



Epicode

Esercizio S5/L2




Lo scopo dell'esercizio di oggi sarà familiarizzare con i tool principali per fare Osint, in questo caso faremo due tipi di ricerche utilizzando due tecniche diverse:

- 1) Con le tecniche passive
- 2) Con le tecniche attive

La ricerca per il mio esercizio sarà incentrata su l'Università degli studi di Palermo.

TECNICHE PASSIVE



Le tecniche passive si concentrano sulla raccolta di informazioni senza interagire direttamente con la fonte. Queste tecniche mirano a raccogliere dati pubblicamente disponibili e legalmente accessibili per ottenere informazioni utili.

Le tecniche passive sono importanti nell'OSINT poiché consentono di ottenere informazioni in modo discreto e non intrusivo, evitando di sollevare sospetti o violare la privacy. Alcuni esempi di tecniche passive includono:

Ricerca su Motori di Ricerca

Analisi di Social Media

Analisi di Siti Web

Ricerca di Domini e Indirizzi IP

Informazioni trovate grazie alle tecniche passive:



Sito web

Indirizzo: Piazza Marina, 61, 90133 Palermo PA

Studenti: 40 422 (2019)

Stato: Italia

Fondazione: 12 gennaio 1806, Palermo

Rettore: Massimo Midiri

Telefono: 091 2388 6472

Altre sedi: Agrigento, Caltanissetta, Erice

Soprannome: UniPa

Instagram

Gruppo Facebook

Articoli di giornale

TECNICHE ATTIVE



A differenza delle tecniche passive, che si concentrano sulla raccolta di informazioni senza coinvolgere direttamente la fonte, le tecniche attive richiedono una partecipazione più diretta per ottenere informazioni specifiche che potrebbero non essere facilmente accessibili attraverso le tecniche passive utilizzando quindi dei tool specifici come “Maltego”.

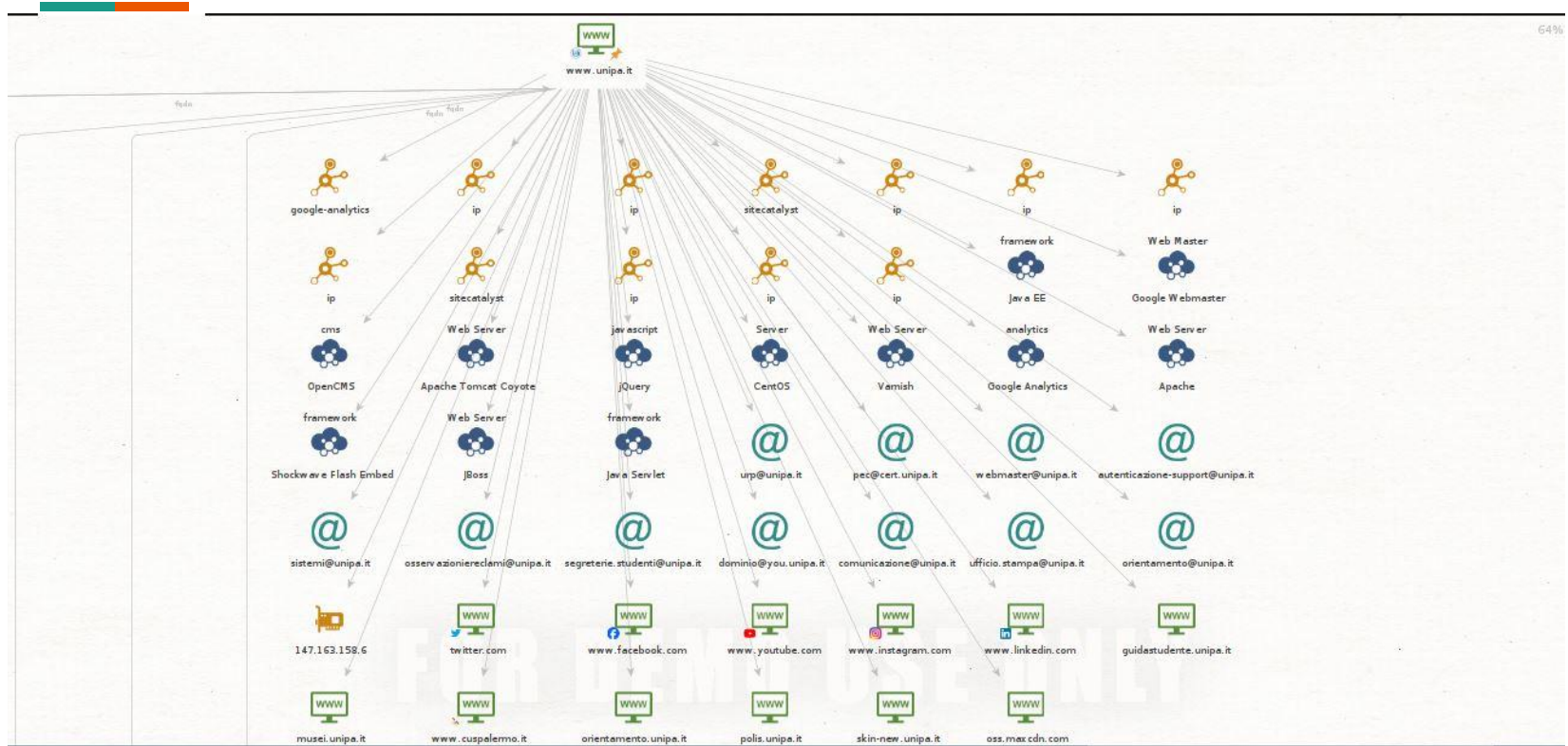
Il tool in questione ci permette di:

Raccogliere informazioni

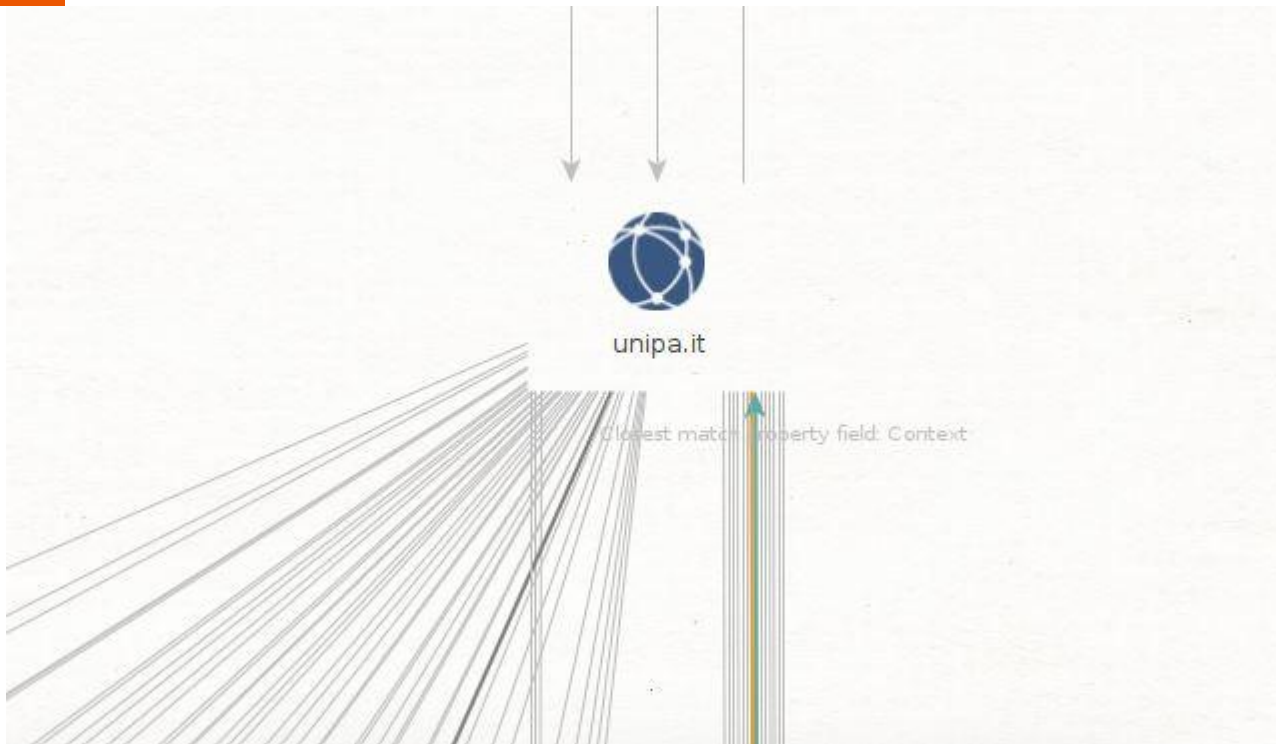
Visualizzare le relazioni tra utenti, aziende, reti etc.

