

# Legal Aspects of Investigating & Prosecuting Computer Crimes

#### 6<sup>th</sup> Annual MSIA Graduate Security Conference Norwich University Workshop: June 10, 2009 M. E. Kabay, PhD, CISSP-ISSMP Maito:mekabay@gmail.com Y: 802.479.7937 Masce Prof Information Assurance, School of Business & Management Norwich University, Vermont <u>http://www.mekabay.com</u> SLIDES AVAILABLE ONLINE AT <u>http://tinyurl.com/I5vusf</u>

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### **Topics: Fire Hose Time**

Introduction (slides 1:24)

Hour 2

Hour 3

Hour 1 T > Search Warrants (25:49=25)

Warrantless Seizure of Evidence (50:73=24)

Electronic Crime Scene Investigation (74:102=29)

Analysis of Digital Evidence (103:143=41)

Using Seized Materials & Results in Evidence (144:160=17)







#### **Disclaimers**

- Instructor is not a lawyer.
- This is not legal advice.
- For legal advice, consult an attorney specializing in this practice area.
- This overview is NOT an in-depth discussion of the entire field of IP law: it is an overview to remind students of key issues. We won't be discussing all the slides in detail.
- You may download the PPT file from <u>http://www.mekabay.com/courses/academic/norwich/msia/ipcc.ppt</u> or <u>http://tinyurl.com/l5vusf</u>

#### Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### Introduction

#### Goals

- Recommended Texts
- Recent Internet Usage Statistics
- Tracing a Suspect on the Internet
- Proactive vs Reactive strategies
- Online Stings: Entrapment?







#### Goals

Review (or introduce) basic concepts Manage evidence **Preserve Present** Law and procedures useful to Law enforcement officials Information security professionals Interest participants in further / deeper study



## **Recommended Texts**

- Burgunder, L. (2007). Legal Aspects of Managing Technology, Fourth Edition. Thomson West Legal Studies in Business (ISBN 0-324-39973-1). xv + 683. Index.
- Moore, R. (2005). Cybercrime: Investigating High-Technology Computer Crime. Matthew Bender & Co. (ISBN 1-59345-303-5). xii + 258. Index.
- Clifford, R. D. (2006). Cybercrime: Investigation, Prosecution and Defense of a Computer-Related Crime, Second Edition. Carolina Academic Press (ISBN 1-59460-150-X). xii + 282. Index.

**These texts are used in the CJ341 Cyberlaw** & Cybercrime course at Norwich University.





#### **Recent Internet Usage Stats**

http://www.internetworldstats.com/stats.htm



#### INTERNET USAGE STATISTICS The Internet Big Picture

World Internet Users and Population Stats

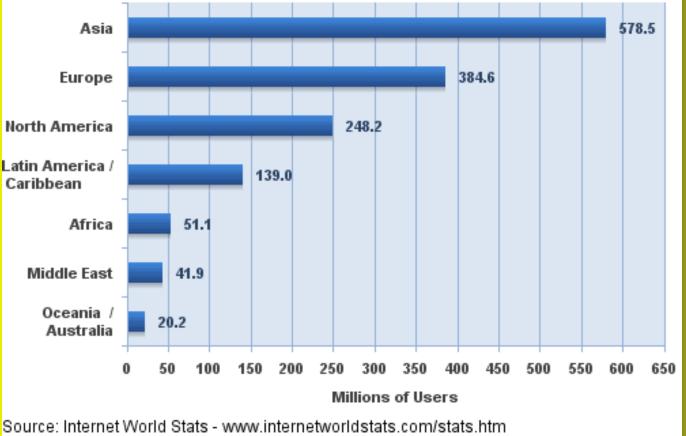
WORL	D INTERNE	ET USAGE AN	ND POPULA	TION STATE	STICS	
World Regions	Population ( 2008 Est.)	Internet Users Dec/31, 2000	Internet Usage, Latest Data		Usage % of World	Usage Growth 2000-2008
<u>Africa</u>	955,206,348	4,514,400	51,065,630	5.3 %	3.5 %	1,031.2 %
Asia	3,776,181,949	114,304,000	578,538,257	15.3 %	39.5 %	406.1 %
Europe	800,401,065	105,096,093	384,633,765	48.1 %	26.3 %	266.0 %
Middle East	197,090,443	3,284,800	41,939,200	21.3 %	2.9 %	1,176.8 %
North America	337,167,248	108,096,800	248,241,969	73.6 %	17.0 %	129.6 %
Latin America/Caribbean	576,091,673	18,068,919	139,009,209	24.1 %	9.5 %	669.3 %
Oceania / Australia	33,981,562	7,620,480	20,204,331	59.5 %	1.4 %	165.1 %
WORLD TOTAL	6,676,120,288	360,985,492	1,463,632,361	21.9 %	100.0 %	305.5 %

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2008. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the <u>US Census Bureau</u>. (4) Internet usage information comes from data published by <u>Nielsen/NetRatings</u>, by the <u>International Telecommunications Union</u>, by local NIC, and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the <u>Site Surfing Guide</u>, now in ten languages. (6) Information in this site may be cited, giving the due credit to <u>www.internetworldstats.com</u>. Copyright © 2001 - 2008, Miniwatts Marketing Group. All rights reserved worldwide.



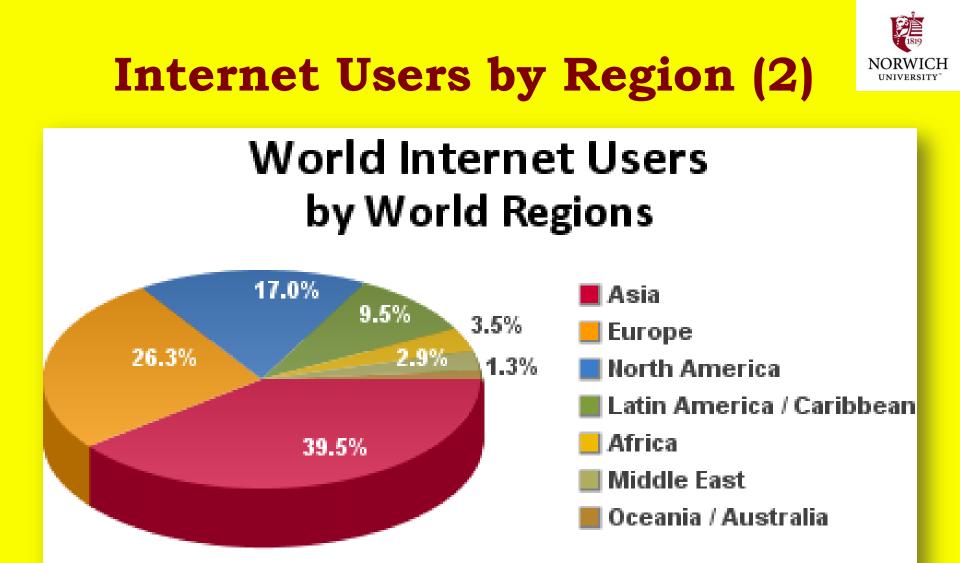
#### **Internet Users by Region (1)**

#### Internet Users in the World by Geographic Regions



Estimated Internet users is 1,463,632,361 for Q2 2008 Copyright © 2008, Miniwatts Marketing Group

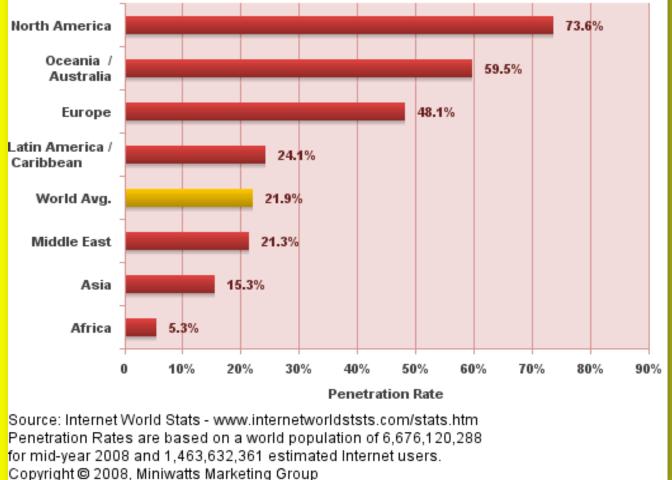
Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.



Source: Internet World Stats - www.internetworldstats.com/stats.htm 1,463,632,361 Internet users for June 30, 2008 Copyright © 2008, Miniwatts Marketing Group

#### Internet Penetration Rates by Region

World Internet Penetration Rates by Geographic Regions UNIVERSITY



Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Tracing a Suspect on the Internet



The Dynamic IP Address

- Locating the Host
- DNS Lookup
- whois.net
- SamSpade Program
- Locating Information from E-Mails
- E-Mail Headers





#### **The Dynamic IP Address**

- Suspect may have own connection to 'Net Has permanent IP address
  - □E.g., gmail.com has IP address 64.233.171.83
  - □Norwich.edu is 192.149.109.197
- Or suspect connects to Internet via ISP
   DHCP (Dynamic Host Configuration Protocol)
   User is assigned temporary "dynamic" address
   Re-used and not unique
  - □Logged by ISP for some time (days to forever)
  - Must absolutely get cooperation of ISP and obtain records (if they still exist) under subpoena

What would an unsecured WAP do to this linkage? The records will show match of dynamic address to user's modem's MAC (media access control) address and from there to the assigned modem location, authorized user, address and so on



#### **Locating the Host**

ICANN (Internet Corporation for Assigned Names and Numbers) <u>http://www.icann.org/</u>

□Global coordination of IP address assignments

□Defines rules for domain names

- InterNIC < <u>http://www.icann.org/</u> > points to registrars around world
  - □See lists e.g., <u>http://www.internic.net/origin.html</u>

□Australia has 13 registrars

- □Canada has 152
- **US has 562**



#### **DNS Lookup**

- WHOIS functions available online from each registrar
  - □But <u>http://www.whois.net/</u> works with all registrars (see next page)
- Many other tools available online for DNS lookup
- SamSpade tool and service from <u>http://www.samspade.org</u> can find many records as well as providing additional functions (see page after next)
- Info in registry may be false or out of date Often see dummy phone numbers in DNS

## **Looking Up DNS Information (1)**



#### Welcome to Whois.net!

Login | Register

NORV

Whois domain name look keyword search, deleted	cup, available domain names, domai domains:	in	Explanation of Tool:
WHOIS Lookup	norwich .edu 💌	Go!	Lookup registration data for domains.
Search by domain or keyword		Go!	Search domains and lookup whois information. Research and protect trademarks.
Domain Lookup	.com 💌	Go!	Find available domains.
Search through deleted domains		Go!	Find previously registered domains that are now available.



# **Looking Up DNS Information (2)**

Domain Name: NORWICH.EDU **Registrant:** Norwich University 158 Harmon Drive Juckett Hall / Computer Service Northfield, VT 05663 UNITED STATES Administrative Contact: NORWICH DNS ADMINISTRATOR Technical Contact: ... Name Servers: NS.NORWICH.EDU 192.149.109.19 A. DNS. TDS. NET



👷 Spo	ide - [who	ois www	norwich.edu, finished]	- @ -	
🏘 Ei	le <u>E</u> dit	<u>V</u> iew	<u>W</u> indow <u>B</u> asics <u>T</u> ools <u>H</u> elp		
	.norwich.e		🗸 🐟 🛛 🔁 10 🗧 🥙 Manic	Ţ Pět	🗸 🖓 NORWICH
<b>1</b>	10/12/(	St Sp	de - [whois tds.net, finished]		
3	.edu is		e <u>E</u> dit <u>V</u> iew <u>W</u> indow <u>B</u> asics <u>T</u> ools <u>H</u> elp		_ B ×
🚱 Log	whois -	tds.n	t ⇒ _ <b>0 10 </b>	ic .net	
		😪 Log	Registrant:		<b>_</b>
Copy	Whois (		TDS Telecom		
B		😵 Log	525 Junction Road		
	Domain	Ē	Madison, WI 53717		
	with ma	Сору	US		
	for det	💼 Paste	Domain Name: TDS.NET		
.net .12.1 DNS	Demi				
<b>e</b>	Dom: Reg:		Administrative Contact:		
Whois	Who:	.net	Marketing, CSSG domainadmin	istrator@tdstelecom.com	
<b>6</b>	Ref(		TDS Telecommunications		
	Name	<b>10</b> 2	525 Junction Road Madison, WI 53717		
Cig	Name		US		
8	Name	IPBlock	1-800-358-3648 fax: 608-664-	-4035	
Trace	Name	Pig			
الے۔ Finger	Name	10 M 10	Technical Contact:		
inger R	Name		Administrator, TDSNET Dns o TDS Telecom	kemoinn@TDS.NET	
SMITP	Name	Finder	525 Junction Road		
()) Time	Stat	j K	Madison, WI 53717		
	Upd: Crea		US		
₩ Web	Exp:	Time	800-358-3648 fax: 608-664-40	544	
<b>ा</b> Awake	-	₩ Web	Record expires on 09-Jul-2010.		
		To	Record created on 08-Jul-1995.		
RBL	>>> La:	Awake	Database last updated on 12-Oct	-2006 11:47:08 EDT.	
Δ	4	RBL			
🧞 ww	w.norwich.		v.norwich.edu (whoi 🏾 🚓 www.norwich.edu (whoi 🖉 a www.norw	ch.edu (whoi khois)	
For Help	), press F1		press F1	0	

