OXYGEN FORENSIC®
DETECTIVE

Bütünleşik Adli Bilişim Aracı

Tarihçemiz

«Bu dünyayı daha güvenli hale getirmek için iyi insanları destekliyoruz»

2019

Oxygen Forensic® JetEngine. Piyasadaki diğer mobil adli bilişim ürünlerinden üç kat daha hızlı veri işler.
Güvenli mesajlaşma adli incelemeleri, Android KeyStore, Signal, Telegram ve Wickr Me.

2018

Telefon numarası, bilgisayardan QR tokeni ve WhatsApp Sunucusuna erişim yoluyla WhatsApp yedekleme şifrelerinin çözülmesini içeren WhatsApp verilerini çıkarma ve şifre çözme için özel yöntemler.

2017

Sektöre özel çıkarım yöntemleri ve bulut çıkarımı ile adli bilişim liderliği.

2015

Bulut verilerini çıkarmada kullanmak amacı ile PC'lerden şifre ve token toplamayan KeyScout yardımcı programı tanıtıldı.

2014

İlk bulut adli inceleme ve çıkarımı. Oxygen Forensic® Cloud Extractor ek bir ücret ödemeden edinilebilir ve **75 bulut hizmetinden** veri alır.

2012

Uygulamalarda veri ayrıştırma tanıtımı ve desteklenen uygulamaların sayısı ve ayrıştırma kalitesi konusunda hala lider.

2010

Mobil adli bilişim alanında, Zaman Çizelgesi bölümünü tanıtarak veri analitiğini birleştiren ilk çözüm.

2004

Nokia telefonlarından veri çıkarmak için Oxygen Forensic® Suite yazılımı yayınlandı. Aynı yıl OxyAgent yardımcı programı Nokia akıllı telefonlardan veri çıkarmak için tasarlanmıştı. Bu yaklaşım en yaygın olarak mantıksal Android veri çıkarımı için kullanılır.

2000

Şirket kuruldu ve Nokia PC Suite'e iyi bir alternatif olan senkronizasyon yazılımı Oxygen Phone Manager üzerine uzmanlaştı.

**Ağustos 2019 itibarıyla*

Veri Çıkartma

MOBİL CİHAZLAR

Oxygen Forensic® Detective; iOS, Android, Windows, BlackBerry cihazları, özellikli telefonlar, medya ve SIM kartlardan veri çıkarımı sağlar. Zaman her zaman önemli olduğundan, birden fazla cihazdan Oxygen Forensic® Detective'e özel eşzamanlı veri çıkarımı yapılabilir. Oxygen Forensic® Detective'e iTunes, Android yedekleri, GrayKey, JTAG, Chip-off, UFED, XRY imajlarıda dahil olmak üzere çok sayıda yedek ve imaj dosyaları aktarılabilir.

Oxygen Forensic® Detective; Samsung, LG, Motorola ve MTK, Spreadtrum, Qualcomm yonga setleri dahil olmak üzere mobil cihazlarda ekran kilitlerini atlama veya devre dışı bırakma için çeşitli tescilli yöntemleri kullanır. Dahili Jet Imager endüstride benzersiz hızlarda fiziksel veri çıkarmayı sağlar. Oxygen Forensic® Detective, şifreli iTunes yedeklerinin ve Android imajların şifrelerini de bulabilir.

DRONLAR

Oxygen Forensic® Detective, drone verileri, uçuş kayıtları, mobil uygulamalar ve bulut hizmetlerinden ayrıntılı veri ayrıştırmayı ve analiz etmeyi sağlar. Oxygen Forensic® Detective, drone fiziksel imajlarını oluşturabilir veya içe aktarabilir ve değerli rota verilerini gösteren GPS konumlarını ve hız, yön, yükseklik, sıcaklık ve daha fazlasını içerecek şekilde cihaz telemetrisini ayrıştırabilir. Şu anda, çeşitli DJI ve Parrot dron modelleri desteklenmektedir.

Drone uygulamalarından veri ayrıştırma, iOS ve Android cihazlardan da mümkündür. İncelemeciler, drone resim ve videolarını, zaman damgaları olan konumları ve diğer verileri deşifre edebilir. Ek olarak, bulut hizmetlerinden drone verilerini çıkarma işlemi DJI, SkyPixel veya My Parrot bulut hizmetlerinden hesap giriş / şifre veya token ile gerçekleştirilebilir.

