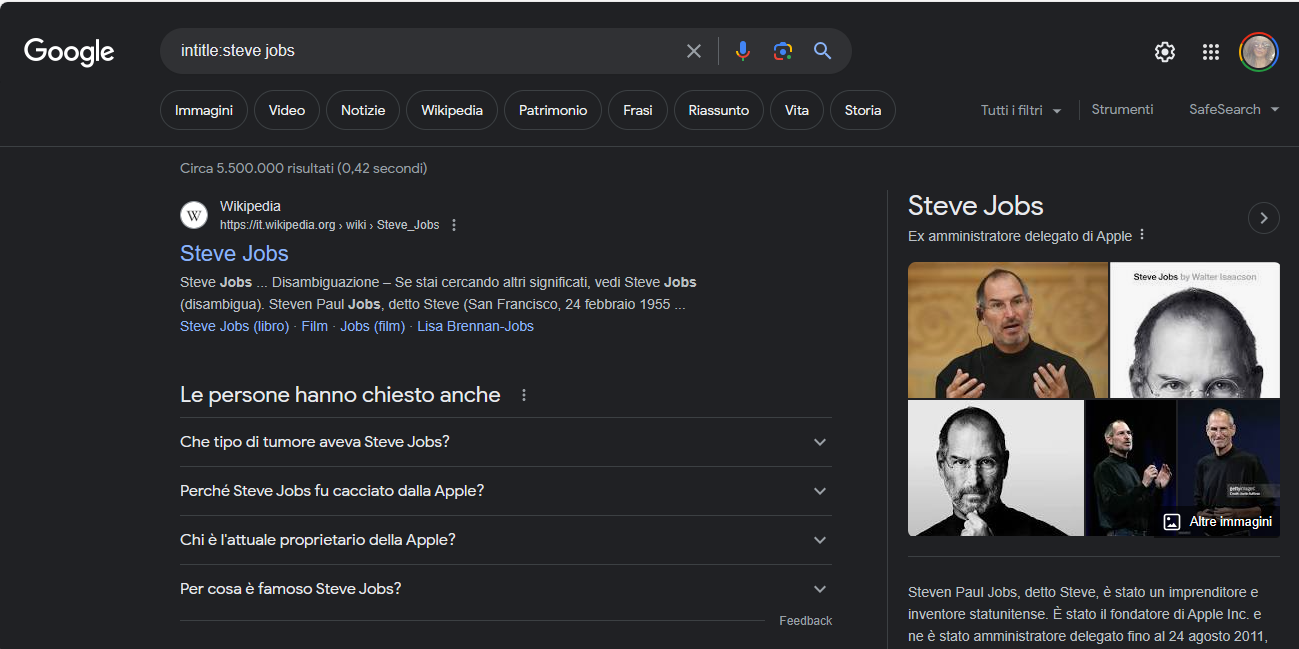
Nell’esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta.

