

Internet of Things Forensics

Jonathan Rajewski @jtrajewski



Digital Forensic Examiner - Vermont Internet Crimes Against Children Task Force









Leahy Center Research Assistants

Thank you!

Joe Diorio Justin Waite Kayla Williford Mary Braden Murphy Michael Cook Mitch Green Zack Smith Tyler Wright





Leahy Center for Digital Investigation

How many of you have an IOT device in your home?





Leahy Center for Digital Investigation

Alexa, can you help with this murder case?

By Eliott C. McLaughlin and Keith Allen, CNN Updated 8:48 PM ET, Wed December 28, 2016

Another smart device, Bates' water heater, points to an exorbitant amount of water being used in the early-morning hours, in what investigators believe was an attempt to cover up a crime, the affidavit says.





Leahy Center for Digital Investigation







Leahy Center for Digital Investigation







Leahy Center for Digital Investigation

Network Forensics of IOT

Quick overview of the findings

- Most IOT devices transmitted encrypted data to content delivery networks
- Others did not
- · Others communicated with China













Where is the data?







Leahy Center for Digital Investigation

Meet Crissy Michaels

I build really fun scenarios for my students

Feel free to help me generate data for students to look at

@missycrissy

missycrissym@gmail.com





Leahy Center for Digital Investigation

Random Artifact 1

Samsung SmartCam

New firmware updates allow for image and video encryption. This is turned off by default when the app and firmware on the camera is updated. The encryption is also only for video and image transmission over the network. Saved media in the /sdcard/SmartCam location as well as /data/data/com.techwin.shc/files location are not encrypted and can be viewed as if encryption was not enabled. ARP spoofed the phone and was able to intercept traffic between the camera and phone. verified that the data sent is encrypted.

Images and videos in two locations. One within /sdcard/ SmartCam and the other /data/data/com.techwin.shc/files/. Pictures (.jpg) are automatically saved to /sdcard/SmartCam when user takes a photo via the application. The .jpg images are named in the format YYYY-MM-DD_HH.MM.SS.jpg. This date and time is the time the user saved the picture. Under /data/data/ com.techwin.shc/files/ are folders named in Epoch timestamp format. These folders are created when a user saves a video. The epoch timestamp is the date and time that user started recording the video. A user can go into the app and to it's saved videos and export a video to /sdcard/SmartCam. This will be saved under the format of

<serialNumberOfDevice>_<epochTimeThatTheVideoWasExport ed>.mp4





Leahy Center for Digital Investigation

Random Artifact 2

	With the addition of image and video encryption for the Samsung SmartCam, encryption must be turned off to use the SmartCam with the SmartThings Hub. If encryption is enabled, when you attempt to view the live stream on the SmartThings app you are prompted to disable encryption to display feed. Events are stored at /data/data/com.smartthings.android/databases/ua_analytics.db with Unix timestamps, whether the activity started or stopped.
Samsung SmartThings Hub + Sensors	event ID, and if it occured as a rooms activity or primary activity. / data/data/com.smartthings.android/databases/ua_preferences.db
	contains the alias for the account, which is the email account logged in to the hub. There are three timestamps com.urbanairship.analytics.LAST_SEND which is a unix value corresponding to the time data was last sent to the analytics server or online application? com.urbanairship.application.metrics.LAST_OPEN is the time the SmartThings app was last opened. Last, com.urbanairship.push.LAST_APID_REGISTRATION_TIME is the time registration was last done on the app. (creating a new account).





Leahy Center for Digital Investigation

canary



The first choice of first responders

"Without Canary none of us would have peace of mind" — Ryan Koehler, Firefighter



See how Canary caught two burglars at Ryan's house



Complete Smart Home Security





Leahy Center for Digital Investigation

Canary





Faster response from the authorities.

Canary automatically pulls in contacts for police, fire and EMS closest to your home, giving you one touch access to the proper authorities no matter where you are in the world. With video and audio evidence of burglaries in progress, your call will get the priority it deserves.

"A notification from Canary alerted me to video of two men entering my home. After I called the police, they were on the scene less than 4 minutes later to catch the would-be thieves."

— Mike, Indiana

2:34 pm





2:35 pm Emergency call placed

2:38 pm Police arrive on the scene



https://canary.is/compare/





LCDI | Leahy Center for Digital Investigation

Canary

Hardware Artifacts

TSOP Chip Hynix H27U2G8F2CTR-BC 2GB NAND









Leahy Center for Digital Investigation

Canary App Artifacts

is.yranac.canary/databases/canary_base.sqlite

customer_table

_id	created	curent_locat ion	email	first_ name	customer_id	last_location_chang e	last_name	notifications_ sound	phone	resource_uri	username
2	2017-05-10T18:44:32	/v1/locations/ 413339/	missycrissym @gmail.com	Crissy	476318	2017-05-11T18:03:57	Michaels	canary.wav	17254651282	/v1/customers/476318/	missycrissym@gmail.com

emergency_contacts_table

_id	id		contact_type	customer_id	location_id	
430		1316953	ems	18026582700	413339	
431		1316954	fire	18028643796	413339	
432		1316952	police	18026582700	413339	
433		1316974	ems	18026582700	413346	
434		1316975	fire	18028643796	413346	
435		1316973	police	18026582700	413346	

*Some columns were removed from this slide





Leahy Center for Digital Investigation

Canary

App Artifacts is.yranac.canary/databases/canary_base.sqlite

location_table

_id	address	city	country	created	current_mode	geofence_radius	location_id	lat	Ing	last_modified	name	owner
3	175 Lakeside Avenue	Burlington	United States	5/10/17 1:44 PM	4	50	413339	44.461011	-73.215953	5/11/17 18:20	Home	/v1/customers/476318/
4	175 Lakeside Avenue	Burlington	United States	5/10/17 2:07 PM	4	50	413346	44.461011	-73.215953	5/11/17 18:20	Home	/v1/customers/476318/

mode_table

_id	id	name
1	2	armed
2	5	away
3	1	disarmed
4	4	home
5	6	night
6	3	privacy

enfuse



Leahy Center for Digital Investigation

19

*Some columns were removed from this slide

Canary

App Artifacts

is.yranac.canary/databases/canary_base.sqlite

entry_table

_id	end_time	entry_de scription	entry_type	entry_id	last_modified	location_id	start_time	device_mode	exported
3	5/10/17 5:26 PM	Crissy left Home	location	2563336143	5/10/17 5:26 PM	413339	5/10/17 4:26 PM	/v1/modes/4/	0
4	5/10/17 5:26 PM	Canary entered away mode	mode	2563336145	5/10/17 5:26 PM	413339	5/10/17 4:26 PM	/v1/modes/5/	0
5	5/10/17 5:03 PM	Crissy arrived at Home	location	2563197429	5/10/17 5:03 PM	413339	5/10/17 4:03 PM	/v1/modes/4/	0
72	5/11/17 8:29 AM	Crissy arrived at Home	location	2567133980	5/11/17 8:29 AM	413339	5/11/17 7:29 AM	/v1/modes/5/	0
73	5/11/17 8:29 AM	Canary entered home mode	mode	2567133981	5/11/17 8:29 AM	413339	5/11/17 7:29 AM *Some columns	/v1/modes/4/ were removed fro	0 om this slide





Leahy Center for Digital Investigation

Canary App Artifacts

is.yranac.canary/databases/canary_base.sqlite

video_export_table

_id	processing	device_uuid	video_size	video_length	download_id	request_at	entryld
3	0	49be340a2ab44e5a8c256026552d95df	0	0		0	2568754949
7	0	49be340a2ab44e5a8c256026552d95df	0	0		0	2568774817
10	0	49be340a2ab44e5a8c256026552d95df	0	0		0	2568806616
19	0	49be340a2ab44e5a8c256026552d95df	28	2380		5/11/17 2:17 PM	2568809577
22	0	49be340a2ab44e5a8c256026552d95df	0	0		0	2568879477







