AJIT-e Academic Journal of Information Technology
10.5824/ajite.2023.02.004.x

2023 . Spring - Bahar . Volume – Cilt: 14 . Issue – Sayı: 53

RAID Sistemlerinin Adli Bilişim Açısından İncelenmesi

Ramazan OĞUZ, *İstanbul Üniversitesi-Cerrahpaşa, Adli Tıp ve Adli Bilimler Enstitüsü, Doktora Programı, 0000-0002-7297-4141*

Yiğithan YILMAZ, *İstanbul Jandarma Kriminal Laboratuvar Amirliği, Bilişim Teknolojileri İnceleme Şube Müdürlüğü, 0000-0002-2093-5124*

ÖZ

Günlük hayatta kullanımının yaygınlaşması ve kriminal laboratuvarlara gelen delil miktarındaki artış nedeniyle, RAID (Redundant Array of Independent Disks – Bağımsız Disklerin Yedekli Dizisi) sistemlerinin adli bilişim açısından incelenmesi bu çalışmanın amacını oluşturmaktadır. Yapılan çalışmada, öncelikli olarak RAID sistemleri ve kullanılan parametreler incelenmiştir. RAID sistemleri tekrardan oluşturulurken bilinmesi gereken parametrelerin, RAID seviyesi, doğru disk sıralaması, şerit boyutu ve geometri bilgisi olduğu anlaşılmıştır. En çok kullanım alanının olduğu belirlenen RAID 0, 1 ve 5 sistemleri ayrıntılı olarak ele alınmıştır. RAID sistemlerinin adli bilişim açısından incelenmesi aşamasında, tüm parametre özelliklerini üzerinde barındıran RAID 5 sistemi VROC (Virtual RAID On CPU) yazılımı ile oluşturulmuştur. Oluşturulan RAID sistemi içerisinde dosya kopyalama ve silme işlemleri gerçekleştirilmiştir. İşlemler sonucunda sabit disklerin imajı Tableau TD2u donanımıyla alınmıştır. Alınan imajlar DiskInternals Raid Recovery isimli yazılım ile incelenmiştir. İncelemeler neticesinde belirtilen yazılımla RAID yapısının tekrardan nasıl oluşturulduğu gösterilmiştir. RAID sistemi oluşturulurken yazılımın, ihtiyaç duyulan tüm parametre kombinasyonlarını otomatik olarak deneyebildiği, otomatik denemelerin başarılı sonuç vermediği durumlarda ihtiyaç duyulan parametrelerin kullanıcı tarafından bilinmesi ve yazılıma girilmesi gerektiği tespit edilmiştir. İhtiyaç duyulan parametrelerin yanlış girilmesi durumunda disk yapısının doğru bir şekilde oluşturulamadığı ve kullanıcı verilerine erişilemediği görülmüştür. Sonuç itibariyle, kriminal incelemelerde son dönemlerde sıkça karşılaşılan fakat uygulamalı gösterimi bulunmayan RAID sistemlerinin tekrardan oluşturulması noktasında ihtiyaç duyulan parametreler ortaya konulmuş ve incelemelerde izlenecek yöntemler belirlenmiştir.

Anahtar Kelimeler **:** RAID, Adli Bilişim, Şeritleme, Aynalama, Eşlik

Araştırma Makalesi / Research Article
Date Received: 3.10.2022
Publishing Date: 31.05.2023

Investigation of RAID Systems in Terms of Forensics

ABSTRACT *The purpose of this study is to examine RAID (Redundant Array of Independent Disks) systems in terms of forensic computing, due to the widespread use in daily life and the increase in the amount of evidence coming to criminal laboratories. In the study, primarily RAID systems and the used parameters were examined. It has been understood that the parameters that need to be known when rebuilding RAID systems are RAID level, correct disk ordering, stripe size and geometry information. RAID 0, 1 and 5 systems, which are determined to be the most used, are discussed in detail. During the examination of RAID systems in terms of forensic computing, the RAID 5 system, which includes all parameter features, was created with VROC (Virtual RAID On CPU) software. File copying and deletion operations were performed within the created RAID system. As a result of the processes, the image of the hard disks was taken with the Tableau TD2u hardware. The images taken were examined with the software named DiskInternals Raid Recovery. As a result of the examinations, it has been shown how the RAID structure is rebuilt with the specified software. While creating the RAID system, it has been determined that the software can automatically try all required parameter combinations, and in cases where automatic attempts do not yield successful results, the required parameters should be known by the user and entered into the software. It has been observed that if the required parameters are entered incorrectly, the disk structure cannot be created correctly and user data cannot be accessed. As a result, the parameters needed for the re-creation of RAID systems, which are frequently encountered in criminal investigations but have not been demonstrated in practice, have been put forward and the methods to be followed in the investigations have been determined.*

Keywords : *RAID, Forensics, Striping, Mirroring, Parity*

GİRİŞ

Bilişim sistemlerinin hayatımızın her alanında olması sebebiyle pek çok veri artık bilgisayar ortamında tutulmaktadır. Kişi, kurum ya da kuruluşlar, verilerini fiziksel olarak saklamaktan ziyade bilgisayar ortamında tutmayı tercih etmektedir. Teknolojinin gelişimi ve yaygınlaşması ile birlikte bilgisayar ortamına aktarılan verilerin kapasitesi günden güne artmaktadır (Oğuz, 2013, s. 2). Konuyu örneklerle açıklayacak olursak, cep telefonları günümüzde vazgeçilmez bir bilişim ürünüdür. İlk çıkan kameralı cep telefonları ile çekilen fotoğraf ve videoların boyutları KB (Kilobayt) cinsindeyken günümüzdeki cep telefonlarıyla çekilenler ise GB (Gigabayt) boyutunda olabilmektedir. Cep telefonu kameralarının 4K (Yatay çözünürlük yaklaşık 4000 piksel) görüntü kalitesinde görüntü vermeye başladığı bu günlerde birçok film çekimi cep telefonları ile yapılmaktadır (Demirel, 2021, s. 95). Kullanıcılar cep telefonlarındaki verileri depolamak için genel itibariyle sabit veya taşınabilir diskler kullanmaktadır. Ayrıca, kamera teknolojisinin giderek gelişmesi ve insanların güvenlik kaygıları sebebiyle, gerek kamusal alanlarda, gerekse özel alanlarda güvenlik kameralarının

yaygın olarak kullanıldığını rahatlıkla görülebilmektedir (Bahar, 2013, s. 207). Meydana gelen bir suçta, kamera kaydı görüntüleri kolluk kuvveti için oldukça kıymetli bir delildir. Güvenlik kameralarının sürekli kayıt yapmaları sebebiyle çok büyük boyutta veri depolama alanına ihtiyaç duyulmaktadır. Kaydın yapıldığı veri depolama alanları ne kadar büyükse, daha eski tarihlere ait kayıtların saklanabilmesi de o kadar mümkündür. Başka bir örnekte ise, bir bankanın veri tabanını düşünülecek olursa, müşterilerinin kişisel bilgileri ile tüm hesap hareketlerinin kaydedildiği TB (Terabayt)'lar büyüklüğünde veriler akıllara gelebilir. Kasım 2018 tarihli ABD merkezli market araştırmaları şirketi olan IDC (International Data Corporation) tarafından hazırlanan bir raporda, 2018 yılında 33 ZB (Zettabayt) olan küresel veri dünyasının, 2025 yılında 175 ZB'a yükseleceği belirtilmektedir (1 ZB = 1 000 000 000 TB) (Reinsel, 2018, s. 6). Bu büyüklükteki verinin depolanabilmesi için en az o boyutta depolama alanına ihtiyaç duyulacaktır. Anlaşılacağı üzere her geçen gün daha fazla veri depolama alanına ihtiyaç vardır. Bu veri depolama alanlarını günümüz teknolojisi ile oluşturmak için birden çok sabit diski belirli bir algoritmayla birbiriyle uyumlu biçimde çalıştırarak depolama alanını ve güvenliğini arttıran RAID sistemleri kullanılmaktadır.

