

Biome, la nouvelle pépite pour les smartphones et les ordinateurs Apple

5 avril 2023

Jean-Philippe Noat, Expert judiciaire, Digital Intelligence Expert



- Spécialiste en intelligence digitale (Engagement team Cellebrite)
- 20 ans d'expérience en assistance LE
- 7 ans expérience formateur Cellebrite
- EnCE CCME, CFCE
- Plus de 320 différents dossiers pour différentes activités judiciaires internationaux ou locales (Monaco, France, Belgique, Luxembourg etc...)
- Expert près la cours pénale internationale de La Haye



We help you make
more possible even

We help you make
a safer world possible by
prote

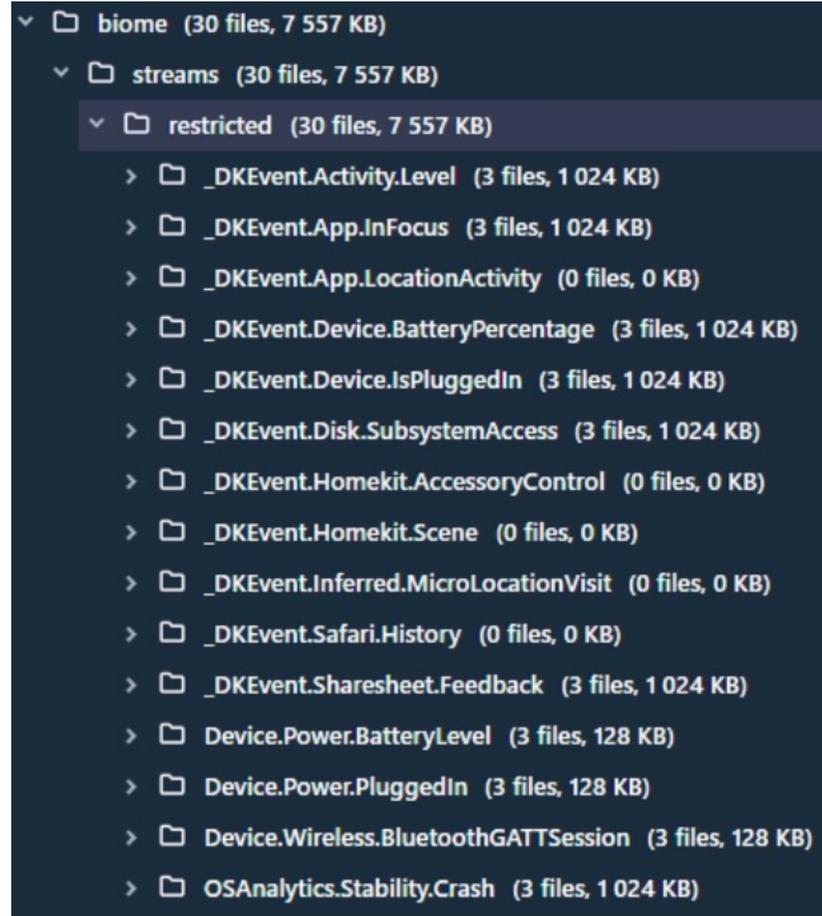


EXAMEN DES BASES CLASSIQUES (KNOWLEDGE C / POWERLOG) avec iOS 16

- Powerlog : peu de changements
- Knowledge C : données limitées (et disparition progressive) (source très utile sur ce que faisait un utilisateur à une date précise).
- Nouvelles sources de données trouvées : BIOME (et encore plus riche que le knowledge c)
- Liées à l'intelligence artificielle et l'analyse prédictive d'Apple.
- Tend à regrouper tous les services d'Apple afin de prédire l'utilisation du téléphone. (moteur intelligence artificielle)
- Données accessibles en FFS.

