

Disklerde Bulunan MFT Tablolarının Analizi

Tuba KAVGACI¹, Nafiye Nur APAYDIN²

^{1,2}Adli Bilişim Mühendisliği Bölümü
Fırat Üniversitesi, Elazığ

¹200525001@firat.edu.tr, ²200509008@firat.edu.tr

Özet

MFT (Master File Table), Microsoft Windows işletim sistemi tarafından kullanılan bir dosya sistemi yapısıdır. MFT, bilgisayarda depolanan dosyaların erişim bilgilerini tutar ve bu bilgilerin hızlı bir şekilde erişilebilmesini sağlar. Bu makalede, MFT kavramı ve dosya sistem yapısı daha ayrıntılı bir şekilde incelenecektir. MFT' nin ne olduğu, yapısı, nasıl çalıştığı, hangi avantajlara, dezavantajlara sahip olduğu, bir dosyanın silinmesi durumunda hangi değişikliklerin meydana geleceği, bu silinmeler sonucunda hangi durumlarda veri elde edilebileceği ve hangi alanlarda kullanılabileceği ele alınacaktır. Ayrıca FTK ve Autopsy kullanılarak gerçekleştirilen örnek bir analiz uygulaması da sunulmaktadır. Sonuçlarımız, MFT' nin tüm dosyaların kaydını tutan bir veri tabanı olduğunu doğrulamaktadır.

Anahtar kelimeler: mft, ntfs, autopsy, ftk imager, adli bilişim.

1 Giriş

MFT, Windows NT işletim sisteminin ilk sürümünde tanıtılmıştır. Daha sonra Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 ve sonraki Windows sürümlerinde de kullanılmıştır. Microsoft'un Windows işletim sistemi geliştirme süreciyle yakından ilişkilendirilen MFT, NTFS dosya sistemi tarafından kullanılır. Dosyaların adını, boyutunu, fiziksel ve mantıksal konumlarını, değiştirilme, oluşturulma, erişim tarihlerini içeren bir kayıt yapısı olan MFT, dosyaların erişimi ve yönetimi için kullanılır. Adli bilişim uzmanları da, dijital delillerin analizi sırasında MFT'nin içerdiği verileri kullanır. Bu nedenle MFT'nin önemi sürekli olarak artmaktadır.

2 Açıklama

2.1 MFT nedir?

MFT (Master File Table), NTFS dosya sistemi için oluşturulan bir veritabanıdır. Her dosya ve klasör için bir kayıt barındırır ve NTFS dosya sisteminin kalbi niteliğindedir.

Tüm dosyaların sabit diskteki fiziksel ve klasördeki mantıksal konumlarını, boyutlarını, metadatalarını vb. tutan MFT, bir dosyayı tanımlayan tüm bilgileri içinde bulundurmaktadır.

MFT, NTFS dosya sistemi için verimli bir dosya yönetimi sağlar ve dosya erişimi için hızlı bir yol sunar.

2.2 NTFS nedir?

NTFS (New Technology File System), dosya ve klasörlerin yönetimini sağlayan, FAT (File Allocation Table) dosya sisteminin yeniden yapılandırılmasıyla oluşmuş bir dosya sistem standardıdır. Windows NT sürümünde kullanılmaya başlanan NTFS, günümüzde Windows 2000, Windows XP ve Unix tabanlı birçok işletim sistemi tarafından desteklenmektedir.

2.3 NTFS dosya sistemi içindeki MFT'nin rolü nedir?

NTFS dosya sistemi, dosya ve klasörleri güvenli bir şekilde saklamak ve yönetmek için birçok özellik sunar. MFT tabloları sayesinde dosya erişimi hızlanır ve sistem performansı artar. Ayrıca her işleme ait bilgi anlık kaydedilir, böylece veri kaybı durumunda kurtarma yapılabilir.

2.4 MFT tablosu üzerinde yer alan dosyaların özellikleri nelerdir?

Tüm dosyaların sabit diskteki fiziksel ve klasördeki mantıksal konumlarının yanı sıra;

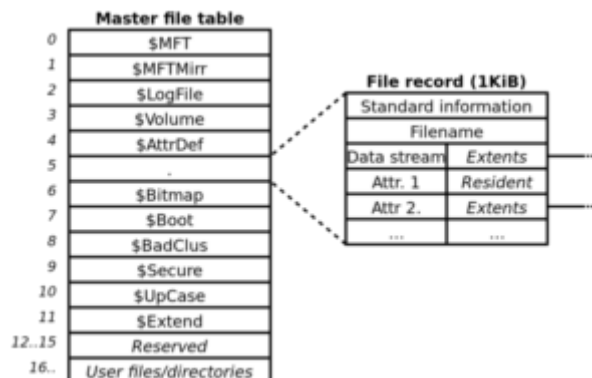
- 1) Dosya Adı
- 2) Dosya Boyutu
- 3) Oluşturma, Değiştirilme ve Erişim Tarihleri
- 4) Dosya Sahibi
- 5) Dosya İzinleri
- 6) Dosya İçeriği
- 7) Dosya Sürücüsü
- 8) Dosya Şifreleme gibi meta verileri MFT dosyalarının özelliklerindendir. Kısacası MFT, bir dosyayı tanımlayan ve tüm bilgileri tutan veri tabanıdır.

2.5 MFT tablosu üzerinde ne kadar veri tutabilir?

MFT tablosu, istenildiği kadar veri tutabilecek kapasiteye sahiptir. Ancak dosya sayısı arttıkça ve dosya sistemi kullanıldıkça MFT tablosu büyür ve dosya sistemi performansını olumsuz etkileyebilir. MFT tablosunun boyutu arttırılabilir. Bu yüzden MFT normal kullanımlarda genişleyebilir ancak hiçbir zaman küçülemez.

2.6 MFT yapısı nedir?

MFT'nin tuttuğu tüm bilgiler "MFT Girişi" olarak adlandırılan MFT'nin içinde bulunan bir girişte saklanır. MFT Girişleri standart olarak 1024 byte'dır. Bilgisayarın dosya ve klasörleri tanıyabilmesi için bir MFT Girişi olmalıdır. Buna MFT dosyası da dahildir. Yani bilgisayarın MFT dosyasını tanıyabilmesi için MFT dosyasının da bir MFT girişi olmak zorundadır. MFT'nin ilk 16 girişi NTFS sistem dosyaları için ayrılmıştır. Bu kayıtlar, özel sistem dosyalarını, öznitelikleri, verileri ve yapılandırma bilgilerini içerir. Bu rezervasyon, dosya sistemi işleyişi için kritik olan kayıtların korunmasını sağlar. Bu sayede, dosya sistemi işlemleri esnasında bu kayıtların zarar görmesi veya silinmesi önlenir. Metadata dosyaları \$ ile başlar ve ilk harfi her zaman büyüktür. Dosyalar diskin kök dizininde saklanır.

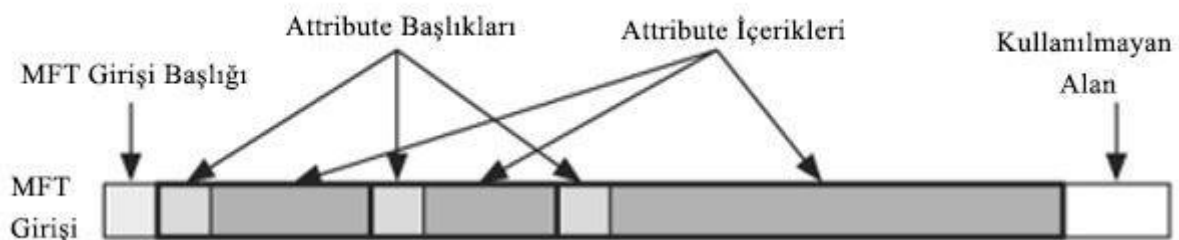


Şekil 1. MFT'nin NTFS sistem dosyaları için ayrılmış ilk 16 girişi.

Tablo 1. MFT tablosundaki ayrılmış ilk 16 sistem dosyasının depoladıkları bilgiler.

Sıra Numarası	İsim	Depolanan Bilgiler
1	\$MFT	Tablodaki ilk girdidir ve MFT'nin diskteki konumunu tutar. MFT'nin tamamını parse etmek istiyorsak eğer bu dosyayı kullanırız. Ancak belli bir bilgiyi elde etmek istiyorsak yani bilgiler arasında bir filtreleme yapmak istiyorsak eğer diğer 15 kayıt içerisindeki dosyaları parse edebiliriz.
2	\$MFTMirr	MFT'nin ilk 4 kaydının yedek kopyasını tutar.
3	\$LogFile	Meta veri işlemlerini kaydeden günlüktür. Sistem çökmesi, elektrik kesintisi gibi durumlarda dosya sisteminin bozulmaması için kullanılmaktadır.
4	\$Volume	NTFS biriminin adı, sürüm numarası ve bayraklarını içerir.
5	\$AttrDef	Tanımlayıcı değerleri, ad, boyut gibi özellik bilgilerini içerir.
6	.	Dosya sisteminin kök dizinini içerir.
7	\$Bitmap	Dosya sistemindeki kullanımda veya boş olan clusterlarının bir haritasını içerir.
8	\$Boot	Dosya sistemi için ön yükleme sektörü ve kodunu içerir.
9	\$BadClus	Kötü sektörlerle sahip partitionsları (bölümleri) tutar.
10	\$Secure	Dosyalar için güvenlik ve erişim kontrolü hakkında bilgi içerir. (Yalnızca Windows 2000 ve XP sürümü).
11	\$Upcase	Dosya adının sıralanmasına yardımcı olan Unicode büyük harfli karakter tablosudur yani her Unicode karakterinin büyük harflerini içerir.
12	\$Extend	İsteğe bağlı uzantılar için dosyalar içeren bir dizindir. Microsoft genellikle bu dizindeki dosyaları ayrılmış MFT girişlerine yerleştirmez.
13	\$Quota	Kota bilgilerini içeren dizin.
14	\$ObjId	NTFS'nin nesne kimliklerini izlediği dizin.
15	\$Reparse	Yeniden yönlendirme ve simgeleri içeren dizin
16	\$UsnJrnl	Microsoft dosya güvenilirliği açısından NTFS içerisine journal (günlük) kayıt dosyası eklemiştir. Yapılan tüm işlemlerin log kayıtlarının tutulduğu özel bir dosyadır. Herhangi bir sistem çökmesi durumunda burada yer alan kayıtlar kullanılarak bilgilerin kurtarılmasına olanak sağlamaktadır. Kısacası birimdeki dosya değişikliklerini izleyen dosyadır.

