The Investigation, Forensics, and Governance of ATM Heist Threats in Law Enforcement Agencies

Associate Professor Dayu Kao (Ph. D.)
Department of Information Management,
Central Police University, Taiwan
camel@mail.cpu.edu.tw

Table of Content

I. Introduction

- Law enforcement agencies (LEAs) should
  - make certain observations and interpretations of the digital data,
  - supply sufficient evidence in crime reconstruction, and
  - prove the suspect's illegal access to the computer itself.

Inferring Traits from Profiles

- ✓ People say a lot online.
- ✓ Computer scientists are actively developing technology that reveals all kinds of secrets about social media users.
- ✓ When data from millions of people can be analyzed, statistical analysis and advanced computational techniques can detect patterns that **indicate** that a person has a particular **attribute**.

OSINT

- Open Source INTelligence (OSINT) is the intelligence collected from the sources which are present openly in the public.
- OSINT comprises of various public sources, such as:
  - Academic publications: research papers, conference publications, etc.
  - Media sources: newspaper, radio channels, television, etc.
  - Web content: websites, social media, etc.
  - Public data: open government documents, public companies announcements, etc.

OSINT Types

- Literature
  - White literature: Published
  - Black literature: Non-Published
  - Grey literature (or gray literature): Published but not easy to (specialized) access.
- Sources
  - The Internet: geolocation data, people search engines
  - Traditional mass media (e.g., television, radio)
  - Specialized journals, academic publications
  - Photos and videos including metadata
  - Geospatial information (e.g., maps and commercial imagery products)

Benefits of OSINT

- Less risky
- Cost effective
- Ease of accessibility
- Legal issues: without worrying about breaching any copyright license as these resources are already published publicly.
- Aiding financial (criminal) investigators
- Fighting against online counterfeiting (fake news)
- Maintaining national security and political stability

What are the challenges of open source intelligence?

- Sheer volume of data
- Reliability of sources
- Human efforts

Techniques, methods and opportunities in Social Media Intelligence (SOCMINT)

The ‘state of the art’ for generating insight from SOCMINT (Social Media Intelligence).

(1) Evidence for law enforcement: establish and generate evidence to situational awareness

(2) Big data Insight: aid understanding and explanation

(3) An aid to Prediction: apply predictive analytics to social media datasets to predict a range of social behaviors and phenomena

Categories of social media

✓There are many types of social media:

- Social networks: Facebook, Google+, VK,
- Photo sharing: Instagram, Flickr
- Video sharing: YouTube
- Microblogging: Twitter, Tumblr
- Social bookmarking: Pinterest
- Social gaming
- Review sites: LinkedIn (business-oriented)
- App
- forums
- and more.

Information from social media

- ✓ Major categories include
  - basic demographic information,
  - social connections,
  - location information,
  - patterns of behavior, and
  - the content of the posts themselves.

What are the attributes of social networks?

- ✓ Anonymity and confidentiality
- ✓ Going undetected
- ✓ Use of pseudonames
- ✓ No computer savvy

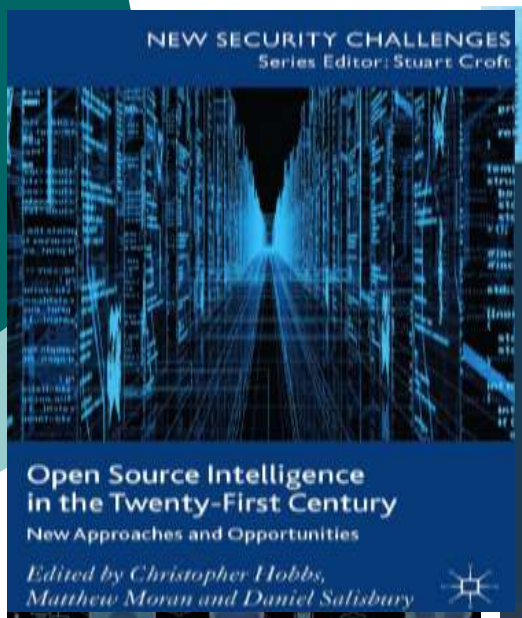
What is the relationship between Social Networking and Crime?

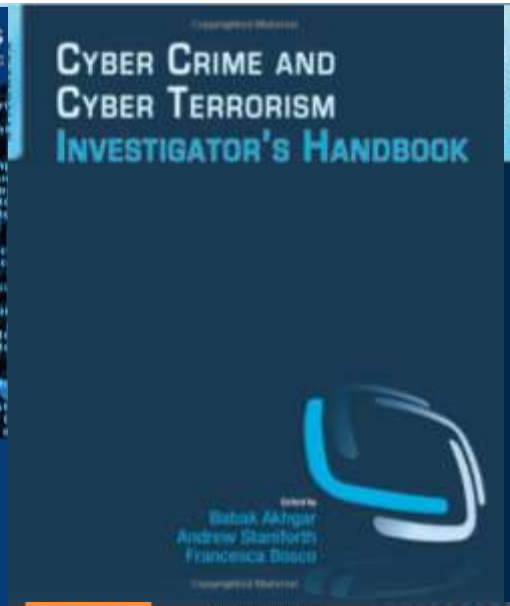
- ✓ Users must decide
  - whether their presentation will be accurate or idealized,
  - what and how much to disclose,
  - who their audience consists of, and
  - how they will interact with them.

