UNIVERSITY OF OXFORD

SyncTriage:

Using synchronisation artefacts to optimise acquisition order.

Dr Chris Hargreaves

26th April 2019

The Challenge

- “Obtaining actionable evidence more quickly”
- Potential approaches
  - Faster keyword searching
  - Techniques to get access to encrypted data
  - Improved triage software
  - …

The Challenge

The Challenge

The Challenge

acquisition → analysis → reporting

The Challenge

gain access — acquisition — analysis — reporting

The Challenge

gain access

triage approach

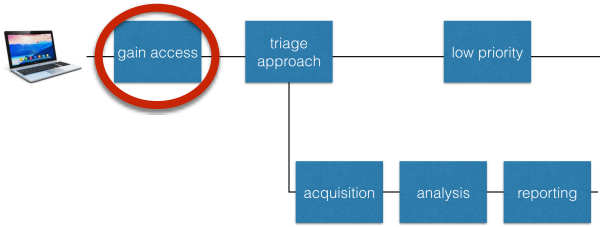
low priority

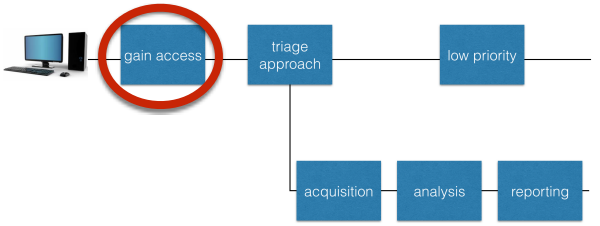
acquisition

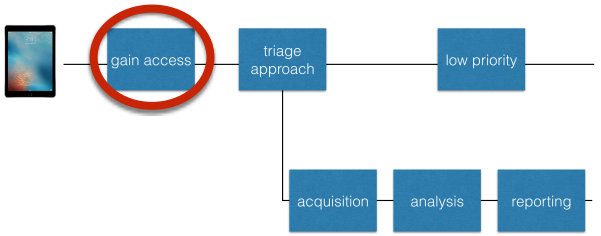
analysis

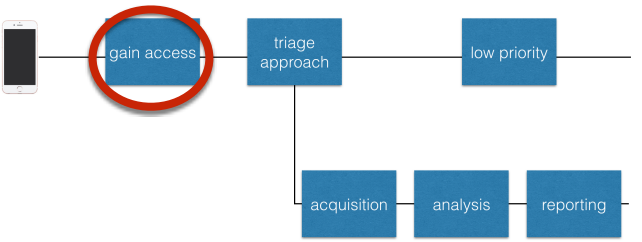
reporting

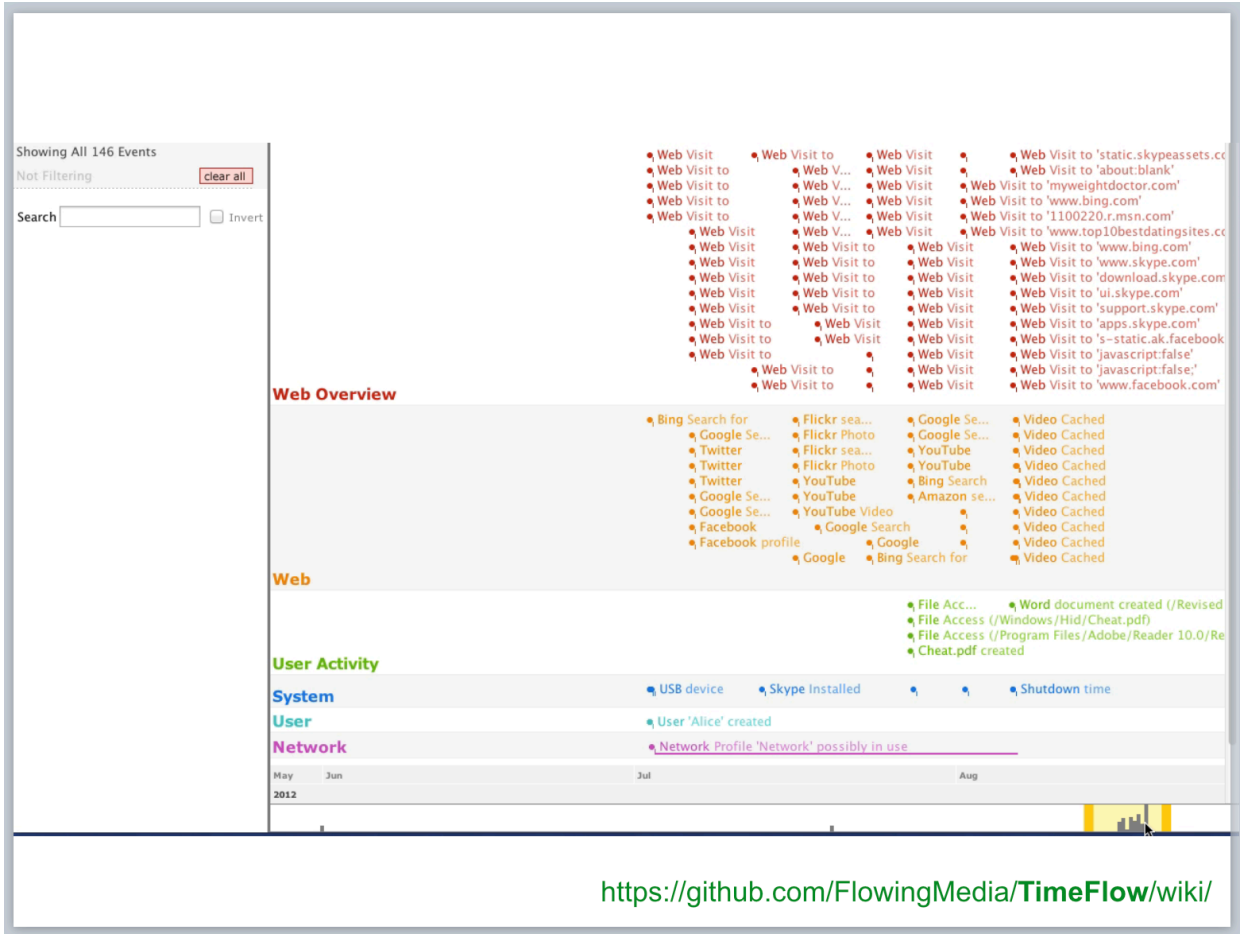
The Challenge











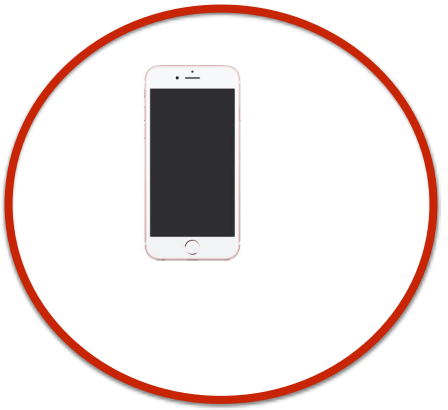
Hargreaves, C. & Patterson, J. (2012) An automated timeline reconstruction approach for digital forensic investigations, Presentation at the 12th Digital Forensics Research Workshop (DFRWS), Washington DC, and Digital Investigation, Volume 9, Supplement, p69-79

Patterson, J. & Hargreaves, C. (2012) The potential for cross-drive analysis using automated digital forensic timelines, Proceedings from 6th Cybercrime Forensics Education and Training, Canterbury Christchurch University, Canterbury, UK

Overall Concept

Overall Concept

Overall Concept



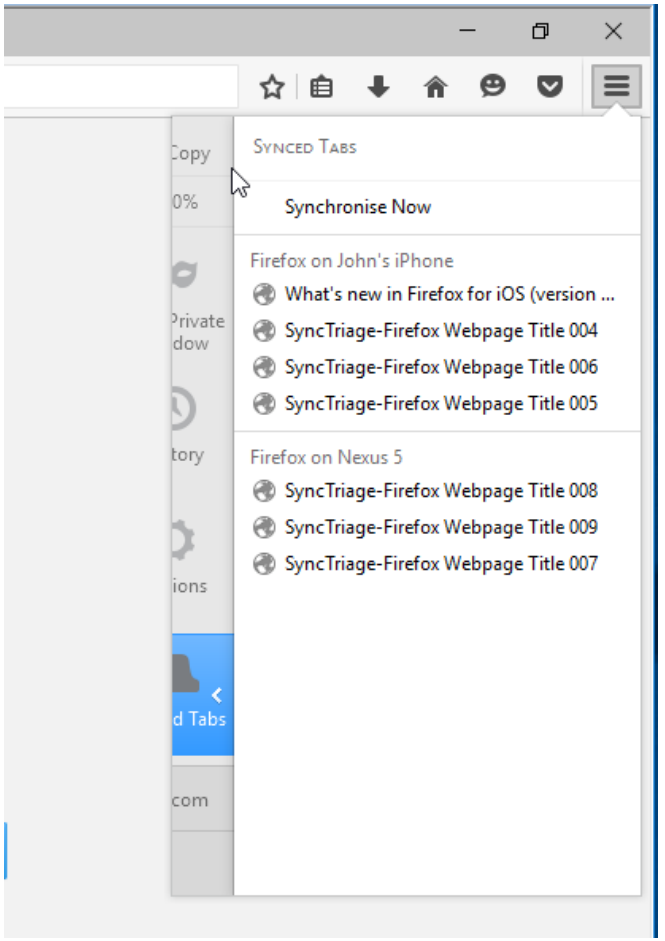
Overall Concept

Overall Concept

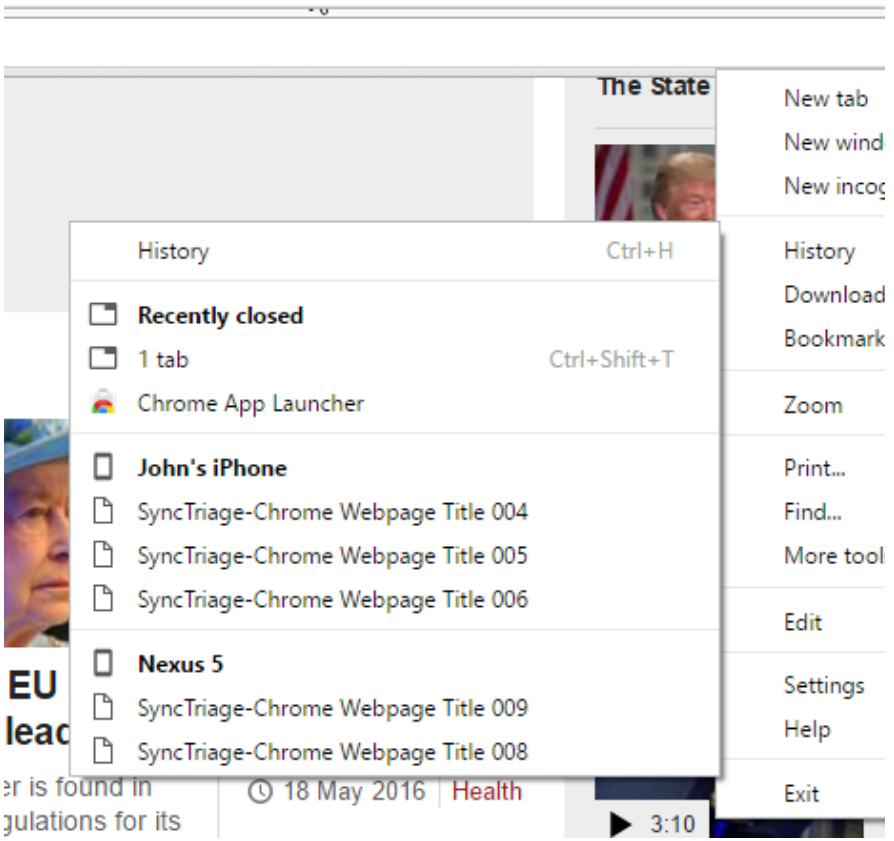
Overall Concept

Overall Concept

Syncing Technologies

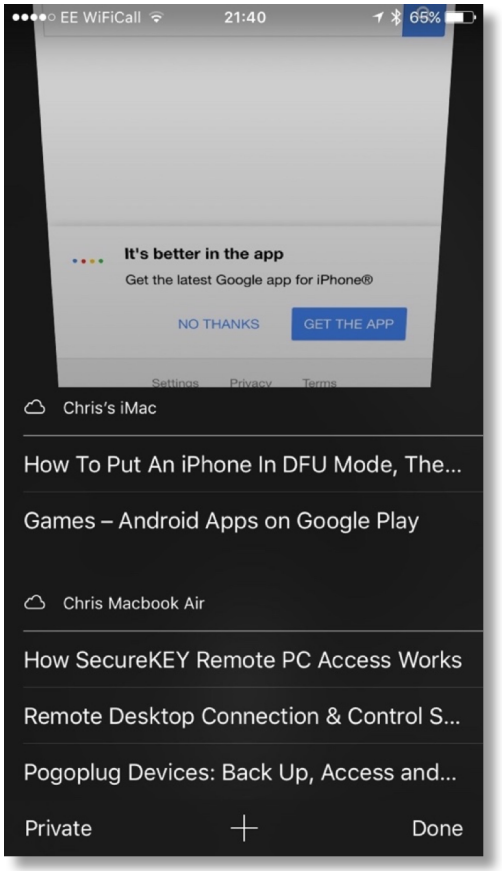


Firefox (Win 10)

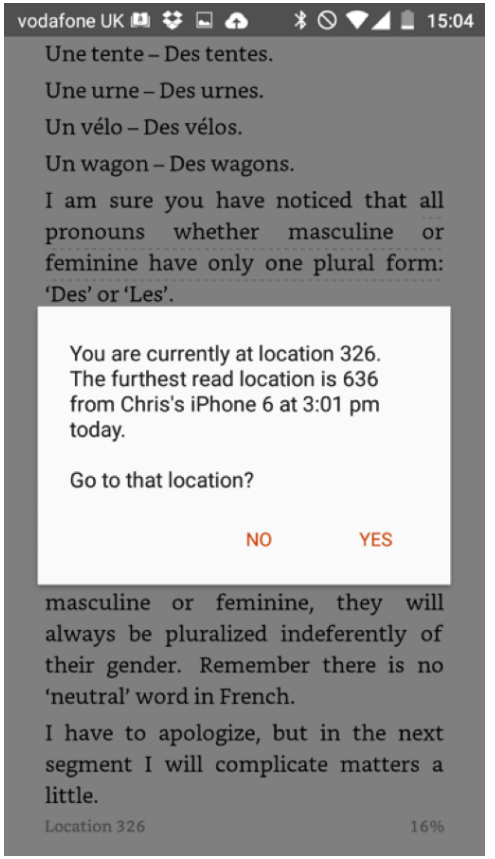


Chrome (Win 10)

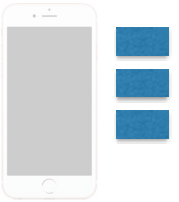
Syncing Technologies



Safari (iOS)

