Cyber Crime and Cyber Forensics for Criminal Law Practitioners

Steven Chabinsky

General Counsel and Chief Risk Officer, CrowdStrike

CROWDSTRIKE

Presented 20 May 2014, Continuing Legal Education & Training, U.S. Court of Appeals for the Armed Forces

Today's Agenda

4:00pm – 5:00pm

- Defining "Cyber"
- Exploring the Cyber Threat Actor Landscape
- Legal Considerations for Search and Seizure
- Overview of Computer Forensics
- Q&A – if we don't have time for all questions, contact me:
  - Steve.Chabinsky@CrowdStrike.com

1 Hour Goal: General Knowledge, Specific Resources

Defining “Cyber”

and

Exploring the Cyber Threat Actor Landscape

Cyber: What is it?

- The military is becoming 100% reliant upon vulnerable technologies to:
  - Communicate, whether internally, with government partners, or with the public (email, VoIP, social media, websites)
  - Store sensitive information up to the Top Secret level, as well as unclassified data about personnel.
  - Procuring/Delivery of products and services (think USTRANSCOM for starters)
  - Manufacture equipment, many of these products also contain computer chips (including biomedical devices)
  - Control industrial systems, including critical infrastructure

Exploring the Cyber Threat Actor Landscape

WHO?

- Spies
- Criminals
- Warriors
- Terrorists

WHAT?

- Confidentiality
- Integrity
- Availability

of information
and
Technology enabled systems

Where/When?

"Everything,
All the time"

-the Eagles

Life in the Fast Lane

HOW?

- Remote Access
- Close Access
- Insider Access
- Supply Chain

Why? If you're the bad guy, why not?!?

What's a System? It's not just "data"

- Industrial Control Systems
  - Stuxnet
  - Aurora Generator Test
- Transportation
  - Hacking cars!

- Biomedical Devices
  - Hacking insulin injection pumps!
  - VPOTUS's Pacemaker?

Victims? Private and "Closed" Classified Systems

CSO
SECURITY AND RISK

Print Close Window

From: www.csoonline.com

Costly cyberespionage on 'relentless upward trend'

Defense Security Service report says attacks were up 75% in one year, with new focus on space and military technology

by Taylor Armerding, CSO

December 18, 2012

Cyberespionage is nothing new. So a report from the
countries to steal U.S. technology, intellectual proper
like just more of the same.

DSS Director Stanley L. Sims said it is more of the sa
old cyberespionage technology is now more sophist
Technologies: A Trend Analysis of Reporting from D
sensitive or classified information and technology in

While the percentage of attacks from different region
in the data is the relentless upward trend," the report

"During fiscal year 2011, the persistent, pervasive, a
noteworthy, and the pattern became even more firm

It noted that attackers from East Asia and the Pacific,
Korea, New Zealand, the Philippines and Taiwan, w
– specifically "radiation-hardened" microelectronics
to withstand radiation in high-altitude flight, space op

How much this costs the U.S. is difficult to quantify. A
estimated that economic espionage had cost the nat
year, which ended Sept. 30. That is obviously a significant amount of money, but in an economy with a gross domestic product of about $14.6 trillion, it is barely a rounding error.

The Washington Post

NEWS | LOCAL | POLITICS | SPORTS | OPINIONS | BUSINESS | ARTS & LIVING | GOING OUT GUIDE | JOBS | CARS | REAL ESTATE | SHOPPING

Defense official discloses cyberattack

By Ellen Nakashima
Tuesday, August 24, 2010; 9:26 PM

Now it is official: The most significant breach of U.S. military computers was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in 2008.

In an article to be published Wednesday discussing the Pentagon's cyberstrategy, Deputy Defense Secretary William J. Lynn III says malicious code placed on the drive by a foreign intelligence agency uploaded itself onto a network run by the U.S. military's Central Command.

"That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control," he says in the Foreign Affairs article.

"It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary."

CrowdStrike: 2013 Global Threat Report

PRC actors remain the world's most active and persistent perpetrators of economic espionage.

