DIGITAL FORENSICS

SOCIAL NETWORK FORENSICS

CANDIDATO: **ANIELLO GIUGLIANO**

MATRICOLA: **0522500620**

DOCENTE: **R.PIZZOLANTE**

Indice

- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

- **Introduzione alla presentazione**
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Abstract

I **Social Network** hanno cambiato il modo in cui interagiamo nella nostra vita personale, il nostro modo di conoscere e presentarci agli altri, generando un mondo parallelo al mondo reale. Anche nella vita professionale stanno acquistando sempre maggior spazio, permettendo infatti alle aziende di incrementare i servizi, mantenere e rafforzare le relazioni, svolgere iniziative di marketing e generare nuovi contatti. Con centinaia di milioni di utenti ogni giorno, i Social Network hanno attratto "attaccanti" più di ogni altro obiettivo negli ultimi anni. La presentazione che ho fatto,ha come scopo principale quello di capire,come la Digital Forensics si è evoluta nel tempo per adattarsi al Web 2.0.

Obiettivo

L'obiettivo principale di questa presentazione,è quello di fare una trattazione approfondita sulla **Social Network Forensics**. Verrà prima data una panoramica generale su cosa sono i Social Network e come si sono evoluti nel tempo.Poi vedremo quali sono i principali attacchi possibili contro un SN e contro gli utenti che utilizzano i SN. Dopodichè introdurremo la SNF,ne approfondiremo le principali caratteristiche ,vedremo due Conceptual Framework,ed infine analizzeremo meglio alcuni tool che vengono usati nella pratica.

- Introduzione alla presentazione
- **Introduzione ai Social Network**
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Cos'è un Social Network?

Una **Rete Sociale**,anche nota come **Social Network** , consiste in un qualsiasi gruppo di individui connessi tra loro da diversi legami sociali. Per gli esseri umani i legami vanno dalla conoscenza casuale, ai rapporti di lavoro, ai vincoli familiari. –**Wikipedia**

Un **Social Media** (la versione di Internet di un Social Network) è una forma di comunicazione elettronica (come siti web e blog) attraverso il quale gli utenti creano comunità online per condividere informazioni, idee, messaggi personali, e altri contenuti (come video,foto, ecc.) –**Merriam Webster Dictionary**

Un **Social Media** è un sito web interattivo progettato per creare una comunità online per individui che hanno qualcosa in comune (un interesse per un hobby, un argomento) o organizzazioni - ed un semplice desiderio di comunicare oltre i confini fisici(geografici)con altre persone interessate

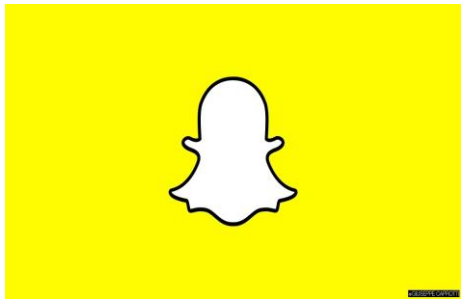
Storia dei Social Network

- **Dipinti dei cavernicoli della preistoria** : Primo esempio di comunicazione ed interazione reciproca usato dall'uomo
- **Telegrafo** (1873)
- **Telefono** (1876)
- **Radio** (1896)
- **Usenet**(1979): Bacheca che collegava la Duke University e la Nord Carolina University
- **SixDegrees.com** (1997): Primo Social Network del Web , aveva l'obbiettivo di combinare incontri amorosi
- **Linkedin,MySpace,Flickr**(2003)
- **YouTube,Yahoo**(2005)
- **Facebook,Twitter** (2006)

E tantissimi altri negli ultimi anni.


