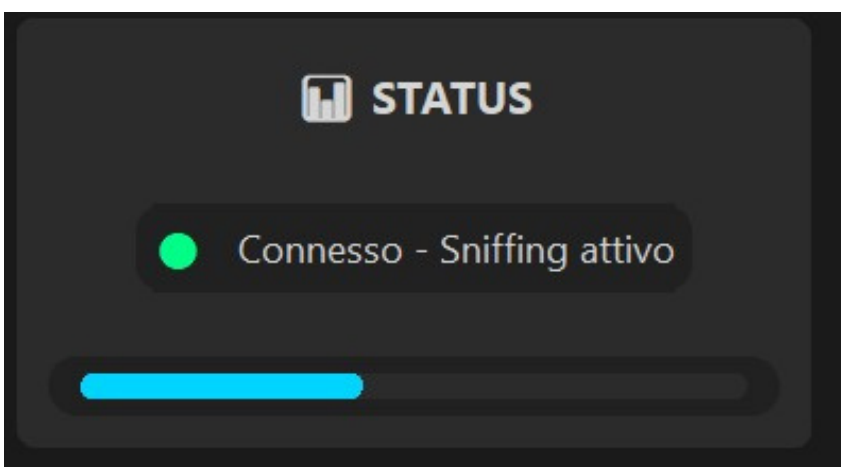
Indicatore rosso: il sistema è disconnesso

Barra di progresso (azzurra): indica l'avanzamento di un'operazione in corso o il livello di attività del processo di sniffing.



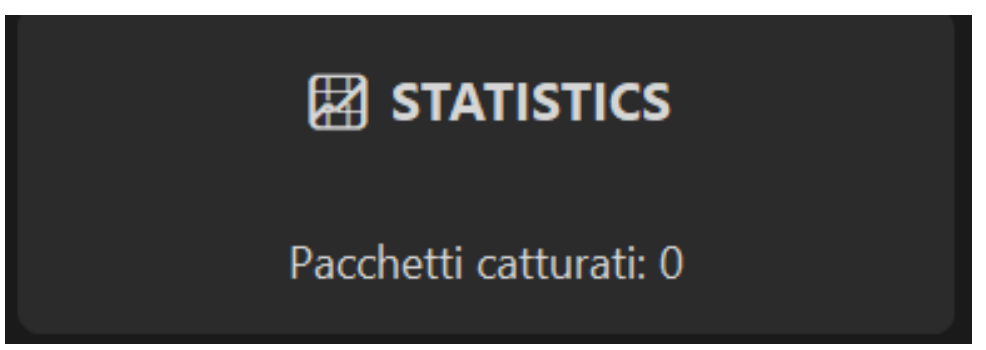
Indicatore verde: il sistema è connesso e il processo di sniffing (analisi del traffico di rete) è attivo.

Barra di progresso (spenta o quasi vuota): segnala che non è in corso alcuna attività di sniffing o trasferimento dati