Canary **App Artifacts**

Name

-1186526778.0

-1195853946.0

-1200061464.0

-1339617210.0

-1382465580.0

-1422192897.0

-1452926054.0

-1525534627.0

-1555726184.0

-1631687449.0

-1766647700.0

-1779945366.0

-1847170527.0

-1908026663.0

-1909360632.0

-1913227146.0

-2042185819.0

-2066514346.0

-2088185929.0

12782737.0

111126654.0

150680188.0

-1861339396.0

is.yranac.canary/cache

DIRTY 1888009917 CLEAN 1888009917 26587

READ 1888009917

READ 1888009917

DIRTY -1908026663

READ -1908026663

DIRTY -1908026663

DIRTY -1861339396

READ -1861339396

DIRTY -255522701

DIRTY 629010386

READ 629010386

READ 629010386

READ -122032055

READ -122032055

DIRTY 629010386

READ -200

DIRTY -1861339396

CLEAN -1908026663 25885

CLEAN -1908026663 99245

CLEAN -1861339396 26416

CLEAN -1861339396 100961 READ -1861339396

255522701 26036

CLEAN -255522701 100113 READ -255522701

CLEAN 629010386 25342

CLEAN 629010386 97674

DIRTY 1888009917 CLEAN 1888009917 101270 https://developer.android.com/samples/DisplayingBitmaps/src/com.example.android.displayingbitmaps/util/DiskLruCache.html

* The first five lines of the journal form its header. They are the * constant string "libcore.io.DiskLruCache", the disk cache's version,

- \ast the application's version, the value count, and a blank line.
- * Each of the subsequent lines in the file is a record of the state of a \ast cache entry. Each line contains space-separated values: a state, a key, \ast and optional state-specific values.
- * o DIRTY lines track that an entry is actively being created or updated. Every successful DIRTY action should be followed by a CLEAN or REMOVE
- action. DIRTY lines without a matching CLEAN or REMOVE indicate that
- temporary files may need to be deleted.
- o CLEAN lines track a cache entry that has been successfully published and may be read. A publish line is followed by the lengths of each of
- its values.
- o READ lines track accesses for LRU.

journal

journal

- o REMOVE lines track entries that have been deleted.
- * The journal file is appended to as cache operations occur. The journal may

* occasionally be compacted by dropping redundant lines. A temporary file named * "journal.tmp" will be used during compaction; that file should be deleted if

Size

52 KB

52 KB

46 KB

45 KB

100 KB

100 KB

96 KB

207 KB

96 KB

101 KB

99 KB

207 KB

101 KB

101 KB

99 KB

46 KB

45 KB

100 KB

207 KB

100 KB

98 KB

207 KB

Kind

TextEd...ument

TextEd....

extEd...ument

TextEd...ument

TextEd...ument

TextEd...ument

- * it exists when the cache is opened.
- Home Thursday 3:21 PM Activity detected in home mode









LCDI | Leahy Center for Digital Investigation

Canary

Cloud Artifacts

Overviev	V				
Location Details					
Name	Home				
Address	175 Lakeside Avenue, Burlington, VT 05401				
Plan	Membership Preview 7 days left of your Membership preview Manage Plan				
Promo Code	Add promo code				
Canary Devic	OFFLINE Office				
Members					
CM Cris © mi € +11	sy Michaels ssycrissym⊛gmail.com ₽254651282				





Leahy Center for Digital Investigation

Even the bad guys will stop and stare.

BUY NOW

*This data has been heavily redacted - personal devices/network used







Leahy Center for Digital Investigation

App Artifacts

All Nest Products are bundled into one app folder

com.nest.android/files/com.nest.android.preferences.xml

xml version='1.0' encoding='utf-8' standalone='yes' ?	
<map></map>	
<string name="dropcam_token"></string>	</td
string>	
<string name="userLogin">; Name @gmail.com</string>	
<string :="" <="" name="account_snapshot_transport_url" td=""><td>string></td></string>	string>
<pre><boolean name="snapshot_load_from" value="true"></boolean></pre>	
<string name="<b">"tier_id">Production</string>	
<string name="user_id"> </string>	
<string name="user_token">b.</string>	





Leahy Center for Digital Investigation

App Artifacts

com.nest.android/files/com.google.android.gms.analytics.prefs.xml



com.nest.android/databases/cache.db

	key	path	created	last_modified	last_accessed	policy	Motodata
	Filter	Filter	Filter	Filter	Filter	Filter	melauala
1	bucketMap	cache1725969177.json	1494106249573	1495295042009	1494106249573	0	
2	account	cache1488797587.json	1495295041918	1495295041918	1495295041918	0	 Subscriber data





com.nest.android/databases/cache.db

	key	path	created	last_modified	last_accessed	policy
	Filter	Filter	Filter	Filter	Filter	Filter
1	bucketMap	cache1725969177.json	1494106249573	1495295042009	1494106249573	0
2	account	cache1488797587.json	1495295041918	1495295041918	1495295041918	0

App Artifacts

Nest

com.nest.android/cache/cache/cache1488797587.json







Leahy Center for Digital Investigation

com.nest.android/databases/cache.db

	key	path	created	last_modified	last_accessed	policy
	Filter	Filter	Filter	Filter	Filter	Filter
1	bucketMap	cache1725969177.json	1494106249573	1495295042009	1494106249573	0
2	account	cache1488797587.json	1495295041918	1495295041918	1495295041918	0

App Artifacts

com.nest.android/cache/cache/cache1725969177.json

- Nest Metadata for all devices the user has permission to access
- Users, locations and device specific behavioral artifacts will be discussed in this presentation

▶ array [57]







App Artifacts

com.nest.android/cache/cache/cache1725969177.json

- This is the primary user's profile
 - user_settings.######
 - location_primary_Device
 - primary_phone

▼ 17 {4} object_key : user_settings. object revision : 9779 object_timestamp = 1488944341639 ▼ value {21} email_verified : 🗹 true tos_accepted_version = 1434564000001 receive marketing emails : 🗹 true receive nest emails : 🗹 true receive support emails : 🗹 true max structures : 2 max thermostats : 40 max thermostats per structure : 20 max_smoke_detectors_per_structure : 18 max smoke detectors : 36 max wwn devices per structure : 10 max wwn devices : 20 tos_minimum_version : 1434564000001 tos_current_version : 1434564000001 app_swu_minimum_version {1} lang : en US location_primary_device : has_location_history : 🗹 true primary_phone : +1 state 2fa : enrolled state_changed_2fa : 2017-03-08 03:39:02.0



Leahy Center for Digital Investigation



App Artifacts

com.nest.android/cache/cache1725969177.json

- User The user who is signed into the Nest App
- Structures are logical groups
- Two memberships Owner vs. Member

•	37	{4}	
		object_key : user. My user number	
		object_revision : 24889	
		object_timestamp: 1485447963166	
	▼	value {7}	
		email: egmail.com	
		name : egmail.com	
		<pre>w acknowledged_onboarding_screens [2]</pre>	
		0 : eco	
		1 : timeline	
		<pre>invite_accepted_timestamp : 1485447963160</pre>	
		short_name : Jon	
		▼ structures [1]	
		0 : structure.	
		▼ structure_memberships [2]	
		▼ 0 {2}	
		structure : structure.(6
		▼ roles [1]	
		0 : owner	
		▼ 1 {2}	
		structure : structure.	4
		▼ roles [1]	_
		0 : member	
		Leohy Center for	





Locations aka "Structure"







LCDI | Leahy Center for Digital Investigation

Locations aka "Structure"