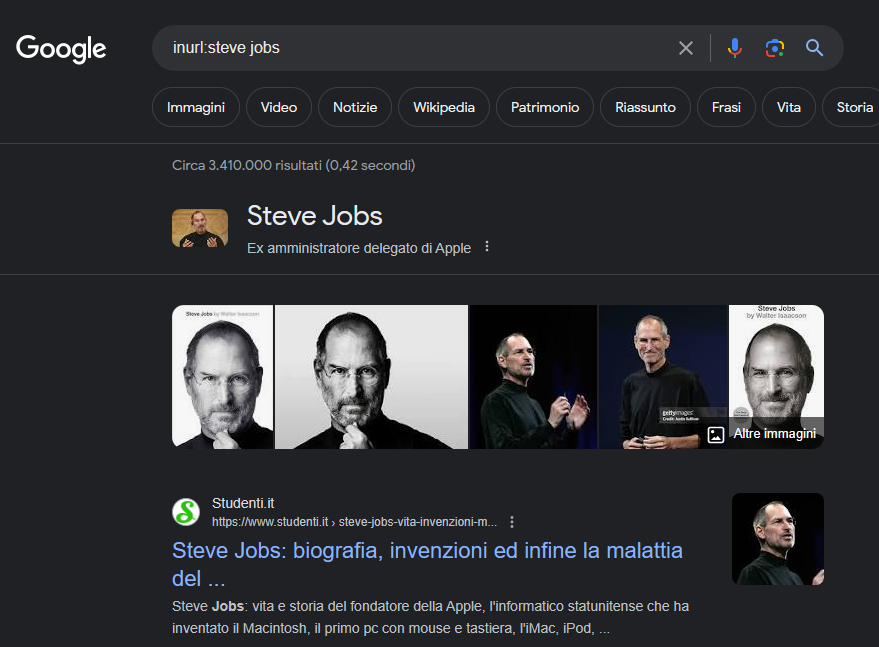
La buona riuscita di un pentesting è strettamente legata alla comprensione dell’organizzazione, al fine di allargare il nostro bersaglio e configurare degli attacchi ad hoc, in modo da rendere efficienti le analisi. A tale fine, una delle prime e fondamentali fasi sta nella raccolta delle informazioni.

Tutti noi, quotidianamente, usiamo Google per le più svariate ricerche. Ma pochi sanno che può essere utilizzato in maniera più precisa ed avanzata. Questo grazie all’utilizzo di particolari operatori (query) come ad esempio:

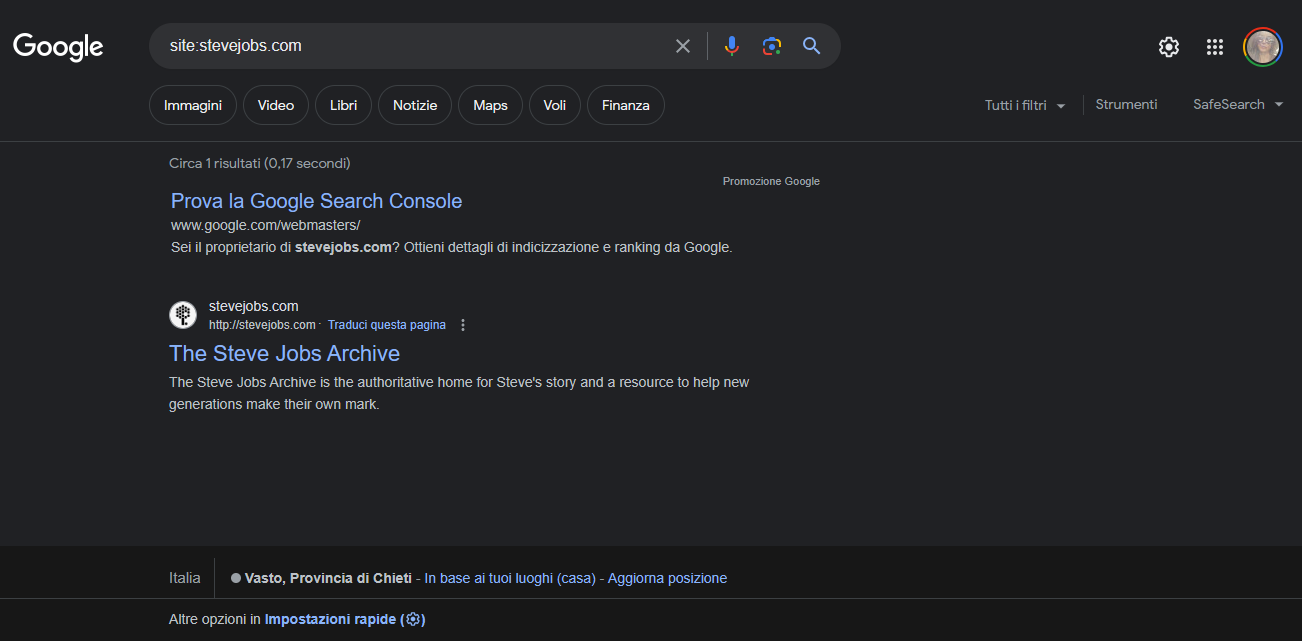
* Intitle 🡪 questa query restituirà tutte le pagine che hanno una parola, o nome, o ciò che ci interessa ricercare, nel loro titolo. Nel mio esempio useremo Steve Jobs:



* Inurl 🡪 ha lo stesso comportamento di intitle, ma a differenza di quest’ultimo, restituirà solo i risultati che contengono nell’URL la parola specificata:



* Site 🡪 è una parte dell’URL che non comprende i filename o tutto ciò che segue. È particolarmente utile per cercare contenuti circa una determinata azienda, o per restituire i sottodomini di uno specifico URL:



* Numrange 🡪 richiede 2 numeri come parametro, separati da un «-», e restituisce tutti i numeri nel range specificato; è utilizzato dai black hat hacker per recuperare numeri di telefono esistenti, codici sanitari e altre informazioni in formato numerico, per poi configurare degli attacchi personalizzati per ognuna delle vittime.
* Phonebook 🡪 l’operatore phonebook ricerca sul web numeri di telefono resi pubblici appartenenti sia a privati che non:

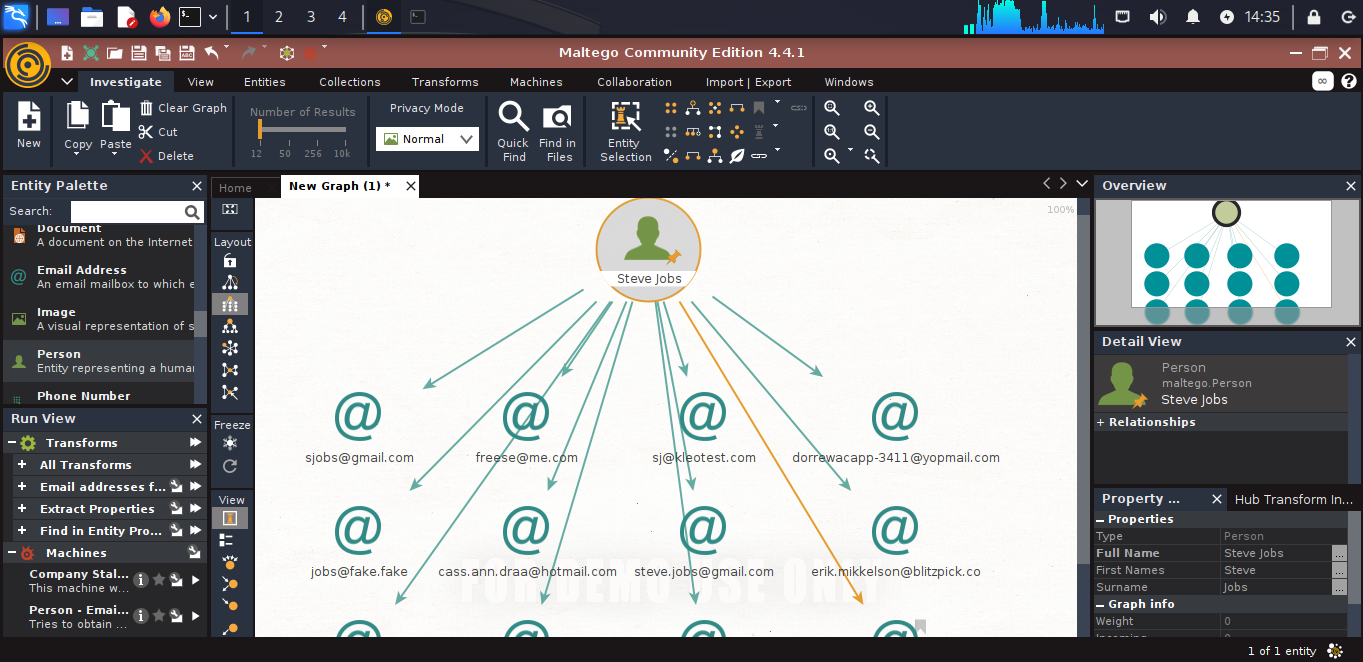
1 - rphonebook → contatti privati o «residenziali».

