Cybersecurity and Digital Forensics

At Wilmington University

Jason Silva, Director of Operations
Cornerstone Discovery

What is Cybersecurity?

"Cybersecurity is the body of technologies, processes and practices (i.e. measures) designed to protect networks, computers, programs and data from attack, damage or unauthorized access."

Source: TechTarget

What is a Cyber Threat?

*"A cyber threat is the possibility of a malicious attempt to 1) access files and infiltrate or **steal data** or 2) to **damage or disrupt** a computer network or system."*

Sources: SecureWorks/Oxford Dictionary

The Statistics Are Alarming

- Hackers attack every 39 Seconds
- 43% of cyber attacks target small business
- Only 14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective
- 60% of small companies go out of business within six months of a cyber attack
- 48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest
- In 2016, 40% of companies expect a data breach caused by malicious insiders

Most Frequent Types of Cyber Threats

- Distributed Denial of Service (DDoD) Attacks
- Insider Threat
- Malware/Spyware
- Password Attacks
- Phishing
- Ransomware

Distributed Denial of Service (DDoS)

- DDoS attacks occur when a server is intentionally overloaded with requests, with the goal of shutting down the target's website or network system

Insider Threat

- Someone with administrative privileges, usually from within the organization, purposely misuses his or her credentials to gain access to confidential company information

Malware/Spyware

- This umbrella term is short for "malicious software," and covers any program introduced into the target's computer with the intent to cause damage or gain unauthorized access

Password Attacks

- 3 main types of password attacks:
  - Brute-force attack, which involves guessing at passwords until the hacker gets in
  - Dictionary attack, which uses a program to try different combinations of dictionary words
  - Keylogging, which tracks all of a user's keystrokes, including login IDs and passwords

Phishing

- Involves collecting sensitive information like login credentials and credit-card information through a legitimate-looking (but ultimately fraudulent) website, often sent to unsuspecting individuals in an email

Ransomware

- Ransomware will either lock you out of your computer and demand money in return for access or threaten to publish private information if you don't pay a specified amount. Ransomware is one of the fastest growing types of security breaches.

Most Common Sources of Cyber Threats

- Nation states or national governments
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists and hackers
- Business competitors
- Disgruntled insiders

Source: SecureWorks

Technology Trends Driving Cyber Threats

- Internet of Things
  - Individual devices connected to the internet or other networks (i.e. Amazon Echo, Smart Devices, etc.)
- Explosion of Data (It's everywhere!)
  - Stored in devices such as cellphones, laptops and elsewhere

Source: SecureWorks

Main Elements of Cybersecurity

- Ensuring Cybersecurity requires coordinated efforts throughout an information system.
  - Application security
  - Information security
  - Network security
  - Disaster recovery / business continuity planning
  - End-user compliance

Ever Increasing Sources of ESI

Not Just about Desktops, Laptops, Servers, Tablets & Cell Phones

Ever Increasing Sources of ESI

Growing List of Sources From Which Information Might Be Obtainable

- Computers (Desktops, Laptops)
- Mobile Devices (iPhone, Smartphone, iPad, iPod, Tablet)
- Servers, Backup Tapes, NAS, Appliances (Barracuda, Mimecast)
- Service Provider Records (AT&T, Verizon, T-Mobile, E-ZPass)
- Portable Storage (Thumb Drive, SD Cards, External Hard Drives)
- Surveillance Video
- Cloud Email (Gmail, Apple Mail, Microsoft Office 365, Hotmail, Yahoo)
- Cloud Storage (Apple iCloud, Google Drive, Dropbox, Microsoft Skydrive)
- Cloud Backup (Druva, Crashplan, iBackup)
- Apps (Snapchat, Skype, Viber, Tinder)
- Social Networking (Facebook, Twitter, Linkedin)

And Now The Internet of Things (IoT)

What is the IoT?

- The IoT is a **Giant Network of Connected "Things“**
- A System of **Interrelated Computing Devices, Mechanical and Digital Machines, Objects, Animals or People** That are Provided With Unique Identifiers and the Ability to Transfer Data Over a Network Without Requiring Human-to-Human or Human-to-Computer Interaction

Pertinent Questions

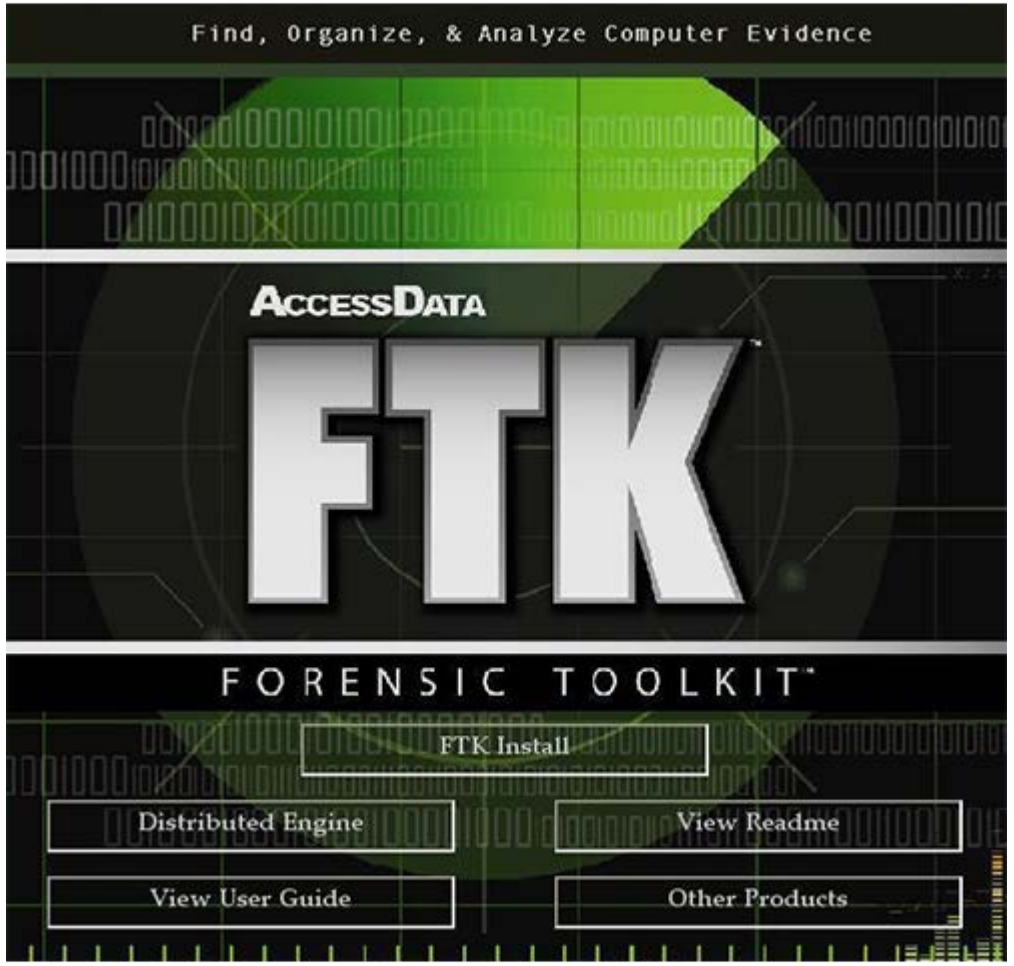
- Where Was Someone at any Point in Time?
- How Fast Was Someone Travelling and What Route Did They Take?
- When Was Someone Using One of Their Electronic Devices?
- What, in Particular, Were They Doing On Their Device at any Point in Time?
- With Whom Were They Communicating On Their Device at any Point in Time?

