UNIVERSITÀ DI PISA

Corso di Laurea in Informatica Umanistica

RELAZIONE

Progettazione e sviluppo di uno strumento web per l'analisi di accounts malevoli su Twitter

Candidato: *Jessica Braschi*

Relatore: *Prof. Maurizio Tesconi*

Correlatore: *Prof. Stefano Cresci*

Prof. Mariantonietta Noemi La Polla

Anno Accademico 2014-2015

Indice

Indice delle figure

1.Introduzione

1.1. Social network e web reputation

Nella vita odierna internet occupa una posizione molto importante per ogni persona, infatti attraverso la rete è possibile acquisire informazioni di qualsiasi tipo (sociale, commerciale, culturale, tecnico, etc.), svolgere operazioni finanziarie, condividere contenuti multimediali, accedere a molteplici servizi e comunicare. Proprio la comunicazione è una caratteristica importante del web che ha portato alla nascita di blog, forum e social network.

I social network a loro volta si sono sviluppati divenendo un vero strumento di comunicazione di massa dove è possibile condividere le proprie idee, i propri pensieri e diversi contenuti multimediali (foto, video).

Fin dalla loro introduzione i social network hanno attirato milioni di utenti, divenendo, con il passare del tempo, parte integrante della loro vita, andando così a modificare la quotidianità dell'individuo e i suoi rapporti sociali con il mondo circostante.

La maggior parte dei social network è accomunata da una struttura molto simile, ovvero basata sulle relazioni, sulle connessioni tra i vari utenti iscritti al servizio e sui contenuti che vengono messi a disposizione dai vari utenti (D.M.Boyd, N.B.Ellison, 2007).

Gran parte dei social network si occupa della gestione delle reti sociali degli utenti e fa in modo che questi possano esprimere le proprie opinioni e i propri pensieri, in modo libero e su qualsiasi argomento. Invece, le maggiori differenze possono essere riscontrate nei paradigmi di comunicazione implementati: se gli utenti comunicano attraverso testo, video o immagini; se la comunicazione tra gli utenti avviene in modo sincrono o asincrono (L.Garton, C.Haythornthwaite, B.Wellman. 2006).

I social network, e in particolare i dati che vengono raccolti attraverso queste piattaforme, stanno sempre più attirando e incuriosendo il mondo della ricerca e dell'industria.

Questo è dovuto alla loro diffusione di massa, ai loro molteplici utilizzi e soprattutto per il cambiamento che hanno apportato al modo di comunicare e di rapportarsi nella società. I social network sono molto importanti da un punto di vista sociologico, infatti le informazioni che un utente può trovare al suo interno possono influenzare il suo pensiero e il suo modo d'agire (D.M.Boyd, N.B.Ellison. 2007).

A questo proposito è interessante sottolineare degli studi che hanno evidenziato come all'interno dei social network esistano degli algoritmi che riescono a gestire e scegliere i contenuti da mostrare ad un particolare utente (E. Pariser. 2011). Questo avviene al fine di suscitare l'attenzione e la curiosità dell'utente, assicurandosi così una sua prossima visita, attirato dai propri interessi, nel social network.
Il tutto è possibile grazie alle informazioni acquisite dall'utente, come per esempio gli utenti che segue, le pagine che preferisce o gli argomenti che predilige; in sintesi: il comportamento che tiene un utente all'interno del social network.

Questo comporta però una problematica importante all'interno del social network dal punto di vista dell'utente: infatti non solo rimane chiuso all'interno della "bolla"[1] creata intorno a lui dal social network, ma gli viene anche limitata l'opportunità di accedere ai molteplici contenuti e alle diverse informazioni che si trovano all'interno della piattaforma.

Le caratteristiche e l'importanza che i social network rivestono oggi, li hanno resi un campo appetibile non solo per i ricercatori, ma anche e soprattutto per le aziende che intendono pubblicizzare un prodotto su grande scala.

Oltre a questi settori, i social network suscitano interesse anche nel campo politico: attualmente molti politici stanno spostando le proprie campagne elettorali e la divulgazione delle proprie idee dalle piazze alla rete, proprio tramite i canali social (P.Rutledge. 2013).

Pertanto ecco che i social network assumo un'importanza particolare per la nostra attualità, occupando un posto di prestigio in diverse sfere d'interesse, che vanno dal marketing di un'azienda, alla popolarità di un particolare individuo proprio grazie

[1] Con "bolla" intendiamo una bolla di filtraggio, in inglese "filter bubble", cioè il risultato di un sistema automatico di personalizzazione dei risultati di ricerca di un sito, che avviene attraverso l'utilizzo d'informazioni ricavate dal comportamento di un utente.

alla loro caratteristica di informare un grande numero di persone e anche di influenzare quelle che possono essere delle scelte e dei pensieri.

I social network divengono quindi un campo di notevole interesse per il controllo della *web reputation.*

Con il termine web reputation indichiamo l'insieme delle attività che esprimono e rendono pubblico il pensiero degli utenti in rete riguardante prodotti, eventi, personaggi, etc.

È un fenomeno molto importante in quanto permette di rilevare le opinioni diffuse in rete riguardanti un particolare argomento e, in base a queste, agire di conseguenza.

Come evidenziato in precedenza, per la web reputation è di fondamentale importanza il monitoraggio del pensiero espresso in rete, quest'attività può essere di due tipi:

- **Monitoraggio continuo**, che viene utilizzato per il monitorate le attività per un determinato arco di tempo. Questo è utile per verificare l'andamento della reputazione di qualcosa o qualcuno in relazione al tempo, e per andare ad analizzare il risultato di alcune azione che possono aver modificato la web reputation in quel periodo.
- **Monitoraggio istantaneo**, utilizzato quando vogliamo avere un riscontro immediato della web reputation in quel particolare momento, riportando lo stato reale della reputazione osservata.

Oltre a questo, la web reputation, si differenzia a seconda del tipo di utente di cui andiamo a monitorare il pensiero. Infatti possiamo scegliere di osservare le opinioni che provengono dalla stampa online o da giornalisti di professione che si interessano all'argomento; oppure possiamo spostare l'attenzione sull'opinione collettiva e quindi sulle persone comuni che esprimono il proprio pensiero in rete. Dato che la maggior parte dei pensieri e delle opinioni degli utenti vengono pubblicate online attraverso i social network, questi assumono un'importanza rilevante.

È proprio in questo campo infatti che nascono diversi espedienti e trovate per andare ad alterare quella che è la web reputation di un prodotto o, ancora più frequentemente, di un personaggio d'importanza collettiva. Esistono diverse tecniche

utilizzate per accrescere la propria web reputation, come, per esempio, essere presenti su diverse piattaforme social, sviluppare contenuti interessanti che possono stimolare l'engagement degli altri utenti, oppure monitorare le attività dei competitors per un confronto diretto con le proprie. Per aiutare gli utenti a migliorare la propria web reputation vengono messi a disposizione nel web diversi tool gratuiti come *Mention*[2] e *LikeAlyzer*[3] .

Oltre a queste tecniche, esistono dei metodi meno onesti, che sono mirati ad alterare la web reputation, è questo il caso della creazione di spammer, fake e bot.
Questi sono dei particolari account che vanno ad operare in modo differente, che vedremo nello specifico in seguito; ma ci sono anche pratiche che possono danneggiare la figura di una persona o di un prodotto in rete.

Un fenomeno molto diffuso che fornisce un esempio di questi avvenimenti si trova all'interno delle community come *Foursquare*[4] o *TripAdvisor*[5]. In queste piattaforme gli utenti descrivono luoghi d'interesse pubblico come ristoranti, bar, etc; fornendo anche commenti e valutazioni personali. I commenti o le valutazioni possono essere utilizzati in maniera disonesta, per aumentare, o anche per discreditare la reputazione dell'attività o del luogo che viene preso in considerazione. Per aumentare la reputazione, per esempio, possono essere creati e gestiti degli account multipli, da una stessa persona, che andranno poi a commentare in modo positivo un particolare luogo.

Al contrario, un'altra attività praticata all'interno dei social network che può andare a danneggiare la reputazione di una persona è la creazione di un profilo fingendosi un'altra persona. Questo fenomeno colpisce moltissimi personaggi popolari tra cui politici, attori, cantanti, etc. Questi profili possono essere molto dannosi per l'immagine di una persona, in quanto le azioni svolte all'interno dei social network possono essere attribuite poi al personaggio in questione.

[2] https://en.mention.com/
[3] http://likealyzer.com/
[4] https://it.foursquare.com/
[5] http://www.tripadvisor.it/

I danni all'immagine causati da questo fenomeno possono essere molteplici, tanto che è intervenuta anche la legge, infatti la *sentenza 25774 del 16 giugno 2014 della cassazione* si pronuncia così:

> *"Creare un falso profilo su un social network integra il reato di sostituzione di persona perché il dolo specifico previsto dalla norma è rappresentato dal soddisfacimento di una propria vanità (vantaggio non patrimoniale) o dall'altrui danno (arrecato alla persona cui si sottrae l'identità). Commette lo stesso reato chi apre un account mail sotto falso nome, inducendo in errore gli utenti della rete."*

Per cercare di eliminare questo problema i social network hanno iniziato ad attuare alcune strategie interne. Piattaforme come Facebook[6] e Twitter[7] hanno infatti apposto ai profili ufficiali e reali delle persone di rilevanza pubblica, un simbolo che ne garantisca la validità (v. fig. 1). Questo comporta maggiore sicurezza per i personaggi pubblici, che non rischiano di essere "contraffatti" e strumentalizzati, ma anche per tutti gli utenti del social che non vengono più tratti in inganno da falsi profili.

Figura 1. Profili verificati su Facebook e Twitter

[6] https://www.facebook.com/
[7] https://twitter.com

1.2. Spammer, Fake, Bot e profili multipli

Come è stato evidenziato in precedenza, per alterare la web reputation c'è bisogno di andare a manipolare il materiale che si trova in rete su di un particolare argomento.

Uno dei modi più diffusi e in atto già da molto tempo, è quello basato sull'utilizzo di spammer. Gli spammer inviano e postano una quantità considerevole di messaggi di uguale entità, riguardanti l'argomento o la persona interessata, attraverso la rete, e in particolare attraverso forum, social network ma soprattutto posta elettronica.

Gli indirizzi a cui vengono inviate le mail dagli spammer sono recuperati in rete attraverso spambot e appositi programmi che li generano casualmente o che li leggono da databases già esistenti.

Ad oggi gli spammer e i loro messaggi cambiano le loro caratteristiche e i loro comportamenti all'interno di quello che viene definito Web 2.0. Il Web 2.0 viene comunemente associato alle web-application che facilitano la condivisione di contenuti e informazioni, e inoltre pongono l'utente al centro di tutta la struttura rendendolo in grado di collaborare alla produzione di contenuti Web. Questi concetti di apertura all'utente del Web 2.0 incoraggiano gli utenti stessi alla partecipazione e alla condivisione di contenuti, ciò avviene particolarmente in applicazioni web come social network, blog, wiki, etc.

In questo panorama lo spam non si limita più alla messaggistica via mail, ma diventa uno spam 2.0 che si adegua ai nuovi contesti e alle nuove applicazioni web (P.Hayati, V.Potdar, A.Talevski, N.Firoozeh, S.Sarenke, E.A.Yeganeh. 2010). Le nuove tipologie di spam si differenziano dai classici spam utilizzati prevalentemente nella posta elettronica per queste caratteristiche:

- Si rivolgono ampiamente alle applicazioni web 2.0;
- Non temono nessuna contromisura che li limiti o che li prevenga;
- Lo spam 2.0 si diffonde attraverso qualsiasi tipo di sito o applicazione web;
- Può essere diffuso anche attraverso degli agenti automatizzati e quindi non solo attraverso persone reali.

Questa nuova frontiera dello spam 2.0 porta nuovi problemi correlati alle sue caratteristiche, infatti vista la sua possibilità di diffondersi attraverso qualsiasi sito e applicazione, lo spam 2.0 può essere molto dannoso per l'immagine dei siti che li contengono. Contenuti Web malevoli o ingannevoli possono inoltre piazzarsi ai primi posti dei risultati dei maggiori motori di ricerca, oscurando quindi dei contenuti di qualità del web. Infine questi spam occupano risorse preziose, ma ancor più ingannano gli utenti del web 2.0 e danneggiano l'immagine di applicazioni e siti web.