1


YouTube

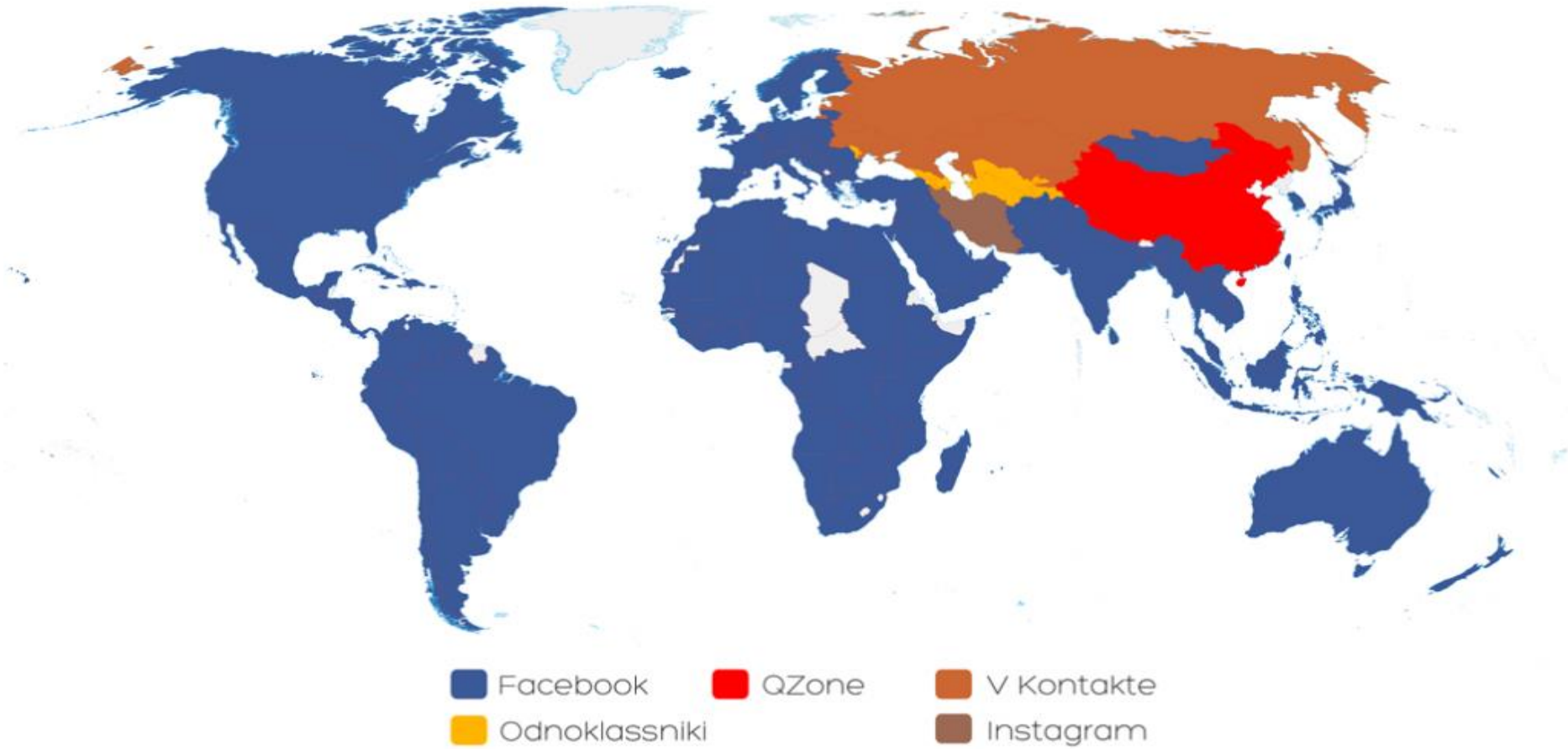



Pinterest


WeChat

WORLD MAP OF SOCIAL NETWORKS

January 2018

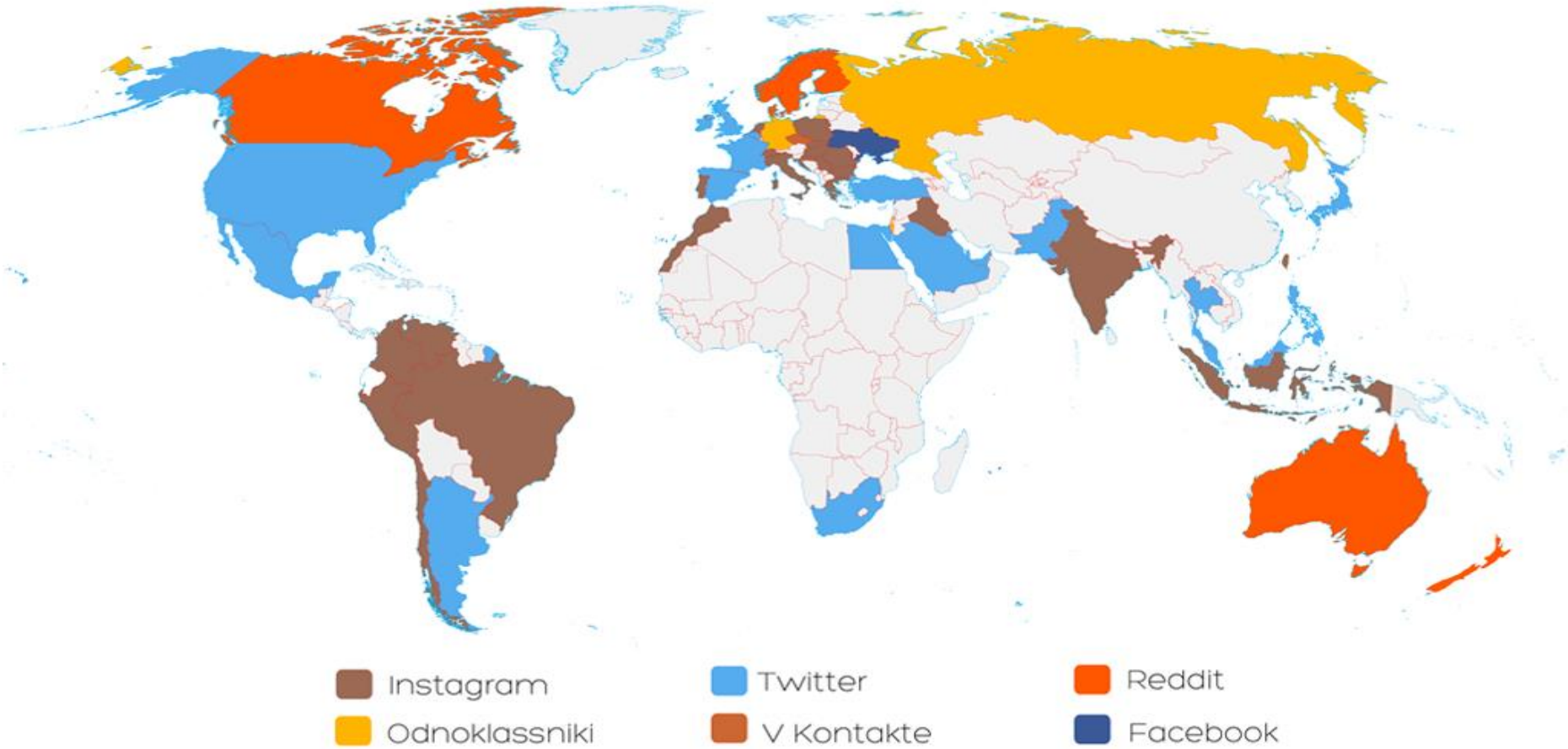


credits: Vincenzo Cosenza vincos.it

source: Alexa/SimilarWeb

WORLD MAP OF SOCIAL NETWORKS

Ranked 2nd - January 2018



credits: Vincenzo Cosenza vincos.it

source: SimilarWeb/Alexa

Classificazione dei Social Network

Esistono vari modi per classificare un Social Network:

- **Dominio**: *Locale* o *Globale*. I Social Network in base ai concetti e agli obiettivi potrebbero essere disponibili in tutto il mondo o solo in alcuni luoghi geografici specifici, ad es. all'interno di una città o persino una società.
- **Disponibilità:** *Privato* o *Publico* . Il livello di disponibilità per un determinato SN dipende da più criteri come l'obiettivo ed il tipo di applicazioni. Per esempio, è ovvio che un SN all'interno di una società dovrebbe essere accessibile solo dal suo personale e non da altri.

Classificazione dei Social Network

- **Scopo :** *Single Purpose* o *Multi Purposes*. La maggior parte dei SN è multiuso ,gli utenti possono fare tutto ciò che vogliono, dalla pubblicazione di immagini e video all'organizzazione incontri e anche conversazioni scientifiche. In genere, tali SN hanno gruppi di utenti diversi; tuttavia,ci sono SN che hanno scopi specifici e richiamano solo determinati tipi di utenti.
- **Accessibilità**: *Aperta* o *Ristretta*. In base al contenuto e al tema, i SN potrebbero essere limitati per l'uso solo, ad esempio, agli adulti. Certo, a differenza di altre classi, verificare i requisiti degli utenti dichiarati in questa categoria è più difficile e costoso. In tali SN, alcuni meccanismi di autorizzazione come l'identità univoca degli utenti sono necessari.

Classificazione dei Social Network

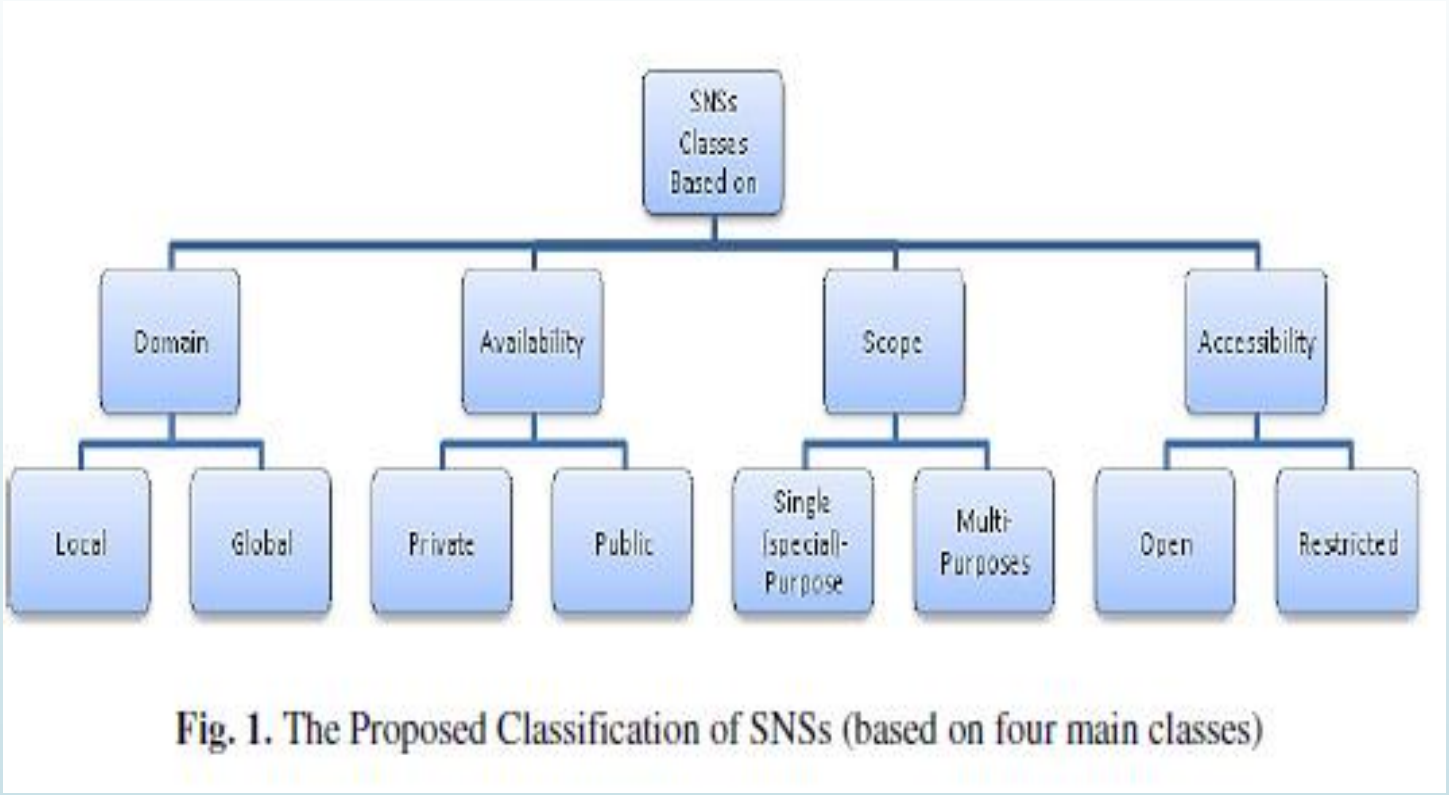


Fig. 1. The Proposed Classification of SNSs (based on four main classes)

- Introduzione alla presentazione
- Introduzione ai Social Network
- **Attacchi ad un Social Network**
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Attacchi ad un Social Network

Poiché i SN sono utilizzati da molti utenti in posizioni e luoghi diversi, i loro rischi e minacce hanno diversi aspetti. Il più delle volte, la privacy e le informazioni personali degli utenti sono bersaglio di attacchi. A volte, in base ai ruoli e alla posizione degli utenti all'interno di un'organizzazione o società, saranno attaccati per quello che sanno o per quello a cui hanno accesso. Questi tipi di attacchi di solito sono finalizzati allo spionaggio aziendale, minaccia alla sicurezza nazionale, ecc.

Attacchi ad un Social Network

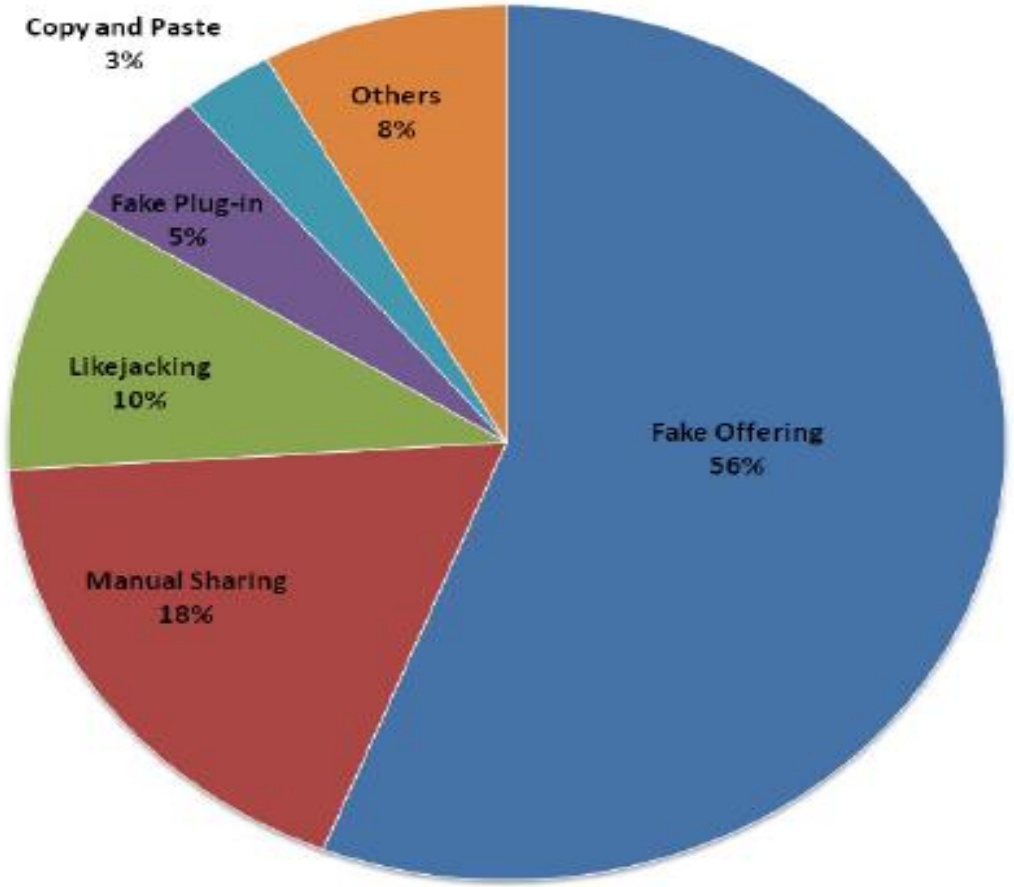
I principali tipi di attacco che si verificano ad un Social Network sono :

