opentext™

What’s in your smartphone?

Deletion does not make it disappear

Adam Kuhn

NeLI
National eDiscovery Leadership Institute

Introductions

Adam Kuhn
Director of Product Marketing
OpenText | Discovery

@AHKuhn

METROPOLITAN
CORPORATE COUNSEL
VOLUME 25, NO 3
MARCH 2017
WWW.METROCORPCOUNSEL.COM

Special Section
FCPA
PAGE 21

IN SEARCH OF THE UNKNOWN UNKNOWNS
(WITH THE HELP OF TECHNOLOGY-ASSISTED INVESTIGATIONS)
PAGE 8

Adam Kuhn (L) & Hal Marcus / OpenText Discovery

DATA MANAGEMENT
5 Tips To Mitigate Insider Theft
Julian Ackert
iDiscovery Solutions
10

RISK MANAGEMENT
Identify Scope, Impact & Likelihood Of Risk
Tina Ayotte Welu
Wolters Kluwer Legal & Regulatory U.S.
17

LIFE SCIENCES
Big Year Expected in Patent Litigation
Chad Shear
Fish & Richardson
16

SUSTAINABILITY
Renewable Energy: The State Of the Art
Susan E. Bruce
McNees Wallace & Nurick
18

IN-HOUSE OPS
DOJ's Missed Guidance
David Hechler
33

A Word From <u>My</u> Lawyers:

The views and opinions expressed in this presentation are those of the speaker and do not necessarily reflect the views and opinions of his employer.

Agenda

- Policy considerations
- Tools for investigations
- Application data
- Text and chat data
- Call and contact data
- Picture data
- Browser
- Summary
- Q&A

Policy considerations

Your cellphone is special

Cell phones and cloud storage as evidence

COPE

Company-Owned, Personally-Enabled phone

BYOD

Bring Your Own Device

Personal phone/cloud service corporate use policy

Unoffical BYOD

Personal phone/cloud service, but occasionally used for work

Tools of the trade

Now is a good time to check Amazon Prime

Tools used in Mobile Investigations

1. ***SIM Reader*** Using a SIM card reader, it is possible to access the information on the SIM card from EnCase Mobile Investigator.

2. ***Faraday Bag*** Gives the examiner piece of mind that no signals are being transferred while they are in possession on the device. ***Use patented versions only.

Application data

We know when you downloaded an unauthorized app

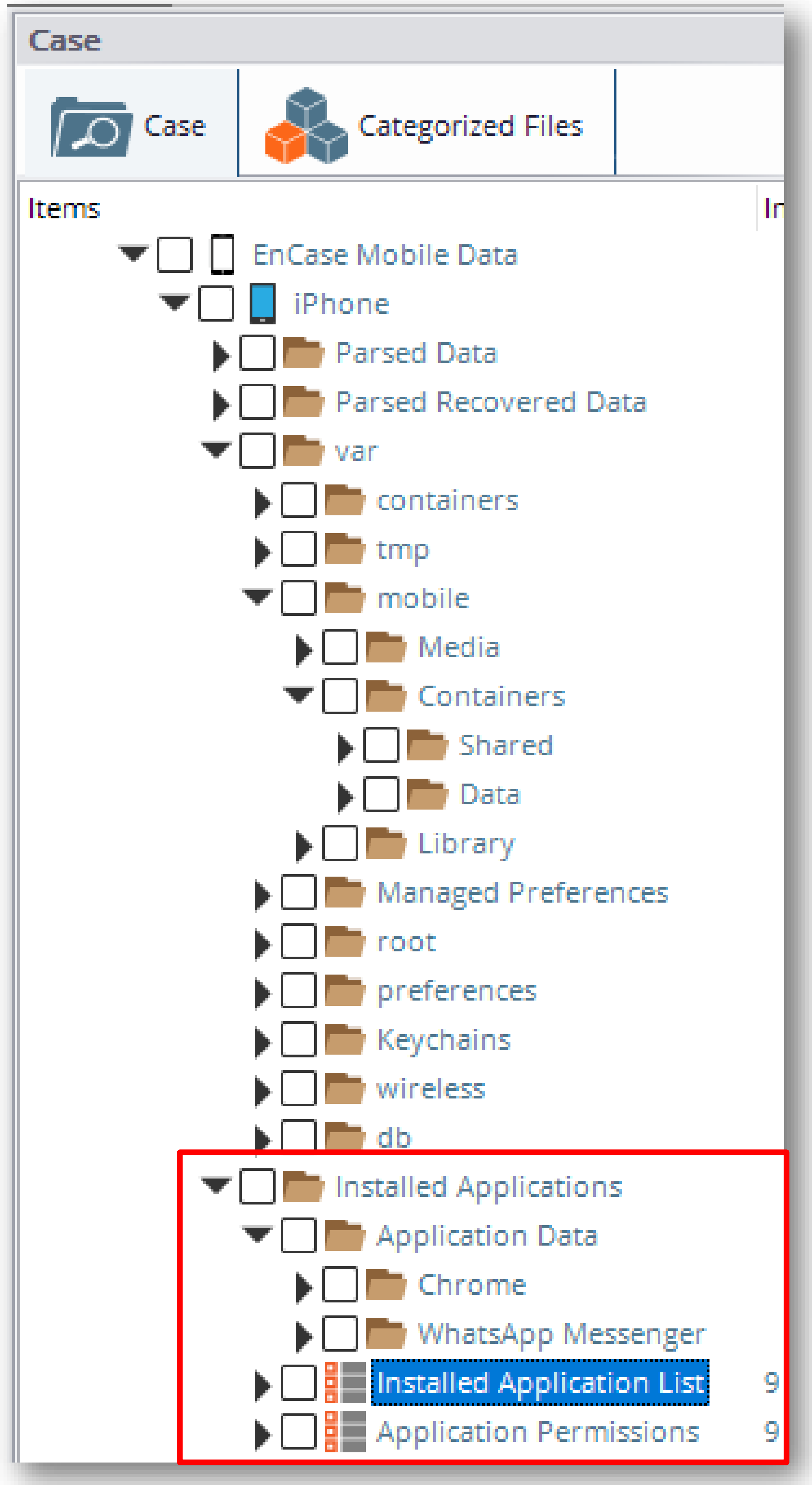
Mobile Device Examination - Artifacts

*EnCase Mobile Investigator automatically parses data from these applications:

Messenger Apps	Messenger / Platform Apps
BB Messenger	Chrome
Facebook Messenger	Facebook
Skype	Gmail
Jott Messenger	Instagram
KIK	LinkedIn
Pinger	Firefox
Telegram	TextFree
WeChat	Twitter
VoiceMail	Tinder
Whisper	Snapchat
WhatsApp	YikYak
TextPlus	Vkontakte

Misc Apps
DJI Go
Evernote
Fitbit
Google Maps
Mail.ru

Mobile device examination – iOS Example

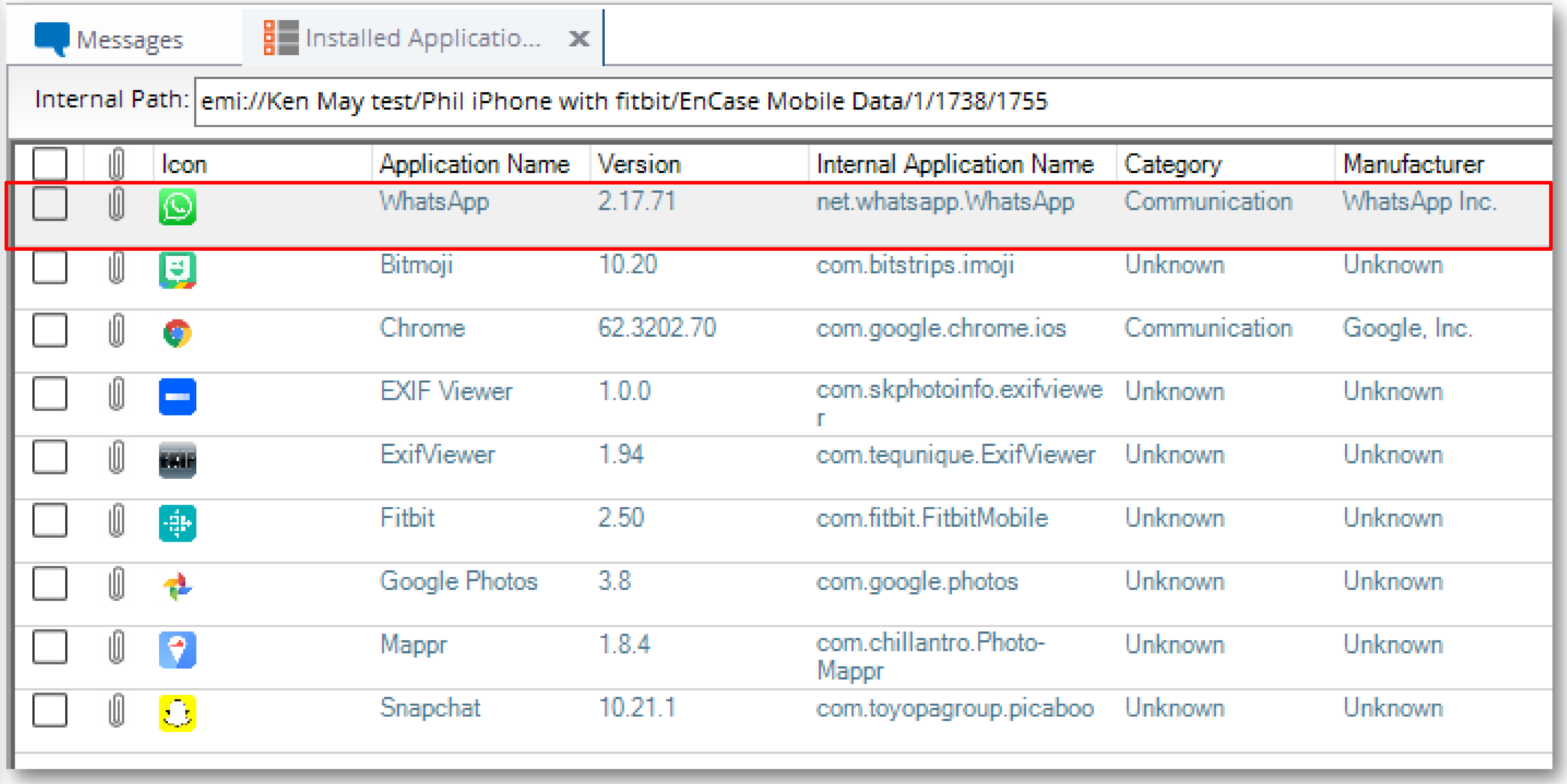


Case

Case | Categorized Files

Items

- ☐ EnCase Mobile Data
  - ☐ iPhone
    - ☐ Parsed Data
    - ☐ Parsed Recovered Data
    - ☐ var
      - ☐ containers
      - ☐ tmp
      - ☐ mobile
        - ☐ Media
        - ☐ Containers
          - ☐ Shared
          - ☐ Data
        - ☐ Library
      - ☐ Managed Preferences
      - ☐ root
      - ☐ preferences
      - ☐ Keychains
      - ☐ wireless
      - ☐ db
    - ☐ Installed Applications
      - ☐ Application Data
        - ☐ Chrome
        - ☐ WhatsApp Messenger
      - ☐ Installed Application List 9
      - ☐ Application Permissions 9

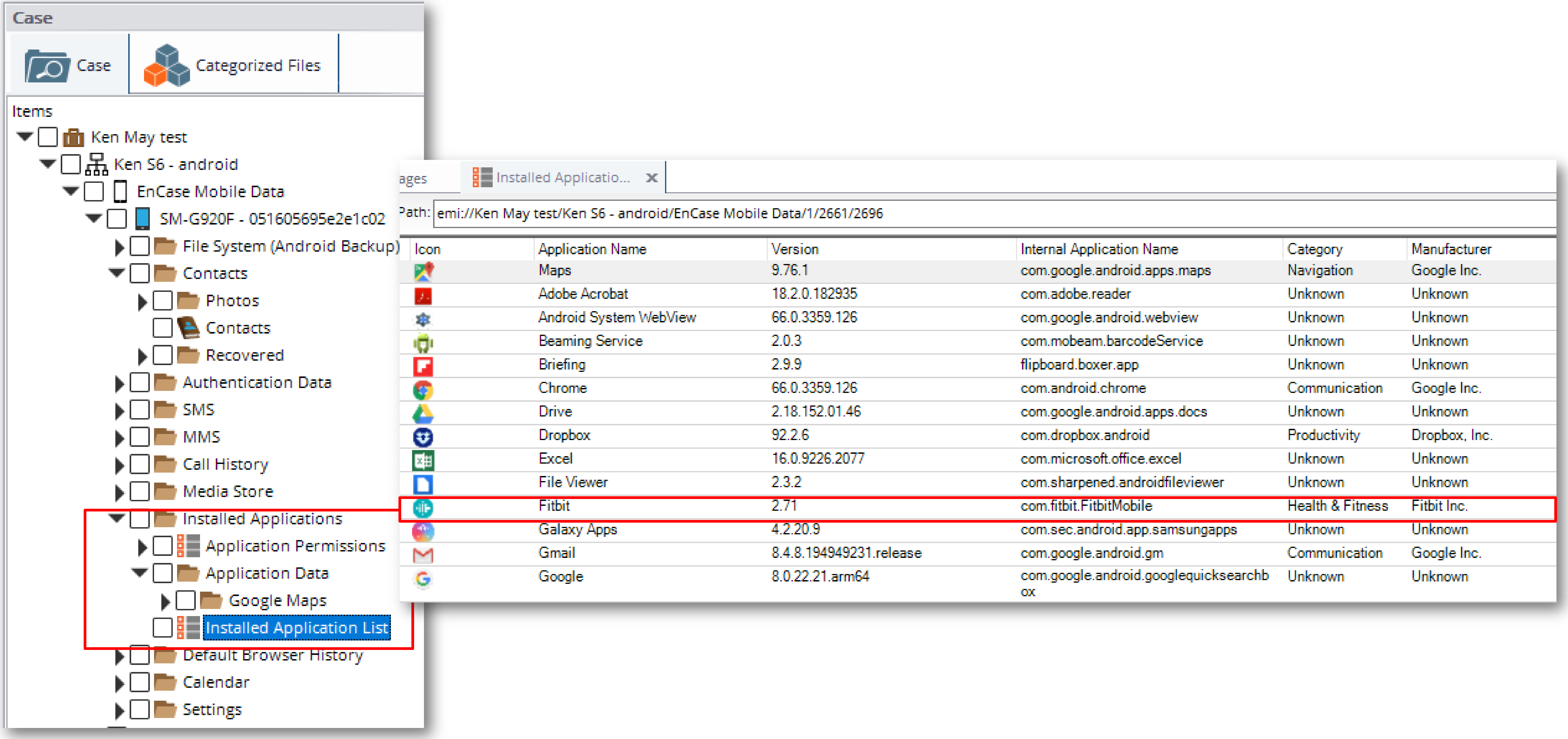


Messages | Installed Applicatio... ✕

Internal Path: emi://Ken May test/Phil iPhone with fitbit/EnCase Mobile Data/1/1738/1755