Digital Forensics!

cellebrite
delivering mobile expertise

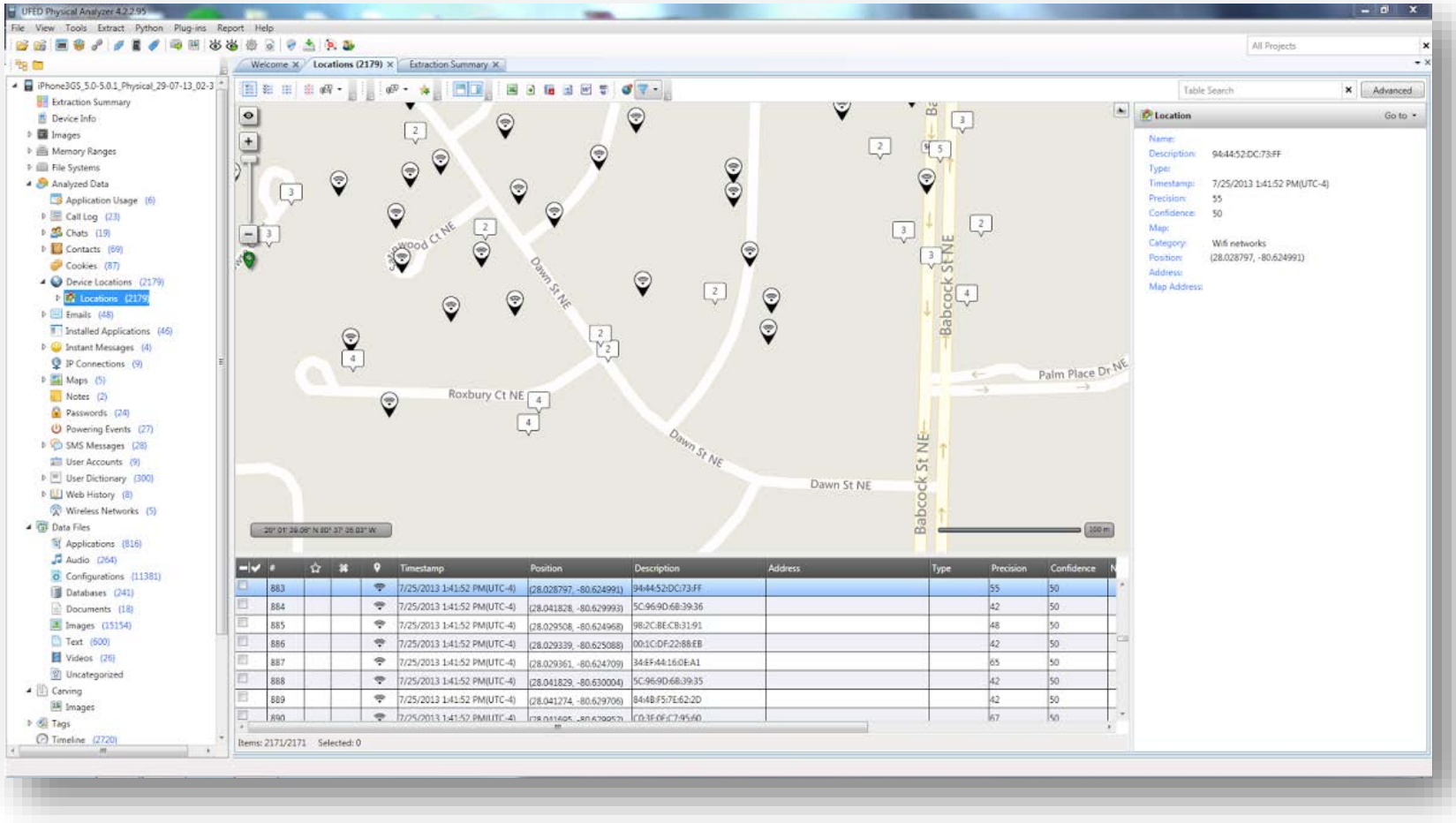
nuix
Simple. Powerful. Precise.

MAGNET AXIOM™
FOR COMPUTERS



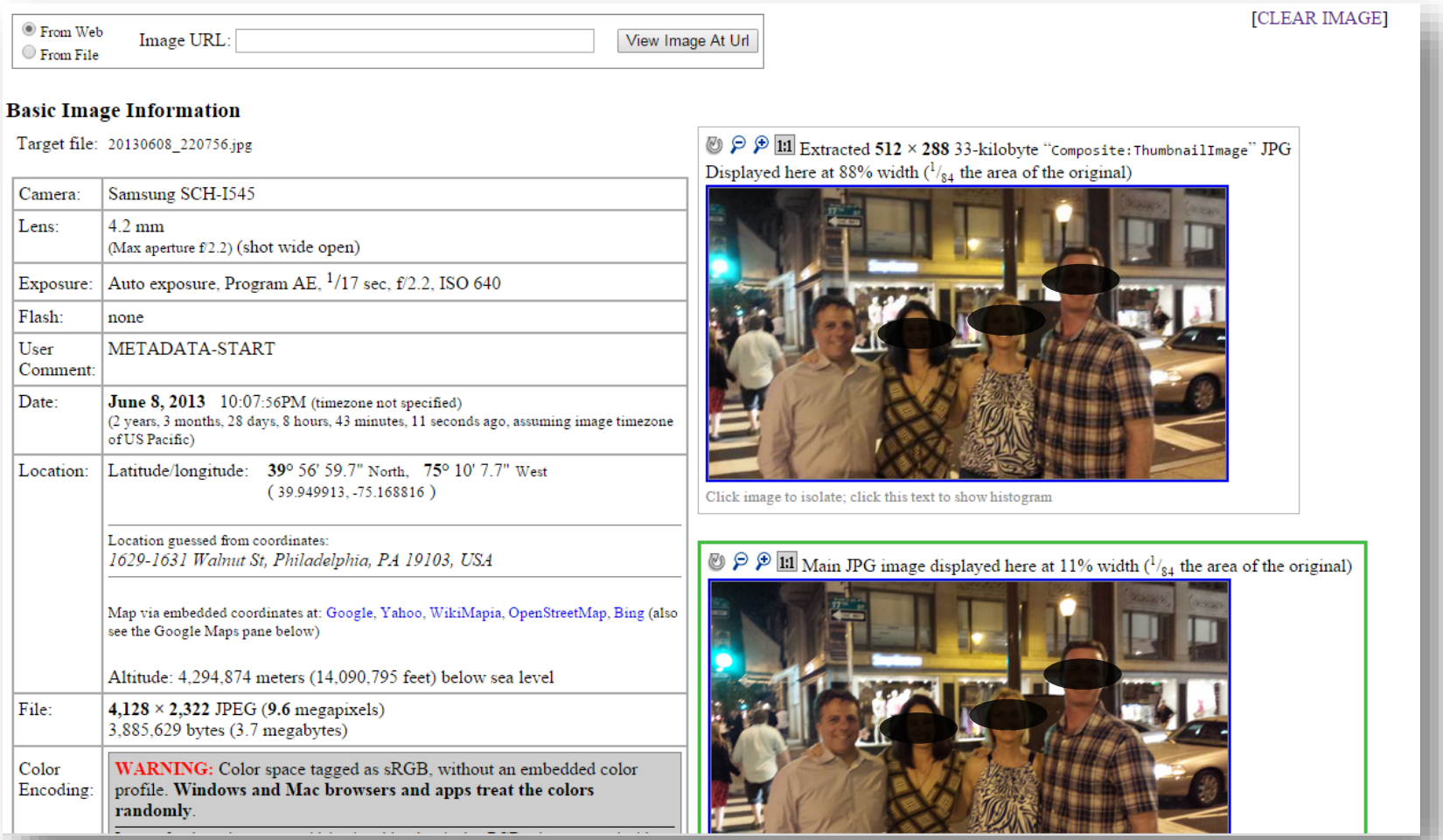
Where Was Someone at any Point in Time?

- Remember …Not Just Laptops, Cell Phones, Tablets, and GPS
- **IoT Devices Communicate Over Cell Networks too**