#### Locating Information from E-Mails



# Headers are crucially important Often stripped from display

🖾 Re: O	rangutans -	Message (P	lain Text)		∎◙⊐⊡		
<u>F</u> ile <u>E</u>	dit <u>V</u> iew	<u>I</u> nsert F <u>o</u>	ormat <u>P</u> GP	<u>T</u> ools	<u>A</u> ctions	<u>H</u> elp	
\$∕ ≥	? 🖻   🖃 <u>s</u>	end 🛃 🔒	<b>*</b>  Q <sub>4</sub>   6	) 😂 🐧	1	X   🔺	
Extra line	breaks in this m	essage were re	moved.				
From:	Shirley McGrea	l [smcgreal@ipj	ol.org] Se	nt: Thu 20	06-10-12 10	):54	
To:	mekabay@gma	ail.com					
Cc: Subject:	Re: Orangutar	IS					
We're any way for spe Bogota which I	hanks for the quite concerr y to help her cified work ( for a comput agree is rea 't really be in	ed about So get organize on producing er and replo Ily needed,	ara's grant, d ed. She asked g educational acement/repo but our audit	d to spend materials air of her tor checks	l our \$2,0 s on a \$50 computer s our gran	100 grant 10 trip to instead, ts and thi	



#### **E-Mail Headers**

#### Can be displayed through e-mail options

Message Options X Message settings Security Encrypt message contents and attachments rd-l Importance: Normal Add digital signature to outgoing message Sensitivity: Normal This example Request S/MIME receipt for this message is from Tracking options **MS-Outlook** Request a delivery receipt for this message Request a read receipt for this message Delivery options Have replies sent to: Expires after: None Contacts... Categories.. Internet headers: X-Gmail-Received: 0dfd13bc11b16fda1ec3cf714c213e6751429e16 Delivered-To: mekabay@gmail.com Received: by 10.78.147.3 with SMTP id u3cs86635hud; Thu, 12 Oct 2006 08:22:55 -0700 (PDT) Received: by 10.90.78.9 with SMTP id a9mr 1401879agb; Thu, 12 Oct 2006 08:22:54 -0700 (PDT) Return-Path: <smcgreal@ippl.org> Close

#### **E-Mail Headers**

Show details of who sent e-mail and how it was routed X-Gmail-Received: 0dfd13bc11b16fda1ec3cf714c213e6751429e16 Delivered-To: mekabav@gmail.com Received: by 10.78.147.3 with SMTP id u3cs86635hud; Thu, 12 Oct 2006 08:22:55 -0700 (PDT) Return-Path: <smcgreal@ippl.org> Received: from mail42.opentransfer.com (mail42.opentransfer.com [71.18.111.198])by mx.google.com with SMTP id 29si861796wrl.2006.10.12.08.22.53; Thu, 12 Oct 2006 08:22:54 -0700 (PDT) Received-SPF: neutral (google.com: 71.18.111.198 is neither permitted nor denied by best quess record for domain of smcgreal@ippl.org) Received: (qmail 11919 invoked by uid 399); 12 Oct 2006 14:54:05 -0000 Received: from unknown (HELO System5.ippl.org) (70.60.217.92) by mail42.opentransfer.com with SMTP; 12 Oct 2006 14:54:05 -0000 Message-Id: <7.0.1.0.2.20061012104204.03a1daf8@ippl.org> X-Mailer: OUALCOMM Windows Eudora Version 7.0.1.0 Date: Thu, 12 Oct 2006 10:54:04 -0400 To: <mekabay@gmail.com> From: Shirley McGreal <smcgreal@ippl.org> Subject: Re: Orangutans In-Reply-To: <200610121353.k9CDrlN3004352@cronus.email.starband.net>

NEVER simply forward an e-mail of interest to an investigator; always copy and paste the headers into your message to avoid corrupting the header.



#### **Proactive vs Reactive Strategies**







#### **Online Stings: Entrapment?**

- Must not give any basis for claim that officer initiated, suggested, prompted, or encouraged
  - □Illegal activity or
  - Investigative actions that violate privacy or
  - Convert a civilian into an agent of law enforcement to violate legal restrictions
- ENTRAPMENT can destroy case
  - □Why? 4<sup>th</sup> Amendment safeguards
- A CONTRACT

- Sorrells v. United States (1932)
  - Scotus ruled that entrapment defense must show proof that LEO encouraged crime
  - Defendant would not have been predisposed to commit crime



#### United States v. Poehlman (2000)

- Poehlman alleged to have met undercover LEO to have sex with minor
- But defendant said he started online discussions with LEO to form adult relationship
- LEO wrote she was looking for someone "to train her daughters in the ways of the world"
- Poehlman explicitly said he wasn't interested and LEO responded that she would terminate relationship



- Poehlman offered to "train" daughters as way of continuing relation but claimed he had no intention of having sex with them – was ploy
- SCOTUS ruled in favor of defendant: evidence that pedophilia was not his original intent & LEO was significantly responsible for his actions



# BREAK

# 5'12''

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### Search Warrants & Seizure of Electronic Evidence



ECPA Effects on Data Acquisition

Collaboration from Third-Party Record-Holders

Which Computers?

Legal Limits on Searches
 Federal Constitutional Limits
 State Constitutional Limits
 Reference



References: Clifford pp 111-137 Moore pp 141-153; 148-155



#### Identifying Physical Location of Electronic Evidence

- General Principles
- ECPA Effects on Data Acquisition

  - Disclosure to Government Agents
  - □ Contents of Electronic Communications
  - □ Violations of the ECPA
- Collaboration from Third-Party Record-Holders
  - **□** Finding the Records
  - Evaluating Utility of Records
  - □ Authenticating Records
  - **Obtaining Records**
  - □ Contacting ISP & Serving Papers



#### **General Principles**



news

- Katz v US (1967): SCOTUS held that publicly disclosed information is not constitutionally protected
  - Includes voluntarily transferred info in hands of third parties
  - Thus third-party repositories limited by statute, not 4<sup>th</sup> amendment
- Restrictions include laws protecting
  - □Bank records
  - **Cable TV & video rentals**
  - **DE-mail & other electronic communications**



#### **ECPA Coverage**





- 2000: Updated Wiretap law (18 USC §2510-22)
- 2004: Added Stored Electronic Communications Privacy Act (SECA, 18 USC §2701-11)
- Protects contents of ecommunications in storage by service
- Prohibits provision of communications to government agencies without strict controls

#### Disclosure to Government Agents

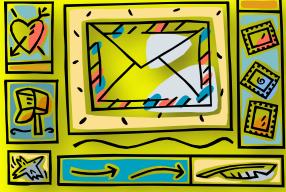
- All records may be obtained through warrant
- Subscriber/customer records (identity, services) may also be obtained by subpoena
- Transaction history available through subpoena since U.S.A.P.A.T.R.I.O.T. Act passed
- E-mail may be retrieved by subpoena provided user given notice (up to 90-180 days delay)
- May use "§2703(d) court order" to access everything except unopened e-mail stored < 180 days</p>

	Anited St	ates <b>Bis</b>	strict Com	:t _
-	SOUTHE	RN DISTRICT OF	LORIDA	alking south
In the M	alter of the Search of			
	soription of person or property to be wo		SEARCH WA	DD ANT
	RO GONZALEZ, LOCATED AT ET, MIAMI, MIAMI-DADE			INIGHT I
COUNTY, FLORIDA		CASE	E NUMBER:	
- 10 S		128 -		
TO SALLEY A RO	riquez, U.S. Immig. & Natz. Se	Nice and any Auto	conized Officer of the Unite	d Ebalan
		and any had	An 200 Childe of the Unite	o sanca
Allidavit(s) having	been made before me b	y 50A M	ary A. Rodriguez	who has reason to
Association and	a Socialization and the social statistics		Atlant	-
	he person of or 🛛 on the p		김 승규는 아이에 가지도 아내가 말을 들었다. 가격 전망 문	
THE RESIDENCE OF	LAZARO GONZALEZ. LOCATE	ED AT 2319 N.W. 2ND	STREET, MIAMI, MIAMI-DAC	E COUNTY,
r conten				
in the	SOUTHERN	District of	FLORIDA	there is now
concented a certain p	erson or property, namely to			
concented a certain p	1			
concented a certain p	erson or property, namely to			
concented a certain p	erson or property, namely to			
concepted a certain p	erson or property, namely to			
connected a certain p THE PERSON OF ELL	erson or property, namely a NN GONZALEZ, DATE OF BIR	to be parted of breakly TH DECEMBER 8, 1997	3, A NATIVE AND CITIZEN C	F CUBA,
concreted a certain p THE PERSON OF ELL	erson or property, namely <sub>te</sub> NN GONZALEZ, DATE OF BIR	to be parted of breakly TH DECEMBER 8, 1997	3, A NATIVE AND CITIZEN C	F CUBA,
concepted a certain p THE PERSON OF ELL 1 am satisfied that the so described is now a warrant.	erson or property, namely a NN GONZALEZ, DATE OF BIR affidavil(a) and any record soncealed on the parson or ;	th DECEMBER 5, 199 testimony establish p	3, A NATIVE AND CITIZEN C	F CUBA,
concreted a certain p THE PERSON OF ELL 1 am setisfied that the so described is now of warrant. YOU ARE HEREBY	erson or property, namely a NN GONZALEZ, DATE OF BIR affidavil(a) and any record concested on the parson or j COMMANDED to search o	th DECEMBER 5, 199 TH DECEMBER 5, 199 testimony establish p premises above-desc n or before	3, A NATIVE AND CITIZEN C roboble cause to boliave th ribed and establish ground 5-1-0	F CUBA, at this person or properties is for this issuance of this
concreted a certain p THE PERSON OF ELL 1 am setisfied that the so described is now of warrant. YOU ARE HEREBY	erson or property, namely a NN GONZALEZ, DATE OF BIR affidavil(a) and any record concested on the parson or j COMMANDED to search o	th DECEMBER 5, 199 TH DECEMBER 5, 199 testimony establish p premises above-desc n or before	3, A NATIVE AND CITIZEN C roboble cause to boliave th ribed and establish ground 5-1-0	F CUBA, at this person or properties is for this issuance of this
connected a certain p THE PERSON OF ELL I am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da making the search (h has been established	erson or property, namely to NN SCHZALEZ, DATE OF BIR softdevil(s) and any record i concessed on the person or ; COMMANDED to search or ys) the person or place nam the daySine _ GOD MM. It	testimony establish p premises above-desc n or before - texter for the pe	3, A NATIVE AND CITIZEN C robable cause to believe th ribed and establish grouns S-1-0 Data rison or property specified, firms in the day or night a	F CUBA.
connected a certain p THE PERSON OF ELU 1 am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da mething the search (h has been establishe receipt for the putso	erson or property, namely a with SONZALEZ, DATE OF BIR concessed on the person or ; COMMANDED to search or ys) the person or place name the upsine <u>Geotechne</u> d) and if the person or pro; n or property taken, and pro	testimony establish p premises above-desc n or before here the term the par- serve to compare a written increa pare a written increa	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish grouns 5-1-0 Bas rson or property specified, fime in the day or night a to seize some, leaving a to seize some, leaving a	F CUBA, all this person or property is for the issuence of this surving this warrant and I find reasonable cause come of this warrant and
connected a certain p THE PERSON OF ELU 1 am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da mething the search (h has been establishe receipt for the putso	erson or property, namely as NN SCHIZALEZ, DATE OF BIR addidavii(n) and any record concested on the person or j COMMANDED to search or ys) the person or place name in the daySine - Gabland at 0) and if the person or property taken, and pri n or property taken, and pri	testimony establish p premises above-desc n or before here the term the par- serve to compare a written increa pare a written increa	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish grouns 5-1-0 Bas rson or property specified, fime in the day or night a to seize some, leaving a to seize some, leaving a	F CUBA, all this person or properti is for the issuence of this surving this warrant and I find reasonable cause copy of this warrant and rety solved and prompt
connected a certain p THE PERSON OF ELU 1 am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da mething the search (h has been establishe receipt for the putso	erson or property, namely as NN SCHIZALEZ, DATE OF BIR addidavii(n) and any record concested on the person or j COMMANDED to search or ys) the person or place name in the daySine - Gabland at 0) and if the person or property taken, and pri n or property taken, and pri	testimony establish p premises above-desc n or before hood there are the part of the part of the part of the part of the part of the part	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish grouns 5-1-0 Bas rson or property specified, fime in the day or night a to seize some, leaving a to seize some, leaving a	F CUBA, all this person or properti is for the issuence of this surving this warrant and I find reasonable cause copy of this warrant and rety solved and prompt
connected a certain p THE PERSON OF ELU 1 am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da mething the search (h has been establishe receipt for the putso	erson or property, namely as NN SCHIZALEZ, DATE OF BIR addidavii(n) and any record concested on the person or j COMMANDED to search or ys) the person or place name in the daySine - Gabland at 0) and if the person or property taken, and pri n or property taken, and pri	testimony establish p premises above-desc n or before hood there are the part of the part of the part of the part of the part of the part	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish grouns 5-1-0 Bas rson or property specified, fime in the day or night a to seize some, leaving a to seize some, leaving a	F CUBA, all this person or properti is for the issuence of this surving this warrant and I find reasonable cause copy of this warrant and rety solved and prompt
connected a certain p THE PERSON OF ELU 1 am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da mething the search (h has been establishe receipt for the putso	erson or property, namely as NN SCHIZALEZ, DATE OF BIR addidavii(n) and any record concested on the person or j COMMANDED to search or ys) the person or place name in the daySine - Gabland at 0) and if the person or property taken, and pri n or property taken, and pri	testimony establish p premises above-desc n or before hood there are the part of the part of the part of the part of the part of the part	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish grouns 5-1-0 Bas rson or property specified, fime in the day or night a to seize some, leaving a to seize some, leaving a	F CUBA, all this person or property is for the issuence of this surving this warrant and I find reasonable cause copy of this warrant and roy solved and prompto
connected a certain p THE PERSON OF ELU I am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da meting the search (h has been establishe receipt for the putso return this weath to	erson or property, namely a with GONZALEZ, DATE OF BIR concessed on the person or p concessed on the person or p concessed on the person or ys) the person or place name the upsine <u>Geotechne</u> d) and if the person or prop a or property taken, and pro 	testimony establish p premises above-desc n or before hood there are the part of the part of the part of the part of the part of the part	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish ground <u>S-1-0</u> Bas son or property predited, from in the day or relified, to seize same, leaving a to seize same, leaving a toggi the person or prop	F CUBA, all this person or property is for the issuence of this surving this warrant and I find reasonable cause come of this warrant and
connected a certain p THE PERSON OF ELU I am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da meting the search (h has been establishe receipt for the putso return this weath to	erson or property, namely a with GONZALEZ, DATE OF BIR concessed on the person or p concessed on the person or p concessed on the person or ys) the person or place name the upsine <u>Geotechne</u> d) and if the person or prop a or property taken, and pro 	testimony establish p premises above-desc n or before nor before here the start the pa series of the pa before down of the pa before the start the start the start the start the	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish ground <u>S-1-0</u> Bas son or property predited, from in the day or relified, to seize same, leaving a to seize same, leaving a toggi the person or prop	F CUBA, all this person or property is for the issuence of this serving this warrant and I find reasonable cause copy of this warrant awanty solved and prompto as required by law
connected a certain p THE PERSON OF ELU 1 am satisfied that the so described is now o warrant. YOU ARE HEREBY (not to exceed 10 da mething the search (h has been establishe receipt for the putso	erson or property, namely as NN SCHIZALEZ, DATE OF BIR adfidevil(a) and any record concessed on the parson or p COMMANDED to search or ys) the person or place name the daySine Coop MM. It d) and if the person or pro- d) and if the person or place name the daySine Coop MM. It d) and if the person or pro- n or property taken, and pri- us.	testimony establish p premises above-desc n or before nor before here the start the pa series of the pa before down of the pa before the start the start the start the start the	s, a NATIVE AND CITIZEN C robable cause to believe th ribed and establish ground <u>S-1-0</u> Bas son or property predited, from in the day or relified, to seize same, leaving a to seize same, leaving a toggi the person or prop	F CUBA, all this person or property is for the issuence of this serving this warrant and I find reasonable cause copy of this warrant awanty solved and prompto as required by law



