Magnet IEF

İnternet aktirifleri üzerine araştırma yapmak için kullanılır.

DRIVES, canlı bir diski fiziksel olarak mantıksal olarak belli partionsları açıp inceleyebiliyoruz.

Bir imajdan ya da canlı olarak bağlanılan disklerden mantıksal alanlardan ya da fiziksel alanlardan belli bir dosyayı ya da belli bir dizini açıp inceleyebiliyoruz. Sistemden sisteme bağlı bir şekilde ağ varsa o yerel ağdan bağlı olan bilgisayarlardan belli dosyaları açabiliriz.

Volume Shadow Copies, bilgisayara bağlı olan disklerde veya imaj içerisinde Volume shadow copyleri açabiliriz.

Mobile, bu platformdaki cihazları bağlayıp inceleyebiliyoruz ve istersek imajını alabiliyoruz.

Yani fiziksel ya da mantıksal alanları bir imajdan ya da bilgisayara bağlı olan disklerden belli dosyaları ya da klasörleri imajları volume shadow copies alanlarını veya bir mobili inceleyebiliriz.

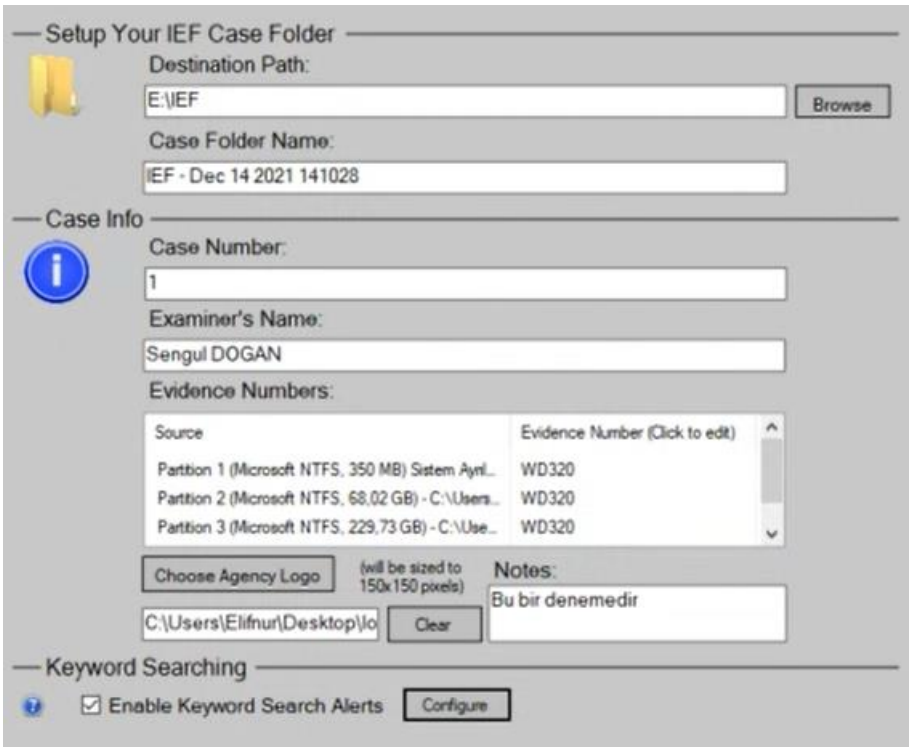
**Images'i seçip devam ediyoruz:quick,sector level,custom,full

Hangi partionda ne tür inceleme yapacağımızı seçiyoruz(detaylı,full,sektör seviyesinde ayrıntılı bir şekilde).Veya *Custom* dersek belli alanları seçip inceleyebiliriz(File Slack Space(dosya artık alanı),$MFT(işletim sisteminde dosyaların nerede olduğunu tutan tablodur),pagefile.sys(windows işletim sisteminde bilgisayarda ramin yetmediği durumlarda harddiskin belli bir oranı ram gibi kullanıldığı alanlar.sanal bellek olarak adlandırılabilir.ram gibi hızlı erişilebilen bir alan değildir.ramin yettiği durumlarda da kullanılabilir.),hiberfil.sys(bilgisayarı uyku moduna aldığımızda ramin kaydedildiği dosyadır.ramle aynı boyutta olur.),Unallocated Clusters(bir dosyaya tahsis edilmemiş alanlar),Unintialized File Area(başlangıç alanı olarak tanımlanır.)).

- Diğer programlar bunları sormaz hepsini direkt dahil eder.

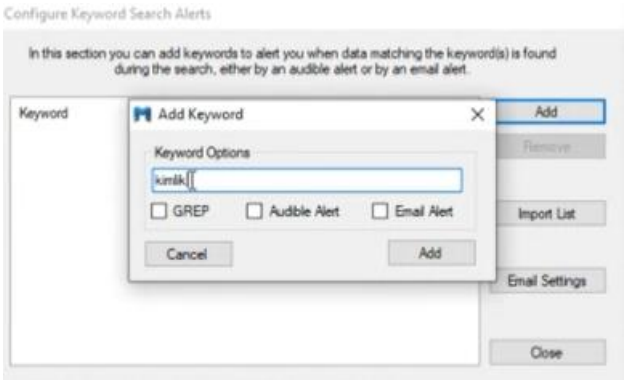
**Bunlar seçildikten sonra OK denildiğinde inceleyeceğimiz alanlar karşımıza gelir.Geldiğinde istediklerimizi kaldırabiliriz.Yeni alanlar da ekleyebiliriz.NEXT deriz.Karşımıza tanıdığı Artifactslar çıkar.İstediğimiz seçimleri yapıp profil olarak kaydedip seçimimizi default olarak ayarlayabiliyoruz.İstediğimiz profilleri silebiliriz.ini şeklinde kaydedilmiş bir profili açıp kullanabiliriz.Next denir.

Karşımıza nereye kaydedileceği,ismi,case number,inceleyici,rapor oluştururken kurumun ya da firmanın logosu varsa eklenir,notes yazılır.Keyword araması isteniyorsa seçilir.

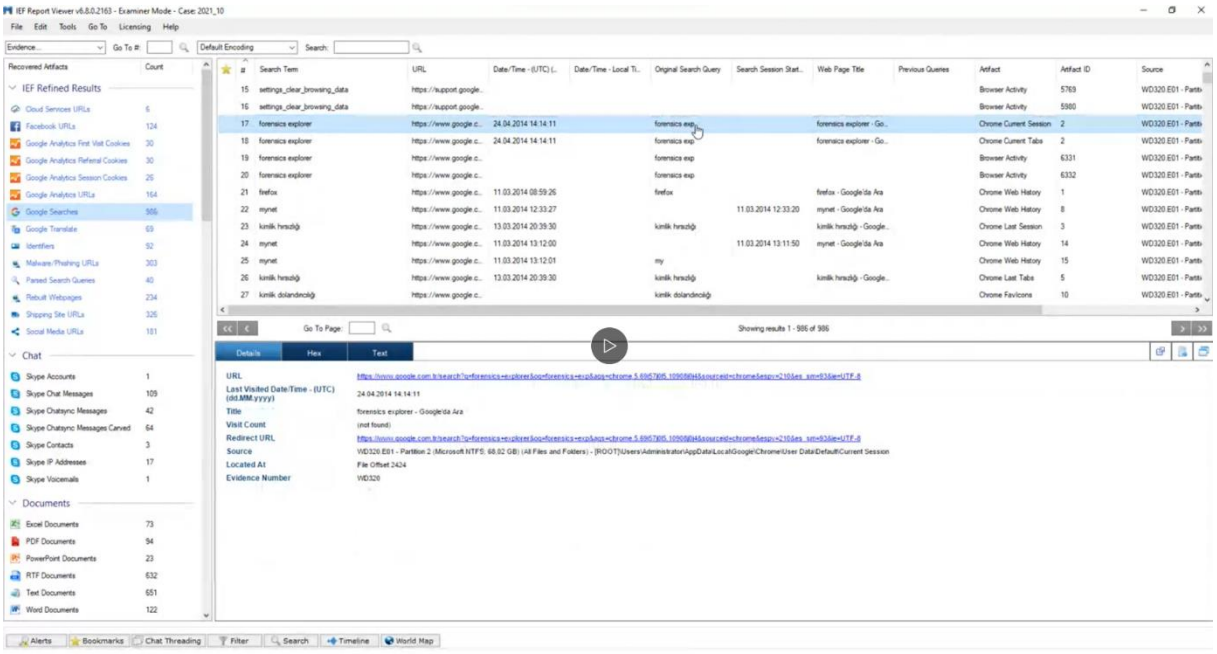


Grep kendine özgü desen örneğin emailin veya kredi kartının kendine özgü deseni var bu tür desenleri tanımlamak istiyorsak GREP tanımlarız.Yazdığımız kelimeyi bulduğunda sesli bir şekilde mi yoksa emaille mi uyarı vereceğini soruyor.

