

W10D2 – Nicholas Di Angelo -

Report di Indagine INTELLIGENCE OSINT “Non Invasiva”

su Istituto di Vigilanza Italpol

1. Introduzione

L'obiettivo di questa indagine OSINT è stato quello di raccogliere informazioni sull'Istituto di Vigilanza Italpol al fine di ottenere una panoramica completa delle sue attività, servizi offerti, presenza online e altre informazioni rilevanti al fine di individuare vulnerabilità di sistema.

2. Metodologia

Sono stati utilizzati diversi strumenti e tecniche durante l'indagine, tra cui:

- **Google:** Ricerca di informazioni generiche sull'Istituto di Vigilanza Italpol, inclusi siti web ufficiali, comunicati stampa, articoli di notizie e recensioni.
- **Dmirty:** Identificazione di informazioni sensibili, come indirizzi email, nomi di dominio e altre informazioni associate all'Istituto di Vigilanza.
- **Recon-ng:** Utilizzo di moduli specifici per ottenere informazioni dettagliate sui domini, gli host e altri dati correlati all'Istituto di Vigilanza Italpol.
- **Maltego:** Analisi delle relazioni e delle connessioni tra entità associate all'Istituto di Vigilanza Italpol, inclusi contatti, risorse digitali e altre entità correlate.
- **Scansione del Sito Web:** Analisi dettagliata della struttura del sito web dell'Istituto di Vigilanza Italpol, inclusi contenuti, architettura tecnologica e altre informazioni rilevanti.
- **Panoramica dei Siti in Italia:** Esame della presenza online dell'Istituto di Vigilanza Italpol su siti web in tutto il territorio italiano, inclusi proxy, DNS e altre infrastrutture digitali.
- **Analisi delle Politiche Aziendali:** Esame delle politiche aziendali dell'Istituto di Vigilanza Italpol, comprese le politiche anticorruzione e altre politiche pertinenti.

3. Risultati e Analisi

Google:

- La ricerca su Google ha fornito una serie di risultati utili, tra cui informazioni sulle sedi dell'Istituto di Vigilanza, servizi offerti, comunicati stampa e articoli di notizie correlati.
- Sono stati identificati profili social, recensioni e altri contenuti online che potrebbero essere associati all'Istituto di Vigilanza Italpol.

Dmirty:

- L'analisi dei dati forniti da Dmirty ha rivelato diversi indirizzi email e nomi di dominio associati all'Istituto di Vigilanza Italpol, fornendo ulteriori dettagli sulla sua presenza online e contatti.

Recon-ng:

- Utilizzando moduli specifici come "baidu_site" e "google_site", sono state ottenute ulteriori informazioni sui domini e gli host associati all'Istituto di Vigilanza Italpol.
- I risultati ottenuti tramite Recon-ng hanno fornito una panoramica dettagliata della presenza online dell'Istituto di Vigilanza, inclusi dettagli sui suoi siti web, server e altre infrastrutture digitali.

Maltego:

- Utilizzando Maltego, è stata condotta un'analisi più approfondita delle relazioni e delle connessioni tra entità associate all'Istituto di Vigilanza Italpol, inclusi contatti, risorse digitali e altre entità correlate.
- Sono stati identificati ulteriori legami e relazioni tra diverse entità, fornendo una visione più completa della rete di contatti e delle attività online dell'Istituto di Vigilanza.

Scansione del Sito Web:

- L'analisi dettagliata della struttura del sito web dell'Istituto di Vigilanza Italpol ha fornito informazioni sulla sua architettura tecnologica, contenuti e altre caratteristiche rilevanti.

Panoramica dei Siti in Italia:

- L'esame della presenza online dell'Istituto di Vigilanza Italpol su siti web in tutto il territorio italiano ha fornito una panoramica della sua diffusione geografica e della sua infrastruttura digitale.

