Mining Digital Evidence from the Internet and Social Media

Jeffery Owen, Sergeant
Missouri State Highway Patrol / DDCC
DEA TFO- Kansas City Division

Objectives

1. Describe the strengths and weaknesses of digital evidence from online sources
2. Describe the evidentiary concerns of digital evidence
3. List OSINT tools to locate online evidence
4. List preservation techniques possible with Internet Service Providers (ISP)
5. Describe methods to document user visible data
6. Describe methods used to parse data provided by ISP

Outline

I. Identifying sources of digital evidence including social media
   a. Strengths and weaknesses of digital evidence online
   b. evidentiary concerns
   c. toolbox- OSINT tools

II. Preserving online evidence
   a. preservation techniques
   b. documenting visible data through sites and apps

III. Parsing through data provided by ISP
   a. IP tracking
   b. phone number -tolls
   c. link charts.

Basic Process

1/ Locate account identifier
2/ Identify Social Media LEO process
3/ Send Preservation Request
4/. Determine level/type of information required
5/ Consult Social Media Company guides to use their language
6/. Acquire Legal Process (2 ways)
   Option 1: Subpoena/Court-Order
   Option 2: Search Warrant
7/ Parse and Review data

I. Identifying sources of digital evidence including social media

4

1/ Locate account identifier

OSINT Framework / https://osintframework.com/

Mike Bazzell -Intel Techniques

https://inteltechniques.com/training.html

5

Documentation

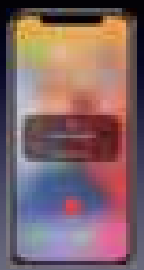
Screenshot immediately (or photograph)

Video long screen shots. Do not use with Snapchat unless you want target aware.

>Computer ; Snagit ($$) or Screencast-O-Matic

>iPhone screen record function [https://support.apple.com/en-us/HT207935]

>Android [https://support.google.com/android/answer/9075928?hl=en]

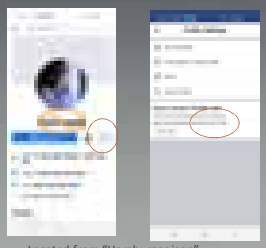


6

Facebook Account Name - PC

7

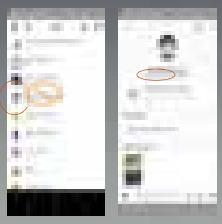
Facebook Account Name – Android/iOS



Located from "Hamburger icon"

8

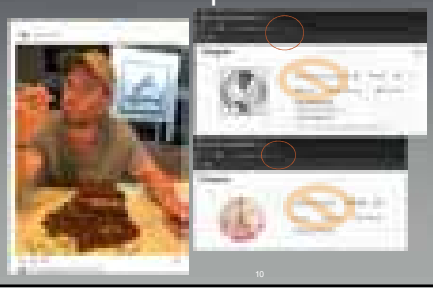
Snapchat Account Name – Android/iOS



Located from profile picture

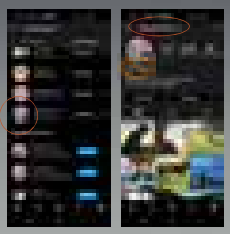
9

Instagram Account Name – Computer View



10

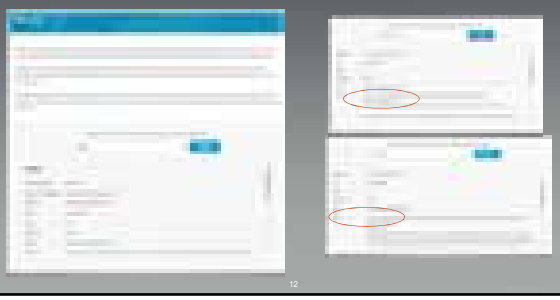
Instagram Account Name – Android/iOS



Located from profile picture

11

2/ Identify Social Media LEO process



12

II. Preserving online evidence

3/ Send Preservation Request

Submit as soon as accounts are located and identified.