QUELQUES SOURCES DE BIOME

/root/private/var/db/biome/streams/restricted



QUELQUES SOURCES DE BIOME

/root/private/var/mobile/library/biome/streams/restricted

```
▼ 📁 streams (135 files, 41 880 KB)
  > 📁 public (39 files, 15 366 KB)
  ▼ 📁 restricted (96 files, 26 513 KB)
    > 📁 _DKEvent.App.ClipUsage (0 files, 0 KB)
    > 📁 _DKEvent.App.Install (3 files, 1 024 KB)
    > 📁 _DKEvent.Audio.InputRoute (3 files, 1 024 KB)
    > 📁 _DKEvent.Audio.OutputRoute (0 files, 0 KB)
    > 📁 _DKEvent.Carplay.IsConnected (0 files, 0 KB)
    > 📁 _DKEvent.Charging.SmartTopOffCheckpoint (0 files, 0 KB)
    > 📁 _DKEvent.Com.apple.spotlightviewer.events (0 files, 0 KB)
    > 📁 _DKEvent.Das.ActivityRuntime (3 files, 1 024 KB)
    > 📁 _DKEvent.Dasd.Activityprofile (3 files, 1 024 KB)
    > 📁 _DKEvent.Dasd.Batterytemperature (3 files, 1 024 KB)
    > 📁 _DKEvent.Dasd.ControlEffort (3 files, 1 024 KB)
    > 📁 _DKEvent.Dasd.WidgetRefresh (3 files, 1 024 KB)
    > 📁 _DKEvent.Dasd.WidgetView (3 files, 1 024 KB)
    > 📁 _DKEvent.DefaultPaired.Nearby (0 files, 0 KB)
    > 📁 _DKEvent.Device.IsLockedImputed (3 files, 1 024 KB)
    > 📁 _DKEvent.Discoverability.Usage (3 files, 1 024 KB)
```

```
> 📁 Device.ScreenLocked (3 files, 128 KB)
> 📁 Device.Wireless.AirplaneMode (0 files, 0 KB)
> 📁 Device.Wireless.Bluetooth (0 files, 0 KB)
> 📁 Device.Wireless.WiFi (3 files, 128 KB)
> 📁 feedbackSocialHighlights (0 files, 0 KB)
> 📁 FrontBoard.DisplayLayout (0 files, 0 KB)
> 📁 iCloud.Subscription (3 files, 128 KB)
> 📁 InferredMode (0 files, 0 KB)
> 📁 Location.HashedCoordinates (3 files, 1 024 KB)
> 📁 MailContent (0 files, 0 KB)
> 📁 MessagesContent (0 files, 0 KB)
> 📁 MicroLocationRestrictedLocalization (0 files, 0 KB)
> 📁 NewsArticleView (0 files, 0 KB)
> 📁 NotesContent (0 files, 0 KB)
> 📁 OSAnalytics.Hardware.Reliability (3 files, 1 024 KB)
> 📁 ParsecSearchEngagement (0 files, 0 KB)
> 📁 PhotosKnowledgeGraphEnrichment (0 files, 0 KB)
> 📁 PhotosPhotoView (0 files, 0 KB)
> 📁 RemindersContent (0 files, 0 KB)
> 📁 SafariPageView (0 files, 0 KB)
```

```
> 📁 SiriMemoryReferenceResolutionStream (0 files, 0 KB)
> 📁 SiriPrivateLearningSELFEvent (0 files, 0 KB)
> 📁 SiriQuery (0 files, 0 KB)
> 📁 ThirdPartyAppContent (0 files, 0 KB)
> 📁 UserActivityMetadata (3 files, 1 024 KB)
> 📁 UserProofingMetadata (0 files, 0 KB)
```

```
> 📁 _DKEvent.Discoverability.Usage (3 files, 1 024 KB)
> 📁 _DKEvent.Display.Orientation (3 files, 1 024 KB)
> 📁 _DKEvent.Family.Prediction (3 files, 1 024 KB)
> 📁 _DKEvent.Inferred.MicroLocationVisit (0 files, 0 KB)
> 📁 _DKEvent.Inferred.Motion (3 files, 1 024 KB)
> 📁 _DKEvent.Keybag.IsLocked (3 files, 1 024 KB)
> 📁 _DKEvent.Photos.Engagement.0To1Seconds (3 files, 1 024 KB)
> 📁 _DKEvent.Photos.Engagement.1To2Seconds (3 files, 1 024 KB)
> 📁 _DKEvent.Siri.Ui (0 files, 0 KB)
> 📁 _DKEvent.System.TLC (3 files, 1 024 KB)
> 📁 _DKEvent.User.IsFirstBacklightOnAfterWakeup (3 files, 1 024 KB)
> 📁 _DKEvent.UserInteraction.AppDirectory (3 files, 1 024 KB)
> 📁 _DKEvent.Widgets.Viewed (0 files, 0 KB)
> 📁 _DKEvent.Wifi.Connection (3 files, 1 024 KB)
> 📁 Audio.Route (3 files, 1 024 KB)
> 📁 ContextualUnderstanding.AmbientLight (3 files, 1 024 KB)
> 📁 Device.Display.Appearance (3 files, 128 KB)
> 📁 Device.Display.InterfaceOrientation (3 files, 128 KB)
> 📁 Device.Keybag.Locked (3 files, 128 KB)
> 📁 Device.Power.LowPowerMode (3 files, 128 KB)
> 📁 Device.ScreenLocked (3 files, 128 KB)
```

DES SOURCES LA OU ON NE LES ATTEND PAS

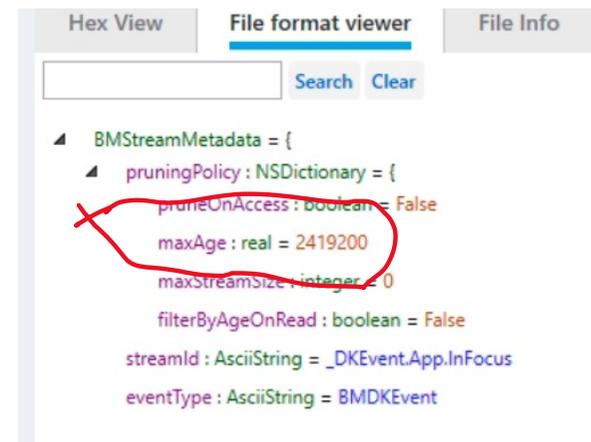
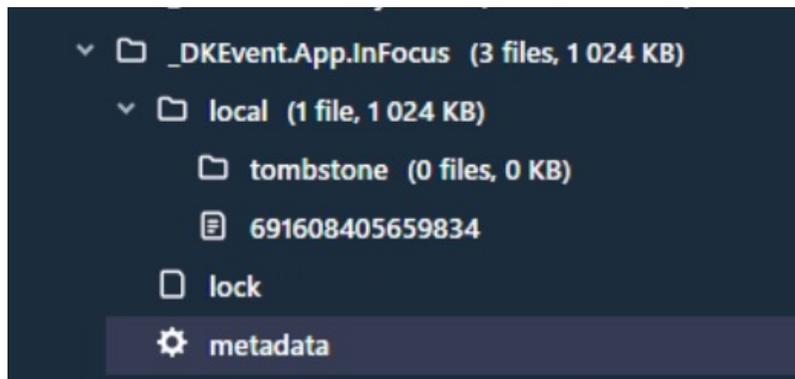
/root/private/var/mobile/Library/DuetExpertCenter/streams

- streams (103 files, 417 806 KB)
 - ActivitySuggestionFeedback (0 files, 0 KB)
 - appLaunchInferredMode (4 files, 16 384 KB)
 - ATXBiomeSuggestedHomePageStream (0 files, 0 KB)
 - blending (0 files, 0 KB)
 - blendingActionLockScreen (4 files, 16 384 KB)
 - blendingActionSpltUnknown (4 files, 16 384 KB)
 - blendingAppDirectory (4 files, 16 384 KB)
 - blendingAppSwitcher (4 files, 16 384 KB)
 - blendingFaceTimeZKW (4 files, 16 384 KB)
 - blendingHomeScreen (4 files, 16 384 KB)
 - blendingMediaControls (4 files, 16 384 KB)
 - blendingMegadomeIntent (4 files, 16 384 KB)
 - blendingShortcutsEditor (4 files, 16 384 KB)
 - blendingSiriDiscoverability (4 files, 16 384 KB)
 - blendingSpotlightUnknown (4 files, 16 384 KB)
 - blendingUIActionLockScreen (0 files, 0 KB)
 - blendingUIAppDirectory (4 files, 16 384 KB)
 - blendingUIHomeScreen (4 files, 16 384 KB)
 - blendingUIShortcutsEditor (0 files, 0 KB)
 - blendingUISpotlightUnknown (4 files, 16 384 KB)
 - clientModel (5 files, 24 576 KB)
 - digestOnboardingAppSelectionLoggingEvent (0 files, 0 KB)
 - digestOnboardingLoggingEvent (0 files, 0 KB)
 - digestOnboardingSuggestionLoggingEvent (0 files, 0 KB)
 - ERM (4 files, 16 384 KB)

