THE CIDER PRESS:
EXTRACTING FORENSIC ARTIFACTS FROM APPLE CONTINUITY

HEATHER MAHALIK | @HEATHERMAHALIK | SMARTERFORENSICS.COM
SARAH EDWARDS | @IAMEVLTWIN | MAC4N6.COM

© 2017 Sarah Edwards and Heather Mahalik
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)

© 2017 Sarah Edwards and Heather Mahalik
### CONNECTED DEVICES - BLUETOOTH IDENTIFIERS - MAC

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

---

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoreBluetoothCache</td>
<td>Dictionary</td>
<td>7</td>
</tr>
<tr>
<td>F788D25B-1EC8-476B-B4A3-D757890CD2E8</td>
<td>Dictionary</td>
<td>6</td>
</tr>
<tr>
<td>Services</td>
<td>Dictionary</td>
<td>3</td>
</tr>
<tr>
<td>DeviceAddressType</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>DeviceAddress</td>
<td>String</td>
<td>b8-53-ac-09-cc-87</td>
</tr>
<tr>
<td>ServiceChangedSubscribed</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>ServiceDiscoveryComplete</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>ServiceChangedHandle</td>
<td>Number</td>
<td>8</td>
</tr>
<tr>
<td>5FC3A49-1C48-4967-819A-539D111AE921</td>
<td>Dictionary</td>
<td>6</td>
</tr>
<tr>
<td>C905A733-B5A0-4680-A41F-4DCCD577A099</td>
<td>Dictionary</td>
<td>5</td>
</tr>
<tr>
<td>DeviceAddressType</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>DeviceAddress</td>
<td>String</td>
<td>ec-ad-b8-06-f2-aa</td>
</tr>
<tr>
<td>ServiceChangedSubscribed</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>ServiceDiscoveryComplete</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>ServiceChangedHandle</td>
<td>Number</td>
<td>8</td>
</tr>
<tr>
<td>b8-53-ac-09-cc-87</td>
<td>Dictionary</td>
<td>3</td>
</tr>
<tr>
<td>LastNameUpdate</td>
<td>Date</td>
<td>Feb 6, 2017, 7:61:42 AM</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>miPhone7</td>
</tr>
<tr>
<td>displayName</td>
<td>String</td>
<td>miPhone7</td>
</tr>
<tr>
<td>80718B4E1-97B8-4B6-90A8-ACB72377ED80</td>
<td>Dictionary</td>
<td>6</td>
</tr>
<tr>
<td>F1BAD73A-97D9-40FB-9C7C-37333322A3A</td>
<td>Dictionary</td>
<td>6</td>
</tr>
<tr>
<td>2B74AD7C-4439-4004-9D6D-3BE1EC152D7A</td>
<td>Dictionary</td>
<td>2</td>
</tr>
<tr>
<td>LastNameUpdate</td>
<td>Date</td>
<td>Feb 6, 2017, 8:04:52 AM</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>miWatch</td>
</tr>
<tr>
<td>displayName</td>
<td>String</td>
<td>miWatch</td>
</tr>
</tbody>
</table>

© 2017 Sarah Edwards and Heather Mahalik
CONNECTED DEVICES - BLUETOOTH IDENTIFIERS - MAC

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

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

© 2017 Sarah Edwards and Heather Mahalik
# CONNECTED DEVICES - BLUETOOTH IDENTIFIERS - IOS

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

<table>
<thead>
<tr>
<th>Uuid</th>
<th>Name</th>
<th>Address</th>
<th>ResolvedAddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>0ADB2DD6-9BFF-423F-9168-E6D2C015BF22</td>
<td>iPad</td>
<td>Public 80:D6:05:77:50:03</td>
<td>Public 80:D6:05:77:50:03</td>
</tr>
</tbody>
</table>
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, let’s AirDrop!”