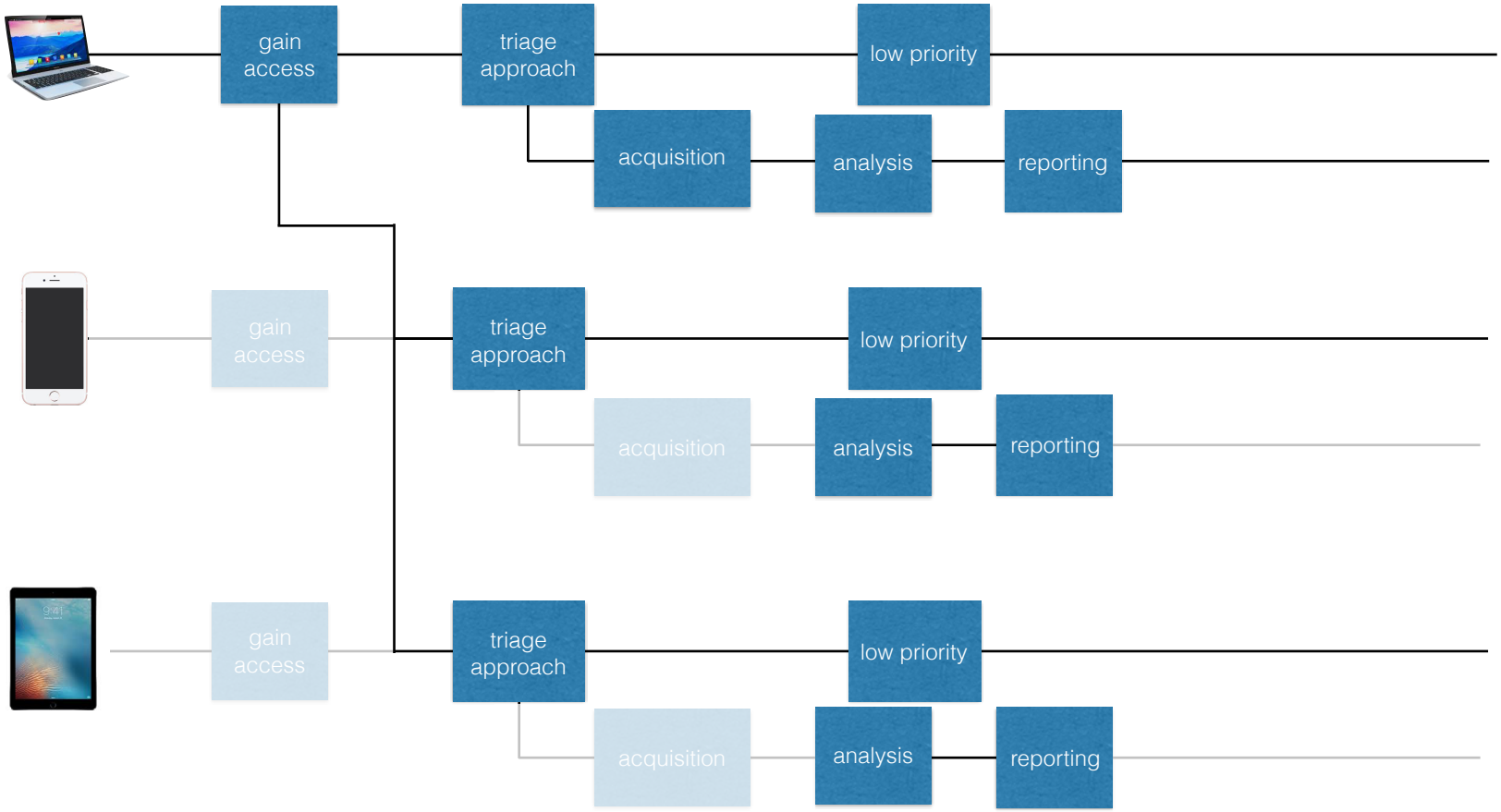


Kindle (Android)



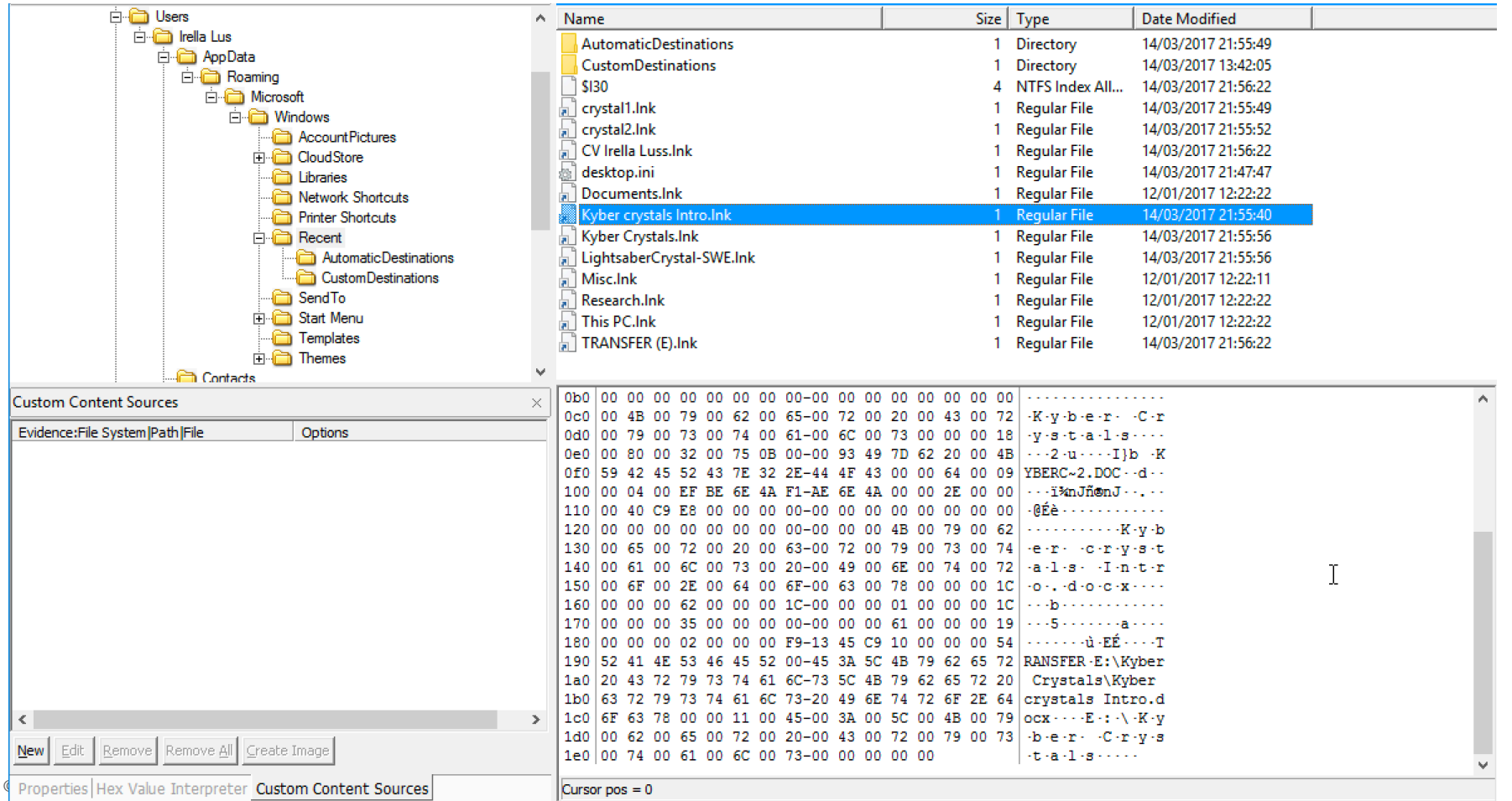
Overall Concept

Overall Concept



Existing examples (not quite syncing but related)

- Files on USB inferred using link files



Name	Size	Type	Date Modified
AutomaticDestinations	1	Directory	14/03/2017 21:55:49
CustomDestinations	1	Directory	14/03/2017 13:42:05
$I30	4	NTFS Index All...	14/03/2017 21:56:22
crystal1.lnk	1	Regular File	14/03/2017 21:55:49
crystal2.lnk	1	Regular File	14/03/2017 21:55:52
CV Irella Luss.lnk	1	Regular File	14/03/2017 21:56:22
desktop.ini	1	Regular File	14/03/2017 21:47:47
Documents.lnk	1	Regular File	12/01/2017 12:22:22
Kyber crystals Intro.lnk	1	Regular File	14/03/2017 21:55:40
Kyber Crystals.lnk	1	Regular File	14/03/2017 21:55:56
LightsaberCrystal-SWE.lnk	1	Regular File	14/03/2017 21:55:56
Misc.lnk	1	Regular File	12/01/2017 12:22:11
Research.lnk	1	Regular File	12/01/2017 12:22:22
This PC.lnk	1	Regular File	12/01/2017 12:22:22
TRANSFER (E).lnk	1	Regular File	14/03/2017 21:56:22

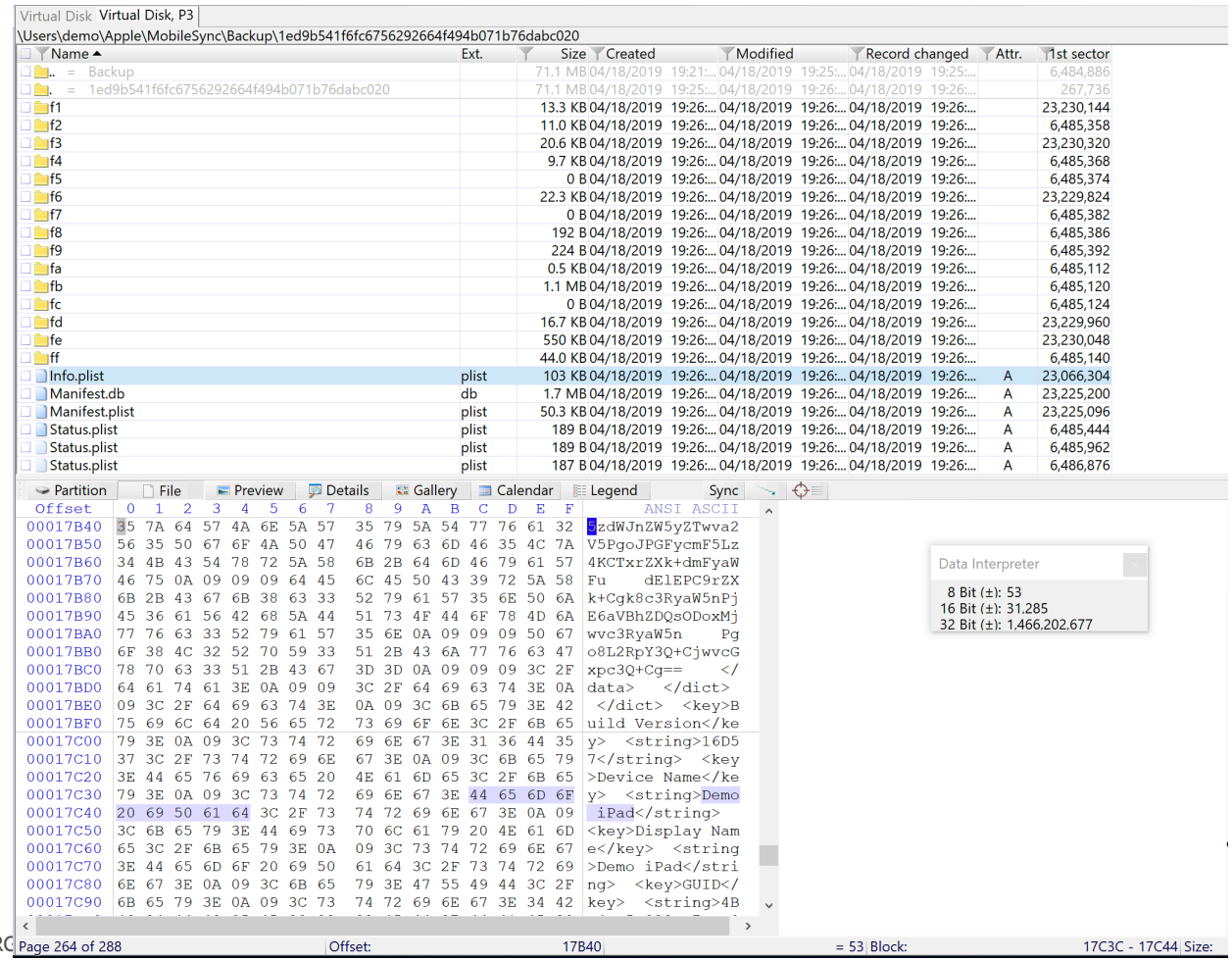
```
0b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0c0 00 4B 00 79 00 62 00 65-00 72 00 20 00 43 00 72 .K.y.b.e.r. .C.r
0d0 00 79 00 73 00 74 00 61-00 6C 00 73 00 00 00 18 .y.s.t.a.l.s....
0e0 00 80 00 32 00 75 0B 00-00 93 49 7D 62 20 00 4B ...2.u....I}b .K
0f0 59 42 45 52 43 7E 32 2E-44 4F 43 00 00 64 00 09 YBERC~2.DOC..d..
100 00 04 00 EF BE 6E 4A F1-AE 6E 4A 00 00 2E 00 00 ...ï¾nJñ®nJ....
110 00 40 C9 E8 00 00 00 00-00 00 00 00 00 00 00 00 .@Éè............
120 00 00 00 00 00 00 00 00-00 00 00 4B 00 79 00 62 ...........K.y.b
130 00 65 00 72 00 20 00 63-00 72 00 79 00 73 00 74 .e.r. .c.r.y.s.t
140 00 61 00 6C 00 73 00 20-00 49 00 6E 00 74 00 72 .a.l.s. .I.n.t.r
150 00 6F 00 2E 00 64 00 6F-00 63 00 78 00 00 00 1C .o...d.o.c.x....
160 00 00 00 62 00 00 00 1C-00 00 00 01 00 00 00 1C ...b............
170 00 00 00 35 00 00 00 00-00 00 00 61 00 00 00 19 ...5.......a....
180 00 00 00 02 00 00 00 F9-13 45 C9 10 00 00 00 54 .......ù.EÉ....T
190 52 41 4E 53 46 45 52 00-45 3A 5C 4B 79 62 65 72 RANSFER.E:\Kyber
1a0 20 43 72 79 73 74 61 6C-73 5C 4B 79 62 65 72 20  Crystals\Kyber
1b0 63 72 79 73 74 61 6C 73-20 49 6E 74 72 6F 2E 64 crystals Intro.d
1c0 6F 63 78 00 00 11 00 45-00 3A 00 5C 00 4B 00 79 ocx....E.:.\.K.y
1d0 00 62 00 65 00 72 00 20-00 43 00 72 00 79 00 73 .b.e.r. .C.r.y.s
1e0 00 74 00 61 00 6C 00 73-00 00 00 00 00          .t.a.l.s.....
```