Spostandoci più verso il contesto dei social network, qui la reputazione viene alterata mediante la creazione di falsi utenti che, a seconda del loro comportamento in rete, possono essere classificati come Fake o Bot. Questi tipi di utenti hanno, comunque, anche dei punti in comune, infatti oltre alla caratteristica di alterare la reputazione, questi solitamente dispongono di profili utente molto realistici, spesso creati in modo da attirare l'attenzione di altri utenti reali dei social.

Gli utenti fake hanno la particolare caratteristica di manifestare poche interazioni e di creare un esiguo numero di contenuti all'interno del social network, ma allo stesso tempo seguono un ampio numero di utenti. Questo perché l'obiettivo principale dell'utente Fake è quello di alterare il numero di amici o di followers[8] di un altro utente al fine di aumentare la sua popolarità e la sua influenza.

Questo dato ha molta importanza al giorno d'oggi, basti pensare che, negli USA, il numero di followers di un soggetto è tra i parametri valutati da alcune banche per concedere un prestito (*Le monde. 2013*).

Inoltre è altrettanto influente per la reputazione di un personaggio pubblico: al giorno d'oggi si sente sempre più parlare del numero di utenti che seguono personaggi di spicco, come politici ed artisti, creando una vera e propria *corsa al seguace* sui social. Ecco che questi utenti Fake vanno ad alimentare il numero di amici o followers di un personaggio e quindi la sua reputazione agli occhi della massa.

Quando questo tipo di problema è emerso nella coscienza comune, la collettività e quindi di conseguenza i mass media, si sono interessati all'argomento, per cercare di capire quali, tra le persone popolari presenti nei social network, utilizzassero

[8] Il follower, all'interno della piattaforma Twitter, è un utente che segue un altro account e che può visualizzare le sue attività su Twitter.

i fake per falsare la propria reputazione. Infatti troviamo molti articoli di testate online importanti che trattano l'argomento. Degli esempi significativi riguardanti politici di spicco nella nostra era sono per esempio un articolo nella pagina web dell'*NBC NEWS* ha riportato che durante la campagna elettorale 2012 di Romney, per le elezioni presidenziali negli USA, questa aveva avuto un fortissimo incremento di followers su Twitter, che nella maggio parte dei casi sono stati poi rivelati come fake; in Italia uscì un articolo analogo del *Corriere della sera* (D.Casati. 2012) che esponeva dei risultati accademici sul sospetto che il 54% dei follower del profilo Twitter di Beppe Grillo fossero dei fake.

Oltre ad articoli incentrati sui politici possiamo trovarne di analoghi riguardanti anche gli artisti di spicco al giorno d'oggi, un esempio sono gli articoli che accusano artisti del calibro di Lady Gaga, Justin Bieber e Katy Parry di ricorrere a dei fake followers per aumentare la loro visibilità.

La peculiarità dei Bot invece è quella di interagire sui social network postandovi moltissimi messaggi con continuità. Una volta che il bot viene attivato per pubblicizzare un prodotto o un personaggio questo posterà un particolare messaggio creato per tale scopo. Il punto di forza del Bot è proprio quello di *nascondere* tra i moltissimi messaggi postati automaticamente, dei messaggi pubblicitari. Utilizzando quindi molti Bot per alterare la reputazione avremo come risultato molti post pubblicati riguardanti l'argomento interessato. L'utilizzo di questo particolare profilo non è gestito da una persona fisica bensì da un software automatico programmato per farlo.

Nel particolare caso di Twitter, su cui ci si è soffermati per lo sviluppo di questa tesi, i Bot pubblicano con continuità dei tweets preimpostati, attingendo da un apposito database. Questi particolari twees hanno la caratteristica di non essere mai legati alla realtà, o meglio non citano mai eventi di particolare interesse per l'attualità, ma prediligono frasi generiche e in particolare citazioni di personaggi illustri. Anche grazie a questa strategia i bot riescono ad acquisire molti followers, presumibilmente utenti reali, che innalzano ancor più la loro credibilità contribuendo a renderli difficilmente distinguibili dalla massa degli utenti Twitter.

Gli accounts Bot non sono quindi di facile individuazione tra tutti gli utenti Twitter, infatti possono essere scambiati per un qualsiasi utente che twitta normalmente. Ad ogni modo, se viene presa in analisi la timeline dell'utente, cioè un certo numero degli ultimi tweets postati, possiamo renderci conto se questo è un bot o meno.

Oltre a postare messaggi con continuità, che hanno la caratteristica di non essere legati a degli eventi dell'attualità, possiamo trovare un considerevole numero di citazioni e frasi che possono attirare l'attenzione degli utenti reali, per far in modo che questi possano interagire con i bot (inserire tra i peferiti il tweet, seguire quel profilo, etc.), allo scopo di rendere l'account più credibile possibile, cioè più "reale".

Infine troviamo un'altra tendenza che riscontriamo spesso sui social network ed è quella dei *profili multipli*. Con profili multipli si intendono tutte quelle registrazioni di account predisposte da parte di una solita persona. Questo fenomeno viene utilizzato nella maggior parte dei casi al fine di incrementare i *like* o il numero di amici o di followers, sulle proprie pagine o su quelle dei propri clienti. A differenza dei profili che popolano i social network visti in precedenza, cioè fake e bot, dietro questa tipologia di profilo si celano persone reali che li utilizzano.

Dopo uno studio approfondito di tutte le caratteristiche di queste tipologie di "utenti", per questo progetto è stato scelto di concentrarsi maggiormente sui bot di Twitter, per la loro complessità che li rende sempre più difficili da scovare, e per la novità dell'oggetto di studio. Infatti non esistono molti precedenti nella letteratura accademica; proprio per questo è stato progettato e realizzato *"investigator-tool"*.

Investigator-tool è un web-tool in grado di recuperare le informazioni degli utenti Twitter, compresi i propri tweets, attraverso le Twitter API[9], e che permette di analizzare tali dati acquisiti, in maniera approfondita, in modo da poter studiare, identificare e catalogare questi utenti.

I dati ottenuti attraverso investigator-tool vengono raccolti all'interno di un database, per permettere maggiori studi e analisi su questi dati e per poterli utilizzare anche per un diverso scopo da quello dello studio dei bot.

[9] https://dev.twitter.com/overview/documentation

La struttura del database che raccoglie i dati acquisiti relativi agli utenti Twitter è stata progettata per rendere compatibili i dati con un altro tool, #tweetag. Il tool #tweetag è uno strumento di annotazione che è stato ampliato per permettere l'annotazione delle timeline degli utenti analizzati con investigator-tool. Il fine ultimo di questi progetti è quello di avere dei dataset annotati riguardanti gli utenti Twitter, che possono essere utilizzati per permettere la creazione di un algoritmo di riconoscimento automatico dei bot.

2.Related work

Twitter è un'applicazione web, nata nel 2006, che offre un servizio di social network e di microblogging e che ha avuto un grandissimo successo a livello mondiale. Basti pensare che nel Dicembre 2013 le statistiche hanno riportato la presenza di 645 milioni di utenti Twitter, per un complessivo di 300 miliardi di tweets inviati (C. Smith. 2013).

Per microblogging si intende una forma di comunicazione emergente che consente agli utenti di pubblicare dei brevi messaggi che possono essere inoltrati su differenti canali. È dunque una pubblicazione costante di piccoli contenuti in Rete, sotto forma di messaggi di testo (fino a 140 caratteri per quanto riguarda Twitter). Si tratta di un servizio molto simile all'invio di sms, con la differenza sostanziale che il destinatario non è una sola persona ma un'intera comunità formata, potenzialmente, da milioni di persone.

Uno dei punti di forza di questo tipo di blogging risiede proprio nella brevità del messaggio, che consente al lettore di acquisire le informazioni molto più velocemente rispetto, ad esempio, ad un articolo su un comune blog. Dato il ristretto numero di caratteri messo a disposizione dalla piattaforma, si è costretti a scrivere solo l'essenziale. Questo ne facilita la lettura, permettendo a chi segue le discussioni su queste piattaforme, di rimanere sempre aggiornato.

Queste caratteristiche e queste peculiarità proprie di Twitter comportano che tale social network sia stato molte volte oggetto di studi accademici, volti ad analizzare questo nuovo mezzo di comunicazione e le dinamiche sociali che si svolgono al suo interno, in quanto questa piattaforma è diventata sempre più influente nella società moderna. Analizzando ed interagendo con Twitter è infatti possibile anticipare o creare tendenze che vanno ad influire in modo concreto sul mondo reale.

Un esempio di questo tipo di studi è stato fatto nel 2010 da H.Kwak, C.Lee, H.Park e S.Moon che hanno scansionato l'intera piattaforma Twitter ottenendo 41,7 milioni di profili utente, 1,47 miliardi di relazioni sociali, 4262 argomenti di tendenza e 106 milioni di tweets, da cui hanno ricavato diverse statistiche su quello che è il modo di comunicare e diffondere informazioni su questa piattaforma in particolare

concentrandosi sull'importanza dei retweets (H.Kwak, C.Lee, H.Park e S.Moon. 2010).

Proprio sulla diffusione delle informazione e sull'influenza che hanno i vari account Twitter tra di loro, si concentra lo studio di M.Cha, H.Haddadi, F.Benevenuto e K.P.Gummadi dell'Università di Londra mettendo in esame uno dei punti fondamentali del social marketing, cioè quello riguardante i diversi modi e l'efficacia dell'influenza tra vari utenti Twitter.

Questo studio ha evidenziato come l'influenza degli utenti Twitter non si ottenga spontaneamente o accidentalmente, ma attraverso delle azioni che siano in grado di ottenere e mantenere l'influenza stessa; azioni di cui gli utenti hanno bisogno per mantenere alto il coinvolgimento personale (M.Cha, H.Haddadi, F.Benevenuto, K.P.Gummadi. 2012). Questo potrebbe significare che gli utenti più influenti siano più prevedibili, con delle caratteristiche e dei comportamenti precisi, che possono essere utilizzati quindi per identificare altri utenti influenti.

Da queste tipologie di studi, di stampo più generale, nascono studi sull'argomento specifico dei fake, spam e bot. Tali studi hanno gettato le basi per la creazione di diversi tool per l'individuazione automatica di questi particolari account.

Nella letteratura accademica si è dato più spazio agli spam, infatti, un esempio è lo studio condotto da K.Thomas, C.Grier, V.Paxson e D.Song dove viene analizzato l'abuso dei social network da parte di questi account, in particolare degli spam che si trovano su Twitter. Per condurre le analisi, sono stati identificati 1.1 milioni di account sospesi da Twitter per attività sospette. Sono inoltre stati ricavati 1,8 miliardi di tweets, di cui 80 milioni riconducibili a spam.

Attraverso questi dati, i ricercatori hanno potuto studiare le caratteristiche generali di questi particolari account ed il mercato online che si cela dietro di essi. I risultati pubblicati hanno evidenziato come il 77% degli account presi in considerazione fosse stato individuato e sospeso da Twitter già dopo il primo tweet, per questo meno del 9% stringono relazioni con altri account; inoltre hanno specificato come il 17% degli account si concentrino sull'alterazione dei trends di Twitter, mentre il 52% degli account utilizza mention verso altri utenti (K. Thomas, C. Grier, V. Paxson, D. Song. 2011).

Altro studio condotto da C.Grier, K.Thomas, V.Paxon e M.Zhang analizza a fondo le caratteristiche degli spammer attraverso l'analisi dei messaggi di spam che vengono inviati sulla piattaforma Twitter (C. Grier, K. Thomas, V. Paxson, M. Zhang. 2010).

Altri studi invece, oltre ad analizzare le caratteristiche degli spam come quelli sopracitati, addestrano un classificatore in grado di individuare automaticamente gli utenti fake. Un esempio di questi sono gli studi condotti da G.Stringhini, C.Kruegel e G.Vigna. I risultati di questo studio in stretta collaborazione con la piattaforma Twitter, hanno permesso di individuare e sospendere 15.857 account identificati come spammer (G. Stringhini, C. Kruegel, G. Vigna. 2010).

Il fenomeno degli utenti fake, degli spam e dei bot ha suscitato sempre più la curiosità della società, e questo ha portato a svolgere diversi studi sui follower di persone influenti, come politici o artisti. Si ricorda a tal proposito lo studio di M.Camisani-Calzolari che ha effettuato un'analisi sui follower di Obama e Romney durante la loro campagna elettorale, rilevando gli utenti fake che ne facevano parte (M.Camisani-Calzolari. 2012).