LCDI | Leahy Center for Digital Investigation

message_center_USERNUMBER







LCDI | Leahy Center for Digital Investigation









LCDI | Leahy Center for Digital Investigation

App Artifacts

com.nest.android/cache/cache/cache##########.json

You will find historical data not merged into the main history file

Name	^	Size
cache1205760548.json		74 KB
cache1224464172.json		75 KB
cache1436717850.json		74 KB
📄 cache1488797587.json		485 bytes
cache1510259999.json		485 bytes
📄 cache1725969177.json		121 KB






Nest

VIDEO RECOVERY This trick doesn't work anymore

ffmpeg -f h264 -i VIDEOFILE -vcodec copy OUTPUT.mp4

V		cad	che	
	$\overline{\mathbf{v}}$		cad	che
				cache-754510979.json
				cache-1234703618.json
				cache2091562039.json
	${f v}$		ima	age_manager_disk_cache
				Off13085d81bae921142c985d170b845325ad60d1bdf9e35227bff1133b77f9c.0
				4b43d475ab446d8e4d6a5b0e805f47478e161f3524f4fca8e9d7aca1e3847183.0
				4b86dd13b067761cad9b4d0231af452a935caccd333b5209df9d15efcdd9b185.0
				5cbc23d7b1a083ac89d85f6dbedd991f58c748a01f81247981784efd00ec4d3e.0
				5d47d521f6902d70c0293eea312f2dc3cfa3ea5a99626eea7d19a5321b5ad599.0
				6d9e29e718ddef2914932143883abe0572f472518aabc71f46246f659517e3a1.0
				8b7545ca291d69469abe58a2e3e564595489b2c2dda99ca9f53ef7fa8043d1dc.0
				8bcb0dba7c87765292d4d90a02db2c7bc0d0926a273b9af7e9588f1edd4f3e46.0
				08d4df5f58363e572e2db92fd284db1cb4871a67b72eb2050cc8b281d8ddd711.0
				8df945760c7bb77fa7dbc50add7c6329730d159df5c549d093c171f9f464a2b7.0
				13c271f05aee7fa724947d0af6be390fa1c69e831bd83e3a358b941c193ea892.0
				33eddaa6321016b13f716bfe6f546edbebad7fce6196cbf496075a0ce95964b9.0
				52eb85c26f3a08b4724a5663f8f12c4ccc6c30c387f55e548ca32312c84ac127.0
				196cc7ba313370c59f9d2cc2df3b70baf7fc931ad414efd6ca671aae57778fb6.0
				393ec4a655378f14b3ebce70db91112db497f4b19db965408c7c503dfee7c8af.0
				741a0a4d472bf931c553e755cca33b0d79d86ae725f92619fd40a11c78de4e75.0
				0220876e4b13da25c1d0e1cb6f3b11c93a9fc3d58b6170f88f4a45cf9f194d51.0
				bc02ba74462ab5101c5c50d0f36f61df514556b958cd64202c592da6886161a7.0 = 0.00000000000000000000000000000000
				efaf55b9bd33a5777787f2fc7e30cce25c036e00c593b25320e5fb1053333758.0





Nest

App Artifacts

com.nest.android/cache/...

Nar	me					
W	Bd14a1449c4a4b76b230f597cfb04814	Table	e: Chunk	_metadata_table		0
	frame_database-journal					
	frame_database				1	
Ŧ	903aa6a1e3ff42c1afc179db20fdb3ab		chunk_id	cache_token	chunk_version	
	frame_database-journal		Filter	Filter	Filter	
	frame_database		1 11.01	1 1101	1 1101	
▼	3269d5b29f5e46728d3fd1e8eb38e392		1404422592	b1_1404422582000	1	
	frame_database-journal		1484400000	111-1484433563000	'	
	frame_database		1404421220	b1-1404421220000	1	
▼	b28aa399ee61442a3d22a7bc57d1aa	2	1484431230	111-1484431230000	'	
	frame_database-journal		1404432416	b1-1404422416000	1	
	frame_database	3	1434432410	111-1494432410000	'	
			1404424760	b1-1404424760000	1	
▼	a7b3269c7354bd7f68e217424557c	4	1434434703	111-1494434709000	'	
	frame_database-journal	-	1404454000	b1-1404454000000	0	
	frame_database	5	1434434330	111-1494404990000	0	
			1404451446	b1-1404451446000	0	
₹	f6c6d439ce344a9d87cc2b4265c3ab02	0	1484451440	111-1494401440000		
	frame_database-journal	-	1404457994	b1_1404457324000	0	
	frame_database	'	1484457324	111-1434437324000	v	







able:	frame_ra	aw_data_table			6		New Re	cord Delete	Record
	frame_time	chunk_id	chunk_version	gop_start_rowid	sps_bytes	pps_bytes	frame_bytes	chunk_complete	
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter]
1	1494430042644	1494430044	NULL	-1	BLOB	BLOB	BLOB	0	
2	1494430106644	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0]
3	1494430170644	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0]
4	1494430234644	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
5	1494430299132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
3	1494430363132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
7	1494430427132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
в	1494430491132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
9	1494430555132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
10	1494430618645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
11	1494430642645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
12	1494430706645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
13	1494430770645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
14	1494430837312	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
15	1494430901825	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1
16	1494430965825	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0	1







able:	frame_ra	aw_data_table			6		New Re	Cord Delete Red
	frame_time	chunk_id	chunk_version	gop_start_rowid	sps_bytes	pps_bytes	frame_bytes	chunk_complete
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1494430042644	1494430044	NULL	-1	BLOB	BLOB	BLOB	0
2	1494430106644	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
3	1494430170644	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
4	1494430234644	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
5	1494430299132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
6	1494430363132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
7	1494430427132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
8	1494430491132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
9	1494430555132	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
10	1494430618645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
11	1494430642645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
12	1494430706645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
13	1494430770645	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
14	1494430837312	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
15	1494430901825	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0
16	1494430965825	1494430044	NULL	1494430042644	NULL	NULL	BLOB	0





LCDI | Leahy Center for Digital Investigation

Name						
	1					
-	2.jp2					
-	3.jp2					
=	4.jp2					
-	5.jp2					
=	6.jp2					
	7.jp2					
	8.jp2					
-	9.jp2					
	10					
	11					
	12					
	13					
	14					
	15					
	16					
	17					
	18					
	19					
	20					
	67					
	68.txt					
	superjoin					

cat 67 68.txt 1 2.jp2 3.jp2 4.jp2 5.jp2 6.jp2 7.jp2 8.jp2 9.jp2 10 11 12 13 14 15 16 17 18 19 20 > superjoin

ffmpeg -i superjoin -c copy output.mp4



Proof of Concept - https://github.com/bicyclemicycle/NestVideoConverter





Leahy Center for Digital Investigation

amazon echo

Always ready, connected, and fast. Just ask.



Roll over image to zoom in



Amazon 54,966 customer reviews | 1000+ answered questions #1 Best Seller (in Home Automation Hubs & Controllers

Price: \$179.99 */Prime*

or 5 monthly payments of \$36.00

In Stock.

Want it tomorrow, May 19? Order within 5 hrs 13 mins and choose One-Day Shipping at checkout. Details Ships from and sold by Amazon Digital Services LLC. Gift-wrap available.