Her girdi 1KB depolama alanına sahiptir. Bu alanın ilk 42 baytının tanımlanmış amacı vardır. Geriye kalanlar öznitelik bölümlerini içerir. Örneğin bir öznitelik, sadece dosyanın boyutunu depolamak için kullanılabilir.



Şekil 2. Örnek bir MFT girişi.

Tablodaki her girdi uniq (eşsiz) ve ardışık 16 bitlik sıra numarasına sahiptir ve sıfırdan başlar.

MFT Tablosu							
MFT Giriş Başlığı	Attribute Başlığı	Attribute İçeriği	Attribute Başlığı	Attribute İçeriği	Kullanılmayan Alan	1 KB
MFT Giriş Başlığı	Attribute Başlığı	Attribute İçeriği	Attribute Başlığı	Attribute İçeriği	Kullanılmayan Alan	1 KB
MFT Giriş Başlığı	Attribute Başlığı	Attribute İçeriği	Attribute Başlığı	Attribute İçeriği	Kullanılmayan Alan	1 KB
•							1 KB
•							
•							

Şekil 3. MFT kaydında bulunanlar.

MFT kaydında bulunanlar:

- 1) Giriş Başlığı (Entry Header).
- 2) Attributes (Öznitelikler) : Başlık ve içerik olarak ikiye ayrılmaktadır.
- 3) Kullanılmayan alan (Unused Space).

2.6.1 Attribute başlıkları:

Attributelar tür, boyut ve ismi tanımlar. Attribute türü sayısal bir tanımlayıcı ile ifade edilir. Ayrıca bir MFT girişi aynı türden birden fazla attribute içerebilir. (Bir girdinin birden fazla \$DATA attribute'u içerebilmesi gibi.)

Bu Attributeleri anlamak MFT'deki verileri analiz etmemiz ve yorumlayabilmemiz için oldukça önemlidir.

Standart Info Attribute: Dosya hakkındaki standart bilgileri; sahiplik bilgilerini, meta verilerini, tarih ve zaman damgalarını içerir. Tanımlayıcı kodu 16'dır. Bu Attribute içerisinde 4 adet zaman damgası bulunmaktadır. (Windows gezgini, fls ve yardımcı programlardan topladığı zaman damgasını depolar.)

Zaman Damgası Türleri
a) Dosyanın Oluşturma Zamanı
b) Son Değiştirme Zamanı
c) MFT Değiştirme Zamanı
d) Son Erişim Zamanı

Şekil 4. Standart Info Attribute'deki zaman damgaları.

FileName Attribute: Dosya veya dizinlerin isimlerini ve onların DOS veya Win32 isim alanı gibi ilişkili isim alanlarını da içerir. Dosya adı değişken bir uzunlukta UTF-16 formatında saklanmaktadır. Ayrıca Standart Info Attribute'te olduğu gibi 4 zaman damgasını da içerir. (Zaman damgaları sadece attribute değiştiğinde değişir.)

MAC(b) Zamanları:

MAC(b) ZAMANLARI

-Modified

-Accessed

-Changed (\$MFT
Değiştirme Zamanı)

-Birth (Dosya Oluşturma Zamanı)

! Tüm dosya sistemleri birth time
(dosya oluşturma zamanını)
tutmamaktadır.

Şekil 5. MAC (Modified, Accessed, Changed, Birth) Zamanları.

Bu bilgiler Standart Info Attribute ve File Name Attributelerinde yer almaktadır. Her dosya için MFT’de; dört tane Standart Info ve dört tane de File Name Attributeten olmak üzere toplamda sekiz tane zaman damgası bulunmaktadır.

Standart Info Attribute Ve FileName Attribute Arasındaki Fark: Standart Info kullanıcı düzeyindedir ve kolayca değiştirilebilir fakat File Info zaman damgaları sadece sistem çekirdeği tarafından değiştirilebilir. Her işlem için ayrı kurallar vardır. Kurallar aşağıdadır:

The diagram illustrates the Windows 10 Time Rules for MAC(b) attributes. It is organized into two main sections: \$STANDARD_INFO and \$FILE_NAME. Each section contains a grid of rules for different file operations. The rules are color-coded: red for 'Changed' and blue for 'No Change'.

\$STANDARD_INFO							
File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified - No Change	Modified - No Change	Modified - No Change	Modified - No Change	Modified - No Change	Modified - Changed	Modified - Changed	Modified - No Change
Access - No Change	Access - No Change	Access - Changed	Access - Changed	Access - No Change	Access - Changed	Access - Changed	Access - No Change
Creation - No Change	Creation - No Change	Creation - Changed	Creation - Changed	Creation - No Change	Creation - No Change	Creation - No Change	Creation - No Change
Metadata - Changed	Metadata - Changed	Metadata - No change	Metadata - No change	Metadata - No Change	Metadata - Changed	Metadata - Changed	Metadata - No Change

\$FILE_NAME							
File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified - No Change	Modified - No Change	Modified - Changed	Modified - Changed	Modified - No Change	Modified - Changed	Modified - Changed	Modified - No Change
Access - No Change	Access - No Change	Access - Changed	Access - Changed	Access - No Change	Access - Changed	Access - Changed	Access - No Change
Creation - No Change	Creation - No Change	Creation - Changed	Creation - Changed	Creation - No Change	Creation - No Change	Creation - Changed	Creation - No Change
Metadata - No change	Metadata - No change	Metadata - Changed	Metadata - Changed	Metadata - No Change	Metadata - Changed	Metadata - Changed	Metadata - No Change

CYBERFORENSICATOR.COM

Şekil 6. Windows 10 sistemler için hazırlanmış ve test edilmiş MFT zaman çizelgesi.

Standart Info Attribute ve FileName Attribute'ün Aynı Bilgileri İçermesinin Biz Adli Bilişimcilere Katkıları Nelerdir?

Dosyaların, anti-forensic yöntemler uygulanarak değiştirilmesi mümkündür. Böylece saldırganlar bilgileri değiştirerek kendilerini gizler. Burada da Standart Info Attribute alanındaki verileri kolayca değiştirebilirler. Fakat FileName Attribute alanındaki verileri değiştirebilmek için üst düzey yetkiye sahip olmaları gerektiğinden işleri zordur. Bu yüzden analiz yapacağımız zaman bu iki alandaki verileri kıyasladığımızda birbiriyle eşleşmiyorsa bu durum bize Standart Info Attribute alanındaki verilerin değiştiğini gösterir.

Data Attribute: Dosyanın içeriği ile ilgili bilgiyi tutar. MFT'de, oluşturulan bir veriye standart olarak 1024 byte değeri atanır. Datamızda bir şey olmasa bile 1024 byte atandığı için 700-800 byte (kimi kaynaklarda bu 600 veya 900 bytetir) arasında oluşan bir veriye yeni bir tablo oluşturmak yerine var olan bu tabloya sığdırır.

2.7 MFT'nin Avantajları ve Dezavantajları Nelerdir?

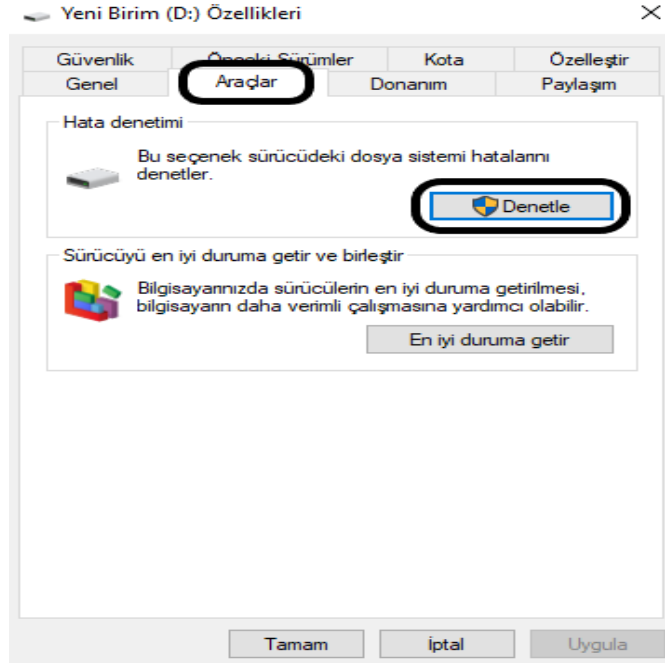
Tablo 2. MFT'nin avantajları ve dezavantajları.

MFT'nin Avantajları	MFT'nin Dezavantajları
Hızlı erişim: MFT dosya ve klasörlerle ilgili tüm meta dataları bir konumda depoladığı için daha hızlı dosya alımı ve erişimi sağlamaktadır.	Dosya boyutu sınırlı: MFT yapısı, dosyaların boyutunu sınırlar. Bu nedenle büyük dosyalar için ayrı bir MFT tablosu oluşturmak gerekebilir.
Bozuk veri kurtarma: MFT yapısı, dosyaların kaybolması veya bozulması durumunda verilerin kurtarılmasını kolaylaştırır.	Yavaş büyüme: MFT tablosu sürekli büyüyebilir bu durum da maksimum boyut sınırına ulaşınca yeni dosyaların oluşturulmasını engelleyerek sistem performansını düşürür veya sistem çökmelerine neden olabilir.
Dosya bütünlüğü: MFT yapısı, dosya bütünlüğünü korumak için checksumlar gibi özellikler içerir.	Veri kurtarma sınırlamaları: MFT yapısı, bazı durumlarda veri kurtarmayı zorlaştırabilir. Örneğin, silinen bir dosya için MFT'de yeterli bilgi yoksa veriler kurtarılamaz. Ayrıca karmaşık bir veri yapısı olduğundan, MFT'ye erişmek ve bunları analiz etmek zor olabilir.
Düzenli depolama: MFT yapısı, dosyaların düzenli ve yapılandırılmış bir şekilde depolanmasını sağlar.	Veri bütünlüğü sorunları: MFT yapısı, dosyaların bölünmesine neden olabilir ve bu da veri bütünlüğü sorunlarına yol açabilir.

