

W4

Kim, Ne, Nerede, Ne Zaman



ÜRÜN TANIMI

- W4 kullanıcı dostu ve esnek bir adli bilişim analiz ve canlı triaj aracıdır.
- W4 fonksiyonları ve arayüzüyle adli bilişim incelemesine birçok kolaylık sağlar.
- İndeksleme sırasında bulgu ve delillerin incelenmesini sağlar.
- Bilinen tüm disk ve cep telefonu imaj formatlarını destekler.
- İndeksleme başladıktan sonra dakikalar içerisinde ilk sonuçlar incelemeye sunulur.
- Canlı sistemlerden RAM bilgisi ve registry kayıtları başta olmak üzere imaj alma yeteneğiyle, saatler sürecekleme dakikalara indirir.
- Dosyalar arasındaki ilişkilendirme ve zaman çizgisinde gösterme yeteneği olay çözümüne katkı sağlar.



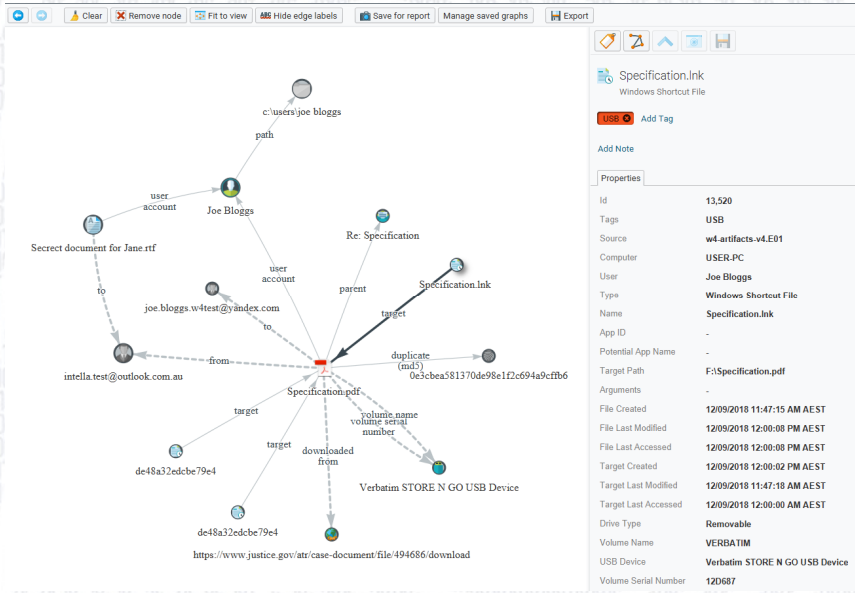
TONLARCA BULGU

- Uzman olmayanların da kullanabileceği basit bir arayüz
- Güçlü indeksleme motoru
- Özelleştirilmiş arama profilleri
- İndeksleme sırasında vaka inceleme
- Canlı sistemlerden otomatik RAM imaj alma
- Kullanıcı aktivitelerini zaman çizelgesinde gösterme
- Çalışan makinaların imajının alınması ve indeksleme
- Link özelliğiyle bulgular arasında ilişkilendirme
- Bulgu ve delilleri işaretleme ve not ekleme yeteneği
- Güçlü ve esnek raporlama yeteneği
- Kapsamlı olay görüntüleme yeteneği
- Olay mahallinde triaj ve canlı imaj alma



Desteklenen Dosya Formatları

- EnCase adli kopyaları (Eo1, Exo1, Lo1, Lx01 ve S01 dosyaları)
- FTK adli kopyaları (AD1 dosyaları), versiyon 3 ve 4
- DMG
- DD adli kopyaları
- MacQuisition adli kopyaları (RAW, .00001 dosyaları)
- VMware adli kopyaları (VMDK dosyaları)
- VHD disk adli kopyaları
- VHDX ve AVHDX disk adli kopyaları
- BitLocker kriptolu sürücüler
- Volume Shadow kopyalar
- Cellebrite UFED XML veya UFDR dosyası
- Micro Systemation XRY XML ve Extended XML dosyaları
- Oxygen Forensic Suite XML dosyaları
- iTunes yedekleri



W4 aşağıda sıralanan dosyaları ayrıntılı şekilde size sunar

- Sistem bulguları (disk bilgisi, olay kayıtları, kullanıcı bilgileri vb.)
- Programlar
- Cihazlar (USB, network vb.)
- Dosya ve Klasörler
- İnternet Tarama Geçmişi
- Program kullanım durumu
- İletişim
- Dokümanlar
- Medya (resim, video vb.)
- Arşiv dosyaları
- Kripto Para bilgileri