Color: Black

Configuration: Amazon Echo

Amazon Echo	Amazon Echo + Philips Hue Color Starter Kit	Amazon Echo + TP-Link Smart Plug Mini
-------------	---	---------------------------------------

- Plays all your music from Amazon Music, Spotify, Pandora, iHeartRadio, TuneIn, and more using just your voice
- Introducing Alexa calling and messaging, a new way to be together with family and friends. Just ask Alexa to call or message anyone with an Echo, Echo Dot, or the Alexa App.
- Fills the room with immersive, 360^o omni-directional audio
- Hears you from across the room with far-field voice recognition, even while music is playing
- Answers questions, reads the news, reports traffic and weather, reads audiobooks from Audible, gives info on local businesses, provides sports scores and schedules, and more using the Alexa Voice Service
- Controls lights, fans, switches, thermostats, garage doors, sprinklers, locks, and more with compatible connected devices from WeMo, Philips Hue, Samsung SmartThings, Nest, ecobee, and others
- Always getting smarter and adding new features, plus thousands of skills like Uber, Domino's, and more

Jump to: Compare devices | Technical details

New (1) from \$179.99 *√Prime*





LCDI | Leahy Center for Digital Investigation

App Artifacts

com.amazon.dee.app/shared_prefs/service.identity.xml





Leahy Center for Digital Investigation

App Artifacts

com.amazon.dee.app/app_webview/Local Storage/http_alexa.amazon.com_0.localstorage



Echo Serial Number





LCDI | Leahy Center for Digital Investigation

App Artifacts

com.amazon.dee.app/databases/datastore.db

80 Edit Database Cell Database Structure Browse Data Edit Pragmas Execute SQL Set as NULL Mode: Text Import Export 0 🔁 🔏 Table: 📃 Dataltem New Record Delete Record [{"complete":false,"createdDate": key value 1494853818207, "customerid": "A2XASK2DFR7ZCX", "deleted":false, "itemId": "A2XASK2DFR7ZCX#89285c04-Filter Filter 6d94-34d3-9231-142bf449b1a8","lastLocalUpdatedDate":null,"lastUpdatedDate": 1494853818207, "nbestItems": ["oranges strawberries", "oranges and strawberries", "add oranges {"inAnyPool":false,"states": 1 feature-access-collection-using-map strawberries","oranges "ALEXA_MUSIC_KIT_ORBIT":false,"ALWAYS_ON_TEST_FEATURE":true,"ARTHUR_FEATURE":false,"AV_KNIGHT_FEATURE":false,"BLACK_ZEBRA_(strawberries"],"originalAudiold":"AB72C64C86AW2:1.0/2017/05/15/13/90F007187025080R/ [{"complete":false,"createdDate": 2 ToDoCollection.SHOPPING_ITEM 10:14::TNIH_2V.95ad6a7b-3b15-47f7-8fcf-c47dc16ac5a0ZXV/0","reminderTime":null,"text":"oranges 1494853818207, "customerid": "A2XASK2DFR7ZCX", "deleted": false, "itemId": "A2XASK2DFR7ZCX#89285c04-6d94-34d3-9231-142bf449b1a8", strawberries", "type":"SHOPPING_ITEM", "version":1, "utteranceld":null}, {"complete":false, "createdDate": 1494853794008, "customerid": "A2XASK2DFR7ZCX", "deleted": false, "itemId": "A2XASK2DFR7ZCX#65171151-3 ToDoCollection.TASK [] 63b3-37d0-b1bd-4fddf33c270e","lastLocalUpdatedDate":null,"lastUpdatedDate": 1494853794008,"nbestItems": ["avocado"],"originalAudiold":"AB72C64C86AW2:1.0/2017/05/15/13/90F007187025080R/ 09:50::TNIH_2V.d1b37cd4-3dd6-467e-9def-01bb90bf19e6ZXV/ 1","reminderTime":null,"text":"avocado","type":"SHOPPING_ITEM","version":1,"utteranceld":null}]

> Customer ID - A2XASK2DFR7ZCX Echo Device Type - AB72C64C86AW2





LCDI | Leahy Center for Digital Investigation

App Artifacts







Leahy Center for Digital Investigation

App Artifacts

com.amazon.dee.app/cache/sound

Name	
app_901ad8be11e4424f875dc792db51f34d515d6767-01b7-49e5-8273-c8d11b0f331d	
app_NORMALNORMAL_ANONYMOUS	
app_webview	
🔻 🚞 cache	
org.chromium.android_webview	
sound	
code_cache	
databases	
🕨 🚞 files	
no_backup	
shared_prefs	

□



How long does it take to get to Hong Kong from burlington...

(Image: Wikipedia)

Burlington, Vermont is 7,800 miles (12,600 kilometers) from Hong Kong. As I don't know your speed I can't tell you how long it will take.

LEARN MORE ON WIKIPEDIA







Leahy Center for Digital Investigation



App Artifacts

com.amazon.dee.app/cache/org.chromium.android_webview

Step 1 - Decompress the gziped files (7zip)



enfuse



```
token : null
```

```
wrapTitle : 🗹 true
```



LCDI | Leahy Center for Digital Investigation

App Artifacts

com.amazon.dee.app/cache/org.chromium.android_webview

Step 2 – Search for the following:

- Alexa heard: or maintext This will show you the location of "cards" that contain text Alexa heard from the user
- primaryActions This is what Alexa did with the query (backend). Also typically options for the user to interact with
- *"descriptiveText": This will show you the response from Alexa what was said out* loud or played.
- "cardType": This is present in all "cards", will yield more results





App Artifacts

com.amazon.dee.app/cache/org.chromium.android_webview







App Artifacts

com.amazon.dee.app/cache/org.chromium.android_webview

Step 3 – Find your favorite JSON parser

	Remove card Learn more
Amazon Echo	
App Artifacts com.amazon.dee.app/cache/ <u>org.chromium.android_webview</u> Step 2 – Search for the following:	
 Alexa heard: or maintext Alexa heard from the user 	playbackAudioAction {5}
 primaryActions – This is what Alexa did with the query (backend). Also typically options for the user to interact with 	actionType : PlayAudioAction
 "descriptiveText": - This will show you the response from Alexa – what was said out loud or played. ,"cardType": - This is present in all "cards", will yield more results 	<pre>mainText : Alexa heard: \"alexa how long does it take to get to hong kong from burlington vermont\"</pre>
* enfuse Leahy Center for Digital Investigation 27	





Leahy Center for Digital Investigation

∃ Home

S

(Image: Wikipedia)

how long it will take.

Voice feedback

LEARN MORE ON WIKIPEDIA

vermont"

😑 💎 🖹 🛧 🖬 9:40

No

51

How long does it take to get to Hong Kong from burlington...

Burlington, Vermont is 7,800 miles (12,600 kilometers) from Hong Kong. As I don't know your speed I can't tell you

> Alexa heard: "alexa how long does it take to get to hong kong from burlington

Did Alexa do what you wanted?

∃ Home Amazon Echo 5 How long does it take to get to Hong Kong from burlington... (Image: Wikipedia Burlington, Vermont is 7,800 miles (12,600 kilometers) from Hong Kong. As I don't know your speed I can't tell you how long it will take **App Artifacts** LEARN MORE ON WIKIPEDIA Voice feedback com.amazon.dee.app/cache/org.chromium.android_webview Alexa heard: "alexa how long does it take to get to hong kong from burlington vermont' Step 3 – Find your favorite JSON parser Did Alexa do what you wanted? Yes No primaryActions [2] Remove carc Learn more ▼ 0 {5} Less Amazon Echo actionType : OpenUrlAction \bigcirc G 6 mainText : Learn more on Wikipedia \triangleleft 0 subText : null App Artifacts subTextRoute : null com.amazon.dee.app/cache/org.chromium.android webview Step 2 – Search for the following: url : https://en.wikipedia.org/wiki/Hong Kong Alexa heard: or maintext -This will show you the location of "cards" that contain text **v** 1 {5} Alexa heard from the user actionType : OpenUrlAction primaryActions - This is what Alexa did with the query (backend). Also typically options for the user to interact with mainText : Search Bing for \"how long does it take to get to hong kong from burlington vermont\" "descriptive Text": - This will show you the response from Alexa - what was said out loud or played. subText : null . ,"cardType": - This is present in all "cards", will yield more results subTextRoute : null url : http://www.bing.com/search/search.aspx? pc=DPL1&form=AMZND1&g=how+long+does+it+take+to+get+to+hong+kong+from+bur lington+vermont Leahy Center for enfuse LCDi Digital Investigation