IOT CİHAZLAR

Oxygen Forensic® Detective şu anda iki popüler IoT cihazından (Amazon Alexa ve Google Home) veri çıkarma özelliği sunmaktadır. Verileri doğrudan cihazlardan elde etmek zor olduğu için incelemecilere bulut ve mobil uygulamalar gibi alternatif kaynaklara erişme olanağı sağlıyoruz. Araştırmacılar, çoğunlukla kullanıcının bilgisayarından veya mobil cihazlarından çıkarılabilen kullanıcı adı / şifre veya token ile bulut bilgilerine erişebilir. Oxygen Forensic® Cloud Extractor, doğrudan yazılım üzerinde çalınabilecek ses kayıtlarınıda içeren eksiksiz bir kanıt seti elde eder. Oxygen Forensic® Detective, IoT uygulama verilerini Apple iOS ve Android cihazlardan da çıkartır.

BULUT SERVİSLERİ

Dahili Oxygen Forensic® Cloud Extractor; iCloud, Google, Microsoft, Samsung, Huawei, Mi Cloud hesapları, E-posta sunucuları ve Facebook, Twitter, Instagram, Dropbox, WhatsApp, Telegram gibi diğer hizmetlere erişim sağlamanıza izin verir. Cloud Extractor ayrıca WhatsApp yedeklerinin şifresini çözme ve veri çıkarımını yapmak için özel bir yeteneğe sahiptir.
Desteklenen bulut depolama hizmetlerine erişim sağlamak için hesap kimlik bilgilerini veya tokenleri kullanabilirsiniz. Oxygen Forensic® Detective hesap kimlik bilgilerini ve tokenleri doğrudan mobil cihazlardan çıkarırken Oxygen Forensic KeyScout şifre ve tokenleri Windows tabanlı bilgisayarlardan toplar. Bu değerli veriler daha sonra incelenen ilgili bulut hizmeti hesaplarından veri toplamak ve çıkarım için kullanılabilir.

BİLGİSAYAR

Oxygen Forensic® KeyScout yardımcı programı, hem web tarayıcılarından hem de masaüstü uygulamalarından şifreleri, tokenleri ve kullanıcı verilerini çıkarmanın yanı sıra iTunes yedeklerini ve Windows işletim sistemli bilgisayarlarda Wi-Fi hotspot şifrelerini bulma üzerine odaklanmıştır.

Şu anda WhatsApp, Viber, WickrMe, Telegram, Skype, Microsoft Mail, Microsoft Outlook, Thunderbird, tüm popüler Web tarayıcıları, Windows için iCloud, vb. dahil olmak üzere desteklenen birçok masaüstü uygulaması vardır. Toplanan tokenler ve şifreler bulut verileri için hemen kullanılabilir. Çıkarılan web tarayıcısı, mesajlaşma ve e-posta verileri daha ileri analiz ve mobil cihaz kalıntıları ile tek bir dava dosyasında inceleme için Oxygen Forensic® Detective yazılımına aktarılabilir.