#### **Contents of Electronic Communications**

- Agreement of one party in electronic communication suffices for legal disclosure
- Take that fact into account when you are writing e-mail
  - In general, when writing with employee userID, all e-mail must be considered equivalent to using company letterhead
  - □All official e-mail may become evidence in a court of law



When writing informally using your own address, remember that everything on Internet is POTENTIALLY PERMANENT and may affect your future employment prospects





## **Violations of the ECPA**

- Criminal liability
  - □Up to 2 years in federal prison
- Civil liability
  - □Damages & attorneys' fees
  - Government agent may be personally liable
- Suppression: NOT a remedy
- Good faith defense:
  - Government agent may



- Rely on good faith application of warrant or subpoena
- As absolute defense against civil or criminal charges stemming from actions



# **Evaluating Utility of Records**

Records may not be available

Typically 30-60 day retention of log ta records

But look for video camera tapes

- Dynamic IP addresses may make identification difficult for older evidence
- Some records may originate in public computers that are effectively anonymous
  - □Business services (e.g., Kinko's)
  - □Libraries, Internet cafés
  - **□Wireless services**
  - □Hijacked services
  - ❑Anonymizers





## **Authenticating Records**

- Spoofing may disguise origin
  - Naïve users alter originating address
  - But headers show real IP addresses
- More sophisticated criminals add faked header lines



- □Must always analyze entire header
- SamSpade does this (discussed in lecture 16)
- Open spam relay a danger
   Logon to unprotected SMTP server
   Send mail from someone else's system

#### **Obtaining Records**



Typically obtain search warrant Better than subpoena □Can obtain any records at all Avoids problem of more restrictive state laws that require warrant So why not use a warrant? □Might not have probable cause Difficulty getting warrant across state lines



#### **Contacting ISP & Serving Papers**

Call ISP to be sure they have records you need

- □Discuss IP addresses with technical staff
- Identify possible errors of analysis
- Find out if there have been mergers or acquisitions
- Identify possible IP sub-blocks owned/used by other entities \_
- >Ask if ISP will accept warrant by fax
- Explain exactly what you need







#### **Search Warrants**

Which Computers?
 Legal Limits on Searches

 Federal Constitutional Limits
 State Constitutional Limits
 Statutes





# **Which Computers?**

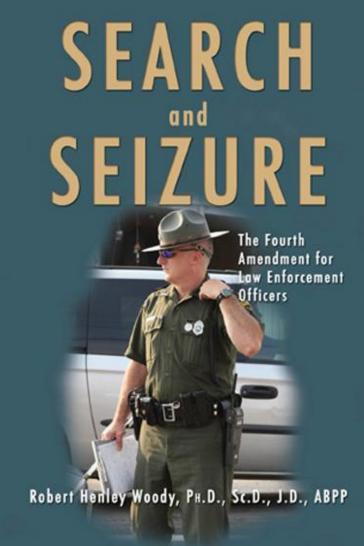
- Goal of tracing electronic communications:
  - Locate computer at origin of evidence of crime
  - □Link to specific person
- Computers that may be involved
  - Victims' computers may be searched without warrant with permission
  - Publishers' computers not restricted if publisher is the victim
  - ECPA does not apply to suspects' computers





#### Federal Constitutional Limits

Fourth Amendment expectation of privacy Government action Legal Warrant □**Probable cause** Neutral/detached magistrate Reasonably precise Rules for Executing Warrant



http://tinyurl.com/4jmcaz

## **The Fourth Amendment Text**



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.

**Bold** emphasis added



# **4th Amendment Issues (1)**

**Reasonable expectation of privacy (EOP)** 

- Subjective expectation
  - □Computer *in home* has *higher* EOP
  - □ Shared computer has lower EOP
  - **Employer's computer: depends** 
    - ✓ Policy?
    - ✓ Awareness?
    - ✓ Enforcement?
- Social acceptance or expectation of search



## 4th Amendment Issues (2)



Government action

Searches by state law enforcement may transfer results to federal agencies



✓ But federal authorities must not have been involved in a way that would require suppression of evidence

Private citizens

Constitution does not affect search by private citizen not acting as an agent of law enforcement

**Thus evidence usually admissible in court** 

# Legal Warrant

Probable cause *Evidence* of a crime

- Live like a state of a crime
- Likelihood that evidence will be found in location to be searched
  - How do you know suspect used computer in home? Could have been elsewhere



- May need circumstantial evidence such as time stamps, stakeout
- Neutral/detached magistrate
  - □Who has authority for warrant location
  - □ Watch out for cross-state jurisdiction
- Reasonably precise
  - □ *General* description may lead to suppression □ Best to mention computers & media *explicitly*





**Rules for Executing Warrant (1)** 

- purpose in entering premises
- Take items in plain view
  - But contraband and tools for
    - crime may also be seized if they
    - are visible and obviously incriminating





#### **Rules for Executing Warrant (2)**





- Evidence seized under faulty warrant may be suppressed
- But generally LEOs not prosecuted if acting under good faith in legality of (later overturned) warrant
- Remove computers for analysis off-site
- Prompt execution
  - □Don't let evidence evaporate
  - Cannot hold warrant in abeyance indefinitely



# **State Constitutional Limits**

- Some states more restrictive than federal rules
- Some do not allow good-faith exception to requirement for valid warrant
- Some may protect vehicles (and by implication portable computers) more than federal courts



#### **Statutes**

ECPA (as discussed above)
 Zurcher v. Stanford Daily
 LEOs had warrant to search student newspaper's computer for pictures of political demonstration
 SCOTUS ruled that 1st

Amendment issues did not further limit warranted searches



This is not a statute.



## **Statutes: PPA**

- PPA passed to further restrict warrants
  - Privacy Protection Act (42 USC §2000aa)
  - □Passed in 2000
  - Any material intended for publication or broadcasting requires a subpoena
  - Exceptions
    - Contraband, fruits or tools for crime
    - Preventing imminent death or injury
    - Material held by target of investigation
    - Child pornography







# **PPA & Steve Jackson Games**

- March 1990: Secret Service raided Steve Jackson Games
  - Looking for info about BellSouth's emergency service
  - □ Had been posted on BBS
  - □ Seized entire computer for BBS
  - □ Held for months
  - Severely damaged company
- SJG sued under PPA & ECPA
  - □ Won trial
  - □ Awarded damages \$51K
  - □ Attorneys' fees \$250K



Irony: BellSouth info was actually public & available for sale from company



# BREAK 10'27''

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Warrantless Seizure of Evidence

- Exceptions to the Requirement for Warrant
- Consent
- Search Incident to Arrest
- Exigent Circumstances
- > Inventory
- Stop and Frisk
- > Mobility
- Plain View

**Clifford pp 137-155 Moore pp 153-165** 

## **Exceptions to Requirement for Warrant**

Long-standing view in jurisprudence:
 Warrant not necessary IF
 Owner of property agrees to search
 Issues
 Does consenter have legitimate right to consent to search?
 Expectation of privacy
 Degree of ownership of property



### Consent

Who May Consent? **Employer □**Spouse **Co-User Third-Party Holder** Notification of Right to Withhold Consent

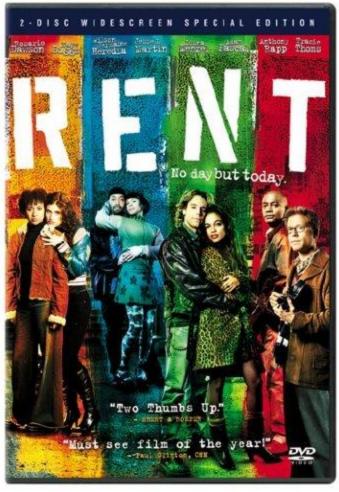


Limitations and Withdrawal of Consent



# **Who May Consent?**

- Matlock 1974: Common authority or sufficient relationship to the premises or effects
- Rith 1999: Mutual use
  - □ Joint access
  - Control of property for most purposes
- Crucial test: expectation of privacy
  - Reduced in shared accommodations
  - But evidence of rent & of security strengthens expectation of privacy (see later slides)





# **Private Employers**

Employer not acting as agent of LEO is free to search own property without suppression of evidence



General acceptance of right of search

□For area not exclusively reserved for a particular employee

**Expect same rule for computers** 

Explicit policy reducing expectation of privacy strengthens admissibility of evidence

# **Public Employers**



- SCOTUS: O'Connor v. Ortega (1987) established expectation of privacy for government employees
  - But open office could reduce expectation
  - Also affected by specific policy
- Policy effectiveness depends on
  - Clear enunciation of limits to privacy (e.g., logon banner)
  - Evidence that employees are aware of policy



Used with permission of artist. <u>http://tinyurl.com/6pszy7</u> Copyright © 1998 Steve Greenberg. All rights reserved.