2.8 MFT ' nin Korunması ve Onarımı

1. Disk imajı ve Yedeği Oluşturarak Üzerinde Çalışma: Disk imajı veya yedeği alınarak bir kopya oluşturup veri kaybı önlenebilir. Ayrıca bu kopyalar üzerinde işlem yaparak, yapacağımız işlemlerde orijinal diske zarar vermeden MFT'yi korur ve onarırız.
2. Disk Bakımı: Microsoft, güvenlik açıklarını ve hataları düzeltmek için düzenli olarak Windows güncellemeleri yayınlar. Sistemimizin ve MFT'nin sağlığı için düzenli olarak bu güncellemeleri yüklemek, disk bakımı yapmak, gereksiz dosyaları silmek, disk hatalarını düzeltmek vb. işlemler aksatılmadan yapılmalıdır.
3. Disk Onarma Yazılımları: MFT'nin onarımı için disk onarma yazılımları kullanılabilir. Bu yazılımlar, bozuk MFT yapısını tespit eder ve onarır. Ancak, bu yazılımların kullanımı riskli olabilir ve her zaman tamamen başarılı sonuçlar vermeyebilir. Örneğin CHKDSK (Check Disk), diski hatalara karşı tarayabilen ve bunları onarabilen yerleşik bir Windows aracıdır. CHKDSK'yi kullanmak için, komut istemini yönetici olarak açın ve 'chkdsk /f /r' komudunu yazdıktan sonra onarmak istediğiniz diskin sürücü harfini yazın. Bu, diski hatalara karşı tarar ve onarmaya çalışır. Ayrıca üçüncü taraf disk onarım araçlarından bazı popüler seçenekler arasında EaseUS Partition Master, Acronis Disk Director ve Stellar Partition Manager bulunur.

4. Kötü amaçlı yazılım ve virüsler MFT'ye zarar verebilir. Bu yüzden güncel bir virüsten koruma yazılımı yükleyerek sistemimizi korumak için düzenli taramalar yapmalıyız.
5. Windows, bozulursa diye önlem amaçlı MFT'yi onarmanıza yardımcı olabilecek yerleşik disk denetleme araçları içerir. Dosya Gezinini açın, kontrol etmek istediğiniz sürücüyü sağ tıklayın, Özellikleri seçin, Araçlar sekmesine gidin ve Hata denetimi altındaki Denetle düğmesine tıklayın.



Şekil 7. Windows'un D sürücüsü için yerleşik disk denetleme aracı.

6. MFT'nizin bozuk olduğundan şüpheleniyorsanız, diski tamir edene kadar mümkün olduğunca kullanmaktan kaçının. Bu, daha fazla hasarın önlenmesine yardımcı olacak ve başarılı bir onarım şansını artıracaktır.
7. Profesyonel Yardım: Yukarıdaki yöntemlerden hiçbiri işe yaramazsa veya veriler kritikse, MFT'yi onarmak ve verileri kurtarmak için gelişmiş teknikleri kullanabilen profesyonel bir veri kurtarma hizmeti sağlayıcısıyla iletişime geçmeniz gerekebilir. Profesyonel veri kurtarma hizmetleri, MFT'nin onarımı için gerekli araçlara ve bilgiye daha fazla sahip olabilirler.

2.9 Bir Dosya Silindiği Zaman MFT'de Hangi Değişiklikler Meydana Gelir?

Bir dosya silindiği zaman MFT girişi yeniden kullanılmaya hazır olarak işaretlenir. MFT girişi, dosya sistemi tarafından yeni dosyaları tahsis etmek için kullanılabilen mevcut MFT kayıtları listesine eklenir. Ancak burada belirtmemiz gereken önemli bir konu vardır. O da; Microsoft'un MFT girişlerini oluşturduktan sonra bir daha silme işlemi yapmamasıdır. Sadece içeriği temizler. Yani, sıra numarası sürekli artmaktadır. Bu yüzden MFT normal kullanımlarda genişleyebilir ancak hiçbir zaman küçülemez. (Ayrıca eğer bir dosyanın konumu hakkındaki tüm bilgileri kaybolursa cluster zinciri adresleme bilgilerini kullanarak tüm dosya clusterlarını bellekten çıkarabiliriz.) Daha önce dosyanın verileri tarafından kullanılan diskteki clusterlar 'boş' olarak işaretlenir ve dosya sistemi tarafından yeni verileri depolamak için kullanılabilir. Dosyanın verileri, üzerine yeni veriler yazılana kadar diskte kalır.

2.10 Silinmiş Dosyaları MFT'den Kurtarmak

MFT'den dosya kurtarmak için şu adımları izleyebilirsiniz:

1. Öncelikle, zarar gören diski bağlamak için sağlam bir sabit disk veya harici bir cihaz kullanın. Dosyalarınızı kurtarmak istediğiniz diski takın ve çalıştırın.

2. MFT tablosunu görüntülemek için bir MFT görüntüleyicisi kullanın. Bu araçlar, Windows İşletim Sistemi için üçüncü taraf yazılımlar olarak mevcuttur. MFT görüntüleyicisi, MFT tablosunu görüntüleyebilir ve aradığınız dosyaları bulmanızı kolaylaştırabilir.
3. İstenen dosyanın başlık numarasını not edin. Başlık numarası, MFT tablosunda dosyaların benzersiz tanımlayıcısıdır.
4. Başlık numarasını kullanarak MFT tablosunda ilgili girdiyi bulun ve dosya adını ve diğer özniteliklerini not edin.
5. Dosyalarınızı kurtarmak için özel bir yazılım kullanın. Bu yazılımlar genellikle MFT tablosundaki girdilere göre arama yaparak kayıp dosyaları bulabilir ve kurtarabilir. Örneğin Recuva yazılımı.

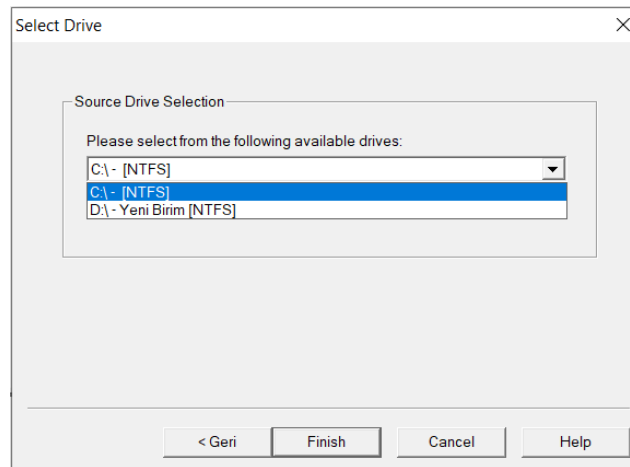
2.11 Silinmiş Verilerin Kurtarılabilir ve Kurtarılamaz Olma Durumları

Eldeki veriler, bir sabit sürücünün dosya sistemi MFT girişlerinin dosya verilerinden ayrıldığını göstermektedir. Bu durum, sabit sürücünün silinmesi ve ardından kullanılması sırasında birkaç farklı senaryoya yol açabilir.

- İlk senaryoda, dosya silinir ancak MFT girişi ve dosya verileri %100 kurtarılabilir. Bu durumda, silinen dosya tamamen kurtarılabilecektir.
- İkinci senaryoda, dosya silinir ve MFT girişi kurtarılabilir ancak dosya verilerinin bir kısmı üzerine yazılır. Bu durumda, dosya yalnızca kısmen kurtarılabilir.
- Üçüncü senaryoda, dosya silinir ve MFT girişi kurtarılabilir ancak dosya verileri %100 üzerine yazılır. Bu durumda, dosya kurtarılamaz ancak dosya hakkında bilgiler, ad, tarihler, boyutlar vb. MFT girişi kurtarılabildiği için elde edilebilir.
- Dördüncü senaryoda, dosya silinir ve MFT girişi ile dosya verileri %100 kurtarılamaz. Bu durumda, dosya %100 kayıp olacaktır. Adli soruşturmalar için MFT girişi aracılığıyla dosya hakkında bazı bilgiler elde edilebilir ancak diğer adli inceleme araçları kullanılarak daha fazla bilgi toplanabilir.
- Beşinci senaryoda, dosya silinir ve MFT'nin %100 üzerine yazılır ancak dosya verilerinin tamamı üzerine yazılmaz. Bu durumda, kalan dosya sabit sürücüdeki ayrılmamış alandan çıkarılabilir. Verilerin bölünme yeteneği, parçalanma durumuna, kurtarılabilir veri miktarına ve dosyanın yapısına bağlı olacaktır.

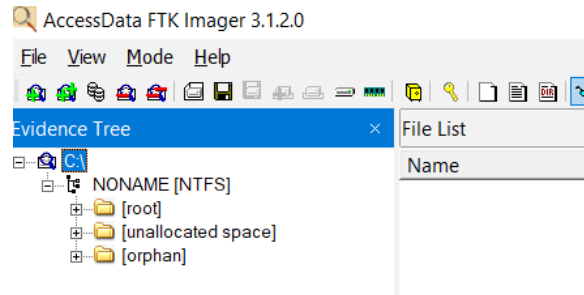
2.12 Uygulama 1: FTK Imager kullanarak MFT Dosyasını İnceleme

Manuel olarak MFT kayıtlarına erişmek ve içeriğine bakmak oldukça zahmetli bir işlemdir. Bu nedenle adli bilişim araçları, örneğin FTK Imager gibi araçlar kullanarak MFT dosyasının kopyası alınabilir. Bu işlem için FTK Imager programı açılır ve "File" sekmesi altından "Add Evidence Item" seçeneği seçilerek, NTFS dosya sistemli diskimiz seçilir. Örneğin, C diski seçilerek mantıksal imajı alınabilir.