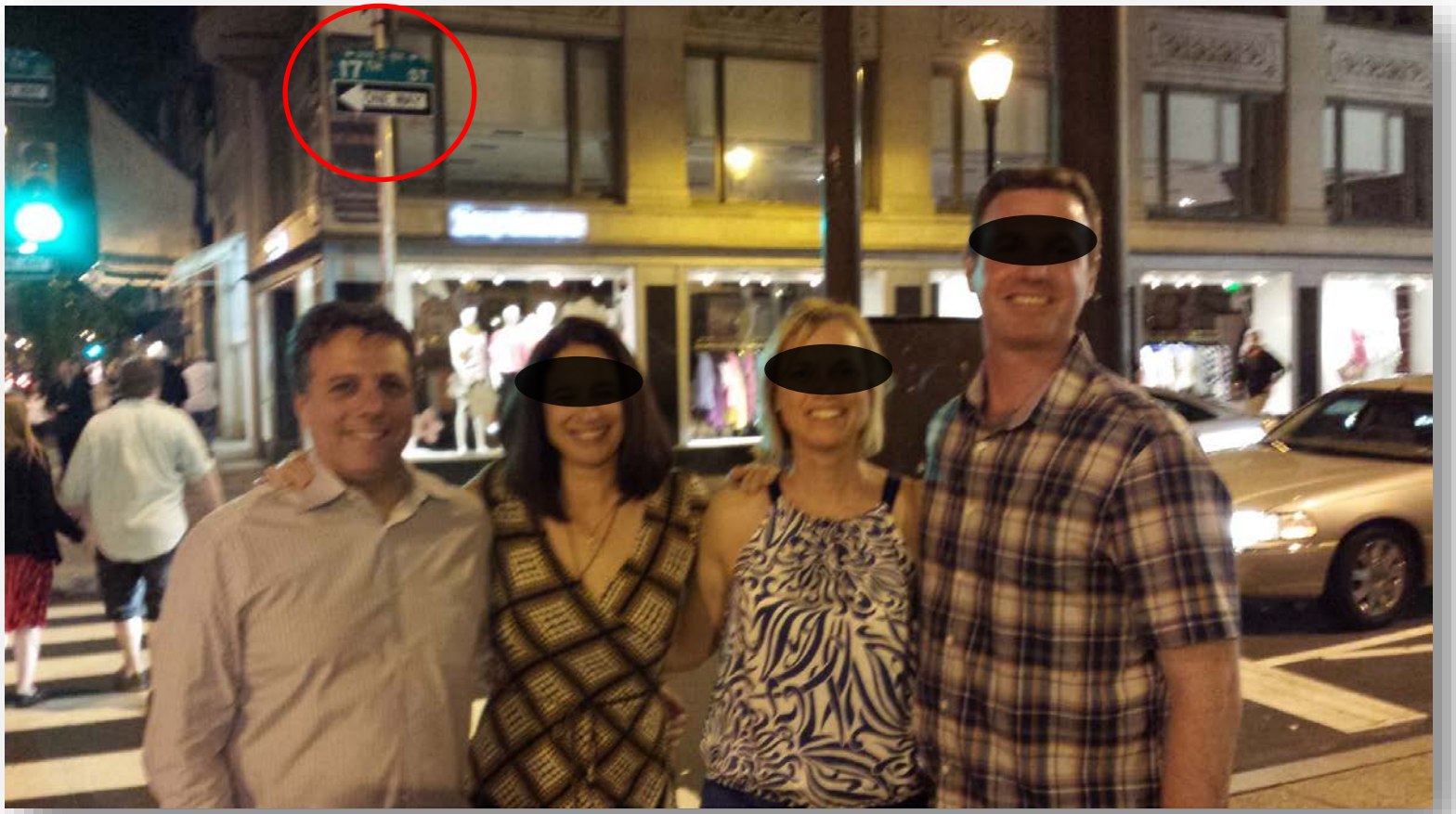
Where Was Someone at any Point in Time?

- Pictures and Videos – EXIF Data – Date, Time, Location ..and More!
- Free EXIF Viewer at: **thetechgazette.com**



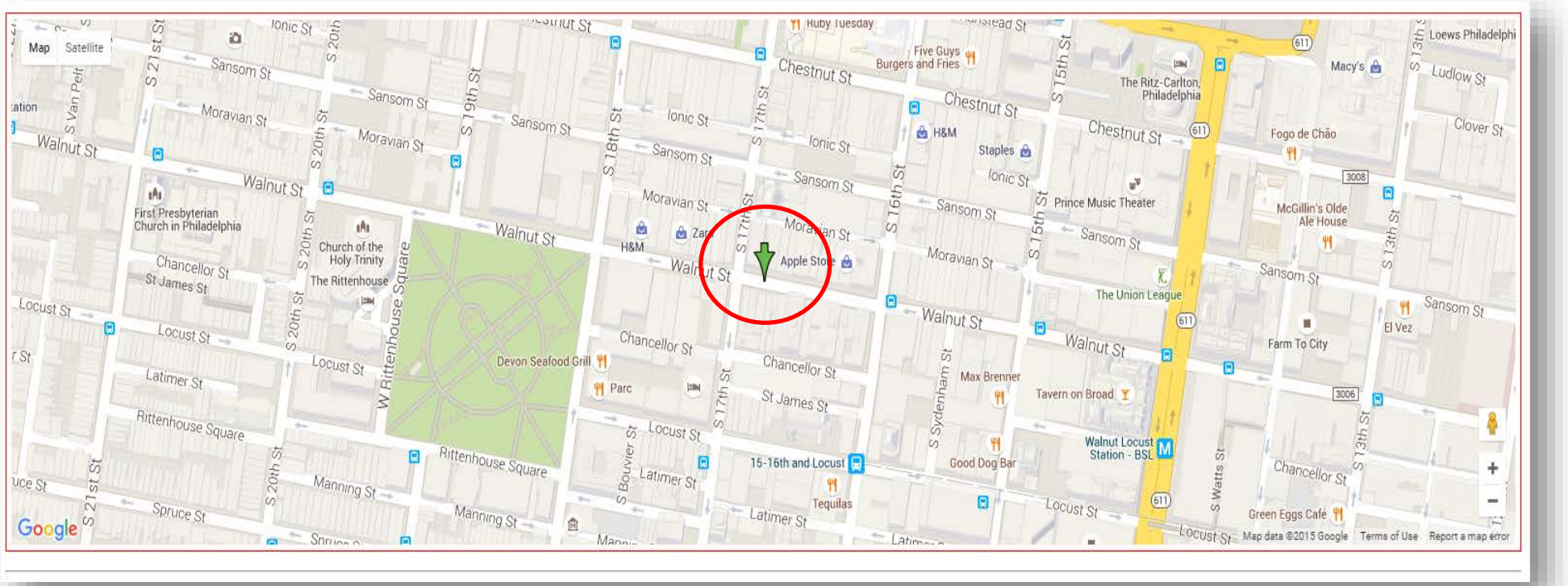
Where Was Someone at any Point in Time?

- EXIF Data



Where Was Someone at any Point in Time?

- Location information

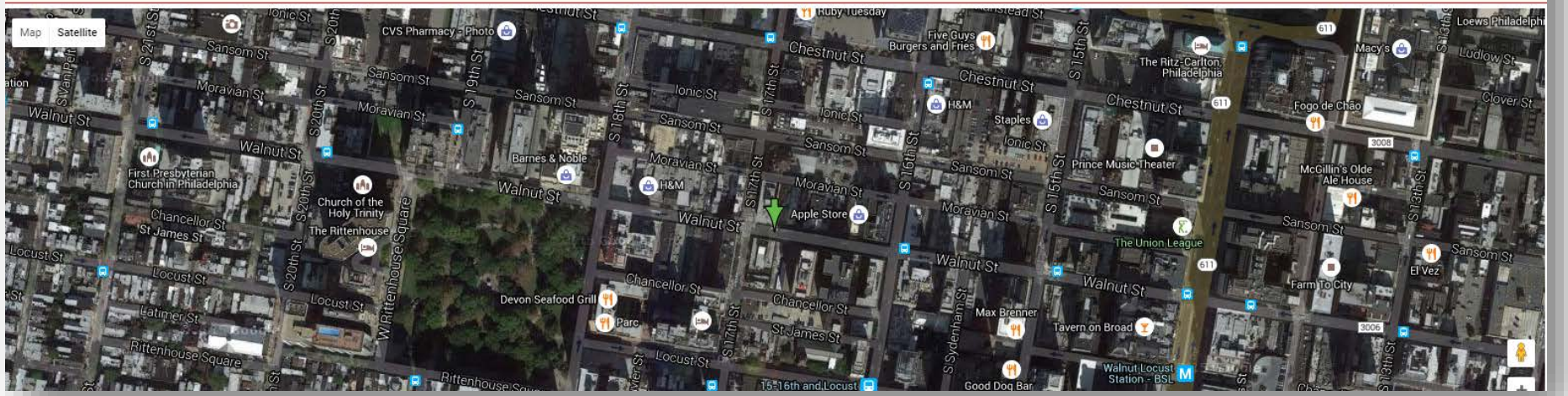


Where Was Someone at any Point in Time?