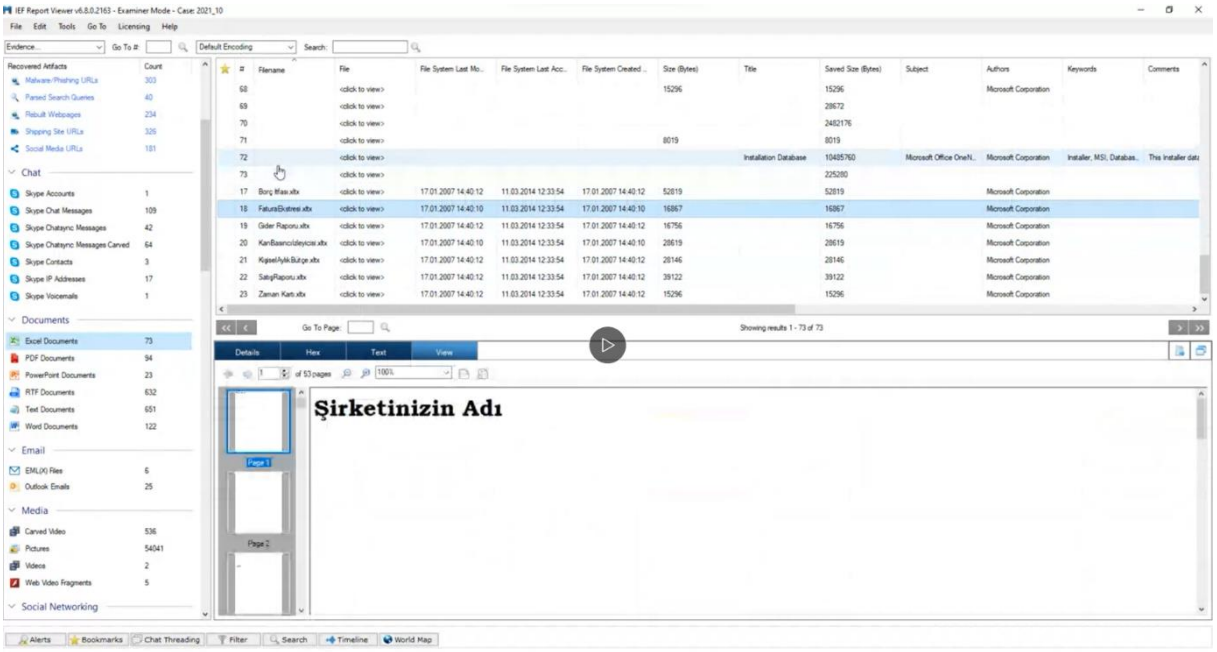
Import List denildiğinde keyword listesi ekleyebiliyoruz.İndex yapmıyor.



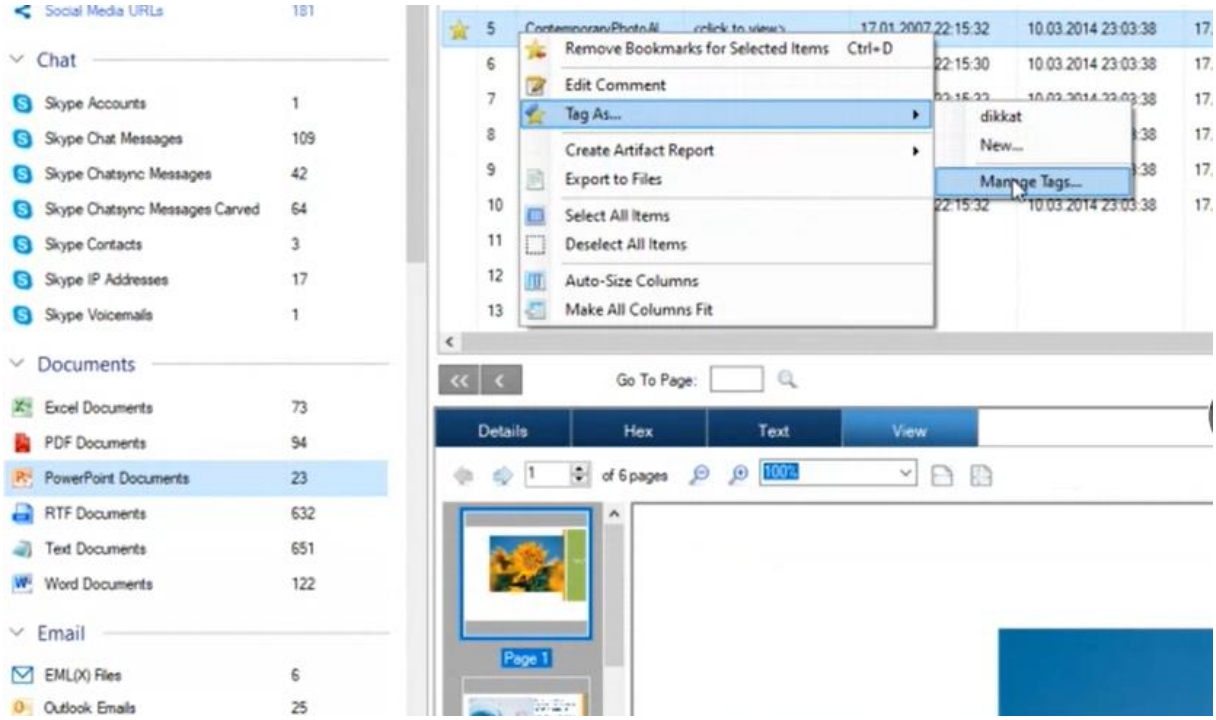
**FIND EVIDENCE denir.Examier penceresi gelir.Bulunanlar examier penceresinde sunuluyor.Proses tamamlandıktan sonra sistemimizi incelemeye başlarız.



Skype contacts'da kimlerle iletişim kurulduğu gözükür.Skype IP Addresses iletişim kurulan hesapların IP adresleri gözükür.Skype Vocemals'da sesli aramalar gözükür.

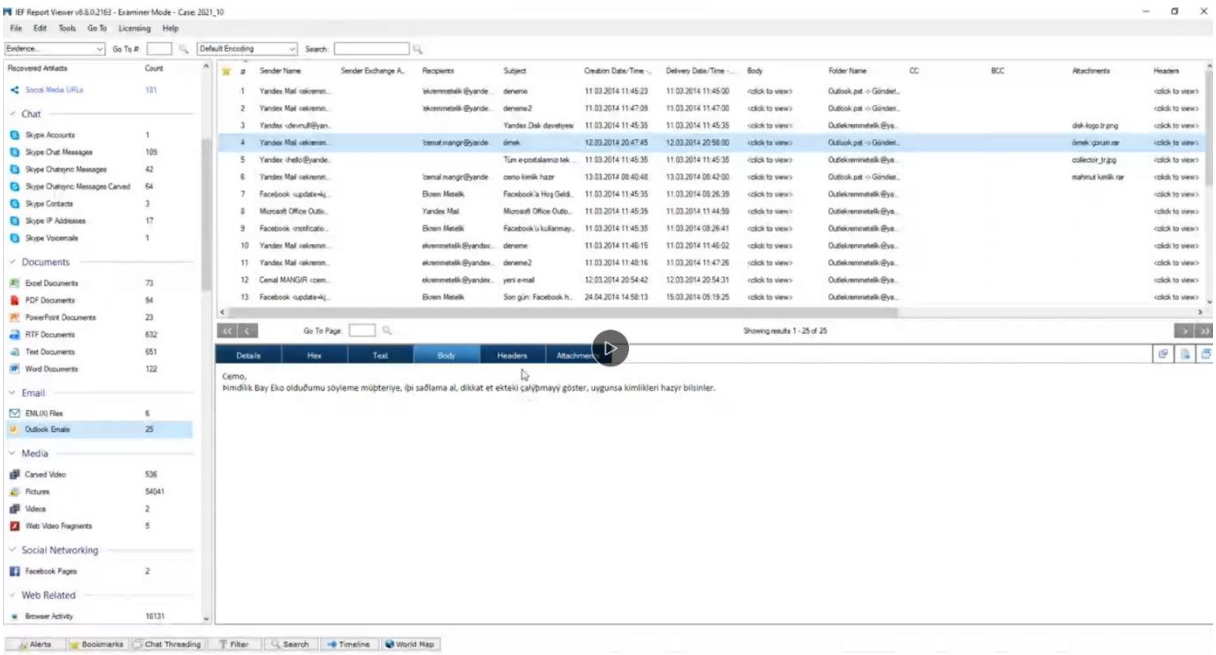


Excel Documents'de bazıları carve edilmiş ancak kurtaralamamış sayfalar olabilir.Yani carve edilen dosyalar açılamayabilir.Export to Files diyip dışarı aktarabiliriz.



