BKD Forensics Institute

Computer Forensics: More Places to Look – Social Networking & Cell Phone Evidence

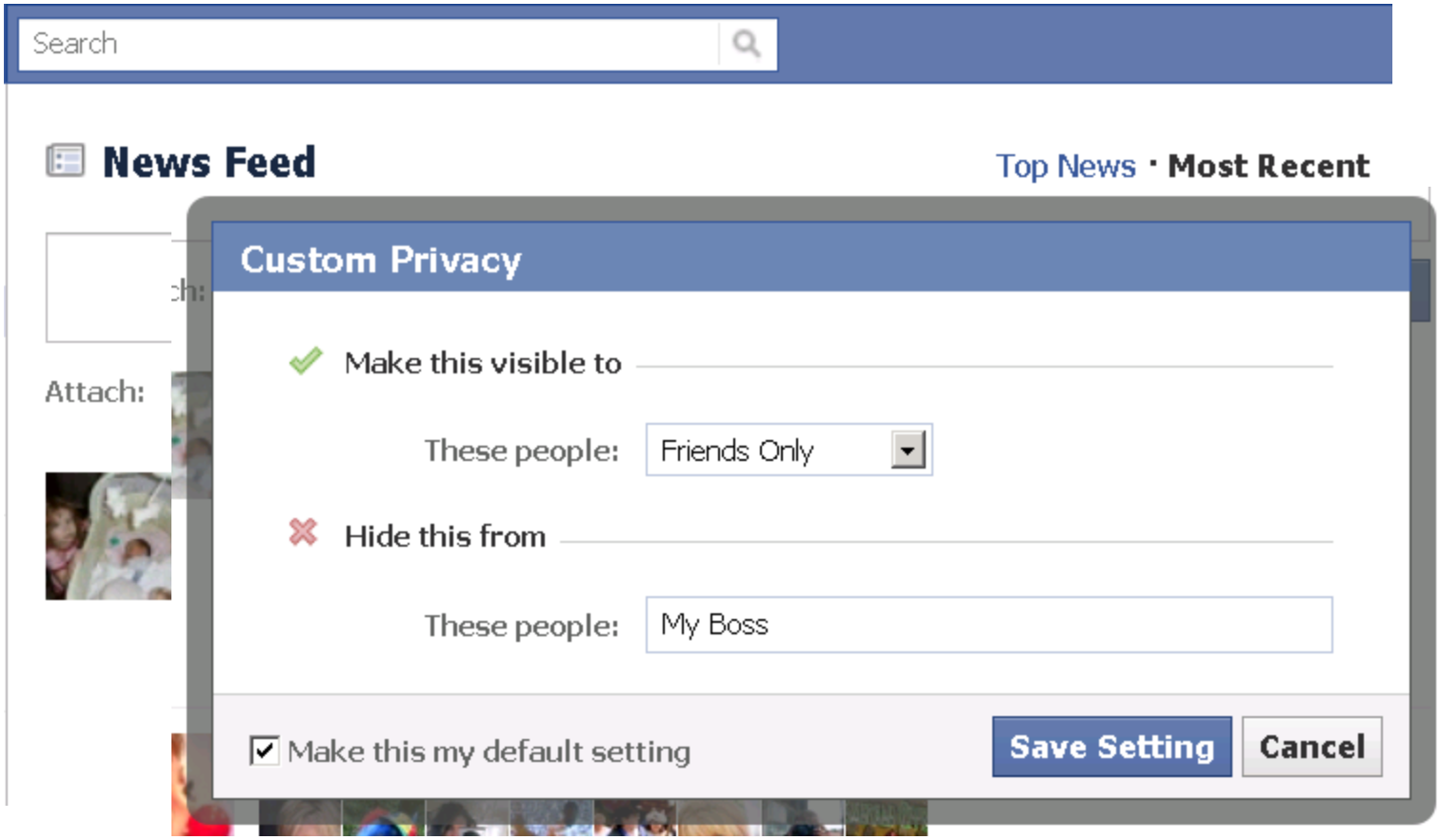
John R. Mallery
Managing Consultant

experience BKD CPAs & Advisors

Introduction

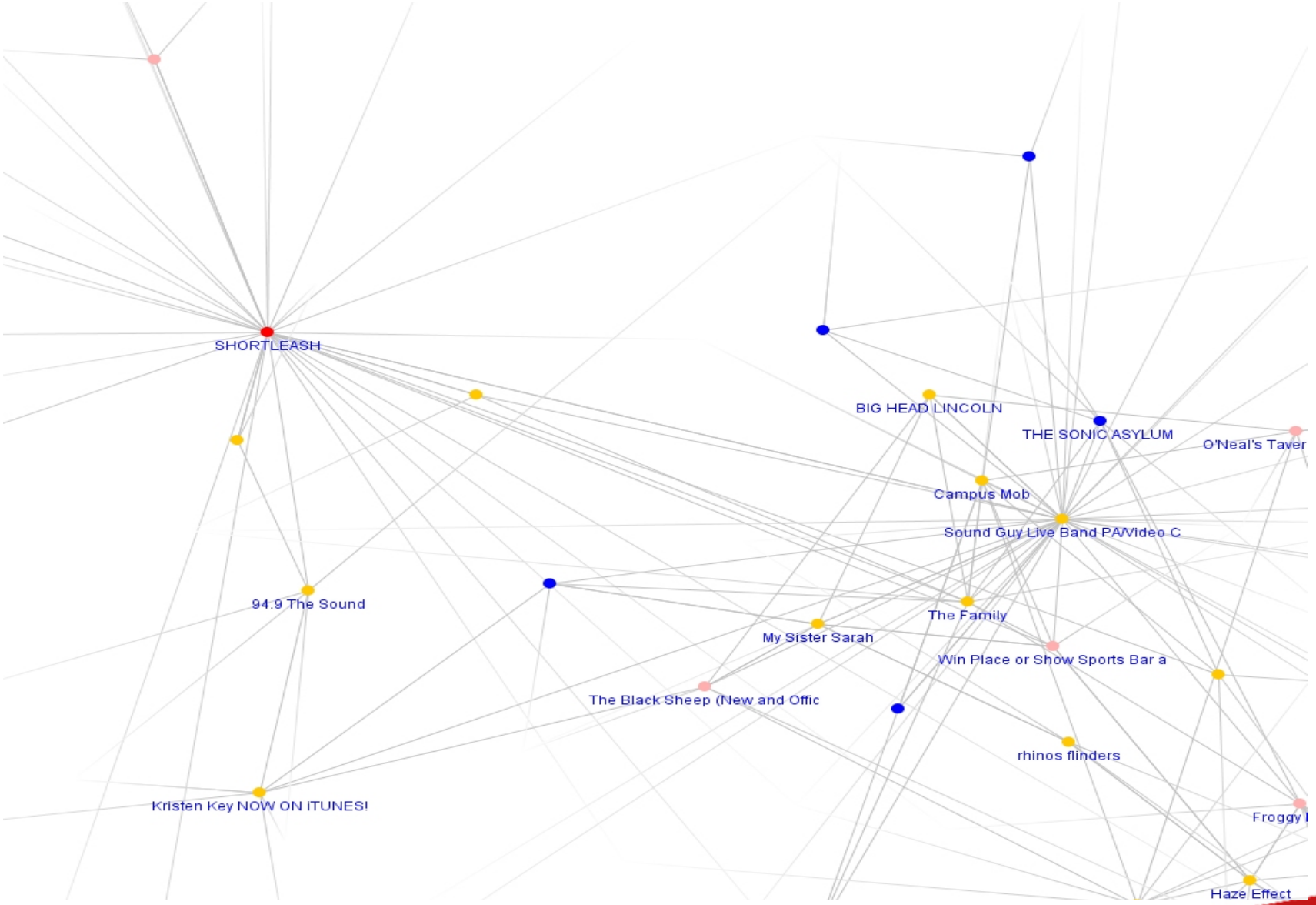
- Wikipedia lists more than 175 social network sites
- Risks
  - Productivity Issues
  - Harassment Issues
  - “Image” Issues
  - Disclosure of proprietary or confidential information
  - Safety issues

BKD Forensics Institute


Search
News Feed
Top News · Most Recent
Attach:
Custom Privacy
Make this visible to
These people:
Friends Only
Hide this from
These people:
My Boss
Make this my default setting
Save Setting
Cancel

Social Network Mapping

- Loco Citato (www.lococitato.com) has created several tools to visually map, search & record social networks
- Can export Network to a CSV file
- MySpace Visualizer & YouTube Visualizer available, Facebook Visualizer available to law enforcement



experience BKD LLP CPAs & Advisors

BKD Forensics Institute

Methods to Capture Webpages & Blog Postings, etc.

