UFED NOTLAR:

Mobil cihaz analizlerinde kullanılır.

Harddiskte imaj alma kolay inceleme zor.Mobil cihaz incelemesinde imaj alma zor ve kesinlikle çok önemlidir , inceleme daha basit.

Ufed içerisinde birkaç araç barındırır bunlardan ilki UFED 4PC dir bu araç mobil cihazlarda imaj alma işine yarar.

7. Maddede olan kamerada telefonun uyku süresi varsa oraya lazer ışığı gönderir ve telefonun kapanmamasını sağlar sürekli atak yaparak telefon şifresini kırmaya yarar.

Herhangi bir inceleme aracının arayüzüne girdiğimizde önce ayarlara bakmalıyız.Default ayarlarına bakmalı hangi ayarları değiştirebileceğimizi bilmeliyiz .

Ayarlarda imajları nereye kaydeceğini bilmemiz lazım bu cihaz genelde imajları C sürücüsüne kaydeder boyut büyük olduğu için C sürücüsünde imaj alınırken yer kalmayabilir ve imaj yarıda kesilebilir.Bunun için imaj başlatılmadan farklı bir sürücü varsa orayı seçmeli ve imajı oraya kaydetmeliyiz.

SIM karttan silinen mesajları ayıklanması etkinleştirilmeli

Android Yedekleme APK sürüm düşürmeyi etkinleştirilmelidir.Bu seçenek cihazın içerisindeki mevcut sürümü kopyalayıp bir yere kaydeder daha sonra eski sürümlere düşüp o sohbetleride çeker .İşi bittiğinde güncel sürüme geri gelir.Bu da sürüm düşürmeye, eski sürümlerdeki verilerinde imajını almamızı sağlar .

Cihazların yeniden başlatma ikazlarını göster

Kablo ve İpucu Modu

Hangi kabloyla hangi uçu kullanmasını tavsiye etmesini istiyorsak seçiyoruz.

Kapalı imaj ve sim kartı imajı almak için cellebrite device adaptöre muhakkak ihtiyaç vardır.

Ayarların Rapor kısmında yapılacaklar:

Rapor kısmında gerekli etiketler(Bookmark) yapılmalı .Bu bölümde bu etiketler hakkında bilgi verdiğimiz bir rapor oluşturmalıyız.Çünkü bu raporlar adli makamlarada gidiyor.Raporlama kısmında bir diğer önemli husus rapor oluştururken dışarı aktaracağımız her bir değere SHA-256 ya da MD5 değeri oluşturmaktadır.Çünkü bu işlemle bir anahtar atamış oluruz eğer bu anahtar değeri değişmişse delil değişmiştir demektir.

Ayarlardaki etkinlik günlüğü hangi telefonun imajı alınmışsa, ne zaman alınmışsa bunun kaydı vardır.

Cihaz Araçları Kısmı:

1) APK sürüm Düşürmeden kaydedilen APK lar: APK sürümleri düşürülürken alınan APK ların kaydedildiği yerdir.Manuel olarakta ayarlanabilir.
2) Android Debug Consele : Android cep telefonun şifresi olmadığını düşünürsek belirli bir ayar aktif edilmediği sürece imaj alınamayacaktır.Bu ayar Android Debug ayarıdır.Telefonun ayarlarına geldik ordan telefon hakkında kısmına girmeliyiz.Burdaki değerleme ya da yapı numarasına 7 defa bastıktan sonra uyarı verir artık bir geliştiricisiniz diye.Geri çıkıp tekrar ayarlara geldiğimizde geliştirici seçeneklerinin aktif olduğunu görürüz.Geliştirici seçeneklerine tıklayıp uyanık kalma ve USB hata ayıklama kısmını aktif etmeliyiz.Buraya tıkladığımızda direkt bu görevi yapar.
3) Android Kurtarma Modundan Çık: İmaj almak için telefona baktık ama telefon kilitli ve ekran kapalıysa kapalı imaj alınacaktır.Recovry de işlem başarısız olursa ya da imaj çeşitli sebeplerden yarım kalırsa bu seçenek kullanıllır.Recoveryde kaldıysa kurtarma modundan çıka tıkla.Sürekli kendini başlatıyorsa Android başlatma döngüsünden çıka tıkla.
4) Android Ayıklama Dosayalarını Kaldırın: Burdaki amaç telefondaki imaj işlemi bittikten sonra telefonda herhangi bir kalıntının kalmamasıdır.
5) Bluetooth taraması: Bluetooth üzerinden mantıksal imaj alınabilir. Eski telefonlarda daha çok kullanılır.
6) CDMA çevrim dışı moda geçirme: Eski motorla çalışan telefonların imajını almak için çevrim dışı moda geçirmemiz gerekiyor.Bunu yapar.
7) Exit Celebrite Mode: Celebrite kendi toolunu yüklediğinde ordan çıkış yapmak için kullanılır.
8) Exit Motorola Bootloop: Motorola telefonlar için başlatma döngüsüne girdiyse telefonu başlatma döngüsünden çıkarmak için kullanılır.
9) Exit chat capture: Celebrite aracında ekran görüntüsüs alma özelliği vardır ama bu özellik bazen takılma yapabiliyor burdan rahat çıkmak için yapılan bir araçtır.Telefonda nereye girersek girelim ekran görüntüsü almak istiyorsak.
10) LG EDL recovery: LG cep telefonlarında EDL moduna alınmışsa burdan çıkılamıyorsa bu araç EDL den çıkmaya yarar.
11) Flash Cable 500 Firmware: Özel bir kablodur her iki tarafıda usb girişlidir.Bu kabloyla bilgisayara baladığımızda ekran kilitini atlayarak imajını almayı sağlar.
12) Nokia WP8 kurtarma aracı: Recovery başlatma modunda takılı kalınırsa ordan çıkmaya yarar.
13) Odin Modundan Çık: Odin mod samsung telefonlarda yazılım yüklemek için kullanılan bir moddur .Bu moda geçmek için home başlatma tuşu,ses kısma tuşu ve güç tuşuna basılarak bu moda geçebilirirz.Eğer bu moda girilir ve çıkış yapılamazsa bu araç kullanılacaktır.
14) Samsung Exynos Recovery: Samsun telefonlarda Exynos şirketi kullanılır genelde .Eğer kapalı bir cihaz varsa elimizde recoverye müdahale durmunda takılı kalırsak hangi cihazsa bunu tespit edip onarmaya yarar.Telefon eski haline gelir.
15) Tom Tom gezi günlüğünü etkinleştir: Kapalı bir gezi ğünlüğü , navigasyon varsa bunun imajını almaya yarar.
16) Windows Mobile İst.yi kaldır: Windows için celebrite ın yüklediği işletim sistemini windowstan silmek için kullanılır.Windows mobile farklı bir işletim sistemi kullandığı için.
17) İTunes şifreleme parolasını devre dışı bırak: Iphone imajı alınırken yedeklemeyi şifrele diyip o şekilde imaj alınabilir .Bu aracı aktif ettiğimizde eğer imaj yarıda kalırsa yedeğin şifresini kaldırmamıza yarar.

