****

**T.C**

**FIRAT ÜNİVERSİTESİ**

**TEKNOLOJİ FAKÜLTESİ**

**ADLİ BİLİŞİM MÜHENDİSLİĞİ BÖLÜMÜ**

**X-Ways**

**Kullanma Klavuzu**

**DANIŞMAN HAZIRLAYAN**

Doç. Dr. Şengül DOĞAN Mazlum BAYDAR-16525006

**ELAZIĞ-2019**

İÇİNDEKİLER

[1.X-Ways Programının Yüklenmesi 1](#_Toc28214337)

[2.X-Ways Programının Çalıştırılması 1](#_Toc28214338)

[3. Yeni dava dosyası oluşturulması 1](#_Toc28214339)

[4. İncelemeye Başlama 4](#_Toc28214340)

[5. Güvenlik Ayarı 6](#_Toc28214341)

[6. Dosya Kopyalama Ve Kurtarma 6](#_Toc28214342)

[7. Dosya kurtarma 8](#_Toc28214343)

[8. General Options bölümü 9](#_Toc28214344)

[9. Notation (işaret ve rakamlarla gösterme sistemi) 11](#_Toc28214345)

[10. Program başlangıç seçenekleri 11](#_Toc28214346)

[11. Display time zone - Zaman Dilimi Ayarlama 12](#_Toc28214347)

[12. Konfigürasyon Ayarları 12](#_Toc28214348)

[13. Evidence Object Açıklamaları 13](#_Toc28214349)

[14. Program Arayüzü 13](#_Toc28214350)

[15. Rapor Oluşturma 14](#_Toc28214351)

[16. Rapor dosyasına veri ekleme 16](#_Toc28214352)

[17. Dosya Özellikleri Listesi Oluşturmak-1 17](#_Toc28214353)

[18. Dosya Özellikleri Listesi Oluşturmak -2 18](#_Toc28214354)

[19. Case Data bölümü 18](#_Toc28214355)

[20. Bellek İmajı Alma Bilgileri 18](#_Toc28214356)

[21. X-Ways ile Bellek İmajı Alma 19](#_Toc28214357)

[22. Disk Klonlama 20](#_Toc28214358)

[23.Program Bilgileri 20](#_Toc28214359)

[24. Directory Browser Options, Filters (Dosya Filtreleme) 21](#_Toc28214360)

[25. Dosya İsmine Göre Dosya Filtreleme 23](#_Toc28214361)

[26. Dosya Boyutuna Göre Filtreleme 24](#_Toc28214362)

[27. Yeni Dosya Türü Ekleme 24](#_Toc28214363)

[28. İçinde Geçen Kelimeye Göre Dosya Filtreleme 24](#_Toc28214364)

[29. Simultaneous Search Menü Açıklaması 25](#_Toc28214365)

[30. Resim Dosyasının Pikseline Göre Filtreleme 26](#_Toc28214366)

[31. Refine Volume Snapshot 26](#_Toc28214367)

[32. Compute hash – Dosya Hash Değeri Hesaplama 27](#_Toc28214368)

[33. Compute hash –Hash Değeri Karşılaştırma 27](#_Toc28214369)

[34. Skin tone and b&w detection in Picture 28](#_Toc28214370)

[35. File header signature search (Dosya başlığına Göre Arama) 28](#_Toc28214371)

[36. Şifreli Dosyaları Bulma 29](#_Toc28214372)

[37. Hash’leri Aynı Olan Dosyaları Ayırma 29](#_Toc28214373)

[38. Dosya Gizleme 30](#_Toc28214374)

[39. Dosya Seçme (Tag); 30](#_Toc28214375)

[40.Dosyaların metadata özelliklerini inceleme; 31](#_Toc28214376)

[41. Registry kayıtları 32](#_Toc28214377)

[42. İnternet Kayıtlarını İncelemek 35](#_Toc28214378)

[43. EMail Kayıtlarını İncelemek; 36](#_Toc28214379)

[44. Silinmiş dosyaları kurtarmak; 36](#_Toc28214380)

[45. Mevcut Dosyaları Kopyalamak; 37](#_Toc28214381)

[46. Sistem dosya sayıları 37](#_Toc28214382)

[47. Sistem İnceleme 37](#_Toc28214383)

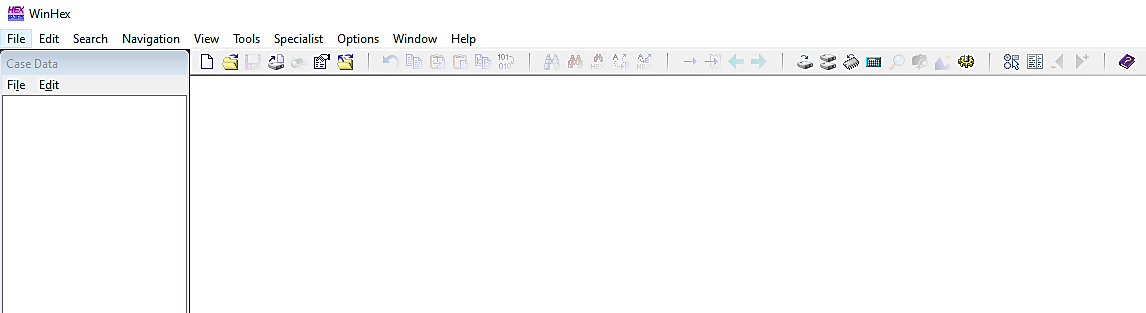
# 1.X-Ways Programının Yüklenmesi

X-Ways program klasörü içerisindeki setup.exe dosyası ile program bilgisayarımıza yüklenir.Program default ayar olarak genellikle C sürücü içerisindeki program files klasörünün içerisine yüklenir. Eğer başka bir sürücüye yüklenmek istenirse kurulum sırasında hedef sürücü değiştirilmelidir. Program boyutu 80 MB civarında olup kısa sürede yüklenecektir.

X-Ways vasıtasıyla yapılabilecek işlemler,

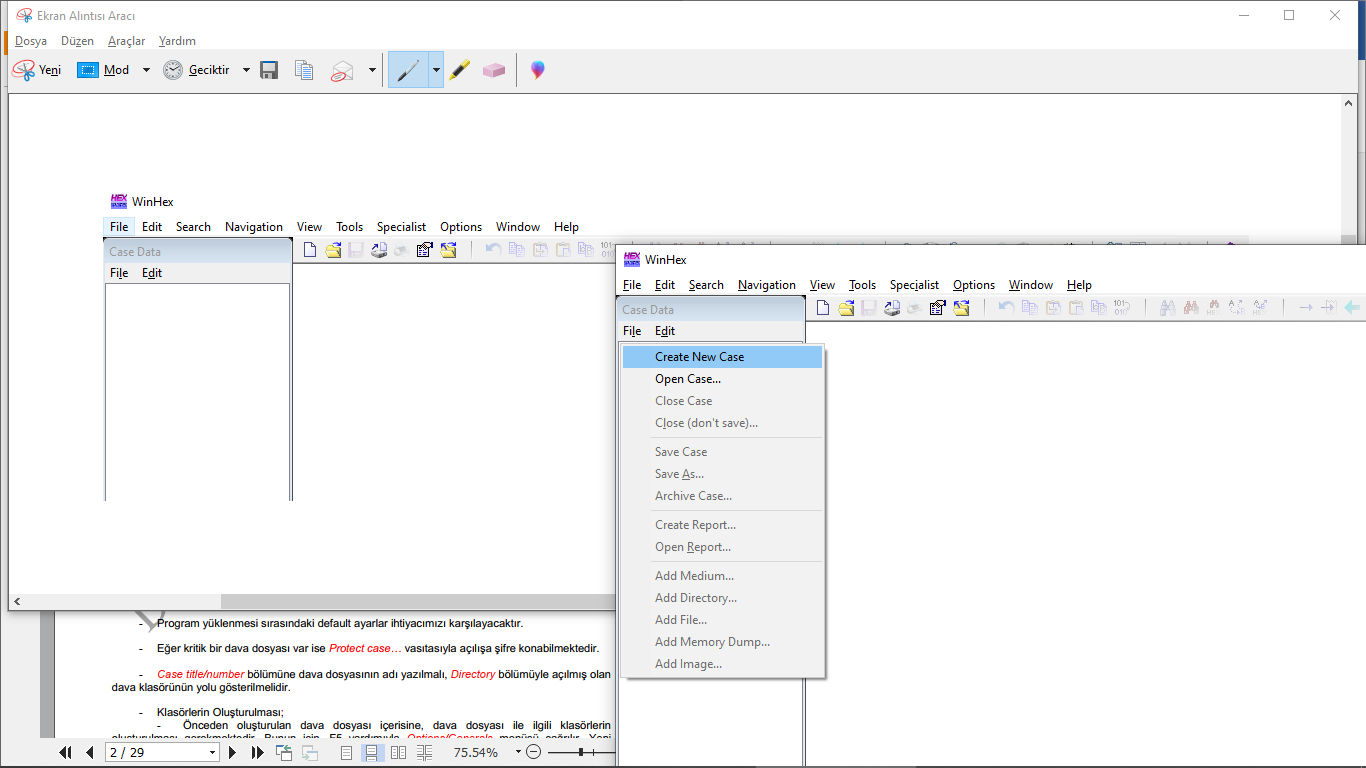
* İşletim sistemi ve dosyalar hakkında bilgi elde etme,
* Mevcut dosya ve dizinlerin kopyalanması,
* Silinen verilerin çıkartılması,
* Dosya kurtarması yapılması,
* Mail kayıtlarına ulaşılması,
* Kontak kişilerinin çıkartılması,
* İnternet kayıtlarının çıkartılması,
* Kullanıcı kayıtlarının çıkartılması,
* Gömülü nesnelerin çıkartılması ile,
* Sabit ve USB bellek ile CD/DVD’lerin imajlarının alınması mümkündür.

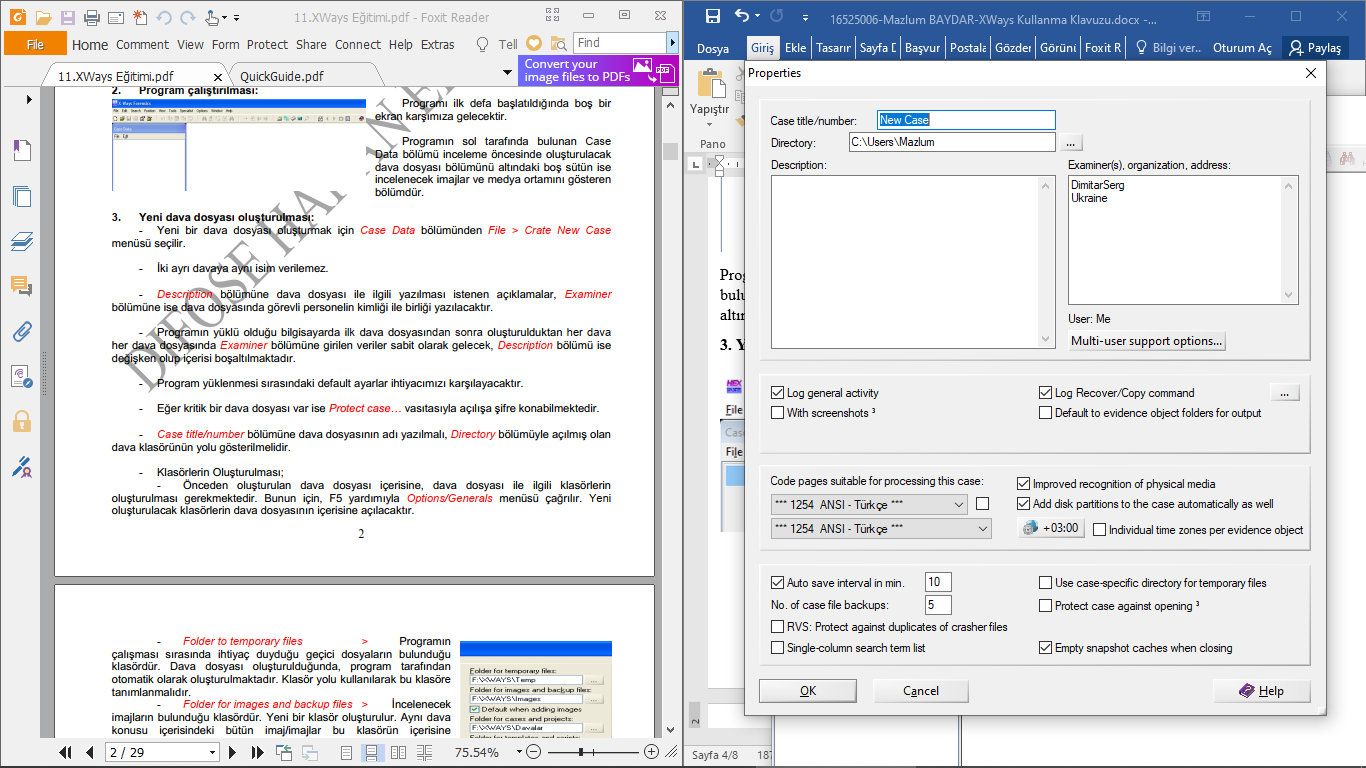
# 2.X-Ways Programının Çalıştırılması



Programı ilk defa başlatıldığında boş bir ekran karşımıza gelecektir. Programın sol tarafında bulunan Case Data bölümü inceleme öncesinde oluşturulacak dava dosyası bölümünü altındaki boş sütün ise incelenecek imajlar ve medya ortamını gösteren bölümdür.

# 3. Yeni dava dosyası oluşturulması

Yeni bir dava dosyası oluşturmak için **Case Data** bölümünden **File > Crate New Case** menüsü seçilir.

**Case title/number:** Davaya vericek isim

**Directory:** Oluşturulacak dava dosyasının diskimizde nereye kayıt edileceğini belirtiyoruz.

**Description:**Dava ile ilgili alınacak notlar vs bilgilerin yazıldığı alandır.

**Examiner(s),organization,address:** Davayı İnceleyen kişinin isimi adresi, girildiği alan.

**Multi-user support options:** Birden fazla kullanıcının seçilme için detaylı ayarlamalarının yapıldığı alandır.

**Log general activity**: Log genel etkinliği log kayıtların alınmasını sağlayan seçenektir.

**Log recovery/copy command:**Log kayıtlarını kurtarma / kopyalama komutu

**Default to evidence object folders for output:** varsayılan çıktı için nesne klasörlerini kanıtlama seçeneği

**Code pages suitable for processing this case:**Bu kısım kullanılan dil ,time zone zaman bilgisi gibi bilgilerin olduğu alandır.

**Auto save interval in minimum:** minimum otomatik kaydetme aralığıdır bir davayı kaç kez kayıt edeceğini belirler.

**No. of case file backups:** Oluşturulan vaka dosyası yedeklerinin sayısını belirleme.

**Use case-specific directory for temporary files:** Geçici dosyalar için duruma özel dizini kullanma

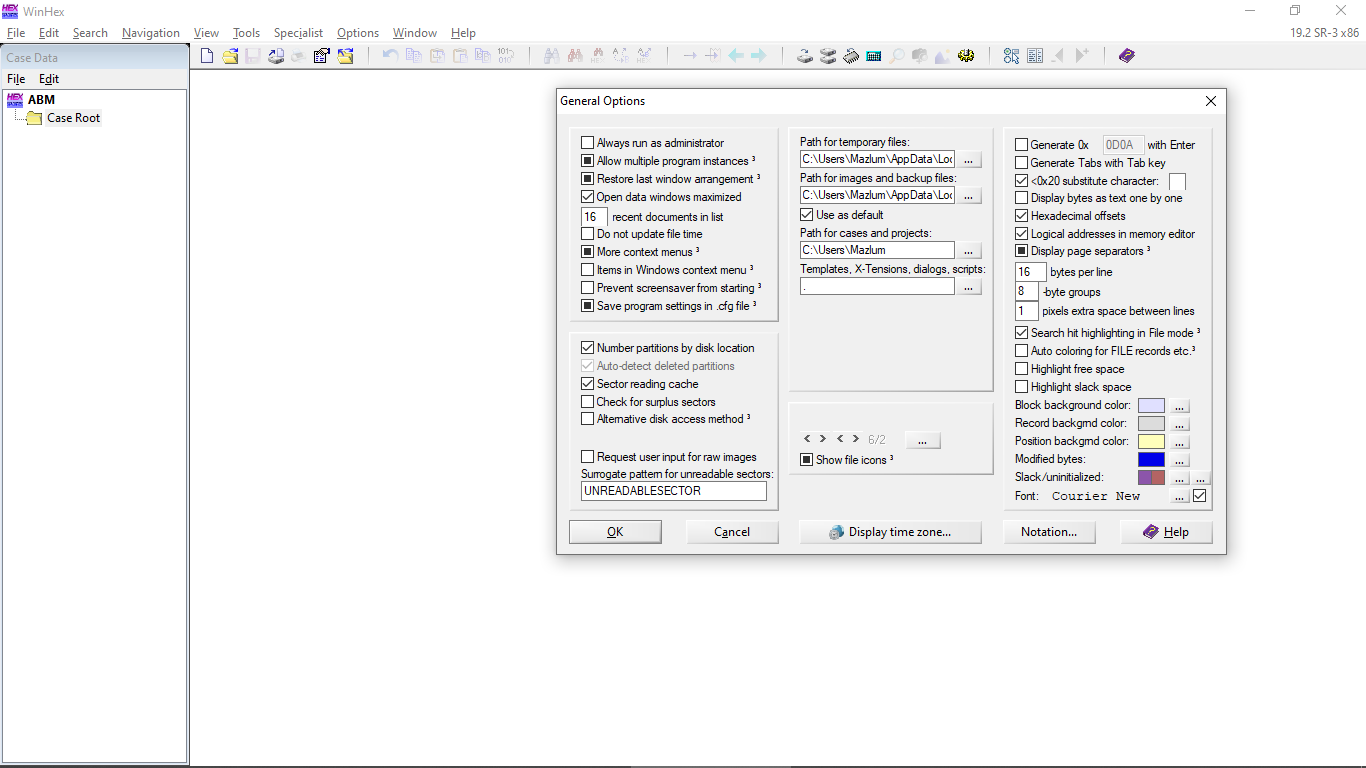
**Protect case against opening:** Davayı açılmalara karşı korumak için şifre koyma alanıdır.

