

MD-RED

MD-RED, bir mobil veya dijital aygıttan MD-NEXT veya diğer çıkarım araçlarıyla toplanan delil verisinin kurtarılması, şifrelerinin çözülmesi, görsel olarak sunulması ve raporlanması işlemlerini yapan bir adli bilişim veri analizi yazılımıdır. Vakaların ve olayların soruşturulması için analize ait bütün sonuçlar adli bilişim raporu olarak çıkarılabilir. İlave olarak, en yeni mobil uygulamaların analiz modülü araştırma ve geliştirmeyle sürekli güncellenir.

Mobil işletim sistemlerini ve mevcut telefon markalarını destekler

- iOS, Android, Windows, Tizen ve Blackberry işletim sistemini, Samsung, LG, Pantech, Apple, Microsoft, Nokia, Motorola Global, Çin, Japon ve Hindistan üretimi cep telefonlarını destekler.

Ekran kilidi bilgisini-şifresini çözme

- Telefon kilidini açmak için desen, PIN veya parolaları çözer.
- GPU hızlandırma ile kaba kuvvet saldırısı (Brute forcing)
- iPhone keychain veri analizi

Kriptolanmış-şifrelenmiş uygulama verilerini çözme

- Kriptolanmış-şifrelenmiş chat mesajlarını, e-postaları, dosyaları ve uygulama verilerini çözer.

Mobil veri ve iOS/Android uygulamalarının analizi

- Telefon kamerası tarafından çekilen multimedya dosyaları
- Arama kayıtları, adres defteri, SMS/MMS, e-posta, not, internet tarama geçmişi
- Yüzlerce popüler uygulama- Facebook, Twitter, Whatspp, Wechat
- SMS, harita, navigasyon, sağlık, bankacılık bilgileri ve ilave birçok uygulama
- Anti-forensic uygulamalar



Popüler mesajlaşma uygulamaları için derinlemesine analiz

- **Serialization (serileştirme)**, bir nesnenin saklanacak/transfer edilecek forma dönüştürülme işlemidir. Bu şekilde veriler küçülür ve aynı zamanda daha performanslı hale gelir. Serileşmenin tersi olarak **Deserialization (ters serileştirme)** ise serileştirme uygulanmış olan nesne, verinin tekrar okunabilir hale getirilmesidir.
- Ters serileştirme, şifre çözme (decryption) ve veri kurtarma
- WhatsApp-Çeşitli yedekleme (backup) dosyalarının analizi
- WeChat-Çeşitli hesap analizleri ve Rainbow tablosu
- Skype, Facebook messenger, Telegram, Wickr
- QQ, Kakaotalk, Line, Zalo, Viber, Snapchat gibi 1450'den fazla uygulama desteği

Multimedia veri kurtarma ve analizi

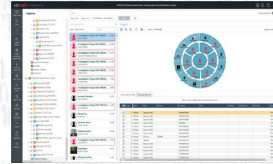
- Silinmiş veya zarar görmüş video dosyalarında frame kurtarma
- Ses dosyası dönüştürücüsü (AMR/AUD/QCP/SILK'den MP3/AMR/WAV'ye)
- QCP dosya oynatmayı, Silk codec decode'u destekler.

Sosyal ilişki analizi

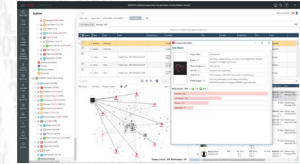
- Tek bir telefon incelemesi için basit mod
- Birden çok telefon incelemesi için ileri düzey mod
- Aramalar, mesajlaşmalar ve e-posta iletişimi veri analizi
- Rehberdeki ortak ve farklı kişilerin tespiti
- Uygulama, zaman, rehber ve iletişim tipine göre filtreleme

Yeni dijital aygıtların analizi

- Drone veri analizi - uçuş geçmişi, multimedya verisi, DJI/Parrot/PixHawk
- IoT veri analizi - Akıllı hoparlör, Smart TV, araç navigasyonu



Basit Mod



İleri Düzey Mod

- Log-Kayıt analizi
- Gömülü veri görüntüleme seçenekleri
- İleri düzey veri filtreleme seçenekleri
- Çeşitli dosya sistemlerinin kurtarılması ve ayrıştırılması
- Analiz edilen verinin görselleştirilmesi
- Yenilikçi performans artırım yöntemleri
- Kullanıcının belirleyeceği analiz scripti için Python Editörü
- Görselleştirilmiş analiz verisi
- Raporlama özellikleri



Sistem Gereksinimleri

- OS : Windows 7/8/10 64bit
- CPU : i7 ve üstü
- RAM : 8GB ve üstü
- HDD : 1 TB ve üstü
- Ekran : 1024x768 üstü
- USB : USB 2.0 x 2 ve üstü USB 2.0/3.0/3.1 portları
- Microsoft.Net Framework 4.5

Paket İçeriği

- MD-RED CD Kutusu
- USB Dongle Key
- 1 yıllık donanım garantisi