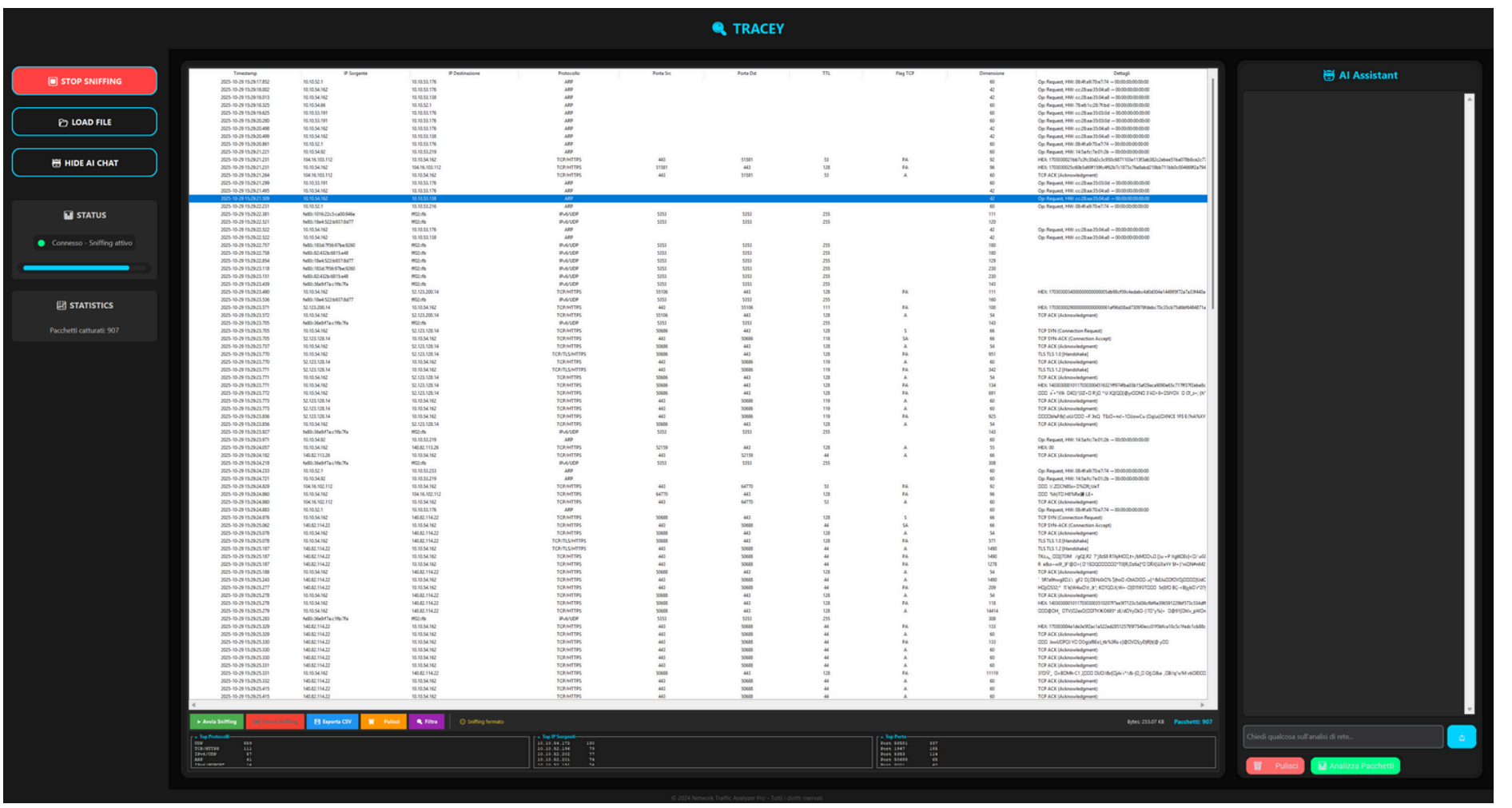


L'icona con il simbolo del grafico rappresenta la sezione Statistiche di cattura.
Qui vengono visualizzate le informazioni relative ai pacchetti di rete analizzati durante la sessione di sniffing.

• **Pacchetti catturati:** indica il numero totale di pacchetti di rete rilevati e registrati dal programma.
Nel caso mostrato, il valore è 0, quindi non è stato ancora catturato alcun pacchetto.
In fase di sniffing attivo il valore 0 cambierà