Screen Capture

- When material you want to capture is on screen, hit "Prnt Scrn" (Print Screen) button
- Paste screenshot into "Paint"
- Save captured information as an image (JPG, BMP)

Print to PDF

- Print webpage to "PDF"
- Use Adobe Acrobat drivers or "CutePDF" http://www.cutepdf.com/
- Captures date & time site was captured

Pages with Animation

- Can use a tool like Camtasia to capture everything
- http://www.techsmith.com/camtasia.asp

What Social Network Activity Can be Recovered From Computers?

experience BKD LLP CPAs & Advisors

BKD Forensics Institute

Internet History

- Visits to social networking sites can be captured in Internet history files
- Information can include number of visits to a particular page
- Date & time of last visit

Example Xanga URL's

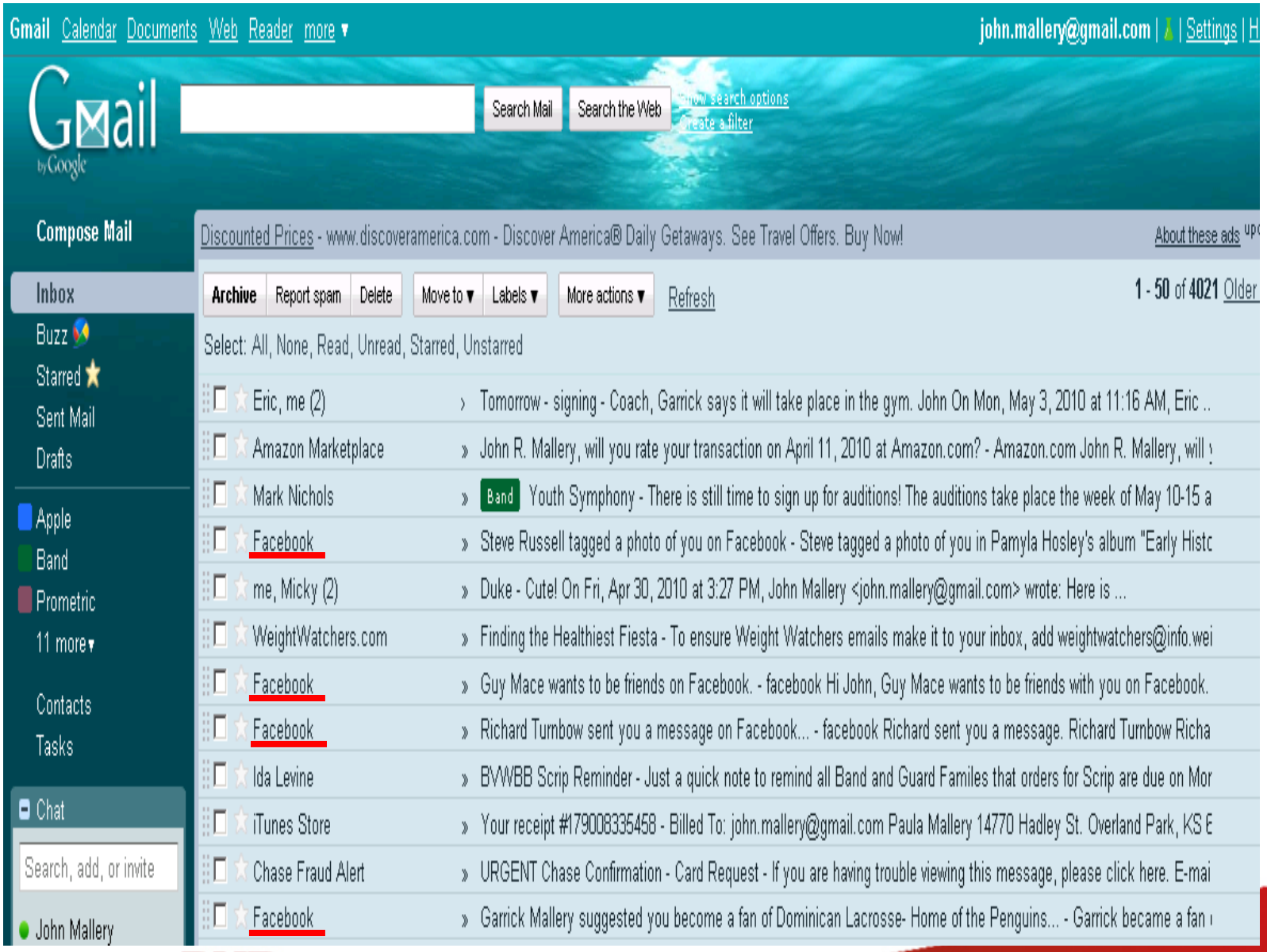
- http://profile.xanga.com/ProfileWizard.aspx?new=true#
- http://www.xanga.com/private/sitewizard.aspx?new=true
- http://profile.xanga.com/edit/invite.aspx?new=true&r=http%3a%2f%2fwww.xanga.com%2fprivate%2feditorx.aspx%3fsample%3d1
- http://www.xanga.com/private/yourhome.aspx

