Università degli Studi di Verona

DIPARTIMENTO DI INFORMATICA
Corso di Laurea in Informatica

WhatsApp Messenger

Candidato:
Alberto Marini
Matricola VR359129

Relatore:
Prof. Damiano Carra

Anno Accademico 2013 - 2014

Indice

Capitolo 1

Introduzione

Negli anni in cui ci troviamo, pare sempre più impensabile riuscire a lavorare, divertirsi e progredire senza l'utilizzo degli smartphone. La società di ricerche International Data Corporation (Idc), ha segnalato nel suo Worldwide Quarterly Mobile Phone Tracker che, durante lo scorso anno, le consegne di smartphone sono aumentate del 38,4% ad addirittura 1,0042 miliardi di unità. Oramai, tali dispositivi mobili sono entrati a far parte della vita quotidiana di tutti noi soprattutto grazie alla loro versatilità, ottenuta con l'utilizzo di applicazioni. Tali "app" permettono di fare infinite cose e in qualsiasi ambito, dallo sport, alla cucina, al business. Con l'avvento degli smartphone è cambiato anche il modo di comunicare. Gli SMS, utilizzati fino a qualche anno fa, sono quasi superati da applicazioni che permettono di scambiarsi messaggi in maniera totalmente gratuita sfruttando la rete dati del dispositivo. Tali applicazioni non si limitano al semplice scambio di messaggi di testo, ma danno la possibilità, anche, di scambiarsi immagini, video, audio e di creare messaggi di gruppo. Le applicazioni più conosciute sotto l'ambito della messaggistica sono WhatsApp [1], WeChat [2], Telegram [3] e Viber [4].

Tra le applicazioni sopra citate, la prima ad "esplodere" in termini di numero di utenti è stata WhatsApp, pubblicata nel 2009. A differenza di altre app che sono opensource, come per esempio Telegram, WhatsApp è "chiusa", nel senso che gli sviluppatori non hanno reso pubbliche informazioni specifiche dell'applicazione riguardanti per esempio i protocolli utilizzati, le modalità di scambio dei messaggi, la gestione della sicurezza e della privacy. Per questo motivo, molti dettagli implementativi riguardanti WhatsApp non si sanno con certezza, come ad esempio la dislocazione dei server nel territorio modiale, le modalità di scambio dei messaggi e le questioni legate alla sicurezza e alla crittografia.

Abbiamo deciso, pertanto, di dare delle risposte ad alcune questioni aperte riguardanti WhatsApp e, in particolare, ci siamo focalizzati su:

- localizzare (per quanto possibile) i server nel territorio mondiale;
- capire come avviene lo scambio di messaggi tra due dispositivi;
- verificare come cambiano i server connessi ad un dispositivo al cambiare della rete utilizzata.

Come vedremo in seguito, probabilmente l'architettura interpone qualche server tra due dispositivi durante l'invio di un messaggio; la scelta del server stesso, viene fatta al momento dell'inizio della connessione alla rete da parte dello smartphone.

La tesi è strutturata in 4 capitoli.
Nel secondo capitolo sono elencati e descritti gli strumenti utilizzati durante i test, con l'ausilio di immagini che ne mostrano le relative interfacce grafiche.
Il terzo capitolo, invece, descrive tutti gli studi e le misurazioni effettuate per ottenere i risultati necessari per dare delle risposte ai quesiti che ci siamo posti.
Il quarto capitolo, infine, è quello conclusivo.

Capitolo 2

Strumenti utilizzati

2.1 WhatsApp Messenger

WhatsApp Messenger è un'applicazione di messaggistica mobile multi piattaforma che consente di scambiarsi messaggi coi propri contatti senza dover pagare gli SMS. WhatsApp Messenger è disponibile per iPhone, BlackBerry, Android, Windows Phone e Nokia. Tutti questi telefoni possono scambiarsi messaggi gli uni gli altri. Dato che ormai tutti coloro che posseggono uno smartphone hanno un piano tariffario flat, non vi sono costi aggiuntivi per mandare messaggi e restare in contatto coi propri amici, dal momento che WhatsApp Messenger si serve dello stesso piano dati Internet usato per le e-mail e la navigazione web, ed è sicuramente questo uno dei motivi per i quali questa applicazione ha ottenuto un così gran successo in poco tempo.

Oltre alla messaggistica di base, gli utenti di WhatsApp possono creare gruppi, scambiarsi messaggi illimitati, video e messaggi audio multimediali.

Nell'aprile 2014 è arrivato il via libera all'acquisizione di WhatsApp da parte di Facebook dalla Federal Trade Commission (Ftc), l'ente governativo americano per la protezione dei consumatori.

