Es.4 SQL

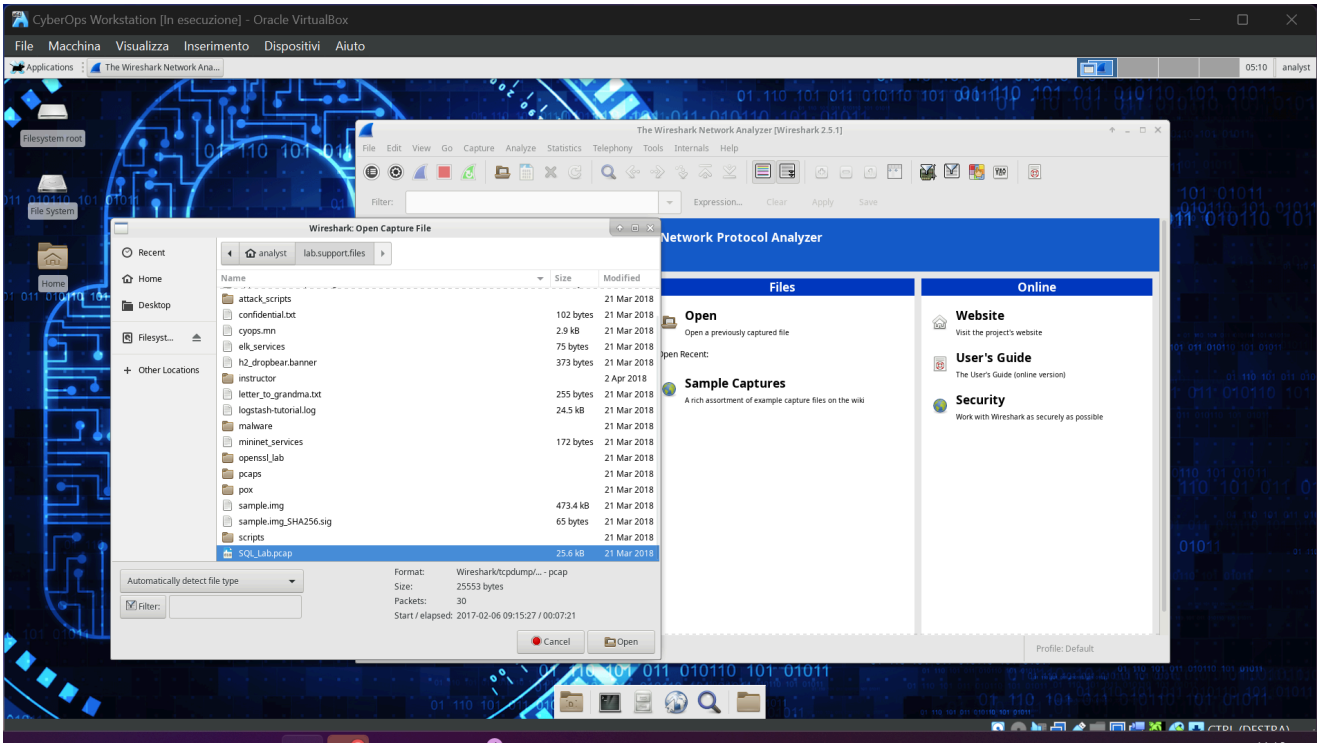
⚜️ Relazione: Analisi di un file di cattura SQL con Wireshark