**Empty snapshot catches when closing:** Davayı kapatırken anlık görüntü yakalansınmı seçeneğidir.

**RVS: Protect against duplicates of crasher files:** RVS: Silginen dosyalarının kopyalarına karşı koruma

**Single column search term list:** Tek sütun da arama terimi listesi seçeneği

- Klasörlerin Oluşturulması;  
Önceden oluşturulan dava dosyası içerisine, dava dosyası ile ilgili klasörlerin oluşturulması gerekmektedir. Bunun için, F5 yardımıyla **Options/Generals** menüsü çağrılır. Yeni oluşturulacak klasörlerin dava dosyasının içerisine açılacaktır.

**Path for temporary files:** Programın çalışması sırasında ihtiyaç duyduğu geçici dosyaların bulunduğu klasördür. Dava dosyası oluşturulduğunda, program tarafından otomatik olarak oluşturulmaktadır. Klasör yolu kullanılarak bu klasöre tanımlanmalıdır.

**Path for images and backup files:** İncelenecek imajların bulunduğu klasördür. Yeni bir klasör oluşturulur. Aynı dava konusu içerisindeki bütün imaj/imajlar bu klasörün içerisine konulacaktır. Bu menü altında bulunan **Use as default** menüsünün seçili olması, kullanıcının programa imaj yüklemek için *Case Data> File > Add image…* menüsü açıldığında, kullanıcıyı önceden oluşturulmuş olan imajlar klasörüne yönlendirecektir.

**Path for cases and project :** Öndecen oluşturulan dava dosyası veya proje klasörüne yönlendirilir.

**Templates,X-Tensions,dialogs,scripts**:Dava dosyası içerisinde scripts isimli yeni bir klasör oluşturulur.

# 4. İncelemeye Başlama

Dava dosyasına imaj ***Case Data > File > Add image*** menüsü kullanılarak yapılacaktır. Bu menü, kullanıcıyı daha önce oluşturulmuş olan imajlar klasörüne yönlendirecektir. Birden fazla imajı aynı anda eklemek mümkündür.

İmajlar programa yüklendikten sonra, program imajları inceleyerek kendisi her imaj için bir veri tabanı (snapshot) oluşturacaktır. Bu sayede yapılacak işlem hızı artacaktır.

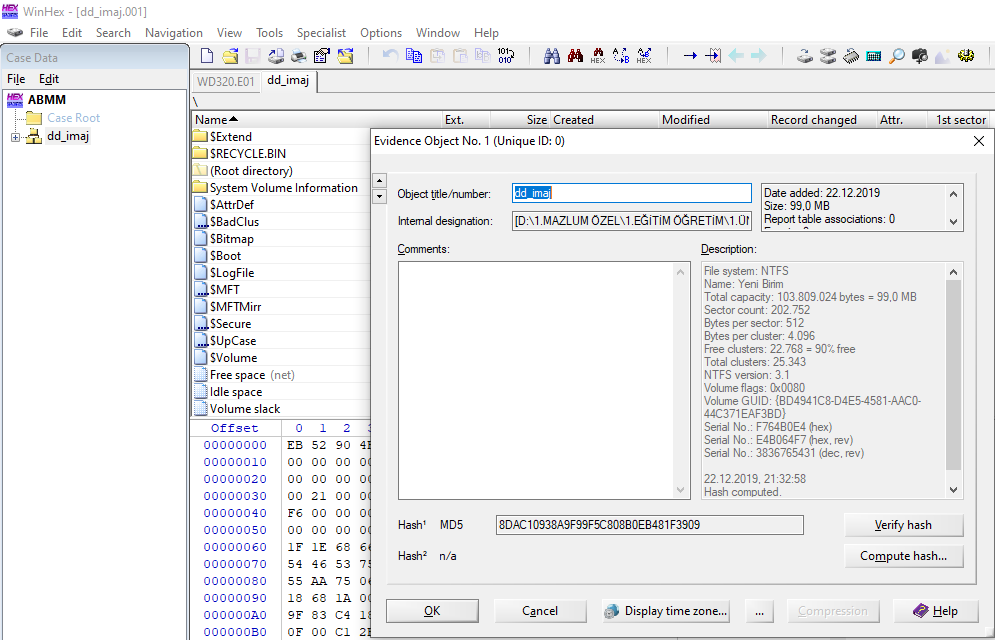
Eklenen bir imajın fiziksel veya partition imajı olup olmadığı imajın önünde bulunan şekilden anlaşılmaktadır.

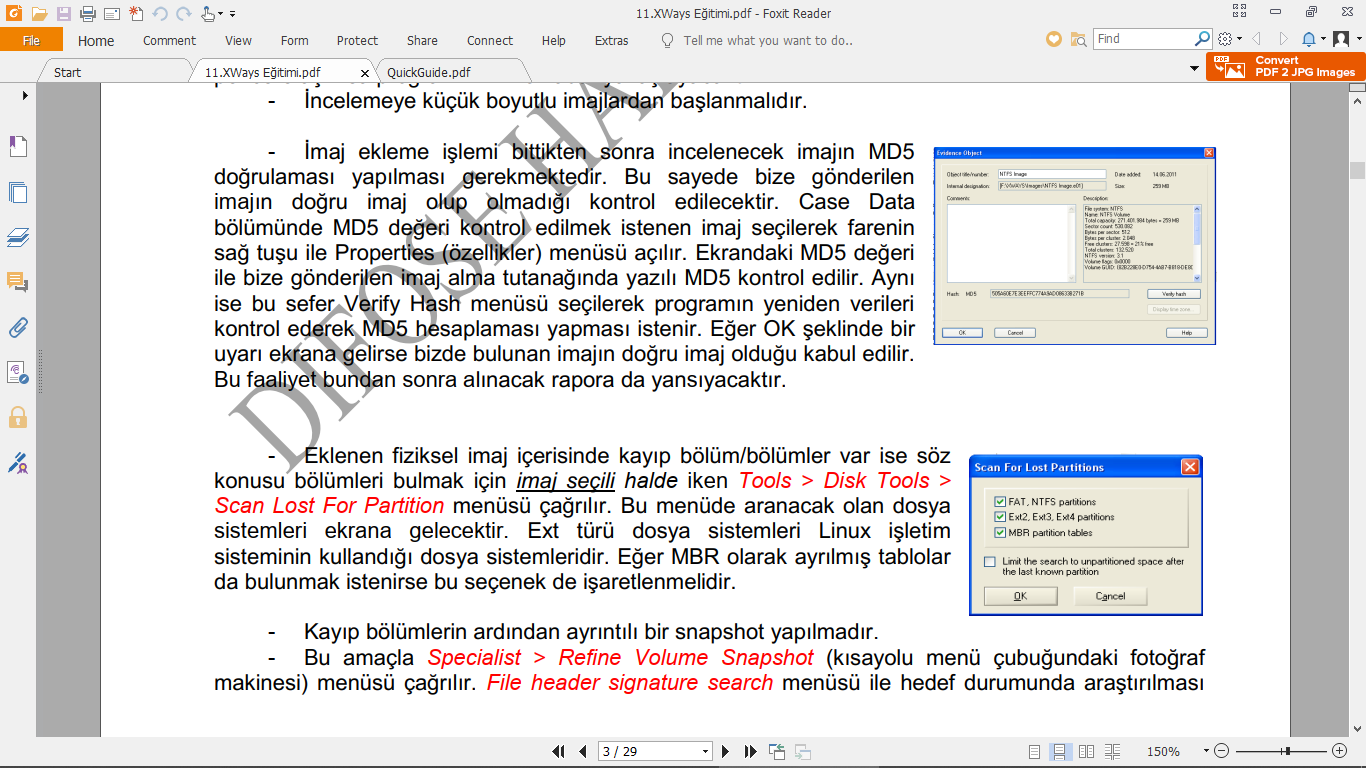
Programa aynı dava konusunu ilgilendiren bütün imajlar yüklenebilir. Yüklenen imajların listesi ***Case Data*** bölümünde görülecektir.

Üzerinde çalışılan imaj penceresi tab bölümünde ön plandadır. Tab bölümüne ne kadar fazla pencere açılırsa programın hızı o kadar yavaşlayacaktır.

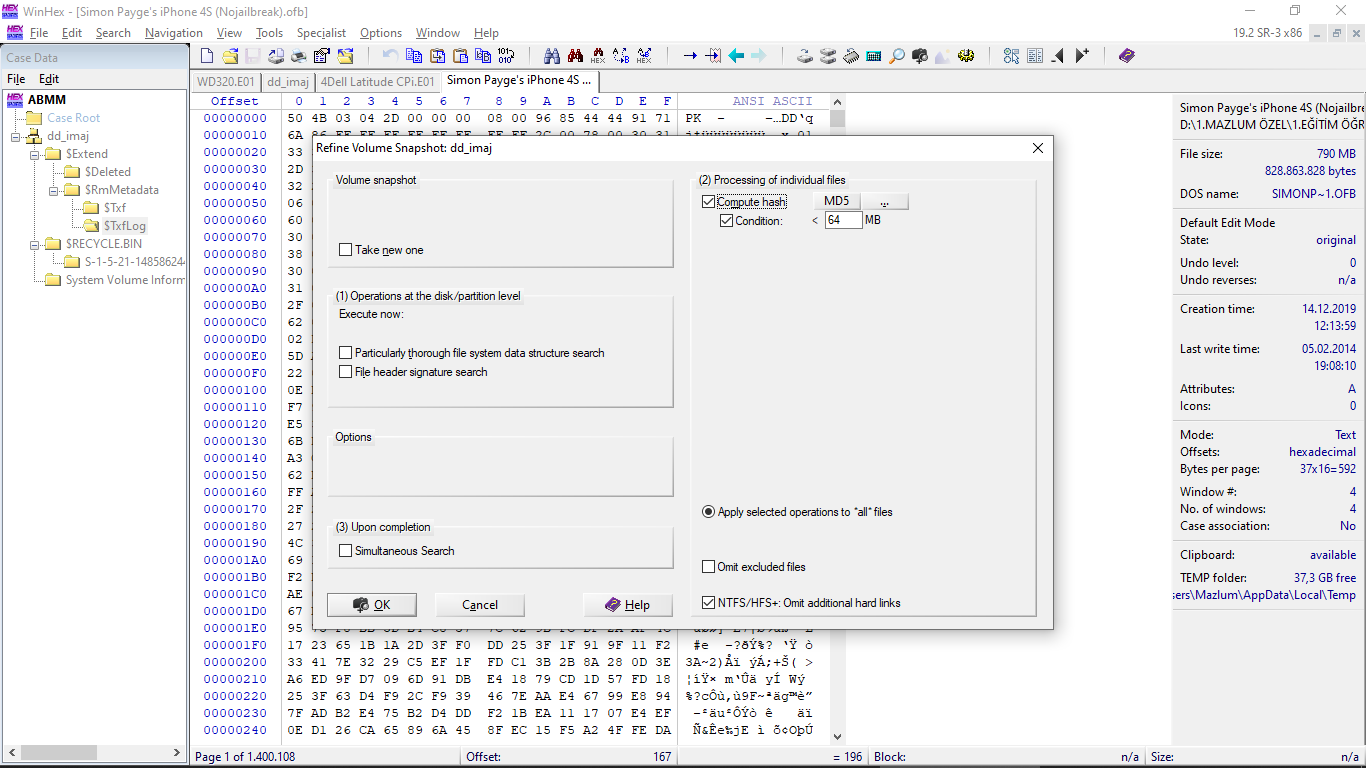
İncelemeye küçük boyutlu imajlardan başlanmalıdır.

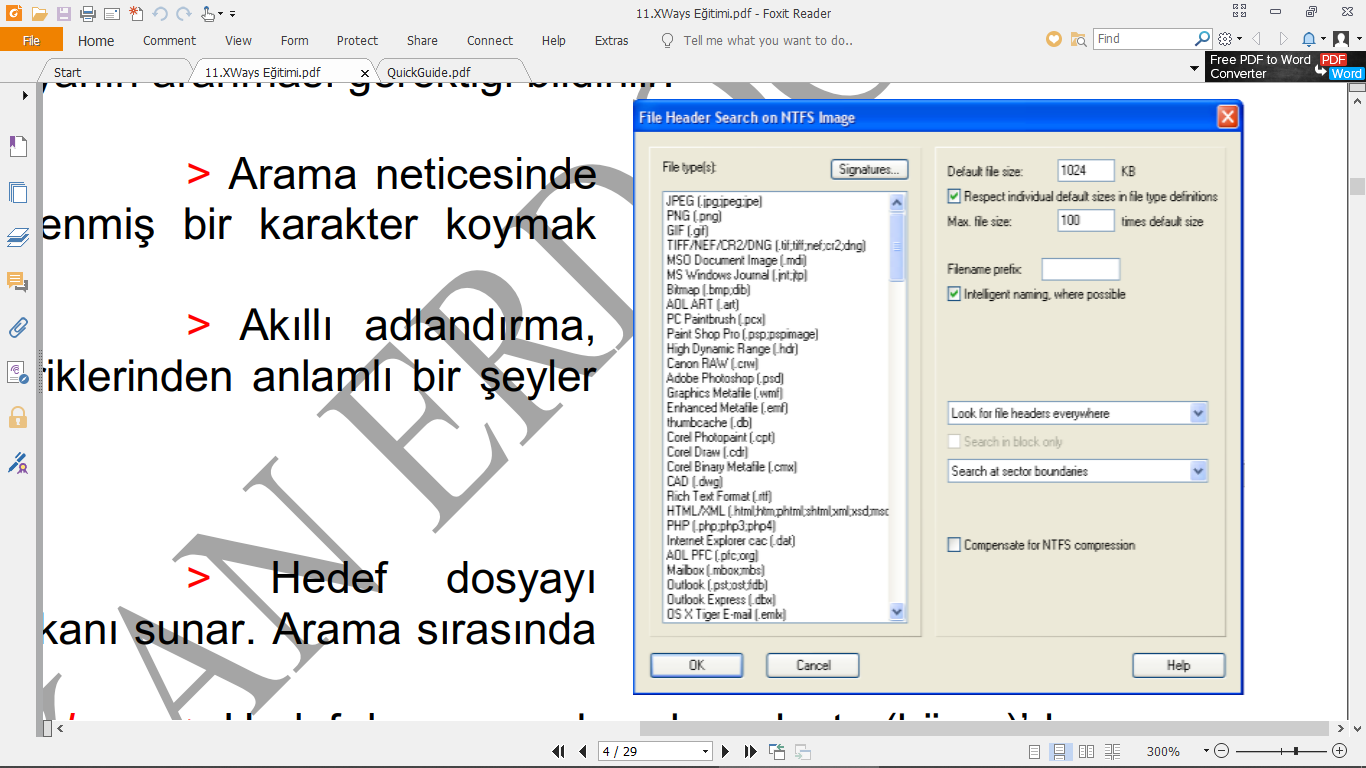
İmaj ekleme işlemi bittikten sonra incelenecek imajın MD5 doğrulaması yapılması gerekmektedir. Bu sayede bize gönderilen imajın doğru imaj olup olmadığı kontrol edilecektir. Case Data bölümünde MD5 değeri kontrol edilmek istenen imaj *seçilerek farenin sağ tuşu ile Properties (özellikler) menüsü* açılır. Ekrandaki MD5 değeri ile bize gönderilen imaj alma tutanağında yazılı MD5 kontrol edilir. Aynı ise bu sefer Verify Hash menüsü seçilerek programın yeniden verileri kontrol ederek MD5 hesaplaması yapması istenir. Eğer OK şeklinde bir uyarı ekrana gelirse bizde bulunan imajın doğru imaj olduğu kabul edilir. Bu faaliyet bundan sonra alınacak rapora da yansıyacaktır.



Eklenen fiziksel imaj içerisinde kayıp bölüm/bölümler var ise söz  
konusu bölümleri bulmak için *imaj seçili halde* iken ***Tools > Disk Tools >Scan Lost For Partition***menüsü çağrılır. Bu menüde aranacak olan dosya sistemleri ekrana gelecektir. Ext türü dosya sistemleri Linux işletim sisteminin kullandığı dosya sistemleridir. Eğer MBR olarak ayrılmış tablolar da bulunmak istenirse bu seçenek de işaretlenmelidir.

Kayıp bölümlerin ardından ayrıntılı bir snapshot yapılmadır.

Bu amaçla ***Specialist > Refine Volume Snapshot***(kısayolu menü çubuğundaki fotoğraf  
makinesi) menüsü çağrılır. *File* ***header signature search***menüsü ile hedef durumunda araştırılması  
istenen dosyaların seçilmesi snapshot’u hızlandıracaktır. Eğer belirli bir hedef yok ve imaj içerisinde suç unsuru tespit edilmesi istenmişse bütün dosya türü seçilmelidir.

**File header….** Menüsü yanında bulunan Signature açılırsa, programda yüklü olan dosya isimleri ile türlerinin, sabit belleğe kaydedilen dosya başlığı gözükecektir. JPEG uzantılı dosyalar sabit belleğe FF D8 FF E0 olarak kaydedildiği görülecektir. Snapshot aradığı dosya türlerini bu kodlara göre aramaktadır.

Tamam ile birlikte dosya türü ve boyutu ile hangi bölgelerde arama yapılacağı ekran gelecektir. Burada bulunması veya incelenmesi istenen dosya türü var ise onlar, yok ise hepsi shift tuşunun yardımı ile seçilmelidir.

**Default file size :** Varsayılan dosya boyutu olup hedef durumundaki dosya boyutundaki en küçük değerdir.

**Respect individual default sizes in file type definitions :** Hedef durumundaki dosya boyutu biliniyorsa bu menüden istifade edilir. Bu alan işaretlendiğinde Default file size ile Max. File… arasında kalan dosya boyutlarında arama yapacaktır.

**Max.File Size 100 times default size :** Bu alan Default file size kutusunda bulunan değerin kaç katına kadarlık bir dosyanın aranması gerektiği bildirilir.

**Filename prefix >** Arama neticesinde bulunan dosyaların önüne karakter belirlenmiş bir karakter koymak mümkündür.

**İntelligent namig, where possible >** Akıllı adlandırma, orijinal dosya isimlerinden değil dosya içeriklerinden anlamlı bir şeyler tespit etmek amacıyla işaretlenir.