>No penalty if you never request data

>Can make multiple requests to preserve later data

>May help preserve user "deleted" data

At minimum, needs the following information

A. Identify yourself

B. Identify the account

C. State you are seeking further legal process

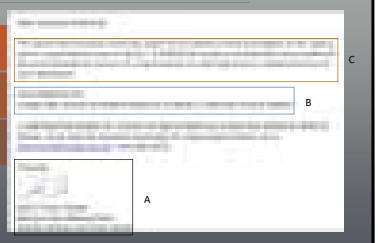
Usually requested on letter-head with agency information

Must be signed, digitally or physically

Send to location identified by Search.org

Preservation Request Contents

A	Identify yourself
B	Identify the account
C	State you are seeking further legal process



Preservation Request Follow-up

If you make a preservation request:

- Reference preservation date and number in legal documents
  - Search Warrant, Subpoena, Faxed/emailed/LEO-Portal Consent
- Be sure to request the PRESERVED COPY of data
  - Many companies will give you LIVE/Current data if preserved copy isn't requested

Non-Disclosure

As default, most companies will disclose to the subscriber:

- The execution of the search warrant
- The data being sought

As default, subscribers are given an opportunity to stop process

- Subscriber must submit legal process to quash the legal process

Non-Disclosure prevents the notification of the subscriber

- Reminder: Endangering life or safety, Flight, Destruction of evidence, Intimidation of witness, Jeopardize investigation or delay a trial

Sample NDO Language

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Snap Inc. (hereinafter "Snapchat"), an electronic communication service and/or a remote computing service, not to notify any person (including the subscribers and customers of the account(s) listed in the attached search warrant #### of the existence of the attached search warrant for one year from the date of this Order.

The Court determines that there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving the targets an opportunity to flee, or to continue flight from prosecution or to tamper with evidence or to change their patterns of behavior if they find that the accounts have been compromised. *See* 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Snapchat shall not disclose the existence of the attached search warrant, or this Order of the Court, to the listed subscriber or to any other person for one year from the date of this Order, unless and until otherwise authorized to do so by the Court, except that Snapchat may disclose the attached search warrant and the attached Order to an attorney for Snapchat, for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until further notice of the Court, except for use by the United States as they deem necessary to further the investigation and/or prosecution of the ongoing criminal investigation.

4/ Determine level of information required

- Metadata or Content?
- Can user download?
- Can it be publicly seen?
- Limit by date/ user- Avoid “general warrants”.

5/ Consult Social Media Company guides to use their language

SAME TERMS AS USED BY COMPANIES

Need to use exact terms that the companies use themselves

Terms can be found in the following pages

- LE guides
- Privacy pages
- User guides
- User DIY Downloads

EXAMPLES:

- Location History
- Search History
- Device fingerprints
- Google Takeout
- Fusion Tables
- Mail mBox or Json
- Location KMZ
- Fit data
- Machine Cookies

Example 2703(d) Affidavit Order

Example 2703(d) Order

6/ Acquire Legal Proces

SUBPOENA/COURT ORDER - 2703

- Subscriber Data (what sub. give up)
  - Address
  - Telephone numbers
  - Emails
- Transactional Data (Technical data)
  - Account creation date
  - Account identifiers
  - Account standing
  - Machine Cookies (FB)
  - Security/Login information
    - Date
    - Time
    - IP Address
- Payment History
  - Purchase date and item
  - CC information if stored

SEARCH WARRANT - 2703

- Chat/Message-History/Email
- Photos/Videos
- Drive/Cloud Contents
- Backup Data
- Search/Web History
- Friends/Followers/Following
- MarketPlace (FB)
- Calendar
- Device Configuration
- Location Information (Used to be included in Technical Data)
  - Within 24 meters, typically

Consent/DIY-Download with give most of the same information as Search Warrant

Foreign or Domestic

Check the MO Secretary of State's website for corporation location

- https://www.sos.mo.gov/business

Typically based in Delaware if foreign

https://icis.corp.delaware.gov/ecorp/entitysearch/NameSearch.aspx

Victim Downloads

All Social Media accounts allow for download of personal data

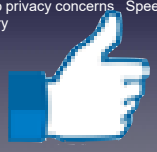
Must have access to Passwords and email for account

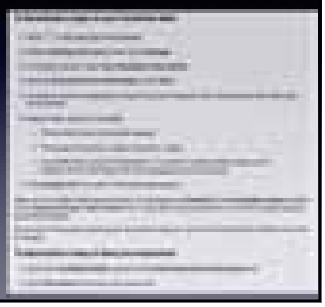
Weigh case value to privacy concerns. Speed of access / Discovery

Facebook

Snapchat

Instagram





25

RSMO for Legal Process

RSMO 351.609 – Investigative Subpoena, Search Warrant
- Requires foreign and domestic businesses to respond to legal documents
- Businesses must provide a Verified Affidavit for records

Investigative Subpoena
- RSMO 56.085 "to any witness who may have information . . . to require the production of books, papers, records, or other material of any evidentiary nature."
- Based on Reasonable Suspicion. Records about records/metadata

Search Warrant
- RSMO 542.276 -Governs who may apply, must be accompanied by an affidavit, probable cause required, may be issued electronically or by fax, must be executed asap, return must be within ten days, subsequent searches of property taken is OK as long as PC still exists. Content

26

United States 4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized but upon probable cause, supported by oath or affirmation

27

Missouri Constitution Article 1, Section 15

That the people shall be secure in their persons, papers, homes, effects, and electronic communications and data, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, or access electronic data or communication, shall issue without describing the place to be searched, or the person or thing to be seized, or the data or communication to be accessed, as nearly as may be; nor without probable cause, supported by written oath or affirmation.