- **Fake Offering**:Sono truffe che invitano gli utenti dei SN a partecipare ad un evento o gruppo falso attraverso degli incentivi come buoni regalo gratuiti. La partecipazione spesso richiede all'utente di condividere le credenziali con l'attaccante o inviare un SMS a un numero di tariffa premium.
- **Manual Sharing Scams**: Gli utenti stessi condividono l'offerta falsa,con la promessa di benefici
- **Likejacking**: Utilizzando falsi pulsanti "Mi piace", gli aggressori inducono gli utenti ad andare su siti Web falsi che installano malware.

Attacchi ad un Social Network

- **Fake Plug-in Scams :** Gli utenti sono indotti a scaricare estensioni del browser false sulle loro macchine. Queste estensioni non autorizzate possono sembrare legittime ma una volta installate rubano le informazioni sensibili dalla macchina infetta.
- **Copy and Paste Scam**: Copia ed incolla di codice Java Script malevolo all'interno del browser web della vittima.

Attacchi ad un Social Network



- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- **Attacchi agli Utenti**
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Attacchi agli Utenti

La letteratura e la comunità di Sicurezza Informatica ,hanno proposto diversi elenchi e classi per le minacce ed i rischi dei SN da diverse prospettive .Dal punto di vista degli utenti classifichiamo le minacce come segue :

- **Propagazione**: Basati su cosa gli attaccanti vogliono ottenere dagli utenti
- **Infiltrazione**: Basati sulla posizione degli utenti
- **Divulgazione**: Basati su cosa gli utenti possiedono

Propagazione

La propagazione sfrutta le connessioni degli utenti attraverso la loro rete di contatti. Gli obbiettivi di questa attività sono:

- **Marketing e pubblicità** : Lo spamming viene utilizzato come tentativo a basso costo (e solitamente efficace) per il marketing virale e potrebbe anche essere considerato uno strumento per la diffusione di messaggi organizzati attraverso la popolazione.
- **Context-aware Spamming:** offre agli spammer una percentuale di clic elevata sfruttando il contesto condiviso tra amici sui SN. Questa classe di spamming è molto mirata, e trae vantaggio dalla fiducia degli utenti collegati all'interno degli SN.

Propagazione

- **Broadcast Spamming :** non ha obiettivi specifici, ma piuttosto abusa dei meccanismi di interazione pubblica per la diffusione di informazione (quanto piu possibile). Un'altra forma di abuso è la diffusione (organizzata) di voci. Questo azione è una cosa normale nella vita quotidiana della maggior parte delle persone e trae beneficio dal potere della word-ofmouth delle comunità sociali (umane). Tuttavia, quando la si utilizza per scopi organizzati , potrebbe influenzare la società, gli affari e persino la politica (es diffamando un politico , generando il focolaio di un disastro e plasmando il pensiero pubblico)

Propagazione

- **Tiny URL:** Gli URL abbreviati sono fenomeni di SN, in modo specifico Twitter, che oltre ai loro benefici, potrebbe essere usati come uno strumento per ingannare utenti che visitano siti dannosi. Possono estrarre informazioni personali (e aziendali), in particolare se vi si accede tramite un computer sul posto di lavoro. In altre parole, si nasconde il vero link ai siti web. Twitter è particolarmente vulnerabile a questo metodo perché è molto facile ritwittare un post in modo che alla fine possa essere visto da centinaia di migliaia di persone. La decodifica di tali link prima di fare clic dovrebbe essere la prima azione da eseguire.

Infiltrazione

In base alla posizione degli utenti all'interno di un organizzazione, essi hanno accesso ad informazioni sensibili che potrebbero essere molto preziose o addirittura critiche in alcuni contesti.

- **Perdita di informazioni sensibili**
- **Spionaggio Aziendale**

Infiltrazione

Durante un monitoraggio della durata di sei mesi di 20 aziende tramite un social media attivo di ricercatori Cyberoam, è stata trovata perdita di informazione da parte di tutte loro. Naturalmente, la gravità dei meccanismi di sicurezza dipende direttamente dal grado di sensibilità delle informazioni perse. Per **mitigare** il problema le aziende creano delle policy riguardanti l'uso dei Social Network all'interno del contesto aziendale.

Divulgazione

Obbiettivo degli attacchi è rappresentato dalle risorse correlate alla privacy degli utenti ed alle loro informazioni (sensibili) private :

- **Password private**
- **Informazioni Sensibili**

Tali informazioni possono essere utilizzate per scopi molteplici:

- **Truffa**
- **Spamming Mirato**
- **Estorsione**
- **Ricatto**
- **Diffamazione**

- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- **Introduzione alla Social Network Forensics**
- Conceptual Framework
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Social Network Forensics

L'uso di metodi scientificamente comprovati per la conservazione, la raccolta, validazione, identificazione, analisi, interpretazione, documentazione e presentazione di prove digitali derivate da fonti digitali per agevolare o promuovere la ricostruzione di eventi ritenuti criminali o contribuire ad anticipare azioni non autorizzate dimostrate dirompenti per le operazioni pianificate – **Definizione di Digital Forensics**

Il **Social Network Forensics** è la Digital Forensics applicata al Web 2.0 ,nel quale gli utenti utilizzano i Social maggiormente.

Social Network Forensics

Applicazione di tecniche informatiche di indagine,raccolta ed analisi dei dati dai vari Social Network e successiva memorizzazione di queste informazioni con lo scopo di portarle in tribunale come prove.

Scopi della SNF

Alcuni degli obbiettivi principali della SNF sono:

- Dimostrare se una persona è vittima di minacce(cyber-bullismo,ecc.)
- Stabilire se un sogetto è associato ad una persona di interesse
- Rilevamento di elementi di prova dai post di una persona di interesse
- Rintracciare utenti che pubblicano contenuti offensivi
- Scoprire reti terroristiche o criminali
- Anticipare crimini organizzati

Scopi della SNF

Naturalmente la maggior parte delle volte, l'analisi SNF viene eseguita da settori privati , agenzie di intelligence e autorità legali. Poiché il contenuto dei SN è direttamente (o indirettamente) correlato a persone fisiche ed entità giuridiche è necessaria un'autorizzazione legale per poterli controllare, rintracciare e monitorare. Inoltre, poiché i social network sono molto dinamici (in continua evoluzione) e la quantità di dati è piuttosto grande, l'acquisizione dei dati per l'analisi forense è una challange aperta. Nonostante i suoi molti benefici, SNF è costoso e relativamente difficile da eseguire. A causa di tutto questo, le esperienze pratiche di utilizzo di SNF sono legate alle autorità legali - in particolare agenzie di polizia e di intelligence.

SNF vs CF

Il **primo** e **principale** aspetto per differenziare la CF da SNF sono i dati che vengono collezionati per fare l'indagine. Come notato nella ***Tabella 1***, a causa delle caratteristiche specifiche dei dataset, il processo di collezione dei dati è molto diverso. I dati dei SN, a causa della loro natura dinamica e del grande numero di utenti che interagiscono al loro interno, sono in continua crescita sia in termini di dimensioni (quantità) che di dominio (interconnessioni). Pertanto, l'elaborazione di tali insiemi di dati è una sfida piuttosto difficile,rispetto all'acquisizione dei dati da un dispositivo digitale,che è un processo statico e di solito semplice.

SNF vs CF

Il **secondo** aspetto importante della differenza tra CF e SNF, che è in stretta relazione con il contesto (set di dati), è la qualità dell'attività di elaborazione dei dati. Inutile dire che, più complesso è il contesto, più difficile sarà l'operazione di implementazione. Come descritto nella ***tabella 2***, a causa del complicato compito di elaborazione di SNF, nel complesso **il costo** (compreso il tempo, la complessità e l'utilizzo delle risorse) è generalmente superiore a CF. Inoltre, a causa dei numerosi problemi con l'acquisizione dei dati dai SN ed all'applicazione di algoritmi appropriati, il **livello di accuratezza** per tali metodi è inferiore a compiti simili nel CF.