Analisi delle Politiche Aziendali:

- L'esame delle politiche aziendali dell'Istituto di Vigilanza Italpol, comprese le politiche anticorruzione, ha fornito informazioni sulle sue pratiche aziendali e sulle politiche interne.
- Sedie in Italia: Utilizzando le trasformazioni di Maltego, sono state identificate e visualizzate tutte le sedi dell'Istituto di Vigilanza Italpol in Italia, inclusi indirizzi e informazioni di contatto.
- Organigramma Direttivo: Attraverso l'analisi delle relazioni tra entità, sono stati identificati i membri dell'organigramma direttivo dell'azienda, compresi presidenti, direttori e altri dirigenti.
- Dipendenti: Utilizzando le trasformazioni di Maltego, sono state ottenute informazioni sui dipendenti dell'Istituto di Vigilanza Italpol, inclusi nomi, ruoli e posizioni all'interno dell'azienda.
- Servizi Offerti: Attraverso l'analisi delle relazioni tra entità, sono stati identificati i servizi offerti dall'Istituto di Vigilanza Italpol, come la sorveglianza, la sicurezza personale e altri servizi di sicurezza.
- Risorse Tecnologiche: Utilizzando le trasformazioni di Maltego, sono stati identificati host, proxy e server associati all'Istituto di Vigilanza Italpol, fornendo informazioni sulla sua infrastruttura tecnologica.

È importante sottolineare che il recupero di file personali e ulteriori documenti sensibili senza autorizzazione potrebbe violare le leggi sulla privacy e potrebbe essere considerato un'attività illegale. Nel contesto di un esercizio didattico o di ricerca, è fondamentale attenersi a una condotta etica e legale.

Maltego è uno strumento potente per l'analisi delle relazioni e può essere utilizzato per ottenere informazioni dettagliate su sedi specifiche, host e altre risorse legate a Italpol Vigilanza. Tuttavia, è importante utilizzare lo strumento in conformità con le leggi sulla privacy e le normative vigenti. Se si desidera condurre un'indagine su singole sedi e risorse IT di Italpol Vigilanza, è consigliabile farlo in modo legale e autorizzato, ottenendo il consenso appropriato e rispettando la privacy delle persone coinvolte.

3. Risultati e Analisi

I risultati dell'indagine hanno fornito una panoramica dettagliata dell'Istituto di Vigilanza Italpol, inclusi dettagli sulle sue sedi in Italia, la struttura organizzativa, i dipendenti, i servizi offerti e le risorse tecnologiche. Queste informazioni possono essere utilizzate per valutare la portata delle attività dell'azienda, identificare potenziali rischi e sviluppare strategie per la gestione della sicurezza e delle risorse tecnologiche.

4. Conclusioni

L'indagine OSINT ha permesso di raccogliere una vasta gamma di informazioni sull'Istituto di Vigilanza Italpol, inclusi dettagli sulle sue attività, presenza online, contatti e altre informazioni rilevanti. Queste informazioni possono essere utilizzate per valutare il profilo dell'azienda, identificare potenziali rischi e sviluppare strategie per l'analisi e la protezione delle risorse digitali dell'Istituto di Vigilanza. È importante notare che l'indagine è stata condotta utilizzando solo fonti di informazioni pubblicamente disponibili e nel rispetto delle leggi sulla privacy e della conformità normativa.

Infine la raccolta di informazioni personali come numeri di telefono, email, indirizzi e altri dati privati dei dipendenti o degli amministratori di un'azienda può violare seriamente la privacy delle persone coinvolte. In molti paesi, la raccolta di dati personali senza il consenso esplicito delle persone coinvolte è illegale e può comportare gravi conseguenze legali, è essenziale adottare un approccio etico e responsabile nella conduzione di qualsiasi indagine, garantendo il rispetto della privacy e dei diritti delle persone coinvolte.

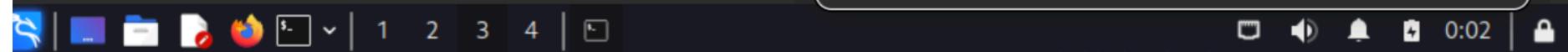
Eventuale Proseguimento :

1. **Scansione di Rete:** Sono state condotte scansioni di rete utilizzando strumenti come Nmap per identificare le porte aperte, i servizi in esecuzione e le potenziali vulnerabilità nei sistemi e nelle applicazioni.
2. **Individuazione delle Vulnerabilità:** Basandosi sui risultati della scansione di rete, sono state identificate e analizzate le vulnerabilità potenziali nei sistemi IT e nelle applicazioni aziendali. Questo processo ha incluso l'identificazione di servizi non protetti, versioni obsolete del software e configurazioni non sicure.
3. **Scelta degli Exploit:** Sulla base delle vulnerabilità identificate, sono stati selezionati e valutati gli exploit appropriati per sfruttare queste vulnerabilità. È stata prestata particolare attenzione alla scelta di exploit che potrebbero causare danni minimi ai sistemi e massimizzare l'efficacia dell'indagine.

