

What's Behind the Apple Magic, Forensically Speaking

Sarah Edwards - Station X Labs, LLC

SANS Author & Instructor
FOR518 – Mac and iOS Forensic Analysis and
Incident Response

info@mac4n6.com | [@iamevl twin](https://twitter.com/iamevl twin) | mac4n6.com



Introduced at WWDC 2024

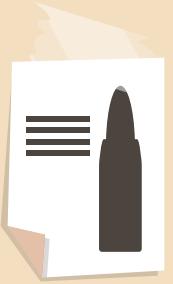
Coming this fall in iOS 18 & macOS Sequoia





"We're thrilled to introduce a new chapter in Apple innovation. Apple Intelligence will transform what users can do with our products — and what our products can do for our users," said Tim Cook, Apple's CEO. "Our unique approach combines generative AI with a user's personal context to deliver truly helpful intelligence. And it can access that information in a completely private and secure way to help users do the things that matter most to them. This is AI as only Apple can deliver it, and we can't wait for users to experience what it can do."

<https://www.apple.com/newsroom/2024/06/introducing-apple-intelligence-for-iphone-ipad-and-mac/>



Pattern of Life



Device Acquisition



Mac

Forensic Tools
Sysdiagnose



iPad & iPhone
(w/ Apple Watch)

Forensic Tools
Jailbreak
Sysdiagnose



Apple TV

Forensic Tools
Jailbreak
Sysdiagnose



Vision Pro

Sysdiagnose

Caveats & Assumptions

Authorization / Ownership
Data Access
Data Retention
Data File Types

This may get a bit dark, it is forensics after all.



Hit and Run



Location

Was the device at
the scene?

Hands Free (CarPlay)

Was the user distracted?

Speed

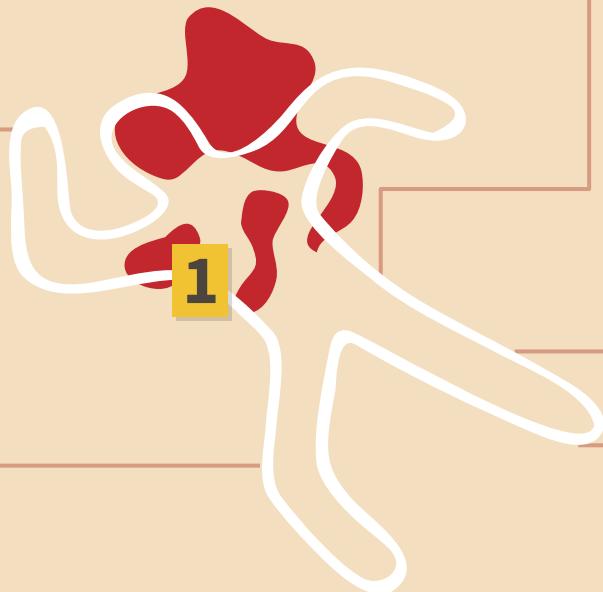
Going too fast?

Audio Volume

Was the user
distracted?

Crash Detection

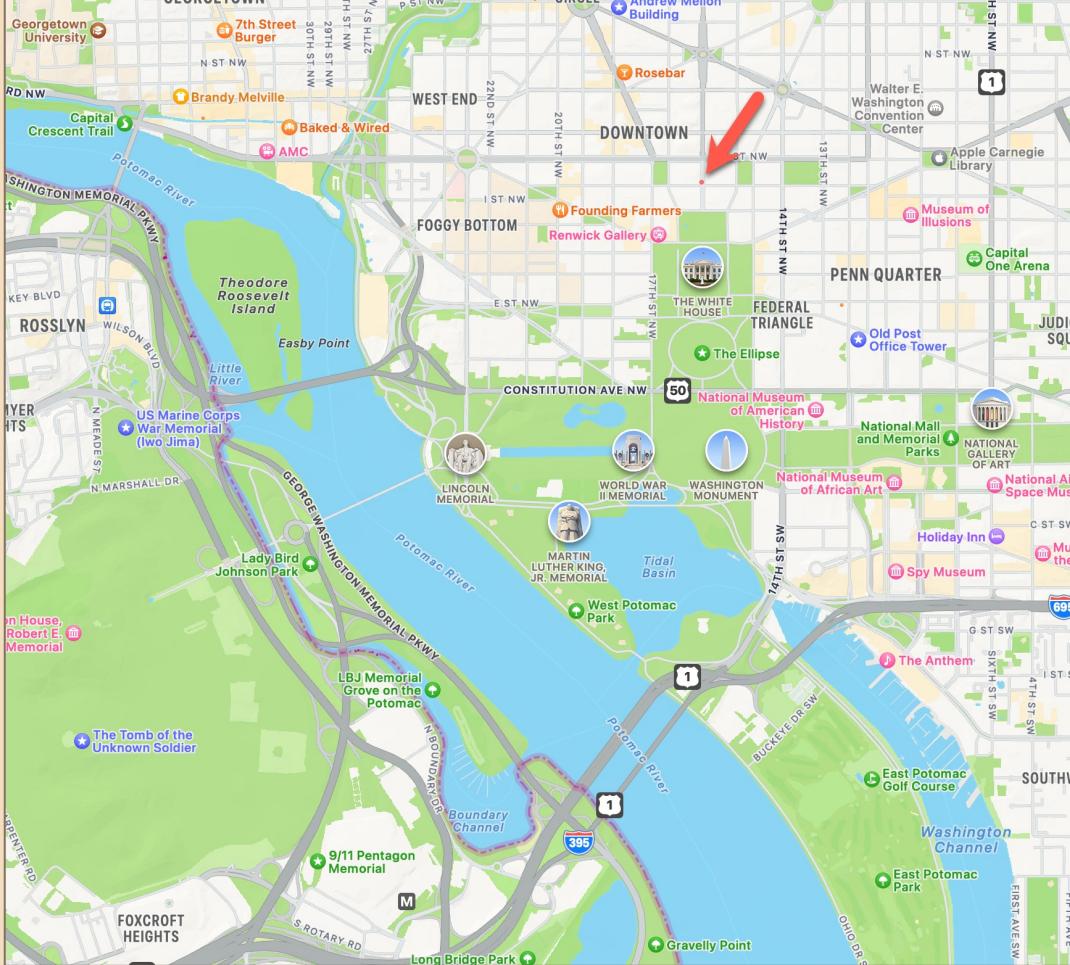
Was an impact
detected?