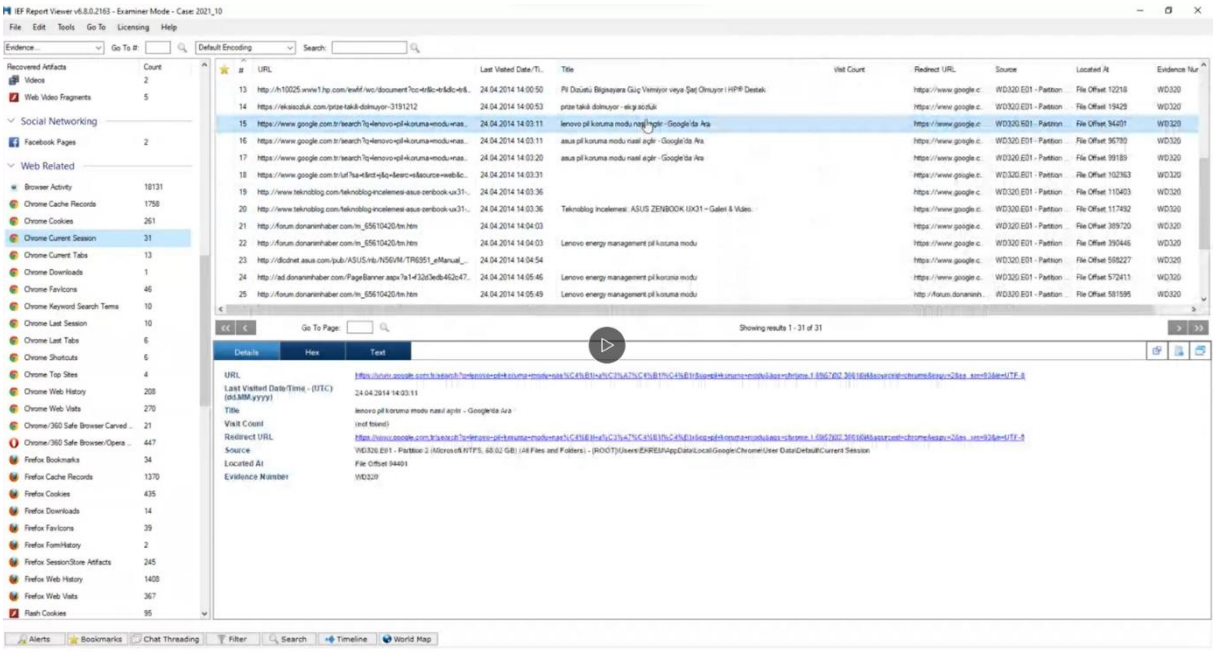
Tag As'a tıklayıp New diyip yeni taglar oluşturabiliyoruz. Toolsda da Manage tagsları görebiliriz.

RTF Documents zenginleştirilmiş metin belgesi.



Videolardan kesit resimler oluşturamıyor.?1.11

Facebook Pages'te facebook pagesleri sayfaları burda gözüküyor.



Chrome Current Session’da Oturumda girilen sayfalar gözüküyor.

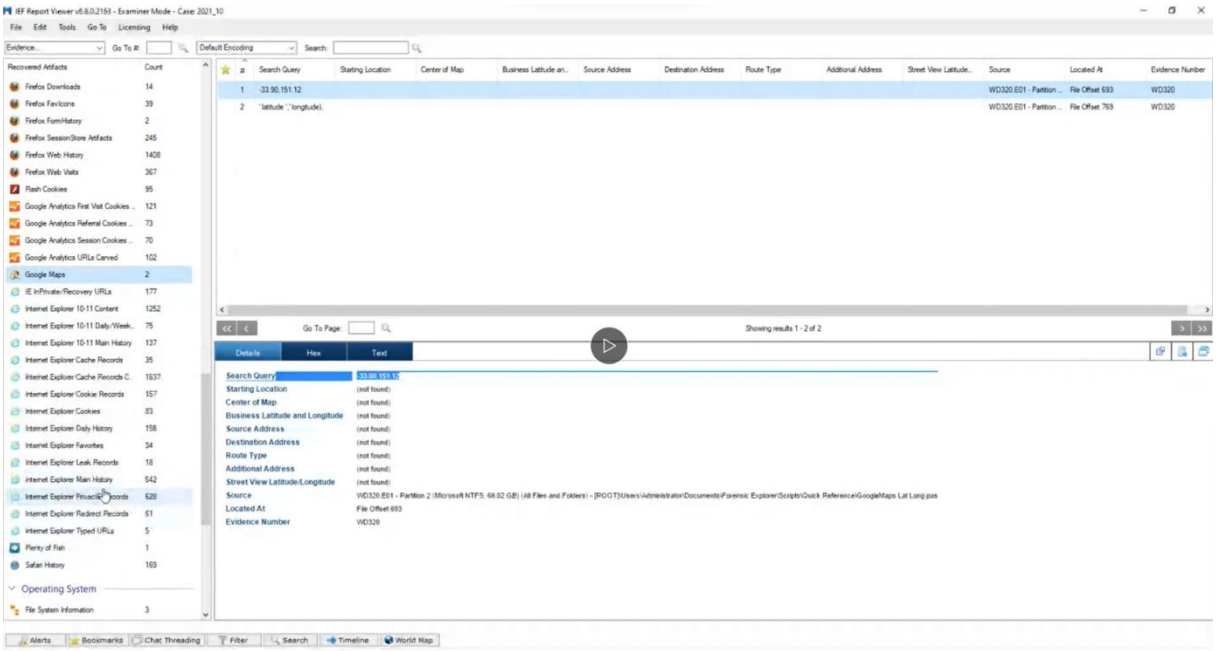
Chrome Current Tabs’da farklı tablarda farklı sekmelerde girilen sayfaları gösteriyor.

Chrome Shotcuts kısayolda eklenenler.

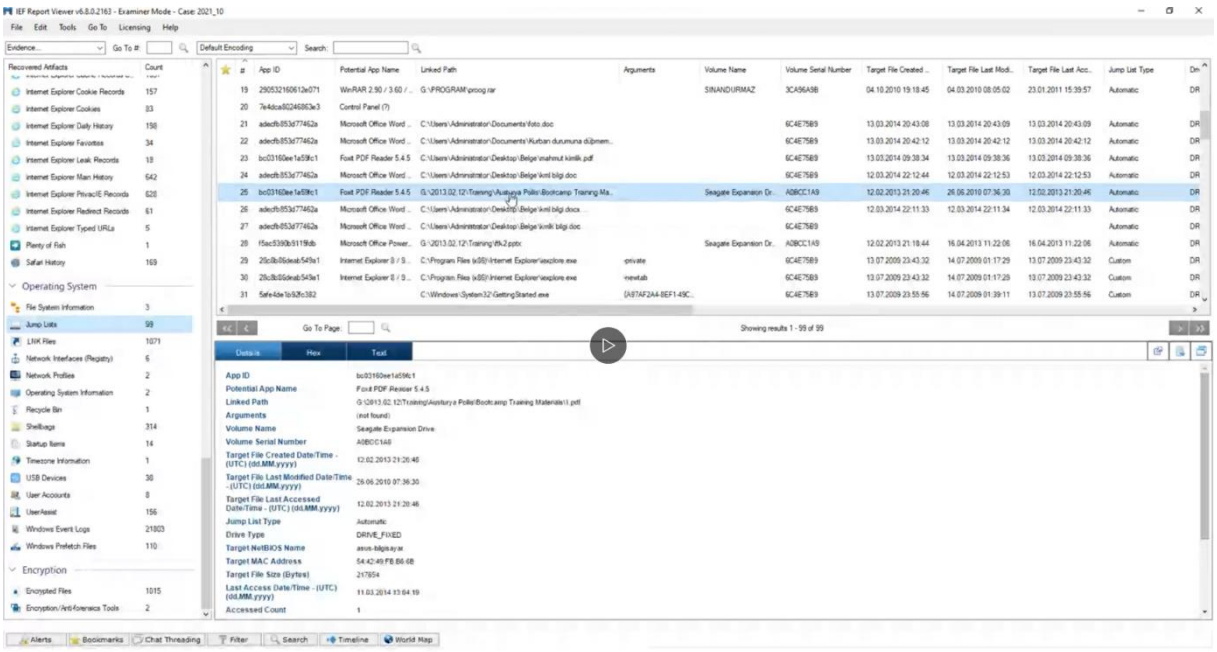
Chrome Top Sites, en fazla girilen siteler.

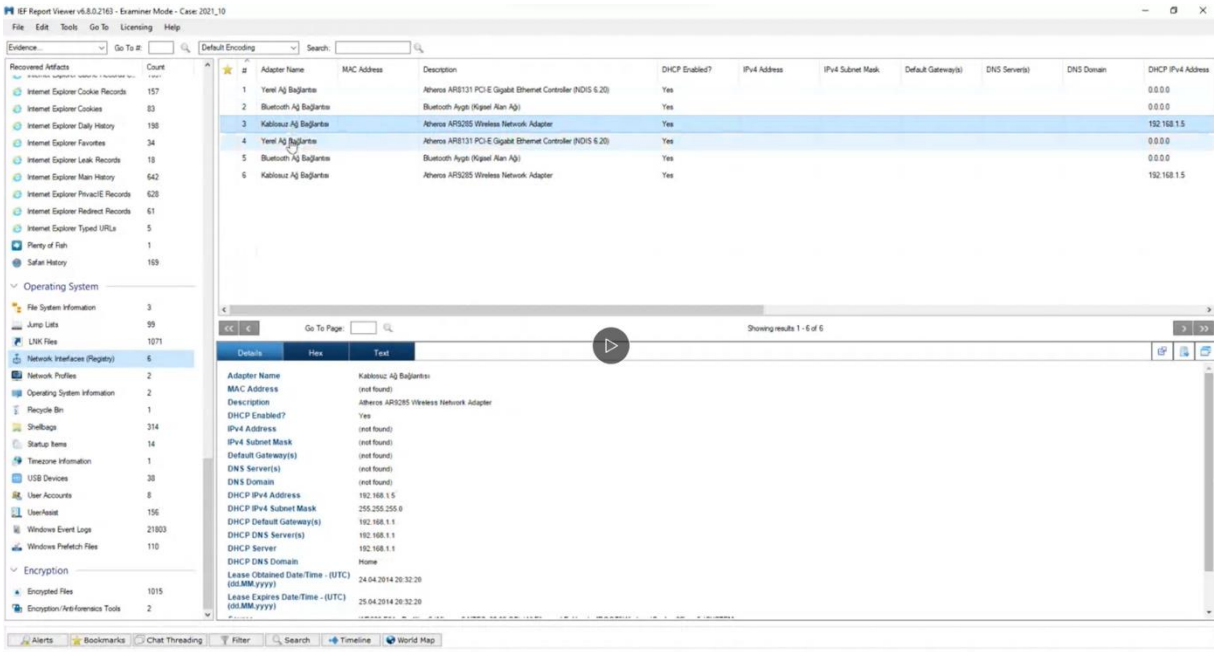
Firefox FavIcons, ikonları gösteriyor.

