

Magnet IEF

İnternet aktifleri 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 ramın 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 ramın 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.

— Setup Your IEF Case Folder —

Destination Path:
E:\IEF Browse

Case Folder Name:
IEF - Dec 14 2021 141028

— Case Info —

Case Number:
1

Examiner's Name:
Sengul DOGAN

Evidence Numbers:

Source	Evidence Number (Click to edit)
Partition 1 (Microsoft NTFS, 350 MB) Sistem Ayri...	WD320
Partition 2 (Microsoft NTFS, 68.02 GB) - C:\Users...	WD320
Partition 3 (Microsoft NTFS, 229.73 GB) - C:\Use...	WD320

Choose Agency Logo (will be sized to 150x150 pixels) Clear

Notes:
Bu bir denemedir

— Keyword Searching —

☒ Enable Keyword Search Alerts Configure

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.Index yapmıyor.

Configure Keyword Search Alerts

In this section you can add keywords to alert you when data matching the keyword(s) is found during the search, either by an audible alert or by an email alert.

Keyword

Add Keyword

Keyword Options

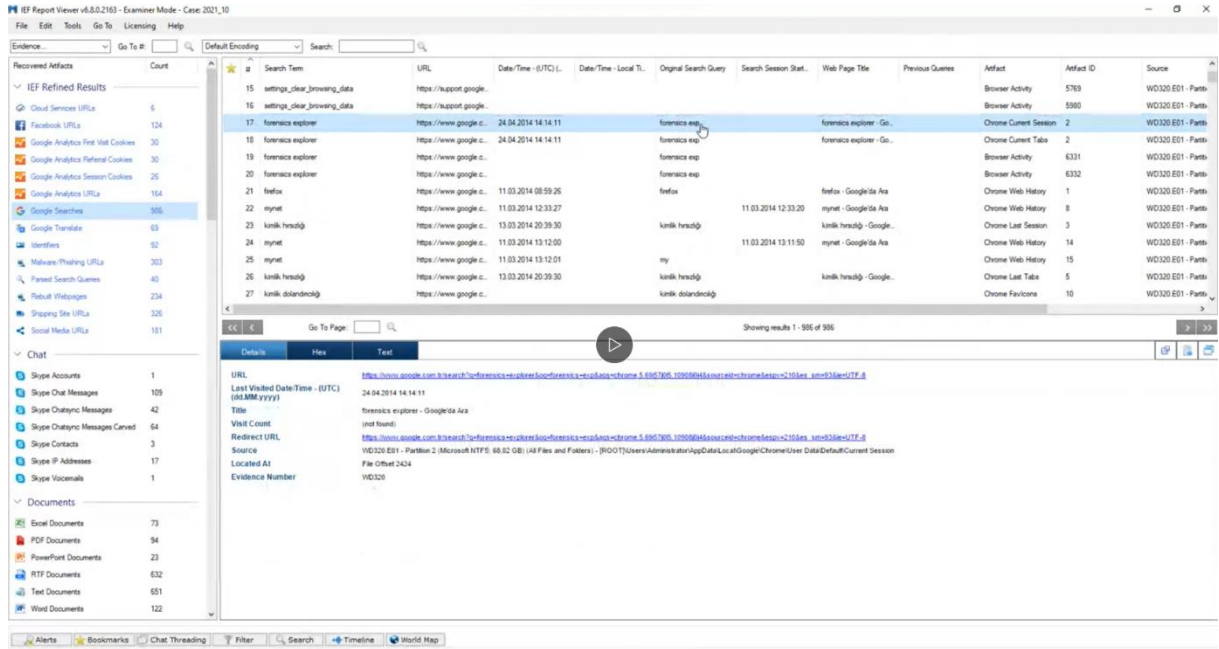
kimlik

☐ GREP ☐ Audible Alert ☐ Email Alert

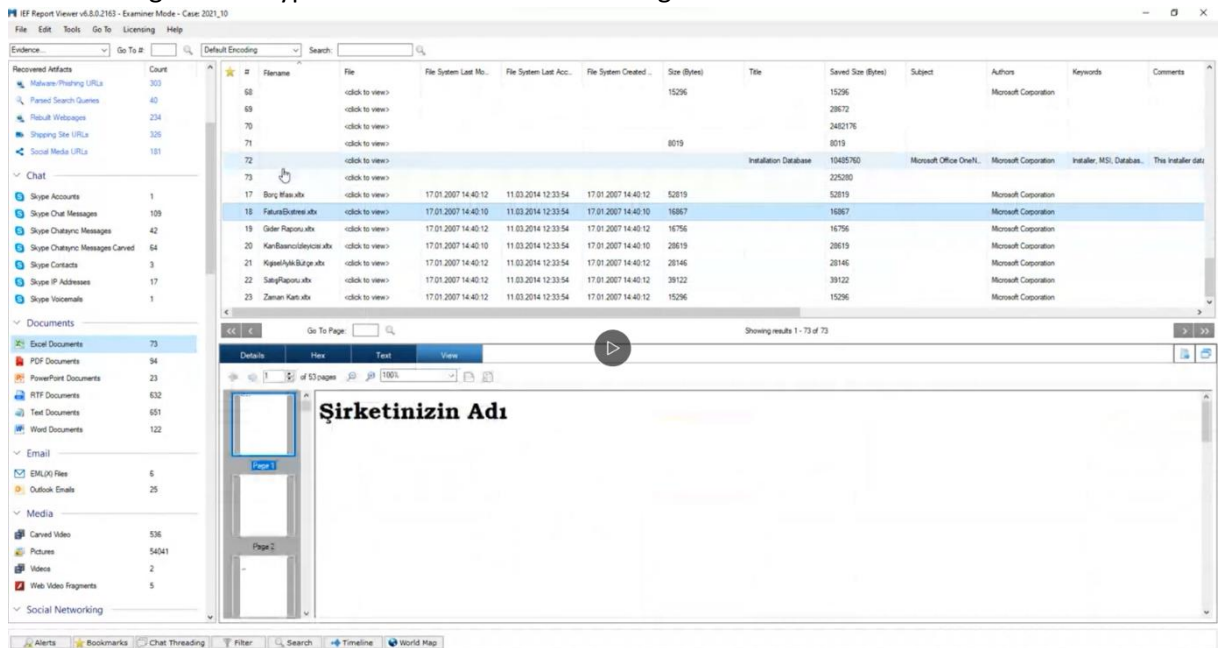
Cancel Add

Add Remove Import List Email Settings Close

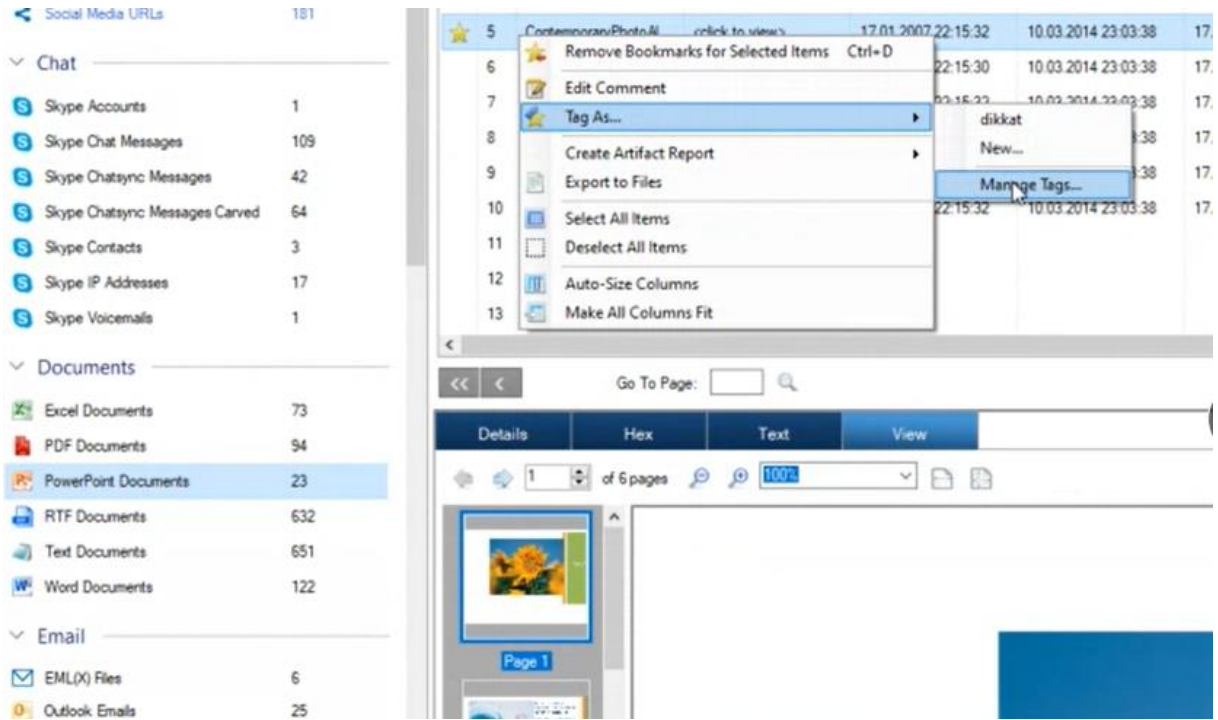
**FIND EVIDENCE denir.Examier penceresi gelir.Bulunanlar examier penceresinde sunuluyor.Proses tamamlandıktan sonra sistemimizi incelemeye başlarız.



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

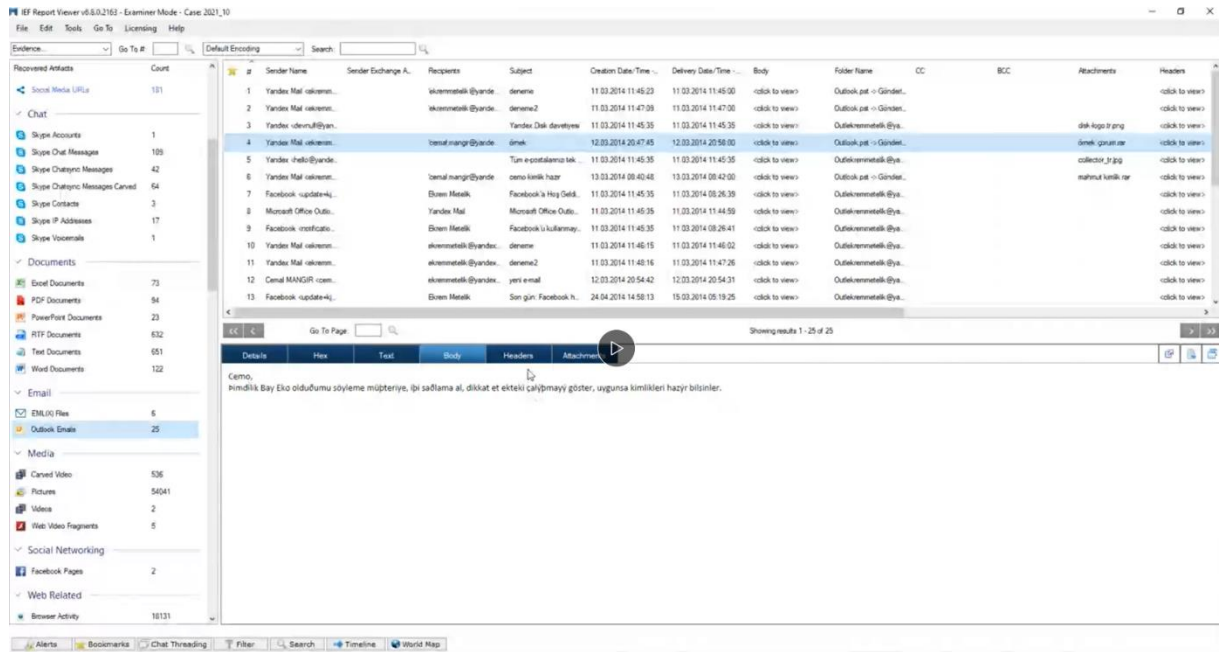


Excel Documents'de bazıları carve edilmiş ancak kurtarılabilmiş sayfalar olabilir.Yani carve edilen dosyalar açılmayabilir.Export to Files diyip dışarı aktarabiliriz.



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.

Jump Lists, girilen sayfalar,flashbellek,haricidiskler görülür.