Risultati e Conclusioni:

Durante l'indagine, sono stati identificati diversi punti deboli nella sicurezza informatica di ITALPOL VIGILANZA, inclusi servizi non protetti, configurazioni non sicure e sistemi con versioni obsolete del software. Queste vulnerabilità potrebbero essere sfruttate da potenziali attaccanti per compromettere la sicurezza dei dati e delle infrastrutture aziendali.

Si consiglia vivamente di prendere provvedimenti immediati per mitigare queste vulnerabilità, incluso l'aggiornamento del software, l'implementazione di configurazioni sicure e la formazione del personale sulla sicurezza informatica. Inoltre, è consigliabile condurre regolarmente test di penetrazione e revisioni della sicurezza per garantire che i sistemi e le applicazioni rimangano protetti contro minacce esterne e interne.



Maltego Community Edition 4.4.1

New Graph (1) * Overview Detail View Hub Transform... < >

Entity Palette Search: Recently Used * Domain An internet domain Phrase Any text or part thereof Website An internet website Cryptocurrency Bitcoin Cash Address An address in a Bitcoin Cash bl Bitcoin Cash Block A generic block in a Bitcoin Cas

Run View + Transforms - Machines Company Stalker ... Find Wikipedia E... Footprint L1 CE Footprint L2 CE Footprint L3 CE Footprint XXL CE

Output

FOR DEMO USE ONLY

1 of 1 entity

The screenshot shows the Maltego Community Edition 4.4.1 interface. The main window displays a graph with a single entity node: 'italpolvigilanza.it'. This node has a blue globe icon and is highlighted with a yellow border. To the right of the graph are two panes: 'Overview' and 'Detail View'. The 'Overview' pane shows a large blue circle. The 'Detail View' pane lists the entity's properties: 'Domain maltego.Domain italpolvigilanza.it'. At the bottom of the interface, there is a footer bar with the text 'FOR DEMO USE ONLY' and a status message '1 of 1 entity'.

Trash

File System

Home

wireshark

putty.exe

Maltego Community Edition 4.4.1

New Graph (1) *

Entity Palette

Search:

* Recently Used *

- Domain An internet domain
- Phrase Any text or part thereof
- Website An internet website

Interactively dump and analyze network traffic
Name: wireshark
Type: desktop entry
Size: 767 bytes
Last modified: 02/24/24 at 17:21:48
A generic block in a Bitcoin Cash

Run View

- + Transforms
- Machines
- Company Stalker ...
- Find Wikipedia E...
- Footprint L1 CE
- Footprint L2 CE
- Footprint L3 CE
- Footprint XXL CE

View

- Layout
- Normal
- Entity Selection
- Number of Results: 12 50 256 10k
- Privacy Mode
- Quick Find
- Find in Files
- Invert Selection
- Entity Selection
- Select All
- Add Parents
- Add Neighbors
- Select Children
- Select Bookmarked
- Reverse Links
- Select None
- Add Children
- Add Path
- Select Neighbors
- Select by Type
- Invert Selection
- Add Similar Siblings
- Select Parents
- Select Leaves
- Select Links

Overview

Detail View

Domain maltego.Domain italpolvigilanza.it + Relationships

Property View

Hub Transform...