☐		Icon	Application Name	Version	Internal Application Name	Category	Manufacturer
☐			WhatsApp	2.17.71	net.whatsapp.WhatsApp	Communication	WhatsApp Inc.
☐			Bitmoji	10.20	com.bitstrips.imoji	Unknown	Unknown
☐			Chrome	62.3202.70	com.google.chrome.ios	Communication	Google, Inc.
☐			EXIF Viewer	1.0.0	com.skphotoinfo.exifviewer	Unknown	Unknown
☐			ExifViewer	1.94	com.tequnique.ExifViewer	Unknown	Unknown
☐			Fitbit	2.50	com.fitbit.FitbitMobile	Unknown	Unknown
☐			Google Photos	3.8	com.google.photos	Unknown	Unknown
☐			Mappr	1.8.4	com.chillantro.Photo-Mappr	Unknown	Unknown
☐			Snapchat	10.21.1	com.toyopagroup.picaboo	Unknown	Unknown

Mobile Device Examination – Android Example



Items
- ☐ Ken May test
  - ☐ Ken S6 - android
    - ☐ EnCase Mobile Data
      - ☐ SM-G920F - 051605695e2e1c02
        - ☐ File System (Android Backup)
        - ☐ Contacts
          - ☐ Photos
          - ☐ Contacts
          - ☐ Recovered
        - ☐ Authentication Data
        - ☐ SMS
        - ☐ MMS
        - ☐ Call History
        - ☐ Media Store
        - ☐ Installed Applications
          - ☐ Application Permissions
          - ☐ Application Data
            - ☐ Google Maps
          - ☐ Installed Application List
        - ☐ Default Browser History
        - ☐ Calendar
        - ☐ Settings

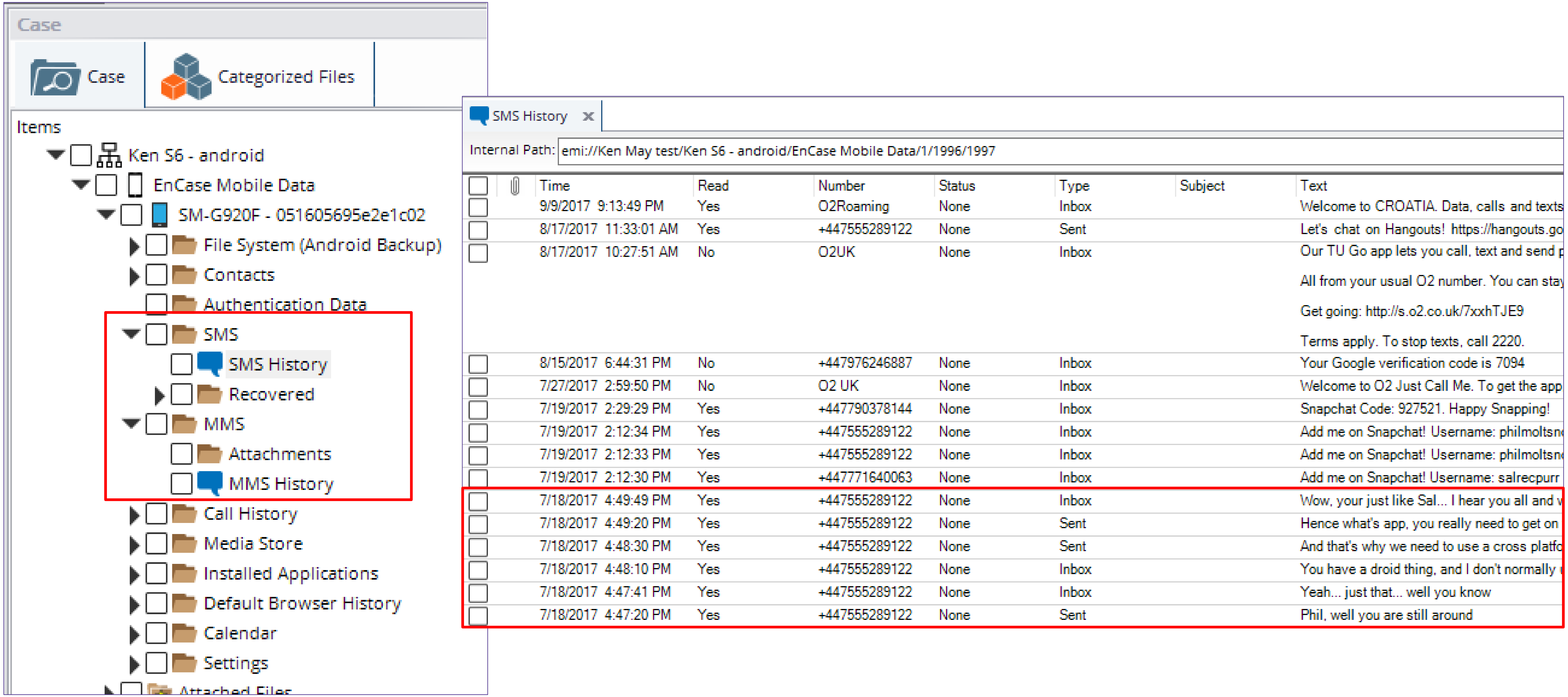
Path: emi://Ken May test/Ken S6 - android/EnCase Mobile Data/1/2661/2696

Icon	Application Name	Version	Internal Application Name	Category	Manufacturer
	Maps	9.76.1	com.google.android.apps.maps	Navigation	Google Inc.
	Adobe Acrobat	18.2.0.182935	com.adobe.reader	Unknown	Unknown
	Android System WebView	66.0.3359.126	com.google.android.webview	Unknown	Unknown
	Beaming Service	2.0.3	com.mobeam.barcodeService	Unknown	Unknown
	Briefing	2.9.9	flipboard.boxer.app	Unknown	Unknown
	Chrome	66.0.3359.126	com.android.chrome	Communication	Google Inc.
	Drive	2.18.152.01.46	com.google.android.apps.docs	Unknown	Unknown
	Dropbox	92.2.6	com.dropbox.android	Productivity	Dropbox, Inc.
	Excel	16.0.9226.2077	com.microsoft.office.excel	Unknown	Unknown
	File Viewer	2.3.2	com.sharpened.androidfileviewer	Unknown	Unknown
	Fitbit	2.71	com.fitbit.FitbitMobile	Health & Fitness	Fitbit Inc.
	Galaxy Apps	4.2.20.9	com.sec.android.app.samsungapps	Unknown	Unknown
	Gmail	8.4.8.194949231.release	com.google.android.gm	Communication	Google Inc.
	Google	8.0.22.21.arm64	com.google.android.googlequicksearchbox	Unknown	Unknown

Text message data

The real reason we own smartphones

Mobile Device Examination – SMS and MMS



Case

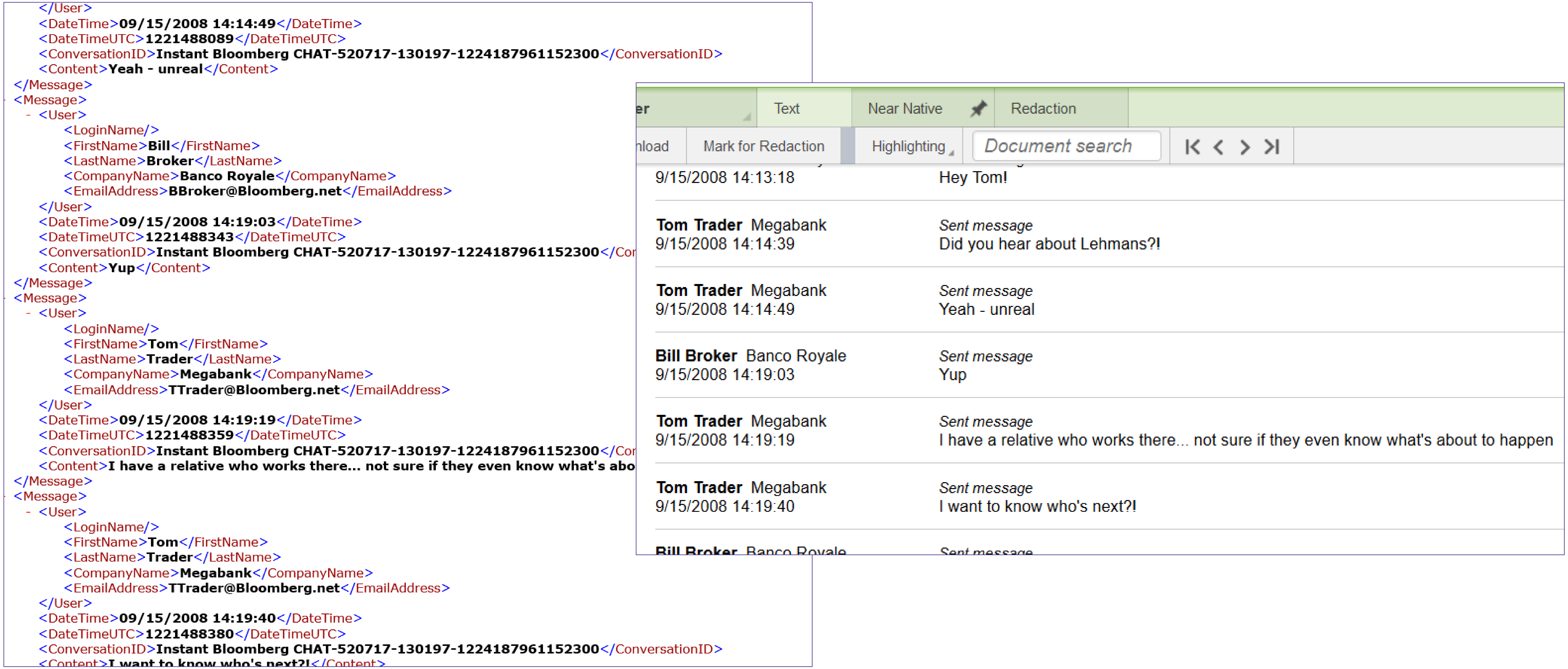
Items

- ☐ Ken S6 - android
  - ☐ EnCase Mobile Data
    - ☐ SM-G920F - 051605695e2e1c02
      - ☐ File System (Android Backup)
      - ☐ Contacts
      - ☐ Authentication Data
      - ☐ SMS
        - ☐ SMS History
        - ☐ Recovered
      - ☐ MMS
        - ☐ Attachments
        - ☐ MMS History
      - ☐ Call History
      - ☐ Media Store
      - ☐ Installed Applications
      - ☐ Default Browser History
      - ☐ Calendar
      - ☐ Settings
  - ☐ Attached Files

Internal Path: emi://Ken May test/Ken S6 - android/EnCase Mobile Data/1/1996/1997

☐		Time	Read	Number	Status	Type	Subject	Text
☐		9/9/2017 9:13:49 PM	Yes	O2Roaming	None	Inbox		Welcome to CROATIA. Data, calls and texts
☐		8/17/2017 11:33:01 AM	Yes	+447555289122	None	Sent		Let's chat on Hangouts! https://hangouts.go
☐		8/17/2017 10:27:51 AM	No	O2UK	None	Inbox		Our TU Go app lets you call, text and send p All from your usual O2 number. You can sta Get going: http://s.o2.co.uk/7xxhTJE9 Terms apply. To stop texts, call 2220.
☐		8/15/2017 6:44:31 PM	No	+447976246887	None	Inbox		Your Google verification code is 7094
☐		7/27/2017 2:59:50 PM	No	O2 UK	None	Inbox		Welcome to O2 Just Call Me. To get the app
☐		7/19/2017 2:29:29 PM	Yes	+447790378144	None	Inbox		Snapchat Code: 927521. Happy Snapping!
☐		7/19/2017 2:12:34 PM	Yes	+447555289122	None	Inbox		Add me on Snapchat! Username: philmoltsn
☐		7/19/2017 2:12:33 PM	Yes	+447555289122	None	Inbox		Add me on Snapchat! Username: philmoltsn
☐		7/19/2017 2:12:30 PM	Yes	+447771640063	None	Inbox		Add me on Snapchat! Username: salrecpurr
☐		7/18/2017 4:49:49 PM	Yes	+447555289122	None	Inbox		Wow, your just like Sal... I hear you all and
☐		7/18/2017 4:49:20 PM	Yes	+447555289122	None	Sent		Hence what's app, you really need to get on
☐		7/18/2017 4:48:30 PM	Yes	+447555289122	None	Sent		And that's why we need to use a cross platfo
☐		7/18/2017 4:48:10 PM	Yes	+447555289122	None	Inbox		You have a droid thing, and I don't normally
☐		7/18/2017 4:47:41 PM	Yes	+447555289122	None	Inbox		Yeah... just that... well you know
☐		7/18/2017 4:47:20 PM	Yes	+447555289122	None	Sent		Phil, well you are still around

Comparison of raw XML output to parsed



```
    </User>
    <DateTime>09/15/2008 14:14:49</DateTime>
    <DateTimeUTC>1221488089</DateTimeUTC>
    <ConversationID>Instant Bloomberg CHAT-520717-130197-1224187961152300</ConversationID>
    <Content>Yeah - unreal</Content>
 </Message>
- <Message>
  - <User>
        <LoginName/>
        <FirstName>Bill</FirstName>
        <LastName>Broker</LastName>
        <CompanyName>Banco Royale</CompanyName>
        <EmailAddress>BBroker@Bloomberg.net</EmailAddress>
    </User>
    <DateTime>09/15/2008 14:19:03</DateTime>
    <DateTimeUTC>1221488343</DateTimeUTC>
    <ConversationID>Instant Bloomberg CHAT-520717-130197-1224187961152300</Cor
    <Content>Yup</Content>
 </Message>
- <Message>
  - <User>
        <LoginName/>
        <FirstName>Tom</FirstName>
        <LastName>Trader</LastName>
        <CompanyName>Megabank</CompanyName>
        <EmailAddress>TTrader@Bloomberg.net</EmailAddress>
    </User>
    <DateTime>09/15/2008 14:19:19</DateTime>
    <DateTimeUTC>1221488359</DateTimeUTC>
    <ConversationID>Instant Bloomberg CHAT-520717-130197-1224187961152300</Cor
    <Content>I have a relative who works there... not sure if they even know what's abo
 </Message>
- <Message>
  - <User>
        <LoginName/>
        <FirstName>Tom</FirstName>
        <LastName>Trader</LastName>
        <CompanyName>Megabank</CompanyName>
        <EmailAddress>TTrader@Bloomberg.net</EmailAddress>
    </User>
    <DateTime>09/15/2008 14:19:40</DateTime>
    <DateTimeUTC>1221488380</DateTimeUTC>
    <ConversationID>Instant Bloomberg CHAT-520717-130197-1224187961152300</ConversationID>
    <Content>I want to know who's next?!</Content>
```

9/15/2008 14:13:18 — Hey Tom!

Tom Trader Megabank
9/15/2008 14:14:39
Sent message
Did you hear about Lehmans?!