Entire Pages

- Since social networking sites are webpages, they are cached like any other page
- Visits to social networking sites will generate cached pages that are recoverable

Comments & Requests, etc. in Email

- If a page is private, you may not be able to see posts & status updates on page
- But you can recover comments & friend requests, etc. from email


Gmail Calendar Documents Web Reader more ▾
john.mallery@gmail.com | Settings | H
Gmail by Google
Search Mail
Search the Web
Show search options
Create a filter
Compose Mail
Inbox
Buzz
Starred
Sent Mail
Drafts
Apple
Band
Prometric
11 more ▾
Contacts
Tasks
Chat
Search, add, or invite
John Mallery
Discounted Prices - www.discoveramerica.com - Discover America® Daily Getaways. See Travel Offers. Buy Now!
About these ads
Archive
Report spam
Delete
Move to ▾
Labels ▾
More actions ▾
Refresh
1 - 50 of 4021 Older
Select: All, None, Read, Unread, Starred, Unstarred
Eric, me (2) › Tomorrow - signing - Coach, Garrick says it will take place in the gym. John On Mon, May 3, 2010 at 11:16 AM, Eric ..
Amazon Marketplace » John R. Mallery, will you rate your transaction on April 11, 2010 at Amazon.com? - Amazon.com John R. Mallery, will
Mark Nichols » Band Youth Symphony - There is still time to sign up for auditions! The auditions take place the week of May 10-15 a
Facebook » Steve Russell tagged a photo of you on Facebook - Steve tagged a photo of you in Pamyla Hosley's album "Early Histc
me, Micky (2) » Duke - Cute! On Fri, Apr 30, 2010 at 3:27 PM, John Mallery <john.mallery@gmail.com> wrote: Here is ...
WeightWatchers.com » Finding the Healthiest Fiesta - To ensure Weight Watchers emails make it to your inbox, add weightwatchers@info.wei
Facebook » Guy Mace wants to be friends on Facebook. - facebook Hi John, Guy Mace wants to be friends with you on Facebook.
Facebook » Richard Turnbow sent you a message on Facebook... - facebook Richard sent you a message. Richard Turnbow Richa
Ida Levine » BVWBB Scrip Reminder - Just a quick note to remind all Band and Guard Familes that orders for Scrip are due on Mor
iTunes Store » Your receipt #179008335458 - Billed To: john.mallery@gmail.com Paula Mallery 14770 Hadley St. Overland Park, KS E
Chase Fraud Alert » URGENT Chase Confirmation - Card Request - If you are having trouble viewing this message, please click here. E-mai
Facebook » Garrick Mallery suggested you become a fan of Dominican Lacrosse- Home of the Penguins... - Garrick became a fan

Facebook Status Updates

- Facebook status updates are recoverable from Internet history

http://ww	www.facebook.com	Facebook | David Roe's Photos - big carrots
http://ww	www.facebook.com	Facebook
https://lo	login.facebook.com	Login | Facebook
http://ww	www.facebook.com	Facebook | Springfield Metropolitan Bar Association: SMBA Monthly Lunch: How to Win Your Case with Technology
http://ww	www.facebook.com	Facebook | Springfield Metropolitan Bar Association: SMBA Monthly Lunch: How to Win Your Case with Technology
http://ww	www.facebook.com	Facebook | Springfield Metropolitan Bar Association's Notes
http://ww	www.google.com	url
http://ww	www.facebook.com	Springfield Metropolitan Bar Association: SMBA events in November | Facebook
http://ww	www.google.com	url
http://ww	www.facebook.com	SMBA | Facebook
http://ww	www.facebook.com	Facebook | Confirm Requests
http://ww	www.facebook.com	Facebook | Confirm Requests
http://ww	www.facebook.com	Facebook (3)
http://	www.facebook.com	Facebook (3)
http:/,		Facebook | John Mallery The problem with the gene pool is there is no life guard.
https://lo	login.facebook.com	Login | Facebook
http://ww	www.facebook.com	Facebook | Confirm Requests
http://ww	www.facebook.com	
http://ww	www.facebook.com	/n/?reqs.php&mid=21575e8G6b66c354G7e432aG2&n_m=john.mallery%40gmail.com