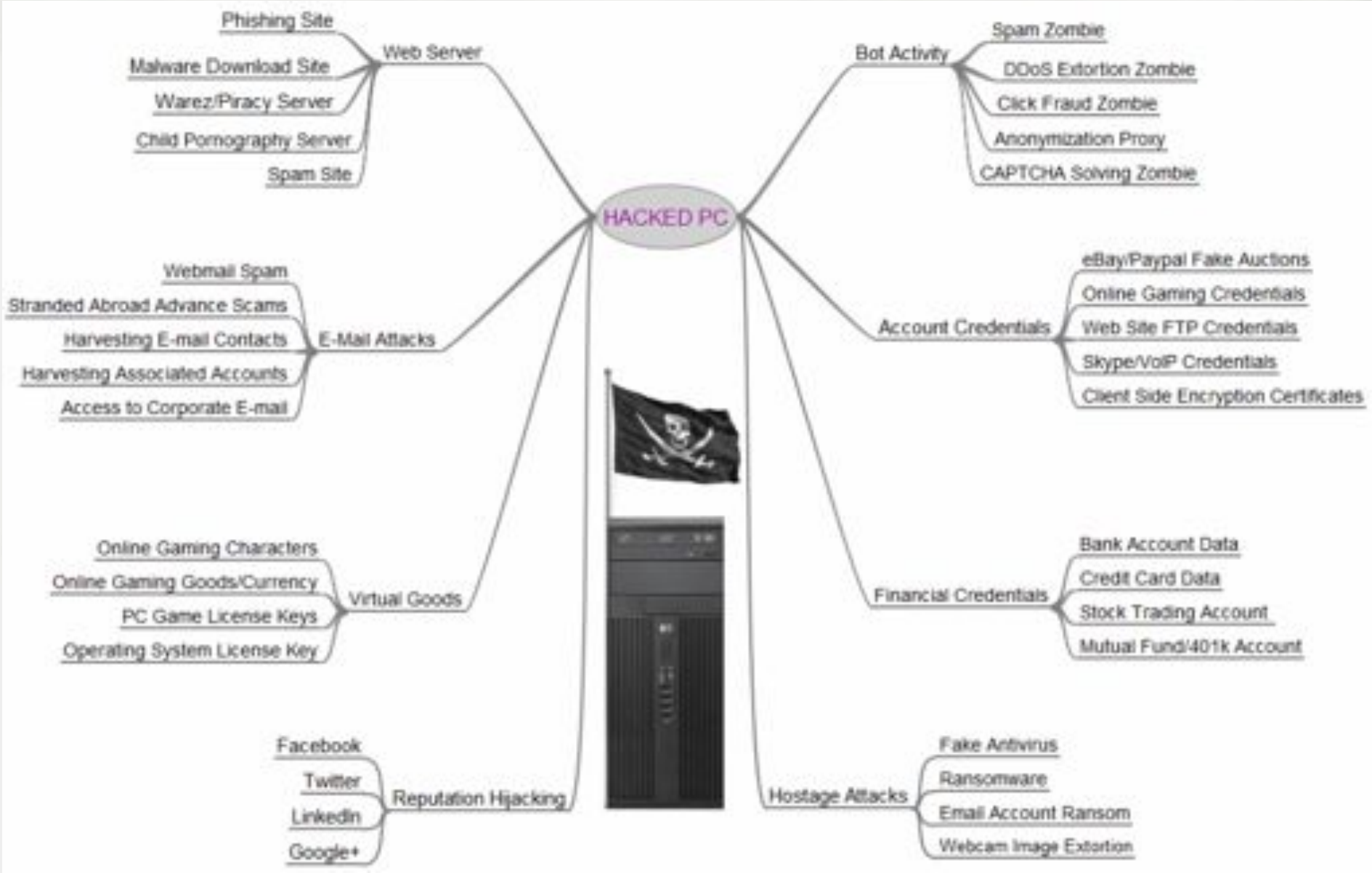
But, the Russians and others also are in the economic espionage game.

Source: http://www.crowdstrike.com/global-threat/

Organized Cybercrime:

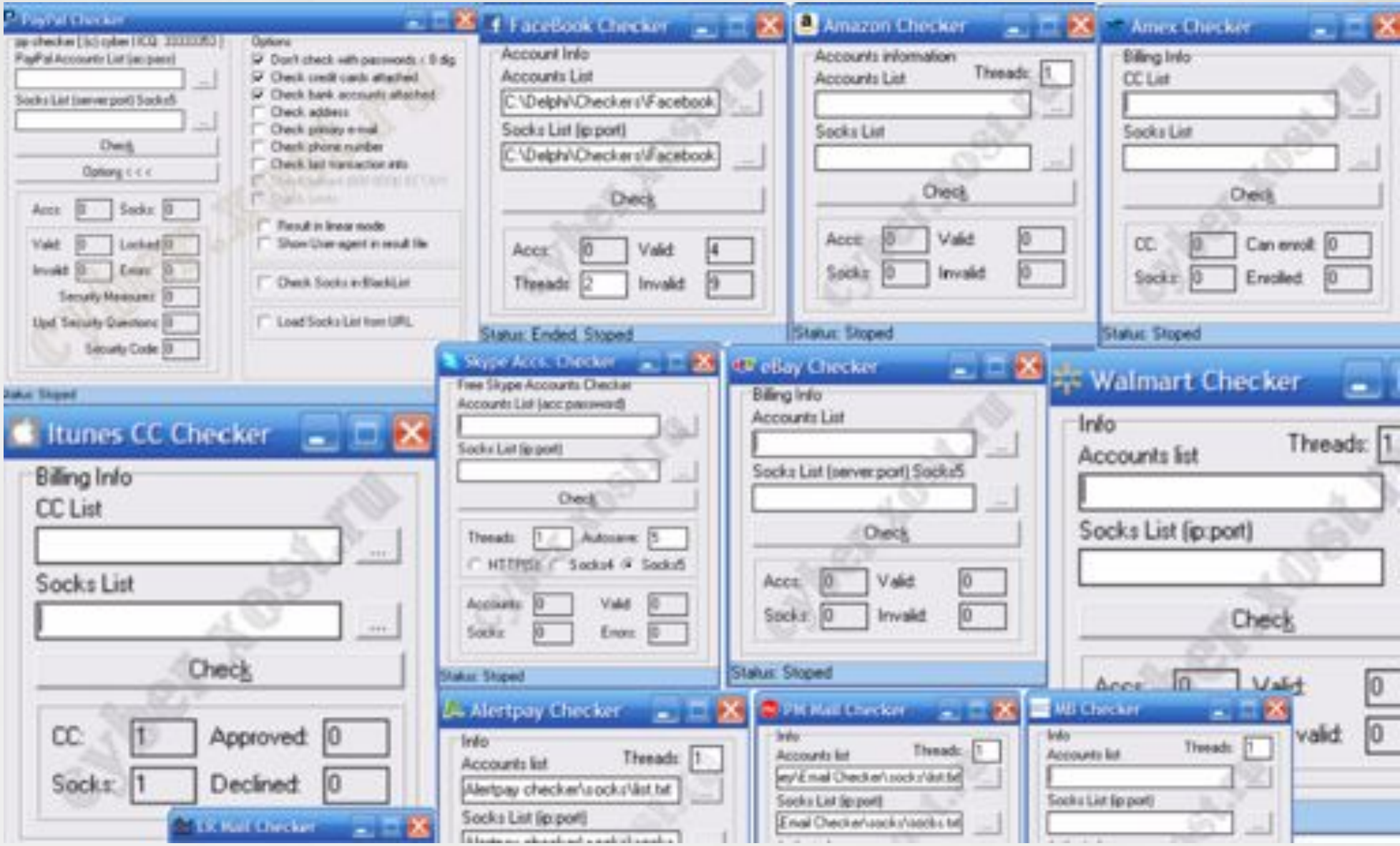
Graphic by:
Brian Krebs

Source:
http://krebsonsecurity.com



Organized Cybercrime:

Source:
http://krebsonsecurity.com



Cybercrime: Really is Organized

10 specializations in organized cyber crime:

1. Coders/Programmers
2. Distributors/Vendors
3. Techies
4. Hackers
5. Fraudsters
6. Hosters
7. Cashers
8. Money Mules
9. Tellers
10. Leaders

Cyber Terrorism


Sociology Working Papers
Paper Number 2007-10

Engineers of Jihad

Diego Gambetta
Steffen Hertog

Department of Sociology
University of Oxford
Manor Road
Oxford OX1 3UQ
www.sociology.ox.ac.uk/swp.html

Oxford Study: compiled a list of 404 members of violent Islamist groups

Engineers are strongly over-represented among graduates in violent Islamic groups

Cyber War?

- Alleged Russian use in conflicts with Estonia (2007) and Georgia (2008)
- Alleged North Korean DDoS against U.S. and South Korea (2009)
- Alleged U.S. use of Stuxnet in nuclear enrichment standoff with Iran (discovered 2010)

Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate

All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

—Article 2(4), Charter of the United Nations

Legal Considerations for Search and Seizure

USDOJ CCIPS: The Experts

Great Free Resources available at www.cybercrime.gov

CCIPS DOCUMENTS AND REPORTS

Manuals

- Prosecuting Computer Crimes manual
- Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual
- Prosecuting Intellectual Property Crimes manual
- IP Victim Guide
- Digital Forensic Analysis Methodology Flowchart (August 22, 2007)

White Papers

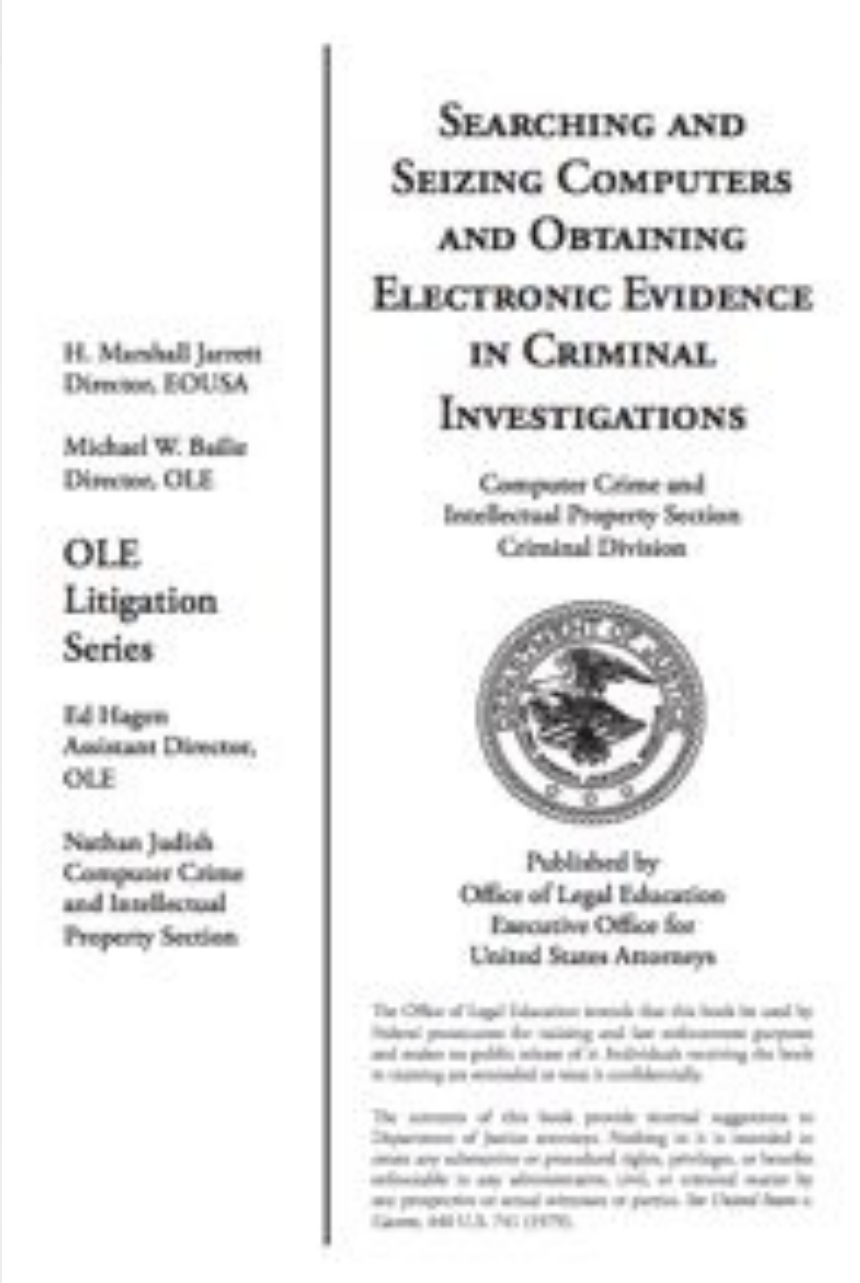
- Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)

Searching & Seizing Computers

Source www.cybercrime.gov

Over 200 pages long (plus best Appendix ever!)