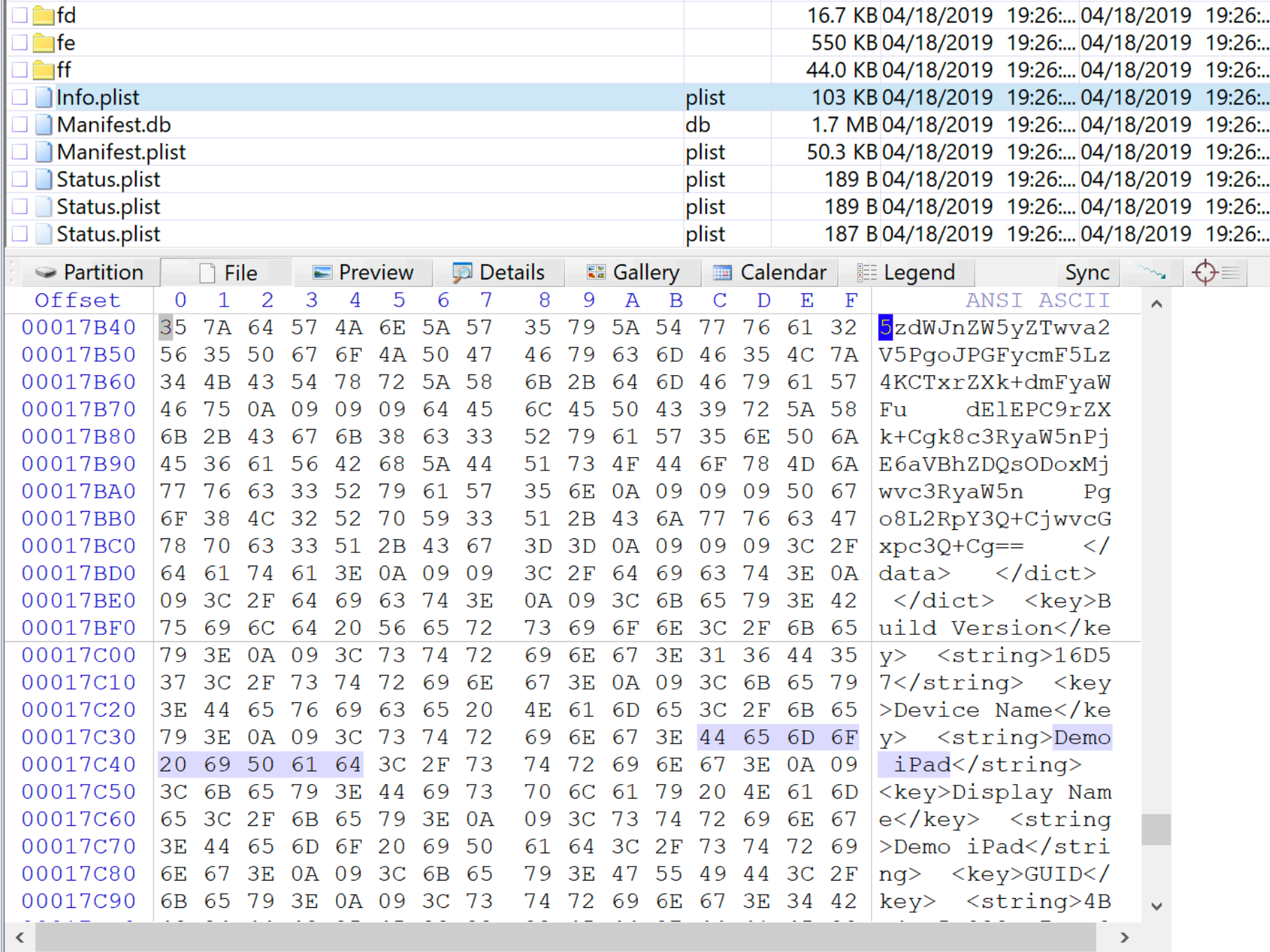
Cursor pos = 0

[AD1]/Luss-2017-03-15-CH-01.e01:Partition 2 [60938MB]:NONAME [NTFS]/[root]/Users/Irella Lus/AppData/Roaming/Microsoft/Win

Existing examples (not quite syncing but related)

- iPhone backups on a computer




fd 16.7 KB 04/18/2019 19:26:... 04/18/2019 19:26:...
fe 550 KB 04/18/2019 19:26:... 04/18/2019 19:26:...
ff 44.0 KB 04/18/2019 19:26:... 04/18/2019 19:26:...
Info.plist plist 103 KB 04/18/2019 19:26:... 04/18/2019 19:26:...
Manifest.db db 1.7 MB 04/18/2019 19:26:... 04/18/2019 19:26:...
Manifest.plist plist 50.3 KB 04/18/2019 19:26:... 04/18/2019 19:26:...
Status.plist plist 189 B 04/18/2019 19:26:... 04/18/2019 19:26:...
Status.plist plist 189 B 04/18/2019 19:26:... 04/18/2019 19:26:...
Status.plist plist 187 B 04/18/2019 19:26:... 04/18/2019 19:26:...
Partition File Preview Details Gallery Calendar Legend Sync
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F ANSI ASCII
00017B40 35 7A 64 57 4A 6E 5A 57 35 79 5A 54 77 76 61 32 5zdWJnZW5yZTwva2
00017B50 56 35 50 67 6F 4A 50 47 46 79 63 6D 46 35 4C 7A V5PgoJPGFycmF5Lz
00017B60 34 4B 43 54 78 72 5A 58 6B 2B 64 6D 46 79 61 57 4KCTxrZXk+dmFyaW
00017B70 46 75 0A 09 09 09 64 45 6C 45 50 43 39 72 5A 58 Fu dElEPC9rZX
00017B80 6B 2B 43 67 6B 38 63 33 52 79 61 57 35 6E 50 6A k+Cgk8c3RyaW5nPj
00017B90 45 36 61 56 42 68 5A 44 51 73 4F 44 6F 78 4D 6A E6aVBhZDQsODoxMj
00017BA0 77 76 63 33 52 79 61 57 35 6E 0A 09 09 09 50 67 wvc3RyaW5n Pg
00017BB0 6F 38 4C 32 52 70 59 33 51 2B 43 6A 77 76 63 47 o8L2RpY3Q+CjwvcG
00017BC0 78 70 63 33 51 2B 43 67 3D 3D 0A 09 09 09 3C 2F xpc3Q+Cg== </
00017BD0 64 61 74 61 3E 0A 09 09 3C 2F 64 69 63 74 3E 0A data> </dict>
00017BE0 09 3C 2F 64 69 63 74 3E 0A 09 3C 6B 65 79 3E 42 </dict> <key>B
00017BF0 75 69 6C 64 20 56 65 72 73 69 6F 6E 3C 2F 6B 65 uild Version</ke
00017C00 79 3E 0A 09 3C 73 74 72 69 6E 67 3E 31 36 44 35 y> <string>16D5
00017C10 37 3C 2F 73 74 72 69 6E 67 3E 0A 09 3C 6B 65 79 7</string> <key
00017C20 3E 44 65 76 69 63 65 20 4E 61 6D 65 3C 2F 6B 65 >Device Name</ke
00017C30 79 3E 0A 09 3C 73 74 72 69 6E 67 3E 44 65 6D 6F y> <string>Demo
00017C40 20 69 50 61 64 3C 2F 73 74 72 69 6E 67 3E 0A 09 iPad</string>
00017C50 3C 6B 65 79 3E 44 69 73 70 6C 61 79 20 4E 61 6D <key>Display Nam
00017C60 65 3C 2F 6B 65 79 3E 0A 09 3C 73 74 72 69 6E 67 e</key> <string
00017C70 3E 44 65 6D 6F 20 69 50 61 64 3C 2F 73 74 72 69 >Demo iPad</stri
00017C80 6E 67 3E 0A 09 3C 6B 65 79 3E 47 55 49 44 3C 2F ng> <key>GUID</
00017C90 6B 65 79 3E 0A 09 3C 73 74 72 69 6E 67 3E 34 42 key> <string>4B

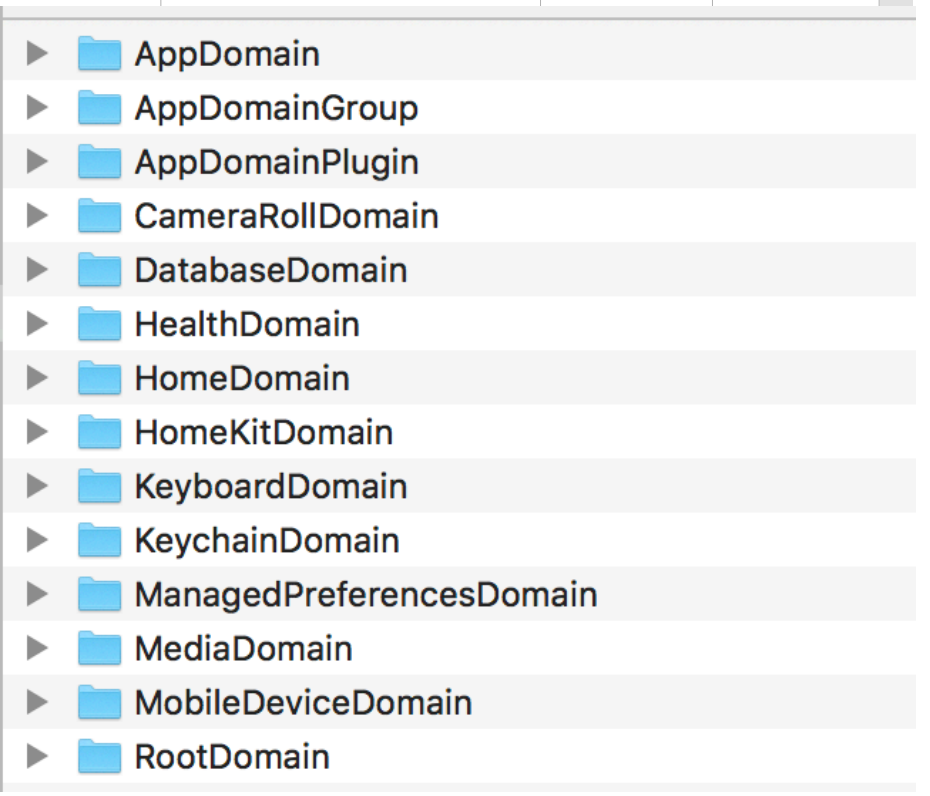
Manifest.db

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: Files

New Record | Delete Record

	fileID	domain	relativePath	flags	file
	Filter	Filter	Filter	Filter	Filter
931	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c	HomeDomain	Library/Notes/notes.sqlite	1	BLOB
932	c8ada38b9acf7368c6647be1c353dc68ed2c7741	CameraRollDomain	Media/DCIM/100APPLE/IMG_0001.PNG	1	BLOB
933	6b97989189901ceaa4e5be9b7f05fb584120e27b	HomeDomain	Library/Preferences/com.apple.identityservices.idstatuscache...	1	BLOB
934	ee77759a5f936cb2e4b030694ee739f111552b46	AppDomain-com.apple.mobilesafari	Library/Preferences/com.apple.mobilesafari.plist	1	BLOB
935	f65b5fafc69bbd3c60be019c6e938e146825fa83	HomeDomain	Library/Preferences/com.apple.osanalytics.addaily.plist	1	BLOB
936	75b12106910f0b106f64d72eb75397427884fd5a	HomeDomain			
937	0ba0507b7b46ab4bc1378adb3a9431cd145ad405	HomeDomain			
938	e5df80f87a44d0e0c4851a9ee673758d98931087	CameraRollDomain			
939	8d12d5c0ac27fc05078e2a97e9d355b48b4def1c	HomeDomain			
940	4003654e0b99fca239478606cdc0830a244d60a4	HomeDomain			



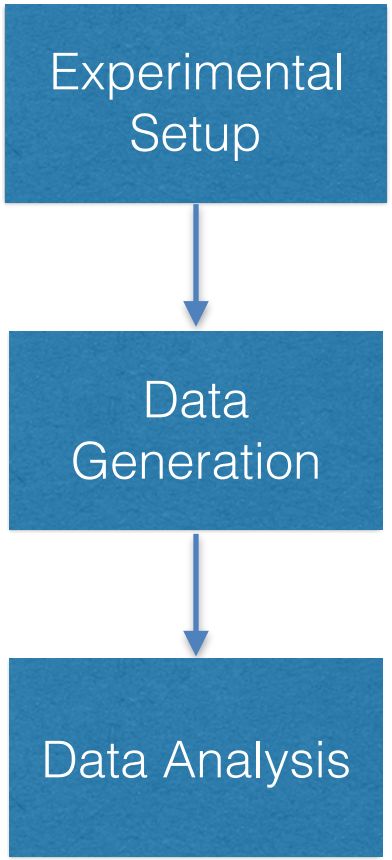
Previous work on synchronisation artefacts

- Chung et al. (2012) *Digital forensic investigation of cloud storage services.*
- Friedman et al. (2012) *A Digital Forensic Analysis on the iCloud and its Synchronization to Apple Devices*
- Farina and Kechadi (2014) *BitTorrent sync: first impressions and digital forensic implications.*
- Bubbins (2015) *Identification of Devices Connected to a Suspect's iCloud Account when Using the Application Find My iPhone.*
- Wright (2015) *Forensic Artefacts Related to Google's Chrome Synchronisation Feature.*
- Boucher and Le-Khac (2018) *Forensic framework to identify local vs synced artefacts.*

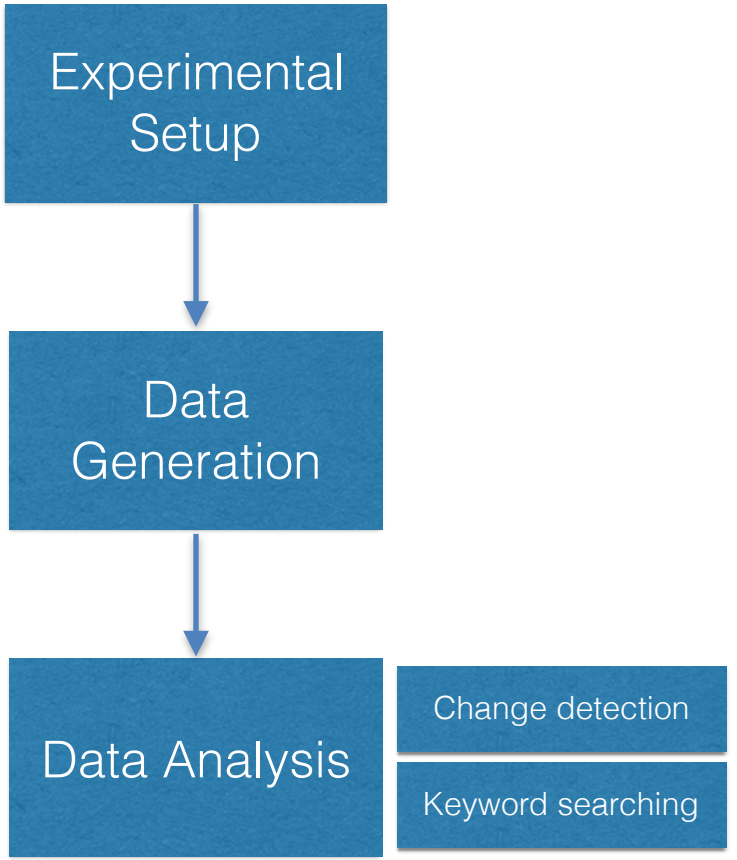
Experiments: Selection of Apps

Application	Category
Chrome	Browsers
Firefox	Browsers
Facebook Messenger	Messengers
WhatsApp	Messengers
Google Hangouts	Messengers
Telegram	Messengers
Viber	Messengers
Skype	VOIP
VLC	Media
AllCast	Media
YouTube	Media
Evernote	Notes
Google Photos	Photos
Instagram	Social Networking/Photos
Facebook	Social Networking
Twitter	Social Networking
Dropbox	Cloud Storage