Figura 2.1: Interfaccia di WhatsApp

Servendosi della rete dati, WhatsApp messenger permette di inviare messaggi a qualsiasi altro utente connesso ad una rete, a patto che anch'esso sia in possesso dell'applicazione. Inoltre, l'invio di un messaggio avviene anche se il destinatario non ha l'applicazione online. Questa modalità di funzionamento ci fa pensare che possa esserci un server tra i due dispositivi, il quale avrà il compito di smistarlo al dispositivo di destinazione. In particolare, all'invio di un messaggio verranno effettuate le seguenti operazioni:

- Il messaggio arriva ad un server;
- Il server comunica al mittente l'avvenuta presa in consegna del messaggio;
- Il server inoltra il messaggio al destinatario;
- Il destinatario comunica al server l'avvenuta ricezione del messaggio;
- Il server comunica al mittente l'avvenuta ricezione del messaggio da parte del destinatario.

Quando il server riceve il messaggio, nel dispositivo mittente compare una spunta; quando il destinatario riceve il messaggio, al mittente compare la seconda spunta.

La Figura 2.2 illustra tale funzionamento.

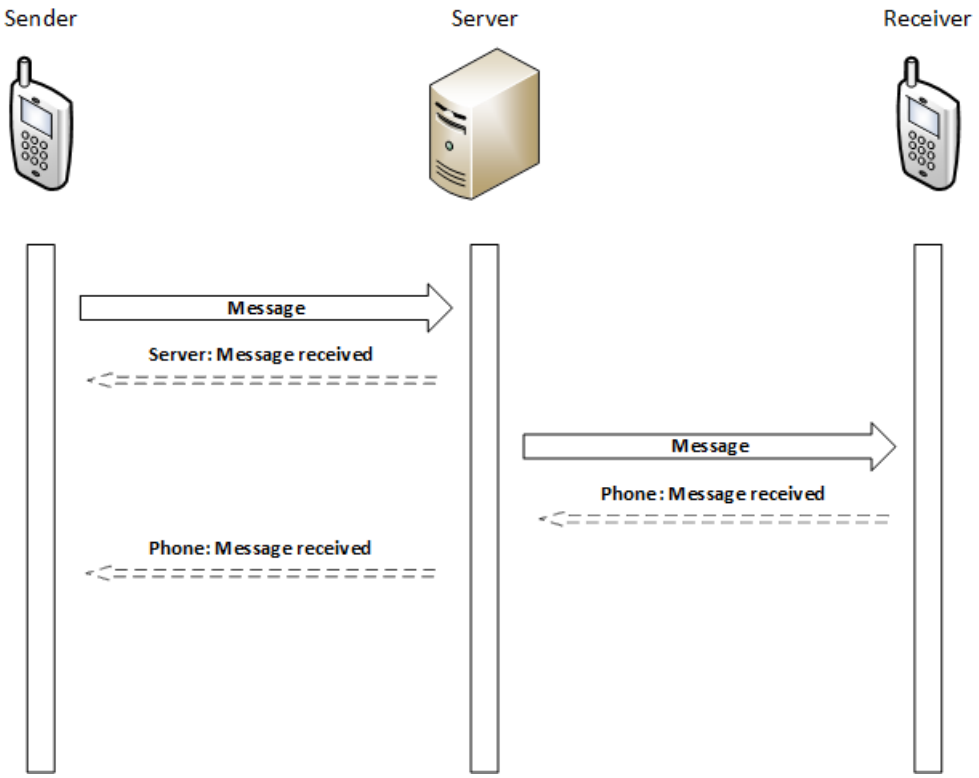

Figura 2.2: Funzionamento WhatsApp

2.2 Packet Sniffer e Analisi

Wireshark [5] è un analizzatore di rete. Consente di catturare direttamente i dati da una rete attiva oppure di analizzare file contenenti pacchetti precedentemente ottenuti. Inizialmente, il formato dei file catturati da Wireshark era il formato libpcap, che è il formato usato da tcpdump ed altri tools.

I pacchetti catturati sono conformi alla libreria pcap [6]. È possibile applicare filtri ai pacchetti ottenuti, selezionando, per esempio, solo quelli provenienti da un determinato IP sorgente. I filtri applicabili ai pacchetti seguono le regole della libreria pcap.

L'interfaccia grafica di Wireshark (Figura 2.3) mostra il numero di pacchetti catturati, il tempo trascorso tra la cattura dei pacchetti, l'indirizzo sorgente e quello di destinazione, il protocollo usato, la lunghezza del pacchetto ed altre informazioni.