- ERM (4 files, 16 384 KB)
- faceGallery (0 files, 0 KB)
- homeScreen (0 files, 0 KB)
- lightweightClientModelCacheUpdates (4 files, 16 384 KB)
- location (4 files, 16 384 KB)
- missedNotificationRankingLoggingEvent (0 files, 0 KB)
- modeConfigurationUIFlowLoggingEvent (0 files, 0 KB)
- notificationDigestLoggingEvents (0 files, 0 KB)
- notificationGroupEvent (4 files, 16 384 KB)
- notificationSuggestion (4 files, 16 384 KB)
- notificationSuggestionDelivery (3 files, 8 192 KB)
- notificationSuggestionInteraction (4 files, 16 384 KB)
- predictionContext (4 files, 16 384 KB)
- proactiveSuggestionUIFeedbackResults (3 files, 8 192 KB)
- proactiveSuggestionUIFeedbackResultStreamWriterBookmarkURL
- userNotificationEvents (4 files, 16 384 KB)

EXEMPLES BIOME : APP IN FOCUS

- Pas de documentation Apple (comme pour le knowledgeC / les logs unifiés)
- Seule la recherche et l'expérimentation permettent de valider les résultats
- On peut trouver 2 fichiers : metadata.plist et le fichier BIOM lui-même au format SEGB
- Examen du maxAge : 2419200 secondes
- Cela correspond à 28 jours.
- Format différent suivant les Biome



EXEMPLES BIOME : User Notifications Events

```

    userNotificationEvents (4 files, 16 384 KB)
    local (2 files, 16 384 KB)
    > tombstone (1 file, 8 192 KB)
        691610890741130
    lock
    metadata

    BMStreamMetadata = {
    pruningPolicy : NSDictionary = {
        pruneOnAccess : boolean = False
        maxAge : real = 2419200
        maxStreamSize : integer = 0
        filterByAgeOnRead : boolean = False
    }
    streamId : AsciiString = userNotificationEvents
    eventType : AsciiString = ATXUserNotificationLoggingEvent
  
```

- Les notifications sont accessibles même si l'application a été effacée.
- Titres de message qui peuvent indiquer une information

```

    Attributes : = {
      State : = Written
      Create Timestamp : = 08/03/2023 15:05:41
      Modify Timestamp : = 08/03/2023 15:05:41
      CRC32 : = -102750478
      Data Version : = 2
    }
    Payload : Complex = {
    1 : = [
      Complex = {
      1 : = [
      2 : = [
        LengthValue = C09CAB7C-055E-4328-BF9A-C1AEC376010E
      3 : = [
        LengthValue = FIC 2023
      5 : = [
        LengthValue = J-30 : Rejoignez-nous au FIC 2023
      6 : = [
        Varint = 0
      8 : = [
        LengthValue = ch.protonmail.protonmail
      9 : = [
  
```

```

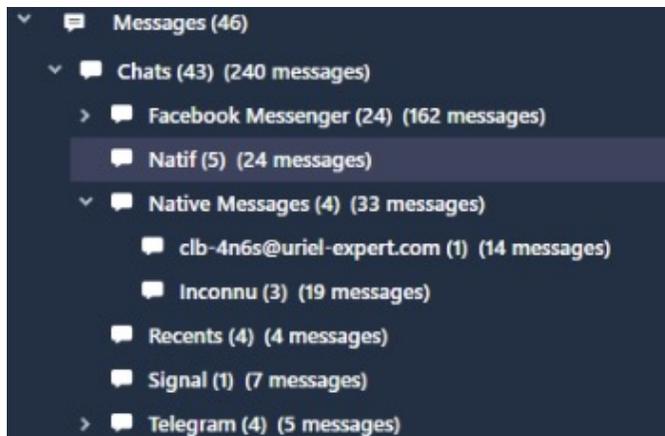
.....K..z..A(...
.....".z..A..".z..A...
.....v.f.H..A.$AF424848-B
14F-4427-9B40-3F3EE9EF88C2..S
NCF Connect*%.. vos vacances,
pr..t... r..servez !0.B.ch.p
rotonmail.protonmailJ.R 5r6pm
k7zrknt3n3uul55iku64h4k2uheb.
ch.protonmail.protonmailp.x..
.....".z..A(..
.....#..z..A..#..z..A
Q..N.....C.m..A.$C09CAB7
C-055E-4328-BF9A-C1AEC376010E
..FIC 2023*!J-30 : Rejoignez-
nous au FIC 20230.B.ch.proton
mail.protonmailJ.R 5r6pmk7zrk
nt3n3uul55iku64h4k2uheb.ch.pr
otonmail.protonmailp.x.....
.....r.#..z..A(.....
.....RL)..A..RL)..AM....
.....q.L)..A.$9A95C65D-E08
5-4D74-845E-94BA9FB30CAF..Chr
is Walsh*.RE: [IACIS] PLOT Fi
le0.B.ch.protonmail.protonmai
lJ.R 5r6pmk7zrknt3n3uul55iku6
4h4k2uheb.ch.protonmail.proto
nmailp.x.....6
.RL)..A(...../3..
..A./3....A.....
.A.$1C4D9338-5F61-466E-A4A4-9
EA3C3EE6419..Miles & More*,Ac
t fast, and get extra miles w
  