⚜️ **Tag:** #analisi #wireshark #sqlinjection #pentesting

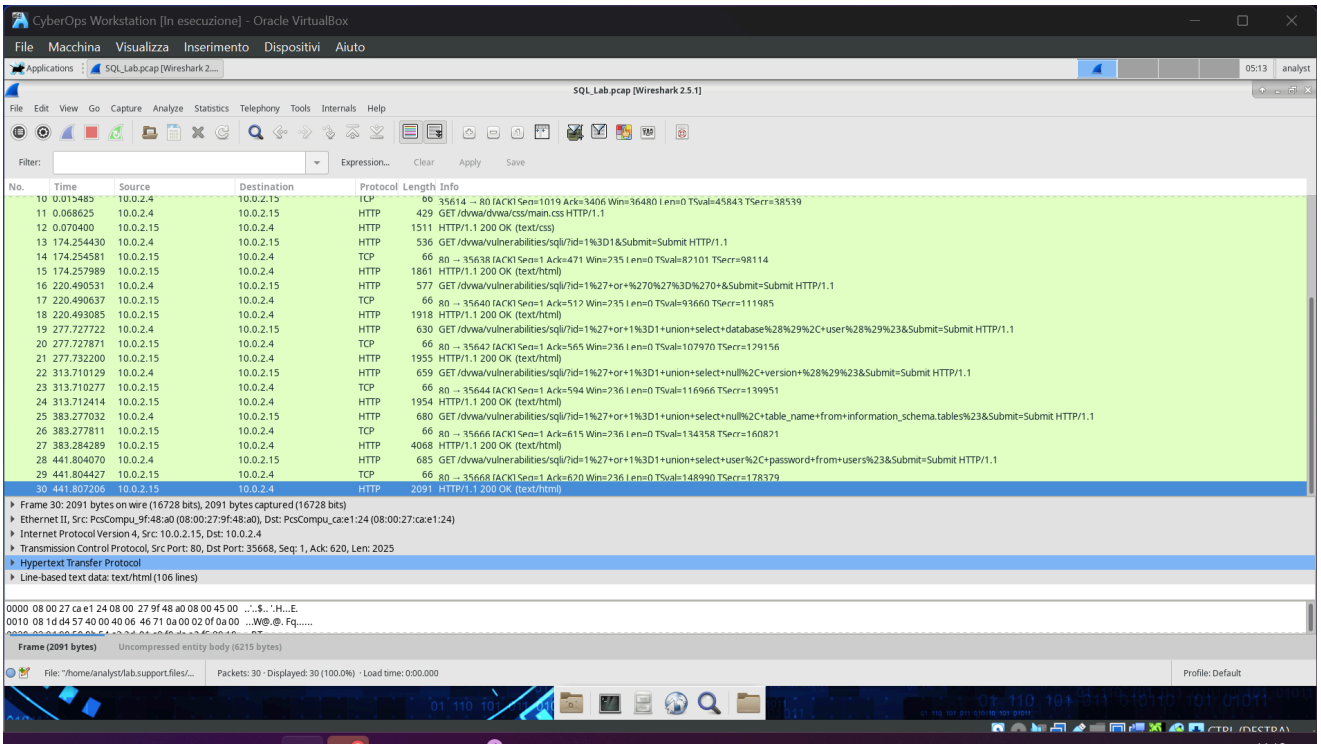
---

1. Apertura del file di cattura

- Il file `SQL_Lab.pcap` è stato caricato in Wireshark, come mostrato nella prima immagine.



- Wireshark mostra una serie di pacchetti HTTP e TCP tra il client (10.0.2.4) e il server (10.0.2.15).



- La comunicazione evidenzia delle richieste SQL inviate tramite HTTP. L'analisi si concentrerà sulla verifica delle vulnerabilità SQL Injection.