	1629-1631 Walnut St, Philadelphia, PA 19103, USA Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 4,294,874 meters (14,090,795 feet) below sea level
File:	**4,128 × 2,322** JPEG (**9.6** megapixels) 3,885,629 bytes (3.7 megabytes)
Color Encoding:	**WARNING:** Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly**. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

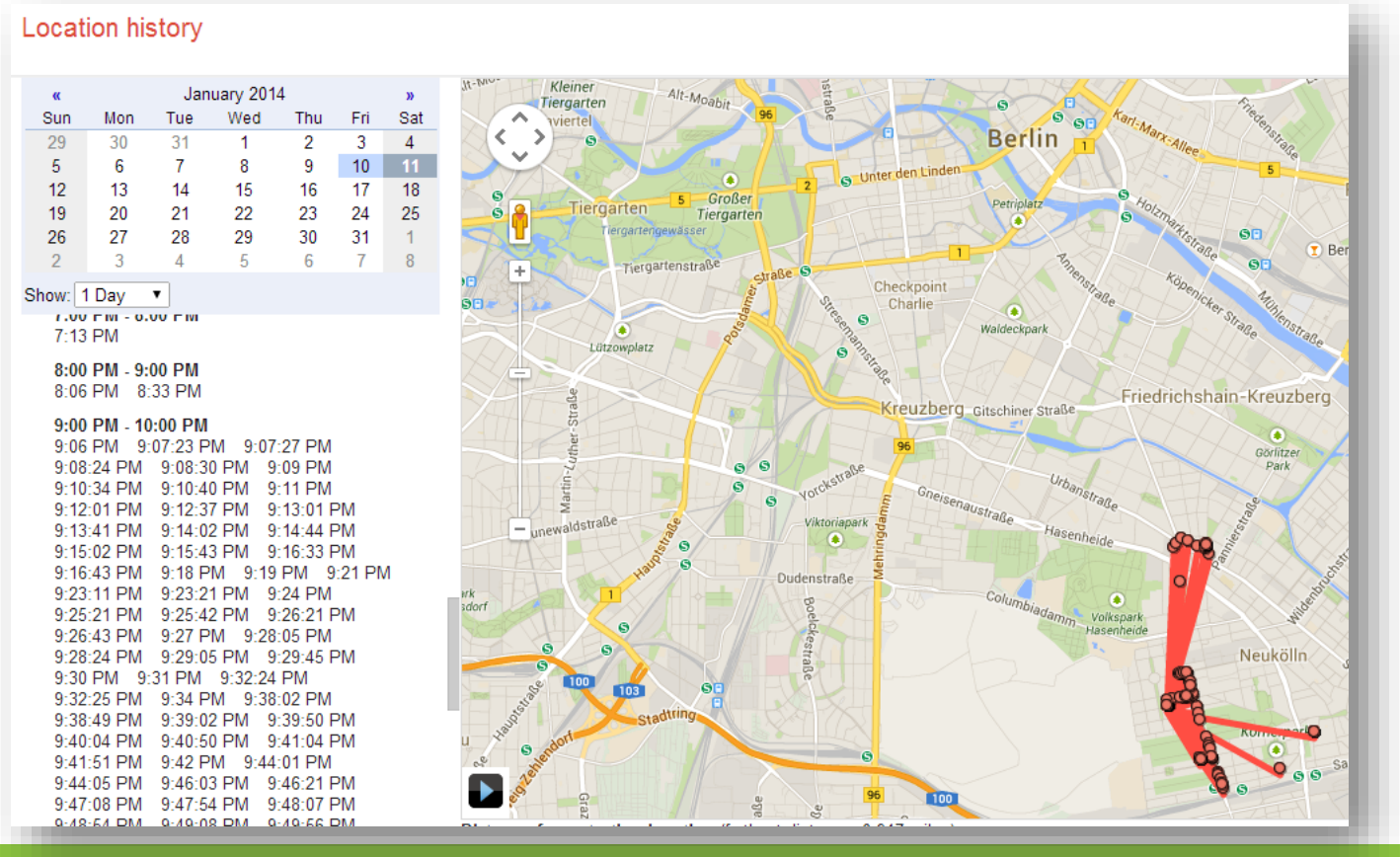
1:1 Main JPG image displayed here at 11% width ($^{1}/_{84}$ the area of the original)

Click image to isolate; click this text to show histogram



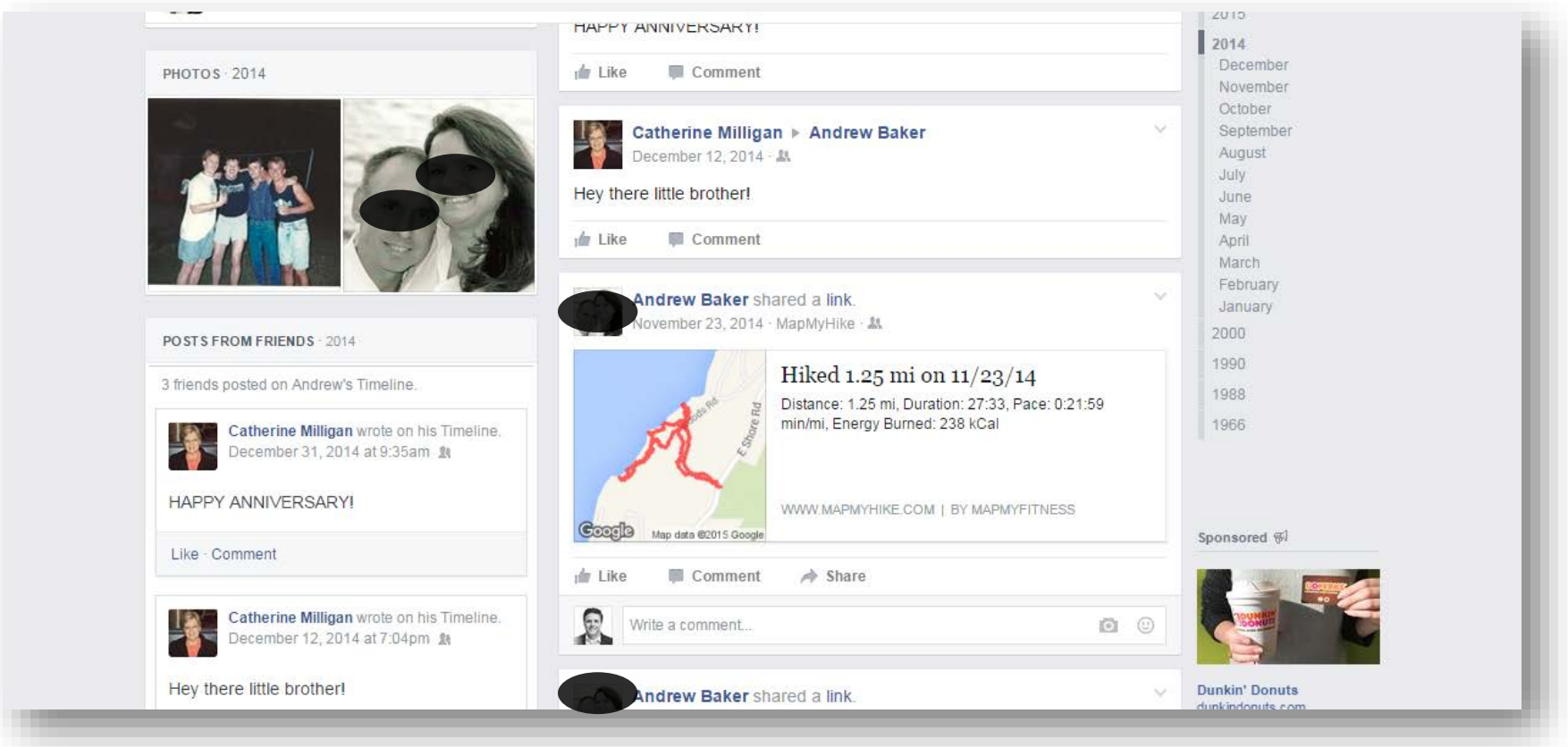
How Fast was Someone Travelling? What Route did They Take?

- Google Location History



How Fast Was Someone Travelling? What Route did They Take?

- Social Media



How Fast was Someone Travelling? What Route did They Take?