SNF vs CF

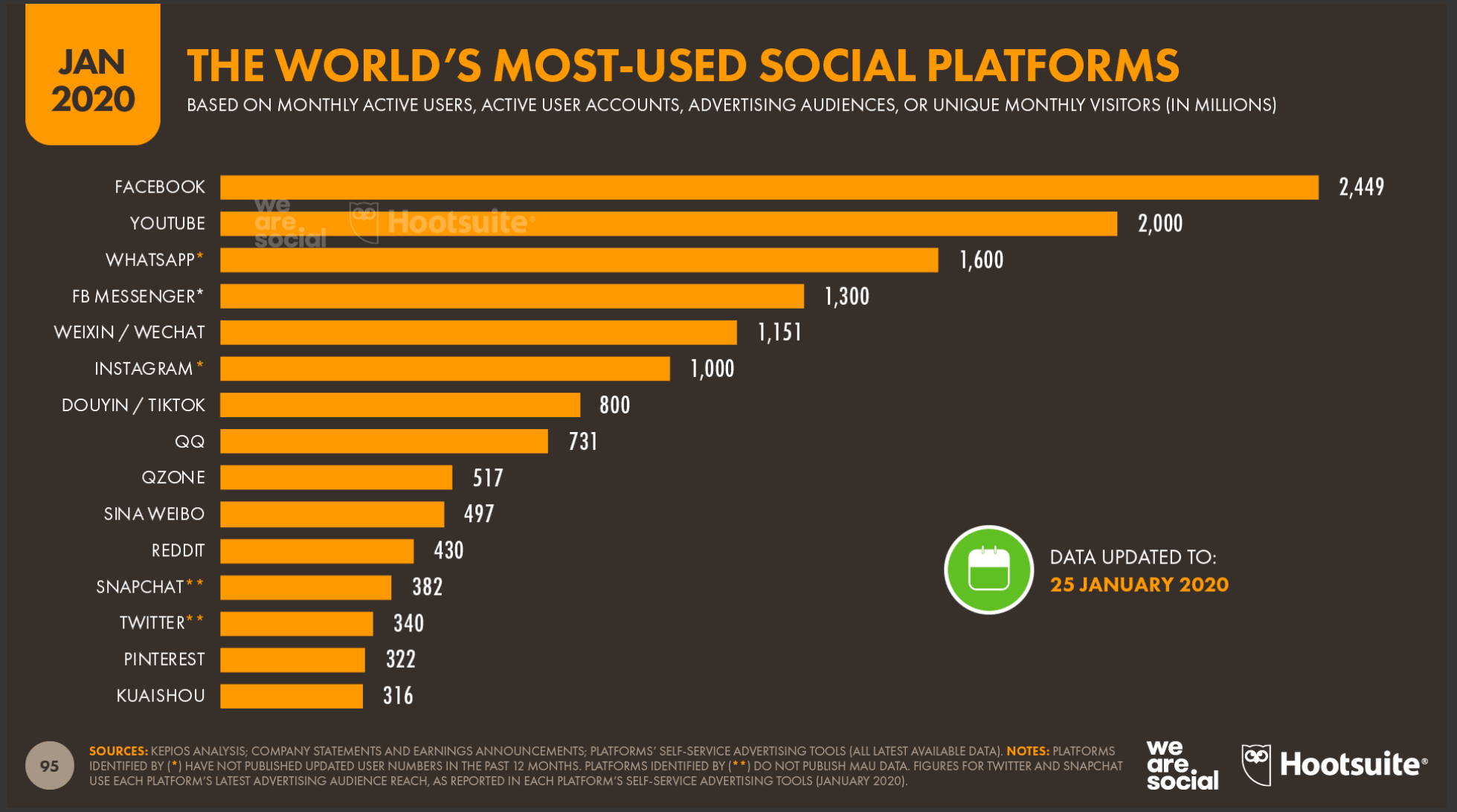
Table 1. Comparing SNF and CF based on type of data

Measure 1 : Type of Data	Computer Forensics (CF)	Social Network Forensics (SNF)
Context (scope)	Digital devices (limited)	SNSs (widespread and interconnected)
Nature of data	(usually) Static	(most often) Dynamic
Complexity	(depending on the situation) Low to high	(based on the underlying structure) High
Data quantity	(depending on the situation) Small to large	(based on the underlying structure) Large and increasing

Table 2. Comparing SNF and CF based on quality of operation

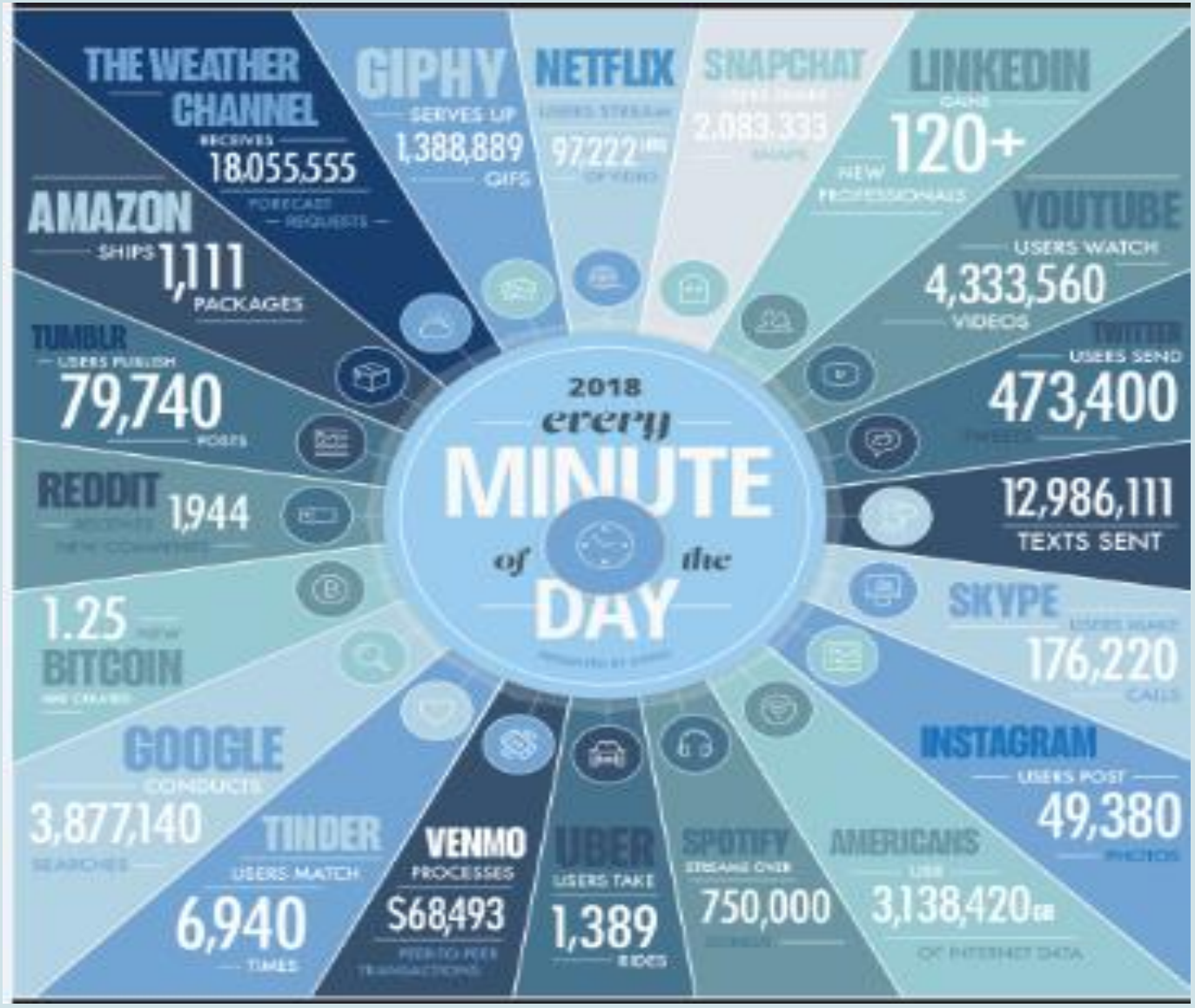
Measure 2 : Operation	Computer Forensics (CF)	Social Network Forensics (SNF)
Data acquisition	(depending on the situation) Easy to hard	(most often) Hard and challenging
Executability	(depending on the situation) Easy to hard	(most often) Hard
Accuracy	More precise	(currently) less precise
Cost	(depending on the situation) Low to high	(most often) High