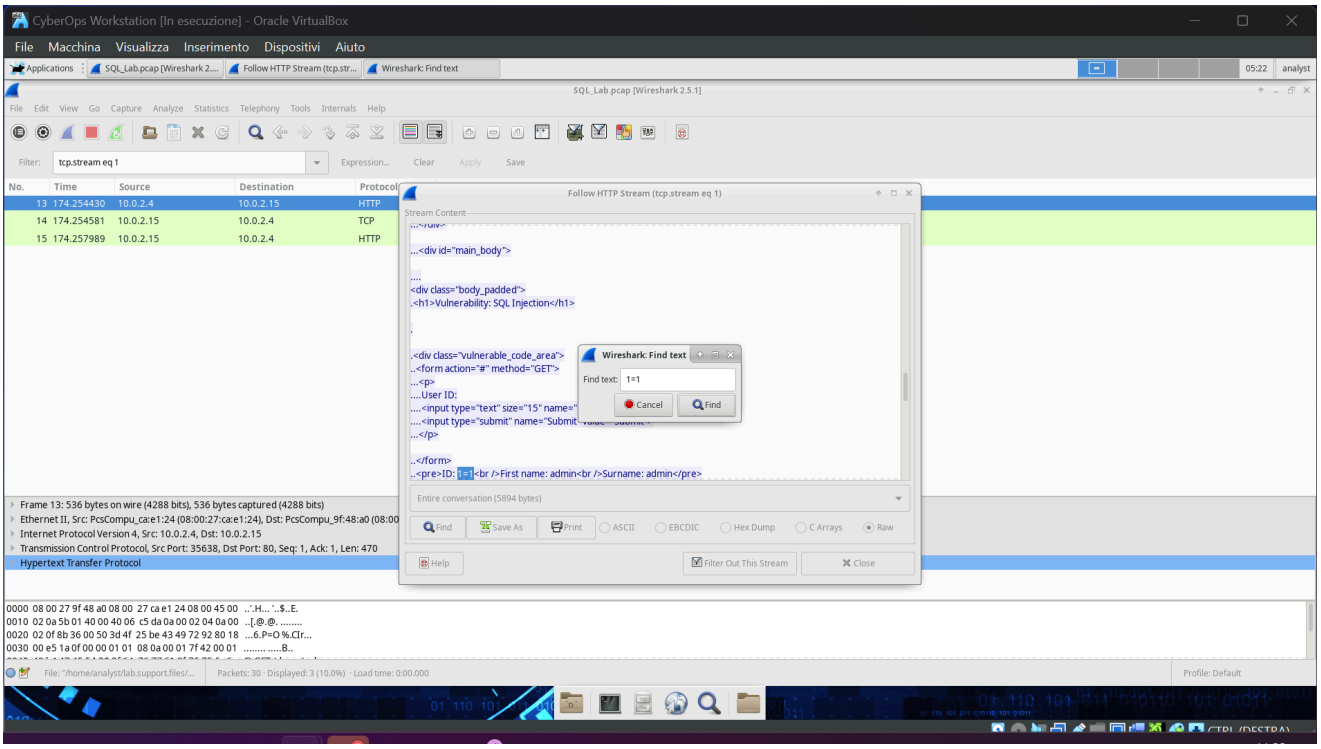
---

2. Dettaglio dei pacchetti HTTP

- L'immagine successiva mostra richieste HTTP che evidenziano l'invio di parametri SQL vulnerabili attraverso il metodo GET.
- Viene esaminata una vulnerabilità SQL, rappresentata dalla query:

sql:
id=1'+UNION+SELECT+NULL,database(),user(),...

Questa query SQL UNION tenta di estrarre informazioni dal database.



