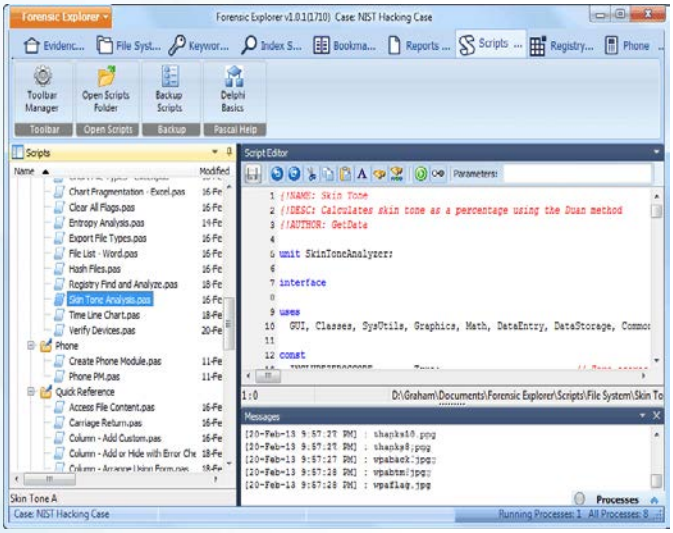
GetData FORENSICS

FORENSIC EXPLORER

Türkiye'de adli bilişim alanında kullanılan temel inceleme ve analiz yazılımlarının ara yüzlerinin İngilizce olması etkili kullanım, eğitim, yaygınlaştırma ve adli mercilerce anlaşılması konularında bir takım zorluklar ve problemler yaşanmasına neden olmaktadır. Bu nedenle, Türkçe ara yüzlü bir adli bilişim yazılımı önemli bir ihtiyaç halini almıştır.

DIFOSE, Türkiye'deki adli bilişim sektörüne hem bir yenilik kazandırmak hem de bu alandaki Türkçe yazılım ihtiyacını karşılamak amacıyla Haziran 2013'te Avustralya'nın veri kurtarma alanında dünyaca tanınmış firması GetData ile işbirliği yaparak ve ilk Türkçe adli bilişim yazılımını Aralık 2013 tarihinde yayınlamıştır.

DIFOSE, zaman içerisinde yazılım içeriğinde ve özelliklerinde yapmış olduğu tekliflerle yazılımın üretim ve güncelleşmesinde söz sahibi olmuştur. Forensic Explorer yazılımın bazı bölümleri ve modülleri DIFOSE tarafından geliştirilerek tüm dünya tarafından kullanılan ortak sürüme kazandırılmıştır. Forensic Explorer adli bilişim yazılımın Türkiye'deki satış, dağıtım, güncelleme ve eğitim hakları DIFOSE'a aittir.



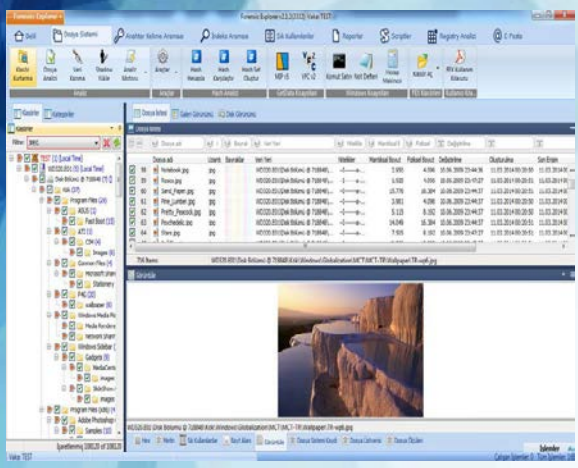
Tel : +90 312 219 56 16
Fax : +90 312 219 46 05
E-Posta : info@difose.com.tr
Adres : Ümit Mah. 2481.Sok. Kafkas Sitesi No:6 Ümitköy/ANKARA

ADLİ BİLİŞİM HİZMETLERİ
DIFOSE
DIGITAL FORENSIC SERVICES

www.difose.com.tr

GetData FORENSICS

FORENSIC EXPLORER



Desteklenen Adli Kopya Formatları :

- DD ya da RAW (*.DD, *.BIN, *.RAW, *.CTR)
- EnCase® (*.E01, *.Ex01, *.L01, *.LX01, *.S01)
- FTK® (*.AD1 formatları)
- Forensic File Format (.AFF)
- ISO (CD ve DVD kopyaları)• SMART®
- VMWare®(*.VMD, *.VMDK)
- ProDiscover® (*.EVE)
- Microsoft (*.VHD)
- Apple (*.DMG)
- XWays (*.CTR)

