

THE CIDER PRESS: EXTRACTING FORENSIC ARTIFACTS FROM APPLE CONTINUITY

HEATHER MAHALIK | @HEATHERMAHALIK |

SMARTERFORENSICS.COM

SARAH EDWARDS | @IAMEVLTWIN | MAC4N6.COM

WHO THE HECK ARE WE?

HEATHER MAHALIK

- SANS SENIOR INSTRUCTOR AND AUTHOR
- DIRECTOR OF FORENSIC ENGINEERING,
MANTECH CARD
- SMARTPHONE NERD

SARAH EDWARDS

- SANS CERTIFIED INSTRUCTOR AND AUTHOR
- MOBILE FORENSICS ENGINEER AT PARSONS
CORPORATION
- MAC NERD



© 2017 Sarah Edwards and Heather Mahalik

WHAT IS CONTINUITY?

- “SEAMLESS” INTERACTION BETWEEN ALL APPLE DEVICES:

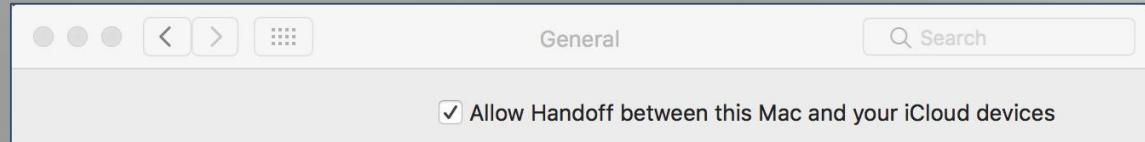
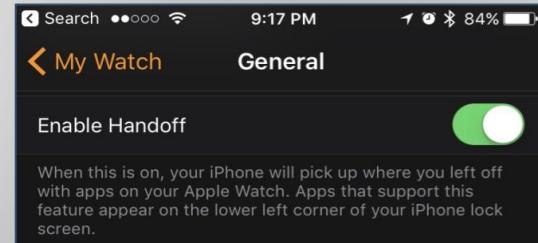
- MACS
- IPHONE
- IPAD
- APPLE WATCH

- SOFTWARE REQUIREMENTS:

- WI-FI & BLUETOOTH ON
- SIGNED IN ON ALL DEVICES WITH ICLOUD ACCOUNT
- “HANDOFF” SET TO ON

- HARDWARE REQUIREMENTS:

- MACOS 10.10+ (MACBOOK EARLY 2015)
- IOS 8+ (IPHONE 5+)
- WATCHOS3 - (SERIES 1+)



THE METHOD TO OUR MADNESS

- IPHONE 7 IOS 10.3.2
- JAILBROKEN IPHONE 7 IOS 10.1.1
- APPLE WATCH OS 3.1.3
- APPLE WATCH 2 OS 3.1
- MACBOOK PRO X 2 (10.12.3 & 10.12.5)



CONNECTED DEVICES - BLUETOOTH IDENTIFIERS - MAC

- /LIBRARY/PREFERENCES/COM.APPLE.BLUETOOTH.PLIST
- MATCH GUID -> GET MAC ADDRESS -> ASSOCIATE WITH DEVICE

▼ CoreBluetoothCache	Dictionary	(7 items)
▶ 1CD03591-2A13-4775-A3AD-6B2B14534303	Dictionary	(3 items)
▼ F768D25B-1EC8-476B-B4A3-D757890CD2E8	Dictionary	(6 items)
Services	Data	<62706c69 73743030
DeviceAddressType	Boolean	NO
DeviceAddress	String	b8-53-ac-09-cc-87
ServiceChangedSubscribed	Boolean	YES
ServiceDiscoveryComplete	Boolean	YES
ServiceChangedHandle	Number	8
▶ 5FC3A499-1C18-4957-819A-539D111AE921	Dictionary	(6 items)
▼ C905A733-BEA0-4680-A41F-4DCDF577A099	Dictionary	(5 items)
DeviceAddressType	Boolean	NO
DeviceAddress	String	ec-ad-b8-06-f2-aa
ServiceChangedSubscribed	Boolean	YES
ServiceDiscoveryComplete	Boolean	YES
ServiceChangedHandle	Number	8
▶ 8071B4E1-97B8-4B6B-90A8-ACB72377ED80	Dictionary	(6 items)
▶ F1BAD73A-97D9-40FB-9C7C-37333322A3A	Dictionary	(6 items)
▶ 2B74AD7C-4439-4004-9D6D-3BE1EC152D7A	Dictionary	(2 items)

▼ DeviceCache	Dictionary	(16 items)
▶	Dictionary	(3 items)
▶	Dictionary	(17 items)
▼ b8-53-ac-09-cc-87	Dictionary	(3 items)
LastNameUpdate	Date	Feb 6, 2017, 7:51:42 AM
Name	String	miPhone7
displayName	String	miPhone7
▶	Dictionary	(16 items)
▶	Dictionary	(2 items)
▶	Dictionary	(4 items)
▶	Dictionary	(20 items)
▶	Dictionary	(3 items)
▶	Dictionary	(1 item)
▶	Dictionary	(2 items)
▶	Dictionary	(7 items)
▼ ec-ad-b8-06-f2-aa	Dictionary	(3 items)
LastNameUpdate	Date	Feb 6, 2017, 8:04:52 AM
Name	String	miWatch
displayName	String	miWatch

CONNECTED DEVICES - BLUETOOTH IDENTIFIERS - MAC

- `~/LIBRARY/PREFERENCES/BYHOST/COM.APPLE.BLUETOOTH.<HW_UUID>.PLIST`
- ASSOCIATE WITH A SPECIFIC USER

▼ Root	Dictionary	(3 items)
BluetoothVersionNumber	Number	3
▼ IDSPairedDevices	Array	(5 items)
Item 0	String	[REDACTED]
Item 1	String	[REDACTED]
Item 2	String	b8-53-ac-09-cc-87
Item 3	String	ec-ad-b8-06-f2-aa
Item 4	String	[REDACTED]
▼ RecentDevices	Dictionary	(10 items)
[REDACTED]	Date	Feb 12, 2017, 9:00:01 AM
[REDACTED]	Date	Apr 14, 2017, 1:25:29 PM
[REDACTED]	Date	Jun 14, 2017, 8:29:51 PM
b8-53-ac-09-cc-87	Date	Jun 14, 2017, 8:29:42 PM
[REDACTED]	Date	Jun 11, 2017, 6:35:08 PM
[REDACTED]	Date	May 21, 2017, 5:42:46 PM
[REDACTED]	Date	May 2, 2017, 10:28:21 PM
[REDACTED]	Date	May 16, 2017, 12:05:07 PM
ec-ad-b8-06-f2-aa	Date	Jun 14, 2017, 8:29:43 PM
	Date	Jun 10, 2017, 5:09:12 PM

CONNECTED DEVICES - BLUETOOTH IDENTIFIERS - IOS

- /LIBRARY/MOBLEBLUETOOTH/COM.APPLE.MOBILEBLUETOOTH.LEDEVICES.PAIRED.DB

Uuid	Name	Address	ResolvedAddress
OADB2DD6-9BFF-423F-9168-E6D2C015BF22	iPad	Public 80:D6:05:77:50:03	Public 80:D6:05:77:50:03
97FE0DEF-3A2B-4283-A03B-D15A2106A0B2	Heather's MacBook Pro	Public 80:E6:50:26:42:FF	Public 80:E6:50:26:42:FF
532E3D99-F21D-4091-87D6-FD2202B3BBD5	Heather's Apple Watch	Random 7A:65:D5:6D:DC:8A	Public C0:CE:CD:E0:10:BA

BONJOUR – ZERO CONFIGURATION NETWORKING

“I JUST WANT ACCESS TO A THING, I DON’T WANT TO CONFIGURE ANYTHING!”

PUBLICATION:
“Hey ya’ll! I can do AirDrop!”

DISCOVERY:
“I have no friends. Who can I
AirDrop with?”