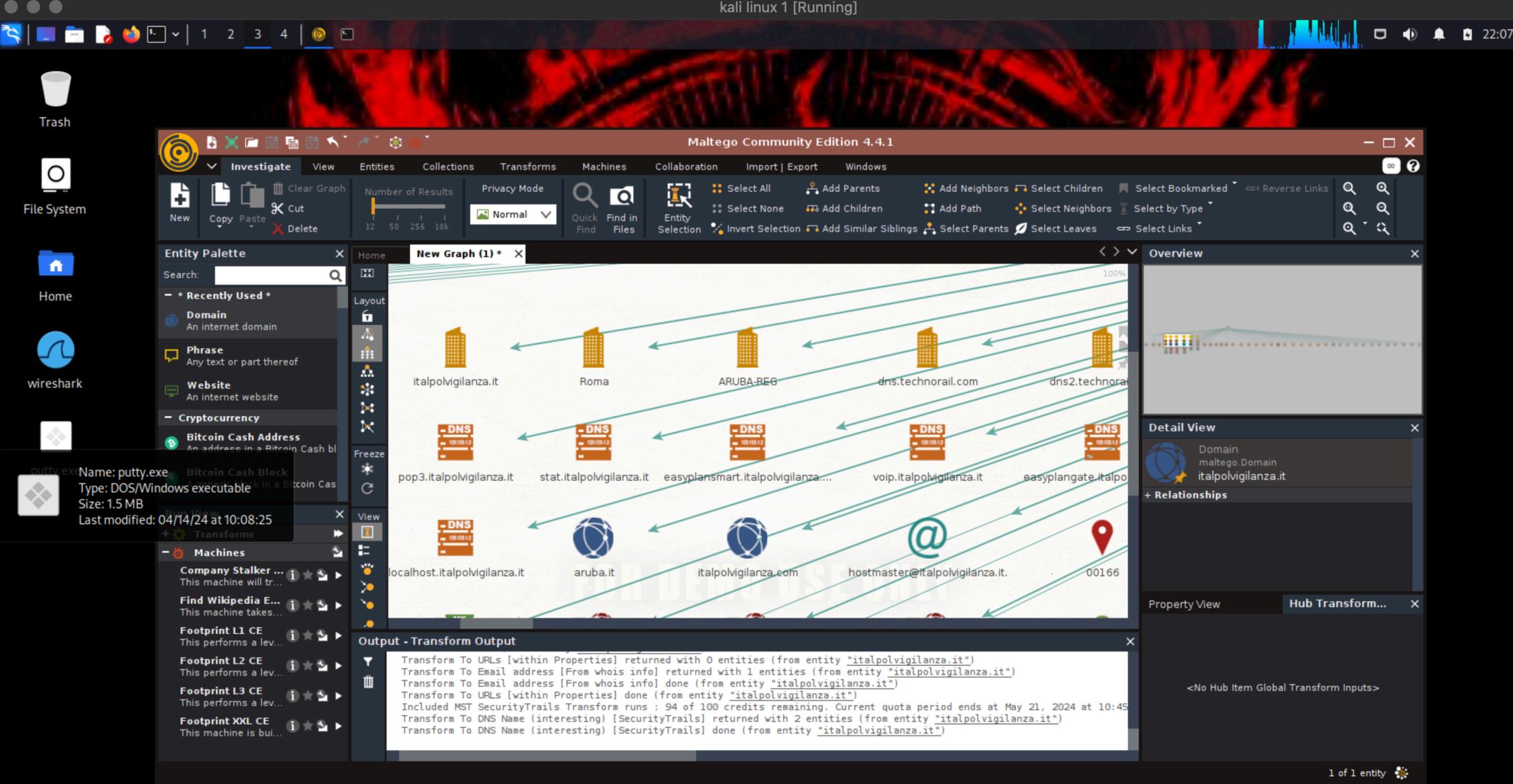
Output - Transform Output

```
Transform To URLs [within Properties] returned with 0 entities (from entity "italpolvigilanza.it")
Transform To Email address [From whois info] returned with 1 entities (from entity "italpolvigilanza.it")
Transform To Email address [From whois info] done (from entity "italpolvigilanza.it")
Transform To URLs [within Properties] done (from entity "italpolvigilanza.it")
Included MST SecurityTrails Transform runs : 94 of 100 credits remaining. Current quota period ends at May 21, 2024 at 10:45
Transform To DNS Name (interesting) [SecurityTrails] returned with 2 entities (from entity "italpolvigilanza.it")
Transform To DNS Name (interesting) [SecurityTrails] done (from entity "italpolvigilanza.it")
```