RAID sistemlerinin kullanımının yaygınlaşması ile birlikte incelenmek üzere kriminal laboratuvarlara gönderilen sabit diskler içerisinde çok sayıda RAID yapısında diskle karşılaşılmaktadır. RAID yapıdaki diskler karmaşık yapıları nedeni ile incelemesini yapan uzman personeli zaman ve emek bakımından oldukça uğraştırdığı ayrıca maliyetli olduğu bilinmektedir (Zoubek vd, 2016, s 45). Bazen de RAID yapısındaki diskler başarılı bir şekilde birleştirilemediği için içerisindeki anlamlı verilere ulaşılamadığı gözlemlenmektedir Bu konuyla ilgili yapılan araştırmalarda, Zoubek ve ark. Blok seviye entropi yöntemi kullanarak tüm ilgili RAID parametrelerini otomatik olarak tespit etmek için yeni bir yaklaşım sunduğu bilinmektedir (Zoubek vd, 2016, s. 45). Xiang, 2 parity şerit aracılığı ile daha yüksek seviyede güvenlik sağlayan RAID 6 sistemlerden veri kurtarma yaklaşımı tanımlamaktadır (Xiang vd, 2011, s. 1). Corbett ve ark. RDP (Row-Diagonal Parity – Satır Çapraz Parite) algoritması gibi RAID 6 kodlarının 2 disk hatasına karşı verileri koruduğunu çalışmalarında göstermektedir (Corbett vd, 2004, s. 1). Kiselev ve ark. ise bir parity RAID sistemi içerisinde bozulmuş olan verileri otomatik olarak tespit etme ve kurtarma konusunda bir yaklaşım ortaya koymuştur (Kiselev vd, 2006 s.1). Hart tarafından sunulan çalışmada, RAID sistem üzerinde işletim sistemi çalışırken bir sistem hatası meydana gelmesi durumunda RAID sistemi yeniden oluşturmak için gerekli olan ayarlar için otomatik bir yaklaşım tanımladığı anlaşılmıştır (Hart, 2002, s.1). Goel and Corbett, 3 parity disk kullanarak 3 disk hatasından korunmayı sağlayan bir algoritma geliştirmiştir (Goel & Corbett, 2012, s. 41). Hausknecht ve ark. özellikle anti forensic olarak kullanılan standart olmayan RAID konfigürasyonlarını bildirdiler. Eğer RAID parametreleri bilinmiyorsa yeniden inşası mümkün olmayabilmektedir . Onlar, inceleyici personelin ihtiyaç duyulan parametreleri ve şüphelinin bilgisayarına ait konfigürasyon bilgilerini fiziksel disklerden ziyade mantıksal bölümlerden toplamayı önerdiler (Hausknecht

vd, 2017 s. 1237). Hilgert ve ark. Linux işletim sisteminde çoklu diskleri destekleyen BTRFS (B-Tree File System – B-Tree Dosya Sistemi)'de RAID konseptinin nasıl uygulandığını gösterdi (Hilgert vd, 2018 s.21-29). Choi ve ark. Standart olmayan RAID türlerinden olan ve Linux işletim sistemi üzerine kurulu olan hibrit RAID sistemlerinin yeniden inşası için yeni bir yöntem sundu (Choi vd, 2020;65(3):966-73). "Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler" (Gül, 2018, s. 77) ve "Memory Forensics" (Bolat, 2015, s. 28) isimli yüksek lisans tez çalışmalarında, RAID olarak yapılandırılan sabit disklerin adli bilişim açısından incelenmesi hususu daha fazla teknik bilgi ve imkân gerektirmesi nedeniyle, sistem faal olarak çalışırken RAID yapıdaki disklerin olay yerinde mantıksal bölüm olarak kopyasının alınması önerilmektedir.

Yapılan araştırmalar neticesinde, RAID sistemlerinin adli bilişim açısından incelenmesine yönelik uygulamalı çalışmaların bulunmadığı anlaşılmıştır. Kriminal laboratuvarlara delil kapsamında gelen RAID sistemlerinin incelenmesi aşamasında, RAID sistemini oluşturan disklerin yapısının anlaşılması, diskleri inşa edecek olan yazılımların tespiti ve kullanılması, ayrıca yazılımları kullanırken hangi parametrelerin önemli olduğunun bilinmesi gerekmektedir. Tüm bu bilgilere, uzun süreli yapılan araştırmalar ve kriminal laboratuvarlarda kazanılan tecrübeler neticesinde ulaşılabileceği değerlendirilmektedir. Bu çalışmada, ileriki süreçlerde RAID sistemlerinin adli yönden incelemesinin tam ve eksiksiz bir şekilde yapılabilmesi amacıyla RAID sistemlerinin çeşitleri (RAID seviyeleri), en çok kullanım alanı olan RAID 0, 1 ve 5 seviyelerinin çalışma mantıkları ile kullanılan parametreler ortaya konulmuştur. Ayrıca RAID 5 olarak yapılandırılan sabit disklerin adli bilişim açısından incelemesi yapılarak kullanılan yazılımlar ve izlenecek yöntemler uygulamalı olarak gösterilmiştir. RAID 5 sisteminin yeniden inşası için gerekli olan parametrelerin eksik veya yanlış girilmesi sonucunda oluşan disk yapıları da ortaya konulmuştur.

1. RAID VE SEVİYELERİ

1.1. RAID

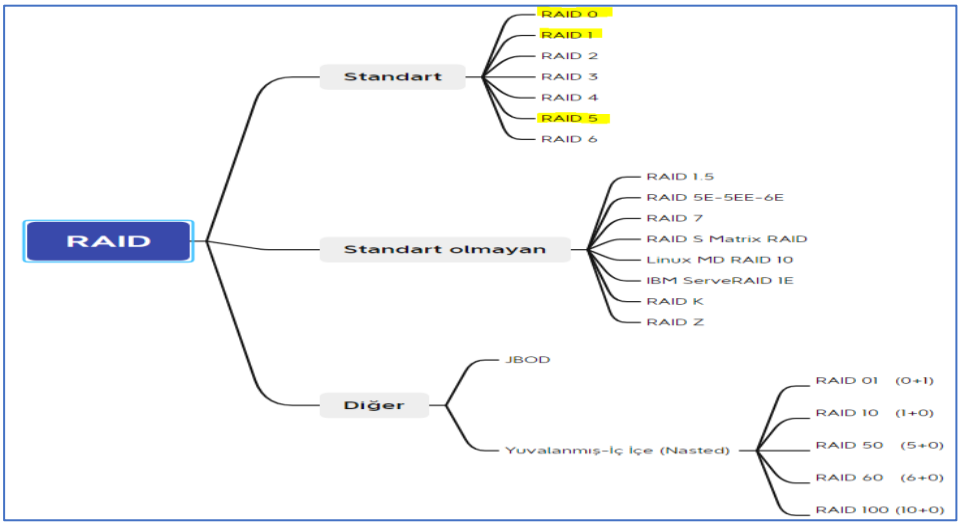
RAID, yüksek performanslı ve yedekli disk sistemleri elde etmek için tasarlanmış bir depolama mimarisi olduğu şeklinde tanımlanmıştır (Balı, 2010, s 1). RAID aralarında verilerin belirli bir algoritmayla dağıtıldığı veya çoğaltıldığı birden çok sürücüyü tek bir mantıksal sürücü gibi kullanan veri depolama sistemini ifade etmektedir. RAID yapılandırmasına bağlı olarak (genellikle seviye olarak adlandırılır. RAID 0, 1 ve 5 gibi) kullanıcılara güvenilirlik, kullanılabilirlik, performans ve kapasite gibi faydalar sağladığı bilinmektedir.

RAID kavramı ilk olarak, California Üniversitesi akademisyenleri olan David A. Patterson, Garth A. Gibson ve Randy H. Katz'ın 1988 yılında hazırladığı "A Case for Redundant Arrays of Inexpensive Disks (RAID)" isimli makalede kullanılmıştır (Sammes & Jenkinson, 2007, s. 207). RAID kelimesi içerisinde kullanılan "I" harfinin şu an ki tanımında bulunan Independent (bağımsız) kelimesinden değil Inexpensive (ucuz) kelimesinden geliyor olmasıdır. Bunun sebebi, 1980'li yıllarda veri depolama birimlerinin maliyetlerinin yüksek

olması, ucuz olan depolama birimlerinin ise kapasitelerinin düşük olmasıydı. Patterson, Gibson ve Katz bu soruna karşı yaptıkları çalışmada ucuz ve düşük kapasiteli depolama birimlerini birleştirerek pahalı ve büyük kapasiteli birimlerin yerine geçebileceğini göstermiştir (Patterson vd, 1988, s 115). Ayrıca veri kaybını önlemek maksadıyla, disk hatalarından kaynaklı veri kayıplarına karşı olan koruma düzeyinin de artmış olduğu belirtilmiş (Stott, 1998, s. 17) ve zaman içinde geliştirilerek günümüz RAID seviyeleri haline getirilmiştir. RAID seviyeleri donanımsal ve yazılımsal olarak 2 farklı türde gerçekleştirilebilmektedir. İki türünde kendilerine göre artı ve eksi taraflarının bulunduğu bilinmektedir.