EF Report Viewer v6.8.0.2163 - Examiner Mode - Case 2021_10

File Edit Tools Go To Licensing Help

Evidence: Go To # [] Default Encoding [] Search: []

Recovered Artifacts

Count	#	App ID	Potential App Name	Linked Path	Arguments	Volume Name	Volume Serial Number	Target File Created	Target File Last Mod.	Target File Last Acc.	Jump List Type	Dr
157	19	290532160126071	WinRAR 2.90 / 3.60 /	G:\PROGRAM	program	SINANDURMAZ	3CA96A8B	04.10.2010 19:18:45	04.03.2010 08:05:02	23.01.2011 15:39:57	Automatic	DR
83	20	7d4bca8246830a3	Control Panel (7)									
158	21	adeb5853677462a	Microsoft Office Word	C:\Users\Administrator\Documents\Kutu	adumuna d3tem...		6C4E7589	13.03.2014 20:43:08	13.03.2014 20:43:09	13.03.2014 20:43:09	Automatic	DR
34	22	adeb5853677462a	Microsoft Office Word	C:\Users\Administrator\Documents\Kutu	adumuna d3tem...		6C4E7589	13.03.2014 20:42:12	13.03.2014 20:42:12	13.03.2014 20:42:12	Automatic	DR
18	23	bc03150ea1e59e1	Foxit PDF Reader 5.4.5	C:\Users\Administrator\Desktop\Belge	isimli klasör		6C4E7589	13.03.2014 09:38:34	13.03.2014 09:38:36	13.03.2014 09:38:36	Automatic	DR
542	24	adeb5853677462a	Microsoft Office Word	C:\Users\Administrator\Desktop\Belge	isimli klasör		6C4E7589	12.03.2014 22:12:44	12.03.2014 22:12:53	12.03.2014 22:12:53	Automatic	DR
628	25	bc03150ea1e59e1	Foxit PDF Reader 5.4.5	G:\2013.02.12\Training\Avanturya	Poker Bootcamp Training Ma...	Seagule Expansion Dr...	AB0CC1A8	12.02.2013 21:20:46	26.06.2010 07:36:30	12.02.2013 21:20:46	Automatic	DR
61	26	adeb5853677462a	Microsoft Office Word	C:\Users\Administrator\Desktop\Belge	isimli klasör		6C4E7589	12.03.2014 22:11:33	12.03.2014 22:11:34	12.03.2014 22:11:33	Automatic	DR
5	27	adeb5853677462a	Microsoft Office Word	C:\Users\Administrator\Desktop\Belge	isimli klasör		6C4E7589				Automatic	DR
1	28	5fac330b3119ab	Microsoft Office Power...	G:\2013.02.12\Training\Avanturya	Poker Bootcamp Training Ma...	Seagule Expansion Dr...	AB0CC1A8	12.02.2013 21:18:44	16.04.2013 11:22:06	16.04.2013 11:22:06	Automatic	DR
169	29	25b3b550ea545a1	Internet Explorer 8 / 9	C:\Program Files (x86)\Internet Explorer	explore.exe	private	6C4E7589	13.07.2009 23:43:32	14.07.2009 01:17:29	13.07.2009 23:43:32	Custom	DR
	30	25b3b550ea545a1	Internet Explorer 8 / 9	C:\Program Files (x86)\Internet Explorer	explore.exe	neutral	6C4E7589	13.07.2009 23:43:32	14.07.2009 01:17:29	13.07.2009 23:43:32	Custom	DR
	31	5efeb51a3b2b382	C:\Windows\System32\Gating\Gating.exe		(A97AF2AA-BEF1-43C...		6C4E7589	13.07.2009 23:55:56	14.07.2009 01:39:11	13.07.2009 23:55:56	Custom	DR

Showing results 1 - 99 of 99

Details | Hex | Text

App ID: bc03150ea1e59e1
Potential App Name: Foxit PDF Reader 5.4.5
Linked Path: G:\2013.02.12\Training\Avanturya\Poker Bootcamp Training Materials\1.pdf
Arguments: (not found)
Volume Name: Seagule Expansion Drive
Volume Serial Number: AB0CC1A8
Target File Created Date/Time - (UTC) (dd.MM.yyyy): 12.02.2013 21:20:46
Target File Last Modified Date/Time - (UTC) (dd.MM.yyyy): 26.06.2010 07:36:30
Target File Last Accessed Date/Time - (UTC) (dd.MM.yyyy): 12.02.2013 21:20:46
Jump List Type: Automatic
Drive Type: DRIVE_FIXED
Target Hardware Name: jesus-ahpkeyay
Target MAC Address: 54-c4-49-fb-86-08
Target File Size (bytes): 217054
Last Access Date/Time - (UTC) (dd.MM.yyyy): 11.03.2014 13:04:19
Accessed Count: 1

Alerts | Bookmarks | Chat Threading | Filter | Search | Timeline | World Map

EF Report Viewer v6.8.0.2163 - Examiner Mode - Case 2021_10

File Edit Tools Go To Licensing Help

Evidence: Go To # [] Default Encoding [] Search: []

Recovered Artifacts

Count	#	Adapter Name	MAC Address	Description	DHCP Enabled?	IPv4 Address	IPv4 Subnet Mask	Default Gateway(s)	DNS Server(s)	DNS Domain	DHCP IPv4 Address
157	1	Yeni Ağ Bağlantısı		Atheros AR8131 PCI-E Gigabit Ethernet Controller (NDIS 6.20)	Yes						0.0.0.0
83	2	Bluetooth Ağ Bağlantısı		Bluetooth-Ağ Bağlantısı (Kısmi Alan Ağı)	Yes						0.0.0.0
158	3	Kablolu Ağ Bağlantısı		Atheros AR5285 Wireless Network Adapter	Yes						192.168.1.5
34	4	Yeni Ağ Bağlantısı		Atheros AR8131 PCI-E Gigabit Ethernet Controller (NDIS 6.20)	Yes						0.0.0.0
18	5	Bluetooth Ağ Bağlantısı		Bluetooth-Ağ Bağlantısı (Kısmi Alan Ağı)	Yes						0.0.0.0
642	6	Kablolu Ağ Bağlantısı		Atheros AR5285 Wireless Network Adapter	Yes						192.168.1.5

Showing results 1 - 6 of 6

Details | Hex | Text

Adapter Name: Kablolu Ağ Bağlantısı
MAC Address: (not found)
Description: Atheros AR5285 Wireless Network Adapter
DHCP Enabled?: Yes
IPv4 Address: (not found)
IPv4 Subnet Mask: (not found)
Default Gateway(s): (not found)
DNS Server(s): (not found)
DNS Domain: (not found)
DHCP IPv4 Address: 192.168.1.5
DHCP IPv4 Subnet Mask: 255.255.255.0
DHCP Default Gateway(s): 192.168.1.1
DHCP DNS Server(s): 192.168.1.1
DHCP DNS Domain: Home
Lease Obtained Date/Time - (UTC) (dd.MM.yyyy): 24.04.2014 20:32:20
Lease Expires Date/Time - (UTC) (dd.MM.yyyy): 25.04.2014 20:32:20

Alerts | Bookmarks | Chat Threading | Filter | Search | Timeline | World Map

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.