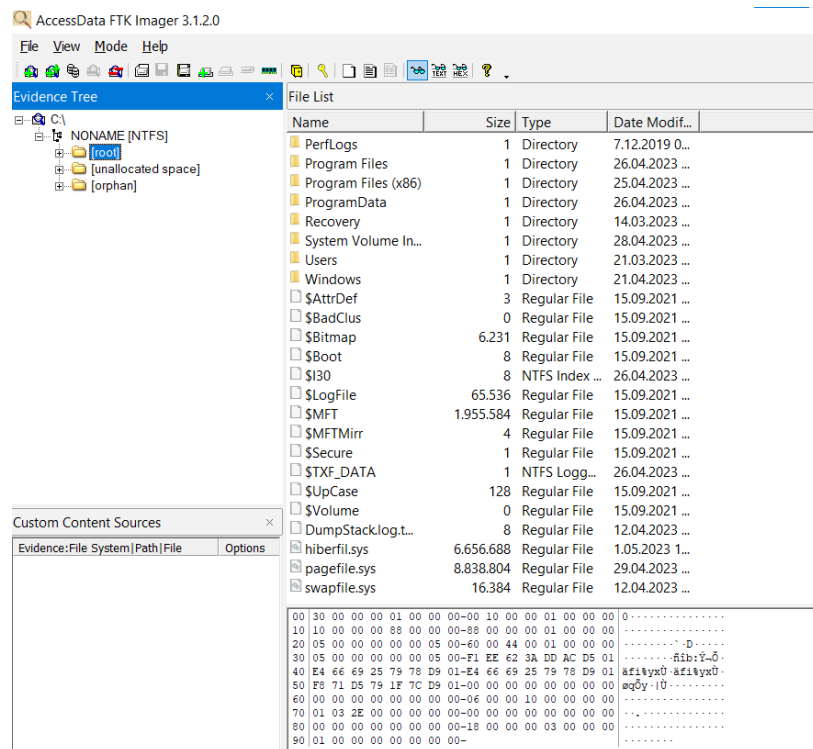


Şekil 8. Kaynak sürücü seçimi.

Ardından, seçtiğimiz diskimizin \$MFT dosyasının yer aldığı root klasörüne erişmek için programda açılan sekmede gezinme işlemi yapılır. Bu işlemle root klasörüne ulaşarak \$MFT dosyasının kopyası alınabilir.

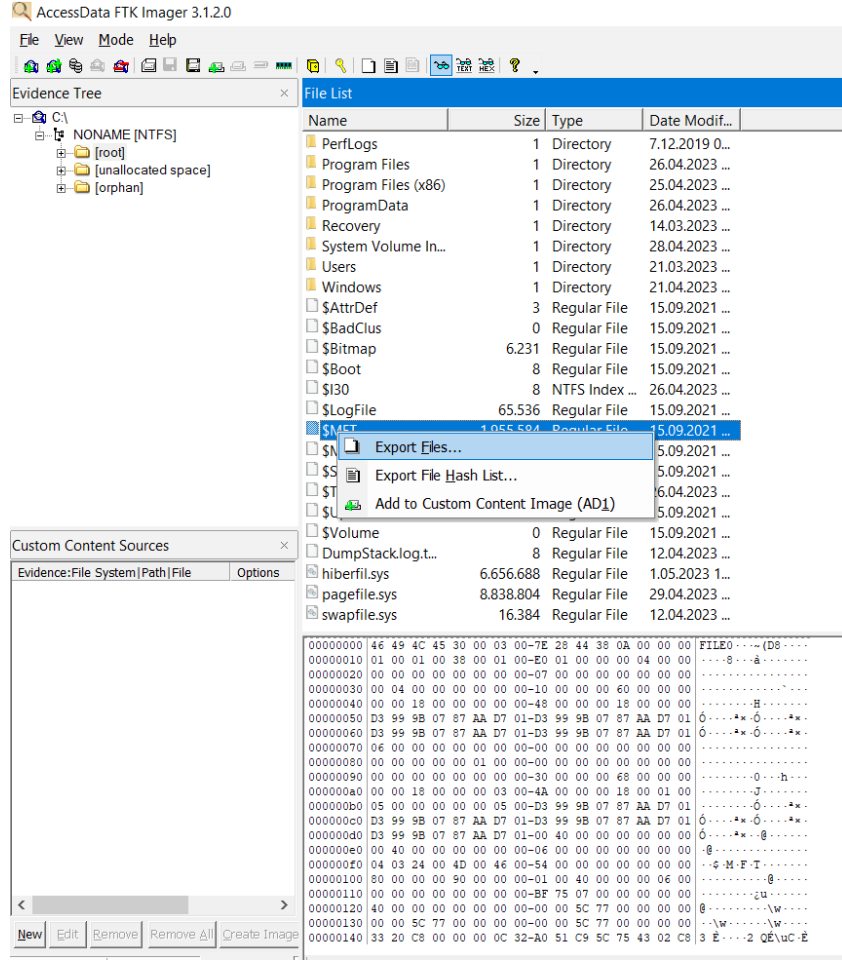


Şekil 9. \$MFT dosyasının yer aldığı root klasörünün konumu.



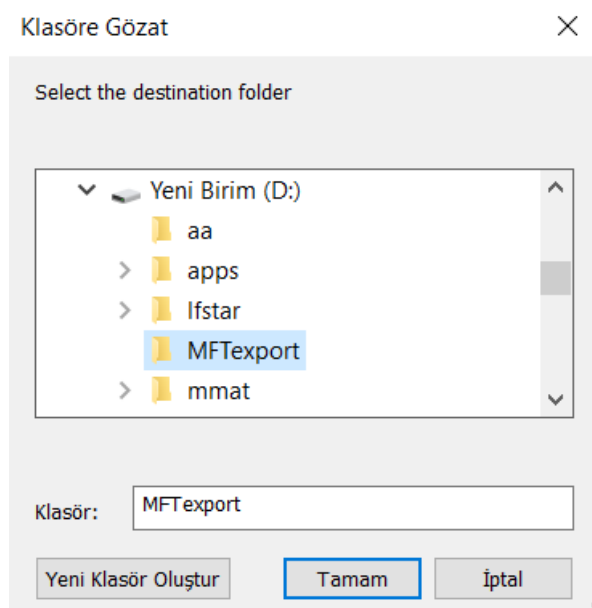
Şekil 10. root klasörünün içindekilerinin görüntülenmesi.

Programda root klasörüne tıkladığımızda içindeki dosyalar listelenir ve buradan \$MFT dosyasına erişebiliriz. Bu dosyaya erişmek için, üzerine sağ tık yapılarak "export" seçeneği seçilir ve \$MFT dosyasının kopyası export işlemine başlatılır.



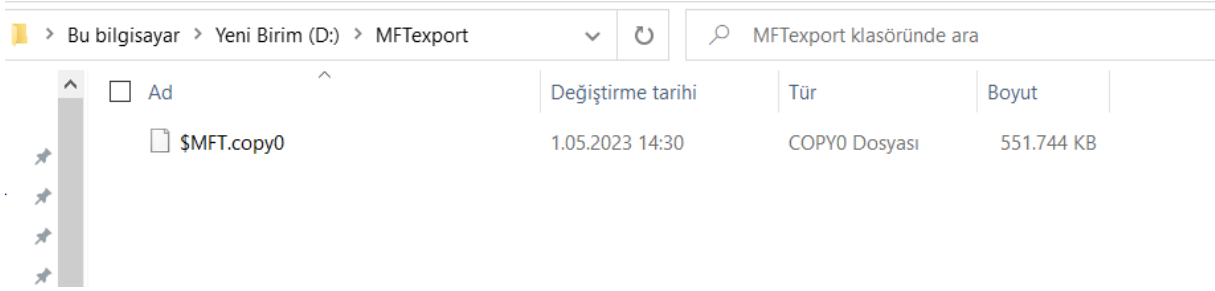
Şekil 11. \$MFT dosyasının export edilmesi.

Kopyalamaya başlamadan önce, açılan pencerede export edilecek dizini seçmeliyiz. Bu işlemle birlikte, kopyalanan \$MFT dosyası belirtilen dizine kaydedilir.



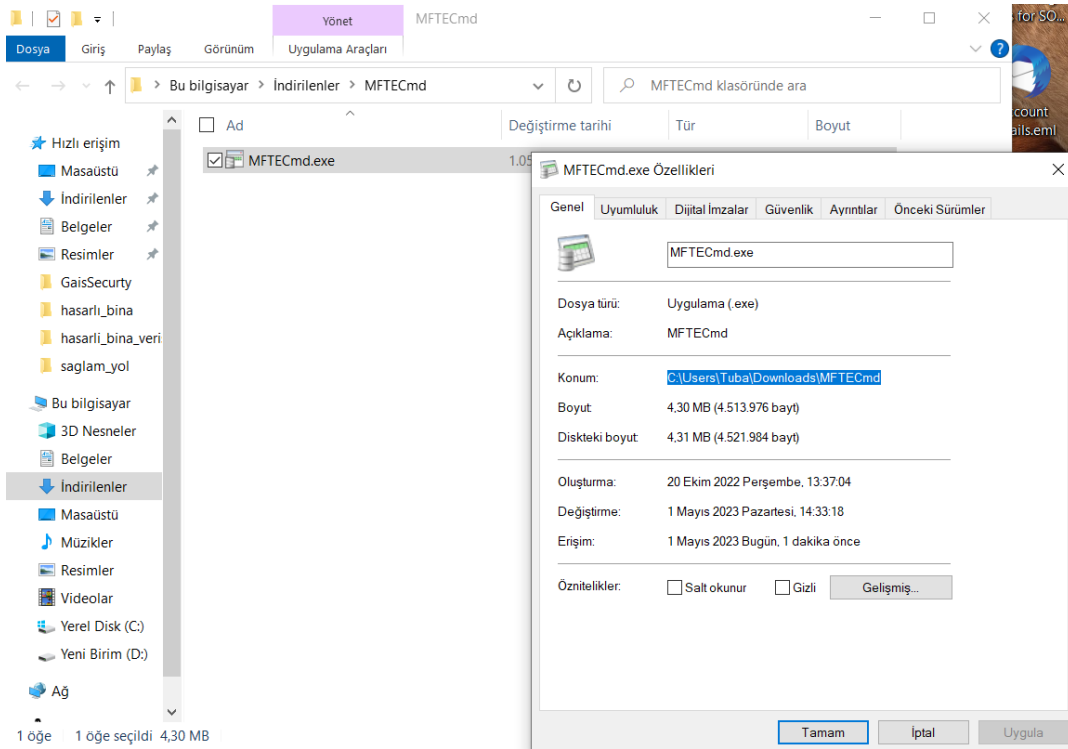
Şekil 12. \$MFT dosyasının export edileceği klasörü seçme.

Ve artık export edildi. Dizine gelip kontrol edelim.



Şekil 13. MFTexport klasörüne export edilen \$MFT dosyasını görüntüleme.

\$MFT dosyasını parse etmek için birçok araç mevcuttur. Bunlardan biri, Eric Zimmerman tarafından geliştirilen ve GitHub adresinde bulunan "MFTECmd.exe" aracıdır. Bu aracı indirdikten sonra, parse işlemi için CMD ekranını açarak aracın konumuna geçmeliyiz. Aracın konumunu öğrenmek için, sağ tık yapıp dosya yolu adlı değişkenden yararlanılabilir.



Şekil 14. MFTECmd.exe aracının konumunu alma.