52

E M 🛛 💆

😑 💎 🖹 🛧 🖬 9:40

App Artifacts

com.amazon.dee.app/cache/org.chromium.android_webview

Step 3 – Find your favorite JSON parser

Amazon Echo		
 App Artifacts com.amazon.dee.app/cache/org.chromium.android_webview. Step 2 – Search for the following: Alexa heard: or maintext This will show you the location of "cards" that contain text Alexa heard from the user primaryActions – This is what Alexa did with the query (backend). Also typically options for the user to interact with "descriptiveText": - This will show you the response from Alexa – what was said out loud or played. , "cardType": - This is present in all "cards", will yield more results 	ľ	descrip 0 :
Renfuse Leahy Center for Digital Investigation 27		



			⊖ ♥ 🛛 🛿 9:40				
	≡ Home						
	Sec.	How long does Hong Kong fro	it take to get to m burlington				
	Burlington, Veri from Hong Kon- how long it will	¹¹⁰⁾ Vermont is 7,800 miles (12,600 kilometers) Kong. As I don't know your speed I can't tell you will take.					
7	LEARN MORE ON WIKIPEDIA Voice feedback						
	 Alex to get verm 	a heard: "alexa how lo et to hong kong from bi nont"	ng does it take vrlington				
	Did	Alexa do what you war	ted?				
		Yes	No				
	Remove card		Learn more				
			Less ^				
	Ŵ	Q	Ŀ				
	\bigtriangledown	0					

descriptiveText [1]

0 : Burlington, Vermont is 7,800 miles (12,600 kilometers) from Hong Kong. As I don't know your speed I can't tell you how long it will take.



Leahy Center for Digital Investigation

Hardware Artifacts



enfuse

https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa





Leahy Center for Digital Investigation

Hardware Artifacts

\data\local\token\registrationInfo.JSON

"registrationCredentials": {
 "userID": "amzn1.account.AEHA7OWPJNYSHCUXNX7CRVI6NKHQ",
 "firstName": "Crissy",
 "fullName": "Crissy Michaels",
 "deviceName": "Crissy's Echo
 "accountPool": "Amazon",
 "countryOfResidence": "",
 "preferredMarketplace": ""



https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa



Leahy Center for Digital Investigation

Hardware Artifacts

\hda1\mfg.idme.rec

IDMEø...y~als0=50,0,0 als1=51,0,75 als10=96,100,75 als11=97,100,150 als12=133,200,0 als13=134,200,75 als14=134,200,150 als2=52,0,150 als3=62,25,0 als4=62,25,75 als5=63,25,150 als6=73,50,0 als7=74,50,75 als8=75,50,150 als9=95,100,0 btmac=74C2466BC78C devicetype=AB72C64C86AW2 dsn=B0F00715544703K4 mac=74C2467D1C48 mfg=0ZRY2T2GTGA0IRGWFD08 mic0=14243 mic1=15907 mic2=16093 mic3=23717 mic4=17073 mic5=17124 mic6=14559 pcbsn=02807011544702MX wifimodulerev=3M2D





Leahy Center for Digital Investigation

Hardware Artifacts

\data\log*

There are many logs that one would expect to find on a linux system...

\data\log\messages_####....

20170518:200045 AlexaDaemon[1044]: I SpdyClient:controlFrameSent_Values:type=SYN_STREAM, streamId=51, key=header, value={"entries":[{"key":"protocolVersion", "value":{"protocolVersion":"1"}}, {"key":"messageIdentifier", "value": ("identifier":"563d85ba-a354-4c70-8e66-f2a60ae7dd27"}), {"key":"messageType", "value":{"namespace":"Microphone", "name":"doppler.metadata.media"}}, {"key":"body", "value":{"contentType":"application/otet-stream"}}, {"key":"voiceRequestIdentifier":"771f96d5-d1bd-40d3-8a59-9fcd6666e7f7c"}}]: 20170518:200045 AlexaDaemon[1044]: I SpdyClient:controlFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"topler.metadata.media"}}, {"key":"body", "value":{"contentType":"application/json"}}, {"key":"attachment", "value": {"contentType":"application/otet-stream"}, {"key":"voiceRequestIdentifier":"771f96d5-d1bd-40d3-8a59-9fcd666e7f7c"}}]: 20170518:200045 AlexaDaemon[1044]: I SpdyClient:controlFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Values:type=SYN_STREAM, streamId=50, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Key=header, key=header, value={"entries":{{"toplce":"discontrolFrameReceived_Key=header, value=:"discontrolFrameReceived_Key=header, key="citedotifier":"discontrolFrameReceived_Key=header, key="citedotifier":"discontrolFrameReceived_Key=header, key="citedotifier":"discontrolFrameReceived_Key=header, key="citedotifier":"discontrolFrameReceived_Key=header, key="citedotifier":"discontrolFrameReceived_Key

\data\log*.gz Make sure you mount these before you search!





Leahy Center for Digital Investigation

Hardware Artifacts

\data\log\metrics_generic

May 18 20:00:47 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137647,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer.speak,391,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7 May 18 20:01:22 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137682,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer.speak,359,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe36 May 18 20:01:59 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137719,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer.speak,373,voiceRequestId=f7a19124-0bc5-4e48-8d2f-f876c6e5111a May 18 20:02:35 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137755,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer.speak,378,voiceRequestId=e4a79317-e597-4827-b87d-b7151d5d70aa May 18 20:03:19 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137799,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer.speak,416,voiceRequestId=ced963e6-bb88-4c41-8d9b-4c8d74549760 May 18 20:08:39 localhost AlexaSpeechPlayer[1290]: metric generic,1495138119,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer.speak,402,voiceRequestId=ef2fde56-9161-4dc3-a3c2-0acd88d8bcd1