1.2. Seviyeleri

RAID seviyelerini, standart, diğer ve standart olmayan RAID seviyeleri olarak gruplandırılmaktadır (Şekil 1). Standart RAID seviyeleri RAID 0, 1, 2, 3, 4, 5, 6 olarak adlandırılabilir (Wayne, 2015, s. 58). Diğer RAID seviyeleri, Sadece Bir Yığın Disk (Just a Bunch of Discs - JBOD) ve Yuvalanmış/İç İçe (Nested) geçmiş RAID seviyeleri (RAID 01, RAID 10, RAID 50, RAID 60 ve RAID100) olarak adlandırılır. Standart olmayan RAID seviyeleri ise bazı şirketlerin veya ürünlerin kendilerinin geliştirdiği RAID seviyeleridir ve standart RAID seviyeleri ile temelde aynı mantık kullanılsa da bazı farklılıklarının bulunduğu bilinmektedir. Kullanım alanları kısıtlı olan bu RAID seviyelerine RAID 1.5, RAID 5E-5EE-6E, RAID 7, RAID S Matrix RAID, Linux MD RAID 10, IBM ServeRAID 1E, RAID K ve RAID Z örnek verilebilir (*en-academic.com, 2022, s. 1*).



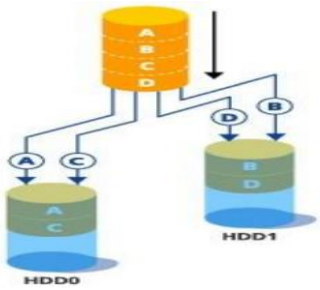
Şekil 1: RAID Seviyeleri

1.3. En sık kullanılan RAID seviyeleri

RAID (0, 1 ve 5) seviyelerinin en sık kullanılan ve en çok dikkate alınması gereken RAID seviyeleri olduğu belirtilmektedir (Wayne, 2015, s. 59). Diğer RAID seviyelerinin neredeyse tamamı bu üçünün çalışma mantığı temelinde oluşturulmaktadır.

1.3.1. RAID 0 seviyesi

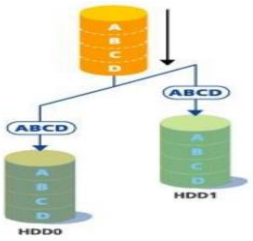
Bu RAID seviyesi en az 2 adet disk kullanılarak oluşturulur. Bu yapılandırmada, sabit sürücülerin tamamı tek bir birim olarak değerlendirilir ve toplam alanı tüm sabit sürücülerin alanlarının toplamı kadardır. İki adet 1 TB kapasiteli sabit disk varsa, RAID 0 bunları etkili bir şekilde tek bir 2 TB kapasiteli birime dönüştürecektir. Veriler birden fazla diske aynı anda yazılıp okunduğu için hız artışı sağlar, ancak herhangi bir hata toleransı sunmaz. Bir sabit disk bozulursa, tüm disklerdeki tüm bilgiler kaybolabilmektedir (Wayne, 2015, s. 60). (Şekil 2).



Şekil 2: RAID 0 Çalışma Mantığı Şekilsel Gösterimi

1.3.2. RAID 1 seviyesi

Bu RAID seviyesi en az 2 adet disk kullanılarak oluşturulur. Veriler bir diske yazılırken bir kopyası da diğer diske yazılır. Sabit sürücülerden biri arızalanırsa aynı bilgiler diğer sürücüde olduğundan veri kaybı olmaz. Hasarlı olan değiştirildiğinde, veriler yeni diske tekrar kopyalanacaktır. En büyük dezavantajı, RAID 1'in toplam alanının, sabit disklerin toplam alanının yarısı kadar olmasıdır. İki adet 1 TB kapasiteli sabit disk varsa, yalnızca 1 TB kapasiteli kullanılabilir alan olur. Çünkü her sabit disk birbirinin kopyası olduğundan aynı verileri içerecektir (Wayne, 2015, s. 60). Herhangi bir veri silindiğinde, o veri tüm disklerden silinir. Tüm disklerin boyutları birbirine eşit olmak zorundadır (Şekil 3).

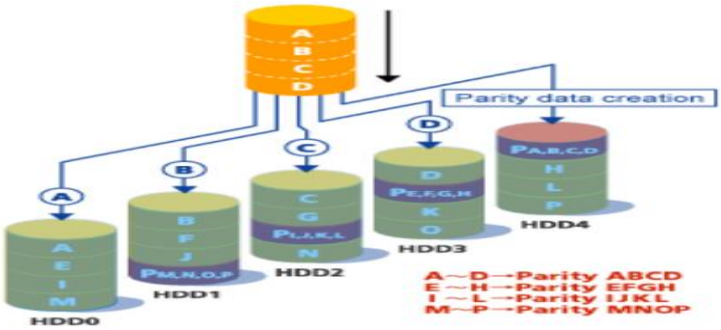


Şekil 3: RAID 1 Çalışma Mantığı Şekilsel Gösterimi

AJIT-e Academic Journal of Information Tecnology
2023 Spring/Bahar – Cilt/Vol: 14 - Sayı/Issue: 53
10.5824/ajite.2023.02.004.x

1.3.3. RAID 5 seviyesi

Bu RAID seviyesi en az 3 adet disk ile oluşturulabilir. Şeritlemenin yanı sıra dağıtılmış eşlik bilgisi veriler disklere yazılır. Eşlik bilgisi için tahsis edilen ayrıca bir disk yoktur. Eşlik bilgisi kullandığı geometri mantığına göre ilgili disklere dağıtılarak yazılır. Dolayısıyla eşlik bilgisi tüm sürücülere dağıtılmış olur (Sammes & Jenkinson, 2007, s. 208). Sürücülerden birinin boyutu, tüm sabit sürücüler arasında dağıtılan eşlik bilgisi için ayrılmıştır. Yani eşlik bilgisi boyutu 1 diske eşittir. Var olan toplam disk sayısı "x" olarak belirlenirse, kullanılabilir disk/alan boyutu "x-1" olarak hesaplanabilir. Örneğin; 3 disk kullanılarak oluşturulan RAID 5 yapılandırmasında 1 disk boyutu kadar boyut eşlik bilgisi için kullanılır. Disklerden herhangi birinde problem olması durumunda veri kaybı yaşanmaz. Fakat aynı anda iki veya daha fazla disk bozulması durumunda ise veriler kaybolabilmektedir. Bozulan diskin yerine yeni bir disk takıldığında eşlik bilgisi sayesinde bozulan diskteki veriler aynı şekilde yeniden oluşturulup yeni diske yazılacaktır (Şekil 4).



Şekil 4: RAID 5 Çalışma Mantığı Şekilsel Gösterimi

1.4. RAID parametreleri

RAID seviyelerinin oluşturulması esnasında kullanıcı tarafından ayarlanan veya ayarlanmayıp varsayılan değerlerinde bırakılan önemli parametreler bulunmaktadır. Bu parametreler, RAID yapısının yeniden inşa edilmesi esnasında önemli rol almaktadır. Bu parametreler disk sırası, diskler içerisinde kullanılacak veri kümelerinin şerit boyutu ve geometri bilgisidir.

1.4.1. Şerit boyutu parametresi

Şerit boyutu, verinin belirli boyutlara ayrılarak disklere yazılması durumudur. RAID 0 ve RAID 5 seviyesindeki bir RAID yapılandırmasının yeniden inşasında bilinmesi gereken çok önemli bir husustur. Şerit boyutu üretici firmadan firmaya farklılık gösterebildiği için RAID yapılandırmasının hangi firma tarafından oluşturulduğunun bilinmesi inceleyiciye büyük bir ipucu verebilir. RAID yapılandırması için önde gelen firmalar ile kullandığı şerit boyutları ve varsayılan değerler "Diskinternals RAID Recovery" yazılımı aracılığıyla tespit edilmiş olup, Tablo 1'de sunulmuştur.