```

Exemples BIOME : Utilisation de Siri

```
692382711295337 x sms.db x Conseils et astuces x Résumé d'extraction (2) x Journal Utilisation des applic... x
Affichage hexadécimal Info du fichier
Affichage hexadécimal
00000000 00 08 00 00 00 00 00 00 88 10 11 10 76 A2 C4 41 09 00 00 00 36 39 32 33 38 32 37 31 31 32 .....v..A....6923827112
0000001E 39 35 33 33 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 45 47 42 85 00 00 00 95337.....SEGB....
0000003C 01 00 00 00 9A CD A5 FB 75 A2 C4 41 9A CD A5 FB 75 A2 C4 41 0B 8A 46 89 02 00 00 00 0A 24 .....u..A....u..A..F.....$
0000005A 39 46 41 32 36 42 46 38 2D 44 43 46 44 2D 34 45 42 30 2D 39 32 34 30 2D 44 36 44 42 33 37 9FA26BF8-DCFD-4EB0-9240-D6DB37
00000078 39 38 36 36 41 34 10 00 1A 16 66 6C 6F 77 4F 6E 44 65 76 69 63 65 49 6E 76 6F 63 61 74 69 9866A4....flowOnDeviceInvocati
00000096 6F 6E 22 04 6E 6F 6E 65 2A 08 4E 4C 20 70 61 72 73 65 32 04 6E 6F 6E 65 3A 24 43 33 46 44 on".none*.NL_parse2:none:$C3FD
000000B4 31 30 36 35 2D 35 38 38 34 2D 34 42 35 45 2D 42 46 34 33 2D 36 34 45 35 30 31 36 36 38 34 1065-5884-4B5E-BF43-64E5016684
000000D2 42 38 41 22 39 A5 FB 75 A2 C4 41 00 00 00 88 00 00 01 00 00 32 FF B0 FB 75 A2 C4 41 B8A"9..u..A.....2...u..A
000000F0 32 FF B0 FB 75 A2 C4 41 0E 04 67 19 02 00 00 00 0A 24 39 46 41 32 36 42 46 38 2D 44 43 46 2...u..A..g.....$9FA26BF8-DCF
0000010E 44 2D 34 45 42 30 2D 39 32 34 30 2D 44 36 44 42 33 37 39 38 36 36 41 34 10 14 1A 07 73 75 D-4EB0-9240-D6DB379866A4....su
0000012C 63 63 65 73 73 22 04 6E 6F 6E 65 2A 0B 43 75 72 72 65 6E 74 54 61 73 6B 32 13 63 6F 6D 2E ccess".none*.CurrentTask2.com.
0000014A 61 70 70 6C 65 2E 4D 6F 62 69 6C 65 53 4D 53 3A 24 43 33 46 44 31 30 36 35 2D 35 38 38 34 apple.MobileSMS:$C3FD1065-5884
00000168 2D 34 42 35 45 2D 42 46 34 33 2D 36 34 45 35 30 31 36 36 38 34 42 38 41 23 82 AF FB 75 A2 -4B5E-BF43-64E5016684B8A#...u.
00000186 C4 41 96 00 00 01 00 00 00 93 C3 B1 FB 75 A2 C4 41 93 C3 B1 FB 75 A2 C4 41 82 60 E6 2A .A.....u..A....u..A.`*
000001A4 02 00 00 0A 24 39 46 41 32 36 42 46 38 2D 44 43 46 44 2D 34 45 42 30 2D 39 32 34 30 2D .....$9FA26BF8-DCFD-4EB0-9240-
000001C2 44 36 44 42 33 37 39 38 36 36 41 34 10 0B 1A 06 6E 6F 72 6D 61 6C 22 04 6E 6F 6E 65 2A 29 D6DB379866A4....normal".none*)
000001E0 73 69 72 69 6B 69 74 2E 69 6E 74 65 6E 74 2E 6D 65 73 73 61 67 65 73 2E 53 65 6E 64 4D 65 sirikit.intent.messages.SendMessage
000001FE 73 73 61 67 65 49 6E 74 65 6E 74 32 04 6E 6F 6E 65 3A 24 43 33 46 44 31 30 36 35 2D 35 38 84-4B5E-BF43-64E5016684B8A.h..
0000021C 38 34 2D 34 42 35 45 2D 42 46 34 33 2D 36 34 45 35 30 31 36 36 38 34 42 38 41 1F 68 B1 FB u..A.....u..A....u..A
0000023A 75 A2 C4 41 00 00 AA 00 00 01 00 00 00 89 D2 BC FB 75 A2 C4 41 89 D2 BC FB 75 A2 C4 41 A.M.....$9FA26BF8-DCFD-4EB0-9
00000258 41 9A 4D A8 02 00 00 0A 24 39 46 41 32 36 42 46 38 2D 44 43 46 44 2D 34 45 42 30 2D 39 240-D6DB379866A4....normal".re
00000276 32 34 30 2D 44 36 44 42 33 37 39 38 36 36 41 34 10 10 1A 06 6E 6F 72 6D 61 6C 22 09 72 65 recipient*)sirikit.intent.messages.SendMessageIntent2.com.apple
00000294 63 69 70 69 65 6E 74 2A 29 73 69 72 69 6B 69 74 2E 69 6E 74 65 6E 74 2E 6D 65 73 73 61 67 es.SendMessageIntent2.com.appl
000002B2 65 73 2E 53 65 6E 64 4D 65 73 73 61 67 65 49 6E 74 65 6E 74 32 13 63 6F 6D 2E 61 70 70 6C e.MobileSMS:$C3FD1065-5884-4B5
000002D0 65 2E 4D 6F 62 69 6C 65 53 4D 53 3A 24 43 33 46 44 31 30 36 35 2D 35 38 38 34 2D 34 42 35 E-BF43-64E5016684B8A....u..A..
000002EE 45 2D 42 46 34 33 2D 36 34 45 35 30 31 36 36 38 34 42 38 41 19 C9 BC FB 75 A2 C4 41 00 00 .....DF.v..A.DF.v..A.0
0000030C 00 00 00 0A 00 00 01 00 00 00 D0 44 46 04 76 A2 C4 41 D0 44 46 04 76 A2 C4 41 10 30 .....$9FA26BF8-DCFD-4EB0-924
0000032A 87 06 02 00 00 0A 24 39 46 41 32 36 42 46 38 2D 44 43 46 44 2D 34 45 42 30 2D 39 32 34 0-D6DB379866A4....normal".cont
00000348 30 2D 44 36 44 42 33 37 39 38 36 36 41 34 10 10 1A 06 6E 6F 72 6D 61 6C 22 07 63 6F 6E 74 ent*)sirikit.intent.messages.S
00000366 65 6E 74 2A 29 73 69 72 69 6B 69 74 2E 69 6E 74 65 6E 74 2E 6D 65 73 73 61 67 65 73 2E 53 endMessageIntent2.com.apple.Mo
00000384 65 6E 64 4D 65 73 73 61 67 65 49 6E 74 65 6E 74 32 13 63 6F 6D 2E 61 70 70 6C 65 2E 4D 6F
```