Parse işlemi için, "MFTECmd.exe -f D:\MFTexport -csv D:\MFTparse" şeklinde bir komut kullanılır. Burada "-f" parametresi ile parse edilecek dosya belirtilirken, "--csv" parametresi ile parse sonucunda çıkartılan dosyaların kaydedileceği dizin belirtilir.

```
C:\Users\Tuba\Downloads\MFTECmd>MFTECmd.exe -f "D:\MFTexport\<div data-bbox="250 844 746 859" data-label="Caption">

Şekil 15. MFTECmd.exe aracını kullanarak $MFT dosyasını parse etme.


```

Bu komutu girdikten sonra "Enter" tuşuna basarak işlemi başlatabiliriz. Böylece, parse işlemi başlatılır ve MFTECmd.exe aracı belirtilen \$MFT dosyasını parse eder.

```
Se Komut İstemi - MFTECmd.exe -f "D:\MFTexport\MFT.copy0" --csv D:\MFTparse
C:\Users\Tuba\Downloads\MFTECmd>MFTECmd.exe -f "D:\MFTexport" --csv D:\MFTparse
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\MFTexport --csv D:\MFTparse

Warning: Administrator privileges not found!

Error opening file D:\MFTexport. Does it exist? Error: Administrator privileges not found! Cannot get raw files! Exiting
System.UnauthorizedAccessException: Administrator privileges not found! Cannot get raw files!
    konum: RawCopy.Helper.GetRawFiles(List`1 fileNames, Boolean dedupe)
    konum: MFTECmd.Program.GetFileType(String file)

C:\Users\Tuba\Downloads\MFTECmd>MFTECmd.exe -f "D:\MFTexport\MFT.copy0" --csv D:\MFTparse
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\MFTexport\MFT.copy0 --csv D:\MFTparse

Warning: Administrator privileges not found!

File type: Mft
```

Şekil 16. Parse etme işlemi.

Bu işlem biraz uzun sürebilir.

```
C:\Users\Tuba\Downloads\MFTECmd>MFTECmd.exe -f "D:\MFTexport\MFT.copy0" --csv D:\MFTparse
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\MFTexport\MFT.copy0 --csv D:\MFTparse

Warning: Administrator privileges not found!

File type: Mft

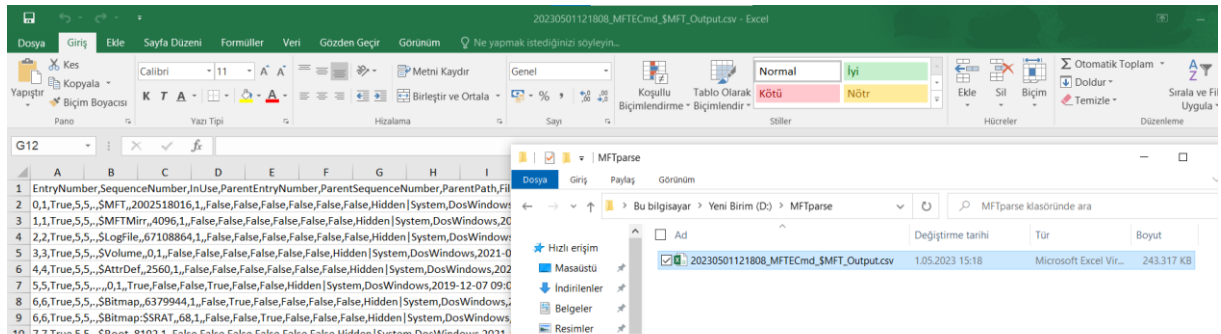
Processed D:\MFTexport\MFT.copy0 in 15,1824 seconds

D:\MFTexport\MFT.copy0: FILE records found: 539.357 (Free records: 12.379) File size: 538,8MB
CSV output will be saved to D:\MFTparse\20230501121808_MFTECmd_MFT_Output.csv

C:\Users\Tuba\Downloads\MFTECmd>
```

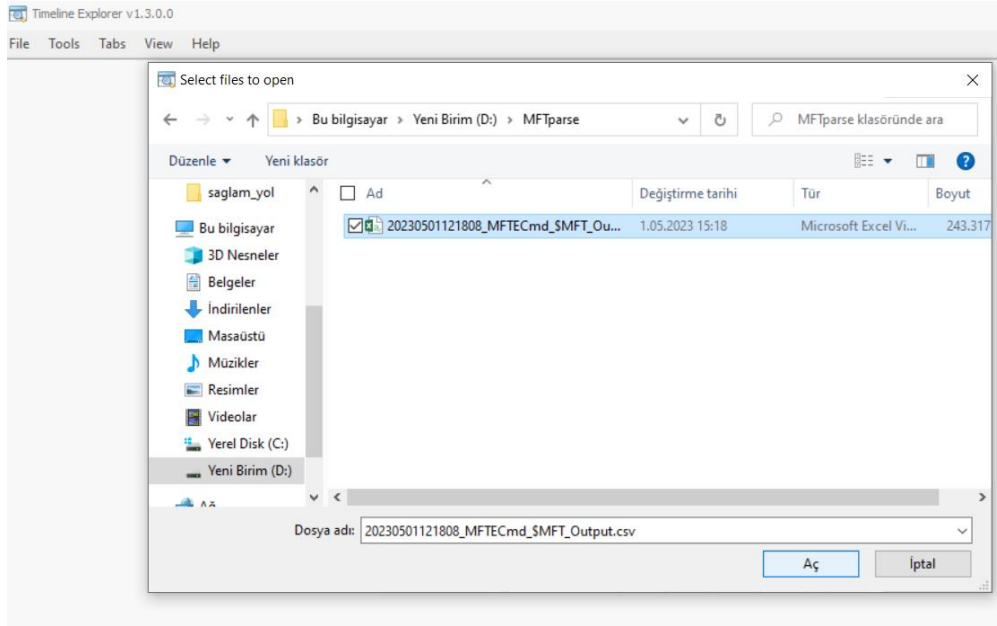
Şekil 17. Tamamlanan parse işlemi.

Ve tamamlandı gidip dosyamıza bakalım.



Şekil 18. Parse edilen dosyanın görüntülenmesi.

\$MFT dosyasını açtığımızda, genellikle karmaşık ve okunması zor bir yapıda olabilir. Bu nedenle, okunabilirliği artırmak için genellikle TimelineExplorer.exe aracından yararlanılır. Bu araç, parse edilmiş \$MFT dosyasının içeriğini daha iyi okuyabileceğimiz bir ara yüz sunar.



Şekil 19. TimelineExplorer.exe aracında parse edilen dosyayı seçerek açma.

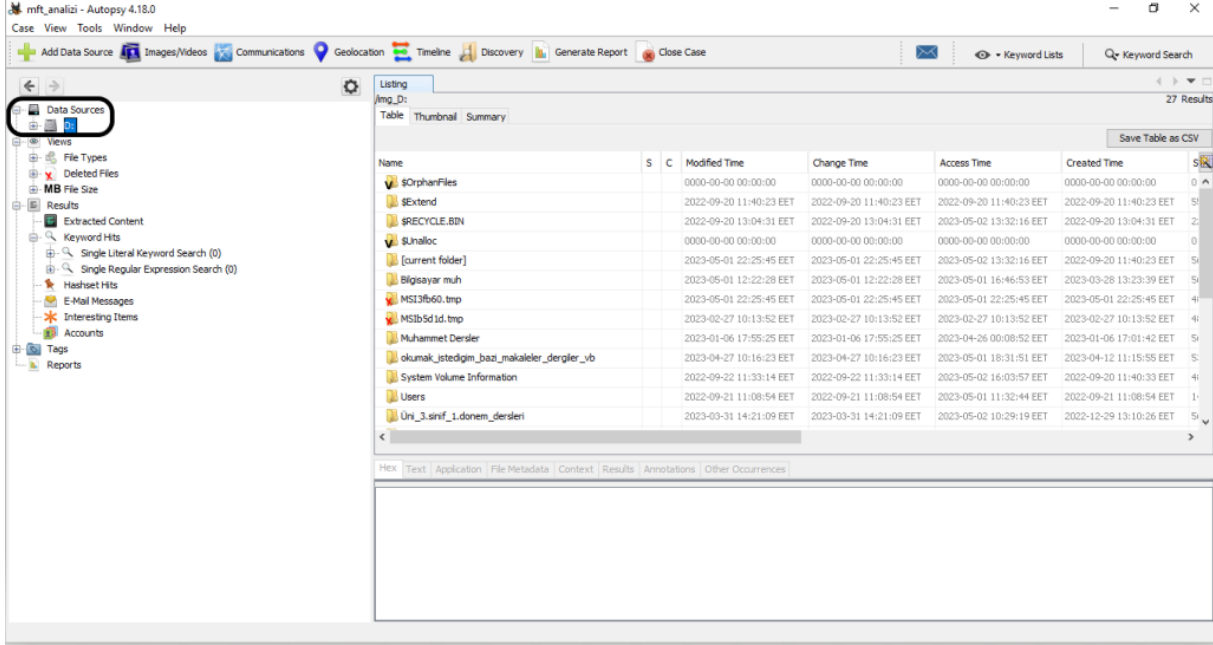
TimelineExplorer.exe aracını kullanarak parse edilmiş \$MFT dosyasının içeriğini daha iyi okuyabildiğimizi fark ederiz. Ayrıca bu aracı kullandığımızda, dosyanın ilk 16 girdisinin yukarıda bahsettiğimiz 16 başlıktan oluştuğunu görebiliriz.

