



epiq agility

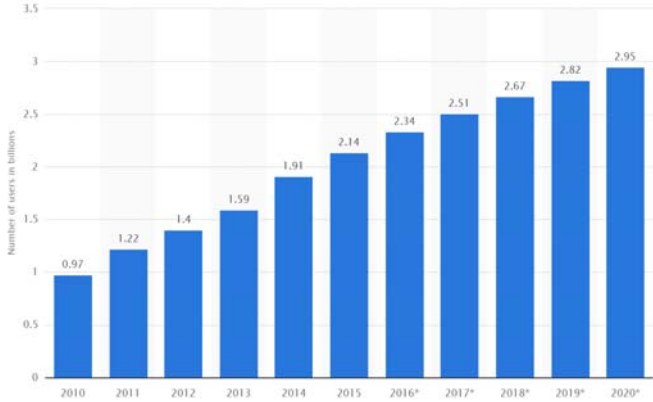
Social Media and Mobile Device eDiscovery
 East Valley Bar Association
 April 17, 2020

Matthew F Porter, Esq. – Solution Architect

1 People. Partnership. Performance. epiqglobal.com


Social Media Growth

- Hyper growth of information disseminated through social media platforms such as Facebook, LinkedIn, Twitter, Slack as evidence in civil and criminal proceeding
- Social Media data is:
 - Easily altered/spoiled
 - Hard to erase completely
 - Ever expanding
 - Challenging to preserve, collect and authenticate



Year	Number of users in billions
2010	0.97
2011	1.22
2012	1.4
2013	1.59
2014	1.91
2015	2.14
2016*	2.34
2017*	2.51
2018*	2.67
2019*	2.82
2020*	2.95

2 People. Partnership. Performance. epiqglobal.com



Preservation Issues

- Data is ephemeral by design
- Retention Policies
- Timing
- Technological Limitations
- Cost Restriction



3

People. Partnership. Performance. epiqglobal.com

Collection/Authentication

- Collection
 - Social Media Streams
 - Linked Content
 - Websites
 - Webmail
 - Messaging
 - Continuous Monitoring
- Authentication
 - Hash based logging
 - Direct Access through the sites API



4

People. Partnership. Performance. epiqglobal.com

Changes to Social Media

- A number of significant changes to Social Media have occurred recently.
- These changes have made the collection and preservation of Social Media much more challenging because many of the common collection approaches are no longer usable.
- We will highlight these changes, discuss the limitations, and provide insight into alternative collection techniques.

5

People. Partnership. Performance. epiqglobal.com

Facebook Limitations

- Facebook restricts APIs, and axes old Instagram platform amidst scandals.
 - “[Facebook](#) is entering a tough transition period where it won’t take chances around data privacy in the wake of the Cambridge Analytica fiasco, CTO Mike Schroepfer tells TechCrunch. That’s why it’s moving up the shut down of part of the Instagram API. It’s [significantly limiting data available](#) from or requiring approval for access to Facebook’s Events, Groups, and Pages APIs plus Facebook Login.”
- <https://techcrunch.com/2018/04/04/facebook-instagram-api-shut-down/>

6

People. Partnership. Performance. epiqglobal.com

Instagram Limitations

- ["Instagram"](#) will immediately shut down part of its old platform API that was scheduled for deprecation on July 31st. [TechCrunch first reported that developers' Instagram apps were breaking](#) over the weekend due to a sudden reduction in the API call limit. Instagram refused to comment, leading to developer frustration as their apps that analyze people's followers and help them grow their audiences stopped working."
- <https://techcrunch.com/2018/04/04/facebook-instagram-api-shut-down/>

7

People. Partnership. Performance. epiqglobal.com

Twitter Limitations

- "[The Twitter API] can only return up to 3,200 of the user's most recent Tweets."
- <https://developer.twitter.com/en/docs/tweets/timelines/api-reference/get-statuses-user-timeline.html>

8

People. Partnership. Performance. epiqglobal.com

3rd Party Messaging Applications

- Many third-party messaging applications only store the message content on the mobile device. Some popular examples:
 - Apple iMessages
 - WhatsApp
 - WeChat
 - Viber
- For Android devices, one must collect a physical image to collect and access the 3rd Party messaging data. In many cases, this is not possible due to Android security features.