- Searching Without a Warrant
- **Searching With a Warrant**
- Preserving and Obtaining stored data from special 3rd parties (18 USC § 2703)
  - Electronic Communication Service
  - Remote Computing Service
- Surveillance (18 USC § 3121; 18 USC § 2511)
  - Pen Register/Trap & Trace (incl. cell-site)
  - Full Content
- Evidence
  - Authentication



H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director, OLE

Nathan Judish
Computer Crime and Intellectual Property Section

SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

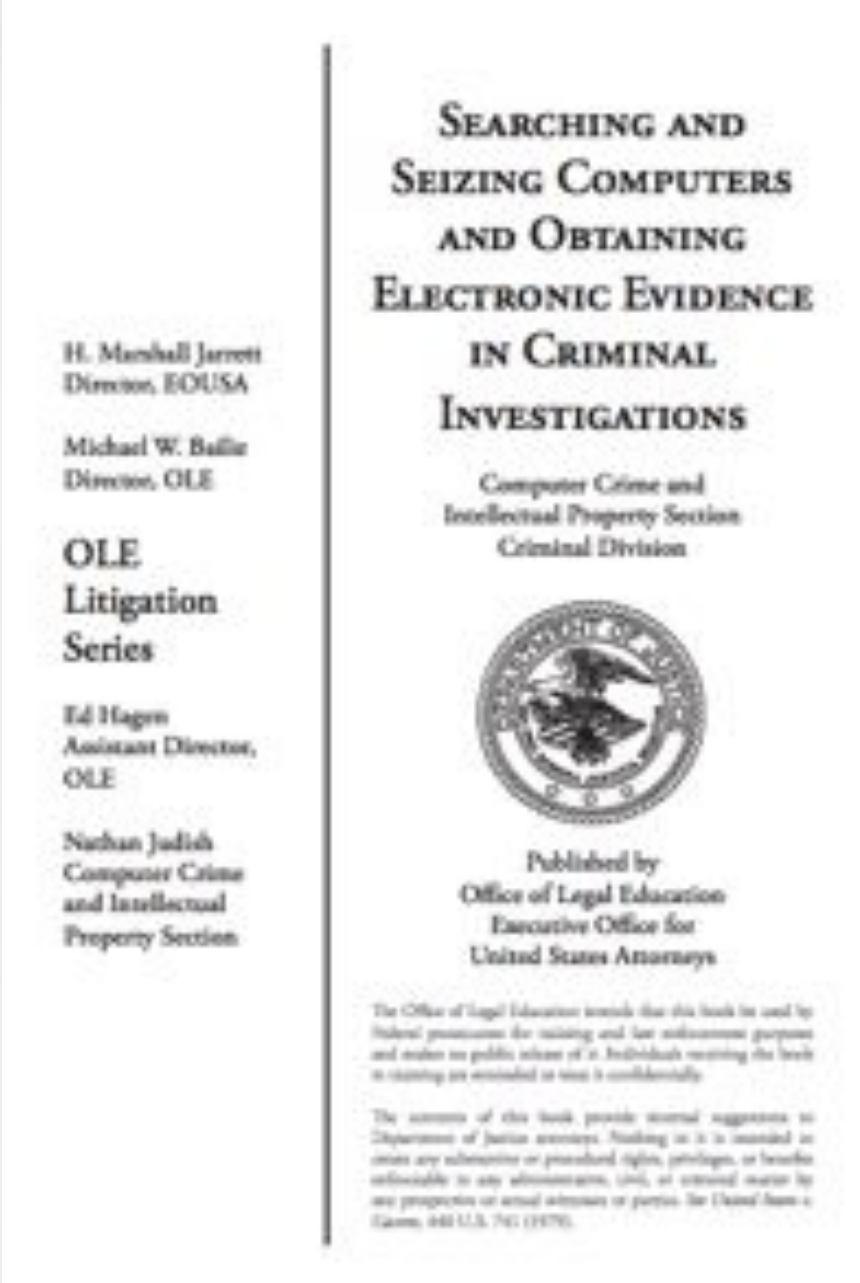
Computer Crime and Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

Searching With a Warrant

Source: www.cybercrime.gov

- Search Strategy
- Drafting Affidavits, Applications, and Warrants
  - Describing what is to be seized with particularity
  - The need for imaging and off-site examination
  - Keeping your options open for search techniques
  - Delayed notification requirements
  - Potential need for multiple warrants
- Forensic Analysis: legal aspects
  - Two-Stage search
  - Commingled records
  - Use of forensic software in analysis
  - Changing focus/Need for new warrant
  - Time limitations
  - Rule 41(f) Inventory
- Special rules: Privacy Protection Act (journalists/authors); 28 CFR § 59.4(b) regulations relating to doctors, lawyers, clergy.