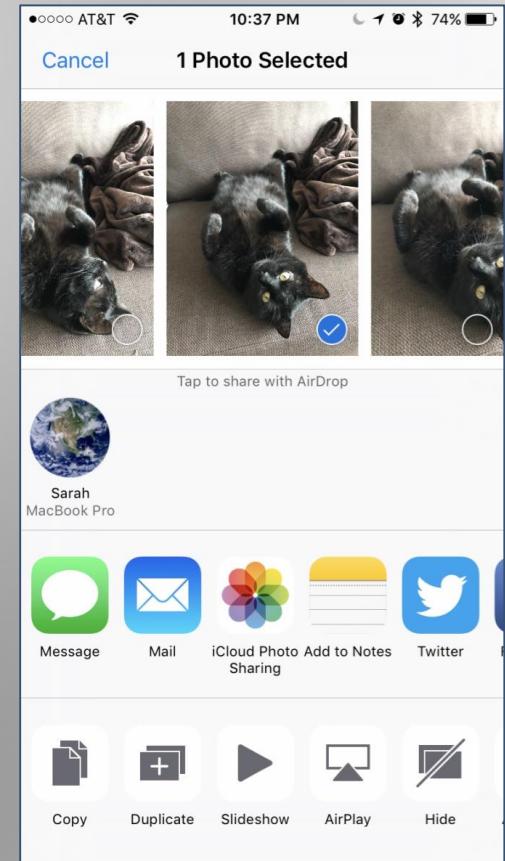
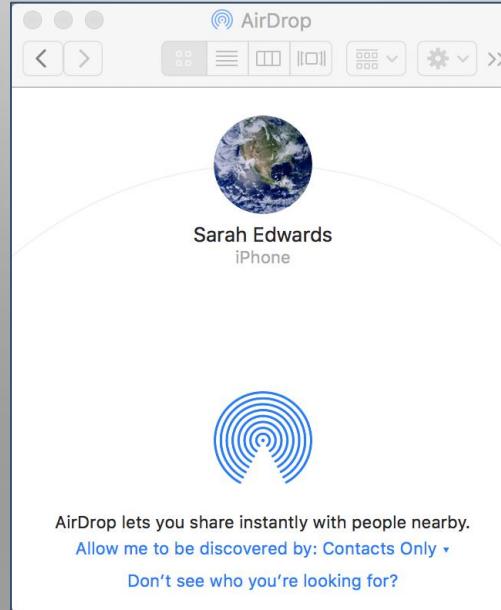
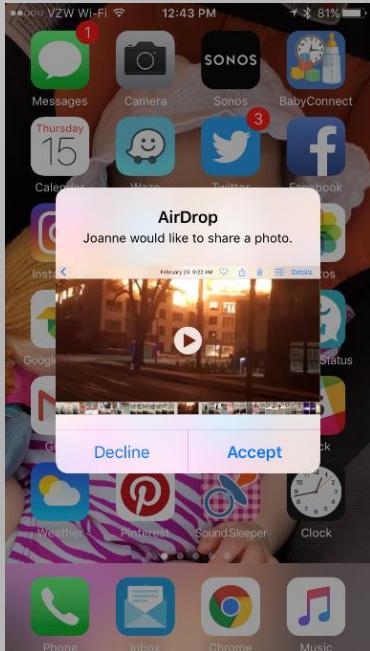
RESOLUTION: “I can be your
friend, lets AirDrop!”

RESOLUTION: “Excellent, I’m
gonna drop it like its hot!”



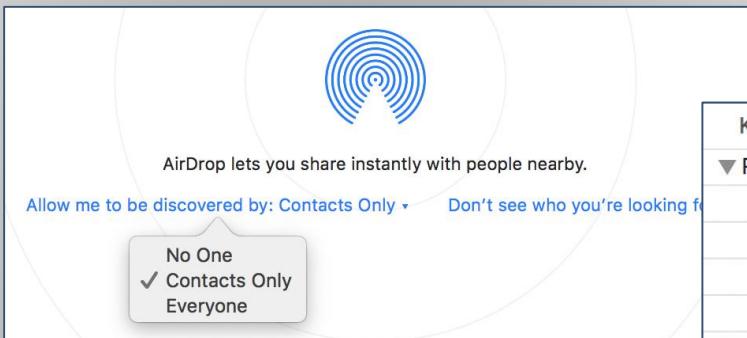
AIRDROP

- SHARE FILES ACROSS DEVICES, WITHOUT THE NEED TO BE ON THE SAME NETWORK!



MAC AIRDROP ID & DISCOVERABLE MODE

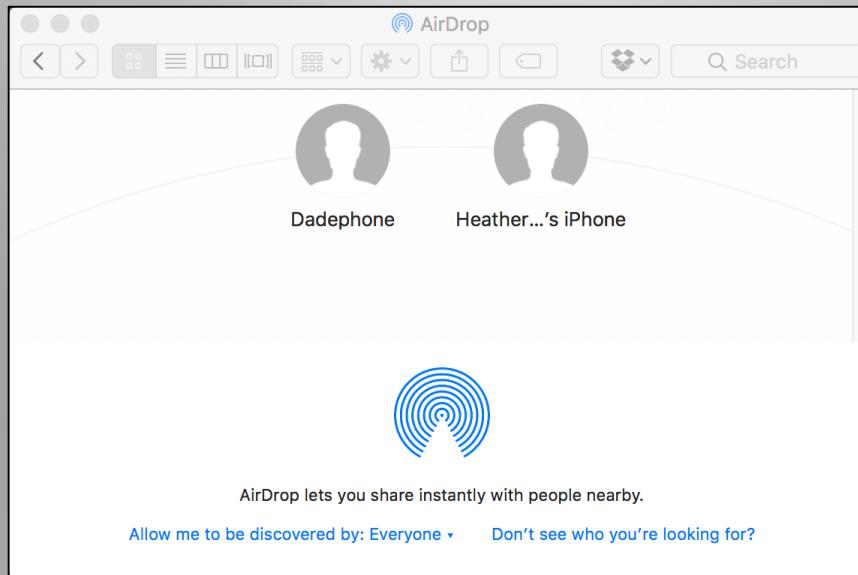
- MAC: ~/LIBRARY/PREFERENCES/BYHOST/COM.APPLE.SHARINGD.<HOST_UUID>.PLIST
- MAC: ~/LIBRARY/PREFERENCES/COM.APPLE.SHARINGD.PLIST - "DISCOVERABLEMODE"
- IOS: ~/LIBRARY/PREFERENCES/COM.APPLE.SHARINGD.PLIST



Key	Type	Value
▼ Root	Dictionary	(2 items)
AirDropID	String	6E732744D084
StreamID	String	41AFCDB030C8
AutoUnlockWatchCurrentlyInList	Boolean	YES
AutoUnlockWatchExistedInUnlockList	Boolean	YES
AutoUnlockPresentedBluetoothError	Boolean	NO
► EncryptionKeyRequests	Dictionary	(4 items)
► AutoUnlockPeerRetries	Dictionary	(1 item)
AutoUnlockSetupRetryVersion	Number	1
AutoUnlockLastSeenWatchDate	Date	Feb 6, 2017, 7:48:21 AM
DiscoverableMode	String	Contacts Only
AutoUnlockPresentedWiFiError	Boolean	NO

AIRDROP - DISCOVERY OF DEVICES (NO TRANSFER) - MAC UNIFIED LOGS

- JUST OPENING THE FINDER “AIRDROP” WINDOW
- TWO DEVICES FOUND:
 - DADEPHONE
 - HEATHER MAHALIK’S IPHONE



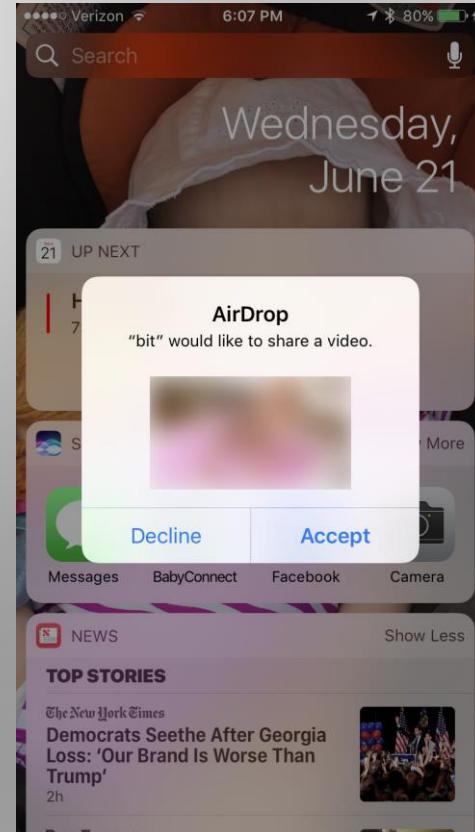
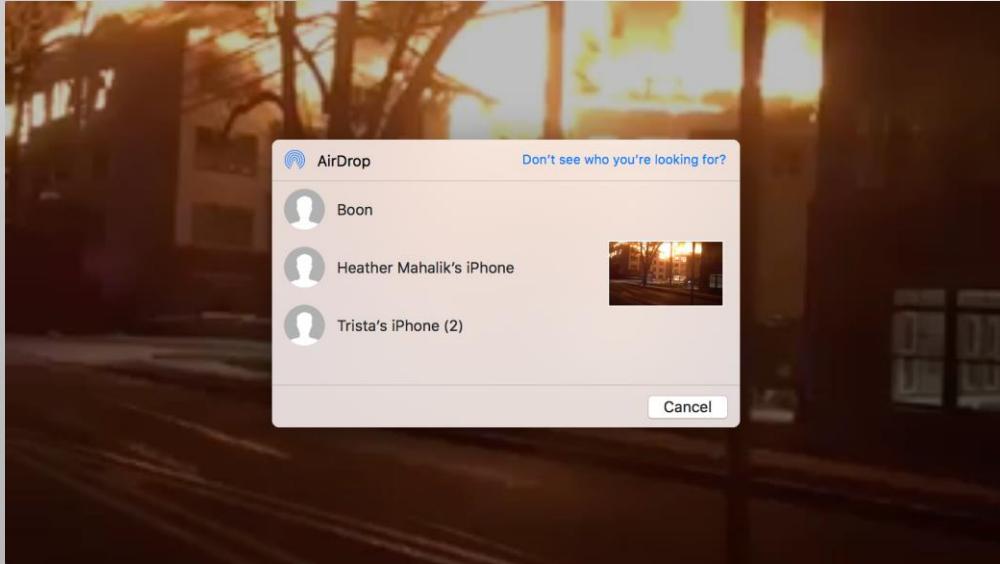
AIRDROP - DISCOVERY OF DEVICES (NO TRANSFER) - MAC UNIFIED LOGS

SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP SERVER INITIALIZED
SHARINGD: [COM.APPLE.SHARING.AIRDROP] FINDER ENTERED AIRDROP
SHARINGD: [COM.APPLE.SHARING.AIRDROP] BTLE SCANNING STARTED
SHARINGD: [COM.APPLE.SHARING.AIRDROP] SCANNING MODE CONTACTS ONLY
MDNSRESPONDER: [COM.APPLE.MDNSRESPONDER.ALLINFO] 66:
DNSSERVICECREATECONNECTION START PID[359] (**SHARINGD**)
MDNSRESPONDER: (AWDL_D2D) **AWDL**D2D AWDLD2DSTARTBROWSINGFORKEY: '_AIRDROP'
BROWSING SERVICE STARTED
SHARINGD: [COM.APPLE.SHARING.AIRDROP] BONJOUR DISCOVERY STARTED
SHARINGD: [COM.APPLE.SHARING.AIRDROP] BTLE SCANNER POWERED ON
FINDER: (SHARING) [COM.APPLE.SHARING.BROWSER] SFROWSERCALLBACK (NODE =
<SFNODE 0X6000000EF880>{DOMAIN = AIRDROP})
SHARINGD: [COM.APPLE.SHARING.NETWORKING.FUNCTIONAL] COM.APPLE.SHARINGD
NO AIRDROP PEOPLE DISCOVERED AFTER 8 SECONDS

AIRDROP - DISCOVERY OF DEVICES (NO TRANSFER) - MAC UNIFIED LOGS

```
SHARINGD: [COM.APPLE.SHARING.AIRDROP] BONJOUR DISCOVERED ED2AB55F0119 OVER AWDL0 IN 9217 MS
MDNSRESPONDER: [COM.APPLE.MDNSRESPONDER.ALLINFO] 66: DNSSERVICEQUERYRECORD(104100, 12,
    ED2AB55F0119._AIRDROP._TCP.LOCAL., TXT) START PID[359] (SHARINGD)
SHARINGD: [COM.APPLE.SHARING.AIRDROP] BONJOUR RESOLVED ED2AB55F0119 OVER AWDL0
MDNSRESPONDER: (AWDL_D2D) AWDLD2D AWDLD2DSTARTBROWSINGFORKEY: 'DADEPHONE' BROWSING SERVICE
    STARTED
SHARINGD: [COM.APPLE.SHARING.AIRDROP] DISCOVERED VERIFIABLE IDENTITY OF ED2AB55F0119 IN 5202 MS
SHARINGD: [COM.APPLE.SHARING.AIRDROP] BONJOUR DISCOVERED 771DAA6859EF OVER AWDL0 IN 14655 MS
MDNSRESPONDER: [COM.APPLE.MDNSRESPONDER.ALLINFO] 66: DNSSERVICEQUERYRECORD(104100, 12,
    771DAA6859EF._AIRDROP._TCP.LOCAL., TXT) START PID[359] (SHARINGD)
MDNSRESPONDER: (AWDL_D2D) AWDLD2D AWDLD2DSTOPBROWSINGFORKEY: 'HEATHER-MAHALIKS-IPHONE' BROWSING
    SERVICE STOPPED
FINDER: (SHARING) [COM.APPLE.SHARING.BROWSER] (
    "<SFNODE 0X6080002F8800>{DADEPHONE, ID = ED2AB55F0119, USER = IPHONE, ICON = 972674}",
    "<SFNODE 0X6080006FFD00>{HEATHER MAHALIK\u2019S IPHONE, ID = 771DAA6859EF, USER = (NULL),
    ICON = 972674}"
)
```

AIRDROP - FILE TRANSFER TO IPHONE FROM MAC



AIRDROP - FILE TRANSFER (IPHONE TO MAC) - MAC UNIFIED LOGS

```
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP SERVER ENABLED ON PORT 8770
SHARINGD: [COM.APPLE.SHARING.AIRDROP] NEW AIRDROP CONNECTION
SHARINGD: (CFNETWORK) TCP CONN 0X7FBCC300B9E0 STARTED
SHARINGD: (CFNETWORK) TCP CONN 0X7FBCC300B9E0 STARTING SSL NEGOTIATION
SHARINGD: (CFNETWORK) TCP CONN 0X7FBCC300B9E0 SSL HANDSHAKE DONE
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP RECEIVED DISCOVERY REQUEST
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP SERVER TRANSACTION BEGIN (1)
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP RECEIVED ASK REQUEST
SHARINGD: [COM.APPLE.SHARING.AIRDROP] POSTING <NSUSERNOTIFICATION:0X7FBCC3411B00> { TITLE:
"AIRDROP" INFORMATIVETEXT: "RECEIVING VIDEO FROM \"MIPHONE7\"" ACTIONBUTTONTITLE: "(NULL)"
OTHERBUTTONTITLE: "CANCEL" IDENTIFIER: 177E31AF-C280-449F-8B44-C05045F3242C } TO
<NSCONCRETEUSERNOTIFICATIONCENTER: 0X7FBCC0C1D510>
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP RECEIVED UPLOAD REQUEST
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP IS USING ADAPTIVE COMPRESSION
SHARINGD: [COM.APPLE.SHARING.DAEMON] SFOPERATIONCALLBACK (<0X7FBCC3090D10>{KIND = RECEIVER},
EVENT = PROGRESS, RESULTS = 0X7FBCC347EC80)
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP SERVER TRANSACTION END (0)
SHARINGD: [COM.APPLE.SHARING.AIRDROP] CONNECTION FROM ED2AB55F0119 CLOSED
FINDER: (SHARING) SFOPERATIONCALLBACK (<PRIVATE>, EVENT = FINISHED, RESULTS = <PRIVATE>)
```

AIRDROP - FILE TRANSFER (TO) - DIRECTORY / PERMISSIONS / TIMESTAMPS

- FILES GET DOWNLOADED TO DEFAULT DOWNLOADS DIRECTORY (~/DOWNLOADS)
- AIRDROP TRANSFER KEEPS SOME ORIGINAL DEVICE ACCESS/MODIFY TIMESTAMPS
- PERMISSIONS MAY SHOW “ACCESS_BPF” AS OWNERSHIP GROUP

```
[bit:Downloads oompa$ stat -x IMG_1442.MOV
File: "IMG_1442.MOV"
Size: 91427908      FileType: Regular File
Mode: (0644/-rw-r--r--)          Uid: (  501/    oompa)  Gid: (  501/access_bpf)
Device: 1,4   Inode: 17196622   Links: 1
Access: Thu Jun 15 18:03:37 2017
Modify: Thu Jun 15 18:03:37 2017
Change: Sun Jun 18 16:35:13 2017
```

AIRDROP - FILE TRANSFER (TO) - EXTENDED ATTRIBUTES / SPOTLIGHT

- COM.APPLE.METADATA:KMDITEMWHEREFROMS - SHOWS WHO/HOSTNAME WHERE IT CAME FROM (IE: SARAH EDWARDS, 'MIPHONE7')
- COM.APPLE.QUARANTINE - MAY SHOW IT CAME FROM 'SHARINGD' PROCESS, DATE AIRDROPPED, QUARANTINE GUID. IF VIDEO IS VIEWED, THIS MAY BE UPDATED (IE: VIEWER LIKE QUICKTIME PLAYER)

```
bit:Downloads oompa$ xattr -xl IMG_1442.MOV
com.apple.metadata:kMDItemWhereFroms:
00000000 62 70 6C 69 73 74 30 30 A2 01 02 5D 53 61 72 61 |bplist00...|Sara|
00000010 68 20 45 64 77 61 72 64 73 58 6D 69 50 68 6F 6E |h EdwardsXmiPhon|
00000020 65 37 08 0B 19 00 00 00 00 00 00 01 01 00 00 00 |e7.....|
00000030 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000040 00 00 00 00 22 |....|
00000045
com.apple.metadata:kMDLabel_r6hlhm73c2owhai3h2gch5251a:
00000000 F2 6E C6 FD 59 BB 0B 5A 71 F3 CD 29 4D 1E 39 57 |.n..Y..Zq..)M.9W|
00000190 4E 5B 72 DF 23 4C CA 44 58 50 F3 6C BB D0 2B 56 |N[r.#L.DXP.I..+V|
000001A0 02 00 AF 56 F3 DA D6 17 84 |....V.....|
000001a9
com.apple.quarantine:
00000000 30 30 38 31 3B 35 39 34 36 65 62 33 66 3B 73 68 |0081;5946eb3f;sh|
00000010 61 72 69 6E 67 64 3B 44 46 33 30 34 36 44 34 2D |aringd;DF3046D4-|
00000020 33 46 35 39 2D 34 41 35 46 2D 41 33 36 43 2D 37 |3F59-4A5F-A36C-7|
00000030 31 41 46 30 37 39 39 37 41 42 37 |1AF07997AB7|
0000003b
```

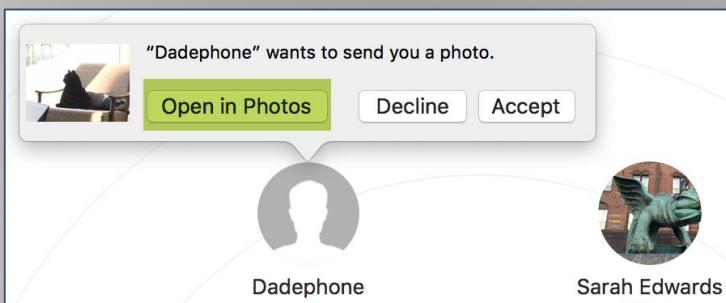
AIRDROP - FILE TRANSFER (TO) - QUARANTINE DATABASE

- `~/LIBRARY/PREFERENCES/COM.APPLE.LAUNCHSERVICES.QUARANTINEEVENTSV2`
 - GUID SHOWN IN QUARANTINE EXTENDED ATTRIBUTE
 - WHEN IT WAS AIRDROPPED (MAC EPOCH)
 - WHERE IT CAME FROM (SHARINGD)
 - WHO SENT IT (SARAH EDWARDS)