Google Maps’te aranan koordinatlar gözükür.



Jump Lists, girilen sayfalar,flashbellek,haricidiskler görülür.





Recycle Bin, geri dönüşüm kutusunda olanlar.

Shellbags, control panel denetim masasına girilmiş,my computera girilmiş,Belge isimli klasöre girilmiş,girilen sayfaları alt dizinleriyle birlikte gösteriyor.

Startup Items, başlangıç nesnelerini gösteriyor.

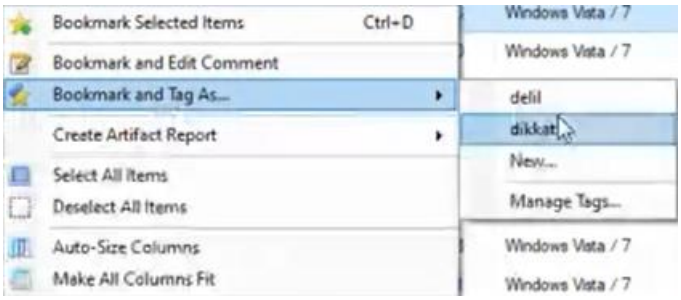
USB Devices, usb bilgilerini görebiliyoruz.

User Accounts, kullanıcı hesaplarını görebiliyoruz.

UserAssist, Administrator kullanılarak yapılan işlemler,ASUS kullanılarak gerçekleştirilen burdaki dosyaları görebiliyoruz.

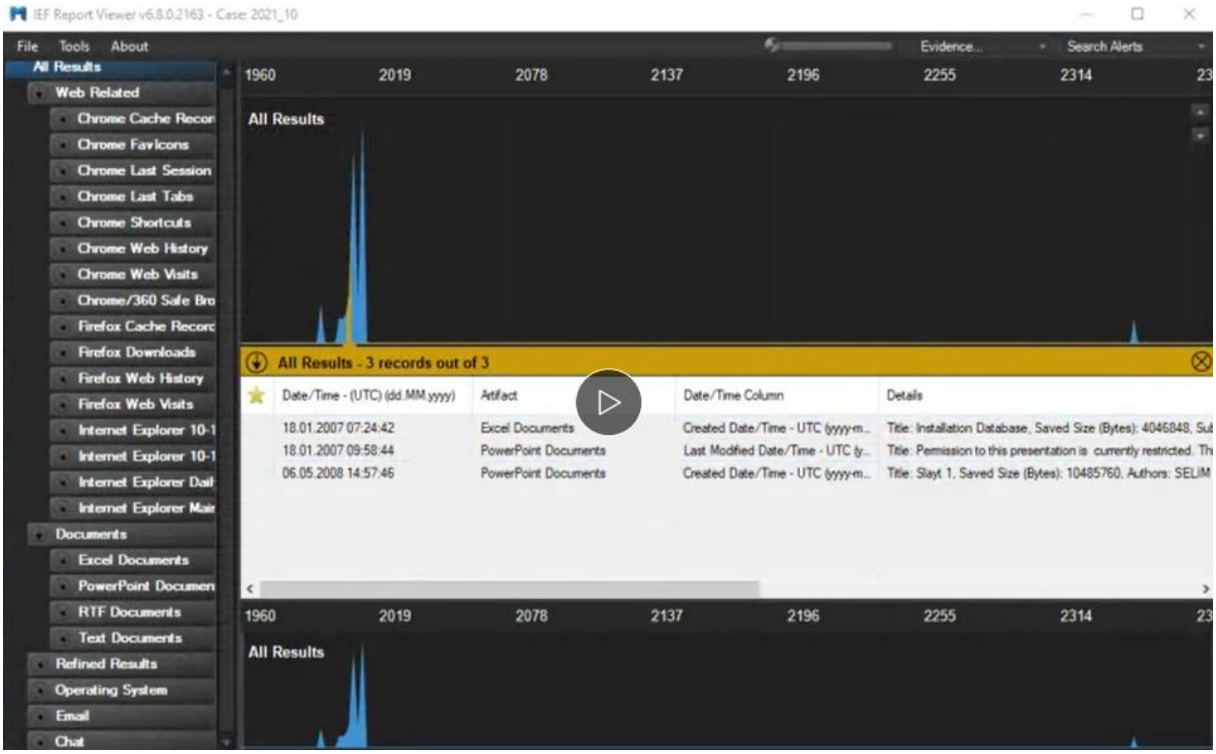
Windows Event Logs, olay günlükleri olarak sunulan event logları burada görebiliyoruz.

Windows Prefetch Files, windows7 kullanılarak öncelikli çalıştırılan dosyalar gözükür.

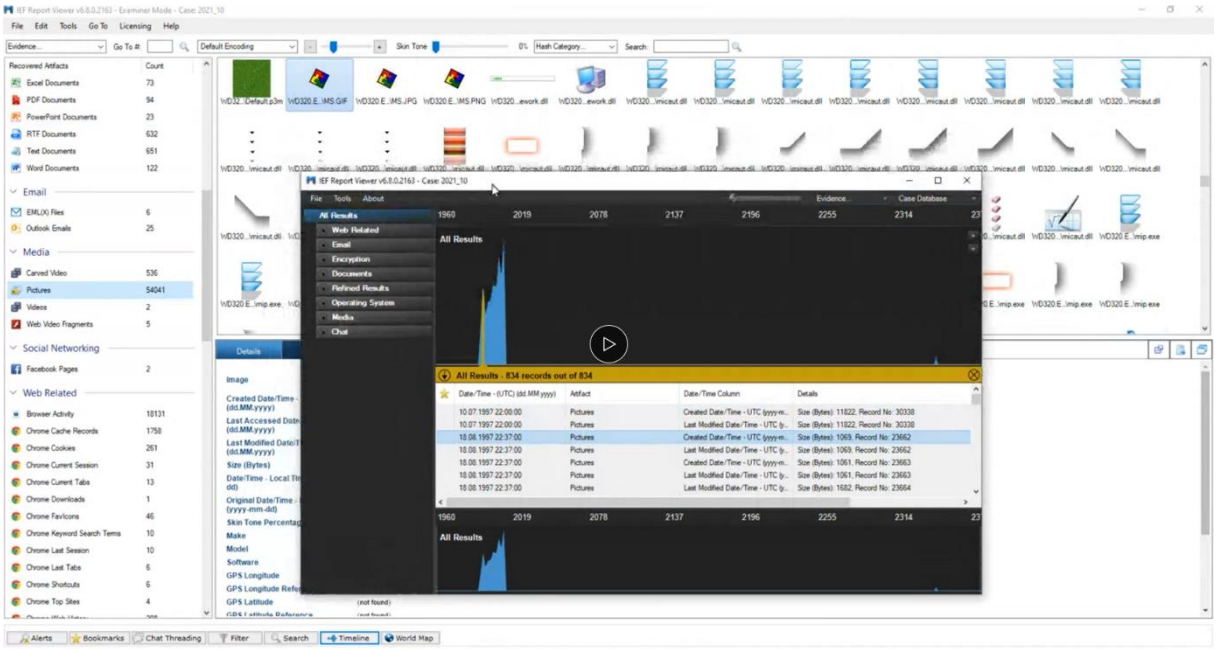


Bookmark and Edit Comment'e tıklandığında dosyaya comment yazılır.Seçilen dosya bookmark olarak eklenir ve comment(yorum) eklenir.