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

© 2017 Sarah Edwards and Heather Mahalik
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

© 2017 Sarah Edwards and Heather Mahalik
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) AWDL2D AWDL2DSTARTBROWSINGFORKEY: '_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] SFBROWSERCALLBACK (NODE = <SFNODE 0x6000000EF880>{DOMAIN = AIRDROP})

**SHARINGD**: [COM.APPLE.SHARING.NETWORKING.FUNCTIONAL] COM.APPLE.SHARINGD NO AIRDROP PEOPLE DISCOVERED AFTER 8 SECONDS

© 2017 Sarah Edwards and Heather Mahalik
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}"
}

© 2017 Sarah Edwards and Heather Mahalik
AIRDROP - FILE TRANSFER TO IPHONE FROM MAC

© 2017 Sarah Edwards and Heather Mahalik
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 SERVER TRANSACTION BEGIN (1)
SHARINGD: [COM.APPLE.SHARING.AIRDROP] AIRDROP RECEIVED DISCOVERY REQUEST
SHARINGD: [COM.APPLE.SHARING.AIRDROP] POSTING <NSUSERNOTIFICATION:0X7FBCC3411B00> {
    TITLE: "AIRDROP" INFORMATIVE TEXT: "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>)

© 2017 Sarah Edwards and Heather Mahalik
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)

```
<table>
<thead>
<tr>
<th>com.apple.metadata:kMDItemWhereFroms:</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000 62 70 6c 69 73 74 30 30</td>
</tr>
<tr>
<td>00000010 68 20 45 66 77 61 72 64</td>
</tr>
<tr>
<td>00000020 65 37 00 00 03 00 00 00</td>
</tr>
<tr>
<td>00000030 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000040 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000045</td>
</tr>
<tr>
<td>com.apple.metadata:kMDLabel_r6h1hm73c2owhai3h2gch525la:</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>00000000 F2 6e C6 F9 59 BB 08 5A 71 F3 CD 29 4D</td>
</tr>
<tr>
<td>00000010 4E 5B 72 DF 23 4C CA 44 58 56 F3 6C BB</td>
</tr>
<tr>
<td>0000001A 02 00 AF 56 F3 DA D6 17 84</td>
</tr>
<tr>
<td>00000019</td>
</tr>
<tr>
<td>com.apple.quarantine:</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>00000000 30 30 38 31 3B 35 39 34 36 65 62 33</td>
</tr>
<tr>
<td>00000010 61 72 69 66 67 64 38 44 46 33 30</td>
</tr>
<tr>
<td>00000020 33 46 35 39 2D 34 41 35 34 46 2D</td>
</tr>
<tr>
<td>00000030 31 41 46 30 37 39 39 37 41 42 37</td>
</tr>
</tbody>
</table>
```
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)