CELLEBRİTE İLE İMAJ ALMA:

Dron imajı,USB imajı,harddisk imajı, SIM kart imajı alabilirsiniz bu araç ile.

UFED kamerası:

Hiçbir şekilde imaj alamadıysak UFED kamerasıyla manuel çekim yapabiliriz.

DRON İMAJI:

Bazı dronların imajı alınabilir kendi dahili hafızalarının imajı alınabiilir ve yine takılan hafıza kartının imajı alınabilir .Bütün multimedyaların imajı alınabilir.Bütün hafizanın imajı alınabilir.

YIĞIN DEPOLAMA İMAJI ALMA:

Burda 3G modemlerin mantıksal imajı alınabilir.Hafıza kartının imajınıda burdan alabilirirz,Harddiskin imajını alabiliriz.

SIM Kart İmajı Alma:

Yurtiçi ve Yutdışı olarak iki seçenek çıkar hangisini istiyorsak onu seçerek devam ederiz.Bu seçenek seçildikten sonra karşımıza Gelişmiş mantıksal , SIM kopyalama ve Kamera seçenekleri çıkar.

Gelişmiş mantıksal yöntemi genelde kullanılır.SIM kart takılır pin kodu varsa onu girmeliyiz ve imajı almalıyız.

Genelde SIM kartların imajı gelişmiş mantıksal yöntemle alınır.

SIM kopyalama eski tuşlu telefonlarda kullanılır çünkü eskilerin çoğunda SIM kartı olmadan telefon açılmazdı.SIM kart taktığımızda herhangi güncel bir mesaj geldiğinde delil bütünlüğü bozulabilir o yüzden bu özellik kullanılır.Kopyaladığımız SIM kartı telefona taktıp rahatça imajını alabiliriz.

SIM kartı resmi çekmek istiyorsak Kamera kullanılır.

Mobil Cihaz İmajı Alma :

Cihaz bağlıysa ve şifresi yoksa eğer araç hemen cihazı tanır.KONSOL seçeneği aktifleşir ve oraya tıklarsak debug ayarlarını otomatik yapar , imaj alma işlemine başlayabiliriz.

İmaj alma işlemine başlamadan önce aracımız cihazımızı destekliyor mu buna bakılır.Celebriteda cihazlara gözat kısmı vardır buraya girerek telefonun modelini yazıyoruz.**CİHAZLARA GÖZAT** kısmında **TÜMÜ,SATICILAR,GENEL PROFİLLER,SON KULLANILAN** gibi bölümler vardır.

Bu seçeneklerden kolayca arama yaparız.Önce tümü kısmından cihazın ismini yazarak arama yaparız eğer bulamazsak satıcı kısmına gireriz.Dünyada birkaç tane çip ve birkaç tane anakart üreten firma vardır.Genelde çoğu telefon markası aynı çip ve anakartı kullanır.Bu yüzden satıcı kısmını girerek farklı bir markanın çok benzer telefonunu seçebiliriz ve yüksek bir başarıyla imaj alabiliriz.Satıcıdan yola çıkılarak çok başarılı imajlar alabiliriz ama burdan da bir şey bulamazsak genel profiller kısmına gireriz.Burda ipuçlarından yola çıkmalıyız elimizdeki telefon nedir , örneğin hangi işletim sistemi(android) olmasından yola çıkarak cipsetinden yola çıkarak mantıksal imajını alabiliriz.

Son kulanılan kısmında ise son kullandığımız cihazlar kayıtlı kalır .

Xry Adli Aracı

Oxygen Forensic Adli Aracı

UFED 4 PC Adli Aracı

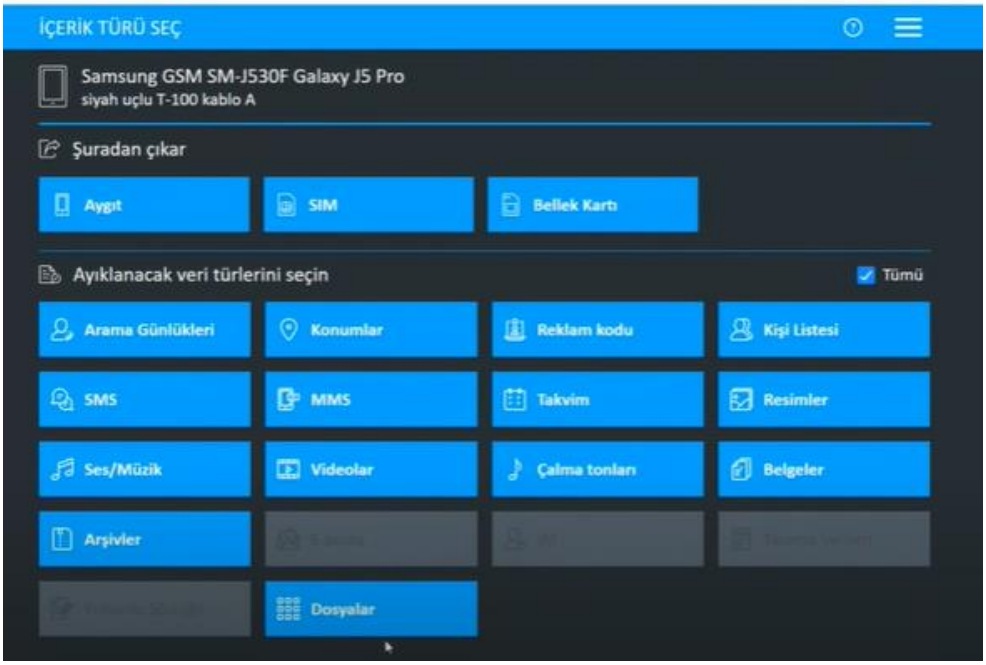
Celebrite kilidi kırar , kilidi olsa dahi dosya sistemli imajını alır , kilidi olsa bile fiziksel imajı alır.Ama bu işlemi Android 8 ve 6 sürümlerinde destekler.Bu yöntemlede imaj alınamazsa, EPEY sitesine kendi cihazımızı yazarız cipsetine tıklayıp, aynı çip setini kullanan yani aynı benzer özellikleri olan cihazları görürüz.Bu aynı çip setini kullanan cihazları tek tek deneriz eğer aracımız imajı alabiliyorsa o cihazı seçip imajını almak istediğimiz telefonun imajını o şekilde alırız.