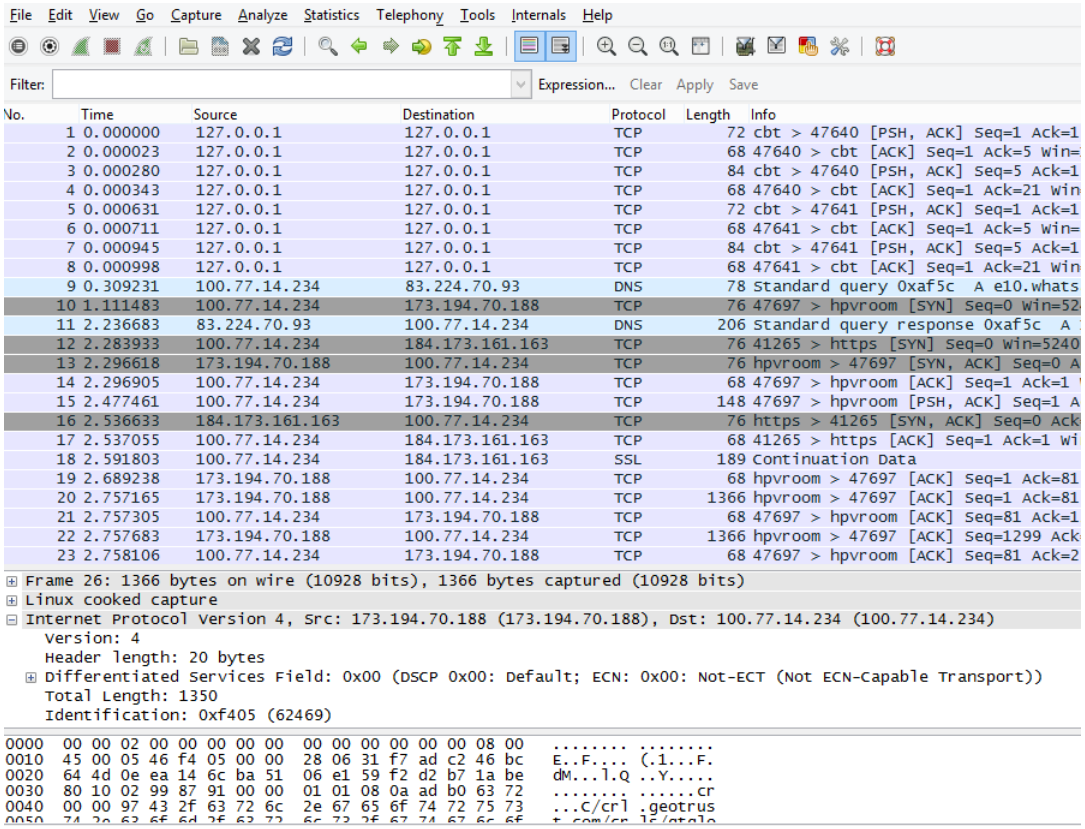

Figura 2.3: Interfaccia di Wireshark

Wireshark permette di analizzare e filtrare il traffico di rete dal PC. La stessa operazione può essere effettuata anche da un dispositivo mobile. Shark [7] è un "packet sniffer" del traffico di rete. Cattura tutti i pacchetti scambiati da un dispositivo sia utilizzando rete 3G sia utilizzando rete WiFi. Permette di impostare dei parametri che fungono da filtri durante la cattura e i risultati vengono salvati nella memoria dello smartphone (o nella microSD) in formato pcap. Con l'utilizzo dei filtri è possibile catturare e memorizzare solamente i pacchetti con una certa caratteristica, come, per esempio, uno stesso indirizzo IP destinatario.

La Figura 2.4 illustra l'interfaccia dell'applicazione durante la fase di "cattura".

Figura 2.4: Anteprima Shark - Running

2.3 Whois

Whois [8] è un servizio utilizzabile da shell di Ubuntu che permette di visualizzare informazioni riguardanti un determinato indirizzo IP. In particolare, applicando whois ad un indirizzo IP, vengono visualizzati il nome della rete, il range di indirizzi ai quali la rete fa riferimento, il luogo in cui si situa l'IP ricercato, l'organizzazione che lo gestisce ed altre informazioni di rete.

```
inetnum:        157.27.0.0 - 157.27.255.255
netname:        IVRUNIV-NET
org:            ORG-UDSD45-RIPE
descr:          Universit◆ degli Studi di Verona
country:        IT
admin-c:        GB6434-RIPE
tech-c:         AS9924-RIPE
status:         LEGACY
remarks:        For information on "status:" attribute read https://www.ripe.net/data-tools/
tus-values-legacy-resources
remarks:        This prefix is statically assigned
remarks:        To notify abuse mailto: cert@garr.it
remarks:        Centro di Informatica e Calcolo Automatico
remarks:        Universita' di Verona
remarks:        GARR - Italian academic and research network
mnt-irt:        IRT-GARR-CERT
mnt-by:         GARR-LIR
source:         RIPE # Filtered

organisation:   ORG-UDSD45-RIPE
org-name:       Universita' degli Studi di Verona
org-type:       OTHER
address:        Via S.Francesco, 22
address:        I - 37129 Verona (VR)
phone:          +39 045 8028713
fax-no:         +39 045 8028471
mnt-ref:        GARR-LIR
mnt-by:         GARR-LIR
abuse-c:        AG16225-RIPE
source:         RIPE # Filtered
```