9

People. Partnership. Performance. epiqglobal.com

web crawl approach

- Tools
 - HTTrack
 - Portable Offline Browser
 - Adobe Acrobat
- Most of the commercially available web page and website collection tools have limited success in collecting the more dynamic HTML5 web content. For example:
 - Expandable content
 - Roll over image
 - Dynamic content like videos and animation
- Other Crawling Third-party Tools/Services



10

People. Partnership. Performance. epiqglobal.com

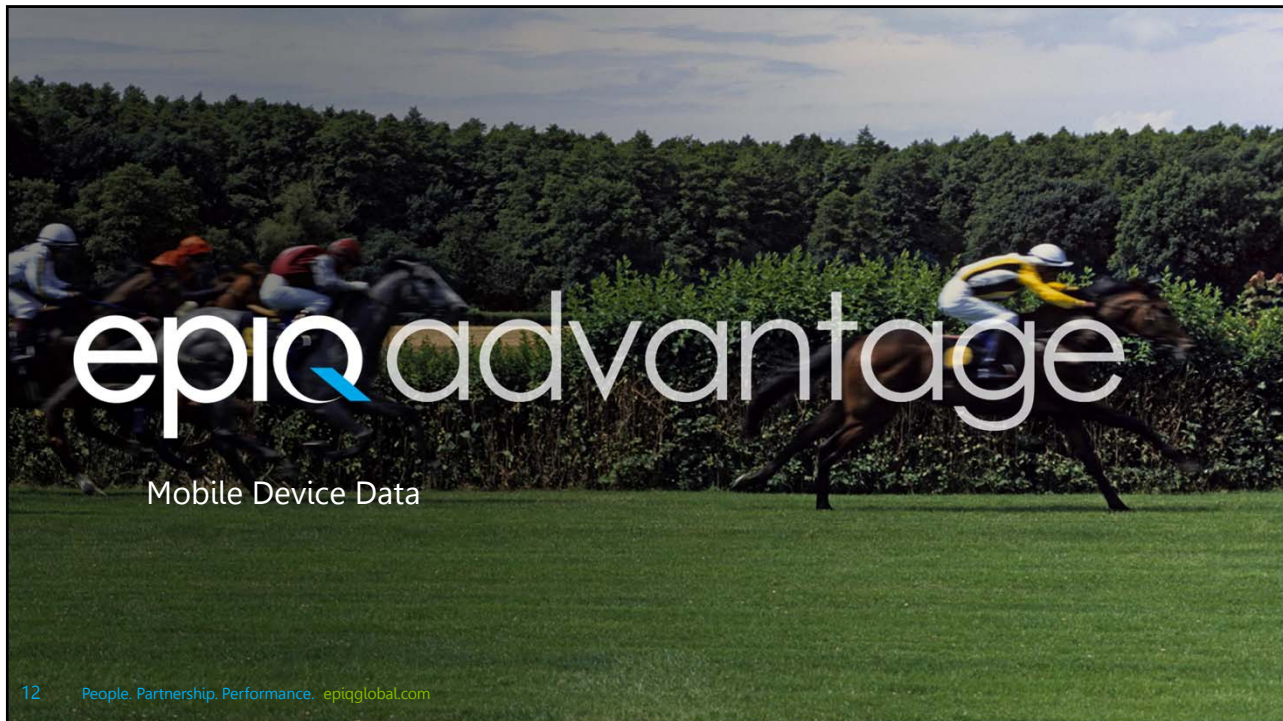
collection capabilities



- Collection Capabilities
- With username and password
 - All activity Sent and Received, including private messages
- Without username or password
 - All publicly available information