OTOMATİK SAPTAMA: Bu kısımda araç taktığımız cihazın çip setini otomatik algılayarak aynı çip setini kullanan cihazları getiriyor.

GELİŞMİŞ MANTIKSAL İMAJ:

Bir telefondaki en basit imaj alma yöntemidir.En temel veriler olan; SMS,çağrı kaydı,MMS,takvimler,bazı medya dosyaları.Android sürümleri için ayrı bölümler vardır her bir android sürümü farklı güvenlik seviyesi içerdiği için böyle bir durum vardır.Bu yöntemin kullanılması için debug ayarlarının yapılmış olması ve ekran kilidinin olmaması gerekir.

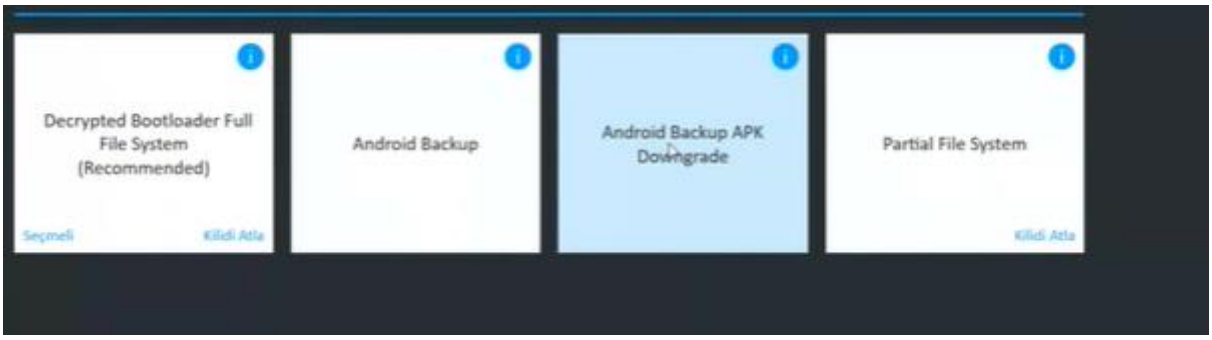
İçerik türlerini seçerek veri türüne göre sadece belirli bölümün imajı alınabilir.Örneğin sadece SMS ile ilgili bir dava varsa sadece SMS bölümünü seçerek buranın imajını alabiliriz.



Kullanıcı Kilidini Devre Dışı Bırakma/Etkinleştirme: Disable User Lock butonuyla ekran kilidinin olduğu herhangi bir cihazdan imaj alamayacağımız için bu bölümü kullarak kullanıcı kilidini geçici olarak devredışı bırakırız.İmajı aldıktan sonra devredışı bıraktığımız kilidi Re-Enable User Lock butonuyla silmiş olduğumuz ya da devredışı bırakmış olduğumuz kilidi tekrar aktif hale getirebiliriz.Lockpick butonuyla ekran kilidini pasif hale getirdiysek tekrar etkinleştiremeyiz.

Dosya Sistemli İmaj: Bu imaj gelişmiş mantıksal imajın bir üst seviyesidir.Gelişmiş mantıksal imajda alınmış olan tüm verileri alır ilave olarak dosya sistemli imaj da alır.Böylece bazı silinen verileri de getirir.Bu bölümünde kendi içinde farlı versiyonları vardır.

Bunlar:



Android Backup: Android Backup bir telefonun , telefon üreticisinin o telefonun içerisindeki temel verileri dosya yapısını yedekleme yöntemiyle almış olduğu imaj formatıdır.Bu şekilde bir imaj formatı oluşturur.Bu yöntemle telefonun temel sistem uygulamalarıyla telefonun temel verilerinin imajını alır ama ekstra indirilen uygulamaların yedeği alınmaz örneğin whatsap verileri gibi,sadece temel dosya verilerini,temel sistem verilerine erişebiliriz.**İlave Ayıklamalar kısmında ayrı ayrı alınan imajları birleştirir.**

Android Backup APK Downgrade: 3.parti uygulamalarının sürümünü düşürerek imajını alır.Bu işlem yapılırken veri kaybı yaşanabilir.

Partial File System: Android 6 sürümünden sonra kullanışsız olmaya başladı.Bu seçenekte dosya sistemli imaj alır ve pasword kullanıcı kilidini okuyup bize şifreyi verir.

Decrypted Bootloader Full ..: Dosya sistemini full imajını alabilir şifreyi de atlayabilir.Fiziksele yakın dosya sistemli imajı alır.

ADB: Kök iznine sahipsek ADB komutu çalışır.

Full File system (FBE): Telefonun şifresini passcode'nu bulmaya çalışacak.Bulduğu şifreyle telefonu açıp bu şekilde imajını alabiliriz**.**

MTK Live :

Fiziksel İmaj alma yöntemleri:

Decrypted Boot Loader(Recommended): Telefon kapalı kilit atlama yöntemiyle recovery'e müdehale ederek imajını alabiliriz.

ADB (Rooted): Kökü belli değilse imaj alamaz.Kök izni varsa burdan başlatabiliriz.

Boot Loader: Recoveryde şifre yoksa download moduna alarak telefonu bağladığımızda imaj alabiliriz.

Advanced ADB: Açıksa şifresi yoksa direk bu yötemle başlatılabilir.Bu yöntemin çalışma mantığı cihaza açıksa bir istemci yükler.Yükleme bittikten sonra(bilgisayara bağlı olduğu süreç buraya kadar sonrasında bilgisayardan sökebiliriz), hafıza kartıyla ya da bir usb takarak FAT32 şeklinde biçimlendirmemizi ister .Daha sonra telefonun imajını açık bir şekilde bilgisayara bağlı olmadan USB ya da hafıza kartına imajı alır.