	LSQuarantineEventIdentifier	LSQuarantineTimeStamp	LSQuarantineAgentBundleIdentifier	LSQuarantineAgentName	LSQuarantineDataURLString	LSQuarantineSenderName	LSQuarantineSenderAddress	LSQuarantineTypeNumber
1	1728DFEE-BBDD-4AB7-...	519425134.856411	com.apple.iChat	iChat	NULL	NULL	NULL	3
2	61BF37FA-B8D7-4E46-...	519498761.0	com.google.Chrome	Google Chrome.app	https://github-productio...	NULL	NULL	0
3	23B510BB-D128-4552-...	519510843.197536	NULL	sharingd	NULL	Sarah Edwards	NULL	6
4	9A72A23D-225B-4858-...	519510912.485851	NULL	sharingd	NULL	Sarah Edwards	NULL	6
5	DF3046D4-3F59-4A5F...	519512767.901828	NULL	sharingd	NULL	Sarah Edwards	NULL	6

AIRDROP - FILE TRANSFER (TO) - ~/LIBRARY/CACHES/CLEANUP AT STARTUP/

- UNKNOWN USERS, AIRDROP SET TO “EVERYONE”
- ‘ACCEPT’:
 - DEFAULT DOWNLOADS DIRECTORY
- ‘OPEN IN PHOTOS’:
 - ‘CLEANUP AT STARTUP/’



```
[bit:Cleanup At Startup oompa$ pwd  
/Users/oompa/Library/Caches/Cleanup At Startup  
[bit:Cleanup At Startup oompa$ ls -laR  
total 16  
drwx-----@ 5 oompa staff 170 Jun 18 19:11 .  
drwx-----+ 102 oompa staff 3468 Jun 18 19:07 ..  
-rw-r--r--@ 1 oompa staff 6148 Jun 18 19:11 .DS_Store  
drwxr-xr-x 3 oompa staff 102 Jun 18 19:11 5453CE6C-E443-4E02-AA50-2C6C839D6747  
drwxr-xr-x 5 oompa staff 170 Jun 18 19:07 C6FA490C-D1CA-4DCC-886B-C9C83DC4B30E  
  
. /5453CE6C-E443-4E02-AA50-2C6C839D6747:  
total 1232  
drwxr-xr-x 3 oompa staff 102 Jun 18 19:11 .  
drwx-----@ 5 oompa staff 170 Jun 18 19:11 ..  
-rw-r--r--@ 1 oompa access_bpf 629552 Jun 11 18:12 IMG_0005.JPG  
  
. /C6FA490C-D1CA-4DCC-886B-C9C83DC4B30E:  
total 2024  
drwxr-xr-x 5 oompa staff 170 Jun 18 19:07 .  
drwx-----@ 5 oompa staff 170 Jun 18 19:11 ..  
-rw-r--r--@ 1 oompa access_bpf 100105 Jun 11 17:44 IMG_0001.PNG  
-rw-r--r--@ 1 oompa access_bpf 86919 Jun 11 17:48 IMG_0002.PNG  
-rw-r--r--@ 1 oompa access_bpf 843358 Jun 11 19:21 IMG_0013.PNG  
[bit:Cleanup At Startup oompa$ xattr -xl 5453CE6C-E443-4E02-AA50-2C6C839D6747/IMG_0005.JPG  
com.apple.metadata:kMDItemWhereFroms:  
00000000 62 70 6C 69 73 74 30 30 A1 01 59 44 61 64 65 70 |bplist00..YDadep|  
00000010 68 6F 6E 65 08 0A 00 00 00 00 00 01 01 00 00 |hone.....|  
00000020 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 |.....|  
00000030 00 00 00 00 00 14 |.....|  
00000036
```

AIRDROP - FILE TRANSFER (FROM MAC TO IPHONE) - MAC UNIFIED LOGS

```
SHARINGD: [COM.APPLE.SHARING.AIRDROP] CONNECTING TO ED2AB55F0119 AT  
[MIPHONE7.LOCAL]:8770  
SHARINGD: [COM.APPLE.SHARING.AIRDROP] SENDING CLIENT CERTIFICATE TO ED2AB55F0119  
SHARINGD: [COM.APPLE.SHARING.AIRDROP] STARTING TO SEND FILES (  
"FILE:///FILE/ID=6571367.17174270" )  
SHARINGD: [COM.APPLE.SHARING.AIRDROP] 17174270 = File's Inode/CNID  
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP IS USING ADAPTIVE COMPRESSION  
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP SENDING OVER AWDL0  
SHARINGD: [COM.APPLE.SHARING.AIRDROP] STARTING TO SEND FILES (  
"FILE:///VAR/FOLDERS/N7/VNFZC155443_QG0ZP2CWZ1880000GN/T/COM.APPLE.PHOTOS/SHAREK  
IT-EXPORTS/1C200C5D-81C8-4C4D-96B1-67D078DC7198/3252/IMG_1438.JPG",  
"FILE:///VAR/FOLDERS/N7/VNFZC155443_QG0ZP2CWZ1880000GN/T/COM.APPLE.PHOTOS/SHAREK  
IT-EXPORTS/1C200C5D-81C8-4C4D-96B1-67D078DC7198/3254/IMG_1439.JPG"  
)
```

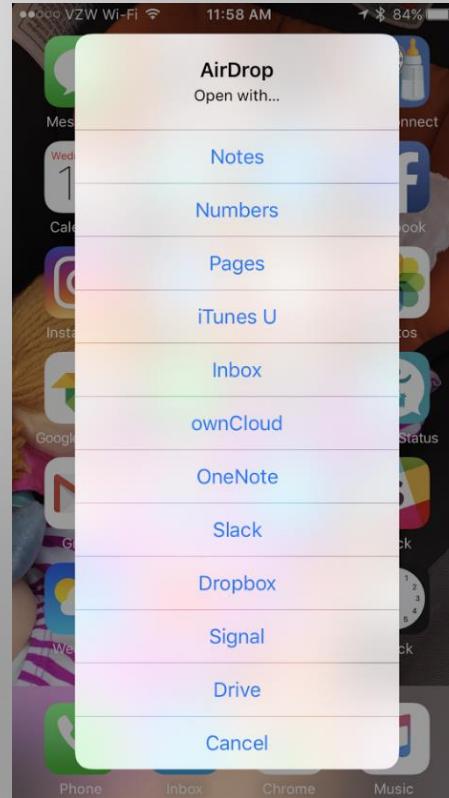
AIRDROP - IOS ARTIFACTS – PHONE BACKUP UNASSOCIATED DEVICES

- GIVEN OPTION TO ACCEPT OR DECLINE
- ‘ACCEPT’:
 - DEFAULT DCIM DIRECTORY FOR PICTURE OR VIDEO
 - OPTION TO OPEN FOR OTHER ATTACHMENTS
- ‘DECLINE’:
 - NO LOGS... 😞



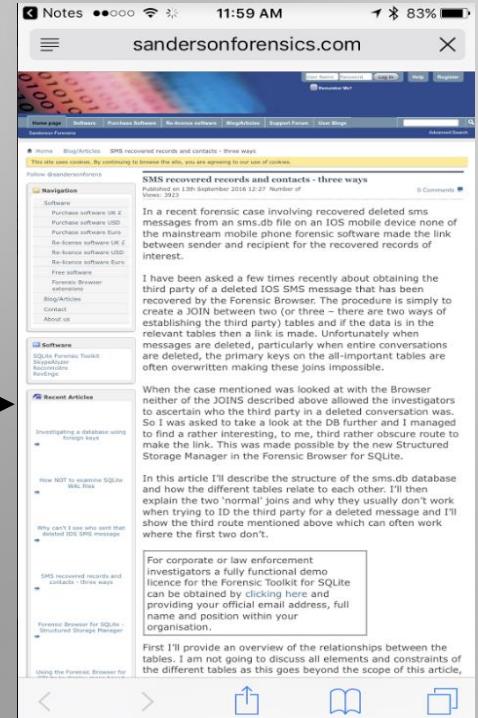
AIRDROP - IOS ARTIFACTS -PHONE BACKUP DEVICES ON SAME ICLOUD

- ‘ACCEPT’ (AUTOMATIC):
 - DEFAULT DCIM DIRECTORY FOR PICTURE OR VIDEO
 - OPTION TO OPEN FOR OTHER ATTACHMENTS
- NO OPTION TO DECLINE “DROP” WHEN BOTH DEVICES ARE ON THE SAME ICLOUD ACCOUNT



AIRDROP - IOS ARTIFACTS [1] – PHONE BACKUP

- TIME-LINING MAY BE POSSIBLE, BUT DIFFICULT
- IMAGES AND VIDEOS – IF YOU KNOW WHAT WAS DROPPED
 - TIMESTAMPS NOT ALWAYS IN TEMPORAL IN DCIM DIR IF FOLLOWING IMG_#### ORDER
- EXIF DATA NOT HELPFUL
- HOW WAS THE FILE ACCESSED BY THE USER? (YOU ARE NOW DESPERATE)
 - NATIVE APPS (NOTES)
 - SAFARI
 - THIRD - PARTY APPLICATIONS