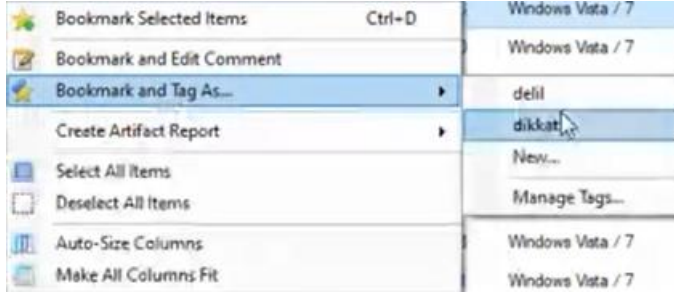
USB Devices, usb bilgilerini görebiliyoruz.

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.

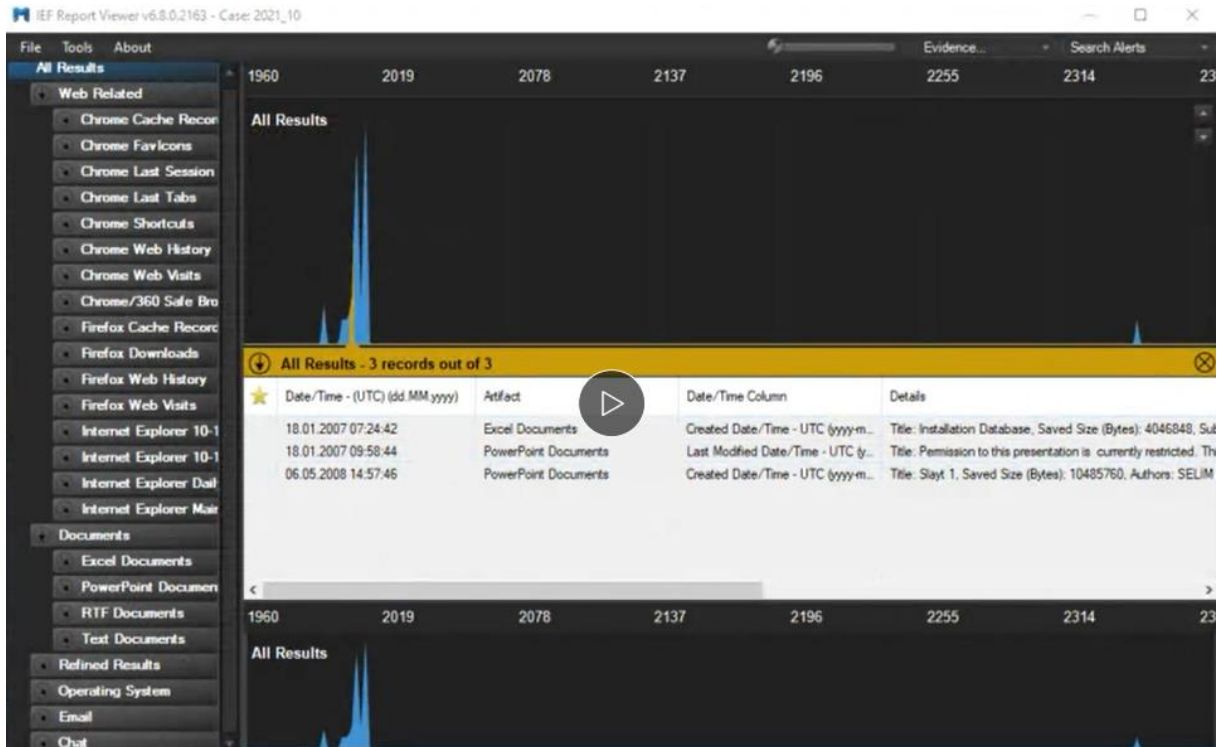
Windows Prefetch Files, windows7 kullanılarak öncelikli çalıştırılan dosyalar gözükür.



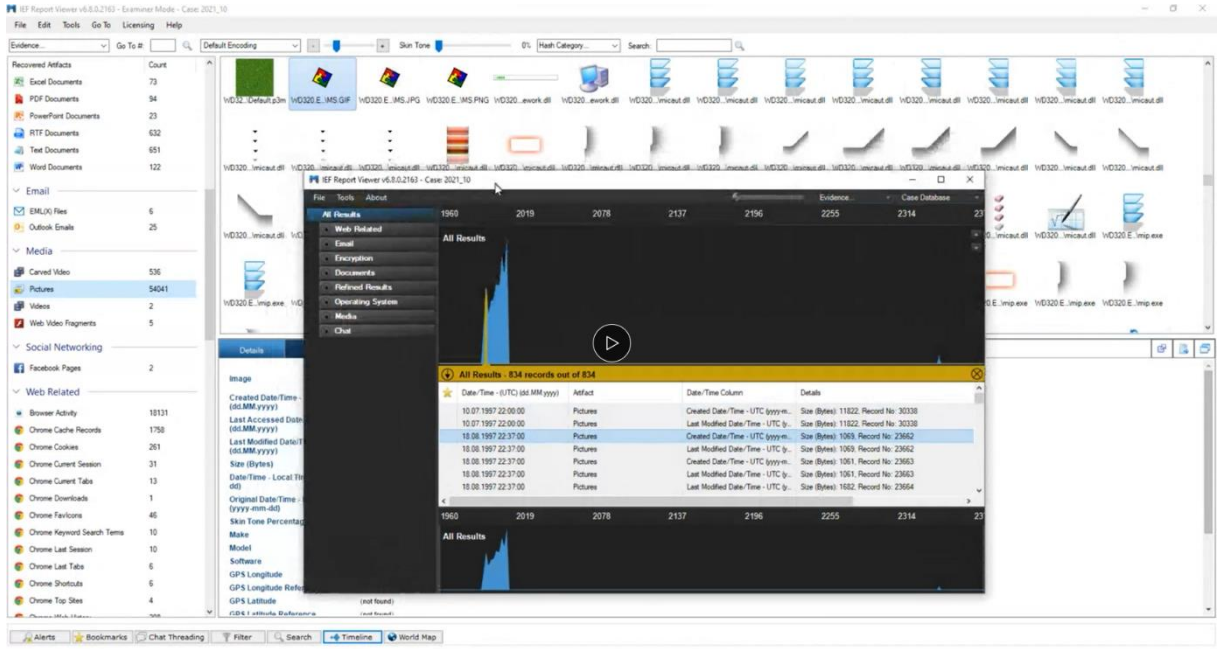
Bookmark and Edit Comment'e tıklandığında dosyaya comment yazılır. Seçilen dosya bookmark olarak eklenir ve comment(yorum) eklenir.