H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director, OLE

Nathan Judish
Computer Crime and Intellectual Property Section

SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

Computer Crime and Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

Important/Sobering Thought:

(Release Point 113-100+u1)

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

This title was enacted by act June 25, 1948, ch. 645, §1, 62 Stat. 683

Part		Sec.
I.	Crimes	1
II.	Criminal Procedure	3001
III.	Prisons and Prisoners	4001
IV.	Correction of Youthful Offenders	5001
V.	Immunity of Witnesses	6001

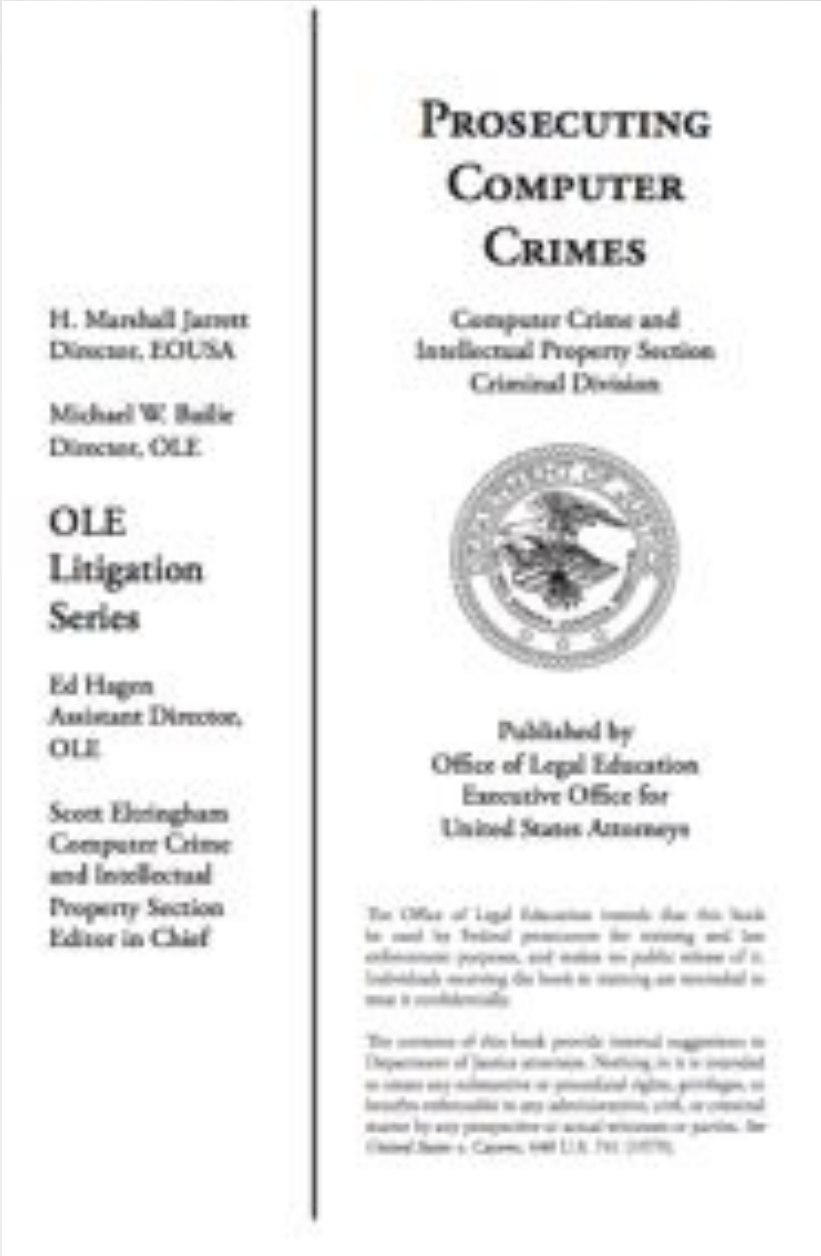
Stored Comms Act
Wiretap Laws

Q: Why are some federal law enforcement <u>investigative authorities</u> located in the "Crimes" part of Title 18 of the United States Code, rather than in the "Criminal Procedure" part?

What are Computer Crimes?

Source: www.cybercrime.gov

- Computer Fraud & Abuse Act (18 USC § 1030)
- Wiretap Act (18 USC § 2511)
- Pen/Trap (18 USC § 3121)
- Stored Communications (18 USC § 2701)
- Identity Theft (18 USC § 1028)
- Access Device Fraud (18 USC § 1029)
- Spam (18 USC § 1037)
- Wire Fraud (18 USC 1343)
- Communication Interference (18 USC § 1362)



H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE
Litigation
Series

Ed Hagen
Assistant Director,
OLE

Scott Eltringham
Computer Crime
and Intellectual
Property Section
Editor in Chief

PROSECUTING
COMPUTER
CRIMES

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

18 USC 1029: Access Devices (passwords)

- Prohibits certain activities relating to the use, production, or trafficking in access devices with intent to defraud:
  - -- an access device refers to any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)

18 USC 1030: National Security Information

1030(a)(1) Summary (Felony)

1. Knowingly access computer without or in excess of authorization
2. obtain national security information
3. reason to believe the information could injure the U.S. or benefit a foreign nation
4. willful communication, delivery, transmission (or attempt)

   OR

   willful retention of the information

18 USC 1030: Unauthorized Access

1030(a)(2) Summary (Misd.)

1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from

   financial records of financial institution or consumer reporting agency

   OR

   the U.S. government

   OR

   a protected computer

↓

(Felony)

5. committed for commercial advantage or private financial gain

   OR

   committed in furtherance of any criminal or tortious act

   OR

   the value of the information obtained exceeds $5,000

18 USC 1030: USG Computers and Fraud

1030(a)(3) Summary (Misd.)