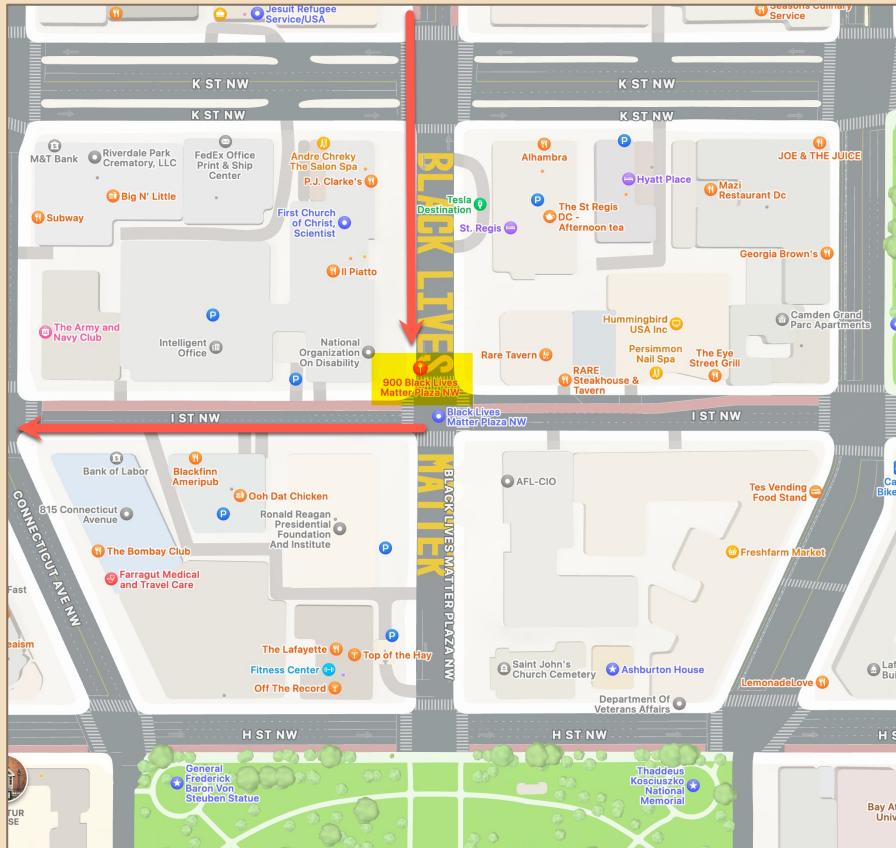
Location & Speed Routined Cache.sqlite

TIMESTAMP	COORDINATES	ALTITUDE	COURSE	SPEED (M/S)	SPEED (MPH)	SPEED (KMPH)	HORIZONTAL ACCURACY	VERTICAL ACCURACY
2024-08-16 15:52:50	38.9017147408613, -77.0366139124883	87.2	180.510208129883	0.411555555555556	0.920625084444445	1.4816	10.0	19.0
2024-08-16 15:52:51	38.9017139241434, -77.036613921796	87.3	180.510208129883	0.0514444444444445	0.115078135555556	0.1852	10.0	19.0
2024-08-16 15:52:52	38.9017139241434, -77.0366139217958	87.4	180.510208129883	0.0	0.0	0.0	10.0	19.0
2024-08-16 15:52:53	38.9017139241434, -77.0366139217958	87.4	180.510208129883	0.0514444444444445	0.115078135555556	0.1852	10.0	19.0
2024-08-16 15:52:54	38.9017112742376, -77.036613951996	87.4	180.510208129883	0.411555555555556	0.920625084444445	1.4816	10.0	19.0
2024-08-16 15:52:55	38.9017027076704, -77.0366140496264	87.4	180.510208129883	1.080333333333333	2.41664084666667	3.8892	10.0	19.0
2024-08-16 15:52:56	38.9016906080501, -77.0366141875224	87.1	180.510208129883	1.33755555555556	2.99203152444444	4.8152	10.0	19.0
2024-08-16 15:52:57	38.9016788953274, -77.0366143210086	87.0	180.510208129883	1.286111111111111	2.87695338888889	4.63	10.0	19.0
2024-08-16 15:52:58	38.901666648502, -77.0366144605822	86.8	180.510208129883	1.33755555555556	2.99203152444444	4.8152	10.0	19.0
2024-08-16 15:52:59	38.9016506833333, -77.03663565	86.6	180.510208129883	1.90344444444444	4.25789101555556	6.8524	10.0	19.0
2024-08-16 15:53:00	38.9016289, -77.03663515	86.5	180.510208129883	2.62366666666667	5.86898491333333	9.4452	10.0	19.0
2024-08-16 15:53:01	38.9015949, -77.0366349666667	86.4	180.510208129883	3.96122222222222	8.86101643777778	14.2604	10.0	19.0
2024-08-16 15:53:02	38.9015550666667, -77.0366359333333	86.4	180.510208129883	4.63	10.3570322	16.668	10.0	19.0
2024-08-16 15:53:03	38.9015096302719, -77.0366162500693	86.4	180.510208129883	4.93866666666667	11.0475010133333	17.7792	10.0	19.0
2024-08-16 15:53:04	38.9014712246388, -77.0366166877662	86.3	217.8	4.78433333333333	10.7022666066667	17.2236	10.0	19.0
2024-08-16 15:53:05	38.9014408166667, -77.0367146333333	86.4	240.0	5.35022222222222	11.9681260977778	19.2608	10.0	19.0
2024-08-16 15:53:06	38.90142275, -77.0367824666667	86.4	259.6	6.482	14.49984508	23.3352	10.0	19.0
2024-08-16 15:53:07	38.9014157166667, -77.0368717333333	86.4	267.1	8.02533333333333	17.9521891466667	28.8912	10.0	19.0

~60k location
entries
(in 1 table)



Enhance, Enhance, Enhance...



CarPlay Connected Biome [1]

```
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.All
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.All/local
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.All/local/tombstone
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_Metadata
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_Metadata/lock
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_Metadata/local
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_Metadata/local/745534093381697
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_Metadata/local/tombstone
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_Metadata/metadata
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.Airplay
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.Airplay/local
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.Airplay/local/tombstone
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Carplay.IsConnected
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Carplay.IsConnected/lock
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Carplay.IsConnected/local
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Carplay.IsConnected/local/745515656867666
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Carplay.IsConnected/local/tombstone
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Carplay.IsConnected/metadata
./private/var/mobile/Library/Biomestreams/restricted/NotesContent
./private/var/mobile/Library/Biomestreams/restricted/NotesContent/lock
./private/var/mobile/Library/Biomestreams/restricted/NotesContent/local
./private/var/mobile/Library/Biomestreams/restricted/NotesContent/local/745530073498792
./private/var/mobile/Library/Biomestreams/restricted/NotesContent/local/tombstone
./private/var/mobile/Library/Biomestreams/restricted/NotesContent/local/tombstone/745564637605411
./private/var/mobile/Library/Biomestreams/restricted/NotesContent/metadata
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.UseAsWallpaper
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.UseAsWallpaper/local
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Photos.Share.UseAsWallpaper/local/tombstone
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Family.Prediction
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Family.Prediction/lock
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Family.Prediction/local
./private/var/mobile/Library/Biomestreams/restricted/_DKEvent.Family.Prediction/local/744863926512616
```

CarPlay Connected Biome [2]

0	C8060000	00000000	08E9E7F7	FE37C641	09000000	37343535	31353635	363836377.A	745515656867
32	36363600	00000000	00000000	00000000	00000000	53454742	86000000	01000000	666	SEGB.	
64	AE0F6F44	D537C641	AE0F6F44	D537C641	CA04DD56	02000000	0A250A14	2F636172	. oD.7.A. oD.7.A. .V % /car		
96	706C6179	2F697343	6F6E6E65	63746564	120D0800	10C7F7E1	AE92DE9B	D2DD0111	play/isConnected	
128	0000002A	CD33C641	19000000	44D537C6	4122110A	0D080010	C7F7E1AE	92DE9BD2	*.3.A D.7.A"	
160	DD012000	2A244438	32353145	42372D43	3841442D	34354643	2D423032	372D4335	.*\$D8251EB7-C8AD-45FC-B027-C5		
192	45364241	37383737	463141BC	086344D5	37C64150	C08FFFFF	FFFFFFFF	FF010000	E6BA7877F1A. cD.7.AP.....		
224	86000000	01000000	D0B87683	DA37C641	D0B87683	DA37C641	9188446B	02000000	.. .v..7.A..v..7.A..Dk		
256	0A250A14	2F636172	706C6179	2F697343	6F6E6E65	63746564	120D0800	10C7F7E1	% /carplay/isConnected	...	
288	AE92DE9B	D2DD0111	00000044	D537C641	19000000	82DA37C6	4122110A	0D080010 D.7.A ..7.A"	
320	C7F7E1AE	92DE9BD2	DD012001	2A243341	36303845	45452D36	3843462D	34423634 *\$3A608EEE-68CF-4B64		
352	2D424239	412D3035	46464432	43374341	323241E9	B67683DA	37C64150	C08FFFFF	-BB9A-05FFD2C7CA22A..v..7.AP....		
384	FFFFFFFFFF	FF010000	86000000	01000000	D6525694	ED37C641	D6525694	ED37C641RV..7.A.RV..7.A		
416	0834A6DC	02000000	0A250A14	2F636172	706C6179	2F697343	6F6E6E65	63746564	4.. % /carplay/isConnected		
448	120D0800	10C7F7E1	AE92DE9B	D2DD0111	00000082	DA37C641	19000000	94ED37C67.A ..7.		
480	4122110A	0D080010	C7F7E1AE	92DE9BD2	DD012000	2A244636	42324441	32462D38	A" *\$F6B2DA2F-8		
512	4643462D	34313134	2D383545	452D4442	34334337	36304446	354641C0	405694ED	FCF-4114-85EE-DB43C760DF5FA.@V..		
544	37C64150	C08FFFFF	FFFFFFFFF	FF010000	86000000	01000000	138213F9	ED37C641	7.AP..... . .7.A		
576	138213F9	ED37C641	05684F0B	02000000	0A250A14	2F636172	706C6179	2F697343	.. .7.A h0 % /carplay/isC		
608	6F6E6E65	63746564	120D0800	10C7F7E1	AE92DE9B	D2DD0111	00000094	ED37C641	onnected7.A		
640	19000000	F6ED37C6	4122110A	0D080010	C7F7E1AE	92DE9BD2	DD012001	2A243244	.. .7.A" *\$2D		
672	39393336	35392D43	3645462D	34413342	2D424335	442D3235	36334635	34393742	993659-C6EF-4A3B-BC5D-2563F5497B		
704	4636411F	8113F9ED	37C64150	C08FFFFF	FFFFFFFFF	FF010000	86000000	01000000	F6A . .7.AP..... .		
736	8ACB1DFE	ED37C641	8ACB1DFE	ED37C641	8C04401D	02000000	0A250A14	2F636172	.. .7.A.. .7.A. @ % /car		