MTK Live: ADB değil ekran kilidi de yok.Root atmadan da açık fiziksel alabiliriz.

- **Farklı çip setlerinde farklı yöntemler çıkabilir.Huawei Generic Android yazarak çip setlerini karıştırabiliriz.**

Kamera:

Web kamerası yardımıyla telefon içerisindeki verileri görüntülememize fayda verir.En son çare.

Ekran görüntüsü:

Eğer verileri alamadıysak en kötü ihtimalle fotoğraflarız.

Sohbet Kaydı:

Mesela WhatsApp sohbetini görmek istiyorsak konuşmaları sıralar.Yazıları tarayıp metin haline getirir.Otomatik tarar.Ekran görüntüsünde elle yapıyoduk burda kendi yapar.Yukarı kaldırıp çekecek,yukarı kaldırıp çekecek,kayıt altına alacak.En kötü ihtimal manuel bir yöntem olarak bu yöntemi kullanabiliriz.

Apple cihazlarda imaj alma işlemi :

- **Kullanıcı Kilidini Devre Dışı Bırakma/Etkinleştirme :Fakeler için**

Mantıksal(Kısmi):

Gelişmiş Mantıksal :

Full File System: Telefon şifresizse burdan da alınır.

Full File System (checkm8): checkm8 açığını uygulayabilir.Kilitli olsa dahi alabilir.Bu açığı kullanabiliyorsa burdan alıyor.

- Iphone'nun imajını Celebrit'ten mantıksal almıyoruz.Bunun yerine inceleme yazılımı olan Physical Analyzer kullanarak ayıkla kısmına gelip İOS Cihazı Fiziksel Ayıklama'ya tıklayıp burda iphone 4'e kadar olan telefonların fiziksel imajını,kapalı full imajını alabiliyoruz.Artık check1 checkm8 açıklarıyla bazı modellerin bazı sürümleri için full file system alabiliyoruz.Ekran kilidi yoksa iphonun gelişmiş mantıksal imajını UFED for pc den almak yerine Phiysical Analyer'dan almayı tercih ediyoruz,daha fazla veri getirdiği biliniyor.Fiziksel imaja yakın imaj getirir.

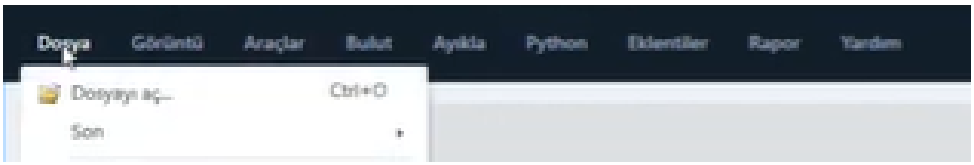
Fiziksel almıyor. Nedeni iPhone'da donanım kilidi var.O da şu,Key dosyası silikonla yazılıyor.Sonra key dosyası oluşturduğumuz passcode'la birleşiyor,daha farklı bir anahtarla dönüşüyor.10 defa yanlış girdiğimizde password'ü siliyor.Silindiğinde donanım kilidi orda olsa dahi verilere erişemiyoruz.Üst düzey güvenlik var.

Kamera:

Ekran görüntüsü:

- **Şifre çözmek için Oxygen'de kendimizin oluşturduğu wordlisten atak yapabiliriz.Kendisi de yapabiliyor.Huwavey cihazların imajını almak için Oxygen çünkü fiziksel alabilir ama cellebrite'da alamayız.Cellebrite'ın arayüzü daha kullanışlı donanım yazılım işbirliği var.**
- **Cellebrite bütün imajın,her partion'un,her bir verinin veri bütünlük değerini hesaplıyor.Bunu Oxygen de , Mobile Edit de yapıyor.Bu zorunlu.**
- **Mobile cihazlarda her seferinde imaj aldığımızda farklı bir bütünlük değeri oluşur.Çünkü dinamik bir sistem,dinamik bir sistem sürekli değişkendir.En son aldığımız imaj geçerli olacaktır.**

Cellebrite Physical Analyzer: Cellebrite'ın imaj alma yazılımı ayrı bir yazılım,inceleme yaptığımız yazılım ayrı bir yazılım.Her ikisinin setup'ını ayrı ayrı kurmak zorundayız.Arayüz olarak oldukça basittir.Şimdi menüleri inceleyelim:



Dosya

Dosyayı aç:

Dosyayı aç' tıklarız.Ekle'ye basarız.Almış olduğumuz bir imajı açmamıza yarar.Genel olarak **Aç(Gelişmiş)** kısmı ile dosyayı açarız.Cellebrite alınmış bir dosyanın imajını açmak için Ayıklama yükle seçeneği seçilir.Farklı bir forensic yazılımıyla almış olduğumuz bütün imajları açmak için kullanılan sekme Aç(Gelişmiş).

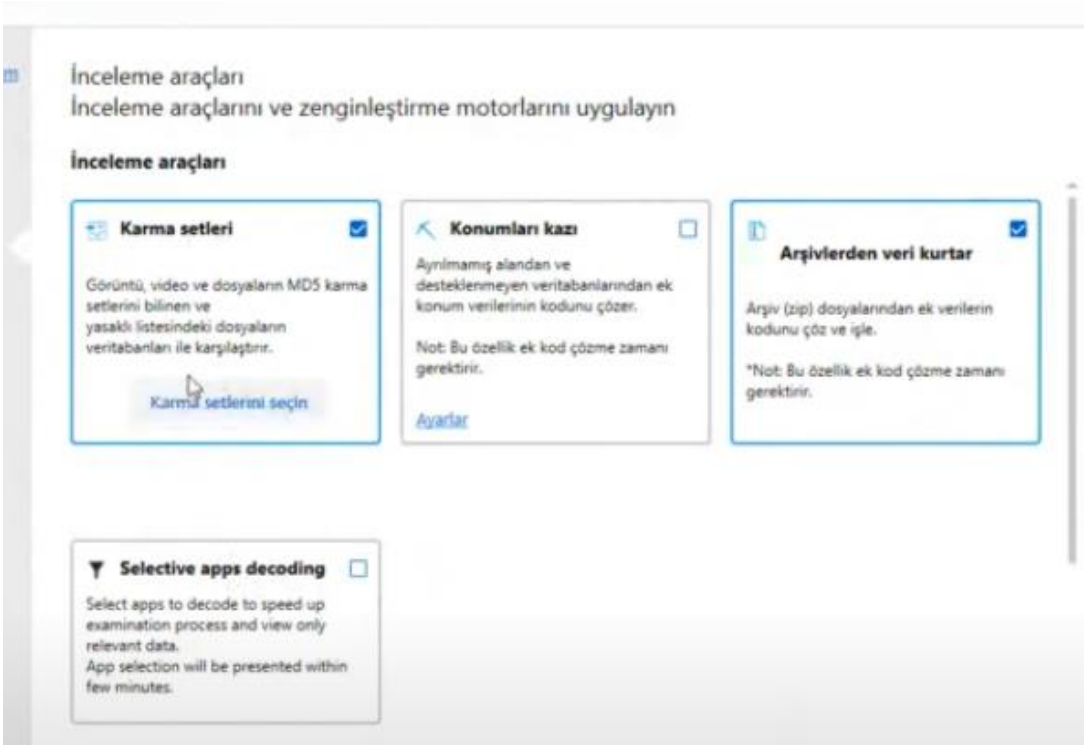
Karma setleri: MD5 hesaplamasını istiyorsak buraya tıklanır.