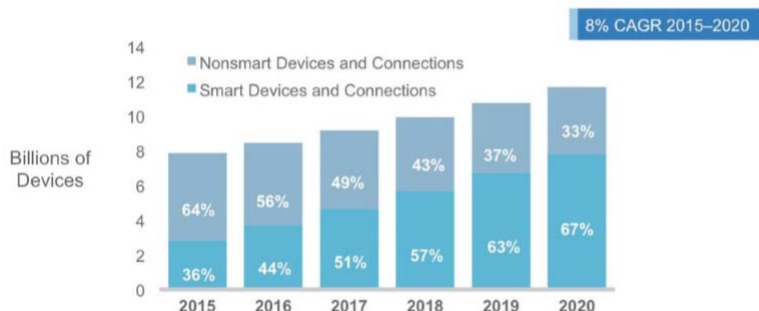
- Export Capabilities
- Paginated Searchable PDF
- Load Files
- Native Files (Videos and Images)



Mobile Devices – the primary internet tool

- It is estimated more than 5-billion people have a mobile device and over half these devices are smart phones.

Figure 6. Global Growth of Smart Mobile Devices and Connections



Percentages refer to device and connections share.
Source: Cisco VNI Mobile, 2016

https://www.cisco.com/c/dam/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf

13

People. Partnership. Performance. epiqglobal.com



Forensic and eDiscovery Challenges

- Mobile device data is:
 - Stored and managed differently
 - Widely variable
 - Third party applications
 - Rapidly changing technologies
 - Easily altered / spoliated
 - Devices designed to be always connected
 - Constantly updating when connected



14

People. Partnership. Performance. epiqglobal.com



Forensic and eDiscovery Challenges

- Ownership, Control, and Security:
 - Who owns the device? Who owns the data?
 - BYOD
 - Company Ownership
 - MDM
 - Encryption and Security work against preservation and collection



15

People. Partnership. Performance. epiqglobal.com

• Mobile Collections



Mobile Device Preservation and Collection

- Mobile device must be isolated from cell towers and Wi-Fi (radio frequencies – RF) to prevent changes/destruction
- Airplane mode is a common method for RF avoidance
 - ***But use caution***
- Special faraday bags and boxes can forensically maintain RF isolation



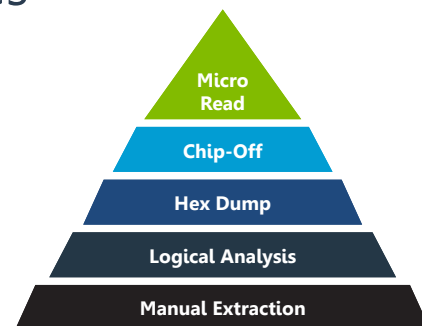
epiq

17

People. Partnership. Performance. epiqglobal.com

Mobile Device Collection Types

- Manual capture
 - Scroll & screenshot
 - Used only when can't use forensic tools
- Logical acquisition
 - Most common – captures user data
 - Limits on data, depending on device
 - i.e. no e-mail on iOS devices
- Hex Dump
 - Full physical image of device's memory.
 - Not well supported on most devices
- Chip-Off/ J-Tag /Micro Read
 - Damaged or locked devices
 - No commercial tools exist for Micro Read



Cell phone tool leveling pyramid (Sam Brothers, 2009)

epiq

Mobile Device Collection Tools

- [Tools currently available at Epiq:](#)

- Cellebrite
- XRY
- Blacklight*
- Axiom*
- Elcomsoft**
- Oxygen Forensics*



Across all products
support for over
10,000 mobile
devices

- *Limited to iOS and certain logical Android collections
- **Limited to iOS and cloud-based iOS and Google collections

19

People. Partnership. Performance. epiqglobal.com



Cellebrite Collection Method Overview



- Industry standard in mobile collections, application decoding, forensic analysis, and advanced reporting.
- Apple iOS collections
 - Advanced Logical Method 1 & 2
- Android
 - Physical (if supported)
 - Logical
 - File System (typically Android Backup)




20

People. Partnership. Performance. epiqglobal.com



Collection Time

- Phone sizes have increased 10x over the last five years with volume of text and chat messages growing at a similar rate. With the growth in device capacity, the time to collect a large phone is comparable to imaging a workstation at 3-5 hours.

iPhone XS Max	iPhone 7	iPhone 6
		
Capacity*		
64GB	32GB	16GB
256GB	128GB	32GB
512GB		64GB

21

People. Partnership. Performance. epiqglobal.com

Encryption

- Becoming more popular on mobile devices
- Hardware/File Based
 - Blackberry, Android, and iOS
- Software
 - iTunes Backup Encryption
- Application Level
 - Messaging Apps: Signal, Wickr, WhatsApp



22

People. Partnership. Performance. epiqglobal.com

Apple iOS collection issues



- The new iPhones support 512 GB of storage making the collection times longer than most custodian's will want to be without their device.
- iTunes Backup Encryption
- Recent changes to the iCloud security protocols preventing direct downloads of iOS 11 or newer backups
- MDM client software restricting what applications can be backed up.