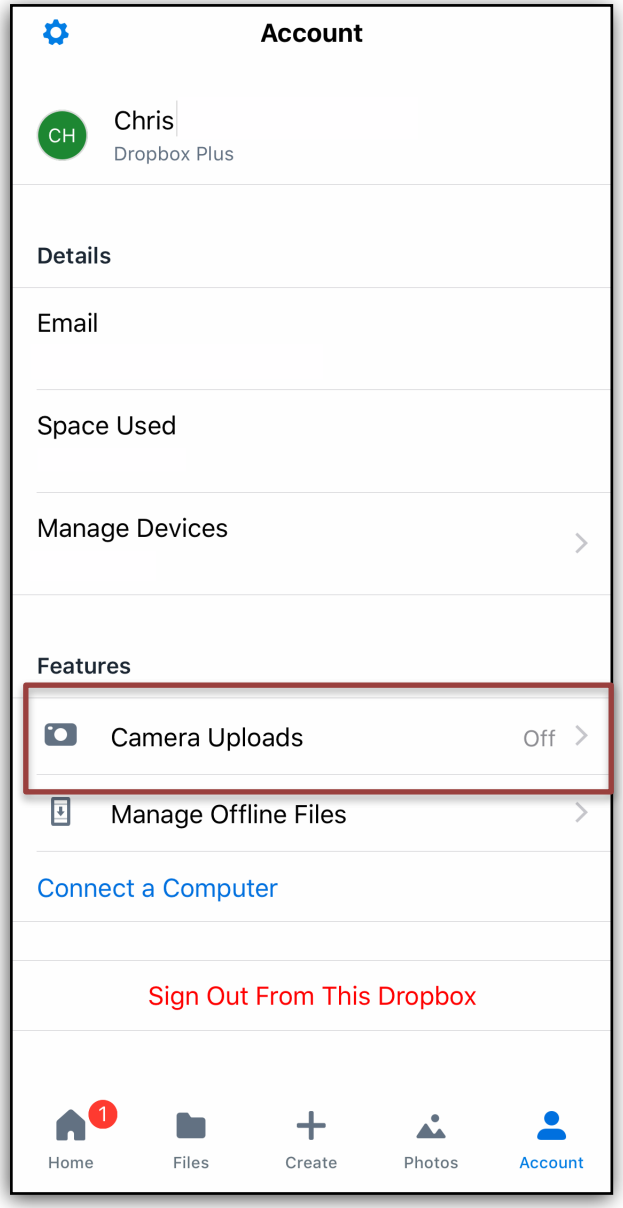
Experimental Method

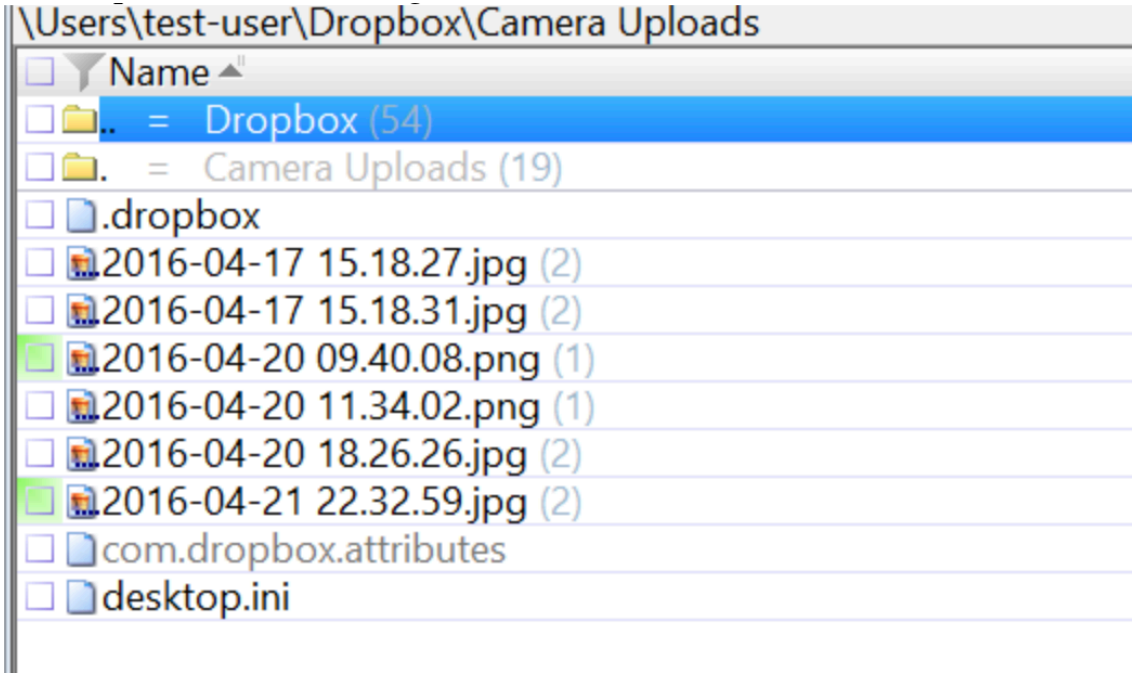


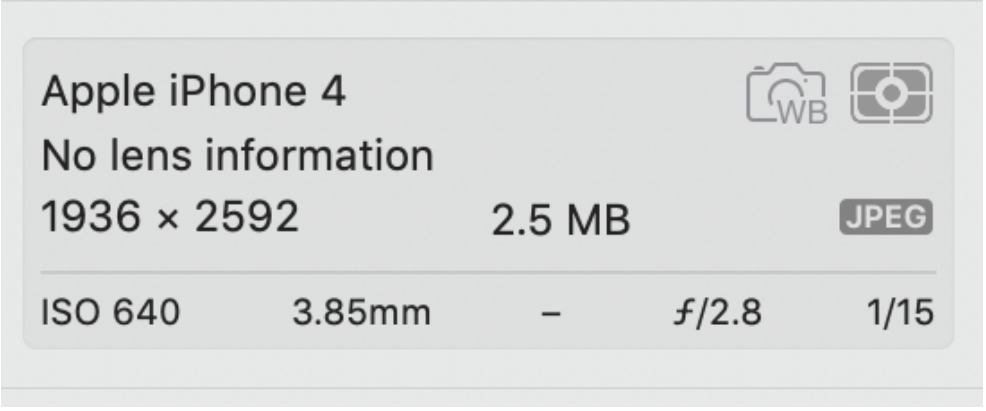
Experimental Method



EXIF Data







This same information can also be extracted from Google Photos app and Apple's Photos app.

Evernote Example

New Note

Shortcuts

All Notes

Notebooks

Shared with Me

Tags

Trash

All notes

4 notes

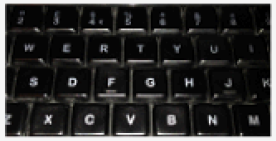
Search notes

Synctriagekw-evernote-android-note-title

Synctriagekw-evernote-android-note-body

18/05/2016

Snapshot from



21/04/2016

Synctriagekw-Evernote-note title-002-iOS

Synctriagekw-Evernote-notecontent-002-iOS

21/04/2016

synctriagekw-evernote-notetitle-001-desktop

synctriagekw-evernote-notecontent-001-desktop

21/04/2016

Synctriagekw-Evernote-note title-002-iOS

Share

First Notebook

Add tag...