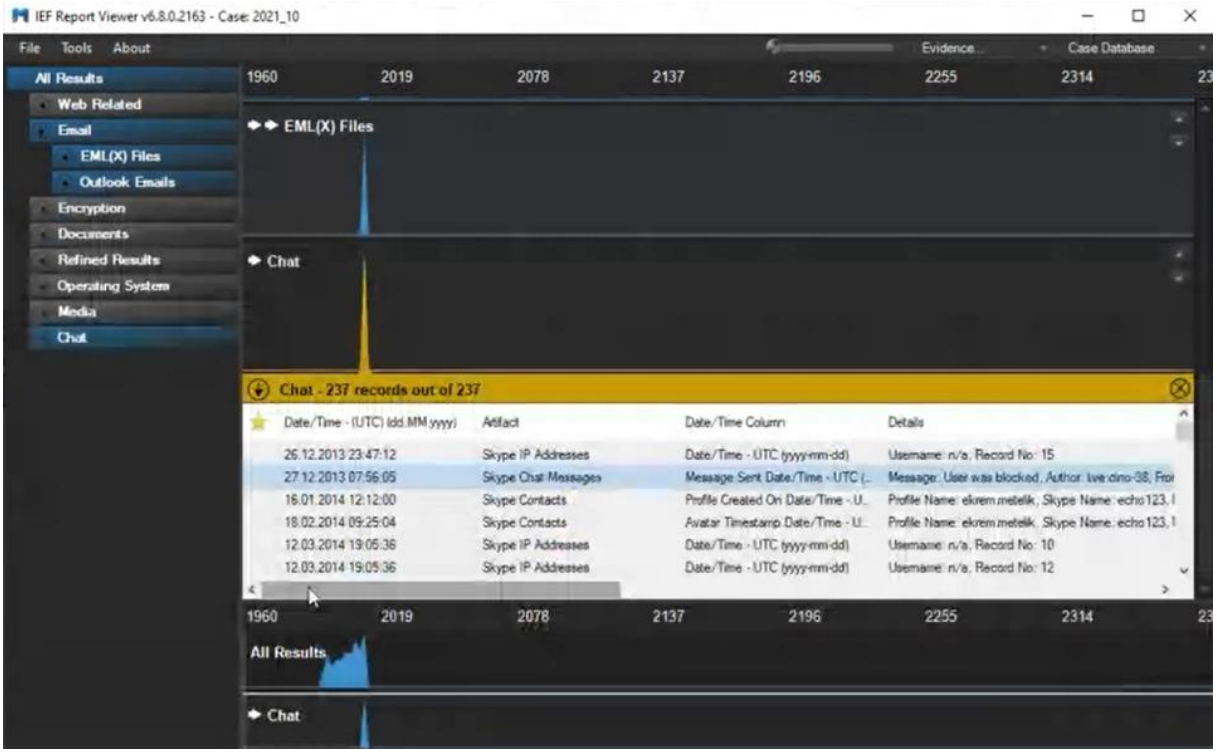
☺Alerts sekmesine tıklanıldığında aranan kelimelerin sonuçları görülebilir.Timeline tıklanıldığında bu kelimelerin zaman dağılımlarını görebiliriz.



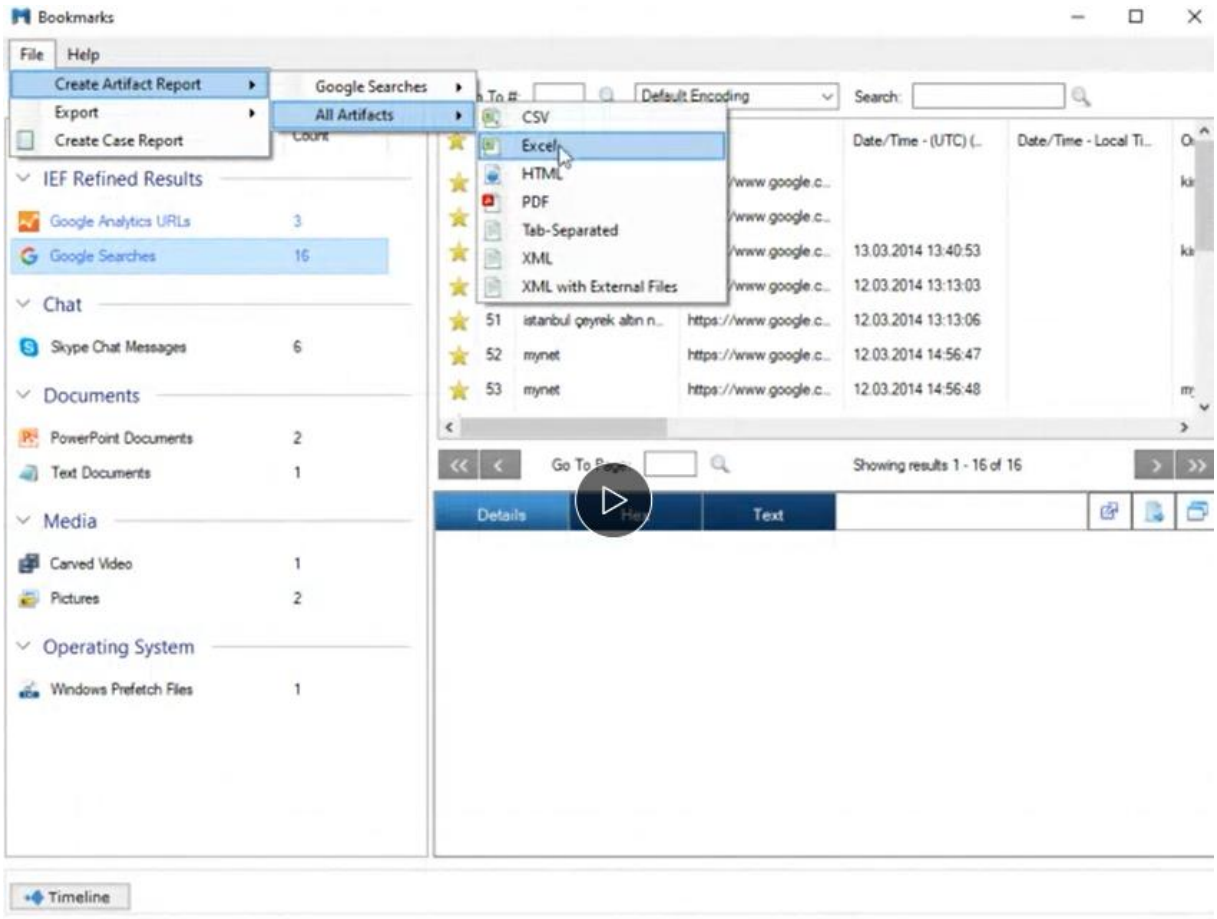
☺Timeline sekmesine tıklanıldığında tüm dosyaları zaman dağılımında görebiliriz.Tıkladığımız dosyanın kendisini katagorisinde gösterir.

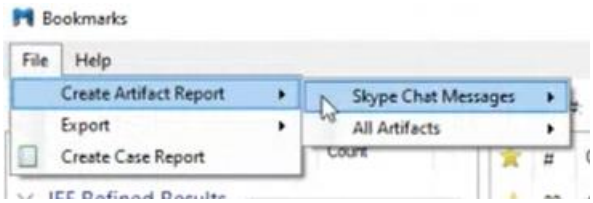


Alt tarafta istediğimiz alana getirip üst tarafta yakınlaştırma işlemi gerçekleştiriliyor,gün bazında saat bazında görmek için.Lazım olan zamana tıklayıp yapılan hareketleri görebiliriz.

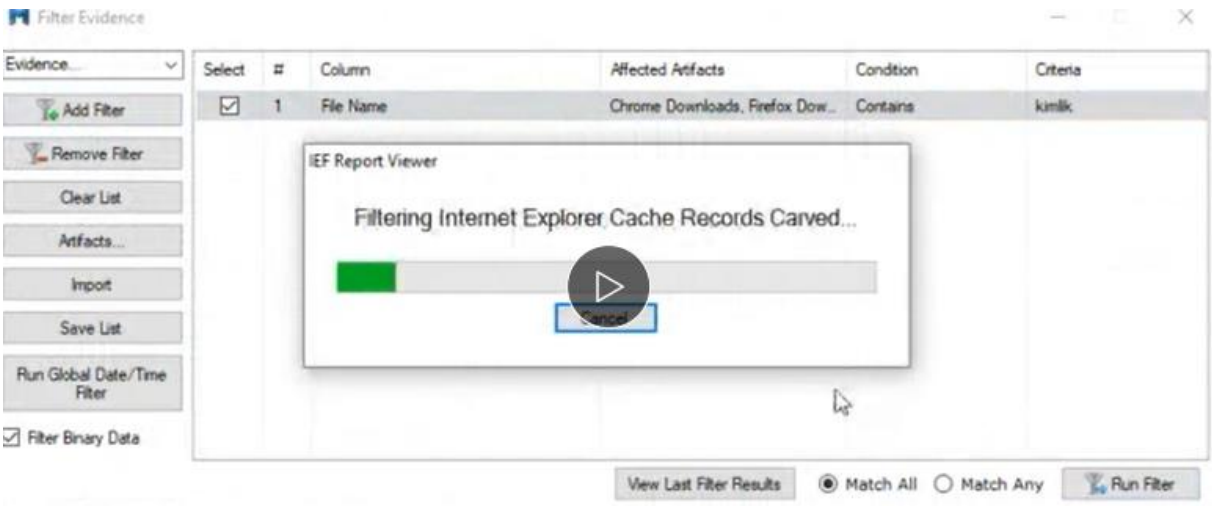


☺Bookmarks Bizim için delil olan nesneleri Create Artifact Report diyip All Artifacts'ı(hangi alanı istiyorsak) seçip istediğimiz formatta rapor oluşturulur.