\data\log\metric_high_priority

May 18 20:00:45 localhost ASRD[1431]: metric_high_priority,1495137645,timer,asrd,WW,pryon_latency_msec,254,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7c May 18 20:00:45 localhost MetricsCollector[976]: metric_high_priority,1495137645,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,40,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7c May 18 20:00:45 localhost MetricsCollector[976]: metric_high_priority,1495137645,timer,metrics-collector,asrd,WakewordToOpenASRStream,91,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7c May 18 20:00:45 localhost MetricsCollector[976]: metric_high_priority,1495137645,timer,metrics-collector,asrd,WakewordToBeamLed,142,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7c May 18 20:00:46 localhost MetricsCollector[976]: metric_high_priority,1495137646, timer, metrics-collector, alexad, WakewordToThinkingStart, 1609, voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7c May 18 20:00:47 localhost AlexaSpeechPlayer[1290]: metric_high_priority,1495137647,timer,AlexaSpeechPlayer,TTS,UserPerceivedLatency.SpeechSynthesizer.speak,1356,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7 May 18 20:01:20 localhost ASRD[1431]: metric_high_priority,1495137680,timer,asrd,WW,pryon_latency_msec,260,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:20 localhost MetricsCollector[976]: metric_high_priority,1495137680, timer, metrics-collector,asrd, WakewordToBeamLed, 35, voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:20 localhost MetricsCollector[976]: metric_high_priority,1495137680,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,81,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:20 localhost MetricsCollector[976]: metric_high_priority,1495137680,timer,metrics-collector,asrd,WakewordToOpenASRStream,168,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:22 localhost MetricsCollector[976]: metric_high_priority,1495137682, timer, metrics-collector, alexad, WakewordToThinkingStart, 1610, voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:22 localhost AlexaSpeechPlayer[1290]: metric_high_priority,1495137682,timer,AlexaSpeechPlayer,TTS,UserPerceivedLatency.SpeechSynthesizer.speak,1892,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:56 localhost ASRD[1431]: metric_high_priority,1495137716,timer,asrd,WW,pryon_latency_msec,245,voiceRequestId=f7a19124-0bc5-4e48-8d2f-f876c6e5111a May 18 20:01:56 localhost MetricsCollector[976]: metric_high_priority,1495137716,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,76,voiceRequestId=f7a19124-0bc5-4e48-8d2f-f876c6e5111a May 18 20:01:56 localhost MetricsCollector[976]: metric_high_priority,1495137716,timer,metrics-collector,asrd,WakewordToBeamLed,117,voiceRequestId=f7a19124-0bc5-4e48-8d2f-f876c6e5111a May 18 20:01:57 localhost MetricsCollector[976]: metric_high_priority,1495137717,timer,metrics-collector,asrd,WakewordToOpenASRStream,166,voiceRequestId=f7a19124-0bc5-4e48-8d2f-f876c6e5111a May 18 20:01:58 localhost MetricsCollector[976]: metric_high_priority,1495137718,timer,metrics-collector,alexad,WakewordToThinkingStart,1857,voiceRequestId=f7a19124-0bc5-4e48-8d2f-f876c6e5111a May 18 20:01:59 localhost AlexaSpeechPlayer[1290]: metric_high_priority,1495137719,timer,AlexaSpeechPlayer,TTS,UserPerceivedLatency.SpeechSynthesizer.speak,1526,voiceRequestId=f7a19124-0bc5-4e48-8d2f=f876c6e5111





5/18/2017, 4:00:46EDT

Amazon Echo

1495137646

1495137646832

Hardware Artifacts

May 18 20:00:47 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137647,timer,AlexaSpeechPlayer,TTS,FistDataToAudioOutput.SpeechSynthesizer,Speak,391,voiceRequestId=771f96d5-d1bd-40d3-8a59-9fcd666e7f7c May 18 20:01:22 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137682,timer,AlexaSpeechPlayer,TTS,FistDataToAudioOutput.SpeechSynthesizer,speak,359,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e May 18 20:01:59 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137719,timer,AlexaSpeechPlayer,TTS,FistDataToAudioOutput.SpeechSynthesizer,speak,373,voiceRequestId=7419124-@bc5-4e48_8d2f-f876c6e5111a May 18 20:02:35 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137755,timer,AlexaSpeechPlayer,7TS,FistDataToAudioOutput.SpeechSynthesizer,speak,378,voiceRequestId=e4a79317-e597-4827-b87d-b7151d5d70aa May 18 20:03:19 localhost AlexaSpeechPlayer[1290]: metric_generic,1495137799,timer,AlexaSpeechPlayer,TTS,FistDataToAudioOutput.SpeechSynthesizer,speak,416,voiceRequestId=e4a79317-e597-4827-b87d-b716d5d70aa May 18 20:03:19 localhost AlexaSpeechPlayer[1290]: metric_generic,149513799,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer,speak,416,voiceRequestId=e4a79317-e597-4827-b87d-b78d-464-8d9b-4c8d7660 May 18 20:08:39 localhost AlexaSpeechPlayer[1290]: metric_generic,1495138119,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer,speak,416,voiceRequestId=e4636e-b88a-4c41-8d9b-4c8d7660 May 18 20:08:39 localhost AlexaSpeechPlayer[1290]: metric_generic,1495138119,timer,AlexaSpeechPlayer,TTS,FirstDataToAudioOutput.SpeechSynthesizer,speak,416,voiceRequestId=e42fde56-916-4d63-a3c2-acd88d8bcd1

May 18 20:00:45 localhost ASRD[1431]: metric_high_priority, <mark>1495137645</mark> ,timer,asrd,W	W, pryon_latency_msec, 254, voiceRequestId= <mark>771f96d5-d1bd-40d3-84 59-9fcd666e7f7c</mark>
May 18 20:00:45 localhost MetricsCollector[976]: metric_high_priority, <mark>1495137645,</mark> t	imer, setrics-collector, audioencoderd, WakewordToEncodeStream, 0, voiceRequestId= <mark>771f96d5-d1bd-40d3-8a59-9fcd666e7f7c</mark>
May 18 20:00:45 localhost MetricsCollector[976]: metric_high_priority, <mark>1495137645,</mark> t	ime y ,metrics-collector,asrd,WakewordToOpenASRStream,91,voice <mark>R</mark> equestId= <mark>771f96d5-d1bd-40d3-8a59-9fcd666e7f7c</mark>
May 18 20:00:45 localhost MetricsCollector[976]: metric_high_priority, <mark>1495137645,</mark> t	imer,metrics-collector,asrd,WakewordToBeamLed,142,voiceRequ <mark>r</mark> stId= <mark>771f96d5-d1bd-40d3-8a59-9fcd666e7f7c</mark>
May 18 20:00:46 localhost MetricsCollector[976]: metric_high_priority, <mark>1495137646,</mark> t	imer,metrics-collector,alexad,WakewordToThinkingStart,1609,/oiceRequestId= <mark>771f96d5-d1bd-40d3-8a59-9fcd666e7f7c</mark>
May 18 20:00:47 localhost AlexaSpeechPlayer[1290]: metric_high_priority, <mark>1495137647</mark>	, timer, AlexaSpeechPlayer, TTS, UserPerceivedLatency.SpeechSynthesizer.speak, 1356, voiceRequestId= <mark>771f96d5-d1bd-40d3-8a59-9fcd666e7f7c</mark>
May 18 20:01:20 localhost ASRD[1431]: metric_high_priority,1495137680,timer,asrd,W	W,pryon_latency_msec,260,voiceRequestId= <mark>845758c5-3030-4426</mark> 9378-e01504c6fe3e
May 18 20:01:20 localhost MetricsCollector[976]: metric_high_priority,1495137680,t	imer,metrics-collector,asrd,WakewordToBeamLed,35,voiceRequestId= <mark>845758c5-3030-4426-9378-e01504c6fe3e</mark>
May 18 20:01:20 localhost MetricsCollector[976]: metric_high_priority,1495137680,t	imer,metrics-collector,audioencoderd,WakewordToEncodeStrean,81,voiceRequestId=845758c5-3030-4426-9378-e01504c6fe3e
May 18 20:01:20 localhost MetricsCollector[976]: metric_high_priority,1495137680,t	imer,metrics-collector,asrd,WakewordToOpenASRStream,168,v1iceRequestId=845758c5-3030-4426-9378-001504c6fe3e
May 18 20:01:22 localhost MetricsCollector[976]: metric_high_priority,1495137682,t	imer,metrics-collector,alexad,Wakeword[0]hinkingStart,1619,voiceRequestId=845/58c5-3030-4426-93/8-e01504c6fe3e
May 18 20:01:22 localhost AlexaSpeechPlayer[1290]: metric_high_priority,149513/682	, timer, AlexaSpeechPlayer, IIS, UserPerceivedLatency, Speech ynthesizer.speak, 1892, volceRequestId=845/5865-3030-4426-93/8-e01504c6te3e
May 18 20:01:56 localhost Asku[1431]; metric_nign_priority,149013//16,timer,4810,W	w, pryon_latency_msec, 249, voicerequestic=//alvi24-9000-40/8-8027-18/000e0111a
May 10 20:01:50 localhost MetricsCollector[976]; metric_high_priority,1495137716,t	Imerines-collector, audioencoderd, wakeword Dencodestram, 76, volcereduesti = //1/1/24-0005-440-0021-167000001114
May 18 20:01:57 localhost MetricsCollector[770]. metric_high_priority,14513710,0	lmer metrics-collector, astd, watewordtoDeantes, if / volce eduesticu-/airiz4-buds-4445-buds-4445-buds-4445-buds-4445-buds-4445-buds-4445-buds-4445-buds-4445-buds-4445-buds-4445-buds-445
May 18 20:01:58 localhost MetricsCollector(7/0), metric_high_priority,1495137718 +	imer metrics-collector, asleyad wakawordToTbinkinoStart 1357 voiceBenuetTd=7731912-0h5-6648-8025-1570000001113
May 18 20:01:59 localhost AlexaSpeechPlayer[1290]: metric high priority, 1495137719	timer. AlexaSpeechPlayer. TIS. UserPerceived atency. SpeechSynthesizer. speak. 1526. voi ceRequest Id=7a194-0bc5-6468-8d2f-f876c6e5111a
Talling a jake	> <diy class="d-card d-feature-card">_</diy>
Tell me a joke	<div class="d-card d-standard-card" id="a2XASK2DER77CX#1405138119067#AR72C64C86AW2#B0E00715544703K4">=</div>
3	
	<pre>><div class="d=card" id="a2XaSK2DER77CX#1445137897933#aR72C64C86aW2#80E00715544703K4"> </div></pre>
Why did the invisible man turn down the job? He couldn't see himself doing the	
WOR.	►<01V 10= AZAA3AZUFK/ZLA#149113/040632#AB/ZL04L60AWZ#D0700/13344/060K4 Class= 0-Card > 01V
	► <pre><div 1d="A2XASK2DFR/ZCX#1495137531510#AB/2C64C86AW2#B0F00/15544/03K4" class="d-card d-standard-card"></div></pre>
	-
Search Bing for "Tell me a joke"	<pre><div class="d-card d-standard-card" id="A2XASK2DFR7ZCX#1495137392049#AB72C64C86AW2#80F00715544703K4"></div></pre>
Search bing for Teache a joke	





