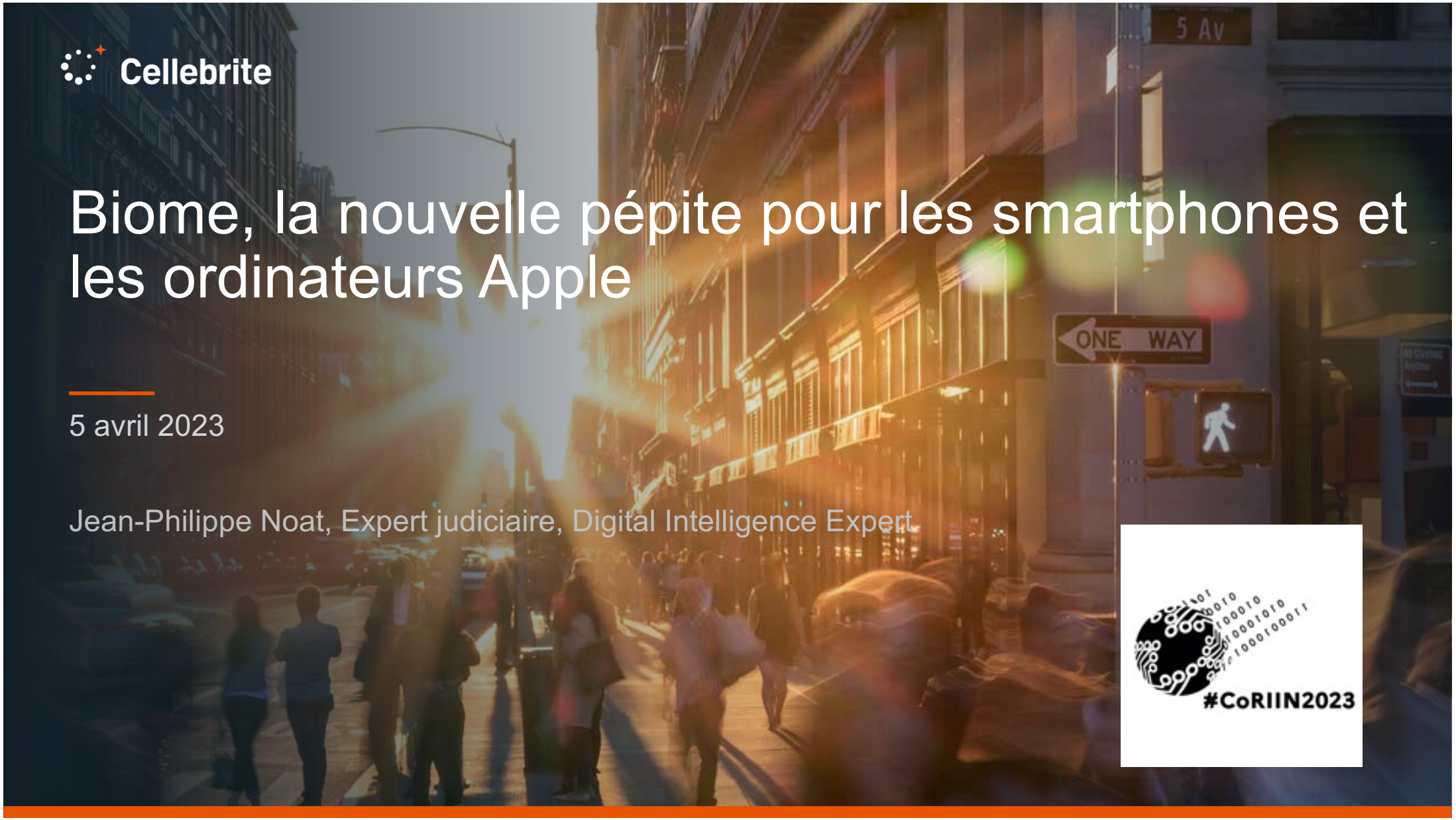


Cellebrite

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

5 avril 2023

Jean-Philippe Noat, Expert judiciaire, Digital Intelligence Expert

#CoRIIN2023

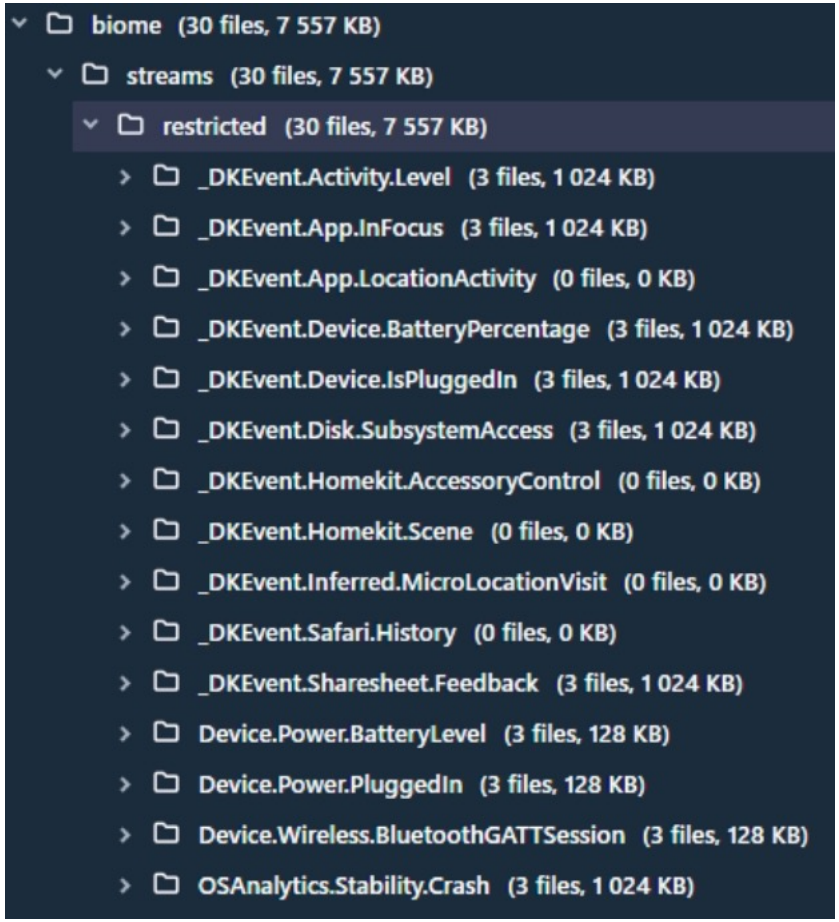
- Spécialiste en intelligence digitale (Engagement team Cellebrite)
- 20 ans d’experience en assistance LE
- 7 ans experience formateur Cellebrite
- EnCE CCME, CFCE
- Plus de 320 differents dossiers pour différentes activités judiciaires internationals ou locales (Monaco, France, Belgique, Luxembourg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