***Aranacak yer belirleme;***

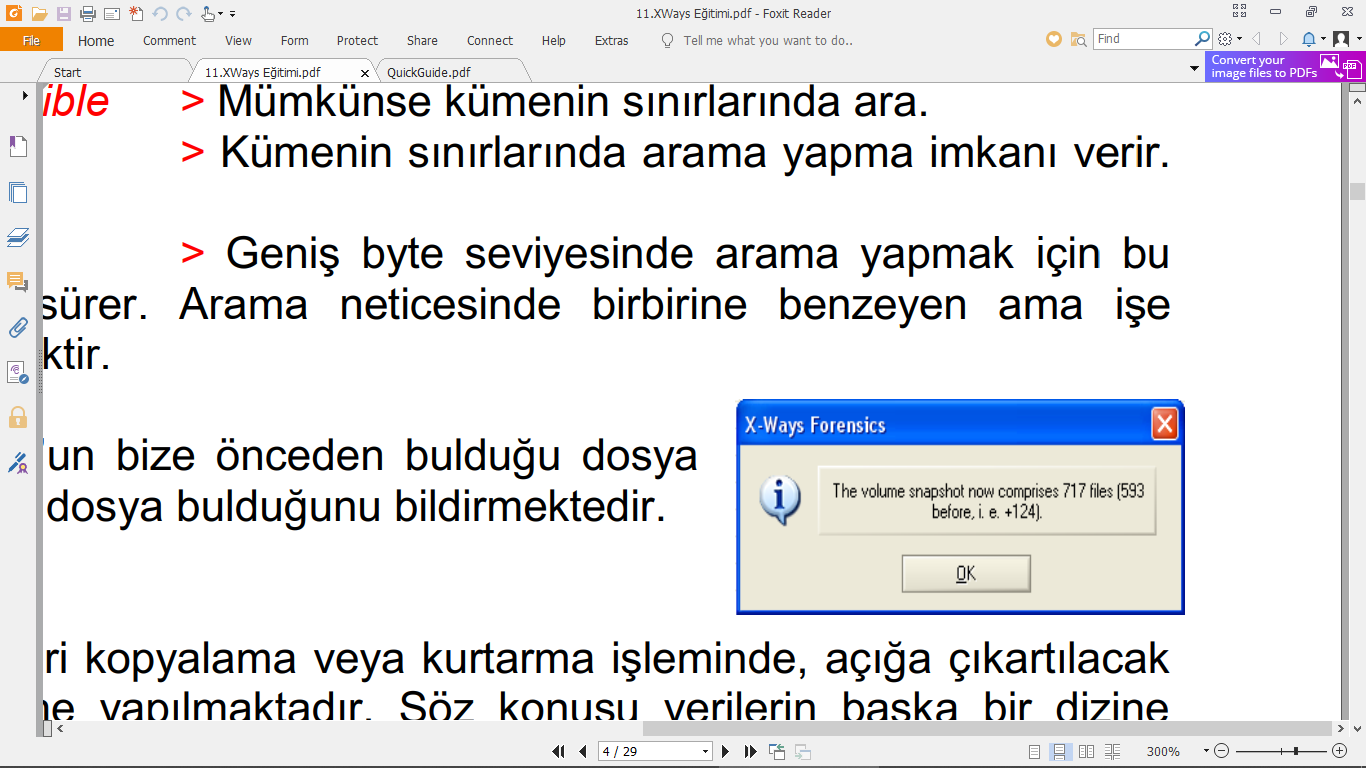
**Look for headers everywhere** > Hedef dosyayı sabit belleğin her yerinde her yerde ara imkanı sunar. Arama sırasında bu seçeneğin işaretli olması gerekmektedir.

**Look for headers in free clusters only >** Hedef dosyayı sadece boş cluster(küme)’da ara.

**Look for headers in allocated space only >** Hedef dosyayı sadece ayrılmış boş alanlarda ara.

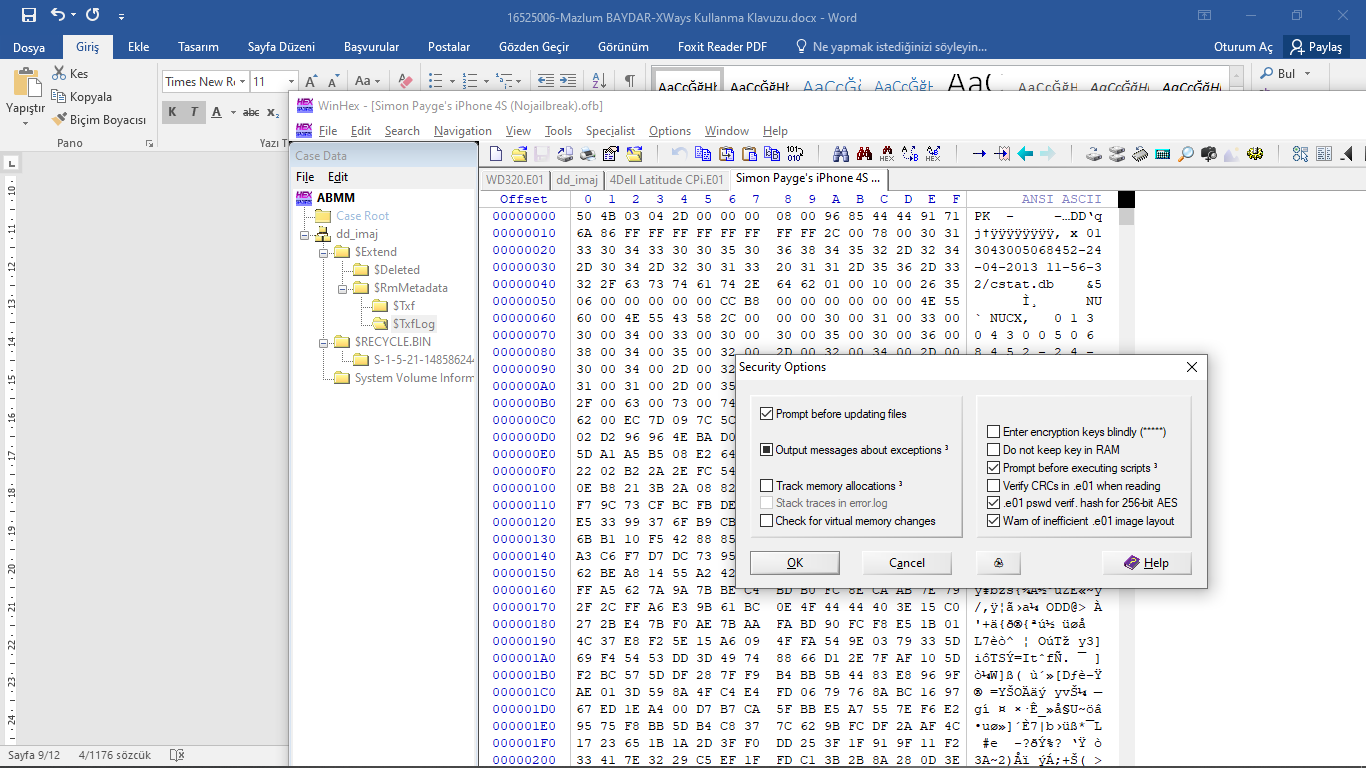
**Search at cluster boundaries, if possible >** Mümkünse kümenin sınırlarında ara.

**Search at cluster boundaries >** Kümenin sınırlarında arama yapma imkanı verir.Bu seçenek ile arama yapmak daha iyidir.

**Extensive byte-level search >** Geniş byte seviyesinde arama yapmak için bu menü seçilir. Bu menüde arama uzun sürer. Arama neticesinde birbirine benzeyen ama işe yaramayacak dosyalar da bir araya getirecektir.

Arama işlemi bittiğinde, snapshot’un bize önceden bulduğu dosya sayısı olan (593)’e ilaveten (124) adet daha dosya bulduğunu bildirmektedir.

# 5. Güvenlik Ayarı

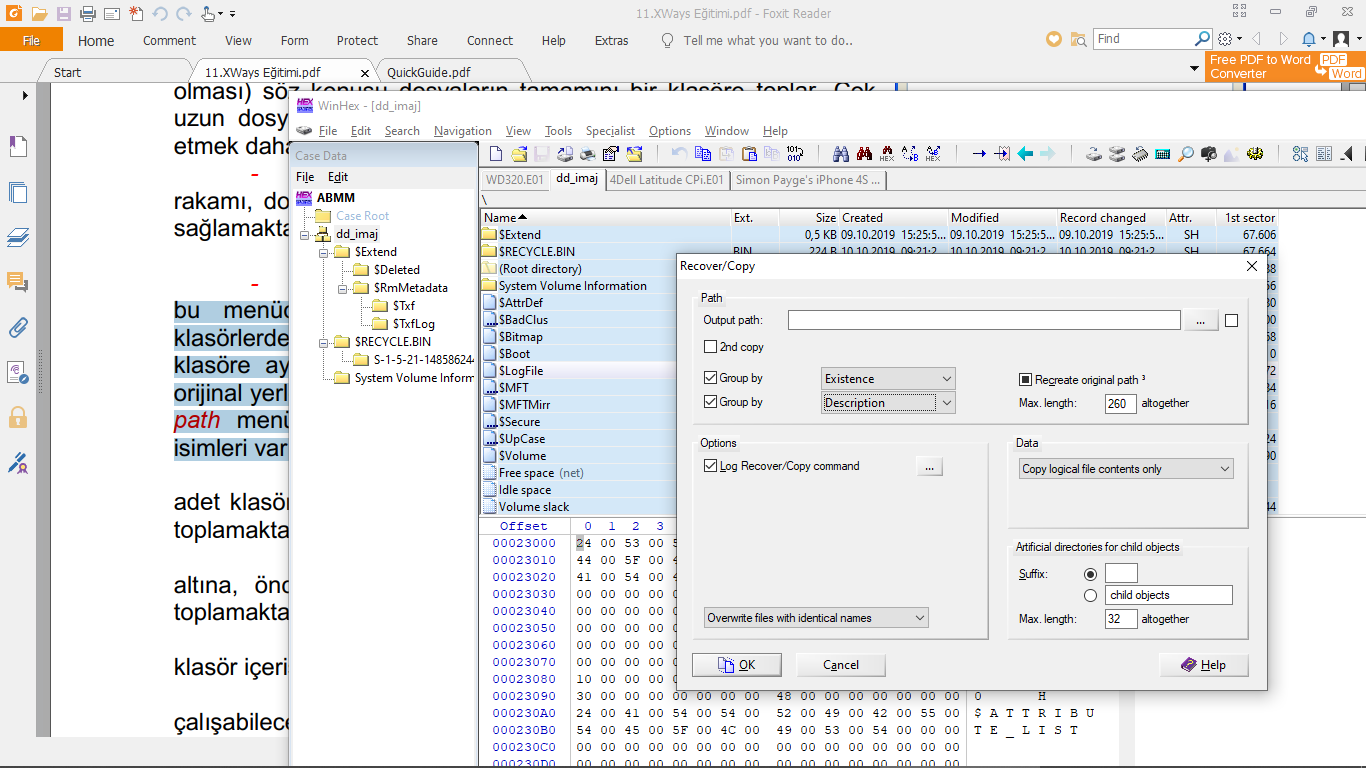
İnceleme sırasında, imaj içerisinde veri kopyalama veya kurtarma işleminde, açığa çıkartılacak  
veriler programın kurulduğu klasör içerisine yapılmaktadır. Söz konusu verilerin başka bir dizine  
kopyalanması istenirse (Örneğin dava dosyasının içerisine) ***Options>Security***menüsünün altında  
bulunan ***Script drive letter protection***seçeneği kapatılmalıdır. Bu seçeneği kapatmak isteğimizde bize  
doğrulama ekranı gelecektir. Bu ekrana *yes* yazarak kapatıyoruz.

# 6. Dosya Kopyalama Ve Kurtarma

İmaj programa yüklendiğinde, sabit bellek üzerinde bulunan mevcut dosyalar ile silinmiş  
ancak üzerine veri yazılmamış olan dosyaları görmek mümkündür. Bu tür dosyaları programı  
kullanarak tek tek incelemek mümkündür. Ancak bu uzun zaman alacak bir işlemdir. Bunun yerine söz konusu sislinmiş ve mevcut dosyalar belirlenen bir klasöre çıkarılmak suretiyle inceleme için zaman tasarrufu sağlanabilmektedir.  
  
Kopyalanacak veya kurtarılacak dosyaların tamamı seçilir. Burada $ işareti ile başlayanlar dosya sistemi ile alakalı veriler olduğundan bu dosyaların seçilmesine gerek yoktur.

Seçim işleminden sonra farenin sağ tuşu ile Recorvery/Copy komutu vasıtasıyla kurtarma veya kopyalama işleminin hangi klasör altına yapılacağı seçilir.

Burada dava dosyasının içerisine Mevcut ve Silinenler isimli bir klasör oluşturularak ona  
yönlendirilir.

**Path Menüsü:** Bu menüde 3 adet  
seçenek bulunmaktadır. Birinci menü, kopyalanan/kurtarılan  
dosyalar hedef klasör içerisine orijinal dosya yolu ile oluşturulur.  
İkinci menüyü işaretlemek ise opsiyonel olup hemen hemen birinci menü ile aynı işlevi yerine getirmektedir. Üçüncü seçenek ise (boş olması) söz konusu dosyaların tamamını bir klasöre toplar. Çok  
uzun dosya yolu var ise bunları kurtarmak yerine rapora dahil  
etmek daha sağlıklı olacaktır.

**Max. length :** Buraya yazılı 260  
rakamı, dosya isimleri dahil orijinal dosya yolunun gösterilmesini sağlamaktadır. Maksimum rakam 510’dur.

**Group by *:***Kurtarılan dosyalar, bu menüde yapılacak seçime göre gruplandırılarak hedef klasörlerde toplanır. Örneğin, resimler bir klasöre, veri tabanları bir klasöre ayırması gibi. Bu menü işaretlenmeden önce verilerin orijinal yerlerini tespit etmek bulmak için mutlaka ***Recreate original path***menüsü işaretlenmelidir. Kurtarma sırasında aynı dosya isimleri var ise ilk kurtarmadan sonraki aynı dosya isimlerine rakamsal değer verilmektedir.

* **Existence :** Program tarafından hedef klasör içerisinde Del ve Ex isimli 2 adet klasör oluşturmakta, silinmiş dosyalar Del klasörüne, mevcut dosyalar ise Ex klasörü içerisine toplamaktadır.
* **Description :** Tanımlama özelliğine göre sınıflandırır. Yine mevcutları existing altına, önceden mevcut olup sonradan içeriği değiştirilmiş olanları başka bir klasör içerisinde  
  toplamaktadır.

**Data menüsü:** Dosya ismi ile uzantısı farklı olan dosyalar için geçerlidir. Kurtarılan bir dosyanın resim dosyası ihtimali yüksek ancak uzantısı farklı olan dosyaları kurtarmaya dahil eder.

**Log recovery/copy command:**Log kayıtlarını kurtarma / kopyalama komutu dur.Bu kısımda Log kayıtlarının ne tarzta kurtarılacağı seçilip ayarlanır.

**Artificial directories for child objects**: Alt nesneler için yapay dizinlerlerin bellirlendiği alan

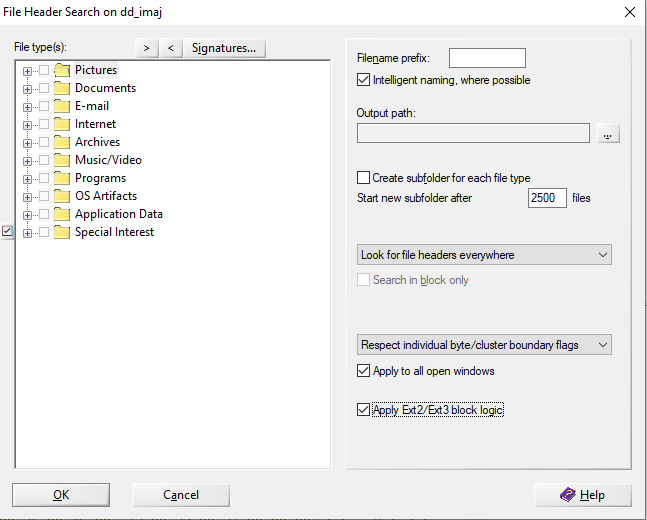
* **Suffix**: son ek kaynağı
* **Max length**: maksimum uzunluk belirleme

Kurtarma ve kopyalama işlemi dava dosyasına yapıldıktan sonra, ilgili dosyalar davada görevli diğer personel tarafından incelemeye başlanabilir. Bu sayede dongle ile yapılacak olan registry ve mail gibi kayıtların incelemesine devam edilebilir.

Kurtarma ve kopyalama işlemi neticesindeki dosyalarda suç unsuru olanlar var ise, orijinal  
isimleri değiştirilmeden ayrı bir klasöre kopyalanır

# 7. Dosya kurtarma

İmaj içerisindeki gömülü olan (mevcut ve silinmiş olmayan) dosyaları kurtarmak seçilen imaj  
sonrasında *Tools>Disk Tools>File Recorvery By Type* menüsü açılır.  
Program bize bu işlemden önce bir snapshot yapılabileceği konusunda uyarı verecektir.  
Hangi dosya türlerinin kurtarılacağı biliniyorsa gelecek pencereden onlar seçilir. Eğer belirli  
bir hedef yok ise hepsi seçilir.

**File types:** Kurtalırlacak dosya türlerini belirler.

**Filename prefix:**dosya öneki adı

**Output Folder :**Dava dosyası  
içerisine Kurtarılanlar isimli bir klasör oluşturulmalı ve kurtarılacak  
veriler bu klasöre yönlendirilmelidir

**Create sub folder for each file type :** kurtarılacak veriler türlerine göre oluşturulacak klasörler içerisine toplanmaktadır.

**Look for file headers everywhere:**Dosya arama türlerinin belirlendiği alan, her yerde dosya başlıkları arayın gibi seçenekleri mevcuttur.