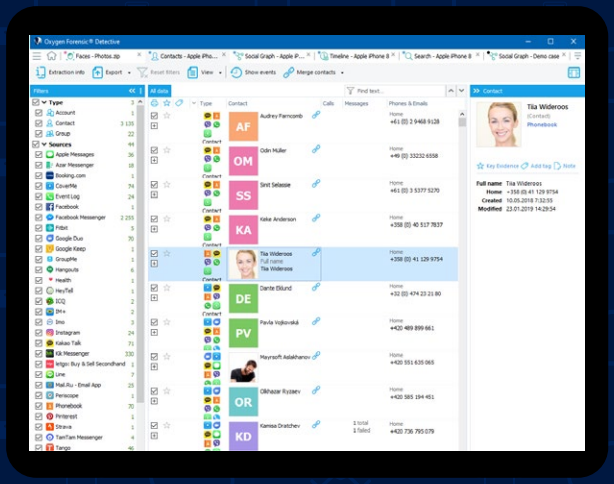
GİYİLEBİLİR CİHAZLAR

Oxygen Forensic® Detective, adli incelemecilerin cihaz modeli, kişiler, aramalar, mesajlar, multimedya dosyaları ve diğer verileri çıkarmasına olanak tanıyan MTK yonga setine dayalı akıllı saatlerin mantıksal imajını alır. Ayrıca, yazılım Apple Health (Apple Watch ile senkronize edilen veriler dahil), Samsung Health, Google Fit, FitBit, Endomondo ve birçok farklı uygulamalardan komple veri alır. Bu değerli veriler hem mobil cihazlardan hem de bulut hizmetlerinden çıkarılabilir ve genellikle zaman damgaları ile çok sayıda coğrafi konum, sağlık verileri, adımlar ve merdiven sayısı gibi ek kullanıcı istatistiklerini içerir.

Veri Analizi

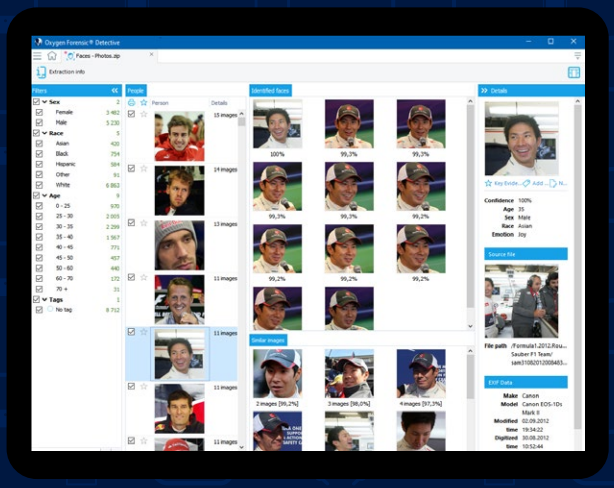
VERİLERİN İŞLENMESİ

Oxygen Forensic® Detective'in güçlü 64 bit adli mimarisi, araştırmacıların önemli miktarda veriyi hızlı bir şekilde ayrıştırmasına ve kritik verileri hızlı bir şekilde tanımlamak için Sosyal Grafik, Zaman Çizelgesi, Yüz Tanıma gibi gelişmiş analitik araçlardan yararlanmasına olanak tanır. Oxygen Forensic® Detective, mobil cihazlardan, yedeklerden, drone'lardan ve bulut hizmetlerinden gelen büyük veri setlerini desteklemek için önde gelen rakiplerden üç kat daha hızlı veri ayrıştırma ve kod çözme sağlar. Bu güçlü araç aynı zamanda çok sekmeli bir kullanıcı arayüzü sunar, böylece aynı anda birkaç pencere üzerinden çalışmak zahmetsiz veri karşılaştırmasına olanak tanır.



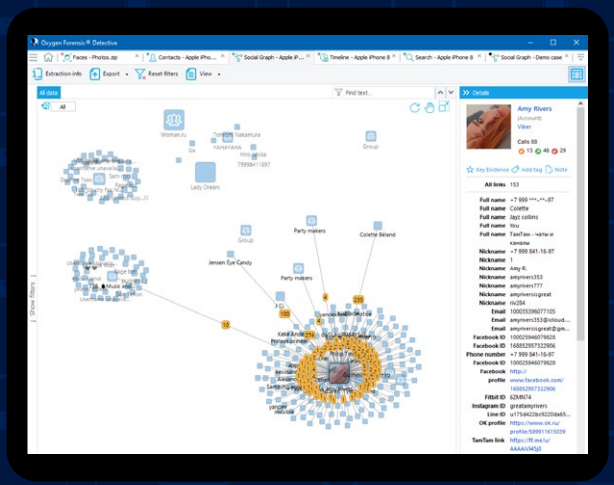
YÜZ TANIMA

Oxygen Forensic® Detective, incelemecilere insan yüzlerini sınıflandırma olanağı sunar. Yüz tanıma özelliği Yüzler bölümünde ek bir ücret ödenmeden kullanılabilir. Benzersiz özellikleri: endüstri lideri doğruluk (NIST tarafından ölçülmüş şeklinde), detaylı yüz analizi (cinsiyet, ırk, duygu ve daha fazlası), anında sınıflandırma ve eşleştirme (5 yüz / saniye) ve büyük boyutta veri desteği. Yerleşik yüz tanıma ile incelemeciler mobil, bulut veya drone imajlarındaki binlerce fotoğraf veya videoya bakmak için daha az zaman harcayacaktır.