Figura 2.5: Esempio Whois

2.4 Cloud Monitor

Cloud Monitor [9] è un'azienda che si occupa del monitoraggio delle prestazioni di siti ed applicazioni Web. Verifica le prestazioni di siti e server grazie a 95 stazioni di monitoraggio disposte in 48 paesi del mondo. Dato un indirizzo IP o un sito web, effettua, attraverso le 95 stazioni, ping verso quell'indirizzo registrando l'esito dello stesso e, in caso di ping eseguito con successo, RTT minimo, RTT medio ed RTT massimo (RTT - Round Trip Time, tempo impiegato da un pacchetto di dimensione trascurabile per viaggiare da un computer ad un altro e tornare indietro).

Esegui il ping su: www.google.com

Punto di controllo	Risultato	RTT minimo	RTT medio	RTT massimo	IP
Arabia Saudita - Riyadh (saruh01)	Unknown result from ping				2a00:1450:4009:808::1011
Argentina - Buenos Aires (arbue01)	Unknown result from ping				2800:3f0:4002:800::1014
Australia - Brisbane (aubne01)	Okay	19.3	19.4	19.6	2404:6800:4006:804::1014
Australia - Melbourne (aumel02)	Unknown result from ping				2404:6800:4006:803::1013
Australia - Perth (auper01)	Unknown result from ping				2404:6800:4006:806::1012
Australia - Sydney (ausyd02)	Packets lost (100%)				2404:6800:4006:803::1011
Austria - Vienna (atvie01)	Unknown result from ping				2a00:1450:4001:80e::1010
Belgio - Anversa (beanr02)	Unknown result from ping				2a00:1450:4005:809::1012
Brasile - Porto Alegre (brpoa01)	Unknown result from ping				2607:f8b0:4008:800::1013
Brasile - Rio de Janeiro (brrio01)	Unknown result from ping				2800:3f0:4004:800::1014
Brasile - San Paolo (brsao03)	Okay	139.9	142.4	143.5	2607:f8b0:4000:807::1012
Bulgaria - Sofia (bgsof01)	Unknown result from ping				2a00:1450:4001:c02::67
Canada - Calgary (cacal01)	Unknown result from ping				2607:f8b0:400a:803::1014
Canada - Montreal (camtr01)	Okay	26.1	27.5	30.5	2607:f8b0:4009:806::1011
Canada - Toronto (cator01)	Packets lost (100%)				2607:f8b0:400b:806::1012
Canada - Vancouver (cavan02)	Okay	25.7	25.8	25.9	2001:4860:400b:c01::68
Cina - Hong Kong (hkhkg01)	Okay	4.5	4.9	5.3	2404:6800:4005:806::1013

Figura 2.6: Esempio Cloud Monitor

Capitolo 3

Misurazioni

L'obiettivo di questo progetto è quello di scoprire informazioni riguardo WhatsApp e, in particolare, la modalità di scambio dei messaggi e il dislocamento dei server nel mondo. Per fare ciò, sono state fatte rilevazioni giornaliere per più di 30 giorni, con l'utilizzo degli strumenti citati nel capitolo precedente.

Attraverso Shark, ogni giorno sono state rilevate le informazioni contenute nei pacchetti scambiati tra 2 dispositivi durante l'invio e la ricezione di messaggi. Dopodiché, sono stati analizzati gli indirizzi IP di destinazione in modo da risalire agli indirizzi dei server di WhatsApp.

Dopo aver scartato gli indirizzi IP di servizi noti (e.g. Facebook, Google, Yahoo), è stato ottenuto un pool di indirizzi associabile all'applicazione studiata.

La Figura 3.1 mostra tutti gli indirizzi IP catturati giorno per giorno.

