



A Forensic Approach to Technology and Social Media

Legalwise

February 2021

Agenda

- Forensic Technology 101
- Social Media Evidence
- Innovative Solutions
- Forensic Expert Witness View



Forensic Technology 101



What is Forensic Technology or Digital Forensics

- A branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on electronic data.
- Involves the handling of data for the purpose of legal proceedings.
- All processes must utilise sound forensic techniques to ensure that the findings are admissible in court.

What is Electronic Evidence

- Electronic evidence includes any data that may be located on a wide range of storage locations. e.g servers, personal computers, laptops, mobile devices, cloud repositories etc
- Electronic evidence is unique as it:
 - Can be distributed across physical and jurisdictional locations
 - Is volatile and can be easily altered, overwritten, damaged or permanently destroyed by a single keystroke or mouse click
 - Can be copied without degradation
 - May not be 'readily retrievable' if the necessary hardware and software is not preserved.


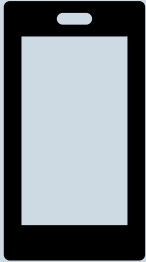


Forensic Investigation Lifecycle

- Acquisition
- Processing
- Analysis
- Reporting

Acquisition

- Preserve the integrity of the electronic evidence
- Identical copy without changing the content of the electronic evidence
- Creates a hash value to prove that the copy is sound
- Analysis typically performed on the copy

Acquisition

Computer	Mobile	Cloud	Warrant Return
			



Social Media Evidence



Social Media Uses

As a platform



As electronic evidence



Social Media as a Platform

Social Media can be used as an investigative tool when seeking evidence or information about:

- missing persons
- wanted persons
- crimes perpetrated online
- photos or videos of a crime posted online

International Association of Chiefs of Police Survey - 2013

90% use social media to support criminal investigations.

80% claim social media has helped solve crime.

Most common Sources:

- Facebook - 92%
- Twitter - 65%
- YouTube - 43%

A total of 500 law enforcement agencies, representing 48 States, participated in the survey.

Social Media as Electronic Evidence

Preserve Social Media Account Data

Litigation Support

Forensic Examination

Recovery of Deleted Data

Deleted Social Media





Innovative Solutions



Mobile Devices – Security

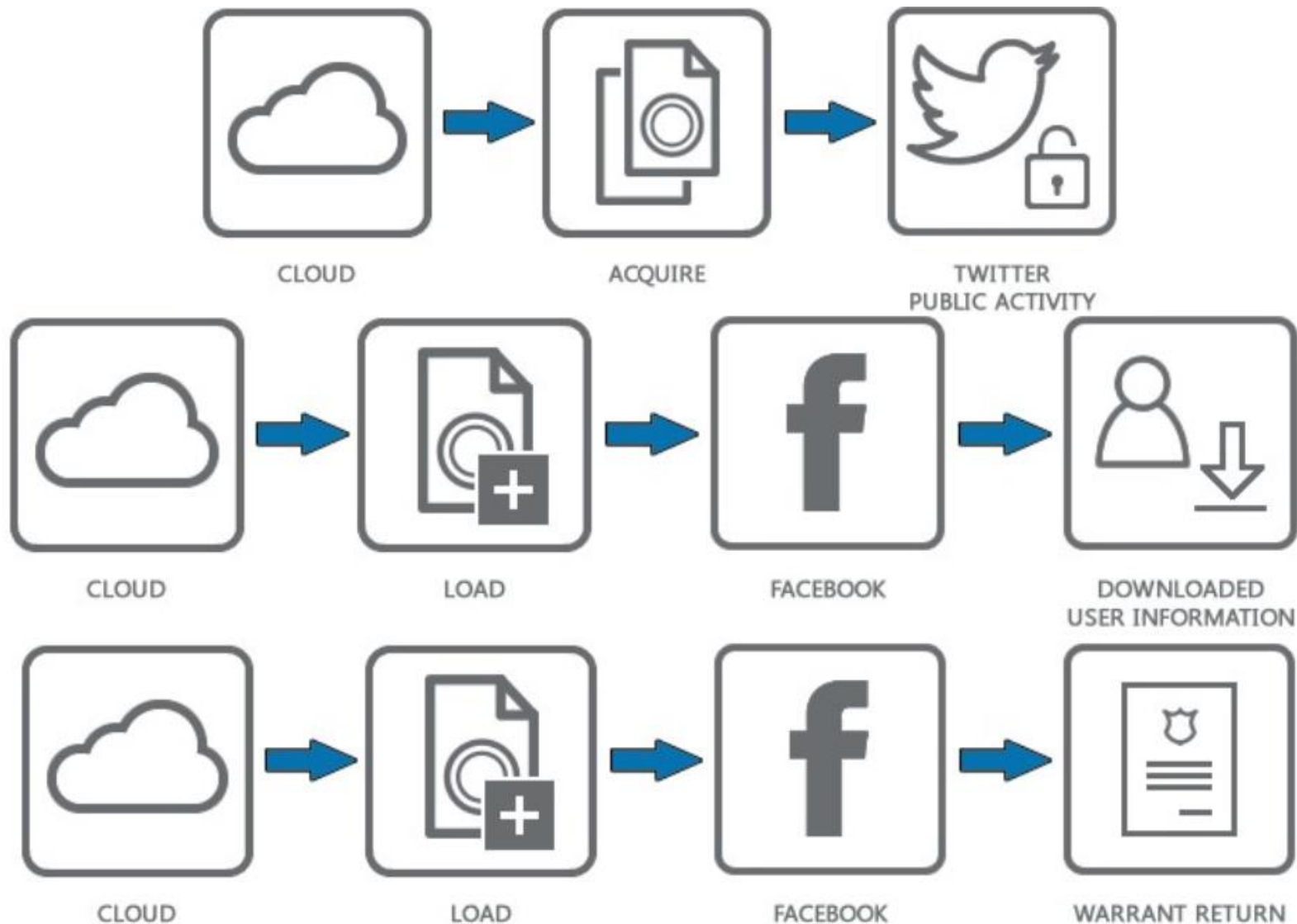
Quick Extraction:

The Quick Extraction method will work on any iOS device, version 5 or newer. Magnet ACQUIRE will combine an iTunes backup, with some additional acquisition techniques, to obtain both native and third-party data. A Quick image from Android devices will include an ADB backup, as well as an additional extraction to obtain browser history and/or native application data (depending on the version of Android). Magnet ACQUIRE supports Android version 2.1 or newer.


Full Extraction:

Magnet ACQUIRE can also help you obtain a full, physical image of many Android devices by using either the built-in privilege escalation exploits or by imaging a device that has already been rooted. Full Extraction is also supported for jailbroken iOS devices. To use Magnet ACQUIRE, start by connecting the mobile device to your examination computer. Run the tool and you should be presented with a list of devices that are connected to your system.

Example Forensic Collection of Social Media




Evidence Examples - Twitter



- Home
- Explore
- Notifications
- Messages
- Bookmarks
- Lists
- Profile
- More

Tweet



PRADA

@Prada

Thinking fashion since 1913.

Milano Joined February 2013

5 Following 1.3M Followers


Not followed by anyone you're following

Tweets

Tweets & replies

Media

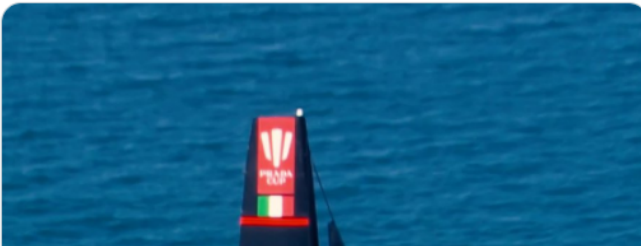
Likes




PRADA @Prada · 59s

#PradaCup has come to an end and @lunarossa moves on to the 36th America's Cup. The team will face the defender @EmiratesTeamNZ from 6th to 15th March to decide who will win the oldest trophy in international sport.

#AmericasCup
#LunaRossaPradaPirelli




Search Twitter



CyFi @CyFi10


Promoted

Follow



Vogue Magazine @voguemagazine

Follow



British Vogue @BritishVogue


Follow

Show more

Incident Response S... @IncidentRespNZ

18

Evidence Examples - Facebook



Request copy

Available copies

Date range: All of my data

Format: JSON

Media quality: High

Create File

Settings

General

Security and

Your Facebook

Privacy

Face recogni

Profile and ta

Public posts

Blocking

Location

Language an

Stories

Journalist re

Your information

Posts

Photos and videos

Comments

Likes and reactions

Friends

Stories

Following and followers

Messages

Deselect all

View

View

View

View

View

View

View

View

View

View

View

Forensic Tools



Social Media Tools

The screenshot displays the Mention App interface, which is used for monitoring social media mentions. The interface is divided into several sections:

- Left Sidebar:** Contains navigation options like 'Feed', 'Dashboard', 'Influencer', 'Insight Center', and 'Reports'. It also lists mentions for 'Nasa' (59,308 mentions) and 'Space X' (35,903 mentions), along with filters for 'Inbox', 'Unread', 'Priority', 'Favorites', 'Social Messages', 'TAGS', 'TASKS', and 'ACTIVITY'. A button 'Add a new alert' is visible at the bottom.
- Top Bar:** Features a search bar labeled 'Recherche ...' and a user profile for 'Thomas Michel NASA'.
- Central Feed:** Displays a list of mentions under the heading 'All Sources'. The mentions include:
 - From **elle.com**: 'Mode brand of the yar' (22h).
 - From **nytimes.com**: 'Story with Lewis Hamilton' (22h).
 - From **KONA Morning News**: 'KONA Morning News' (22h).
 - From **@vogue**: 'Vogue Magazine' (22h).
 - From **@elliotpuzenat**: 'Simple Inspiration' (22h).
 - From **Uber Company**: 'Nasa partnership with Uber US' (22h).
 - From **selenagomez.news.co**: 'S.Gomez Partnership with Nasa' (22h).
- Right Panel:** Provides a detailed view of the 'Nasa partnership with Uber US' mention. It includes the Uber logo, the text 'Super Excited to announce a partnership with Nasa this year! They provides Agency-level strategic policy and procedural guidance for all domestic, unclassified partnerships matters.', and a link to 'UBER.COM'. Below this, there are reactions from 'Taylor Swift' and 'Nasa', and a comment section.
- Bottom Bar:** Shows the 'Uber Company' profile, the Facebook post URL 'facebook.com/26169/posts/128499032155', and engagement metrics: '582M REACH' and '85/100'.



Forensic Expert Witness View



Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310
campbell@incidentresponse.co.nz
incidentresponse.co.nz
whistleblowers.co.nz



We help you Prepare, Respond and Recover
from Forensic and Cyber Incidents