2 - bphonebook → contatti non privati esempio società, detti anche «business» contact .

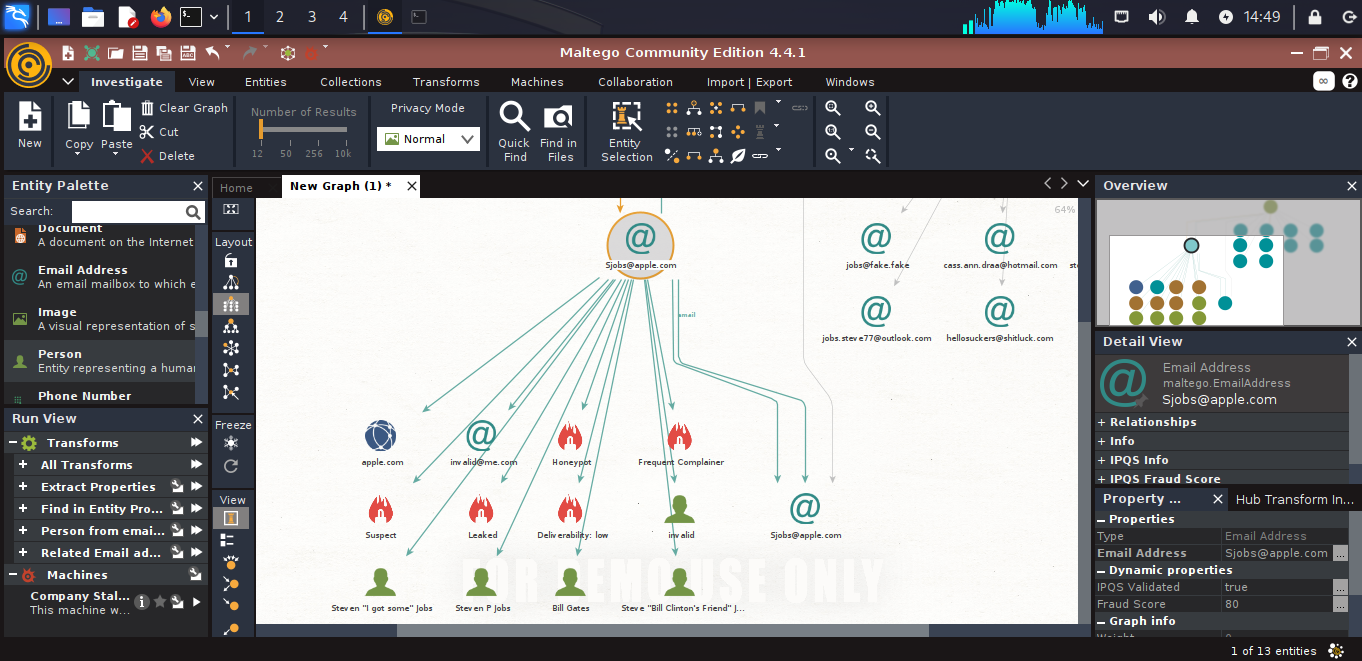
3 - phonebook → entrambi.