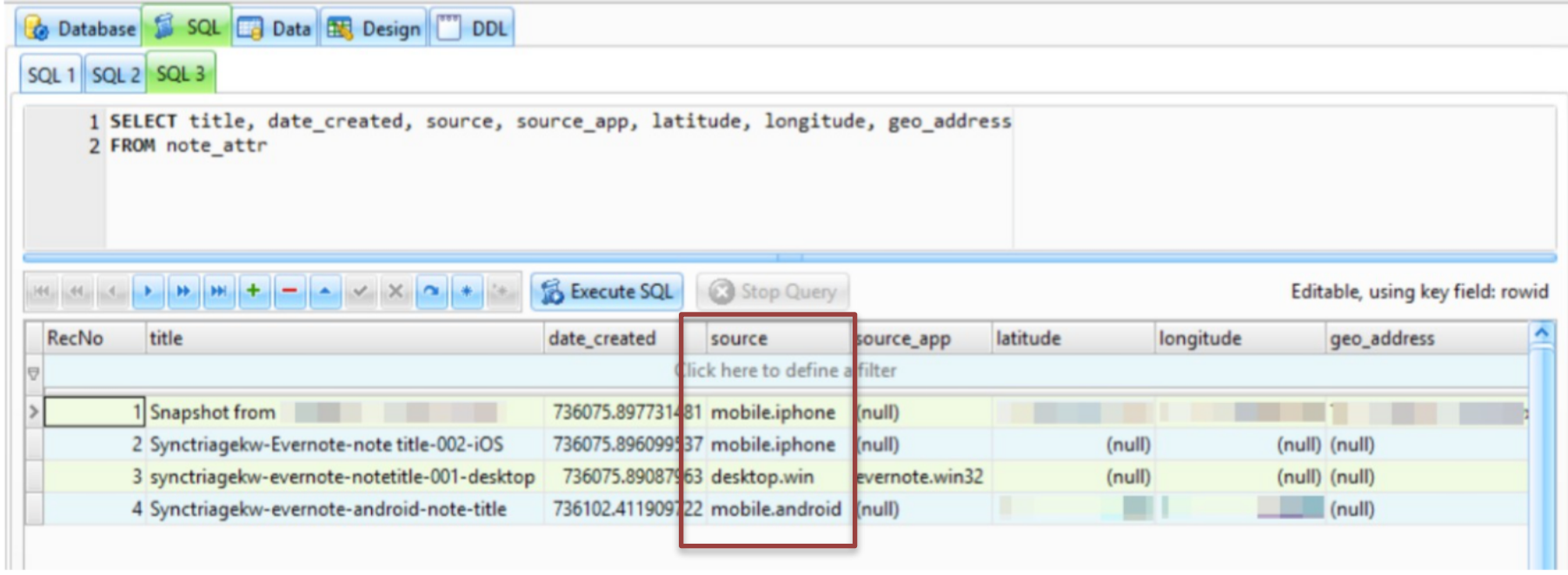
21/04/2016

Segoe UI

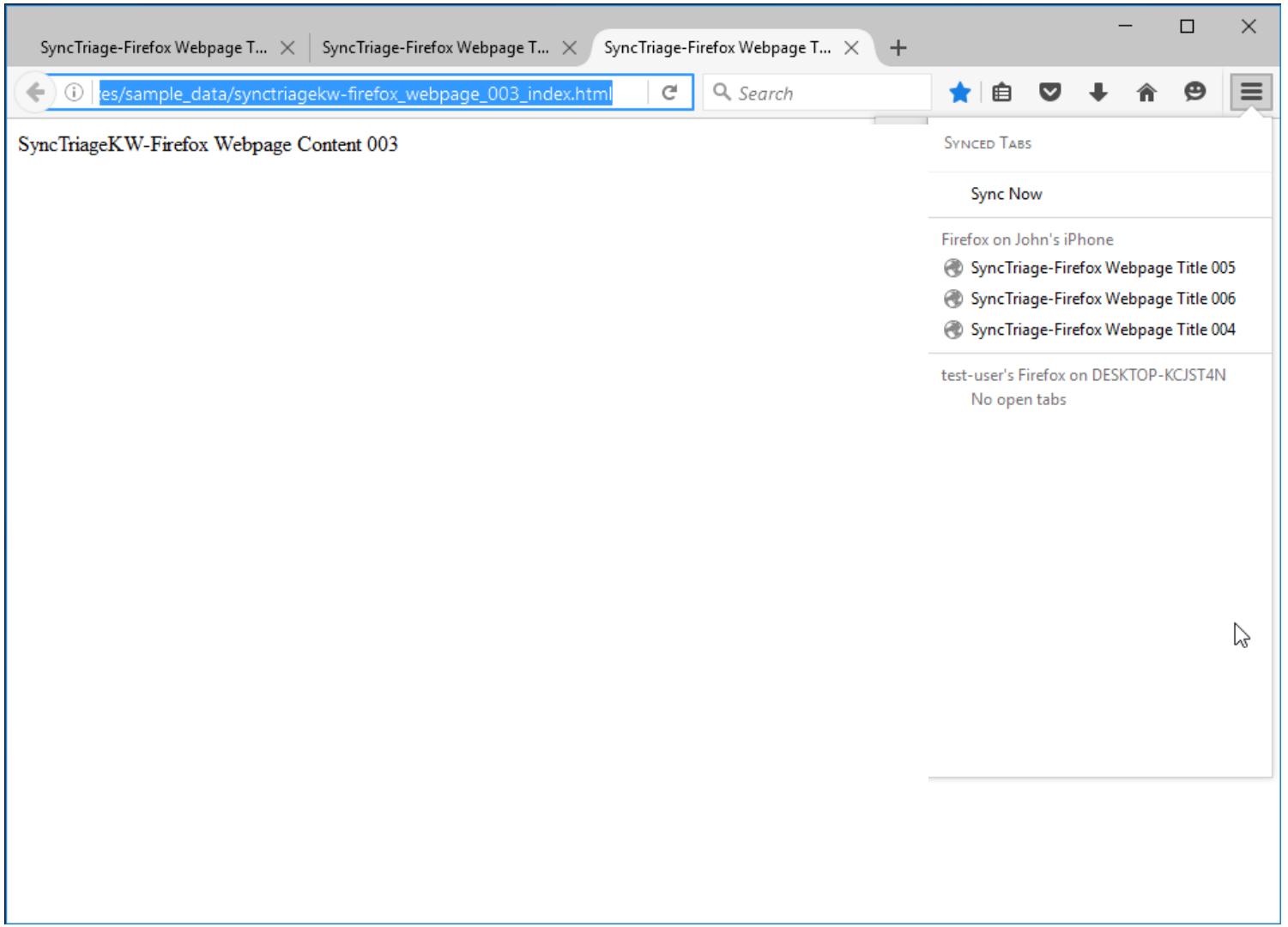
10

Synctriagekw-Evernote-notecontent-002-iOS

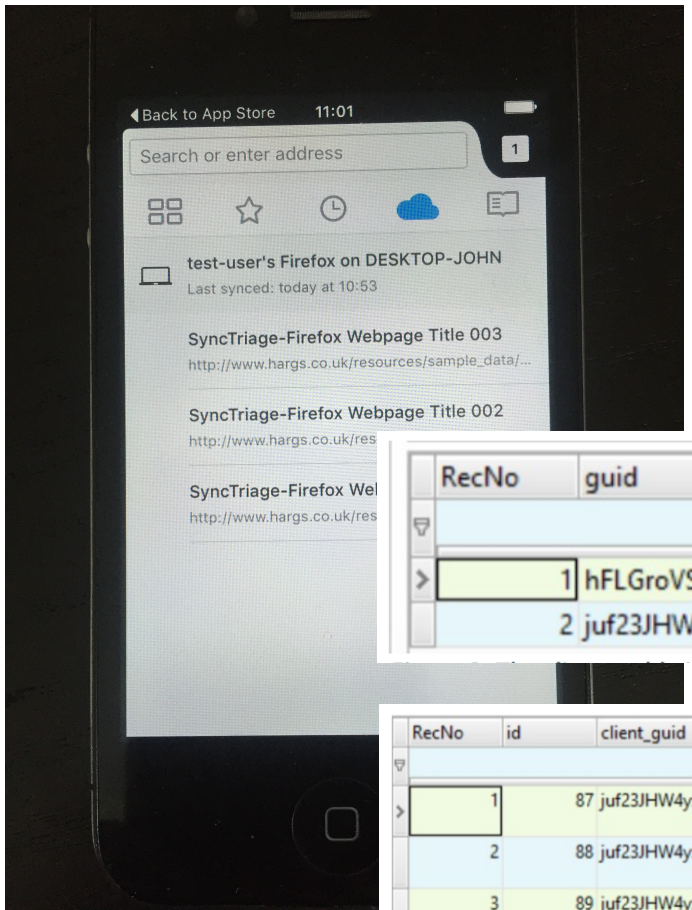
\Users\[username]\AppData\Local\Evernote\Evernote\Databases\[evernote_user_id].exb



Firefox Example



AppDomainGroup-group.org.mozilla.ios.Firefox/profile.profile/browser.db



RecNo	guid	name	modified	type	formfactor	os
Click here to define a filter						
1	hFLGroVSvdiz	John's Firefox on john-desktop	1463567418280	desktop	(null)	WINNT
2	juf23JHW4yzg	Firefox on Nexus 5	1463500519870	mobile	phone	Android

The *clients* table in browser.db

RecNo	id	client_guid	url	title
Click here to define a filter				
1	87	juf23JHW4yzg	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_007_index.html	SyncTriage-Firefox Webpage Title 007
2	88	juf23JHW4yzg	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_008_index.html	SyncTriage-Firefox Webpage Title 008
3	89	juf23JHW4yzg	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_009_index.html	SyncTriage-Firefox Webpage Title 009
4	94	(null)	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_004_index.html	SyncTriage-Firefox Webpage Title 004
5	95	(null)	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_005_index.html	SyncTriage-Firefox Webpage Title 005
6	96	(null)	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_006_index.html	SyncTriage-Firefox Webpage Title 006
7	97	(null)	https://support.mozilla.org/en-US/kb/whats-new-firefox-ios-version-40?mobile=1&as=u&utm_source=inproduct&minimal=1	What's new in Firefox for iOS (version 4.0) | How to | Mozilla
8	98	hFLGroVSvdiz	http://www.bbc.co.uk/news	Home - BBC News

The *tabs* table in browser.db

SQL query to extract open tabs on other devices

SQL 1 | SQL 2 | SQL 3

```
1 SELECT client_guid, name, last_used, modified, clients.type, clients.formfactor, clients.os,
2 url, title
3 FROM clients, tabs
4 WHERE clients.guid = tabs.client_guid
5
6
```

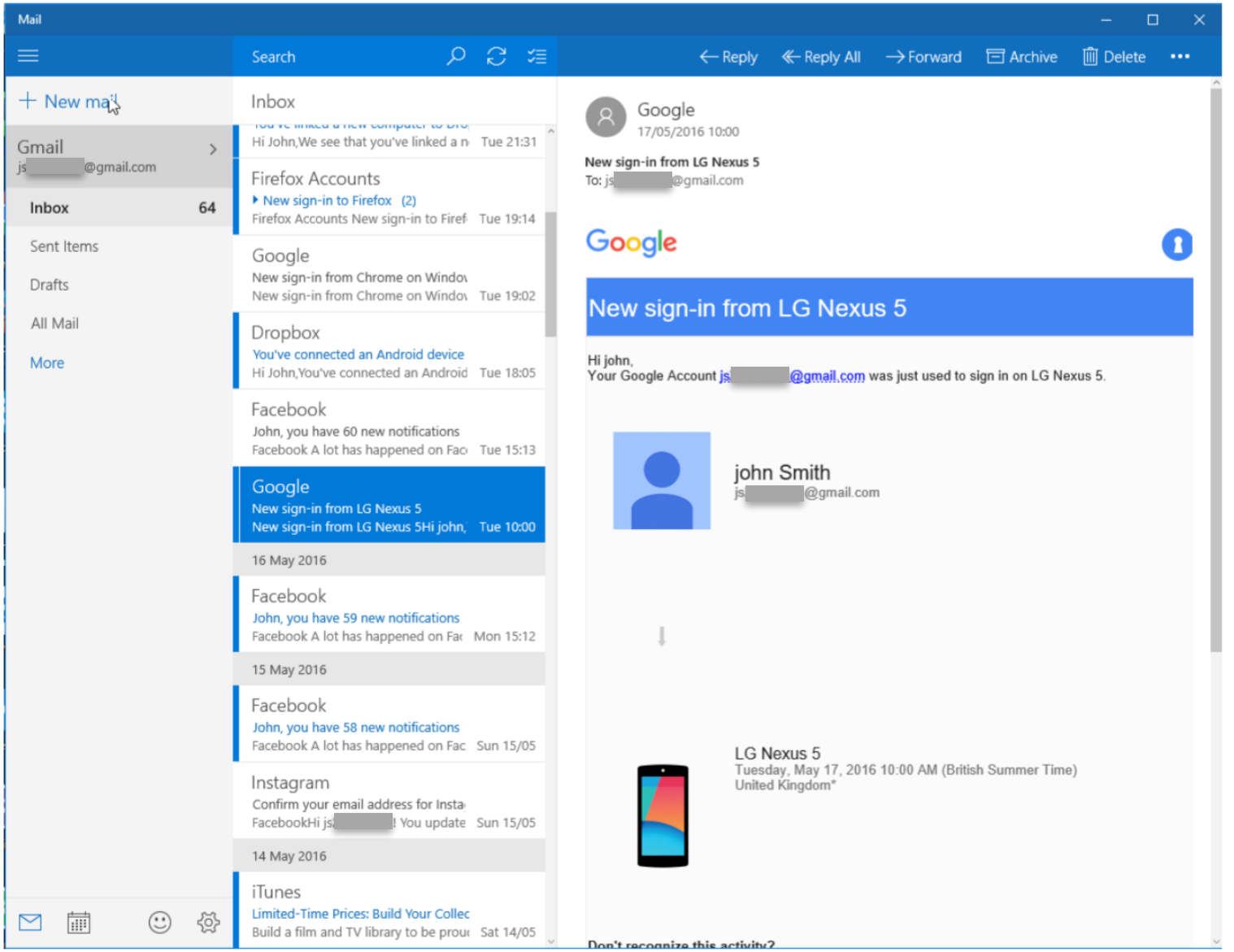
Execute SQL | Stop Query | Read-only

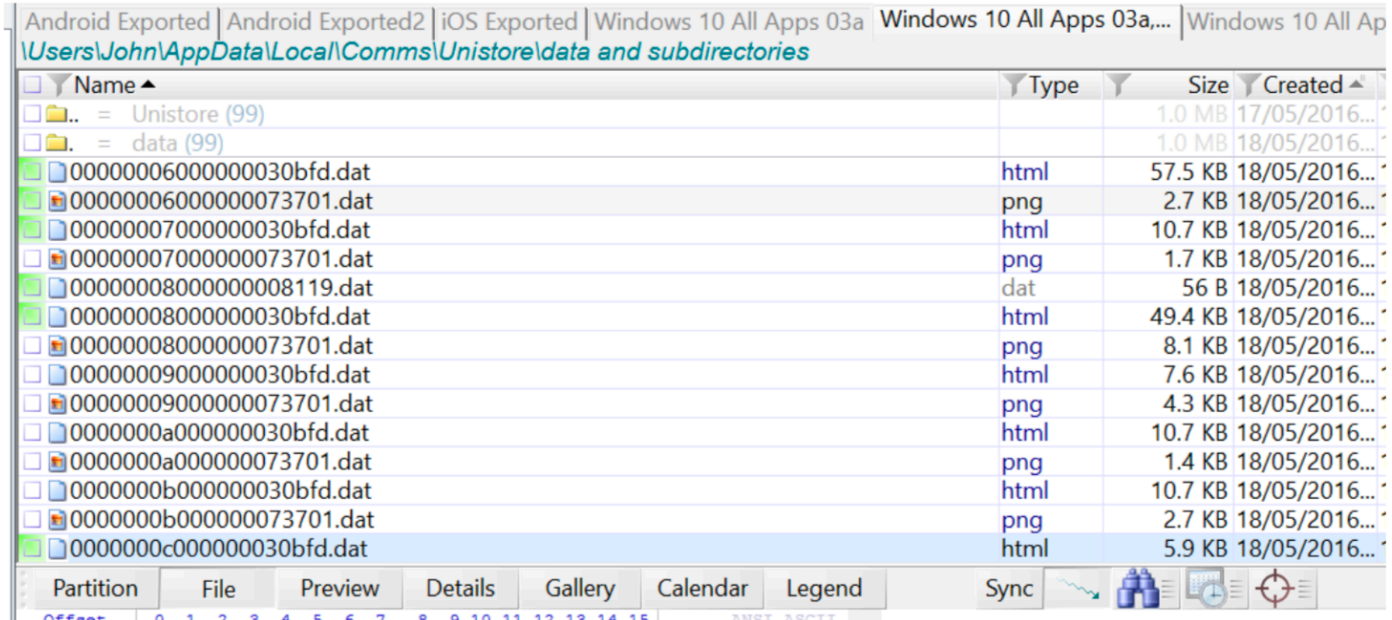
RecNo	client_guid	name	last_used	modified	type	formfactor	os	url	title
	Click here to define a filter								
1	juf23JHW4yzg	Firefox on Nexus 5	1463521319000	1463500519870	mobile	phone	Android	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_007_index.html	SyncTriage-Fi
2	juf23JHW4yzg	Firefox on Nexus 5	1463521431000	1463500519870	mobile	phone	Android	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_008_index.html	SyncTriage-Fi
3	juf23JHW4yzg	Firefox on Nexus 5	1463521431000	1463500519870	mobile	phone	Android	http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_009_index.html	SyncTriage-Fi
4	hFLGroVSvdiz	John's Firefox on john-desktop	1463567494000	1463567418280	desktop	(null)	WINNT	http://www.bbc.co.uk/news	Home - BBC N

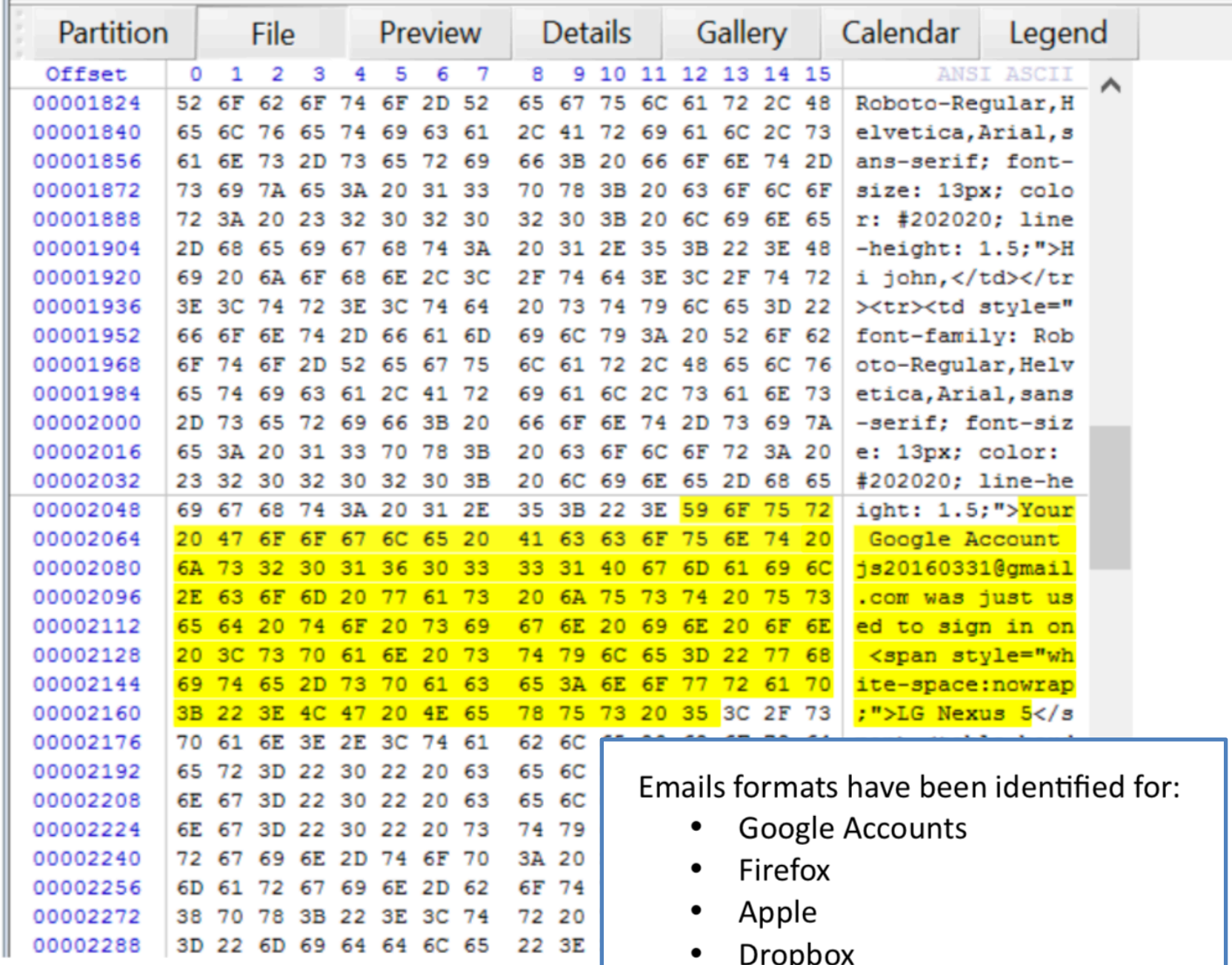
`\Users\[username]\AppData\Roaming\Mozilla\Firefox\Profiles\[profile_id]\weave\logs`

```
1460890759222    Sync.RemoteTabs    INFO    Generating tab list with filter
1460890759223    Sync.RemoteTabs    DEBUG    Processing client:
{"id":"2fhe0NcdN4n8","type":"client","name":"Firefox on John's iPhone","icon":"chrome://browser/skin/sync-
mobileIcon.png","tabs":[]}
1460890759223    Sync.RemoteTabs    DEBUG    remote tab:
http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_004_index.html
1460890759223    browserwindow.syncui    DEBUG    _loginFailed has sync
state=success.login
1460890759224    browserwindow.syncui    DEBUG    _loginFailed has sync
state=success.login
1460890759225    browserwindow.syncui    DEBUG    observed: weave:ui:sync:finish
1460890759226    Sync.RemoteTabs    DEBUG    remote tab:
http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_005_index.html
1460890759226    Sync.RemoteTabs    DEBUG    remote tab:
http://www.hargs.co.uk/resources/sample_data/synctriagekw-firefox_webpage_006_index.html
1460890759227    Sync.RemoteTabs    DEBUG    Processing client:
{"id":"1FbF8mpGzhSp","type":"client","name":"test-user's Firefox on DESKTOP-
KCJST4N","icon":"chrome://browser/skin/sync-desktopIcon.png","tabs":[]}
1460890759227    Sync.RemoteTabs    INFO    Final tab list has 2 clients with 3 tabs.
1460890760053    Sync.Tracker.Clients    DEBUG    Saving changed IDs to clients
```