---

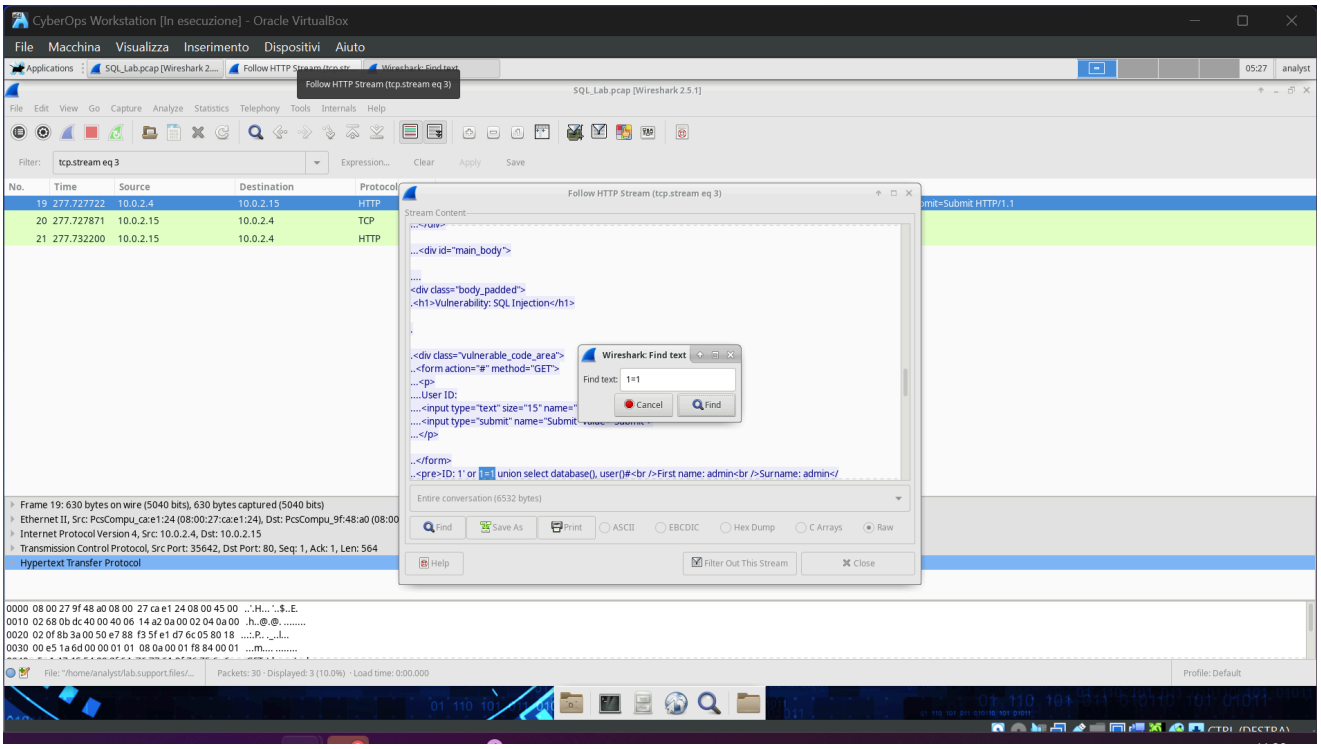
3. Esame dei flussi HTTP

- Seguiamo i flussi HTTP per osservare in dettaglio le risposte del server. Nell'immagine viene visualizzata una risposta HTTP, dove il server restituisce le informazioni di vulnerabilità.
- L'intestazione della risposta include dettagli sull'applicazione web, che utilizza **Apache 2.4.18** su un server **Ubuntu**.