<table>
<thead>
<tr>
<th>LSQuarantineEventIdentifier</th>
<th>LSQuarantineTimeStamp</th>
<th>LSQuarantineBundleIdentifier</th>
<th>LSQuarantineAgentBundleIdentifier</th>
<th>LSQuarantineAgentName</th>
<th>LSQuarantineDataURLString</th>
<th>LSQuarantineSenderName</th>
<th>LSQuarantineSenderAddress</th>
<th>LSQuarantineTypeNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>1728DFEE-BBDD-4A87-4DFC-0</td>
<td>519425134.856411</td>
<td>com.apple.icChat</td>
<td>iChat</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>3</td>
</tr>
<tr>
<td>61BF37FA-B8D7-4E46-4AE3-0</td>
<td>519498761.0</td>
<td>com.google.Chrome</td>
<td>Google Chrome.app</td>
<td><a href="https://github-productio">https://github-productio</a>...</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>0</td>
</tr>
<tr>
<td>23B510BB-D128-4552-4AE3-0</td>
<td>519510843.197536</td>
<td>sharingd</td>
<td>sharingd</td>
<td>NULL</td>
<td>NULL</td>
<td>Sarah Edwards</td>
<td>NULL</td>
<td>6</td>
</tr>
<tr>
<td>9A72A23D-225B-4859-4A5F-0</td>
<td>519510912.485851</td>
<td>sharingd</td>
<td>sharingd</td>
<td>NULL</td>
<td>NULL</td>
<td>Sarah Edwards</td>
<td>NULL</td>
<td>6</td>
</tr>
<tr>
<td>DF3046D4-3F59-4A5F-4DFE-0</td>
<td>519512767.901828</td>
<td>sharingd</td>
<td>sharingd</td>
<td>NULL</td>
<td>NULL</td>
<td>Sarah Edwards</td>
<td>NULL</td>
<td>6</td>
</tr>
</tbody>
</table>
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 178 Jun 18 19:11 .
drw-------+ 182 oompa staff 3468 Jun 18 19:07 ..
-rw-r--r--@  1 oompa staff 6148 Jun 18 19:11 .DS_Store
drw-xr-x  3 oompa staff 102 Jun 18 19:11 5453CE6C-E443-4E02-AA5B-2C6CE839D6747
-dw-xr-x  5 oompa staff 170 Jun 18 19:07 .
```

© 2017 Sarah Edwards and Heather Mahalik
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"

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"

© 2017 Sarah Edwards and Heather Mahalik
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

© 2017 Sarah Edwards and Heather Mahalik
AIRDROP - IOS ARTIFACTS [2] – PHONE BACKUP

• ~LIBRARY/DATABASES/DATAUSAGE.SQLITE
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

BTSERVER[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>: SFBROWSERCALLBACK (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>

© 2017 Sarah Edwards and Heather Mahalik
SHARINGD[64] <NOTICE>: **ACCEPTING TRANSFER** <SF AIRDROPTRANSFERDATA: 0x159341920> RECORDID: 5CF33654-103D-42D5-9F3C-927BFE023E1F

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

SHARINGD(CFNETWORK)[64] <NOTICE>: TCP CONN 0x15932f560 CANCELED
HANDOFF

• 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
• HANDOFF ENABLED
SHARINGD: [COM.APPL.E.SHARING.HANDOFF] SUCCESSFULLY DECRYPTED ADVERTISEMENT (SHARING FLAGS + ADVERTISEMENTPAYLOAD):
<B3A7F3448A2BCD1E7D46> => <008E6F4D00476ED213EFA5140188>, COUNTER: 28558

SHARINGD: [COM.APPL.E.SHARING.HANDOFF] 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>
HANDOFF FROM IPHONE TO MAC - MAC LOGS [2]

USERACTIVITYD: (SHARING) [COM.APPE.SHARING.HANDOFF] [SFCONTINUITYSCANMANAGER]
RECEIVED ADVERTISEMENT <SFACTIVITYADVERTISEMENT: 0x7ffC7AE219F0,
DEVICEIDENTIFIER:F9B85FFC-2BC6-4E80-93DA-675084
DOCK: (USERACTIVITY) [COM.APPE.USERACTIVITY.MAIN]
NOTIFYBESTAPPCHANGED:B81C0F47-0724-4E2B-966C-67C9E2FBA669 USERACTIVITY
<PRIVATE>/<PRIVATE> OPTS={
    SFACTIVITYADVERTISEMENTOPTIONFLAGCOPYPASTEKEY = 0;
    SFACTIVITYADVERTISEMENTOPTIONMINORVERSIONKEY = 0;
    SFACTIVITYADVERTISEMENTOPTIONVERSIONKEY = 0;
    USERACTIVITYHASWEBPAGEURL = 1;
} WHEN=2017-06-17 20:53:38 +0000 CONFIDENCE=1 FROM=<PRIVATE>/<PRIVATE>

BIRD: (CLOUDDOCSDAEMON) [COM.APPE.CLOUDDOCS.DEFAULT] [INFO] 172 <PRIVATE>
(<PRIVATE>) -[ BRCPXPCREGULARIPCCLIENT
DIDRECEIVEHANDOFFREQUESTFORBUNDLEID ]
HANDOFF 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: HANDOFF WAS NOT COMPLETED - ACTIVITY JUST HAPPENS IN THE BACKGROUND.
HANDOFF 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.HANDOFF] [SFCONTINUITYSCANMANAGER] DISPATCHING PAYLOAD REQUEST TO F9B85FFC-2BC6-4E80-93DA-67508472C8F8 FOR <41E36BAF264809>