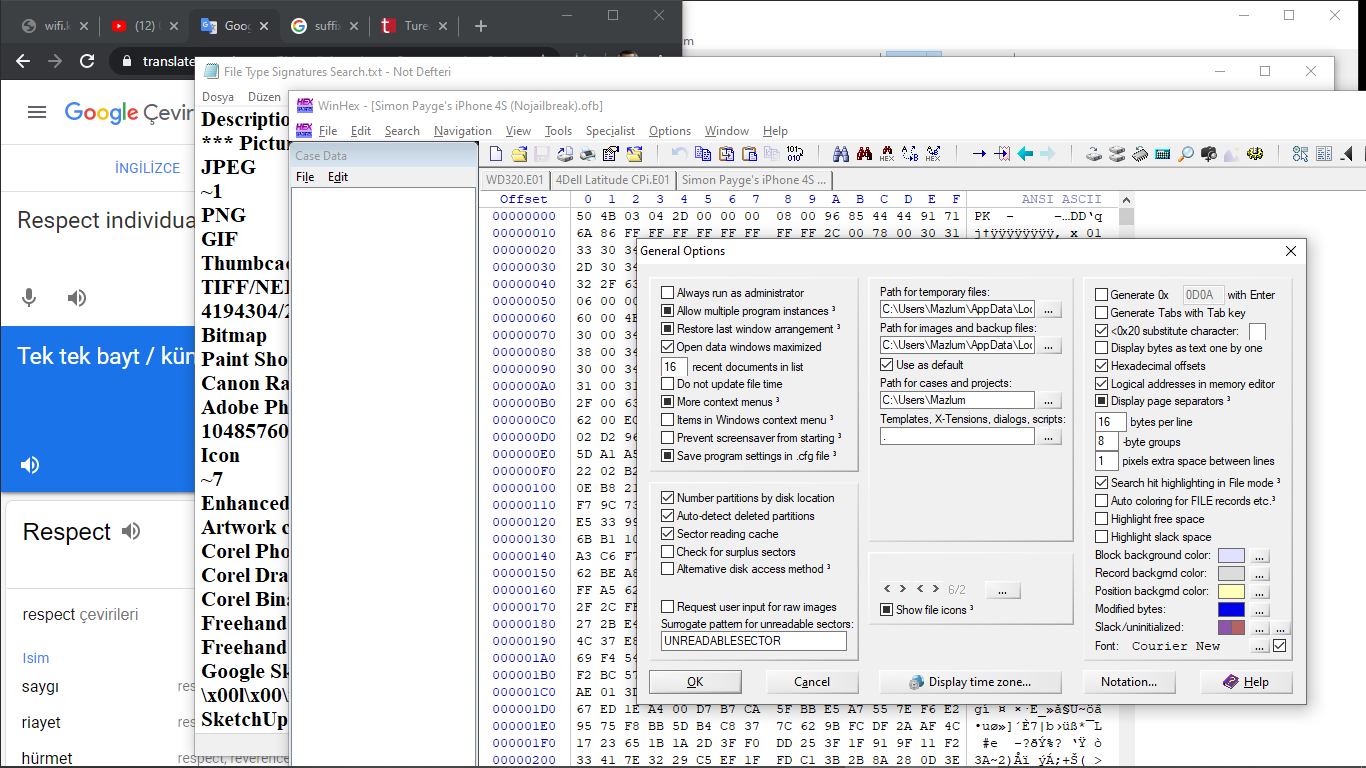
**Respect individual byte/cluster boundary flags:** Tek tek bayt / küme sınır bayraklarına öncellik duyun seçeneğidir.

**Apply to all open Windows :** Programın menülerinin altındaki imaj izleme penceresindeki açık bütün imajlarda kurtarma yapar.

**Apply Ext2/Ext3 block logic :** Mantıksal Linux dosya sistemi var ise bunları da kurtarmaya dahil edilmesini sağlar.

# 8. General Options bölümü

Program ile ilgili genel ayarlamalar General options bölümünde yapılmaktadır. Bu menü, F5  
tuşu veya program kısa yollarında üzerinde *c:\* işareti olan menü vasıtasıyla çağrılır.

Birinci (sol menü) bölüm:

**Always run as administrator:** Her zaman yönetici olarak çalıştır

**Allow Multiple Program instances :** Aynı anda birden fazla programın çalışmasına izin verir.

**Restore Last Windows Arrangement:**Üzerinde çalışmaya başlanılan dava dosyasının her program başlatıldığında son hali ile karşımıza gelmesi isteniyorsa bu seçenek işaretli kalmalıdır.

**Open data Windows maximized :** Menülerin altında açılabilecek maksimum pencere sayısına izin verir. Burada dikkat edilecek konu ne kadar fazla pencere açılırsa program o kadar fazla çalışacağından bilgisayarın hızı azalacaktır.Kullanılmayan pencerelerin kapatılması uygun olacaktır.

**Do not update file time :** Bu menünün seçili olması, dosyaların güncellenmesi veya başka bir yere kopyalanması neticesinde son değişikliğin tarihini muhafaza edecektir.

**More context menü:** Winhex programındaki menüleri bu programa eklenmesine izin verir.

**Items in Windows context menü:** Windows bağlam menüsündeki öğeleri gösterir.

**Prevent screensaver from starting:** Ekran koruyucunun başlamasını önleme

**Save program setting in cfg file:** Program ayarını cfg dosyasına kaydetme

**Number partitions by disk location*:***Fiziksel bölüm olarak alınan imaj içerisindeki  
bölümleri numara sırasına göre sıralar. **Auto-detect deleted partitons**: Fiziksel sürücü içerisinde, mevcut bölüm ile  
silinmiş en son bölüm arasında kalan bütün bölümleri otomatik bulmaya işlemi yapar.  
**Sector reading cache :** Cahce (PC ön belleği) sektörleri okumaktadır.

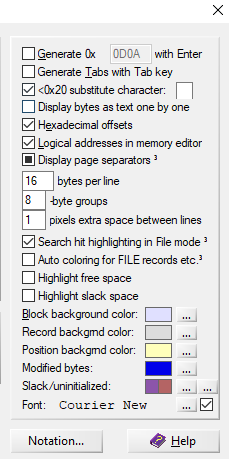
**Check for surplus sectors:** Artık sektörleri kontrol etme

**Alternative disk Access method:** Alternatif disk erişim yöntemi

**Request user input for raw images:** Ham görüntüler için kullanıcı girişi isteme

**Surrogate pattern for unreadable sectors:** Okunamayan sektörler için vekil kalıp seçme

İkinci (sağ) bölüm:

**Generate 0x … with Enter:** ENTER tuşu, dört adede kadar iki basamaklı onaltılık değer girmek için kullanılabilir. Örnek olarak Windows dünyasında satır sonu işareti olarak yorumlanan 0x0D0A (Unix: 0x0D).Başlangıç Merkezi yine de ÜSTKRKT + ENTER tuşlarını kullanarak açılabilir.

**Generate Tabs with Tab Key:** Metinten onaltılık moda geçmek için SEKME tuşunu kullanıp kullanmayacağınıza karar verme modudur.

**<0x20 substiture character:** Karakter kümesi değeri 0x20'den küçük olan yazdırılamayan karakterler kullanıcı tanımlı başka bir karakterle temsil etme

**Display bytes as text one by one :** Baytları tek tek metin olarak görüntüleme

**Hexadecimal offsets:** Ofsetler ondalık veya onaltılı gösterimde sunulabilir ve istenebilir. Bu ayar tüm program için geçerlidir

**Logical addresses in memory editör:** Bellek düzenleyicisini kullanırken, WinHex'in sıfır tabanlı, doğrusal, bitişik olarak sayılan ofsetler yerine işlemler için mantıksal bellek adresleri görüntülemesi yararlı olabilir. Bu her zaman onaltılı gösterimde yapılır. Ofsete Git komutunun iletişim penceresi mantıksal adresleri de soracaktır.

**Display page separators:** Sayfa ve sektör ayırıcılar görüntülenebilir. Bu seçenek kısmen etkinleştirilirse, yalnızca sektör ayırıcılar görüntülenir.

**Search hit highlighting in File mode:** Dosya modunda isabetli vurgulamayı ara

**Automatic coloring for FILE records etc.:** DOSYA kayıtları vb. İçin otomatik renklendirme seçeneği

**Highlight free space:** Boş alanı vurgulama

**Highlight slack space:** Bellek boşluğu olan alanı vurgula.

**Block background color:** Geçerli bloğun arka planı olarak kullanılan bir renk seçin. Rengi yalnızca “Windows varsayılan renklerini kullan” seçeneği kapalıysa değiştirebilirsiniz.

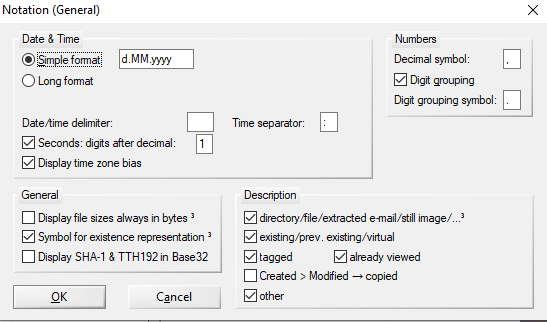
**Record background color:** Kayıt sunumu etkinleştirilmişse, diğer tüm sabit uzunluklu kayıtların arka planı olarak kullanılan bir renk seçin (bkz. Konum menüsü).

**Position background color:** Yeni oluşturulan ek açıklamalar / pozisyonlar / yer işaretleri için varsayılan rengi seçin.

**Modified bytes:** Değiştirilmiş baytları renklendirme seçeneği.

**Slack/uninitialized:** Bellek boşluğu olan alan ve başlatılmamış alan için renk seçin.

# 9. Notation (işaret ve rakamlarla gösterme sistemi)

**Date & Time**: Tarihin görüntülenme şekli. Türkiye için dd.mm.yyyy olacaktır 

**Time separator**: Zaman bölümü arasındaki işaret. Saat, dakika ve saniyeyi ayıracak işaret bu bölümden değiştirilir.

**Date/time delimiter :** Tarih ve zaman arasına gelmesi istenen  
işaret.

**Seconds: digits after decimal :** Saniyeden sonra gelmesi istenen salisenin basamak ayarı,(en fazla 3 basamak)  
**Display time zone bias :** Greenwhich’e göre dosya  
zamanının ayarı, **Decimal symbol** : Tam sayı ile ondalık sayıları ayırma işareti, **Digit grouping with*:***Yüzler basamağını arasına konacak ayırma sembolü

**Display file sizes always in bytes:** Dosya boyutları isteğe bağlı olarak her zaman yuvarlak yerine bayt olarak görüntülenebilir. Onay kutusu yarı işaretliyse, bu yalnızca birimlerdeki öğeler için geçerlidir, aksi takdirde fiziksel, bölümlenmiş ortamdaki öğeler için de geçerlidir.

**Symbol for existence representation:** Varlık gösterimi sembolü

**Display SHA-1 &TTH192 in Base32:** SHA-1 ve TTH192 karmaları isteğe bağlı olarak P2P programlarında yaygın olarak dizin tarayıcısında Base32 gösterimlerinde görüntülemedir.

# 10. Program başlangıç seçenekleri

Program her başlatıldığında kullanıcıyı 3 farklı ekran karşılayacaktır. Bunu ayarlamak F5

General option ile mümkündür.

**Open File:**Herhangi bir dosyayı açma,

**Open Disk**: Physical veya Logical diski seçme.Bu özellik kullanılarak bir bellek dava dosyası açılmadanincelenebilir.

**Open RAM :** RAM’da o için yüklü programları gösterir.

**Open Folder:** Mevcut dosya ve klasörleri görüntülemek veya programa yükleme bölümü,

**Recently Opened:** En son kullanılanların listelendiği bölümdür. Ulaşmak istenilen dosyalara hızlı erişim sağlar.

**Project:**En son kullanılan dava (case) veya projeleri listeler,

**Scripts :** Program içerisinde kullanılan scriptleri listeler.

# 11. Display time zone - Zaman Dilimi Ayarlama

Create New case menüsü ile General Options bölümünde  
bulunan Display time zone menüsü programın hangi dünya saat  
dilimine göre çalışacağı belirlenir.  
**Observe dayligtht…** : Programın gün ışına göre  
ayarlanmasının otomatik olarak yapılmasını sağlar.

**Hour:**gün ışının başlayacağı ve biteceği saati göstermektedir. Başlama saati 02.00 bitiş saati ise 03.00’dır.  
**Day of week :** Gün ışığının başlayacağı günü göstermektedir. 0 değeri Pazar gününü işaret etmektedir.  
**Week of month :** Ayın içerisindeki hafta sayısını göstermektedir.  
**Month** : Gün ışığının başladığı ve bittiği ayı göstermektedir. 3 rakamı Mart ayını, 10 rakamı Ekim ayını göstermektedir.

# 12. Konfigürasyon Ayarları

**Options > Viewer Programs** menüsü kullanılarak incelenecek dosyaları gösterecek programların tanıtımı buradan yapılması gerekmektedir.

Normal son sürüm X-Ways kurulduğunda bizim ilave bir program yüklememize gerekyoktur.

Bu bölüm ihtiyaç duyulacak yeni tip dosya sistemlerini görüntülemek için yeni programların XWays programına tanıtılması içindir.

Program kurulduktan sonra default ayarlar normalde bütün ihtiyaçlarımızı karşılayacaktır. Programla birlikte kurulan Viewer programı, çoğu dosya türünü açabilmektedir.

Eğer bilinmeyen bir dosya türü tespit edilmiş ve viewer programı ile açılmaz ise, o dosya türünü açabilecek program kullanılan işletim sistemine yüklenmelidir. Custom viewer programs altındaki dosya yolu açılır ve yeni yüklenen dosyanın isminin bulunduğu exe dosyası bu programa tanıtılmalıdır. Bu sayede bilinmeyen/açılamayan dosya türleri yeni yüklenen program vasıtasıyla açılmış olacaktır.

Custom viewer programs başlığı altındaki ilk program internet Explorer programıdır.

T**ext Editor:** Text dosyalarını görüntülemek için gösterilecek notepad.exe programı tercih edilmiş olup istenirse değiştirilebilmektedir.

**HTML output viewer** : Web sayfası türündeki dosyaların hangi program vasıtasıyla gösterilmesi (firefox, ie gibi) isteniyorsa o seçilmelidir.

**MPlayer:** Video türündeki dosyaları açmak için gerekli program. Kurulum sırasında otomatik kendisi yüklemektedir.

**Preferred… :** Alternatif video izleme programı. MPlayer ile açılamayan dosyaları incelemek için alternatif video izleme programı.

**Crash safe text decoding (slower) :** Güvenli metin kod çözme (daha yavaş)

**Buffer decoded text for context preview :** Bağlam önizlemesi için arabellek kodu çözülmüş metin

**Custom viewer programs :** Özel görüntüleyici programları

**Use associated programs for viewing… :** Bilinen dosya türlerini hatırlamasının sağlanması için dosya türleri yazılmıştır.

# 13. Evidence Object Açıklamaları

**Object title/number:** İncelenecek imaj adı,

**İnternal desigration:** İncelenecek imajın bulunduğu yer,

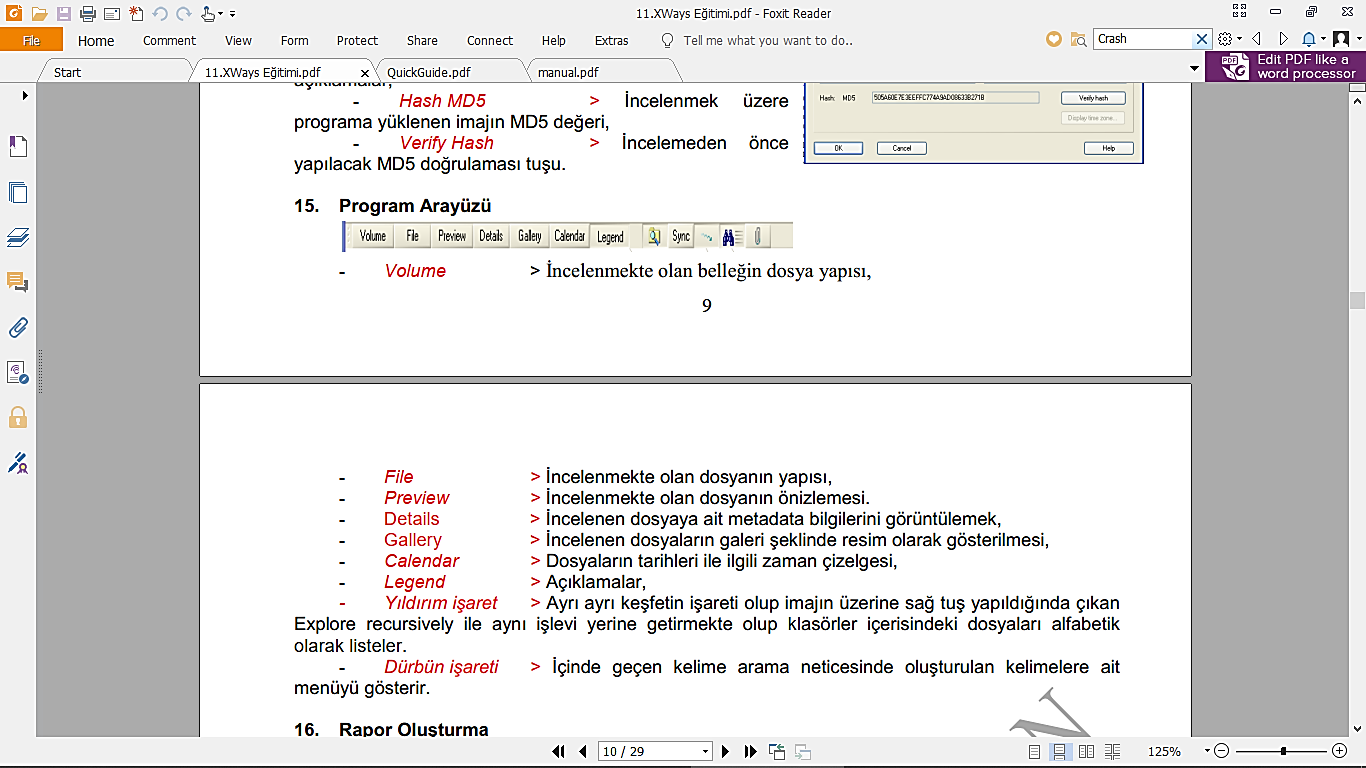
**Comments:** Yorumlar, incelemeye başlamadan önce bu delil ile ilgili olarak yapılacak bir değerlendirme veya yorum var ise buraya yazılmalı,

**Description:** İmage ile ilgili bilgiler,açıklamalar,

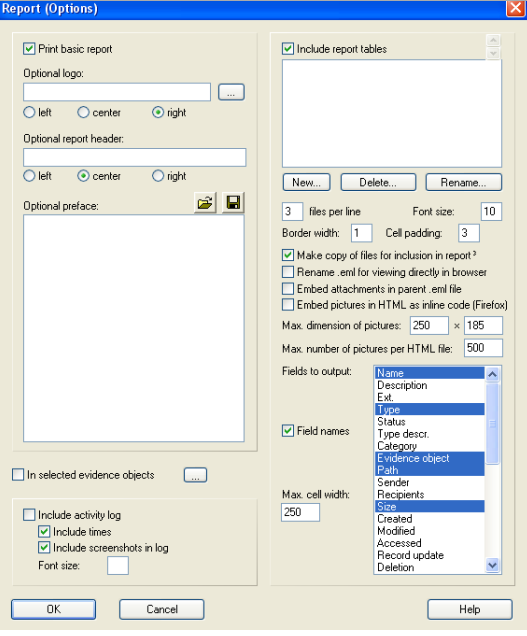
**Hash MD5 :** İncelenmek üzere programa yüklenen imajın MD5 değeri,

**Verify Hash :** İncelemeden önce yapılacak MD5 doğrulaması tuşu.

# 14. Program Arayüzü

 **Volume:** İncelenmekte olan belleğin dosya yapısı, **File**:İncelenmekte olan dosyanın yapısı,  
**Preview:** İncelenmekte olan dosyanın önizlemesi. **Details:** İncelenen dosyaya ait metadata bilgilerini görüntülemek, **Gallery:**İncelenen dosyaların galeri şeklinde resim olarak gösterilmesi,  
**Calendar:** Dosyaların tarihleri ile ilgili zaman çizelgesi, **Legend :**Açıklamalar, **Yıldırım işaret :** Ayrı ayrı keşfetin işareti olup imajın üzerine sağ tuş yapıldığında çıkan  
Explore recursively ile aynı işlevi yerine getirmekte olup klasörler içerisindeki dosyaları alfabetik olarak listeler.  
**Dürbün işareti :** İçinde geçen kelime arama neticesinde oluşturulan kelimelere ait  
menüyü gösterir.