Visto l'interesse per l'argomento suscitato da diversi studi e pubblicazioni in giornali online, sono nati diversi strumenti, offerti da diversi enti, per lo studio dei social network e del fenomeno di fake, spam e bot.

Online possiamo trovare diversi strumenti d'individuazione di utenti fake, come per esempio i tool offerti da Socialbakers, un'azienda d'analisi dei social network che ha sviluppato l'applicazione "*Fake Follower Check*"[10]; Statuspeople, un'azienda inglese fondata nel 2011 che offre supporto per gli utenti dei social media che offre il tool "*Fakers*"[11], e Twitteraudit[12], che è sede di una web-application dedicata a queste funzioni di individuazione dei fake.

Uno studio accademico che ha confrontato questi tool online e che ha ispirato questo progetto di cui è al centro l'investigator-tool, è *@thefakeproject*, un progetto del CNR di Pisa che studia e confronta questi strumenti, con l'obiettivo di creare un

[10] http://www.socialbakers.com/twitter/fakefollowercheck/
[11] https://fakers.statuspeople.com/
[12] https://www.twitteraudit.com/

algoritmo di riconoscimento automatico dei fake, migliore rispetto a quelli esistenti (S.Cresci, M.Petrocchi, A.Spognardi, M.Tesconi, & R.D.Pietro. 2014).

Nell'ambito degli studi accademici rivolti nel particolare agli account bot spicca lo studio di Z. Chu, S. Gianvecchio, H. Wang, e S. Jajo che studiano e analizzano in particolare le caratteristiche dei bot, introducendo anche una nuova categoria di utente, cioè i cyborg, alla fine dei loro studi propongono un classificatore di riconoscimento automatico di bot e cyborg.

Gli utenti che vengono classificati come cyborg hanno la caratteristica di essere o utenti umani reali che delle volte twittano attraverso l'utilizzo di software automatici, sono quindi assistiti da bot, oppure sono degli account bot che delle volte sono assistiti da umani. Questi sono riconoscibili in quanto non utilizzano sempre una stessa tipologia di tweets, infatti nella timeline di utenti cyborg possiamo trovare diversi tipi di tweets a differenza invece delle timeline dei bot che contengono tweets che hanno una struttura simile tra loro.

Il classificatore che hanno realizzato, prende in considerazione quattro componenti:

- **L'entropia**, che misura la periodicità con cui vengono postati i vari tweets dagli utenti, differenziandoli tra periodici o regolari;
- **Machine learning**, che analizza il contenuto dei tweets per riconoscere le tipologie di messaggi appartenenti solitamente ai bot;
- **Proprietà**, vengono prese in considerazioni le proprietà degli account per verificare la presenza di anomalie particolari che caratterizzano i bot;
- **Decisore**, questa ultima componente riassume e analizza i risultati delle tre componenti precedenti e stabilisce se l'utente analizzato è un account umano, un bot oppure un cyborg.

2.1. @TheFakeProject

@Thefakeproject[13] è un progetto di ricerca interno all'istituto di Informatica e Telematica del CNR di Pisa, rivolto allo studio scientifico del fenomeno degli utenti

[13] http://wafi.iit.cnr.it/fake/fake/app/

fake nella piattaforma Twitter. L'obiettivo di tale progetto è quello di creare un algoritmo di riconoscimento automatico degli utenti fake, più efficiente rispetto a quelli fino ad oggi creati.

Questo progetto nasce nel Dicembre 2012 attraverso la creazione dell'account Twitter *@Thefakeproject*[14]: l'obiettivo di questo account è quello di raccogliere più follower umani possibili da inserire all'interno di un training set di dati da utilizzare per il confronto degli algoritmi esistenti e per lo sviluppo di uno ancor più migliore.

Gli account che hanno aderito all'iniziativa e che quindi sono divenuti follower della pagina sono stati 574. Attraverso le Twitter API sono state acquisite le informazioni pubbliche riguardanti gli account, compresi la timeline e le informazioni dei loro follower e following, per un complessivo di 616,193 tweets e 971,649 relazioni tra account Twitter (S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi. 2014).

A questa fase di acquisizione dei volontari, è seguita quella di verifica di tali utenti Twitter, infatti ogni account che ha iniziato a seguire la pagina è stato contattato da *@Thefakeproject* attraverso un messaggio diretto su Twitter, contenente un URL che rimandava ad un CAPTCHA, cioè ad un test univoco per ogni utente, che questi dovevano completare per dimostrare di essere dei veri account umani. Dei 574 account che hanno aderito al progetto, hanno completato con successo il CAPTCHA 469 utenti, che sono stati etichettati quindi come utenti umani verificati.

Altri 1841 account umani sono stati ottenuti attraverso il dataset #elezioni2013[15].

A questo punto per @thefakeproject sono stati ottenuti 1950 utenti umani.

---

[14] https://twitter.com/TheFakeProject

[15] Questo dataset è nato per sostenere un progetto di ricerca sociologica, realizzato in collaborazione con l'Università di Perugia e l'Università Sapienza di Roma, sui cambiamenti strategici nel panorama politico Italiano in un triennio (2013-2015). Sono stati rilevati 84.033 account che hanno utilizzato l'hashtag elezioni2013, tra il 9 Gennaio e il 28 Febbraio 2013. Tra questi sono stati scartati gli account di politici, giornalisti, blogger e gli account che non avevano una biografia. I restanti sono stati catalogati come cittadini. Questi a loro volta sono stati campionati e poi analizzati manualmente. Per un totale finale di 1481 account inseriti all'interno del dataset #elezioni2013.

Analogamente, sono stati reperiti 3000 profili fake certificati, acquistandoli direttamente da 3 differenti shop online dedicati a Twitter: http://fastfollowerz.com, http://intertwitter.com e http://twittertechnology.com.

Il totale degli utenti raccolti nel set attraverso l'account @thefakeproject (469 account) e il dataset #elezioni2013 (1481 account) sono stati utilizzati per verificare tre algoritmi esistenti di riconoscimento degli utenti fake. Uno di questi algoritmi deriva dallo studio accademico di M.Camisani-Calzolari sull'analisi dei follower di Romney e Obama durante l'ultima campagna elettorale per l'elezioni presidenziali degli USA; un altro è invece utilizzato da un servizio web per l'analisi degli account Twitter, questo è *stateofsearch.com;* mentre l'ultimo algoritmo è distribuito da un'azienda che si occupa dell'analisi dei social media, cioè *Socialbakers.*

I tre algoritmi hanno una struttura simile, infatti tutti si basano su di un elenco di regole e criteri con cui confrontare gli account. Ogni regola darà un risultato, un punteggio, che alla fine sarà sommato ai risultati di tutte le regole per dare un verdetto finale sull'account.

Gli account acquisiti sono stati confrontati con ogni criterio dei tre algoritmi e per riassumere i risultati sono state ideate quattro categorie in cui inserire i risultati ottenuti:

- **Vero Positivo (TP)**, per indicare il numero di account fake che sono stati riconosciuti correttamente (cioè fake) dal criterio a cui era sottoposto l'account;
- **Vero negativo (TN)**, utilizzato per indicare il numero di account umani che sono stati individuati come;
- **Falso Positivo (FP)**, indica il numero di account umani che sono stati riconosciuti erroneamente come account fake dalla regola che li prende in esame;
- **Falso negativo (FN)**, categoria impiegata per identificare gli account fake che sono stati erroneamente riconosciuti come account umani.

Il primo algoritmo di analisi degli account nasce in ambito accademico e utilizza ventidue criteri di individuazione per verificare se un account è umano o bot. Ogni account analizzato viene confrontato con ogni regola e li viene dato un punteggio positivo (umano) o negativo (bot).

Il risultato finale dipende dalla somma di tutti i risultati delle regole, se la somma dei punti è maggiore di 0 allora l'account è considerato umano, se è compreso tra 0 e -4 è considerato neutro, in caso contrario è considerato bot.

L'algoritmo ha ottenuto ottimi risultati con l'individuazione dei veri utenti umani, ma non si può dire lo stesso per il risultato ottenuto nell'analisi degli utenti fake, infatti la maggior parte degli account realmente fake, sono stati etichettati come account umani. Questo risultato evidenzia come questo algoritmo utilizzi dei criteri di analisi non adatti alle caratteristiche di questi fake.

Il secondo algoritmo si basa su sette regole fornite dal fondatore del sito sui social media stateofsearch.com. Per questo test non sono state prese in considerazione due regole, perché necessitavano di interagire con l'account analizzato, infatti una prendeva in considerazione il tempo di risposta ad un tweet e l'altra se l'account seguiva o smetteva di seguire altri account in 24 ore.

Il terzo algoritmo invece è alla base dello strumento online *FakeFollowerCheck*, un tool di riconoscimento dei fake offerto dall'azienda Socialbakers. Il sito rende pubblici gli otto criteri utilizzati dall'algoritmo per identificare i fake, ma non mette in luce quelle che sono le metodologie per utilizzare i criteri e valutare un account.

I risultati ottenuti dal confronto con ogni singola regola degli algoritmi, mostrano come solo alcuni criteri siano efficaci per l'individuazione di utenti fake.

Le regole che si sono mostrate idonee per questo scopo e successivamente sono state analizzate e classificate in base al loro costo di utilizzo.

Infine è stato quindi creato un classificatore ottimizzato per il rilevamento degli account fake che utilizza solo i criteri che sono risultati efficaci ed efficienti per il rilevamento di fake e che hanno avuto una buona classificazione in base al loro costo di utilizzo. Il classificatore creato raggiunge alti livelli di riconoscimento degli account fake, utilizzando criteri con un basso costo.

Successivamente sono stati analizzati altri strumenti online per il rilevamento di utenti fake oltre che a FakeFollowerCheck di Socialbakers, come il tool della compagnia inglese StatusPeople e l'applicazione di Twitteraudit.com.

I risultati ricavati da questi confronti sono poco omogenei. Questo sembra supportare la tesi che gli attuali strumenti di individuazione di profili fake siano scarsamente affidabili e quindi inadatti allo scopo.

3.Investigator-tool

Lo strumento investigator-tool nasce dalla necessità di disporre di uno strumento per la raccolta di informazioni sugli utenti iscritti alla piattaforma Twitter, infatti questo tool è stato progettato e sviluppato per lavorare nello specifico contesto di Twitter.

La scelta di ricavare informazioni sugli utenti Twitter è dovuta dalle caratteristiche di questo social network, infatti oltre ad essere molto usato e attivo, basti pensare che vanta 500 milioni di tweets postati ogni giorno.

Twitter è un'applicazione web che offre oltre al servizio di social network, quello di microblogging, utilizzando una struttura aperta. Questo ha portato personaggi pubblici di diverso calibro, quali artisti, così come i mass media tradizionali come giornali, TV e radio a utilizzare Twitter come un nuovo canale di comunicazione alla massa.

Anche i politici hanno spostato una parte consistente delle loro campagne elettorali all'interno di Twitter. Di conseguenza, questo social network ha suscitato molto interesse da parte delle imprese, delle aziende e dei marchi commerciali più famosi che hanno iniziato ad usare questo social network come uno strumento pubblicitario.

Tale estensione d'uso e la molteplicità di frangenti d'azione, hanno reso Twitter una piattaforma soggetta alla nascita di diversi espedienti per l'alterazione delle informazioni reali, soprattutto nel campo della web reputation, è questo il caso, appunto, dei bot.

Inoltre ha influenzato la scelta di Twitter anche il fatto che la necessità di creazione di questo tool sia nata inizialmente all'interno del progetto @t*hefakeproject*, che opera nel suddetto social network per l'individuazione degli utenti Fake, per poi essere sviluppato indipendentemente, con altri obiettivi rispetto a quello del progetto guida.

Come appena accennato, l'idea di partenza per la creazione di questo tool nasce all'interno del progetto @t*hefakeproject.* Qui si era creata la necessità di recuperare le informazioni degli account degli utenti Twitter, al fine di creare dei dataset di utenti, da poter annotare manualmente, attraverso l'annotatore #tweetag, per etichettarli come fake o come utenti reali, questo con l'obiettivo di avere a disposizione dei dataset, annotati manualmente, di utenti e poterli usare all'interno di questo progetto.