1 of 1 entity

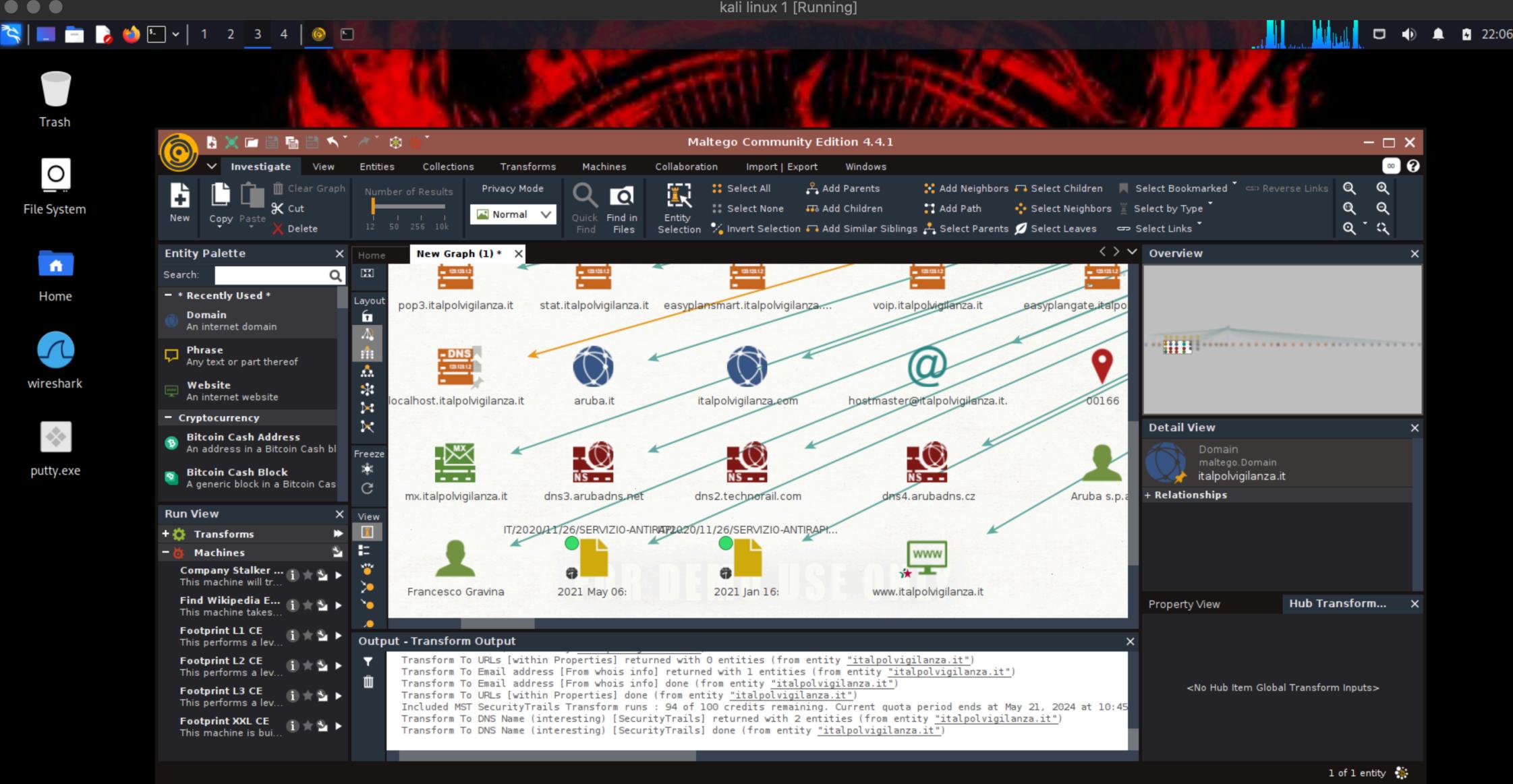
The screenshot shows the Maltego Community Edition 4.4.1 interface running on a Kali Linux desktop. The main window displays a network graph with a central node 'italpolvigilanza.it' connected to numerous other entities. The Entity Palette on the left lists recently used entities like 'Domain', 'Phrase', and 'Website'. The Overview panel shows a small preview of the graph structure. The Detail View panel shows the selected entity 'italpolvigilanza.it' and its relationships. The Property View and Hub Transform tabs are also visible. A status bar at the bottom provides information about transforms and a quota period. The desktop environment includes icons for Trash, File System, Home, and Wireshark.