Numero di Utenti nei SN



https://wearesocial.com/us/blog/

Volume di Dati generati dai SN



https://www.domo.com/learn/data-never-sleeps-6

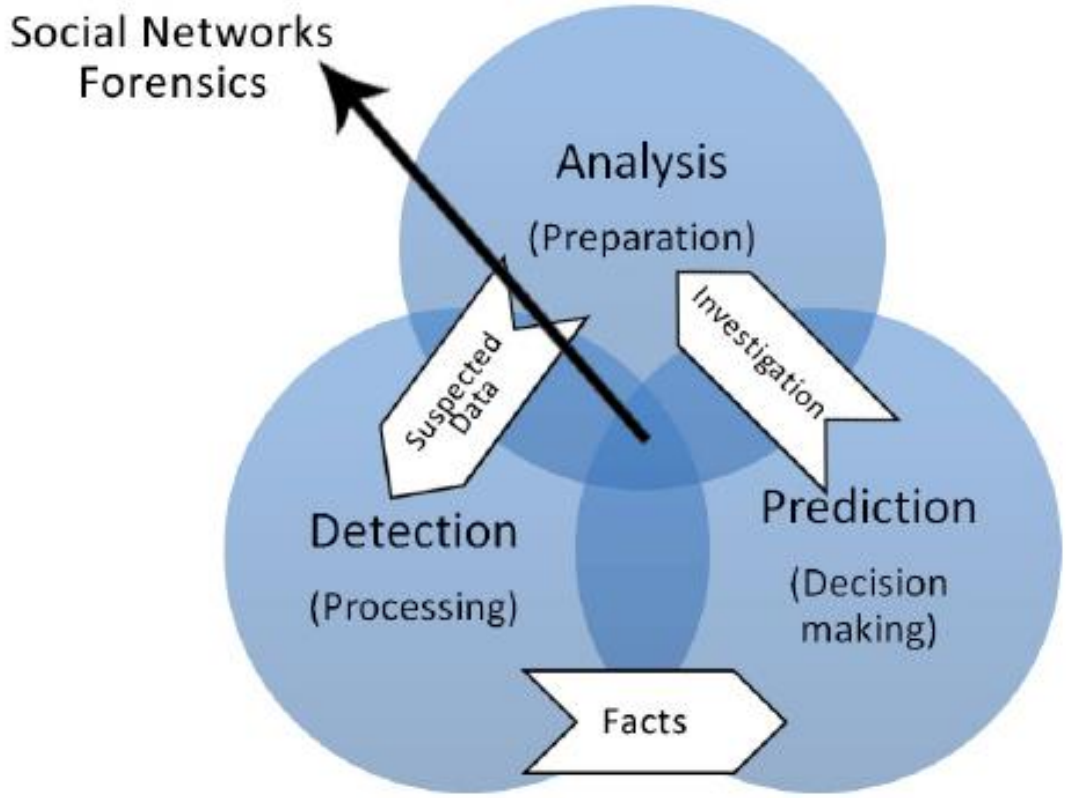
Approccio al SNF

Poiché SNF è un nuovo argomento, non ci sono molti lavori al riguardo.Sulla base di diverse ricerche svolte in questo ambito, noi classifichiamo gli approcci SNF in tre classi come segue:

- **Analysis**: in questa fase, il SN sarà sogetto dell'analisi per differenti scopi,come il monitoraggio e detenzione di anomalie
- **Detection**: Si cerca di trovare anomalie,attività criminali ecc.
- **Prediction**: Si cerca di predire crimini futuri ed attività illegali non ancora avvenute

Queste tre classi,non hanno confini solidi di separazione,e si sovrappongono le une alle altre.

Approccio al SNF



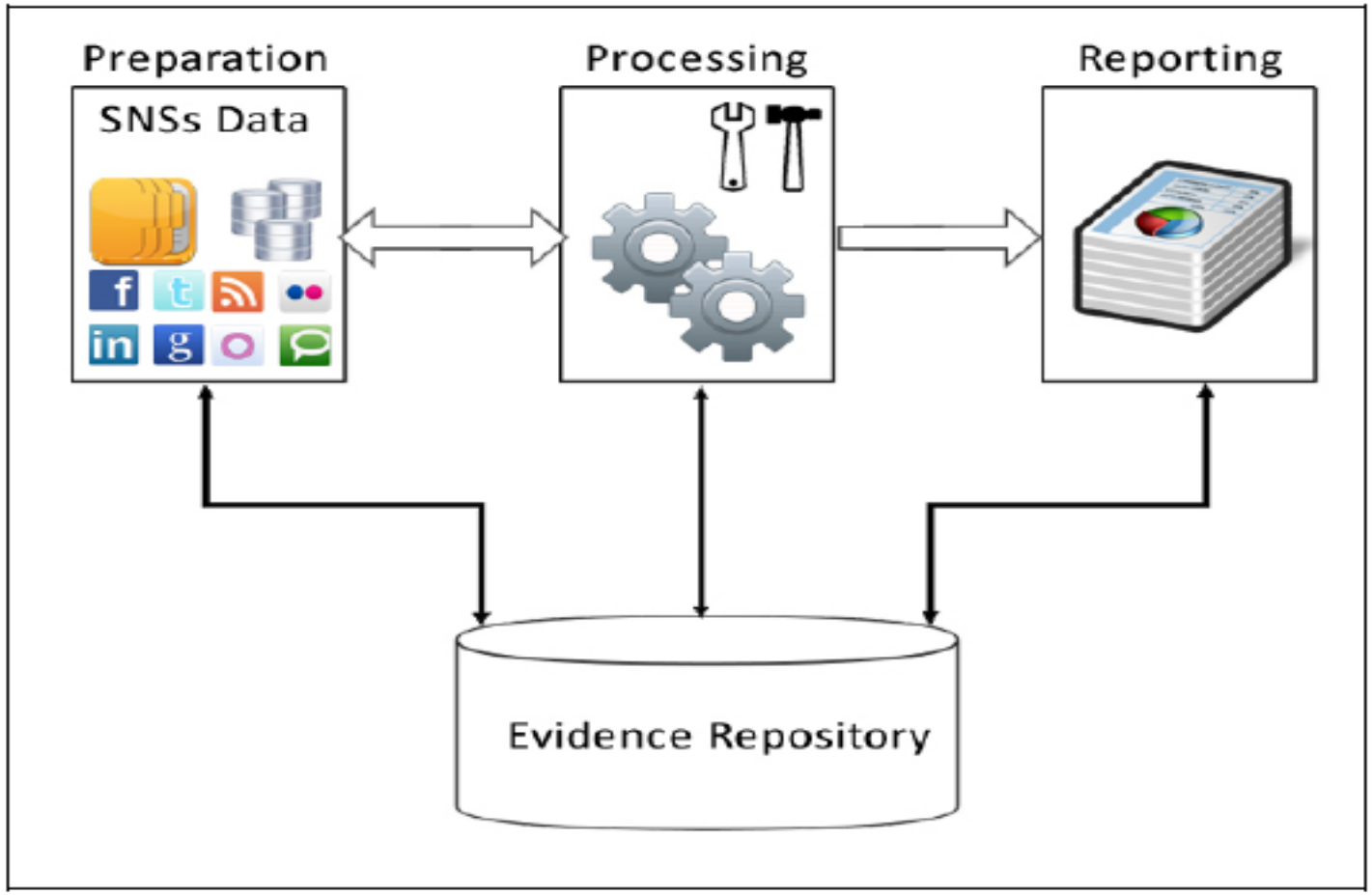
- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- **Conceptual Framework**
- Cloud Based Forensics Framework
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Conceptual Framework

Il ***framework*** proposto è composto da tre fasi principali:

- **Preparation**:Preparazione dei dati
- **Processing**: analysis,detection e prediction
- **Reporting**:generare i risultati trovati

Conceptual Framework



Preparation

La prima fase rappresenta un passo importante verso una procedura SNF di successo. Poiché questo passaggio riguarda i dati (set), ha due compiti essenziali:

- **Definizione dell'ambito**: si seleziona l'ambito a cui il processo si dovrebbe applicare,si specificano le delimitazioni dei processi e si selezionano gli algoritmi che devono essere usati.
- **Acquisizione dei dati**: la parte piu importante e difficile da implementare.Qualsiasi carenza all'interno di questa fase,influisce sui risultati e sul processo in generale.

Reporting

Generazione dei risultati ottenuti dalle fasi precedenti.

Tali risultati verranno utilizzati per prendere decisioni o verranno mostrati alle autorità legali.Esistono diverse attività principali all'interno di questa fase e sono:

- **Classificazione dei risultati**: Vengono organizzati i risultati ottenuti,per poterli processare successivamente(es. Confronto o Analisi)
- **Visualizzazione dei fatti**: Vengono rappresentati i fatti in modo facile da usare, cercando di scorpire nuove conoscenze nascoste
- **Documentazione della procedura**: questa fase aiuta gli altri(analisti,investigatori,ricercatori) a conoscere i dettagli tecnici

- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- **Cloud Based Forensics Framework**
- Problemi della Social Network Forensics
- Tool utilizzati per la SNF

Cloud Based Forensics Framework

Il framework consiste di 5 layer :