1. Intentionally access
2. without authorization
3. a nonpublic computer of the U.S. that was exclusively for the use of U.S. or was used by or for U.S.
4. affected U.S. use of computer

1030(a)(4) Summary (Felony)

1. Knowingly access a protected computer without or in excess of authorization
2. with intent to defraud
3. access furthered the intended fraud
4. obtained anything of value, including use if value exceeded $5000

18 USC 1030: Causing Damage

Misdemeanor

Summary of (a)(5)(A)	Summary of (a)(5)(B)	Summary of (a)(5)(C)
1. Knowingly cause transmission of a program, information, code, or command 2. intentionally cause damage to protected computer without authorization	1. Intentionally access a protected computer without authorization 2. recklessly cause damage	1. Intentionally access a protected computer without authorization 2. cause damage 3. cause loss

Felony

3. resulting in loss of $1,000 during 1 year
   OR
   modifies medical care of a person
   OR
   causes physical injury
   OR
   threatens public health or safety
   OR
   damages systems used by or for government entity for administration of justice, national defense, or national security
   OR
   damages affect 10 or more protected computers during 1 year

18 USC 1030: Penalties

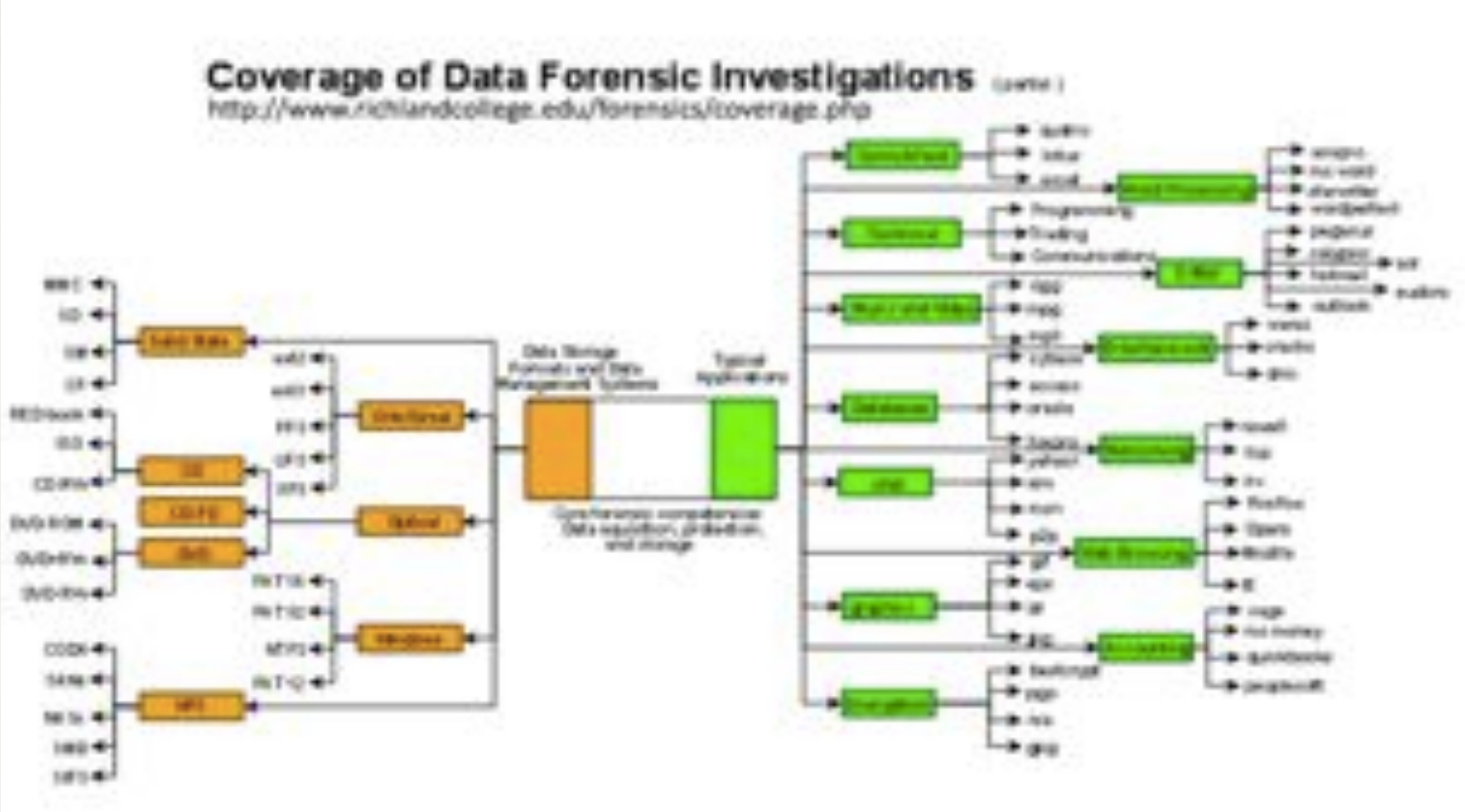
Table 1. Summary of CFAA Penalties

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parentheses.

Computer Forensics

Forensics: Complicated enough to start with . . .

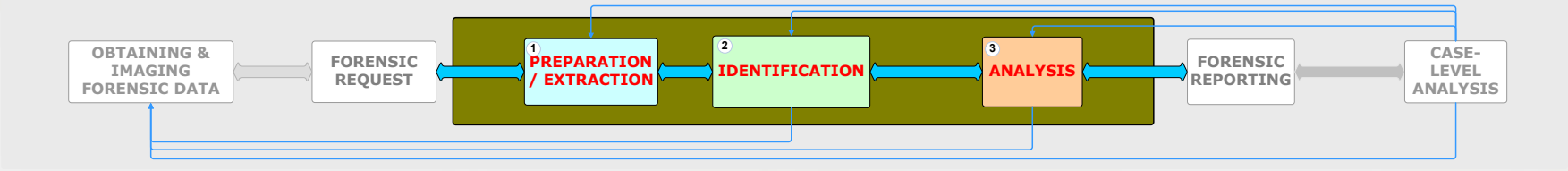


Now add legal:

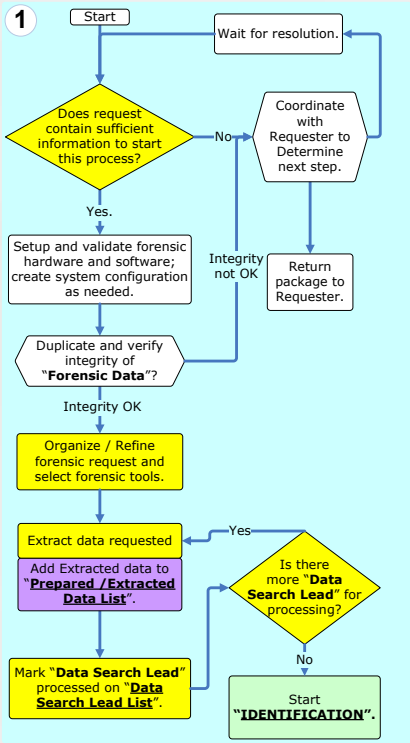
DIGITAL FORENSIC ANALYSIS METHODOLOGY

Last Updated: August 22, 2007

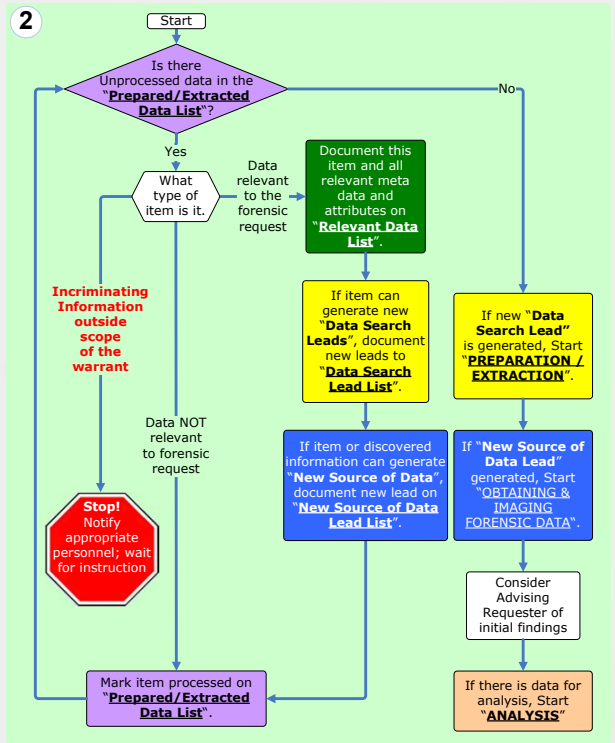
PROCESS OVERVIEW



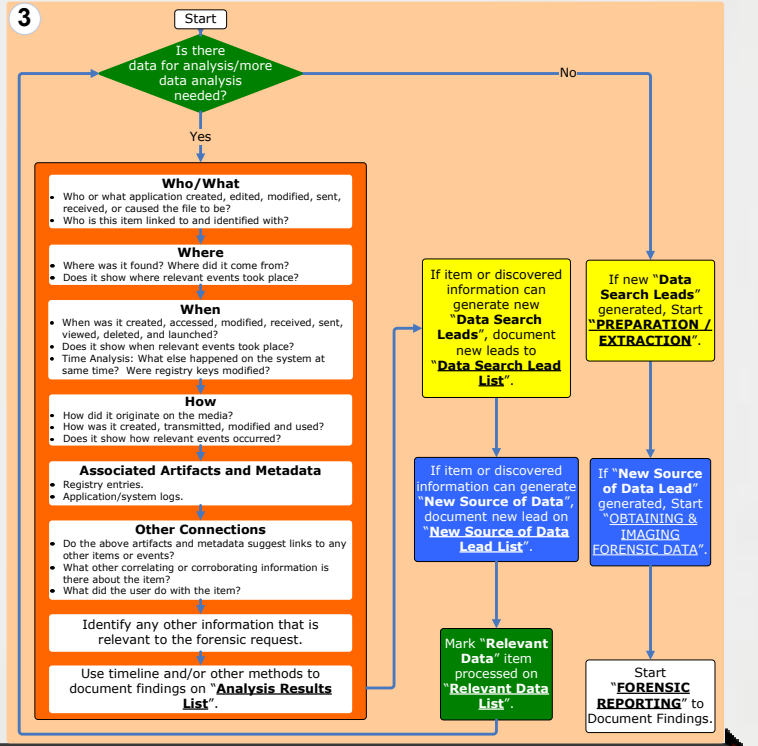
PREPARATION / EXTRACTION



IDENTIFICATION



ANALYSIS



Return On Investment (Determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)

LISTS

Search Leads

Data Search Leads	Comments/Notes/Messages
Generally this involves opening a case file in the tool of choice and importing forensic image file. This could also include recreating a network environment or database to mimic the original environment. Sample Data Search Leads: • Identify and extract all email and deleted items. • Search media for evidence of child pornography. • Configure and load seized database for data mining. • Recover all deleted files and index drive for review by case agent/forensic examiner.	Use this section as needed. Sample Note: • Please notify case agent when forensic data preparation is completed.

Extracted Data

Prepared / Extracted Data	Comments/Notes/Messages
Prepared / Extracted Data List is a list of items that are prepared or extracted to allow identification of Data pertaining to the forensic request. Sample Prepared / Extracted Data items: • Processed hard drive image using Encase or FTK to allow a case agent to triage the contents. • Exported registry files and installed registry viewer to allow a forensic examiner to examine registry entries. • A seized database files is loaded on a database server ready for data mining.	Use this section as needed. Sample Message: • Numerous files located in c:\movies directory have .avi extensions but are actually Excel spreadsheets.