Line	T	Entry No.	Seq.	Parent No.	In Use	Parent Path	File Name	Created@x10
1		0	1	5	5	✓	.\$MFT	2021-09-15 23:11:35
2		1	1	5	5	✓	.\$MFTMirr	2021-09-15 23:11:35
3		2	2	5	5	✓	.\$LogFile	2021-09-15 23:11:35
4		3	3	5	5	✓	.\$Volume	2021-09-15 23:11:35
5		4	4	5	5	✓	.\$AttrDef	2021-09-15 23:11:35
6		5	5	5	5	✓	.\$	2019-12-07 09:03:44
7		6	6	5	5	✓	.\$Bitmap	2021-09-15 23:11:35
8		6	6	5	5	✓	.\$Bitmap:\$SRAT	2021-09-15 23:11:35
9		7	7	5	5	✓	.\$Boot	2021-09-15 23:11:35
10		8	8	5	5	✓	.\$BadClus	2021-09-15 23:11:35
11		8	8	5	5	✓	.\$BadClus:\$Bad	2021-09-15 23:11:35
12		9	9	5	5	✓	.\$Secure	2021-09-15 23:11:35
13		9	9	5	5	✓	.\$Secure:\$SDS	2021-09-15 23:11:35
14		10	10	5	5	✓	.\$UpCase	2021-09-15 23:11:35
15		10	10	5	5	✓	.\$UpCase:\$Info	2021-09-15 23:11:35
16		11	11	5	5	✓	.\$Extend	2021-09-15 23:11:35
17		24	1	11	11	✓	.\$Extend	2021-09-15 23:11:35
18		25	1	11	11	✓	.\$Extend	2021-09-15 23:11:35
19		26	1	11	11	✓	.\$Extend	2021-09-15 23:11:35
20		27	1	11	11	✓	.\$Extend	2021-09-15 23:11:35
21		28	1	27	1	✓	.\$Extend\.\$RmMetadata	2021-09-15 23:11:35
22		28	1	27	1	✓	.\$Extend\.\$RmMetadata	2021-09-15 23:11:35
23		28	1	27	1	✓	.\$Extend\.\$RmMetadata	2021-09-15 23:11:35

Şekil 20. TimelineExplorer.exe aracında parse edilmiş dosyanın görüntülenerek incelenmesi.

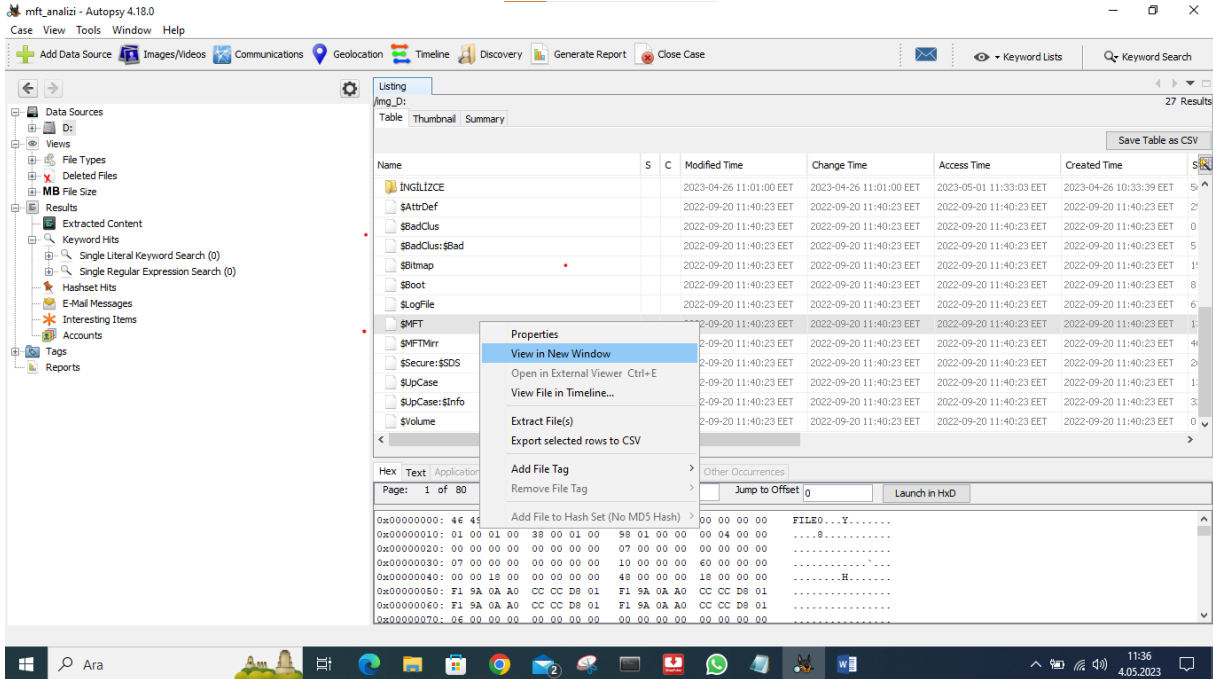
2.13 Uygulama 2: Autopsy kullanarak MFT Dosyasını İnceleme

Autopsy 4.18.0 sürümü kullanılarak imaj alındıktan sonra (bu uygulamada Yerel Disk D sürücüsünün imajı alınmış ve bu imaj üzerinde işlemler yapılmıştır) Data Soruce (Veri Kaynağı) kısmından D'yi seçerek içerisindeki dosyaları görüntüleriz.



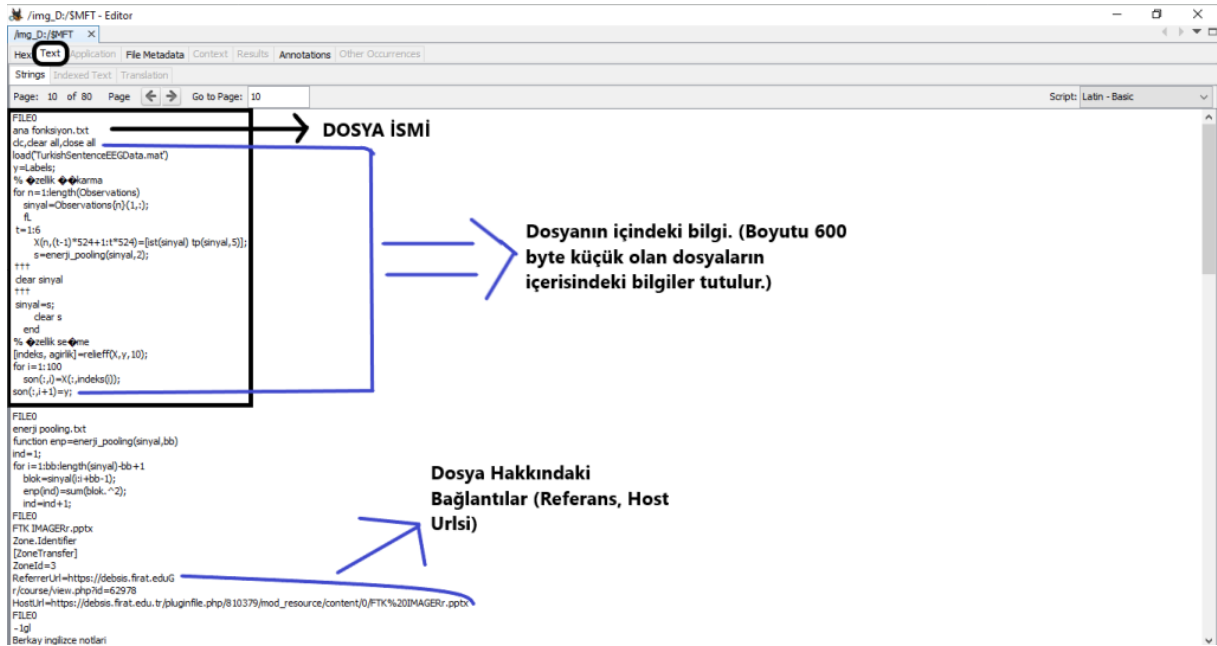
Şekil 21. İmajı alınmış D sürücüsünün içerisindeki dosyaları görüntüleme.

Daha sonra \$MFT dosyasını bularak “View in New Window” seçeneğiyle yeni bir pencerede görüntüleriz.



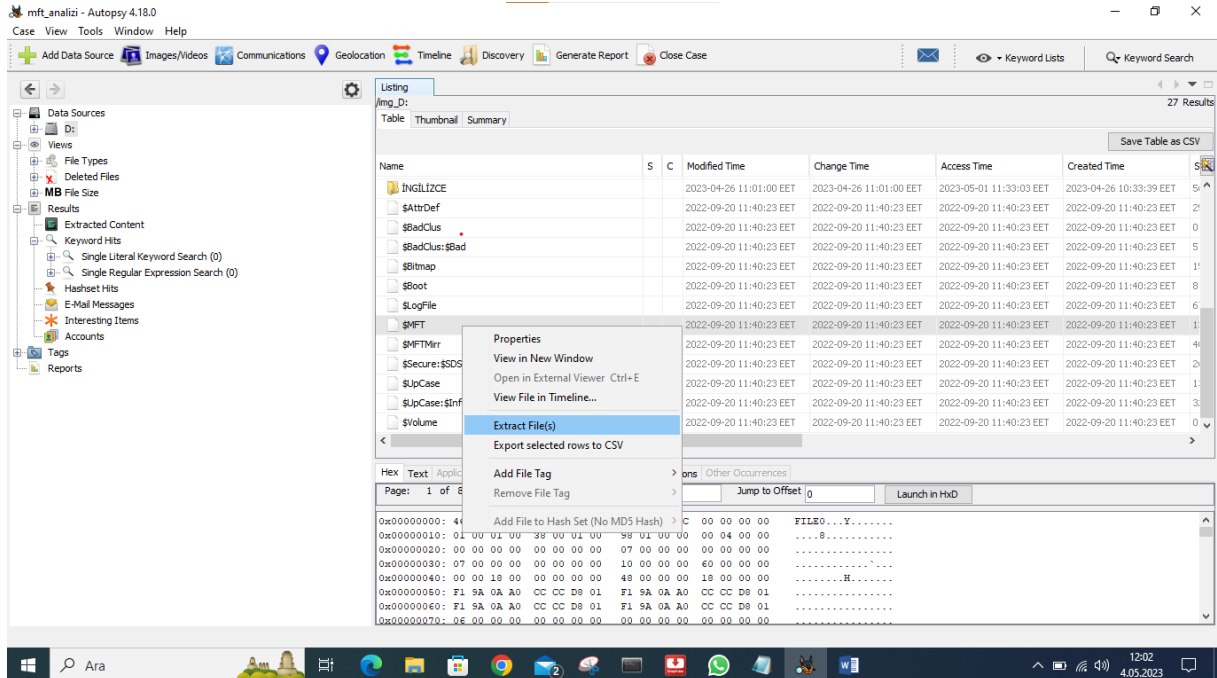
Şekil 22. \$MFT dosyasını bularak “View in New Window” seçeneğiyle yeni bir pencerede görüntüleme.

Açılan yeni sekmede görüntüleme olarak “text” seçeneğini seçtikten sonra dosya adı, daha öncede anlatıldığı gibi eğer boyutu 600 byte'dan küçükse içerisindeki bilgi, referans ve host url'leri gibi birkaç bilgi edinebiliriz.