CarPlay Connected Protobufs

```
oompa@Sarahs-MacBook-Air-2 ISF_Preso % protoc --decode_raw < iphone_carplay_connected_biome_pb1
1 {
 1: "/carplay/isConnected"
2 {
 1: 0
 2: 15971012160563739591
}
}2: 0x41c633cd2a000000
3: 0x41c637d544000000
4 {
 1 {
 1: 0
 2: 15971012160563739591
}
4: 0
}
5: "D8251EB7-C8AD-45FC-B027-C5E6BA7877F1"
8: 0x41c637d5446308bc
10: 18446744073709537216
oompa@Sarahs-MacBook-Air-2 ISF_Preso % protoc --decode_raw < iphone_carplay_connected_biome_pb2
1 {
 1: "/carplay/isConnected"
2 {
 1: 0
 2: 15971012160563739591
}
}2: 0x41c637d544000000
3: 0x41c637da82000000
4 {
 1 {
 1: 0
 2: 15971012160563739591
}
4: 1
}
5: "3A608EEE-68CF-4B64-BB9A-05FFD2C7CA22"
8: 0x41c637da8376b6e9
10: 18446744073709537216
```

```
oompa@Sarahs-MacBook-Air-2 ISF_Preso % date -ur $((744987220+978307200))
Sat Aug 10 12:53:40 UTC 2024
oompa@Sarahs-MacBook-Air-2 ISF_Preso % date -ur $((745515656+978307200))
Fri Aug 16 15:40:56 UTC 2024
oompa@Sarahs-MacBook-Air-2 ISF_Preso % date -ur $((745515656+978307200))
Fri Aug 16 15:40:56 UTC 2024
oompa@Sarahs-MacBook-Air-2 ISF_Preso % date -ur $((745518340+978307200))
Fri Aug 16 16:25:40 UTC 2024
```

Start & End Timestamps

User Distraction – knowledgeC.db

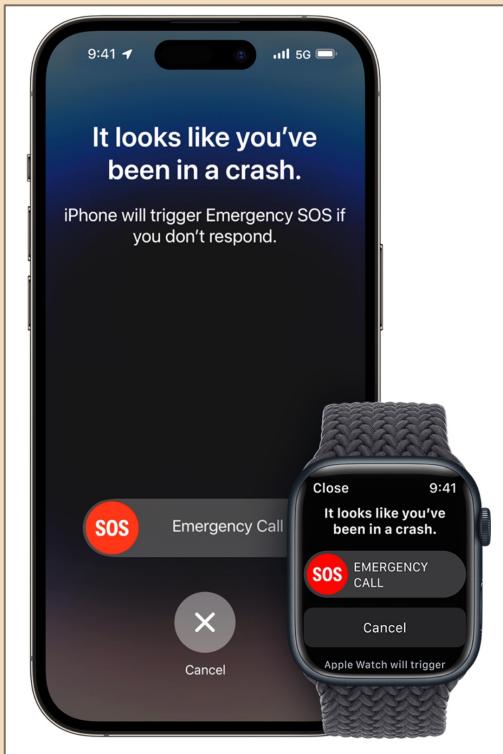
Watching videos on your iPad while driving?*

START	END	USAGE IN SECONDS	USAGE IN MINUTES	BUNDLE ID	NOW PLAYING ALBUM	NOW PLAYING TITLE
2024-08-22 12:55:43	2024-08-22 12:55:50	7	0.1166666666666667	com.netflix.Neflix	S3:E6 "The Minstrel Boy"	Netflix - Lilyhammer
2024-08-22 12:55:50	2024-08-22 15:11:23	8133	135.55	com.netflix.Neflix	S3:E6 "The Minstrel Boy"	Netflix - Lilyhammer
2024-08-22 19:06:16	2024-08-22 19:06:17	1	0.0166666666666667	com.netflix.Neflix	NULL	NULL
2024-08-22 19:06:17	2024-08-22 19:23:09	1012	16.86666666666667	com.netflix.Neflix	S3:E6 "The Minstrel Boy"	Netflix - Lilyhammer
2024-08-22 19:23:09	2024-08-22 19:23:39	30	0.5	com.netflix.Neflix	S3:E6 "The Minstrel Boy"	Netflix - Lilyhammer
2024-08-22 19:23:39	2024-08-22 19:37:02	803	13.3833333333333	com.netflix.Neflix	S3:E6 "The Minstrel Boy"	Netflix - Lilyhammer
2024-08-22 19:37:02	2024-08-22 19:37:02	0	0.0	com.netflix.Neflix	NULL	NULL
2024-08-22 19:37:02	2024-08-22 19:37:05	3	0.05	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-22 19:37:05	2024-08-23 10:49:51	54766	912.766666666667	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-23 10:50:01	2024-08-23 10:50:01	0	0.0	com.netflix.Neflix	NULL	NULL
2024-08-23 10:50:01	2024-08-23 11:06:33	992	16.5333333333333	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-23 11:06:33	2024-08-23 11:07:44	71	1.1833333333333	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-23 11:07:44	2024-08-23 11:14:23	399	6.65	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-23 11:14:23	2024-08-23 11:19:27	304	5.06666666666667	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-23 11:19:27	2024-08-23 11:39:40	1213	20.21666666666667	com.netflix.Neflix	S3:E7 "The Funeral"	Netflix - Lilyhammer
2024-08-23 11:39:40	2024-08-23 12:35:51	3371	56.1833333333333	com.netflix.Neflix	S3:E8 "Loose Ends"	Netflix - Lilyhammer

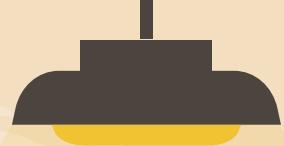
Device Volume & Routing Power Logs

ADJUSTED_TIMESTAMP	VOLUME_PERCENTAGE	MUTED	ORIGINAL_VOLUME_TIMESTAMP	OFFSET_TIMESTAMP	TIME_OFFSET						
2024-08-22 19:06:20	25.0	No	2024-08-22 19:09:27	2024-08-22 19:42:47	-186.819604039192						
2024-08-22 19:06:20	31.25	No	2024-08-22 19:09:27	2024-08-22 19:42:47	-186.819604039192						
2024-08-22 19:06:21	37.5	No	2024-08-22 19:09:28	2024-08-22 19:4	ADJUSTED_TIMESTAMP	ACTIVEROUTE	ACTIVE	OUTPUT	CATEGORY		
2024-08-22 19:06:24	43.75	No	2024-08-22 19:09:30	2024-08-22 19:4	2024-08-21 01:19:28	Speaker	No	Audio/Video			
2024-08-22 19:06:30	50.0	No	2024-08-22 19:09:37	2024-08-22 19:4	2024-08-21 01:19:28	Speaker	No	Audio/Video			
2024-08-22 19:10:28	56.25	No	2024-08-22 19:13:35	2024-08-22 19:4	2024-08-21 17:18:08	INVALID	No	Ringtone			
2024-08-22 19:10:30	62.5	No	2024-08-22 19:13:37	2024-08-22 19:4	2024-08-21 17:18:09	INVALID	No	Ringtone			
2024-08-22 19:10:33	56.25	No	2024-08-22 19:13:40	2024-08-22 19:4	2024-08-21 17:18:09	INVALID	Yes	Ringtone			
2024-08-22 19:39:41	56.25	No	2024-08-22 19:42:48	2024-08-22 19:4	2024-08-21 17:18:09	INVALID	Yes	Ringtone			
2024-08-23 10:50:03	56.25	No	2024-08-23 10:53:09	2024-08-22 19:4	2024-08-21 17:18:33	Speaker	No	Audio/Video			
2024-08-23 10:50:03	50.0	No	2024-08-23 10:53:10	2024-08-22 19:4	2024-08-21 17:18:33	Speaker	No	Audio/Video			
2024-08-23 10:50:04	25.0	No	2024-08-23 10:53:10	2024-08-22 19:4	2024-08-21 17:18:33	Speaker	No	Audio/Video			
2024-08-23 12:14:27	31.25	No	2024-08-23 12:17:34	2024-08-22 19:4	2024-08-21 17:18:33	Speaker	No	Audio/Video			
2024-08-23 12:14:28	37.5	No	2024-08-23 12:17:34	2024-08-22 19:4	2024-08-21 19:56:37	Speaker	Yes	Audio/Video			
					2024-08-21 19:56:37	Speaker	Yes	Audio/Video			
					2024-08-21 19:56:44	HeadphonesBT	Yes	Audio/Video			
					2024-08-21 19:56:44	HeadphonesBT	Yes	Audio/Video			
					2024-08-21 19:56:56	HeadphonesBT	No	Audio/Video			