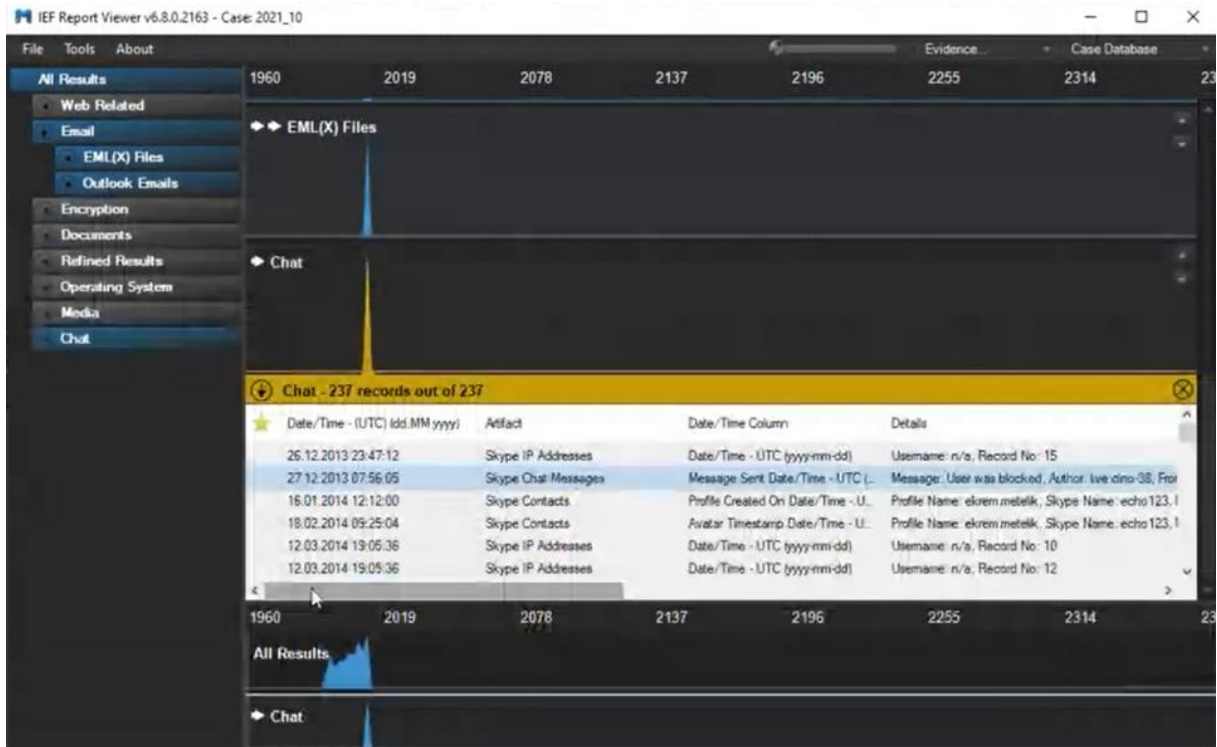
☺Alerts sekmesine tıklanıldığında aranan kelimelerin sonuçları görülebilir. Timeline tıklanıldığında bu kelimelerin zaman dağılımlarını görebiliriz.



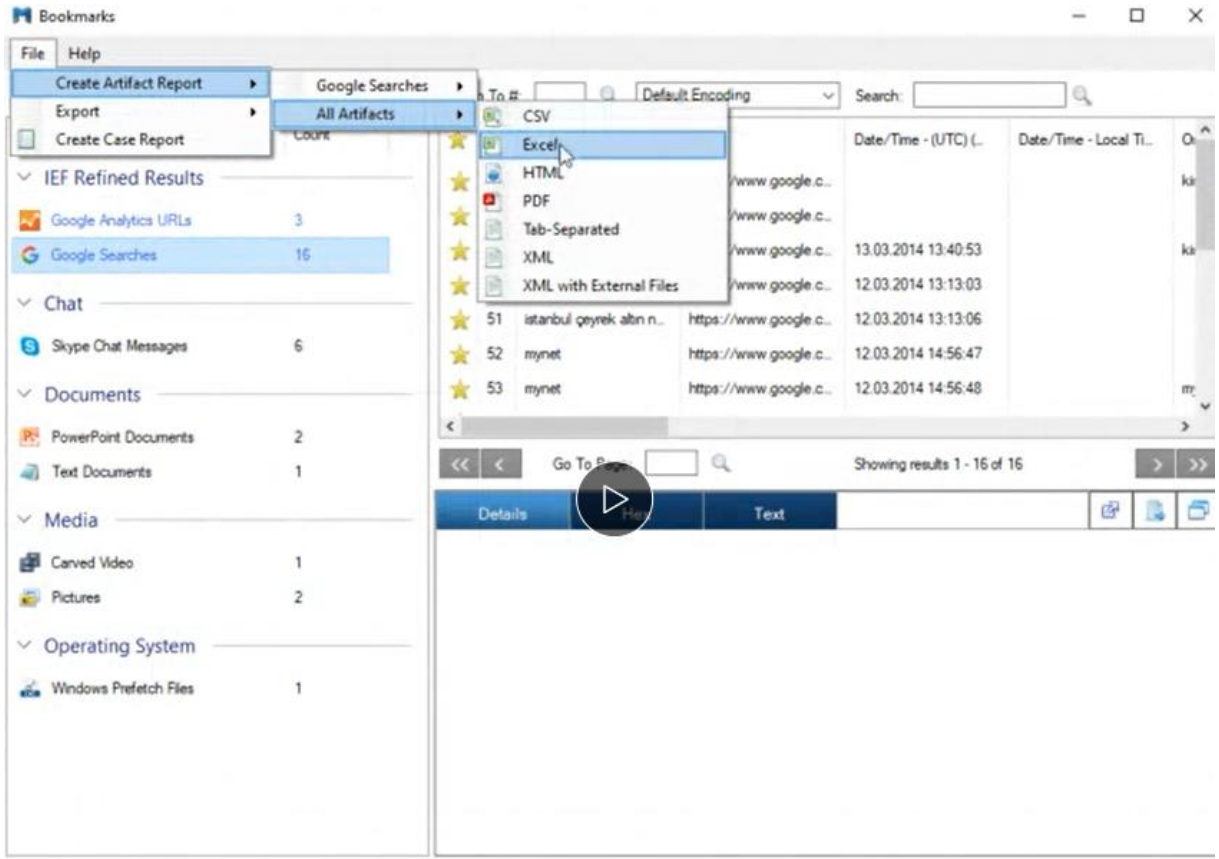
☺Timeline sekmesine tıklanıldığında tüm dosyaları zaman dağılımında görebiliriz. Tıklandığımız dosyanın kendisini katagorisinde gösterir.