Konumları kazı: Konum kazımasını istiyorsak buraya tıklanır.

Arşivlerden veri kurtar: Arşivlerden veri kurtarmak istiyorsak tıklıyoruz.

Selective apps decoding: Decod edilememiş uygulamaları decod etmesini istiyorsak filtrelemesini istiyorsak seçebiliriz.

Ortam sınıflandırması: Fotoğrafları içeriğine göre katagorilerine göre sınıflandırmasını istiyorsak seçebiliriz.



Aç(Gelişmiş):

- Cihaz Seç'e basarsak,telefon marka modeli seçiyoruz.Image'ye tıklayıp imajı gösteriyoruz.
- Boş projeye basarsak,Zinciri Özelleştir sekmesinde cellebrite bu imajların içeriğini çözmek için kullanmış olduğu küçük toollar var.Eklentiler'in her birini,Zincirler'in her birini bu şekilde saklıyor.Cihazlar da burda var bu sekmeye burdan da erişebiliriz.Seçtiğimiz komutları kullanarak bu imajı açar.
  Android imajımız varsa ilk kullanacağımız komut AndroidDD.AndroidDD komutunu hem imajı alırken hem de imajı açarken kullanırız.
  AndroidContent,file system'i record etmek için bu komutu kullanırız.
  Android Generic komutunu kullanırız.
  Hangi çipsete sahip olduğunu biliyorsak onu da ekleyebiliriz.
  AndroidMTK NAND'ı seçiyoruz.
  Zincir olarak bunları ekleyip tamam diyoruz.
- İkili ayıklama'ya gelip image'ı ekledik.Sonraki dedik.
- Ayıklamayı ayrı bir proje olarak aç diyip sonraki dedik.
- **Karma setleri:**MD5 hesaplamasını istiyorsak buraya tıklanır.

Konumları kazı: Konum kazımasını istiyorsak buraya tıklanır.

Arşivlerden veri kurtar: Arşivlerden veri kurtarmak istiyorsak tıklıyoruz.

Selective apps decoding: Decod edilememiş uygulamaları decod etmesini istiyorsak filtrelemesini istiyorsak seçebiliriz.

Ortam sınıflandırması: Fotoğrafları içeriğine göre katagorilerine göre sınıflandırmasını istiyorsak seçebiliriz.

Üsttekilerden istediğimizi seçip Verileri incele deriz.

Aç(Gelişmiş):

Dosya sistemli imajı eklemek için

- Boş projeyi seçiyoruz.
- General mobile telefon varsa,AndroidContent'ekledik.AndroidDD'yi ekledik.Android Generic'i ekleyip tamam dedik.
- **ZIP arşivi'ne** basıyoruz çünkü artık imajımız bir backup imaj yani bir yedekleme dosyası.ZIP olarak dışarıya aktardığımız bir imaj olduğunda burdan Zıp arşivinden ekleyebiliriz.Mantıksal imaj göstereceksek,E01 ya da bin şeklinde bir fiziksel imaj,dosya sistemli imaj göstereceksek **Klasör seç** diyip gösterebilirdik.
- Sonraki diyoruz.
- Sonraki diyoruz.
- İnceleme araçlarını seçiyoruz.
- Verileri incele diyoruz.
- Verileri çözmeye başlar.İmajı açar.

Yaygın kaynak:

Telefon şifreli,ilk bakacağımız yer bu yol.itunes yedeklemesi aldıysak,itunes yedeklemesi C-Kullanıcılar-Ana kullanıcılar-AppData-Roaming-Apple Computer-mobilesynyc içerisinde gözükür.Burdaki yedek dosyası iPhonun backup'ı olacaktır.Nasıl açacağımıza bakalım:

- Yedekleme'ye tıklayıp iTunes yedekleme'yi seçip,klasörse Klasör seç'e,ZIP'se ZIP arşivi'ne tıklanır.
- Klasörü seçtikten sonra Sonraki denir.
- Sonraki denir.
- İnceleme araçlarını seçiyoruz.
- Verileri incele diyoruz.
- iPhone'nin imajını açar.

Ayıklamayı ekle:

Daha önceden açmış olduğumuz imaj varsa hızlı bir şekilde eski açtığımız imajı açabiliriz.

Harici dosya ekle:

Bu imajla ilgili harici dosyalar varsa bunları da ekleyebiliriz.

UFDX olarak kaydet:

UFDX bir UFD imaj formatıdır.İstediğimiz bir imaj dosyasını dışarıya bu şekilde aktarabiliriz.

Proje Oturumunu Kaydet:

Bazen çok büyük imajlarla çalışabiliriz bu çalışmalarda çeşitli incelemeler yapmış veya etiketleme işlemi yapmış olabiliriz.Böyle bir projede herhangi bir aksilik yaşandığında bilgisayar kapandığında etiketler ve incelenen proje silinecektir.Bu sorunu önlemek için ara ara oturumu kaydetmeliyiz.pas dosyası olarak oturumu kaydeder.Biz kaydetmezsek kendisi bu işlemleri ara ara yapmaz.

Proje Oturumunu Yükle:

Buraya bastığımızda önceden kaydettiğimiz pas dosyasını gösterdiğimizde etiketlerimiz en son kaydettiğimiz şekliyle açılacaktır.