Hardware Artifacts

Hypothetical scenario

A crime was committed in the home on May 18, 2017 between 3-4PM The phone and Alexa app data are currently unavailable





Leahy Center for Digital Investigation



Hardware Artifacts

- \data\local\token\registrationInfo.JSON
 - Find userID
- \hda1\mfg.idme.rec
 - Find devicetype and dsn
- \data\log
 - Mount everything, search for "May 18 19"
- Timeline Analysis
- Search "voiceRequestId="
 - Document that GUID this will help you search for all metadata for that audio (from what I can tell, this does not hit the cloud)
- Search devicetype:1.0/YYY/MM/DD/HH/XXXXXXXXXXXXXXXX/##:##
 - Document "::TNIH_2V.GUIDGUID-GUID-GUID-GUID-GUID-GUID-GUI/0" this data hits the app and the cloud
- You now have:
 - Timeline
 - Unique identifiers that can be used to locate the transcript/audio





Leahy Center for Digital Investigation







LCDI | Leahy Center for Digital Investigation

Amazon Echo

Hardware Artifacts

\data\local\token\registrationInfo.JSON

Find userID

\hda1\mfg.idme.rec

· Find devicetype and dsn

- \data\log
- · Mount everything, search for "May 18 19"
- Timeline Analysis
- Search "voiceRequestId="
- · Document that GUID this will help you search for all metadata for that audio (from what I can tell, this does not hit the cloud)
- Search <u>devicetype</u>:1.0/YYYY/MM/DD/HH/XXXXXXXXXXXXXXXXX/##:##
- · Document "::TNIH 2V.GUIDGUID-GUID-GUID-GUID-GUID-GUID-GUI/0" this data hits the app and the cloud
- You now have:
 - Timeline
 - · Unique identifiers that can be used to locate the transcript/audio

🔆 enfuse

LCDI | Digital Investigation Leahy Center for

IDMEø...y~als0=50,0,0 als1=51,0,75 als10=96,100,75 als11=97,100,150 als12=133,200,0 als13=134,200,75 als14=134,200,150 als2=52,0,150 als3=62,25,0 als4=62,25,75 als5=63,25,150 als6=73,50,0 als7=74,50,75 als8=75,50,150 als9=95,100,0 btmac=74C2466BC78C devicetype=AB72C64C86AW2 dsn=B0F00715544703K4 mac=74C2467D1C48 mfg=0ZRY2T2GTGA0IRGWFD08 mic0=14243 mic1=15907 mic2=16093 mic3=23717 mic4=17073 mic5=17124 mic6=14559 pcbsn=02807011544702MX wifimodulerev=3M2D



LCDI | Leahy Center for Digital Investigation









LCDI | Leahy Center for Digital Investigation

Amazon Echo	
Hardware Artifacts \data\local\token\registrationInfo.JSON • Find userID	
\hda1\mfg.idme.rec • Find <u>devicetype</u> and <u>den</u> \data\log	
Mount everything, search for "May 18 10" Timeline Analysis	
 Search "voiceRequestid=" Document that GUID - this will help you search for all metadata for that audio (fro Search <u>devicetyper1.0/YYYIMM/DD/HH/XXXXXXXXXXXXXXXXX/#####</u> 	om what I ca., tell, this does not hit the cloud)
You now have: Timeline Unique identifiers that can be used to locate the transcript/audio	nits the app and the clous
en fuse	LCDI Leahy Center for Digital Investigation 44

May 18 19:58:46 (none) ASRD[1431]: metric_high_priority, 1495137526, timer, asrd, WW, pryon_latency_msec, 250, voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:46 (none) MetricsCollector[976]: metric_high_priority, 1495137526, timer, metrics-collector, audioencoderd, WakewordToEncodeStream, 54, voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:46 (none) MetricsCollector[976]: metric_high_priority,1495137526, timer,metrics-collector,asrd,WakewordToBeamLed,96, voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:46 (none) MetricsCollector[976]: metric_high_priority,1495137526, timer,metrics-collector,asrd,WakewordToOpenASRStream,128,voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:51 (none) MetricsCollector[976]: metric_high_priority,1495137531,timer,metrics-collector,alexad,WakewordToOhinkingStart,5135,voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:52 (none) AlexaSpeechPlayer[1290]: metric_high_priority,1495137532,timer,AlexaSpeechPlayer,TTS,UserPerceivedLatency.SpeechSynthesizer.speak,1920,voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010





LCDI | Leahy Center for Digital Investigation

Amazon Echo	
Hardware Artifacts	
data\local\token\registrationInfo.JSON	
Find userID	
hda1\mfg.idme.rec	
Find devicetype and dsn	
data\log	
Mount everything, search for "May 18 19"	
Timeline Analysis	
Search "voiceRequestId="	
 Document that GUID - this will help you search for all metadate 	ta for that sudio (from what I can tell, this does not hit the cloud)
Search <u>devicetype:1.0</u> /YYYY/MM/DD/HH/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	#
 Document ":: TNIH_2V.GUIDGUID-GUID-GUID-GUID-GUID-GUID-GUID-G	<u>D-GUI</u> /0" - this data hits the app and the cloud
You now have:	
Timeline	
 Unique identifiers that can be used to locate the transcript/au 	dio
enfuse	LCDI Leahy Center for Digital Investigation 44