Email Example




Android Exported
Android Exported2
iOS Exported
Windows 10 All Apps 03a
Windows 10 All Apps 03a,...
Windows 10 All Ap
\Users\John\AppData\Local\Comms\Unistore\data and subdirectories
Name
Type
Size
Created
.. = Unistore (99)
. = data (99)
0000000060000000030bfd.dat html 57.5 KB 18/05/2016...
0000000060000000073701.dat png 2.7 KB 18/05/2016...
0000000070000000030bfd.dat html 10.7 KB 18/05/2016...
0000000070000000073701.dat png 1.7 KB 18/05/2016...
0000000080000000008119.dat dat 56 B 18/05/2016...
0000000080000000030bfd.dat html 49.4 KB 18/05/2016...
0000000080000000073701.dat png 8.1 KB 18/05/2016...
0000000090000000030bfd.dat html 7.6 KB 18/05/2016...
0000000090000000073701.dat png 4.3 KB 18/05/2016...
0000000a000000030bfd.dat html 10.7 KB 18/05/2016...
0000000a000000073701.dat png 1.4 KB 18/05/2016...
0000000b000000030bfd.dat html 10.7 KB 18/05/2016...
0000000b000000073701.dat png 2.7 KB 18/05/2016...
0000000c000000030bfd.dat html 5.9 KB 18/05/2016...
Partition
File
Preview
Details
Gallery
Calendar
Legend
Sync
Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ANSI ASCII
00001824 52 6F 62 6F 74 6F 2D 52 65 67 75 6C 61 72 2C 48 Roboto-Regular,H
00001840 65 6C 76 65 74 69 63 61 2C 41 72 69 61 6C 2C 73 elvetica,Arial,s
00001856 61 6E 73 2D 73 65 72 69 66 3B 20 66 6F 6E 74 2D ans-serif; font-
00001872 73 69 7A 65 3A 20 31 33 70 78 3B 20 63 6F 6C 6F size: 13px; colo
00001888 72 3A 20 23 32 30 32 30 32 30 3B 20 6C 69 6E 65 r: #202020; line
00001904 2D 68 65 69 67 68 74 3A 20 31 2E 35 3B 22 3E 48 -height: 1.5;">H
00001920 69 20 6A 6F 68 6E 2C 3C 2F 74 64 3E 3C 2F 74 72 i john,</td></tr
00001936 3E 3C 74 72 3E 3C 74 64 20 73 74 79 6C 65 3D 22 ><tr><td style="
00001952 66 6F 6E 74 2D 66 61 6D 69 6C 79 3A 20 52 6F 62 font-family: Rob
00001968 6F 74 6F 2D 52 65 67 75 6C 61 72 2C 48 65 6C 76 oto-Regular,Helv
00001984 65 74 69 63 61 2C 41 72 69 61 6C 2C 73 61 6E 73 etica,Arial,sans
00002000 2D 73 65 72 69 66 3B 20 66 6F 6E 74 2D 73 69 7A -serif; font-siz
00002016 65 3A 20 31 33 70 78 3B 20 63 6F 6C 6F 72 3A 20 e: 13px; color:
00002032 23 32 30 32 30 32 30 3B 20 6C 69 6E 65 2D 68 65 #202020; line-he
00002048 69 67 68 74 3A 20 31 2E 35 3B 22 3E 59 6F 75 72 ight: 1.5;">Your
00002064 20 47 6F 6F 67 6C 65 20 41 63 63 6F 75 6E 74 20 Google Account
00002080 6A 73 32 30 31 36 30 33 33 31 40 67 6D 61 69 6C js20160331@gmail
00002096 2E 63 6F 6D 20 77 61 73 20 6A 75 73 74 20 75 73 .com was just us
00002112 65 64 20 74 6F 20 73 69 67 6E 20 69 6E 20 6F 6E ed to sign in on
00002128 20 3C 73 70 61 6E 20 73 74 79 6C 65 3D 22 77 68 <span style="wh
00002144 69 74 65 2D 73 70 61 63 65 3A 6E 6F 77 72 61 70 ite-space:nowrap
00002160 3B 22 3E 4C 47 20 4E 65 78 75 73 20 35 3C 2F 73 ;">LG Nexus 5</s
00002176 70 61 6E 3E 2E 3C 74 61 62 6C 65 20 62 6F 72 64 pan>.<table bord
00002192 65 72 3D 22 30 22 20 63 65 6C 6C 73 70 61 63 69 er="0" cellspaci
00002208 6E 67 3D 22 30 22 20 63 65 6C 6C 70 61 64 64 69 ng="0" cellpaddi
00002224 6E 67 3D 22 30 22 20 73 74 79 6C 65 3D 22 6D 61 ng="0" style="ma
00002240 72 67 69 6E 2D 74 6F 70 3A 20 34 38 70 78 3B 20 rgin-top: 48px;
00002256 6D 61 72 67 69 6E 2D 62 6F 74 74 6F 6D 3A 20 34 margin-bottom: 4
00002272 38 70 78 3B 22 3E 3C 74 72 20 76 61 6C 69 67 6E 8px;"><tr valign
00002288 3D 22 6D 69 64 64 6C 65 22 3E 3C 74 64 20 77 69 ="middle"><td wi

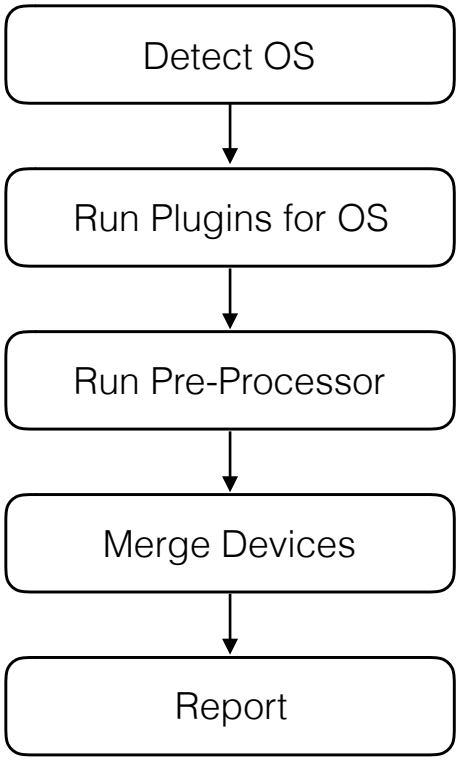


Emails formats have been identified for:

- Google Accounts
- Firefox
- Apple
- Dropbox

Prototype development

Prototype Overall Approach



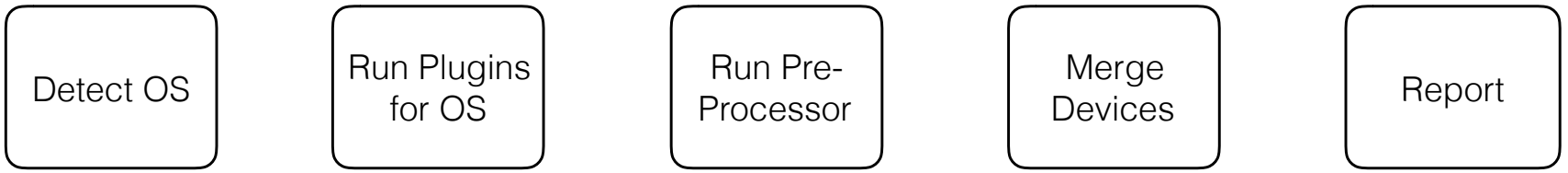
detects the OS/device at the target path e.g. Windows, iPhone Backup etc.

produces *SyncedDevice* objects.

adds obvious information e.g. if the device is an iPhone it must be running iOS.

takes all of the *SyncedDevice* objects and merges those that are deemed to be the same. Produces *MergedSyncedDevice* objects.

generates appropriate output based on the user supplied options.


Detect OS
Run Plugins for OS
Run Pre-Processor
Merge Devices
Report

Detect OS

Run Plugins for OS

Run Pre-Processor

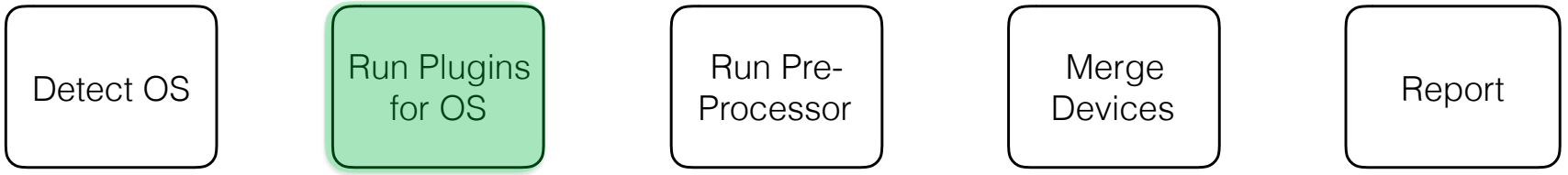
Merge Devices

Report

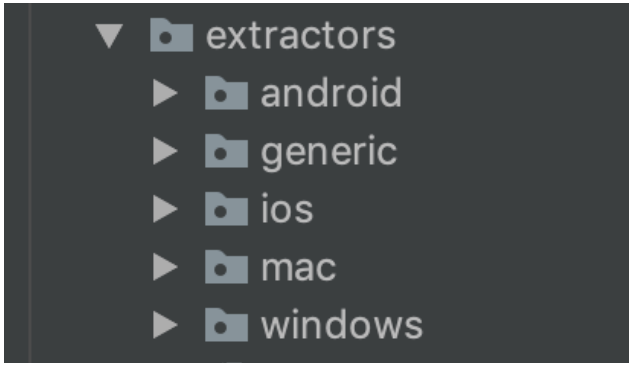

```
\Windows
\Users
```

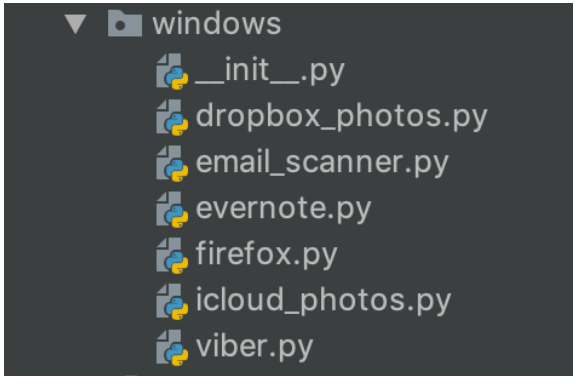
```
info.plist
Manifest.plist
Manifest.mbdb
```

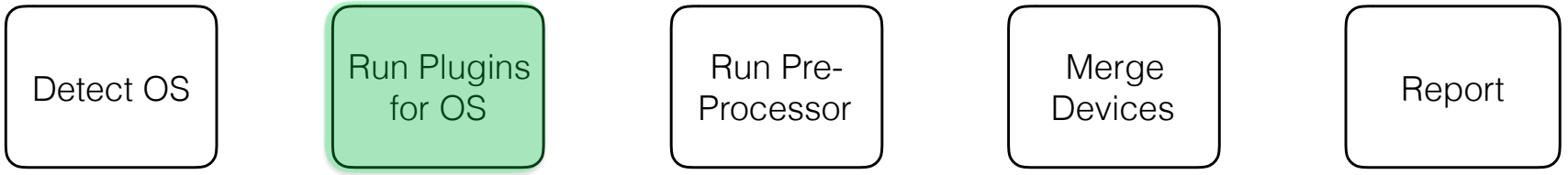
```
header:
'ANDROID BACKUP'
```



Target Device	Plugins Implemented
Windows	chrome – *extracts devices from SyncData.sqlite3* dropbox_photos – *scans exif data in photos for devices* email_scanner – *scans emails for 'account in use on device' emails* evernote – *scans note_attr table for references to devices* icloud_photos – *scans client.db for photos in server_items table* *viber – extracts phone number of device used for service*
Mac OS	-
iOS	chrome – *extracts devices from SyncData.sqlite3* firefox – *scans browser.db for clients* sms – *searches for references to service authentication messages*
Android	google_photos – *extracts exif data from remote_media table*



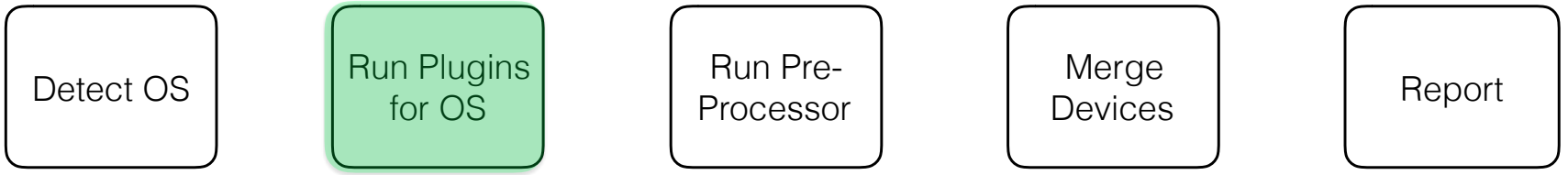




Target Device	Plugins Implemented
Windows	chrome – *extracts devices from SyncData.sqlite3* dropbox_photos – *scans exif data in photos for devices* email_scanner – *scans emails for 'account in use on device' emails* evernote – *scans note_attr table for references to devices* icloud_photos – *scans client.db for photos in server_items table* *viber – extracts phone number of device used for service*
Mac OS	-
iOS	chrome – *extracts devices from SyncData.sqlite3* firefox – *scans browser.db for clients* sms – *searches for references to service authentication messages*
Android	google_photos – *extracts exif data from remote_media table*

```
class SyncedDevice(dfpy.types.device.Device):

    def __init__(self):
        self.name = '[Unknown]'
        self.make = '[Unknown]'
        self.model = '[Unknown]'
        self.os = '[Unknown]'
        self.installed_software = []
        self.events = []
        self.info = {}
        self.source_file = ''
        self.__log = ''
```