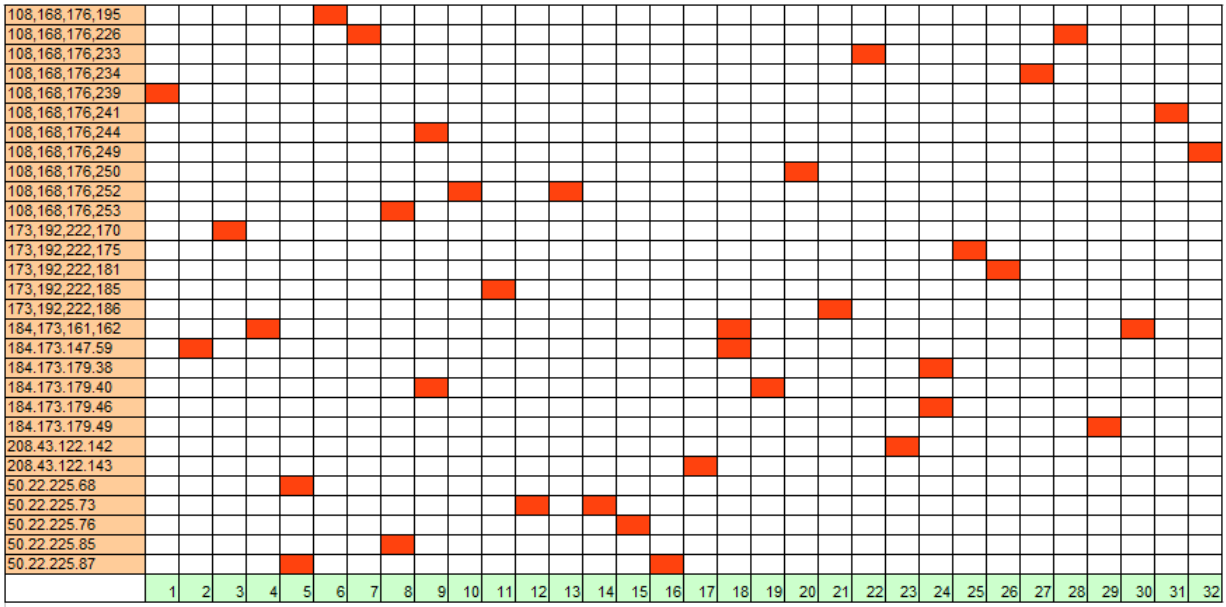

Figura 3.1: Rilevamenti. Il giorno 1 corrisponde al 25/04/2014

Ottenuto questo insieme di indirizzi IP, è stato utilizzato il servizio "Whois" di Ubuntu per controllare la provenienza di tutti gli indirizzi e l'azienda in possesso degli stessi. È emerso che, alla fine, tutti gli indirizzi trovati fanno parte di 5 range di indirizzi i quali appartengono a due aziende. Le aziende in questione sono la "SoftLayer" e la "ThePlanet". "SoftLayer" è una società del gruppo IBM, è stata fondata nel 2005 e ha sede a Dallas, Texas. L'azienda ha acquisito "ThePlanet" con sede a Houston, Texas. Possiamo quindi affermare che tutti gli indirizzi IP trovati appartengono alla stessa azienda, la "SoftLayer".

La Tabella 3.1 mostra i 5 range di indirizzi trovati e l'azienda che li gestisce.

Tabella 3.1: Range di IP collegati a WhatsApp

IP - range	**Company**	**Position**
108.168.128.0 - 108.168.255.255	SoftLayer Technologies Inc.	Dallas
173.192.0.0 - 173.193.255.255	SoftLayer Technologies Inc.	Dallas
184.172.0.0 - 184.173.255.255	ThePlanet.com Internet Services, Inc.	Houston
208.43.0.0 - 208.43.255.255	SoftLayer Technologies Inc.	Dallas
50.22.0.0 - 50.23.255.255	SoftLayer Technologies Inc.	Dallas

La Figura 3.2 rappresenta gli indirizzi IP catturati giorno per giorno, suddivisi nei 5 range di indirizzi trovati.

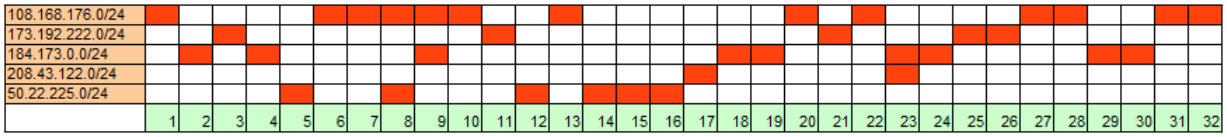

Figura 3.2: Rilevamenti. Il giorno 1 corrisponde al 25/04/2014

Gli IP trovati, dunque, sono stati associati ad aziende di Dallas e Houston. Per analizzare questo fatto e, soprattutto, per cercare di accertare tale posizione, è stato utilizzato il servizio di "Cloud Monitor", inserendo nel campo di ricerca un indirizzo IP appartenente ad ogni range e controllando l'RTT medio. Generalmente, se un terminale si trovasse in America, l'RTT medio proveniente da stati americani verso quel dispositivo sarebbe inferiore rispetto all'RTT medio proveniente da stati europei.

Attraverso il servizio di "Cloud Monitor", dunque, sono stati fatti questi test e le Tabelle 3.2 - 3.6 riportano i risultati ottenuti per un IP appartenente ad ogni range di indirizzi trovato.

Come si può notare in tutte le tabelle sotto elencate, l'RTT medio proveniente da server americani è inferiore rispetto ad altri server. Questa soluzione permette di confermare l'effettiva collocazione geografica degli indirizzi IP trovati.