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

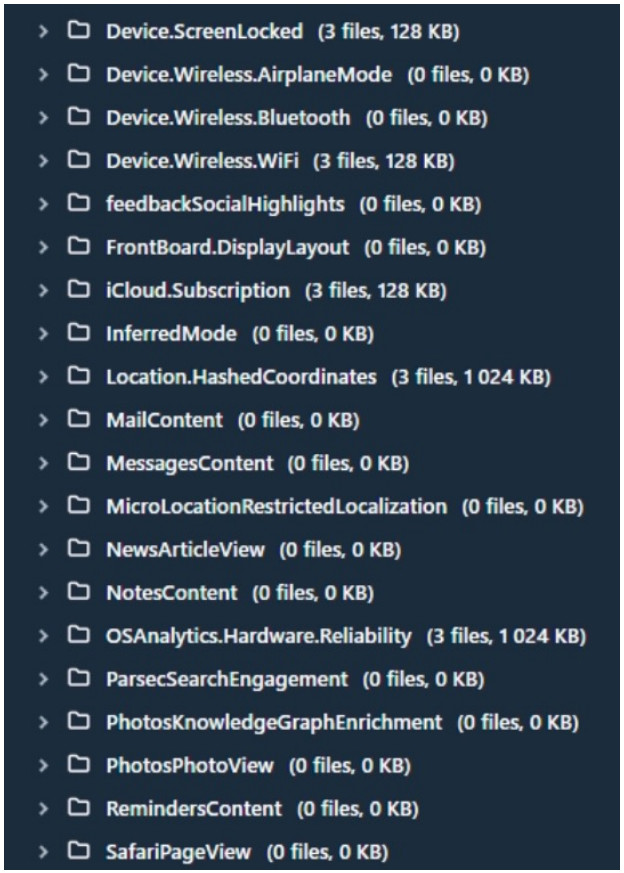
/root/private/var/db/biome/streams/restricted