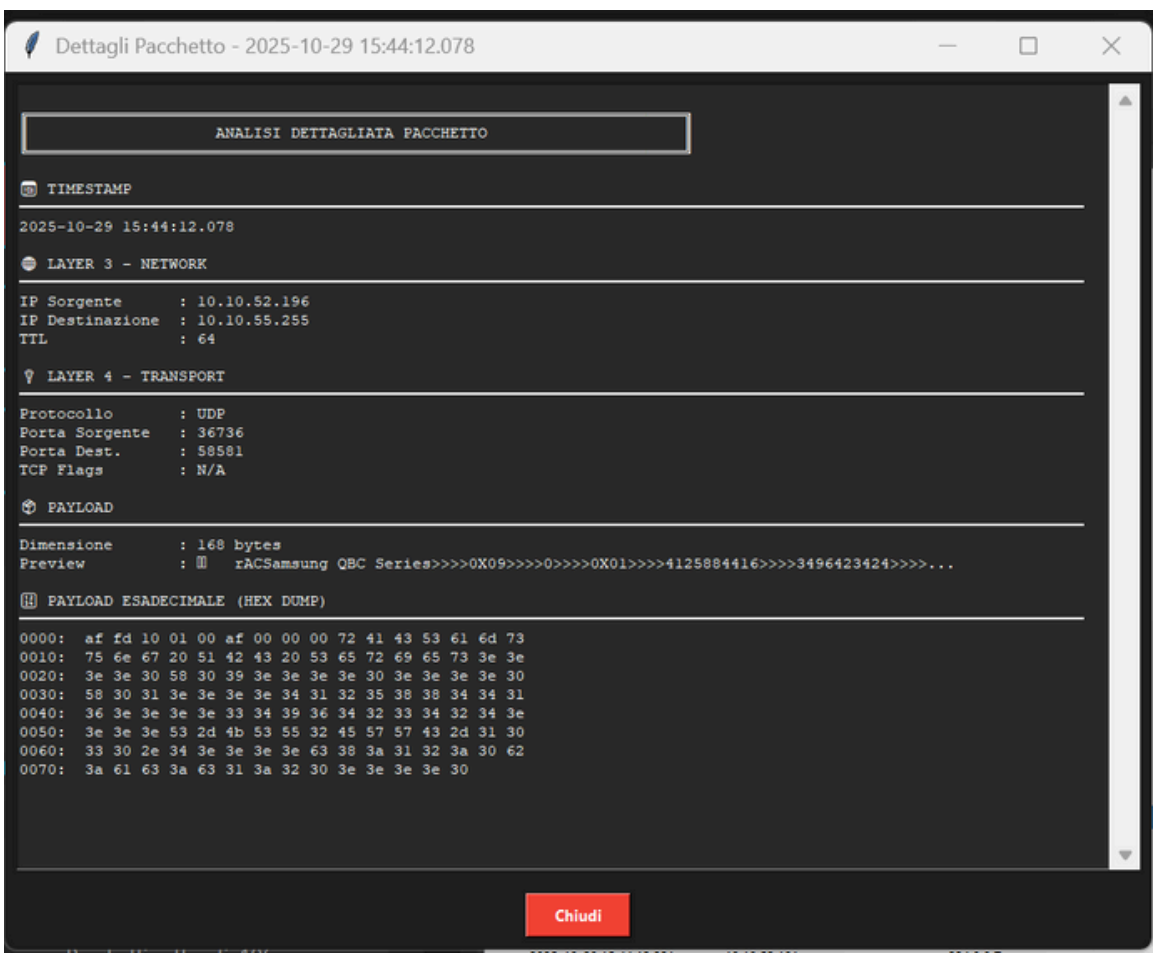


Questa schermata mostra la fase di **sniffing attivo**, ovvero la cattura in tempo reale dei pacchetti di rete analizzati dal programma **TRACEY**



Nella parte inferiore dell' applicazione, viene notificato all'utente le porte/protocolli/indirizzi più frequenti

facendo **doppio click sul pacchetto interessato** , sarà possibile **accedere a delle informazioni** in modo più dettagliato



La tabella principale elenca i pacchetti catturati con le seguenti colonne:

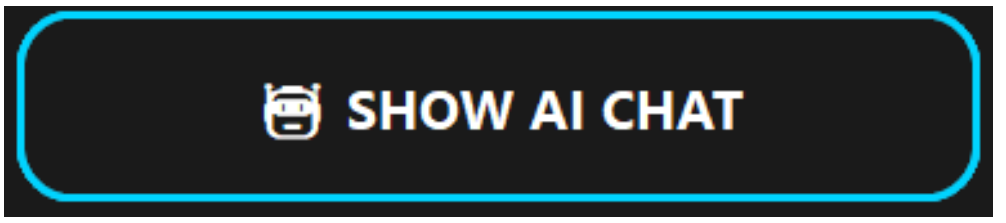
Colonna	Descrizione
Timestamp	Data e ora di cattura del pacchetto.
IP Sorgente	Indirizzo IP del dispositivo che ha inviato il pacchetto.
IP Destinazione	Indirizzo IP del dispositivo destinatario.
Protocollo	Protocollo di trasporto utilizzato (es. TCP, UDP).
Porta Src / Porta Dst	Porte sorgente e destinazione associate alla connessione.
TTL	"Time To Live": numero massimo di passaggi (hop) consentiti prima che il pacchetto venga scartato.
Flag TCP	Eventuali flag impostati nel pacchetto TCP (es. SYN, ACK, PA).
Dimensione Payload	Dimensione del contenuto effettivo del pacchetto (in byte).
Preview Payload	Anteprima in formato testuale o esadecimale del contenuto del pacchetto.