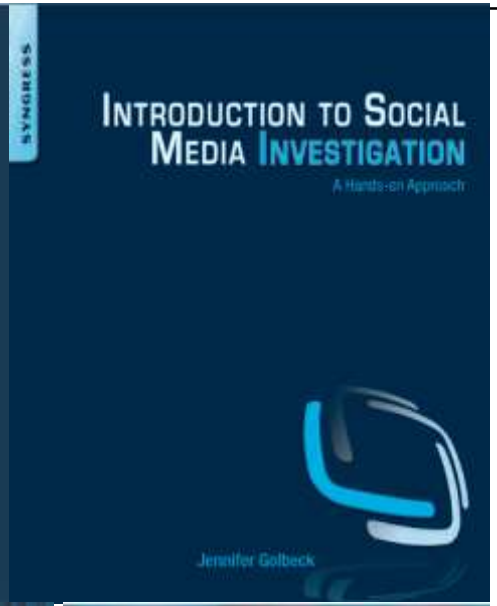
Why might the police conduct an investigation online via OSINT/SOCMINT?

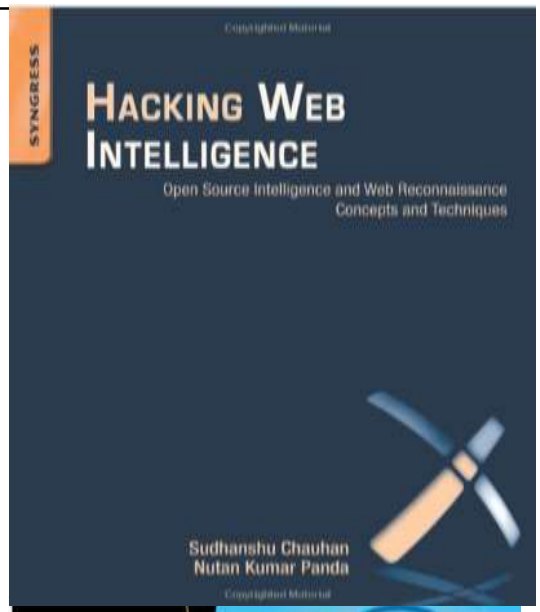
- ✓ Law enforcement and lawyers in civil suits certainly want to gather information on suspects or the opposing side of a dispute.
- ✓ The information that people reveal online is valuable as evidence.
- ✓ It quite easy to mistake one person for another online, and information needs to be analyzed carefully.