Tablo 1: RAID 0 ve RAID 5 İçin Önde Gelen Firmaların Kullandığı Şeritleme Değerleri

RAID Yapılandırmasında Önde Gelen Firmalar	**RAID 0 Seviyesi**		**RAID 5 Seviyesi**	
	Kullanılan Varsayılan Değer	Desteklediği Diğer Değerler	Kullanılan Varsayılan Değer	Desteklediği Diğer Değerler
Linux	512 KB	2-4-8-16-32-64-128-256 KB, 1 MB	512 KB	2-4-8-16-32-64-128-256 KB, 1 MB
Silicon	-	4-8-16-32-64-128 KB	-	-
Adaptec	512 KB	16-32-64-128-256 KB, 1 MB	512 KB	16-32-64-128-256 KB, 1 MB
HP	512 KB	8-16-32-64-128-256 KB, 1 MB	512 KB	8-16-32-64-128-256 KB, 1 MB
Megaraid	512 KB	16-32-64-128-256 KB, 1 MB	512 KB	8-16-32-64-128-256 KB, 1 MB
DELL	-	8-16-32-64-128-256-512 KB, 1 MB	-	8-16-32-64-256-512 KB, 1 MB
DDF	512 KB	16-32-64-128-256 KB, 1 MB	512 KB	16-32-64-128-256 KB, 1 MB
Intel	128 KB	4-8-16-32-64 KB, 1 MB	64 KB	8-16-32-128 KB
nVidia	64 KB	2-4-8-16-32 KB	64 KB	2-4-8-16-32-128 KB
Via	64 KB	2-4-8-16-32 KB	64 KB	2-4-8-16-32 KB
Ldm	64 KB	-	64 KB	64 KB
Apple	32 KB	16-64-128-256 KB	-	-

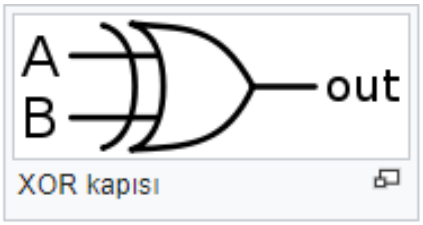
1.4.2. Eşlik (Parity) parametresi

RAID 5 seviyesi çalışma mantığının temelini oluşturur. Veriler disklere bölünerek yazılırken, aynı zamanda bölünen verilerin eşlik bilgileri de oluşturulur ve bu eşlik bilgisi disklere bölüştürülerek yazılır. Eşlik bilgisi XOR kapısı ile işleme sokularak oluşturulmaktadır. XOR (eXclusive OR - özel veya) kapısını oluşturan giriş veya çıkış değerlerinden herhangi ikisi biliniyorsa üçüncü veri hesaplanıp yeniden oluşturulabilmektedir(Şekil-1.5) (Carrier, 2005, s. 112, 113). XOR kapısı mantık tablosu Tablo 2'de sunulmuştur (*tr.wikipedia.org, 2022 s.1*).

AJIT-e Academic Journal of Information Tecnology
2023 Spring/Bahar – Cilt/Vol: 14 - Sayı/Issue: 53
10.5824/ajite.2023.02.004.x

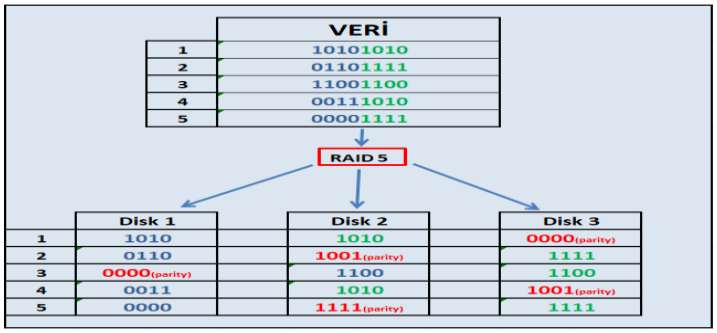
Tablo 2: XOR Kapısı Doğruluk Tablosu

A	B	Çıkış
0	0	0
0	1	1
1	0	1
1	1	0



Şekil 5: XOR Kapısı Şekilsel Gösterimi

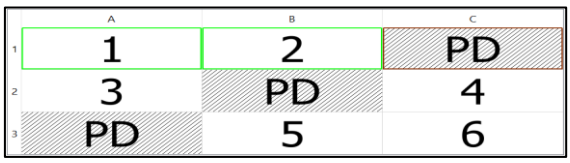
Eşlik bilgisinin çalışma mantığının daha iyi anlaşılabilmesi amacıyla Şekil-1.6'da görüldüğü üzere "Veri" sütunu disklere yazılacak veriyi temsil etmektedir ve 8 bit (1 byte) büyüklüğünde beş ayrı veri RAID 5 yapılandırması ile 3 adet diske yazılacaktır. 8 bitlik her bir veri 4'er bitlik şeritler haline bölünerek disklere yazıldığı görülmektedir. Her bir şerit farklı renkler ile belirtilmiştir. Her bir şerit(4'er bitlik veri) XOR kapısı mantığı ile işleme sokularak eşlik bilgisi elde edilmektedir. (Carrier, 2005, s 113).



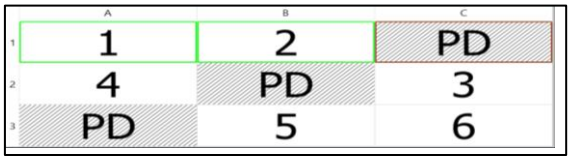
Şekil 6: Eşlik Bilgisinin Çalışma Mantığı

1.4.3. Eşlik bilgisinin disklere yazılma düzeni/ geometri

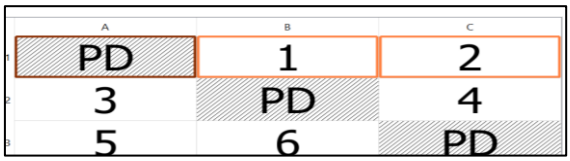
Eşlik bilgisi disklere yazılırken birkaç farklı mantık ile yazılmaktadır. Bu yazım mantıklarına genel olarak geometri adı verilmektedir. Bunlar; "Backward (Left Asynchronous)" (Şekil 7), "Backward Continuation (Left Synchronous)" (Şekil-1.8), "Forward (Right Asynchronous)" (Şekil-1.9) ve "Forward Continuation (Right Synchronous)" (Şekil 10) olarak isimlendirilirler (*www.seagate.com ,2022_s.1 & ark.intel.com, 2022, s.1*). Bu geometrilerin eşlik bilgisini disklere yazma mantığı aşağıda gösterilmiştir. (PD: Parity Disk – parity bilginin yazıldığı disk)



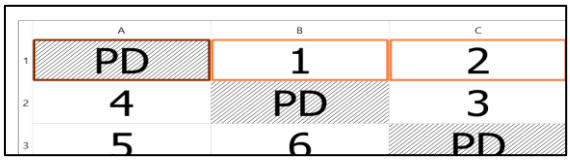
Şekil 7: Backward (Left Asynchronous) Eşlik Verisinin Yazılma Mantığı



Şekil 8: Backward Continuation (Left Synchronous) Eşlik Verisinin Yazılma Mantığı



Şekil 9: Forward (Right Asynchronous) Eşlik Verisinin Yazılma Mantığı



Şekil 10: Forward Continuation (Right Synchronous) Eşlik Verisinin Yazılma Mantığı

2. GEREÇ VE YÖNTEM

2.1. Gereç

Yapılan araştırmalarda en sık kullanılan RAID sistemlerinden biri olan ve tüm parametre özelliklerini üzerinde barındıran RAID 5 sisteminin aşağıda belirtilen donanım ve yazılımlar ile adli bilişim yönünden incelenmesi gerçekleştirilmiştir.