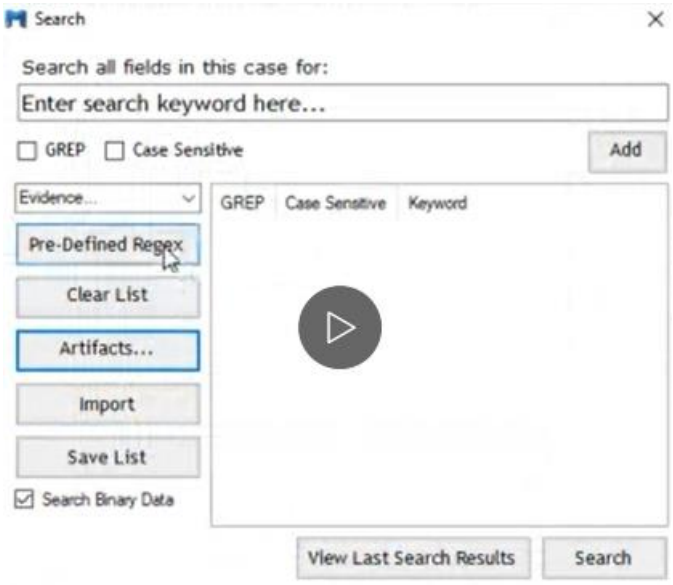


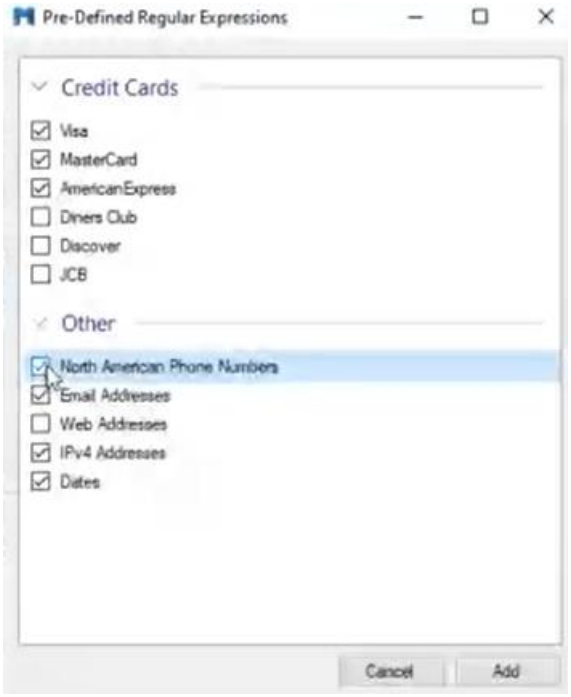


☺Filter, istediğimiz yerlerde filtreleme yaparak kimlik geçen yerleri bulur ekrana getirir. Action filtre anlamında bunun daha geliştirilmiş şekli.

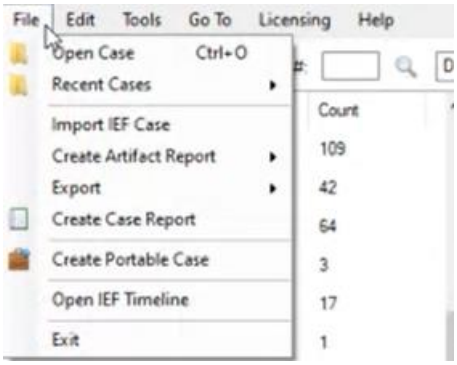


☺Search'e tıklanıldığında belli kelimeleri aratabiliyoruz.Hangi Artifactslerde aratma yapmak istiyorsak seçebiliriz.Pre-Defined Regex'te desen yazmayı bilmiyorsak istediklerimizi(bunlar GREPtir) ekleyip Add diyip View Last Search Results denildiğinde aranan sonuçları ekranda görürüz,bulunan kelimeleri burdan bulabileceğiz.





☺World Map, farklı dosyalar için elde edilen veriler konum bilgisi içeriyorsa burda görebiliriz.



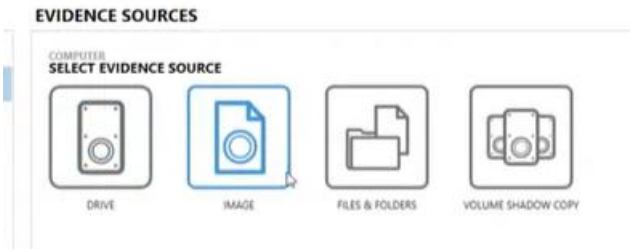
Create Portable Case seçeneği dangıl olmadığı zaman bu case'i inceleme imkanı sunuyor. Hangi alanları dangıl olmadan incelemek istiyorsak seçeriz.

Magnet AXIOM

AXIOM Process çalıştırılır.Proses işlemini tamamladıktan sonra Examine karşımıza otomatik bir şekilde gelir.

Case tanımlama kısmı yapılır.Vakayı oluşturacağımız yer ve imajda alınacaksa onunda kaydedileceği yer gözükür.Bu ekranı geçtiğimizde computer(bilgisayar tabanlı bir aygıtsa),mobile(mobil tabanlı bir aygıtsa), cloud(cloud ekranıysa) sekmeleri gelir.

-Computeri seçersek diğer ekrana geldiğimizde *LOAD EVIDENCE'ye* tıklandığında delil ekleyebiliriz. Burayı seçersek sonrasında aşağıdaki ekran karşımıza gelir.Bir drive'ı canlı inceleyebiliriz,imajı inceleyebiliriz,klasör ya da dosyayı inceleyebiliriz,volume shadow alanını inceleyebiliriz.



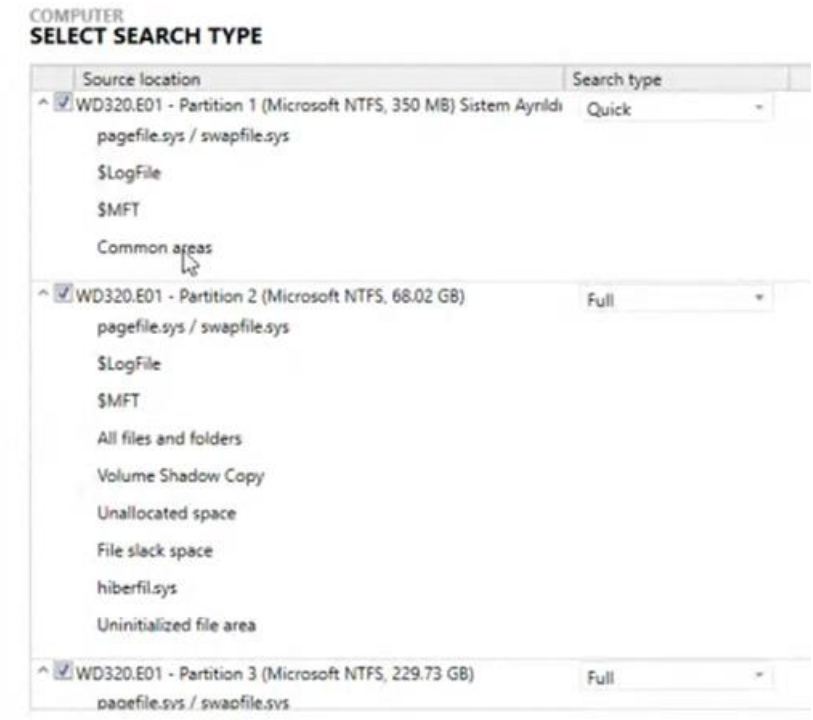
ACOURE EVIDENCE'ye tıkladığımızda mevcut delilin imajını kazanımını sağlayabiliyoruz.Burda bağlı olan diski seçip fiziksel veri kazanılması işlemini gerçekleştirebiliriz.

-Mobile'ı seçersek aşağıdaki ekran gelir.

ANDROİD= Android cihazı seçersek kilitli kilitsiz diye cihazı seçebiliriz ve fiziksel kazanımını elde edebiliriz.İmaj ya da file folder ekleyip inceleme işlemini gerçekleştirebiliriz.

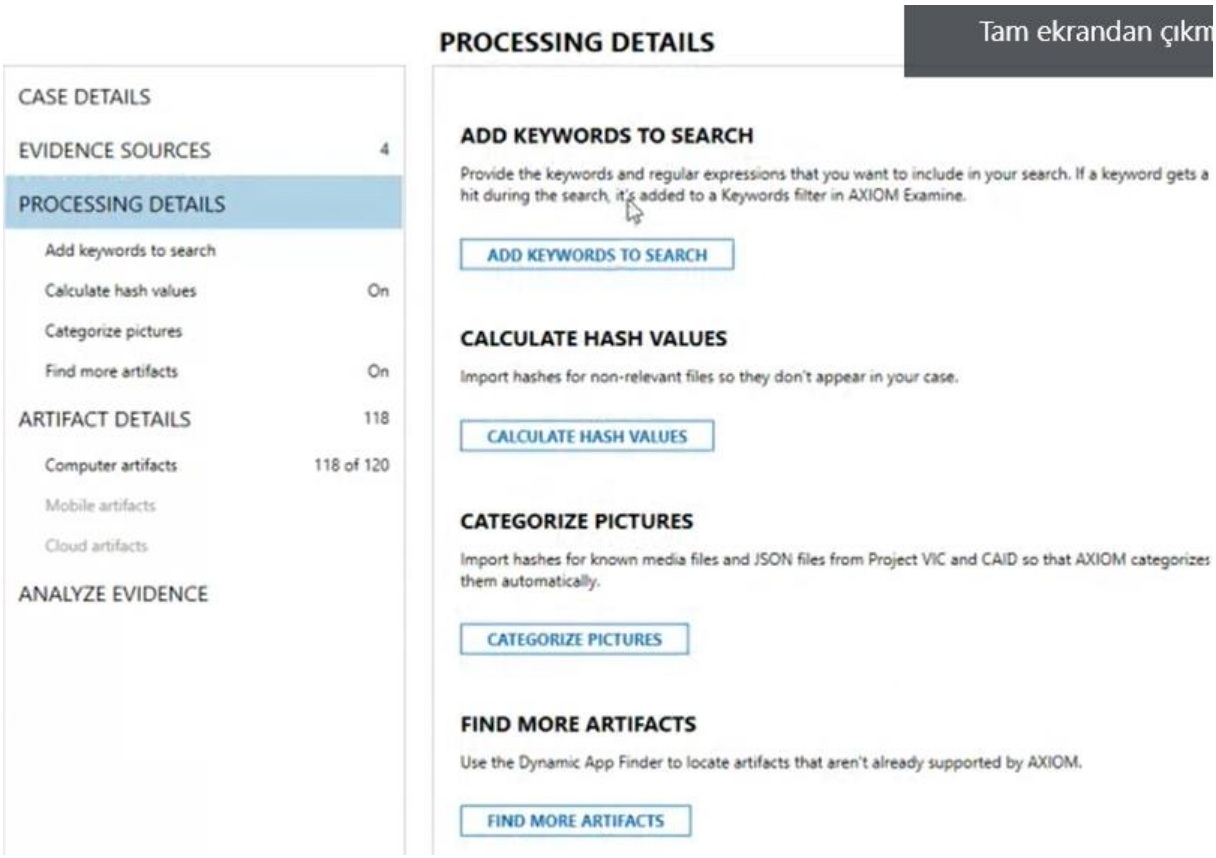
MEDIA DEVICE= Dijital fotoğraf makinası,tablet veya başka elektronik cihazları da media device olaarak takıp inceleyebiliriz.