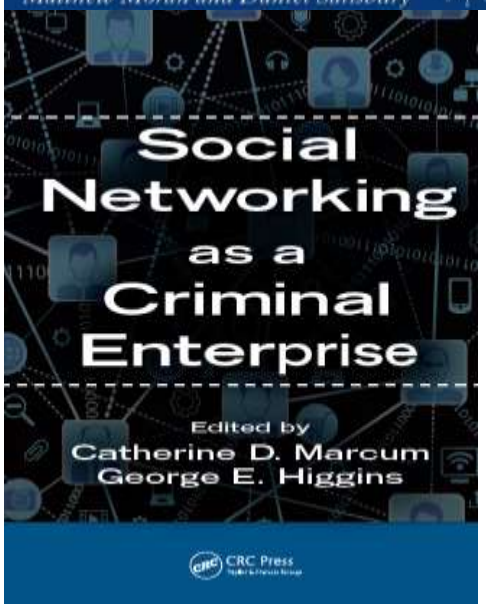
II. Literature Reviews

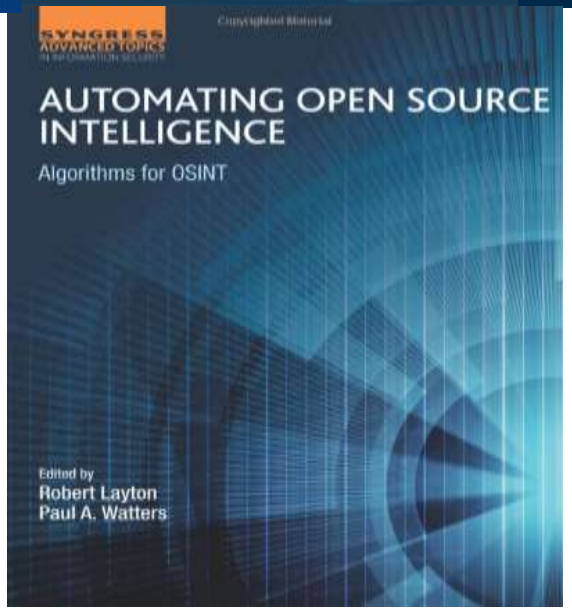


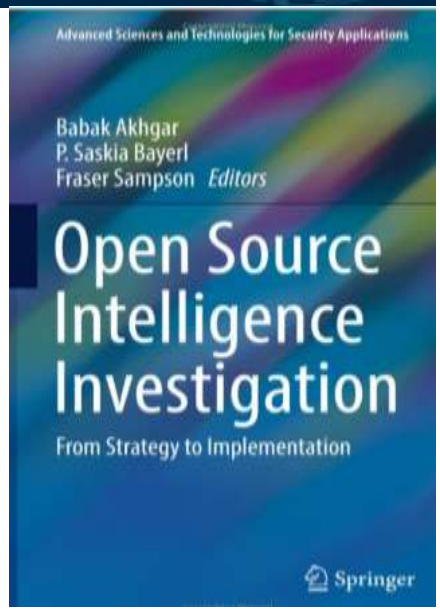


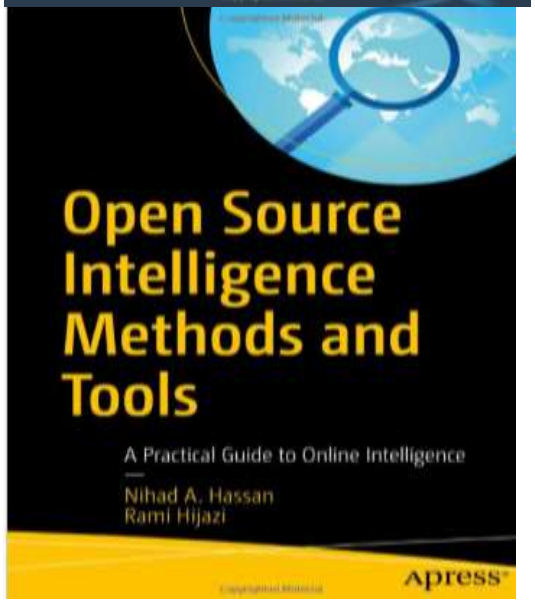












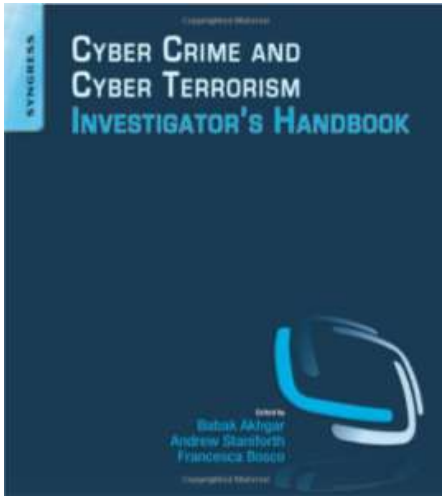
Organizational Cybercrime Activities

Year	Group Name	Actor Type
1993~2001	DrinkOrDie (DoD)	Non-state
1996~1998	The Wonderland Club	
2003~	Anonymous	
2006~2008	Dark Market	
2006~2010	PLA Unit 61398	State
	Shady RAT	
	Aurora	
	GhostNet	
2007~2013	PRISM	
2010	Operation Olympic Games	
	Stuxnet	
2010~2012	Ukrainian ZeuS Group	Non-state

Investigators' Golden Rule

- *The golden rule is for investigators to apply what is known as the 'ABC' principle throughout the life of an investigation as follows:*

- A. Assume nothing
- B. Believe nothing
- C. Challenge and check everything



2014

Cybercrime Investigation

- Criminal investigation actually begins with data on a crime.
- The presence of relevant, reliable, and sufficient evidence can officially open a case in LEAs.
- The identification, collection, examination, analysis, and presentation of evidence in law.
- Cyber threats leave some traces in the packets.

Inman-Rudin Paradigm

- Inman-Rudin Paradigm expanded the Locard Exchange Principle into two principles and four processes.
- The principles include:
  - Transfer
  - The divisibility of matter
- The processes include:
  - Identification
  - Classification/individualization
  - Association
  - Reconstruction

Cybercrime Investigation

- Digital evidence has become an essential part of crime scene investigation to collect live/volatile network information in cybersecurity breaches.
- Cybercrime investigation focuses on
  - (1) identifying the digital evidence from essential logs (identification),
  - (2) finding the suspect ID/account and determining a common class from evidence process (individualization/classification),
  - (3) inferring interactions between the evidence and the suspect from copied data (association), and
  - ordering the associations in time and space from necessary information (reconstruction).

Digital Forensic Process

1. Identification: 6W1H Questions
2. Collection: at scene, in lab, chain of custody
3. Examination: data, information, knowledge, intelligence
4. Analysis: temporal, relational, functional reconstruction
5. Presentation: relevant, reliable, sufficient evidences

III. Sample Case

- A. Taiwan's Russian Mafia Group on Banks and Payment Systems **in July 2016**
- B. **Answering Some Questions**
  - 1) Who: Andrejs Peregudovs, Mihail Colibaba and Nikolay Penkov
  - 2) What: US$2.61 Million Theft in an ATM Looting
  - 3) When: July 9 ~ 10, 2016
  - 4) Where: Three Suspects Were Charged in Taipei
  - 5) How: ATM Attacks Targeting Wincor Nixdorf Model
- C. **Answering Follow-up Questions:** How can OSINT/SOCMINT help in this case?

Money Flow in Taiwan ATM Heist

Date	Money	Activity
July 9 and 10, 2016	NT$83.27 million (US$2.61 million)	Seventeen suspects was illegally withdrawn
July 11, 2016	NT$200,000	Two suspects have converted more than NT$200,000 into South Korean won, Australian dollars and US dollars
July 17, 2016	NT$60.24 million	Two suspects were arrested. Some money was recovered
July 20, 2016	NT$12.63 million	police found Andrejs's bag
July 20, 2016	NT$4.54 million	Mr. Ko handed another bag to police.

93% Money Back

Time and luck

Are there any insiders involved?

- Irregularities in the connections between the voice server in London, the bank's internal network and the ATMs in Taiwan.
- Because the bank's computer system is a closed network, insider assistance could not be ruled out yet in this case.
- Cybercrime investigators will try their best to find evidence in computers or networks.

No sufficient evidence to prove the insiders' illegal access!

Practices on Cybercrime Issues

- **Be collaborating and making efforts to combat cybercrime.**
- **Consider Private-Public-Partnership (PPP) to bring research into reality for cybercrime investigation.**

Actionable Intelligence Practices on Cybercrime Issues

	Near-Term	Mid-Term	Long-Term
Cybercrime Governance	Draw a strategic roadmap to combat cybercrime	Develop SOPs	Facilitate cross-border Cooperation
People	Cybersecurity Capacity Building	Cybersecurity Reporting Mechanism	Private-Public-Partnership
Process	National Agency for Cybersecurity	Legal Measures	International Cooperation
Technology	Cybersecurity Strategy	R&D on advanced Tools and Technology	Active Participation
Tasks	●Create new procedures or policies to deter, respond to, and prosecute cybercrime. ●Enhance the actionable intelligence capability to rapidly gather data, accurately process information, and strategically combat cybercrime.		

Longer Arm of Cybercrime Investigation

- Making sound judgments at low cost is a core role and important attribute for LEAs, who must maximize the potential and exploit the possibilities to ensure things are what they see.
- Various kind of intelligence provide important information in a timely manner to an appropriate audience for better informed decision making.
- Actionable intelligence is related to the investigation or incident at hand within the wider intelligence mix.
- LEAs have produced actionable intelligence from criminal investigation to gain knowledge in support of preventing cybercrime or pursuing terrorists.