Dopo attenti studi sulle caratteristiche degli utenti fake è emerso che un utente fake, durante l'annotazione manuale, poteva essere scambiato, per le sue proprietà, come un utente reale inattivo, e viceversa; un utente inattivo è un utente reale che ha dei follower e dei following, ma che non ha tweets all'interno della sua timeline.

Questo comporta un margine d'errore possibile anche attraverso l'annotazione da parte di annotatori umani. L'unica prova del nove finale per disambiguare i due tipi di profili sarebbe stato il contatto diretto con l'account, interagendoci per verificare la sua reale natura. Questa limitazione è stata uno dei motivi che ha portato alla decisione di concentrarsi maggiormente sui bot, creando un tool in grado non solo di creare dataset predisposti all'annotazione, ma anche di analizzare i dati offrendo un'interfaccia grafica semplice ed intuitiva.

3.1. Implementazione #tweetag

#tweetag è un tool di annotazione manuale rivolto unicamente alla piattaforma Twitter creato all'interno del progetto SOS – Social Sensing[16] dell'istituto di Informatica e Telematica del CNR di Pisa (v. fig. 2).

[16] http://socialsensing.it

Figura 2. Pagina login di #tweetag

Questo strumento ha l'obiettivo di annotare i tweets in modo da estrapolare delle informazioni utili alla ricerca; una volta nata l'esigenza di annotare l'intero profilo degli utenti attraverso la timeline è stato deciso di ampliare questo tool rendendolo in grado di poter annotare un complesso di dati provenienti da Twitter che non si limitino solo ai tweets, ma che si apra anche agli utenti stessi.

La sezione aggiunta, che riguarda l'annotazione della timeline è strutturata analogamente alle altre sezioni del tool. Infatti troviamo la pagina dedicata alle annotazioni, e una pagina dedicata al riepilogo e alla revisione delle annotazioni stesse.

Questo tipo di annotazione prende in considerazione gli ultimi 20 tweets dell'utente mostrati attraverso un'embedded view, possibile grazie agli widget Twitter (v. fig. 3).

Figura 3. Pagina annotazione delle timeline di #tweetag

La pagina è suddivisa in due colonne principali, la prima presenta la lista degli utenti Twitter ancora da annotare visualizzati attraverso il loro screen name; cliccando su di essi attraverso l'utilizzo di una funzione jQuery apparirà nella colonna destra la suddetta timeline relativa all'utente e vicino allo screen name appariranno dinamicamente i bottoni che permettono l'annotazione, insieme ad una textarea per eventuali commenti.

Una volta effettuata l'annotazione di un utente, il suo screen name scomparirà dalla colonna sinistra una volta registrata l'annotazione nel database centrale dell'applicazione. Nel caso in cui la timeline non basti a dare le giuste informazioni per un'annotazione è possibile cliccare sullo screen name dell'utente per essere rinviati alla pagina del profilo Twitter per maggiori dettagli sull'account.

3.2. Progettazione investigator-tool

Inizialmente il tool è stato progettato per ricavare le informazioni degli utenti Twitter attraverso le apposite Twitter API, per poi utilizzarle successivamente per un'annotazione manuale di questi utenti per catalogarli come utenti reali, fake o bot

attraverso il tool #tweetag che è stato ampliato specificatamente per l'annotazione delle timeline degli utenti.

In un secondo momento la progettazione del tool ha avuto un cambiamento di rotta, si è infatti scelto di concentrarsi principalmente sullo studio dei bot. Per fare questo, il tool ha acquisito una funzione bivalente: la prima è rimasta quella originale, cioè il recupero delle informazioni degli utenti; la seconda invece prevede una fase di investigazione e comparazione degli utenti che consente di capire l'effettiva entità di un utente e di analizzare più a fondo il comportamento di questi bot.

Nonostante questa scelta di progettazione il tool non perde quella caratteristica di estrazione di informazioni degli utenti per poi andarli ad inserire all'interno del tool di annotazione #tweetag. Infatti l'utilizzo di investigator-tool è pevista in una fase precedente all'annotazione degli utenti stessi che non si limita al recupero di informazioni, ma che va a fondo attraverso l'analisi dei dati ricavati.

3.3. Realizzazione

Investigator-tool è stato realizzato per presentarsi come un'applicazione web, cioè utilizzabile tramite un qualsiasi browser. La decisione di creare un tool online permette di non dover distribuire successive versioni di aggiornamento e allo stesso tempo questa caratteristica consente di avere un forte potenziale per sviluppi futuri; infatti oltre a non dover dispensare le varie versioni di aggiornamento future, permette di evolvere il suo utilizzo attraverso un modello di tipo crowdsourcing.

Il target di utenti previsto per l'utilizzo dello strumento comprende persone coinvolte in prima linea nella ricerca e nello studio di questi fenomeni, strettamente legati agli account Twitter, ma prendendo in considerazione i potenziali sopra citati di una web application, non si esclude un futuro utilizzo da parte di persone al di fuori della ricerca.

Inizialmente è stato progettato e realizzato un database MySQL di supporto per l'applicazione; qui troviamo due tabelle distinte, in una vengono registrate le credenziali degli utenti che utilizzano l'applicazione, che da ora in poi chiameremo

investigatori, e nell'altra tabella, sono registrati i token di accesso, necessari per l'autenticazione dell'applicazione, per l'utilizzo delle Twitter API.

In particolare il database centrale è suddiviso nelle seguenti tabelle:

- **Investigators**, in cui vengono salvate le credenziali dell'utente; questa tabella ha la seguente struttura:
  - **Id_investigator,** dove viene registrato un ID numerico univoco per ogni investigatore;
  - **Username,** qui verrà registrato lo username scelto dell'investigatore;
  - **Password**, dove viene registrata la password personale dell'investigatore;
  - **Dataset**, qui viene registrato il nome del dataset assegnato all'investigatore che viene creato automaticamente durante la fase di registrazione.
- **Log**, in questa tabella sono registrate le chiavi che servono per autenticare l'applicazione e permettere così di utilizzare le Twitter API, la tabella prevede quindi i seguenti campi:
  - **Consumer_key**;
  - **Consumer_secret**;
  - **Access_token**;
  - **Access_token_secret**.

Per la struttura del database centrale dell'applicazione v. fig. 4.

Figura 4. Struttura del database di supporto dell'investigator-tool

Come principale linguaggio di programmazione è stato scelto PHP[17] (versione 5.3.8), mentre per la gestione dinamica delle componenti HTML è stato utilizzato Javascript e in particolare la libreria jQuery[18] (versione 1.8.2).

Questo strumento è suddiviso in tre parti principali: il login, la pagina di ricerca e acquisizione delle informazioni e la pagina di investigazione.

Il login è un'azione essenziale per questo tool, non solo perché, come ogni login permette l'accesso e l'utilizzo del tool, ma perché attraverso il login dell'utente, viene creato un database personale dove verranno registrate tutte le informazioni ricavate durante le fasi di ricerca.

Il login viene anticipato dalla fase di registrazione, possibile attraverso una specifica pagina. Qui l'utente inserisce all'interno di un form HTML le proprie credenziali, cioè il suo username e la sua password. Una volta verificato attraverso delle query che non ci siano altri utenti registrati con quelle credenziali, all'interno del database di supporto dell'intera applicazione, l'investigatore viene registrato.

Quando viene effettuata la registrazione, le credenziali dell'investigatore vengono inviate ad un file php attraverso una chiamata AJAX (Asynchronous JavaScript And XML), qui i dati specifici vengono salvati in una sessione php e successivamente attraverso una query specifica viene creato un database personale dell'investigatore chiamato *dataset_inv_username*, dove verranno salvate tutte le sue ricerche. Il database personale è suddiviso nelle seguenti tabelle:

- **Users**, qui vengono salvati tutti i dati relativi agli account degli utenti che siamo andati a cercare nella sezione di ricerca;
- **Timeline**, questa tabella raccoglie, nel caso fosse stato richiesto, le informazioni degli ultimi n tweets dell'utente analizzato;
- **Preferiti**, in questa tabella vengono salvati i dati relativi ai tweets che sono segnalati come preferiti dall'utente analizzato
- **Follower**, in questa tabella vengono raccolti gli ID dei follower dell'utente esaminato;

[17] http://php.net/manual/en/
[18] http://api.jquery.com/

- **Following**, questa tabella raccoglie invece gli ID degli account seguiti dall'utente analizzato.

Per la struttura del database personale dell'investigatore v. fig. 5.

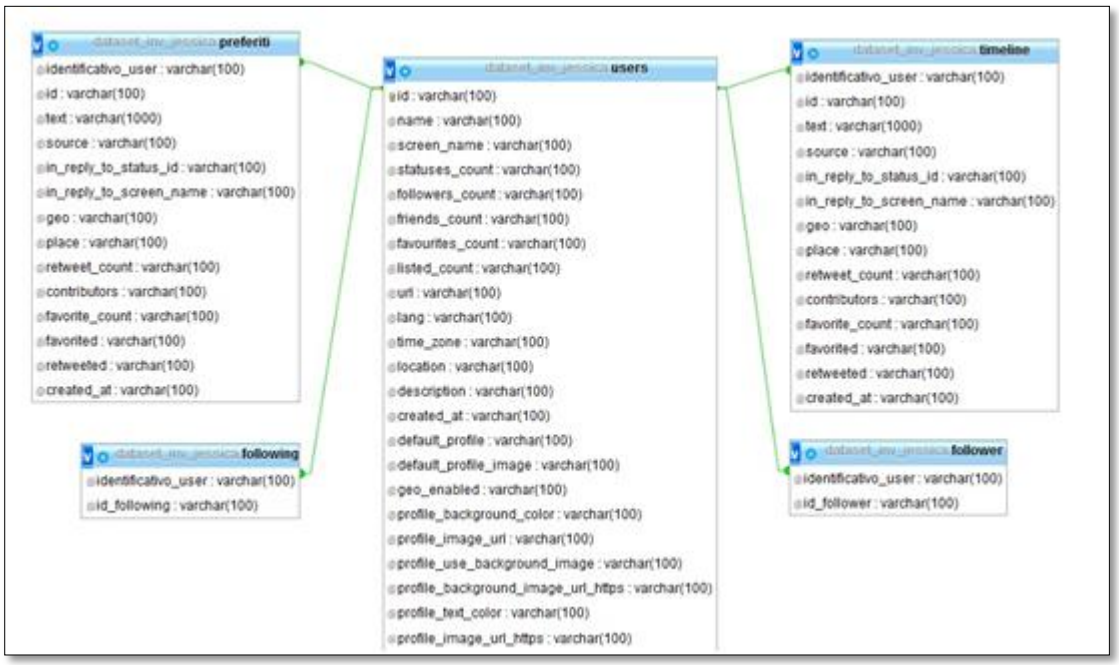

Figura 5. Struttura del dataset personale dell'investigatore

3.3.1. Ricerca

Una volta effettuato il login e creato automaticamente il database di riferimento dell'investigatore, il nuovo investigatore viene ricondotto nella schermata principale dell'investigator-tool, cioè la pagina di ricerca (v. fig. 6) e acquisizione dei dati.