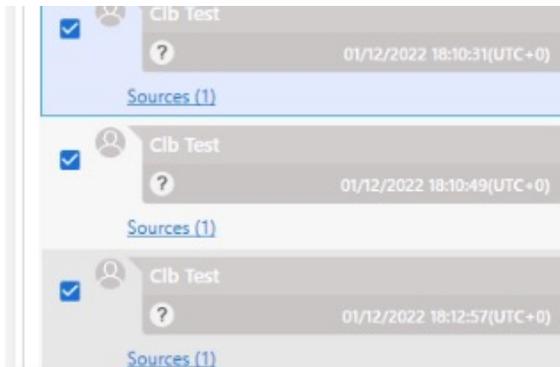
Exemples BIOME : iOS MESSAGES

Présent dans la 7.59 (version actuelle)



	✓	#		✕	↶	✎	📍	🗨	👤	Participants
✓		1		?				2	1	PR:HQ7zxOCMk0CiOQki97FK_Vm9Ta6OO,
✓		2		?				1	1	tg687512989 Jp Noat
✓		3		?				3	2	+33785650921 Clb Test +33608980894 Jp Noat
✓		4		?				7	1	+33 6 08 98 08 94 Jp Noat
✓		5		?				11	1	+33 6 08 98 08 94 Jp Noat

[File system Extraction.zip/root/private/var/mobile/Library/Biome/streams/public/AppIntent/local/691610034492436:34957/0x888D \(Taille: 1048576 o](#)



EXEMPLES BIOME : MESSAGES

```
Affichage hexadécimal
0000807A 30 00 28 00 10 02 0A 0C 2B 33 33 36 30 38 39 38 30 38 39 34 12 02 4A 70 22 07
00008094 4A 70 20 4E 6F 61 74 32 9F 01 40 00 38 02 12 98 01 69 6E 74 65 6E 74 73 2D 72
000080AE 65 6D 6F 74 65 2D 69 6D 61 67 65 2D 70 72 6F 78 79 3A 3F 70 72 6F 78 79 49 64
000080C8 65 6E 74 69 66 69 65 72 3D 35 30 43 44 45 45 43 38 2D 35 35 36 41 2D 42 32 30
000080E2 37 2D 32 46 31 39 2D 33 37 46 38 38 46 41 35 39 42 31 41 2E 70 6E 67 26 73 74
000080FC 6F 72 61 67 65 53 65 72 76 69 63 65 49 64 65 6E 74 69 66 69 65 72 3D 63 6F 6D
00008116 2E 61 70 70 6C 65 2E 49 6E 74 65 6E 74 73 2E 49 4E 49 6D 61 67 65 53 65 72 76
00008130 69 63 65 43 6F 6E 6E 65 63 74 69 6F 6E B8 01 00 50 00 1A 04 4E 6F 61 74 C0 01
0000814A 00 58 00 52 DC 01 0A D9 01 3A 16 20 00 30 00 28 00 10 02 0A 0C 2B 33 33 37 38
00008164 35 36 35 30 39 32 31 12 03 43 6C 62 22 08 43 6C 62 20 54 65 73 74 32 9F 01 40
0000817E 00 38 02 12 98 01 69 6E 74 65 6E 74 73 2D 72 65 6D 6F 74 65 2D 69 6D 61 67 65
00008198 2D 70 72 6F 78 79 3A 3F 70 72 6F 78 79 49 64 65 6E 74 69 66 69 65 72 3D 32 33
000081B2 30 35 45 42 42 42 2D 36 37 31 37 2D 38 31 42 30 2D 32 33 35 45 2D 36 39 46 39
000081CC 31 30 39 31 33 38 32 39 2E 70 6E 67 26 73 74 6F 72 61 67 65 53 65 72 76 69 63
000081E6 65 49 64 65 6E 74 69 66 69 65 72 3D 63 6F 6D 2E 61 70 70 6C 65 2E 49 6E 74 65
00008200 6E 74 73 2E 49 4E 49 6D 61 67 65 53 65 72 76 69 63 65 43 6F 6E 6E 65 63 74 69
0000821A 6F 6E B8 01 00 50 00 1A 04 54 65 73 74 C0 01 00 58 00 80 05 D2 00 3D 00 3E 00
00008234 3F 00 40 5A 24 63 6C 61 73 73 6E 61 6D 65 58 24 63 6C 61 73 73 65 73 5F 10 16
0000824E 5F 49 4E 50 42 53 65 6E 64 4D 65 73 73 61 67 65 49 6E 74 65 6E 74 A3 00 41 00
00008268 42 00 43 5F 10 16 5F 49 4E 50 42 53 65 6E 64 4D 65 73 73 61 67 65 49 6E 74 65
00008282 6E 74 59 50 42 43 6F 64 61 62 6C 65 58 4E 53 4F 62 6A 65 63 74 D3 00 45 00 46
0000829C 00 10 00 47 00 4E 00 55 57 4E 53 2E 6B 65 79 73 5A 4E 53 2E 6F 62 6A 65 63 74
0.(.....+33608980894..Jp".
Jp Noat2..@.8....intents-r
emote-image-proxy:?proxyId
entifier=50CDEEC8-556A-B20
7-2F19-37F88FA59B1A.png&st
orageServiceIdentifier=com
.apple.Intents.INImageServ
iceConnection...P...Noat..
.X.R..... .0.(.....+3378
5650921..Clb".Clb Test2..@
.8....intents-remote-image
-proxy:?proxyIdentifier=23
05EBBB-6717-81B0-235E-69F9
10913829.png&storageServic
eIdentifier=com.apple.Inte
nts.INImageServiceConnecti
on...P...Test...X.....=>.
?.@Z$classnameX$classes..
_INPBSendMessageIntent..A.
B.C..._INPBSendMessageInte
ntYPBCodableXNSObject..E.F
...G.N.UWNS.keysZNS.object
```