---

4. Ricerca e conferma delle vulnerabilità

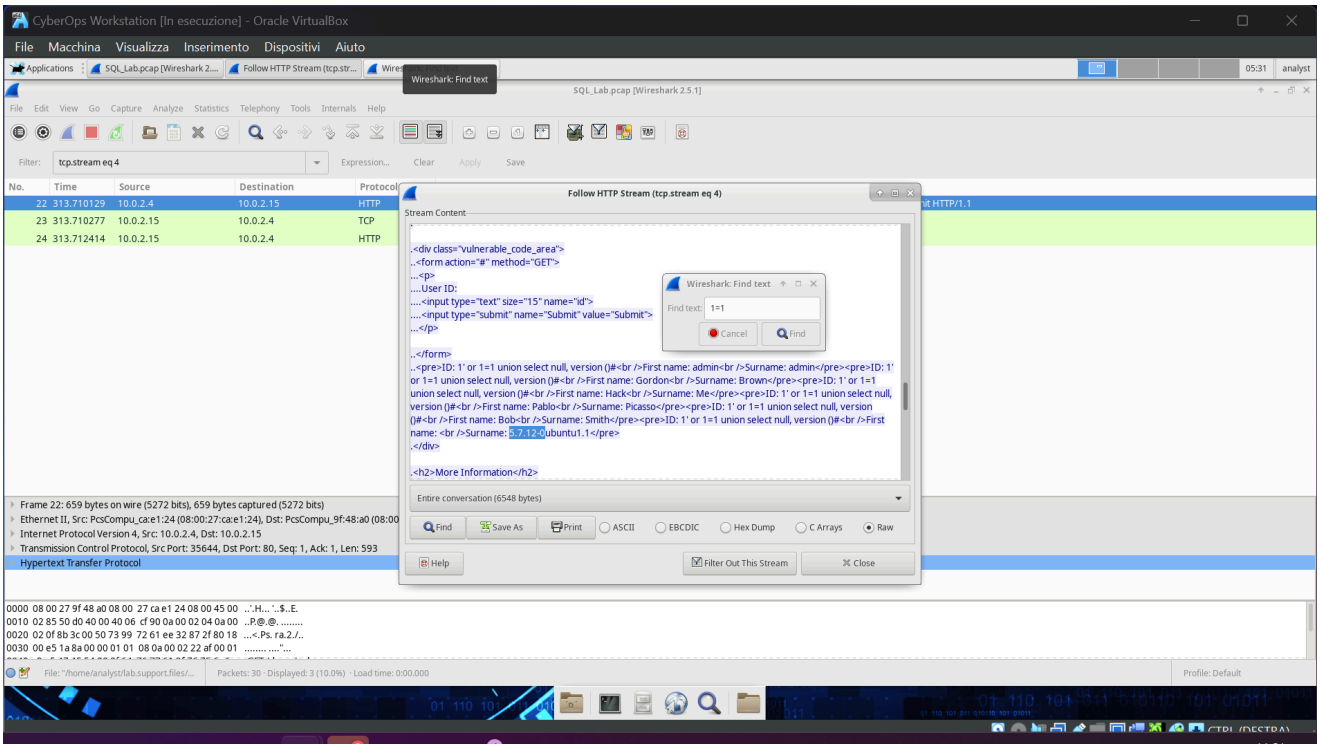
- Le immagini evidenziano l'uso del filtro di ricerca "1=1", confermando che il server è vulnerabile alla SQL Injection.
- Il payload iniettato viene eseguito con successo, come dimostrato dalle risposte del server che includono i dati richiesti.