Target Device	Plugins Implemented
Windows	chrome – *extracts devices from SyncData.sqlite3* dropbox_photos – *scans exif data in photos for devices* email_scanner – *scans emails for 'account in use on device' emails* evernote – *scans note_attr table for references to devices* icloud_photos – *scans client.db for photos in server_items table* *viber – extracts phone number of device used for service*
Mac OS	-
iOS	chrome – *extracts devices from SyncData.sqlite3* firefox – *scans browser.db for clients* sms – *searches for references to service authentication messages*
Android	google_photos – *extracts exif data from remote_media table*

```
logging.debug('Not seen a {} device before - making new'.format(poss_os))
new_device = core.synced_device.SyncedDevice()
new_device.source_file = path_to_db
new_device.os = poss_os
new_device.installed_software.append('Evernote')
if db_author:
    new_device.info['Evernote User'] = db_author
```

Before Pre-Processor

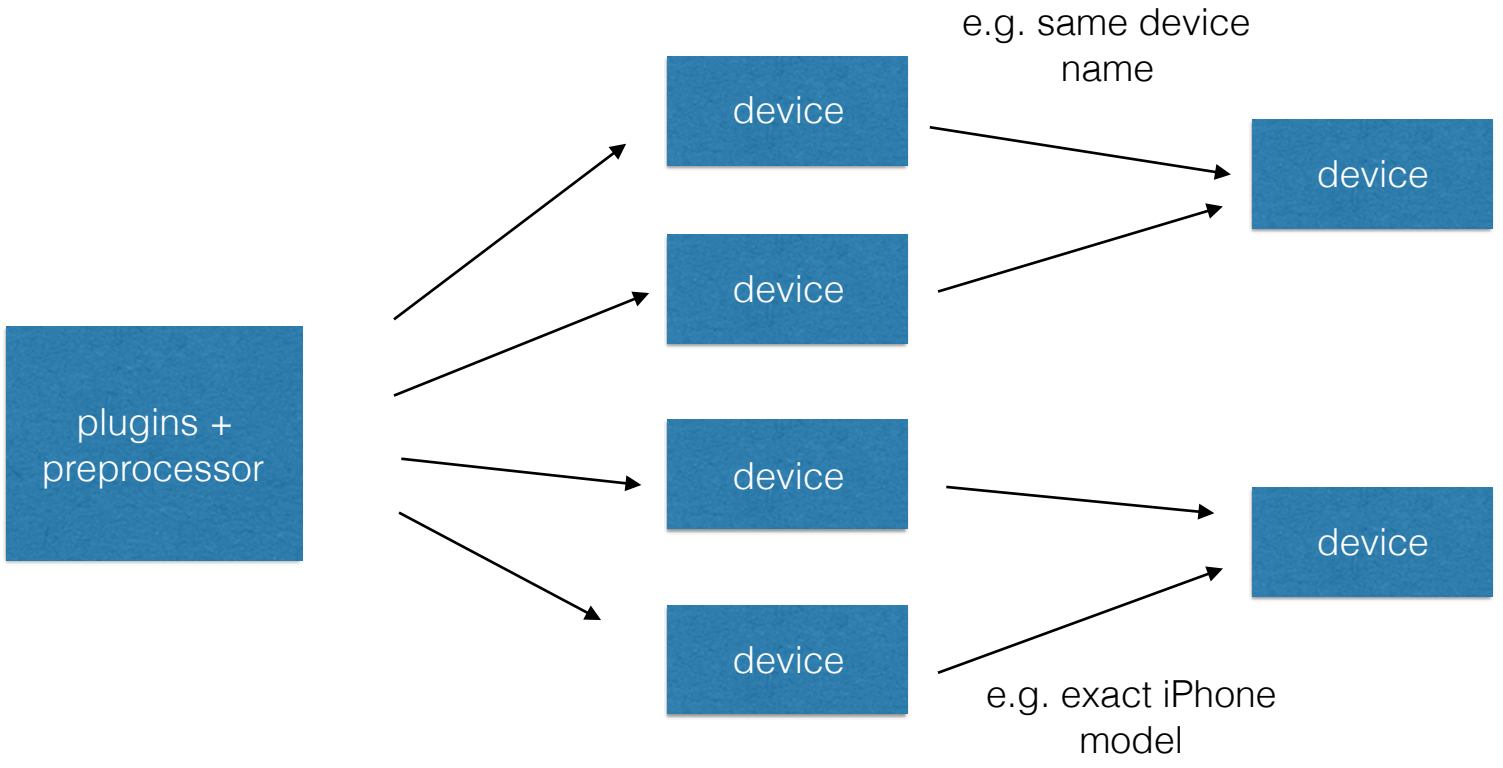
Name	Make	Model	OS
DESKTOP-KCJST4N	[Unknown]	[Unknown]	Windows
John's iPhone	[Unknown]	[Unknown]	iOS
John's iPhone	[Unknown]	iPhone 4S	iOS 9.3
JOHN-DESKTOP	[Unknown]	[Unknown]	Windows
john-desktop	[Unknown]	[Unknown]	[Unknown]
Nexus 5	[Unknown]	[Unknown]	Android
VF-895N	[Unknown]	[Unknown]	Android
[Unknown]	Apple	iPhone 4S	[Unknown]
[Unknown]	Apple	iPhone 4S	[Unknown]
[Unknown]	Apple	iPhone 4S	[Unknown]
[Unknown]	LG	Nexus 5	[Unknown]
[Unknown]	LGE	Nexus 5	[Unknown]

After Pre-Processor

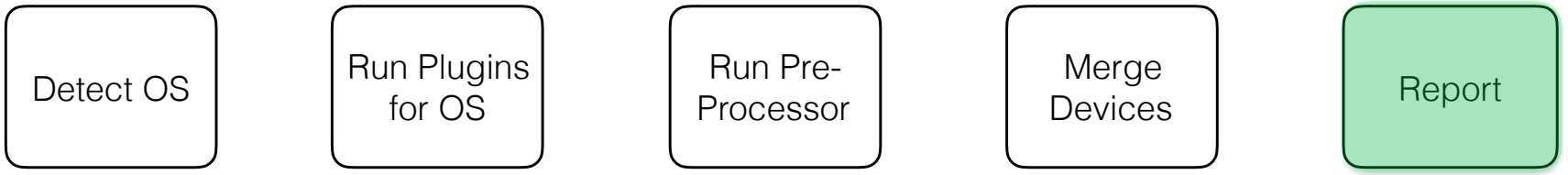
Name	Make	Model	OS
DESKTOP-KCJST4N	[Unknown]	[Unknown]	Windows
John's iPhone	[Apple]	[Unknown]	iOS
John's iPhone	[Apple]	iPhone 4S	iOS 9.3
JOHN-DESKTOP	[Unknown]	[Unknown]	Windows
john-desktop	[Unknown]	[Unknown]	[Unknown]
Nexus 5	[Unknown]	[Unknown]	Android
VF-895N	[Unknown]	[Unknown]	Android
[Unknown]	Apple	iPhone 4S	[iOS]
[Unknown]	Apple	iPhone 4S	[iOS]
[Unknown]	Apple	iPhone 4S	[iOS]
[Unknown]	LG	Nexus 5	[Android]
[Unknown]	LGE	Nexus 5	[Android]

```
if each.os == '[Unknown]':
    inferred_os = core.device_entity_finder.infer_os_from_model(each.model)  # try from model
    if inferred_os:
        logging.info('Inferred os \'{}\' from \'{}\' in {}'.format(inferred_os, each.model, each.name))
        each.os = inferred_os
        preprocess_updates += 1
if each.make == '[Unknown]':
    inferred_make = core.device_entity_finder.infer_make_from_model(each.model)
    if inferred_make:
        logging.info('Inferred make \'{}\' from \'{}\' in {}'.format(inferred_make, each.model, each.name))
        each.make = inferred_make
        preprocess_updates += 1
if each.make == '[Unknown]':
    inferred_make = core.device_entity_finder.infer_make_from_os(each.os)
    if inferred_make:
```

Detect OS | Run Plugins for OS | Run Pre-Processor | Merge Devices | Report




```
def merge_into_list_if_you_can(self, new_device):
    """This attempts to merge the supplied device into the MergedDevice list"""
    for each_merged_device in self.devices:
        should_merge = each_merged_device.should_be_merged(new_device)
        if should_merge:
            logging.debug('Should attempt merge.')
            each_merged_device.add(new_device)
            return each_merged_device # once merged return the new merged device
    return None
```



This is basically the output, so lets have a look at a complete run of the tool…

Usage

```
usage: sync_triage.exe [-h] [--details] [--debug] [--timeline] path

Perform triage based on syncronisation artefacts

positional arguments:
  path        path to target device. this can be the root of a mounted disk
              image, an iOS backup folder, or an Android .ab backup file.

optional arguments:
  -h, --help  show this help message and exit
  --details   prints details of discovered devices rather than a summary
  --debug     adds detail to log file
  --timeline  prints a basic timeline of activity on the discovered devices
```

```
PS C:\Users\chris\Development\synctriage\dist> .\sync_triage.exe E:\[root]
Detected OS: vista+
Running Windows plugins...
Device detection completed.
Total potential devices detected: 32

Pre-processing to infer OS etc...
Made 19 updates using pre-processor

Merging 32 devices... now 21 total devices

====================
NAMED DEVICE LIST (5) (MERGED)
====================
+-----------------+----------+----------+---------+------+----------+--------+------+
| Name            | Make     | Model    | OS      | Refs | Software | Events | Info |
+-----------------+----------+----------+---------+------+----------+--------+------+
| DESKTOP-KCJST4N | [Unknown] | [Unknown] | Windows | 1    | 1        | 0      | 0    |
| John's iPhone   | Apple    | iPhone 4S | iOS 9.3 | 6    | 4        | 3      | 6    |
| john-desktop    | [Unknown] | [Unknown] | Windows | 2    | 2        | 0      | 2    |
| Nexus 5         | [Unknown] | [Unknown] | Android | 1    | 1        | 0      | 2    |
| VF-895N         | [Unknown] | [Unknown] | Android | 1    | 1        | 0      | 0    |
+-----------------+----------+----------+---------+------+----------+--------+------+
====================
UNNAMED DEVICE LIST (16) (MERGED)
====================
+-----------+-----------+-----------+------------+------+----------+--------+------+
| Name      | Make      | Model     | OS         | Refs | Software | Events | Info |
+-----------+-----------+-----------+------------+------+----------+--------+------+
| [Unknown] | LG        | Nexus 5   | [Android]  | 1    | 0        | 0      | 1    |
| [Unknown] | LGE       | Nexus 5   | [Android]  | 5    | 0        | 5      | 0    |
| [Unknown] | [Apple]   | [Unknown] | Mac        | 1    | 0        | 0      | 1    |
| [Unknown] | [Apple]   | [Unknown] | [iOS]      | 1    | 0        | 7      | 0    |
| [Unknown] | [Apple]   | [Unknown] | iOS        | 1    | 1        | 3      | 0    |
| [Unknown] | [Apple]   | [Unknown] | iOS 9.3    | 1    | 2        | 0      | 0    |
| [Unknown] | [Apple]   | iPhone    | [iOS]      | 2    | 2        | 0      | 0    |
| [Unknown] | [Unknown] | [Unknown] | Android    | 1    | 2        | 0      | 0    |
| [Unknown] | [Unknown] | [Unknown] | Android    | 1    | 1        | 1      | 0    |
| [Unknown] | [Unknown] | [Unknown] | Windows    | 1    | 1        | 0      | 1    |
| [Unknown] | [Unknown] | [Unknown] | Windows    | 1    | 1        | 0      | 1    |
| [Unknown] | [Unknown] | [Unknown] | Windows    | 1    | 1        | 0      | 1    |
| [Unknown] | [Unknown] | [Unknown] | Windows    | 1    | 1        | 0      | 0    |
| [Unknown] | [Unknown] | [Unknown] | Windows    | 1    | 1        | 2      | 1    |
| [Unknown] | [Unknown] | [Unknown] | Windows 10 | 1    | 2        | 0      | 0    |
| [Unknown] | [Unknown] | [Unknown] | Windows 10 | 1    | 2        | 0      | 0    |
+-----------+-----------+-----------+------------+------+----------+--------+------+
```