Crash Detection - Power Logs...probably. (iPhone 14+, iOS 16+)



ADJUSTED_TIMESTAMP	BUNDLE_ID
2024-08-21 17:18:09	com.apple.InCallService
2024-08-21 17:18:36	com.apple.lock-screen
2024-08-21 18:11:33	com.apple.lock-screen
2024-08-21 18:12:47	com.apple.lock-screen
2024-08-21 18:15:04	com.apple.lock-screen
2024-08-21 18:23:31	com.apple.lock-screen
2024-08-21 18:36:59	com.apple.lock-screen
2024-08-21 18:37:01	com.apple.camera
2024-08-21 18:37:01	com.apple.camera
2024-08-21 18:38:51	com.apple.lock-screen
2024-08-21 18:38:55	com.apple.control-center
2024-08-21 18:38:56	com.apple.lock-screen
2024-08-21 18:38:56	com.apple.lock-screen
2024-08-21 18:38:59	com.apple.springboard.home-screen
2024-08-21 18:38:59	com.apple.weather
2024-08-21 18:38:59	com.apple.weather
2024-08-21 18:38:59	com.apple.springboard.home-screen
2024-08-21 18:38:59	com.apple.springboard.spotlight
2024-08-21 18:39:01	com.magmic.NYTCrosswords09
2024-08-21 18:39:03	com.magmic.NYTCrosswords09
2024-08-21 18:39:40	com.magmic.NYTCrosswords09
2024-08-21 18:39:41	com.apple.springboard.home-screen
2024-08-21 18:39:42	com.appleMaps



Murder



Location

Wrong place, wrong
time?

Health

Physical Activity

Maps

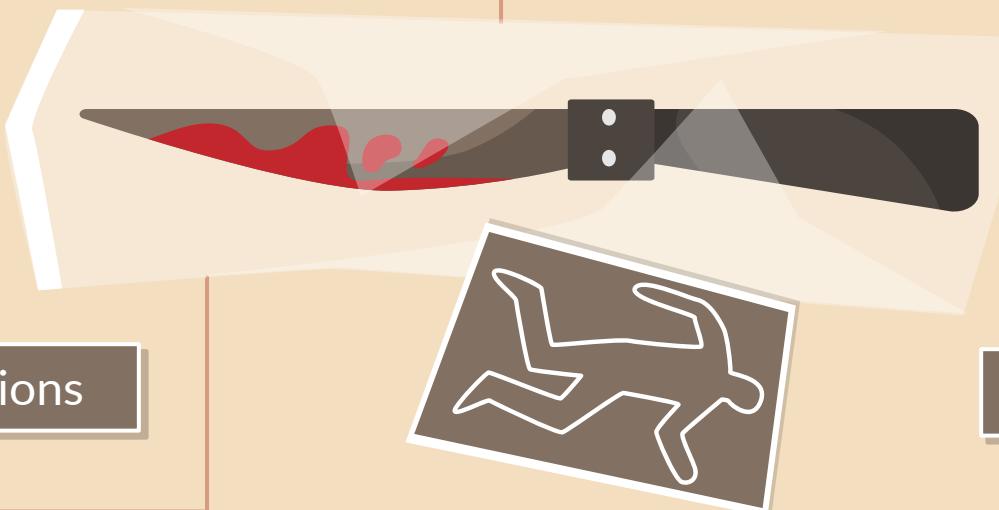
Potential Intent

Wallet Transactions

Potential Intent

Application Usage

Adds Context



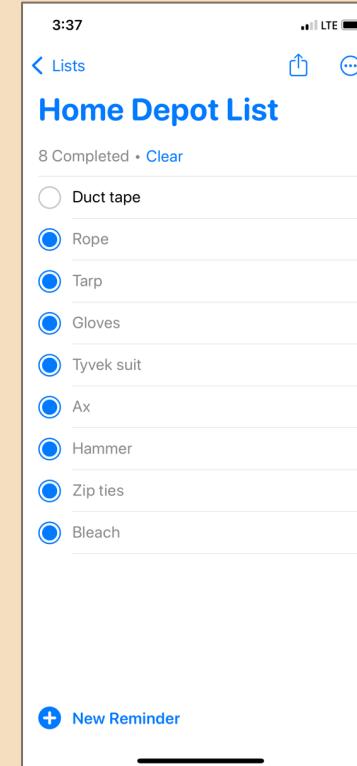
Application Usage - knowledgeC.db

START	END	BUNDLE ID	USAGE IN SECONDS
2024-08-16 19:07:01	2024-08-16 19:07:40	com.apple.mobilenotes	39
2024-08-16 19:07:41	2024-08-16 19:07:43	com.apple.mobilenotes	2
2024-08-16 19:07:43	2024-08-16 19:07:55	com.apple.reminders	12
2024-08-16 19:07:59	2024-08-16 19:08:30	com.apple.Maps	31
2024-08-16 19:08:25	2024-08-16 19:11:45	com.apple.Music	200
2024-08-16 19:08:31	2024-08-16 19:09:13	com.apple.mobilesafari	42
2024-08-16 19:10:42	2024-08-16 19:11:20	com.apple.Maps	38
2024-08-16 19:11:45	2024-08-16 19:11:55	com.apple.Music	10
2024-08-16 19:11:57	2024-08-16 19:12:12	com.apple.Music	15
2024-08-16 19:12:12	2024-08-16 19:18:52	com.apple.Maps	400
2024-08-16 19:16:54	2024-08-16 19:18:38	com.apple.reminders	104
2024-08-16 19:18:46	2024-08-16 19:18:51	com.apple.reminders	5
2024-08-16 19:21:35	2024-08-16 19:21:38	com.apple.reminders	3
2024-08-16 19:22:06	2024-08-16 19:22:16	com.apple.reminders	10
2024-08-16 19:22:38	2024-08-16 19:22:45	com.apple.reminders	7
2024-08-16 19:24:06	2024-08-16 19:24:13	com.apple.reminders	7
2024-08-16 19:25:05	2024-08-16 19:25:11	com.apple.reminders	6
2024-08-16 19:25:11	2024-08-16 19:25:17	com.apple.reminders	6
2024-08-16 19:27:35	2024-08-16 19:27:41	com.apple.reminders	6
2024-08-16 19:37:02	2024-08-16 19:37:13	com.apple.reminders	11
2024-08-16 19:39:44	2024-08-16 19:53:46	com.apple.Maps	842