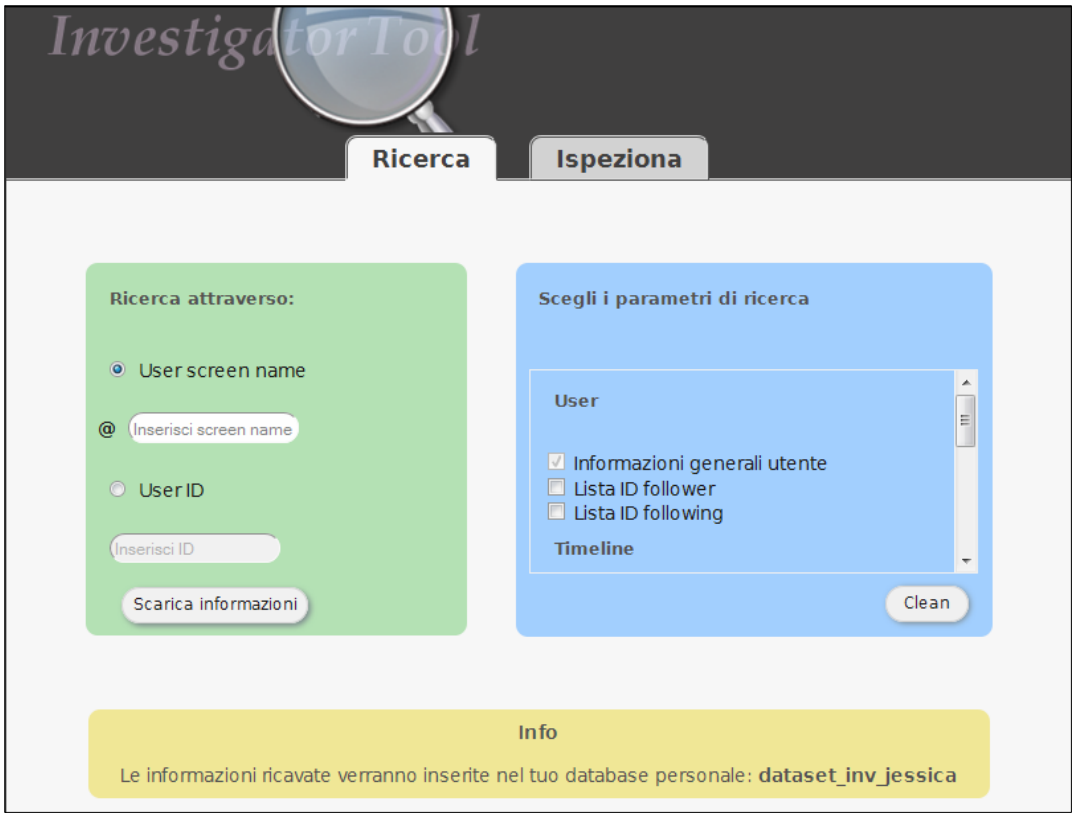

Figura 6. Pagina di ricerca dell'investigator-tool

Questa pagina è suddivisa in due colonne principali. Nella colonna sinistra viene richiesto di scegliere se effettuare la ricerca attraverso ID oppure attraverso screen name dell'utente Twitter da analizzare.

Una volta effettuata la scelta attraverso un input di tipo radio, si attiverà la textarea dove è possibile inserire la chiave di ricerca.

Nella colonna destra invece troviamo una serie di parametri, essenziali per quanto riguarda i dati che si vuole acquisire, infatti qui scegliamo cosa ci interessa ricavare dell'utente indicato nella colonna sinistra. I parametri si suddividono in tre macro sezioni di interesse, cioè User, Timeline e Preferiti.

Nella sezione User, attraverso tre input di tipo checkbox, possiamo scegliere tre dati importanti da ottenere, cioè le informazioni generali dell'account, la lista degli ID dei follower e la lista degli ID dei following.

La possibilità di poter acquisire la lista degli ID di follower e following di un certo utente spiega la scelta di decidere se ricercare un utente attraverso screen name o

ID; infatti, la ricerca attraverso ID, permette di poter effettuare ricerche anche sui follower o sui following acquisiti di un certo account. Questo comporta una possibilità di ricerca e analisi molto approfondita che permette di studiare anche i legami tra i vari utenti.

Nella seconda sezione riguardante le timeline possiamo ottenere gli ultimi tweets dell'utente attraverso la scelta della quantità degli ultimi tweets che vogliamo acquisire per mezzo degli input radio; la scelta è tra 1, 5, 10 o 20 tweets. Se nessuno di questi viene selezionato, non verrà acquisito nessun tweets dell'utente.

Nell'ultima sezione, cioè quella riguardanti i tweets preferiti troviamo una scelta analoga alla sezione precedente, infatti anche qui viene richiesto il numero di tweets preferiti da ottenere attraverso input radio, e nel caso in cui questi non vengano selezionati non verranno acquisiti i tweets preferiti.

La sezione dei parametri di ricerca può essere resettata attraverso il pulsante *Clean* che agisce attraverso dei comandi impostati attraverso jQuery.

Una volta cliccato il pulsante *Scarica informazioni*, attraverso il file jQuery sarà fatto un controllo sull'inserimento di ID o screen name e la scelta dei parametri, in modo da avvertire l'investigatore nel caso in cui ci fossero degli errori che impedirebbero l'operazione. Nel caso in cui il controllo fosse andato a buon fine, attraverso il file jQuery partirà una chiamata AJAX che invierà ad un file PHP tutti i parametri di ricerca (v. fig. 7).

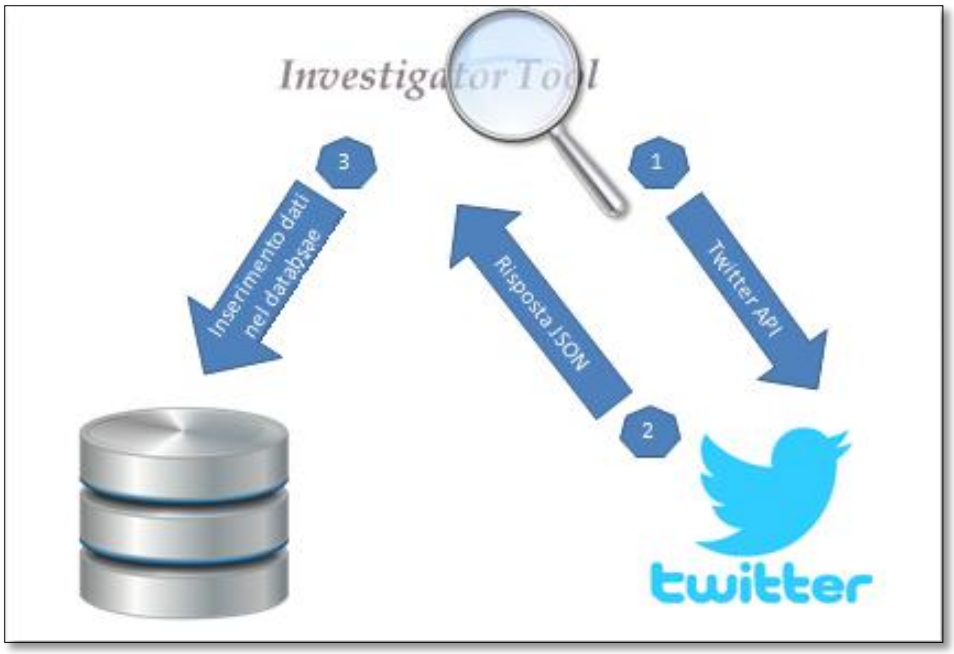

Figura 7. Interazione componenti dell'architettura

La chiamata API sarà inviata insieme ai token di accesso dell'applicazione, salvati nel database centrale, per determinare l'autenticazione e quindi permettere l'utilizzo di tali API. Questo è possibile grazie all'utilizzo della libreria php open source *twitteroauth.php*[19] creata da Abraham Williams per il supporto di OAuth e quindi per utilizzare le Twitter API. Insieme a questa è stata utilizzata anche la libreria OAuth.php necessaria per il funzionamento della prima.

Attraverso l'utilizzo delle Twitter API, verranno acquisiti tutti i dati richiesti e inseriti, tramite il file PHP, all'interno del database personale dell'investigatore. Qui di seguito vengono riportate le API utilizzate, presentate senza i parametri di ricerca:

- **https://api.twitter.com/1.1/users/show.json**, utilizzata per recuperare tutte le informazioni generali dell'utente da analizzare, quali ID, name, screen name ed altri dati riguardanti l'account Twitter;
- **https://api.twitter.com/1.1/statuses/user_timeline.json**, impiegata per acquisire la timeline dell'utente;
- **https://api.twitter.com/1.1/followers/ids.json**, usata per ricavare la lista degli ID dei follower;

[19] https://github.com/abraham/twitteroauth

- **https://api.twitter.com/1.1/friends/ids.json**, utilizzata per ricavare la lista degli ID dei following dell'utente analizzato;

3.3.2. Investigazione

La seconda pagina che troviamo nel menù di navigazione dello strumento è quella dedicata all'investigazione dei dati ottenuti attraverso la sezione di ricerca (v. fig. 8).

Figura 8. Pagina d'investigazione dell'investigator-tool

In questa pagina è possibile scegliere quali dati andare ad analizzare, in particolare abbiamo la scelta tra utenti, timeline o preferiti.

Se viene scelto di analizzare i dati attraverso una ricerca in base all'utente, è possibile scegliere, grazie a degli input radio, se visualizzare tutti gli utenti salvati nel database personale, oppure cercare un particolare utente per mezzo di una textarea dove sarà possibile inserire uno screen name o un ID come parametro di ricerca.

Le informazioni verranno ricavate attraverso delle interrogazioni del database, per mezzo di apposite query SQL, fornite dei parametri di ricerca grazie ad uno script jQuery.

Una volta inseriti i filtri di ricerca, cliccando sul pulsante *Mostra utenti*, apparirà nella parte inferiore della pagina il risultato. Più precisamente, verrà visualizzata una tabella con i risultati della ricerca (v. fig. 9). La tabella mostrerà varie informazioni degli utenti, cioè il loro screen name, l'ID, il numero di tweets creati, il numero dei follower e dei following ed infine il numero di tweets preferiti.

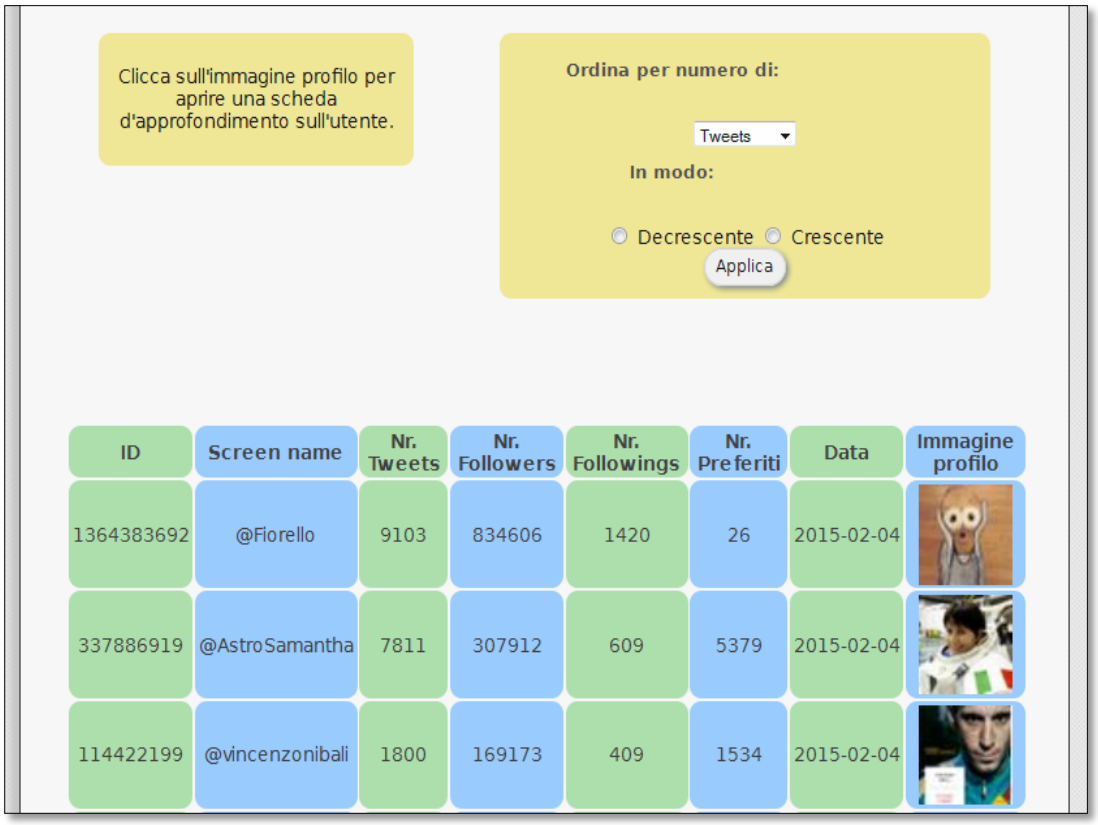

Figura 9. Risultato investigazione degli utenti

I risultati nella tabella possono essere visualizzati in ordine diverso a seconda delle esigenze dell'investigatore, infatti attraverso una select e dei bottoni radio posizionati sopra il risultato della ricerca è possibile scegliere se ordinare in modo crescente o decrescente gli utenti in base al numero di tweets, di follower, following e di tweets preferiti.