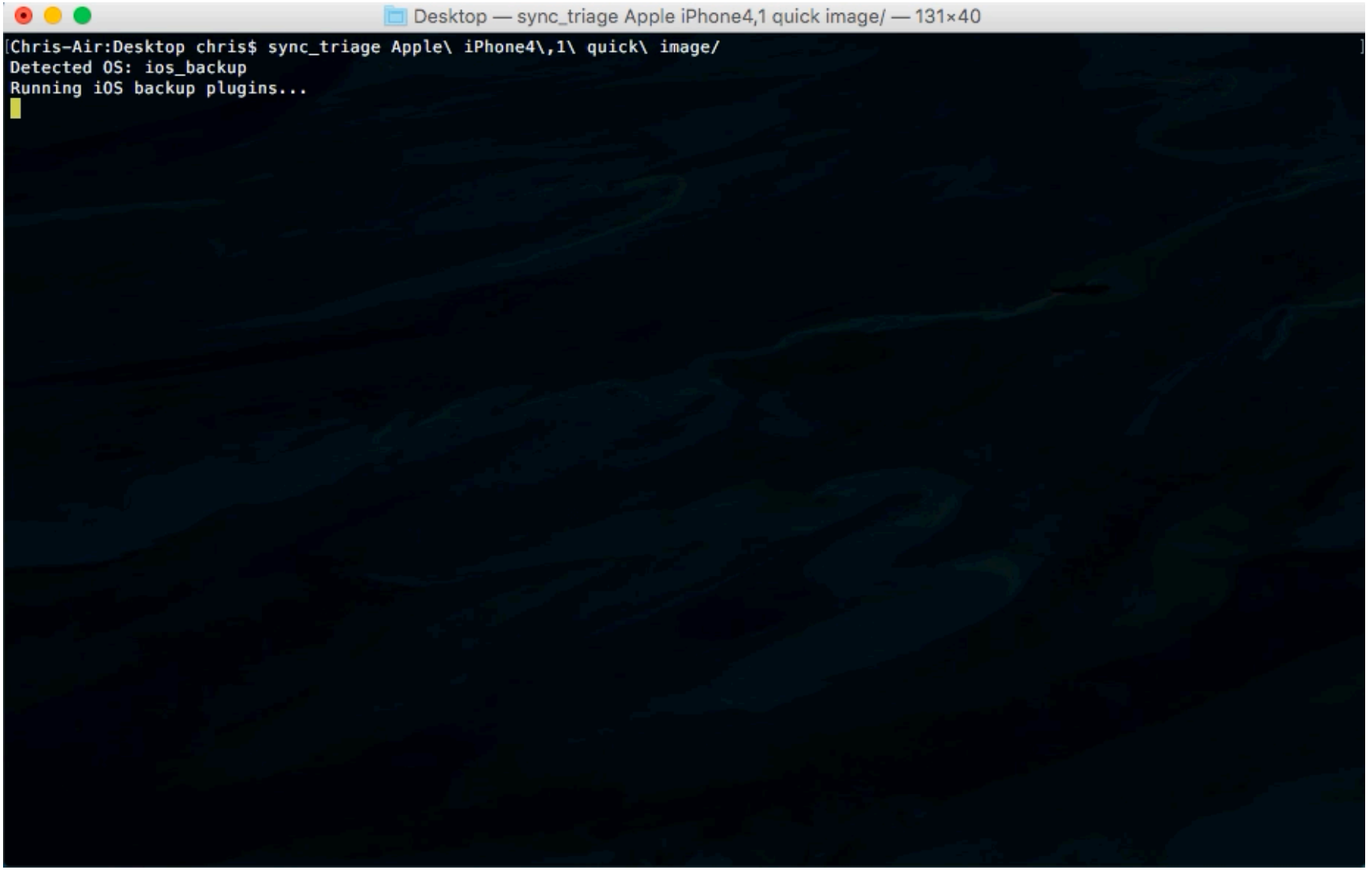
Details view of a device

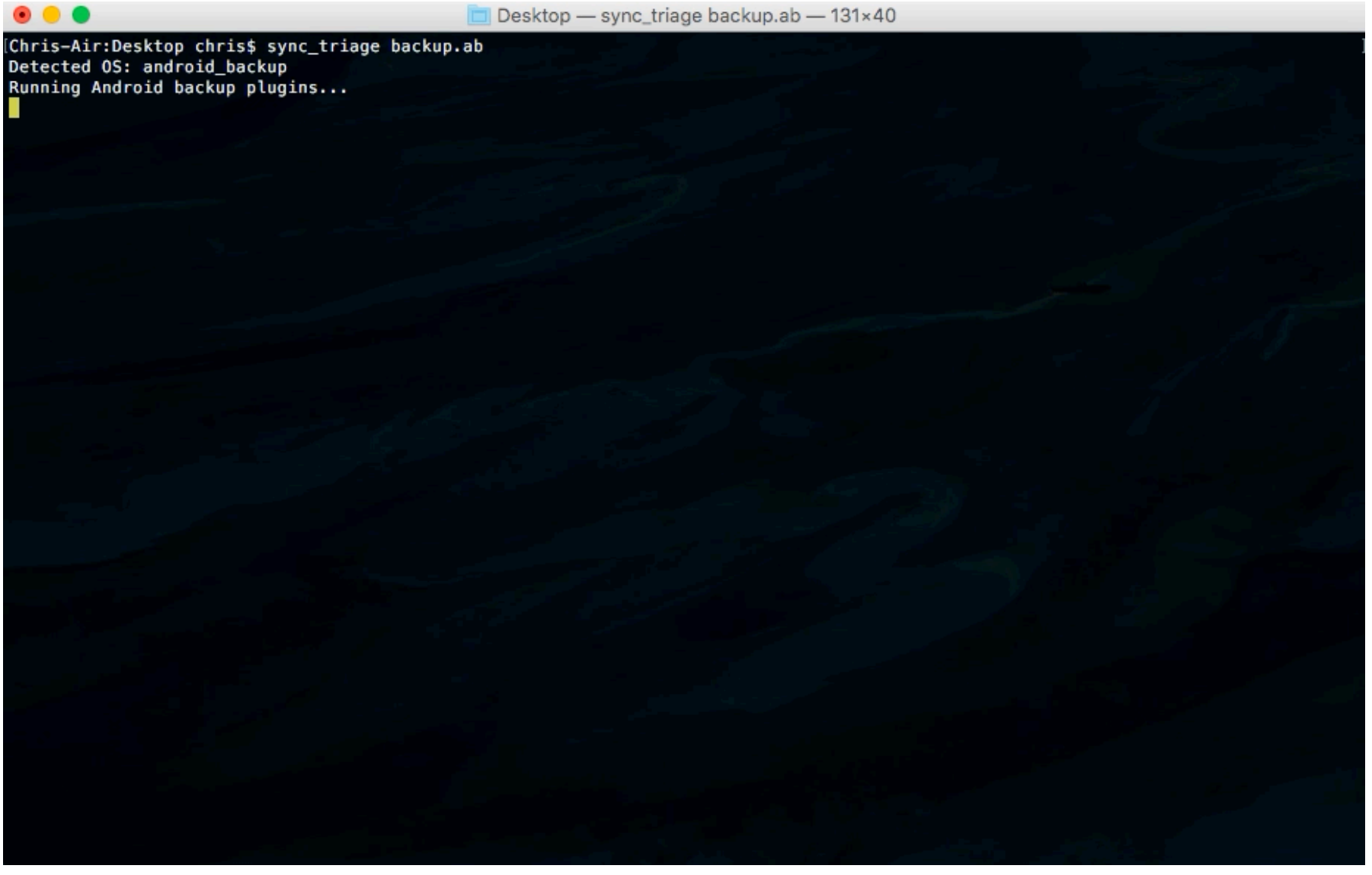
```
====================
DISCOVERED DEVICE
Name: John's iPhone
Make: Apple
Model: iPhone 4S
OS: iOS 9.3
Software:
        Chrome IOS-PHONE 50.0.2661.95
        Facetime
        iCloud
        iMessage
Info:
        EXIF Image Software:9.3
        chrome url visit:https://www.google.co.uk/search?q=synctriage-chrome+google+search+3&rlz=1CDGOYI_enGB688&oq=syn
e=UTF-8
        chrome url visit[2]:http://www.hargs.co.uk/resources/sample_data/synctriagekw-chrome_webpage_006_index.html
        chrome url visit[3]:http://www.hargs.co.uk/resources/sample_data/synctriagekw-chrome_webpage_005_index.html
        chrome url visit[4]:http://www.hargs.co.uk/resources/sample_data/synctriagekw-chrome_webpage_004_index.html
        iCloud Account:js20160331@gmail.com
Events:
        2016-04-17 15:18:27     51.[redacted]N, 1.[redacted]W           Picture was taken
        2016-04-17 15:18:31     51.[redacted]N, 1.[redacted]W           Picture was taken
        2016-04-20 18:26:26     51.[redacted]N, 1.[redacted]W           Picture was taken
Base Synced Devices: (6)
        John's iPhone           [Apple]     [Unknown]   iOS         e:\[root]\Users\John\AppData\Local\Google\Chrome\User Dat
        John's iPhone           [Apple]     iPhone 4S   iOS 9.3     e:\[root]\Users\John\AppData\Local\Comms\Unistore\data\3\
        [Unknown]               Apple       iPhone 4S   [iOS]       e:\[root]\Users\John\Dropbox\Camera Uploads\2016-04-20 18
        [Unknown]               Apple       iPhone 4S   [iOS]       e:\[root]\Users\John\Dropbox\Camera Uploads\2016-04-17 15
        [Unknown]               Apple       iPhone 4S   [iOS]       e:\[root]\Users\John\Dropbox\Camera Uploads\2016-04-17 15
        [Unknown]               [Apple]     iPhone 4S   iOS 9.3     e:\[root]\Users\John\AppData\Local\Comms\Unistore\data\3\
```

Timeline view of all devices

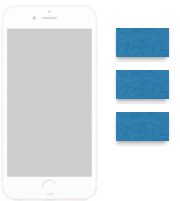
```
====================
UNIVERSAL TIMELINE
==================
2016-04-17 14:16:21*                                  Photograph taken                [iOS]
2016-04-17 14:18:27*                                  Photograph taken                [iOS]
2016-04-17 14:18:31*                                  Photograph taken                [iOS]
2016-04-17 15:18:27     51.                 1.        Picture was taken               John's iPhone
2016-04-17 15:18:31     51.                 1.        Picture was taken               John's iPhone
2016-04-20 17:26:26*                                  Photograph taken                [iOS]
2016-04-20 18:26:26     51.                 , 1.      Picture was taken               John's iPhone
2016-04-21 21:22:52*                                  EverNote note created           Windows
2016-04-21 21:23:18*                                  EverNote note updated           Windows
2016-04-21 21:30:22*                                  EverNote note created           iOS
2016-04-21 21:31:14*                                  EverNote note updated           iOS
2016-04-21 21:32:43*    51.                 , -1.     EverNote note created           iOS
2016-04-21 21:32:59*                                  Photograph taken                [iOS]
2016-04-24 09:04:37*                                  Photograph taken                [iOS]
2016-05-15 11:22:25*                                  Photograph taken                [iOS]
2016-05-17 17:03:20     51.                 , 1.      Picture was taken               Nexus 5
2016-05-18 09:53:09*    51.                 -1.       EverNote note created           Android
2016-05-18 10:53:44     51.                 N, 1.     Picture was taken               Nexus 5
2016-05-18 10:54:06     51.                 N, 1.     Picture was taken               Nexus 5
2016-05-18 10:55:33     51.                 N, 1.     Picture was taken               Nexus 5
2016-05-19 11:22:49     51.                 N, 1.     Picture was taken               Nexus 5
```


Desktop — sync_triage /Volumes/Untitled/ — 131×40
Chris-Air:Desktop chris$ sync_triage /Volumes/Untitled/
Detected OS: vista+
Running Windows plugins...


Desktop — sync_triage Apple iPhone4,1 quick image/ — 131×40
Chris-Air:Desktop chris$ sync_triage Apple\ iPhone4\,1\ quick\ image/
Detected OS: ios_backup
Running iOS backup plugins...


Desktop — sync_triage backup.ab — 131×40
Chris-Air:Desktop chris$ sync_triage backup.ab
Detected OS: android_backup
Running Android backup plugins...

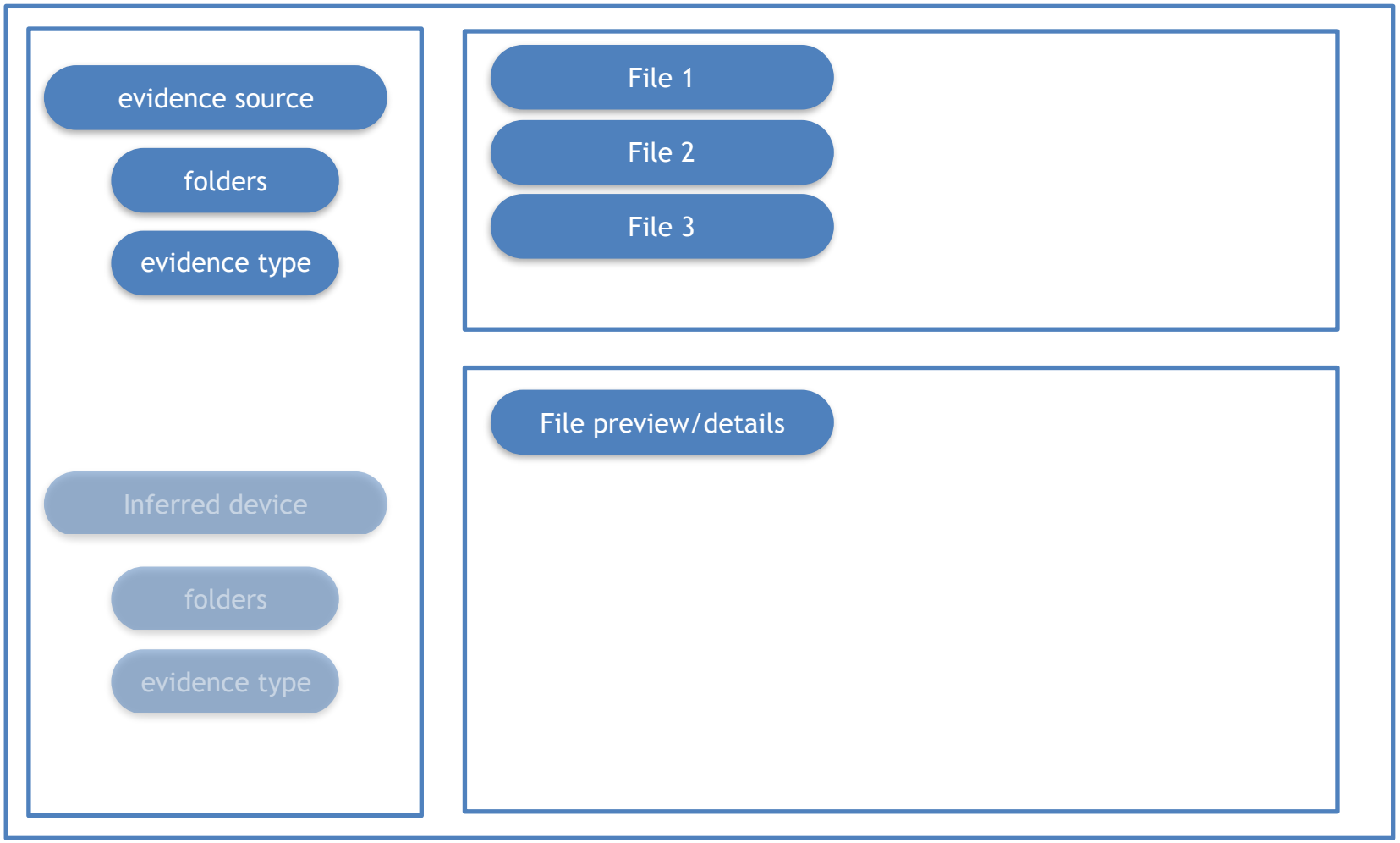
How could this be used?



How could this be used?

- Existence of devices
- Software installed on a device
- Files present on other devices, and that they may have originated on a certain device.
- Locations in which a specific device was in use
- Timeline of events on a device

Forensic tool integration?



Further work

- Re-brand as ‘inferred devices’
- User assisted merging of detected devices

- More/updated plugins for additional applications
- Integration of MacOS, rooted android, cloud data
- Multiple source devices (replacing inferred ones)

- Use at scene to detect devices that have not yet been seized
- Playbook for ‘given a set of devices’, which should be examined to get the most from the overall investigation

Questions?

christopher.hargreaves@cs.ox.ac.uk

chris@hargs.co.uk