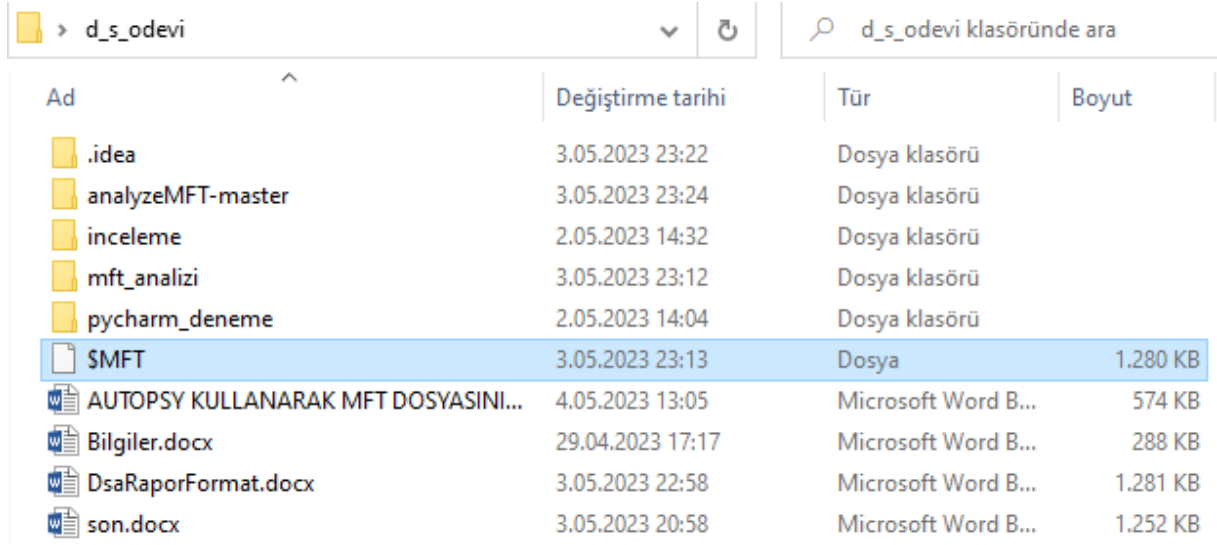


Şekil 23. Görüntüleme olarak “text” seçeneğini seçerek dosya adı, url'ler, içerikler gibi bazı bilgileri elde etme.

Fakat daha fazla bilgi edinmek için (örneğin oluşturulma, değiştirilme tarihleri gibi bilgilere ulaşmak için) \$MFT dosyası export edildikten sonra “analyzeMFT.py” aracı kullanılarak parse edilecektir.



Şekil 24. \$MFT dosyasını export etme.

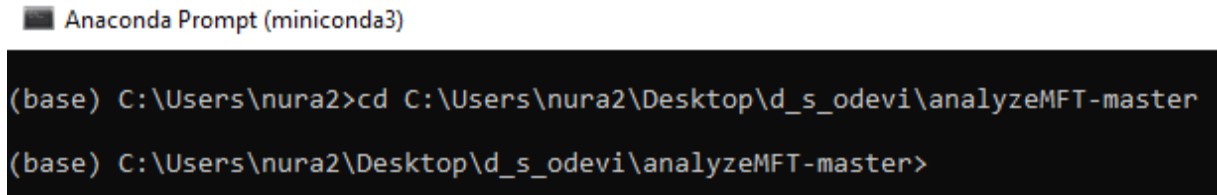


Ad	Değiştirme tarihi	Tür	Boyut
.idea	3.05.2023 23:22	Dosya klasörü	
analyzeMFT-master	3.05.2023 23:24	Dosya klasörü	
inceleme	2.05.2023 14:32	Dosya klasörü	
mft_analizi	3.05.2023 23:12	Dosya klasörü	
pycharm_deneme	2.05.2023 14:04	Dosya klasörü	
SMFT	3.05.2023 23:13	Dosya	1.280 KB
AUTOPSY KULLANARAK MFT DOSYASINI...	4.05.2023 13:05	Microsoft Word B...	574 KB
Bilgiler.docx	29.04.2023 17:17	Microsoft Word B...	288 KB
DsaRaporFormat.docx	3.05.2023 22:58	Microsoft Word B...	1.281 KB
son.docx	3.05.2023 20:58	Microsoft Word B...	1.252 KB

Şekil 25. Export edilen \$MFT dosyasının klasörde görüntülenmesi.

Daha sonra Anaconda Prompt (miniconda3)'yı açtıktan sonra analyzeMFT.py aracını kullanarak \$MFT dosyasını parse etmek için gerekli kurulumlar yapılır.

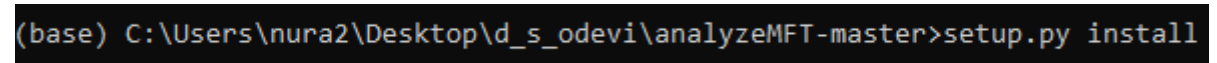
Öncelikle analyzeMFT.py aracının bulunduğu “analyzeMFT-master” klasörüne gitmek için: “**cd C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master**” komudunu yazarız.



```
Anaconda Prompt (miniconda3)
(base) C:\Users\nura2>cd C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master
(base) C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master>
```

Şekil 26. analyzeMFT.py aracının bulunduğu klasöre gitme.

Sonra bu klasörün içinde bulunan setup.py dosyası “setup.py install” komuduyla çalıştırılarak gerekli yüklenmelerin yapılması sağlanır.



```
(base) C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master>setup.py install
```

Şekil 27. setup.py dosyasının çalıştırılarak gerekli kurulumların yapılması.

Şimdi sıra analyzeMFT.py aracını kullanarak \$MFT dosyasını parse etmeye geldi. Parse etmek için aşağıdaki komut kullanılır:

```
python analyzeMFT.py -f "C:\Users\nura2\Desktop\d_s_odevi\SMFT" -o "C:\Users\nura2\Desktop\d_s_odevi\sonuc.csv"
```



```
Anaconda Prompt (miniconda3)
(base) C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master>python analyzeMFT.py -f "C:\Users\nura2\Desktop\d_s_odevi\MFT"
-o "C:\Users\nura2\Desktop\d_s_odevi\sonuc.csv"
Traceback (most recent call last):
  File "C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master\analyzeMFT.py", line 12, in <module>
    session.process_mft_file()
  File "C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master\analyzemft\mftsession.py", line 206, in process_mft_file
    self.do_output(record)
  File "C:\Users\nura2\Desktop\d_s_odevi\analyzeMFT-master\analyzemft\mftsession.py", line 226, in do_output
    self.file_csv.writerow(mft.mft_to_csv(record, False, self.options))
  File "C:\Users\nura2\miniconda3\lib\encodings\cp1254.py", line 19, in encode
    return codecs.charmap_encode(input,self.errors,encoding_table)[0]
UnicodeEncodeError: 'charmap' codec can't encode character '\u0307' in position 90: character maps to <undefined>
```

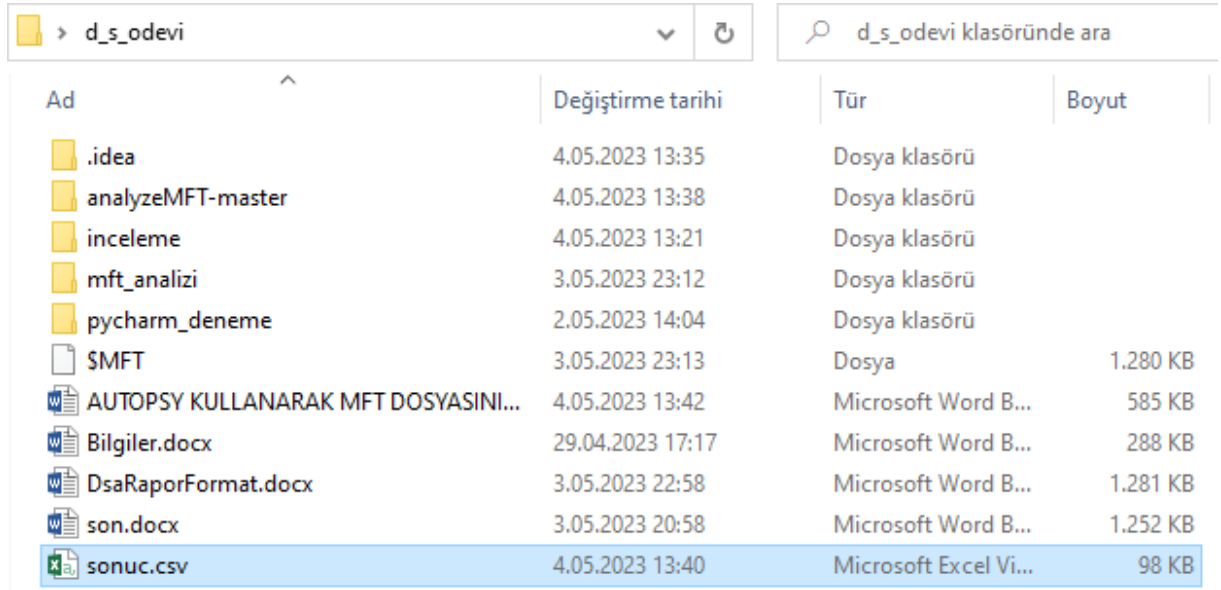
Şekil 28. analyzeMFT.py aracının kullanılarak \$MFT dosyasının parse edilmesi.

Kodu açıklamak gerekirse:

python analyzeMFT.py : analyzeMFT.py dosyasının çalıştırılacağı belirtilir.

-f "C:\Users\nura2\Desktop\d_s_odevi\MFT" : -f parametresi ile \$MFT dosyasının konumu belirtilir.

-o "C:\Users\nura2\Desktop\d_s_odevi\sonuc.csv" : -o parametresi ile parse etme işlemi sonunda çıktının hangi dosyaya yazılacağı belirtilir.