Per ogni utente sarà possibile andare ad analizzare le informazioni personali, acquisite nella fase di ricerca, per mezzo dell'immagine del profilo dell'utente. Cliccando sull'immagine si aprirà una nuova finestra del browser, denominata *scheda d'approfondimento* (v. fig. 10), che permetterà di visualizzare e analizzare i vari dati ottenuti dell'utente.

Figura 10. Scheda d'approfondimento

La scheda d'approfondimento è strutturata in cinque sezioni principali:

- **Info generali**, qui viene presentato uno specchietto con le informazioni generali dell'utente, tra cui e screen name. Inoltre viene indicato il numero di tweets, follower, following e preferiti totali dell'utene e quelli salvati all'interno del database.
- **Timeline**, in questa sezione vengono presentati i tweet acquisiti dell'utente attraverso la loro embedded view. Inoltre viene visualizzata la loro ricorrenza all'interno del database, questo dato è molto importante per evidenziare la

presenza di altri utenti analizzati che hanno dei tweets in comune[20]. Cliccando sulla ricorrenza del tweets sarà possibile visualizzare le informazioni degli utenti che condividono il tweet;

- **Follower**, qui verrà presentata la lista degli ID dei follower dell'utente e la loro ricorrenza all'interno della tabella *follower,* per far rilevare dei collegamenti tra i vari utenti che siamo andati ad analizzare. Cliccando sulla ricorrenza comparirà uno specchietto con le informazioni degli utenti che condividono il follower;
- **Following**, questa sezione si presenta analogalmente a quella precedente dedicata ai follower;
- **Preferiti**, qui vengono visulaizzati i tweets preferiti dell'utente in modo equivalente alla sezione Timeline.

Se invece vogliamo effettuare una ricerca per timeline (v. fig. 11) o per tweets preferiti, sono previsti tre parametri di ricerca tra cui scegliere. Possiamo infatti effettuare una ricerca per utente, inserendo l'ID o lo screen name per cui vogliamo visualizzare i tweets; inserendo una stringa di testo da cercare all'interno del tweets stesso oppure scegliere di visualizzare l'intero dataset di tweet indipendentemente dal loro contenuto e dall'utente che li ha pubblicati.

[20] Una delle caratteristiche principali dei bot che condividono un dataset di tweets è proprio quello di avere dei tweets in comune.

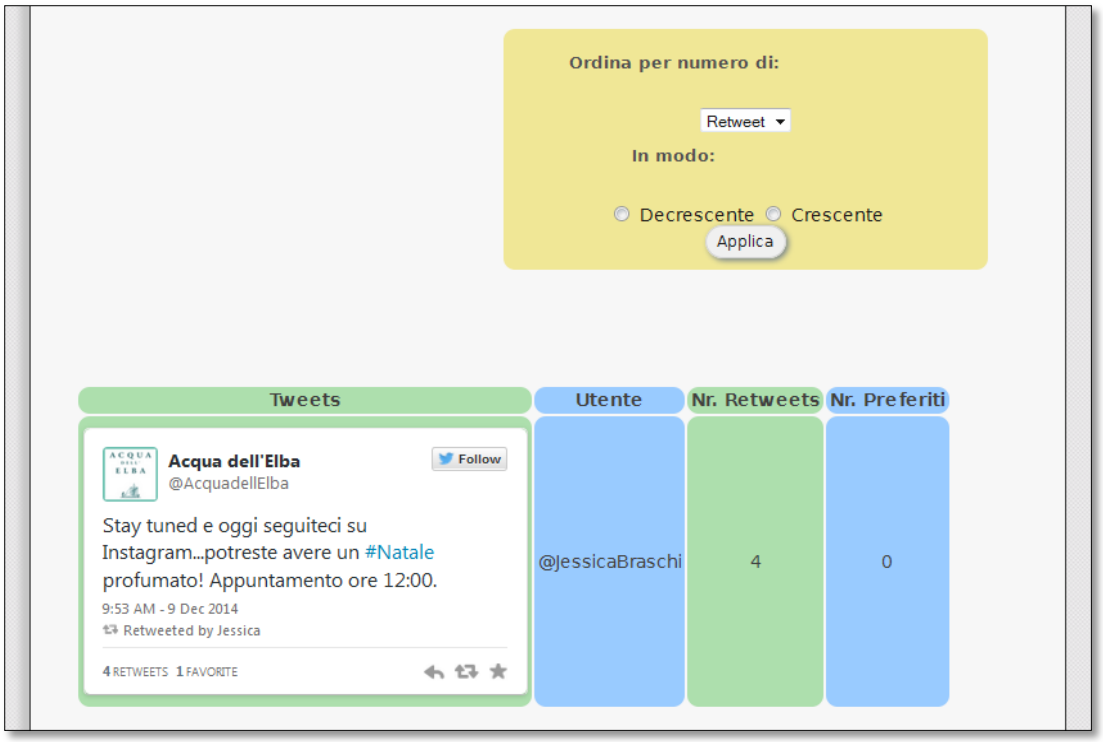

Figura 11. Risultato investigazione dei tweets

Nel primo caso verranno visualizzati, attraverso un embedded view, i tweets dello specifico utente indicato, salvati all'interno del database. Qui sarà possibile ordinarli in ordine crescente o decrescente in base al numero di retweets o preferiti che ha ottenuto.

L'embedded view del tweet permette all'investigatore di approfondire la propria ricerca, infatti questo tipo di visualizzazione del tweets permette di interagire con esso e di acquisire informazioni più dettagliate attraverso la sola visualizzazione.

Questa particolare visualizzazione è permessa attraverso l'utilizzo di uno specifico widget Twitter, munito dei parametri specifici dell'utente, il quale si presenta sottoforma di una linea di codice HTML.

3.4. Problemi e soluzioni

Durante la fase di progettazione iniziale è stata riscontrata un'unica difficoltà che ha fatto ripensare alla struttura generale dell'applicazione. Infatti inizialmente il tool, oltre a non prevedere una sezione dedicata all'analisi dei dati, non permetteva la scelta delle informazioni che si volevano acquisire.

Il tool prevedeva il solo inserimento dello screen name dell'utente da analizzare e attraverso quello venivano scaricate tutte le informazioni generali dell'utente, tutti i tweets pubblicati dall'account e tutte le informazioni generali dei follower e dei following. Questo voleva dire effettuare una chiamata API per ogni singolo follower ed ogni following.

Dopo un attento utilizzo del tool è stato riscontrato che questa impostazione strutturale poteva funzionare bene se si andava a lavorare con account che possedevano numeri limitati di tweets, follower e following; questo perché l'utilizzo delle Twitter API prevede un limite alle chiamate che si possono effettuare, questo limite è detto *Rate Limit*[21].

Il rate limit impostato per la maggior parte di API Twitter è di 15 chiamate ogni 15 minuti, una volta superato il limite le chiamate si bloccano. Questa caratteristica delle API comportava un enorme problema, infatti, con queste specifiche tecniche, se avessimo voluto prendere in considerazione un account molto popolare come quello di Barack Obama[22], (che, al momento della scrittura di questa tesi, vanta 12900 tweets, 646000 following e 52,6 milioni di follower), avremmo ottenuto dei risultati incompleti, e quindi l'applicazione non sarebbe stata né efficace né efficiente.

Il problema è stato risolto attraverso la riprogettazione della sezione dedicata alla ricerca, a questo punto, sono stati inseriti dei parametri, secondo i quali l'investigatore avrebbe potuto scegliere cosa andare ad acquisire di ogni singolo utente. Questa soluzione è stata ancora più apprezzata, quando l'obiettivo del tool si è spostato, dalla creazione di uno strumento di recupero delle informazioni su account Twitter, con lo scopo di annotarli, a strumento di acquisizione di informazioni su account Twitter per successive analisi, specificatamente rivolte allo studio del

[21] https://dev.twitter.com/rest/public/rate-limiting
[22] https://twitter.com/BarackObama

fenomeno dei Bot. Questo grazie alla nuova impostazione del tool che permette di effettuare analisi più precise e mirate, per mezzo della sezione d'investigazione.

4.Twitter API

In genere le API o *Application Programming Interface* sono, come suggerisce il loro nome, delle interfacce, che divengono essenziali per far in modo che uno sviluppatore possa interagire con una certa piattaforma, in modo da poter così estendere la struttura base della piattaforma stessa.

Le API infatti permettono di accedere a molteplici funzionalità di una piattaforma e di utilizzarle per andare ad ampliare una propria applicazione attraverso l'interazione con la piattaforma stessa. Da questo punto di vista le API sono un ottimo strumento per promuovere una piattaforma offrendo ad altri un modo per interagirci.

Possiamo trovare due tipologie di API: queste infatti possono presentarsi come librerie di codice con funzioni che possono essere utilizzate da uno sviluppatore, oppure possono essere delle singole linee di codice, cioè delle chiamate alla piattaforma distributrice che ci invia il risultato di tale chiamate.

Le API Twitter utilizzate per la creazione dell'investigator-tool appartengono alla seconda tipologia.

La piattaforma di Twitter in particolare, mette a disposizione degli sviluppatori diversi moduli di interazione con la piattaforma. Uno di questi è *Fabric*, utilizzato per l'implementazione di applicazioni mobile, che fornisce un'insieme di strumenti, suddivisi rispettivamente a seconda del sistema operativo per il quale stiamo sviluppando (Android e iOS). Questo modulo permette di rendere l'applicazione compatibile con Twitter, rendendo possibile, per esempio, la condivisione diretta di materiale sulla piattaforma o il login attraverso le proprie credenziali Twitter.

Un altro modulo interessante è quello dedicato agli widgets che, non solo mette a disposizione degli sviluppatori widgets da integrare nel proprio sito o nella propria applicazione, ma anche script per integrare al meglio Twitter all'interno della propria pagina, infatti il modulo mette a disposizione anche bottoni di interazione diretta con Twitter, come il tweet botton e il follower botton.

Per la creazione di investigator-tool, e in particolare della pagina dedicata all'investigazione, è stato utilizzato questo modulo, infatti sono stati utilizzati gli widgets che permettono una vista embeddata delle timeline dell'utente e dei tweets preferiti. Questo ha permesso di avere, non solo un'applicazione esteticamente più gradevole, ma anche maggiori informazioni sul materiale di studio degli investigatori, attraverso i dati ricavabili da questa tipologia di visualizzazione, quali data e ora della pubblicazione, e eventuali retweets e replies esistenti.

Il modulo più significativo per questo tool, che mette a disposizione Twitter per gli sviluppatori, è quello dedicato alle rest API, infatti su queste si basa la funzionalità principale di Investigator-tool.

Le API permettono l'accesso ai dati di Twitter, come per esempio alle informazioni di un particolare profilo, informazioni legate ai follower e molto altro. Il risultato delle chiamate API viene restituito nel formato JSON.

Per accedere all'utilizzo delle API Twitter dalla versione 1.1, cioè la corrente, è necessaria un'autenticazione dell'utente o dell'applicazione che ne fa uso attraverso OAuth, un protocollo aperto che consente un accesso sicuro grazie ad una semplice autenticazione attraverso le credenziali del proprio account Twitter, o i token acquisiti durante la registrazione della propria applicazione. Nel caso in cui si inviasse una chiamata API con un'autenticazione errata il risultato sarà:

- {"errors": [{"message": "Bad Authentication data", "code": 215}]}

Le API si differenziano in due tipologie principali:

- **GET API**, questa tipologia di API è quella che è stata utilizzata all'interno di Investigator-tool; queste API permettono una lettura dei dati richiesti senza andarli a modificare all'interno della struttura di Twitter;
- **POST API**, questa tipologia di API invece permette di modificare i dati Twitter, possiamo per esempio modificare, abilitare o disabilitare un'immagine del profilo Twitter.

Come precedentemente spiegato, le Twitter API dispongono di una limitazione di chiamate in una finestra di tempo di 15 minuti, questo limite è chiamato Rate limit.

I Rate limit si differenziano a seconda dell'autenticazione che andiamo a fare, che può essere un'autenticazione di un'applicazione, oppure di un utente. Nel nostro caso ci ritroviamo all'interno di un contesto di autentificazione attraverso un'applicazione.