28

III. Parsing through data provided by ISP's

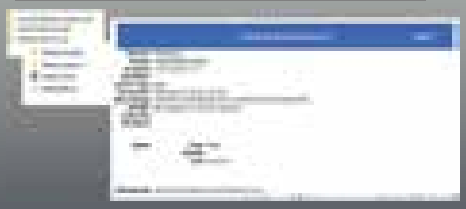
29

7/ Parse and Review data

- Do not simply dump data on PA - organize and present
- Ensure a complete discovery copy is available
  - Redaction / compromised data
- Organize
- A complete set of data must be retained for Discovery purposes

30

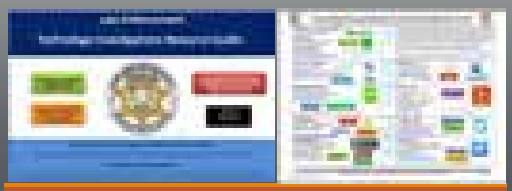
Facebook Response Example

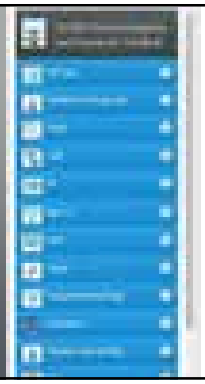


Build your toolbox

LE Resource Guide – Provides links to LE Guides, Investigative Tools, Browser/OSINT tools, and example warrants

- Creator has requested we don't pass out PDF
- Request it from here: https://www.orhia.com/le-technology-guide



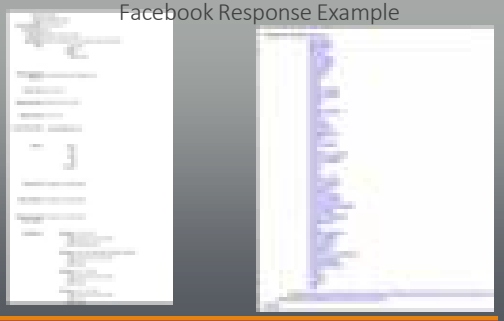


MORE Resources

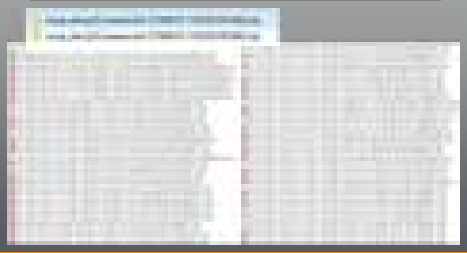
Search.org offers more than ISP lists

- Investigations Web Browser Add-on with OSINT
- Podcasts
- Video presentations
- Publications and Trainings
- Tech Guides

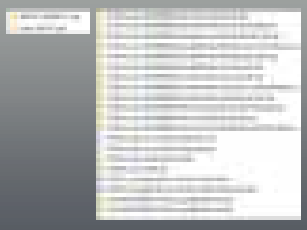
Facebook Response Example



SnapChat Response Example



Google Response Example



Words of Caution

YOU are responsible for the data you possess

Only view/use the data when work related

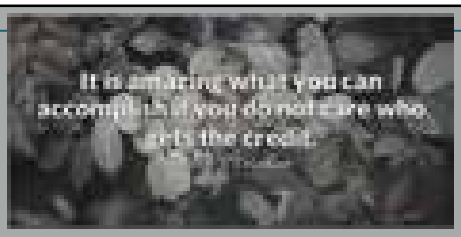
Do not show others who do not need to see the data

You can be prosecuted
- Example: RSMO 573.110 – non-consensual dissemination of private sexual images

You can be disciplined according to your rules/regulations

You can be disciplined by POST

Example: University of Utah officer showed multiple co-workers intimate evidence photos of Lauren McCluskey.



Jeffery Owen, Sergeant
Missouri State Highway Patrol - DDCC
TFO - Drug Enforcement Administration
816.787.7218
jeffery.owen@mshp.dps.mo.gov
jeffery.m.owen@dea.gov