Sharing Malware Source Codes

Carberp/source - absourc

GitHub, Inc. [US] https://[redacted]

hzeroo / Carberp

Watch 53 | Star 267 | Fork 256

Code | Issues 0 | Pull requests 0 | Pulse | Graphs

Branch: master | Carberp / source - absource / pro / all source / | Create new file | Find file | History

hzeroo First commit — Latest commit 6d449af on Jun 26, 2013

..		
BC	First commit	3 years ago
BJWJ	First commit	3 years ago
BSS	First commit	3 years ago
BinToHex	First commit	3 years ago
BlackJoeWhiteJoe	First commit	3 years ago
BootkitDropper	First commit	3 years ago
Demo_Cur2	First commit	3 years ago
Demo_Cur3	First commit	3 years ago
Demo_cur	First commit	3 years ago
DllLoaderHook	First commit	3 years ago
DllLoaderHook1	First commit	3 years ago
DropSploit	First commit	3 years ago
DropSploit1/src	First commit	3 years ago

8:09 AM 30/07/2016

Functional Comparison of ATM Malware Family

Malware Family	Carberp	Anunak	Carbanak
Group	Carberp, Pawn Storm or APT28	Anunak hacker group	Carbanak criminal gang
Identified by the Internet security companies	Federal Office for Information Security, BSI (Germany) and Trend Micro (Taiwan).	Group-IB (Russia) and Fox-IT (The Netherlands)	Kaspersky (Russian/UK)
Malware Successor (initially based on)	Zeus, Rovnix, RDPdor, Hodprot, and Origami		Carberp (source code) + Anunak (Wincor ATMs)
Finding Time	2009	December 2014	2015
Victim Location	Russian	Eastern Europe, the U.S.	Russia, the United States, Germany, China and Ukraine

Behavioral Attribute Comparison of ATM Malware Family

Category	Case	1	2	3
Who	An organized criminal group name	Carberp, Pawn Storm or APT28	Unlimited Operations	Russian Mafia
	Suspect numbers	8	8	19
	Arrest by	Russia	USA	Taiwan
	Arrested suspects name (from Newspaper)	Germes and Arashi (Alias)	Elvis Rafael Rodriguez, Emir Yasser Yeje, and Alberto Yusi Lajud-Peña	Andrejs Peregudovs, Mihail Colibaba and Nikolay Penkov
What	USD theft in an ATM looting	$1 Billion	$45 Million	$2.6 Million (NT$83.27 Million)
When	From plan to ATM heist	2009 ~ February 2015	December 2012 and February 2013	July 2016
	Arrest date	March 2012	May 2013	July 2016
Where	ATM location	Moscow in Russia	New York in USA (More than 24 countries)	Taipei City, New Taipei City, and Taichung in Taiwan
How	Money from	the financial institution itself	Prepaid Debit Accounts	the financial institution itself

IV. Investigation, Forensics, and Governance of ATM Heist Threats

https://tw.appledaily.com

Prevention Strategy on ICT Governance

People

- Commit Cross-Border Cybercrimes
- Need for Global Cooperation

Process

- Limit Remote Access for ATMs
- Limit Convenient Access for ATM Cabinets

Technology

- Choose Closed System
- Protect Internal Information

Governance

- Protect against Computer Security Threats
- Enhance Access Control Practices

Cybercrime Countermeasure of Insider Threat Investigation

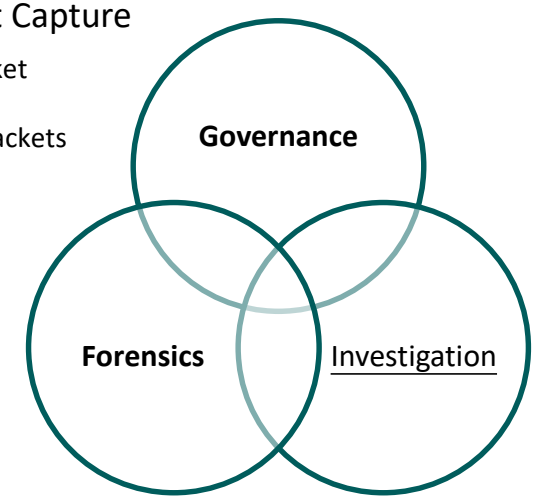
1. Track the Pathway of a Threat
   - Payload-based inspection
   - Port-based identification