# 15. Rapor Oluşturma

İncelemesi yapılan veya tamamlanan dosyalardan önem arz edenlerle ilgili bir rapor  
dosyası hazırlamak mümkündür. Raporda görüntülenmesi istenen bilgiler ile kuruma ait logolar davadosyası oluşturulmaya başlandığı sırada **Report (Options)**bölümünden ayarlanabilir.  
Oluşturulacak bütün raporlar, dava klasörünün içerisine açılacak Raporlar isimli bir klasör  
içerisinde toplanması dağınıklığın önüne geçecektir.  
Rapor menüsünü açmak için **Case Data > File > Create Rapor**yolu izlenmelidir.  
Karşımıza gelecek rapor menüsündeki veriler girildikten sonra değişiklik olmadığı sürece girilen bilgiler sabit kalacaktır.

**Print Basic Report***:* Oluşturulan raporu  
yazdırmaya hazırlama özelliği. Bu seçenek işaretli değilse rapor yazdırılmamaktadır. Hazırlanan raporlar yüklü internet programları internet Explorer veya firefox ile görüntülenmektedir.

**Optional logo:**Kuruma ait bir logo  
eklemek mümkündür. Rapora eklenecek resim önce  
açılmış olan rapor dosyasının içerisine konmalıdır.  
Rapora eklenecek resmin raporun header bölümünün  
sol, orta veya sağ bölümde görülmesini sağlamak  
mümkündür.

**Optional report header:**Opsiyonel olarak rapor başlığı ekleme ve yine başlığın raporun sol, orta veya sağ bölümde görülmesini sağlamak mümkündür.

**Optional preface:**Rapor için bir açıklama yazma veya başka bir yerde yazılmış olan açıklamayı rapora dahil etmek mümkündür.

**In selected evidence object***:* İncelenmek üzere programa yüklenmiş ve Case Data  
bölümünde görülen imaj/belleklerin hepsi otomatik olarak rapora dahil edilmektedir. Bu menü  
vasıtasıyla hangi materyallerin rapora dahil edilmesi isteniyorsa onları seçmek mümkündür.

**İnclude actvity log***:* Programın Properties bölümündeki *Include screenshots in log*menüsü, programın faaliyetlerini resim çekerek kayıt altına almaktadır. Çekilen resimler dava dosyası içerisindeki \_log dosyası içerisine PNG uzantılı olarak depolanmaktadır. Bu menü seçildiğinde rapora log kayıtları da dahil edilmekte, çekilmiş resimler log kayıtlarının arasına ilave edilmektedir.

**İnclude times:** Yapılan aktivitelerin zamanın rapora dahil edilmesi.

**İnclude screenshots in log***:* Yapılan aktiviteler sırasında program tarafından yapılan Print  
Screen özelliğine ilaveten log kayıtlarının dahil edilmesi.

**Font Size :** Raporun yazı büyüklüğünü ayarlama

**İnclude report tables***:* Rapor oluşturulacak klasörlerin tutulduğu bölüm. Bu bölümde New  
komutu ile yeni bir klasör oluşturulur. İnceleme sırasında rapor dosyasına dahil edilecek resimler işaretlenerek farenin sağ tuşu ile *Report Table association* komutu ile oluşturmuş olduğumuz klasöre dahil edilir.

**File Per line:**Bir satırda gösterilecek fotoğraf sayısı

**Font Size :**Fotoğrafların bilgilerinin görüntülendiği yazıların font büyüklüğü

**Border with:** Resimlere ait çerçevelerin kalınlığını artırma. 0 olursa çerçeve yoktur. 0-3  
arasında bir rakam girilmelidir.

**Cell padding :**Resimleri sayfaya en iyi şekilde yerleştirme

**Make copy of Picture for inclusion in report :** Rapora eklenen resimleri ayrı bir klasörde ek  
olarak toplanır. Bu sayede rapor başka bilgisayara gönderildiğinde orada da çalışır. Tıpkı internet dosyasının kopyalandığında yardımcı dosya ve resimlerin ayrı bir klasörde toplanması gibi. Rapor dosyası silindiği zaman ekleri olan resim dosyaları da rapor ile birlikte silinmektedir. Bir kaçlı farklı rapor oluşturulsa bile resimler tek bir klasör içerisine toplanmaktadır.

**Rename .eml for viewing directly in bowser :**Eml dosyasını göstermek için dosya isminin  
yeniden adlandırılması gerekmekte olup bu sayede Eml dosyası metin olarak görülebilir. Ancak nitelikli mailler görülemez. Eml dosyalarını açmak için mail programlarının yüklü olması gerekmektedir.

**Embed attachment in parent .eml file :**Eki olan mail dosyasının kendisini sola, eklerini ise  
sağa çıkartmaktadır.

**Embed pictures in HTML as inline code (Firefox) :**Resim dosyalarını HTML dosyasının  
içine gömmekte olup resimleri ayrı bir klasöre çıkartmaz.

**Max. Dimension of Picture:**Resimlerin maximum boyutunu ayarlamamızı sağlar.

**Max. Number of Picture per HTML file :**Rapor dosyası HTML şeklinde oluşturulmaktadır. Bir rapor dosyasında ne kadar fazla resim var ise programın hızı o kadar düşecektir. Bunun önüne geçmek için bir rapor dosyasına eklenecek resim sayısı buradan ayarlanabilmektedir.Bu özellik sadece resim dosyaları için geçerli olup diğer dosyalar için bu seçenek geçerli değildir.

**Fields to output:** Raporda gözükmesi istenilen sütun başlıkları seçilmektedir.

**Fields name***:* Sütun başlıkları verilerin sol tarafında gözükmesi istenirse bu menü  
işaretlenmelidir.

**Max. Width for filenames and paths:** Dosya adı ve yol uzunluğunu bir sütunda göstermek  
için girilebilecek karakter sayısı.  
- Ayarlamaların bitmesi ile birlikte raporun kaydedileceği yer sorulmaktadır. Dosya ismi  
verilirken ileride karışıklığa sebep teşkil etmeyecek isimlerin verilmesi önemlidir.  
- Raporun başarılı şekilde kaydedildiği ve raporun görüntülenmesi istenmekte midir diye  
uyarı menüsü gelmektedir. Evet seçildiğinde hazırlanmış olan rapor internet Explorer ile bize  
sunulmaktadır.  
- Oluşturulan rapor dosyasına, dava dosyasının özellikleri bölümünde yazılı bilgiler,  
incelenen imajlarla ilgili bilgiler ile yapılan hash doğrulaması gibi bilgiler dahil edilmektedir.

# 16. Rapor dosyasına veri ekleme

- İnceleme sırasında, önem arz eden dosyalar tespit edildiğinde, bu dosyalar tag menüsü  
kullanılarak işaretlenmelidir. (Bk.: Tag Menüsü)

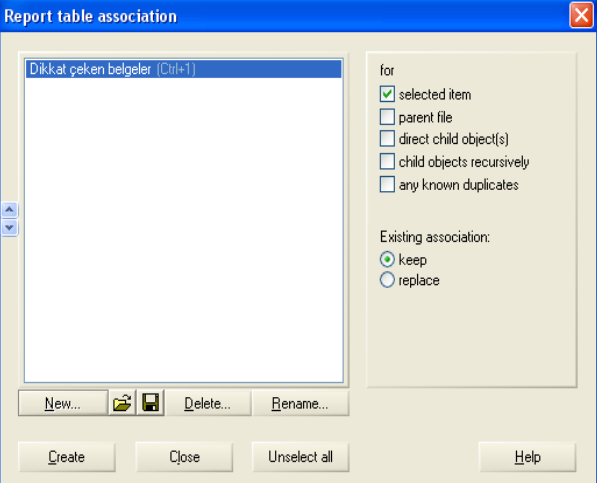
- **Directory Browser Options** menüsü içerisindeki **List tagged items** kutucuğu vasıtasıyla  
ekranda sadece Tag’lenmiş dosyaların gösterilmesi sağlanır.

- İşlem tamamlandığında ekranda sadece tag’lanmış dosyalar listelenmiş olacaktır.

- Listelenmiş dosyalar seçili halde iken farenin sağ tuşu ile açılan menüden **Report table  
association** seçilir. Açılan menü penceresinden New düğmesi ile yeni bir klasör oluşturulur. Create ile birlikte Tag’lenmiş dosyaların kısa yolları oluşturulmuş klasörün içerine kopyalanmıştır.

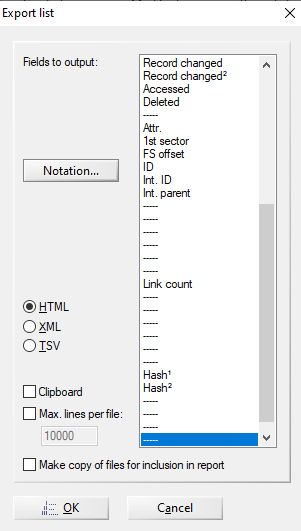
- Rapora dahil edilen dosyaların Name sütunundaki isimlerinin karşısında yeşil küçük bir  
üçgen işareti çıkacaktır. Üçgen sayısı, o dosyanın eklendiği Report table sayısını göstermektedir.

- Report Table klasörüne eklenen dosyalar **Case Data > File > Create** Report bölümü  
kullanılarak rapora dönüştürülür.

- Aynı dava dosyası ile ilgili farklı şüphelilerden alınan imajların içerisinde aynı suç şüphesi  
olduğu değerlendirilen dosyalar tag’lenmiş olarak rapora dahil edilebilir. Rapora dahil edilen suç dosyalarının hangi imaj içerisinde bulunduğu görülecektir. Bu sayede şüphelilerin arasındaki bağlantının ortaya konulması daha net olacaktır.  
Report Table Association Açıklamaları

**New:** Yeni bir klasör oluşturma,  
**Delete** : Oluşturulan klasörü silme,  
**Rename:** Oluşturulan klasörün ismini  
değiştirme,  
**Selected item :** Seçilmiş dosyalar  
**Direct child object:** Doğrudan küçük nesneler  
**Existing association** : Mevcut dosyaların ilişkileri  
**Keep :** Muhafaza et  
**Replace:** Değiştir

# 17. Dosya Özellikleri Listesi Oluşturmak-1

İnceleme sırasında önem arz eden dosyaların metadata  
bilgileri hakkında da bir rapor hazırlamak da mümkündür.

- Rapor oluşturacak dosyalar seçilir.

- Farenin sağ tuşu ile ***Export List…***menüsü seçilir.

- Karşımıza gelen pencereden**, *Fields to output***bölümünden rapora dahil edilmesi istenen dosya özellikleri seçilir.

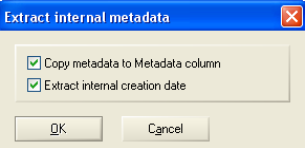
- Seçilen dosya özellikleri sonrası HTML kutucuğu işaretli ise web sayfası, Unicode kutucuğu işaretli ise Excel türünde bir rapor almak mümkündür.

- Kaydedilecek yer ve dosya isminin belirtilmesi ile birlikte dosya özelliklerini içeren rapor hazırlanmış olacaktır.

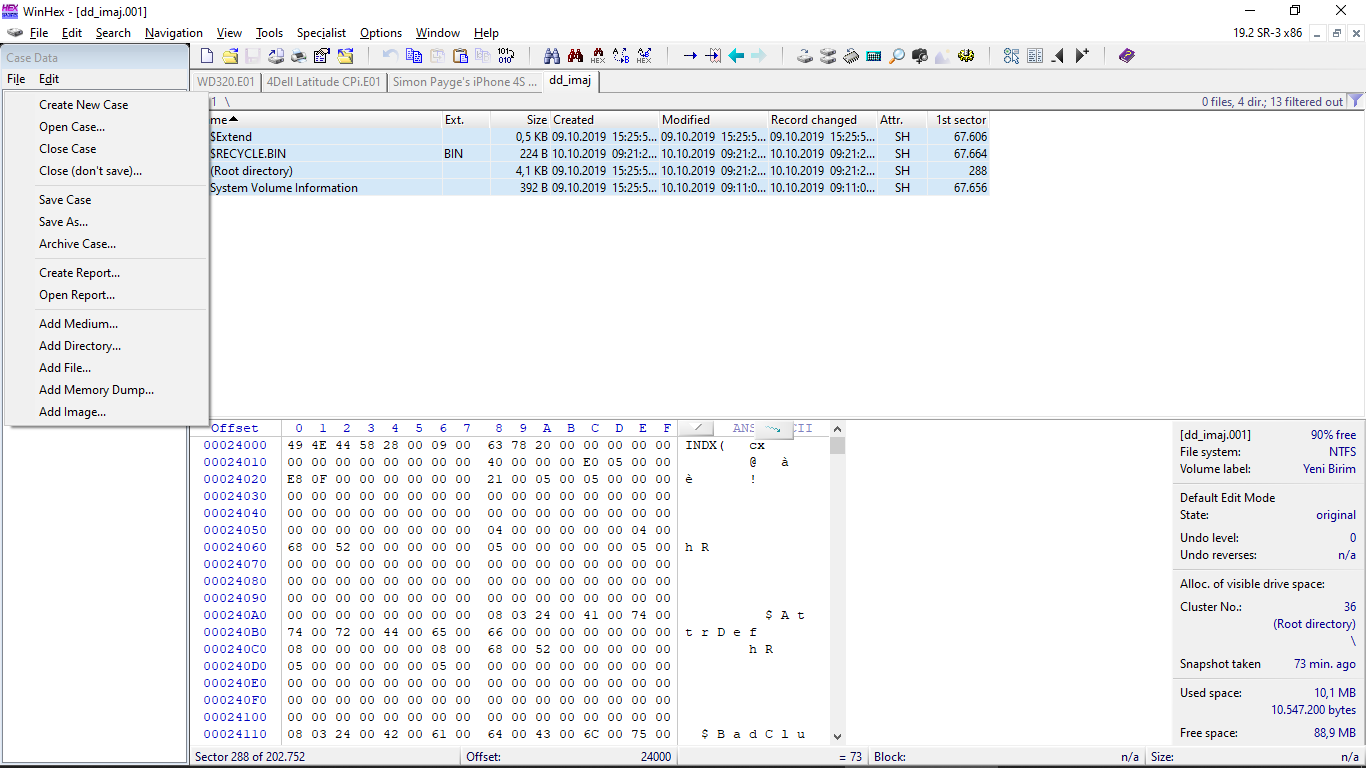
- Bu tür dosyalar yine önceden açılmış rapor klasörünün içerisine oluşturulmalıdır.

- Bunun seçenek, şüphelinin bilgisayarındaki suç dosyaları ile ilgili oluşturulma, silinme,  
güncellenme, kullanıcı gibi bilgileri bir arada görmemizi sağlar.

# 18. Dosya Özellikleri Listesi Oluşturmak -2

Dosyalara ait özellikler listelerken her bir özellik ayrı ayrı sutunlar yerine bütün özellikleri tek bir sutunda görmek mümkündür.  
- Bunun için işlem yapılacak dosyalar seçili halde iken  
farenin sağ tuşu ile **Exract İnternal Metada**menüsü seçilir.  
- Her iki seçenekde işaretlenir.  
- Eğer Metada bilgilerinin hepsini tek sutunda görmek  
istersek Directory Browser Options menüsündeki sutun başlıklarının olduğu bölümden Metada sutunun değeri 100 yapılır.  
- İşlem tamamlandıktan sonra yine farenin sağ tuşu ile **Export List***…* menüsü seçilerek işleme devam edilir. Bu özellik ile dosyaya ait metadata dosyalarını tek bir sütun içerisinde görmek  
mümkündür.

# 19. Case Data bölümü

**Create New Case :** Yeni bir dava dosyası oluşturma,

**Open Case :** Daha önce oluşturulmuş bir dava dosyasını açma,

**Close Case :** Açık olan dava dosyasını kapatma. Dava dosyası kapatıldığında programın yapmış olduğu snapshot silinmektedir.

**Close(don’t save)..** kayıt etmeden kapatma

**Save Case:** Dava dosyasını kaydetme,

**Save As..:** Dava dosyanı başka bir isim ile farklı kaydetme,

**Archive Case… :** Dava dosyasını sıkıştırmak suretiyle arşivlemek,

**Create Report:** Yeni rapor oluşturma

**Open Report:** Rapor açma

**Add Medium…:** Herhangi bir sürücü ekleme,

**Add Image…:** İmaj dosyası ekleme bölümü, buradan birden fazla imaj eklemek mümkündür. İmajları sürükle bırak yöntemi ile programa yüklenebilir. Bunun için programın yönetici (admin) ile başlatılması gerekmektedir.

**Add File… :** Dışarıdan bir dosya ekleme yapmak mümkündür.

# 20. Bellek İmajı Alma Bilgileri

Encase veri inceleme yazılı sadece MD5 anahtarı kullanırken, X-Ways programı hem MD5  
hem de SHA1 anahtarını kullanabilmektedir.