- HP marka, Z840 model iş istasyonu (RAID sisteminin oluşturulması aşamasında kullanılmıştır.).
- Lenovo marka, P920 model iş istasyonu (RAID sisteminin incelenmesi aşamasında kullanılmıştır.).
- Toshiba marka, "DT01ACA050" model, "Y5RAPGNAS" seri numaralı sabit disk.
- WD marka, "WD5000AAKX" model, "WMAYU6039620" seri numaralı sabit disk.
- Hitachi marka, "HTS545050B9A300" model, "110923PBN408P7GBNKGE" seri numaralı sabit disk.
- Tableau TD2u Birebir Kopyalama Alma Donanımı
- Tableau Forensic Bridge Yazma Koruma Donanımı
- VROC Yazılımı (Version 7.7.0.1260)
- AccessData FTK Imager Yazılımı (Version 4.3.1.1)
- DiskInternals Raid Recovery Yazılımı (Version 6.8.0)

2.2. Yöntem

Gereç bölümünde ayrıntıları belirtilen Toshiba, WD ve Hitachi marka sabit disklere Tableau TD2u Birebir Kopyalama Alma Donanımı kullanılarak güvenli silme işlemi (wipe) uygulandıktan sonra Windows 10 Pro for Workstations işletim sistemi yüklü HP marka, Z840 model iş istasyonuna takılmıştır. Bilgisayar içerisinde takılı vaziyette bulunan sabit disklere

VROC yazılımı ile RAID 5 sistemi oluşturulmuştur. Oluşturulan RAID sistemi içerisinde bazı kullanıcı işlemleri (dosya kopyalanması ve silinmesi) gerçekleştirilmiş ve Tableau Forensic Bridge yazma koruma donanımı ile bilgisayar bağlantısı yapılmış ve RAID sistemini oluşturan sabit disklerin ayrı ayrı imajları (birebir kopyaları) AccessData FTK Imager yazılımı ile alınmıştır. Alınan birebir kopyalar inceleme bilgisayarına kopyalandıktan sonra DiskInternals Raid Recovery yazılımı ile RAID 5 sistemi tekrardan oluşturulmak suretiyle içeriğinde incelemeler gerçekleştirilmiştir. Ayrıca RAID sisteminin tekrardan oluşturulması esnasında parametrelerin doğru ve yanlış girilmesi neticesinde oluşan sonuçlar ortaya konulmuştur.

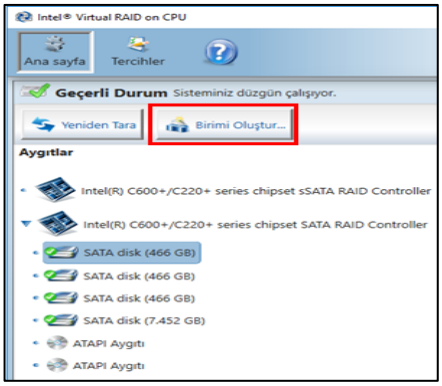
2.2.1. Sabit disklerin güvenli silme işlemi

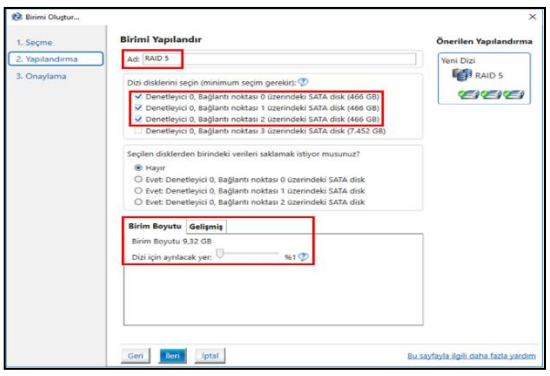
RAID 5 sistemi oluşturulmadan önce kullanılacak sabit disklerin güvenli silme işlemleri Tableu TD2u Birebir Kopyalama Alma Donanımı ile yapılmıştır (Şekil 11).

Şekil 11: Sabit Disklere Uygulanan Güvenli Silme İşlemi

2.2.2. Intel VROC Yazılımı ile RAID 5 Seviyesi Oluşturma

RAID 5 seviyesi oluşturulurken 3 adet disk kullanılmıştır. Bilgisayarda kurulu olan VROC yazılımı kullanılarak RAID 5 seviyesi oluşturulmuştur (RAID 5 birimi boyutu inceleme esnasında zamandan tasarruf sağlamak maksadıyla 9,31 GB olarak sınırlandırılmıştır) (Şekil 12 ve Şekil 13.).

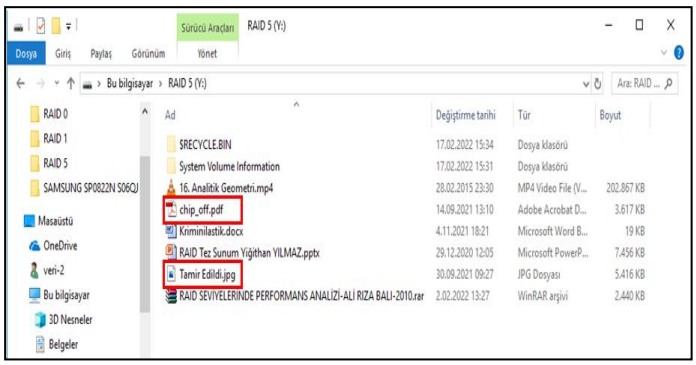




Şekil 12: "Birim Oluştur" Sekmesi

Şekil 13: RAID 5 Seçeneğinin Seçilmesi

İlerleyen aşamada, açılan pencerede "Gelişmiş" sekmesi altında ise veri şeridi boyutu (stripe size), Intel firmasının varsayılan değeri olan 64 KB seçilmiştir. Daha sonra "Bilgisayarım-Yönet-Disk Yönetimi" kısmı altında görüntülenen disk başlatılmış ve MBR (Master Boot Record – Ana Önyükleme Kaydı) bölümleme sistemi seçilmiştir. Sonraki aşamada NTFS (New Technology File System – Yeni Teknoloji Dosya Sistemi) dosya sistemi ile biçimlendirilmiş ve kullanıma hazır hale getirilmiştir. Oluşan RAID 5 bölümü içerisine Şekil-2.4'te belirtilen dosyalar kopyalanmış ve içerisinden "chip_off.pdf" ve "Tamir Edildi.jpg" dosyaları "shift+del" tuş kombinasyonları kullanılarak silinmiştir.

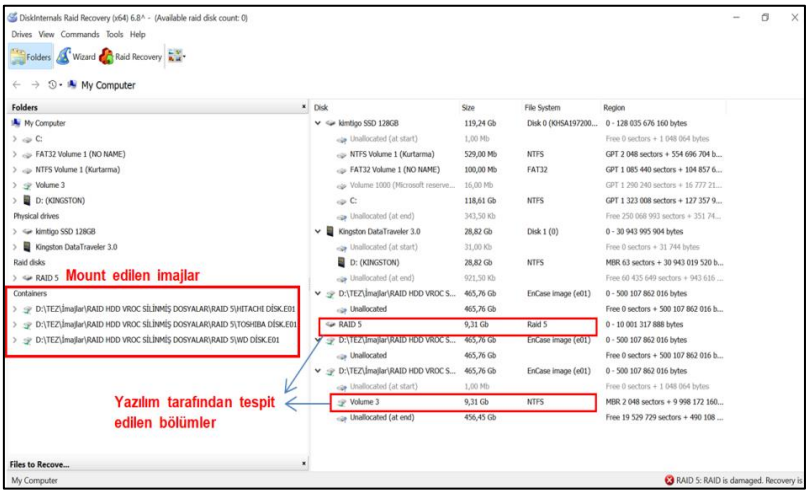


Şekil 14: RAID 5 Biriminin İçerisine Kopyalanan ve Silinen Dosyalar

3. BULGULAR

3.1. RAID 5 Olarak Yapılandırılan Disk İmajlarının DiskInternals Yazılımı ile İncelenmesi

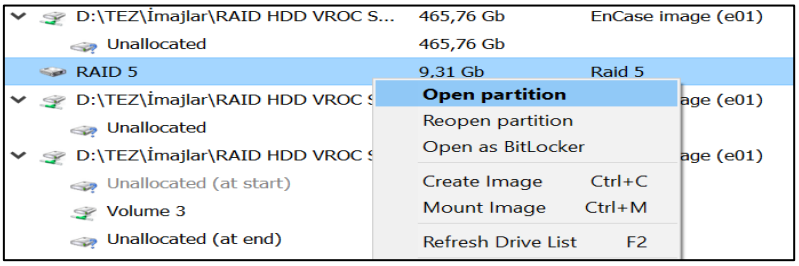
AccessData FTK Imager yazılımı ile alınan 3 adet disk imajı DiskInternals Raid Recovery yazılımının imaj mount etme (Bir imajın bilgisayar içerisine bir disk bölümü olarak eklemesi) özelliği kullanılarak mount edilmiş ve yazılım arayüzünde görüntülenmiştir. Diskler mount edildikten sonra yazılım tarafından "RAID 5" ve "Volume 3" (9,31 GB kapasiteli) isimlerinde bölümlerin oluşturulduğu görülmüştür (Şekil-3.1).