Relevant Data

Relevant Data	Comments/Notes/Messages
Relevant Data List is a list of data that is relevant to the forensic request. For example: • If the forensic request is finding information relating credit card fraud, any credit card number, image of credit card, emails discussing making credit card, web cache that shows the date, time and search term used to find credit card number program, Etc are Relevant Data as evidence. In addition, Victim information retrieved is also Relevant Data for purpose of victim notification.	Use this section as needed. Sample Note: • Attachment in Outlook.pst>message05 has a virus in it. Make sure an anti-virus software is installed before exporting and opening it. • Identified and recovered 12 emails detailing plan to commit crime.

New Data Source Leads

New Source of Data Leads	Comments/Notes/Messages
New Source of Data Lead List is a list of data that should be obtained to corroborate or further investigative efforts. Sample New Source of Data Leads: • Email address: 3doe@email.com. • Server logs from FTP server. • Subscriber information for an IP address. • Transaction logs from server.	This is self explanatory. Use this section as needed. Sample Notes: During forensic analysis of subject John Doe's hard drive image on credit card fraud, a email message revealed that Jane Doe asks John Doe for payment on credit card printing machine.

Analysis Results

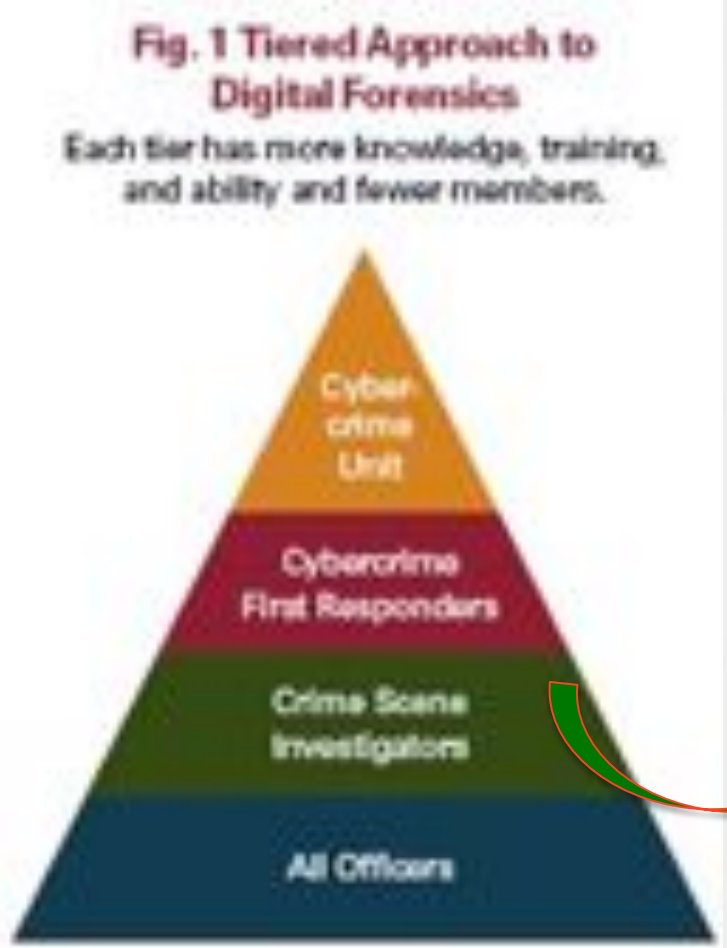
Analysis Results	Comments/Notes/Messages
Analysis Result List is a list of meaningful data that answers the who, what, when, where and how questions in satisfying the forensic request. Sample Analysis Results: 1. \Windows\$NtUninstallKB887472$\10.dat \data\sentbox.dbx\message5.eml \Special Tools\stegano.exe Modified and emailed img to ... 1/4/03 1/5/03	Use this section as needed Sample Notes: 1. 10.dat, message5.eml and stegano.exe show that John Doe used steganography tool to hides a ten dollar image in 10.dat at 11:03 PM 01/05/03 and emailed it to Jane Doe at 11:10 PM 01/05/03.

Department of Justice (DOJ)
Computer Crime and Intellectual Property Section (CCIPS)
Cybercrime Lab
http://www.cybercrime.gov
(202) 514-1026

NW3C Training Approach: Break it into 4 Tiers. . .

- Identify all types of digital storage media
- Prepare affidavits related to digital evidence
- Avoid inadvertent alteration of digital evidence
- Employ faraday cage to secure small digital devices
- Understand how to effectively integrate digital evidence into investigations

NW3C Training Approach: Break it into 4 Tiers. . .



- Identify, locate, document, and disable wireless networks
- Document hardware configurations
- Identify indicators of forensics countermeasures
- Properly package hardware and storage media

NW3C Training Approach: Break it into 4 Tiers. . .

- Remove hard drives from desktop and laptop computers
- Preview hard drives in forensically sound manner using hardware write-blocker
- Examine storage media in forensically sound manner
- Obtain certification in at least one automated forensic software tool

NW3C Training Approach: Break it into 4 Tiers. . .

- Conduct full on-scene examinations using mobile computer forensics laboratory
- Conduct live examinations to preserve volatile memory and defeat countermeasures
- Serve as subject matter experts for police department and courts
- Conduct strategic research and tactical advanced data recovery in fixed laboratory
- Examine exotic media and multiple operating systems
- Obtain certification in all major forensic software tools

Closing Thoughts

Cybercrime and Cyber Forensics

- Cybercrime is here to stay
  - Harms to confidentiality, integrity, and availability will increasingly impact military administrative matters, logistics, defenses, and warfighting functions.
- Cyber investigations and forensics
  - Are increasingly required for internal personnel matters
  - Are increasingly required for criminal and espionage investigations
  - May be required to properly *categorize and attribute* acts of terrorism and war

Thank you for your service!

CROWDSTRIKE

Steve.Chabinsky@CrowdStrike.com

(202) 870-1442

Follow me on  : @StevenChabinsky