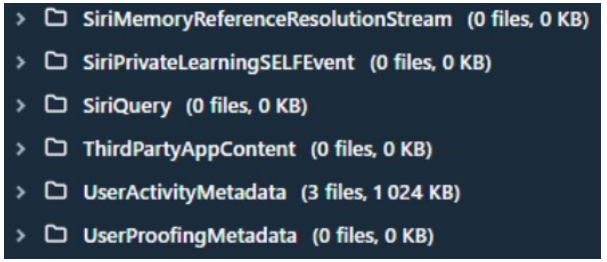


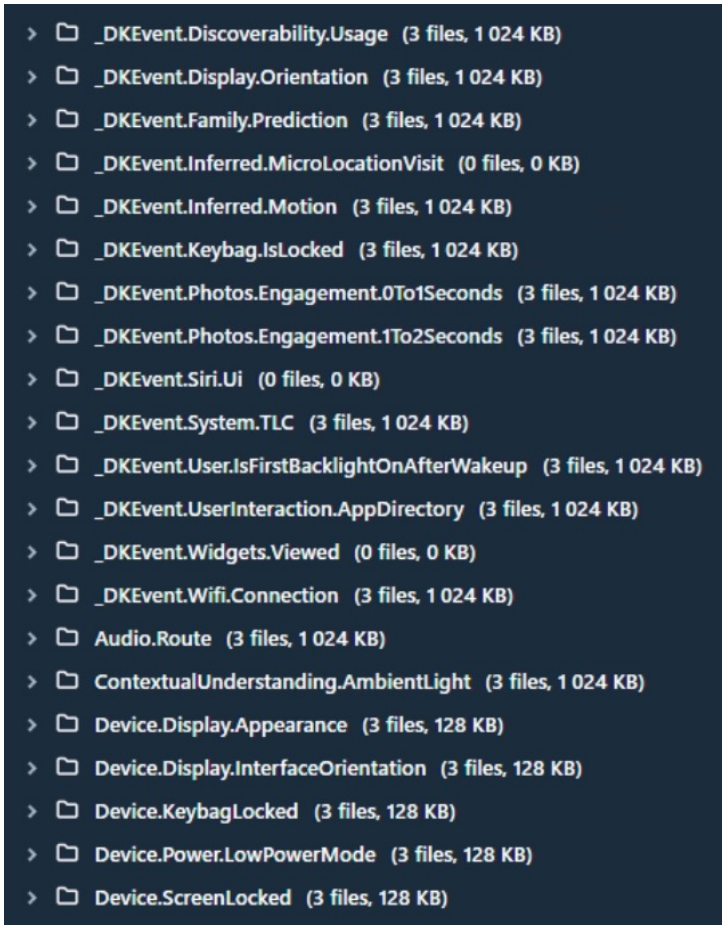
Cellebrite

QUELQUES SOURCES DE BIOME

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

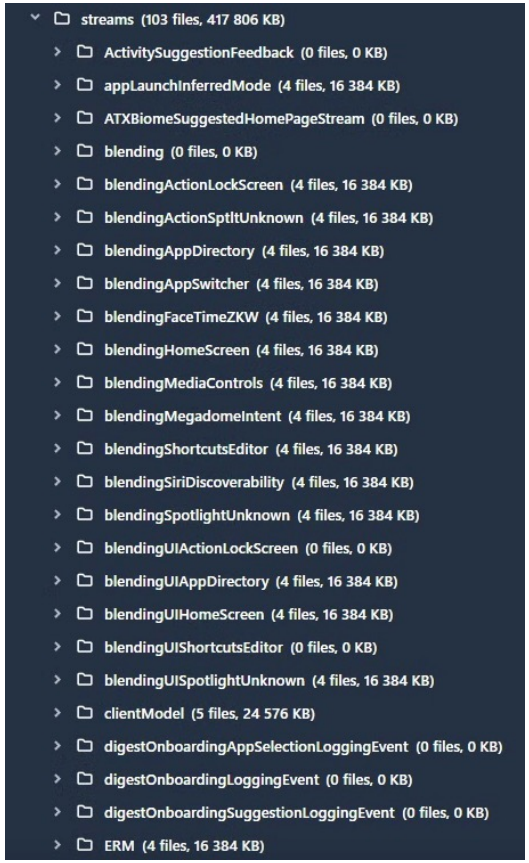


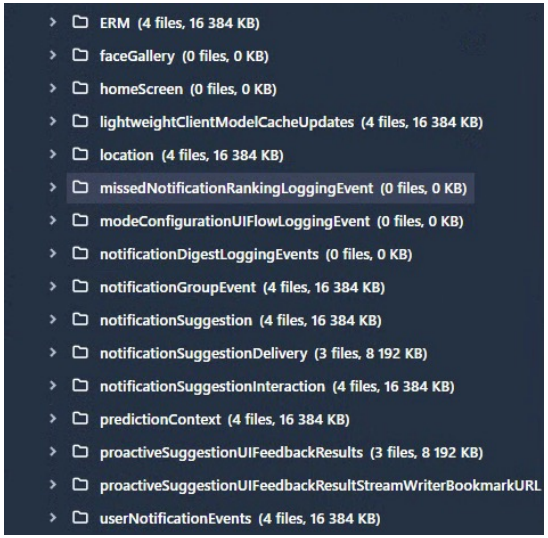




DES SOURCES LA OU ON NE LES ATTEND PAS

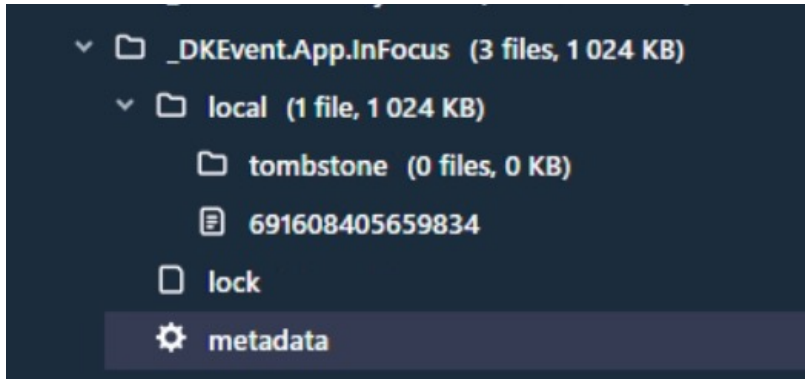
/root/private/var/mobile/Library/DuetExpertCenter/streams