Analizzare le reti

Cercando solamente il sito web www.unipa.it sono già riuscito a trovare molte più informazioni rispetto alle tecniche passive, ma proviamo a scavare più in fondo per cercare ancora più informazioni:



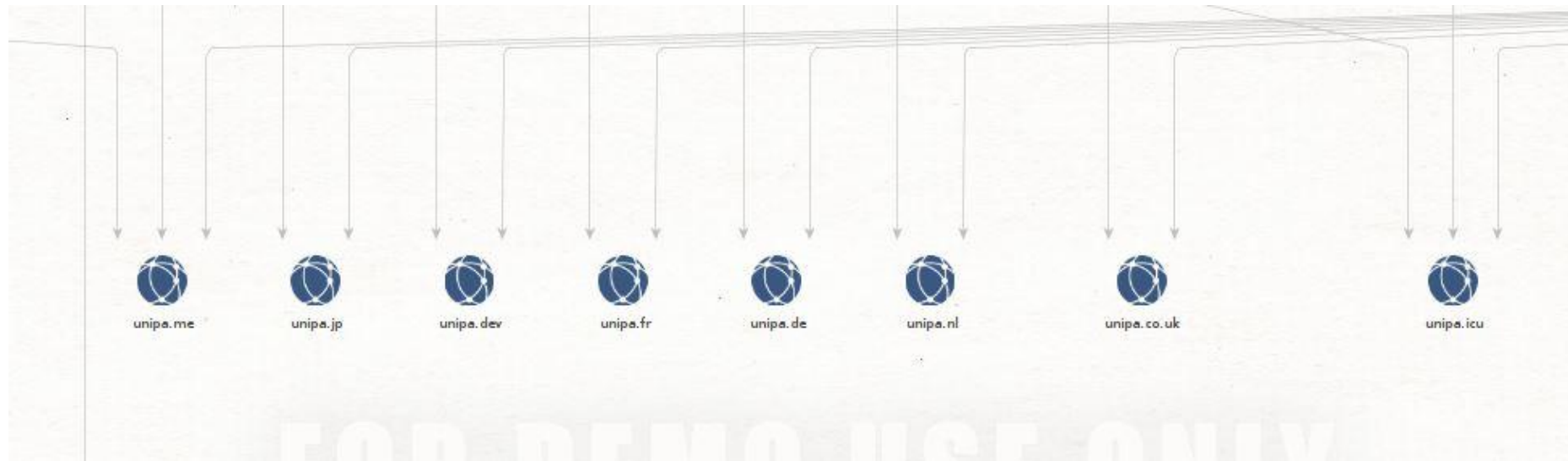
apro unipa.it:

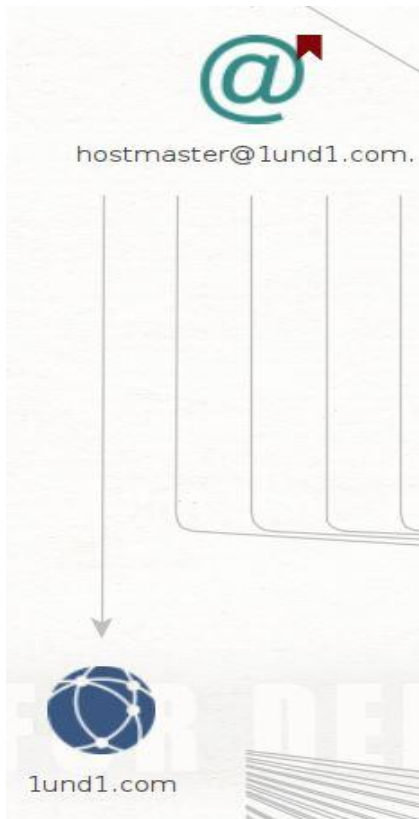


Grazie ad esso sono riuscito a trovare informazioni più interne: come chi lavora su unipa; le loro mail; gli NS ed i DNS del sito