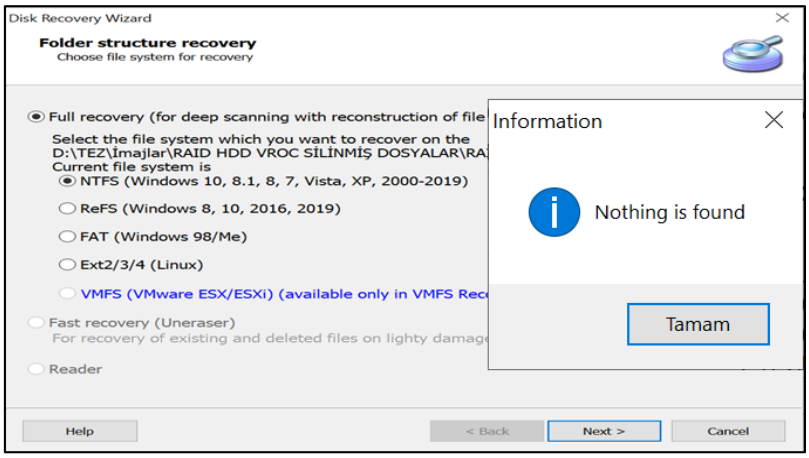
Şekil 14: DiskInternals Yazılımında İmajların Mount İşlemi Sonrası Görüntülenmesi

AJIT-e Academic Journal of Information Tecnology
2023 Spring/Bahar – Cilt/Vol: 14 - Sayı/Issue: 53
10.5824/ajite.2023.02.004.x

"RAID 5" bölümü görüntülenmek istendiğinde, açılan pencerede "Full recovery" ve "NTFS" seçenekleri seçilerek tarama işlemi başlatılmaya çalışılmış fakat "Nothing is found" uyarısıyla karşılaşılmış ve dosya sistemi tanımlanamadığından içeriğinde bulunan dosyalara erişim sağlanamamıştır (Şekil 15, Şekil 16).

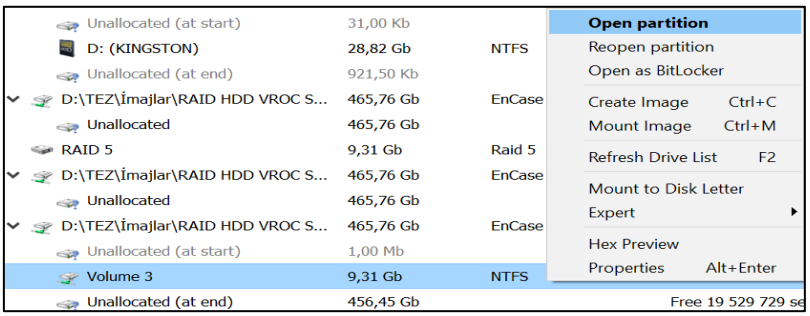


Şekil 15: "RAID 5" Bölümünün Görüntülenmeye Çalışılması

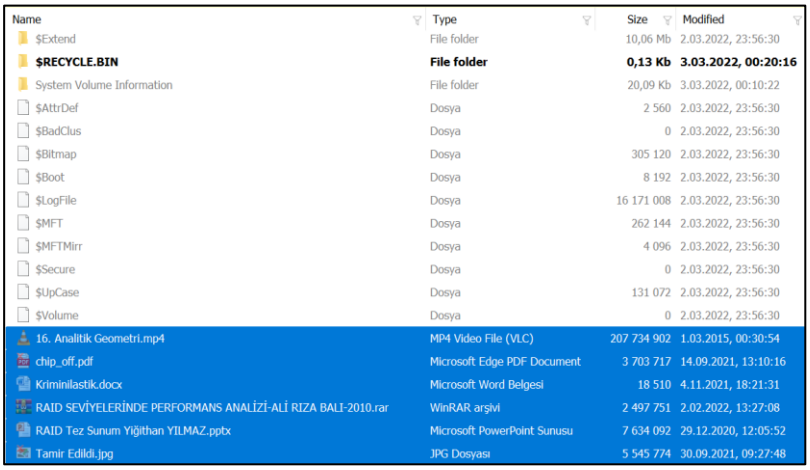


Şekil 16: Tarama İşlemi Sonucu Tanınan Herhangi Bir Dosyanın Bulunamadığı

"Volume 3" bölümü üzerinden tarama işlemi gerçekleştirildiğinde, dosya isim bilgilerini doğru bir şekilde tespit ettiği fakat tespit edilen dosyaların içeriğinin görüntülenemediği tespit edilmiştir (Şekil 17, Şekil18 ve Şekil 19).



Şekil 17: "Volume 3" Bölümünün Görüntülenmeye Çalışılması

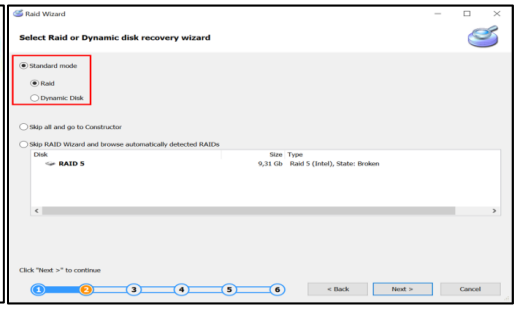


Şekil 18: İlgili Dosyaların Bölüm İçerisinde Görülmesi

Şekil 19: İlgili Dosyaların Görüntülenemediği

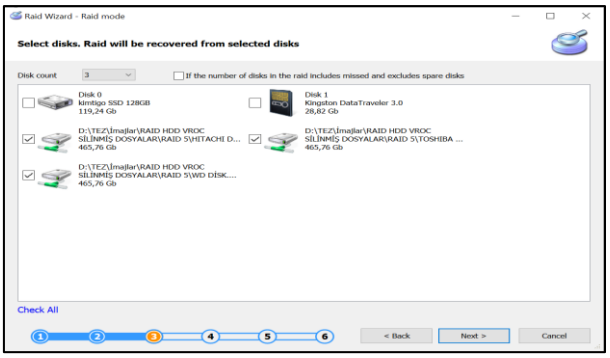
Ardından RAID parametreleri inceleyici personel tarafından girilerek RAID yapısı yeniden inşa edilmeye çalışılmıştır. Yazılım arayüzünde bulunan "Raid Recovery" sekmesi seçilerek (Şekil-3.7) açılan pencerede, "Standart mode" ve "Raid" seçenekleri işaretlenmiş, bir sonraki adımda mount edilen disk imajları seçilmiştir (Şekil 20 ve Şekil 21)

Şekil 20: DiskInternals Yazılımı "Raid Recovery" Sekmesi Seçeneğinin Seçilmesi



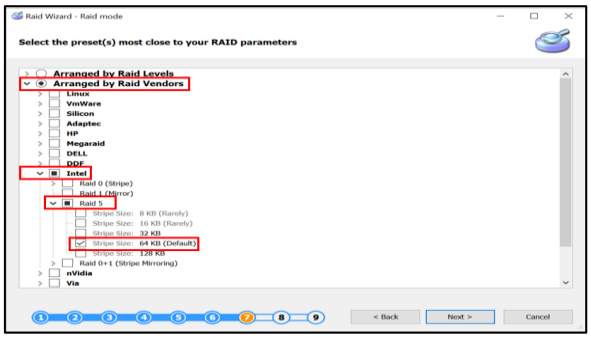
Şekil 21: Standart Mode-Raid

AJIT-e Academic Journal of Information Tecnology
2023 Spring/Bahar – Cilt/Vol: 14 - Sayı/Issue: 53
10.5824/ajite.2023.02.004.x



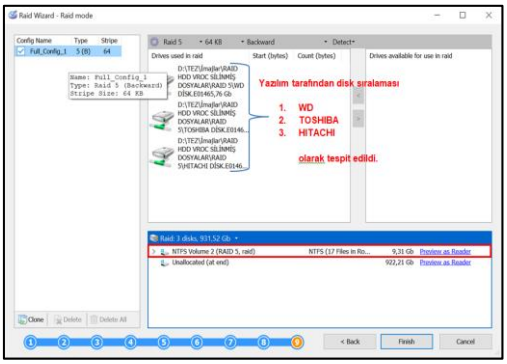
Şekil 22: Mount Edilen Disk İmajlarının Seçilmesi

Bu durumda iki farklı yol izlenerek devam edilebilir. İlk yol olarak "Arranged by Raid Vendors" (RAID Satıcılarınca Göre Düzenlenmiş) seçeneği altında bulunan parametreler; satıcı olarak Intel, RAID seviyesi olarak Raid 5, ve şerit boyutu olarak 64 KB girilmiştir (Şekil 23).