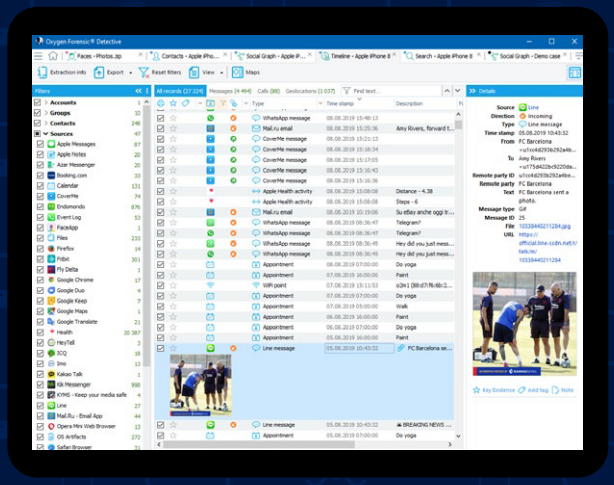


SOSYAL BAĞLANTILAR

Yerleşik Social Graph, bir cihaz sahibi ile kişiler arasındaki veya çeşitli cihazlar arasındaki sosyal bağlantıları keşfetmek için uygun bir platform sağlar. Social Graph ile incelemeciler tek bir tıklamayla cihaz sahiplerine en yakın kişileri belirleyebilir. Seçilen kişi ve cihaz kaynakları arasındaki tüm iletişim hakkında ayrıntılı bilgi içeren bir görünüm açmak için herhangi bir kişiyi tıklamak yeterlidir. Social Graph arayüzü dinamik ve çeviktir, ve incelemeciler cihaz ve dava bağlantılarının çok net bir görünümünü oluştururken kişileri taşımak, gizlemek veya birleştirmek için sürükleyip bırakabilirler.

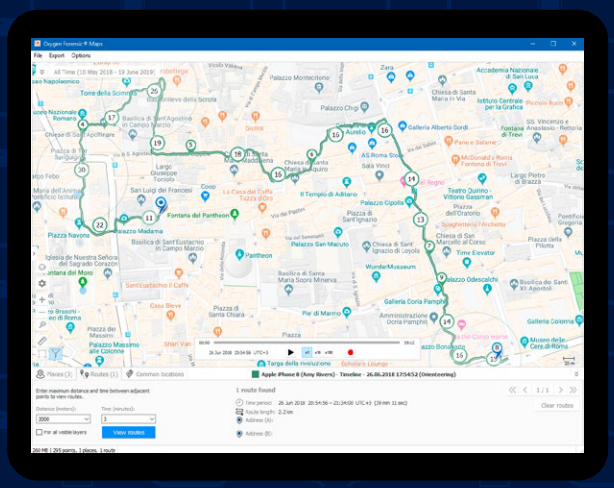


Veri Analizi



ZAMAN ÇİZELGESİ

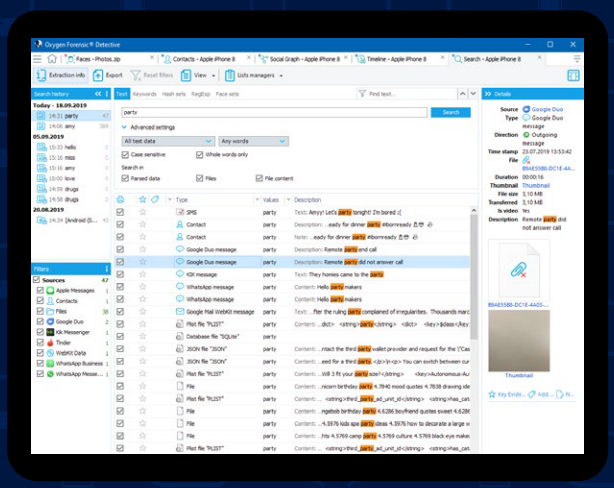
Zaman Çizelgesi bölümü tüm cihaz olaylarının tek bir listede görüntülenmesini sağlar – uygulamalar içerisindeki sohbetler, aramalar, web etkinliği, web bağlantıları, fotoğraflar ve videolar, takvim etkinlikleri ve daha fazlası. Olaylar bir cihaz veya bir grup cihaz için görüntülenebilir ve ortak grup etkinliklerinin kolayca tanımlanmasını sağlar. Yalnızca en alakalı verilere odaklanmak için tarihe, saate, etkinlik sıklığına, ilgili kişiye, ddiğr kişiye veya diğer veri noktalarına göre sıralayın ve filtreleyin. GEO Zaman Çizelgesi sekmesi fotoğraflar, videolar, uygulamalar, drone uçuş logları vb. içeren tüm kaynaklardan coğrafi koordinatların tam listesini gösterir.