2. Perform 24/7 Full-packet Capture
   - Getting packet analyzers
   - Capturing packets

3. Check All Network Connections
   - Real-time situational awareness
   - Inspecting packets

4. Track the Source IP Address
   - Differentiation with user-generated content
   - IP Address-based filter

5. Show the Digital Evidence
   - Testify tools and processes
   - Evaluate admissibility and weight



The Governance of Digital Forensic Investigation in Law Enforcement Agencies

Forensic Thoughts

People : LEAs

Triage

Sufficiency

Digital Evidence

A. Principles

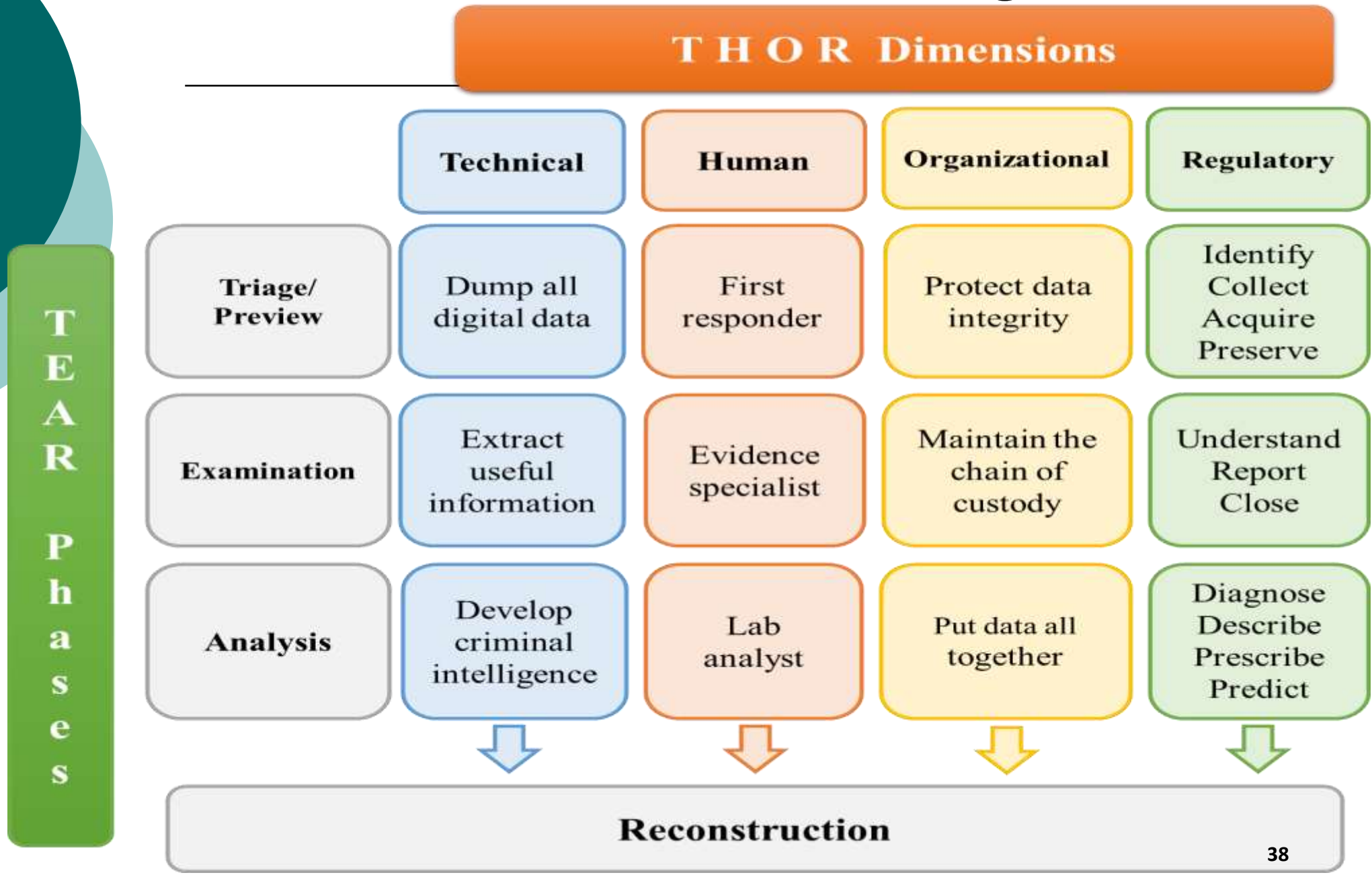
Relevancy B. Forensics Reliability

At Scene C. Governance In Lab

Process :
THOR Dimensions

Technology :
Encase, The Sleuth Kit, Autopsy…

The multi-dimensional framework of digital forensics



Phases	Functions	Tools
Triage/Preview	Packet capture	Wireshark
	Make an image file create hashes of files Data recovery	FTK Imager
	Dump the memory	RAM Capturer
Examination	Browser information extraction	Dumpzilla
	capture the physical memory analyze artifacts in memory	Magnet RAM Capture
	Network sniffering	Network Miner
Analysis	Timeline Analysis Hash Filtering File System Analysis Keyword Searching	Autopsy and The Sleuth Kit
	extract applications data	Xplico
	Comprehensive analysis and forensics	EnCASE FTK TCT
Reconstruction	Temporal, Functional, and Relational Analysis	