Yazılım Özellikleri

- **Vakaya tekil ve çoklu adli kopya ya da dosya ekleme:** Oluşturulan bir vakaya, bir ve birden fazla adli kopya eklenerek inceleme ve analiz bir bütün olarak yapılabilmektedir. Ayrıca, Cellebrite, XRY, Oxygen Forensics ya da mobil cihaz hex dump dosyaları dosya olarak eklenip üzerinde veri kurtarma, inceleme ve analiz yapılabilmektedir.
- **Ağdan disk ekleme:** Bir bilgisayar ağında yer alan disk alanına TCP/IP protokolü üzerinden erişim sağlanarak ağ üzerinden inceleme ve analiz yapılabilmektedir.
- **RAID sistemi ya da RAID diski ekleme:** RAID sisteme ait fiziksel ya da mantıksal olarak alınmış adli kopyaları birleştirerek yeniden RAID sistemi inşa edilerek inceleme ve analiz yapılabilmektedir.
- **İleri seviye klasör kurtarma:** FAT, exFAT, NTFS, HFS dosya formatlarına ait silinmiş klasörlerin kurtarılarak incelenmesi yapılabilmektedir.
- **İleri seviye dosya kurtarma (kazıma):** Otomatik veri kazıma sayesinde yüzlerce tür silinmiş dosyalar özel işlemler kullanılarak kurtarılmakta ve kısa sürede kurtarılan veriler üzerinde inceleme ve analiz yapılabilmektedir.
- **Dosya imza analizi:** Dosya imza analizi ile uzantısı değiştirilmiş, şifrelenmiş, parola korumalı ya da bazı özellikleri gizlenmiş dosyalar çok kısa sürede tespit edilebilmektedir.
- **Dosya Hash (Sayısal) değeri hesaplama ve karşılaştırma:** Adli bilişimde veri analizinde bir dosyayı aramak ya da aynı dosyayı bulmak için kullanılan en hızlı yöntemlerden birisi dosyaların hash (sayısal) değerlerini hesaplayarak bu değerleri bir biri ile karşılaştırmaktır. Forensic Explorer kullanıcı dostu ara yüzü ile çok kısa sürede hash (sayısal) değeri hesaplama ve karşılaştırma işlemini yerine getirebilmektedir.

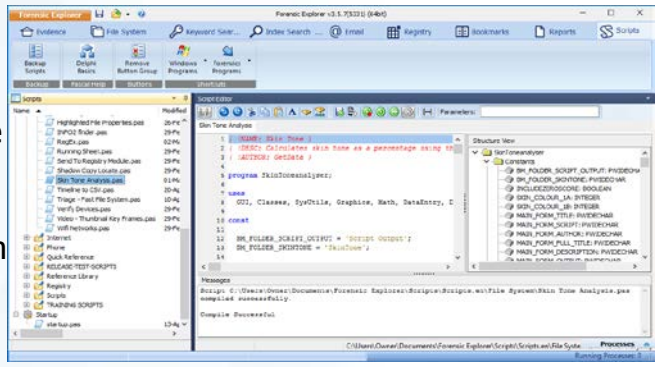
Tel : +90 312 219 56 16
Fax : +90 312 219 46 05
E-Posta : info@difose.com.tr
Adres : Ümit Mah. 2481.Sok. Kafkas Sitesi No:6 Ümitköy/ANKARA

ADLİ BİLİŞİM HİZMETLERİ
DIFOSE
DIGITAL FORENSIC SERVICES

www.difose.com.tr

- **Çoklu dil anahtar kelime arama (Basit metin, Grep, Hexadecimal):** Adli bilişimde en sık kullanılan özelliklerden birisi anahtar kelime arama yöntemidir. Forensic Explorer kullanıcı için bu konuda hızlı ve esnek çözümler sunmaktadır. Türkçe dahil çoklu dil desteği, basit ifade arama özelliği, hexadecimal arama özelliği ile bu konuda komple çözüm sunmaktadır.

- **İndeksleme ve hızlı sorgulama:** Forensic Explorer, gelişmiş indeksleme metodu ile adli kopya içerisindeki tüm kelimeler indeksleyerek incelemeci için büyük kolaylıklar sağlamaktadır.