AIRDROP - IOS ARTIFACTS [2] – PHONE BACKUP

- ~LIBRARY/DATABASES/DATAUSAGE.SQLITE

Table:  ZPROCESS

Z_PK	Z_ENT	Z_OPT	ZFIRSTTIMESTAMP	ZTIMESTAMP	ZBUNDLENAME	▲	ZPROCNAME
Fil...	Fil...	Fil...	Filter	Filter	datausage	✖	Filter
1	186	7	2424	453124545.171082	518472124.632133	com.apple.datausage.airdrop	sharingd/com.apple.datausage.airdrop
2	82	7	231	414816042.639162	518472125.09033	com.apple.datausage.appleid	AppleIDAuthAgent/com.apple.datausage.appleid
3	331	7	1246	496273311.670504	513554363.023668	com.apple.datausage.appleid	identityservicesd/com.apple.datausage.appleid
4	15	7	60703	401275316.417027	519237146.046816	com.apple.datausage.applepushservice	apsd/com.apple.datausage.applepushservice
5	119	7	47	432909486.968011	432918386.218557	com.apple.datausage.atc	nsurlsessiond/com.apple.datausage.atc
6	73	7	95	410818950.090341	466394367.037485	com.apple.datausage.backup	backupd/com.apple.datausage.backup
7	324	7	4512	495519880.562882	519237145.30366	com.apple.datausage.bluetooth	BTServer/com.apple.datausage.bluetooth

AIRDROP - DISCOVERY OF DEVICES - IOS LOGS – DYNAMIC ANALYSIS

```
SHARINGD[64] <NOTICE>: BTLE SCANNING STARTED
SHARINGD[64] <NOTICE>: SCANNING MODE EVERYONE
SHARINGD(WIRELESSPROXIMITY) [64] <NOTICE>: STATE CHANGED TO 3 FROM 0
SHARINGD(WIRELESSPROXIMITY) [64] <NOTICE>: ADVERTISER STATE CHANGED TO 3 FROM 0
SHARINGD(WIRELESSPROXIMITY) [64] <NOTICE>: STATE IS ON, ADDING SERVICES IF NECESSARY
SHARINGD[64] <NOTICE>: BTLE SCANNER POWERED ON

BT SERVER[5960] <NOTICE>: SCANNING STARTED SUCCESSFULLY
SHARINGD[64] <NOTICE>: BTLE SCANNING STOPPED
SHARINGD(WIRELESSPROXIMITY) [64] <NOTICE>: WPCLIENT (0X15904CA30 - WPAWDL) XPC CONNECTION
    INVALIDATED
SHARINGD(WIRELESSPROXIMITY) [64] <NOTICE>: STATE CHANGED TO 0 FROM 3
SHARINGD(WIRELESSPROXIMITY) [64] <NOTICE>: ADVERTISER STATE CHANGED TO 0 FROM 3
WIRELESSPROXD[60] <NOTICE>: WPDCLIENT XPC CONNECTION FOR PROCESS SHARINGD (64) IS BECOMING
    INVALIDATED
WIRELESSPROXD[60] <NOTICE>: REMOVING WPDCLIENT 19B28287-93F0-41B0-A968-62DD5FB14DA4 OF
    PROCESS SHARINGD (64)
```

AIRDROP - FILE TRANSFER (IPHONE TO IPHONE) [1] - IOS LOGS – DYNAMIC ANALYSIS

```
MOBILESLIDESHOW(SHARING) [13181] <NOTICE>: SFBROWERCALLBACK (NODE = <SFNODE 0X1746E5680>
{DOMAIN = AIRDROP})
MOBILESLIDESHOW(SHARING) [13181] <NOTICE>: ( "<SFNODE 0X1746E1880>{HEATHER MAHALIK, ID =
DE8110984FD3, DEVICE = (NULL) }")
SHARINGD[64] <NOTICE>: NEW AIRDROP CONNECTION
SHARINGD(CFNETWORK) [64] <NOTICE>: TCP CONN 0X1593A7C60 STARTED
SHARINGD(CFNETWORK) [64] <NOTICE>: TCP CONN 0X1593A7C60 STARTING SSL NEGOTIATION
SHARINGD(CFNETWORK) [64] <NOTICE>: TCP CONN 0X1593A7C60 SSL HANDSHAKE DONE
SHARINGD[64] <NOTICE>: AIRDROP SERVER TRANSACTION BEGIN (1)
SHARINGD[64] <NOTICE>: AIRDROP RECEIVED ASK REQUEST
SHARINGD[64] <NOTICE>: AIRDROP PARSING ASK REQUEST
SHARINGD[64] <NOTICE>: AIRDROP RECEIVED UPLOAD REQUEST
SHARINGD[64] <NOTICE>: AIRDROP IS USING ADAPTIVE COMPRESSION
SPRINGBOARD(COREMOTION) [7792] <NOTICE>: NOTIFY FROM, FACEUP -> PORTRAIT
SPRINGBOARD[7792] <NOTICE>: RECEIVED REQUEST TO ACTIVATE ALERTITEM: <SFALERTITEM:
0X1748C3FE0>
SPRINGBOARD[7792] <NOTICE>: ACTIVATION - PRESENTING <SFALERTITEM: 0X1748C3FE0> WITH
PRESENTER: <SBUNLOCKEDALERTITEMPRESENTER: 0X174212690>
```

AIRDROP - FILE TRANSFER (IPHONE TO IPHONE) [2] - IOS LOGS – DYNAMIC ANALYSIS

SHARINGD [64] <NOTICE>: **ACCEPTING TRANSFER** <SFAIRDROPTERNSFERDATA:
0X159341920> RECORDID: **5CF33654-103D-42D5-9F3C-927BFE023E1F**

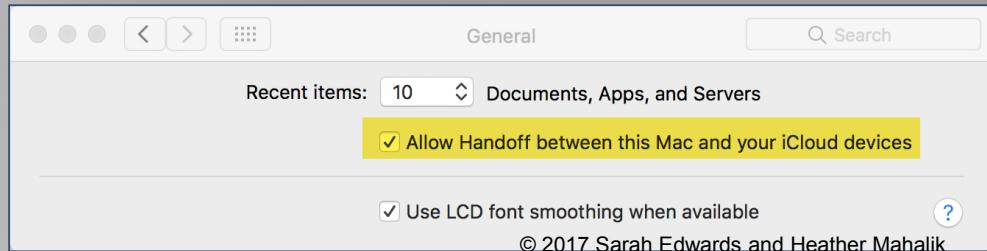
SHARINGD [64] <NOTICE>: AIRDROP **SERVER TRANSACTION END** (0)

SHARINGD (CFNETWORK) [64] <NOTICE>: TCP CONN 0X15932F560 CANCELED



HANOFF

- CONTINUE USING APPLICATIONS BETWEEN YOUR IPHONE AND MAC (AND VICE VERSA!)
 - MESSAGES, NOTES, BROWSERS, MAIL, MAPS, REMINDERS, CALENDAR, CONTACTS, PAGES, NUMBERS, KEYNOTE, AND THIRD-PARTY APPS!
- BLUETOOTH & WI-FI ENABLED
- SAME WI-FI NETWORK
- SAME ICLOUD ACCOUNTS
- HANOFF ENABLED



HANOFF FROM IPHONE TO MAC - MAC LOGS [1]

SHARINGD: [COM.APPLE.SHARING.HANOFF] SUCCESSFULLY DECRYPTED

ADVERTISEMENT (SHARING FLAGS + ADVERTISEMENTPAYLOAD) :

<B3A7F3448A2BCD1E7D46> => <008E6F4D00**476ED213EFA514018828558**

SHARINGD: [COM.APPLE.SHARING.HANOFF] RECEIVED A NEW ADVERTISEMENT

<SFACTIVITYADVERTISEMENT: 0X7FBCC0C86420, **DEVICEUNIQUEID:F9B85FFC-2BC6-4E80-93DA-67508472C8F8**, ADVERTISEMENTPAYLOAD:<**476ED213EFA5140188**>,
OPTIONS:{SFACTIVITYADVERTISEROPTIONFLAGCOPYPASTEKEY =
0;SFACTIVITYADVERTISEROPTIONMINORVERSIONKEY =
0;SFACTIVITYADVERTISEROPTIONVERSIONKEY = 0;}, **DEVICENAME:MIPHONE7**,
DEVICEMODELIDENTIFIER:IPHONE9,3>

HANOFF FROM IPHONE TO MAC - MAC LOGS [2]

```
USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANOFF] [SFCONTINUITYSCANMANAGER]
RECEIVED ADVERTISEMENT <SFACTIVITYADVERTISEMENT: 0X7FFC7AE219F0,
DEVICEIDENTIFIER:F9B85FFC-2BC6-4E80-93DA-675084
DOCK: (USERACTIVITY) [COM.APPLE.USERACTIVITY.MAIN]
NOTIFYBESTAPPCHANGED:B81C0F47-0724-4E2B-966C-67C9E2FBA669 USERACTIVITY
<PRIVATE>/<PRIVATE> OPTS={
    SFACTIVITYADVERTISEROPTIONFLAGCOPYPASTEKEY = 0;
    SFACTIVITYADVERTISEROPTIONMINORVERSIONKEY = 0;
    SFACTIVITYADVERTISEROPTIONVERSIONKEY = 0;
USERACTIVITYHASWEBPAGEURL = 1;
} WHEN=2017-06-17 20:53:38 +0000 CONFIDENCE=1 FROM=<PRIVATE>/<PRIVATE>
```

```
BIRD: (CLOUDDOCSDAEMON) [COM.APPLE.CLOUDDOCS.DEFAULT] [INFO] ↳172 <PRIVATE>
(<PRIVATE>) - [BRCXPCREGULARIPCSCLIENT
DIDRECEIVEHANOFFREQUESTFORBUNDLEID:REPLY:] ↳172 <PRIVATE>
```

HANOFF FROM IPHONE TO MAC - MAC LOGS [3]

- BROWSING IN SAFARI ON IPHONE, WHILE MACBOOK PRO IS LOGGED IN
- WILL OPEN SAFARI LINK IN DEFAULT WEB BROWSER ON MAC - CHROME!
- NOTE: HANOFF WAS NOT COMPLETED - ACTIVITY JUST HAPPENS IN THE BACKGROUND.