Tom Trader Megabank
9/15/2008 14:14:49
Sent message
Yeah - unreal

Bill Broker Banco Royale
9/15/2008 14:19:03
Sent message
Yup

Tom Trader Megabank
9/15/2008 14:19:19
Sent message
I have a relative who works there... not sure if they even know what's about to happen

Tom Trader Megabank
9/15/2008 14:19:40
Sent message
I want to know who's next?!

Bill Broker Banco Royale
Sent message

Analyzing text data with unsupervised machine learning

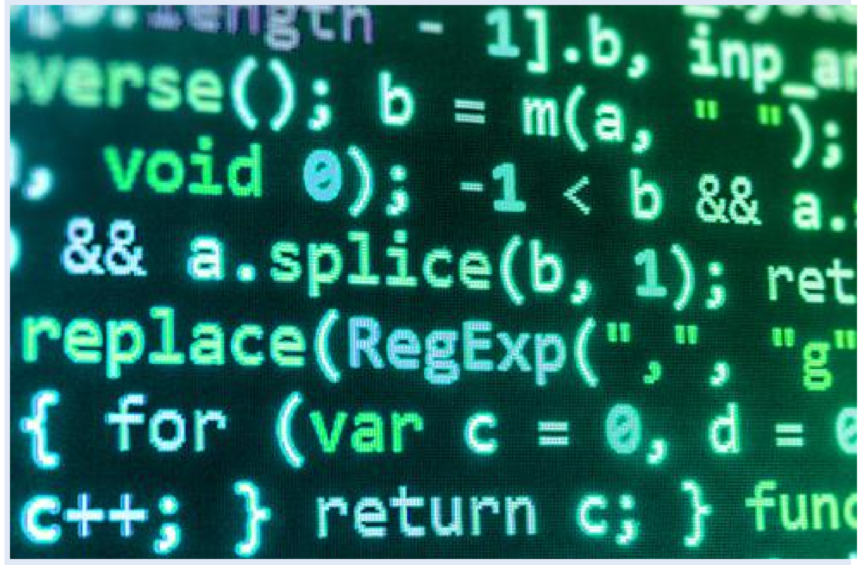
“Java”

java
coffee
starbucks
espresso
bean
latte

CONCEPT 34

indonesia
sumatra
island
java
beach
bali

CONCEPT 76

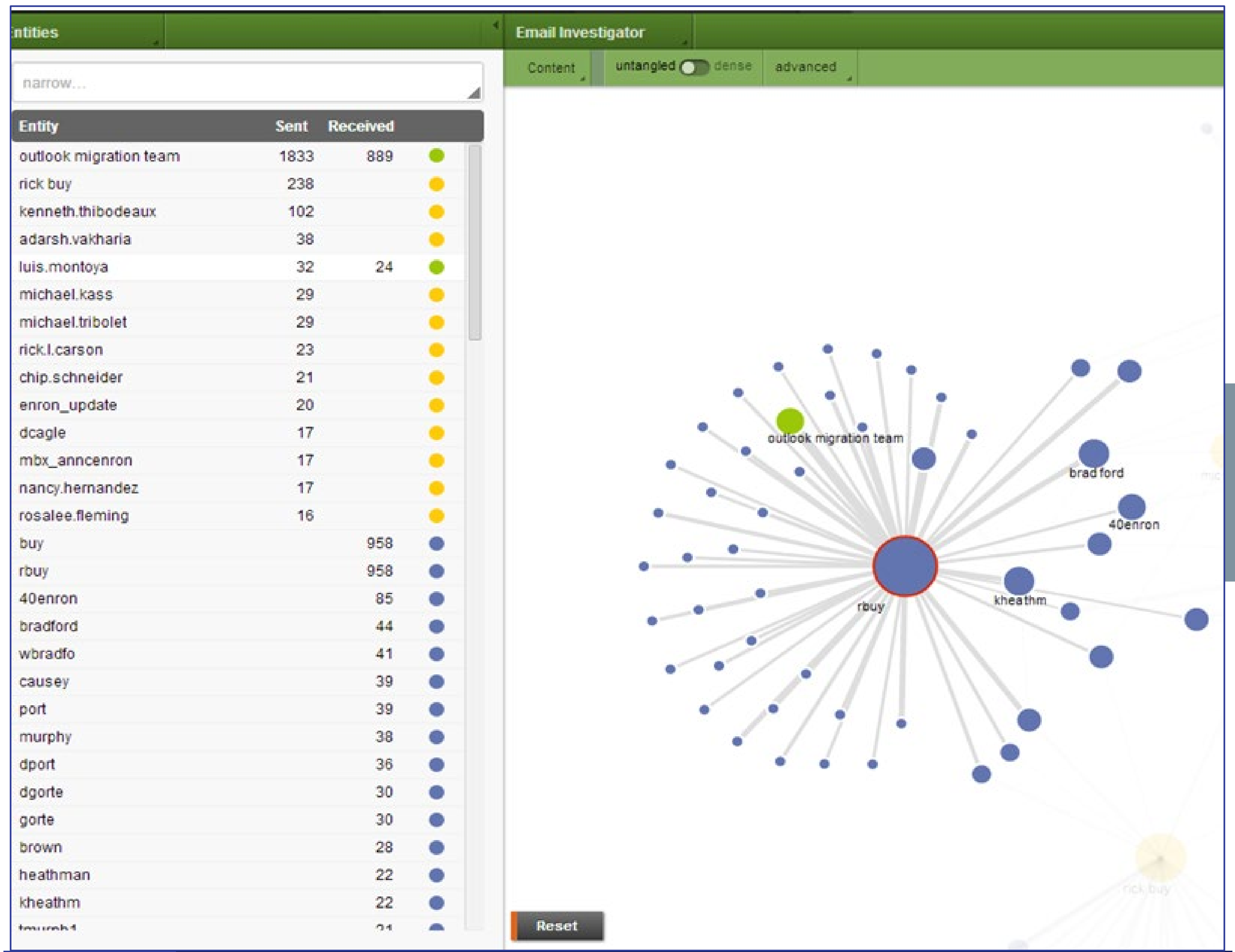


```
.length - 1].b, inp_a
verse(); b = m(a, " ");
, void 0); -1 < b && a.
&& a.splice(b, 1); ret
replace(RegExp(",", "g"
{ for (var c = 0, d = 
c++; } return c; } fun
```

software
development
script
java
code
compile

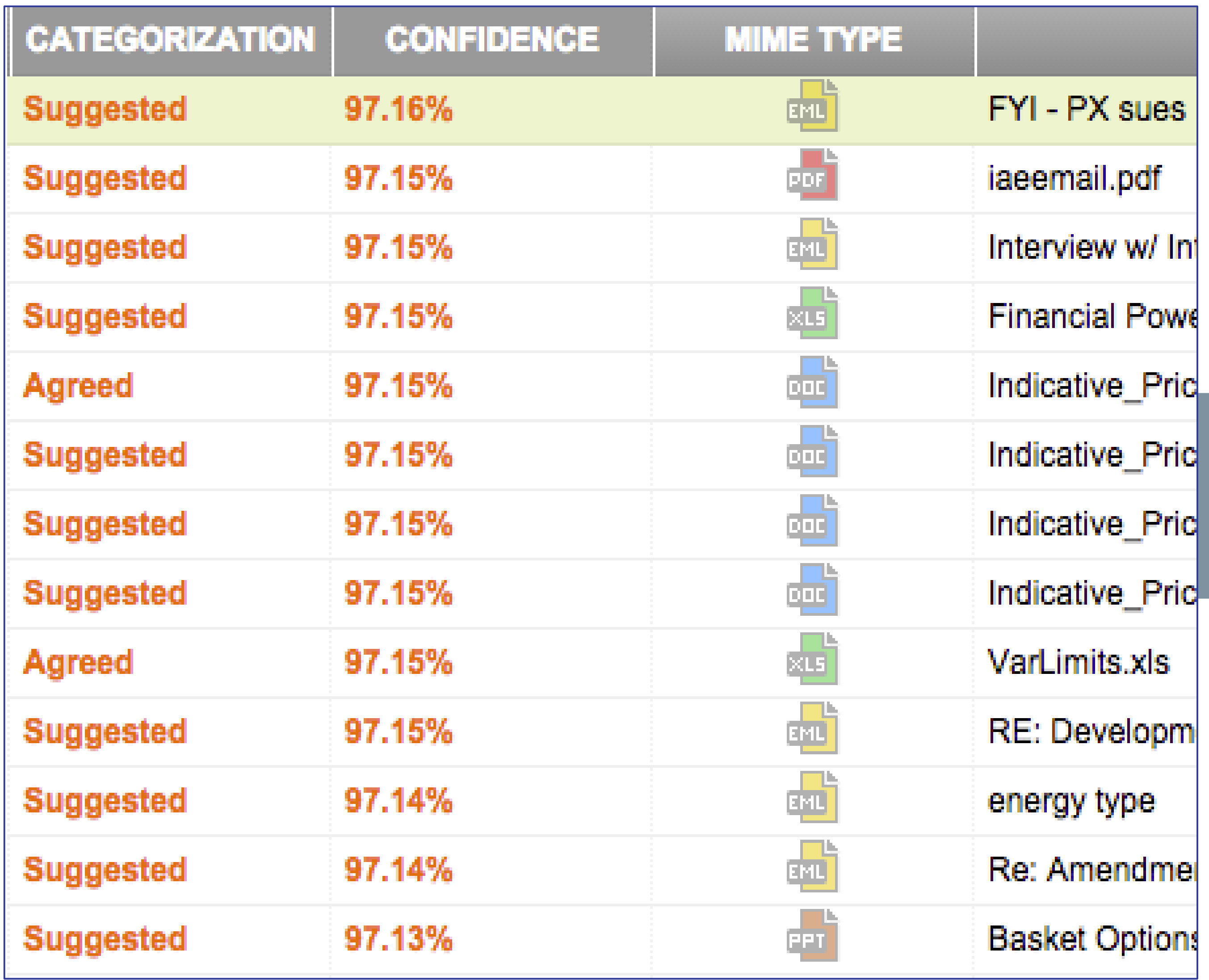
CONCEPT 149

Analyzing text data with supervised machine learning



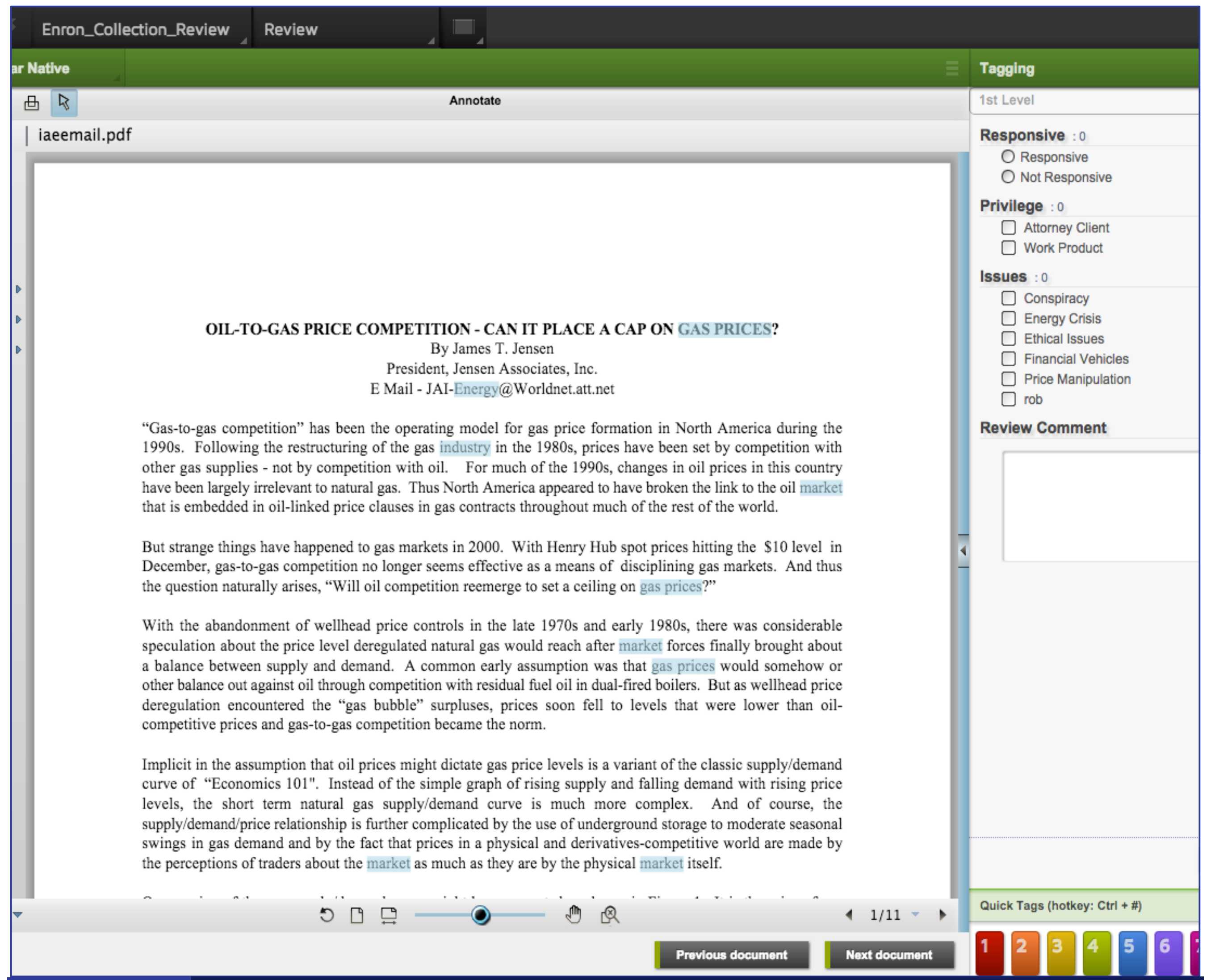
Entity	Sent	Received	
outlook migration team	1833	889	●
rick buy	238		●
kenneth.thibodeaux	102		●
adarsh.vakharia	38		●
luis.montoya	32	24	●
michael.kass	29		●
michael.tribolet	29		●
rick.l.carson	23		●
chip.schneider	21		●
enron_update	20		●
dcagle	17		●
mbx_anncenron	17		●
nancy.hernandez	17		●
rosalee.fleming	16		●
buy		958	●
rbuy		958	●
40enron		85	●
bradford		44	●
wbradfo		41	●
causey		39	●
port		39	●
murphy		38	●
dport		36	●
dgorte		30	●
gorte		30	●
brown		28	●
heathman		22	●
kheathm		22	●

1. Humans find and code relevant documents



CATEGORIZATION	CONFIDENCE	MIME TYPE	
Suggested	97.16%	EML	FYI - PX sues
Suggested	97.15%	PDF	iaeemail.pdf
Suggested	97.15%	EML	Interview w/ In
Suggested	97.15%	XLS	Financial Powe
Agreed	97.15%	DOC	Indicative_Pric
Suggested	97.15%	DOC	Indicative_Pric
Suggested	97.15%	DOC	Indicative_Pric
Suggested	97.15%	DOC	Indicative_Pric
Agreed	97.15%	XLS	VarLimits.xls
Suggested	97.15%	EML	RE: Developm
Suggested	97.14%	EML	energy type
Suggested	97.14%	EML	Re: Amendme
Suggested	97.13%	PPT	Basket Options

2. Machine suggests more relevant docs



iaeemail.pdf

OIL-TO-GAS PRICE COMPETITION - CAN IT PLACE A CAP ON GAS PRICES?
By James T. Jensen
President, Jensen Associates, Inc.
E Mail - JAI-Energy@Worldnet.att.net

"Gas-to-gas competition" has been the operating model for gas price formation in North America during the 1990s. Following the restructuring of the gas industry in the 1980s, prices have been set by competition with other gas supplies - not by competition with oil. For much of the 1990s, changes in oil prices in this country have been largely irrelevant to natural gas. Thus North America appeared to have broken the link to the oil market that is embedded in oil-linked price clauses in gas contracts throughout much of the rest of the world.