Tabella 3.2: Cloud Monitoring - IP 108.168.176.252

Checkpoint	**RTT minimo**	**RTT medio**	**RTT massimo**
U.S.A. - Atlanta (usatl02)	14.958	15.028	15.089
U.S.A. - Charlotte (usclt01)	19.020	21.000	22.897
U.S.A. - Orlando (usorl01)	26.692	26.802	26.919
United Arab Emirates - Dubai (aedxb01)	210.377	214.806	223.568
India - New Delhi (inicd01)	307.221	314.655	324.349
Italy - Padova (itpda01)	182.594	182.884	183.131
U.S.A. - Miami (usmia01)	26.171	26.234	26.430
Russia - St. Petersburg (ruled01)	121.567	123.462	124.885
Sweden - Stockholm (sesto01)	107.762	108.445	109.035
South Africa - Durban (zadur01)	250.564	253.342	258.785

Tabella 3.3: Cloud Monitoring - IP 173.192.222.185

Checkpoint	**RTT minimo**	**RTT medio**	**RTT massimo**
U.S.A. - Atlanta (usatl02)	13.494	13.538	13.649
U.S.A. - Boston (usbos01)	12.680	12.741	12.833
U.S.A. - Chicago (uschi04)	24.325	24.528	24.900
China - Shanghai (cnsha02)	320.647	320.975	321.679
Germany - Berlin (deber01)	102.908	104.259	111.722
United Arab Emirates - Dubai (aedxb01)	200.551	204.575	215.826
Greece - Athens (grath01)	139.524	142.028	145.369
India - New Delhi (inicd01)	316.189	318.277	331.124
Israel - Kiryat-Matalon (ilktm01)	140.603	143.412	144.149
U.S.A. - Philadelphia (usphl01)	7.698	7.898	8.571

Tabella 3.4: Cloud Monitoring - IP 184.173.179.46

Checkpoint	**RTT minimo**	**RTT medio**	**RTT massimo**
U.S.A. - Ashburn (usabn06)	1.867	4.997	31.552
Canada - Montreal (camtr01)	15.638	18.000	26.510
U.S.A. - Philadelphia (usphl01)	7.763	7.867	8.016
Malaysia - Kuala Lumpur (mykul01)	249.499	250.963	254.803
South Korea - Seoul (krsel01)	209.901	239.262	268.693
South Africa - Cape Town (zacpt02)	224.220	224.339	224.573
Turkey - Istanbul (trist01)	164.054	168.212	184.680
U.S.A. - St. Louis (usstl01)	23.335	23.447	23.569
Singapore - Singapore (sgsin02)	235.687	236.045	236.759
Poland - Warsaw (plwrs01)	191.815	193.114	197.813

Tabella 3.5: Cloud Monitoring - IP 208.43.122.142

Checkpoint	**RTT minimo**	**RTT medio**	**RTT massimo**
U.S.A. - Ashburn (usabn06)	1.763	1.959	2.151
U.S.A. - Philadelphia (usphl01)	6.055	6.176	6.452
Singapore - Singapore (sgsin02)	234.976	236.185	242.457
Australia - Melbourne (aumel02)	242.088	242.273	242.494
Vietnam - Ho Chi Minh City (vnsgn01)	292.203	293.812	295.187
Italy - Rome (itrom01)	107.327	108.855	110.644
Norway - Oslo (noosl02)	102.496	105.621	129.432
Malaysia - Kuala Lumpur (mykul01)	257.579	259.167	262.955
U.S.A. - St. Louis (usstl01)	22.873	22.955	23.073
United Kingdom - Glasgow (gbglw01)	75.504	75.587	75.727

Tabella 3.6: Cloud Monitoring - IP 50.22.225.85

Checkpoint	**RTT minimo**	**RTT medio**	**RTT massimo**
U.S.A. - Atlanta (usatl02)	14.374	14.466	14.532
U.S.A. - Boston (usbos01)	13.064	13.098	13.132
U.S.A. - Ashburn (usabn06)	1.741	1.942	2.225
China - Hong Kong (hkhkg01)	224.032	224.907	226.799
Thailand - Bangkok (thbkk02)	277.834	277.929	278.014
Austria - Vienna (atvie01)	104.221	104.262	104.286
Hungary - Budapest (hubud01)	113.398	113.641	114.190
Czech Republic - Prague (czprg01)	95.966	96.028	96.099
Brazil - Sao Paulo (brsao03)	155.717	155.935	156.290
Spain - Madrid (esmad01)	125.545	128.065	132.618

Un altro test effettuato è stato quello di pre-filtrare i pacchetti che sarebbero stati rilevati dall'applicazione "Shark". In questo modo, l'applicazione ha catturato solo i pacchetti aventi come destinazione un indirizzo IP appartenente ad uno dei range scoperti in precedenza. Di conseguenza, la quantità di informazione catturata era limitata a quella che ci interessava. Durante la cattura, durata alcune ore, sono state ottenute altre importanti informazioni. Durante le ore, infatti, il dispositivo cellulare ha cambiato più volte rete (passando da WiFi a 3G e viceversa) e, in concomitanza con questi cambiamenti, sono cambiati anche gli indirizzi di destinazione. Questo fatto ci permette di affermare che uno smartphone comunica con un server (deciso al momento dell'inizio della connessione) e cambia con la modifica della rete utilizzata dal dispositivo.