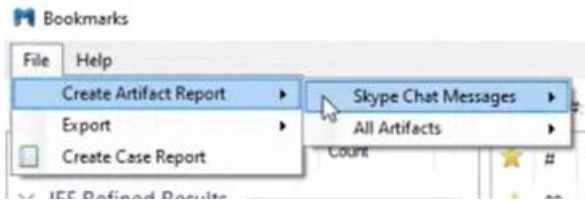
Alt tarafta istediğimiz alana getirip üst tarafta yakınlaştırma işlemi gerçekleştiriliyor,gün bazında saat bazında görmek için.Lazım olan zamana tıklayıp yapılan hareketleri görebiliriz.



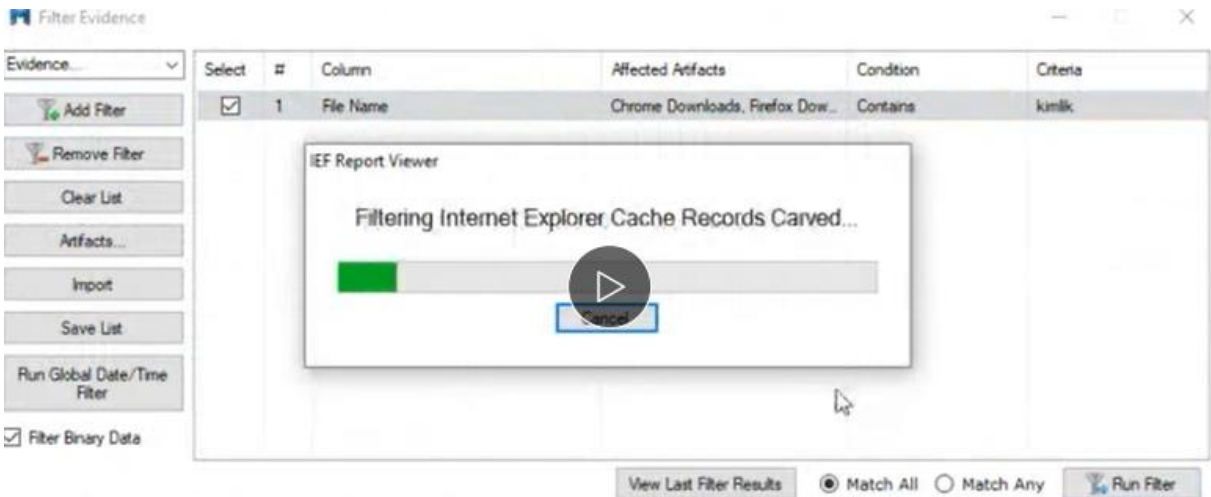
😊Bookmarks Bizim için delil olan nesneleri Create Artifact Report diyip All Artifacts'ı(hangi alanı istiyorsak) seçip istediğimiz formatta rapor oluşturulur.



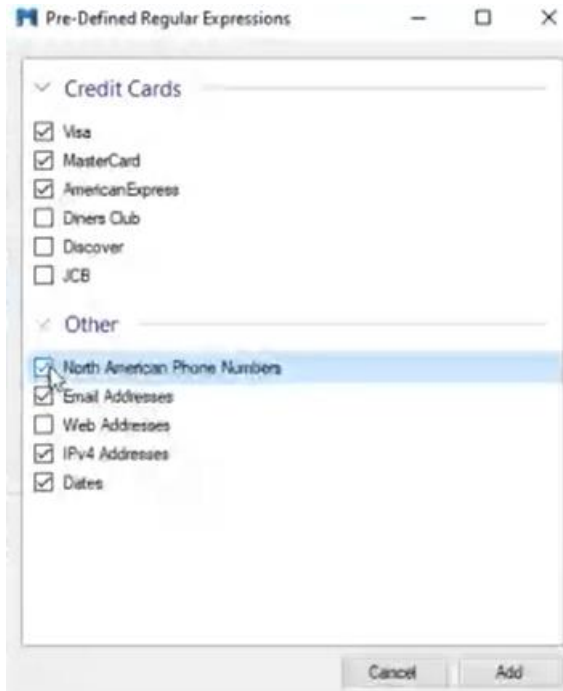
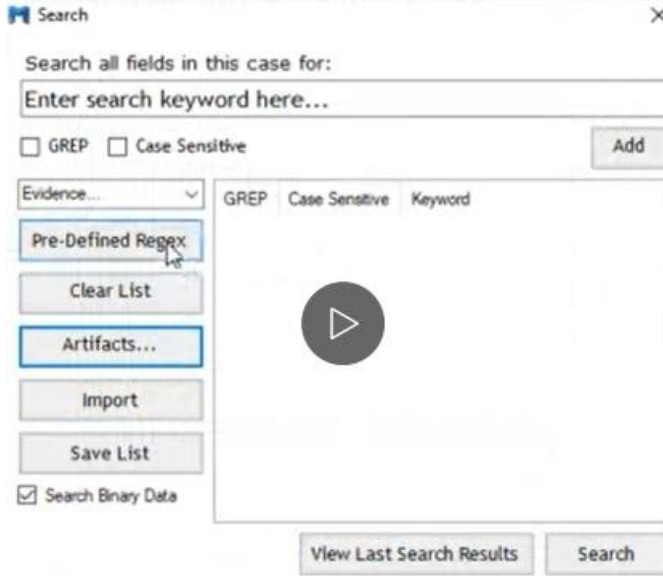
Timeline



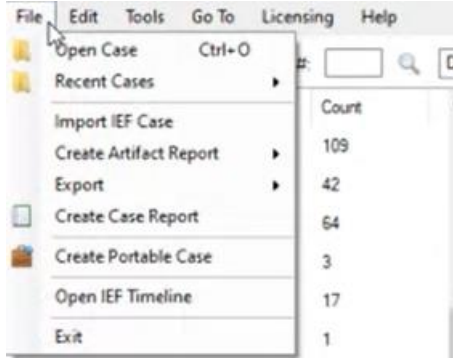
☺Filter, istediğimiz yerlerde filtreleme yaparak kimlik geçen yerleri bulur ekrana getirir. Action filtre anlamında bunun daha geliştirilmiş şekli.



☺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 aygıt),mobile(mobil tabanlı bir aygıt), 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.



ACQUIRE 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.

