



FORENSAFE ARTIFAST



ÇAPRAZ PLATFORM ARACI

Forensafe Artifast, tercih ettiğiniz platformda çalışmak üzere tasarlanmıştır. Motor çok çeşitli Artifact türlerini destekler. Artifast, farklı kaynaklardan gelen 975'ten fazla türü ayrıştırabilir ve analiz edebilir. PC için Windows, macOS ve Linux, mobil cihaz için iOS ve Android desteği vardır. Herhangi bir cihazdan kanıt toplayin ve tercih edilen platforma göre Windows, macOS veya Linux'ta analiz edin.



HIZ DÜŞÜNÜLEREK TASARLANDI

Uzmanların görevlerinin tamamlanmasının zaman aldığını biliyoruz. Bu nedenle, Artifast'ı, adli bilişim uzmanlarının kanıt toplamaya daha az zaman ayırarak, istenen kanıt bulmak için incelemeye daha fazla zaman harcamasını sağlamak için geliştirdik. Özel ve güçlü sorgu dilimiz FQL ile, milyonlarca kayıtlı uğraşılıyor olsanız bile, aradığınızı bulmak yalnızca saniyeler sürer.



ORGANİZE ZAMAN ÇİZELGESİ

Ekranlar arasında kaybolmayın. Artifast, diğer zaman çizelgesi araçlarından daha normalize edilmiş sütunlarla her tür kanıt için tek bir organize zaman çizelgesi sağlar. Artifast ayrıca, adli bilişim uzmanlarına arama kriterine göre herhangi bir kaydı sıralama, gruplama veya yer imlerine ekleme yeteneği sağlamak için notlar ve renklendirme özellikleri sunar.



ZAMAN ÇİZELGESİ TABANLI ADLİ BİLİŞİM ANALİZİ

Adli bilişim hızla değişiyor, siber saldırılar daha karmaşık hale geliyor ve olaylara müdahale daha önemli hale geliyor. Günümüzde adli bilişim analizi, yalnızca verileri ayrıştırmak veya silinmiş öğeleri kurtarmak değildir. Bunun yerine, adli bilişim uzmanları "ne oldu, ne zaman, neden, nasıl oldu ve mümkünse kim yaptı" gibi soruları yanıtlamaya çalışıyorlar. Saldırganlar dijital sistemlerde etkileşimde bulunur ve izlerini bırakır. Adli bilişim uzmanları, olaylar sırasında kullanıcı etkinliği için sistemleri analiz eder. Zaman çizelgesine dayalı adli bilişim analizi, uzmanların, aynı kanıtı işaret edecek, aynı bulguları doğrulayacak ve kanıtın doğruluğunu artıracak çeşitli veriler bulmasına yardımcı olacaktır.





AÇIKLAMALAR

YAPI

Artifast, Artifact analizi için girdi olarak disk, imaj ve klasörleri girdi olarak alabilen Forensafe Yazılım Çözümleri'nin en yeni çözümüdür. Düz metin, XML, ikili, kayıt defteri, şifrelenmiş, bileşik veya karmaşık gibi farklı biçimlerde kazınan tüm Artifact'ler, adli bilişim açısından değerli verilerin çıkarıldığı yerde ayrıştırmadan geçecektir. Tüm Artifact'ler aynı değildir, bu nedenle ayrıştırılan girdiler, kanıtların açık ve kesin bir şekilde organize edilmesine yardımcı olacak normalleştirmeden geçecektir. Çıkarılan veriler kaydedilir ve veritabanlarında kronolojik olarak sıralanır. Etkili kullanıcı arayüzü, adli bilişim uzmanına verimli arama, filtreleme, renklendirme ve raporlama sağlar.

NEDEN ARTIFAST?

Dijital sistemlerde her dakika yüzlerce olay gerçekleşir. Zaman çizelgesi analizi tarafından üretilen büyük miktardaki veri, adli bilişim uzmanlarını kolayca bunaltabilir. Zaman çizelgesine dayalı adli bilişim araçları, uzmanlara milyonlarca kayıt arasından kanıt bulma işini kolaylaştıracak beceriler sağlamalıdır. Artifast bunu çözmek için indekslemeyi, güçlü filtrelemeyi ve aramayı destekler. Artifast, adli bilişim uzmanları için hem "Artifact" hem de "Timeline" görünümleri sağlar. Ayrıca Artifast, daha verimli analiz ortamı oluşturmak için çalışma alanları aracılığıyla vaka yönetimi gerçekleştirir.



ÖZELLİKLER

- 975+ Artifact desteği
- Kolay Ancak Gelişmiş Filtreleme
- Daha Hızlı Arama
- Tüm Kanıtlar İçin Tek Zaman Çizelgesi
- Organize Zaman Çizelgesi
- Meta Veri Ayrıştırma
- İçerik İndeksleme
- Entegre Dosya Görüntüleyici
- Veri görüntüleme
- Normalleştirme
- Raporlama

