

MAGNET AXIOM™

ŞİMDİ MAGNET AXIOM ZAMANI

Akıllı telefon, bilgisayar ve bulut gibi birçok kaynaktan kanıt kurtarın. AXIOM'un güçlü ve sezgisel özellikleri tüm vaka üzerinde baştan sonra daha hızlı bir şekilde çalışmanıza yardımcı olur. Magnet AXIOM eksiksiz bir dijital soruşturma platformudur.

MAGNET AXIOM'UN GÜCÜ

Magnet AXIOM; akıllı telefon, bilgisayar veya bulut gibi tüm veri kaynaklarından en ilgili kanıtları toplamak için özenle hazırlanmıştır.

Dijital adli soruşturma uzmanları tarafından diğer araçların bulamayacağı kanıtları aramak için kullanılan AXIOM, verileri akıllıca görselleştirebilir ve analiz edebilir, verileri doğrulayabilir ve diğer araçlarla elde edilen görüntüleri incelemek üzere tek bir vaka dosyasında birleştirebilir.

Magnet AXIOM'u eksiksiz bir dijital soruşturma platformu haline getiren etkenlerden bazıları şunlardır:



PERFORMANS

Zaman önemli olduğunda AXIOM'u kullanın. AXIOM IEF'ye kıyasla verileri ortalama %40 daha hızlı işler ve vaka verilerini 40 kata kadar daha hızlı inceler. AXIOM'da arama yapmak, IEF'de olduğundan daha hızlıdır ve bu durum soruşturmanın daha kısa sürede tamamlanmasını sağlar.



GELİŞMİŞ MAC DESTEĞİ

IEF HFS+ desteği sunarken AXIOM, hem HFS+ hem de APFS desteği sunar ve ayrıca FileVault 2 şifreli sürücülerin, bölümlerin ve birimlerin şifresini çözer. AXIOM ile FSEvents ve Bash Geçmişi gibi daha fazla macOS yapısı keşfedin.



BAĞLANTILAR

Bağlantılar özelliğiyle dosyalar, yapılar, kişiler ve cihazlar arasındaki ilişkiyi otomatik olarak görselleştirin.



ZAMAN ÇİZELGESİ

AXIOM, tüm yapılarda ve dosya sistemi verilerinde bir zaman çizelgesi oluşturma, Zaman Çizelgesi olaylarını kategorize etme ve filtreleme, her bir tarih/saat damgası için benzersiz satır ögesi gösterme özellikleriyle Zaman Çizelgesi'ni bir üst düzeye taşıyor.



MAGNET.AI

Magnet.AI resimleri arar ve potansiyel çıplaklık, silah, CSAM ve radikal görüntüler gibi birçok içeriği işaretler. Sohbetleri inceleyin ve ayartıcı unsurlar içerebilecek görüşmeleri belirleyin.



GRAYKEY

İnceleyiciler AXIOM'daki yerleşik Plist, SQLite ve dosya sistemi görüntüleyicileri sayesinde IEF'de görüntülenemeyen GrayKey görüntülerindeki ham iOS verilerini inceleyebilir ve analiz edebilir.



MOBİL ALIM

AXIOM, iOS ve Android cihazlar için yerleşik alım özelliklerine sahiptir. AXIOM, binlerce Android cihazındaki parolaları atlayan ve tam fiziksel görüntüleri ayıklayan en gelişmiş özelliklere sahip tek Magnet Forensics aracıdır.



BULUTTA ADLİ İŞLEMLER

AXIOM, bulut verileri için en kapsamlı desteğe sahiptir. Adli olarak işinize yarayabilecek 50'den fazla sosyal ağ, bulut ve e-posta hizmetinden veri alın. Facebook belge iadelerini analiz edin, kullanıcı tarafından Google ve Facebook gibi bulut hizmetlerinden istenen arşivleri inceleyin ve Twitter'dan herkese açık bilgileri alın.



BELLEK ANALİZİ

İnceleyiciler, yapıları seçerek ve doğrudan AXIOM ile entegre olan Volatility'yi çalıştırarak belleği analiz edebilirler.



DOSYA SİSTEMİ VE KAYIT DEFTERİ GÖRÜNÜMLERİ

AXIOM'un dosya sistemi gezgini, belirli bir görüntünün dosya yapısına göz atmanızı sağlar. Ayrıca, kaynak bağlantısıyla yapı bulgularını hızlı bir şekilde doğrulayabilir ve kanıtın depolandığı dosya sistemi veya kayıt defterinin tam konumunu görüntüleyebilirsiniz.



PASSWARE

AXIOM, Passware ile tamamen entegredir (ek ücret ödemezsiniz) ve inceleyicilerin BitLocker, TrueCrypt, PGP ve McAfee şifrelemesi bulunan bilgisayarların şifresini çözmesini sağlar.