"AB72C64C86AW2:1.0"

arching				×
Status: Complete Start: 05/22/17 Stop: 05/22/17 Time: 0:00:49 Stecords: 2 Search Hits: 156 Added Search Hi	ed 03: 17: 57PM 03: 18: 46PM ts: 156		~	Console Console Log Record
		OK Cancel		
	Name	Preview		
	messages	eamId=AB72C64C86AW2:1.0/2		
	messages	param=AB72C64C86AW2:1.0/2		
	messages	nceId=AB72C64C86AW2:1.0/20		
	messages	eamId=AB72C64C86AW2:1.0/2		
	messages	param=AB72C64C86AW2:1.0/2		
	messages	nceId=AB72C64C86AW2:1.0/20		
	messages	eamId=AB72C64C86AW2:1.0/2		
	messages	param=AB72C64C86AW2:1.0/2		
	messages	nceId=AB72C64C86AW2:1.0/20		
	messages	eamId=AB72C64C86AW2:1.0/2		
	messages	param=AB72C64C86AW2:1.0/2		
	messages	nceId=AB72C64C86AW2:1.0/20		
	🗋 messages	eamId=AB72C64C86AW2:1.0/2		





Someone found the phone/app :)





Leahy Center for Digital Investigation



May 18 19:58:46 (none) MetricsCollector[976]: metric_high_priority,1495137526,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,54,voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:46 (none) MetricsCollector[976]: metric_high_priority,1495137526,timer,metrics-collector,asrd,WakewordToBeamLed,96,voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:46 (none) MetricsCollector[976]: metric_high_priority,1495137526,timer,metrics-collector,asrd,WakewordToOpenASRStream,128,voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:51 (none) MetricsCollector[976]: metric_high_priority, 1495137531, timer, metrics-collector, alexad, WakewordToThinkingStart, 5135, voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16010 May 18 19:58:52 (none) AlexaSpeechPlayer[1290]: metric_high_priority,1495137532, timer, AlexaSpeechPlayer, TTS, UserPerceivedLatency.SpeechSynthesizer.speak, 1920, voiceRequestId=72f032e0-9ce0-477c-bb69-49f533c16016





LCDI | Leahy Center for Digital Investigation







LCDI | Leahy Center for Digital Investigation



Sep 13 19:49:13 (none) ASRD[1374]: metric_high_priority,1473796153,timer,asrd,WW,pryon_latency_msec,248,voiceRequestId=15b8237a-2642-467d-8926-d6dee9449420 Sep 13 19:49:13 (none) MetricsCollector[985]: metric_high_priority,1473796153,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,31,voiceRequestId=15b8237a-2642-467d-8926-d6dee9449420 Sep 13 19:49:14 (none) MetricsCollector[985]; metric high priority,1473796154,timer.metrics-collector,asrd.WakewordToOpenASRStream,144,voiceRequestId=15b8237a-2642-467d-8926-d6dee9449420 Sep 13 19:49:14 (none) MetricsCollector[985]: metric_high_priority,1473796154,timer,metrics-collector,asrd,WakewordToBeamLed,175,voiceRequestId=15b8237a-2642-467d-8926-d6dee9449420 Sep 13 19:49:14 (none) MetricsCollector[985]: metric_high_priority,1473796154,timer,metrics-collector,conductor,LocalStopToStopProcessed,9,voiceRequestId=15b8237a-2642-467d-8926-d6dee9449420 Sep 13 19:49:14 (none) ASRD[1374]: metric_high_priority,1473796154,timer,asrd,LocalCmd,pryon_latency_msec,274,voiceRequestId=15b8237a-2642-467d-8926-d6dee9449420 Sep 13 19:51:34 (none) MetricsCollector[985]: metric_high_priority,1473796294,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,28,voiceRequestId=4948aab9-24ee-4f59-a119-c88ed7cea99c Sep 13 19:51:34 (none) ASRD[1374]: metric_high_priority,1473796294,timer,asrd,WW,pryon_latency_msec,251,voiceRequestId=4948aab9-24ee-4f59-a119-c88ed7cea99c Sep 13 19:51:34 (none) MetricsCollector[985]: metric_high_priority,1473796294,timer,metrics-collector,asrd,WakewordToOpenASRStream,93,voiceRequestId=4948aab9-24ee-4f59-a119-c88ed7cea99c Sep 13 19:51:34 (none) MetricsCollector[985]: metric_high_priority,1473796294,timer,metrics-collector,asrd,WakewordToBeamLed,128,voiceRequestId=4948aab9-24ee-4f59-a119-c88ed7cea99c Sep 13 19:51:37 (none) MetricsCollector[985]: metric_high_priority,1473796297,timer,metrics-collector,alexad,WakewordToThinkingStart,3467,voiceRequestId=4948aab9-24ee-4f59-a119-c88ed7cea99c Sep 13 19:51:38 (none) AlexaSpeechPlayer[1251]: metric_high_priority,1473796298,timer,AlexaSpeechPlayer,TTS,UserPerceivedLatency.VoiceRequest.GetTrafficIntent,2375,voiceRequestId=4948aab9-24ee-4f59-a119-c88ed7cea99c Sep 13 19:54:11 (none) ASRD[1374]: metric_high_priority,1473796451,timer,asrd,WW,pryon_latency_msec,255,voiceRequestId=1a6e7d94-2971-481c-aa1c-ecab6ee2b414 Sep 13 19:54:11 (none) MetricsCollector[985]: metric_high_priority,1473796451,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,29,voiceRequestId=1a6e7d94-2971-481c-aa1c-ecab6ee2b414 Sep 13 19:54:11 (none) MetricsCollector[985]: metric_high_priority,1473796451,timer,metrics-collector,asrd,WakewordToOpenASRStream,103,voiceRequestId=1a6e7d94-2971-481c-aa1c-ecab6ee2b414 Sep 13 19:54:12 (none) MetricsCollector[985]: metric_high_priority,1473796452,timer,metrics-collector,asrd,WakewordToBeamLed,147,voiceRequestId=1a6e7d94-2971-481c-aa1c-ecab6ee2b414 Sep 13 19:54:13 (none) MetricsCollector[985]: metric_high_priority,1473796453,timer,metrics-collector,alexad,WakewordToThinkingStart,2111,voiceRequestId=1a6e7d94-2971-481c-aa1c-ecab6ee2b414 Sep 13 19:54:14 (none) AlexaSpeechPlayer[1251]: metric_high_priority,1473796454,timer,AlexaSpeechPlayer,TTS,UserPerceivedLatency.SpeechSynthesizer.speak,1346,voiceRequestId=1a6e7d94-2971-481c-aa1c-ecab6ee2b414 Sep 13 19:55:10 (none) MetricsCollector[985]: metric_high_priority,1473796510,timer,metrics-collector,audioencoderd,WakewordToEncodeStream,32,voiceRequestId=5d3d5e79-3b10-459c-befb-d2f172baab46 Sep 13 19:55:10 (none) ASRD[1374]: metric_high_priority,1473796510,timer,asrd,WW,pryon_latency_msec,236,voiceRequestId=5d3d5e79-3b10-459c-befb-d2f172baab46 Sep 13 19:55:10 (none) MetricsCollector[985]: metric_high_priority,1473796510,timer,metrics-collector,asrd,WakewordToOpenASRStream,92,voiceRequestId=5d3d5e79-3b10-459c-befb-d2f172baab46 Sep 13 19:55:10 (none) MetricsCollector[985]: metric_high_priority,1473796510,timer,metrics-collector,asrd,WakewordToBeamLed,164,voiceRequestId=5d3d5e79-3b10-459c-befb-d2f172baab46 Sep 13 19:55:13 (none) MetricsCollector[985]: metric_high_priority,1473796513,timer,metrics-collector,alexad,WakewordToThinkingStart,2778,voiceRequestId=5d3d5e79-3b10-459c-befb-d2f172baab46





LCDI | Leahy Center for Digital Investigation

Thank You

Jonathan Rajewski | Director | Leahy Center for Digital investigation rajewski@champlain.edu | @jtrajewski





Leahy Center for Digital Investigation