La barra inferiore contiene funzioni operative aggiuntive:

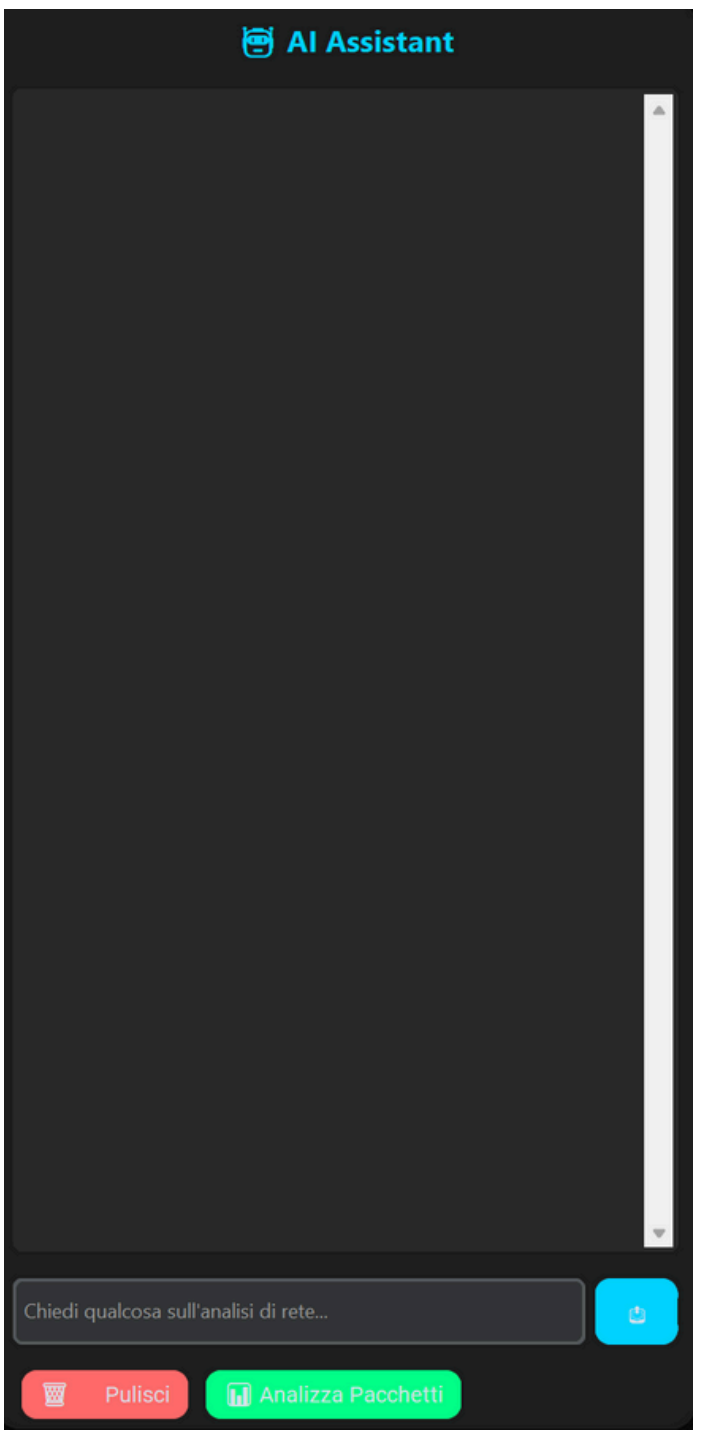
• **Avvia Sniffing / Interrompi / Esporta CSV / Pulisci / Pronto**
Consentono di avviare o fermare la cattura, esportare i dati in formato CSV, pulire la tabella o verificare lo stato del programma
• **Pacchetti**: mostra il numero totale di pacchetti catturati fino a quel momento

Questa icona segnala **l'arresto della funzione di rilevamento o intercettazione** del traffico di rete