MOBILE SELECT EVIDENCE SOURCE



ANDROID



IOS



WINDOWS PHONE



KINDLE FIRE



MEDIA DEVICE (MTP)

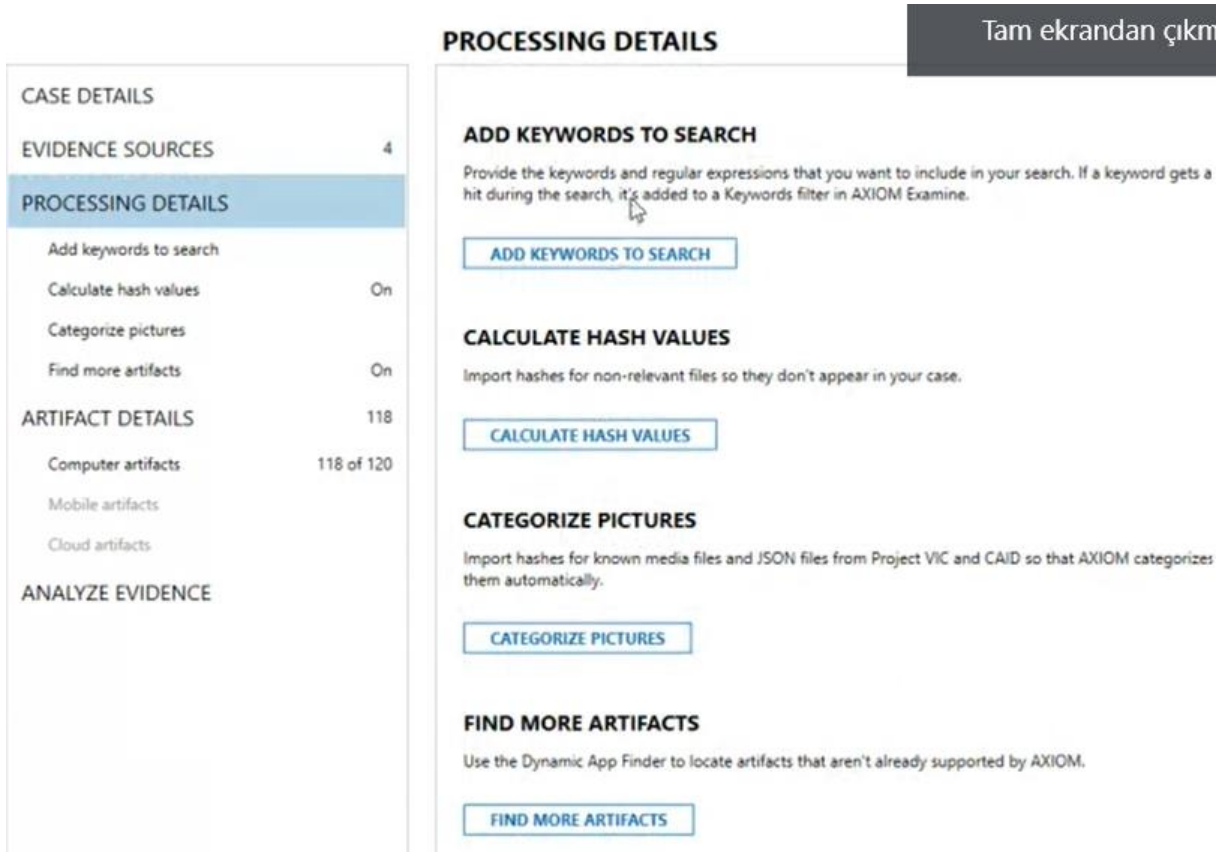
*Computerı seçip imaj ekliyoruz.İncelemek istediğimiz patitionları seçiyoruz.Sonrasında aşağıda gösterildiği gibi hangi patitionda ne tür inceleme yapılacağı seçilir.

COMPUTER SELECT SEARCH TYPE

Source location	Search type
<input checked="" type="checkbox"/> WD320.E01 - Partition 1 (Microsoft NTFS, 350 MB) Sistem Ayrıldı	Quick
pagefile.sys / swapfile.sys	
\$LogFile	
\$MFT	
Common areas	
<input checked="" type="checkbox"/> WD320.E01 - Partition 2 (Microsoft NTFS, 68.02 GB)	Full
pagefile.sys / swapfile.sys	
\$LogFile	
\$MFT	
All files and folders	
Volume Shadow Copy	
Unallocated space	
File slack space	
hiberfil.sys	
Uninitialized file area	
<input checked="" type="checkbox"/> WD320.E01 - Partition 3 (Microsoft NTFS, 229.73 GB)	Full
pagefile.sys / swapfile.sys	

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 ekranı da 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 işlemi 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 mbin 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.

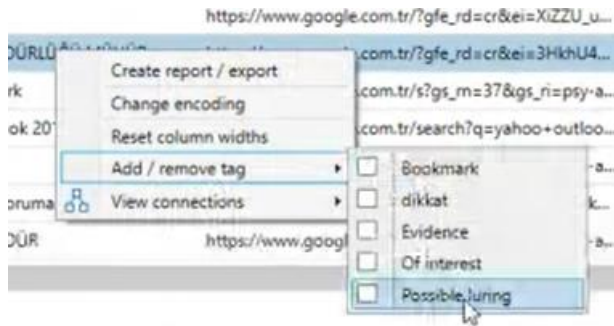
-MD5 formatına ya da SHA1 formatına göre pictureler katagorize edilebiliyor.Hash değerleri için hesaplattığımız hash formatlarına göre belli dosyalar ekleyip resimlerin gruplandırılması işlemini gerçekleştirebiliyoruz,hash değerine göre bu işlemi yapıyoruz.

-Dinamik bir şekilde daha fazla artifacts bulayım diyor.Go to artifact details denildiğinde imajımız bilgisayar olduğu için bilgisayar artifactlarını 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 1e7'ten farklı olan yerleri:

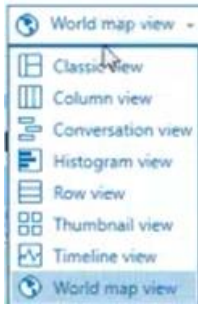


File system= Eklediğimiz imajı ya da dosyayı ya da klasörü ya da telefonu dosya sistem yapısında dizin yapısında görebiliyoruz.