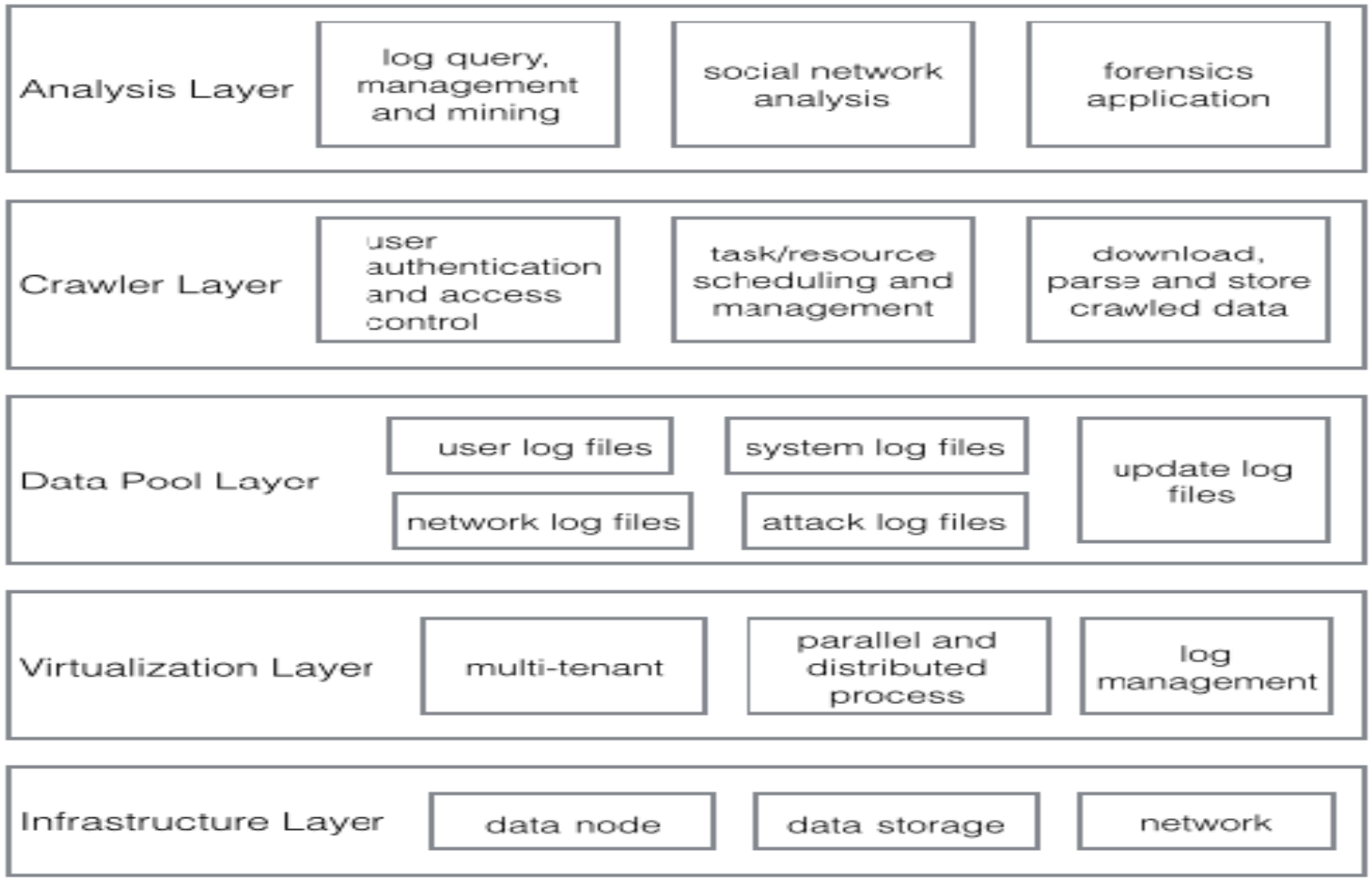
1. **Infrastructure Layer**: include l'infrastruttura sottostante,ed in particolare utilizziamo Hadoop come base di infrastruttura, che fornisce servizi di archiviazione, elaborazione e rete per i livelli superiori
2. **Virtualization layer:** consente la separazione e la condivisione dei dati,rappresenta un processo parallelo e distribuito, che fornisce servizi multi-thread, cache distribuita e funzionalità su larga scala
3. **Data pool layer**: archivia i dati separatamente, inclusi file di registro utente, file di registro di sistema, file di registro di rete, file di registro degli attacchi e file di registro degli aggiornamenti

Cloud Based Forensics Framework

4. Crawler layer : è il livello più importante nel framework. Questo livello è responsabile della raccolta dei dati sui social network. Comprende tre componenti principali: autenticazione dell'utente e controllo degli accessi, pianificazione e gestione delle attività e delle risorse, ed infine download, analisi ed archiviazione dei dati sottoposti a scansione.

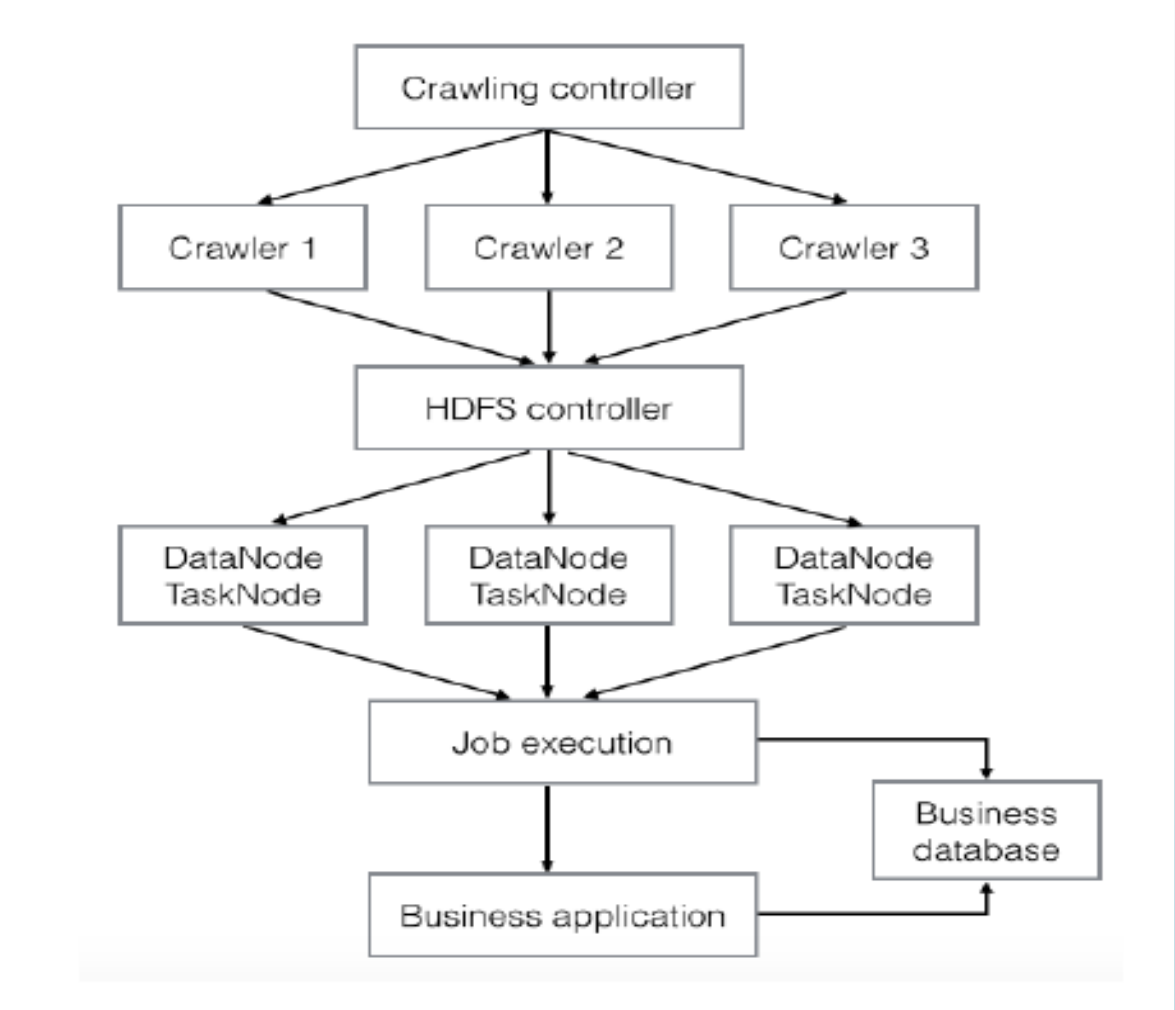
5. Analysis layer : è orientato all'applicazione e include query di log, gestione e mining, che analizza e fornisce approfondimenti in termini di log; analisi dei social network, che analizza i dati dei social network sottoposti a scansione dai livelli inferiori.