* Site crawling 🡪 tecnica utilizzata per scovare tutti i possibili sottodomini di un dato dominio. Con riferimento all’operatore avanzato «site:» possiamo aggiungere un ulteriore check per eliminare dalla query i risultati ridondanti. Es. site:stevejobs.com –www.stevejobs.com

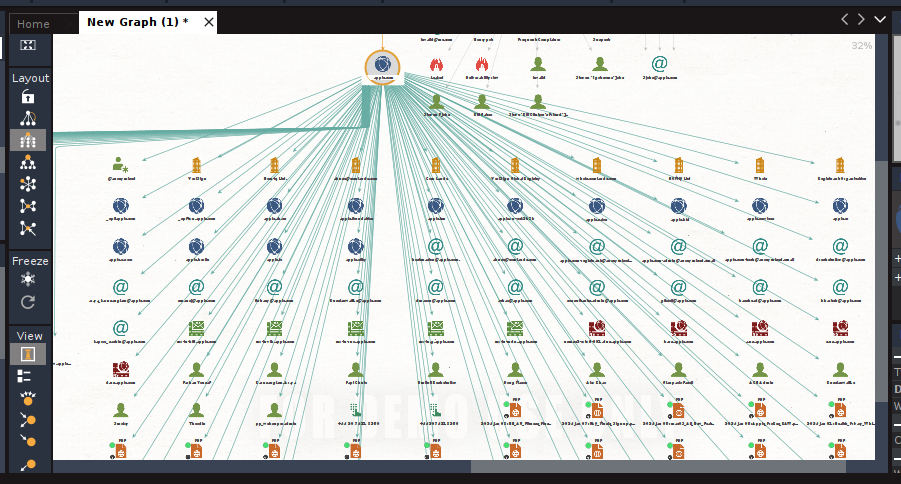
Un altro tools molto utilizzato nella ricerca di informazioni è Maltego, che recupera le informazioni e le correla tra di loro sfruttando sorgenti pubbliche:



Prima di tutto, dal pannello a sinistra, andiamo scegliere un nodo “0”, un punto di inizio della nostra ricerca. Nel mio caso, continuo con Steve Jobs quindi scelgo Person, assegno il nome di interesse ed inizio la ricerca. Il risultato (data la versione free) è di 10 risultati, ma con versioni premium potrebbero anche essere di più. In ogni caso per ogni voce possiamo approfondire la ricerca:



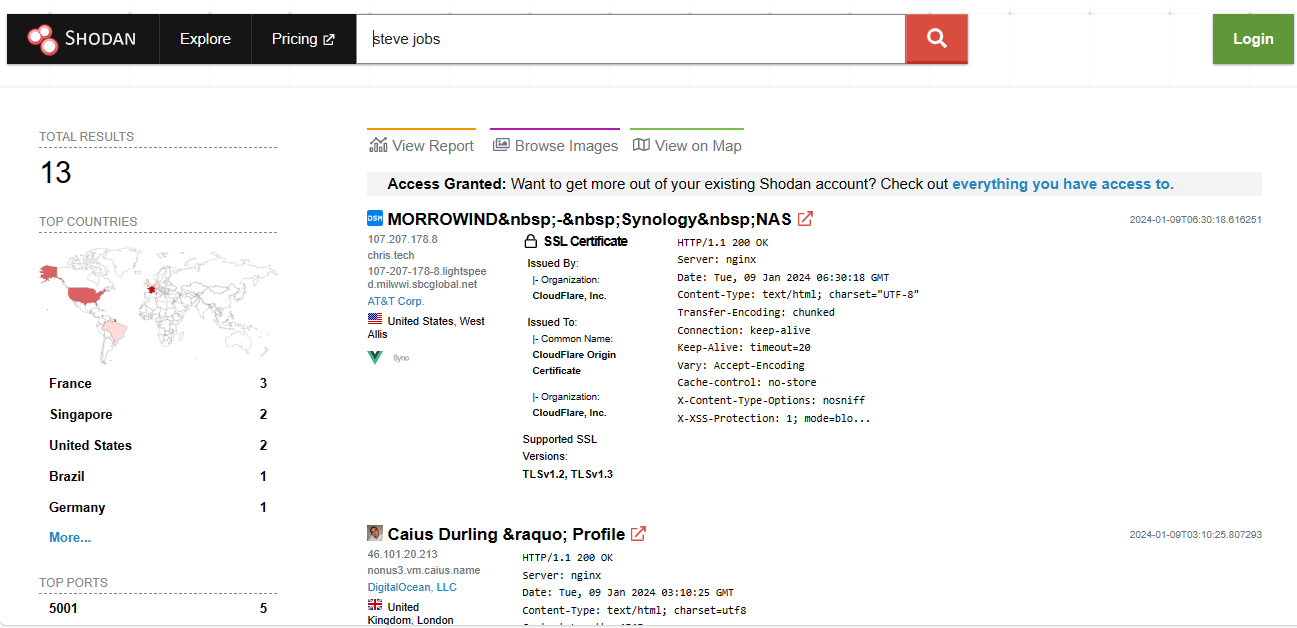
Il grafico inizia ad essere molto ricco di informazioni, Maltego ci aiuta graficamente ad identificare le info categorizzandole per website, phrase, person, URL, company, Location, abbiamo trovato anche dei profili di persone legate alla compagnia. Ad ogni nuovo approfondimento, accediamo a sempre maggiori informazioni:



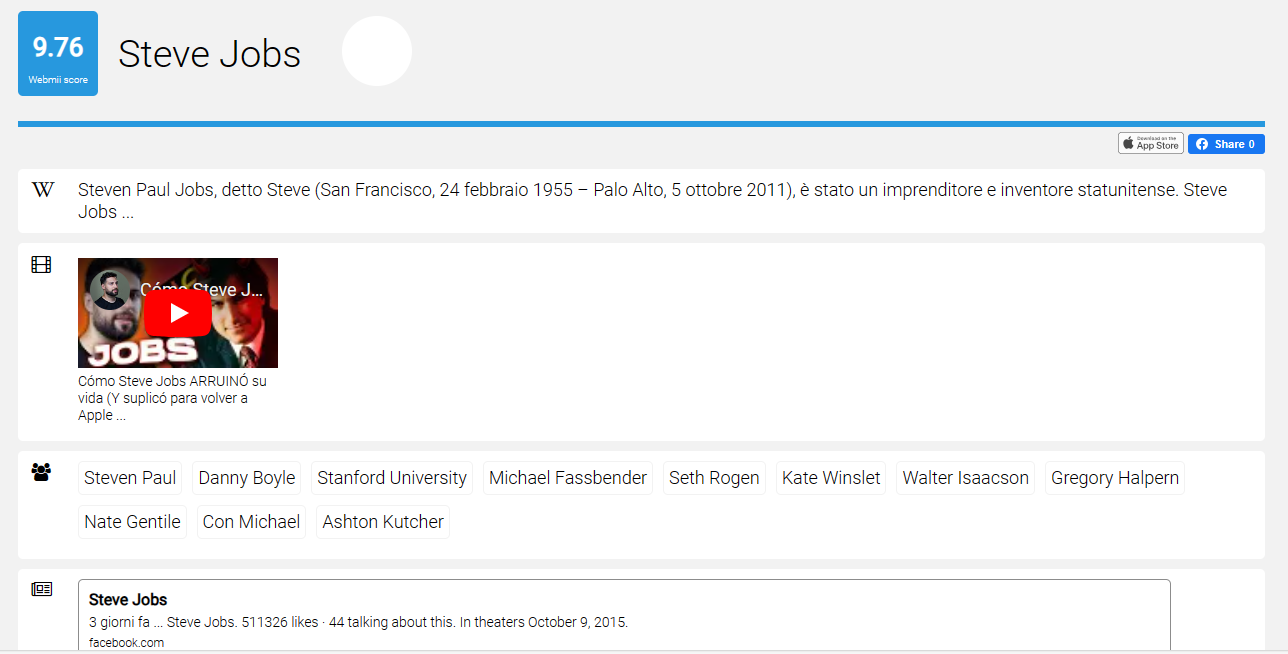
Ovviamente va usate con cautela, diligenza e autorizzazione. Risulta davvero uno strumento di ricerca di informazioni utilissimo.