İmaj alımında doğrulama anahtarı olarak SHA1 tercih edilmiş olan bir imajın incelemesi  
Encase ile yapılmak istenirse Encase programı inceleme yapmasına rağmen SHA1 doğrulama anahtarını göremeyecektir.  
Raw imaj formatı, suspect (şüpheli) diski birebir olarak tek parça olarak almaktadır.Evidence (delil) diskin boyutu suspect (şüpheli) diskin boyundan büyük olmalıdır.

- E01 ile alınan imajlarda, sıkıştırma özelliği bulunmakta, şüpheli disk kullanıcı tarafından  
belirlenen boyutlara bölünebilmektedir. E01 türünde imaj almak daha iyidir.

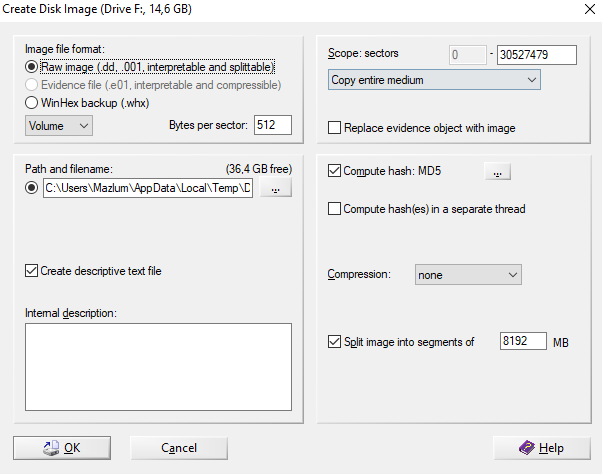
- Raw veya DD türündeki imajları, E01’e çevirmek mümkündür.

- Doğrulama anahtarı olarak çoğunlukla MD5, SHA1 ve SHA5 kullanılmalıdır.

- Evidence (delil) diski mutlaka suspect (şüpheli) diskinden büyük olmalıdır

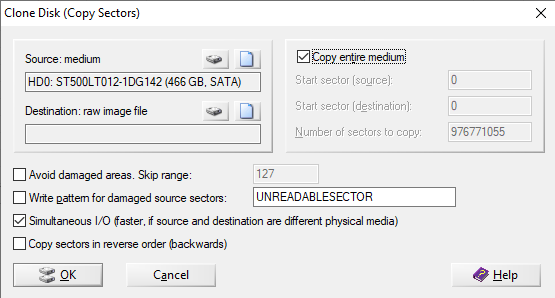
# 21. X-Ways ile Bellek İmajı Alma

X-Ways programı ile fiziksel ve logical diskler ile USB ve hafıza kartlarının imajlarını almak mümkündür.  
İmajı alınacak şüpheli metaryaller mutlaka yazılım koruma özelliği olan donanım ile birlikte  
bilgisayara takılmalıdır. Eğer *doğrudan takılırsa delil bütünlüğüne zarar verilmiş olur.*Case Data > File > Add Medium menüsü kullanılarak View Disk pencresi açılır. Burada o  
an için bilgisayarda takılı bellek ile CD/DVD sürüler gözükmektedir. Buradan imaj alınacak bellek seçilir.  
Tamam ile birlikte program yüklenen media ortamının snapshotunu hazırlar ve Case Data  
bölümüne ekler.  
İmaj alınacak media seçili halde iken **File>Create Disk İmage**menüsü ile Create Disk İmage penceresi ekrana getirilir. Bu menünün en üstünde imaj alınacak media’nın ismi görülmektedir.

Menü açıklamaları;

**İmage File Format :** İmajın formatı seçilir.  
**Path and File name** : İmajın alınacağı yer ile ismi belirtilmelidir.  
**İnternal description:** Açıklamaların yazılacağı bölüm.  
**Replace evidence object with image**:İmaj alma işlemi ile birlikte delili yenileme yapar.  
**Power down computer after completion :** İmaj bittiğinde bilgisayarı kapat.  
**Scope:Sectors:** Başlangıç ile  
son sektör arasında kalan herhangi bir sektörün imajı da alınabilir.  
**Store free cluster as zero-value bytes**: Bazı ülkelerde silinmiş dosyalar delil olarak kabul edilmemektedir. (Ör.: Avustralya) Bu menü o ülkelere hitap etmek için konulmuştur. Eğer bu menü işaretli iken imaj alınırsa silinmiş ve boş kümeler imaja dahil edilmeyecektir. Türkiye şartlarında bu seçenek  
kullanılmamalıdır. Yanlışlıkla bu menü açmaya karşı güvenlik duvarı ile korunmuştur.  
**Compute hash MD5:** Yandaki düğme ile alınacak imajın doğrulama  
anahtarının hangi olması gerektiği seçilebilir. Tercih MD5 den yana olabilir.  
**Compression:** Alınan imajı sıkıştırma hızı buradan ayarlanabilir.  
**Split image into segment of 8192 MB**: Alınacak imajları buradaki yazılı olan  
megabaytlar ölçüsünde parçalara ayırır. Bu özellik, çok büyük imaj alma işlemlerinde, verilen  
taşınmasında kolaylık sağlamaktadır.  
- Gerekli bilgiler girildikten sonra OK seçildiğinde imaj alma işlemineTamam ile birlikte  
program yüklenen media ortamının snapshotunu hazırlar ve Case Data bölümüne ekler.

# 22. Disk Klonlama

Disk kolonlama menüsü Raw türünde alınan bir  
imaj ile aynı sistemde çalışmaktadır.   
- ***Tools > Disk Tools > Clone Disk***menüsü ile  
hedef durumundaki bir belleğin birebir kopyasının (imajını) almak mümkündür.  
- Alınan bu kopyada MD5 değeri bulunmamaktadır.  
- Clone disk ile alınan kopyalar da bu program ile  
incelenebilmektedir.

# 23.Program Bilgileri

- Program başlatıldığında orta bölümde bulunan sütunlar standart olarak gelmektedir. İhtiyaç olmayanları gizlemek, ihtiyaç duyulanları açmak mümkündür.  
- Program başlatıldığında alt tarafta görülen **Messages (mesajlar)**bölümü, programla ilgili bilgiler vermektedir. Kullanıcı mantık dışı hatalar yaparsa (rasgele tıklamalar gibi) program kullanıcının acemi olduğunu varsayarak uyarı mesajı vermektedir.  
- **Did you know**ile kullanıcıya kısa bilgiler verilmektedir.  
- Bir klasör seçildiğinde, programın sağ alt tarafında, seçilen klasörün içerisindeki dosya sayısı ile boyutu hakkında bilgi verilir. Bu özellik, kopyalama başlamadan önce, hedef sürücüde ihtiyaç duyulan boş alanı hesaplayabilmemizi sağlar.  
- Case data bölümünde bulunan imaj veya klasörlere farenin sağ tuşu ile seçilerek çıkan menüden Explore Recursively seçilirse, klasörler içerisindeki bütün dosyalar alfabetik olarak sıralanır.  
- Case Data içerisinden işaretlenen klasörler ile içerisindeki dosya sayıları sağ üst köşede gösterilmektedir. Filtreleme yapılmışsa, yine mevcut ve silinmiş dosya sayısını görmek mümkündür.  
Bir dosya seçtiğimizde **The contents ….**şeklinde bir uyarı mesajı, seçilen dosyanın eksik olabileceğini, içeriğinin tam olarak görülemeyeceğini belirtilmektedir.  
- Bir dosya seçildiğinde hex içerisinde rasgele veriler görülüyorsa, söz konusu dosya ya sıkıştırılmış veya şifrelenmiş bir dosyadır.  
- Şüphelinin incelenen imajında şifreli dosya bulunması halinde, şifreli dosyalar şifre çözme yeteneği olan birimlere gönderilmelidir.  
- Şifreli dosyalara ilaveten, icra edilen operasyonun özelliğine göre, resimler içerisine steganografi ile dosya saklanabileceğinden şüphelenilen resimler steganografi ile şifreyi çözebilen birimlere gönderilmelidir.

# 24. Directory Browser Options, Filters (Dosya Filtreleme)

Birinci bölümde çalışma sırasında ihtiyaç duyulan düzenlemeler, ikinci bölümde dosya görüntüleme ile ilgili özellikler bulunmaktadır. Bu menüye sütun başlıklarının üzerindeki satıra farenin sol tuşuyla ulaşılmaktadır.  
**- Birinci bölüm menü açıklamaları;**

**Group files and directories:** Menü işaretli değil ise seçili klasör içerisindeki bütün dosyalar alfabetik olarak listelenir. Grup olarak listelenmesi daha mantıklıdır.

**Group existing and deleting items:**Mevcut ve silinmiş ögeleri kendi arasında gruplandırır. Böyle olduğu zaman aradığımız dosyanın gözden kaçma ihtimali olabilir. Bunun için bu seçenek boş bırakılarak mevcut dosyadan sonra silinmiş dosyanın gelmesi sağlanmalıdır.

**Dbl-click:** Bir dizini çift tıkladığınızda dizini keşfedeceksiniz. Sıradan bir dosyayı çift tıklatarak görüntüleyebilirsiniz. Bu seçenek, alt nesneleri olan dosyaların tipik olarak çift tıklamayla görüntülenip görüntülenmeyeceğini denetler. Onay kutusu yarım işaretliyse, istenir.

**Open and search files incl.slack:** Dosyalar isteğe bağlı olarak boşluğu da dahil olmak üzere açılabilir ve aranabilir. Bu onay kutusunun orta durumu yalnızca mantıksal aramalarda fark yaratır.

**Show &.. :**Klasörlerin içerisindeki dosya sayılarını yanlarında gösterir.

**Listing the root directory:** Kök dizini listeleme

**List internal file system files:** Dahili dosya sistemi dosyalarını listeleyiniz.

**Appy filters to directories too:** Filtrelerin dizinlere de uygulanması isteğe bağlıdır. Aktif ise, bu sadece uygun filtrelerle ilgilidir. Dizinlere (Mantıksal, Tür Durumu, Karma, Karma Seti, Yazar, ...) uygulanmak için anlamlı olmayan filtreler uygulanmaz.

**Recursive selection statistics**: Özyinelemeli seçim istatistikleri

**Tag recursively:** Yinelemeli olarak etiketleyin

**Exclude recursively:** Yinelemeliri olanları hariç tut

**Advanced sorting(slower):** Gelişmiş sıralama (daha yavaş)

**No sorting initally after start,-up:** Başlangıçtan sonra sıralama yapılamaz

**Store dir. Browser settings in cases:** Mağaza dir.Durumlarda tarayıcı ayarlarının yapıldığı seçenektir.

**Dynamic e-mail & date columns:** Dinamik e-posta ve tarih sütunları

**1st sector:Pyshical sector no:** 1. sektör: Fiziksel sektör Numarası

**Show file count:** Dosya sayısını göster

**Special file icon for pictures:** Resimler için özel dosya simgesi

**Show checkmarks for tagging:** Etiketleme için onay işaretlerini göster:

**Display grid**: Ekran ızgarası

**Conditional cell coloring:** Koşullu hücre renklendirmesi

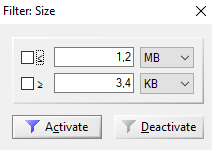
**İkinci bölüm menü açıklamaları;**

**Column widths in pixels**  
- Bu bölüm vasıtasıyla program arayüzünde görülen sütunlara ekleme veya çıkarma yapılabilir.  
- 0 (sıfır) değeri olan sütunlar gizlenmiş olanlardır. Görülmesi istenen sütunun değeri sıfırdan farklı bir rakam yapılmalıdır. Görülen sütunların genişlikleri elle de ayarlanabilir.  
- Sütunların yanlarında bulunan radyo düğmesi seçili hale getirilerek yukarı-aşağı yön tuşları  
ile sütunların yerleri değiştirilebilmektedir.  
- Hunisi mavi renkli olan sütun, o sütun ile ilgili bir filtreleme yapıldığı anlamına gelmektedir.  
- **Name >** Dosya ismi,  
- **Description >** Dosya çeşidi. Bu özelliğe bakarak bir dosyanın durumu hakkında bilgi sahibi olunabilir.  
- existing directory,  
- existing file,  
- previously ex. file, contents may have changed,  
- previously ex. file, first cluster not available  
- Renamed/maoved file, contents may have changed  
- Virtual file listed for examination purposes  
- traces of an e-mail message  
- with attachment  
- extracted e-mail  
- **Ext. >** Mevcut dosya tipini görüntüleme,  
**- Type >** Gerçek dosya türünü görüntüleme, Ext ile Type arasındaki fark, Type gerçek dosya tipini görüntülerken Ext. o an için belleğe kaydedilmiş dosyayı göstermektedir. Gerçekte jpg uzantılı bir dosya belleğe tmp uzantılı olarak kaydedilmiş olabilir.  
- **Status >** Dosya durumu hakkında bilgi verir.  
- **New identified >** Yakın zamanda yeni tespit edilmiş bir dosya türü. Üzerinde değişiklik yapılan dosya türlerini bulmaya yarar. Şüphelilerin mevcut dosya gizlemek/saklamak için uzantısını değiştirmişse bu özellik sayesinde tespit edilebilir.  
- **Confirmed >** Doğrulanmış, teyit edilmiş dosya,  
- **not confirmed >** Doğrulanmamış, teyit edilmemiş dosya. Dosya türünün isme uymamaktadır. Program bu dosya türünün ne olduğunu bilmemektedir. Görünüşte bir resim dosyası olan jpeg dosyası var ancak hiçbir dosyayla uyumlu değildir.  
- **Not in list** > Listeye dahil edilmemiş, listede olmayan dosyalar,  
- **irrelevant >** Konu ile ilgisi olmayan, içi boş dosyalar,  
- **Not verified >** Doğrulanmamış dosyalar,  
- **Type description >** Dosya tipi açıklamaları, dosyanın türüne göre bunun bir arşiv veya word dokümanı olduğunu belirtmektedir.  
- **Category >** Bilgisayarlarda kullanılan dosya tiplerine dosya türlerini göstermektedir. Bahsedilen bir dosyanın resim, text veya video olup olmadığını göstermektedir.  
- **Evidence object** > Dosyaların bulunduğu delil adı.  
- **Path >** Dosyaların delil içindeki yolunu göstermektedir.  
- **Sender >** Delil içindeki dosyayı gönderen kişi.  
- **Recipients >** Delil içindeki dosyaları alan kişi. Sender ve Recipients genellikle mail incelemede yararlandığımız bir özelliktir. Mail yolu ile gelen dosyayı alan kişi ile gönderen kişi buradan bulunabilir.  
- **Size >** Dosya boyutunu gösterir.  
- **Created >** Dosyanın ilk oluşturulma tarihi.  
- **Modified >** Dosyanın değiştirilme tarihi.  
- **Accessed >** Dosyaya son ulaşma tarihi.  
- **Record update >** Dosyanın son kaydedilme tarihi,  
- **Deletion >** Dosyanın silinme tarihi.  
- **Attr. >** Dosya niteliği, (Bkz. Attr. Menüsü)  
- **Owner >** Dosyayı oluşturan kişi, sahibi.  
- **Links >** Bir dosyanın kullanılma sayısı

# 25. Dosya İsmine Göre Dosya Filtreleme

- Name sütunundaki huni tıklanarak Filter menüsü açılır.   
- Bu pencere vasıtasıyla dosyaları ismine göre aramak  
mümkündür.  
- Aranacak kelimelerin başlangıç ve bitişinde yıldız işareti konursa arama daha sağlıklı yapılır.  
- Alt satıra yazılmak kaydıyla birden fazla kelime arama imkanı vardır.  
- İki yıldız arasında olmak kaydıyla tek bir satıra iki kelimeden  
oluşan aranacak kelime yazılabilir.  
- *Match Case* > Büyük küçük harf duyarlı olarak, birebir eşleştirerek arama yapar.  
- Aranan dosya ismi ve uzantısı tam olarak biliniyorsa, buna  
ulaşmak daha hızlı olacaktır. (Örn: index.dat gibi)  
- Dosya isminin ilk birkaç harfini yazıp, geri kalanına yıldız işareti koyarak emin olmadığımız dosya isimlerini de bulmamız mümkündür.  
- FAT dosya sistemine sahip bir sistem incelemesinde, arama neticesinde başında soru  
işareti çıkan dosyalar var ise, program bu tür dosyaların ilk harfini bilmediğini, bunun aranan dosya olma ihtimali olabileceğini tespit ederek filtrelemeye dahil etmektedir. Çünkü, FAT dosya sisteminde bir dosya silindiğinde ilk harfi de silinmektedir. Ancak bu durum NTFS dosya sisteminde geçerli değildir.

# 26. Dosya Boyutuna Göre Filtreleme

- Ana ekrandan size sütunun hunisi seçildiğinde   
karşımıza ***Fitler : Size***menüsü gelecektir.  
- Bu menü vasıtasıyla, belirli bir dosya boyuttan daha  
küçük/büyük dosyalar ile verilen iki kriter arasındaki ölçülere uyan dosyaları listelemek mümkündür.  
- Bu özelliği kullanarak internet resim dosyaları gif  
resimlerini gizleyerek daha rahat bir çalışma ortamı hazırlanabilir.

# 27. Yeni Dosya Türü Ekleme

Program filtre bölümündeki mevcut dosya türlerine yeni tespit edilen dosya isim ve türlerini eklemek mümkündür.  
- Programın kurulu olduğu dizin içerisinde  
(*Files>XWays>File Type Categories.txt*) File Type Categories.txt isimli text dosyası dosya türlerini tutmaktadır.  
- Yeni eklenecek dosya isimi ve formatı uygun olan klasör altına önceki formata uygun olarak eklendikten sonra kaydedilerek çıkılır.  
- Program yeniden başlatıldığında eklenmiş olan dosya adı ve formatını filtre bölümünde gözükecektir.  
- Filtreleme menüsü açıldığında, hangi filtrelemenin otomatik seçilmesi isteniyorsa, o dosya başına artı (+) işareti  
konulması gerekmektedir.

# 28. İçinde Geçen Kelimeye Göre Dosya Filtreleme

İncelenen imaj içerisinde aranılan bir kelimeyi bulmak için, hedef imaj seçili iken **Search> Simultaneous Search (kısayolu Alt+F10 veya mavi dürbün)** yardımıyla kelime arama menüsüekrana çağrılır.

- İmaj üzerindeki kelime aramaya ilaveten klasör üzerinde de kelime araması yapmak mümkündür. Bunun için hedef klasörün üzerinde sağ tuş ile Simultaneous Search menüsü açılmalıdır.

- Kelime araması bittiğinde, önceki aranan kelimeler arama kutusundan bulunabilir.