*Computerı seçip imaj ekliyoruz.İncelemek istediğimiz patitionları seçiyoruz.Sonrasında aşağıda gösterildiği gibi hangi patitionda ne tür inceleme yapılacağı seçilir.



File slack space= Bir veriyi diske kopyaladık,kopyaladıktan sonra diskin belli clusterlarına bu veriler yazılıyor.Sonra bu veriyi sildik,sildikten sonra o verinin üzerine tekrar veri yazdığımızda o clusterdaki o bölümlerdeki veriler tamamen dolmayabiliyor.Ve geride kalan alan bizim için file slack alanı dosya artık alanı olarak tanımlanabiliyor.

*Bu ekranı NEXT diyip geçtikten sonra yeni bir delil ekleyebiliriz veya mevcut delille ilerleyebiliriz.Bu ekranıda geçtikten sonra ;



-Keyword ekleyebiliriz,mevcut keywordlerden ekleyebiliriz ya da yeni keyword listesini bilgisayardan ekleyebiliriz ya da direkt keywordü yeni yazıp ekleyebiliriz(Reges/GREPse işaretleme kutusu var).Listeyi görüntüleyip eklenen kelimeleri görüntüleyebiliriz.Tüm içerikte arayabiliriz ya da Artifactslerde aramayı seçebiliriz.

-Dosya sistem yapısında her bir dosyanın MD5 ya da SHA1 formatında ya da her ikisini seçerek hash değeri hesaplatabiliriz.

Android ya da drive imajlarda özellikle resimlerle ilgili bölükleme işlemi gerçekleştirilebiliyor.Hash değerlerini hesaplatayım mı diyor.Sıkıştırma işemi Compression yapsın mı E01 imajlar için kullanılıyor.Duplicate hash değeri aynı olan yani aynı dosyalar.Önemli olanlar;imajın hash değerini verification yapsın mı yani doğrulama işlemi yapsın mı,Duplicate olan nesneleri remove etsin mi,bu işlemleri yaparken arama hızını kaç kullansın,belirli mbın üstündeki hash değerlerini hesaplatmamak istiyorsak,hash formatlarını seçebiliyoruz,resimlerde photo dna işlemi kullanarak bu işlemleri gerçekleştirsin. Languagesini ayarlarız türkçe desteği var seçip programı türkçede kullanabiliriz.Axiom çalışırken uyku moduna girerse ne yazsa gibi seçenekler var.

MD5 formatında ya da SHA1 formatında hash değeri hesaplatıldıktan sonra hash setleriyle eşleştirme karşılaştırma yapılabilir.

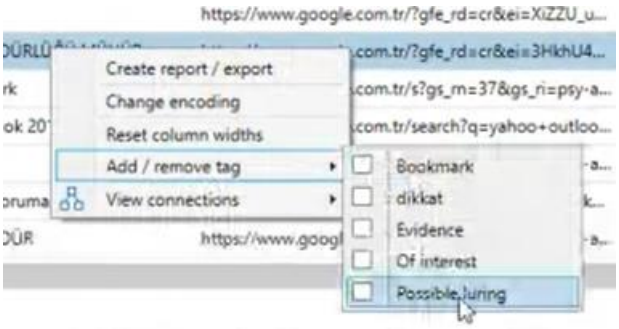
-MD5 formatına ya da SHA1 formatına göre pictureler katagorize edilebiliyor.Hash değerleri için hesaplattığımız hash formatlarına göre belli dosyalar ekleyip resimlerin gruplandırılması işlemini gerçekleştirebiliyoruz,hash değerine göre bu işlemi yapıyoruz.

-Dinamik bir şekilde daha fazla artifacts bulayım diyor.Go to artifact details denildiğinde imajımız bilgisayar olduğu için bilgisayar artifactlarini dahil edebiliriz.İmajımız neyse o aktif haldedir.Üstüne tıkladığımız zaman güncel bütün uygulamaları seçebiliyoruz.Farklı artifactleri seçip yeni profil

oluşturabiliriz.Profil silebiliriz.İleriye gittiğimizde yapacağı işlemleri gösteriyor.Analyze evidence butonuna bastığımızda,examine penceresi otomatik bir şekilde açılacak.

*Dangıl takılıyken proses işlemini gerçekleştiriyoruz.Vakayı açtığımız zaman yine dangılın takılı olması gerekiyor.Dangıl takılıyken Create Portable Case seçeneği istersek belli alanlarda istersek tüm alanlarda create dediğimizde portable case oluşturur.Bu dizini alıp farklı bilgisayarlarda dangılsız bir şekilde çalıştırabiliriz.

Bir dosyaya sağ tıkladığımızda aşağıdaki gibi görünür.Bir dosyaya tag ekleyebiliyoruz.Bookmark olarak ekleyebiliyoruz.Toolsda Manage tagsa geldiğimizde farklı tagları görürüz.ADD TAG dediğimizde yeni tag(etiket) oluşturabiliriz.Kullanıcının oluşturduğu taglar silinebilir.



Bookmark penceresinde sadece belirli tagları ekranda göster diyebiliriz.

Axiomun Ief'ten farklı olan yerleri:

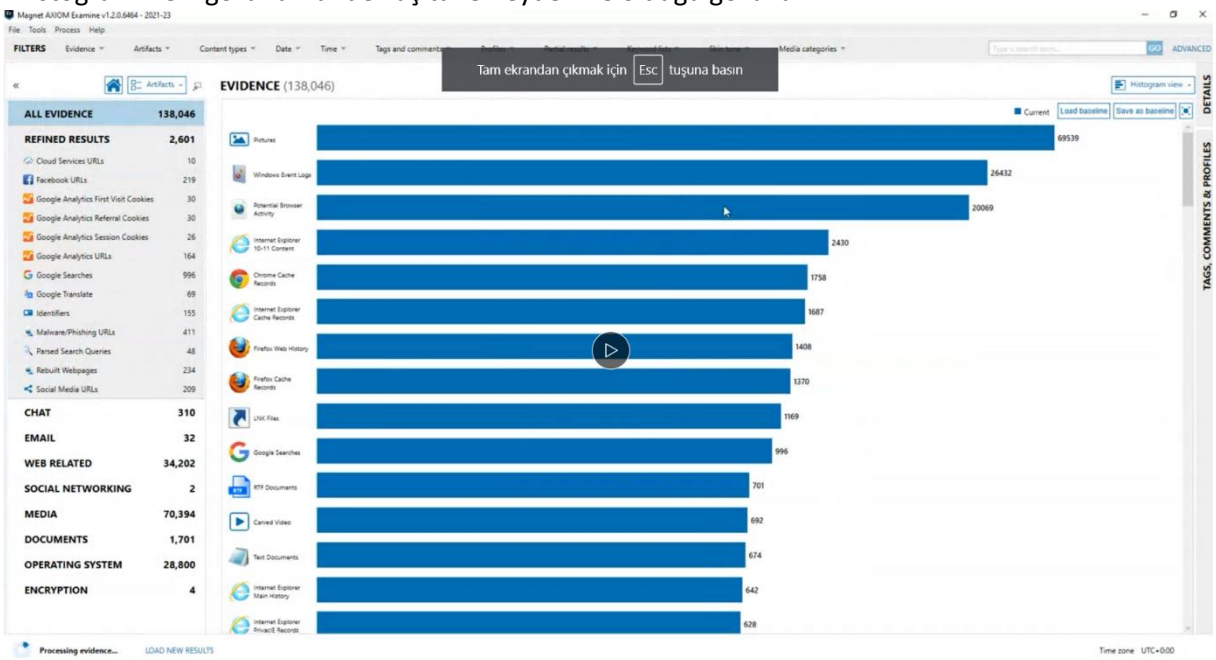
File system= Eklediğimiz imajı ya da dosyayı ya da klasörü ya da telefonu dosya sistem yapısında dizin yapısında görebiliyoruz.