Reminders App Usage

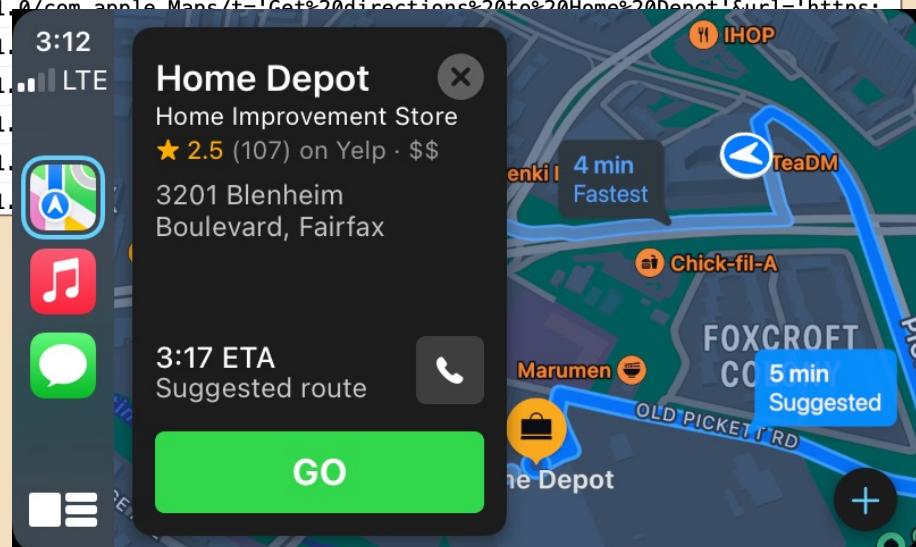
Creating a Murder Kit

START	END	BUNDLE ID	USAGE IN SECONDS
2024-08-16 19:07:01	2024-08-16 19:07:40	com.apple.mobilenotes	39
2024-08-16 19:07:41	2024-08-16 19:07:43	com.apple.mobilenotes	2
2024-08-16 19:07:43	2024-08-16 19:07:55	com.apple.reminders	12
2024-08-16 19:07:59	2024-08-16 19:08:30	com.appleMaps	31
2024-08-16 19:08:25	2024-08-16 19:11:45	com.apple.Music	200
2024-08-16 19:08:31	2024-08-16 19:09:13	com.apple.mobilesafari	42
2024-08-16 19:10:42	2024-08-16 19:11:20	com.appleMaps	38
2024-08-16 19:11:45	2024-08-16 19:11:55	com.apple.Music	10
2024-08-16 19:11:57	2024-08-16 19:12:12	com.apple.Music	15
2024-08-16 19:12:12	2024-08-16 19:18:52	com.appleMaps	400
2024-08-16 19:16:54	2024-08-16 19:18:38	com.apple.reminders	104
2024-08-16 19:18:46	2024-08-16 19:18:51	com.apple.reminders	5
2024-08-16 19:21:35	2024-08-16 19:21:38	com.apple.reminders	3
2024-08-16 19:22:06	2024-08-16 19:22:16	com.apple.reminders	10
2024-08-16 19:22:38	2024-08-16 19:22:45	com.apple.reminders	7
2024-08-16 19:24:06	2024-08-16 19:24:13	com.apple.reminders	7
2024-08-16 19:25:05	2024-08-16 19:25:11	com.apple.reminders	6
2024-08-16 19:25:11	2024-08-16 19:25:17	com.apple.reminders	6
2024-08-16 19:27:35	2024-08-16 19:27:41	com.apple.reminders	6
2024-08-16 19:37:02	2024-08-16 19:37:13	com.apple.reminders	11
2024-08-16 19:39:44	2024-08-16 19:53:46	com.appleMaps	842

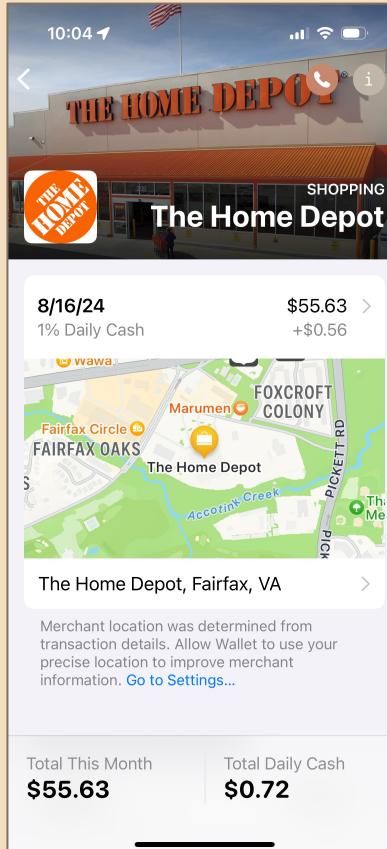
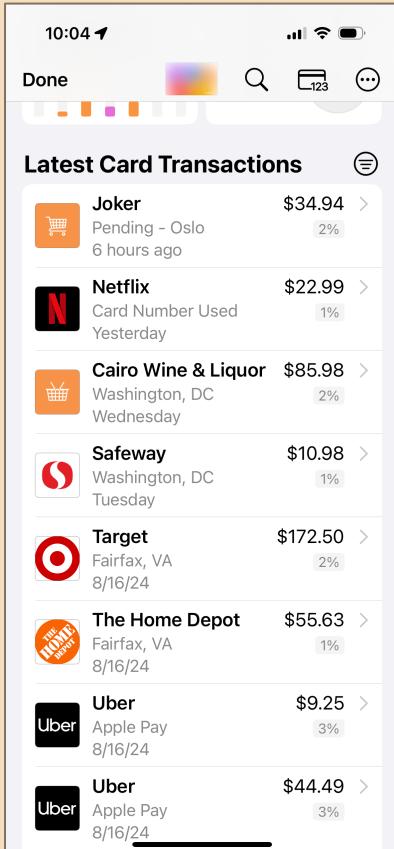


Maps Usage knowledgeC.db

START	END	BUNDLE ID	ACTIVITY TYPE	USER ACTIVITY REQUIRED STRING
2024-08-16 19:10:52	2024-08-16 19:10:52	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Home%20Depot%20in%20Fairfax'&url='https:...'
2024-08-16 19:10:52	2024-08-16 19:10:52	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Home%20Depot%20in%20Fairfax'&url='https:...'
2024-08-16 19:10:52	2024-08-16 19:10:52	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'
2024-08-16 19:10:52	2024-08-16 19:10:52	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'
2024-08-16 19:10:52	2024-08-16 19:10:52	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'
2024-08-16 19:10:53	2024-08-16 19:10:53	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'
2024-08-16 19:10:53	2024-08-16 19:10:53	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'
2024-08-16 19:11:05	2024-08-16 19:11:05	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'
2024-08-16 19:11:05	2024-08-16 19:11:05	com.appleMaps	com.appleMaps	v1.0/com.appleMaps/t='Get%20directions%20to%20Home%20Depot'&url='https:...'



Apple Wallet Transactions



Apple Wallet Transactions

passes23.sqlite

TRANSACTION DATE	STATUS	TRANSACTION TYPE	AMOUNT	CURRENCY CODE	CARD TYPE	PAYMENT TYPE	MERCHANT NAME	MERCHANT CATEGORY
2024-08-16 00:47:44	COMPLETED	PURCHASE	9.25	USD	Mastercard	CREDIT CARD	Uber	Restaurants
2024-08-16 00:47:44	COMPLETED	PURCHASE	44.49	USD	Mastercard	CREDIT CARD	Uber	Restaurants
2024-08-16 18:59:16	COMPLETED	APPLE CASH – DAILY CASH	2.32	USD	Visa	APPLE CASH	NULL	NULL
2024-08-16 20:59:25	COMPLETED	APPLE CASH – DAILY CASH	0.28	USD	Visa	APPLE CASH	NULL	NULL
2024-08-16 21:00:07	COMPLETED	APPLE CASH – DAILY CASH	1.33	USD	Visa	APPLE CASH	NULL	NULL
2024-08-16 21:35:20	COMPLETED	PURCHASE	55.63	USD	Mastercard	CREDIT CARD	Home Depot	Other
2024-08-16 22:21:59	COMPLETED	PURCHASE	172.5	USD	Mastercard	CREDIT CARD	Target	Grocery
2024-08-17 15:54:47	COMPLETED	APPLE CASH – DAILY CASH	3.45	USD	Visa	APPLE CASH	NULL	NULL
2024-08-18 05:30:00	COMPLETED	APPLE CASH – DAILY CASH	0.56	USD	Visa	APPLE CASH	NULL	NULL
2024-08-20 21:12:05	COMPLETED	PURCHASE	10.98	USD	Mastercard	CREDIT CARD	Safeway	Grocery
2024-08-21 18:13:16	COMPLETED	PURCHASE	85.98	USD	Mastercard	CREDIT CARD	Cairo Wine & Liquor	Alcohol
2024-08-22 05:09:15	COMPLETED	APPLE CASH – DAILY CASH	0.11	USD	Visa	APPLE CASH	NULL	NULL
2024-08-22 12:56:34	COMPLETED	PURCHASE	22.99	USD	Mastercard	CREDIT CARD	Netflix	Utilities
2024-08-22 20:08:52	COMPLETED	APPLE CASH – DAILY CASH	1.72	USD	Visa	APPLE CASH	NULL	NULL
2024-08-23 05:26:54	COMPLETED	APPLE CASH – DAILY CASH	0.23	USD	Visa	APPLE CASH	NULL	NULL
2024-08-23 15:24:13	PENDING	PURCHASE	34.94	USD	Mastercard	CREDIT CARD	Joker Skipperga	Grocery

Transaction Locations

passes23.sqlite

MERCHANT NAME	MERCHANT CATEGORY	DEST CURRENCY	LATITUDE	LONGITUDE	ADDRESS
Uber	Restaurants	NULL	NULL	NULL	
Uber	Restaurants	NULL	NULL	NULL	
NULL	NULL	NULL	NULL	NULL	
NULL	NULL	NULL	NULL	NULL	
NULL	NULL	NULL	NULL	NULL	
Home Depot	Other	NULL	38.861908	-77.274828	{"street": "3201 Blenheim Boulevard", "subLocality": "Greater Fairfax", "country": "United States", "postalCode": "20191"}
Target	Grocery	NULL	38.8731726	-77.2291034	{"street": "6100 Arlington Blvd", "subLocality": "Baileys", "country": "United States", "postalCode": "22044", "ci": "US-VA-ARL-6100A"}
NULL	NULL	NULL	NULL	NULL	
NULL	NULL	NULL	NULL	NULL	
Safeway	Grocery	NULL	38.9119423	-77.0387425	{"street": "1701 Corcoran St NW", "subLocality": "Dupont Circle", "country": "United States", "postalCode": "20008"}
Cairo Wine & Liquor	Alcohol	NULL	38.9117815	-77.0386542	{"street": "1618 17th St NW", "subLocality": "Dupont Circle", "country": "United States", "postalCode": "20009", "ci": "US-DC-1618N"}
NULL	NULL	NULL	NULL	NULL	
Netflix	Utilities	NULL	NULL	NULL	
NULL	NULL	NULL	NULL	NULL	
NULL	NULL	NULL	NULL	NULL	
Joker Skipperga	Grocery	NOK	59.912997	10.7496113	{"street": "Skippergata 35", "subLocality": "Sentrum", "country": "Norway", "postalCode": "0154", "city": "Oslo", "ci": "NO-OSE-35"}