Chat

- Many social networking sites offer chat options
- It is sometimes possible to recover chat sessions from unallocated clusters

Recovered Facebook Chat

	E	F	G	H	I	J
1	Date/Time (UTC)	Sender ID	Sender Name	Recipient ID	Recipient Name	Message Text
2	Aug 07, 2009 - 05:21:	15189962XX	Candy Cotton	46XX2031	Dirk Loomis	Please don't ell Ralph that I am asking these questions. Met through friends at work?
3	Aug 07, 2009 - 05:22:	15189962XX	Candy Cotton	46XX2031	Dirk Loomis	That boy better be nice to Ralph or I will have to come up there
4	Aug 07, 2009 - 05:22:	46XX2031	Dirk Loomis	15189962XX	Candy Cotton	haha me too! we only got to hang out with him for the day but he was great. very funny
5	Aug 07, 2009 - 05:23:	15189962XX	Candy Cotton	46XX2031	Dirk Loomis	Ralph did say that he was funny as heck
6	Aug 07, 2009 - 05:24:	46XX2031	Dirk Loomis	15189962XX	Candy Cotton	he is! we are going to see them all again in a few weeks
7	Aug 07, 2009 - 05:24:	15189962XX	Candy Cotton	46XX2031	Dirk Loomis	good, have Ralph take some decent pictures of this guy. What are you going to be doing when you go?

Identifying Owner of Facebook ID

- Create URL like this
  - http://www.facebook.com/profile.php?id=XXXXXXXXX
  - Replace “X’s” with ID number
  - Must have valid Facebook account & be logged in
  - Will take you to user’s profile page
  - You may not see much but you will see name on account

Subpoena

- What can be retrieved through a subpoena varies by provider
- Can be very limited
- Legal contacts for service providers can be found here http://www.search.org/programs/hightech/isp/

John Mallery, MD Cardiac Electrophysiologist in Grass Valley, CA 95945

John Mallery, MD is a Cardiac Electrophysiologist at 150 Catherine Ln Ste D Grass Valley, CA. Wellness.com provides reviews, contact information, **...**

Show map of 150 Catherine Ln, Grass Valley, CA 95945

www.wellness.com/.../**john-mallery**-grass-valley-crdlgy-group-md - Cached - Similar

Amazon.com: **John Mallery**: Books

Hardening Network Security by **John Mallery**, Jason Zann, Patrick Kelly, **...** Levi Whitcomb Bates: His descendants by **John Mallery** Bates (Unknown Binding **...**

www.amazon.com/s?ie=UTF8&rh...field-author...page=1 - Cached

John Mallery (jmalleryks) on Twitter

Interested in cheese, computer forensics, orchids and music.