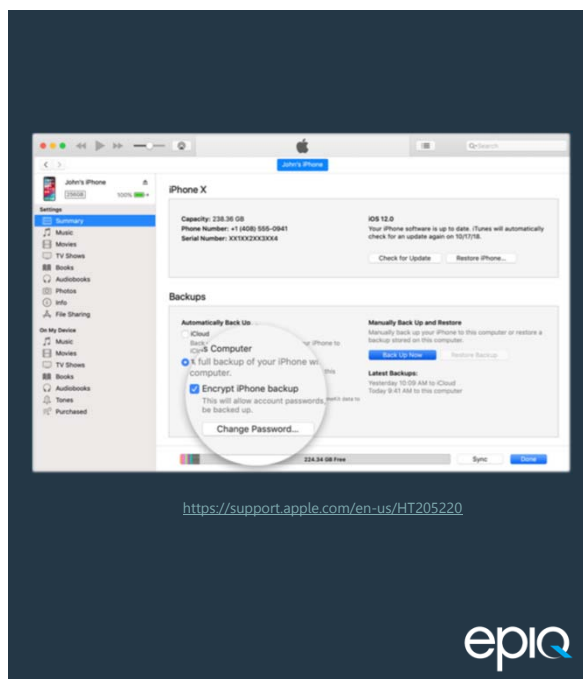
23

Peop



iTunes Backup Encryption

- One-time password
- It can be user initiated or implemented via a MDM policy.
- iTunes (installed version) does not support a forgotten password feature for the backup encryption.
- The device can be collected, however we need the password to decrypt the image.
- Password removal – possible on later IOS versions, but resets many other phone settings. Last resort.



Apple iCloud collection issues



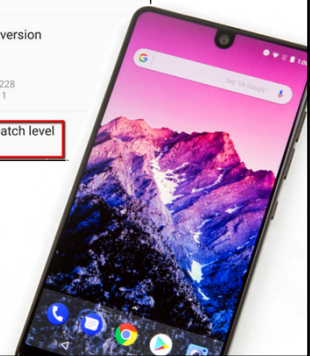
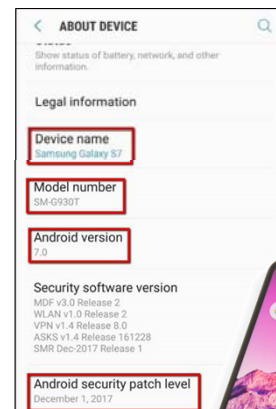
- Apple's iCloud infrastructure underwent massive changes in 2018.
- The iCloud changes significantly affected the ability for the entire industry to collect iCloud backups starting late September 2018 when the backup was iOS 11 or 12, and 2FA was enabled.
- Workaround: restore backup to another device, and collect from that device.
 - Not a true forensic collection.

25

People. Partnership. Performance. epiqglobal.com

Android collection issues

- Strong encryption and hardware security measures on newer devices.
- Android Security Patch Updates
- In many cases, you can only collect a logical extraction because of the Android security patch updates. In order to collect third-party apps or deleted text messages, you need a physical extraction.
- Advanced extraction methods (Custom Boot Loaders, JTAG, Chip Off, etc) are available through Epiq and trusted third party vendors, but not always supported on the newest Android devices. These methods may render the device permanently unusable.