Görüntü

Hoş Geldiniz Ekranı:

Bu zamana kadar hangi imajları açtıysak onu görürüz.

İz penceresi:

Aşağıda ne zaman hangi işlem yapıldıysa onu görürüz.

Araçlar

Daha fazlasını al (Kazıma):

Resimleri kazı,Dize kazı,Konumları kazı,Kazıma dosyaları (genel) seçenekleri var.

Harddiskte sektör sektör gittiğimizde veri kurtarmak çok daha kolayken,Mobil cihazlar genelde veriler bit bit yazıldığı için burda veri kurtarmada silinen verileri kurtarmada çok iyi sonuçlar vermez.

Zenginleştirme motorları:

Resimleri kazı,Dize kazı,Konumları kazı,Kazıma dosyaları (genel) seçenekleri var.

Ortam sınıflandırması:

Çok fazla resim dosyası varsa istediklerimizi katagorize eder.Hangileriyle ilgili resim arıyorsak onlara bakarız(Kredi kartları,Uyuşturucular,Para).

İzleme listesi:

İzleme Listesi Düzenleyicisi:

Anahtar kelimeleri buraya yazarak işlemlerimizi gerçekleştirebiliriz.

Kelimeyi nerede aratmak istiyorsak seçebiliriz,anahtar kelimelerimizi seçip uygulaya basıp tamam diyip listemizi oluştururuz.Otomatik Etkinleştirirsek bütün imajlar açıldığında bu kelimeleri arar.

İzleme listesini çalıştır:

Hangi imajın içerisinde çalıştıracağımızı,hangi izleme listesini seçeceğimizi belirleyip uygula deriz.Aramaya başlar.

Tamamlanan öğelere sağ taraftaki İzlenimler'den ulaşabiliriz.

Kötü Amaçlı Yazılım Tarayıcı:

Kötü Amaçlı Yazılım Tara:

İmaj içerisinde kötü amaçlı yazılım tarayacaksak yardımcı olur.Taramaya başlar.

Sağ taraftaki İzlenimler'den takip edebiliriz.

Çeviri:

İnceleyeceğimiz imajı farklı dile çevirir.

Çevrimdışı haritalar:

Cihaz Konumları'nda fotoğraflar çekilirken konumu açıksa eğer nerede çekildiyse çekilirken konumlarını veriyor.Bu şekilde görebilmemiz için Çevrimdışı Harita Paketini kur'mamız indirmemiz webten güncellememiz gerek.

BSSID ve Baz Kimliklerini zenginleştirme:

Konum verileri çıkarmak için kullanılır.Varsa elimizde İçe Aktar'abiliriz,Yükle'yebiliriz.

SQLite sihirbazı:

SQLite sorgu yöneticisini aç:

Veri tabanları şeklinde sekme var.Bu veri tabanlarını SQLite görünümünde de açabiliriz.Cihaz içerisindeki veritabanlarına burdan bakabiliriz,burdan filtreleme yapabiliriz.Ancak kendimiz sorgu oluşturmak istiyorsak;

İçe Aktar diyerek dışardan bir veritabanı gösterebiliriz.Burda kendimiz bir sorgu oluşturabiliriz,bu veritabanı içerisinde aramalar yapabiliriz.

TomTom:

TomTom'lar bir nagivasyon.Bu nagivasyonu gezi günlüğünü dışarı ve içeri aktarabiliriz.

Virtual Analyzer:

Bazı APKları sanki mobil cihazdaymış gibi canlandırabilir.AndyOS sanal emülatörünü yüklememiz gerekir.

AppGenie:

Bulanık mantık,bazı uygumaları veritabanlarını analiz ederek örneğin bu Whatsapp veritabanı olabilir,bu bir veritabanıdır,bu bir mobil cihaz bir uygulama veritabanıdır diyip kendi kendine bu kararı verip bunun içerisindeki verileri anlamlandırıp karşımıza getirir.Silinenleri de görebiliriz.

Çalıştırırsak işi bittiğinde İncelenen Veri bölümünde görürüz.

Etiketleri yönet:

Etiket(bookmark) demek işaretlemek demektir.Delil bulduysak delili etiketleriz.İsmini,rengini,kısayalonu belirleyebiliyoruz.

Sol tarafta **Etiketler** kısmında etiketlediklerimizi görebiliriz.

Bu etiketleri dışarıya aktaracağız.Dışarı aktardığımızda Rapor'a tıklayıp Rapor oluştur'a tıklayıp Yalnızca etiketler'i dijital olarak dışarıya aktarıp kanıt olarak rapora ekliyoruz.

Sözlük dosyaları oluştur:

Proje içerisinde 4 haneli,6haneli şifre olabilecek her şeyi wordlist oluşturur.Bu wordlisti atak yapmada kullanabiliriz.Telefon içerisindeki verilerden faydalanarak bir sözlük oluşturur.

Ayarlar:

Genel Ayarlar:

Hangi ayarı yaptığımızda bu yazılım nereye müdehale eder bilmemiz lazım.Adli araçlar bazı şeyleri default varsayılan olarak yapar.Birçok değişken seçeneğini de bize bırakır.

Zaman dilimi:

Zaman damgalarını her zaman bu zaman dilimine ayarlayın: Meydana gelen olay Türkiyedeyse UTC3'e göre gerçekleşecek,bu yüzden incelediğimiz imajın zaman dilimini UTC3 seçeriz.Burası varsayılan olarak UTC0 gelir.

Ayıklamalar:

Karşılık gelen ayıklama yüklenirken bir oturum dosyasını geri yüklemeyi öner: Oturum dosyasını kaydettiğimizi biliyorsa bunu bana uyar.

Silinen dosyalar için '.DEL' uzantısı ekle: Silinen dosya varsa silindiğini anlamak için yanına .DEL eklemesini sağlarız.

Küçük resim ön belleği:

Küçük resim önbelleğini belleğe yükle: Resimleri incelerken çok hızlı bir şekilde görürüz.

Kod Çözme:

Android ve Windows Phone cihazlar için silinmiş verileri ayrılmamış alandan kazıyarak kurtar: Bu seçili olmazsa kazıma yapmayacaktır,silinen mesajları ayıklamayacaktır.