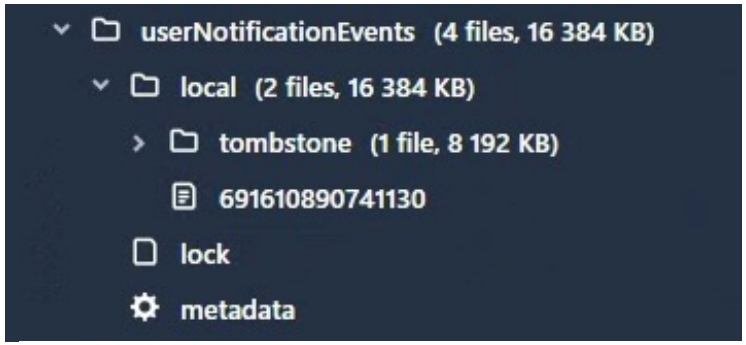


EXEMPLES BIOME : APP IN FOCUS

- 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




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

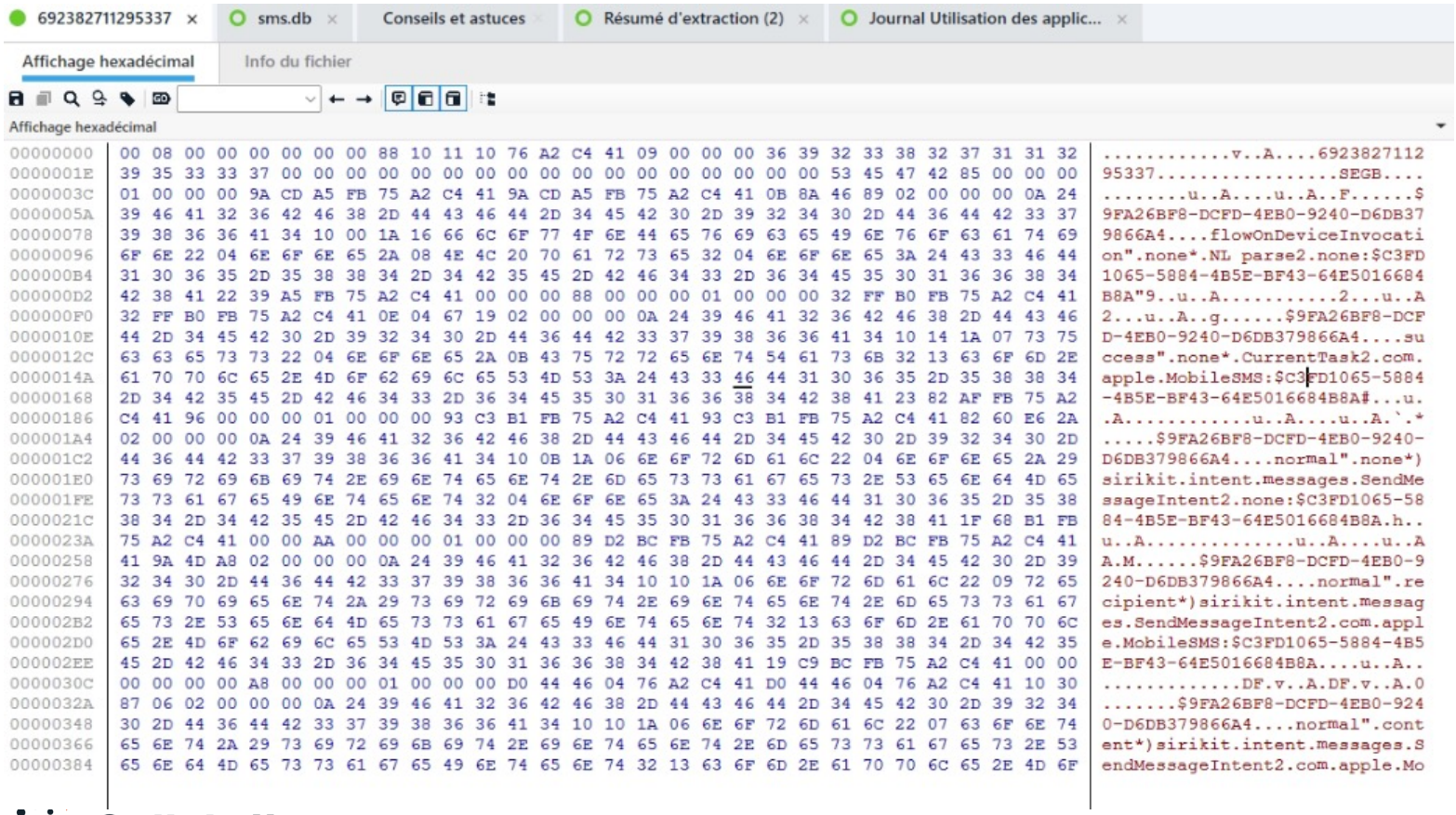
- Les notifications sont accessibles même si l'application a été effacée.
- Titres de message qui peuvent indiquer une information

```
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
```