“Significant Locations”

Routined Cache.sqlite

ENTRY TIMESTAMP	EXIT TIMESTAMP	COORDINATES	DETECTION TIMESTAMP	VISIT TIME (MINUTES)
2024-08-16 16:26:19	NULL	38.8657784264888, -77.2714637577499	2024-08-16 16:26:19	NULL
2024-08-16 19:15:38	NULL	38.8626984380913, -77.2744399549326	2024-08-16 19:19:56	NULL
2024-08-16 19:15:38	NULL	38.8624231775105, -77.2746739735459	2024-08-16 19:31:55	NULL
2024-08-16 19:15:38	2024-08-16 19:42:39	38.8624771246996, -77.2745996558227	2024-08-16 19:43:07	27.0172026336193
2024-08-16 19:15:38	2024-08-16 19:42:39	38.8624771246996, -77.2745996558227	2024-08-16 19:46:12	27.0172026336193
2024-08-16 19:52:20	NULL	38.8727539797834, -77.2294669985967	2024-08-16 19:56:52	NULL
2024-08-16 19:52:20	NULL	38.8728845627831, -77.2294732510462	2024-08-16 19:57:11	NULL
2024-08-16 19:52:20	2024-08-16 20:31:04	38.8732519155597, -77.228881608492	2024-08-16 20:31:33	38.7327599167824
2024-08-16 19:52:20	2024-08-16 20:31:04	38.8732519155597, -77.228881608492	2024-08-16 20:33:01	38.7327599167824



© Station X Labs, LLC

10:41

Back Significant Locations

Significant Locations

Allow your iPhone and iCloud connected devices to learn places significant to you in order to provide useful location-related information in Maps, Calendar, Photos, and more. Significant Locations are end-to-end encrypted and cannot be read by Apple.
[About Location Services & Privacy...](#)

SUMMARY

133 Records
Jun 30 – Aug 22, 2024

RECENT RECORDS

Subway

Hudson News

Washington Dulles International Airport
Aug 21, 2024 at 10:57 PM – Aug 22, 2024 at 12:06 AM

Clear History

Health (Heart Rate)

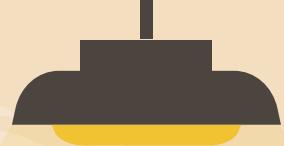
healthdb_secure.sqlite

DATE	HEART RATE	UNITS
2024-08-16 11:43:37	84.0	count/min
2024-08-16 12:13:38	70.0	count/min
2024-08-16 12:43:39	67.0	count/min
2024-08-16 13:13:39	66.0	count/min
2024-08-17 03:01:05	78.0	count/min
2024-08-18 12:28:27	78.0	count/min
2024-08-19 13:02:22	83.0	count/min
2024-08-19 13:43:35	78.0	count/min
2024-08-19 16:06:36	103.0	count/min
2024-08-19 21:50:47	90.0	count/min
2024-08-19 22:51:53	91.0	count/min
2024-08-20 01:36:34	89.0	count/min
2024-08-20 02:38:15	85.0	count/min
2024-08-20 12:46:47	75.0	count/min
2024-08-20 20:05:30	98.0	count/min



Also:

- Flights
- Steps
- Distance
- Loud Noise Detection
- More!



Stalking

Photo & Video

...of stalking subject



Health

Walking, Driving,
etc?

Location

Where have you
followed the
subject?



Camera Usage & State

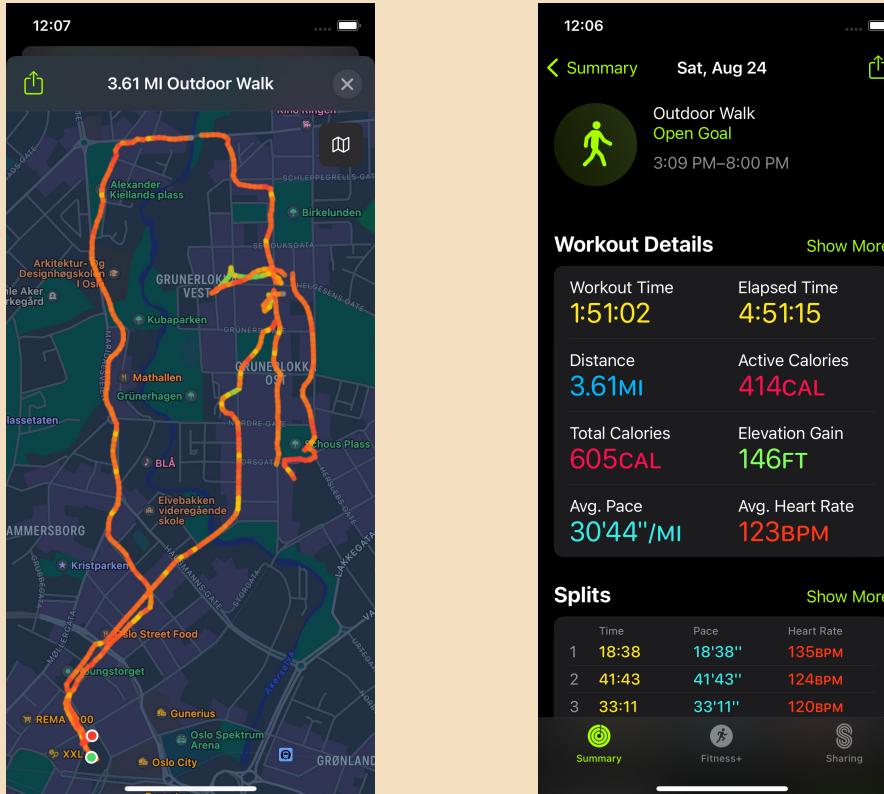
START	END	BUNDLE ID	USAGE IN SECONDS
2024-08-24 13:34:29	2024-08-24 13:34:40	com.apple.camera	11
2024-08-24 13:34:43	2024-08-24 13:34:46	com.apple.weather	3
2024-08-24 13:34:56	2024-08-24 13:35:04	com.apple.camera	8
2024-08-24 13:36:15	2024-08-24 13:36:28	com.apple.Preferences	13
2024-08-24 13:40:44	2024-08-24 13:40:50	com.apple.camera	6
2024-08-24 13:47:53	2024-08-24 13:47:59	com.apple.camera	6
2024-08-24 13:48:02	2024-08-24 13:48:16	com.apple.Preferences	14
2024-08-24 13:48:18	2024-08-24 13:49:48	com.apple.MobileSMS	90
2024-08-24 13:49:53	2024-08-24 13:50:04	com.apple.MobileSMS	11
2024-08-24 14:01:28	2024-08-24 14:02:12	com.apple.MobileSMS	44
2024-08-24 14:02:30	2024-08-24 14:02:45	com.apple.Maps	15
2024-08-24 14:02:45	2024-08-24 14:02:51	com.apple.camera	6
2024-08-24 14:03:35	2024-08-24 14:06:17	com.apple.Maps	162
2024-08-24 14:06:17	2024-08-24 14:06:49	com.apple.mobilenotes	32
2024-08-24 14:06:51	2024-08-24 14:07:11	com.apple.mobilenotes	20
2024-08-24 14:07:11	2024-08-24 14:07:37	com.apple.mobilesafari	26
2024-08-24 14:07:37	2024-08-24 14:11:12	com.apple.Maps	215
2024-08-24 14:11:12	2024-08-24 14:14:05	com.apple.Maps	173
2024-08-24 14:14:05	2024-08-24 14:14:13	com.apple.Maps	8