Registry= SYSTEM-ControlSet001-Control-ComputerName içerisine girersek bilgisayarın adını görürüz.

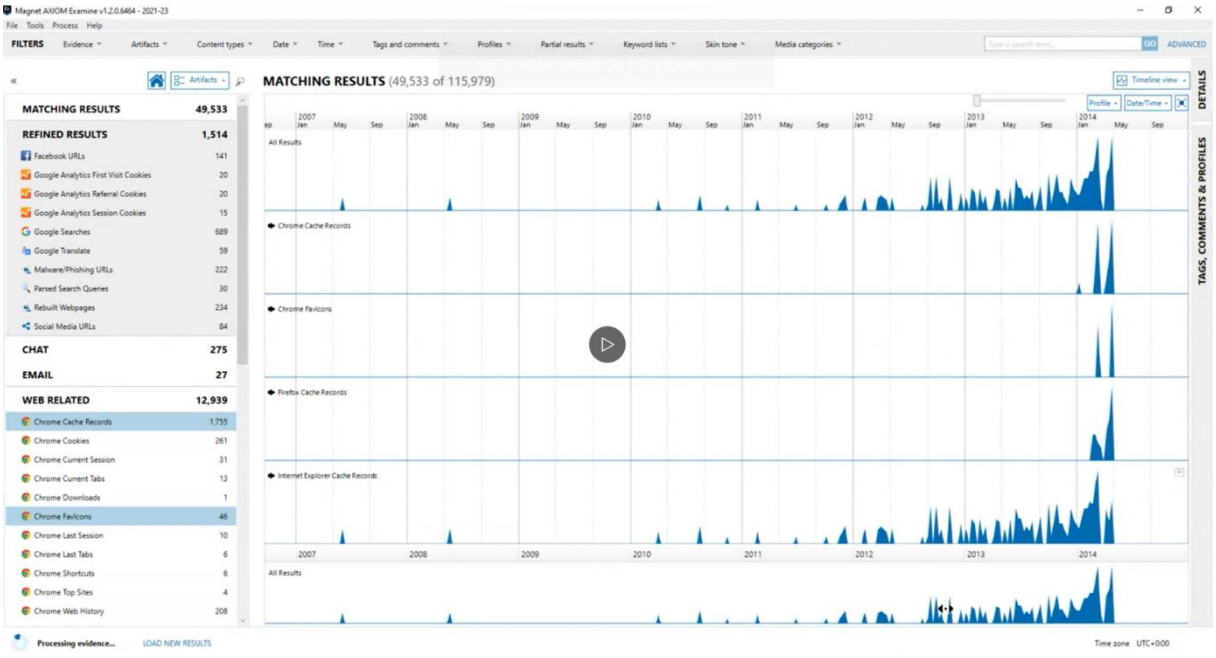
SYSTEM-ControlSet001-Control-TimeZoneInformation içerisine girersek bu bilgisayarın zaman dilimini time zone alanını görürüz.

Artifact=

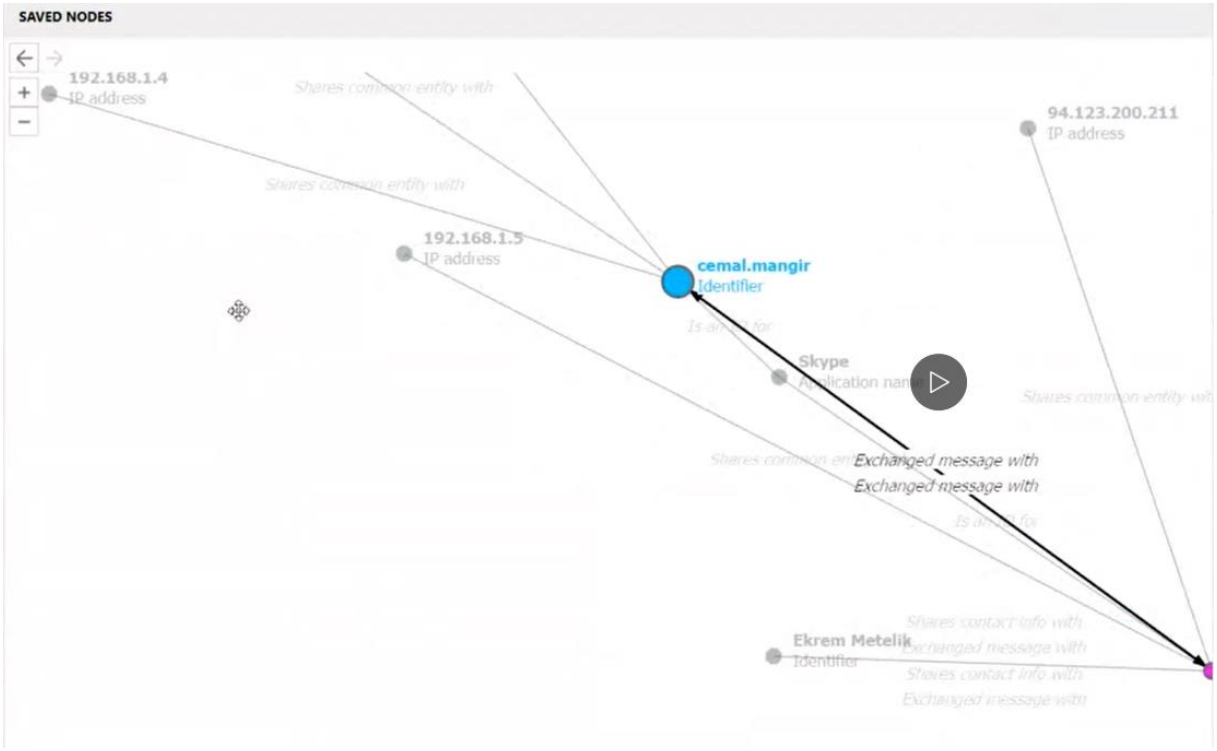
-Histogram view görünümünde kaç tane neyden ne olduğu gözükür.



-Timeline görünümünde=IEFde timeline penceresi açılıyordu burda onu söylemiyor burda diyorki ben kendi içimde timeline'ı bölümsedim.IEFdeki gibi alanları daraltıp genişletip bu alanlara zaman boyutunda ulaşabiliriz.Zaman dilimi üzerinde oluşturulan ve işlenen dosyaları ekranda görebiliyoruz.

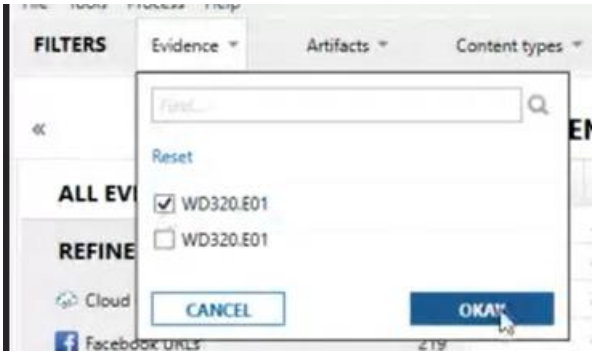


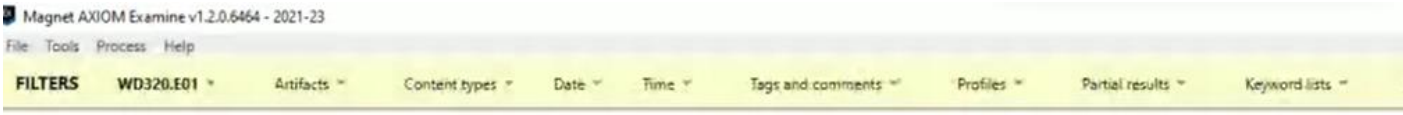
Connections= Tıklandığında nelerle ilişkilendirildiğini görürüz.Örneğin bir IP adresinin hangi uygulamalarla bağlantı kurduğunuki bu axiom için çok önemli bir özelliktir bunları tek tek bu ekranda görebiliyoruz.Örneğin bir adrese tıkladığımızda o adresle başka iletişim kurulmuş mu ne zaman kurulmuş görebiliriz.Örneğin bir urlnin web connectionsuna baktığımızda farklı uygulamalarda kullanılıp kullanılmadığını görebiliriz.Örneğin tıkladığımız ekrem.metelik başka yerde kullanılıyorsa web connectiona geldiğimizde bunları görürüz,ekrem kullanıcısı bu bilgisayarda yaptığı faaliyetleri görebiliyoruz çıkan bağlantılarda kullanılan başka bağlantı var mı görebiliyoruz.Örneğin aynı resimdeki iki farklı tür hash değerini bağlantılı görebiliriz.



*Ief'e göre filtresi kolaylaştırılmış.Sarı ekran filtre olduğunu söyler.

Evidencede hangi delil üzerinde işlem yapılmak isteniyorsa seçilir.





Artifacts=Sadece chati göster diyebiliyoruz.

*File-Create report,rapor oluşturmak için.

*Merge portable case, diyelimki iki farklı portable case oluşturduk.merge’e geldiğimizde diyorki sen portable caseleri buraya yaz ben ikisini tek bir case olarak birleştireyim.Aynı davada portable case olarak oluşturudğumuz farklı alanları birleştirebiliriz.