SQLite için derin kazımayı kullan: Mobil cihazlar veri tabanlarını tutarken SQLite veritabanını kullanır.Bu veritabanını kullandıkları için kazıma yaparken örneğin silinmiş whatsapp sohbetlerinin gelme ihtimali çok daha yüksektir.Bir resim dosyasının gelme ihtimali çok düşükken bir sohbet dosyasından veri kazıma yaptığı zaman o sohbetin gelme ihtimali çok daha yüksektir.

Veri dosyaları:

Birçok veri dosya formatı var.Genel olarak en çok kullanılan dosya formatlarını arar.İstediğimiz dosya formatını ekleyebiliriz.

Proje ayarları:

Saat değerlerini düzeltebiliriz.Vaka bilgisi girebiliriz.

Bulut

Ayıklama:

Özel bulut verileri:

Normal cihaz inceleyebildiğimiz gibi özel bulut verilerini de inceleyebiliriz.Bulut hesabının imajını alabiliriz.

Avatarları yönet:

İncelemek istediğimiz Veri kaynağı'nı (instagramı) direkt açarak inceleme gerçekleştirebiliriz.**Kullanıcı Hesapları'na** tıkladığımızda aktif edilen instagram hesaplarını Kullanıcı adı'nı Parola'larını görebiliriz.

Ayıkla

iOS Cihazı Fiziksel Ayıklama:

iOS cihazlarının fiziksel imajlarını gelişmiş mantıksal imajlarını burdan alabiliyoruz.

GPS / Yığın Depolama Cihazının Dökümünü Al:

GPS yığın depolama cihazlarının dökümünü alabiliyoruz.

Python

Çalıştırılabilir kodları eklenti şeklinde yazmış.Python kodunu buraya girerek burda çalıştırarak imaj üzerinde bu işlemleri gerçekleştirebiliriz.

Eklentiler

Çalıştırılabilir kodları eklenti şeklinde yazmış.Kodları neyle alakalı yazdıysak oraya tıklayıp yükleyebiliriz,çalıştırabiliriz.

Rapor

Dosya incelememizi bitirdikten sonra,eklentilerimizi yaptıktan sonra bir kısmını belirtiriz,bir kısmını da dijital olarak veririz.

Yardım

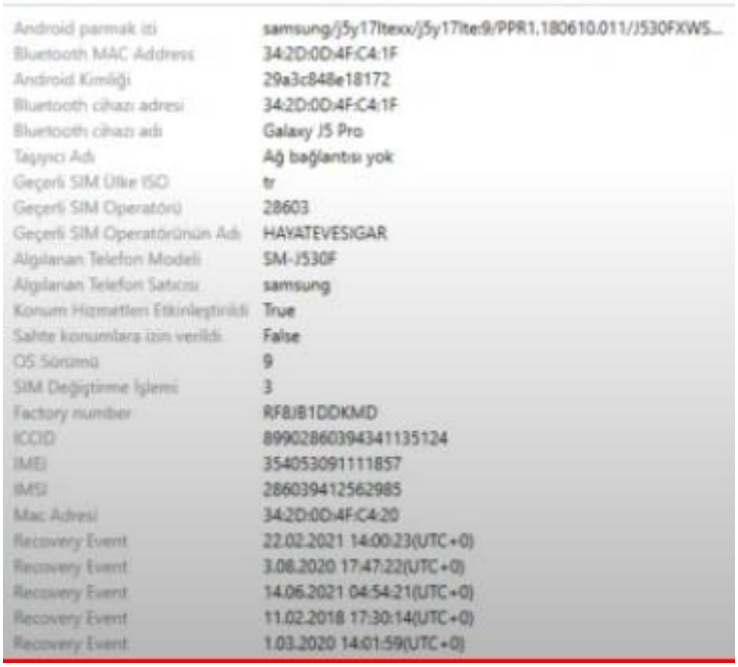
Manuel:

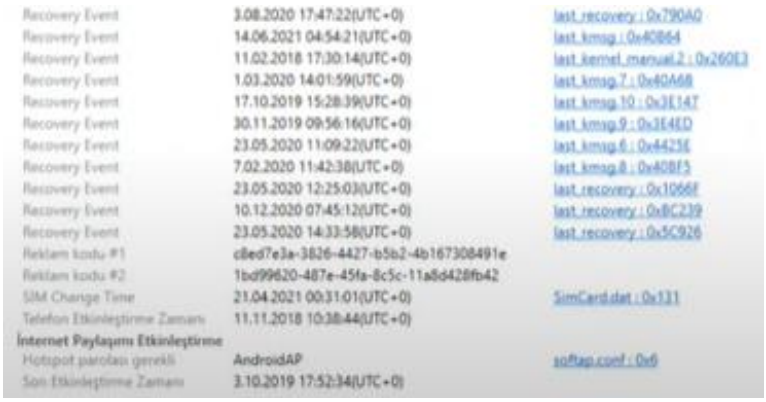
Yardım menüsü açılır.Menüleri tek tek anlatır.

Tüm İçerik

Araç açıldığında ana sayfada bu kısım çıkar.

Ayıklama özetinde cihaz ile ilgili bilgilere erişiriz.Bilgi sayısı telefondan telefona değişiklik gösterir.





Ayıklamanın ne zaman başladığı ne zaman bittiğiyle ilgili verilere erişebiliriz.

Fiziksel

Yine anasayfada olan **FİZİKSEL** kısmında ayrıntıları göster bölümünde her bir bölümün HASH değeri gösterilir.Raporu inceleyen kişinin bakacağı ilk şey imajın HASH değerlerini karşılaştırmak olacaktır o yüzden bu bölüm çok önemlidir.

Ev: İlk açıldığındaki arayüzü görürüz.

Zaman Çizelgesi: Cihazın en son formatlandığı tarihten bu zamana kadar olan bütün zaman aktivitelerini tarihsel bir sıraya göre gösterir.

İncelenen Veri: Bu kısımla ana ekranda gözüken İçerik kısmı aynıdır,sadece İncelenen Veri'de veriler katagorize edilmiştir.Hedefe yönelik araştırma yapmak istiyorsak buradan ilerleriz.