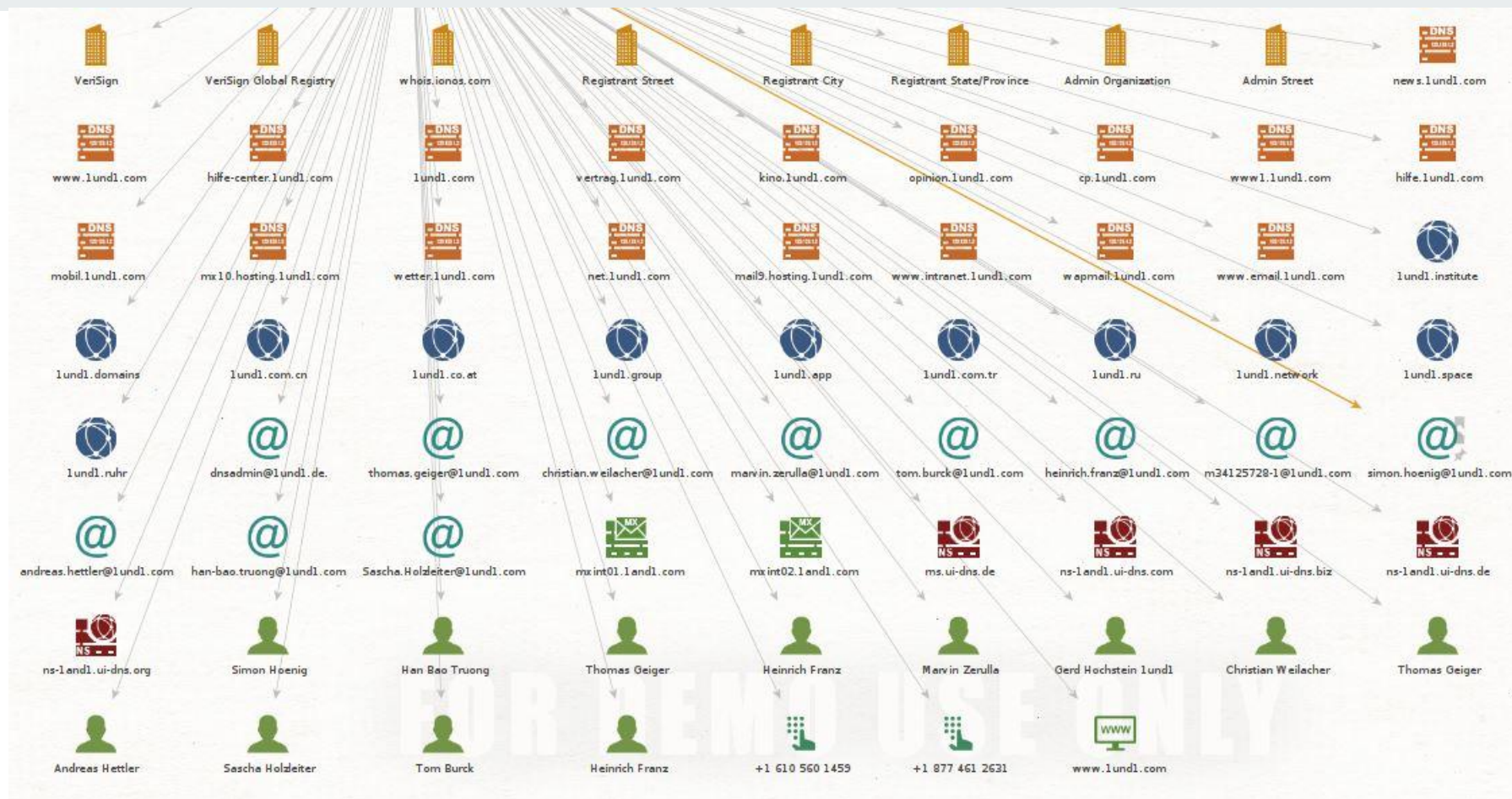


Proviamo ad entrare ancora più a fondo grazie ad uno dei vari domini che Maltego ha trovato:





riesco a trovare una rete di informazioni molto vasta di un sito web tedesco “www.1und1.com” che si occupa di vendere dispositivi elettronici come smartphone, computer etc etc.



Conclusioni finali e differenze sostanziali tra le due tecniche



Google:

Google è principalmente un motore di ricerca che fornisce risultati in base alle parole chiave immesse.

Offre un accesso rapido a una vasta gamma di informazioni pubblicamente disponibili.

Le informazioni ottenute tramite Google sono quelle già presenti e indicizzate sui siti web pubblici, si tratta di dati che gli utenti hanno reso accessibili online.

Google può offrire risultati solo fino a un certo livello di profondità, e molti dati più dettagliati potrebbero non essere facilmente accessibili tramite una ricerca diretta.

Ma è comunque una risorsa molto efficace per cercare notizie recenti e informazioni pubblicamente condivise online.

Conclusioni finali e differenze sostanziali tra le due tecniche



Maltego

Maltego si concentra sull'analisi delle relazioni tra diversi tipi di entità (persone, organizzazioni, siti web) attraverso grafici interattivi.

Maltego può aggregare e correlare dati provenienti da diverse fonti, offrendo una visione più completa delle connessioni tra le informazioni.

Può automatizzare il processo di raccolta e analisi delle informazioni, rendendo più efficiente la visualizzazione delle connessioni tra diverse entità.

Maltego può integrare informazioni da fonti come social media, database pubblici, registri WHOIS e altro ancora, consentendo un'analisi più approfondita.

Fornisce una visione grafica delle reti di informazioni, aiutando a identificare relazioni e pattern che potrebbero non emergere facilmente attraverso una ricerca su Google.

Conclusioni finali e differenze sostanziali tra le due tecniche



In sintesi, mentre Google è efficace per ottenere informazioni rapidamente attraverso ricerche generiche, Maltego è più focalizzato sull'analisi dettagliata delle relazioni e sulla visualizzazione delle connessioni tra dati provenienti da diverse fonti. L'utilizzo di entrambe però può essere complementare per un'analisi OSINT più completa.