- Aranacak kelimeler disket işareti ile bilgisayara txt olarak kaydedilerek diğer yapan personele gönderilme imkanı vardır.

- Her satıra bir kelime yazılmalıdır. Ancak aranacak olan eğer 2 kelimeden oluşuyor ise arada boşluk bırakılmalıdır.

- Arama işlemi bittiğinde Case Data bölümünün altında aranan kelime ile bulunan miktarlar listelenmektedir.

- Kelimenin geçtiği dosyalar listelenmek istenirse, Case Data bölümü altında, arama neticesinde bulunan hedef kelime seçilmelidir.

***- Arama neticesinde,***

- Search hits ile aranan kelimenin yerleri,

- Name ile kelimenin geçtiği dosya isimleri,

- Size ile dosya boyutu,

- #ST ile birden fazla arama yapılan kelimeden hedef dosyada kaç adet bulunduğu,

- Search terms bölümünde hedef dosyada aranılan hangi kelimeler bulunduğu listelenmektedir.

- Bulunan kelimelere ait dosyaları program vasıtasıyla önizleme olarak incelemek, bir rapora dahil etmek veya recorvery/copy yaparak dışarı çıkarmak mümkündür.

- Hedef kelimeleri içeren dosyalar bir rapor dahil edilmek istenirse, farenin sağ tuşunda bulunan Report Table association menüsü yardımıyla rapor klasörüne dahil edilebilir.

- Ofset bölümünün boş olması, bu dosyanın NTFS dosya sistemi ile sıkıştırılmış olduğu veya bunun şifreli bir dosya olduğunu göstermektedir.

# 29. Simultaneous Search Menü Açıklaması

**ANSI-Türkçe(1254):** Arama işlemini kullanıcının bilgisayar diline göre yapar.

**Unicode UTF-16 LE:** Bu seçenek işaretlenmemişse, aradığımız kelime arasında boşluk var ise arama olumsuz sonuçlanacaktır.

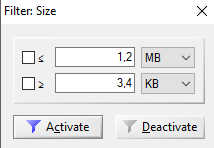
**Unicode UTF8:** Arama işlemini şüphelinin bilgisayar diline göre yapar.

**Match case:** Büyük küçük harf duyarlı olarak arama yapar.

**GREP syntax :** Aranacak iki kelime arasında başka bir karakter veya boşluk olabileceği düşünülüyorsa bu seçenek aktif yapılamalıdır. Bu menü seçildiğinde altında çıkan search Windows kutusu, iki karakter arasındaki boşluk miktarını belirtmek için kullanılır. Bu menü iki kelime arasında normalden bir boşluk bırakılması veya yanlışla bir karakter girmesi gibi konularda önem arz edecektir.

**Whole words only** : Kelimenin tamamını arar. Windows’un tırnak içindeki araması gibi

# 30. Resim Dosyasının Pikseline Göre Filtreleme

Resimlerin pixel özelliğine göre filtreleme yapmak için ***Directory Browser Options > Dimension* (boyut)** menüsü açılır.  
- Buradan istenilen boyuttan küçük, büyük veya iki boyut arasında olan resimlerin filtrelemesi yapılabilir.  
- Bu menünün faydası hedef durumunda olmama ihtimali olan özellikle gif uzantılı resimlerin inceleme ekranından uzaklaştırılarak dosya sayısı azaltılabilir.

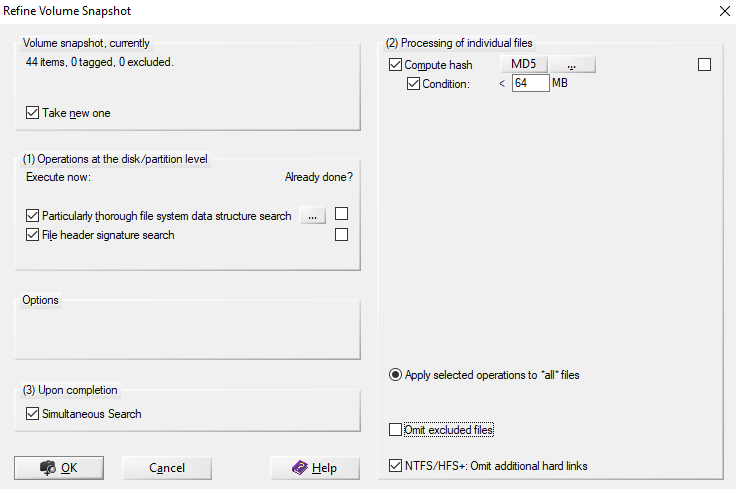
# 31. Refine Volume Snapshot

Dava dosyasına yeni bir imaj eklendiğinde zaman program tarafından bir snapshot başlatılmaktadır. Ancak ayarlamalar yapıldıktan sonra yeniden bir snapshot yapılarak programın bir veri tabanı oluşturarak inceleme hızını arttırmak mümkündür.

- Snapshot bölümünün sağında bulunan **Already done** menüsü tam işaretli ise söz konusu menünün daha önce çalıştırıldığını, yarım işaretli ise menü çalıştırıldıktan sonra yeni bir dosya bulunduğu anlamına gelmektedir.

- Snapshotta bulunan menüler aynı anda kullanılabilir.

- Snapshot veri tabanı boyutu (snapshot kapasitesi), içerisindeki toplam parça sayısı, işaretlenmiş dosya sayısı, gizli dosya sayısı ve daha önceden bakılmış dosya sayısı gösterilmektedir.İnceleme sırasında, program yeni veriler tespit ettikçe items sayısı artacaktır.

***- Refine Volume Snapshot Menüsü***

**Take new one**:Yeni bir snapshot yapmak. Yeni bir snapshot yapılmak istendiğinde,program önceki snapshot ile birlikte toplanmış olan verileri veişaretlemeleri kaybedeceğimiz yönünde bir ikaz verir. Eğer işlemlere yeniden başlamak istenirse bu işaretlenmelidir. Bu işlem ilk dava dosyası oluşturulurken yapılmalı ve inceleme yapılmaya başlandıktan sonra yapılmamalıdır.

**Particularly thorough file system data structure search :** MFT dosya sistemindebulunmayan sektörlerdeki dosyalar aramak içinkullanılır. Bu menü ile yer değiştirmiş, taşınmış veyadefrag neticesinde kümesi değişmiş küçük dosyalarıbulmak için kullanılabilir.

**File header signature search** :(Bkz:File header signature search (Dosya başlığına Göre Arama)

**Compute hash :** Dosya veya klasörlerin MD5 değerlerini hesaplamamızı sağlar. Eğer dosya içeriği yok ise MD5 hesaplama da yapılmayacaktır. (Bkz.: Compute hash – Dosya Hash Değeri Hesaplama)

**Apply selected operations to \*all\* files:** İşlemi bütün dosyalara uygula.

**omit excluded files:**hariç tutulan dosyaları atla

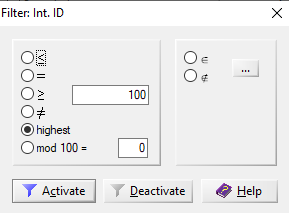
# 32. Compute hash – Dosya Hash Değeri Hesaplama

Dosya veya klasörlerin MD5 değerlerini hesaplamamızı sağlar.  
Eğer dosya içeriği yok ise MD5 hesaplaması da yapılmayacaktır.  
Bu menü seçildiğinde yan tarafında bulunan bir radyo düğmesi aktif olacaktır. Buradan yapılacak olan hash hesaplama türü seçilebilir. Genellikle MD5 ve SHA1 değerleri tercih edilmelidir.  
Yan tarafta çıkan ***Verify hash***kutusu hesaplanan hash değerinden sonra hash değerinin yeniden kontrol edilmesini sağlayacaktır.  
Hesaplama işlemi bittiğinde hash değerlerini görmek için ***Directory Browser***menüsünden  
hash sütunu görünür yapılmalıdır.

# 33. Compute hash –Hash Değeri Karşılaştırma

- ***Matc hash values against hash database***menüsü, şüphelinin bilgisayarındaki sistem  
dosyaları ile bizdeki mevcut sistem dosyaları karşılaştırmak amacıyla kullanılır. Şüphelinin bilgisayara ait sistem dosyaları arasına saklamış olduğu dosyaları bulmak için kullanılabilir. Dosyaları kopyalamak yerine mevcut dosyaların hash değerleri çıkartılır ve hedef durumundaki şüphelinin dosyaları ile karışlaştırılır.  
- Her işletim sistemi için yeni bir temiz kopya oluşturularak bunların imajları alınır. Bu temiz  
sistemde bulunan dosyalar ile şüphelinin imajındaki sistem dosyaları karşılaştırılır. Şüphelinin sistem dosyası içerisindeki dosyalarda bir değişiklik yapıp yapmadığı anlaşılabilir.  
***- Dava dosyası ile ilgili hash setleri oluşturma;***  
- Hash seti hesaplanacak klasör/dosya seçilir,  
- Sağ tuş>*Creaet Hash Set* seçilir,  
- *Add Hash Set to Database* menüsü gelir. Eğer daha önce bir filtreleme var ise bu menünün sağ üst köşesinde huni şeklinde gözükmektedir.  
- Hash değerinin MD5 olarak hesaplanacağı gözükmektedir.  
- Hash Categorisi olarak  
- *İrrelevant*… > ilgisiz dosyalar, (windows işletim sistemi veya ofis dosyaları  
türündeki belgeler)  
- *Notable*… > önemli dosyalar, (şüphelilere ait özel dosyalar)  
- *Only existing files* > Sadece mevcut dosyalar dikkate alınacak, silinmiş veya temp türündeki dosyalar dikkate alınmayacaktır. Hash değeri hesaplanmış dosyalar başka kullanıcılar ile de  
paylaşılabilir.  
- *Name* > Hesaplanan hash değerlerinin kaydedileceği dosya ismi.  
- Tamamı seçtiğimizde işlem bittiğine dair Operation Complete menüsü gelmektedir.  
- OK tuşu ile birlikte daha önce hesaplanmış olan MD5 listesi ekrana gelmektedir.  
- Burada gözüken klasörlerin içerisinde kaç adet dosya bulunduğu görülmektedir.  
- Hash değeri dışarı aktarılacak klasör seçilerek Export tuşu ile istenilen yere kaydedilir.  
- Bu menüdeki Toggle Category ile klasörün yan tarafında bulunan irrelevant veya Notable özelliği değiştirilebilir.  
- Bu işlem sırasında istenmeyen dosyalar filtrelenebilir.

# 34. Skin tone and b&w detection in Picture

Bazı resimler 16X16 picksel boyutunda olabilirler. Bunlar hacim olarak dikkate alınamayacak kadar küçük resimlerdir. Siyah beyaz özelliğindeki resimler ile yine küçük boyutlu resim olduğu değerlendirilen dosyaları bulmak için bu seçenek işaretli iken bir snapshot yapılır.  
- Bu menünün sonucunu görmek için Directory Browser bölümünden SC% sütunu görünür yapılmalıdır.  
- SC% sütunu açıldığında ? filtreleme yapılırsa, bulunanların resim dosyası olabilecekleri tahmin edilmekte ancak hasar görmesi  
sebebi ile resim gösterilememektedir.  
- İrrelevant dosyalar ise ilgisiz resim dosyalarıdır.  
- b/w ise siyah beyaz resim dosyaları bulmak için kullanılabilir. b/w ile fotokopi resimleri  
bulmak için kullanılabilir.

# 35. File header signature search (Dosya başlığına Göre Arama)

- İmaj içerisindeki boş alanlarda dahil olmak üzere veri araması yapmaktadır.

- Menü çalıştırıldığında, inceleme yapılan imaj üzerinde dosya araması için File Type(s) menüsü gelecektir. Burada hangi dosya türü/türleri aranacaksa onlar işaretlenmelidir.

- Default file size > Varsayılan dosya boyutu.

- Respect individual default sizes in file type definitions > Hedef dosyaları arama için kullanılır. Default file size bölümüne en küçük değer girilir, ardından Max.File Size …..times default size kutusuna da Default file size bölümünde yazan değerin kaç katına kadar bir dosya aranması istenilen rakam yazılmalıdır. Eğer belirli bir hedef yok ise respect kutusu kapatılmalıdır.

- Filename prefix > Dosya isminin önüne karakter koyma. Aradığımız dosya türünün diğerlerinden farklı bir şekilde ayrılması isteniyorsa buradaki kutuya bir karakter girilmelidir. Bu alana girilen karakter, arama neticesinde bulunan dosyaların önüne konacaktır. Name (isim) filtrelemesi yapılırken bu karakter joker olarak verildiğinde söz konusu dosyalara daha rahat erişilecektir.

- İntelligent namig, where possible > Akıllı adlandırma, orijinal dosya isimlerinden değil dosya içeriklerinden anlamlı bir şeyler tespit etmek amacıyla işaretlenir.

- Look for headers everywhere > Her yerde ara. Arama sırasında bu seçeneğin işaretli olması gerekmektedir.

- Look for headers in free clusters only > Boş cluster(küme)’da ara.

- Look for headers in allocated space only > Ayrılmış boş alanlarda ara.

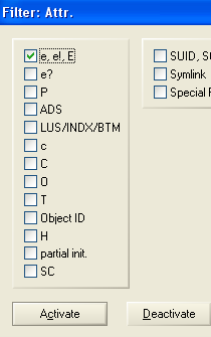
- Search in block only > Sadece block bölümlerde arama yap.

- Search at cluster boundaries, if possible > Mümkünse kümenin sınırlarında ara. Bir önceki kümenin sonu ile diğer kümenin başlangıç kümesi arasında kalan sınırlarda arama yapılmasını sağlar.

- Search at cluster boundaries > Kümenin sınırlarında ara. Bu menüde aramak iyidir.

- Extensive byte-level search > Geniş byte seviyesinde arama yapma. Bu menüde arama uzun sürer, arama neticesinde birbirine benzeyen ama işe yaramayacak olan dosyaları da bir araya getirecektir.

# 36. Şifreli Dosyaları Bulma

-Snapshot menüsünde bulunan File format specific and statistical encryption tests menüsü seçili halde iken yapılan araştırma neticesinde imaj içerisindeki şifreli dosyalar bulunabilir.

- Arama işlemi bittikten sonra Attr. Menüsünün filtresi açılır. Bu filtrede içerisindeki encryption şifre kısaltması olan e harfleri şifreli dosyaları göstermektedir.

- E > dosya sistemi tarafından şifrelenmiş bir dosyayı göstermekte

olup normal bir snapshot ile bulunabilir

- e > bir arşiv sistemi içinde şifrelenmiş,

- e! > şifre korumalı olan dosyaları işaret etmektedir.

- e? > istatiksel şifrelemeyi ortaya çıkarır, ? tahmin anlamına gelmekte olup bu tür dosyaların şifreli olduklarını tahmin edilmektedir.

# 37. Hash’leri Aynı Olan Dosyaları Ayırma

- İnceleme sırasında üzerinde çalıştığımız imajlar içerisinden hash değeri aynı olan dosyalar ile karşılaşabiliriz. Bunu klasik yöntemlerle ayırmaya çalışmak çoğu zaman imkânsız veya çok zaman alan bir iş olacaktır. Hash değeri aynı olan bu tür dosyaları bu program yardımıyla ayırmamız mümkündür.

- İlk önce programa çalışacağımız imaj veya disk programa yüklenir.

- F10 ile **Snapshot** menüsü çağrılır.

- Ayrılacak dosya türleri belli ise **File reader….** menüsünden bu dosyalar seçilir.

- **Compute hash** menüsünün yanındaki kutudan doğrulama şifresinin türü seçilir. Genellikle MD5 kullanılmaktadır. Ayarlar yapıldıktan sonra dosyaların MD5 değerlerinin hesaplamasına geçilir.

- Hesaplama bittiğinde hash değerleri sütunlar arasında gözükmeyebilir. Bunun için **Directory Browser** menüsünden hash sütununun değeri sıfırdan farklı bir rakam girilmelidir.

- İşlemden sonra **partition** üzerinde sağ tuş ile **Explore Recursively** işaretlenerek klasörler içerisindeki dosyalar alfabetik olarak listelenir.

- Attr. Menüsü açılır ve buradan **duplicates found** menüsü aktif edilir.

- Alfabetik olarak sıralanan dosyalar hash değerine göre sıralanacaktır.

- Bu işlemden sonra hash değerleri aynı olan herhangi bir dosyaya bakıldığında bütün dosyalar bakılmış olarak işaretlenecektir.

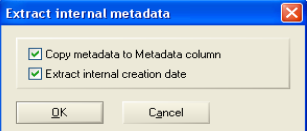
- İnceleme ekranında her dosyadan bir tanesinin kalmasını, diğer dosyaların ise gizlenmesi istenildiğinde, ekrandaki bütün dosyalar seçili hale getirilir.

- Farenin sağ tuşunda bulunan **Hide>Duplicate in dir. Borwser based** on hash menüsü seçilir.

- Bu işlemlerden sonra ekranda hash değeri aynı olan dosyalardan sadece birer adet kalacaktır. Bundan sonra kopyalama işlemine geçilebilir.

# 38. Dosya Gizleme

- Üzerinde çalıştığımız dosyaların başka personel tarafından görülmesi istenmiyor veya gereksiz çok dosya var ise bunlardan bazıları gizlenerek daha rahat bir çalışma ortamı sağlanabilir.  
- Gizlenmek istenen dosyalar fare yardımıyla seçilir.

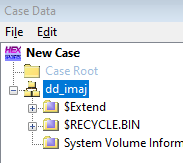
Seçili dosya üzerinde farenin sağ tuşu ile ***Hide***menüsü seçildiğinde sağ tarafta seçilen dosya sayısı gösterilmektedir. Bu menüye basıldığında seçilmiş dosyalar gizlenecektir.  
- Programın sağ üst köşesinde ise yine yapılan filtreleme gösterilmektedir.  
- Yapılan gizlemelerin iptal edilmesi için ***Directory Browser***menüsünde bulunan ***Unhide All***menüsüyle mümkündür. Bütün gizlenmiş dosyalar normale dönecektir.  
- Gizlenmiş dosyalar gözüksün ancak gizli oldukları yine belli olsun istenirse ***Directory Browser***menüsünde bulunan ***List hidden items***in işaretli olması gerekmektedir.

# 39. Dosya Seçme (Tag);

- İnceleme sırasında bazı dosyalar önem arz edebilmektedir. Önem arz eden veya soruşturmayla doğrudan ilgisi olduğu düşünülen dosyalar işaretlenmelidir. Bunun için dosya/dosyalar seçili halde iken farenin sağ tuşunda bulunan Tag menüsü işaretlenmelidir.