La Figura 3.3 mostra il momento nel quale lo smartphone è uscito dalla rete WiFi ed è entrato nella rete 3G. In quel preciso istante, anche l'indirizzo IP di destinazione è cambiato.

No.	Time	Source	Destination	Protocol	Length	Info
1406	3046.238767	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4276 A
1408	3050.261149	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4276 A
1409	3051.150603	100.77.14.234	184.173.161.163	SSL	110	Continuation Data
1413	3081.486956	100.77.14.234	184.173.161.163	SSL	97	Continuation Data
1415	3082.021856	100.77.14.234	184.173.161.163	SSL	109	Continuation Data
1417	3082.601905	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4388 A
1418	3084.344220	100.77.14.234	184.173.161.163	SSL	80	Continuation Data
1420	3084.741780	100.77.14.234	184.173.161.163	SSL	94	Continuation Data
1422	3084.800040	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4426 A
1424	3085.261828	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4426 A
1425	3092.285513	100.77.14.234	184.173.161.163	SSL	134	Continuation Data
1427	3092.751316	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4492 A
1429	3099.138936	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4492 A
1430	3099.151895	100.77.14.234	184.173.161.163	SSL	113	Continuation Data
1432	3112.928983	100.77.14.234	184.173.161.163	SSL	80	Continuation Data
1434	3113.340008	100.77.14.234	184.173.161.163	TCP	68	41265 > https [ACK] Seq=4549 A
1450	3286.552928	100.82.40.187	208.43.122.143	TCP	76	44644 > xmpp-client [SYN] Seq=
1457	3286.806023	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1465	3287.079500	100.82.40.187	208.43.122.143	TCP	189	[TCP segment of a reassembled
1469	3287.446343	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1470	3287.454240	100.82.40.187	208.43.122.143	TCP	97	[TCP segment of a reassembled
1472	3287.517178	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1481	3287.776160	100.82.40.187	208.43.122.143	TCP	91	[TCP segment of a reassembled
1484	3288.527243	100.82.40.187	208.43.122.143	TCP	91	[TCP Retransmission] [TCP segm
1487	3290.047346	100.82.40.187	208.43.122.143	TCP	91	[TCP Retransmission] [TCP segm
1490	3290.366193	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1541	3306.299460	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1543	3311.794252	100.82.40.187	208.43.122.143	TCP	80	[TCP Dup ACK 1541#1] 44644 > x
1544	3312.389573	100.82.40.187	208.43.122.143	TCP	110	[TCP segment of a reassembled
1589	3330.206576	100.82.40.187	208.43.122.143	TCP	97	[TCP segment of a reassembled
1591	3330.696875	100.82.40.187	208.43.122.143	TCP	108	[TCP segment of a reassembled
1593	3331.286536	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1594	3333.149566	100.82.40.187	208.43.122.143	TCP	80	[TCP segment of a reassembled
1596	3333.556821	100.82.40.187	208.43.122.143	TCP	93	[TCP segment of a reassembled
1599	3333.599565	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=
1601	3334.372403	100.82.40.187	208.43.122.143	TCP	68	44644 > xmpp-client [ACK] Seq=

Figura 3.3: Cambiamento rete e cambiamento IP

Come ultimo test effettuato, abbiamo cercato di capire se la Figura 2.2 rispecchiasse il corretto funzionamento dell'applicazione. Tale figura mostra come due dispositivi si scambiano messaggi passando attraverso un server comune. Il controllo effettuato si è basato sull'utilizzo contemporaneo di "Shark" da parte di due dispositivi per catturare i pacchetti scambiati tra di essi. Facendo così, si è potuto controllare l'indirizzo IP di destinazione di entrambi gli smartphone. Se gli IP fossero stati uguali, allora si poteva affermare che, quando due dispositivi comunicano tra di loro, si connettono allo stesso server. In realtà, gli IP di destinazione erano differenti. Questo ci indica con certezza che durante la comunicazione tra più dispositivi, ogni dispositivo si connette ad un proprio server e poi saranno i relativi server a comunicare tra di loro prima di recapitare il messaggio al terminale di competenza.

La Figura 3.4 mostra il funzionamento corretto di WhatsApp.