MAGNET AXIOM – İNCELEME

Özellik	Magnet IEF (+modüller)	Magnet AXIOM
Zaman Çizelgesi görselleştirme	X	X
Tüm yapılarda ve dosya sistemi verilerinde zaman çizelgesi oluşturma		X
Kullanıcı iletişimleri ve web' de gezinme gibi zaman çizelgesi olaylarının kategorizasyonu ve filtrelemesi		X
Her tarih/saat damgası için benzersiz satır ögesi görüntüleme		X
Bilinen materyal için listeleme sıraları aracılığıyla memur tarafından yönetilen medya kategorizasyonu (derecelendirme)	X	X
Ek VIC'lerin istihbarat verilerini görüntüleme ve filtreleme (tanımlanmış, dağıtılmış, etiketler vb.)		X
Gelecek vaka çalışması için listeleme sırası veritabanında memur derecelendirmelerine katkıda bulunma		X
Vaka Panosu		X
Volatility entegrasyonu ile bellek analizi		X
Magnet.AI sohbet ve resim kategorizasyonu		X
Birden fazla veri görünümü	X	X
• Birden fazla yapı türünün sütun veya sekmeli görünümü		X
• Birden fazla yapı türünün özet satır görünümü		X
• Dünya haritası, histogram ve sohbet yazışması görünümleri	X	X
Bağlantılar ile kilit kanıtlar arasında ilişkileri görselleştirme		X
Özizleme görünümü ve Ayrıntılar görünümü (belgeler, resimler vb.)	X	X
Hex ve metin verilerini anında deşifre edin	X	X
İnceleyici tanımlı yapılar oluşturma		X
Web sayfalarını tekrar oluşturma	X	X
Dosya sistemini görüntüleme ve dosyalar ile klasörleri yinelemeli olarak görüntüleme		X
Ayrılmamış alanı görüntüleme ve silinmiş dosyaları ve klasörleri görüntüleme		X
SQLite veritabanları görüntüleyici		X
Kayıt defteri görüntüleyici		X
Yapı filtreleme	X	X
Entegre dosya sistemi filtrelemesi		X
Anahtar kelimeyle yapı arama		X
• Yapıları dizine ekleme (gelişmiş filtreleme ve anahtar kelimeyle arama performansı)	X	X
• Dosya adlarında/yollarında anahtar kelimeyle arama yapma (dosya sistemi görünümü)		X
• Regex aramaları	X	X
Göreceli zaman filtreleme ve, filtre ve anahtar kelime yığınlama		X
Etiketleme, yer işaretleme ve yorum yapma	X	X
Kaynak veriye kaynak bağlantısı		X
İlgili yapılar ve Doğru Görünümlü dışarı aktarım (dosya tabanlı dışarı aktarımlar)		X
HTML, PDF, RTF, XLS, CSV gibi birçok formatta dışarı aktarım	X	X
Sohbet yazışmalarını kaydetme	X	X
Tekli veya çoklu dosyaları bir kapsayıcıya kaydetme		X
Mobil Vakalar Oluşturma	X	X

MAGNET AXIOM – ZPRACOVÁNÍ

Özellik	Magnet IEF (+modüller)	Magnet AXIOM
Facebook belge iadeleri		X
Kullanıcı tarafından Google ve Facebook gibi bulut hizmetlerinden istenen arşivleri inceleme		X
Twitter'dan herkese açık bilgileri alma		X
Mac desteği	X	X
• HFS+ dosya sistemi desteği	X	X
• APFS dosya sistemi desteği		X
• macOS Birleşik Günlüğü Ayırıştırma		X
• FileVault 2 şifreli sürücülerin, bölümlerin ve birimlerin şifresini çözme		X
• macOS medya ve web ile ilgili yapıları kurtarma	X	X
• macOS yerel (FSEvents, Bash Geçmiş gibi) ve özel yapılarını kurtarma		X
Bilinen materyal için listeleme sıraları aracılığıyla yerel medya kategorizasyonu (derecelendirme)	X	X
Mobil alımı - Android, iOS		X
Mobil incelemesi - Windows, JTAG, yedeklemeler, yonga, GrayKey gibi üçüncü taraf görüntüleri	X	X
Android'de parola atlama		X
Bilgisayar alımı - Windows, Linux, USB		X
Bilgisayar incelemesi - EnCase, FTK, MacQuisition gibi üçüncü taraf görüntüleri	X	X
Passware ile disk şifresi çözme		X
Adli açıdan en ilgili 50'yi aşkın bulut hizmetinden bulut verilerinin alımı		X
Cihazların çoklu sıraya alınması ve tek aşamalı kanıt işleme		X
İnternet yapıları	X	X
O/S işletme yapıları		X
Office 365 ve Box gibi birçok hizmetten bulut denetim günlüklerini kurtarma		X
Meta verileri koruma	X	X
Office 365, G Suite, Slack gibi birçok hizmet için yönetici kimlik bilgilerini kullanma		X
Oturum açma belirteçlerini ve anahtar zincirlerini ayıklama	X	X
Parola olmadan bulut hesaplarına erişmek için belirteç ve anahtar zincirlerini inceleme		X
Mobil yapılar ve bilgisayar bellek yapıları		X
Dizine eklenmiş veriler	X	X
Anahtar Kelimeyle Gelişmiş Hızlı Arama		X
Dosya listeleme ve anahtar kelime araması (dosya içeriği ve ayrılmamış)		X
Özel yapılar (yapıların komut dizisini oluşturma)		X
Çok dilli arayüz		X
Ağ lisansı		X

emt.com.tr/tr

+90 (312) 472 20 60

emt@emt.com.tr

[@EMTElectronicsLtd](https://www.facebook.com/EMTElectronicsLtd)

[@EMTAkademi](https://www.instagram.com/EMTAkademi)

[/emt-electronics-engineering-ltd-/](https://www.linkedin.com/company/emt-electronics-engineering-ltd/)

© 2019 Magnet Forensics Inc. Tüm hakları saklıdır. Magnet Forensics® ve ilgili ticari markalar Magnet Forensics Inc. şirketinin mülkiyetindedir ve farklı ülkelerde kullanılmaktadır.

EMT
ELECTRONICS



MAGNET
FORENSICS®

magnetforensics.com