HANOFF FROM IPHONE TO MAC - MAC LOGS (LINK CLICKED) [1]

USERACTIVITYD: [COM.APPLE.USERACTIVITY.MAIN] QUEUING FETCH FOR BESTAPPUUID
009DBBD2-A6F6-4A2E-A5CE-46BD46B90108

USERACTIVITYD: [COM.APPLE.USERACTIVITY.MAIN] -- ACTIVITY WITH UUID 009DBBD2-
A6F6-4A2E-A5CE-46BD46B90108, **SO FETCHING PAYLOAD FOR IT.**

USERACTIVITYD: [COM.APPLE.USERACTIVITY.MAIN] **REQUESTING PAYLOAD** FOR ITEM
009DBBD2-A6F6-4A2E-A5CE-46BD46B90108 ADVERTISEMENTPAYLOAD=**41E36BAF264809**
BUNDLEIDENTIFIER=<PRIVATE>

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANOFF] [SFCONTINUITYSCANMANAGER]
DISPATCHING PAYLOAD REQUEST TO F9B85FFC-2BC6-4E80-93DA-67508472C8F8 FOR
<41E36BAF264809>

SHARINGD: [COM.APPLE.SHARING.HANOFF] **REQUESTING HANDOFF PAYLOAD** FOR
<41E36BAF264809> WITH MESSAGE GUID: AE52B945-31A6-4ABC-8698-F0951E720ACB

HANOFF FROM IPHONE TO MAC - MAC LOGS (LINK CLICKED) [2]

SHARINGD: (IDS) [**COM.APPLE.TRANSPORT.IDS CONNECTION**] CLIENT REQUEST TO SEND PROTOBUF ON SERVICE: **COM.APPLE.PRIVATE.ALLOY.CONTINUITY.ACTIVITY** GUID: AE52B945-31A6-4ABC-8698-F0951E720ACB TO DESTINATIONS: <PRIVATE> OPTIONS: <PRIVATE> **SIZE: 107** (1 PENDING)

IDENTITYSERVICESD: (WIRELESSPROXIMITY) [**COM.APPLE.BLUETOOTH.WIRELESSPROXIMITY**] **CONTINUITY CONNECT TO PEER: F768D25B-1EC8-476B-B4A3-D757890CD2E8**

GOOGLE CHROME: (COREFOUNDATION) [**COM.APPLE.CFPASTEBOARD.ENTRY**] **_COPYDATA('APPLE CFPASTEBOARD FIND' GEN: 215 ITEM: 789514 FLAVOR: 'PUBLIC.UTF8-PLAIN-TEXT')** CURRENT-GEN: 215

SHARINGD: [**COM.APPLE.SHARING.HANOFF**] **RECEIVED REQUESTED HANOFF PAYLOAD FROM "MIPHONE7" (F9B85FFC-2BC6-4E80-93DA-67508472C8F8)** FOR <**41E36BAF264809**> WITH ACTIVITY PAYLOAD OF SIZE 162 FOR REQUESTIDENTIFIER AE52B945-31A6-4ABC-8698-F0951E720ACB ((NULL)). RTT:2S944MS

HANOFF FROM IPHONE TO MAC - MAC LOGS - OTHER APPS

- **LOOK WITHIN CONTEXT!**

NOTES: (LIBSYSTEM_TRACE.DYLIB) SUBSYSTEM: **COM.APPLE.NOTES**, CATEGORY: **HANOFF**, ENABLE_LEVEL: 3, PERSIST_LEVEL: 3, DEFAULT_TTL: 0, INFO_TTL: 0, DEBUG_TTL: 0, GENERATE_SYMPTOMS: 0, ENABLE_OVERSIZE: 0, PRIVACY_SETTING: 2, ENABLE_PRIVATE_DATA: 0

REMINDERS: (COREFOUNDATION) **_COPYDATA**

MAIL: (COREFOUNDATION) **_COPYDATA**

MAPS: (COREFOUNDATION) **_COPYDATA**

NUMBERS: (COREFOUNDATION) **_COPYDATA**

HANOFF FROM MAC TO IPHONE - MAC LOGS [1]

MAPS: (CORESPOTLIGHT) [COM.APPLE.CORESPOTLIGHT.DEFAULT] CREATED UA ITEM,
IDENTIFIER:<PRIVATE>, SHOULDINDEX:YES, TITLE:"<PRIVATE>",
USERACTIVITYTYPE:COM.APPLE.MAPS, BUNDLEID:COM.APPLE.MAPS

SHARINGD: [COM.APPLE.SHARING.HANOFF] REQUEST TO ADVERTISE
<**A0ED1D839414C8008D**> WITH OPTIONS
{SFACTIVITYADVERTISEROPTIONFLAGCOPYPASTEKEY = 0; }

SHARINGD: [COM.APPLE.SHARING.HANOFF] **RECEIVED HANOFF PAYLOAD REQUEST FROM "MIPHONE7" (F9B85FFC-2BC6-4E80-93DA-67508472C8F8)** WITH REQUESTIDENTIFIER
9D4DEC8C-54FB-4B9D-94C1-3AF0143AD42B COMMAND=HANOFF FOR
ADVERTISEMENTPAYLOAD <**A0ED1D839414C8**>

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANOFF] [SFACITIVITYADVERTISER]
RECEIVED PAYLOAD REQUEST FROM <SFPEERDEVICE: 0X7FFC7AF83D40,
UNIQUEID:F9B85FFC-2BC6-4E80-93DA-67508472C8F8, MODELIDENTIFIER:IPHONE9,3,
NAME :MIPHONE7> FOR <**A0ED1D839414C8**>

HANOFF FROM MAC TO IPHONE - MAC LOGS [2]

SHARINGD: [COM.APPLE.SHARING.HANOFF] **READY TO RESPOND TO HANOFF** REQUEST FROM "MIPHONE7" (F9B85FFC-2BC6-4E80-93DA-67508472C8F8) WITH REQUESTIDENTIFIER 9D4DEC8C-54FB-4B9D-94C1-3AF0143AD42B FOR ADVERTISEMENTPAYLOAD <A0ED1D839414C8>, COMMAND: HANOFF. RTT:3MS

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANOFF] [SFACTIVITYADVERTISER] **RECEIVED PAYLOAD REQUEST** FROM <SFPEERDEVICE: 0X7FFC7AF83D40, UNIQUEID:F9B85FFC-2BC6-4E80-93DA-67508472C8F8, MODELIDENTIFIER:IPHONE9,3, NAME:MIPHONE7> FOR <A0ED1D839414C8>. HANDLED: YES

BIRD: (CLOUDDOCSDAEMON) [COM.APPLE.CLOUDDOCS.DEFAULT] [INFO] ↳27C <PRIVATE> (<PRIVATE>) - [BRCXPREGULARIPCSCLIENT DIDRECEIVEHANOFFREQUESTFORBUNDLEID:REPLY:]

SHARINGD: [COM.APPLE.SHARING.HANOFF] **REQUESTING HANOFF ENCRYPTION KEY FROM "MIPHONE7"**

IOS APPLE PAY ARTIFACTS

PAY FOR ITEMS USING SAFARI BY USING YOUR IPHONE TOUCHID OR APPLE WATCH

- /COM.APPLE.MOBILESAFARI/LIBRARY/SAFARI/HISTORY.DB
 - VERIFY ORIGIN COLUMN (ON DEVICE OR NOT)
 - 1= VISITED FROM ANOTHER SYSTEM, 0= ON DEVICE

900	https://www.etsy.com/
901	http://etsy.com/
902	https://www.etsy.com/shop/TinyVibesBoutique?ref=search_shop_redirect
903	https://www.etsy.com/search?q=tiny%20vibes%20boutique
904	https://www.etsy.com/signin?workflow=ZmF2b3JpdGVfdXNlcI9pZDo4MDM1OTA2NDoxNDk3MzE2MTA4OjFiMWI0MmVmMjkwYW
905	https://www.etsy.com/listing/535258907/tiny-vibes-lemon-yellow-maxi-bows?ref=shop_home_active_7
906	https://www.etsy.com/cart?ref=hdr
907	https://www.etsy.com/cart/listing.php
908	https://www.etsy.com/cart/?show_cart=1299846552
909	https://www.etsy.com/cart/1299846552/checkout/?guest=1&payment_method=apple_pay
910	https://www.etsy.com/join/email?from_action=checkout&from_page=https%3A%2F%2Fwww.etsy.com%2Fcart%2F1299846552
911	https://www.etsy.com/signin?from_action=checkout&from_page=https%3A%2F%2Fwww.etsy.com%2Fcart%2F1299846552

- var/mobile/Library/Mail/recents



```
corerecents:frombplist00.....Waddress  
Tkind[displayName_..transaction@etsy.co  
mUemail_..Etsy Transactions .. (?E...  
.....Y.....?x.  
.corerecents:reference-urlbplist00 ..Jme  
ssage:%3C201706130053.v5D0renD156524@pa  
yments-dsworker02.ny5.etsy.com%3E.....  
.....U}..^..3.P..  
corerecents:subjectbplist00 ..6Your Etsy  
Purchase from TinyVibesBoutique (12033  
87156) ..A.....A
```

