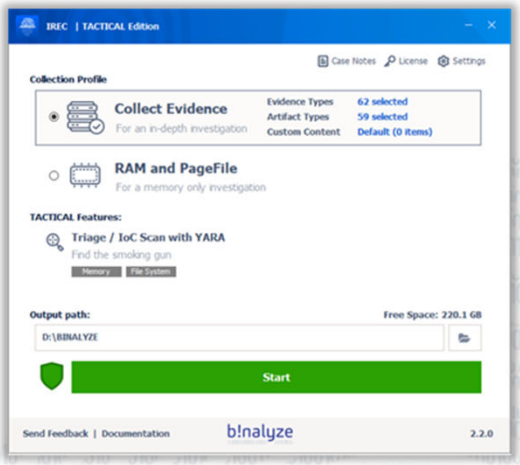
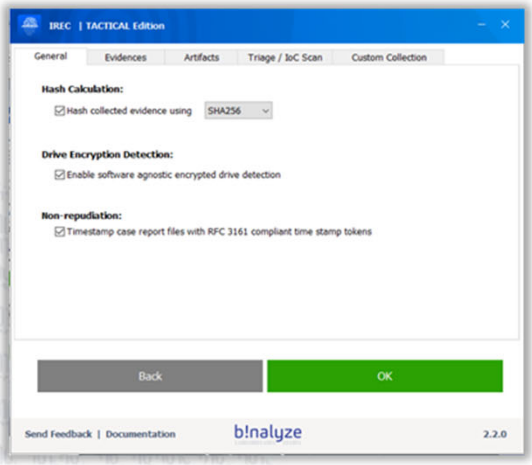
DIFOSE

b!nalyze
1100100011001 101001





IREC TACTICAL All-in-one Evidence Collector

HIZLI & KOLAY

IREC, tüm kritik verileri tek bir fare tıklamasıyla otomatik olarak toplayarak, olay müdahale yeteneklerini artırır ve size şimdiye kadarki en hızlı olay müdahalesini sunar.

KOLAY & KULLANICI DOSTU

Olay Müdahalesi daha önce hiç bu kadar kolay olmamıştı. Kurulum yapmadan tek yapmanız gereken IREC'i çalıştırmak, fareye tıklamak ve sizin için oluşturulan HTML raporunu okumaktır.

HEPSİ BİR ARADA & YETENEKLİ

IREC, kanıtları toplayarak ve koruyarak, siber güvenlik, adli bilişim ve denetim alanlarında amaç ve ihtiyaçları aynı anda karşılar.

TONLARCA BULGU

IREC, siber olayların çözümüne yönelik aşağıdaki tüm kritik verileri tek bir fare tıklamasıyla otomatik olarak toplar:

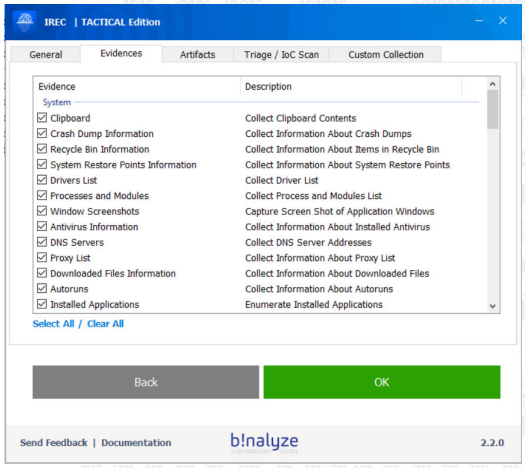
- Sistem bilgisi
- RAM imajı
- PageFile
- CSV formatında MFT
- Olay Günlükleri
- Registry Hive
- Geri Dönüşüm Kutusu Bilgileri
- Prefetch Dosyaları
- WMI Komut Dosyaları
- Route & ARP & TCP & UDP Tabloları
- Ağ Adaptörleri ve Ağ Paylaşımları
- Hibernation Dosya Bilgileri
- Birim bilgisi
- Sistem Geri Yükleme Noktaları
- Bilinen yazılım ve uygulama bulguları

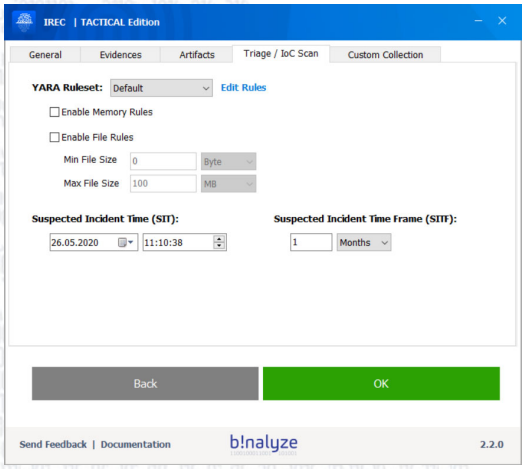
60 adet kanıt ve artifact türü ve daha fazlası...

www.difose.com.tr info@difose.com.tr /difose

Olay Müdahalesi (IR-Incident Response), IR ekipleri için zor ve külfetli bir görevdir, ancak IREC ile tek bir fare tıklaması kadar kolaydır. Hepsi bir arada kanıt toplayıcı IREC, yalnızca göz açıp kapayıncaya kadar canlı bir sistemden kritik kanıtları toplamayı otomatikleştirir. Artık samanlıkta iğne aramak için değerli zamanınızı kaybetmenize gerek yok.

IREC, olay müdahale süresini dakikalara indirir ve size gerekli tüm ipuçlarını sunarak etkinliklerini artırır. Ayrıca delilleri toplayarak ve saklayarak siber güvenlik ve adli bilişim ihtiyaçlarını aynı anda karşılar. Sizin için tüm kritik verileri toplayan ve sunan otomatik bir IR yazılımı hayal edin. Şimdiye kadarki en hızlı IR için ihtiyacınız olan tek şey IREC.





IREC TACTICAL Özellikleri

- Hepsi bir arada çözüm
- Taşınabilir
- Kullanıcı dostu
- YARA Scriptlerini destekler
- Tüm Windows sürümleriyle uyumlu
- Şimdiye kadarki en hızlı kanıt toplama
- Küçük disk alanı (yalnızca 17 MB)
- En Hızlı Triyaj
- Windows ve Linux Desteği
- Dongle (çevrimdışı etkinleştirme)
- Kolay arama özelliği
- Virüs bulaşmış bilgisayarlar için kötü amaçlı yazılım koruması
- HASH hesaplaması
- Zaman damgası işlevi
- Anında sürücü şifreleme tespiti
- Özel içerik kopyalama
- Dosya Sistemi ve RAM'de Hızlı Triyaj
- Özel toplama profilleri
- Mahkemede kabul edilebilirlik (Adli açıdan geçerli)
- Kolay HTML ve JSON rapor paylaşımı

KESİNLİKLE ŞİMDİYE KADARKİ EN KOMPLE KANIT TOPLAYICI!

Ankara: Ümit Mah. 4281 Sok. Kafkas Sitesi No:6 06810 Ümitköy/ÇANKAYA
İstanbul: Esentepe Mah. Kelebek Sk. No:2 Marmara Kule Kat:10 D:79 34870 KARTAL
+90 (312) 219 56 16
+90 (216) 771 07 97