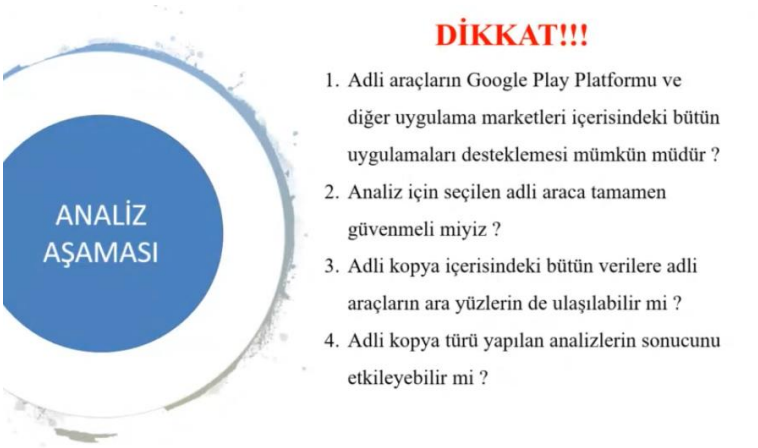
Dosya Sistemleri: Dosya Sistemleri içerisinde incelediğimiz dosyanın konusuna göre ağaç yapısını tek tek aşağı indirerek istediğimiz sonuçlara kısa sürede ulaşabiliriz.**Hafıza Erimlerinden** kasıt,binary olarak hexadecimal olarak arama yapmak istiyorsak buraya gelip grep araması yapabiliriz.Grep demek belirli bir desen,kredi kartı numarası,telefon numarası,kelime gibi arama yapmaya denir.Bütün imajın seçtiğimiz partionun her bir byte'ında istediğimizkelimeyi arar,daha derinlemesine arama yapar.Bura bütün alanda arama yaparken İzleme Listesi yüzeysel arama yapar.Text alanı da gözükür.Gösterir bize o alana da gidebiliriz çift tıklayıp.

İzlenimler: Kötü amaçlı yazılım araması yapıldıysa burda gözükür .İzleme listesi çalıştırıldıysa burda gözükür.

Etiketler: Etiketleme yapıldıysa burda gözükür.

Bulut: Bulut hesaplarının herhangi bir tanesine gittiğimizde verileri çektiğimizde gelen veriler burda gözükür.

Yüklü Uygulamalar kısmında:Tanıtıcı ad kısmında(package) zararlı apk'ları farkedebiliriz.Farklı adları taklit ediyor olabilir ismini benzeretek ya da adları anlamsızdır.



MANTIKSAL AYIKLAMA		FİZİKSEL AYIKLAMA	
Arama Günlüğü	2000 (0)	Arama Günlüğü	2797 (15)
Cihaz Konumları	979 (0)	Aranan Öğeler	4564 (0)
Kişi Listesi	571 (0)	Kişi Listesi	10651 (37)
MMS Mesajları	3 (0)	MMS Mesajları	7 (0)
SMS Mesajları	4063 (0)	SMS Mesajları	9630 (1036)
Takvim Maddeleri	39 (36)	Takvim Maddeleri	19 (18)
Arşivler	22 (0)	Arşivler	237 (131)
Belgeler	93 (0)	Belgeler	414 (18)
Kategorize Edilmemiş	2527 (0)	Kategorize Edilmemiş	135819 (95915)
Metin	993 (0)	Metin	15296 (11127)
Resimler	10287 (0)	Resimler	143492 (11959)
Ses	439 (0)	Ses	568 (118)
Veri tabanları	122 (0)	Veri tabanları	973 (24)
Videolar	423 (0)	Videolar	1156 (331)
-	-	Baz İstasyonları	3574 (0)
-	-	Cihaz Konumları	6115 (60)
-	-	Cihaz Kullanıcıları	1 (0)
-	-	Cihaz Olayları	9 (4)
-	-	Çerezler	2364 (13)

Farklı adli kopya formatları içerisinde elde edilen verilerin karşılaştırması

MANTIKSAL AYIKLAMA		FİZİKSEL AYIKLAMA	
-	-	Downloads	177 (0)
-	-	E-postalar	413 (5)
-	-	Kablosuz Ağlar	1262 (0)
-	-	Kullanıcı Hesapları	42 (0)
-	-	Otomatik doldurma	66 (0)
-	-	Parolalar	815 (2)
-	-	Sohbetler	1518 (76)
-	-	Web Geçmişi	12328 (2)
-	-	Yüklü Uygulamalar	669 (0)
-	-	Uygulamalar	3999 (1165)
-	-	Yapılandırmalar	56 (1)

Web Data içerisinde elde edilen otomatik doldurma kayıtları (Devamı)

- **Elimizdeki Dosya Sistemli imajda hex araması yaptığımızda derinlemesine arama yapar.Fiziksel imajda bu böyleyken dosya sistemli imajda bu aramaya itibar etmeyin.Bu durumda yapmamız gereken manuel olarak veri tabanları içerisine girip arama yapmaktır.**

- **ROOT atılan cihazlara şüpheli yaklaşmalıyız çünkü bu cihazların veritabanları manipüle edilmiş olabilir.**

- **SMS/MMS manipüle edilmiş olsaydı araya mesaj merkezinin numarasını yazamazdı.Yazmadığı zaman ya da eksik yazdığı zaman.**

- **library.db android telefonlarda google playden indirmiş olduğumuz uygulamaları hangi gmail hesabıyla indirmişsek,uygulamanın tanıtıcı uzantısı neyse,hangi tarihte indirdiysek hepsinin kaydının tutulduğu database dosyasıdır.Uygulama harici yüklenmişse şüphelenebiliriz.**

- **package_verification.db telefonda yüklü uygulamalar belli aralıklarla veri doğrulaması yapar.Hangi tarihte güncelleme aldığıyla ilgili kayıtlara ulaşabiliriz.Yüklü uygulama arıyorsak mutlaka bu database içerisine kaydedilmiştir.**

- **suggestions.db google playda aranan uygulamaların kayıtlarını tutar.Kelimeyi bu database altında tutar.**

- **Web Data'nın altında autofill kısmında şifre çözmede kullanabileceğimiz otomatik doldurma kayıtları.**

- **CellebriteReader ikonunu elimizde lisans olmadan Cellebrite Reader'dan açabiliriz.Böyle bir imaj dosyası bize verildiğinde bu şekilde inceleyebiliriz.Tek bir şeye erişemeyiz o da hex araması yapabileceğimiz alana(Hafıza Erimleri kısmına) erişemeyiz.**

- **Her şeyini bildiğim telefon varsa fiziksel imaj alınır.**
- **Eğer telefon açıksa ve pin kodu biliniyorsa önce mantıksal ve dosya sistemli imajını alırım.Ondan sonra fiziksel yöntemlere geçerim.**