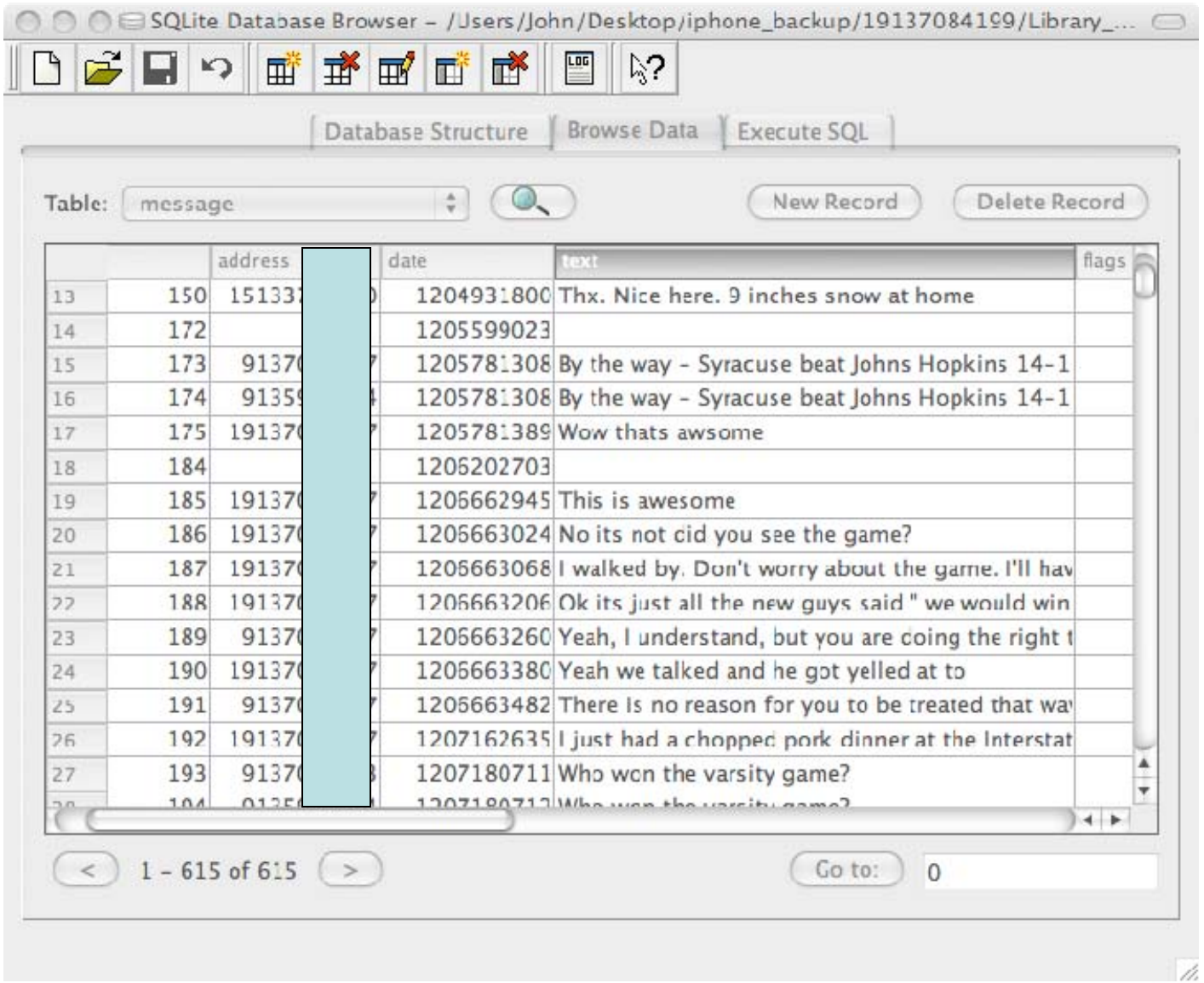
twitter.com/jmalleryks - Cached

Cell Phone Forensics

- No standardization
- What can be recovered often depends on make, model & carrier
- Some cell phones make a backup copy of their data when phone is synced to a computer
- Data can often be recovered from here

iPhones

- iPhone backups are created every time phone is synced
  - Windows – C:\Documents & Settings\USER\Application Data\Apple Computer\MobileSync\ Backup
  - Mac ~/Library/Application Support/MobileSync/Backup/ “hex folder name”


SQLite Database Browser – /Users/John/Desktop/iphone_backup/19137084199/Library_...
Database Structure
Browse Data
Execute SQL
Table: message
New Record
Delete Record
address
date
text
flags
13 150 1204931800 Thx. Nice here. 9 inches snow at home
14 172 1205599023
15 173 1205781308 By the way - Syracuse beat Johns Hopkins 14-1
16 174 1205781308 By the way - Syracuse beat Johns Hopkins 14-1
17 175 1205781389 Wow thats awsome
18 184 1206202703
19 185 1206662945 This is awesome
20 186 1206663024 No its not cid you see the game?
21 187 1206663068 I walked by. Don't worry about the game. I'll hav
22 188 1206663206 Ok its just all the new guys said " we would win
23 189 1206663260 Yeah, I understand, but you are going the right t
24 190 1206663380 Yeah we talked and he got yelled at to
25 191 1206663482 There is no reason for you to be treated that wa
26 192 1207162635 I just had a chopped pork dinner at the Interstat
27 193 1207180711 Who won the varsity game?
1 - 615 of 615
Go to: 0

Applications

GPS


WELCOME TO THE
BONNEVILLE SALT FLATS
AND UTAH'S FAMED MEASURED MILE-
SITE OF WORLD LAND-SPEED RECORD RUNS


Image Edit
Adjust
Effects
Details
GPS
General
Exif
TIFF
Latitude 40° 44' 9" N
Longitude 114° 3' 53.4" W
Time Stamp 10:51:24.57
Locate

Questions?

John Mallery
jmallery@bkd.com
816.221.6300