AUTO UNLOCK

- UNLOCK YOUR MAC WITH YOUR APPLE WATCH
- DEVICES MUST BE USING SAME ICLOUD ACCOUNT
- TWO-FACTOR AUTHENTICATION ENABLED FOR ICLOUD ACCOUNT
- PASSWORD/PASSCODE ON EACH DEVICE
- BLUETOOTH/WI-FI ENABLED (DOES NOT HAVE TO BE ON WI-FI NETWORK)



Security & Privacy

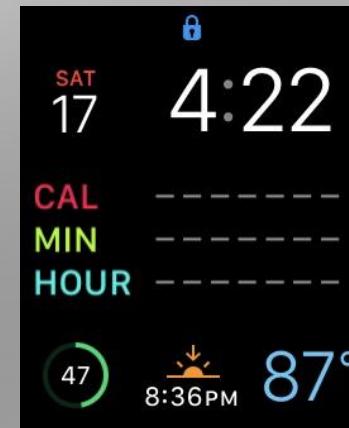
General FileVault Firewall Privacy

A login password has been set for this user [Change Password...](#)

Require password after sleep or screen saver begins

Show a message when the screen is locked [Set Lock Message...](#)

Allow your Apple Watch to unlock your Mac



AUTO UNLOCK - MAC UNIFIED LOGS

- LOOK FOR THE FOLLOWING ENTRIES:

AKD: (AUTHKIT) [COM.APPLE.AUTHKIT.CORE] MKB REPORTED LOCK STATE: #

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] KEYBAG STATE CHANGED #

- DEVICE LOCK STATES:

- “2”: LOCKING DEVICE
- “1”: DEVICE IS LOCKED
- “0”: **DEVICE IS UNLOCKED**

- WILL NEED TO LOOK CLOSER TO SEE IF SPECIFICALLY UNLOCKED WITH APPLE WATCH

- “COM.APPLE.SHARING.AUTOUNLOCK”...BUT ALSO:

- COM.APPLE.BLUETOOTH.WIRELESSPROXIMITY
- COM.APPLE.SHARING.SDNEARBYAGENTCORE
- COM.APPLE.SHARING.HANDOFF
- AND MORE!

AUTO UNLOCK - MAC UNIFIED LOGS

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] HINTS PROVIDER ACTIVATED FOR USER:
OOMPA

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] AUTOMATION: ATTEMPT START

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] **BEGIN AUTO UNLOCK:** 15:00:00.651

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] LAST MACHINE WAKE DATE 2017-06-17
18:49:00 +0000

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] TRYING TO USE CACHED DEVICE:
<SFAUTOUNLOCKDEVICE: 0X7FBCC0F6A810, UNIQUEID:47B476E2-6B76-4D3D-B078-
A24305AF1A21, BLUETOOTH ID:C905A733-BEA0-4680-A41F-4DCDF577A099, CLOUD
PAIRED: YES, MODELIDENTIFIER:WATCH2,3, NAME:MIWATCH, UNLOCKENABLED: YES>

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] SCANNING FOR BLUETOOTH IDS { (
F768D25B-1EC8-476B-B4A3-D757890CD2E8,
C905A733-BEA0-4680-A41F-4DCDF577A099
) }

AUTO UNLOCK - MAC UNIFIED LOGS

```
SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] RETURNING HINTS DICTIONARY {  
    1 = OOMPA;  
    5 = "UNLOCKING WITH APPLE WATCH\U2026";  
}
```

```
SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] FOUND PEER:  
    DEVICE <NAME:MIWATCH, UNIQUEID:47B476E2-6B76-4D3D-B078-A24305AF1A21,  
    BLUETOOTH ID:C905A733-BEA0-4680-A41F-4DCDF577A099,  
MODELIDENTIFIER:WATCH2,3,  
    PEER <SFBLEDEVICE ID C905A733-BEA0-4680-A41F-4DCDF577A099, ADVDATA  
    '0180', RSSI -39, 0, [-39], NAME '?', PAIRED NO>,  
UNLOCK ENABLED: YES,  
    PROXY UNLOCK ENABLED: NO,  
LOCKED ON WRIST: NO
```

AUTO UNLOCK - MAC UNIFIED LOGS

- LOCALLY ADMINISTERED MAC ADDRESS SPACE (SIMILAR TO PRIVATE IP SPACE)
- IF FIRST OCTET'S SECOND CHARACTER = (2, 6, A, E) = LOCALLY ADMINISTERED SPACE
 - RANDOMIZED MAC ADDRESS WHEN WORKING WITH APPLE DEVICES
- **3E:C2:D8:12:E5:21** = NOT THE PERMANENT MAC ADDRESS OF THE APPLE WATCH

SHARINGD: (**CORELOCATION**) [COM.APPLE.LOCATIOND.POSITION.PROXIMITY] WRTT:
RECEIVED ONCLIENTEVENTPEERRANGING

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] CL **COMPLETED RANGING:** (

"PEER: **3E:C2:D8:12:E5:21** TIME:2017-06-17 19:00:02 +0000

DISTANCE [M]:1000.00 ACCURACY [M]:0.00 UNLOCK:YES SECURE:YES

INITIATOR:NO"

)

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] PEER IN RANGE

SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] **AKS UNLOCK SUCCEEDED**

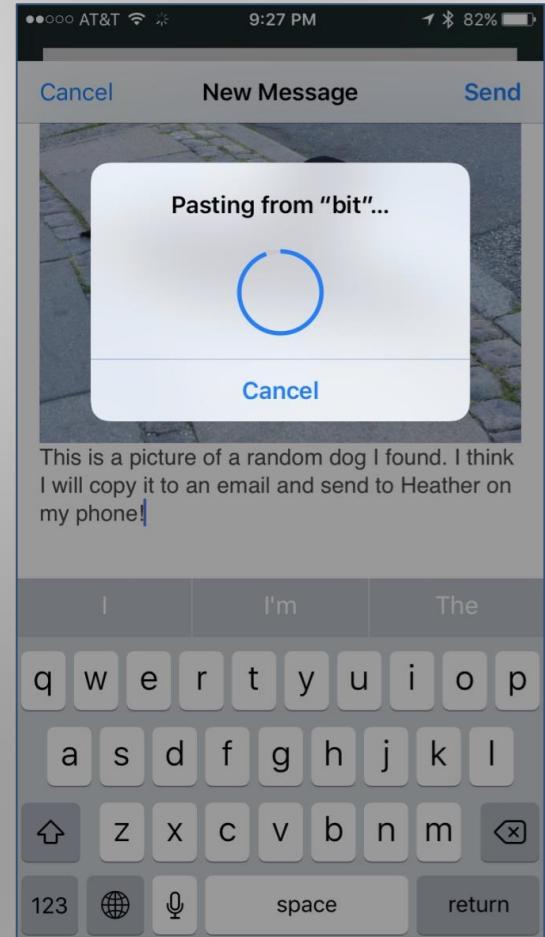
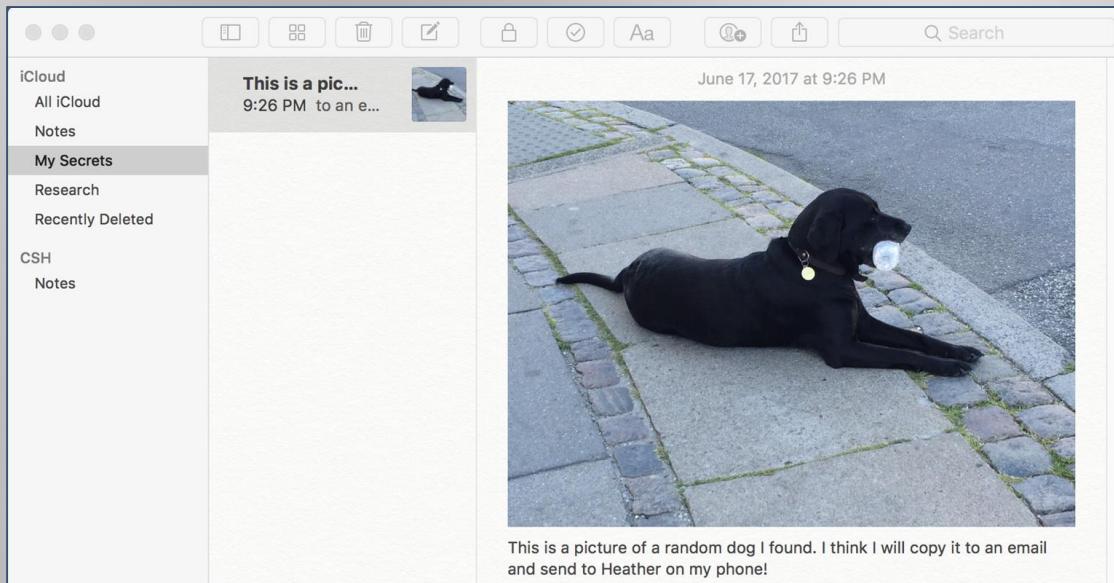
SHARINGD: [COM.APPLE.SHARING.AUTOUNLOCK] **KEYBAG STATE CHANGED 0**

AUTO UNLOCK - LOG CAVEATS

- UNIFIED LOGS
 - MANY, MANY, MANY MORE RELATED LOG ENTRIES!
- BSM AUDIT LOGS
 - DOES NOT GET RECORDED LIKE A LOGIN TYPED IN VIA 'LOGINWINDOW'.
- SYSTEM.LOG
 - LOGIN/LOGOUT ACTIVITY APART FROM BOOT/REBOOT LOGINS DOES NOT GET RECORDED.