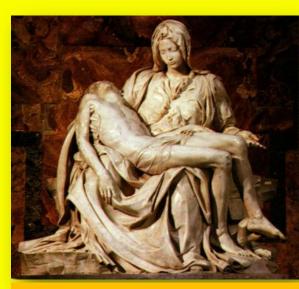
Problems

Allowing private use of government computers
 Allowing unauthorized encryption



#### Parent

- Closer relationship supports consent
- Parents' consent generally accepted by court But child must be "essentially dependent" on parent
  - Payment of rent reduces authority to grant consent
- US v. Durham (1998): Mother could not grant consent for search of son's computer
  - Even though she owned some of equipment
  - Because son applied security to system
  - □And he paid small amount of rent



*Pietà*, marble sculpture by Michelangelo, 1499; in St. Peter's Basilica, Rome

#### Spouse

Generally viewed as having "joint control and equal right to occupancy of premises and access to computers on the premises" [Orton p 141]

BUT consent is invalid if

Computer is used exclusively by nonconsenting partner

□Kept in separate room (esp. if locked)



#### **Co-User**

Shared use reduces expectation of privacy

- But still case law to develop on effects of
  - □Access controls

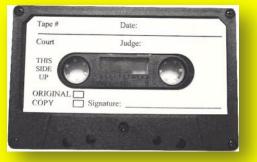
For time being, assume co-user cannot grant consent to prima facie private areas of computer





# **Third-Party Holder**

- If equipment or media left in possession of someone else, does that person have right to consent to search without warrant?
- Problematic case law: contradictions
- US v. James (2003):
  - Court ruled search of data CDs invalid because
  - Owner did not intend to give 3<sup>rd</sup> party authority to grant consent for search
  - □ But note that CDs were in *sealed* envelope
- > US v. Falcon (1985):
  - Cassette tape labeled "confidential/do not play"
  - Court ruled tape admissible without warrant



- Argued holder could have played tape any time
- CONCLUSION: best to proceed with warrant to avoid risk of suppression



## Notification of Right to Withhold Consent



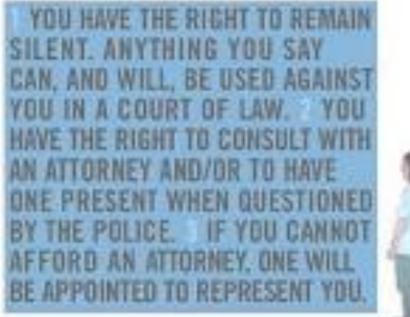


- Is the consent to the search voluntary?
- Federal system imposes burden of proof on government using preponderance of evidence
- Other jurisdictions may be more exigent
  - E.g., requiring "clear and convincing evidence"



## Factors affecting judgement of voluntary consent:

- > Age/intelligence of suspect
- Being advised of constitutional rights (Miranda warning)
- Custody or detention (and length)
- Physical punishment or deprivation (sleep, food)
- Generally, advising person that warrant will be sought if consent not granted is acceptable





# Limitations and Withdrawal of Consent

- Consent for search may be withdrawn at any time
- Area of search may be limited
- Continuing to search after withdrawal or in unauthorized areas leads to suppression of evidence
- Does breaking access protection or encryption violate restrictions on unwarranted search?
- In physical world, breaking locks or sealed containers has led to suppression
- □But no *damage* when breaking security so evidence *may* be accepted by court



## **Search Incident to Arrest**

- General principle allows search and seizure of evidence at time of arrest
  - Purpose: prevent destruction of evidence



Therefore expect same rule for digital evidence

Particularly useful for seizing cell phones and PDAs

□May contain useful data

**DE.g.**, phone lists, calendars, call logs



# **Exigent Circumstances (1)**

#### Probable cause

- Exigent circumstances defined essentially by
  - Imminent destruction of evidence

<mark>≻ BUT</mark>

- Allows for seizure of computer
- **□But NOT for search** 
  - Need separate warrant for search



# **Exigent Circumstances (2)**



- US v. Reed (1991) established requirements for admitting evidence obtained under warrantless search with claim of exigency
  - Must demonstrate degree of urgency
  - Amount of time required for getting warrant would seriously interfere with process of ensuring justice
  - Evidence in danger of destruction or removal
  - Danger to officers or evidence at crime scene
  - Suspect's awareness of anticipated seizure of evidence
  - Ease of destruction of evidence by suspect





# **Exigent Circumstances (3)**

- US v. David (1991)
  - LEO observed suspect deleting data from PDA
  - Seized device and scanned names
  - Court admitted evidence
  - But exigency ended as soon as PDA was seized
- US v. Ortiz (1996): court ruled that search of pager was warranted because of risk of data loss as batteries failed



US v. Romero-Garcia (1997): search of laptop computer was not warranted by fear of battery failure (would not normally destroy data)

Best practice: if device seized under exigent circumstances, obtain a warrant using probable cause to justify search that will ensure evidence is accepted in court unless data are evanescent



## Inventory

- Normally associated with searching vehicles to list all evidence present
- Booking search catalogs possessions of suspect at time of arrest



- Might permit LEO to search computer or electronic device to determine *identity* of suspect
- But should not use as basis for extensive forensic analysis: get a warrant

## **Stop and Frisk**



LEO may search suspect for weapons
 May seize computing device during search
 BUT should not search computer without warrant





# Mobility

- Vehicle's mobility serves as exigent circumstance justifying immediate search without warrant
- Could therefore reasonably seize a computer found in such a search
- But Orton argues that this view could not justify search of computing devices



And there is no current case law supporting such a procedure



# Plain View (1)

Doctrine: If contraband is **Left** in plain view of LEO □Who is in lawful place Then there is no expectation of privacy Limits Incriminating nature must be obvious □LEO must be legally allowed to be in position where item is in view LEO must not alter search process as result of plain-view discovery



# Plain View (2)

- So cannot exceed limits of warrant when searching computer even if plain-view item such as file-name suggests crime
- If protocol in warrant specifies searching all files, may log child porn as long as search continues through all files
- If protocol in warrant specifies searching all files but only for business fraud data, may NOT open file suspected to contain child porn
- So if new evidence of a different crime is discovered in plain view, get a warrant to change search protocol.



# Plain View (3)

- > US v. Carey (1999)
  - □ Narcotics investigation of computer disk
  - Officer's discovery of 1<sup>st</sup> child porn image accepted in court
  - But subsequent discoveries suppressed unlawful search beyond terms of warrant
- US v. Gray (1999)
  - LEO conducting file-by-file search
  - Discovered child porn



- Immediately applied for warrant to search of child porn
- Court ruled that not only was officer correct but also that had other child porn been discovered in systematic examination of all files, those images would have been admissible also



# BREAK 4'58''

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### Electronic Crime Scene Investigation

> Introduction

Nature of Electronic Evidence

Moore Ch 9 Clifford Ch 3 pp 155-160

- Handling Electronic Evidence at the Crime Scene
- Electronic Devices
- Securing and Evaluating the Scene
- Documenting the Scene

ECSIGFR = Electronic Crime Scene Investigation: A Guide for First Responders (NIJ)

Another useful reference: Volonino, L., R. Anzaldua, J. Godwin (2007). *Computer Forensics: Principles and Practices.* Pearson Prentice Hall (ISBN 0-13-154727-5). xviii + 534. Index.

#### Introduction



Law Enforcement Response to Electronic Evidence

- Latent Nature of Electronic Evidence
- RULE 1 OF DIGITAL FORENSICS
- Forensic Process

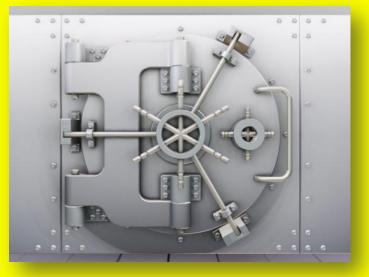




#### Law Enforcement Response to Electronic Evidence

#### Computers involved in crime may be

- Repositories of evidence
- Personnel of many types may be involved in responding to crime involving computers



- Investigators (private, corporate)
- □ Forensic examiners
- □ Managers (case, corporate, political)
- First responder can be anyone in LE
  - Must safeguard EE against loss or tampering



#### Latent Nature of Electronic Evidence [EE]

- "Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device." [ECSIGFR p. 17]
- EE thus *latent* (like fingerprints, DNA evidence) because not immediately visible
  - Requires technical equipment & expertise
  - May need expert testimony in court to explain analysis
- EE fragile
  - Easily destroyed or altered

Chain of custody & technical safeguards essential for successful prosecution





#### **RULE 1 OF DIGITAL FORENSICS**

#### HARM NOTHING! (E.G., DON'T LET AMATEURS COLLECT DIGITAL EVIDENCE)





#### **Forensic Process**

#### Key phases:

Collection: search / recognition / collection / documentation of evidence

#### Examination (technical perspective)

- Document content / state of evidence
- □ Reveal hidden data
- Identify relevant data
- Analysis (legal perspective)
- Reporting
  - Process notes for expert testimony
  - □ Results
  - Reliability



#### Nature of Electronic Evidence Quotin



Quoting directly from ECSIGFR p. 20

- Is often latent in the same sense as fingerprints or DNA evidence.
- Can transcend borders with ease and speed.
- Is fragile and can be easily altered, damaged, or destroyed.
- Is sometimes time-sensitive
- Therefore only those with expertise should handle digital evidence
  - E.g., rebooting alters or destroys data that could be useful in investigation

Forensic data-capture tools often require training



#### Handling Electronic Evidence at the Crime Scene

#### Preparations

Secure and document crime scene (photographs, sketches, notes)

- □Use protective equipment to avoid contaminating crime scene (e.g., gloves)
- Recognize and identify evidence
- Document electronic equipment at crime scene
- Collect and preserve EE
- Package and transport EE
- Maintain chain of custody



#### The Digital Forensics Tool Kit (1)



Volonino *et al.* p 126 ff ECSIGFR p 23 ff

- Cellular phone
- Basic hardware toolkit: screwdrivers, pliers, duct tape etc.
- Watertight & static-resistant plastic evidence bags
- Labels and indelible markers
- Bootable media: DOS startup, bootable CDs, bootable USB drives w/ forensic software
- Cables: USB, FireWire, CAT5 crossover & straight-through, power cables
- Laptop computer for tools and notes
- PDA with integrated camera & link to PC



#### The Digital Forensics Tool Kit (2)



- > High-resolution camera(s) w/ date-time stamps
- Hardware-write blocker (e.g., FastBloc, DriveLock) to prevent damage to removed drive
- Luggage cart
- Flashlight
- Power strip
- Log book
- Gloves
- External USB hard drive



Forensic examiner platform (e.g., specialized tools) for data acquisition



#### **Specialized Forensics Tools**

- E.g., Logicube® < <u>http://www.logicube.com/</u> >
- Popular hard-drive cloning systems
- Used by
  - □Law enforcement
  - **□**Military
  - □Internal IT departments



- Products support various drive interfaces and connectors
  - □IDE □SATA □SAS □SCSI □USB



Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### Establish Your Search Parameters



#### Volonino *et al.* p 129

- What types of evidence are you looking for?
  Photographs? Document? DBs? E-mail?
- What is the user's/suspect's skill level?
- What kind of hardware is involved?
  Computers (Mac? Windows? Linux?)
  PDAs? Cell phones? Watches?
- What kind of software is involved?
- Do I need to preserve other types of evidence?

□ Fingerprints? DNA?

What is the computer environment?



□ Network? (Protocols, topology...) ISP?

Security? UserIDs? Passwords? Encryption?

□ Real bombs inside the cases [thanks to Chris Tanguay]

#### **Managing the Onsite Investigation**



%

#### Volonino et al. p 130 ff

%

- Maintain integrity of data collection process
- Estimate time required for onsite examination
- Limit costs to target organization **Legal liability for interruptions** of business
  - May outweigh importance of crime
  - □ May stop investigation
- Evaluate necessary equipment for onsite work
- Evaluate personnel costs
  - □Who should be onsite?

Would their involvement impede other critical investigations?



