VESTIGE
Digital Investigations

Devices as Witnesses

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

Greg Kelley, EnCE, DFCP
Vestige Digital Investigations
NALS of Northeast Ohio

About Me

- B.S. in Computer Engineering from CWRU
- Computer forensics since 2001
- Examined thousands of computers for hundreds of matters
- Testified in State and Federal Cases for plaintiff, prosecution and defense

Digital Evidence






More Digital Evidence!

What to do?

- It is quite daunting
- You don't know what you don't know
- Lack of resources

Witnesses

- Understand that digital devices are witnesses
- Won't lie
- See things you may not realize
- Can be misinterpreted

What you can expect from Computers

- Content
  - Keyword search for content/communication
    - ALL correspondence
    - Hidden information
    - Deleted information
    - Orphaned information
    - Encrypted information

- Correspondence
  - Memos
  - Emails
  - Instant messages
  - Faxes
  - Deleted
  - Old and forgotten

- Business Records
  - Financial data
  - Assets
  - Calculations
  - PRIOR DRAFTS
  - DELETED DRAFTS
  - Projections
  - Everything you could imagine

- Every Website visited
- All pictures from those websites
- Every Website from popups and popunders
- All maps, from Mapquest for example
- Every Internet Search and Results

What you can expect from Computers

- Conceptual Analysis
  - How the computer was used
    - IMs
    - E-mails
    - Web-based E-mails
    - Deletion activity
    - Wiping activity
    - Software installed
    - File Transfers
    - CD/DVD burning
    - Attached hardware
    - Other networks attached
    - Remote Access activity
    - Do we have the “Right” system?

Mobile Content

A Guide to What's Available on Mobile Devices

Variety of Devices

- Speed of Introduction
  - Worldwide: 1,500/month
  - Latest & Greatest
- Technologies
  - CDMA
  - TDMA
  - GSM
  - iDEN
  - PCS

Below are all of the phones released with major U.S. carriers within the last 45 days. Newest releases are listed first.

Differences

- Operating Systems
  - iOS
  - Android
  - Symbian
  - Does anyone remember Blackberry?
  - Asha
  - Windows Mobile
  - Windows RT
  - Bada
  - Brew
  - GridOS
  - Linux
  - Mer
  - Nemo Mobile
  - S40
  - Sailfish OS
  - SHR
  - Tizen
  - webOS

And now for something completely different…

  - Aliyun OS
  - Firefox OS
  - Ubuntu Touch OS

Differences

- Carrier Dependency

Mobile Content - The Obvious

- Contacts(including Recent)
- Call Logs (In, Out, Missed)
- SMS/MMS
- Calendar Events
- E-mails

A Little Less Obvious

- Voicemails
- Internet History / Searching
- Installed Apps
- Geo-location
  - GPS
  - Cell Towers
  - WiFi Networks
- Info in Log Files

Hmm, Didn't think about that

- History of DHCP servers & settings
- Paired BlueTooth
- Services Subscribed to (i.e. Pandora, TripAdvisor, Yelp!)
- Computer(s) Attached to
- Cloud Storage Info
- Amount of Data Transferred within session

More…

- Temporal Data
  - Log files
  - Crash/Panic Reports
  - Extracted Metadata from events (calendar, images, movies, e-mails, SMS, etc.)
- Maps
- Data from Custom Applications

Gotchas

- Custom Dictionary
- Graphical “decorations”
- Encryption/Decryption keys
- Passwords
- And of course…deleted information in all shades and forms

Intro to Social Media

Definition

The use of web-based and mobile technologies that enable people to communicate easily via the Internet to share information and resources.