BYOD

- Increasing popularity
- Personal device
- Mix of personal and business data
- Company policies and practices?
 - Use of device and data?
 - Preservation?
 - Security?
 - MDM solution?



epiq

27

People. Partnership. Performance. epiqglobal.com

BYOD

- How do you address the privacy concerns to limit what is reviewed?
- How do you address the intermingled data issues?
 - Can you selectively export the requested conversations?
- Collection approach:
 - Collect all data, 2 copies
 - Keep encrypted full copy for preservation
 - Counsel, with forensic consultant, cull and analyze report to hand over only responsive data

epiq

28

People. Partnership. Performance. epiqglobal.com

MDM

• Mobile Device Management Software

- Used by organizations to control device use and security
 - Allows security policy to be managed centrally
 - Allows remote wipe
 - **May inhibit the ability to collect data**

- AirWatch
- MaaS360
- MobiControl
- XenMobile
- Microsoft Intune



29

People. Partnership. Performance. epiqglobal.com

Recovery of deleted messages

- Deleted SMS/MMS/Third Party Chats can be recovered in some instances
- With iOS 11 and the new security feature in Android device, it is becoming less common to recover significant volumes of deleted text messages.



30

People. Partnership. Performance. epiqglobal.com

• Mobile Review and Production



Mobile Reporting & Review Options

- Cellebrite Excel Report contains:
 - Contacts,
 - Call logs,
 - Calendars
 - Internet history
 - Messaging
 - Recorded voicemails
 - User location information
 - Documents
 - Media (pictures & video)
 - Notes
 - And more...

	A	B	C
1		Summary (9)	
2		Name	Value
3		Device	iPhone 6
4		UFED Physical Analyzer version	6.0.0.126
5		Report creation time	3/21/2017 12:12:48 PM -04:00
6		Time zone settings (UTC)	(UTC-05:00) New York (America)
7		Case number	Sample Report
8		Case name	Sample Project
9		Examiner name	Epiq Systems
10		Department	Epiq Systems
11		Location	Washington, D.C.
12		Logical	
13		Extraction start date/time	3/21/2017 11:04:32 AM(UTC-4)
14		Extraction end date/time	3/21/2017 11:05:27 AM(UTC-4)
15		Selected Manufacturer	Apple
16		Selected Device Name	iPhone 6
17		Connection Type	Cable No. 210
18		Is encrypted	Encrypted by UFED Physical/Logical Analyzer during the extraction process
19		Backup password	1234
20		Extraction Type	Logical [Method1]
21		Extraction ID	02e555ad-e88e-49b-3a16
22			
23			
24			
25			
26			

Text message review in Excel

Pro's

- Easy to create
- Simple to review and filter

Con's

- Does not support complex searches and tagging
- Cannot be produced in a granular format
- Cannot easily be redacted
- Does not keep the parent child relationship if processed

SMS Messages (47)										
#	Dirty	Date	Time	Send Date	Read Time	Folder	Status	Message	Deleted	
1	To: +13023589760	3/21/2017	3/21/2017 11:03:38 AM(UTC-4)			Sent	Sent	I think you have the wrong number		
2	From: +16176525950	3/21/2017	3/21/2017 10:34:04 AM(UTC-4)	3/21/2017	3/21/2017 11:03:42 AM(UTC-4)	Inbox	Read	Your Signal verification code: 904-755		
3	From: +13023589760	2/10/2017	2/10/2017 11:46:54 AM(UTC-5)	3/21/2017	3/21/2017 11:03:18 AM(UTC-4)	Inbox	Read	Or tap: signal://verify/904-755 Shane - Given the length of the last and your email indicating that you needed to get home to watch a sick child I wanted to see if this is still a good time to talk. Thanks, AIG		
4	To: +19133076961 Mac Braebum	12/27/2016	12/27/2016 10:38:23 AM(UTC-5)	12/27/2016	12/27/2016 10:47:41 AM(UTC-5)	Inbox	Read	Your iCloud Keychain verification code is: 126715		
5	From: 50472	11/18/2016	11/18/2016 9:58:58 AM(UTC-5)			Sent	Sent	I'm wood_ka7e8eogx712 on WeChat, the best texting and chat app.		
6	To: +14802131466 Daisy Cutter	11/18/2016	11/18/2016 9:57:20 AM(UTC-5)	11/18/2016	11/18/2016 9:57:26 AM(UTC-5)	Inbox	Read	WeChat verification code (8855) is only used to change links		

