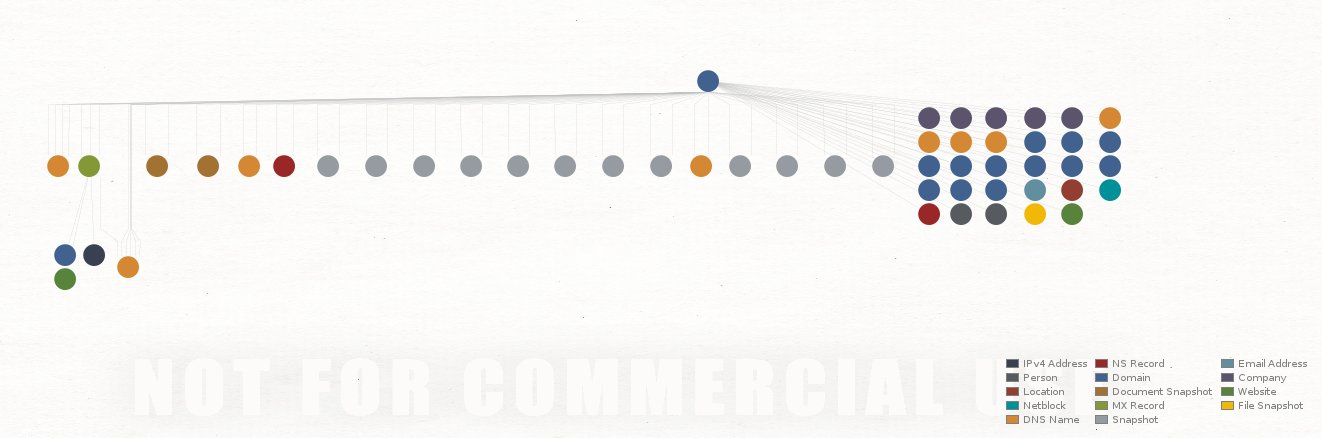
**INFORMATION GATHERING CON MALTEGO E GOOGLE HACKING**

**Maltego:**  
  
Utilizzando il transform domain di Maltego, ho utilizzato come target il domain epicode.it per ottenere tutto ciò che è collegato al dominio.



Maltego da una overview abbastanza comprensiva di tutti i dati connessi a quel determinato target eseguendo tutte le query possibili. Per eseguire determinate query come website e phrases servono gli API Key di determinati siti. Per esempio di Bing.

**Google hacking**: Google Hacking o Dorking è un modo per utilizzare il motore di ricerca di google in maniera mirata per fare ricerche specifiche su determinati target usando operatori di sintassi per gestire la ricerca.

Nel mio caso ho scelto come target Reddit.com.

Con le query Site ho ristretto il campo di ricerca al sito di Reddit. Con la query intext, ho cercato qualsiasi tipo di pagina che nel proprio testo avesse la parola “gatto”.

Con la query intitle ho cercato sempre la parola “gatto”, per vedere pagine che nel titolo avessero la parola gatto. Ho poi cercato con”-intitle:gatto” tutte quelle pagine su reddit che non avessero la parola gatto nel titolo. Poi ho infine cercato con “filetype” tutti i pdf presenti su reddit.

Ho poi usato il database di google hacking per andare a cercare delle webcam.

Con gli operatori intitle:WEBCAM7 -inurl:admin.html, ho trovato tutte quelle pagine che avessero nel titolo WEBCAM7 e che escludessero dall’url amdin.html. Ho trovato una pagina che ritrae una webcam del 2006 che registra un cane in casa sul suo cuscinetto.

Poi ho cercato filetype:env “DB\_Password”, al terzo risultato c’era un piccolo database di password.

Infine ho cercato filetype:reg reg HKEY\_CURRENT\_USER username, per cercare un file di tipo registry di windows. Al primo risultato ho trovato il MIT.