HARİTALAR

Oxygen Forensic® Detective mobil cihazlar, dronlar, bulut depoları, medya kartlar ve içe aktarılan imajlar dahil olmak üzere tüm olası kaynaklardan coğrafi koordinatları alır. Analiz edildikten sonra veriler çevrimiçi veya çevrimdışı olarak Oxygen Forensic® Maps ile görüntülenebilir. Maps modülü ile aşağıda belirtilen işlemler yapılabilir:

- Bir cihazın sık ziyaret edilen yerlerini belirleme
- Belirli bir zaman dilimi içinde bir cihazın hareketlerinin görüntülenmesi
- Birkaç cihazın ortak konumlarını belirleme
- Seyahat yönünü gösteren animasyonlu bir rota oynatma



VERİ ARAMA

Oxygen Forensic® Detective incelemecilerin tek bir cihazda, bir davadaki tüm cihazlarda veya bir veritabanındaki tüm cihazlarda metin, telefon numaraları, e-posta adresleri, coğrafi koordinatlar, IP adresleri, MAC adresleri, kredi kartı numaraları ve Project VIC dahil dosya hashleri için tüm cihazlarda arama yapmasına olanak sağlar. Özel arama işlevleri için bir Regular Expression kütüphanesi mevcuttur. Anahtar Kelime Listesi Yöneticisi ve İzleme Listeleri, araştırmacıların bir çıkarma sırasında veya sonrasında bir dizi anahtar kelime oluşturmasına ve arama yapmasına olanak tanır.

Dışarı Veri Aktarma

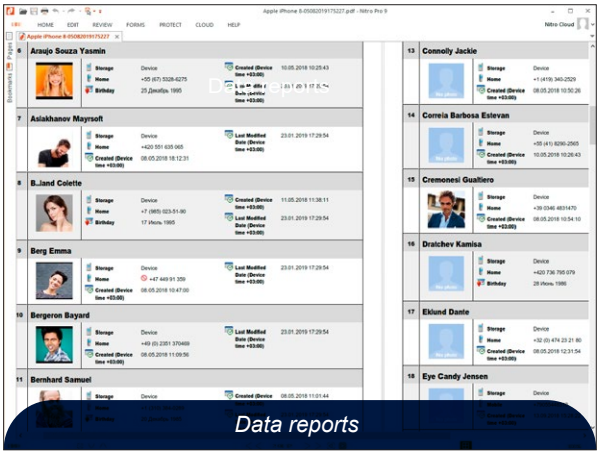
OFB YEDEKLERİ

Çıkarılan tüm veriler, Oxygen Forensic® Detective ana araç çubuğundaki "Save to archive" düğmesine tıklayarak bir Oxygen Forensic Backup (OFBX) dosyası olarak kaydedilebilir. Bu OFB yedeklemesi daha sonra herhangi bir zamanda Oxygen Forensic® Detective'e aktarılabilir veya Oxygen Forensic® Viewer'da açılacak şekilde iş arkadaşlarına gönderilebilir. Viewer, Oxygen Forensic® Detective'ten toplanan kanıtları görüntülemek ve paylaşmak için ücretsiz ve portatif yardımcı programdır. Müşteri portalından indirilebilir, kurulum veya aktivasyon gerektirmez.