- İşaretlenmiş dosyanın başındaki kare kutusunun rengi gri renge dönüşecek, dosyanın bulunduğu klasörün üzerinde ise yarım Tag görülecektir.

- Klasör üzerinde yarım tag lenmiş işaret var ise o klasör içerisinde tag lenmiş dosya bulunduğu anlamına gelmektedir.

- İnceleme işlemi bittiğinde ekrana sadece tag lanmış olan dosyaları getirmek, bir rapora dahil etmek veya sadece onları kopyalamak mümkündür.

- Yine dosya gizleme özelliği olarak bu işaretlenmiş (tag) dosyaları gizlemek mümkündür.**Directory Browser Filters** menüsünden **List Tagged İtems** menüsü vasıtasıyla taglanmış dosyaları göstermek veya gizlemek mümkündür.

- Klasör içerisindeki bütün dosyalar tag’lanmak istenirse **Case Data** bölümünde ilgili klasörün üstüne farenin orta tuşu ile bir kez tıklamak yeterlidir.

# 40.Dosyaların metadata özelliklerini inceleme;

- Dosyaların metadata özellikleri Details menüsüyle mümkündür.

- Dosyaya ait özellikler aşağıda listelenmiştir.

* Name > Dosya ismi
* Description > Mevcut veya silinmiş dosya açıklaması
* Ext. > Mevcut tipi
* Type > Tipi
* Status > Confirmed (doğrulanmış),
* Type desc. > Tip açıklaması
* Category > Kategorisi
* Evidence object > Bulunduğu delilin ismi
* Path > Bulunduğu yol
* Size > Boyutu
* Created > Oluşturulma tarihi
* Modified > Güncellenme tarihi
* Accessed > Ulaşma tarihi
* Record Update > Son kaydedilme
* Attr. > Özelliği
* Owner > Sahibi,
* Links >
* 1st Sector > Dosyanın sabit bellekteki başlangıç sektör numarası
* Hash > Dosyanın hash değeri

- **Directory Browser Options** menüsündeki Metadata değeri sıfırdan farklı bir rakam girildiğinde Metadata sütunu gözükür hale gelecektir.

- Bir dosyanın Metadata özelliğinin hepsi bir sütunda görülmek isteniyorsa, farenin sağ tuşu ile **Extract internal metadata**… menüsü çağrılır.

* Copy metadata to Metadata column > Dosyaların Metadata larını Metadata sütununa kopyala
* Exract internal creation date > Metadata nın oluşturulduğu tarihi oluşturma.

- Bu menü ile dosyaların metadata bilgileri Metadata sütünunda gösterilmiş oldu. Bu metadata bilgileri rapora veya Export List özelliğine dahil edilebilir.

- Office 2003 belgeleri ile ilgili birçok metadata bilgisi tutulmaktadır. Önceki açıklamalara ilaveten,

* Dosya sahibini,
* En son kaydedeni,
* Son yazdırılma tarihini,
* Sayfa sayısı ve karakter sayısını,
* Tanımlanmış yüklü yazıcıyı,
* Belgeye erişen son 10 kullanıcıyı,
* Kullanılan işletim sistemini,
* Belgenin başlığını tespit etmek mümkündür.
* Metadata bilgileri Office 2003 programından sonra tutulmamaktadır.

- 4.0 olup sonu 0 ile biten sistemler server sistemler, 5.1 gibi sonu bir ile bitenler xp gibi kişisel işletim sistemleri olarak tanımlanmaktadır. Kullanılan işletim sistemini tespit etmek için dos komut sistemi açılır ve oraya ver komutu yazılır. Karşımıza kullanılan işletim sisteminin özelliğinin belirtildiği

# 41. Registry kayıtları

- Registry kayıtları bilgisayar sistemlerinin gizli kayıt defteri olup işletim sistemleri ile bu dosyaları incelemek mümkün değildir.

- Bu dosyalar her Windows tabanlı işletim sistemlerinde tutulmaktadır.

- Registry kayıtlarını açığa çıkarmak için **Fitler Type** menüsünden **Windows Registry** aktif edilir.

- İncelenmek istenen dosya/dosyalar farenin sağ tuşunda bulunan view menüsü yardımıyla **registry Viewer** programı ile görüntülenir.

**- Registry Viewer** içerisinde bulunan dosyaları raporlamak için farenin sağ tuşu Create Report seçilmelidir. Program hafızasında tutulan **registry** kalıp dosyaları karşımıza gelecektir. Bu dosyanın hangi registry kalıp dosyası ile açılmak istenirse o dosya seçilmelidir. Kaydedilecek yer ile dosya ismi girildiğinde rapor hazırlanmış olur.

- Bu tür dosyaları incelediğimiz dava dosyası içerisinde oluşturulacak bir klasörde toplamak faydalı olacaktır.

- Rapor dosyasında çıkacak konu başlıklarına bakıldığında;

**- CPU:** Merkezi işlem biriminin ismi ve hızı,

**- Mounted device**: İşletim sistemine yüklenmiş olan her türlü sürücü buradan takip edilebilir.

**- Model description of installed network card:** Bilgisayara takılı network kartı ismi ve numarası

- **Nero Recorder** : CD-DVD yazma programı kurulu olduğu, Edgar isimli kullanıcı tarafından 10.09.2004 tarihinde S sürücüsü içerisinde bulunan Schiller isimi dosyanın yazdırıldığı

- **Autorun Icon :** Y sürücü içerisinde bulunan data.icon isimli dosyanın otomatik olarak yüklendiği

***- Bilgisayara takılı sürücülere yapılan erişimlerin geçmişi***

* **Last Access** > Son ulaşılan tarihi,
* **Description >** Açıklama, ulaşılan sürülere ait açıklamalar
* **DiskID** > Ulaşılan diskin ID numarası
* **User** > Kullanıcı

***- Registry kayıtları (Default- Reg Report Free Space);***

**- Total free space >** Registry dosyalarındaki boş alanları göstermektedir.

**- Extract from value slack** > Slack alanlardaki kısayollar

- **Programs Cache Slack** > Çalıştırılan programlar veya dosyaların Slack alanlardaki izleri26

- **Recent documents opened in Acrobat Reader** >NTUSER.DAt dosyası içerisinde son dönemde açılmış olan PDF dosyaları,

- **MS Access** > Recent File > Son zamanda açılmış Microsoft ofis veri tabanı dosyaları,

**- MS Excel**> Recent File list > Son zamanda açılmış Microsoft ofis veri tabanı dosyaları,

- **Last Download …>** Outlook email programına indirilen dosyanın yeri,

- **Word Recent Files** > Son zamanda açılmış Microsoft ofis word dosyaları,

- **Expression that were searched for in local files, folders, documents** > Bilgisayarın arama özelliği kullanılarak yapılan arama neticesinde tutulan kayıtlar

- **Printers, computers or people that were searched for >** Bilgisayardan çevredeki yazıcı, bilgisayar veya kişi arama neticesinde tutulan kayıtlar

**- Last key edited by ;RegEdit** > Regedit kayıtlarında en son yapılan ayarlamayı gösterir.

**- Folders Visited** > En son ziyaret edilen klasörler

- **File that were opened or saved** > Açılan veya kaydedilen dosyalar

**- Web pages visited with IE (Decrypted**) > İnternet Explorer ile ziyaret edilen web siteleri olup şifrelenmiş haldedir.

- **Program started (Decrypted)** > Çalıştırılan programlar.

- **WallPaper MRU**> Değiştirilen duvar kağıtları,

- **Folder view** > Bakılan klasörler

- **Winrar Compression History >** Sıkıştırma dosyasının geçmişi

**- Active computer name** > Kurulum sırasında bilgisayara verilen isim

- **User-Configured daylight saving time** > Güneş ışığından faydalanma amacıyla o bölgenin saat dilimi

**- User-Configured time zone** > Yükleme sırasındaki o bölgenin saat dilimi

- **Windows installition language** > Windowsun kullandığı dil

**- Bios Date** > Biosun kullandığı zaman

- **Nero Company** > CD yazma programın lisansının alındığı şirket adı.

- **Nero User** > CD yazma programın lisansının alındığı personel adı.

- **Profile location of** > Bilgisayarda bulunan kullanıcılar

**- Name of registered person** > Windows lisansının kayıt ettiren personel

**- Domain that last user logged on to** > Yükleme sırasında oluşturulan Domain adı

- **Last logged on User** > Programın yüklenme sırasında oluşturulan kullanıcı ismi

**- Outlook Profile** > Mail programı olan Outlook’un kurulum sırasında hangi mail adresi ile kurulduğu

**- User spesific directories** > Kullanılan klasörler

- **Unread Mail of** > Okunmayan mailler

**- ICQ user name** > ICQ programında girişte kullanılan isim

- **SAM >** Sam dosyasının içerisinde kullanıcılara ait şifreler tutulmaktadır.

- Default dosyasına ait raporu Reg Report Printer formatı ile oluşturduğumuzda;

- **Default Printer** > Yüklenen varsayılan printer

- **Curren printer** > Güncel olarak kullanılan printer

- **Printer port >**

- **Print providers logon time >** Printerin sisteme yüklendiği tarih

**- User spesific** >

**- Most recent application that used Direct3D** > En son özel olarak kullanılmış program

- **Windows installer** > Son yüklenen Programın yeri Temp dosyası

**- App Management** > D sürücünde bulunan bir programın bir kez yüklendiği

**- USer spesific auto start programs** >Windows yüklendiğinde otomatik çalışan programlar

**- Cache for installed executables** > Windows başlatıldığında RAM a yüklenen programlar

- **App Management** > Windowsa yüklenen programlar ile yüklenme sayıları (count)

**- Dirty shutdown** > Bilgisayarın elektrik düğmesinden kapatılması

**- Atteched devices by serial number** > Bilgisayara takılan sürücülerin seri numaraları

**- Driver installed** > Yüklenen sürücüler/USB ler

**- App Management** > D sürücünde bulunan bir programın bir kez yüklendiği

**- User spesific auto start programs** >Windows yüklendiğinde otomatik çalışan programlar

- **Cache for installed executables** > Windows başlatıldığında RAM a yüklenen programlar

**- App Management** > Windowsa yüklenen programlar ile yüklenme sayıları (count)

**- Version Number** > İşletim sisteminin numarası 5.1, kişisel işletim sistemi XP

- **Installation date >** İşletim sisteminin yüklenme tarihi

- **Product number** > Ürün numarası

- **Windows CD Key** > İşletim sisteminin yükleme anahtarı

- **Name** > İşletim sisteminin adı

- **Name of registered name** > Kayıtlı kullanıcı adı

**- Build Number** >

**- Processor architecture** >

**- Service pack** > Yüklenen servis paketinin adı

- **CPU FrienlyName** > Yükleme sırasında bilgisayardaki işlemcinin ismi ve gücü

**- User-Configured time zone** > Yükleme sırasındaki o bölgenin saat dilimi

- **User-Configured daylight saving time** > Güneş ışığından faydalanma amacıyla o bölgenin saat dilimi

- **Last logged on User** > Programın yüklenme sırasında oluşturulan kullanıcı ismi

- **Time of last system shutdown** > Bilgisayarın en son kapatılma zamanı

**- Mounted device** > Programa takılan sürücülerin listesi, takılan CDRom veya DVD ile USB bellekleri buradan takip edilebilir.

- **Model description of installed network card** > Bilgisayara takılı network kartı isi ve numarası

- **Local Machine > İnstalled Programs >** Name > İşletim sistemin kurulduktan sonra yüklenen programlar,

- **User spesific auto start programs** > Windows yüklendiğinde otomatik çalışan programlar

# 42. İnternet Kayıtlarını İncelemek

- Windows işletim sistemi kullanan şüphelinin internet ortamında hangi siteleri ne sıklıkla kullandığının tespit edilmesi dava dosyası açısından gerekebilir. Bunun için windows’un internet kayıtlarını tuttuğu dat uzantılı internet geçmiş kayıtlarının incelenmesi gerekebilir.

- Filtre özelliğinden History.dat ve index.dat uzantılı dosyalar filtre edilir.

- Ekrana gelen History.dat ve index.dat dosyaları kurtarma yöntemi ile oluşturulacak İndeks isimli klasöre çıkartılır.

- Dışarı çıkartılan bu dosyaların incelemesi X-Ways Trace programı ile yapılacaktır.

- **File>Open** File menüsünden kaydettiğimiz dat dosyaları programa yüklenmelidir.

- Hata mesajı ekrana gelebilir. Bunun anlamı “sadece lisanslı kullanıcılar 500 den fazla kaydı inceleyebilir” anlamına gelmektedir.

- İşlem tamamlandığında daha önceden kaydedilen dat dosyaları programa yüklenmiş olacaktır.

***- Buradaki sutun başlıkları***;

* Last Visited > Web sitesine yapılan en son ziyaretin tarihi,28
* File date of server > Server makinesinde ziyaret edilen dosyanın oluşturulma
* tarihi,
* Prot. > Protokol anlamına gelmekte olup http siteleri normal
* olanlar https ler ise güvenli siteler anlamına gelmektedir.
* Domain > Ziyaret edilen web sitesinin adı,
* Resource > Web sitesinde bakılan dosyanın kaynağı,
* Cache Filename > Bakılan dosyanın ismi,
* Size > Bakılan dosyanın büyüklüğü,
* Ext. > Bakılan dosyanın türü,
* Count > Dosyaya bakılma sayısı,
* User > Kullanıcı,
* Address > Bilgisayarın iletişimde kullandığı adres,

- Bu dosyaları export ederek daha rahat incelemek mümkündür.

- Bütün kayıtlar seçili hale getirilir ve File>Export menüsü seçilir.

- Kayıt yeri ve ismi girilir.

- Tamam seçildiğinde bu export verilen isimde txt dosyası olarak kaydedilir. Program bunun txt dosyasına ilaveten Excel dosyasına aktarılmasını istiyor musun diye soracaktır. Evet seçildiğinde aynı kayıtlar excele dosyasına da aktarılmaktadır. Eğer Excel başlatılmazsa, işlem boş bir Excel sayfası açıldıktan sonra yapılması gerekecektir.

# 43. EMail Kayıtlarını İncelemek;

- İşletim sistemlerinde bulunan e-mail kayıtlarını incelemek için;

- Snapshot bölümünde bulunan maillerle ilgili kutucuk seçildikten sonra yapılacak bir snapshot’tan sonra mail incelemeye geçmek daha iyi olacaktır.

- Filtreleme bölümünden E-Mail kayıtlarını seçiyoruz.

- Bulunan kayıtları incelemek için dosyayı seçtikten sonra farenin sağ tuşu ile view menüsü seçildiğinde, sağ tarafa ilgili mailin içeriği çıkartılacaktır.

- Bir başka mail olan msg uzantılı mail dosyası view ile görüntülendiğinde yine sağ tarafa mail içeriği açılacaktır. Mailin eki altında gözükmektedir. Ek incelenmek istendiğinde, ekin üzerine tıklandığında maile eklenmiş olan resim görülebilecektir.

# 44. Silinmiş dosyaları kurtarmak;

- Sadece silinmiş dosyalar kurtarılmak istenirse **Directory Browser Options** menüsünde bulunan mevcut dosyaları göster menüsü olan **List Existing files** kapatılır.

- Sağ üst köşede mevcut dosya sayısını 0 olarak gözükecektir.

- Ekrana sadece silinmiş dosyalar getirilecektir. Aranan bir dosya türü var ise dosya türünden filtreleme yapılabilir.

- Kurtarılacak dosyalar seçildikten sonra farenin sağ tuşu ile **Recorvery/Copy** menüsü yardımıyla silinmiş dosyalar kurtarılır.

# 45. Mevcut Dosyaları Kopyalamak;

* Sadece mevcut olan dosyalar kurtarılmak istenirse **Directory Browser Options** menüsünde bulunan mevcut dosyaları göster menüsü olan **List Existing files** açılır, silinmiş dosyalar olan Lst previously… kapatılır.
* Sağ üst köşede mevcut dosya sayısını gösterilecektir.
* Ekrana sadece silinmiş dosyalar getirilecektir. Aranan bir dosya türü var ise dosya türünden filtreleme yapılabilir.
* Kurtarılacak dosyalar seçildikten sonra farenin sağ tuşu ile **Recorvery/Copy** menüsü yardımıyla silinmiş dosyalar kurtarılır.

# 46. Sistem dosya sayıları

* Windows XP işletim sisteminde ortalama 20.000-30.000,
* Windows 7 işletim sisteminde 30.000-40.000
* Mac işletim sisteminde 441.000-Bir milyon,
* Ext2 dosya sistemini kullanan Linux sistemlerinde 10 binden fazla,
* Linux işletim sisteminde ise birkaç binden 50 bine kadar çıkabilen dosya sayısı vardır.
* Temp klasörün içerisinde bulunan dosyaların hash değerleri bulunmamaktadır.29
* Ext2 de ise 10 binden fazla en az 175.000 civarında

# 47. Sistem İnceleme

* Bir incelenmeye başlamadan önce yapılacak faaliyetler;
* X-Ways programının son sürümü olmalı,
* İnceleme neticesinde çok sayıda dosya ve klasör açığa çıkabileceğinden, hedef belleğin yeteri büyüklükte olmalı,
* Dava dosyası mutlaka işletim sisteminin olmadığı sürücüye açılmalı,
* Dava dosyası içerisine davalar, indexler, raporlar, imajlar,… isminde klasörler oluşturulmalı,
* İncelenecek imajlar dava dosyası içerisindeki kendi klasörüne konmalı,

- Dosyaları istenilen başka bir sürücüye kopyalamak için **Options > Security** açılmalı,

**- File>Create new case** ile yeni bir dava dosyası oluşturulmalı, hedef klasör olarak oluşturulmuş olan dava dosyasına yönlendirilmeli,

**- File>Add image** ile imaj dosyası programa yüklenmeli,

**- Tools>Disk Tools>Scan for lost partitions** ile kayıp olan bölümler aranmalı,

- Kapsamlı bir snapshot yapılmalı,

- **Tools>Disk Tools>File Recorvery By Type** ile dosya kurtarma işlemi yapılmalı,

* Mevcut ve silinmiş dosyalar kopyalanmalı,
* İnceleme sırasında önem arz eden dosyalarla ilgili rapor hazırlanmalı,
* İşletim sistemi olan imajlar içerisinde internet, bilgisayar ve mail kayıtları incelenmeli,