IV. OSINT/SOCMINT in Law Enforcement Agencies

https://inteltechniques.com/

Search Engines Tool

-Populate all-submit all

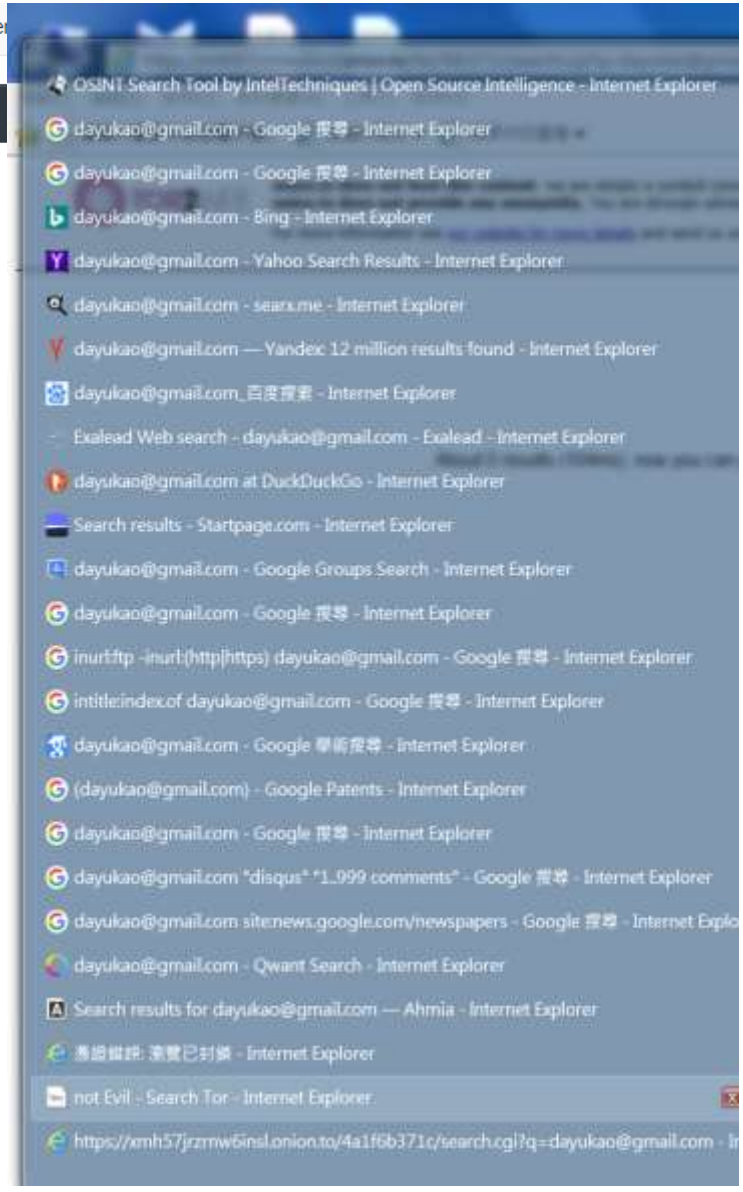
IntelTechniques OSINT Portal

Classic Ve

- Target Data:
- General Search:
  - Search Engines Tool
  - Search Engine Resources
- Email Address:
- Facebook Profile:
- Twitter Profile:
- Instagram Profile:
- Real Name:
- User Name:
- Telephone Number:
- Domain Name:
- IP Address:
- Video:
- Image:
- Documents:
- Business:
- Community:

Search Engines Tool

dayukao@gmail.com	Populate All	
dayukao@gmail.com	Google	
dayukao@gmail.com	Google Date	
dayukao@gmail.com	Bing	
dayukao@gmail.com	Yahoo	
dayukao@gmail.com	Searx	
dayukao@gmail.com	Yandex	
dayukao@gmail.com	Baidu	
dayukao@gmail.com	Exalead	
dayukao@gmail.com	Duck Go	
dayukao@gmail.com	StartPage	
dayukao@gmail.com	Newsgroups	
dayukao@gmail.com	Blogs	
dayukao@gmail.com	FTP Servers	
dayukao@gmail.com	Index Of	
dayukao@gmail.com	Scholar	
dayukao@gmail.com	Patents	
dayukao@gmail.com	News	
dayukao@gmail.com	Disqus	
dayukao@gmail.com	Newspapers	
dayukao@gmail.com	Wayback	
dayukao@gmail.com	Qwant	
dayukao@gmail.com	Ahmia	
dayukao@gmail.com	Onion.Cab	
dayukao@gmail.com	Not Evil	
dayukao@gmail.com	Torch	
dayukao@gmail.com	Submit All	(Allow Pop-ups)
Name or Topic	Go	Search Newspaper Archive (Google)
Name or Topic	Go	Search Newspaper Archive (Site)
Newspaper Name	Go	Newspaper Archive Collection



https://inteltechniques.com/

How can LEAs infer traits from the target's profiles?

- ✓ LEAs can look at
  - where they post from,
  - who they interact with,
  - how people are sharing on social media, and
  - what is reflected in their posts.

Law Enforcement on Social Network Sites

- ✓ **1. Internet Habitats** - Finding people
  - ➢ Look broadly for social networking sites
- ✓ **2. Snowball Sampling** - Social searches
  - ➢ Effective on many sites
- ✓ **3. Social Networking Analysis** - relational linkage
  - ➢ Content is king

Where

Who

How

What

Case Study: Habitats Through Social Network Data

- ✓ Information sharing: There are a substantial number of web forums, Internet relay chat (IRC) channels, blogs, and other online resources that facilitate information sharing between hackers across the world.
- ✓ Facilitate attacks: These resources range from legitimate, ethical discussions of hacking to serious forums where individuals buy, sell, and trade malware and stolen data to facilitate attacks and identity theft.
- ✓ Create software and tools: The top tier of hackers have the complex skills needed to create software and tools to facilitate complex automated attacks against variety of systems.

The Individual ‘s Habitats Where

- **law enforcement** has successfully used social media to investigate street gangs and other small organizations.
- When you have an individual target in mind but you do not know much about him, it can be helpful to understand information about the demographic groups that the target is a member of.

Interest groups investigation on social media sites

Where

- ✓ There is a lot of information available on social media to better understand organizations and communities of people.
- ✓ Learning these insights about groups of people may not reveal exactly what a specific investigation target is doing, but it can provide valuable insight into where that target might be found online, how he or she is using social media as a member of that group, and what topics and activities are of interest.
- ✓ Investigation of groups online can also lead to valuable intelligence about individuals within those groups who late become interesting.

Location Data

Where

The availability of location information can be found in geotagged posts, check-ins, and the embedded metadata of images and videos. What are the challenges to use location data on social media?

- ✓ Only about 30% of adults report including location information. (maybe more!)
- ✓ This is an opt-in process, not an automatic one.
- ✓ It is unlikely to become something we will see by default.