Ad	Değiştirme tarihi	Tür	Boyut
.idea	4.05.2023 13:35	Dosya klasörü	
analyzeMFT-master	4.05.2023 13:38	Dosya klasörü	
inceleme	4.05.2023 13:21	Dosya klasörü	
mft_analizi	3.05.2023 23:12	Dosya klasörü	
pycharm_deneme	2.05.2023 14:04	Dosya klasörü	
\$MFT	3.05.2023 23:13	Dosya	1.280 KB
AUTOPSY KULLANARAK MFT DOSYASINI...	4.05.2023 13:42	Microsoft Word B...	585 KB
Bilgiler.docx	29.04.2023 17:17	Microsoft Word B...	288 KB
DsaRaporFormat.docx	3.05.2023 22:58	Microsoft Word B...	1.281 KB
son.docx	3.05.2023 20:58	Microsoft Word B...	1.252 KB
sonuc.csv	4.05.2023 13:40	Microsoft Excel Vi...	98 KB

Şekil 29. Parse edilmiş “sonuc.csv” dosyasının klasörde görüntülenmesi.

Şimdi bu dosyayı açalım:

sonuc.csv - Excel

Dosya Giriş Ekle Sayfa Düzeni Formüller Veri Gözetim Geçir Görünüm Ne yapmak istediğinizi söyleyin... Paylaş

Calibri 11 A⁺ Metni Kaydır Genel Koşullu Biçimlendirme Tablo Olarak Biçimlendir Hücre Stilleri Ekle Sil Biçim Otomatik Toplam Doldur Temizle Sırala ve Filtre Uygula Bul ve Seç

Pano Yazı Tipi Hizalama Sayı Stiller Hücreler Düzenleme

A1 Record Number,"Good","Active","Record type","Sequence Number","Parent File Rec. #","Parent File Rec. Seq. #","Filename #1","Std Info Creation date","Std Info

151 67,"Good","Active","File","18","49","12","/Users/nura2/VirtualBox VMs/Kali Linux/Logs/VBox.log.1","2023-04-08 09:47:20.586048","2023-04-08 09:53:26.323917","2023-04-08 09:53:26.323917","2023-04-26 20:36:57.1645

152

153 68,"Good","Active","File","14","69","2","/Users/nura2/VirtualBox VMs/BEE/Logs/VBox.log","2022-12-06 20:12:01.117376","2022-12-06 20:14:38.664715","2022-12-06 20:14:38.664715","2022-12-06 20:14:38.664715","202

154

155 69,"Good","Active","Folder","2","64","5","/Users/nura2/VirtualBox VMs/BEE/Logs","2022-11-03 19:59:09.190853","2022-12-06 20:12:01.117376","2023-05-01 08:32:44.943102","2022-12-06 20:12:01.117376","2022-11-03 1

156

157 70,"Good","Active","File","3","69","2","/Users/nura2/VirtualBox VMs/BEE/Logs/VBox.log.1","2022-11-03 20:03:34.710592","2022-11-03 20:40:57.189104","2022-11-03 20:40:57.189104","2022-12-06 20:12:01.117376","202

158

159 71,"Good","Active","File","2","69","2","/Users/nura2/VirtualBox VMs/BEE/Logs/VBox.log.2","2022-11-03 19:59:23.208508","2022-11-03 20:01:22.557579","2022-11-03 20:01:22.557579","2022-12-06 20:12:01.116400","202

160

161 72,"Good","Active","Folder","10","39","1","/ŞRECYCLE.BIN/5-1-5-21-1367824300-1715821844-3292633880-1001/ŞR72FIHK","2023-04-11 11:07:38.077902","2023-04-11 11:08:17.401958","2023-04-25 21:08:28.346491","202

162

163 73,"Good","Active","File","49","12","/Users/nura2/VirtualBox VMs/Kali Linux/Logs/VBox.log.2","2023-03-09 11:08:07.695419","2023-03-09 11:15:02.807812","2023-03-09 11:15:02.807812","2023-04-26 20:36:57.15896

164

165 74,"Good","Active","File","55","319","3","/okumak_istedigim_bazi_makaleler_degiler_vb/File System Forensic Analysis.pdf","2023-04-27 07:16:06.454494","2023-04-27 07:16:24.335920","2023-04-27 07:16:24.335920","2023-04-27 07:16:24.335920"

166

167 74,"Good","Active","File","55","319","3","/okumak_istedigim_bazi_makaleler_degiler_vb/File System Forensic Analysis.pdf:Zone.Identifier","2023-04-27 07:16:06.454494","2023-04-27 07:16:24.335920","2023-04-27 07:16:24.335920","2023-04-27 07:16:24.335920"

168

169 75,"Good","Active","Folder","11","5","5","/Üni_3.sinif_1.donem_dersleri","2022-12-29 10:10:26.517784","2023-03-31 11:21:09.184010","2023-05-02 07:29:19.013155","2023-03-31 11:21:09.184010","2022-12-29 10:10:26.517784"

170

171 76,"Good","Active","File","64","5","/Users/nura2/VirtualBox VMs/BEE/vbox","2022-12-06 20:14:38.008907","2022-12-06 20:14:38.008907","2023-04-26 20:36:17.919083","2022-12-06 20:14:38.034809","2022-12-06 20:14:38.034809"

172

173 77,"Good","Active","Folder","2","75","11","/Üni_3.sinif_1.donem_dersleri/BİLİŞİM SUÇU İNCELEME YAZILIMLARI","2022-12-29 10:11:17.953667","2023-01-09 20:07:01.012794","2023-04-30 09:25:08.762365","2023-01-09 20:07:01.012794"

Hazır Ara

Şekil 30. “sonuc.csv” dosyasının görüntülenmesi.

Gelen bu bilgileri daha iyi incelemek için “CSVQuickViewer.exe” aracımı kullanarak açarız:

C:\Users\nura2\Desktop\d_s_odevi\sonuc.csv - CP 28599 - Türkçe (ISO) - CSV Quick Viewer 1.7.5.582

Open File Setting All Records Unique Values Duplicates Hierarchy Columns Source Write File As Text Log

	Column1	Column2	Column3	Column4	Column5	Column6	Column7	Column8	Column9	Column10	Column11	Column12	Column13
				Record type		Parent File Rec. Seq. #	Parent File Rec. Seq. #	Filename #1	Std Info Creation date	Std Info Modification date	Std Info Access date	Std Info Entry date	FN Info Creation date
0	Good			File	1	5	5	/ŞMFT	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
1	Good			File	1	5	5	/ŞMFTMirr	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
2	Good			File	2	5	5	/ŞLogFile	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
3	Good			File	3	5	5	/ŞVolume	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
4	Good			File	4	5	5	/ŞAttrDef	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
5	Good			Folder	5	5	5	/.	2022-09-20 08:40:23.787...	2023-05-01 19:25:45.959...	2023-05-02 10:32:16.830...	2023-05-01 19:25:45.959...	2022-09-20 08:40:23.787...
6	Good			File	6	5	5	/ŞBitmap	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
7	Good			File	7	5	5	/ŞBoot	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
8	Good			File	8	5	5	/ŞBadClus	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
8	Good			File	8	5	5	/ŞBadClus:\$Bad	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
9	Good			File + Unknown2	9	5	5	/ŞSecure	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
9	Good			File + Unknown2	9	5	5	/ŞSecure:\$SDS	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
10	Good			File	10	5	5	/ŞUpCase	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
10	Good			File	10	5	5	/ŞUpCase:\$I...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
11	Good			Folder	11	5	5	/ŞExtend	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...
12	Good			File	12	NoParent	NoParent	NoFNRecord	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	NoFNRecord
13	Good			File	13	NoParent	NoParent	NoFNRecord	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	NoFNRecord
14	Good			File	14	NoParent	NoParent	NoFNRecord	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	2022-09-20 08:40:23.787...	NoFNRecord

169 / 170 Ara

Şekil 31. “sonuc.csv” dosyasının “CSVQuickViewer.exe” aracı kullanılarak görüntülenmesi.

3 Sonular

Sonularımız, MFT' nin tm dosyaların kaydını tutan bir veri tabanı olduėunu doėrulamaktadır. MFT'nin ierdiėi verilerin adli biliřim aısından byk nem tařıdığını gstermektedir. Bu veriler, adli biliřim uzmanlarının dijital delilleri elde etmek iin kullandıkları birok teknik arata kullanılabilir. MFT'de verilerinin analizi olduka karmařık bir sretir ve eřitli zorluklarla karřılařılabilir. Bu baėlamda, gelecekteki alıřmaların MFT'nin analizini geliřtirmeye odaklanması nerilir.

4 Kaynaklar

- [1] Alexander Riccio. "Forensics: What is the \$MFT?" <https://whereismydata.wordpress.com/2009/06/05/forensics-what-is-the-mft/> (June 5, 2009).
- [2] Mehmet Kadir CIRIK. "Master File Table Nedir? MFT'yi Anlamak" <https://www.kadircirik.com/master-file-tablemftyi-anlamak/> (29 Eyll 2021).
- [3] Enes Aydın. "1 — Ne İře Yarar Bu MFT ?" <https://medium.com/@enesilhaydin/1-ne-i-CC%87%C5%9Fe-yarar-bu-mft-12233b8e9b9a> (23 Temmuz 2018).
- [4] Enes Aydın. "2 - \$MFT Tablosunu Elde Etme Yntemleri" <https://medium.com/@enesilhaydin/mft-tablosunu-elde-etme-y%C3%B6ntemleri-a6edfc99b66b> (27 Temmuz 2018).
- [5] Jonathan Adkins. "NTFS Forensics and the Master File Table" <https://www.youtube.com/watch?v=xW5UwDztX4&t=20s> (16 Haz 2015).
- [6] Wikipedia. "NTFS" <https://tr.wikipedia.org/wiki/NTFS> (21 Ekim 2020).
- [7] Wmaraci. "NTFS Nedir?" <https://wmaraci.com/nedir/ntfs>
- [8] SOURCEFORGE. "CSV Quick Viewer" <https://sourceforge.net/projects/csvquickviewer/> (2023-03-20).
- [9] Dkovar. "analyzeMFT" <https://github.com/dkovar/analyzeMFT> (Sep 8, 2022).
- [10] Autopsy. "Autopsy 4.18.0" <https://github.com/sleuthkit/autopsy/releases/> (Mar 23, 2021).
- [11] NTFS, <http://ntfs.com/ntfs-mft.htm>
- [12] Joe Fichera, Steven Bolt, Host Analysis <https://www.sciencedirect.com/topics/computer-science/master-file-table> (2013)
- [13] Cem Gurkok,in Computer-and-Information-Security-Handbook(ThirdEdition), <https://www.sciencedirect.com/science/article/abs/pii/B9780128038437000417> (2017)
- [14] <https://www.minitool.com/lib/mft.html>
- [15] <https://www.geeksforgeeks.org/what-is-a-master-file-table/>
- [16] <https://threat.media/definition/what-is-the-master-file-table/>