- Call Detail Records - CDR

Combined Detail LE [redacted]-384-1700

MSISDN	Start Time	First Tower Cell ID / ECGI Cell	First Tower Latitude	First Tower Longitude	Last Tower Cell ID / ECGI Cell	Last Tower Latitude	Last Tower Longitude	Duration(Seconds)
[redacted]43841700	8/23/2014 02:13:55 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	43
[redacted]43841700	8/23/2014 02:15:40 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	48
[redacted]43841700	8/23/2014 02:17:15 AM	15523	42.11114849	-80.0794776	16012	42.11005556	-80.1105556	23
[redacted]43841700	8/23/2014 02:28:24 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	2
[redacted]43841700	8/23/2014 02:28:47 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	99
[redacted]43841700	8/23/2014 02:31:54 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	41
[redacted]43841700	8/23/2014 02:32:35 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	28
[redacted]43841700	8/23/2014 02:33:38 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	34
[redacted]43841700	8/23/2014 02:34:13 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	45
[redacted]43841700	8/23/2014 02:35:54 AM	15513	42.12546944	-80.0793222	15523	42.11114849	-80.0794776	37
[redacted]43841700	8/23/2014 02:43:33 AM	16012	42.11005556	-80.1105556	16012	42.11005556	-80.1105556	82
[redacted]43841700	8/23/2014 02:48:27 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	15
[redacted]43841700	8/23/2014 02:52:44 AM	16012	42.11005556	-80.1105556	15523	42.11114849	-80.0794776	37
[redacted]43841700	8/23/2014 02:53:24 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	22
[redacted]43841700	8/23/2014 02:54:42 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	34
[redacted]43841700	8/23/2014 02:55:18 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	34
[redacted]43841700	8/23/2014 02:56:21 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	32
[redacted]43841700	8/23/2014 02:57:09 AM	15523	42.11114849	-80.0794776	15523	42.11114849	-80.0794776	35
[redacted]43841700	8/23/2014 02:58:06 AM	15513	42.12546944	-80.0793222	15513	42.12546944	-80.0793222	22

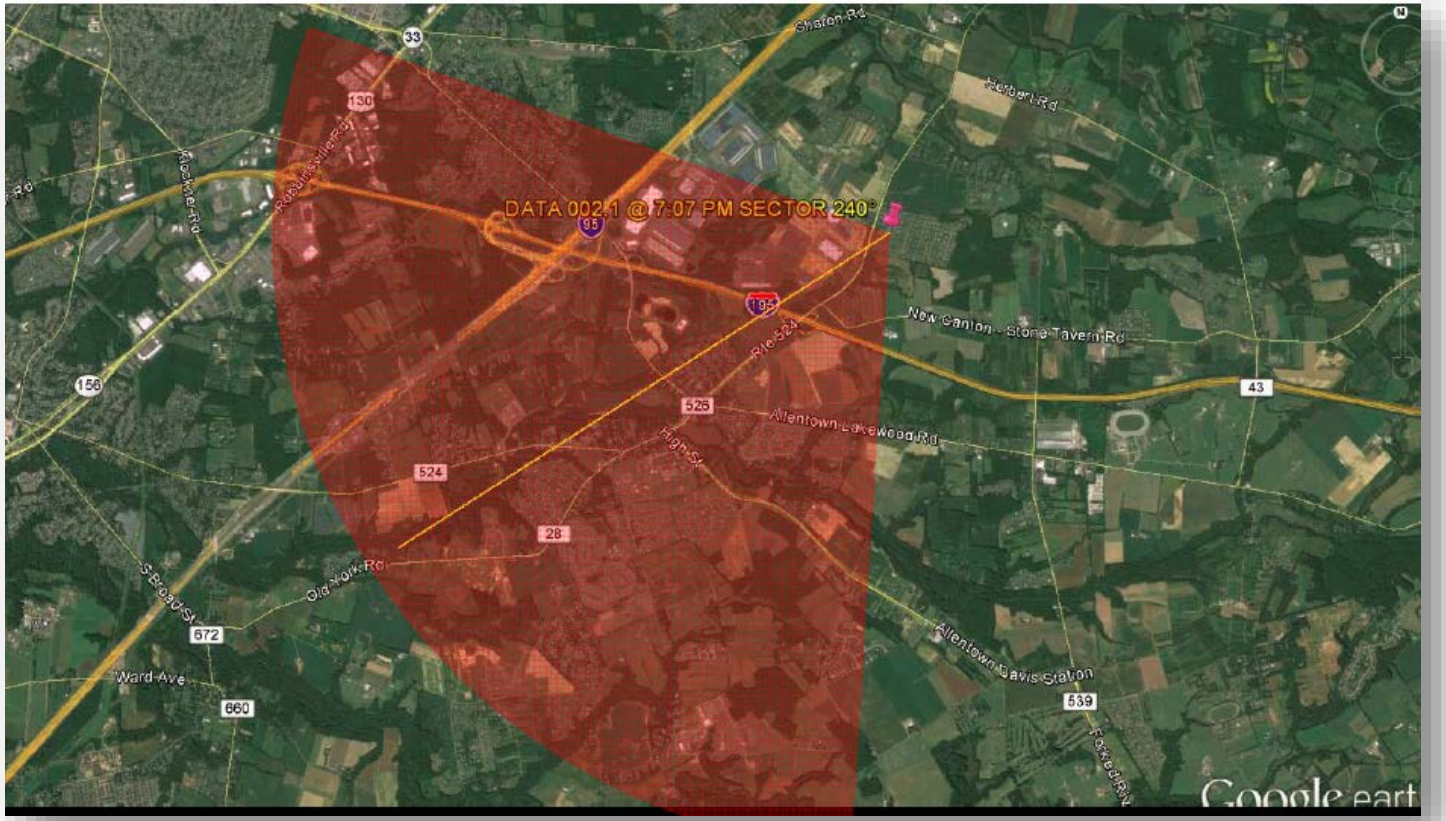
How Fast was Someone Travelling? What Route did They Take?

- IoT Devices That can Communicate Over Cell Networks

T-Mobile

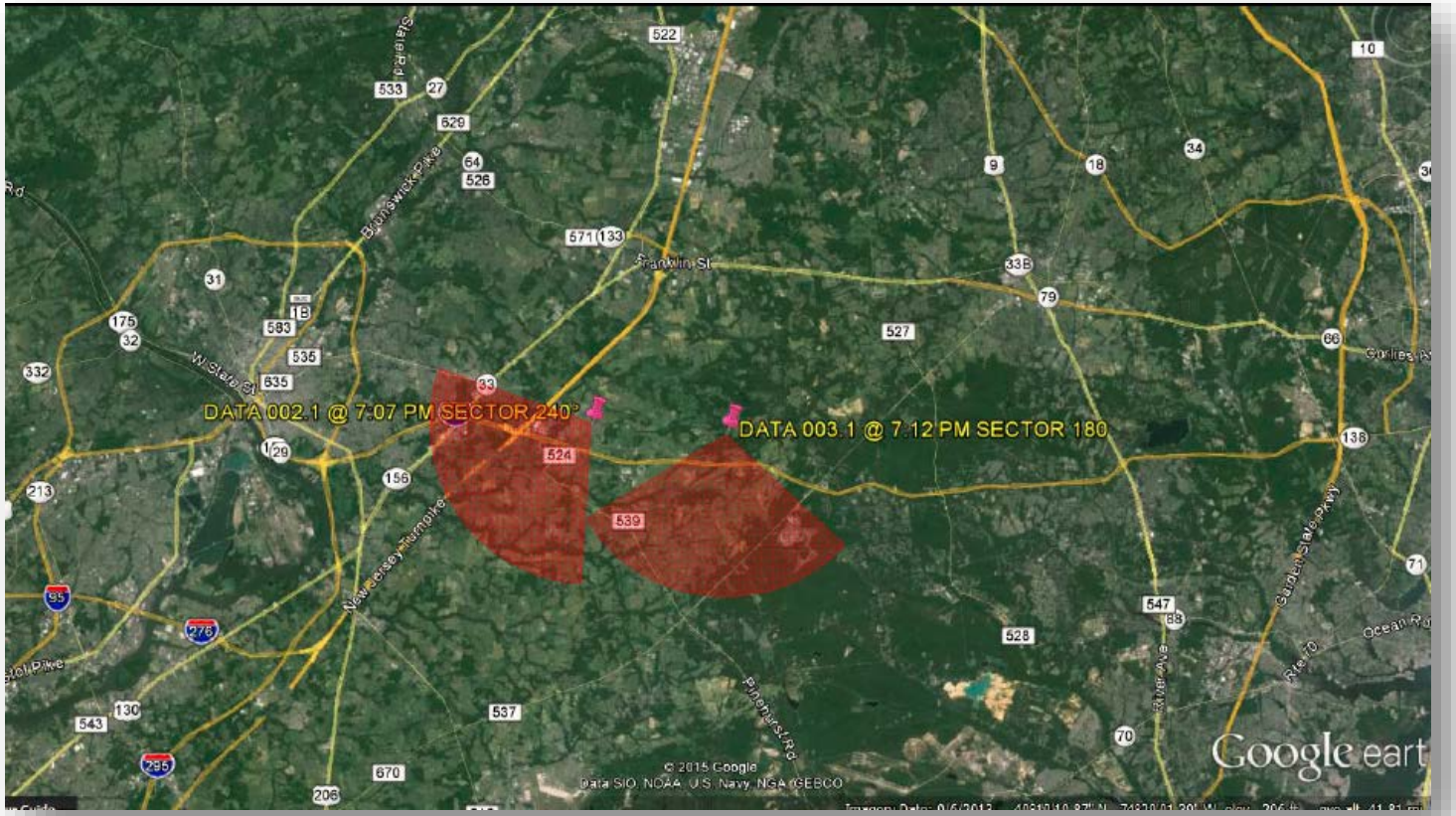
How Fast was Someone Travelling? What Route did They Take?