Popular Social Media Sites


The Big 4 – Monthly Visitors

facebook 1,100,000,000

YouTube 1,000,000,000

310,000,000

LinkedIn 255,000,000

Anatomy of a Tweet

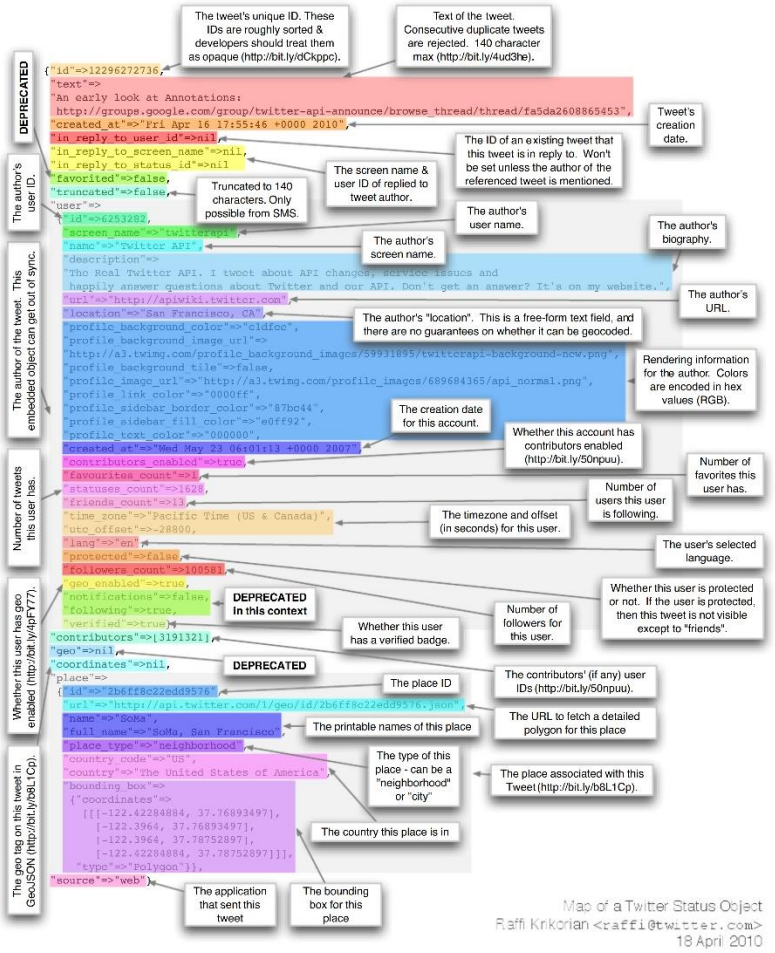
"Twitter Mathematics"

OR

"When is 140 characters not 140 characters?"

This message is 140 characters long. It is a demonstration to show the amount of data that can exist within a single Tweet. Short & Sweet!

Anatomy of a Tweet



- Unique Tweet ID
- Screen name of user ID of reply
- Author's user name
- Author's screen name
- Author's location (free-form)
- Author's biography
- Creation date of account
- Timezone
- Number of users author is following
- Number of favorites this user has
- User's language
- Number of followers this user has
- Geolocation Info
- Application that sent the Tweet

And probably more…

What Will Social Media Show?

- Frame of mind
- Recounting of the crime
- Friends and associates
- Location and Time

Preservation

What Not To Do

- Screen shots of a web page
- Forwarding of emails or text messages
- A simple copy of files
- Rely on someone that just “knows IT”

What To Do

- Hire an expert, or someone that has done this before
- But if you can't
  - Document what you did
  - Document the device
  - Employ the use of MD5 or other type of hash
  - Use a method of verification

Authentication – Legal Issues

- Authentication
  - FRE 901(a)
    - "…must offer evidence sufficient to support a finding that the matter in question is what its proponent claims"
  - FRE 901(b)(4) – can authenticate ESI with circumstantial evidence, reflecting: contents, substance, internal patterns or other distinctive characteristics
    - Court rulings: Metadata supports this

Authentication - Legal Issues

- Authentication
  - State of Connecticut v Eleck (2001 WL 3278663 (Conn.App. 2011))
    - Rejected printouts of FaceBook pages
    - "incumbent on the party seeking to admit the social media data to offer detailed 'circumstantial evidence that tends to authenticate' the unique medium of social media.
  - State v Tienda (5358 S.W.3d 633 (Tx.App.2012))
    - Prosecution successfully admitted key MySpace evidence over defendant's objection based upon circumstantial evidence, including:
      - Relevant Metadata Fields
      - Other MySpace pages of same defendant,
      - User of same username, nickname and e-mail addresses
      - User ID
      - Stated location,
      - Communications with other suspects and
      - Posted photos with associated date and time stamps
  - Commonwealth of PA v Amy N. Koch
    - Evidence existed that others used defendant's phone making authentication of specific messages important to their admissibility.

Sample Case 1

- Defendant suspected of insider trading
- Defendant claimed to never have met the person supposedly providing insider information
- Insider had unique spelling of name
- Name was found in custom dictionary

Sample Case 2

- Sales Engineer left to go to competitor
- Computer analysis showed minimal data theft
- Computer did have pictures that were synchronized from the phone
- What was on those pictures?

Sample Case 3

- Defendant charged with assault
- Claimed he was the victim
- Analysis of computer centered on internet searches, maps and deleted communication

Sample Case 4

- Employee terminated for unsatisfactory performance
- Employee files suit for wrongful termination
- Computer examination showed
  - Shopping
  - Doing class work
  - Social media interaction

Q&A

Greg Kelley, EnCE, DFCP

Vestige Digital Investigations

Cleveland | Columbus | Pittsburgh
330.721.1205
gkelley@vestigeltd.com
www.vestigeltd.com