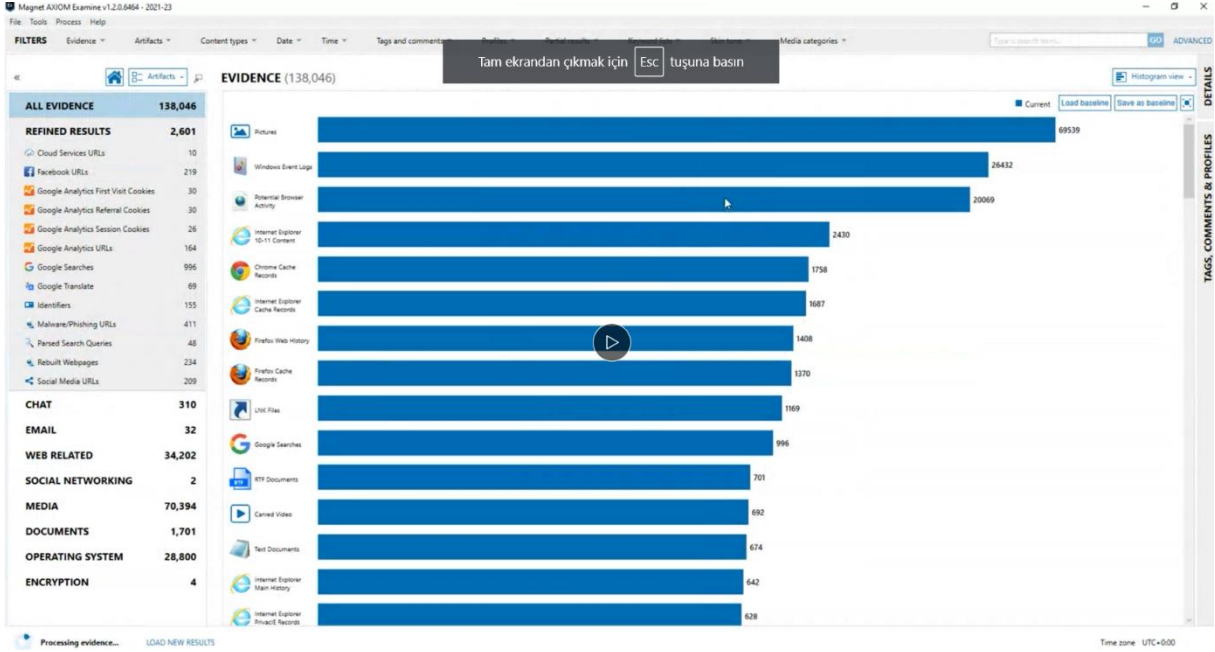
Registry= SYSTEM-ControlSet001-Control-ComputerName içerisine girersek bilgisayarın adını görürüz.

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

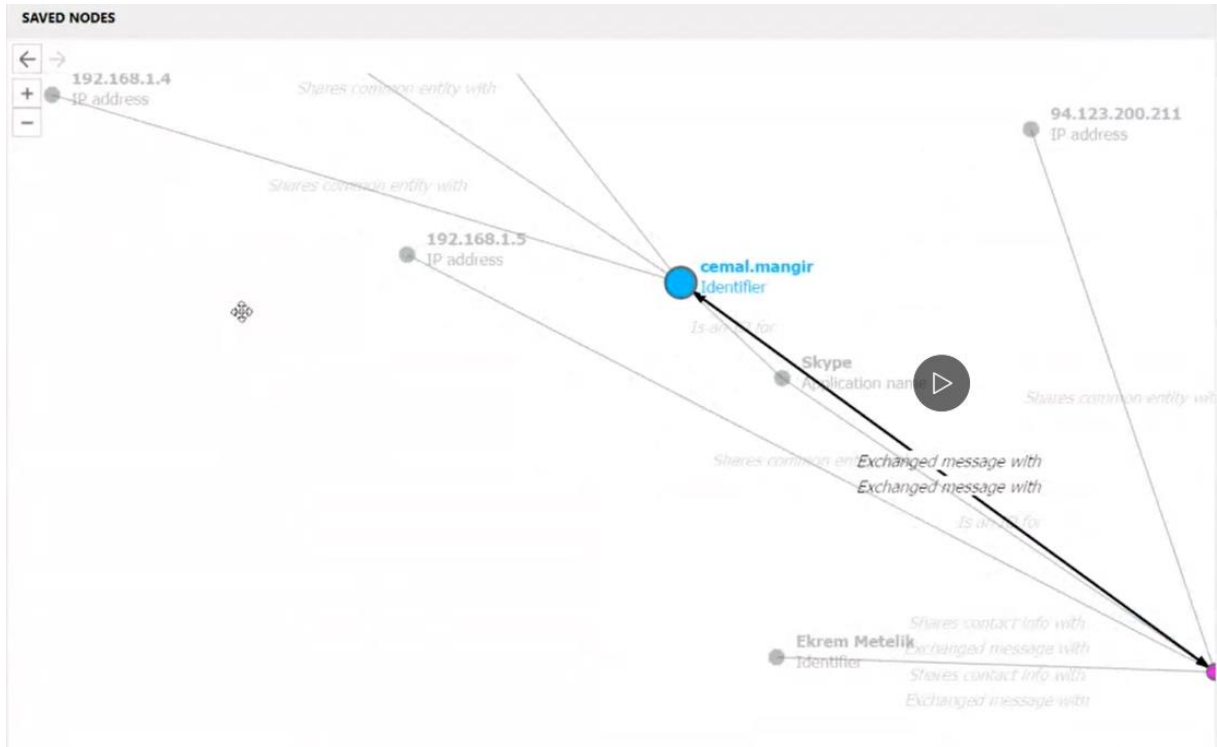
Artifact=



-Histogram view görünümünde kaç tane neyden ne olduğu gözükür.

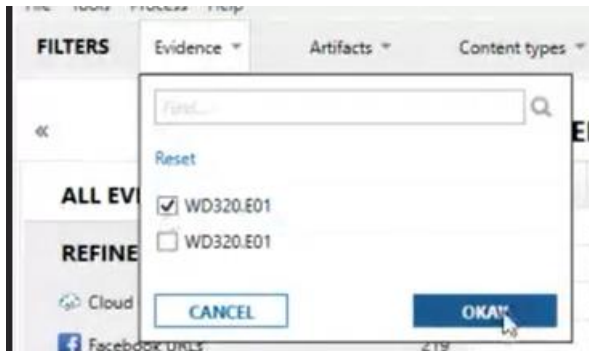


-Timeline görünümünde=IEFde timeline penceresi açılıyordu burda onu söylemiyor burda diyorki ben kendi içimde timeline'ı bölümsedim.IEFdeki gibi alanları daraltıp genişletip bu alanlara zaman boyutunda ulaşabiliriz.Zaman dilimi üzerinde oluşturulan ve işlenen dosyaları ekranda görebiliyoruz.



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

Evidencede hangi delil üzerinde işlem yapılmak isteniyorsa seçilir.



Magnet AXIOM Examine v1.2.0.6464 - 2021-23

File Tools Process Help

FILTERS WD320.E01 Artifacts Content types Date Time Tags and comments Profiles Partial results Keyword lists

Artifacts=Sadece chati göster diyebiliyoruz.

Magnet AXIOM Examine v1.2.0.6464 - 2021-23

File Tools Process Help

FILTERS Evidence Artifacts Pictures, video, audio Date Time Tags and comments Profiles Partial results Keyword lists Skin tone Media categories

*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 oluşturduğumuz farklı alanları birleştirebiliriz.