Cellebrite

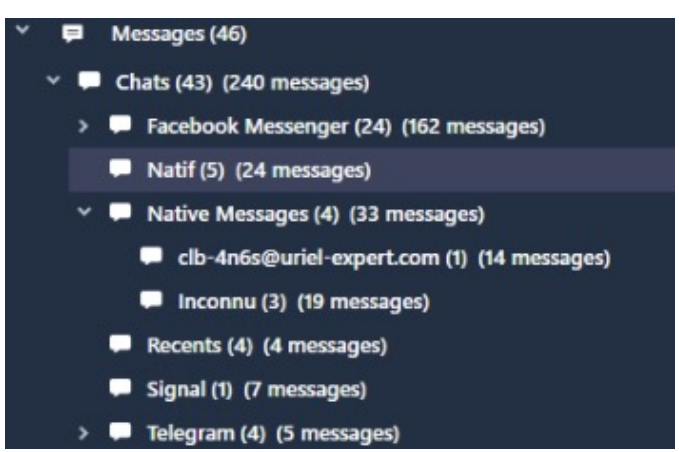
Exemples BIOME : Utilisation de Siri

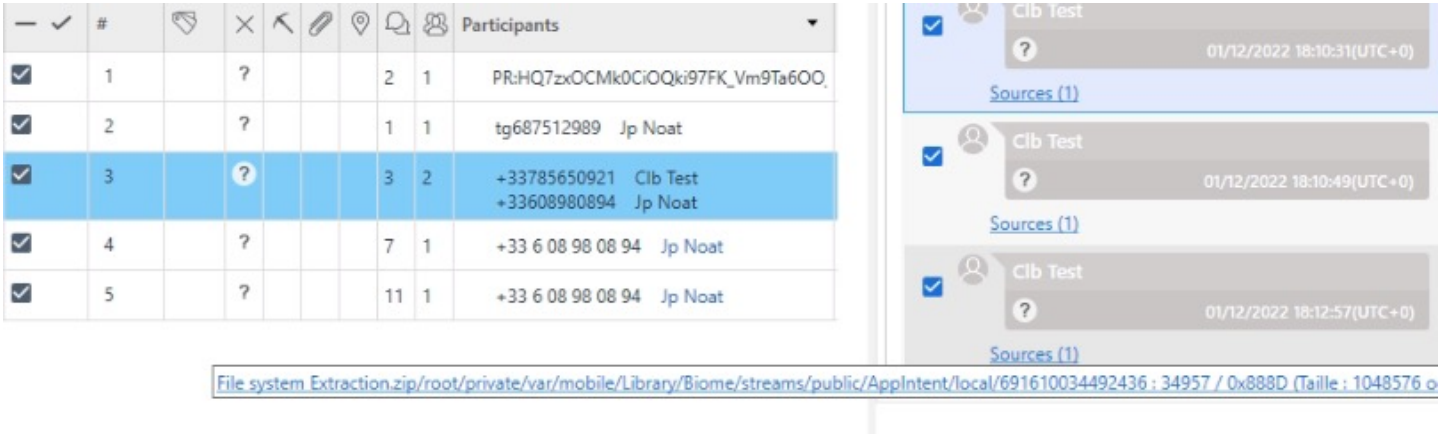


Cellebrite

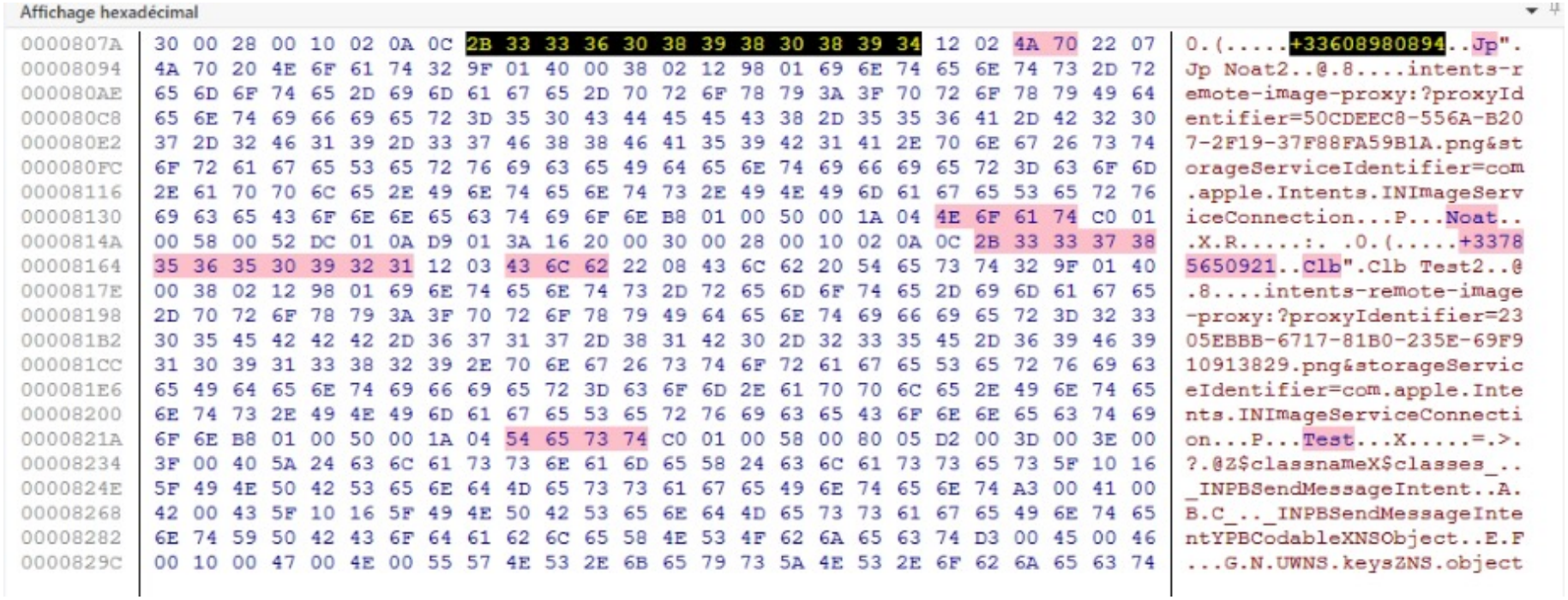
Exemples BIOME : iOS MESSAGES

Présent dans la 7.59 (version actuelle)



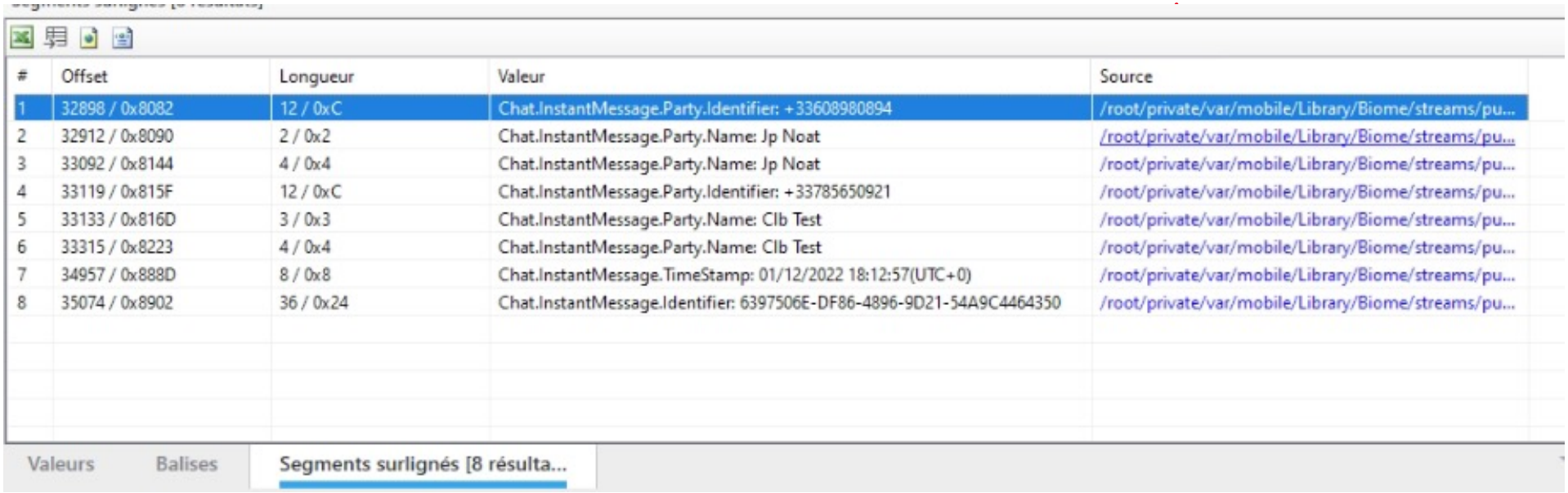


EXEMPLES BIOME : MESSAGES



Cellebrite

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 résulta...

Cellebrite

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 FICHIER 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 longeur 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-BF43-64E501668488",
    "field #8: 64-Bit (e.g. fixed64, double)": 473909133551818500O
}
```

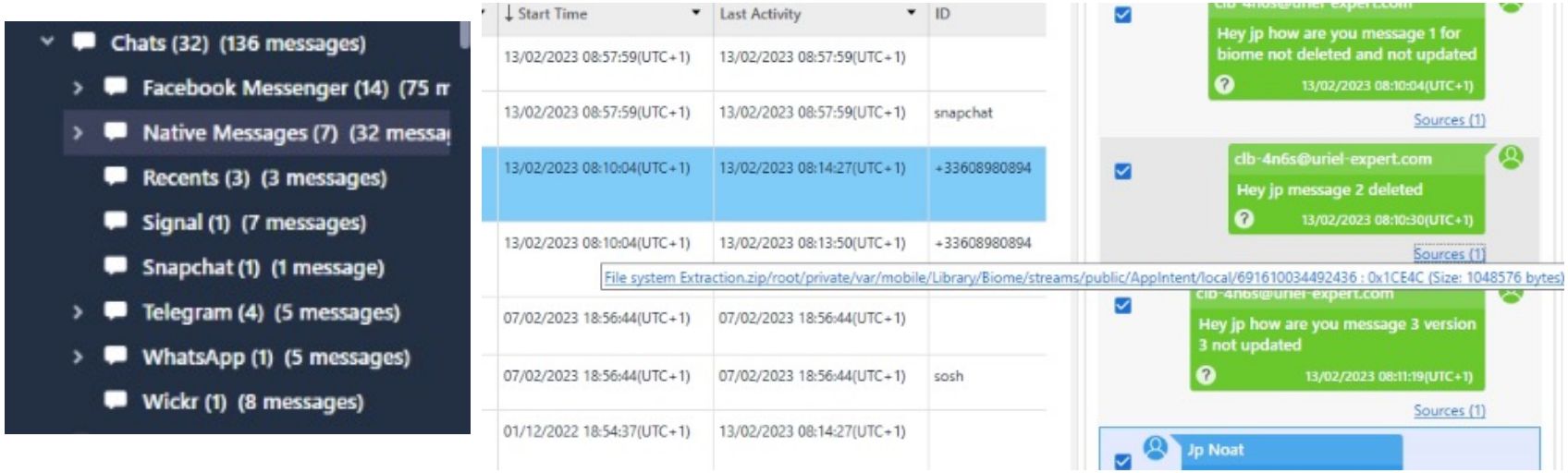
EXEMPLES BIOME : UTILISATION DE SIRI

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

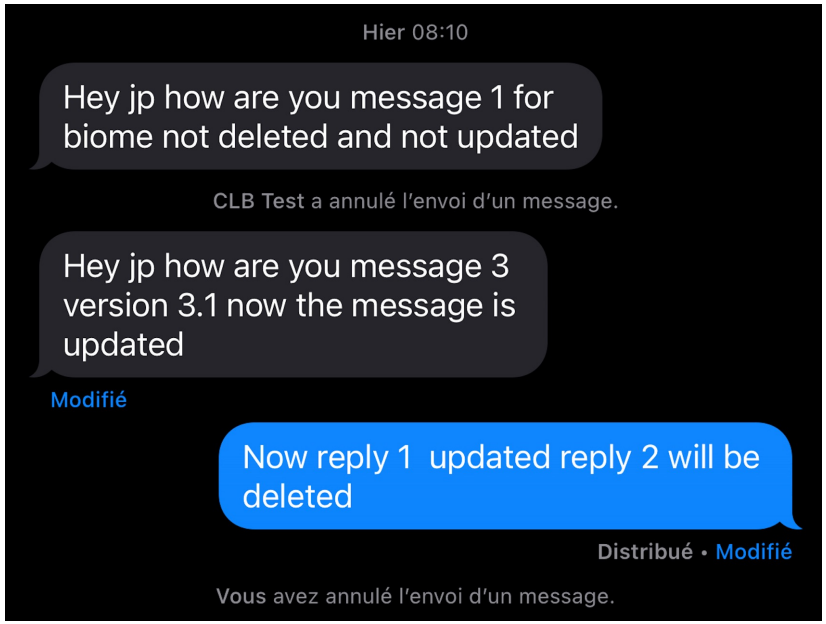

```
{
    "field #1: L-delim (e.g. string, message)": "9FA26BF8-DCFD-4EB0-9240-D6DB379866A4",
    "field #2: VarInt (e.g. int32, bool)": 16,
    "field #3: L-delim (e.g. string, message)": "normal",
    "field #4: L-delim (e.g. string, message)": "recipient",
    "field #5: L-delim (e.g. string, message)": "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-BF43-64E501668488",
    "field #8: 64-Bit (e.g. fixed64, double)": 47390913355189310000
}
```

BIOME Examples: MESSAGES

Depuis PA 7.59



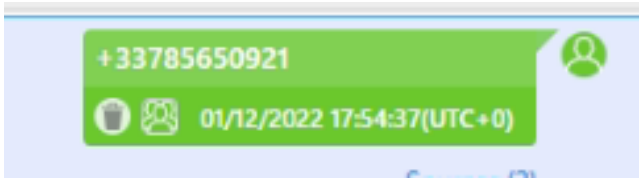
New message management

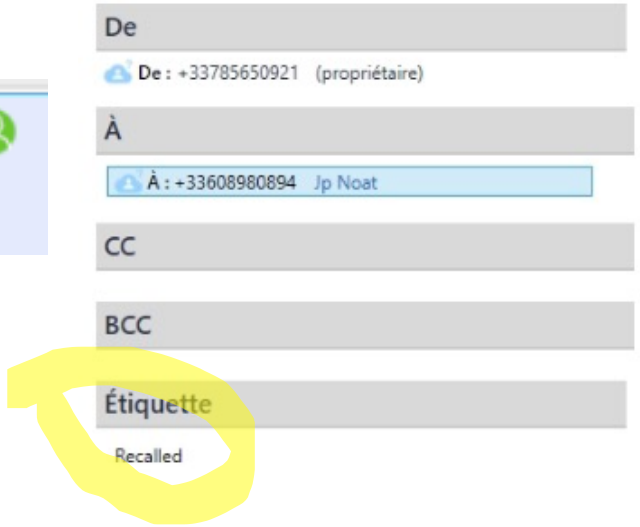


Cellebrite

L’annulation d’envoi des messages

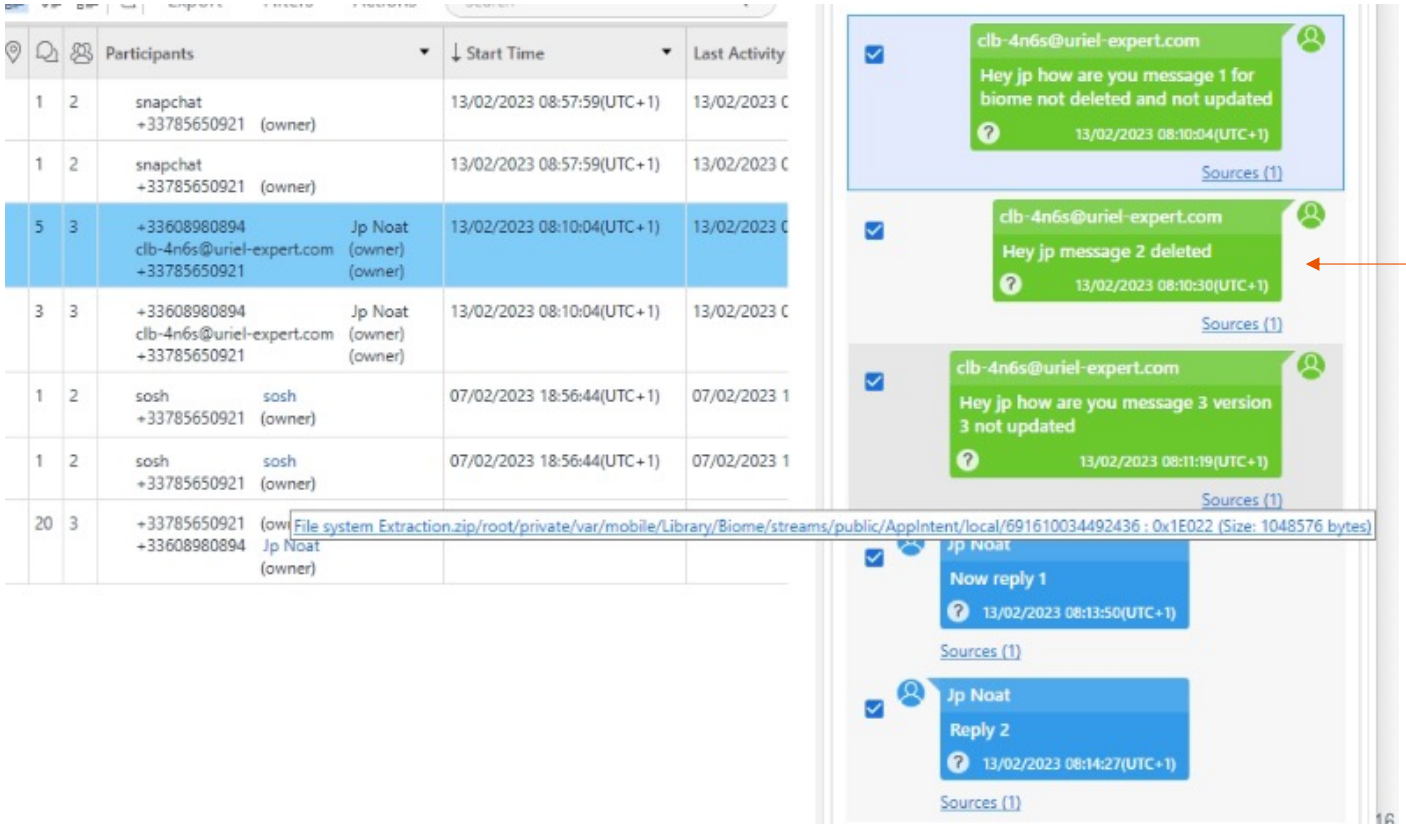