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

© 2017 Sarah Edwards and Heather Mahalik
HANDOFF FROM IPHONE TO MAC - MAC LOGS (LINK CLICKED) [2]

SHARINGD: (IDS) [COM.APPL...E.DATESCONNECTION] CLIENT REQUEST TO SEND PROTOBUF ON SERVICE: COM.APPL...E.DATES.ACTIVITY GUID: AE52B945-31A6-4ABC-8698-F0951E720ACB TO DESTINATIONS: <PRIVATE> OPTIONS: <PRIVATE> SIZE: 107] (1 PENDING)

IDENTITYSERVICESD: (WIRELESSPROXIMITY) [COM.APPL...E.DATES.WIRELESSPROXIMITY] CONTINUITY CONNECT TO PEER: F768D25B-1EC8-476B-B4A3-D757890CD2E8


SHARINGD: [COM.APPL...E.DATESHANDOFF] RECEIVED REQUESTED HANDOFF 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

© 2017 Sarah Edwards and Heather Mahalik
HANDOFF FROM IPHONE TO MAC - MAC LOGS - OTHER APPS

• LOOK WITHIN CONTEXT!

NOTES: (LIBSYSTEM_TRACE.DYLIB) SUBSYSTEM: COM.APPLE.NOTES, CATEGORY: HANDOFF, 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

© 2017 Sarah Edwards and Heather Mahalik
HANDOFF 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.HANDOFF] REQUEST TO ADVERTISE <A0ED1D839414C8008D> WITH OPTIONS 
{SFACTIVITYADVERTISEROPTIONFLAGCOPYPASTEKEY = 0;}

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

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

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

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANDOFF] [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] r27C <PRIVATE>
(<PRIVATE>) -[BRCXPCREGULARIPCSCLIENT
DIDRECEIVEHANDOFFREQUESTFORBUNDLEID:REPLY:]

SHARINGD: [COM.APPLE.SHARING.HANDOFF] REQUESTING HANDOFF 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

© 2017 Sarah Edwards and Heather Mahalik
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)

© 2017 Sarah Edwards and Heather Mahalik
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!

© 2017 Sarah Edwards and Heather Mahalik
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:
<SAUTOUNLOCKDEVICE: 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-D757B890CD2E8,
  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

© 2017 Sarah Edwards and Heather Mahalik
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!

© 2017 Sarah Edwards and Heather Mahalik
UNIVERSAL CLIPBOARD - MAC LOGS (MAC TO IPHONE)

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

USERACTIVITYD: (SHARING) [COM.APPLE.SHARING.HANDOFF] [SFACTIVITYADVERTISER] RECEIVED PAYLOAD REQUEST FROM <SFPEERDEVICE: 0x7ffca18900, 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.HANDOFF] [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 CF PASTEBOARD REMOTE' ITEM: 1 FLAVOR: 'PUBLIC.JPEG' PROVIDER: METADATA RESULT: 0

PBOARD: (COREFOUNDATION) [COM.APPLE.CFPASTEBOARD.ENTRY] _PROMISEDATA('APPLE CF PASTEBOARD 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.SPBPROGRESSUI]
[SHAREDPasteboardProgressUI] 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

© 2017 Sarah Edwards and Heather Mahalik
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.APPL.E.SHARING.TETHERING] STARTING BROWSING

SHARINGD: [COM.APPL.E.SHARING.TETHERING] STARTING BROWSING


SHARINGD: [COM.APPL.E.SHARING.TETHERING] DISCOVERED NEW DEVICE IN 1.677536 SECONDS

WIFIAGENT: (SHARING) [COM.APPL.E.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>

© 2017 Sarah Edwards and Heather Mahalik
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, CHANNEL = 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
STILL THIRSTY? LET US POUR YOU A COLD ONE.

- MUCH MORE RESEARCH TO DO! COME TO OUR UPDATED TALKS AT:
  - NETWORK SECURITY, SANSFIRE, CDI
  - *ADDING IN THE NETWORK PERSPECTIVE (THANKS PHIL HAGEN)
- COME TO OUR CLASSES!
- 585 - ADVANCED SMARTPHONE FORENSICS - FOR585.COM
  - CHICAGO (AUG), VEGAS (SEPT), BERLIN (OCT)
- 518 - MAC FORENSIC ANALYSIS - FOR518.COM
  - VEGAS (SEPT) & PRAGUE, CZ (OCT)

© 2017 Sarah Edwards and Heather Mahalik