33

People. Partnership. Performance. epiqglobal.com



EPIQ's Mobile Chat Analyzer

- Developed in-house to address the complexities of mobile data review.
 - Creates a granular records for each item that can be searched, reviewed, and produced.
 - Creates a native image for each record and extracts the searchable text.
 - Threads conversations
 - Retains the parent child relationship

#	Doc ID	Family ID	CEL - Chat Thread ID	CEL - Body	CEL - Froms	CEL - DateTime Mess...	CEL - Participants	CEL - Source
1	zm000001	zm000001	74380144-80a4-4090-aa1e-678a8983367_1	Daisy Cutter just added you to his/her contacts. Hit send a message to his/her now!		11/19/2016 9:59 AM	wsid_ka7e8eogx712 Mac (owner) wsid_slp9cndpgrC2 Daisy Cutter	WeChat wsid_ka7e8eogx712
2	zm000002	zm000002	74380144-80a4-4090-aa1e-678a8983367_1	You have added Daisy Cutter as your WeChat contact. Start chatting!		11/19/2016 9:59 AM	wsid_ka7e8eogx712 Mac (owner) wsid_slp9cndpgrC2 Daisy Cutter	WeChat wsid_ka7e8eogx712
3	zm000003	zm000003	74380144-80a4-4090-aa1e-678a8983367_1	Hey	wsid_slp9cndpgrC2	11/19/2016 9:59 AM	wsid_ka7e8eogx712 Mac (owner) wsid_slp9cndpgrC2 Daisy Cutter	WeChat wsid_ka7e8eogx712
4	zm000004	zm000004	74380144-80a4-4090-aa1e-678a8983367_1	You got WeChat?	wsid_ka7e8eogx712 Mac	11/19/2016 10:00 AM	wsid_ka7e8eogx712 Mac (owner) wsid_slp9cndpgrC2 Daisy Cutter	WeChat wsid_ka7e8eogx712
5	zm000005	zm000005	74380144-80a4-4090-aa1e-678a8983367_1	Yeah pretty cool. What are you up to?	wsid_slp9cndpgrC2 Daisy Cutter	11/19/2016 10:00 AM	wsid_ka7e8eogx712 Mac (owner) wsid_slp9cndpgrC2 Daisy Cutter	WeChat wsid_ka7e8eogx712

34

People. Partnership. Performance. epiqglobal.com



New DOJ Text Message Specifications

TXT-PARTICIPANTS	List of participant names and/or telephone numbers.
TXT-BODY	Body of text messages, notes, chats, or calendar items. Do not populate for emails.
TXT-STATUS	Indicates whether text was Sent or Read on the device.
TXT-THREAD-GROUP	Populate with the DOCID of the first text in the chat conversation to allow the entire chat conversation to be grouped as a family. (Sort each device by Chat Number and then by Row Number to assign TXT-THREAD-GROUP identifier.) This is NOT the BEGATTACH field or Relativity Group Identifier.
TXT-SMSC	Short Message Service Center (handles SMS text messages on behalf of phone service provider)
TXT-STARREDMESSAGE	Notes whether the message was flagged.
TXT-DELETED	Indicates whether a chat, instant message, or file was deleted from the mobile device and recovered by Cellebrite.
TXT-READDATE	Date and time the chat, text message, or instant message was opened to read. Format: MM/DD/YYYY HH:MM:SS (Use 24-hour times, e.g., 13:32:00 for 1:32 pm); AM, PM, time zone, or day of the week indicators cannot be included.
TXT-TIMESTAMP	Timestamp of item. Equivalent to DateReceived for incoming items or to DateSent for outgoing items. In MM/DD/YYYY HH:MM:SS in 24-hour format that does not include AM, PM, time zone, or day of the week indicators.
TXT-LOCATION	GPS information associated with chats, text messages, or instant messages.
TXT-MESSAGENUMBER	Similar to RowNumber. Individual identifier for message.
TXT-CHATNUMBER	Chat number, identifies chat groups.
TXT-ROWNUMBER	Row number.

35

People. Partnership. Performance. epiqglobal.com

Questions



36

People. Partnership. Performance. epiqglobal.com