#### **Remove Suspect from Computer**



#### Moore Ch 9

Potential for instant data deletion by suspect

- Can prepare programs to delete key evidence
- Activate at touch of keyboard (macros, "hot keys")



- □Or through voice-command interface
  - ✓ E.g., Dragon Dictation, Windows voice-recognition
- > No-knock search warrants still problematic
- Therefore instantly move suspect away from computer

□Shake hands with LEO & prevent return

□Physical force only if necessary

□Allow no return to computer





#### **Secure the Scene**

- Photograph scene
  - □ Agencies are currently using digital cameras
  - But recall discussion of falsifiability of digital images
  - □ Use video camera to document process
  - May see cases hinging on credibility of such evidence
    - ✓ Defense sometimes challenges timestamps
    - ✓ But claims of fraud / error must include likelihood (proffer of proof)
- Photograph computer screen(s)
   Especially evidence of system time
- Photograph everything that may be evidence Cost is not a factor w/ digital cameras



#### **Disconnect Outside Control**

Remove network connectivity □Phone line / DSL □Cable / satellite modem □Suspect may be storing evidence on remote systems Wireless connectivity may be more difficult to handle\* □Wireless I/F may be integrated within computer case – not obvious outside **Especially true in laptop computers** > Look for evidence of home network □May have data storage in other locations

\*For more details see "The Need for a Technical Approach to Digital Forensic Evidence Collection for Wireless Technologies" by B. Turnbull & J. Slay (2006) < <u>http://www.itoc.usma.edu/Workshop/2006/ Program/Presentations/IAW2006-07-1.pdf</u> >

#### **Handling Downloads**

What if system shows signs that user was downloading file(s)? □Could be evidence Photograph download window Reduces chance that suspect can successfully deny involvement in download

□May allow download to complete

Videotape entire process

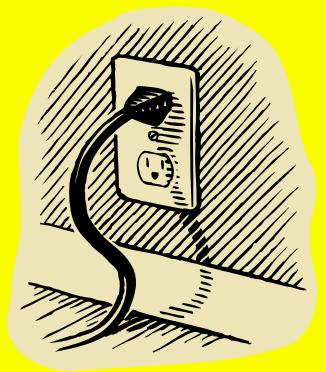


#### **Powering Down Computer**

#### Moore p 172 ff ECSIGFR p 30 ff

#### Want to avoid damaging data

- Determine Operating System
- Save Data from Running Programs?
- Save Data in RAM?
- Handling Specific OSs
- Laptop Computers





#### **Determine Operating System**

- GOAL: make bit-images of RAM and of DISK before going any further
- OS does not influence which tools to use for bit-image capture onsite
  - □Mac versions
  - □Windows versions
  - □Unix flavors



- Hardware-specific OSs (cell phones, PDAs)
- Must have right tools and procedures
  - Avoid imprecise copy
- Subject of more advanced courses



## Save Data from Running Programs?



- May be able to see that programs are running (e.g., on program bar)
- Disagreement among experts
  - Pull the plug: data in temporary regions on disk anyway; or



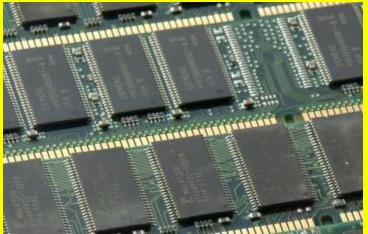
- Save the temporary data explicitly in case they have not yet been written to disk
- Technical knowledge essential
  - E.g., many OS use extensive write-behind buffering
  - Encrypted volumes may be corrupted by instant power-down



#### **Save Data in RAM?**

Most OSs use Virtual Memory (VM)

- Reserve space on hard disk for extension of main memory (RAM)
- Swap data back and forth between VM and RAM
- Thus VM swap file a treasure-trove of potentially valuable data about what was in RAM



However, some users disable VM because of large RAM (e.g., 2 GB)

- Specialized utilities for saving data directly from RAM depending on OS & hardware
- Particularly important for cell phones and PDAs which may depend on battery power for maintenance of volatile memory

## Handling Specific OSs at the Scene



Not suitable topic for this course

- For brief overview of instructions involved, see Moore p 175 ff
  - □Microsoft OSs



✓ Windows 3.11 through XP

- □Macintosh
- <mark>□Unix/Linux</mark>
- Special tools for PDAs (e.g., Palm, Windows

CE)





#### **Laptop Computers**

- Problem: unplugging laptop instantly switches to battery power
- Need to remove battery from laptop
  - □Usually easy



UNIVERS

□Simple latch or an easy screw or two

Keep battery with laptop for bagging & shipment



\* TRS Model 100 from 1983 *Computer Desktop Encyclopedia* Used with permission. Prof Kabay's very first portable!



#### **Disassembling** Computer

- Critically important that each computer can be reassembled exactly as it was
- Identify each computer with unique identifier
- Label absolutely every component with its computer's identifier
  - **Particularly the ports**
  - Mask and mark ports not in use
  - Masking tape or colored labels are fine
  - Colors can be assigned to specific computers
- Show directions of connectors (which end to which computer and port)



#### Moore p 179 ff

#### Securing Additional Evidence (1)



- How much peripheral equipment should you seize?
  - □Terms of warrant
  - □Peculiarities of system (e.g., old)
- Peripherals may have evidence □Cameras, games (XBox, PSPs)





- □Scanners (check the scanner bed)
- Sound recorders, iPods (can even carry computer data or operating environments)\*
- Calculators (large memory)
- Other evidence

- \*Thanks to Ryan Davis & Stanley François
- □Paper notes and documents
- Digital storage media (magnetic & optical disks – but remember old tape systems)
- □Label evidence bags in detail (where, who...)

#### **Securing Additional Evidence (2)**



Already mentioned obvious devices **DPDAs, cell phones, data-watches** USB flash drives may not be obvious □May look like pens □May look like ... wait for it ... sushi!









#### **Preparing for Transport**

- Complete asset-seizure log
  - Provide copy to suspect
  - □ Get suspect to sign log sheet
  - Note refusal & have OIC sign sheet
- Bags or boxes depending on agency
  - □ Do not use Styrofoam static electricity
  - Disk drives that take mobile media (floppies, CDs) should have blanks inserted to prevent damage in transit
- DO NOT PUT IN TRUNK OF CAR
  - Heat & electronic gear can harm evidence
  - □ Place on floor or on storage surface





#### **Chain of Custody**

- Standard concerns about maintaining credible protection of evidence in custody
- NEVER allow evidence to be unsecured at any time
- Digital evidence can be altered at any time
- > Unique identification to ensure credibility in court
- Detailed records of who accessed the evidence at what time and for how long
- Provide detailed records of why individuals needed access to evidence
- Ideally, original data must never be released keep for comparison with digital bitwise copies if anyone challenges authenticity



# **BREAK 11'3'**

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### **Analysis of Evidence**

- Introduction to Computer Forensics
  - **How Computers Store Data**
  - Internet Activity Stored on Disk
- Computer Forensics Process
  - Verifying Files and File Signatures
    - □ Forensic Analysis
    - □ Forensics Report
- Concealing Evidence
- Computer Forensics Software Packages
  - □EnCase
  - □Forensic Tool Kit
  - □Non GUI Software Utilities





#### **Introduction to Computer Forensics**

Forensic science

□Latin *forensis* = "of legal proceedings from *forum* where discussions take place"

Application of scientific techniques to criminal investigation

Presentation of evidence at trial

> Growing value to computer forensics

Increasing role of computers throughout human activity, including crime

Persistence of digital trail useful as evidence

Opportunities for employment in LE and in private industry
Moore Ch 19

Moore Ch 19 Clifford Ch 3 pp 160-174 NIJ Guide for First Responders pp 27-46



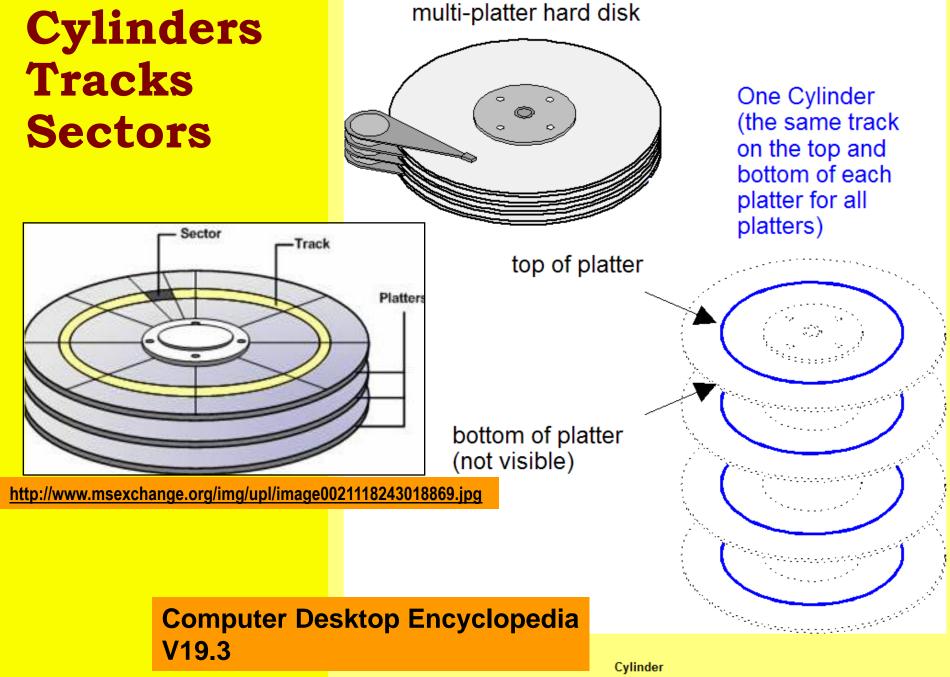
#### **How Computers Store Data**

#### (c) helpwithpes.com

#### fig 1.1

- A Platter/s
- **B Read/Write Head/s (and slider)**
- **C** Actuator Arm/s
- **D** Actuator
- **E Spindle**

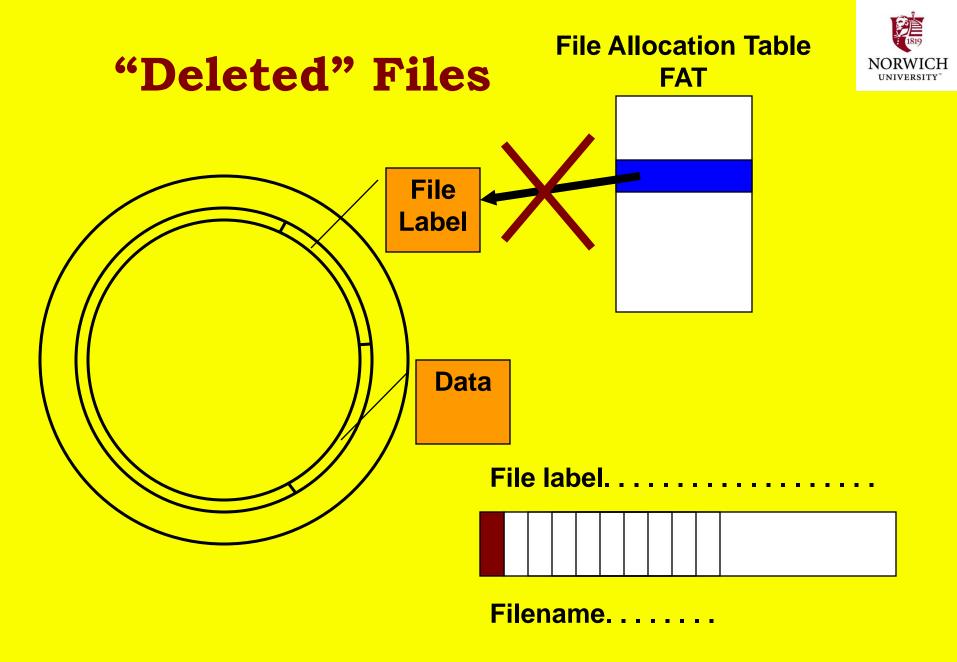
#### http://www.helpwithpcs.com/courses/hard-drive-mechanics.htm



**106** 

Copyrig

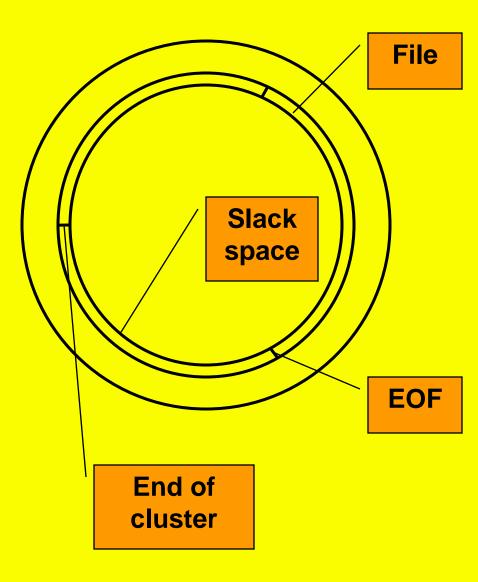
The cylinder is the aggregate of the same track number on every platter used for recording.