VERİ RAPORLARI

Oxygen Forensic® Detective, herhangi bir kısımdan PDF, RTF, XLS, XML, HTML, vb. dahil olmak üzere birçok popüler dosya formatına veri aktarımına olanak tanır. Tek bir cihaz, birkaç cihaz, birkaç bölüm ve hatta sadece seçilen kayıtları içerecek bir rapor oluşturulabilir. Raporlar her tür dava için yalnızca gerekli verileri görüntüleyecek şekilde özelleştirilebilir.

XML raporlarımız diğer analitik yazılım platformlarına entegre edilebilir. Oxygen Forensic® Detective ayrıca verileri Relativity yazılımının formatında dışa aktarabilir.

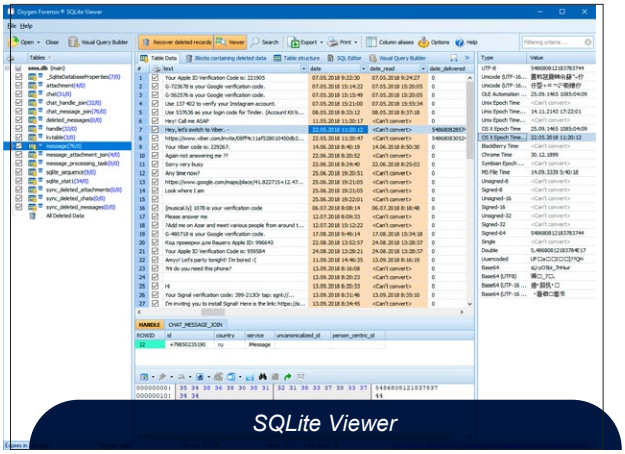


Data reports

Veri Görüntüleyiciler

PLIST GÖRÜNTÜLEYİCİ

Yerleşik Oxygen Forensic® Plist Viewer, Plist dosyalarının gelişmiş analizini sunar: araştırmacılar düz XML ve ikili XML dosyalarını açabilir, girişleri türlerine göre görüntüleyebilir (dize, veri, sayılar vb.), değerleri dönüştürebilir, analiz için harici dosyaları açabilir , harici araçlar tarafından daha ayrıntılı analiz için .plist dosya verilerini XML biçiminde dışa aktaabilir.


SQLite Viewer

SQLITE GÖRÜNTÜLEYİCİ

Yerleşik Oxygen Forensic® SQLite Viewer, SQLite dosyalarını incelemek için güçlü bir 64 bit araçtır. Bu araç ile incelemeciler herhangi bir SQLite veritabanını açabilir, silinen kayıtları kurtarabilir, değerleri okunabilir bir biçime dönüştürebilir, görsel ve görsel olmayan SQL sorguları oluşturabilir ve bunları daha sonra kullanmak üzere kaydedebilir, aramayı çalıştırabilir ve seçilen girdileri özelleştirme veri raporlarına aktarabilir.

Sizin Notlarınız

Eğitim Olanakları

Kullanıcılarımıza 3 gün süreli eğitmen destekli eğitimlerden başlayarak istediğiniz zaman alabileceğiniz uzak eğitimlere kadar çok çeşitli eğitimler sunuyoruz. Ayrıca, ücretsiz 30 dakikalık web seminerleri düzenli olarak canlı veya müşteri portalında kaydedilmiş şekilde izlenebilir. Daha detaylı bilgi için web sitemizi ziyaret edin: www.oxygen-forensic.com

2000 yılında kurulan Oxygen Forensics, mobil bağlantılı dünyamızın başlangıcından bu yana mobil adli inceleme pazarında çözümler sunmaktadır. Günümüzde Oxygen Forensics kolluk kuvvetlerine, federal kurumlara ve işletmelere kritik verilere her zamankinden daha hızlı erişmelerini sağlayan lider global adli bilişim inceleme yazılım sağlayıcısıdır. Mobil cihaz, bulut, dronlar ve IoT verilerinde uzman olan Oxygen Forensics, cezai ve kurumsal soruşturmalar için en gelişmiş dijital adli veri çıkarma ve analitik araçları sağlar.

901 N. Pitt St, Suite 100,Alexandria, VA 22314

support@oxygen-forensic.com

877-969-9436

DUNS 078884550 / CAGE 741G3

www.oxygen-forensic.com