- Call Detail Records - CDR



How Fast was Someone Travelling? What Route did They Take?

- Call Detail Records - CDR



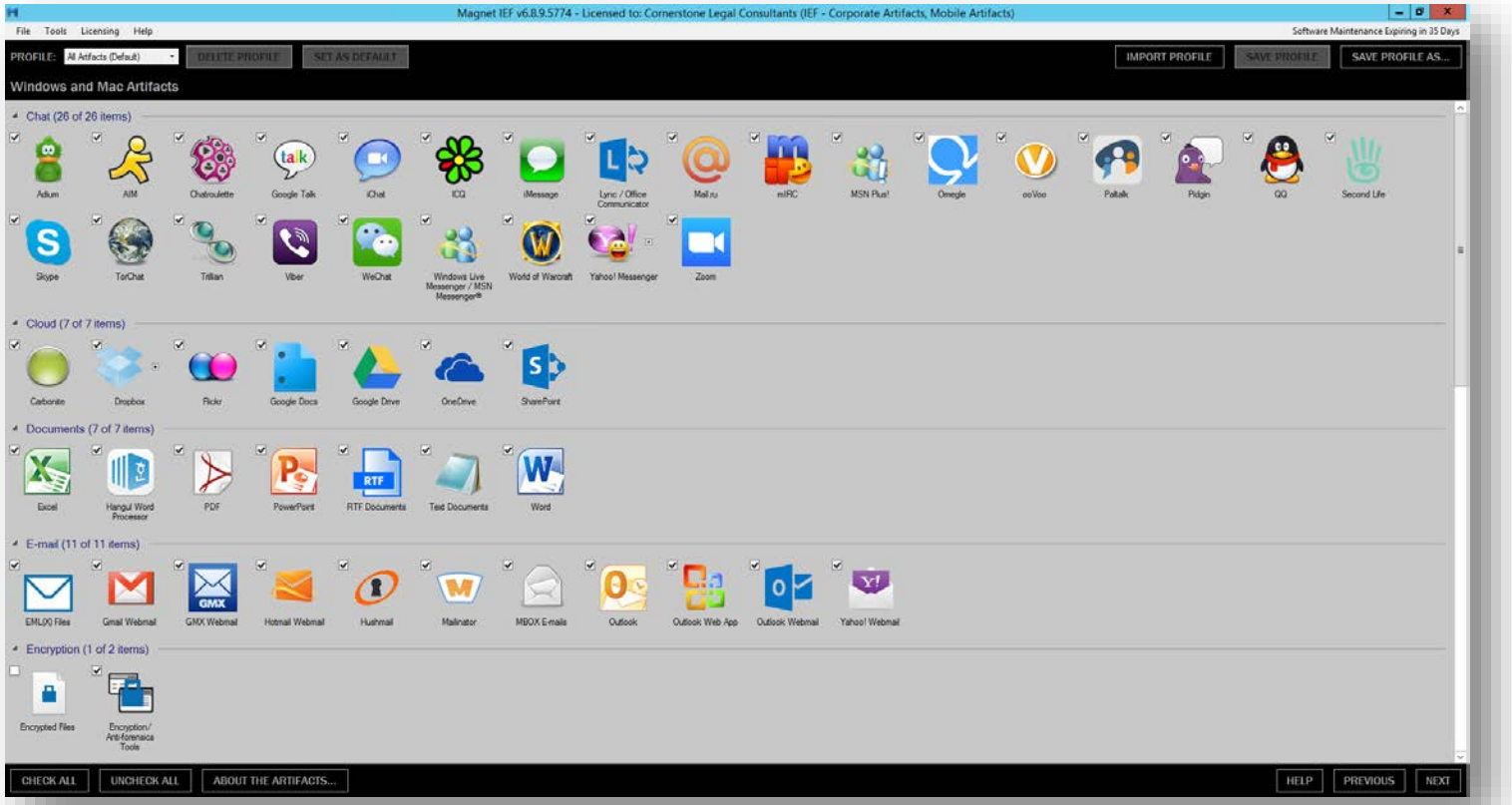
When was Someone Using one of Their Electronic Devices?

- Timeline of Device Activity Obtained via Cell Phone

#	Title	URL	Last Visited	Visits	Source	Deleted
1		https://m.facebook.com/login.php?refsrc [redacted]cebook.com%2Fmessages%2F&lwv=100&refid=8	10/12/2015 6:03:05 PM(UTC-4)	1	Safari	
2	Facebook	https://m.facebook.com/home.php?refsrc [redacted]cebook.com%2Fmessages%2F&refid=8&__rdr	10/12/2015 6:03:05 PM(UTC-4)	1	Safari	
3	Giovanni [redacted]	https://m.facebook.com/messages/read/ [redacted]6%3A80c8af0dd5aa004790	10/12/2015 6:03:16 PM(UTC-4)	1	Safari	
4	[redacted]McDonnell	https://m.facebook.com/messages/read/ [redacted]2ca16416dd531beef32340	10/12/2015 6:03:26 PM(UTC-4)	1	Safari	
5	Facebook	https://m.facebook.com/home.php?refsrc [redacted]cebook.com%2Fmessages%2F	10/12/2015 6:04:02 PM(UTC-4)	5	Safari	
6	Facebook	https://m.facebook.com/home.php?refsrc [redacted]cebook.com%2Fmessages%2F&soft=messages	10/12/2015 6:04:03 PM(UTC-4)	3	Safari	
7	Monica [redacted]	https://m.facebook.com/messages/read/ [redacted]90	10/12/2015 6:04:07 PM(UTC-4)	1	Safari	
8	Monica [redacted]	https://m.facebook.com/messages/read/ [redacted]90&soft=bookmarks	10/12/2015 6:04:49 PM(UTC-4)	1	Safari	
9		https://m.facebook.com/logout.php?h=Aff [redacted]4687386&refid=7	10/12/2015 6:04:54 PM(UTC-4)	1	Safari	