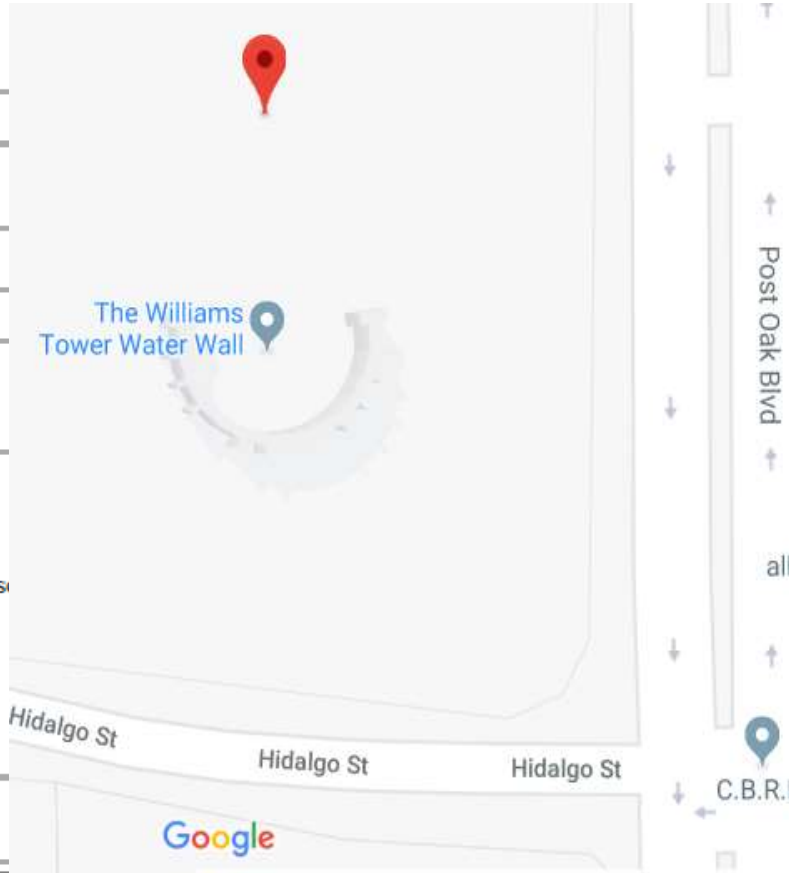
Exif Viewer Where

- Jeffrey's Exif Viewer is an online application (http://regex.info/exif.cgi) which allows us to see this Exif data present in any image file.

Basic Image Information

Target file: IMG_1004.JPG

Camera:	Apple iPhone 8 Plus
Lens:	iPhone 8 Plus back dual camera 3.99mm f/1.8 Shot at 4 mm
Exposure:	Auto exposure, Program AE, 1/1,116 sec, f/1.8, ISO 20
Flash:	Off, Did not fire
Date:	**January 12, 2019** 10:29:19AM (timezone not specified) (2 months, 8 days, 15 hours, 24 minutes, 53 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: **29° 44' 10"** North, **95° 27' 40.7"** West (29.736100, -95.461297) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (als see the Google Maps pane below) Altitude: 13 meters (43 feet) Camera Pointing: South-southwest Timezone guess from earthtools.org: 6 hours behind GMT
File:	**4,032 × 3,024** JPEG (**12.2** megapixels) 4,411,899 bytes (4.2 megabytes)



PEOPLE SEARCH Who

- Spokeo (http://www.spokeo.com)
- Pipl (https://pipl.com/)
- PeekYou (http://www.peekyou.com/)
- Yasni (http://www.yasni.com/)
- LittleSis (http://littlesis.org/)
- MarketVisual (http://www.marketvisual.com/)
- TheyRule (http://theyrule.net/)

Finding people on social media

Who

- ✓ **Non-authoritative answer:** Social media is not an authoritative information source.
- ✓ **Specific sites:** Search for people on the specific sites you care about.
- ✓ **Reuse usernames:** People often reuse their usernames.
- ✓ **Flexible search:** Searching for people through their associates and allowing for flexibility and some incorrectness in search results will help you discover targets in ways that you might not have initially expected.

Finding people on social media Who

- ✓ **Toolkits:** the social media sites' internal search/advanced Google search tools for finding people.
- ✓ **Names or usernames as input:** Social media search engines take names or possible usernames as input and then search across social media sites to find accounts.
- ✓ **Updated list services:** These services are constantly changing, and the companion website for the book has an updated list.