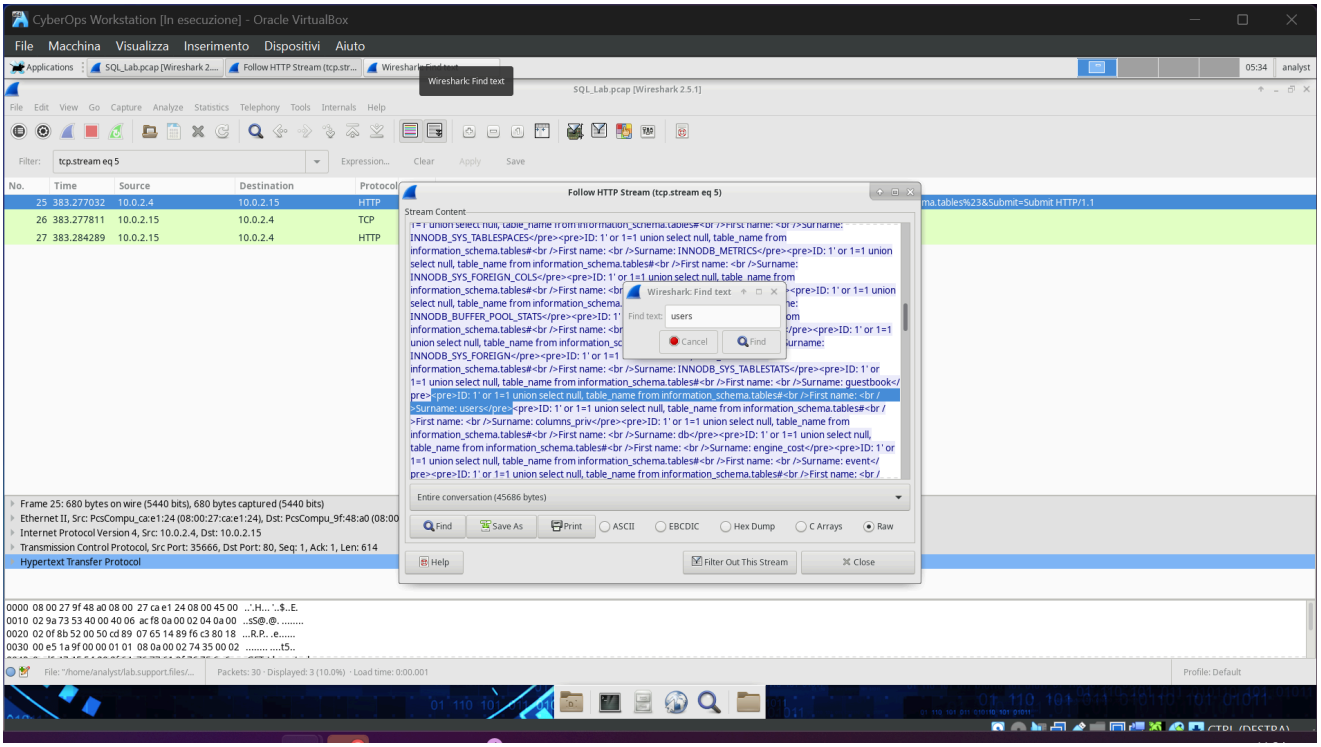
5. Ottenimento di dati sensibili

- L'immagine mostra una query che cerca di ottenere dati dal database, confermando la versione del server MySQL:

```
5.7.12 Ubuntu
```



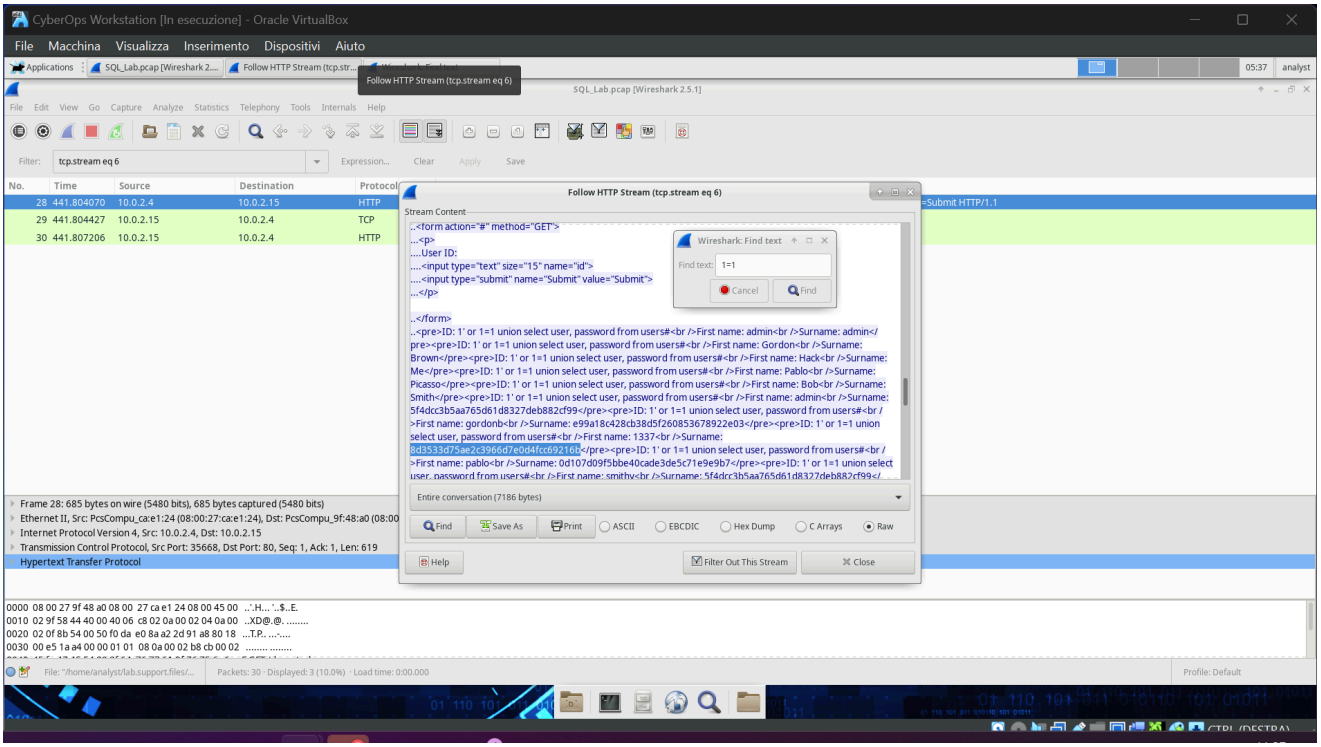
- Nell'immagine vediamo la visualizzazione delle informazioni utente e l'estrazione di tabelle dal database, che indicano una SQL Injection riuscita.