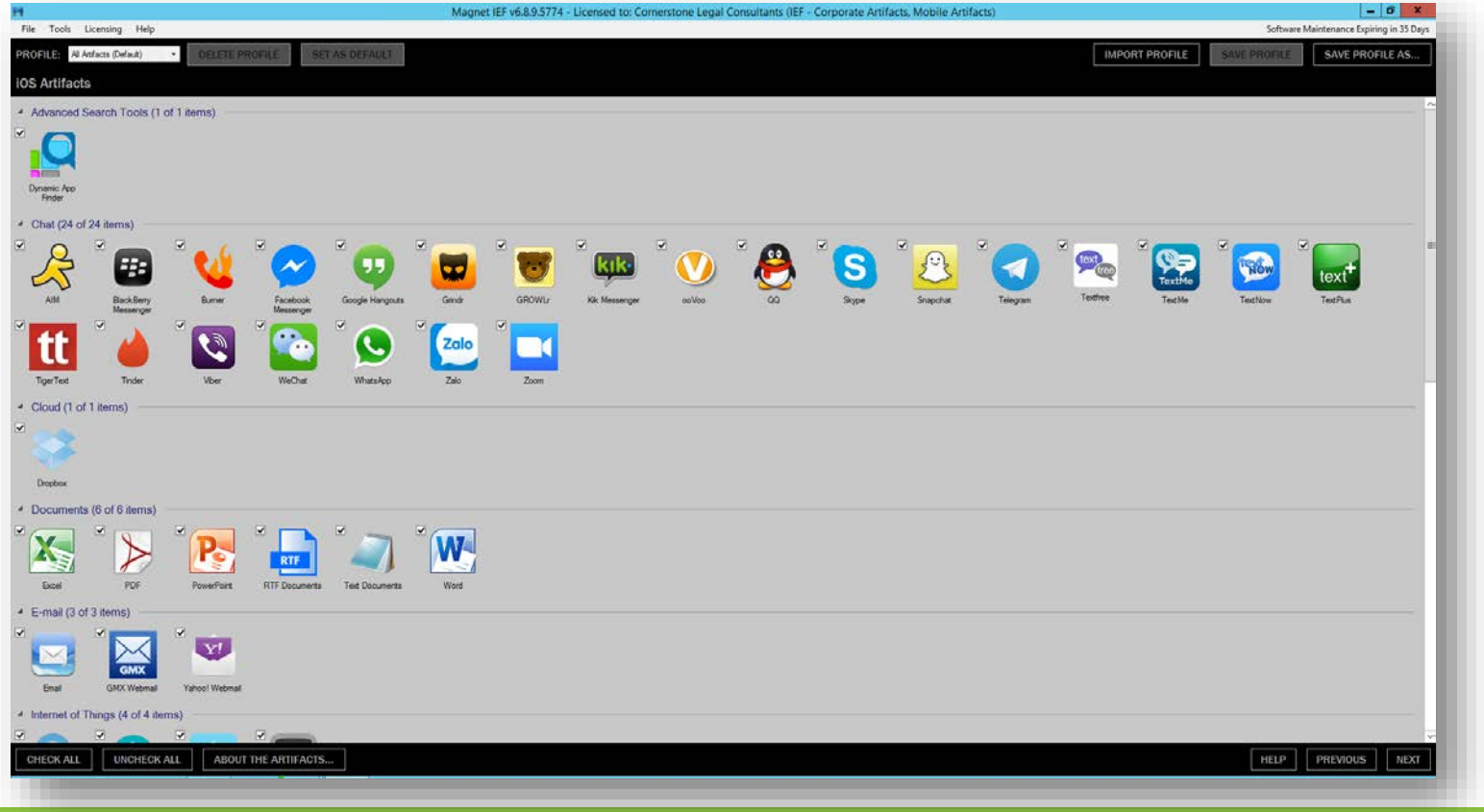
What, in Particular, Were They Doing on Their Device in any Point in Time?

- Internet History



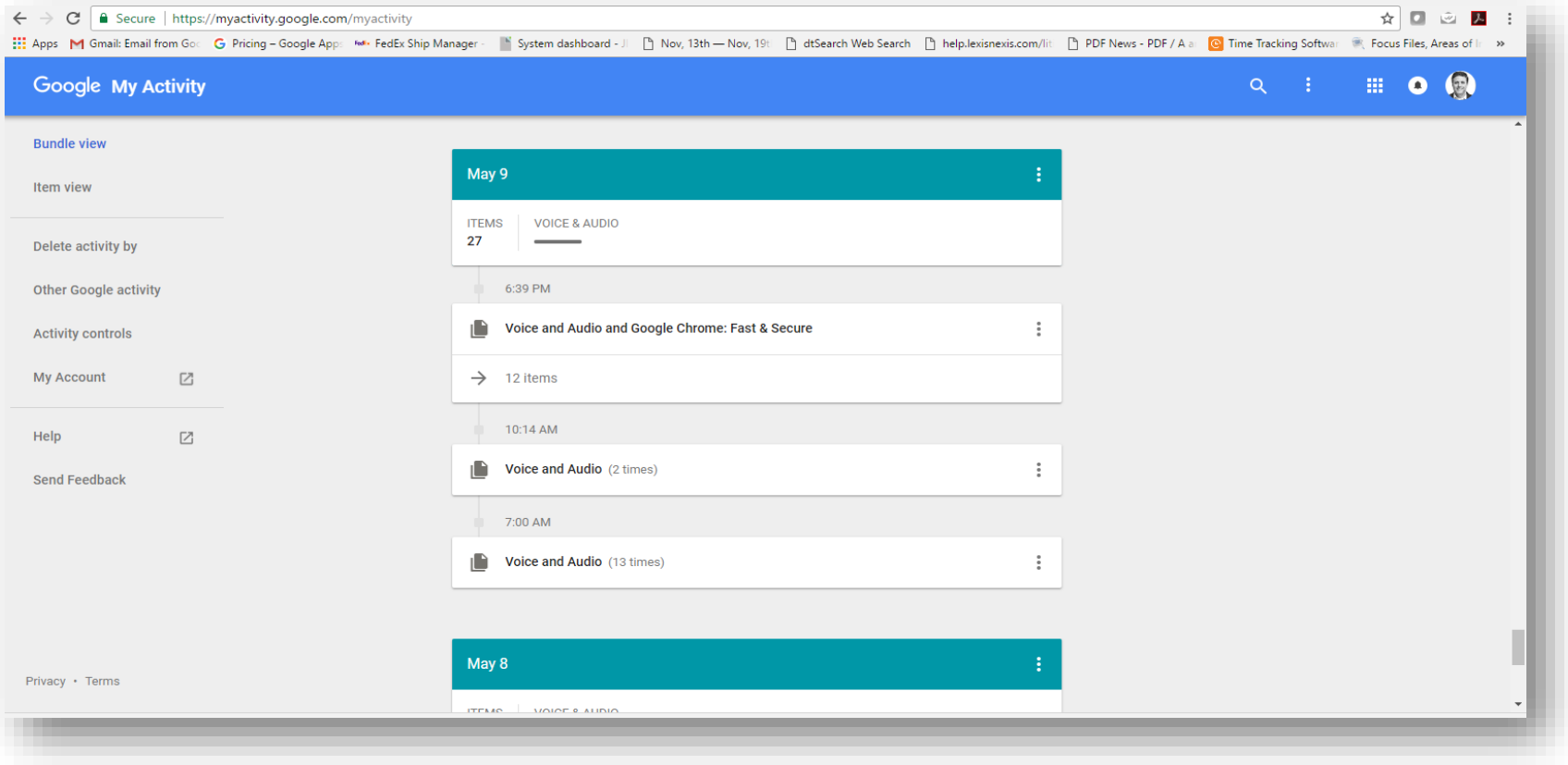
What, in Particular, Were They Doing on Their Device in any Point in Time?

- Internet History



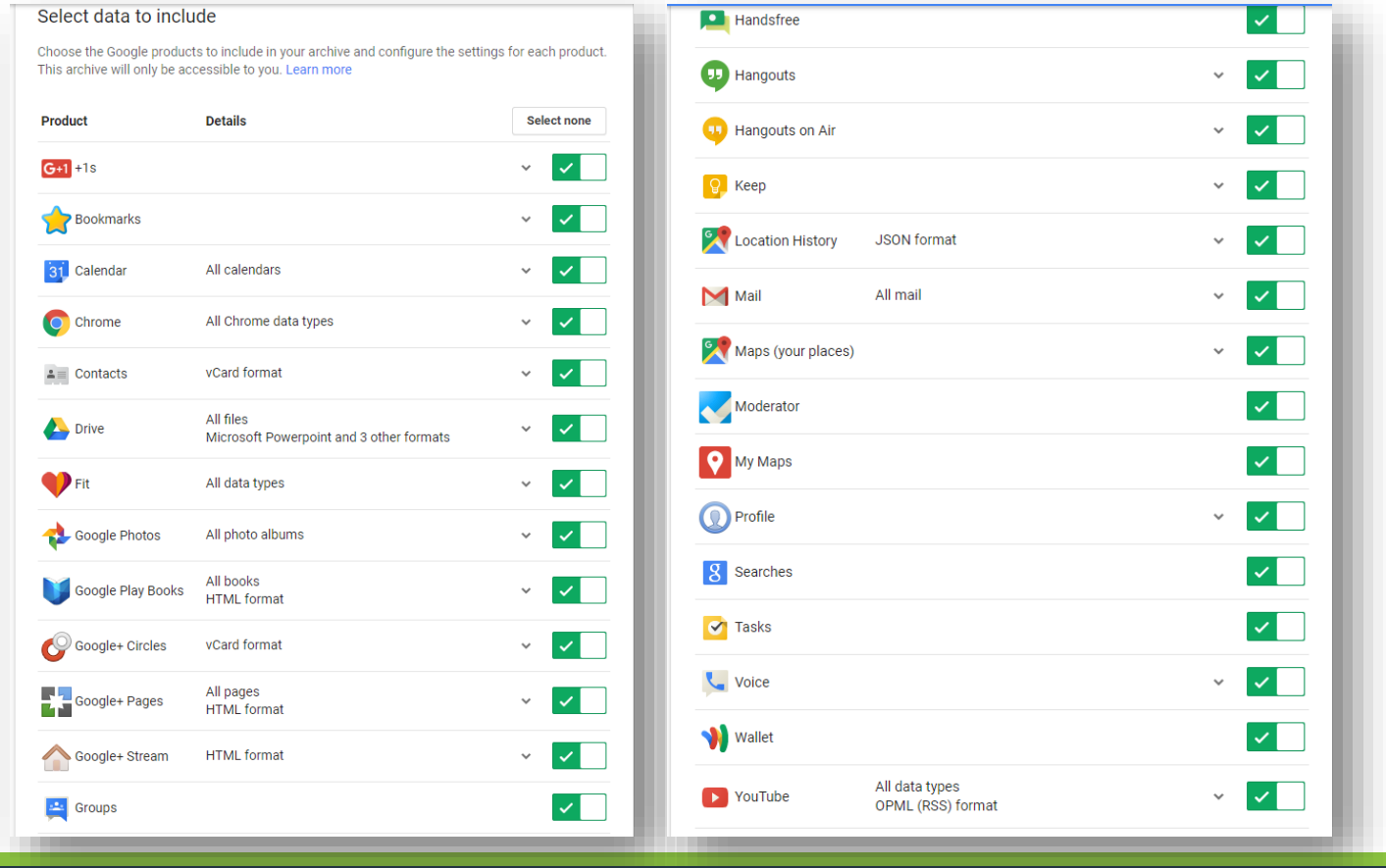
What, in Particular, Were They Doing on Their Device in any Point in Time?