#### **Slack Space**

- Unused space between EOF and end of cluster is slack space
- May contain uninitialized data from previous (different) file use



#### Internet Activity Stored on Disk



Folder Options ? 🗙	Folder Options ? 🗙
Gene al View       ile Types       Offline Files         Tasks <ul> <li>Show common tasks in folders</li> <li>Use Windows classic folders</li> </ul> Browse folders <ul> <li>Open each folder in the same window</li> <li>Open each folder in its own window</li> </ul> <ul> <li>Open each folder in its own window</li> <li>Open each folder in its own window</li> <li>Open each folder in its own window</li> </ul> <ul> <li>Open each folder in its own window</li> <li>Open each folder in its own window</li> </ul> <ul> <li>Open each folder in its own window</li> <li>Underline icon titles consistent with my browser</li> <li>Underline icon titles only when I point at them</li> <li>Double-click to open an item (single-click to select)</li> <li>Restore Defaults</li> </ul>	General       View       File Types       Offline Files         Folder views       You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.         Apply to All Folders       Reset All Folders         Advanced settings:       Automatically search for network folders and printers         Ø Display file size information in folder tips       Image: Display the full path in the address bar         Ø Display the full path in the title bar       Do not cache thumbnails         Ø Display the full path in the title bar       Do not show hidden files and folders         Ø Display the full path in the title bar       Do not show hidden files and folders         Ø Hidden files and folders       Show hidden files and folders         Ø Hide extensions for known file types       The extensions for known file types
OK Cancel Apply	OK Cancel Apply

#### Internet Activity Stored on Disk



C:\Documents and Settings\HP_Administrator\Local Settings\Temporary Internet Files				
<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp				
🔆 Back 🔻 🕥 👻 🦻 Search 📂 Folders 🛛 🎹 🗸				
Address 🔂 C: \Documents and S	5ettings\HP_Administrator\Local Settings\Temporary Internet Files 🛛 🔽			
	Cookie:hp_administrator@www.laplink.com/			
Folder Tasks 🛛 🕆	Cookie:hp_administrator@www.fortinet.com/			
😂 Share this folder	Cookie:hp_administrator@www.wildpackets.com/			
	📃 Cookie:hp_administrator@moodle.org/			
	🗉 Cookie:hp_administrator@advancedmn.com/			
Other Places	Cookie:hp_administrator@moodle.norwich.edu/			
🕞 Local Sattings	🗐 Cookie:hp_administrator@haengr.com/			
Local Settings	Cookie:hp_administrator@chevron.com/			
My Documents	Cookie:hp_administrator@www.wcva-cru.org.uk/			
Shared Documents	🗒 Cookie:hp_administrator@armee.axogyg.info/			
🧐 My Network Places	🗒 Cookie:hp_administrator@www.ihi.org/			
	Cookie:hp_administrator@ihealthbeat.org/			
Details ¥	Cookie:hp_administrator@www.ihealthbeat.org/			
Details ×	Cookie:hp_administrator@cisco.com/			

#### Internet Activity Stored on Disk



Internet Options 🛛 🔹 🔀
General Security Privacy Content Connections Programs Advanced
Home page You can change which page to use for your home page. Address: http://grad.norwich.edu/msia
Use <u>C</u> urrent Use <u>D</u> efault Use <u>B</u> lank
Temporary Internet files         Pages you view on the Internet are stored in a special folder for quick viewing later.         Delete Cookies         Delete Eile         Settings
The History folder contains links to pages you've visited, for quick access to recently viewed pages.
Days to keep pages in history: 20 🕂 Clear History
Colors Fonts Languages Accessibility
OK Cancel Apply

Settings ? 🗙
Check for newer versions of stored pages:
Every visit to the page
Every time you start Internet Explorer
Automatically
C Never
Temporary Internet files folder
Current location: C:\Documents and Settings\HP_Administrator\Local Settings\Temporary Internet Files\
Amount of <u>d</u> isk space to use:
- 4511 🕂 MB
Move Folder View Objects
OK Cancel

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### Internet Activity Stored on Disk

С

112

🗎 C: \Documents and Settin	{P_Administrator\Local	Settings\Temporary Internet Files
<u>File Edit V</u> iew F <u>a</u> vorit	<u>T</u> ools <u>H</u> elp	
🕞 Back 🔻 🕥 🔻 🏂 🔒	5earch 😥 Folders 📔	
Address 🔂 C:\Documents ar	ttings\HP_Administrator	r\Local Settings\Temporary Internet Files
Folder Tasks	🖻 menuicon.jpg	
Folder Tasks	🔊 menuimage.gif	
😂 Share this folder	esdcxmIM.png	
	cinemanow×mlM.png	
Other Places	menuicon.png Cookie:hp_administra	ntor@img.wmp10.elsitiodc.com/
	Cookie:hp_administra	
Local Settings	sm_menu_logo.png	nor envests.com/
My Documents	MM-logo-16x16-xp.gi	f
Shared Documents	16_16_ico.gif	
😼 My Network Places	fye_multiicon_16x16	.png
	audible_a_icon_15T.	
Details	icon_15x15.png	
Details	logo_kitty_16x16.png	1
	🗐 servicexml.aspx?loca	le=409&geoid=f4&version=10.0.0.4036&userlo
	🖻 MPS_My_Station_ica	on_16x16.png
	🖻 MenuIcon.jpg	
	🖻 menu_image_s.png	
	🔰 sgmsn_imageurl.gif	
	🔰 logo-15x15.png	
	novielink-icon_15x15 👱	
	wmp10_musicd_icon_	_16×16.png
	lcIAdv.xml	
	lclsrch.xml	
	🖬 bar.xsl	
	🖬 Iciprog.xml	
	🖬 Icirfine.xml	
	plugins.xml     Cookie:hp_administra	tonQuadate claudmark.com/
		ntor@update.cloudmark.com/ 17EC4468-76A0-49FB-B050-A39660F69E30}
	Germessages.asp??={ supported_domains	1/ CC++00-/ 0A0-+91 B-B050-A59000F09E50}
	Pina.asp	



## **Computer Forensics Process**

Copy entire hard disk(s) Disks typically now 100 GB and up □CD-ROM now too small (700 MB) □Even DVDs too small (4 or 8 GB) □Separate medium – new *hard disk* best ✓ 250 GB Western Digital USB for \$100 ✓1 TB Maxtor external drive for \$200 Make bit-for-bit copy (bit-image) □Ordinary *copy* reads file, creates new file ✓ Lose all data in deleted files ✓ Lose all data in slack space □Bit-image copies everything



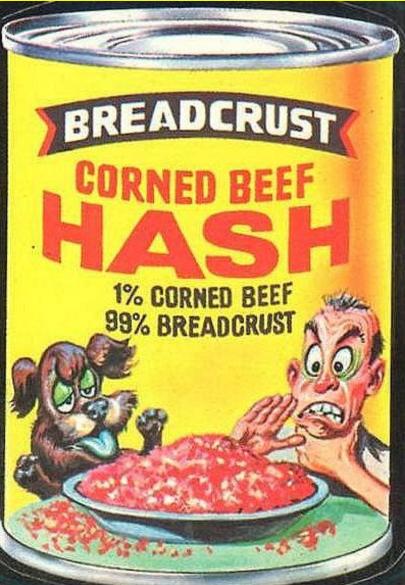




## **Digitally Securing Evidence**

How can one mark digital data so that any change, even to just one bit, flags the copy as bad?

Three approaches
 Hash
 Encryption
 Digital signatures



## Hashing

- HASH FUNCTION: An algorithm that turns a variable-sized amount of text into a fixedsized output (hash value). Hash functions are used in creating digital signatures, hash tables and short condensations of text for analysis purposes (see hash buster). Hash functions are also known as "cryptographic hash functions."\*
- E.g., MD5 (Message Digest 5)\*\*
- Results look something like this:
  - Input: "The quick brown fox jumps over the lazy dog."
  - □ (Made-up) Output: 8u3J50pW
- SHA-512 another popular algorithm\*\*\*

\* Computer Desktop Encyclopedia, v 21.3. Copyright © 2008 Computer Language Company, Inc. All rights reserved. \*\* <u>http://www.ietf.org/rfc/rfc1321.txt?number=1321</u> \*\*\* http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf



🔄 MD5 Decoder			×
<u>F</u> ile <u>H</u> elp			
Paste MD5 Strin	g Here: ——		
5F4DCC3B5	5AA765D61D832	7DEB882CF99	
- Select Dictionary	y:		
C:\M	1D5decoder\com	imon.txt	
Browse	Text file that ha	is possiable choic	es.
Found As \ 18720 of Word	28263		!
	password		
L			

\*\*\*Thanks to Chris Tanguay



## Hashing (cont'd)

- Hashing functions are designed so that any change to the input produces a different output
- E.g. (made-up, not real):
  - □"TIquick brown fox jumped over the lazydotcould hash to "8u3J50p₩"
  - □"Th. quick brown fox jumped over the lazy dog!" could hash to "Y35\_e) t7k"
- Thus keeping a copy of all data with hash function output, one can identify changed

data.

#### Using Hash Function for File Inventory

FileList utility
 Every single file on disk
 Directory tree format

Most important: MD5 hash

Exploring - E:\CompuServ	va \ Dewelaad	- 🗆 ×
	rites <u>T</u> ools <u>H</u> elp	
Back Forward	Up Cut Copy Paste Undo Delete Propert	ties Views 🗸
Address 🗋 E:\CompuServe\D	Download	•
Folders	× Name Size M	Nodified 🔶
● ● My Computer           ● ● PSYS_PROG (C)           ● ● OFSYS_PROG (C)           ● ● OFSYS           ●	23 Aug NIPC DailyV2.doc         163K8         2           27 Aug NIPC Daily.doc         149K8         2           28 Aug NIPC Daily.doc         149K8         2           29 Aug NIPC Daily.doc         167K8         2           29 Aug NIPC Daily.doc         167K8         2           20 Aug NIPC Daily.doc         9K8         2           20 Aug NIPC Daily.doc         10K8         2           20 Aug NIPC Daily.doc         10K8         2           20 Biol Disclor Collor         102K8         2           20 Biol Disclor Equip (1)2.02 fs.doc         10K8         2           20 Director Guide (1)2.02 fs.doc         40K8         2           21 Director Guide (1)2.02 fs.doc         40K8         2           21 Director Werview082002.pdf         250K8         2	002-07-21 21:47 002-08-28 06:41 002-08-28 06:41 002-08-28 11:14 002-08-30 21:10 002-08-30 21:10 002-07-19 19:12 002-07-19 19:12 002-07-19 19:12 002-07-19 19:14 002-07-19 19:19 002-07-19 19:19 002-07-19 19:21 002-07-19 19:21 002-08-22 18:18 002-08-22 18:18 002-08-22 18:18 002-08-22 18:18 002-08-20 02:16 18 002-08-20 18:18 002-08-20 18:18 002
	13.6MB (Disk free space: 3.30GB) 🛄 My Compu	iter //

□Applied to *copy* of original disk

- **Every file marked with** *hash*
- Nearly impossible to alter file without altering hash

Unchanged MD5 hash value is very strong evidence that files have not been altered since the hash was originally calculated

## **Digital Signatures**



- Digital signatures encrypt a hash
- Quicker than encrypting entire source
- Many different tools available for such signature
- Legally recognized as evidence of data integrity
- Can also indicate exactly who signed document
- Contributes to chain of evidence by tying specific analyst to digital copy

#### Digital Signatures Before and After Single-Character Change



## ≻Hi there.

wj8DBQFJBek/UbF73uXqlJ8RA iWVAKDnsmqVn64zcKseFCqecC cHD6xytQCgn+8kT8jUtvEhucb jQXpkqYs66pw==rI4S

## ≻Ho there.

> wj8DBQFJBelkUbF73uXqlJ8R AsHPAKCNrCfv6+N8WDi4V7Pb Hwz62SGwwwCdHAesXOwawwKT zuSvsOqh0DvfovA==0w8t

> Signatures created using Prof Kabay's PGP *private* key.