Şekil 23: Arranged by Raid Vendors Seçeneği Altında Yapılan Parametre Seçimleri

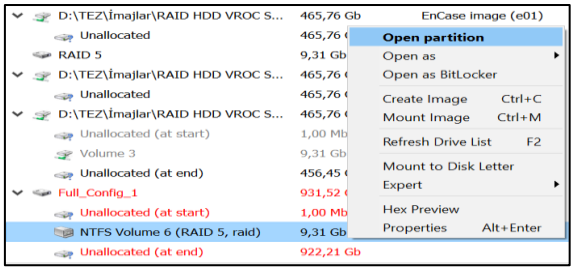
Parametreler girilip devam edildiğinde; "Full_Config_1" ismi altında disk sırasının yazılımca tespit edildiği, geometri bilgisinin "Backward" ve "NTFS" dosya sistemiyle biçimlendirilmiş 9,31 GB kapasiteli bölümün tanındığı görülmüştür (Şekil 24).



Şekil 25: Yazılım Tarafından Disk Sıralamasının Tespiti

Yazılım ana ekranında, "Full_Config_1" başlığı altında oluşan 9.31 GB kapasiteli NTFS bölüm görülmüştür. Bu bölüm üzerinde sağ tıklanıp "Open partition" seçeneği seçilerek açılmıştır. Seçilen bölüm içerisinde NTFS dosya sisteminde tarama işlemi başlatılmış ve

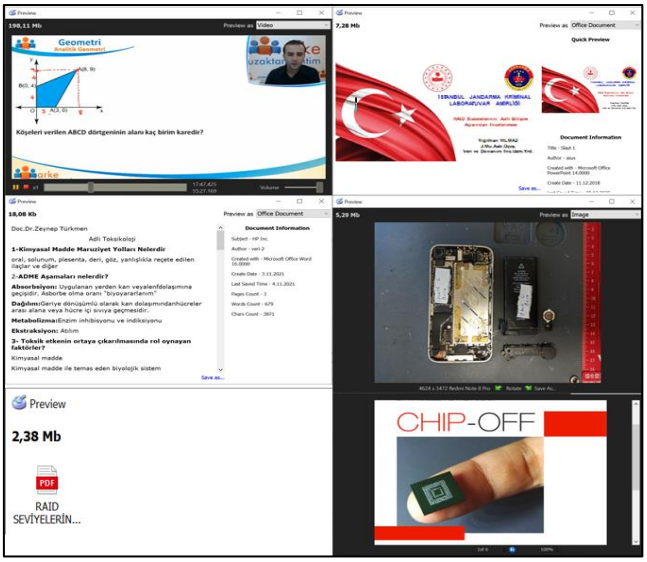
tarama sonucunda kullanıcı tarafından oluşturulan dosyalara ulaşılmıştır (Şekil 26 ve Şekil 27).



Şekil 26: "NTFS Volume 6 (RAID 5, raid)" Bölümünün Görüntülenmeye Çalışılması

Şekil 27: İlgili Dosyaların Bölüm İçerisinde Görülmesi

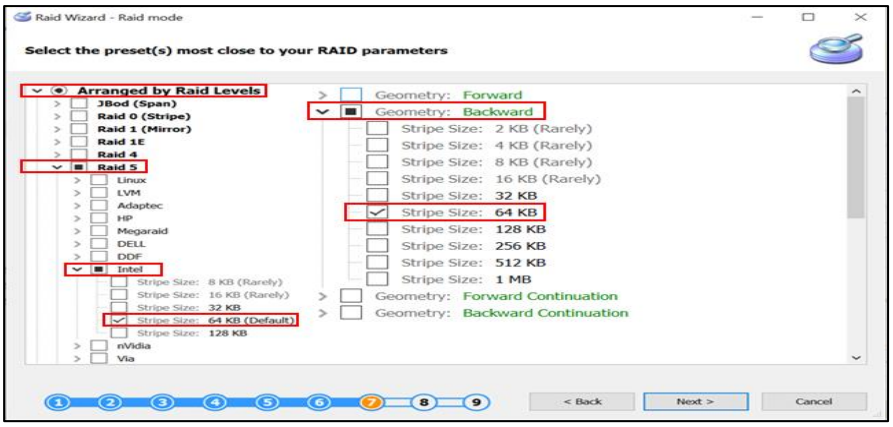
Tespit edilen dosyaların tamamı sorunsuz bir şekilde görüntülenmiştir (Şekil 28).



Şekil 28: İlgili Dosyaların Tamamının Sorunsuz Bir Şekilde Görüntülenmesi

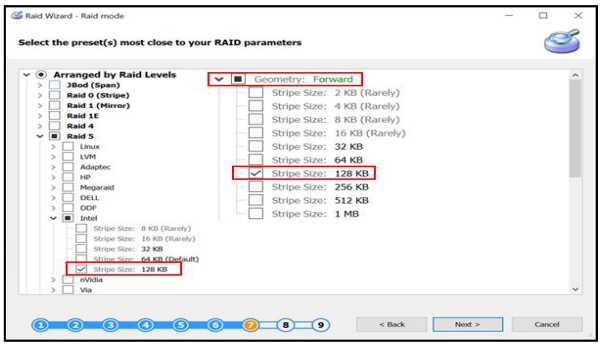
İkinci yol olarak "Arranged by Raid Levels" (RAID seviyelerine göre düzenlenmiş) seçeneği altında bulunan parametreler; "RAID 5", satıcı "Intel", "Stripe Size 64 KB" ve geometri olarak "Backward" ayarı girilerek (Şekil 28) tekrardan denendiğinde Şekil 27'de belirtilen dosyaların tamamı tekrardan sorunsuz bir şekilde görüntülenmiştir.

AJIT-e Academic Journal of Information Tecnology
2023 Spring/Bahar – Cilt/Vol: 14 - Sayı/Issue: 53
10.5824/ajite.2023.02.004.x

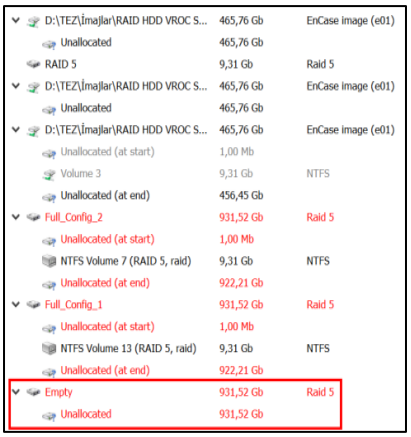


Şekil 29: Arranged by Raid Levels Seçeneği Altında Yapılan Parametre Seçimleri

Son olarak parametrelerden bazıları hatalı girilerek deneme yapılmıştır. "Stripe Size 128 KB" ve geometri bilgisi "Forward (128 KB)" olarak değiştirilmiştir (Şekil 3)0. Parametrelerin yanlış girilmesi sonucu yazılım tarafından tanınmış dosya sistemi görülmemiş olup, herhangi bir dosyaya erişim sağlanamamıştır (Şekil 31).



Şekil 30: Yanlış Girilen Geometri ve Şerit Boyutu Bilgileri



Şekil 31: Yanlış Girilen Geometri ve Şerit Boyutu Bilgileri

TARTIŞMA VE SONUÇ

Bu çalışmada, RAID sistemlerinin çeşitleri, çalışma mantıkları, kullandığı parametreler ortaya konulmuştur. Ayrıca adli bilişim açısından, RAID olarak yapılandırılan sabit diskler incelenirken dikkat edilmesi gereken hususlar ve kullanılan yazılımlar gösterilmiştir.