UNIVERSAL CLIPBOARD

- COPY AND PASTE ACROSS DEVICES.
- VERY SIMILAR TO HANDOFF!



UNIVERSAL CLIPBOARD - MAC LOGS (MAC TO IPHONE)

USERACTIVITYD: [COM.APPLE.USERACTIVITY.PASTEBOARD-SERVER] [PBOARD] PASTE REQUESTED

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANOFF] [SFACTIVITYADVERTISER]
RECEIVED PAYLOAD REQUEST FROM <SFPEERDEVICE: 0X7FFC7AE18900,
UNIQUEID:F9B85FFC-2BC6-4E80-93DA-67508472C8F8, MODELIDENTIFIER:IPHONE9,3,
NAME:MIPHONE7> FOR <7062706173746521>. HANDLED: YES

PBOARD: (COREFOUNDATION) PROVIDE REMOTE PASTEBOARD DATA

PBOARD: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.REMOTE] REMOTE PASTEBOARD
FETCHING LOCAL DATA FOR PROVIDER: (UUID:BF70B19C-4610-403F-A45B-F5C42120E988
GEN: 111 ITEM: 789514 FLAVOR: 'COM.APPLE.FLAT-RTFD')

UNIVERSAL CLIPBOARD - MAC LOGS (IPHONE TO MAC)

PBOARD: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.REMOTE] REMOTE PASTEBOARD
BECAME AVAILABLE

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANOFF] [SFCONTINUITYSCANMANAGER]
DISPATCHING PAYLOAD REQUEST TO F9B85FFC-2BC6-4E80-93DA-67508472C8F8 FOR
<7062747970657321>

PBOARD: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.REMOTE] REMOTE METADATA FETCH
RECEIVED 2 ITEMS

PBOARD: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.REMOTE] PROMISED REMOTE DATA
FOR 'APPLE CFPASTEBOARD REMOTE' ITEM: 1 **FLAVOR: 'PUBLIC.JPEG'** PROVIDER:
METADATA RESULT: 0

PBOARD: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.ENTRY] _PROMISEDATA('APPLE
CFPASTEBOARD REMOTE' GEN: 120 ITEM: 1 **FLAVOR:**
'COM.APPLE.MOBILESLIDESHOW.ASSET.LOCALIDENTIFIER' CONTEXT: (METADATA)
NOTIFYSERVER: 0)

UNIVERSAL CLIPBOARD - MAC LOGS (IPHONE TO MAC)

TEXTEDIT: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.EXIT] NOT SETTING FLAGS FOR
'APPLE CFPASTEBOARD GENERAL' - HAS PENDING REMOTE PASTEBOARD - GEN: -1 ITEM:

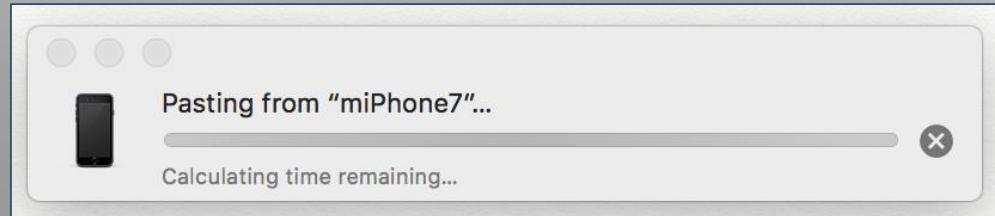
2 FLAVOR: COM.APPLE.QUICKTIME-MOVIE

UASHAREDPASTEBOARDPROGRESSUI: [COM.APPLE.USERACTIVITY.SPBPRESSUI]
[SHARED PASTEBOARD PROGRESSUI] **SHOWING PROGRESS UI**

USERACTIVITYD: [COM.APPLE.USERACTIVITY.PASTEBOARD-SERVER] [**IN STREAM**] STARTED
RECEIVING DATA FILE

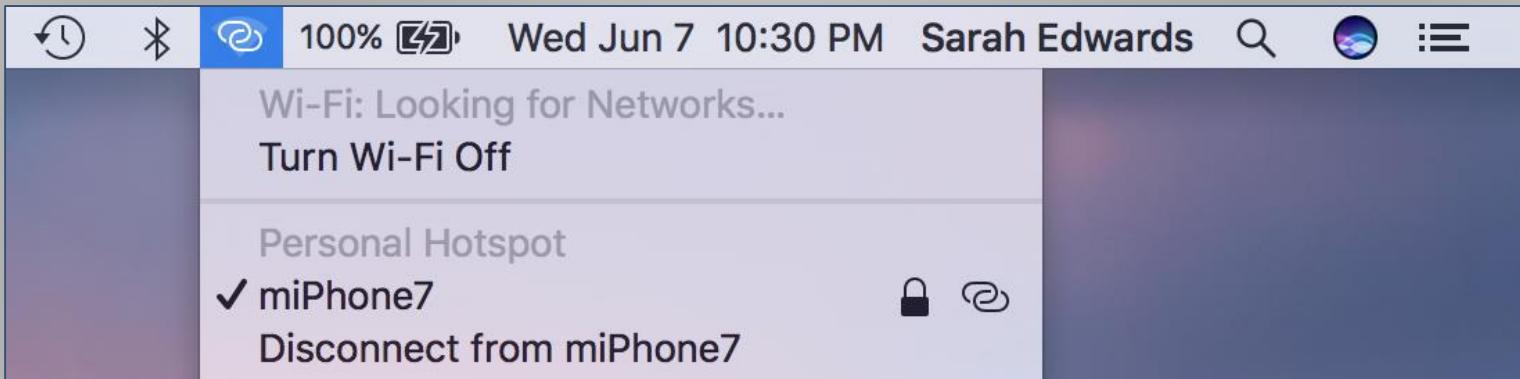
MDNSRESPONDER: [COM.APPLE.MDNSRESPONDER.ALLINFO] 45:

DNSSERVICERESOLVE(A55FF0A47E53._CONTINUITY._TCP.LOCAL.) RESULT
MIPHONE7.LOCAL.:8771



INSTANT HOTSPOT

- CONNECT TO YOUR IPHONE'S HOTSPOT USING YOUR MAC
- 'PERSONAL HOTSPOT' MUST BE ENABLED ON IDEVICE
- DEVICES SIGNED INTO SAME ICLOUD ACCOUNT
- BLUETOOTH AND WI-FI ENABLED



INSTANT HOTSPOT - MAC LOGS

WIFIAGENT: (SHARING) [COM.APPLE.SHARING.TETHERING] STARTING BROWSING

SHARINGD: [COM.APPLE.SHARING.TETHERING] STARTING BROWSING

SHARINGD: [COM.APPLE.SHARING.TETHERING] RESTARTED **SCANNING FOR AVAILABLE TETHERING DEVICES** [5FC3A499-1C18-4957-819A-539D111AE921, F1BAD73A-97D9-40FB-9C7C-37333332A3A, **F768D25B-1EC8-476B-B4A3-D757890CD2E8**]

SHARINGD: [COM.APPLE.SHARING.TETHERING] **DISCOVERED NEW DEVICE** IN 1.677536 SECONDS

WIFIAGENT: (SHARING) [COM.APPLE.SHARING.TETHERING] ENABLING
<SFREMOTEHOTSPOTDEVICE: 0X7FE674E52A10, NAME: MIPHONE7, IDENTIFIER: F768D25B-1EC8-476B-B4A3-D757890CD2E8, BATTERY LIFE: 100, NETWORK TYPE: LTE, SIGNAL STRENGTH: 2, HAS DUPLICATES: NO>

INSTANT HOTSPOT - MAC LOGS

SHARINGD: [COM.APPLE.SHARING.TETHERING] **ENABLING HOTSPOT FOR DEVICE** (NAME = MIPHONE7, IDENTIFIER = F768D25B-1EC8-476B-B4A3-D757890CD2E8, BATTERYLIFE = 100)

SHARINGD: [COM.APPLE.SHARING.TETHERING] **REQUESTING CREDENTIALS** FROM BLUETOOTH PEER = F768D25B-1EC8-476B-B4A3-D757890CD2E8

SHARINGD: [COM.APPLE.SHARING.TETHERING] RECEIVE CREDENTIALS DICTIONARY (DICTIONARY = YES, **NAME = MIPHONE7**, **CHANNNEL = 6**, **PASSWORD = YES**)

WIFIAGENT: (SHARING) [COM.APPLE.SHARING.TETHERING] **ENABLED**
<SFREMOTEHOTSPOTDEVICE: 0X7FE674E52A10, NAME: MIPHONE7, IDENTIFIER: F768D25B-1EC8-476B-B4A3-D757890CD2E8, BATTERY LIFE: 100, NETWORK TYPE: LTE, SIGNAL STRENGTH: 2, HAS DUPLICATES: NO>, <SFREMOTEHOTSPOTINFO: 0X7FE674C3FE20>, ERROR ((NULL))

CAVEATS

WHAT WE KNOW SO FAR...

- MAC ARTIFACTS PROVED TO BE MORE FRUITFUL (PUN INTENDED)
- IOS MAY REQUIRE DYNAMIC ANALYSIS OF THE IPHONE
- DETERMINING WHERE THE ACTION OCCURRED MAY NOT ALWAYS BE POSSIBLE
- TIMESTAMPS ARE TRICKY FOR DCIM
- WE'VE ONLY SCRATCHED THE SURFACE