But strange things have happened to gas markets in 2000. With Henry Hub spot prices hitting the $10 level in December, gas-to-gas competition no longer seems effective as a means of disciplining gas markets. And thus the question naturally arises, "Will oil competition reemerge to set a ceiling on gas prices?"

With the abandonment of wellhead price controls in the late 1970s and early 1980s, there was considerable speculation about the price level deregulated natural gas would reach after market forces finally brought about a balance between supply and demand. A common early assumption was that gas prices would somehow or other balance out against oil through competition with residual fuel oil in dual-fired boilers. But as wellhead price deregulation encountered the "gas bubble" surpluses, prices soon fell to levels that were lower than oil-competitive prices and gas-to-gas competition became the norm.

Implicit in the assumption that oil prices might dictate gas price levels is a variant of the classic supply/demand curve of "Economics 101". Instead of the simple graph of rising supply and falling demand with rising price levels, the short term natural gas supply/demand curve is much more complex. And of course, the supply/demand/price relationship is further complicated by the use of underground storage to moderate seasonal swings in gas demand and by the fact that prices in a physical and derivatives-competitive world are made by the perceptions of traders about the market as much as they are by the physical market itself.

Responsive : 0
○ Responsive
○ Not Responsive

Privilege : 0
☐ Attorney Client
☐ Work Product

Issues : 0
☐ Conspiracy
☐ Energy Crisis
☐ Ethical Issues
☐ Financial Vehicles
☐ Price Manipulation
☐ rob

Review Comment

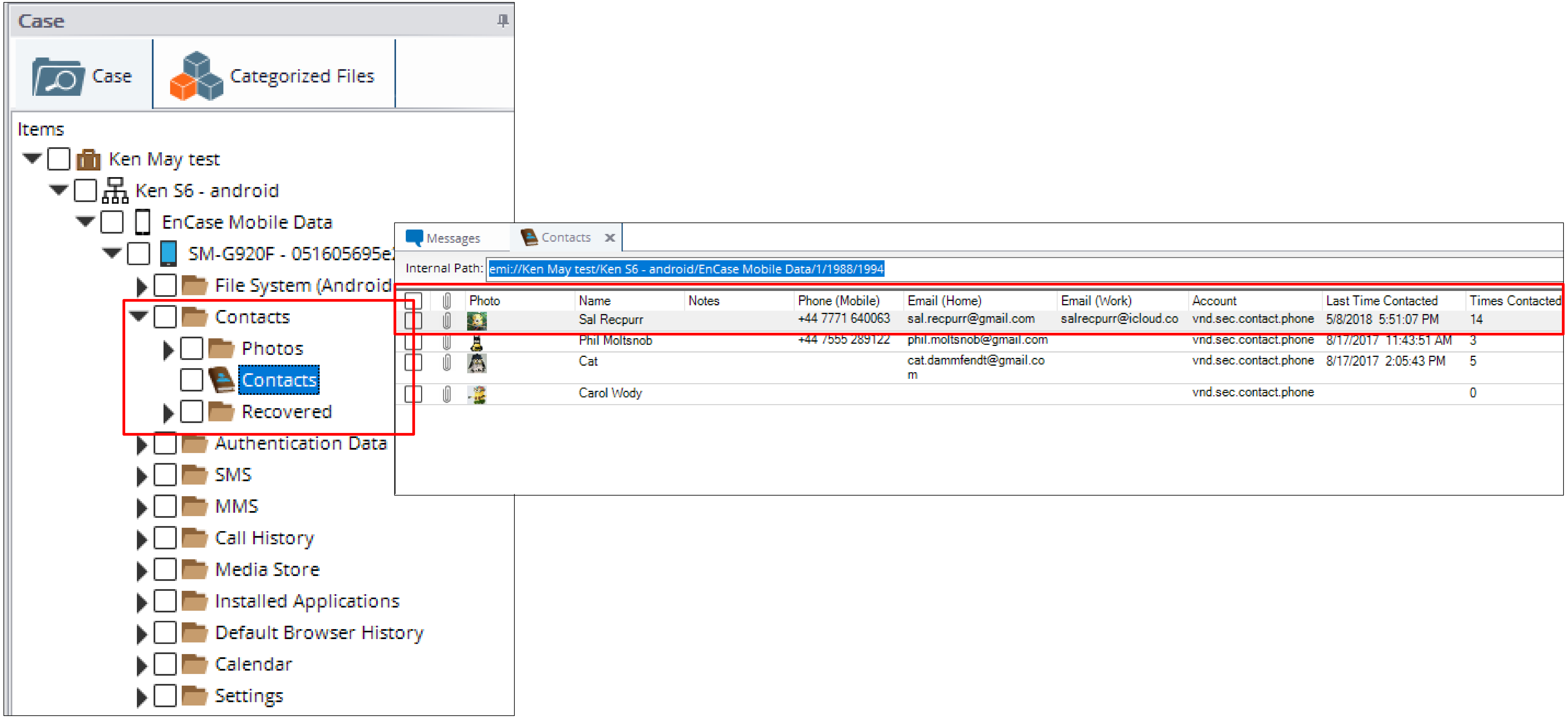
3. Humans review them, adding to the training

National eDiscovery Leadership Institute

Call and contact data

People do still use smartphones to make calls

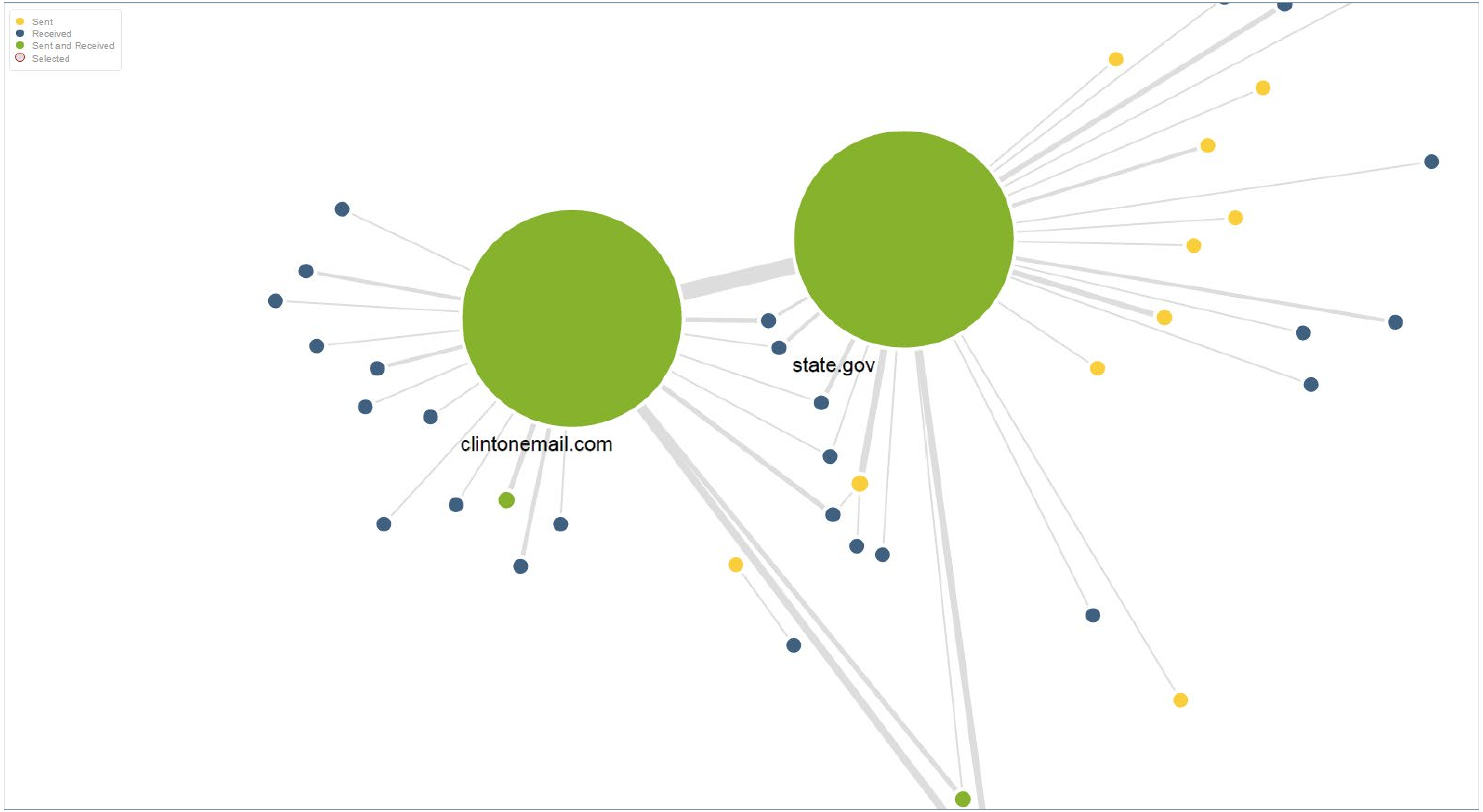
Mobile Device Examination – Contacts list



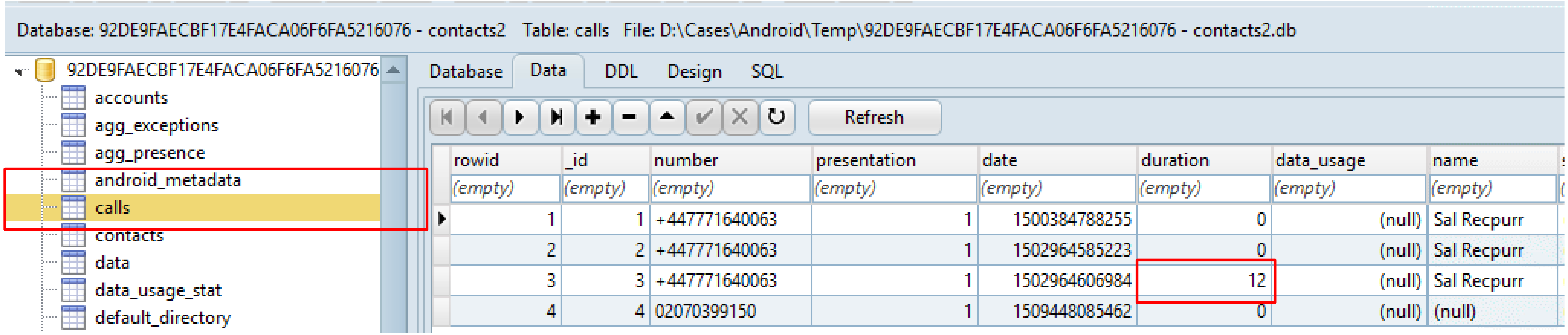
Internal Path: emi://Ken May test/Ken S6 - android/EnCase Mobile Data/1/1988/1994

☐		Photo	Name	Notes	Phone (Mobile)	Email (Home)	Email (Work)	Account	Last Time Contacted	Times Contacted
☐			Sal Recpurr		+44 7771 640063	sal.recpurr@gmail.com	salrecpurr@icloud.co	vnd.sec.contact.phone	5/8/2018 5:51:07 PM	14
☐			Phil Moltsnob		+44 7555 289122	phil.moltsnob@gmail.com		vnd.sec.contact.phone	8/17/2017 11:43:51 AM	3
☐			Cat			cat.dammfendt@gmail.com		vnd.sec.contact.phone	8/17/2017 2:05:43 PM	5
☐			Carol Wody					vnd.sec.contact.phone		0

Contact analysis: Communication map



Mobile Device Examination – Calls

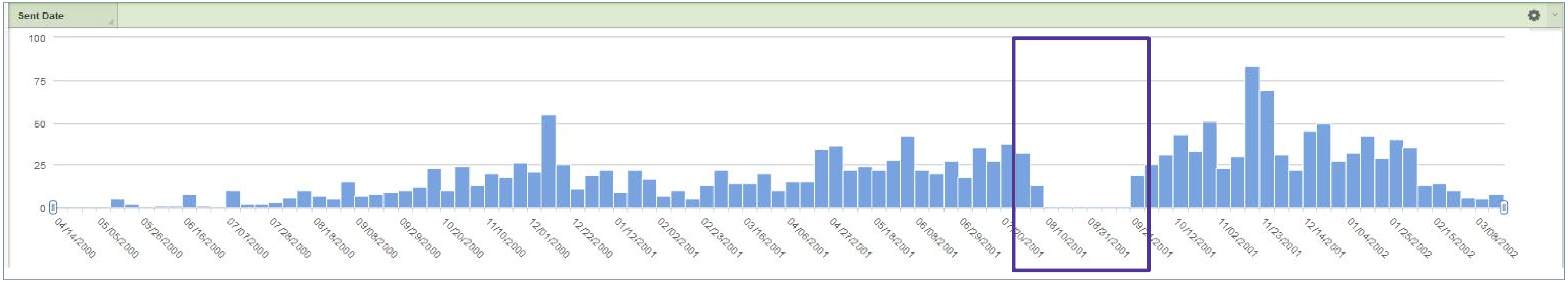


Database: 92DE9FAECBF17E4FACA06F6FA5216076 - contacts2 Table: calls File: D:\Cases\Android\Temp\92DE9FAECBF17E4FACA06F6FA5216076 - contacts2.db

- 92DE9FAECBF17E4FACA06F6FA5216076
  - accounts
  - agg_exceptions
  - agg_presence
  - android_metadata
  - calls
  - contacts
  - data
  - data_usage_stat
  - default_directory

rowid	_id	number	presentation	date	duration	data_usage	name
(empty)	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)
1	1	+447771640063	1	1500384788255	0	(null)	Sal Recpurr
2	2	+447771640063	1	1502964585223	0	(null)	Sal Recpurr
3	3	+447771640063	1	1502964606984	12	(null)	Sal Recpurr
4	4	02070399150	1	1509448085462	0	(null)	(null)