La maggior parte delle API possono effettuare un massimo di 15 chiamate all'interno di questa finestra temporale. Qui di seguito viene mostrata una tabella con inseriti i valori esatti di Rate limit per le API utilizzate per l'investigator-tool:

Titolo API	**Richieste per ogni finestra di 15 minuti (Autenticazione Utente)**	**Richieste per ogni finestra di 15 minuti (Autenticazione Applicazione)**
GET users/show	180	180
GET followers/ids	15	15
GET friends/list	15	15
GET statuses/user_timeline	180	300
GET favorites/list	15	15

Tabella 1. Twitter API utilizzate nell'Investigator-Toor con il loro Rate Limit

Il limite inserito in una finestra di 15 minuti è una novità della versione 1.1 delle API Twitter, infatti con la precedente versione, 1.0 avevamo un blocco di 60 minuti a disposizione, oltre a questa novità viene inserita la necessità di autenticarsi ad ogni finestra di 15 minuti per effettuare nuovamente altre chiamate API, al contrario della precedente versione, dove le applicazioni con OAuth abilitato (strumento per l'autenticazione usato da Twitter) potevano effettuare 350 chiamate con metodo GET all'ora con i soliti token di accesso.

Quando un'applicazione supera il limite di API per una determinata finestra di tempo, l'API Twitter restituirà la risposta HTTP 429, indice di troppe richieste effettuate. Il messaggio visualizzato come risposta dell'API sarà:

- {"Errori": [{"codice": 88, "messaggio": "Rate limite superato"}]}

Per verificare la portata del nostro Rate limit possiamo utilizzare l'API **GET application / rate_limit_status**, che restituirà lo stato del Rate limit per il contesto applicativo della chiamata.

Qui di seguito una panoramica dettagliata sulle API che sono state utilizzate per la creazione di questo tool:

- **GET followers/ids**, questa API restituisce la lista di ID dei follower, cioè degli utenti che seguono l'account indicato attraverso screen name o ID. Questa API distribuisce la risposta in più pagine, infatti ha un limite di 5000 ID di follower restituiti a chiamata, ordinati dal più recente al più vecchio. Nel caso in cui si voglia analizzare un account con più di 5000 follower basterà aggiungere il parametro *cursor* con indicata la pagina del risultato da visualizzare, oppure se si tratta di chiamate in sequenza basta aggiungere l'opzione *previous_cursor* o *next_cursor*, per indicare rispettivamente una pagina precedente o successiva. Oltre a questo parametro molto utile per il tipo di API, ci sono altri parametri che permettono di modificare l'API in questione, come *stringify_ids* che consente di ricevere gli ID sotto forma di stringa. Il rate limit di questa API è di 15 chiamate a finestra in contesto di autenticazione con Utente Twitter, e di 300 nel caso di autenticazione attraverso applicazione.;
- **GET friends/list**, la funzione di questa API è quella di restituire la lista degli ID dei following, cioè degli utenti che sono seguiti dall'account indicato attraverso lo screen name o l'ID. Questa API ha le stesse caratteristiche strutturali dell'API *GET followers/ids* spiegata precedentemente.
- **GET statuses/user_timeline**, questa API permette di recuperare i tweets più recenti inviati da un account Twitter attraverso la specificazione dello screen name o dell'ID dell'utente. Se questa chiamata viene effettuata per acquisire la timeline di un account protetto non sarà possibile il recupero dei dati, a meno che l'utente autenticato che svolge la chiamata non sia un follower autorizzato

di questo utente o il proprietario stesso dell'account protetto. Questa API può restituire un massimo di 3200 tweets, compresi i retweets svolti dall'utente su altri tweets di proprietà di terzi utenti. Il Rate limit di questa API è di 180 chiamate a finestra in contesto di autenticazione con Utente Twitter, e di 300 nel caso di autenticazione con applicazione. Questa API può essere modificata a seconda delle necessità dello sviluppatore attraverso diversi parametri opzionali, infatti possiamo inserire, oltre allo screen name o all'ID per indicare l'account da cui acquisire la timeline, il numero di tweets che vogliamo recuperare attraverso il parametro *count,*la presenza o meno di retweets grazie al parametro *include_rts* oppure escludere o meno le risposte ai tweets attraverso *exclude_replies,* etc.;

- **GET favorites/list**, è un'API che restituisce gli ultimi 20 tweets inseriti tra i preferiti. Nel caso in cui tra i parametri non venga indicato ne lo screen name ne l'ID dell'account di riferimento verranno restituiti i tweets preferiti riguardanti l'utente autenticato che compie la chiamata API. Il Rate limit di questa API è di 15 chiamate a finestra sia in contesto di autenticazione con Utente Twitter che di autenticazione con applicazione. I parametri opzionali che possiamo modificare a seconda delle nostre esigenze sono diversi, tra cui *count*, con il quale possiamo indicare il numero di tweets da acquisire per un massimo di 200, ricordiamo che di default ne vengono recuperati 20; *include_entities,* che ci permette di decidere se visualizzare o meno le entità come URL, hashtags e mentions.

4.1.API console tool

Uno strumento molto utile che mette a disposizione Twitter, e che è stato utilizzato nella progettazione e realizzazione del tool, è la *API console tool*[23], una console online che permette di utilizzare, esplorare e testare le API Twitter. Per utilizzare la console è possibile scegliere attraverso una select, quale tipo di

[23] https://dev.twitter.com/rest/tools/console

autenticazione desideriamo effettuare, la scelta è tra nessuna autenticazione OAuth, autenticazione OAuth oppure autenticazione base.

Se viene scelta un'autenticazione OAuth, avverrà attraverso le credenziali del nostro account Twitter, altrimenti se è stata scelta un'autenticazione base, apparirà un'autenticazione HTTP: infatti verrà richiesto username e password. Lo strumento si presenta in due colonne principali, quella di sinistra racchiude una collezione di tutte le Twitter API ognuna della quali ha un link specifico alla propria documentazione.

Una volta selezionata un'API sarà possibile personalizzare i parametri e interagire con l'API attraverso una textarea, oppure utilizzando una sezione apposita che permette una personalizzazione guidata. Al momento dell'invio della chiamata osserveremo nella colonna destra il risultato in formato JSON.

Questo strumento è risultato molto utile per la realizzazione di investigator-tool, in quanto ha dato la possibilità di vedere in modo quasi istantaneo, la struttura del risultato JSON delle API che si andavano ad utilizzare, dando modo di ottimizzare i tempi sulla realizzazione degli script.

4.2. Autenticazione tramite applicazione

Per accedere alle API Twitter, come precedentemente spiegato, è necessario autenticarsi, grazie allo standard di sicurezza OAuth adottato da Twitter. L'autenticazione può essere fatta in due modi, una attraverso le credenziali del nostro account Twitter che attraverso OAuth riceverà delle chiavi da utilizzare per poter effettuare le chiamata API; oppure attraverso l'autenticazione dell'applicazione che utilizza tali API.

Per la realizzazione di questo tool è stato scelto di effettuare un'autenticazione attraverso l'applicazione, in modo da avere la disponibilità di più chiamate API all'interno di un arco temporale di 15 minuti, come sopra descritto. Per ottenere questo tipo di autenticazione è necessario registrare precedentemente l'applicazione all'indirizzo https://apps.twitter.com/. Una volta effettuata la registrazione, sarà possibile creare gli *access token* nella sezione *API Keys*, attraverso il pulsante *Create*

my access token. Una volta creati, Twitter rilascerà quattro chiavi che saranno associate all'applicazione, queste sono:

- **API key;**
- **API secret;**
- **Access token;**
- **Access token secret.**

5.OAuth

OAuth[24], acronimo di Open Authorization, è un protocollo open che permette l'accesso di un servizio HTTP, in particolare delle API, da parte di applicazioni su sistemi desktop, web e mobile. Lo sviluppo è iniziato nel novembre 2006 ad opera di un gruppo di programmatori web tra cui Blaine Cook, che all'epoca stava sviluppando il sistema Twitter OpenID[25], altro protocollo di autenticazione. L'idea fu quella di utilizzare OpenID in combinazione con le API Twitter per delegare l'autenticazione a Twitter stesso. Da questa idea, nel luglio 2007 fu rilasciata la versione finale di OAuth Core 1.0.

Con il crescente successo di siti web come Twitter, Facebook, Google etc. sono nate intorno ad essi applicazioni, sviluppate da terze parti, per utilizzare questi servizi; basti pensare ai vari client mobile per i social network. Parallelamente è quindi nata la necessità di autorizzare queste applicazioni ad accedere, in modo sicuro, ai dati privati dell'utente.

Prima della creazione di questo protocollo esistevano diversi protocolli proprietari come ad esempio Google AuthSub, AOL OpenAuth, Yahoo BBAuth, Flickr API e Amazon Web Services API. Infatti OAuth si ispira proprio a questi protocolli creando una standardizzazione che integra i migliori elementi di ognuno di essi. OAuth si differenzia dagli altri protocolli anche per la sua gestione e il supporto diretto di applicazioni desktop,dispositivi mobili e siti web.

Nel modello standard di interazione se un utente vuole accedere a dei contenuti riservati ospitati nel server, ha l'obbligo di registrare le proprie credenziali, solitamente attraverso username e password, che verranno registrati per essere riutilizzati; questo comporta un limite alla sicurezza, basti pensare nel caso in cui l'utente utilizzi applicazioni sviluppate da terzi, ecco che qui le credenziali non sono più riservate al servizio e all'utente, infatti vengono salvate anche dall'applicazione client del servizio, e rimarranno in suo possesso fino al cambiamento delle credenziali da parte dell'utente.

[24] http://oauth.net/documentation/
[25] http://openid.net/developers/specs/

Invece con l'utilizzo del protocollo di autenticazione OAuth questo problema viene risolto, grazie all'introduzione di una terza entità che vada a fare da tramite tra l'applicazione client e il server (nel nostro caso rispettivamente Investigator-tool e Twitter), questa entità è il proprietario della risorsa (resource owner). Attraverso OAuth quindi l'applicazione, deve richiede il permesso all'utente per accedere alle sue risorse nel server, e inoltre OAuth permette al server stesso di verificare non solo che il client abbia l'autorizzazione da parte dell'utente, ma anche l'identità dell'applicazione che fa la richiesta.

Quindi, per fare in moda che l'applicazione possa accedere alle risorse dell'utente salvate nel server, in primo luogo deve ottenere il permesso dal proprietario della risorsa, quindi dall'utente stesso. Questa autorizzazione viene espressa attraverso i tokens.

È proprio l'utilizzo dei token cioè di queste chiavi che permette al protocollo di gestire gli accessi senza l'utilizzo e la condivisione delle credenziali. Inoltre questi tokens danno ancora maggiore sicurezza, infatti diversamente dalle credenziali dell'utente, possono essere rilasciati con delle restrizioni e con una durata limitata.

Le caratteristiche principali di questo standard d'autenticazione per l'utilizzo delle API sono:

- **Semplicità**, in quanto è facile da integrare da parte degli sviluppatori grazie alle librerie esistenti;
- **Sicurezza,** perché nessuno sviluppatore può entrare in contatto con le credenziali di un utente come al contrario avviene con l'utilizzo dei classici login che utilizzano la registrazione di username e password;
- **Flessibilità,** in quanto non c'è bisogno della creazione di un database che raccolga le credenziali degli utenti da registrare;
- **Open,** perché le sue librerie sono delle risorse aperte, che ogni sviluppatore può implementare e usare a piacimento, inoltre tutte le specifiche tecniche di OAuth sono pubblicate dalla community. Le librerie di OAuth ad oggi esistenti sono disponibili su diverse piattaforme: Java, PHP, C, C#, Javascript, .NET, Objective-C, Perl, Python, Ruby, ActionScript e altri.

Come detto in precedenza le credenziali assegnate da OAuth per l'autenticazione sono dei token che non vengono registrati da nessuna applicazione per garantire maggiora sicurezza; possiamo trovare tre tipi di credenziali: *client credentials* che comprendono Consumer Key e *Consumer Secret*; *Temporary credentials* distinte in *Request Token* e *Request Token Secret* e *Token credentials* che si distinguono in *Access Token* e *Access Token Secret*.