🔊 Mich Kabay - Key Properties 🗕 🗖 🗙				
🖅 Add Email Address 🛛 📔 Request Certificate 🛛 🏚 Change Passphrase				Passphrase
	Mich Ka	ıbay	mekabay@g	mail.com
-	ID	0xE5EA949F 👻	Created	2002-10-31
THEY CONSTRUCT	Туре	DH/DSS	Expires	Never 🔻
and the second	Size	2048/1024	Group	No 🔻
10 - SA	Trust		Cipher	CAST V SHA-2 256 V
	Verified	Yes	Hash	None V
	Enabled	Unspecified 🔻	Compression	None *
🕘 🔳 🕒	Encoding Keyserver	ldap://keyserver.	pap.com 🔻	
			Copy	
	Hexadecimal Biome	etric		1
	shamrock infer drunken phot	guard mural	enrollment corrosion everyday telephone opulent	
✓ Subkeys Subkeys Subkeys Add				
ID	Valid from	Expires	Size	Usage
0x59BD7D72	2002-10-31	Never	2048	
ADK		🔇 Updat	te 😑 Remove	🕂 Add
Revokers		🔍 🔍 Updat	te \varTheta Remove	🕂 Add

#### Prof Kabay's PGP *public* key.

#### Verifying Files and File Signatures



- Create digital signature for disk contents
  - □Typically use MD5 *hash*
  - Effectively impossible to modify contents of original disk without changing hash

05 Check Utility v2.31 - Freeware from TSoft - www.midwav	i.com 🔣
Please Paste In The MD5 Code 3DB153EFBC96D90EDE3382B21C021650 MD5.ZIP	
3DB153EFBC96D90EDE3382B21C021650	Browse
The Codes Match! Selection ⓒ ⊻erify an MD5 checksum ⓒ <u>C</u> reate an MD5 checksum	
	<u> </u>

- Analyze files to detect altered file types
  - Can crudely hide data by pretending that images are documents (etc)
  - Forensic packages can detect such subterfuges
- Error on p. 196 of Moore (Chapter 10): author meant "algorithm" where "logarithm" is written in paragraph beginning "The MD5 logarithm...."

## **Concealing Evidence**



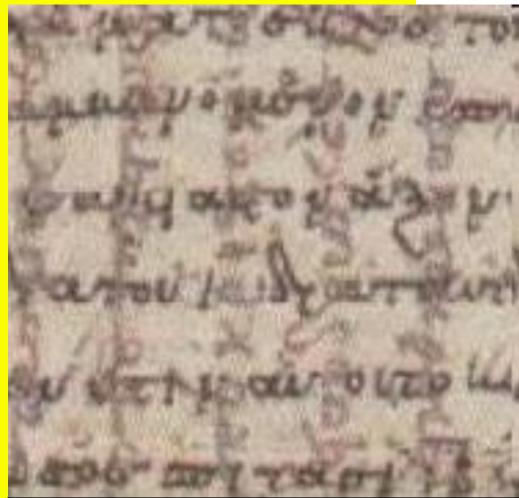
- Stop people from finding or capturing information
  - Prevent penetration of system perimeters
- Stop people from using information
  Encryption
- Stop people from knowing there's any information
  - Misleading directory and file names
  - □Misleading file types
  - Information hiding: steganography





## Hard to Find

- Secret compartments (furniture, clothing, luggage)
- Messages placed inside books, in book covers...
- Palimpsests: overwriting or overpainting



The Archimedes Palimpsest discovered 1899 in Istanbul. Original Greek (3rd century BCE) was overwritten at 90° in 12<sup>th</sup> century CE by Greek Orthodox monks in Constantinople.

Image from < <u>http://www.artlex.com/ArtLex/P.html</u> >

#### Hard to See



#### Invisible ink

Substances change from colorless to colored upon treatment (heat, UV light...) Milk, lemon juice, cobalt chloride solution > Microdots Invented by Germans during WWII Images at high resolution □Shrunken to tiny size – usually that of period (.), dots on i, j or umlauts (ö) in text Read with microscope if you knew where to look

\* Mark IV microdot camera < <u>http://en.wikipedia.org/wiki/Microdot</u> >



## Hard to Notice

- Coded language
  - Writing, speech, symbols in pictorial art
  - Shared code-book + start-point permits decoding (not decryption) of meaning
  - E.g., "The ship sails at midnight" = "Meet Bob on Thursday"
- Chaffing and winnowing
  - □Ron Rivest (1998)



Cipher for Telegraphic Correspondence — a code book used by Union General Joseph Hooker's code clerk (From Answers.com <u>http://tinyurl.com/6gguav</u>)

- Output large volume of info, hide small amounts of significant data
- □ See < <u>http://theory.lcs.mit.edu/~rivest/chaffing.txt</u> >
- Steganography
  - Embedded information in music, pictures, numbers and data communications
  - DExtract hoving the 2008 M. F. Kabay J. Jower-Pierce & P. R. Stephenson. All rights reserved.

#### Searching for Hidden Information

- Intelligent filters
  - □ Filter\_I used only on copy of original data
    - <u>http://www.forensics-intl.com/filter\_i.html</u>
    - ✓ Removes binary data from output
    - ✓ Eliminates useless ASCII strings
    - ✓ Use in multiple passes, step by step
- Slack space & free space
  - Getslack (<u>http://www.forensics-intl.com/getslack.html</u>) & Getfree (<u>http://www.forensics-intl.com/getfree.html</u>)
  - □ Convert these types of disk data into files
  - □ Can also create files from swap and cache
- Steganography and steganalysis
   Hiding data in low-order bits of a file
   E.g., putting text inside a picture file
   See following slides













## Steganography

#### Steganography = information hiding

- □Greek: secret writing
- Hiding existence of message or other data
- Different from cryptography, which hides the *meaning* but not *message* itself
- Sometimes referred to as using covert channels
  - E.g., could conceal text in low-order bits of cells of a spreadsheet

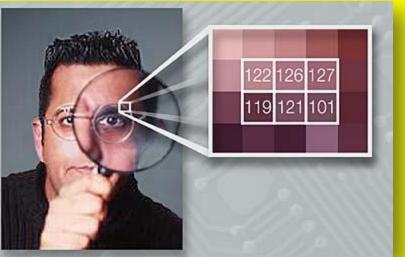


Illustration from article by Rachel Thomas (2002), "Safety in numbers" in *+plus magazine* (21), Sept 2002. < <u>http://tinyurl.com/6yalbs</u> > Used with permission.

- Currently most popular using images and music as channels for message
- Press reports claim terrorists are using steganography – but see later slides

## **Example: Covert Channel Using Low-order Numbers**

Original data	Msg	ASCII	Data + msg
0.982828	Т	84	<mark>0.982828</mark> 084
0.982060	h	104	<b>0.982060</b> 104
0.982530	е	101	0.982530 <mark>101</mark>
0.982988		32	0.982988 <mark>032</mark>
0.982032	q	113	<b>0.982032</b> 113
0.982590	u	117	0.982590 <mark>117</mark>
0.982908	- I -	73	<b>0.982908</b> 073
0.982544	С	99	<b>0.982544</b> 099
0.982742	k	107	<b>0.982742</b> 107

#### **Example: Steganography Using a JPG Image**





"The top image of Voyager contains no stego and is not featured in the search engine's output. However, the second image contains a 10K text file encoded with JSteg...."

**Copyright © 2008 F. C. Gonzalez. All rights reserved. Used with permission.** 

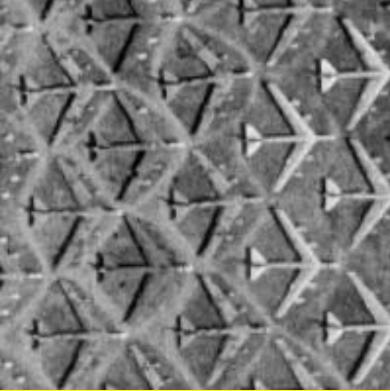
http://mscmese.tripod.com/steg/

## Steganography using JPG (cont'd)



Niels Provos & Peter Honeyman

- University of Michigan Center for Information Technology Integration
- Scanning Web for steganography
- Located sovereigntime.jpg
   Shown on ABC TV program
   Retrieved concealed image embedded in JPG – B52s



#### ONLY case found in 2,000,000 images checked

http://www.citi.umich.edu/projects/steganography/faq.html



## Why Use Steganography?

To avoid notice

- Some governments ban unauthorized use of encryption
- Obvious encryption may draw unwanted attention to its users
- Encrypted traffic may be susceptible to data-flow analysis (e.g., identifying areas of greater operational importance)



 To embed secret information in documents or other files to help protect copyright
 Allow copies to be identified or traced
 Called Digital Watermarking



## **Steganography Tools**

- Medium + message + stegokey = stego-medium
- Freeware, shareware, commercial programs available



□List of over 80 programs at

http://www.stegoarchive.com/

- Many use JPG picture files as carrier
- Scramdisk creates virtual encrypted drives by using a WAV audio file as output
- > MP3Stego program hides data in MPE audio files
- Sam's Big Play Maker hides data in a postmodern play (mostly gibberish)

http://www.scramdisk.clara.net/play/playmaker.html

## Sam's Big Play Maker



Sams big G play maker	2
General Wordlists Equiv.	
Original token:	Replacement:
! 	Ouch Get off my colon I take my hat off to you I'm not sure if I like it You are a little star Trade secret my arse Who knows sql? That is a bonus I need a slash Who said OJ? Do not take it away! Don't be Mike
a a	What keyboard? Mine's a pint
b c d e f g h i i k	I'd say Thursday Show me the fish! Mike - you ladyboy! Did he mean to die just then? I'm so excited And I just can't hide it I love you, no really. I said, you've got beautiful eyes. Has anyone noticed the plot is straying from well re I'll be your private dancer, a dancer for money, I'll do v



#### Steganalysis

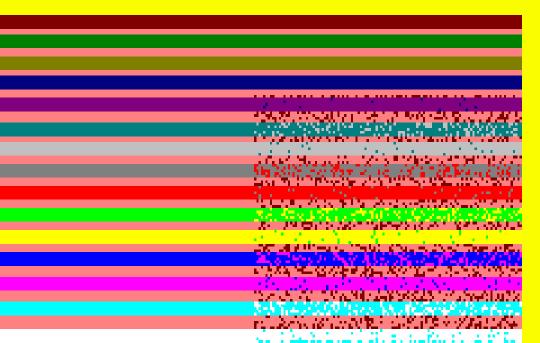
Tools available to identify and reconstitute hidden messages

Carrier-information degradation problem

Any modification of data in original file degrades quality

✓ Image✓ Sound

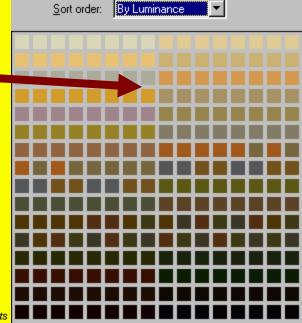
Copyright © 2009



## **Steganalysis (cont'd)**

- Some stego tools generate signatures
  - Statistical techniques use many modified images to identify signatures
  - Can identify repetitive patterns
  - Spot abnormal palette colors in images







#### **Forensic Analysis**

- Examine only bit-image copies of original disks
- Can analyze every file
- Locate files of specified types
- List all file and real types
- Search contents of files for strings
- Search deleted files
- Search unallocated space
- Can take days of work





#### **Forensics Report**

Written report

- □Can be partly software-generated
- Explain exactly how searches were performed
- Detail exact locations of evidence
- Useful in many ways
  - Help prosecutor decide whether to charge suspect



- Help persuade perpetrator to plea-bargain
- □Support testimony in trial



#### **Computer Forensics Software Packages**

GUI-based packages Helpful for LEOs with less experience ✓ EnCase from Guidance **Software** ✓ Forensic Tool Kit from AccessData Command-line interfaces

> Require expert to know command language



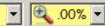






- Preview allows selection of which disks to image (can save time)
- Extensive training available
- Ability to image disk without removal from case
- Extensive automated search capabilities
- <u>http://www.guidancesoftware.com/</u>

Home > EnCase Forensic



#### > products and services > company > resources > support > message boards

#### Guidance

#### **EnCase Forensic**

Modules

Hardware

#### **Brochures:**

EnCase® Forensic for Corporations(PDF)

EnCase Forensic for Law Enforcement and Government(PDF)

#### Webinars:

EnCase Forensic Feature Series - Part I: Installation of EnCase Forensic Version 5

EnCase Forensic Feature Series - Part II: EnCase Forensic Version 5 Interface

EnCase Forensic Feature Series - Part III: EnCase EnScripts and More

#### Whitepapers:

Restore Validation (PDF)

EnCase Forensic Hardware Requirements (PDF)

Computer Hardware Recommendations for EnCase Forensic and EnCase Enterprise (PDF)

CLICK HERE TO SEE ALL WHITEPAPERS



#### EnCase Forensic

> Acquire data as evidence with the leading court-validated solution on the market.