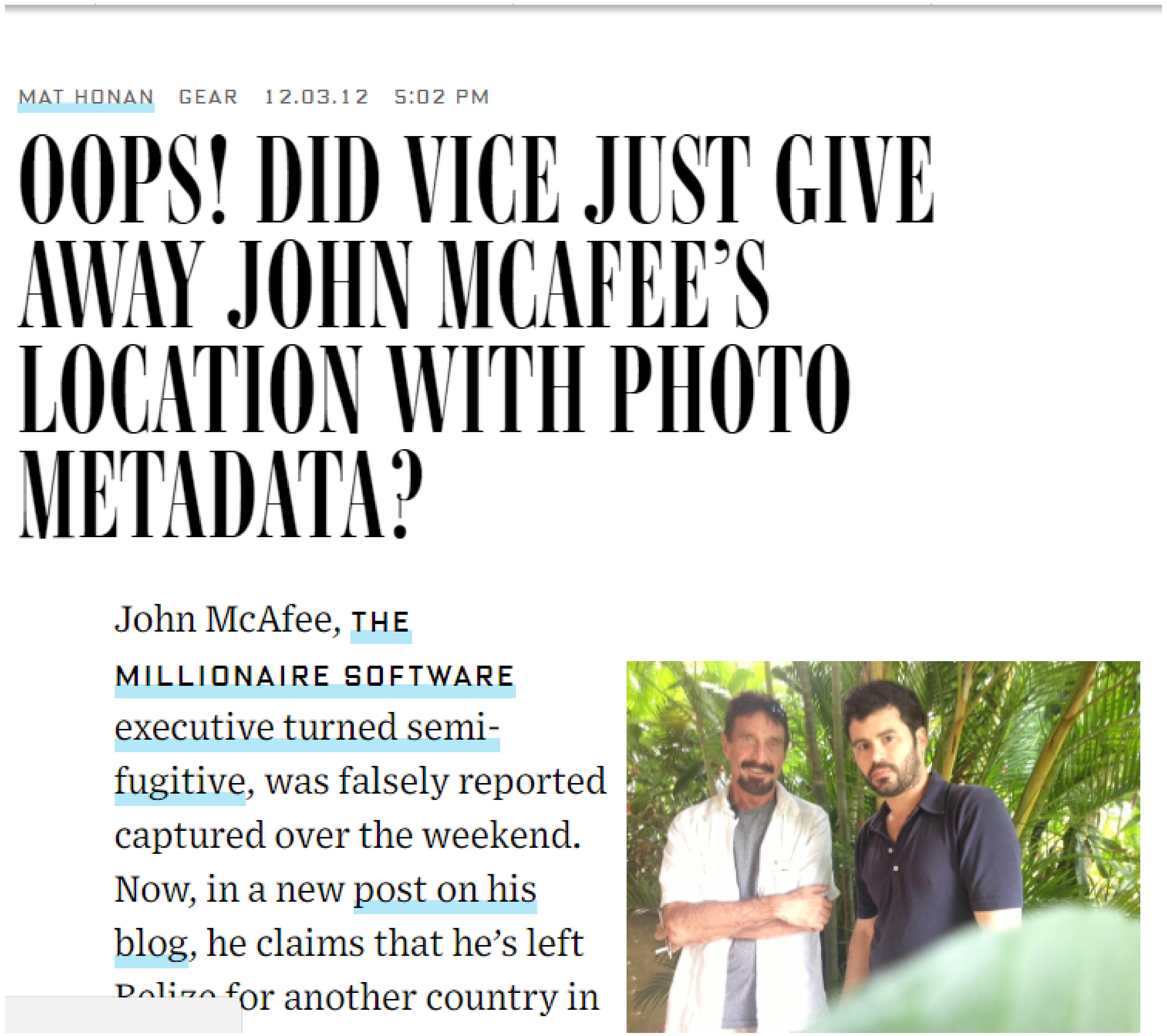
Activity analysis: Histogram



Picture data

It really is worth a million words

NeLI
National eDiscovery Leadership Institute



MAT HONAN GEAR 12.03.12 5:02 PM

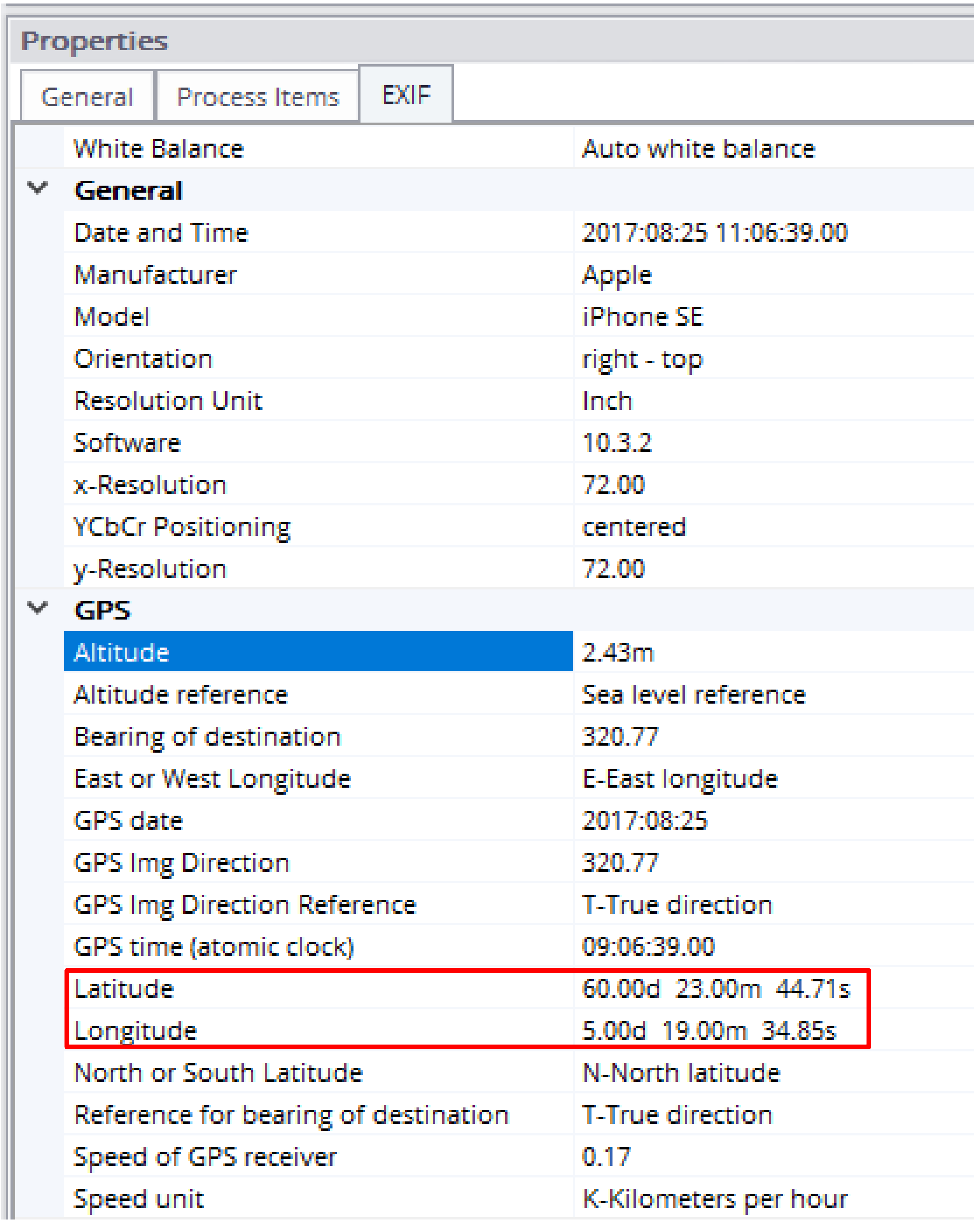
OOPS! DID VICE JUST GIVE AWAY JOHN MCAFEE'S LOCATION WITH PHOTO METADATA?

John McAfee, THE MILLIONAIRE SOFTWARE executive turned semi-fugitive, was falsely reported captured over the weekend. Now, in a new post on his blog, he claims that he's left Belize for another country in

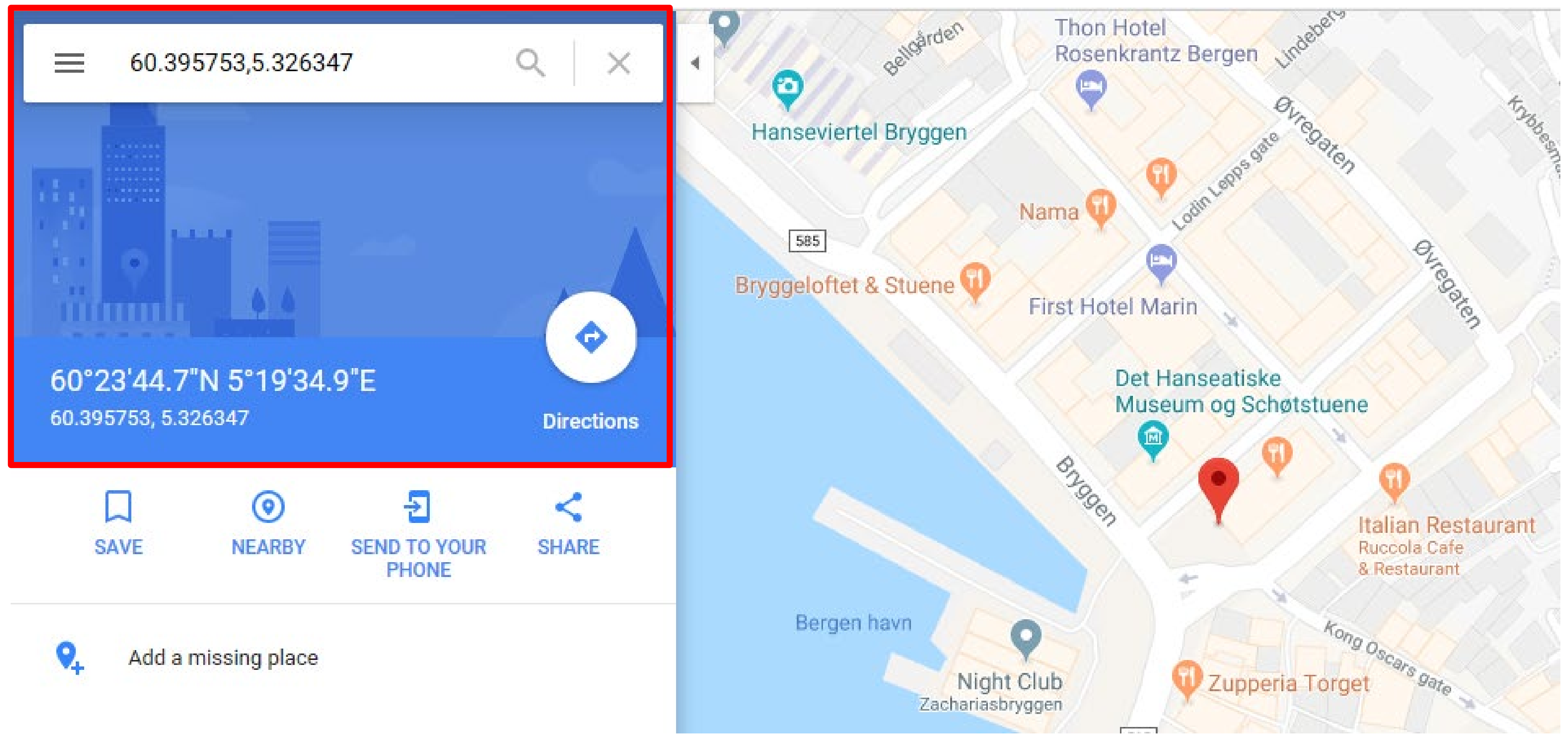
Picture data

- EXIF data is the automatically captured metadata related to a picture
- Answers “when, where, and how”
- Usually includes:
    - Date and time
    - GPS data (latitude, longitude, etc)
    - Photo settings (aperture, orientation, etc)
    - Device information (model, software, etc)
- EXIF data is captured by default
- And most platform providers will preserve it by default

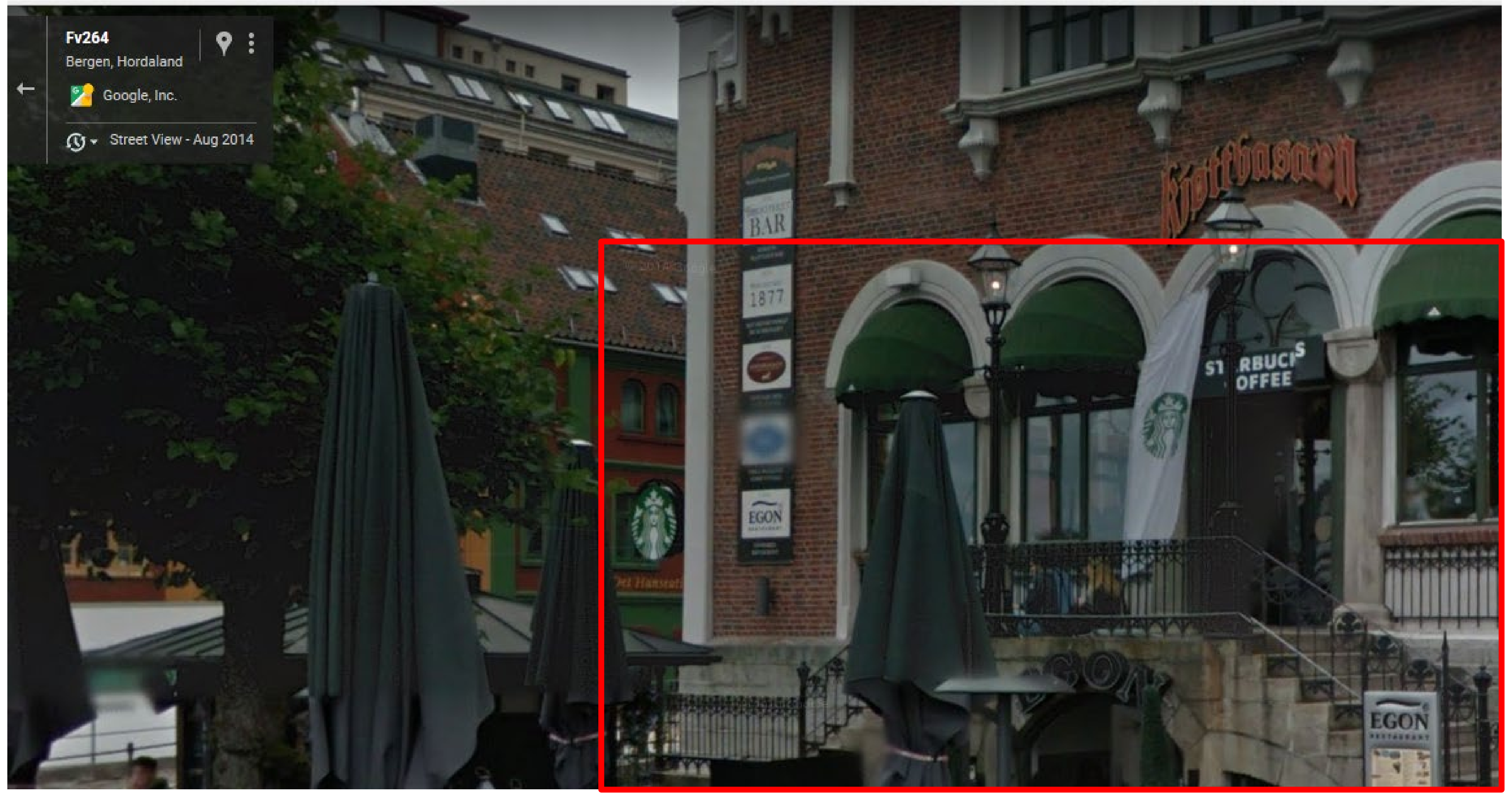
Apple iOS Artifacts



White Balance	Auto white balance
General	
Date and Time	2017:08:25 11:06:39.00
Manufacturer	Apple
Model	iPhone SE
Orientation	right - top
Resolution Unit	Inch
Software	10.3.2
x-Resolution	72.00
YCbCr Positioning	centered
y-Resolution	72.00
GPS	
Altitude	2.43m
Altitude reference	Sea level reference
Bearing of destination	320.77
East or West Longitude	E-East longitude
GPS date	2017:08:25
GPS Img Direction	320.77
GPS Img Direction Reference	T-True direction
GPS time (atomic clock)	09:06:39.00
Latitude	60.00d 23.00m 44.71s
Longitude	5.00d 19.00m 34.85s
North or South Latitude	N-North latitude
Reference for bearing of destination	T-True direction
Speed of GPS receiver	0.17
Speed unit	K-Kilometers per hour