Il protocollo definisce diverse entità per il suo funzionamento, queste sono:

- **Service Provider**, che è il sito o servizio web, all'interno del quale sono memorizzate le risorse;
- **Resource Owner**, cioè colui che possiede un account nel Service Provider, cioè l'utente web;
- **Consumer**, che identifica un sito o applicazione che usa OAuth per accedere alle informazioni dell'utente nel Service Provider attraverso la delega dell'utente stesso;
- **Risorse Protette**; che sono i dati registrati all'interno dal Service Provider, alle quali il Consumer può accedere tramite autenticazione;
- **Consumer Key**, cioè il valore usato dal consumer per identificarsi con il Service Provider;
- **Consumer Secret**, che è il valore segreto usato dal Consumer per stabilire la proprietà della Consumer Key;
- **Request Token**, cioè il valore usato dal consumer per ottenere l'autorizzazione da parte dell'utente e scambiato con un Access Token;
- **Access Token**, che rappresenta il valore usato dal Consumer per avere accesso alle risorse protette per conto dell'utente, invece di usare le credenziali dell'utente stesso sul Service Provider;
- **Token Secret**, che è il valore segreto utilizzato dal consumer per stabilire la proprietà del token ricevuto.

Il protocollo di autenticazione OAuth si divide in due fasi principali. La prima parte permettere agli utenti di autorizzare il client ad accedere alle loro risorse, attraverso l'autenticazione diretta con il server. Quest'ultimo fornirà al client, dopo aver effettuato l'autenticazione nel server, i tokens da usare nel metodo di autenticazione.

Tipicamente, i token sono emessi dal server su richiesta dell'utente, dopo che quest'ultimo è stato autenticato, di solito attraverso l'inserimento delle credenziali con cui è registrato l'utente all'interno del server. Ci sono molti modi in cui il server fornisce i token al client, uno di questi è attraverso uno scambio HTTP, dove il client ottiene dal server delle chiavi temporanee utilizzate per identificare la richiesta di accesso durante l'intera fase di autenticazione. Una volta che l'utente da la sua autorizzazione al server di accettare le richieste del client, questo sarà fornito del set di tokens che gli permetteranno di accedere alle risorse riservate dell'utente. Le credenziali temporanee iniziale verranno revocate una volta ottenuti i tokens necessari e comunque queste hanno una durata limitata per garantire la sicurezza delle risorse dell'utente.

La seconda parte del protocollo invece, definisce un metodo per eseguire richieste HTTP autenticate usando due set di credenziali, uno che identifica il client che fa la richiesta e il secondo che identifica il possessore delle risorse in nome del quale vengono effettuate le richieste.

6.Risultati

I risultati ottenuti hanno evidenziato uno strumento di facile usabilità grazie ad un'interfaccia user-friendly, che permette un utilizzo semplice da parte di ogni tipo di utente.

Nella sezione dedicata alla ricerca, i vari input rendono agevole la scelta delle opzioni riguardanti i dati che vogliamo acquisire; inoltre sono utili per dare all'investigatore un riepilogo, chiaro e semplice da modificare, di ciò che sta per inserire all'interno del proprio database.

Sempre in questa sezione, la possibilità di effettuare la ricerca sia attraverso screen name, sia attraverso ID dell'utente, permette di effettuare ricerche incrociate sui dati acquisiti dei follower o dei following di un particolare utente, dato che questi vengono ottenuti sottoforma di liste di ID.

Grazie a questa caratteristica è possibile ricavare le informazioni generali dei follower o dei following, di un particolare utente, di cui ci interessa approfondire la ricerca.

La scelta di inserire i dati ottenuti all'interno di database separati per ogni investigatore, oltre che ad organizzare in maniera più precisa i vari dati, permette all'investigatore di utilizzare il proprio dataset per diversi impieghi e ambiti di ricerca in modo più semplice e diretto.

La sezione di analisi, nonostante le diverse operazioni che possiamo effettuare sui dati visualizzati, è semplice e di facile utilizzo, permettendo una semplice analisi dei dati, svolgendo quindi la sua funzione in modo efficace.

Le varie schede d'approfondimento rendono possibile la comparazione diretta di più utenti Twitter, mantenendo sempre un'interfaccia semplice e ben organizzata.

Proprio questa caratteristica del tool, che prevede un'interfaccia per l'analisi dei dati, inizialmente non era contemplata: era possibile svolgerla solamente all'interno del database personale dell'investigatore, attraverso delle interrogazioni per mezzo di query SQL.

L’interfaccia grafica non ha solo reso l’analisi dei dati più semplice e intuitiva, ma ha dato al tool la possibilità, che in futuro, sia disponibile anche per individui al di fuori dell’ambito accademico.

Una struttura complessa su più livelli, come quella dell’investigator-tool, che risulta avere un’usabilità così agevole, permette di avere un utilizzo più duraturo dell’applicazione nella solita sessione di lavoro, tuttavia senza andare ad incidere negativamente sui risultati.

7.Conclusioni

Questa attività di studio del fenomeno di spammer, fake e bot all'interno dei social network ed in particolare della piattaforma Twitter, ha portato alla progettazione, lo sviluppo e la realizzazione di investigator-tool, uno web-tool ideato per l'acquisizione e l'analisi degli utenti Twitter, con lo scopo di studiare e individuare gli account bot che si trovano all'interno di questa piattaforma.

Questo strumento è cresciuto sempre più durante le fasi della sua progettazione, infatti la necessità iniziale che ha portato alla creazione del tool deriva dall'esigenza di disporre di uno strumento volto all'acquisizione di informazioni generali riguardante gli account Twitter per poter poi annotare tali utenti attraverso #tweetag (altro tool specifico per l'annotazione), allo scopo di annotare gli utenti fake per il progetto *@thefakeproject*.

Le caratteristiche proprie degli utenti fake hanno spostato il focus dell'investigator-tool, dagli utenti fake, agli utenti bot, che dispongono ancora oggi di una letteratura accademica limitata.

Una delle particolarità di questo tool è che la sua struttura generale non limita il suo utilizzo al solo studio dei bot, infatti può essere utilizzato per diversi studi e funzioni che riguardano l'analisi degli utenti Twitter e dei loro tweets.

Questo è possibile grazie ai database che raccolgono i dati ottenuti; hanno una struttura predisposta per acquisire i dati restituiti dalle Twitter API, in modo che questi possano essere utilizzati per qualsiasi tipo di ricerca, e non nel solo campo di studio dei bot.

Inoltre i dati registrati nella tabella utenti, del database dell'investigatore, costituiscono un dataset compatibile con lo strumento di annotazione #tweetag, sono quindi utilizzabili per l'annotazione delle timeline degli utenti, con lo scopo di realizzare algoritmi di apprendimento automatico basati su tali dati.

Bibliografia

1. M.Cha, H.Haddadi, F.Benevenuto, K.P.Gummadi. 2012. The World of Connections and Information Flow in Twitter. In: *Transactions on Systems, Man and Cybernetics*, pp 991-998.
2. C. Grier, K. Thomas, V. Paxson, M. Zhang. 2010. @spam: the underground on 140 characters or less. In: *Conference on Computer and Communications Security*.
3. C. Smith. 2013. By The Numbers: 68 Amazing Twitter Stats. In: *http://expandedramblings.com/*.
4. D.Casati. 2012. Grillo su Twitter? "Sono fasulli il 54% dei seguaci". In: *Corriere della sera (edizione online).*
5. D.M.Boyd, N.B.Ellison. 2007. Social Network Sites: Definition, History, and Scholarship. In: *Journal of Computer-Mediated Communication*, pp 210-230.
6. E.Pariser. 2011. *The Filter Bubble: What the Internet Is Hiding from You.* New York, Penguin Group.
7. G. Stringhini, C. Kruegel, G. Vigna. 2010. Detecting spammers on social networks. In: *26th Annual Computer Security Applications Conference*, pp 1-9.
8. H.Kwak, C.Lee, H.Park, S.Moon. 2010. What is Twitter, a social network or a news media? In: *WWW '10 Proceedings of the 19th international conference on World wide web*, pp 591-600.
9. K. Thomas, C. Grier, V. Paxson, D. Song. 2011. Suspended accounts in retrospect: an analysis of Twitter spam. In: *Conference on Internet Measurement*.
10. Le monde. 2013. BANQUE POPULAIRE – Dis-moi combien d'amis tu as sur Facebook, je te dirai si ta banque va t'accorder un prêt. In: *Big browser, blog.*
11. L.Garton, C.Haythornthwaite, B.Wellman. 2006. Studying Online Social Networks. In: *Journal of Computer-Mediated Communication*.
12. M.Camisani-Calzolari. 2012.Analysis of Twitter followers of the US Presidential Election candidates: Barack Obama and Mitt Romney. In: *http://digitalevaluations.com/*.

13. P.Hayati, V.Potdar, A.Talevski, N.Firoozeh, S.Sarenke, E.A.Yeganeh. 2010. Definition of Spam 2.0: New Spamming Boom. In: *Digital Ecosystems and Technologies (DEST), 4th IEEE International Conference*, pp 580-584.
14. P.Rutledge. 2013. How Obama Won the Social Media Battle in the 2012 Presidential Campaign. In: *http://mprcenter.org/blog/*.
15. S. Cresci, M. Petrocchi, A. Spognardi, M. Tesconi, & R.D. Pietro. 2014. A Criticism to Society (as seen by Twitter analytics). In: *Distributed Computing Systems Workshops*, pp. 194-200.
16. S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi. 2014. A Fake Follower Story: improving fake accounts detection on Twitter. IIT-CNR, Tech. Rep., submitted.

Sitografia

1. Facebook, http://facebook.com/, (consultato il 05/02/2015).
2. LikeAlyzer, *by meltwater*, http://likealyzer.com/about, (consultato il 04/02/2015).
3. Mention tool, https://en.mention.com/, (consultato il 04/02/2015).
4. OAuth Protocol, *Documentation*, http://oauth.net/documentation/, (consultato il 04/02/2015).
5. Socialbakers, http://www.socialbakers.com/, (consultato il 04/02/2015).
6. Statuspeople, *The Twitter Follower Experts and Inventers of the Fakers App*, https://statuspeople.com/, (consultato il 04/02/2015).
7. Twitter, http://twitter.com/, (consultato il 05/02/2015).
8. Twitter API, *Documentation,* https://dev.twitter.com/overview/documentation, (consultato il 04/02/2015).
9. Twitter API, *Exploring the Twitter API*, https://dev.twitter.com/rest/tools/console, (consultato il 04/02/2015).
10. Twitteraudit, https://www.twitteraudit.com/, (consultato il 04/02/2015).
11. Wikipedia, *L'enciclopedia libera*, Bolla di filtraggio, http://it.wikipedia.org/wiki/Bolla_di_filtraggio, (consultato il 04/02/2015).
12. Wikipedia, *L'enciclopedia libera*, OAuth, http://it.wikipedia.org/wiki/OAuth, (consultato il 04/02/2015).
13. Wikipedia, *L'enciclopedia libera*, Web reputation, http://it.wikipedia.org/wiki/Web_reputation, (consultato il 04/02/2015).

Ringraziamenti

Desidero fortemente ringraziare tutte le persone che mi hanno aiutato in questo periodo importante della mia vita e in particolare chi mi ha aiutato nella stesura di questa tesi, con suggerimenti, critiche ed osservazioni.

Anzitutto vorrei ringraziare il mio relatore Prof. Maurizio Tesconi, che è stato per me una grande guida: con la sua professionalità e la passione per il suo lavoro ha fatto in modo che arrivassi a questo traguardo.

Un ringraziamento particolare va ai miei correlatori Prof. Stefano Cresci e Prof. Mariantonietta Noemi La Polla, per i loro suggerimenti e per l'aiuto che hanno dato per lo sviluppo di questa tesi.

Tra le persone a me più vicine in questo ultimo peridio vorrei mandare un ringraziamento particolare ai miei genitori, che hanno reso possibile questo percorso, ai miei nonni e a Grazia che hanno avuto sempre un momento da dedicarmi per ascoltarmi e per darmi saggi consigli.

Ringrazio Francesco che mi ha accompagnato in questo bellissimo viaggio, supportandomi e incoraggiandomi nei momenti più difficili: senza di lui e i suoi preziosi consigli sarebbe stato tutto molto più difficile.

Inoltre ringrazio la mia collega e amica Serena, non solo per il suo aiuto tecnico ma anche per le nostre chiacchierate che mi hanno aiutato più di quanto lei possa immaginare.

Infine ringrazio Gabriele, a cui dedico questa tesi: ogni giorno provo ad insegnargli qualcosa ma è lui ad insegnarmi quanto bello sia questo viaggio.