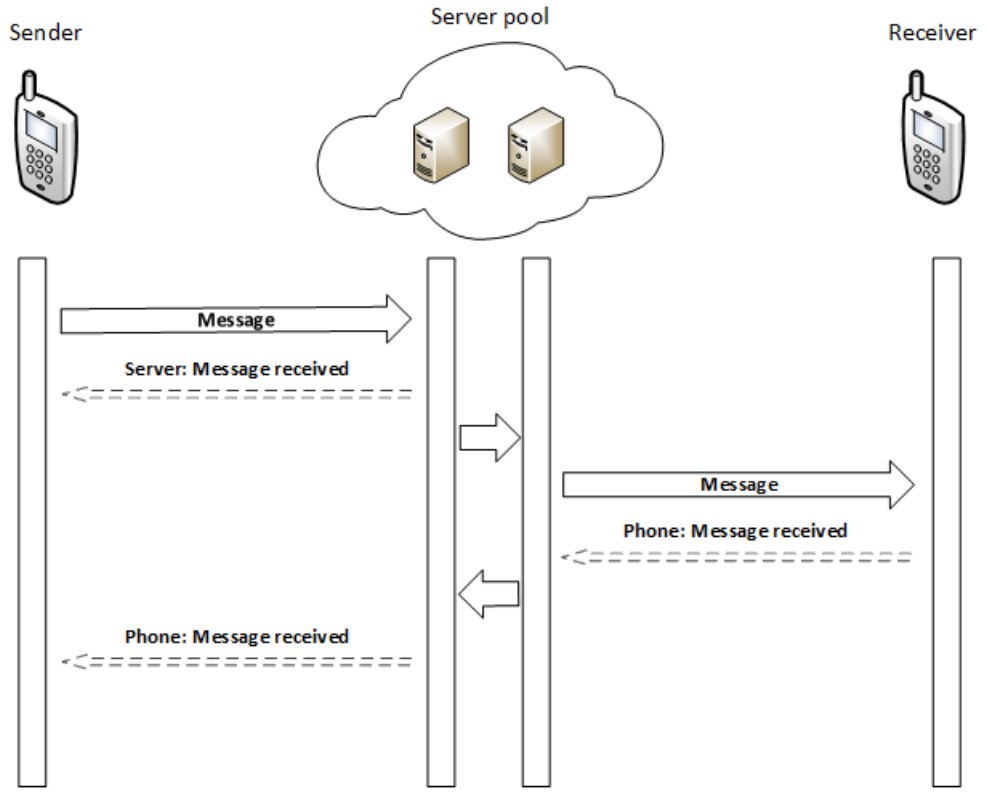

Figura 3.4: Funzionamento corretto di WhatsApp

Capitolo 4

Conclusioni

L'obiettivo della tesi era quello di dimostrare il funzionamento dell'applicazione di messaggistica "WhatsApp" cercando, anche, di trovare la dislocazione dei server nel territorio mondiale.
Per fare ciò, ci siamo serviti di alcuni tools, quali Shark, Wireshark, Whois e CloudMonitor.

Dopo aver effettuato rilevazioni giornaliere per più di 30 giorni (servendoci del tool Shark), sono stati analizzati gli indirizzi IP dei server con i quali lo smartphone ha comunicato durante l'invio dei messaggi ed abbiamo constatato che tutti gli indirizzi appartengono ad un'unica azienda, la SoftLayer Technologies Inc. di Dallas.
Utilizzando il servizio di CloudMonitor sugli indirizzi IP trovati, abbiamo affermato che i server si trovano nel territorio americano.
Abbiamo provato, inoltre, ad analizzare il traffico di rete durante la modifica della rete utilizzata dallo smartphone per comunicare (uscendo da WiFi ed entrando nella rete cellulare e viceversa), ed è stato notato che, nel momento in cui lo smartphone esce da una rete ed entra in un'altra, anche l'indirizzo IP al quale ci si connette cambia. Possiamo quindi affermare che un dispositivo comunica con un server "deciso" al momento dell'ingresso in una rete e cambia nel momento in cui la rete cambia.
Infine, abbiamo fatto comunicare due dispositivi con Shark attivo su entrambi. In questo modo abbiamo visto che l'indirizzo IP con il quale comunicavano i due dispositivi era diverso. Possiamo, perciò, affermare che quando due smartphone comunicano, non si connettono ad un server comune ma a due server differenti e saranno poi tali server a comunicare tra di loro.

Bibliografia

[1] *http://www.whatsapp.com*

[2] *http://www.wechat.com*

[3] *https://telegram.org*

[4] *http://www.viber.com*

[5] *http://www.wireshark.org*

[6] *http://www.winpcap.org/ntar/draft/PCAP-DumpFileFormat.html*

[7] *https://play.google.com/store/apps/details?id=lv.n3o.shark*

[8] *http://packages.ubuntu.com/precise/whois*

[9] *http://cloudmonitor.ca.com/it/ping.php*