60.395753,5.326347

60°23'44.7"N 5°19'34.9"E
60.395753, 5.326347

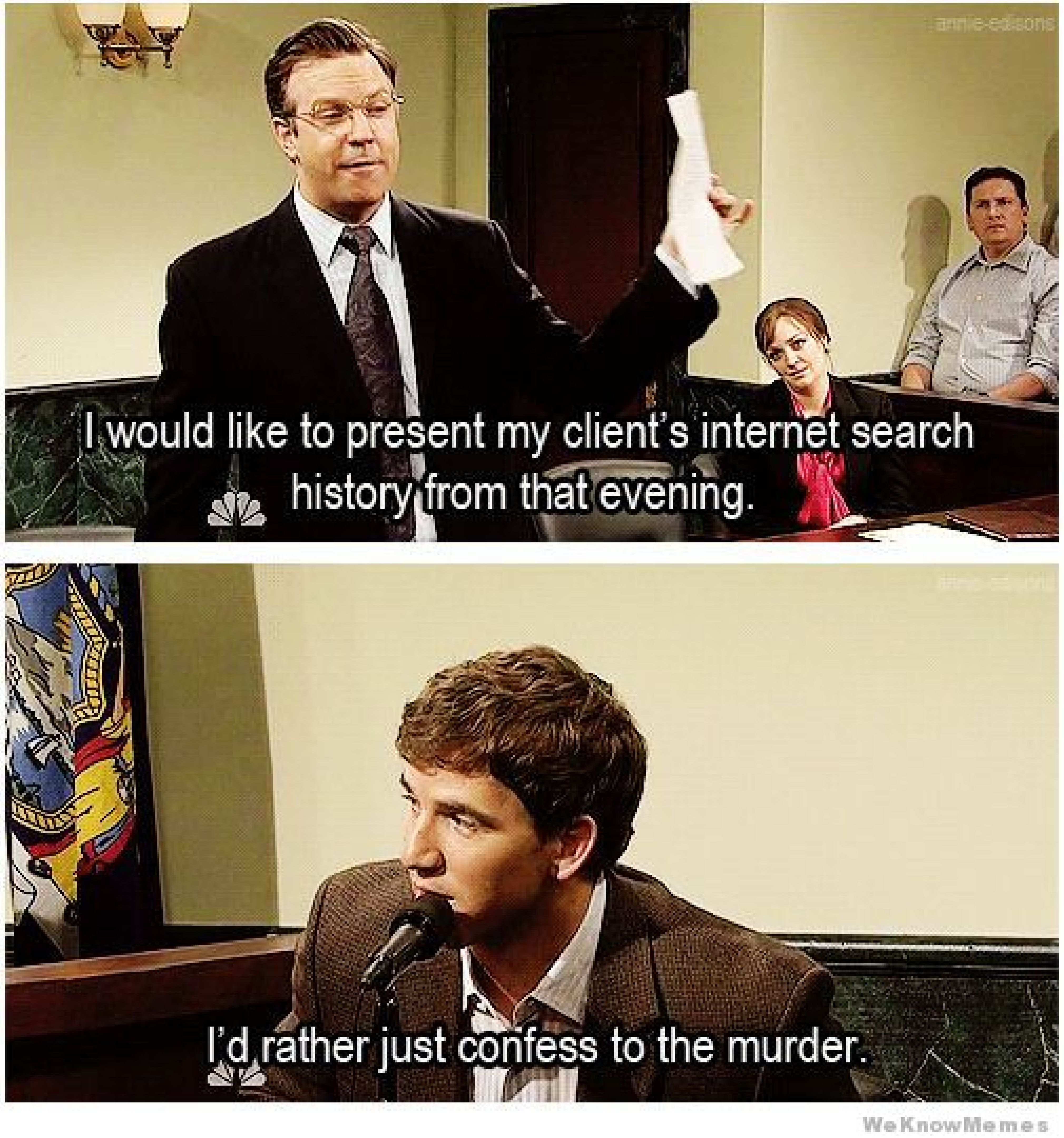


Browser data

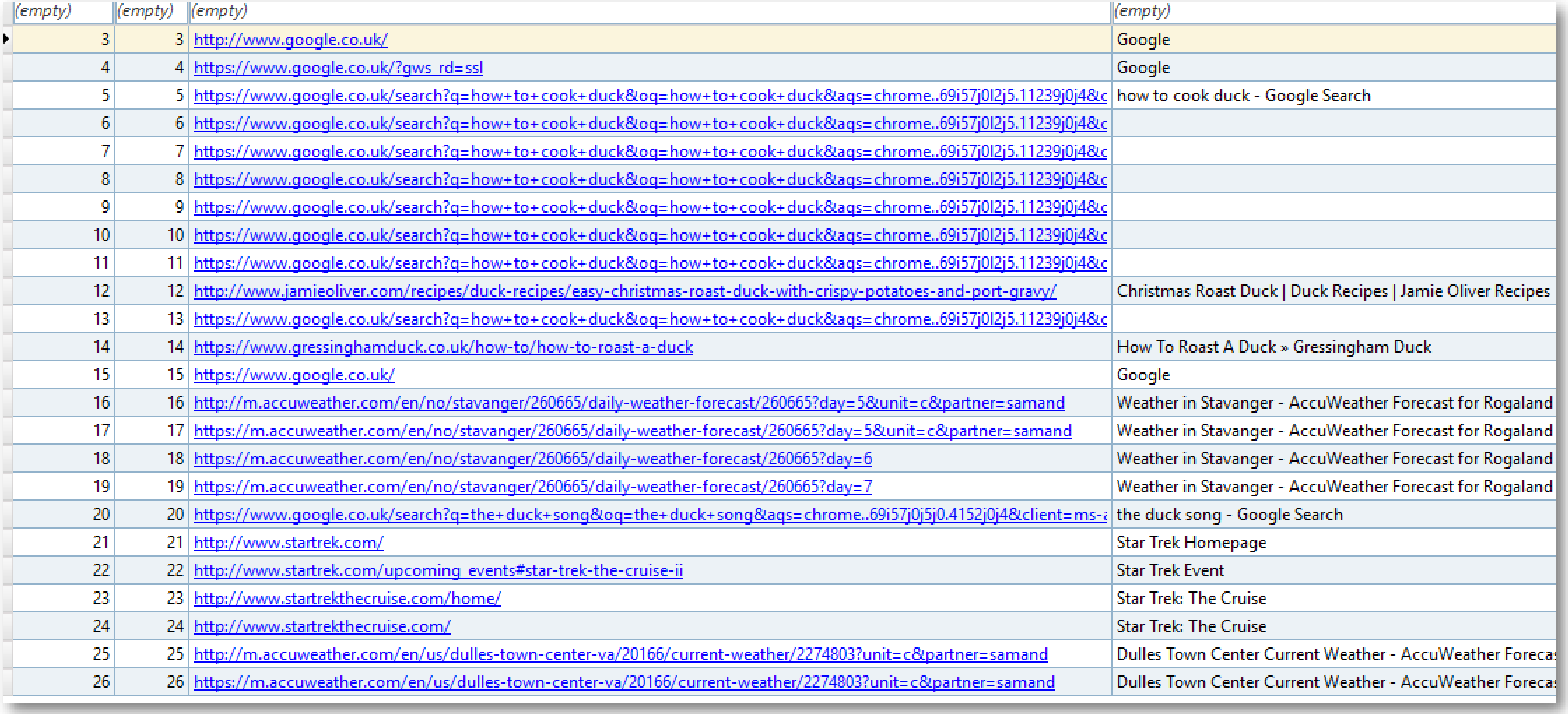
There's a record for that

NeLI
National eDiscovery Leadership Institute

Mobile Device Examination – Web history

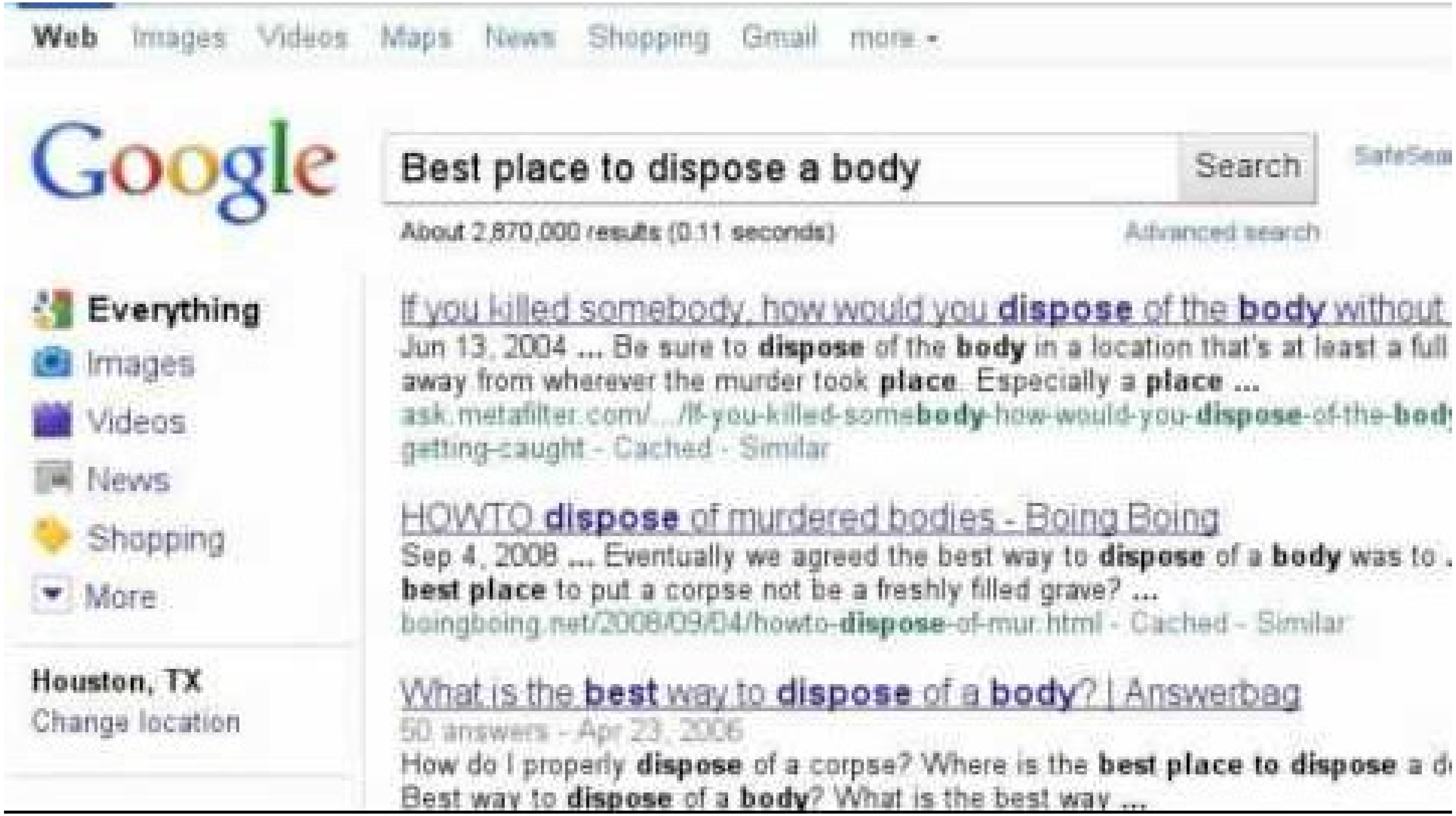

annie-edisons
I would like to present my client's internet search history from that evening.
I'd rather just confess to the murder.
WeKnowMemes

Mobile Device Examination – Web history



(empty)	(empty)	(empty)	(empty)
3	3	http://www.google.co.uk/	Google
4	4	https://www.google.co.uk/?gws_rd=ssl	Google
5	5	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	how to cook duck - Google Search
6	6	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
7	7	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
8	8	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
9	9	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
10	10	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
11	11	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
12	12	http://www.jamieoliver.com/recipes/duck-recipes/easy-christmas-roast-duck-with-crispy-potatoes-and-port-gravy/	Christmas Roast Duck | Duck Recipes | Jamie Oliver Recipes
13	13	https://www.google.co.uk/search?q=how+to+cook+duck&oq=how+to+cook+duck&aqs=chrome..69i57j0l2j5.11239j0j4&c	
14	14	https://www.gressinghamduck.co.uk/how-to/how-to-roast-a-duck	How To Roast A Duck » Gressingham Duck
15	15	https://www.google.co.uk/	Google
16	16	http://m.accuweather.com/en/no/stavanger/260665/daily-weather-forecast/260665?day=5&unit=c&partner=samand	Weather in Stavanger - AccuWeather Forecast for Rogaland
17	17	https://m.accuweather.com/en/no/stavanger/260665/daily-weather-forecast/260665?day=5&unit=c&partner=samand	Weather in Stavanger - AccuWeather Forecast for Rogaland
18	18	https://m.accuweather.com/en/no/stavanger/260665/daily-weather-forecast/260665?day=6	Weather in Stavanger - AccuWeather Forecast for Rogaland
19	19	https://m.accuweather.com/en/no/stavanger/260665/daily-weather-forecast/260665?day=7	Weather in Stavanger - AccuWeather Forecast for Rogaland
20	20	https://www.google.co.uk/search?q=the+duck+song&oq=the+duck+song&aqs=chrome..69i57j0j5j0.4152j0j4&client=ms-	the duck song - Google Search
21	21	http://www.startrek.com/	Star Trek Homepage
22	22	http://www.startrek.com/upcoming_events#star-trek-the-cruise-ii	Star Trek Event
23	23	http://www.startrekthecruise.com/home/	Star Trek: The Cruise
24	24	http://www.startrekthecruise.com/	Star Trek: The Cruise
25	25	http://m.accuweather.com/en/us/dulles-town-center-va/20166/current-weather/2274803?unit=c&partner=samand	Dulles Town Center Current Weather - AccuWeather Forecas
26	26	https://m.accuweather.com/en/us/dulles-town-center-va/20166/current-weather/2274803?unit=c&partner=samand	Dulles Town Center Current Weather - AccuWeather Forecas