Cloud Based Forensics Framework



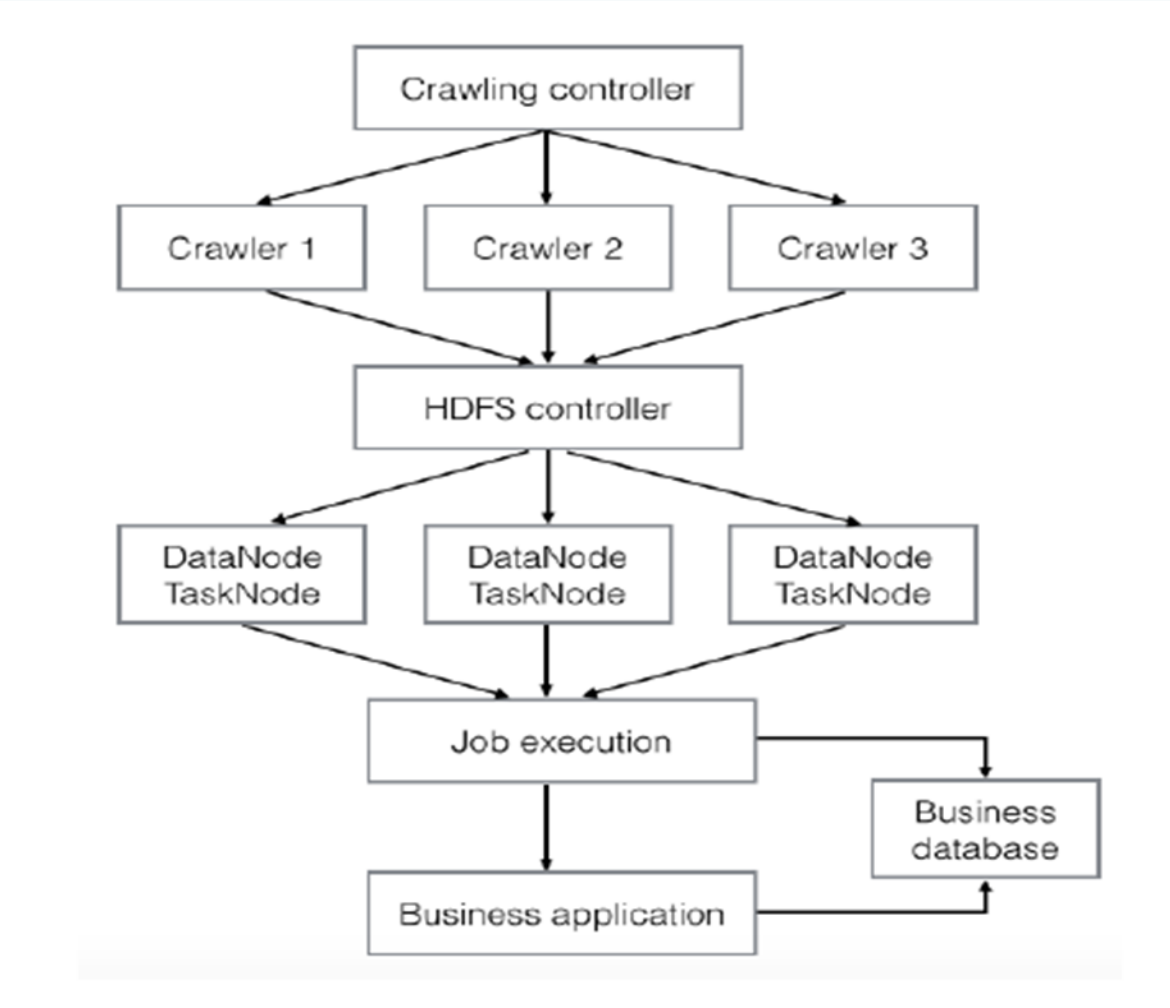
Struttura del Crawler

Più ***crawler*** sono gestiti da un nodo *controller*, che è responsabile dell'avvio, dell'arresto e della pianificazione dei crawler. Quindi, i dati raccolti da ciascun crawler vengono trasferiti nell'archivio *HDFS*



Struttura del Crawler

Il nodo del controller *HDFS* assegna blocchi di dati a diversi *DataNode* e il nodo *JobTracker* pianifica diversi *TaskNode* per l'esecuzione del lavoro. Gli script del lavoro vengono definiti su applicazioni aziendali e i risultati dei dati vengono archiviati in un database aziendale per un ulteriore utilizzo.



Caso di Studio

Se tutti i collegamenti sociali tra i criminali sono stati definiti, possiamo dedurre potenziali relazioni tra criminali o addirittura prevedere chi altro potrebbe essere un potenziale criminale. Il modello si basa su tre caratteristiche:

- *somiglianza della struttura della rete*
- *somiglianza degli interessi dell'utente*
- *somiglianza dei luoghi di check-in*

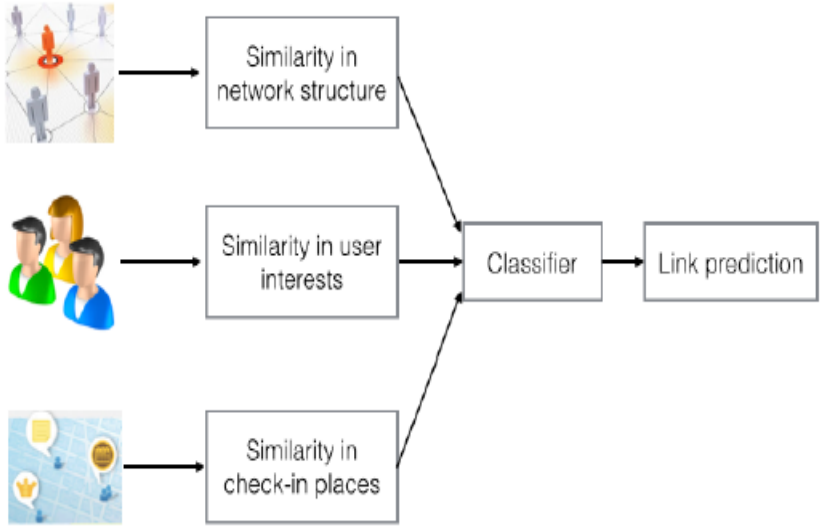
Costruiamo il social network ed estraiamo le informazioni degli utenti dai nodi. Successivamente calcoliamo la somiglianza basata sulla posizione tra gli utenti.

Somiglianza Strutturale

La somiglianza strutturale è positiva in relazione al numero di amici comuni che ci sono tra due nodi. Definiamo la somiglianza strutturale tra il nodo a ed il nodo b come:

$$struc\_score(a,b) = \sum_{c \in N(a) \cap N(b)} \frac{1}{\log \deg(c)}. \quad (1)$$

N(a) ed N(b) indicano i vicini di a e b
Deg(c) rappresenta il grado del nodo c
La sommatoria indica il collegamento sociale è positivamente correlato al numero di vicini comuni.



- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Cloud Based Forensics Framework
- **Problemi della Social Network Forensics**
- Tool utilizzati per la SNF

Problemi della SNF

- Affidabilità dei dati
- Privacy degli utenti
- Mancanza di qualificazione adeguata

Affidabilità dei Dati

- Dati errati o inesatti raccolti dai social media possono deprecare i benefici dell'utilizzo dei social media
- Tendenza naturale degli utenti a modificare e falsare le informazioni pubblicate sui social media
- Pubblicare dati errati che possono sviare le indagini
- I querelanti sono spesso consigliati dai propri avvocati di eliminare i post sui social network

Privacy degli Utenti

- Quali informazioni possono essere ispezionate senza informare il richiedente?
- Quali informazioni sono ritenute «publiche»?
- È opportuno richiedere l'amicizia a qualcuno per ottenere l'accesso a più dati personali ?

Molti siti di SN consentono agli utenti di elencare informazioni personali come: nome,cognome,data di nascita,indirizzo di residenza. Anche se gli utenti pensano di avere il controllo su questi dati,e pensano di sapere esattamente con chi li condividono,molte volte tali informazioni vengono scovate ed utilizzate dagli ispettori forensi durante le indagini.

Se gli ispettori forensi durante un'indagine trovano informazioni confidenziali che non servono al caso a cui stanno lavorando,dovrebbero evitare di divulgarle a terze parti.

Mancanza di qualificazione adeguata

- Gli analisti forensi dovrebbero avere una qualifica adeguata e appartenere ad una associazione professionale.
- Alcuni fornitori offrono corsi e certificazioni per questo tipo di lavoro
- Importante mantenere conoscenze e abilità aggiornate in questo settore poiché si evolve molto velocemente,e le caratteristiche e funzionalità di un Social Network mutano rapidamente.

- Introduzione alla presentazione
- Introduzione ai Social Network
- Attacchi ad un Social Network
- Attacchi agli Utenti
- Introduzione alla Social Network Forensics
- Conceptual Framework
- Problemi della Social Network Forensics
- **Tool utilizzati per la SNF**

Tool utilizzati per la SNF

I tool principali utilizzati nell'ambito del Social Network Forensics sono i seguenti:

- **EnCase Forensics**
- **CacheBack**
- **Internet Evidence Finder**

Internet/Network/Social networking site forensic tools			
Internet Evidence Finder	IEF is a software application that can search a hard drive or files for Internet related artifacts. It is a data recovery tool that is geared towards digital forensics examiners (JAD Software, 2011a)	Windows	Commercial
CacheBack	Internet cache and history analysis + social networking sites analysis	Windows	Commercial