ADJUSTED_TIMESTAMP	STATE	CAMERA_TYPE
2024-08-24 13:40:43	ON	NULL
2024-08-24 13:40:50	OFF	NULL
2024-08-24 13:40:50	OFF	BACK
2024-08-24 13:47:53	ON	BACK
2024-08-24 13:47:53	ON	NULL
2024-08-24 13:47:58	OFF	NULL
2024-08-24 13:47:59	OFF	BACK
2024-08-24 14:02:45	ON	BACK
2024-08-24 14:02:45	ON	NULL
2024-08-24 14:02:51	OFF	NULL
2024-08-24 14:02:51	OFF	BACK
2024-08-24 15:29:45	ON	BACK
2024-08-24 15:29:45	ON	NULL
2024-08-24 15:29:51	OFF	NULL
2024-08-24 15:29:51	OFF	BACK
2024-08-24 16:37:39	ON	BACK
2024-08-24 16:37:39	ON	NULL
2024-08-24 16:37:39	OFF	NULL
2024-08-24 16:37:40	OFF	BACK

Camera Usage & Photos



Health Database Shows an Outdoor Walk Around Oslo

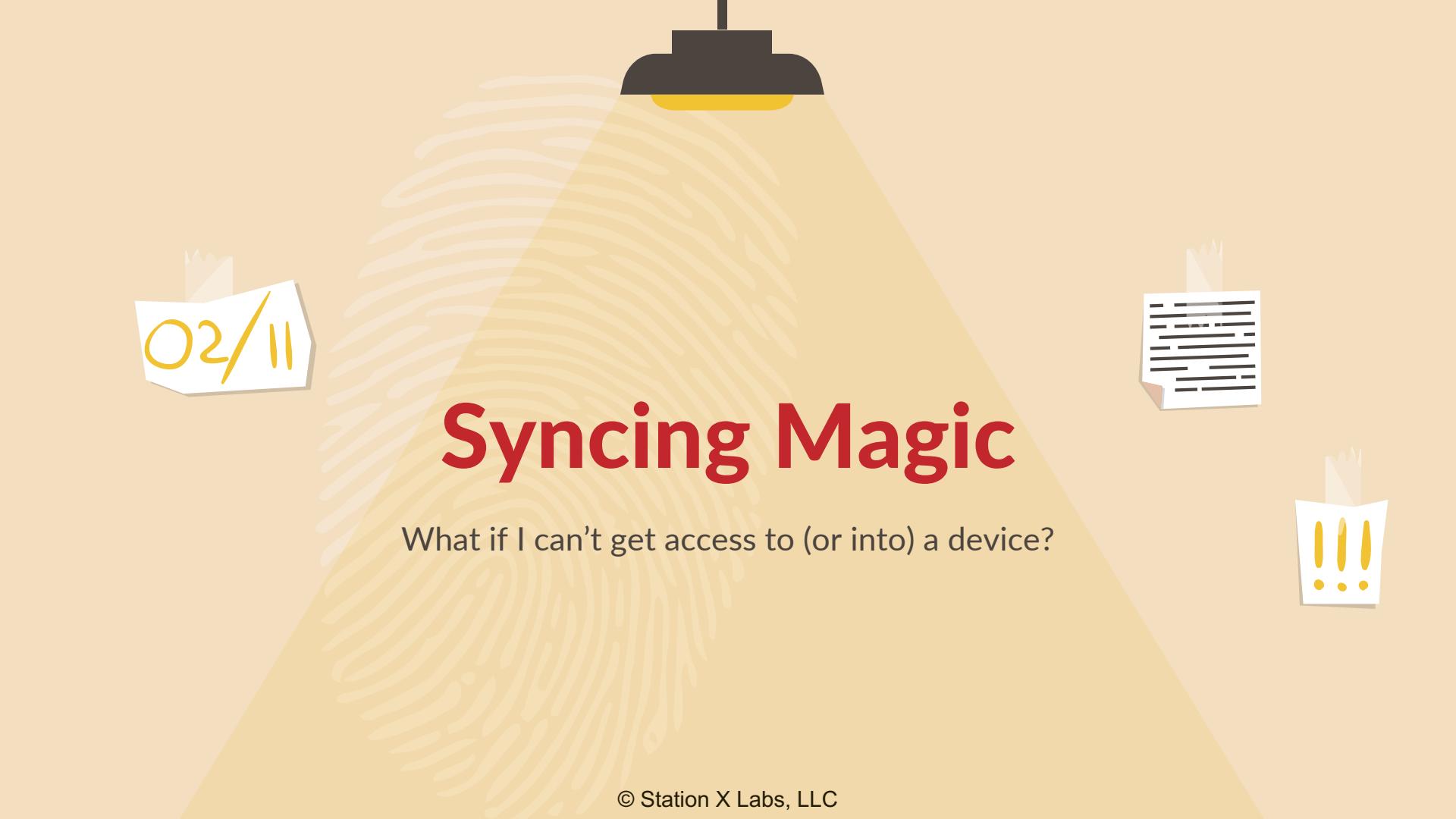


Location & Visit Times

Routined – Cloud-V2.sqlite

VISIT ENTRY	VISIT EXIT	VISIT TIME (MINUTES)	COORDINATES		LOCALITY	SUBLOCALITY	MAP ITEM NAME
2024-08-24 13:37:58	2024-08-24 14:58:58	81.0	59.9247737280242,	10.7592498651	Oslo	Grunerlokka	Bar Boca
2024-08-24 15:05:58	2024-08-24 16:19:58	74.0	59.9193134435119,	10.7594599740263	Oslo	Grunerlokka	Radio Løkka
2024-08-24 16:27:58	2024-08-24 17:36:58	69.0	59.9242697138809,	10.7592207952408	Oslo	Grunerlokka	Chair





02/11

Syncing Magic

What if I can't get access to (or into) a device?



Syncing Biomes – Apps In Focus

~/Library/Biome, /private/var/mobile/Library/Biome

```
./streams/restricted/App.InFocus  
./streams/restricted/App.InFocus/lock  
./streams/restricted/App.InFocus/local  
./streams/restricted/App.InFocus/local/745780160926306  
./streams/restricted/App.InFocus/local/746136217717361  
./streams/restricted/App.InFocus/local/745711495169816  
./streams/restricted/App.InFocus/local/744501260455889  
./streams/restricted/App.InFocus/local/742415088425373  
./streams/restricted/App.InFocus/local/745723872911346  
./streams/restricted/App.InFocus/local/tombstone  
./streams/restricted/App.InFocus/local/tombstone/744165747908317  
./streams/restricted/App.InFocus/local/tombstone/743482807241185  
./streams/restricted/App.InFocus/local/tombstone/745648336343998  
./streams/restricted/App.InFocus/local/tombstone/744078727740683  
./streams/restricted/App.InFocus/remote  
./streams/restricted/App.InFocus/remote/0540EDD3-D2DF-4B08-A858-9AED60492F89  
./streams/restricted/App.InFocus/remote/0540EDD3-D2DF-4B08-A858-9AED60492F89/718198127360572  
./streams/restricted/App.InFocus/remote/0540EDD3-D2DF-4B08-A858-9AED60492F89/tombstone  
./streams/restricted/App.InFocus/remote/0540EDD3-D2DF-4B08-A858-9AED60492F89/tombstone/720355616899398  
./streams/restricted/App.InFocus/remote/0540EDD3-D2DF-4B08-A858-9AED60492F89/tombstone/720826886851748  
./streams/restricted/App.InFocus/remote/3CC4D007-4B22-4572-B9E1-0EB8335B792C  
./streams/restricted/App.InFocus/remote/3CC4D007-4B22-4572-B9E1-0EB8335B792C/718771714260641  
./streams/restricted/App.InFocus/remote/3CC4D007-4B22-4572-B9E1-0EB8335B792C/tombstone  
./streams/restricted/App.InFocus/remote/3CC4D007-4B22-4572-B9E1-0EB8335B792C/tombstone/720890475077336  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/742904220087008  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/744495315334411  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/743782692005045  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/745540037611307  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone/724126429191719  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone/718695155463177  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone/732975019350696  
./streams/restricted/App.InFocus/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone/739140224092107
```