- Google “My Activity”



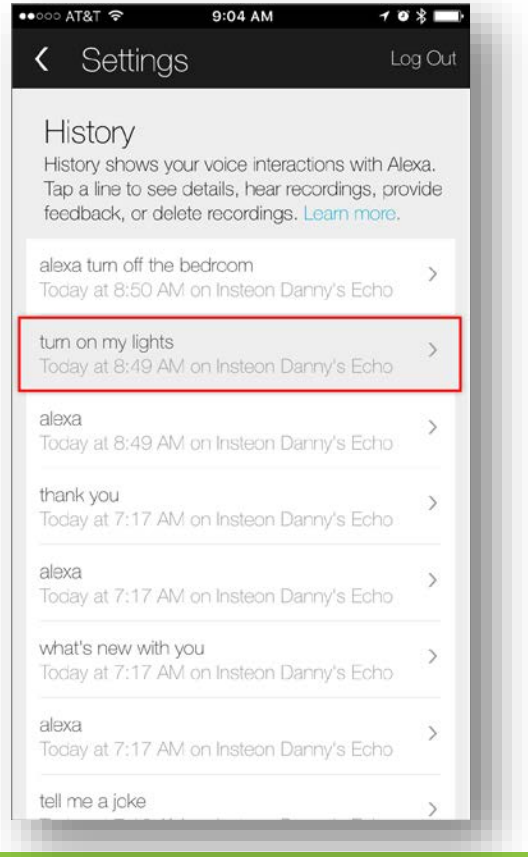
What, in Particular, Were They Doing on Their Device in any Point in Time?

- Google “Takeout”



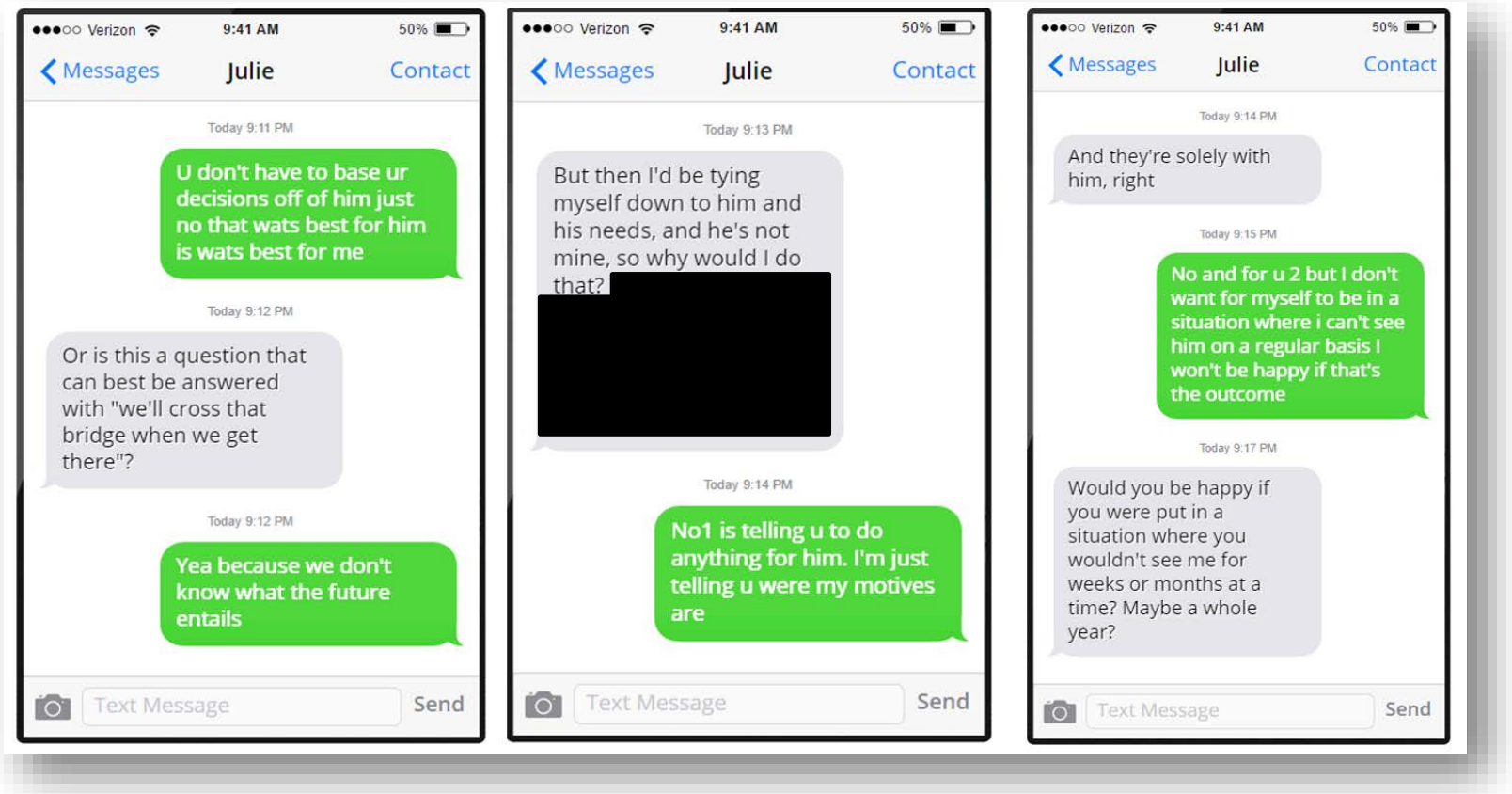
What, in Particular, Were They Doing on Their Device in any Point in Time?

- Activity Reported via Amazon Echo & Dot – Alexa



With Whom Were They Communicating on Their Device at any Point of Time?

- Text Activity Obtained via Cell Phone



Growing List of Sources From Which Information Might Be Obtainable

- Computers (Desktops, Laptops)
- Mobile Devices (iPhone, Smartphone, iPad, iPod, Tablet, GPS)
- Servers, Backup Tapes, NAS, appliances (Barracuda, Mimecast)
- Service Provider Records (AT&T, Verizon, T-Mobile, E-ZPass)
- Portable Storage (Thumb Drive, SD Cards, External Hard Drives)
- Surveillance Video (Body Cams, Dash Cams, Doorbell Cams, etc.)
- Cloud Email (Gmail, Apple Mail, Microsoft Office 365, Hotmail, Yahoo)
- Cloud Storage (Apple iCloud, Google Drive, Dropbox, Microsoft Skydrive)
- Cloud Backup (Druva, Crashplan, iBackup)
- Apps (Snapchat, Skype, Viber, Tinder)
- Social Networking (Facebook, Twitter, Linkedin)
- Gaming Consoles (Xbox, PlayStation)
- IoT - Amazon Echo & Dot (Alexa), Google Home, Fitness Trackers, Appliances, Smart Watches, Hum and More

Thank you!

This Presentation and Other Information Available at:

thetechgazette.com