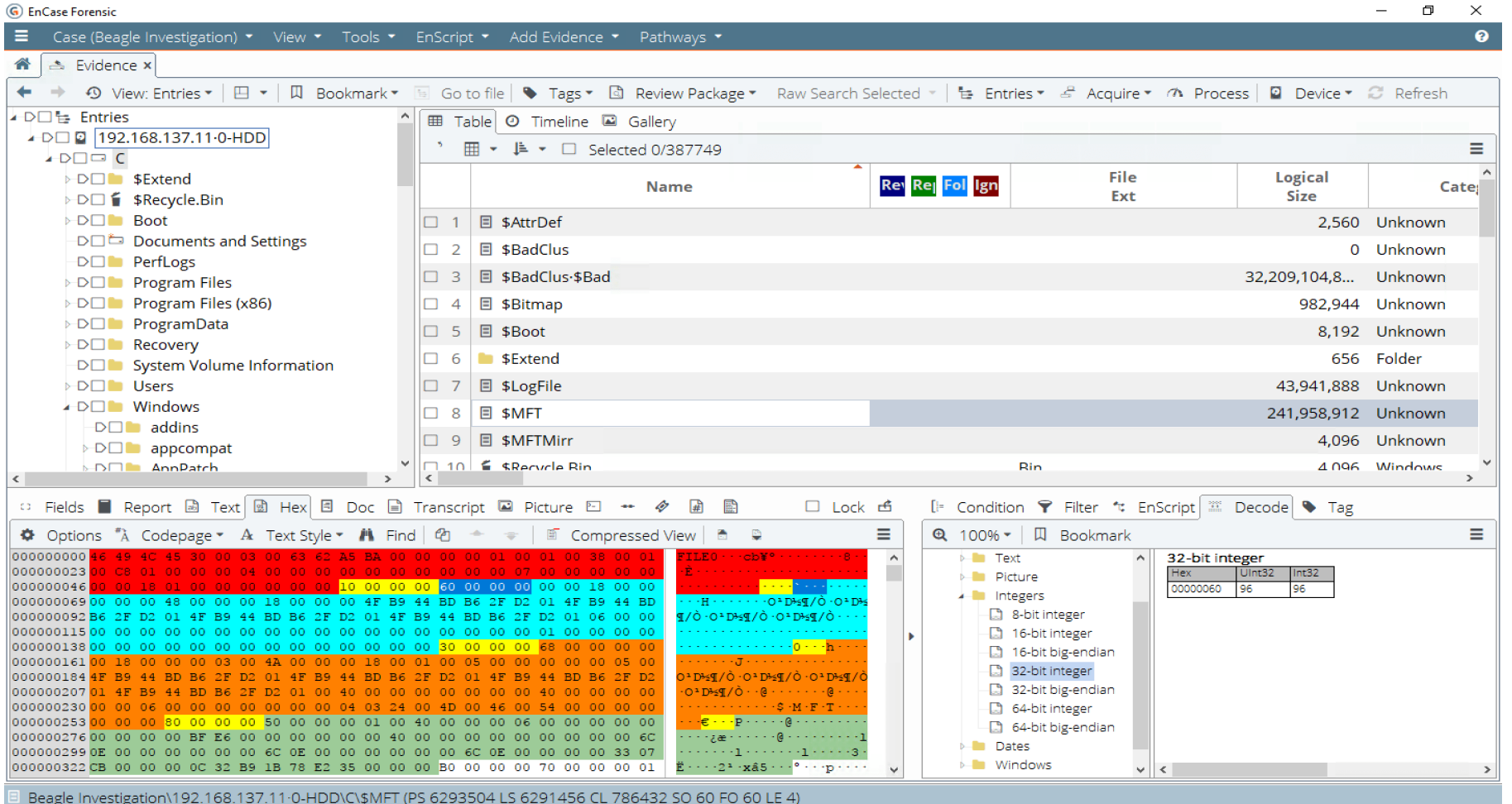
EnCase Forensics

EnCase Forensics viene utilizzato su dispositivi Windows,Mac e Linux per trovare prove e dati.

Le funzionalità di questo tool includono:

- Acquisizione di dati da qualsiasi dispositivo: Memoria Ram,email,immagini,cronologia web,memoria cache,sessione di chat,file compressi e di backup.
- Fornisce un tool per l'analisi avanzata dei dati raccolti
- Fornisce un tool per la generazione automatica di un report
- Fornisce funzionalità di programmazione agli esaminatori forensi, consentendo agli utenti di creare programmi personalizzati per aiutarli ad automatizzare le attività investigative che richiedono tempo


EnCase® Forensic
The Gold Standard in Forensic Investigations. Now Supporting Mobile Acquisition.
Computer & Mobile Device Acquisition
Easy-to-use Interface
Powerful Customizable Processing
Automated External Review
Integrated Investigation Workflows
Flexible Reporting Options


EnCase Forensic
Case (Beagle Investigation)
View
Tools
EnScript
Add Evidence
Pathways
Evidence
Entries
192.168.137.11-0-HDD
C
$Extend
$Recycle.Bin
Boot
Documents and Settings
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
addins
appcompat
Table
Timeline
Gallery
Selected 0/387749
Name
File Ext
Logical Size
1 $AttrDef 2,560 Unknown
2 $BadClus 0 Unknown
3 $BadClus:$Bad 32,209,104,8... Unknown
4 $Bitmap 982,944 Unknown
5 $Boot 8,192 Unknown
6 $Extend 656 Folder
7 $LogFile 43,941,888 Unknown
8 $MFT 241,958,912 Unknown
9 $MFTMirr 4,096 Unknown
Fields
Report
Text
Hex
Doc
Transcript
Picture
Lock
Condition
Filter
EnScript
Decode
Tag
Options
Codepage
Text Style
Find
Compressed View
100%
Bookmark
Text
Picture
Integers
8-bit integer
16-bit integer
16-bit big-endian
32-bit integer
32-bit big-endian
64-bit integer
64-bit big-endian
Dates
Windows
32-bit integer
Hex
UInt32
Int32
00000060
96
96
Beagle Investigation\192.168.137.11-0-HDD\C\$MFT (PS 6293504 LS 6291456 CL 786432 SO 60 FO 60 LE 4)

CacheBack

- **CacheBack** viene utilizzato per ricostruire pagine web memorizzate nella cache ed esaminare la cronologia e le attività dai siti di Social Network(es. chat di Facebook o Messanger).

- Supporta tutti e cinque i principali web browser

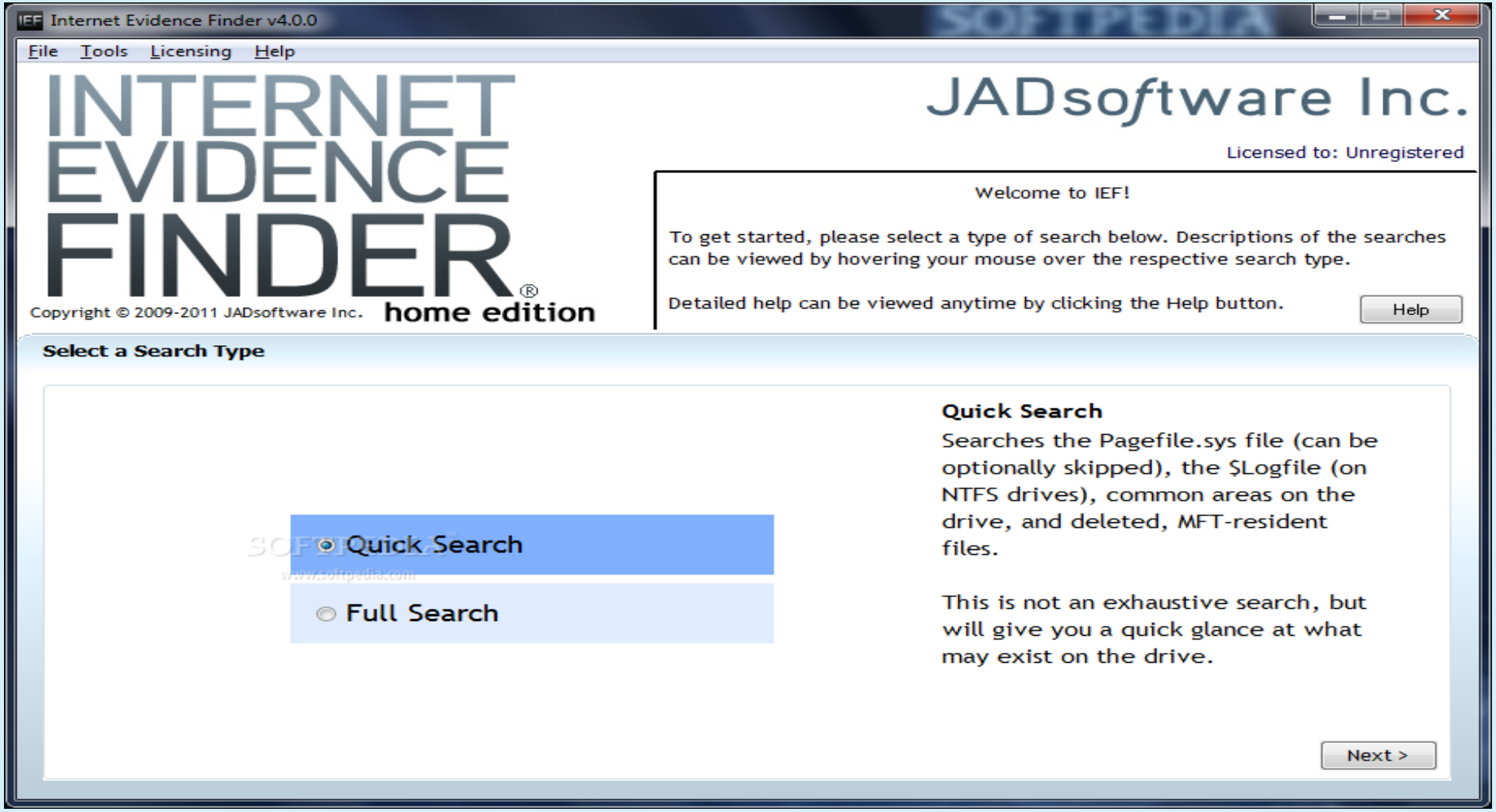
  (Firefox,Chrome,Safari,IE,Opera)

Internet Evidence Finder

Internet Evidence Finder presenta alcune funzionalità interessanti tra cui:

- **Facebook live chat search** :Cerca informazioni nelle chat ,anche quelle dannegiate o cancellate.
- **Convertitore** del testo Unicode di Facebook
- **Trova dati frammentati** di pagine web correlate a Facebook,come ad esempio email,gallerie fotografiche,gruppi ecc. Questi elementi molto spesso sono frammentati e scomposti,ma ci sono funzioni per tentare di ricostruire l'intera pagina.

Internet Evidence Finder



www.softpedia.com

Bibliografia

[1] *Social Network Forensics: Evidence Extraction Tool Capabilities*- JUNG SON

[2] *Digital Forensics 2.0* - MohammadReza Keyvanpour

[3] *Evidence collection and forensics on social networks: Research challenges and directions* - Humaira Arshad

[*4]World Map of Social Network*-vincos.it

[5] *A Multilayered Semantic Framework for Integrated Forensic Acquisition on Social Media* - Humaira Arshad

[6] *blogs.opentext.com*

[7] *Cloud Based Forensics Framework for Social Networks and A Case Study on Reasoning Links between Nodes* - Fawang Han


THANK YOU