- **Analiz motoru ile hızlı analiz yapabilme:** Bir adli kopyanın incelenmesi esnasında ihtiyaç duyulan temel gereksinimler düşünülerek analiz motoru geliştirilmiştir. Analiz motorunda yer alan kullanımı kolay ve basit scriptleri kullanmak suretiyle adli kopya içerisinde detaylı inceleme ve analiz yapılabilmektedir.
- **Öncelikli analiz (Triage) yapma özelliği:** Triage adı verilen öncelikli analiz ile incelemeye başlamadan adli kopya üzerindeki ilk başta incelenecek hususlar tespit edilerek inceleme ve analiz en kısa sürede tamamlanmaktadır.
- **Üstün filtreleme ve kategori özellikleri:** Adli kopya içerisinde yer alan dosyalar çeşitli filtreler kullanılarak kolay ve hızlıca tespit edilebilmektedir.
- **Üstveri (metadata) tespiti ve raporlaması:** Üstveri bilgisi tutan dosyalara (EXIF, GPS, OLE, PDF, NTFS, LNK, Prefetch) ait bilgiler (metadata) seçmeli menüler kullanılarak tespit edilmekte ve kolayca raporlanabilmektedir.
- **Shadow kopya tespiti ve analizi:** Bilişim suçlarının artışına paralel olarak, anti-adli bilişim metot ve tekniklerinin kullanımı da yaygınlaşmıştır. Özellikle bilgisayarın en sık kullanılan masaüstü ve belgelerim gibi klasörlerin şüpheliler tarafından geri kurtarılamayacak şekilde silinmesi adli bilişimcinin işini zorlaştırmaktadır. İşte bu doğrultuda, Windows işletim sisteminde yer alan “Volume Shadow” kopyaları suç ya da suistimal incelemesinde çok büyük imkanlar sunmaktadır. Özellikle geri kurtarılamayacak şekilde silinen veriler, silinme tarihinden önceki bir “Volume Shadow” kopya açılarak elde edilebilmektedir. Adli kopya içerisinde birden fazla “Volume Shadow” kopya bulunabilmekte ve bu durum incelemecinin işini kolaylaştırmaktadır.

Tel : +90 312 219 56 16
Fax : +90 312 219 46 05
E-Posta : info@difose.com.tr
Adres : Ümit Mah. 2481.Sok. Kafkas Sitesi No:6 Ümitköy/ANKARA

ADLİ BİLİŞİM HİZMETLERİ
DIFOSE
DIGITAL FORENSIC SERVICES

www.difose.com.tr

GetData FORENSICS

FORENSIC EXPLORER

- **Kolay ve hızlı Registry analizi:** Forensic Explorer'un kullanıcı dostu ara yüzü ile Windows işletim sistemi registry analalizini hızlı bir şekilde yapabilirsiniz. Yapmanız gereken tek şey, kategoriler bölümünden registry dosyalarını seçmek ve Registry Modülüne göndermektir.
- **Kolay ve hızlı e-posta analizi:** Forensic Exploreren çok kullanılan e-posta formatları olan Microsoft Outlook ve MS Office Outlook e-posta formatlarını (*.PST, *.OST, *.EML, *.MSG, *.DBX, *.EDB) adli kopya içerisinden tespit ederek "Kategoriler" menüsü altında toplayarak hızlı bir e-posta analizi yapmaya imkân sağlar.
- **iTunes yedeklerini tespit, inceleme ve analiz yapma:** Apple ürünlerinin kullanımının yaygınlaşmasına paralel olarak, özellikle mobil cihazlara yüklenecek veriler için bir bilgisayar ile eşleştirmek gerekmektedir. Bu nedenle adli incelemesi yapılan bilgisayarların pek çoğunda Apple cihazların iTunes yedekleri yer almaktadır. Forensic Explorer kullanarak iTunes yedekler üzerinde inceleme ve analiz yapabilir, tespitleri kısa sürede sık kullanılanlara ekleyerek raporlayabilirsiniz.
- **Sık kullanılanlara ekleme ile hızlı ve kolay analiz yapma:** Adli bilişim incelemeleri uzun zaman alan çalışmalardır. Bazen incelemeciler veriler içerisinde kaybolabilir ya da tespit ettikleri verileri raporlamaları uzun zaman alabilir. Bu sorunları çözmek için "Sık Kullanılanlar" özelliği geliştirilmiştir. İnceleme esnasında konu ile ilgili hususları sık kullanılanlara ekleyip daha sonra raporlama yapabilirsiniz.
- **Türkçe raporlama ve rapor özelleştirme:** Forensic Explorer kullanarak yapmış olduğunuz incelemeleri, öncelikli analiz raporu ve sık kullanılanlara ilave edilen verileri hızlı ve sorunsuz bir şekilde Türkçe olarak raporlayabilirsiniz. Hazırlanan raporu (*.PDF, *.RTF ve *.DOCX) formatında dışarı aktararak gerekli düzenlemeleri yapabilir ya da doğrudan yazıcı çıktısını alabilirsiniz.
- **Hızlı, esnek, güçlü, en ekonomik adli bilişim yazılımı:** Forensic Explorer adli bilişim yazılımı rakiplerine göre fiyat ve performans açısından çok avantajlıdır. Ayrıca, Forensic Explorer'ın yazılım dilinin Türkçe olması ve yazılımla ilgili her türlü desteğin DIFOSE tarafından veriliyor olması bir diğer önemli ayrıcalıktır.

Tel : +90 312 219 56 16
Fax : +90 312 219 46 05
E-Posta : info@difose.com.tr
Adres : Ümit Mah. 2481.Sok. Kafkas Sitesi No:6 Ümitköy/ANKARA

ADLİ BİLİŞİM HİZMETLERİ
DIFOSE
DIGITAL FORENSIC SERVICES

www.difose.com.tr