RAID seviyeleri arasında en sık kullanılanlarının RAID 0, RAID 1 ve RAID 5 olduğu tespit edilmiştir. Bunun sebebinin RAID sistemlerinin amacını yerine getirmek için kullandığı 3 farklı parametrenin bu seviyelere ait olmasıdır. Bunlar; RAID 0 için verilerin şeritlere bölünerek disklere yazılması, RAID 1 için verinin disklere aynalanması (yedeklenmesi) ve RAID 5 için ise verilerin şeritlere bölünerek disklere yazılması ve aynı zamanda kurtarma

amaçlı eşlik bilgisi oluşturmasıdır. Neredeyse diğer tüm RAID seviyelerinin tamamı, belirtilen bu seviyelerin (RAID 0, RAID 1 ve RAID 5) çeşitli kombinasyonları üzerine inşa edilmiş olduğu anlaşılmıştır.

RAID 5 sisteminin tekrardan oluşturulması esnasında kullanılan DiskInternals Raid Recovery yazılımının tüm parametre kombinasyonlarını otomatik olarak deneyerek doğru RAID konfigürasyonunu tespit etmeye çalıştığı görülmüştür. Yapılan denemede, RAID yapısının doğru bir şekilde yeniden inşa edilemediği durumlarda ihtiyaç duyulan parametrelerin kullanıcı tarafından bilinmesi ve yazılıma girilmesi gerektiği tespit edilmiştir. Yanlış parametre bilgileri girildiğinde ise özellikle geometri bilgisinin yanlış girilmesi sonucu RAID yapısının tanınmadığı görülmüştür. Kısmen yanlış girilen parametre değerleri (doğru geometri bilgisi, yanlış şerit boyutu ve disk sıralaması) uygulandığında; bazı durumlarda RAID yapısının tanındığı, içerisindeki dosya isim ve boyut bilgilerinin doğru olarak görülebildiği fakat içerisindeki dosyalara erişimin sağlanamadığı görülmüştür.

Diğer bir önemli husus ise RAID sağlayıcıların kullandığı parametre ayarlarının değişkenlik gösterebilmesidir. İnceleyici personelin, RAID sistemine hangi sağlayıcı firma tarafından destek verildiğini bilmesi, kendisine önemli bir ipucu olabilecektir. Bu sebeple, bazı önde gelen RAID sağlayıcı firmaların RAID 0 ve RAID 5 seviyelerinde kullandığı varsayılan ve desteklediği şerit boyutu bilgileri verilmiştir.

Yapılan incelemeler neticesinde; parametre değerlerinin, RAID sistemlerini tekrardan oluştururken gerekli olduğu anlaşıldığından, bilişim suçlarına müdahale eden teknik ekiplerce, olay yerinde bulunan RAID sistemlerine ait sabit diskler sökülmeden önce sıralamasının, RAID sistem sağlayıcısının (HP, Dell. Adaptec vb.) kim olduğunun, hangi RAID seviyesinin kullanıldığının, şerit boyutunun ve geometri bilgilerinin mutlaka not edilmesi gerektiği hususunun önemli olduğu anlaşılmıştır.

Yapılan kapsamlı araştırmalar ve laboratuvar ortamında kazanılan tecrübeler neticesinde, yukarıda belirtilen parametrelerin bilinmemesi veya eksik bilinmesi ile başlayacak adli bir incelemenin, RAID yapısını yeniden inşa ederken tüm parametre kombinasyonlarının denenmesi gerekeceğinden uzun zaman alacağı ve hatta sonuçlara ulaşılamayabileceği değerlendirilmektedir.

RAID sistemlerinin hem yazılımsal hem de donanımsal olarak inşa edilebilmesi sebebiyle; Şekil-1.1'de gösterildiği üzere RAID seviyeleri çok fazla çeşitlilik göstermektedir. Her ne kadar yapılan çalışma RAID (0,1 ve 5) seviyeleri üzerinde gerçekleştirilmiş olsa da kriminal incelemeler kapsamında tüm RAID seviyesine sahip disklerin de gelebileceği bir gerçektir. Bu kapsamda; RAID yapısındaki disklerin hangi seviyeye ait olduğunu tespit edebilen bir yazılımın geliştirilmesinin adli incelemelerde fayda sağlayacağı değerlendirilmektedir.

KAYNAKLAR

Bahar, F. (2022). Küresel güvenlik tedbirleri. Gözetleme olgusu bağlamında özel güvenlik ve mobese kameraları. *Sosyologca*, *3*(6). https://sosyologca.org/?mod=makale_tr_ozet&makale_id=54383

Balı, A. R. (2010). *Performance Analysis On Raid Levels*. [Yayınlamamış Yüksek Lisans Tezi]. Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü.

Bolat, Y. (2015). *Memory Forensics*. [Yayınlanmamış Yüksek Lisans Tezi]. İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü.

Carrier, B. (2005). *File system forensic analysis*. Addison-Wesley.

Choi, J., Park, J., & Lee, S. (2020). Reassembling linux-based hybrid raid. *Journal of Forensic Sciences*, *65*(3), 966-973. https://doi.org/10.1111/1556-4029.14258

Corbett, P., English, B., Goel, A., Grcanac, T., Kleiman, S., Leong, J., & Sankar, S. (2004). *{row-diagonal} parity for double disk failure correction*. 3rd USENIX Conference on File and Storage Technologies (FAST 04).

Demirel, G., ve Kanlioğlu, A. (2021). Fotoğraf Serüveninin Son Durağı, Mobil Fotoğrafçılık. *Erciyes İletişim Dergisi*, *2*, 81-100. https://doi.org/10.17680/erciyesiletisim.973527

Goel, A., & Corbett, P. (2012). RAID triple parity. *ACM SIGOPS Operating Systems Review*, *46*(3), 41-49. https://doi.org/10.1145/2421648.2421655

Gül, M. (2018). *Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler*. [Yayınlanmamış Yüksek Lisans Tezi] Milli Savunma Üniversitesi, Hazerfan Havacılık ve Uzay Teknolojileri Estsitüsü.

Hart, N. (2002). Method, disaster recovery record, back-up apparatus and raid array controller for use in restoring a configuration of a raid device, US Patent App. 10/152,340

Hausknecht, K., & Gruicic, S. (2017). Anti-computer forensics. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1233-1240. https://doi.org/10.23919/MIPRO.2017.7973612

Hilgert, J.-N., Lambertz, M., & Yang, S. (2018). Forensic analysis of multiple device BTRFS configurations using The Sleuth Kit. *Digital Investigation*, *26*, S21-S29. https://doi.org/10.1016/j.diin.2018.04.020

Kiselev, O., & Colgrove, J.A. (2006). *Automated recovery from data corruption of data volumes in parity raid storage systems*. US Patent 7.

Oğuz, H. (2013). Elektronik ortamda kişisel verilerin korunması, bazı ülke uygulamaları ve ülkemizdeki durum. *Uyuşmazlık Mahkemesi Dergisi*, 0 (3), 1-38.

Patterson, D. A., Gibson, G., & Katz, R. H. (1988). A case for redundant arrays of inexpensive disks (Raid). *Proceedings of the 1988 ACM SIGMOD International Conference on Management of Data - SIGMOD '88*, 109-116. https://doi.org/10.1145/50202.50214

Reinsel, D., Gantz, J., & Rydning, J. (2018). *The digitization of the world from edge to core. Framingham: International Data Corporation.*

Sammes, A. J., & Jenkinson, B. (2007). *Forensic computing* (2nd ed). Springer.

Standart Olmayan RAID Seviyeleri (t.y.). Non-standard RAID levels. https://en-academic.com/dic.nsf/enwiki/4462635

Stott, D. (1998). Understanding RAID. *PC Network Advisor*. 95, 17-20.

Wayne, W. (2015). Web User. 372, 58-61.

Xiang, L., Xu, Y., Lui, J. C. S., Chang, Q., Pan, Y., & Li, R. (2011). A hybrid approach to failed disk recovery using raid-6 codes: Algorithms and performance evaluation. *ACM Transactions on Storage*, *7*(3), 11:1-11:34. https://doi.org/10.1145/2027066.2027071

Zoubek, C., Seufert, S., & Dewald, A. (2016). Generic RAID reassembly using block-level entropy. *Digital Investigation*, *16*, S44-S54. https://doi.org/10.1016/j.diin.2016.01.007