kali linux 1 [Running]



kali linux 1 [Running]





Trash

File System

Home

wireshark

putty.exe

Maltego Community Edition 4.4.1

New Graph (1) *

Entity Palette

Search:

- Recently Used *

- Domain An internet domain
- Phrase Any text or part thereof
- Website An internet website
- Cryptocurrency
 - Bitcoin Cash Address An address in a Bitcoin Cash block
 - Bitcoin Cash Block A generic block in a Bitcoin Cas

Run View

+ Transforms

- Machines

Company Stalker ... This machine will tr...

Output - Transform Output

```
Transform To DNSNames [within Properties] done (from entity "Roma")
No results found (from entity "Roma")
Transform To URLs [within Properties] returned with 0 entities (from entity "Roma")
Transform To URLs [within Properties] done (from entity "Roma")
Running transform To Original Document [Wayback Machine] on 1 entities (from entity "2020 Dec 04: Politica-per-la-pre...")
Transform To Original Document [Wayback Machine] returned with 1 entities (from entity "2020 Dec 04: Politica-per-la-pre...
Transform To Original Document [Wayback Machine] done (from entity "2020 Dec 04: Politica-per-la-pre...")
```

Privacy Mode

Normal

Quick Find

Find in Files

Entity Selection

Select All

Add Parents

Add Neighbors

Select Children

Select Bookmarked

Reverse Links

Select None

Add Children

Add Path

Select Neighbors

Select by Type

Invert Selection

Add Similar Siblings

Select Parents

Select Leaves

Select Links

Overview

Detail View

Document Snapshot maltego.wayback.DocumentSnapshot 2020 Dec 04: Politica-per-la-prevenzione-della-corruzi...

- Relationships

- Incoming italpolvigilanza.it

+ Outgoing

- Entity Data

Property View Hub Transform Inputs

- Properties

Type	Document Snapshot
Raw Timestamp	20201204020351
Original URL	https://www.italpolvigilan...
DateTime	2020-12-04 03:03:51 +...
Extension	PDF
HTTP Status	200
Title	2020 Dec 04: Politica-p...
Meta-Data	
URL	https://web.archive.org/w...

1 of 62 entities

Maltego Community Edition

Investigate View Entities Collections Transforms Machines Collaboration Import | Export

New Copy Paste Clear Graph Cut Delete

Entity Palette

Search:

- * Recently Used *

- Domain An internet domain
- Phrase Any text or part thereof
- Website An internet website
- Cryptocurrency
 - Bitcoin Cash Address An address in a Bitcoin Cash block
 - Bitcoin Cash Block A generic block in a Bitcoin Cas

Run View

+ Transforms
- Machines

Company Stalker ... This machine will tr...

Output - Transform Output

```
Transform To DNSNames [within Properties] done (from entity "Roma")
No results found (from entity "Roma")
Transform To URLs [within Properties] returned with 0 entities (from entity "Roma")
Transform To URLs [within Properties] done (from entity "Roma")
Running transform To Original Document [Wayback Machine] on 1 entities
Transform To Original Document [Wayback Machine] returned with 1 entities
Transform To Original Document [Wayback Machine] done (from entity "2020")
```

Details

Summary Attachments (0) Notes Properties (3)

Politica-per-la-prevenzione-della-corruzione.pdf

Document [maltego.Document]

Google Me! Open all URLs Wikipedia Me!

Title: r-la-prevenzione-della-corruzione.pdf

URL: r-la-prevenzione-della-corruzione.pdf

Notes

Use the + button to add images

OK Cancel

1 of 63 entities

The screenshot shows the Maltego Community Edition interface running on a Kali Linux desktop. The main window displays a graph with entities such as 'Monte Carmelo' and 'Politica-per-la-prevenzione-della-corruzione.pdf'. A context menu is open over the PDF entity, listing options like 'Google Me!', 'Open all URLs', and 'Wikipedia Me!'. The left sidebar contains various entity types and a 'Run View' section. The bottom output panel shows transform logs. A notes panel on the right is currently empty.