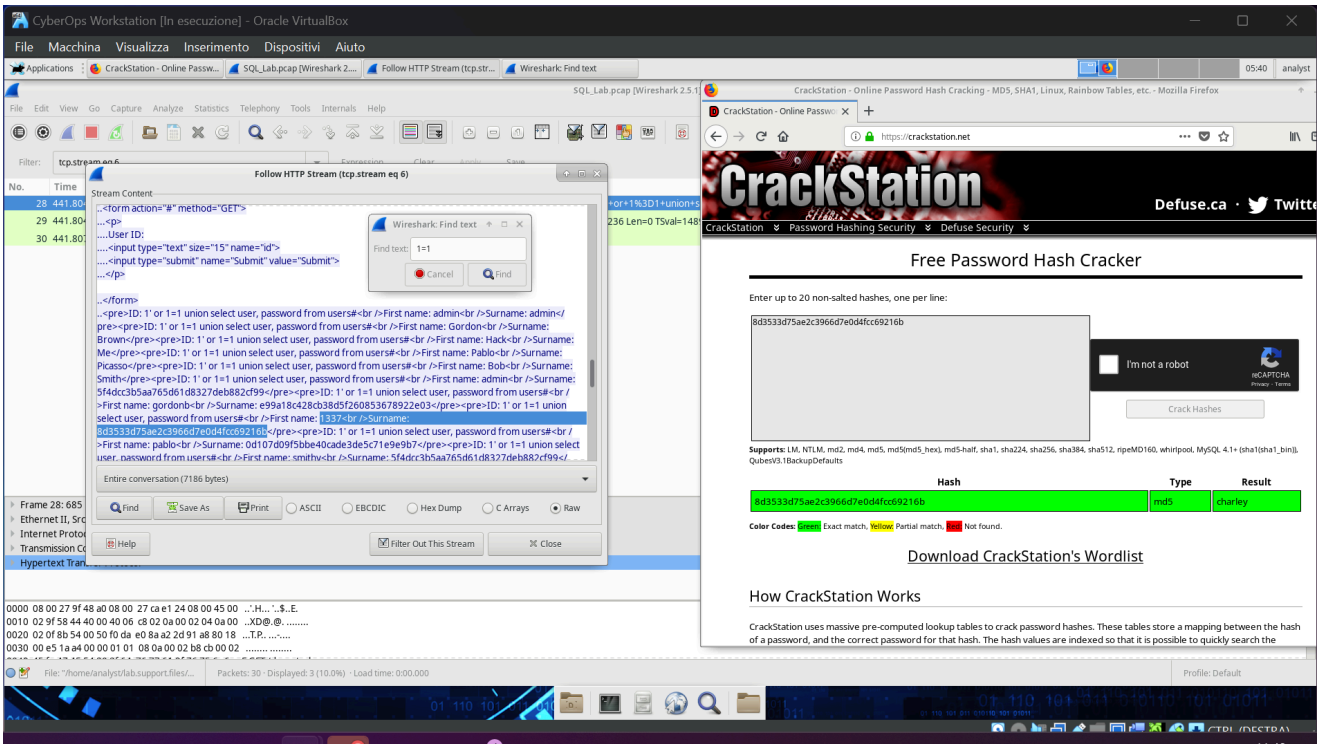
6. Hash e password

- Le immagini mostrano l'estrazione di hash di password. Utilizzando **CrackStation**, l'hash viene decodificato con successo, rivelando la password:

```
charley
```



- L'immagine mostra chiaramente il risultato della decodifica dell'hash MD5.



🔑 Chiavi:

[analisi, wireshark, sqlinjection, pentesting]