Ma per una ricerca a 360 gradi possiamo, anzi dobbiamo, affiancare a questi anche altri strumenti noti:

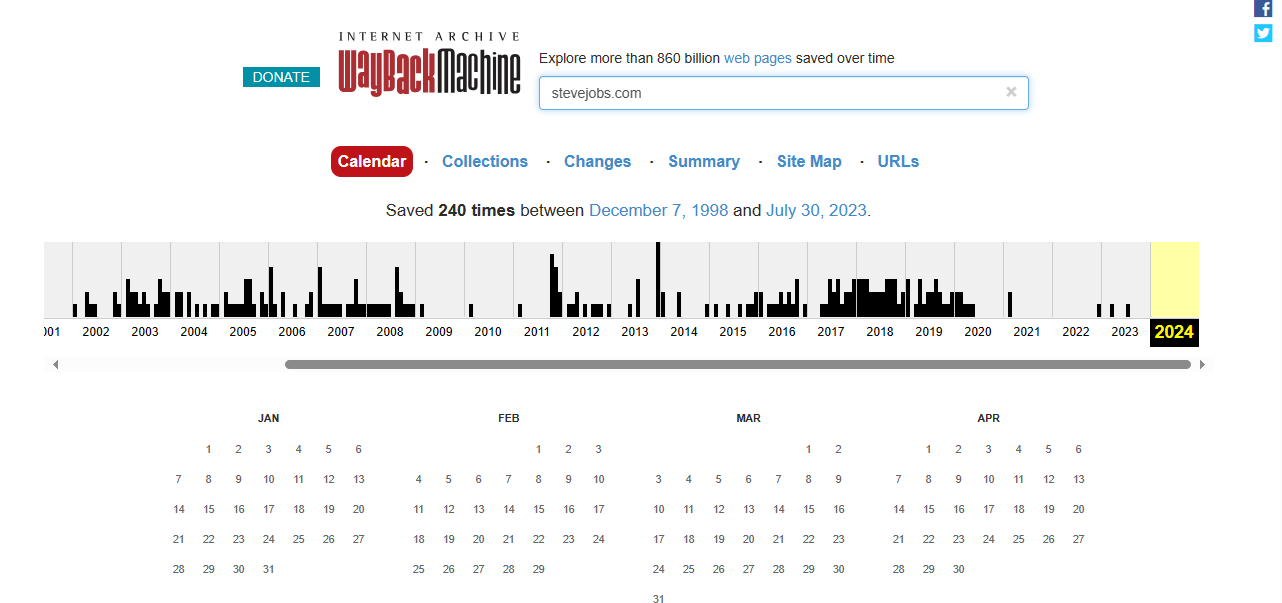
* Shodan 🡪 è un motore di ricerca specializzato in dispositivi connessi a Internet. Esso fornisce informazioni sulle porte e i servizi di dispositivi connessi, come server, router, stampanti, videocamere di sorveglianza. Questo motore di ricerca consente agli utenti di trovare dispositivi specifici in base a diversi parametri come il tipo di dispositivo, il sistema operativo, la località geografica e altro ancora:



* Webmii 🡪 è un motore di ricerca incentrato sulle persone che raccoglie informazioni da varie fonti online per creare profili completi e aggiornati su individui specifici. Utilizza dati da social media, siti web personali, blog e altre fonti pubbliche per fornire una panoramica complessiva di un individuo in un'unica pagina:



* Wayback Machine 🡪 Il principale scopo è quello di offrire agli utenti la possibilità di visualizzare versioni storiche di siti web e pagine web specifiche:



* Whois 🡪 è un protocollo di rete utilizzato per ottenere informazioni sul possesso di risorse Internet, come nomi di dominio, indirizzi IP e blocchi di indirizzi IP. Esso consente agli utenti di interrogare un database centralizzato per ottenere dettagli sulle entità che possiedono o gestiscono determinate risorse su Internet:

