GrayKeyとMagnet AXIOMのパートナーシップの効果を最大化する

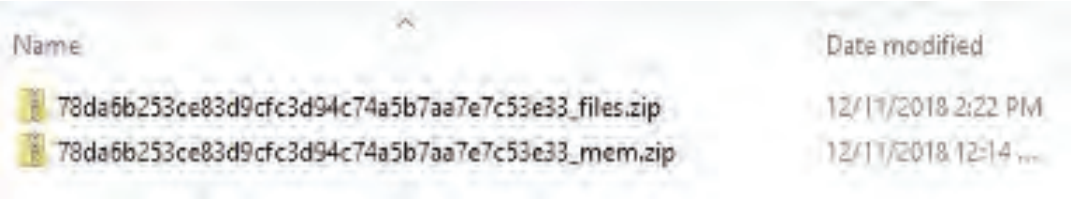
Magnet ForensicsとGrayshiftはiOSデバイスから大部分のデータを取得し処理するために必要とされるツールを捜査機関へ提携すべくパートナーシップを締結しました。このパートナーシップは捜査機関関係のお客様が正義を求め無実の者を守るのに役立たせる当社の共同的使命の結果実現したものです。

長年わたり捜査機関はこれらデバイスから重要な情報を取得するのに奮闘してきました。GrayKeyにより私達はパスコードを潜在的にブルートフォース攻撃で見つけることができるようになると同時に、検査官は市販されている他のどんなソリューションよりも多くのデータを取得し、Magnet AXIOMで精査できるようにもなります。

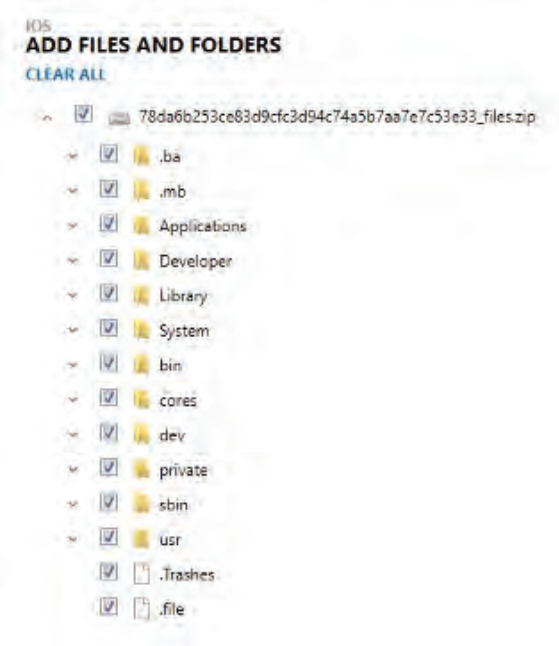
BFUつまり最初のロック解除以前、AFUつまり最初のロック解除以降、またはフルファイルシステムのイメージを含め、GrayKeyによって生成できる様々な種類のイメージがあります。検査官がどの種類のイメージを取得できるかに関わらず、各種類がMagnet AXIOMの中へインジェストでき、また情報用に処理できます。

イメージをMagnet AXIOMへ　み込むためには、ユーザーはAXIOM Processのエビデンスソースから「Mobile -> iOS -> Load Evidence -> Images」と選択すればいいだけです。

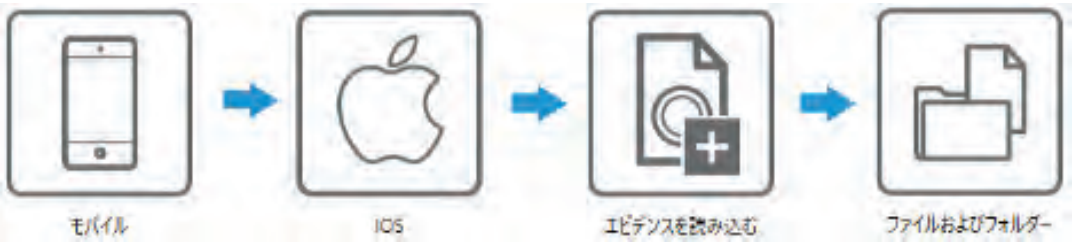
エビデンス選択の画面が　み込まれると、ユーザーは処理用にGrayKeyによって生成されるイメージのフォーマット種類を選択することができます。これらのイメージは 問題となるiOSデバイスのユニークなデバイス識別子へ紐付けされる"<udid>_files_<image type>.zip"のフォーマットで保存されます。このイメージがGrayKeyデバイスから取得されたBFU、AFUまたはファイルシステムのイメージの場合、イメージの種類が反映されます。



ファイルシステムのイメージが選択され　み込まれれば、ユーザーはAXIOMに情報をスキャンできるようにしたいファイルシステムのいずれかまたはすべての領域を選択的に取り上げることができます。これは時間が不足するか、単にファイルシステムでの極めて特殊なアーティファクトを探しているユーザーの役に立ちます。



GrayKeyを　み込む際の唯一の違いは、精査についてのエクスポート可およびエクスポート 不可の値を含むキーチェーンデータを　み込むことに関係します。キーチェーンを　み込むには、ユーザーはイメージと類似する手順に従う必要がありますが、「イメージ」を選択するのではなく「ファイル/フォルダー」を選び、AXIOMを“udid_keychain.plist”へ方向付けます。

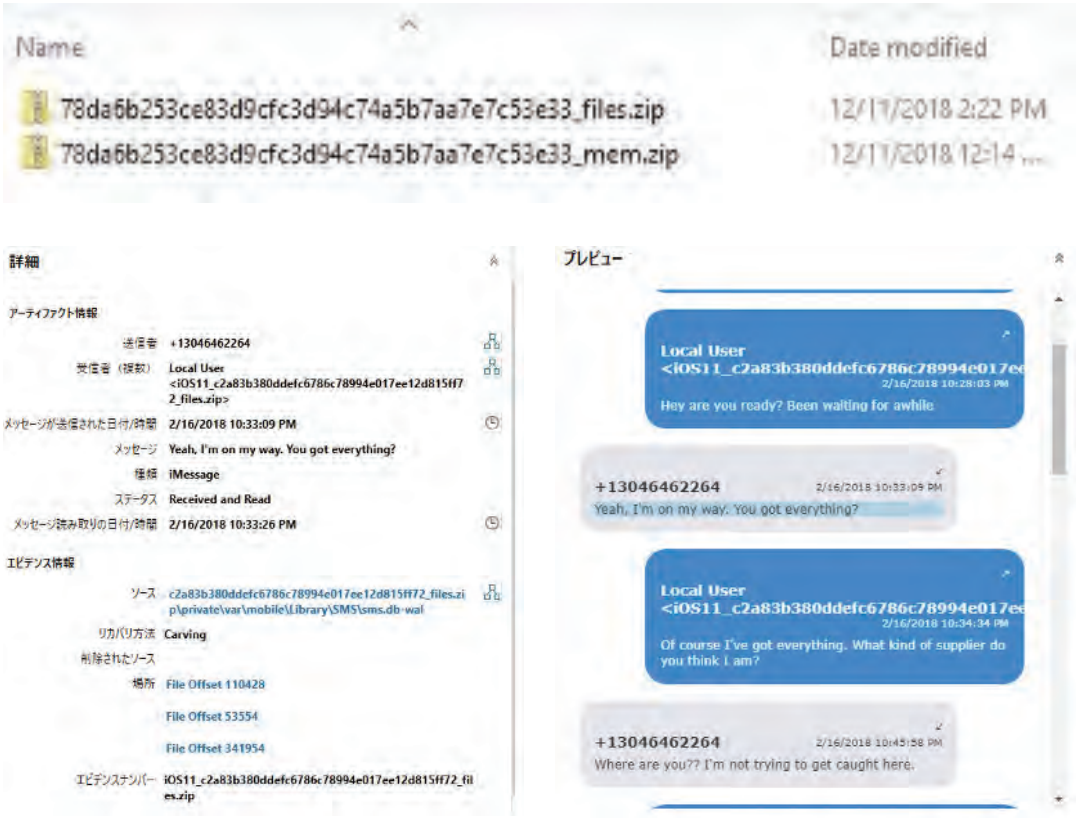


選択されたGrayKeyのすべてがAXIOMにインジェストされてしまえば、検査官はどのアーティファクトを自分達がスキャンしたいかを決め、またその中にある関連するエビデンスを探すイメージを持つ追加データを見つけるためにファイルタイプ別にAXIOMのDynamic App Finder やCustom Searchなどの詳細機能を使用することもできます。

Magnet Examineに情報が　み込まれれば、ユーザーが利用できる情報を最大化するためにMagnetが最近製品へ追加した膨大なアーティファクトがそこに揃います。このブログで、私達はこれらのイメージ中で見つけることが期待できるいくつかの重要なアーティファクトを詳しく説明します。

先書きログ(WRITE AHEAD LOGS)

GrayKeyはデバイスのファイルシステム全体のイメージを取得することができ、それは当社の基準アーティファクトと共存する一時ファイルまたはサポートファイルがいま精査用に利用できることを意味します。これの典型的な例はsms.dbと同じディレクトリーに存在するsms.db-walファイルです。sms.dbによって検査官はiMessage、SMSメッセージおよびMMSメッセージをリカバリーしパースすることができます。しかしながら、このデータベースはSQLiteの「先書きログ」(Write Ahead Logs)機能性を利用するため、メッセージは実際には主要なsms.dbにコミットされるより前にsms.db-walファイルに書き込まれます。これはメッセージが削除されるより前にデバイス上にどのくらい長くあったのかに応じて潜在的に削除されたメッセージをリカバリーする際に問題を引き起こす可能性があります。メッセージが送信/受信されるなりすぐに削除される場合、標準的なiTunesスタイルの抽出からこれらのメッセージをリカバリーすることができる可能性ははるかに低くなります。しかしながら、GrayKeyを使えばフルファイルシステムを抽出できるため、今はこのファイルにアクセスでき、AXIOMは潜在的に削除されたメッセージを含め先書きログに残されたメッセージの痕跡をカービングしようと試みます。



上の例では、sms.dbの先書きログからリカバリーしたメッセージの例、およびどのようにAXIOMがタイムスタンプ、方向性を含めて情報の多くをまだリンクし、Connectionsを使用してユーザー間のコミュニケーションをマッピングすることができます。先書きログでリカバリーしたメッセージはまだAXIOMでのチャットのスレッド作成オプションの一部でもあります、そのためユーザーはこれらのデータポイントが精査するための経時的ビューにスレッド化されているのを見ることができます。

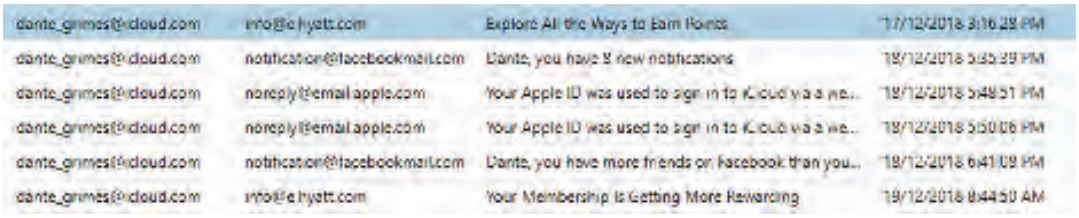
サードパーティのアプリケーションデータ

標準的なiTunesスタイルのバックアップのイメージでは、開発者はアプリケーションから何をインクルードしたいかについて非常に選択的になることができます。これの典型的な例には、これらのバックアップにキーファイルをインクルードしないFacebook、InstagramおよびTwitterなどがあります。AXIOMはGrayKeyイメージからのフルファイルシステムにアクセスするため、このサードパーティのアプリケーションデータは私達がまた利用できます。AXIOMでの簡易な例のいくつかは、Facebook Messengerのメッセージ、Instagram Direct MessagesおよびTwitterのツイートです。

これもDJI Goアプリケーション用データのリカバリーを表示するこの例など、アーティファクトによって通常処理されるのではないアプリケーションを詳しく調査するチャンスを検査官に与えます。

APPLE MAIL

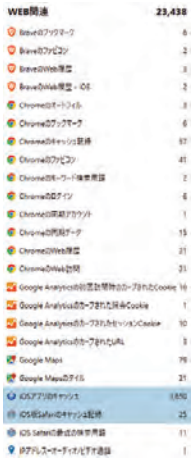
その時から情報が利用できなくなったのでiPhone 4 の登場以来Apple Mailのアプリケーション（Mail.app）は多くのフォレンジック検査官にとって厄介な対象でした。AppleはMail.appのデータをいくつかの最高レベルのファイルシステムで保護します、したがってこの情報はパスコードが決定された後でのみフルファイルシステムで利用できるようになります。見つかった後は、AXIOM Examineはこのアプリケーションからリカバリーされたメールの保存元/保存先、題名、送信日、受信日、要約および　み取りステータスを表示します。これらのメールは貴重なコミュニケーションポイントを提供できるだけでなく、検査官に彼らが探す必要がある他のサービスについて通知も行います



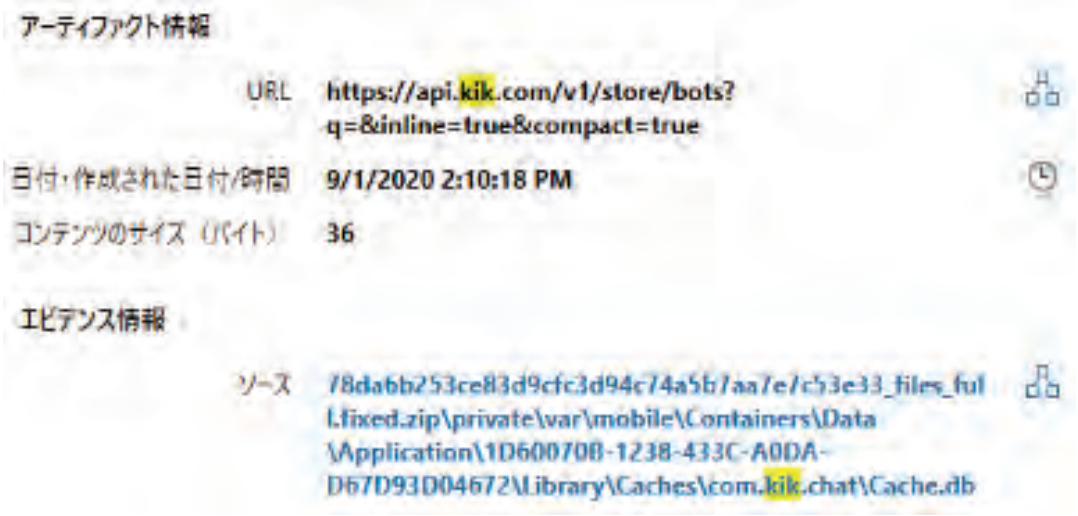
メールアプリケーション内で見つかったデータに加えて、AXIOM Examineはフルファイルシステムが利用できなくても様々なソースからApple Mail Fragmentsとして知られるアーティファクトもリカバリーする場合があります。これらのフラグメントは、デバイスからデータのすべてを取得するためにデバイスのパスワードがリカバリーされるのを待ちながらサービスプロバイダーの側から捜査を開始するために検査官がデバイス上で使用されるメールアドレスを入力するのに役立ちます。例えば、これらのメールのフラグメントは最初のロック解除以降（AFU）状態のデバイスからGrayKeyによって生成されるプロセスメモリのイメージからリカバリー可能な場合があります。

ウェブのキャッシュおよびアプリのキャッシュ

標準のSafariのデータをリカバリーすることに加え、これらのファイルシステムのイメージを使えばSafariアプリのキャッシュ情報など追加のウェブでのデータをリカバリーすることができます。ウェブのキャッシュはユーザーがURLで何を閲覧しているかに関しいくつかのコンテキストを与えてくれるため、この情報はユーザーがオンラインで違法材料を閲覧している場合の特定のケースの種類では非常に貴重になる可能性があります。

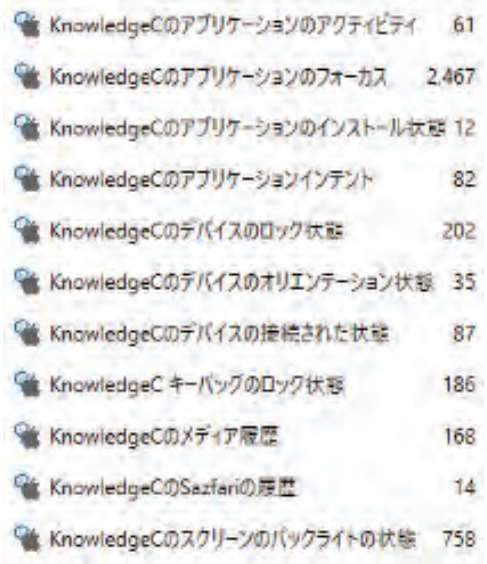


アプリのキャッシュのアーティファクトを使えば検査官は特定のアーティファクト用キャッシュ内に何が保存されるのかを知ることができます。アプリケーションは一般的に内蔵ブラウザーを持ちますがそれらのブラウザー用のウェブ履歴のログは多くを保存しません。これにより検査官にはサードパーティのアプリケーション内のリンクをクリックした時に見つかった情報をリカバリーするチャンスが得られます。



オペレーティングシステムのデータ　ー　KnowledgeC

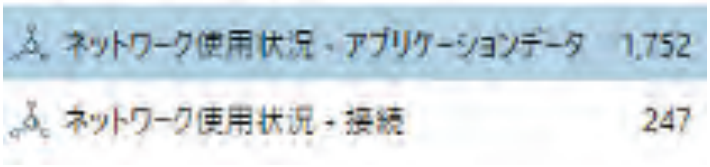
AXIOM Examine内部のオペレーティングシステムのカテゴリーにはこれらのファイルシステムのイメージに対し限定的に利用できる多くのアーティファクトがあります。その優れた例として、KnowledgeCアーティファクトセットがあります。これらのアーティファクトはそのようなアクティビティをマップに描く複数のアーティファクトを考察することでアプリケーションの使用パターンやユーザー一般を究明することに役立ちます。



オペレーティングシステムのデータ　ー　ネットワーク使用量

オペレーティングシステムのカテゴリー下のネットワーク使用量のアーティファクトにより検査官はユーザーが通信していた経路のワイヤレスアクセスポイントおよびユーザーがデータを送信した携帯基地局を知ることができます。ネットワーク使用量ーConnectionsのアーティファクトは種類に応じてCell IDやMACアドレスを表示します。

ネットワーク使用量ーアプリケーションデータのアーティファクトはWindows SRUMと非常によく似た働きをします。このアーティファクトを使えば検査官はどのプロセスがデータを使用したか、どのくらいの量のデータか、さらにWi-Fi、携帯および有線を含むどんな接続種類経由かを知ることができます。ユーザーがアプリケーションを使用したことなどないと主張する場合、アプリケーションIDを検索することでこのことの真偽を証明でき、また正確にどのくらいの量のデータがネットワーク経由で送信されたかが示されます。注記:この情報はユーザーが自分の設定で使用量統計値を消去することによりリセットできますので、デバイスに最初に電源が入れられて以降の完全な履歴ではありません。



オペレーティングシステムのデータ　ー　画面表示時間

iOS 12の新機能としてiOSが生成する画面表示時間のデータを使えば検査官は、アプリケーションがどのくらいの量使用されたか、それがどのくらいの数の通知を生成したか、およびこのアプリケーションに起因してデバイスが何回ピックアップされたかなど1時間の間隔で追跡できます。この情報は極めて貴重なものになる可能性がありますが、押収時直ちにデバイスが取得されなければならない重要な理由でもあります。

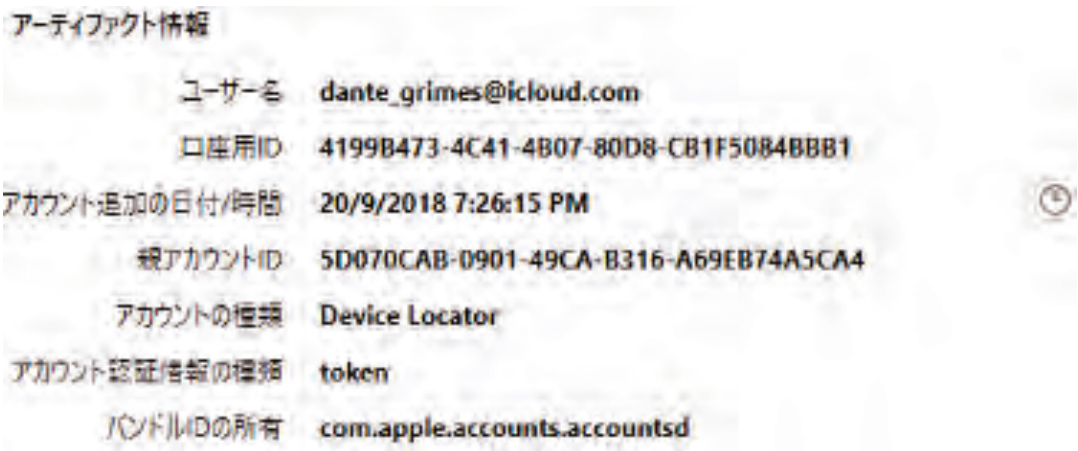
com.google.ios.youtube	29/12/2019 3:00:00 PM	130	0	1
com.apple.MobileSMS	27/12/2019 3:00:00 PM	5	0	1
com.apple.mobilenotes	13/1/2020 2:00:00 PM	172	0	1
com.google.GoogleMobile	8/1/2020 3:00:00 PM	41	1	0
com.zhiliaoapp.musically	27/12/2019 5:00:00 PM	208		
com.maplelabs.fakecalc	18/12/2019 11:00:00 PM	60		
com.facebook.Facebook	12/1/2020 11:00:00 PM	6	0	1
com.ebay.iphone	10/1/2020 4:00:00 PM	23		
com.toyopagroup.picaboo	9/1/2020 3:00:00 AM	22		
com.apple.mobilenotes	13/1/2020 3:00:00 PM	67	0	1

ロケーションのデータ

最近のiOSデバイス内部にはロケーションデータのストレージが複数ポイントあります。キャッシュされたロケーションおよび頻度の高いロケーションはユーザーがアクセスしたロケーションやリージョンを究明するのに密接に関連している可能性があります。Apple Payの取引データなど他の情報もまた、ユーザーのアクティビティの意味を解明するためこれらのロケーションポイントをマップに描くためにAXIOM Examine内部に表示できます。

キーチェーンのデータ

GrayKeyに生成されたキーチェーンファイル内に保存されたデータはエクスポート可およびエクスポート不可の値の両方を保存します。これは暗号化されたiOSバックアップからのキーチェーンのエントリーから利用できないGrayKey生成のキーチェーン内部にデータがあることを意味します。これらにはSSIDやパスコードと共に「AirPort」エントリーとして保存されたワイヤレスアクセスポイント、暗号化されたバックアップ用のバックアップパスワードおよびユーザーがこのデバイスでやりとりした複数のサービス用のトークンなどが含まれる可能性があります。インターネットのパスワードのアーティファクトはSafariブラウザーを使用したことによりキーチェーンへ渡された情報を保存します、またiOSデバイスから別のiOSデバイスへ、MacOSのデバイスへ情報を渡すこともできます。これによってユーザーはクラウドベースのソース用で適切な合法の権限を備えたユーザー名とパスワードをリカバリーすることができ、AXIOM Cloudを使用してそれらを取得することができます。



プロセスメモリのイメージ分析

GrayKeyに生成されたプロセスメモリのイメージを処理することによって、AXIOMはAFU（最初のロック解除以降）デバイスのプロセスメモリ内に保存された情報をカービングすることができます。これにはファイルシステムから削除されたかもしれない情報が含まれる可能性があります。これらのイメージはGrayKeyデバイスから取得され、“<udid>_mem.zip”の名前が付けられ、また他のイメージと同じ方法でAXIOM Processへ　み込むことができます。　み込みが終われば、AXIOMは自動的にウェブ関連、チャット、メール、メディアその他を含む記録をカービングしようと試みます。下の例では、iMessage/SMSメッセージ、メールのフラグメント、通話ログおよび実施されたGoogle検索などの正確な結果を含むプロセスメモリからカービングされた情報をいくつか表示しています。

まとめ

Magnet ForensicsチームはGrayshiftチームが提供したイメージを最近深く追求することに多くの時間を費やしました。私達はこの調査を非常に真剣に捉え、大量のデータによるパーシングをより簡単なものにする目的でフォレンジックのコミュニティへ最新の刺激的なアーティファクトを提供するために全力を注いできました。この新しいパートナーシップによって、Magnet ForensicsとGrayshiftはお客様がiOSデバイスを扱うときに最も簡単で最強のツールを手軽に使えるようにする仕事に専心します。

まもなく登場するいくつかの追加的な刺激的アーティファクトに引き続きご期待ください。