Show AI Chat consente di aprire la finestra di chat con l'assistente AI integrato nell'applicazione. Attraverso questa funzione, l'utente può interagire con l'intelligenza artificiale per ricevere spiegazioni, suggerimenti, analisi o assistenza in tempo reale.
Nel selezionare 'SHOW AI CHAT' si aprirà la chat dove sarà possibile chiedere tutto ciò che riguarda l'informazione dei pacchetti catturati



Facendo click su 'Analizza Pacchetti' dopo aver avviato lo sniffing sarà possibile visualizzare i pacchetti dati trasmessi per verificare la connessione, diagnosticare problemi o monitorare l'attività di rete



Risoluzione dei problemi (Troubleshooting):

Problemi comuni e soluzioni rapide:

Se la cattura dei pacchetti (sniffing) rimane attiva durante l'esportazione in CSV, l'applicazione può diventare instabile e l'esportazione può risultare corrotta o incompleta; una volta che si verifica tale stato, l'unica procedura di ripristino consiste nel chiudere completamente l'applicazione e riavviarla.

Checklist operativa – Cattura ed esportazione dati (sniffing ⟶ CSV)

Prima dell'esportazione:

- Verificare che la sessione di sniffing sia interrotta (Stop capture) situato sotto alla pagina dello sniffing, prima di avviare l'esportazione
- Salvare eventuali dati acquisiti, se necessario, prima di terminare la cattura.
- Controllare che lo spazio su disco sia sufficiente per il file CSV di output.

In caso di blocco o malfunzionamento:

- Se l'applicazione diventa instabile o l'esportazione non si completa, chiudere e riavviare l'applicazione
- Verificare l'integrità del file CSV generato; se corrotto, rieseguire l'esportazione dopo il riavvio

Conclusioni

Grazie per aver scelto DACA!

Siamo lieti che tu abbia utilizzato il nostro software di analisi del traffico di rete con assistente AI.

Il tuo feedback è fondamentale per aiutarci a migliorare continuamente le prestazioni, l'affidabilità e l'esperienza d'uso.

Resta connesso per scoprire le nuove funzionalità e aggiornamenti che renderanno la tua analisi di rete ancora più semplice e intelligente.

Il team di Damiano, Arber, Alessia, Samuele - ITS Umbria Italy

Monitoraggio intelligente. Decisioni migliori.

Glossario

1. **Packet sniffing** – Analisi dei pacchetti di rete per ispezionare dati e protocolli in transito.
2. **Insight** – Informazioni approfondite ottenute dall'analisi del traffico per individuare anomalie o pattern.
3. **A.I.** – Intelligenza artificiale usata per rilevare minacce e automatizzare l'analisi di rete.
4. **Malware** – Software malevolo rilevabile nel traffico grazie a firme o comportamenti anomali.
5. **Alert** – Notifica automatica generata dal sistema in caso di evento sospetto.
6. **Debug** – Processo di identificazione e correzione di errori nel codice o nella configurazione di rete.
7. **SOC** (Security Operations Center) – Centro operativo che monitora e gestisce la sicurezza informatica.
8. **Traffic network analyzer** – Strumento che cattura e analizza pacchetti di rete per valutare prestazioni e sicurezza.
9. **I.A.** (Intelligenza Artificiale) – Sistema automatizzato che apprende dai dati per migliorare il rilevamento delle minacce.
10. **Protocollo** – Insieme di regole che definiscono la comunicazione tra dispositivi di rete.
11. **Servizio Ollama** – Piattaforma AI locale usabile per analisi o automazione in ambienti di rete.
12. **Llama3.2** – Modello linguistico AI impiegabile per classificazione o interpretazione dei log di rete.
13. **Pacchetto** – Unità base di dati trasmessa in una rete.
14. **Ambiente grafico** – Interfaccia visiva per visualizzare statistiche, grafici e flussi di rete.
15. **CSV** – Formato di file usato per esportare o importare dati di traffico in forma tabellare.
16. **Traffico di rete** – Flusso di dati scambiato tra dispositivi connessi.
17. **Indirizzi IP** – Identificatori numerici assegnati a dispositivi di rete per instradare il traffico.
18. **Payload** – Contenuto effettivo di un pacchetto, spesso oggetto di analisi per rilevare minacce.
19. **PCAP** – Formato di file standard per memorizzare pacchetti catturati.
20. **PCAPNG** – Versione estesa del formato PCAP con supporto a metadati e più interfacce di cattura.