EXEMPLES BIOME : MESSAGES

#	Offset	Longueur	Valeur	Source
1	32898 / 0x8082	12 / 0xC	Chat.InstantMessage.Party.Identifier: +33608980894	/root/private/var/mobile/Library/Biome/streams/pu...
2	32912 / 0x8090	2 / 0x2	Chat.InstantMessage.Party.Name: Jp Noat	/root/private/var/mobile/Library/Biome/streams/pu...
3	33092 / 0x8144	4 / 0x4	Chat.InstantMessage.Party.Name: Jp Noat	/root/private/var/mobile/Library/Biome/streams/pu...
4	33119 / 0x815F	12 / 0xC	Chat.InstantMessage.Party.Identifier: +33785650921	/root/private/var/mobile/Library/Biome/streams/pu...
5	33133 / 0x816D	3 / 0x3	Chat.InstantMessage.Party.Name: Clb Test	/root/private/var/mobile/Library/Biome/streams/pu...
6	33315 / 0x8223	4 / 0x4	Chat.InstantMessage.Party.Name: Clb Test	/root/private/var/mobile/Library/Biome/streams/pu...
7	34957 / 0x888D	8 / 0x8	Chat.InstantMessage.TimeStamp: 01/12/2022 18:12:57(UTC+0)	/root/private/var/mobile/Library/Biome/streams/pu...
8	35074 / 0x8902	36 / 0x24	Chat.InstantMessage.Identifier: 6397506E-DF86-4896-9D21-54A9C4464350	/root/private/var/mobile/Library/Biome/streams/pu...

Valeurs Balises Segments surlignés [8 résultats]

FORMAT FICHIER BIOME (SEGB)

Entête du fichier BIOME (expérimental)

Type	Longueur	Description
Entier non signé	8 octets	Offset pour le prochain enregistrement (little endian)
Date (à valider) : double (Apple Absolute Time)	8 octets	
Entier	4 octets	À valider
Ascii	32 octets	Nom de fichier /date et heure
Ascii	4 octets	SEGB (caractéristique de ce type de fichier)

FORMAT FICHER BIOME (SEGB)

Entête d'un enregistrement BIOME

Type	Longueur	Description
Entier non signé au format Little Endian	4 octets	Longueur de l'enregistrement protobuf
Entier non signé	4 octets	Etat de la trame
Date absolue double	8 octets	Date création
Date absolue double	8 octets	Date modification
Entier	4 octets	CRC 32 du protobuf
Entier	4 octets	?
Protobuf d'une longueur correspondante à l'entête		

EXEMPLES BIOME : UTILISATION DE SIRI

Il est possible de visualiser en hexa le contenu du Biome
Certains outils contiennent un visualisateur de Biome.

```
{  
  "field #1: L-delim (e.g. string, message)": "9FA26BF8-DCFD-4EB0-9240-D6DB379866A4",  
  "field #2: VarInt (e.g. int32, bool)": 11,  
  "field #3: L-delim (e.g. string, message)": "normal",  
  "field #4: L-delim (e.g. string, message)": "none",  
  "field #5: L-delim (e.g. string, message)": "sirikit.intent.messages.SendMessageIntent",  
  "field #6: L-delim (e.g. string, message)": "none",  
  "field #7: L-delim (e.g. string, message)": "C3FD1065-5884-4B5E-BF43-64E5016684B8",  
  "field #8: 64-Bit (e.g. fixed64, double)": 4739091335518185000  
}
```

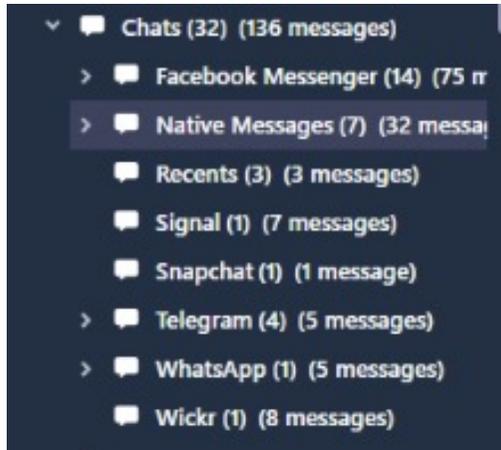
EXEMPLES BIOME : UTILISATION DE SIRI

Il est possible de visualiser en hexa le contenu du Biome
Certains outils contiennent un visualisateur de Biome.

```
{  
  "field #1: L-delim (e.g. string, message)": "9FA26BF8-DCFD-4EB0-9240-D6DB379866A4",  
  "field #2: VarInt (e.g. int32, bool)": 16,  
  "field #3: L-delim (e.g. string, message)": "normal",  
  "field #4: L-delim (e.g. string, message)": "recipient",  
  "field #5: L-delim (e.g. string, message)": "sirikit.intent.messages.SendMessageIntent",  
  "field #6: L-delim (e.g. string, message)": "com.apple.MobileSMS",  
  "field #7: L-delim (e.g. string, message)": "C3FD1065-5884-4B5E-BF43-64E5016684B8",  
  "field #8: 64-Bit (e.g. fixed64, double)": 4739091335518931000  
}
```

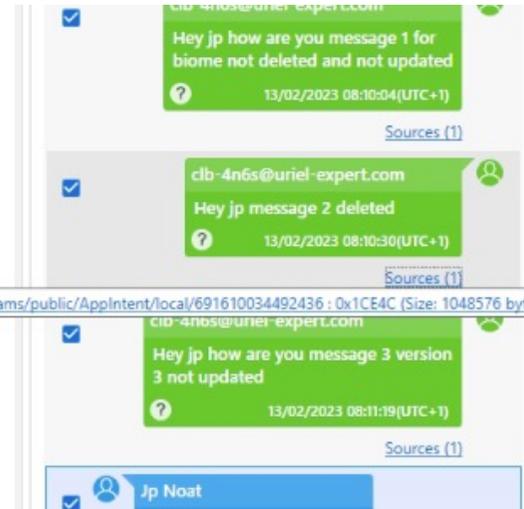
BIOME Examples: MESSAGES

Depuis PA 7.59

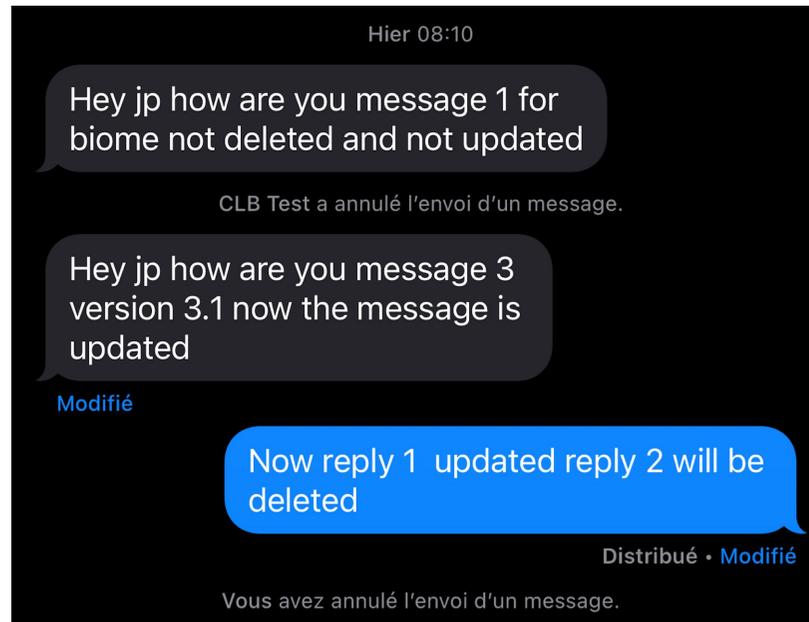
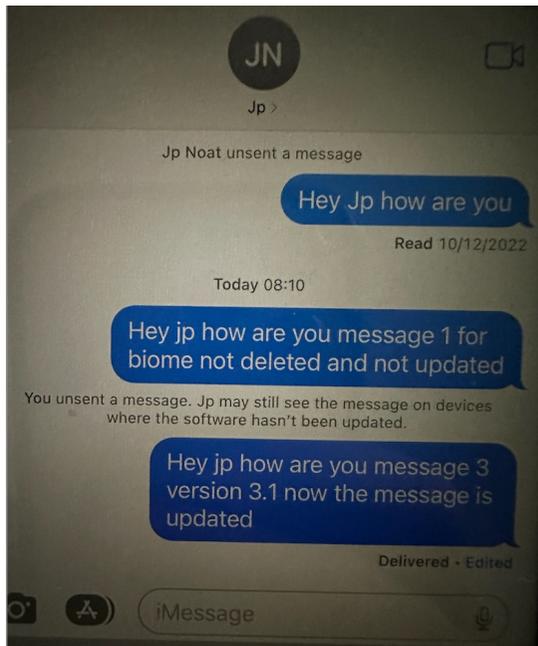


Start Time	Last Activity	ID
13/02/2023 08:57:59(UTC+1)	13/02/2023 08:57:59(UTC+1)	
13/02/2023 08:57:59(UTC+1)	13/02/2023 08:57:59(UTC+1)	snapchat
13/02/2023 08:10:04(UTC+1)	13/02/2023 08:14:27(UTC+1)	+33608980894
13/02/2023 08:10:04(UTC+1)	13/02/2023 08:13:50(UTC+1)	+33608980894
07/02/2023 18:56:44(UTC+1)	07/02/2023 18:56:44(UTC+1)	
07/02/2023 18:56:44(UTC+1)	07/02/2023 18:56:44(UTC+1)	sosh
01/12/2022 18:54:37(UTC+1)	13/02/2023 08:14:27(UTC+1)	

File system Extraction.zip/root/private/var/mobile/Library/Biome/streams/public/AppIntent/local/691610034492436 : 0x1CE4C (Size: 1048576 bytes)

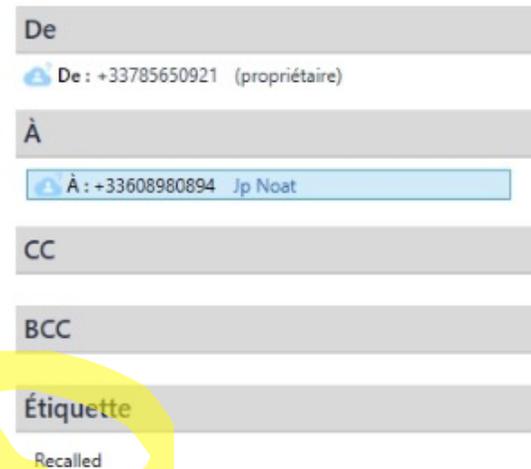
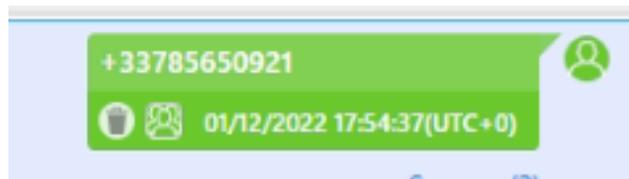


New message management



L'annulation d'envoi des messages

- Tentative de rappel de ces messages au(x) destinaire(s) (terme en anglais recall).
- Si le destinaire est sous MacOS 13 / iOS 16 le message sera effacé de la base de données mais les métadonnées resteront. Possibilité d'annulation jusqu'à 2 minutes après l'envoi initial.
- Les métadonnées contiennent l'expéditeur et le destinataire du message, la date et l'heure mais le contenu du message est bel et bien effacé. Il se peut cependant que l'on retrouve ce message dans d'autres bases de données (notifications, Spotlight,....)