- Tentative de rappel de ces messages au(x) destinaire(s) (terme en anglais recall).
- Si le destinaire est sous MacOS 13 / iOS 16 le message sera effacé de la base de données mais les métadonnées resteront. Possibilité d’annulation jusqu’à 2 minutes après l’envoi initial.
- Les métadonnées contiennent 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,….)





Cellebrite

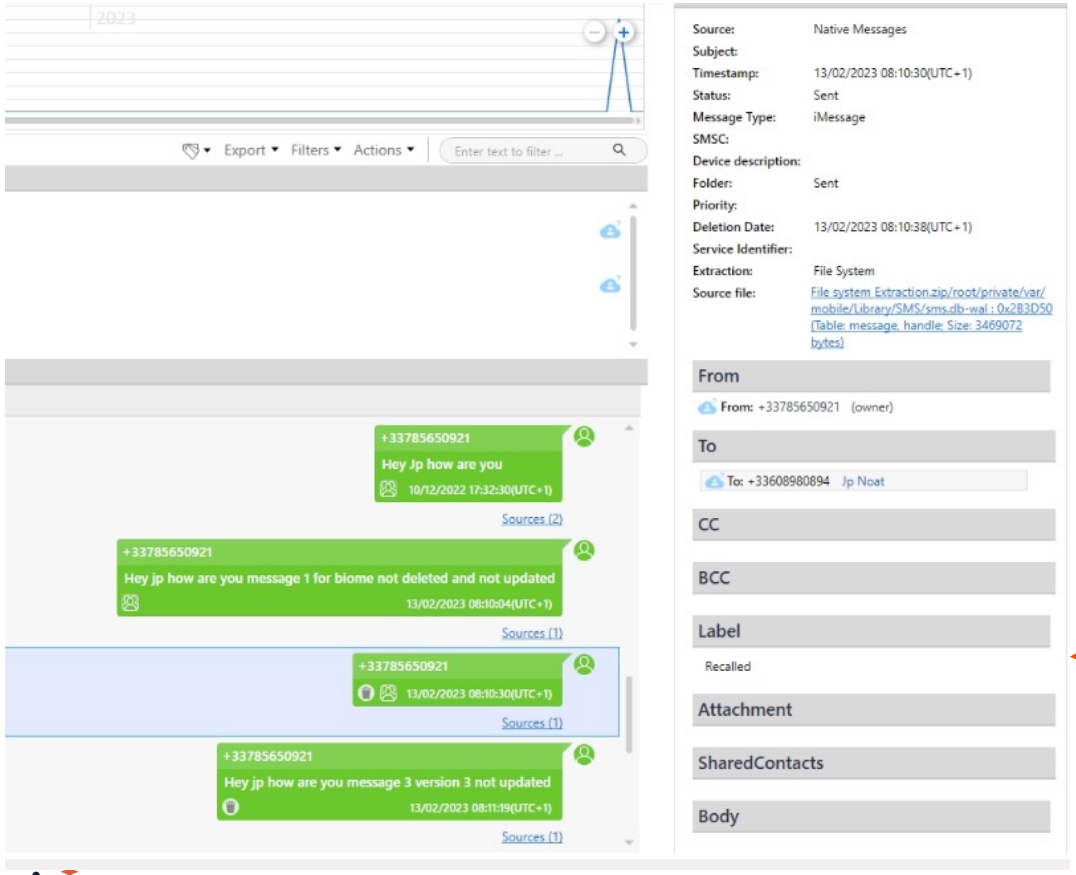
VALEUR AJOUTEE DU BIOME



Cellebrite

VALEUR AJOUTEE DU BIOME

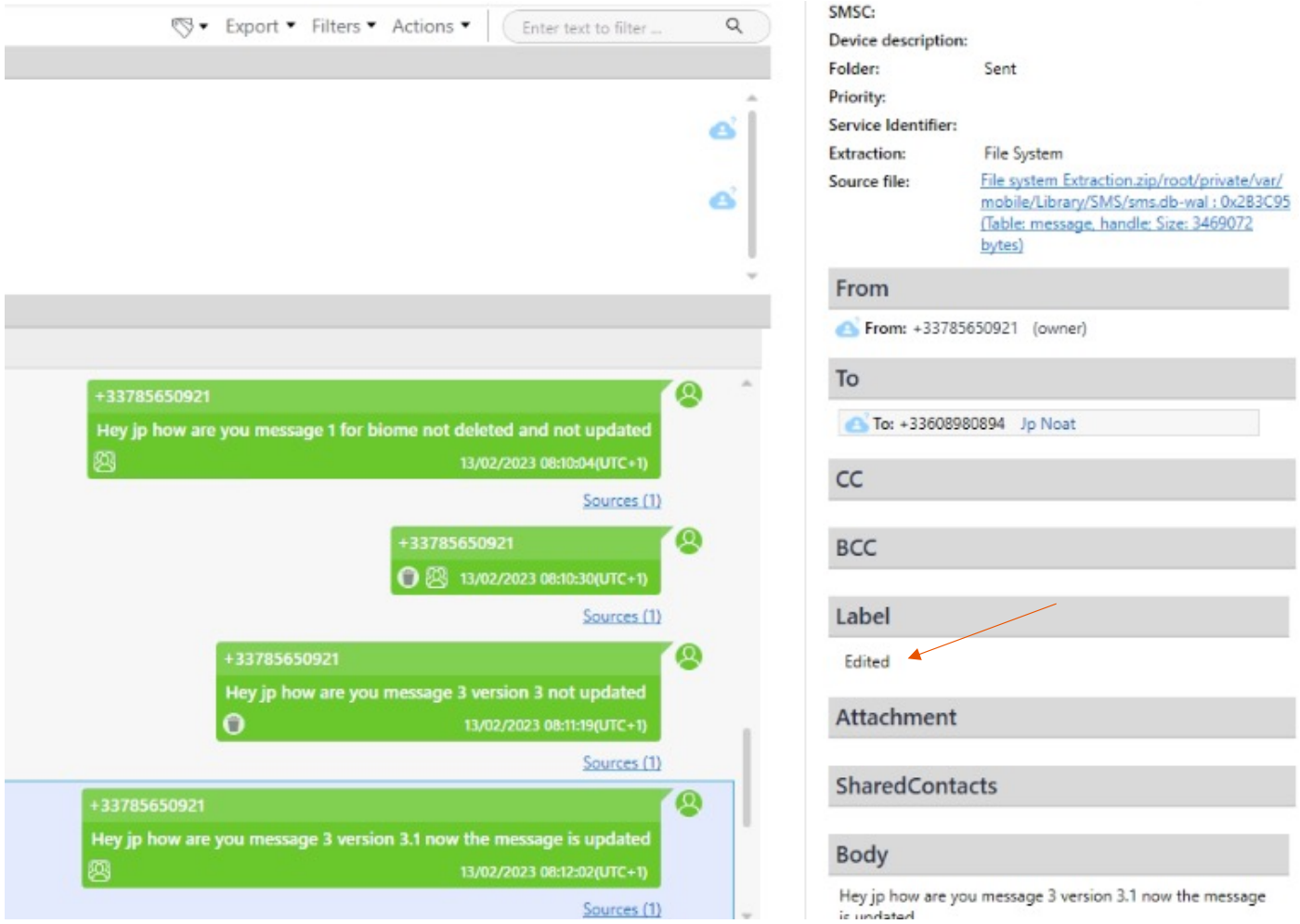
UNIQUE SOURCE OF MESSAGES



Cellebrite

BIOME ET IMESSAGE

On peut voir différentes versions du message édité



Cellebrite

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