#### About EnCase® Forensic

- How it Works
- <u>Detailed Product Description (PDF)</u>
- System Requirements
- <u>Screenshots</u>

EnCase Forensic is the industry standard in computer forensic investigation technology. With an intuitive GUI, superior analytics, enhanced email/Internet support and a powerful scripting engine, EnCase provides investigators with a single tool, capable of conducting large-scale and complex investigations from beginning to end. Law enforcement officers, government/corporate investigators and consultants around the world benefit from the power of EnCase Forensic in a way that far exceeds any other forensic solution.

- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide.
- Investigate and analyze multiple platforms Windows, Linux, AIX, OS X, Solaris and more — using a single tool.
- Save days, if not weeks, of analysis time by automating complex and routine tasks with prebuilt EnScript® modules, such as Initialized Case and Event Log analysis.
- Find information despite efforts to hide, cloak or delete.
- Easily manage large volumes of computer evidence, viewing all relevant files, including "deleted" files, file slack and unallocated space.
- Transfer evidence files directly to law enforcement or legal representatives as necessary.
- Review options allow non-investigators, such as attorneys, to review evidence with ease.
- Reporting options enable quick report preparation.

#### REQUEST A QUOTE REQUEST MORE INFORMATION

**Bundled Solutions** 

Three Years of Upgrades, Modules and Support with the Premium Licence Support Program (PLSP)

Software and Modules with EnCase Corporate Deluxe

EnCase ProSuite

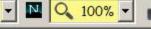
Hardware, Software, Training and Support with EnCase Cybercrime Arsenal



## **Forensic Tool Kit (FTK)**

## A Pioneer in Digital Investigations Since 1987

- Similar to EnCase + improvements
- E-mail search
- Import image files in wide variety of formats
- Password-cracker (Password Recovery Tool Kit, PRTK)
- Distributed Network Attack (DNA) for parallel processing of decryption tasks
- <u>http://www.accessdata.com/</u>





SOLUTION PRODUCTS SERVICES TRAINING NEWS SUPPORT COMPANY

#### FORENSIC TOOLKIT®

Forensic Toolkit Enterprise eDiscovery SilentRunner Lab Classified Spillage Solution Mobile Phone Examiner Decryption Tools

#### Request More Information



#### GET FLEXIBILITY WITH FORENSIC TOOLKIT<sup>®</sup> 2.0!

Memory-based or database-driven technology?

Which one meets your needs? Purchase FTK and get both 1.80 & 2.0!

Options are good ....

DOWNLOAD RESOURCES

Forensics Brochure > AccessData Legal Brief > Laci Peterson Case Study >



FTK @ 2.0 Webinar Series >

- Introduction to FTK 2.0
- FTK 2.0 Interface Overview
- · User and Case Management
- Filtering Basics
- Backup & Restore
- Evidence Refinement and Processing
- Evidence Review Tool (Quickpicks)
- Understanding Search
- Password Cracking

Forensic Toolkit® (FTK®) is recognized around the world as the standard in computer forensic investigation technology. This court-validated platform delivers cutting edge analysis, decryption and password cracking all within an intuitive, customizable and user-friendly interface. In addition, with FTK, you have the option of utilizing a back-end database to handle large data sets. Or you can work without one if application simplicity is your goal. Either way you will get the benefit of best-of-breed technologies that can be expanded to meet your ever-changing needs. Known for its intuitive functionality, email analysis, customizable data views and stability, FTK is the smart choice for stand-alone forensic investigations.

#### PRODUCT FEATURES

#### An Integrated Solution

- Create an image, view the registry, conduct an investigation, decrypt files, crack passwords, and build a report all with a single solution.
- Recover passwords from over 80 applications; harness idle CPUs across the network to decrypt files and perform robust dictionary attacks.
- Full Unicode and Code Page Support lets you search, display and report on data in its native format, in any language Unicode supports.
- Industry-leading data carving engine allows you to specify criteria, such as file size, data type and pixel size to reduce the amount of irrelevant data carved while increasing overall thoroughness.
- + Leverage a number of different integrated viewers and an integrated media player to



## **Non GUI Software Utilities**

- Less expensive than GUI-based tools
- E.g., Maresware Utility Suite
  - Available through Norcross Group as of July 2005
  - Product description at <u>http://www.maresware.com/maresware/suite.htm</u>
- Features
  - □Very fast
  - Provides scripting for automated analysis
  - Complete control of analytical sequence
     Audit trail





# BREAK

# 5'19"

<mark>143</mark>

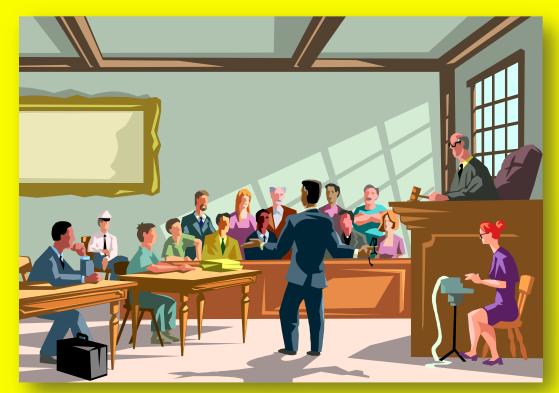
Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

#### NORWICH UNIVERSITY"

#### Use of Seized Materials & Results in Evidence

Admissibility of Digital Evidence
 The Courts & Digital Evidence
 Admission of Digital Evidence at Trial

Moore Chapter 11 Clifford Chapter 3 pp 174-186 SSCOEECI §V (PDF pp 119-128).





#### Admissibility of Digital Evidence

> US v. Liebert (1975)

Could computer records for alleged federal tax-evader be admitted as evidence?

□Yes, provided

 Prosecution could prove digital data were accurate and authentic

Defense was given opportunity to check

Resistance to admitting digital evidence continued

Based on Federal Rules of Evidence
http://www.law.cornell.edu/rules/fre/

Includes hearsay, authentication, nature of writings & copies



#### Hearsay

- Rule 801: "...statement, other than one made by the declarant...."
- Rule 801(d)(1) permits digital evidence such as e-mail or Web postings if
  - Statement contradicts sworn testimony
  - □Statement rebuts accusation of lying
  - Statement helps identify person





## **Authentication (1)**

- Authentication validates evidence
- Rule 901(a) requires authentication
  - One method uses selfauthentication mostly



involving public records and certification (rarely works for digital evidence)

Other approach involves authentication by a qualified professional

Prof Moore argues that only 2 of the Rule 901 subclauses apply to digital evidence: both involve testimony of expert witnesses



#### **Nature of Writings**

- Rule 1002: specifies that original "writing, recording or photograph" must be available to authenticate copies presented in evidence
- Rule 1001(1) stipulates that writings and recordings include "letters, words, or numbers, or their equivalent, set down by...magnetic impulse, mechanical or electronic recording, or other form of data compilation."
- Rule 1004: allows for admission of bit-images of forensic data



#### Copies

Rule 1004 allows submission of copies when

- Originals are lost or destroyed
  - But verifiable copies make it easy to present in court given hash functions, proper bit-image
- Original is not obtainable
  - Usually have to return equipment to suspect



- But data may be destroyed by suspect
- Original is in possession of opponent

Suspect may refuse to grant access to original data

#### The Courts & Digital Evidence



#### Frye v. US (1923)

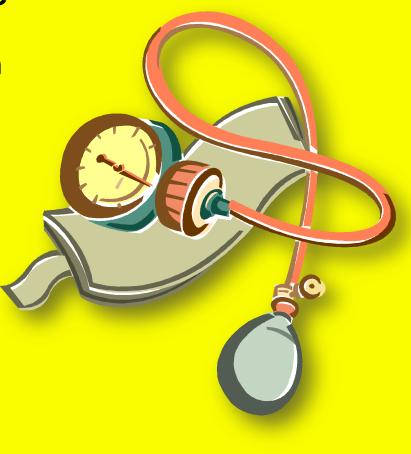
- Daubert v. Merrell Dow Pharmaceuticals (1993)
- State v. Hayden (1998)
- People v. Lugashi (1988)
- US v. Scott-Emuakpor (2000)
- Williford v. State (2004)





## Frye v. US (1923)

- Could scientific evidence about blood pressure and effects on polygraph evidence be introduced at trial?
- Court ruled that evidentiary collection had to cross line from experimental to demonstrative
- Set standard that evidence must be "generally accepted in scientific community"





#### **Daubert v. Merrell Dow Pharmaceuticals (1993)**

- Woman claimed drug company caused birth defects
- Offered scientific studies showing relationship
- Court required method to conform to general acceptance in scientific community using Frye
- SCOTUS overturned verdict



□Scientific evidence need only be reliable and scientifically valid

□Now known as the *Daubert Test* (see next slide)

#### The Daubert Test

Has the scientific theory or technique been empirically tested? According to K. Popper (1989) in The Growth of Scientific Knowledge, "the criterion on the scientific status of a theory is its falsifiability, refutability, and testability."

**ICH** 

- Has the scientific theory or technique been subjected to peer review and publication? This ensures that flaws in the methodology would have been detected and that the technique is finding its way into use via the literature.
- What is the known or potential error rate? Every scientific idea has Type I and Type II error rates, and these can be estimated with a fair amount of precision. There are known threats to validity and reliability in any tests (experimental and quasi-experimental) of a theory.
- What is the expert's qualifications and stature in the scientific community? And does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?
- Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? This is just the Marx standard, which is assumed to be incorporated in Daubert as it was with Frye.

Quoted from <a href="http://faculty.ncwc.edu/toconnor/425/425lect02.htm">http://faculty.ncwc.edu/toconnor/425/425lect02.htm</a>

153



#### State v. Hayden (1998)

- Hayden charged with rape and murder
- Difficulty obtaining fingerprints from bloody sheet
- Forensic specialist used digital photography and computer enhancement to develop fingerprint
- Challenged in court not approved technique



- Prosecutors argued that all steps were scientifically sound
- Court rejected argument, suppressed evidence



#### People v. Lugashi (1988)

- Case involved theft of creditcard data from backup tapes
- Forensic investigator could not explain details of how forensic software worked



- Defense argued for suppression of evidence
- Court ruled that expert had sufficient experience with software to warrant confidence

Relying solely on experts who understood all details of all hardware & software would limit testimony & impede justice



# Nigerian advance-fee fraud

- Secret Service investigators searched defendant's computer □Found evidence of crime
- Defense argued that SS officials were not computer experts and evidence should be suppressed
- Court ruled that SS agents were sufficiently expert in use of forensic tools to qualify as witnesses

#### Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.







## Williford v. State (2004)

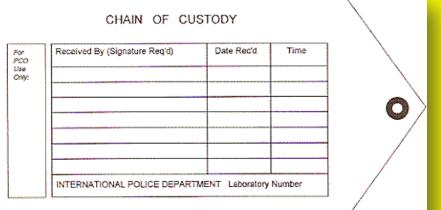
- Computer repair tech found child porn on computer
- Police investigator made bit-image of suspect's HD using EnCase
- Investigator challenged at trial over lack of computer-science education
- Prosecution argued that extensive training in use of EnCase + reliability of software itself warranted admission of evidence
- Court ruled in favor of prosecution (2003)
  - Officer did qualify as expert for purposes of presenting digital forensic evidence
  - EnCase satisfied requirements for admission as scientific evidence
- > Appeals Court of Texas supported decision (2004)



#### Admission of Digital Evidence at Trial

NORWICH UNIVERSITY

- Additional criteria for admissibility
  Authentication
  - □Chain of custody
- Authentication based largely on digital signatures or hashes
- Chain of custody requires minute attention to detail
  - Every person in contact w/ evidence is opportunity for challenge
  - □Must have valid reason for access
  - Detailed records of involvement



#### Supporting the Chain of Custody



#### Chain-of-custody log should include critical elements Moore p 213

- Evidence inventory number
- Date and Time

Moore p 213 Also "Chain of Custody" By R. L. Trench of the Intl Assoc Property & Evidence

- Who Removed the Evidence <a href="http://tinyurl.com/6febwf">http://tinyurl.com/6febwf</a>
- Location Removed and Taken To
- Reason Evidence Being Removed
- Date of return

Item #	International Police Department Property Sign-Out Sheet					Case Number	
	0	UT				IN	
Date and Time Out	Property Rec'd by print name/id#	Signature	Released by	Reason or Destination (Court, DA, Lab, RTO, etc.)	Property Returned by	Date and Time Property In	Property Officer's Signature
				<u> </u>		La contraction of the second s	



# Now go and study\*

\*A Roman prankster once sneeringly asked the famous Jewish sage Hillel the Elder (110 BCE-10 CE), "Can you teach me the whole of the Torah while I stand on one foot?" Hillel answered, "The whole of the Torah is this: what is hateful to you, do not do to others. All the rest is commentary. Now go and study."