Web history example



Best place to dispose a body

About 2,870,000 results (0.11 seconds)

Houston, TX

If you killed somebody, how would you **dispose** of the **body** without

Jun 13, 2004 ... Be sure to **dispose** of the **body** in a location that's at least a full away from wherever the murder took **place**. Especially a **place** ...

ask.metafilter.com/.../If-you-killed-some**body**-how-would-you-**dispose**-of-the-**bod**
getting-caught - Cached - Similar

HOWTO **dispose** of murdered bodies - Boing Boing

Sep 4, 2008 ... Eventually we agreed the best way to **dispose** of a **body** was to
best place to put a corpse not be a freshly filled grave? ...

boingboing.net/2008/09/04/howto-**dispose**-of-mur.html - Cached - Similar

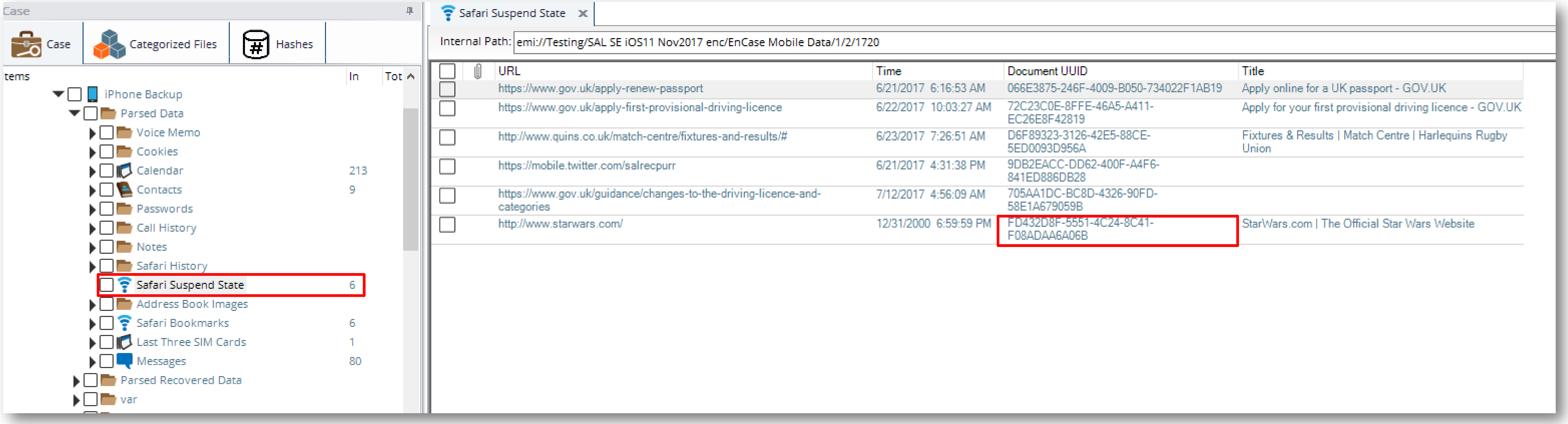
What is the **best** way to **dispose** of a **body**? | Answerbag

50 answers - Apr 23, 2006

How do I properly **dispose** of a corpse? Where is the **best place to dispose** a d
Best way to **dispose** of a **body**? What is the best way ...

Protip: “Private” or “Incognito” browsing won’t save you

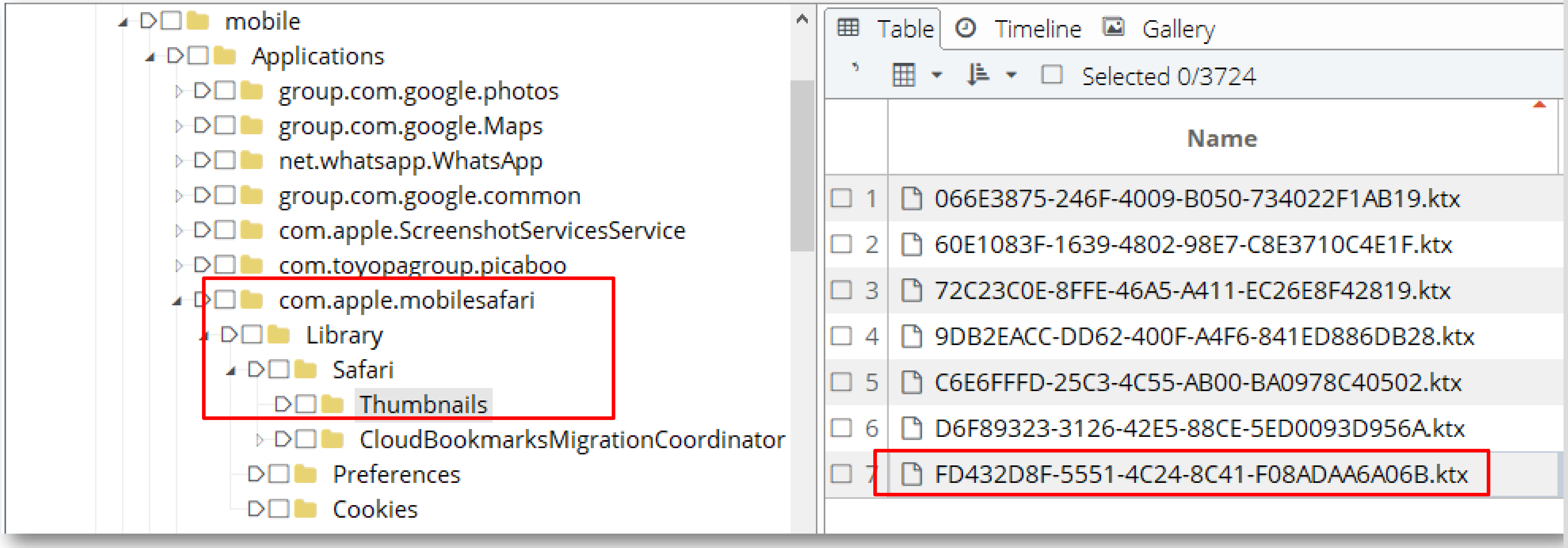
- Safari Suspend State
  - BrowserState.db indicates ‘private_browsing’
  - Document UUID – name of cached image, shows browser tab



Internal Path: emi://Testing/SAL SE iOS11 Nov2017 enc/EnCase Mobile Data/1/2/1720

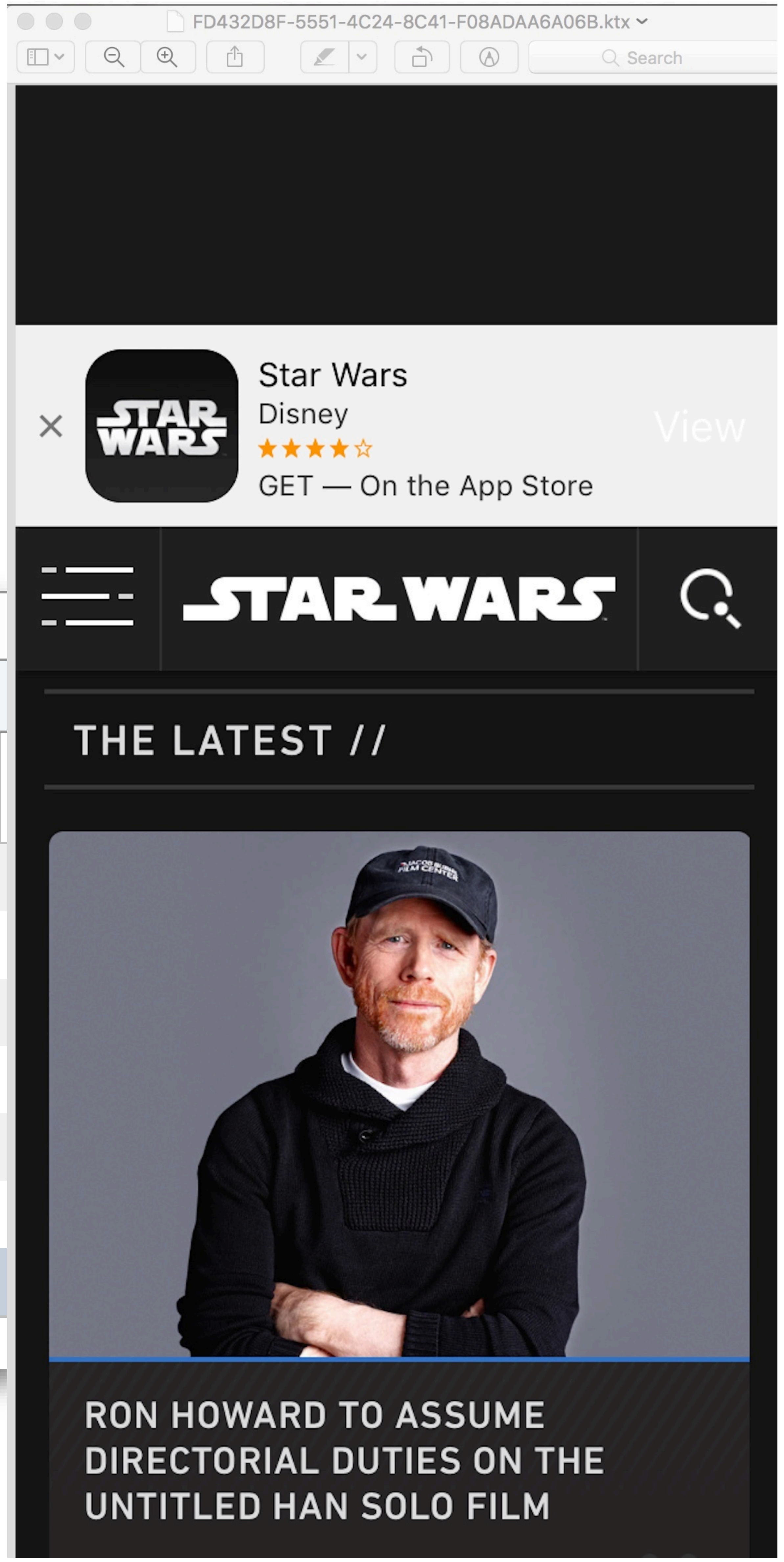
☐	URL	Time	Document UUID	Title
☐	https://www.gov.uk/apply-renew-passport	6/21/2017 6:16:53 AM	066E3875-246F-4009-B050-734022F1AB19	Apply online for a UK passport - GOV.UK
☐	https://www.gov.uk/apply-first-provisional-driving-licence	6/22/2017 10:03:27 AM	72C23C0E-8FFE-46A5-A411-EC26E8F42819	Apply for your first provisional driving licence - GOV.UK
☐	http://www.quins.co.uk/match-centre/fixtures-and-results/#	6/23/2017 7:26:51 AM	D6F89323-3126-42E5-88CE-5ED0093D956A	Fixtures & Results | Match Centre | Harlequins Rugby Union
☐	https://mobile.twitter.com/salrecpurr	6/21/2017 4:31:38 PM	9DB2EACC-DD62-400F-A4F6-841ED886DB28	
☐	https://www.gov.uk/guidance/changes-to-the-driving-licence-and-categories	7/12/2017 4:56:09 AM	705AA1DC-BC8D-4326-90FD-58E1A679059B	
☐	http://www.starwars.com/	12/31/2000 6:59:59 PM	FD432D8F-5551-4C24-8C41-F08ADAA6A06B	StarWars.com | The Official Star Wars Website

Mobile Device Examination – iOS Web history



- mobile
  - Applications
    - group.com.google.photos
    - group.com.google.Maps
    - net.whatsapp.WhatsApp
    - group.com.google.common
    - com.apple.ScreenshotServicesService
    - com.toyopagroup.picaboo
    - com.apple.mobilesafari
      - Library
        - Safari
          - Thumbnails
        - CloudBookmarksMigrationCoordinator
        - Preferences
        - Cookies

	Name
☐ 1	066E3875-246F-4009-B050-734022F1AB19.ktx
☐ 2	60E1083F-1639-4802-98E7-C8E3710C4E1F.ktx
☐ 3	72C23C0E-8FFE-46A5-A411-EC26E8F42819.ktx
☐ 4	9DB2EACC-DD62-400F-A4F6-841ED886DB28.ktx
☐ 5	C6E6FFFD-25C3-4C55-AB00-BA0978C40502.ktx
☐ 6	D6F89323-3126-42E5-8BCE-5ED0093D956A.ktx
☐ 7	FD432D8F-5551-4C24-8C41-F08ADAA6A06B.ktx

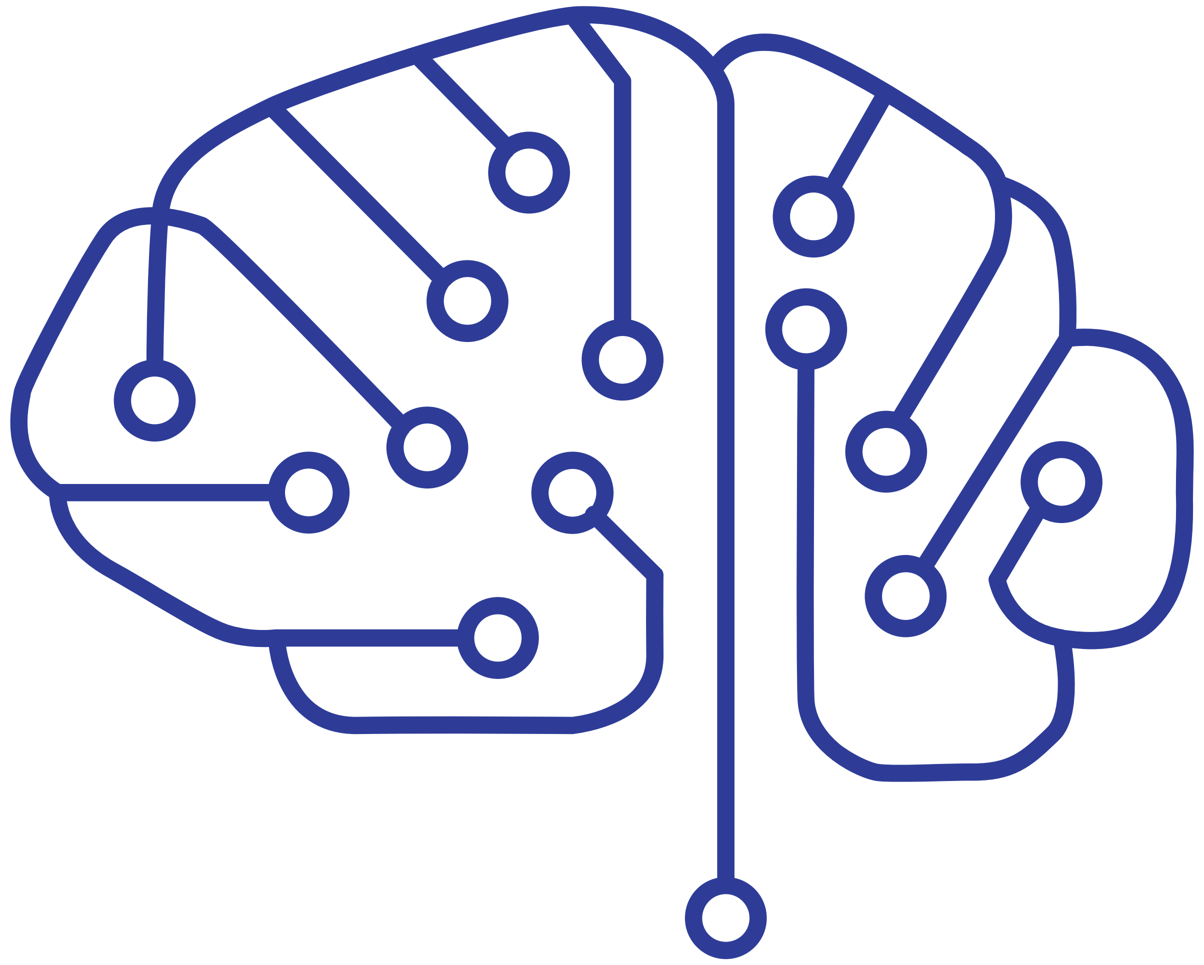

FD432D8F-5551-4C24-8C41-F08ADAA6A06B.ktx
Search
Star Wars
Disney
★★★★☆
GET — On the App Store
View
STAR WARS
THE LATEST //
RON HOWARD TO ASSUME DIRECTORIAL DUTIES ON THE UNTITLED HAN SOLO FILM