AUTHORSHIP ANALYSIS Who

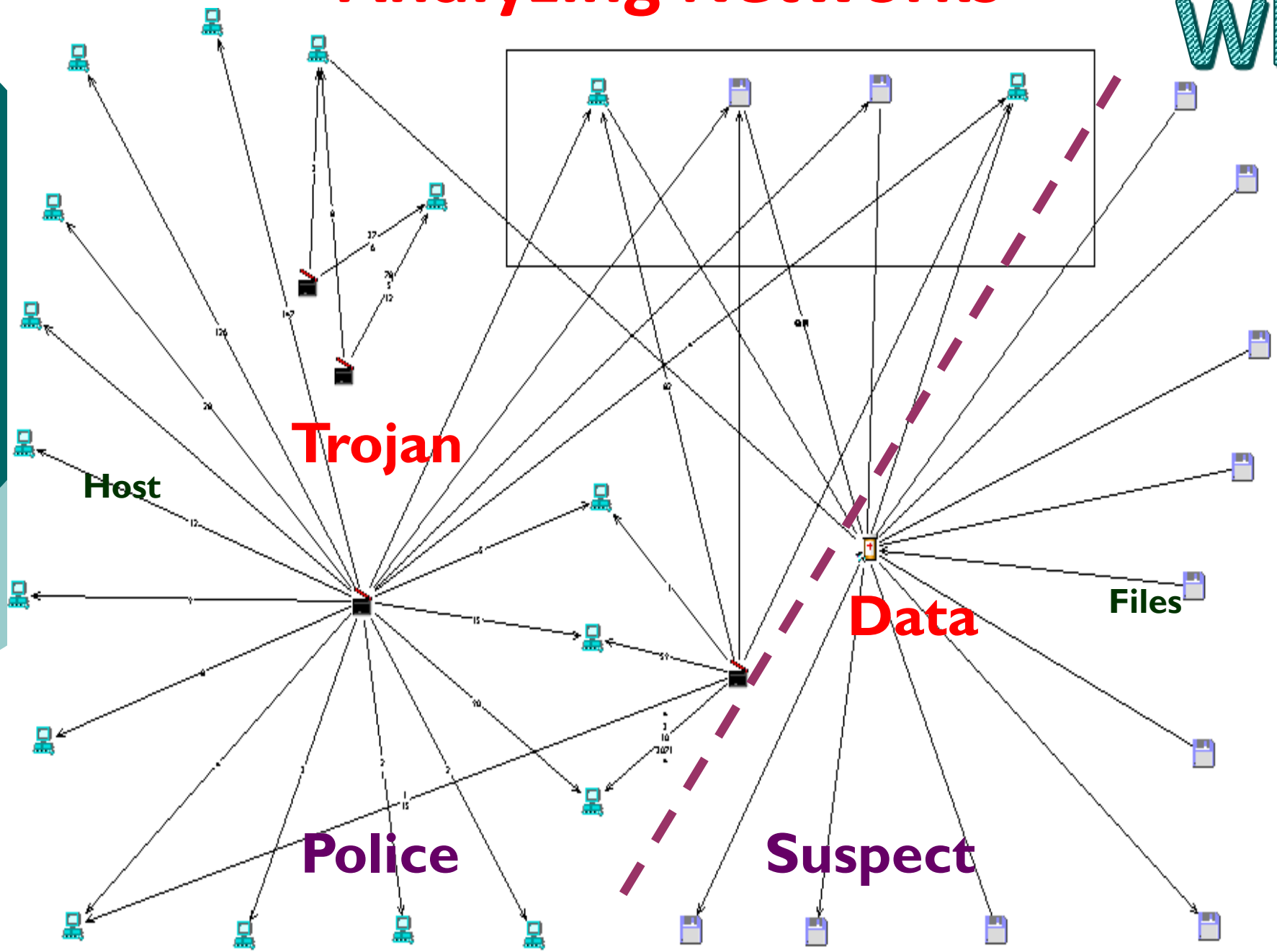
- When the attack consists of documents that have been written by an author, the main method for performing attribution is called authorship analysis.
- In authorship analysis, features from within the text are used to model the writing behavior of the author, and lead to a predictive model that can identify the author of a text.

Looking for Valuable Information Specific to The Target

Who

- ✓ The group characteristics can provide insights about where to start looking for information specific to the target.
- ✓ All types of organizations have presences on social media
- ✓ The activities, motivations, and online statements of the organization can be valuable background for understanding an individual target.

Analyzing Networks



Online Community Policing How

- ✓ Identify various forms of cybercrime: Identify when and how various forms of cybercrime occur.
- ✓ Promote reporting among citizens: Consider how real-world community meetings may be structured to promote reporting among citizens and demonstrate law enforcement's investigative capabilities to the community.
- ✓ Increase exposure of the agency: Help increase exposure of the law enforcement agency to various online populations.

Prosecution and Social Media

How

- ✓Evidence: Social media postings may be used as evidence of cybercrimes, such as cyberstalking, online threats and harassment, child pornography, and sexual assault.
- ✓Powerful tool: Social media is a powerful tool for law enforcement, for investigation and informing or collaborating with the public.

Clues What

- Clues help identify where attacks come from.
  - (1) Keyboard layout: determine the first language of the author
  - (2) Malware metadata
  - (3) Embedded fonts
  - (4) DNS registration: can be easily faked, but still lead to linking attacks
  - (5) Language, such as mistakes, which we outline in the next section on authorship analysis
  - (6) Remote administration tool (RAT) configuration, based on their personal preferences
  - (7) Behavior of the attack

What Contents on social media

- ✓ People can post basically anything on social media, but there are a few terms that are used across sites :
  - *Updates/posts*
  - *Comment/reply*
  - *Photos and videos*
  - *Social networks/friends/contacts*
  - *Metadata*

Online Community Policing How

- ✓ Identify various forms of cybercrime: Identify when and how various forms of cybercrime occur.
- ✓ Promote reporting among citizens: Consider how real-world community meetings may be structured to promote reporting among citizens and demonstrate law enforcement's investigative capabilities to the community.
- ✓ Increase exposure of the agency: Help increase exposure of the law enforcement agency to various online populations.

What does make social media a powerful tool for investigators?

How

Social media sites are full of:

- ✓ demographic information;
- ✓ lists of friends, family, and associates;
- ✓ logs of activities, preferences, and favorites;
- ✓ maps showing places a person goes and how frequently;
- ✓ time-stamped posts that indicate where a person was and when; and
- ✓ the content of the posts themselves, where people detail their thoughts, feelings, and ideas.

What kinds of skills does the police need to search, navigate, and collect information on social media?

How

- ✓The police will have the skills you need to search, navigate, and collect information from many sources.
- ✓The police should learn lessons for the use of social media: being mindful of what you put online, what to expect (or not) in terms of privacy, and how to manage your own online identity.

How

What are the standard investigation techniques in SNSs?

- ✓ Locate a target: trying to find the target themselves, and find their associates.
- ✓ Investigator: keep a low social media profile
- ✓ Target profiles: They use the same email addresses, same usernames, and same profile photos over and over.

Conclusions

- ✓ Law enforcement officials are exploiting social media to
  - investigate crime,
  - identify perpetrators, and
  - build cases for prosecution.
- ➢ A promising approach to ensure efficient and effective strategy is collaborations between various private and public organizations.
- ➢ Security agencies, intelligence agencies and LEAs can apply similar techniques.

中央警察大學
CENTRAL POLICE UNIVERSITY

- **Don't believe everything you are told!**
- **Ask "Where is the EVIDENCE?"**

Dayu Kao (Ph. D.)
Associate Professor
Central Police University, Taiwan
E-mail: camel@mail.cpu.edu.tw

Any comments are appreciated.

Thanks for your listening.