69746564	!^. *. A2%com.united.United
5208342E	CustomerFacingiPhoneJ 4.2.10R 4.
53707269	2.10.0 !.z. 2com.apple.Spri
73776974	ngBoard.transitionReason.appswit
632E4E59	cher !^. *. A2 com.magmic.NY
32343037	TCrosswords09J 5.17.0R 9366.2407
6F6D2E6D	17 o,t. ... *. A2 com.m
30520B39	agmic.NYTCrosswords09J 5.17.0R 9
706C652E	366.240717 3com.apple.
2E6E6F74	SpringBoard.transitionReason.not
6170706C	ification !... *. A2 com.appl
36312E32	e.MobileSMSJ 14.0R 1262.600.61.2
6F6D2E61	.9 .aXo !...[. *. A2 com.a
30302E36	pple.MobileSMSJ 14.0R 1262.600.6
53707269	1.2.9 f`@ 2com.apple.Spri
73776974	ngBoard.transitionReason.appswit
632E4E59	cher !...[. *. A2 com.magmic.NY
32343037	TCrosswords09J 5.17.0R 9366.2407
6F6D2E6D	17 {.<. !: l *. A2 com.m
30520B39	agmic.NYTCrosswords09J 5.17.0R 9
706C652E	366.240717)Z.1 1com.apple.
2E686F6D	SpringBoard.transitionReason.hom
706C652E	escreen !. l *. A2 com.apple.
0A000000	mobilenotesJ 2.11R 2517 ...
696C656E	!='.y *. A2 com.apple.mobilen
6D2E6170	otesJ 2.11R 2517s .X 0com.ap
61736F6E	ple.SpringBoard.transitionReason
2E6D6167	.spotlight !.I.! *. A2 com.mag
0B393336	mic.NYTCrosswords09J 5.17.0R 936

Syncing Biomes – Chat Metadata

~/Library/Biome, /private/var/mobile/Library/Biome

```
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/734908197431964  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/725679511607843  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/717181637427830  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/737734147987890  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/21270103414217  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/729128940908697  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/628855019404  
./streams/restricted/Siri.Remembers.MessageHistory/remote/1381FC52-9528-490D-997B-3BF1E52A745E/722787449277180  
./streams/restricted/Siri.Remembers.MessageHistory/remote/FDB94D96-DD25-41D4-A7AF-3D2C2F2A37BE  
./streams/restricted/Siri.Remembers.MessageHistory/remote/FDB94D96-DD25-41D4-A7AF-3D2C2F2A37BE/74525531550000  
./streams/restricted/Siri.Remembers.MessageHistory/remote/FDB94D96-DD25-41D4-A7AF-3D2C2F2A37BE/tombstone  
./streams/restricted/Siri.Remembers.MessageHistory/remote/9669  
./streams/restricted/Siri.Remembers.MessageHistory/remote/9669  
./streams/restricted/Siri.Remembers.MessageHistory/remote/9669  
./streams/restricted/Siri.Remembers.MessageHistory/remote/9669  
./streams/restricted/Siri.Remembers.MessageHistory/remote/9669  
./streams/restricted/Siri.Remembers.MessageHistory/remote/9669  
./streams/restricted/Siri.Remembers.MessageHistory/remote/0C835605-A8B1-4630-A981-79AEB14E44B9  
./streams/restricted/Siri.Remembers.MessageHistory/remote/0C835605-A8B1-4630-A981-79AEB14E44B9/73318471277380  
./streams/restricted/Siri.Remembers.MessageHistory/remote/0C835605-A8B1-4630-A981-79AEB14E44B9/tombstone
```

Contact Names

Group Names

Contact Numbers & Emails

Slack Hashtags

- iMessage
- SMS
- Slack
- Signal
- WhatsApp

Syncing Biomes - Now Playing

~/Library/Biome, /private/var/mobile/Library/Biome

```
./streams/restricted/Media.NowPlaying/remote/918476FC-4B35-4081-AF4E-E2B8B105C269
./streams/restricted/Media.NowPlaying/remote/918476FC-4B35-4081-AF4E-E2B8B105C269/739565254124893
./streams/restricted/Media.NowPlaying/remote/918476FC-4B35-4081-AF4E-E2B8B105C269/tombstone
./streams/restricted/Media.NowPlaying/remote/918476FC-4B35-4081-AF4E-E2B8B105C269/tombstone/73358329
./streams/restricted/Media.NowPlaying/remote/918476FC-4B35-4081-AF4E-E2B8B105C269/tombstone/72115156
./streams/restricted/Media.NowPlaying/remote/918476FC-4B35-4081-AF4E-E2B8B105C269/745611959233883
./streams/restricted/Media.NowPlaying/remote/0540EDD3-D2DF-4808-A858-9AED60492F89
./streams/restricted/Media.NowPlaying/remote/0540EDD3-D2DF-4808-A858-9AED60492F89/717557193080424
./streams/restricted/Media.NowPlaying/remote/0540EDD3-D2DF-4808-A858-9AED60492F89/tombstone
./streams/restricted/Media.NowPlaying/remote/0540EDD3-D2DF-4808-A858-9AED60492F89/tombstone/72035562
./streams/restricted/Media.NowPlaying/remote/1381FC52-9528-490D-997B-3BF1E52A745E
./streams/restricted/Media.NowPlaying/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone
./streams/restricted/Media.NowPlaying/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone/74223178
./streams/restricted/Media.NowPlaying/remote/1381FC52-9528-490D-997B-3BF1E52A745E/tombstone/72035561
./streams/restricted/Media.NowPlaying/remote/1381FC52-9528-490D-997B-3BF1E52A745E/736677722493855
./streams/restricted/Media.NowPlaying/remote/8497FF53-88B4-4CB9-AFF2-DAE9E9F4AA58
./streams/restricted/Media.NowPlaying/remote/8497FF53-88B4-4CB9-AFF2-DAE9E9F4AA58/723858865549477
./streams/restricted/Media.NowPlaying/remote/8497FF53-88B4-4CB9-AFF2-DAE9E9F4AA58/tombstone
./streams/restricted/Media.NowPlaying/remote/8497FF53-88B4-4CB9-AFF2-DAE9E9F4AA58/tombstone/72629420
./streams/restricted/Media.NowPlaying/remote/DBC27322-757D-4723-A37E-879EB4897D00
./streams/restricted/Media.NowPlaying/remote/DBC27322-757D-4723-A37E-879EB4897D00/744900954936482
./streams/restricted/Media.NowPlaying/remote/DBC27322-757D-4723-A37E-879EB4897D00/tombstone
./streams/restricted/Media.NowPlaying/remote/966909E6-B0A5-47B8-8DE6-3653E61C5505
./streams/restricted/Media.NowPlaying/remote/966909E6-B0A5-47B8-8DE6-3653E61C5505/737605764612393
./streams/restricted/Media.NowPlaying/remote/966909E6-B0A5-47B8-8DE6-3653E61C5505/tombstone
./streams/restricted/Media.NowPlaying/remote/966909E6-B0A5-47B8-8DE6-3653E61C5505/tombstone/739812976042706
./streams/restricted/Media.NowPlaying/remote/966909E6-B0A5-47B8-8DE6-3653E61C5505/tombstone/732219442302579
```

6574666C;A " S3:E5 ...Tommy...0. B Netflix
33352D74	ix - Lilyhammerh r 2C:76:00:CA:A9:35-taclz com.netflix.Netflix. . A.u. ...
11F8A685	..;A " S3:E5 ...Tommy...0. B Netflix - Lil
204C696C	yhammerh r 2C:76:00:CA:A9:35-taclz com.netflix.Netflix. . \. . K...;A "
13636F6D	S3:E6 ...The Minstrel Boy...0. B Netflix -
41180122	Lilyhammerh r 2C:76:00:CA:A9:35-taclz com.netflix.Netflix. . 2 . l.g.;.
78202D20	A " S3:E6 ...The Minstrel Boy...0. B Netflix
636C7A13	- Lilyhammerh r 2C:76:00:CA:A9:35-taclz com.netflix.Netflix. . G..
67B63BC6	..;A " S3:E6 ...The Minstrel Boy...0. B Ne
74666C69	tflix - Lilyhammerh r Speakerz com.net
352D7461	flix.Netflix. . o.# . .;A " S3:
11BCE7A0	E6 ...The Minstrel Boy...0. B Netflix - Lily
42144E65	hammerh r Speakerz com.netflix.Netflix
2E6E6574	65204D69 . . C.q . 7...;A " S3:E6 ...The Mi
1C53333A	nstrel Boy...0. B Netflix - Lilyhammerh r
4C696C79	DC32782C Speakerz com.netflix.Netflix. . .2x,
666C6978	6F79E280 .. o.;A " S3:E6 ...The Minstrel Boy..
65204D69	.0. B Netflix - Lilyhammerh r Speakerz
720D0804	6B65727A com.netflix.Netflix. . .". . } o.;.
6F79E280	6FE53BC6

Takk!

Sarah Edwards | Station X Labs, LLC

info@mac4n6.com | [@iamevtwin](https://twitter.com/iamevtwin) | mac4n6.com

Upcoming SANS FOR518 Classes

- September – Tokyo (Virtual)
- October – DFIR Summit Prague
- November – Miami (Virtual)
- More in 2025! Visit for518.com
- Anytime - OnDemand

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons by [Flaticon](#), and infographics & images by [Freepik](#)