Lessons about smartphone investigations

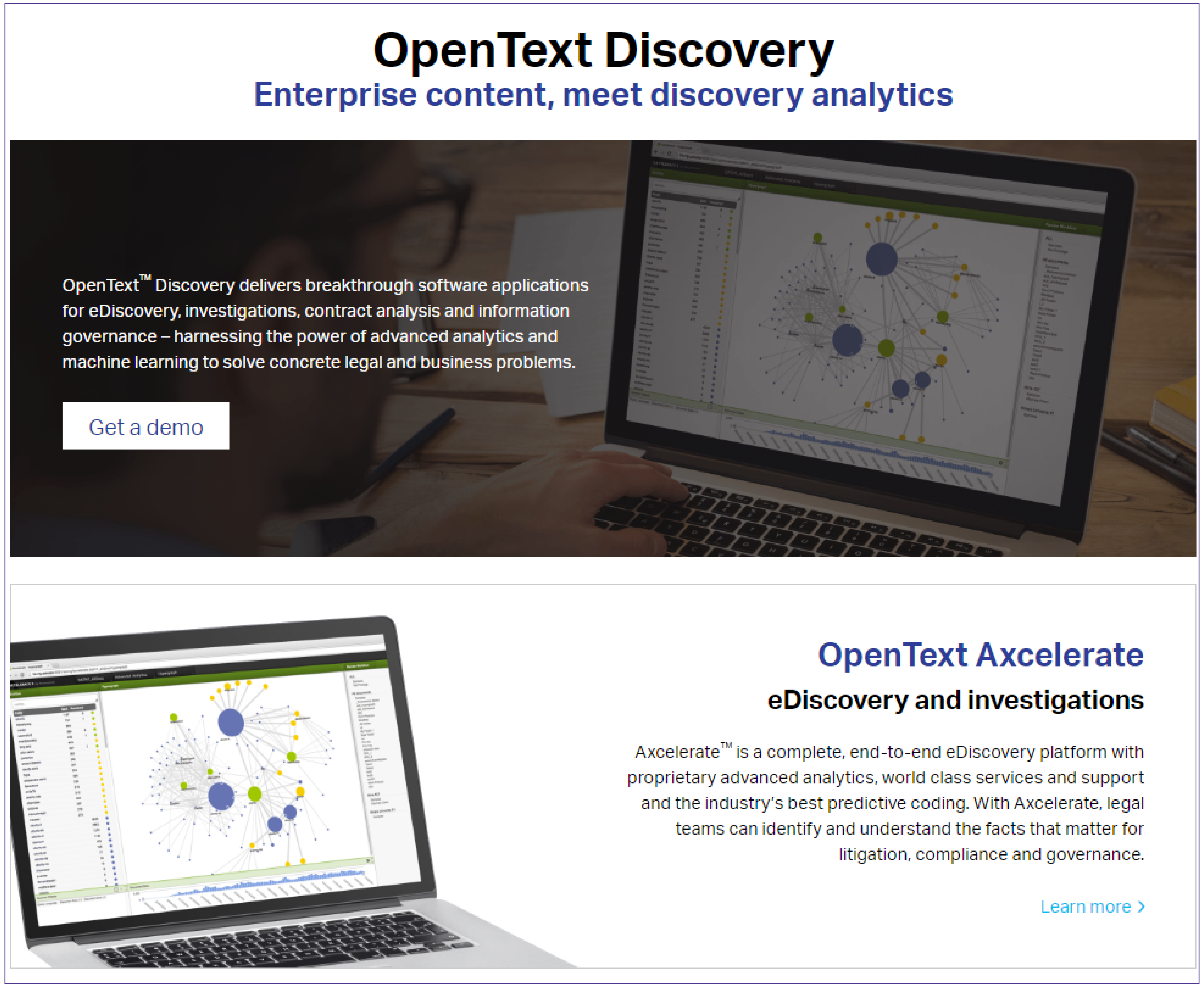
Lightning round

Key takeaways:

- Prepare lists ahead of time
- Anticipate physical device issues
- Collect and preserve early
- Conduct multifaceted analysis
- Learn throughout the investigation
- Update those lists
- Document the workflows



Learn more about OpenText Discovery



OpenText Discovery

Enterprise content, meet discovery analytics

OpenText™ Discovery delivers breakthrough software applications for eDiscovery, investigations, contract analysis and information governance – harnessing the power of advanced analytics and machine learning to solve concrete legal and business problems.

OpenText Axcelerate

eDiscovery and investigations

Axcelerate™ is a complete, end-to-end eDiscovery platform with proprietary advanced analytics, world class services and support and the industry's best predictive coding. With Axcelerate, legal teams can identify and understand the facts that matter for litigation, compliance and governance.

opentext™ | EnCase™

The gold standard in forensic-grade e-discovery collection & preservation

+

opentext™ | Axcelerate™

+

opentext™

+ Catalyst

Award-winning eDiscovery review & analysis with integrated AI & analytics

=

Unparalleled coverage of the EDRM

For more info & a free demo:
opentext.com/campaigns/ediscovery

opentext™

Thank you!

twitter.com/opentext

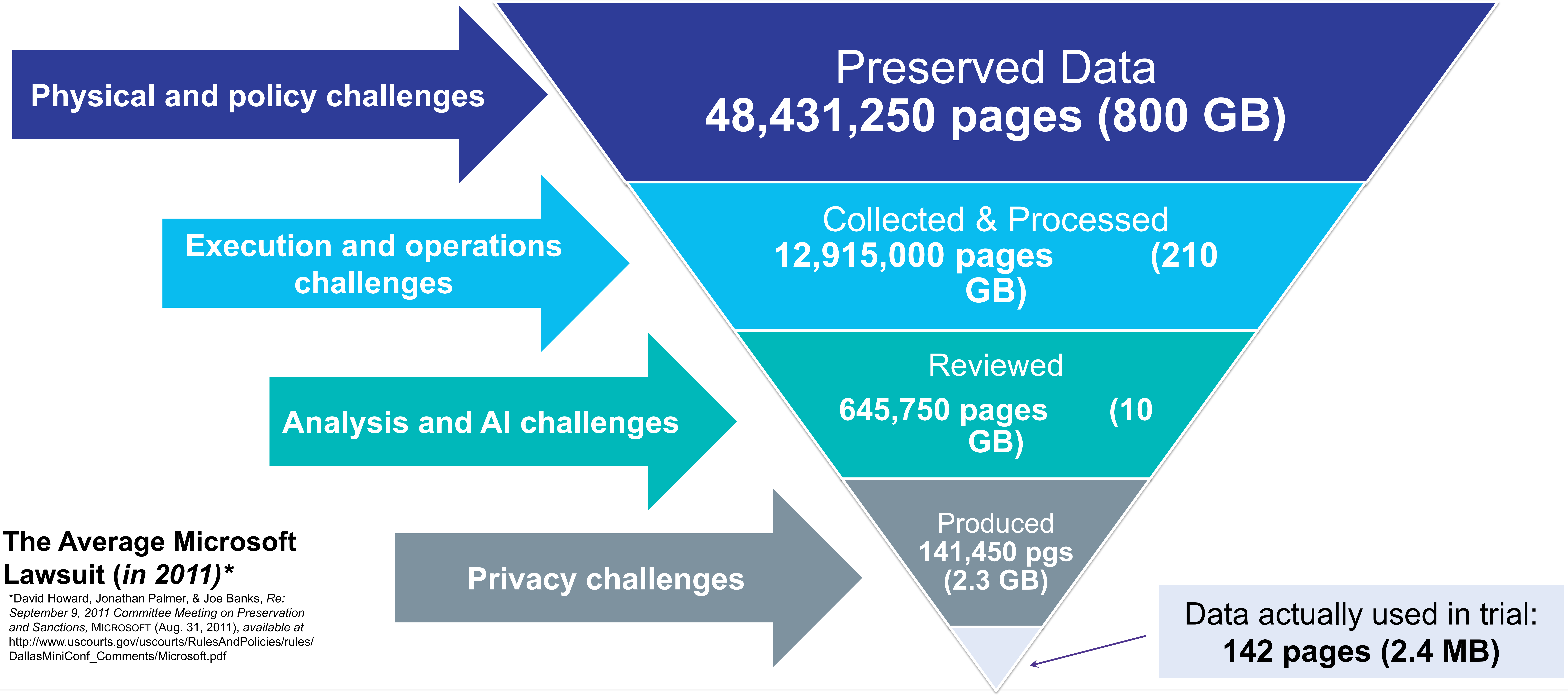
linkedin.com/company/opentext

opentext.com

Appendix content

Extra slides

What’s needed for Discovery



Physical and policy challenges

Execution and operations challenges

Analysis and AI challenges

Privacy challenges

Preserved Data
48,431,250 pages (800 GB)

Collected & Processed
12,915,000 pages (210 GB)

Reviewed
645,750 pages (10 GB)

Produced
141,450 pgs (2.3 GB)

Data actually used in trial:
142 pages (2.4 MB)

The Average Microsoft Lawsuit (*in 2011*)*

*David Howard, Jonathan Palmer, & Joe Banks, *Re: September 9, 2011 Committee Meeting on Preservation and Sanctions*, MICROSOFT (Aug. 31, 2011), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/DallasMiniConf_Comments/Microsoft.pdf

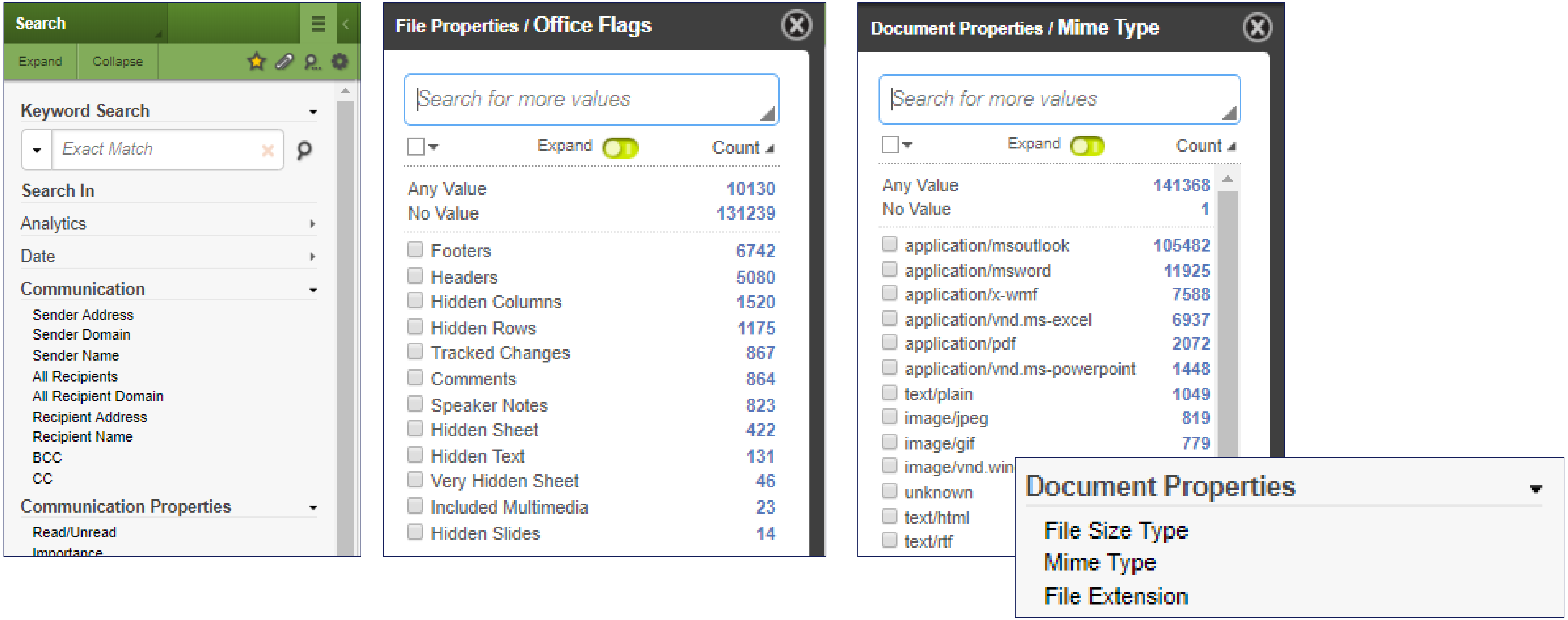
Litigation

- Reviewing for production
- Analyze received productions
- Early fact finding

Investigations

- Internal compliance
- Regulatory response
- Due diligence
- Data security breach response

File and metadata analysis



File Properties / Office Flags

☐	Expand	Count
Any Value		10130
No Value		131239
☐ Footers		6742
☐ Headers		5080
☐ Hidden Columns		1520
☐ Hidden Rows		1175
☐ Tracked Changes		867
☐ Comments		864
☐ Speaker Notes		823
☐ Hidden Sheet		422
☐ Hidden Text		131
☐ Very Hidden Sheet		46
☐ Included Multimedia		23
☐ Hidden Slides		14

Document Properties / Mime Type

☐	Expand	Count
Any Value		141368
No Value		1
☐ application/msoutlook		105482
☐ application/msword		11925
☐ application/x-wmf		7588
☐ application/vnd.ms-excel		6937
☐ application/pdf		2072
☐ application/vnd.ms-powerpoint		1448
☐ text/plain		1049
☐ image/jpeg		819
☐ image/gif		779
☐ image/vnd.win		
☐ unknown		
☐ text/html		
☐ text/rtf		