VALEUR AJOUTEE DU BIOME

		Participants	Start Time	Last Activity
1	2	snapchat +33785650921 (owner)	13/02/2023 08:57:59(UTC+1)	13/02/2023 C
1	2	snapchat +33785650921 (owner)	13/02/2023 08:57:59(UTC+1)	13/02/2023 C
5	3	+33608980894 Jp Noat (owner) clb-4n6s@uriel-expert.com (owner) +33785650921 (owner)	13/02/2023 08:10:04(UTC+1)	13/02/2023 C
3	3	+33608980894 Jp Noat (owner) clb-4n6s@uriel-expert.com (owner) +33785650921 (owner)	13/02/2023 08:10:04(UTC+1)	13/02/2023 C
1	2	sosh sosh (owner) +33785650921 (owner)	07/02/2023 18:56:44(UTC+1)	07/02/2023 1
1	2	sosh sosh (owner) +33785650921 (owner)	07/02/2023 18:56:44(UTC+1)	07/02/2023 1
20	3	+33785650921 (ow +33608980894 Jp Noat (owner)	File system Extraction.zip/root/private/var/mobile/Library/Biome/streams/public/AppIntent/local/691610034492436 : 0x1E022 (Size: 1048576 bytes)	

VALEUR AJOUTEE DU BIOME

UNIQUE SOURCE OF MESSAGES

The screenshot displays a mobile messaging application interface. The top part shows a list of messages from a contact with the phone number +33785650921. The messages are:

- Message 1: "Hey Jp how are you" (Timestamp: 10/12/2022 17:32:30(UTC+1), Sources: 2)
- Message 2: "Hey jp how are you message 1 for biome not deleted and not updated" (Timestamp: 13/02/2023 08:10:04(UTC+1), Sources: 1)
- Message 3: "Hey jp how are you message 1 for biome not deleted and not updated" (Timestamp: 13/02/2023 08:10:30(UTC+1), Sources: 1)
- Message 4: "Hey jp how are you message 3 version 3 not updated" (Timestamp: 13/02/2023 08:11:19(UTC+1), Sources: 1)

The bottom part of the screenshot shows a detailed view of the selected message (Message 3). The details are as follows:

- Source: Native Messages
- Subject: (Empty)
- Timestamp: 13/02/2023 08:10:30(UTC+1)
- Status: Sent
- Message Type: iMessage
- SMSC: (Empty)
- Device description: (Empty)
- Folder: Sent
- Priority: (Empty)
- Deletion Date: 13/02/2023 08:10:38(UTC+1)
- Service Identifier: (Empty)
- Extraction: File System
- Source file: [File System Extraction.zip/root/private/var/mobile/Library/SMS/sms.db-wal : 0x283D50 \(Table: message_handle; Size: 3469072 bytes\)](#)

Below the details, there are fields for From, To, CC, BCC, Label, Attachment, SharedContacts, and Body. The Label field is highlighted with a blue background and contains the text "Recalled". An orange arrow points to the Label field.

BIOME ET IMESSAGE

On peut voir différentes versions du message édité

Export Filters Actions Enter text to filter ...

+33785650921
Hey jp how are you message 1 for biome not deleted and not updated
13/02/2023 08:10:04(UTC+1)
Sources (1)

+33785650921
Hey jp how are you message 3 version 3 not updated
13/02/2023 08:11:19(UTC+1)
Sources (1)

+33785650921
Hey jp how are you message 3 version 3.1 now the message is updated
13/02/2023 08:12:02(UTC+1)
Sources (1)

SMSC:
Device description:
Folder: Sent
Priority:
Service Identifier:
Extraction: File System
Source file: [File system Extraction.zip/root/private/var/mobile/Library/SMS/sms.db-wal : 0x2B3C95 \(Table: message_handle: Size: 3469072 bytes\)](#)

From
From: +33785650921 (owner)

To
To: +33608980894 Jp Noat

CC

BCC

Label
Edited

Attachment

SharedContacts

Body
Hey jp how are you message 3 version 3.1 now the message is updated

LES OUTILS S'Y METTENT

Comme chaque format est différent l'approche est progressive

Cellebrite, Magnet, Oxygen et MSAB supportent certaines données du Biome

Des Biomes sont découverts tous les jours et donc nécessitent de fréquentes mises à jour.

Impatient de les voir dans iLeap

Artex (Doubleblak l'outil de Ian Whiffin) les intègre déjà partiellement avec également un visualisateur.

Quelques liens pour iOS 16

Biome : <https://blog.d204n6.com/> (5 parties sur le Biome un must) de Cryptid Vance

iOS 16 (1ères recherches de CLB) en anglais : <https://www.youtube.com/watch?v=WwMfPm1UMp0>

Le blog de Scott_Kjr3347 : <https://github.com/ScottKjr3347/> et en particulier les requêtes adaptées à l'iOS16 : https://github.com/ScottKjr3347/iOS_Local_PL_Photos.sqlite_Queries/tree/main/iOS16

L'outil Artex de Ian Whiffin : <https://www.doubleblak.com/>

Cyberchef : <https://gchq.github.io/CyberChef/>

iLEAP : <https://github.com/abrignoni/iLEAPP>

Structure interne du Biome : <https://bluecrewforensics.com/2022/03/07/ios-app-intents/>

 Cellebrite

Email : jean-philippe.noat@cellebrite.com

Twitter : @4n6s_mc

Linkedin : jean-philippe Noat

Notebook : <https://community.cellebrite.com>

Questions

Bon FIC à tous