

*Uzmanlık Tezleri Serisi No: 181*

# REKABET KURUMU

## YERİNDE İNCELEMELERİN WINDOWS CANLI SİSTEMLER ÜZERİNDE GERÇEKLEŞTİRİLMESİ

*ALİ OZAN*

# **YERİNDE İNCELEMELERİN WINDOWS CANLI SİSTEMLER ÜZERİNDE GERÇEKLEŞTİRİLMESİ**

*Ali OZAN*

Ağustos 2020

©Bu eserin tüm telif hakları  
Rekabet Kurumuna aittir. 2020

Baskı, Ağustos 2020  
Rekabet Kurumu-ANKARA

Bu kitapta öne sürülen fikirler eserin yazarına aittir;  
Rekabet Kurumunun görüşlerini yansıtmaz.

Bu tez, Rekabet Kurumu Başkan Yardımcısı Abdulgani GÜNGÖRDÜ, Rekabet Kurumu Başkan Yardımcısı Kürşat ÜNLÜSOY, Bilgi Yönetimi Dairesi Başkanı Haluk Recai BOSTAN, Prof. Dr. Mahmut YAVAŞI ve Doç. Dr. Fatih Cemil ÖZBUĞDAY'dan oluşan Tez Değerlendirme Heyeti tarafından 30 Eylül 2019 tarihinde yürütülen Tez Savunma Toplantısı sonucunda yeterli ve başarılı kabul edilmiştir.

Tez yazarı Ali OZAN, 24.01.2020 tarihinde yapılan Yeterlik Sınavında başarılı olmuş ve Başkanlık Makamının 06.02.2020 tarih ve 2252 sayılı onayı ile Rekabet Uzmanı olarak atanmıştır.

YAYIN NO

364

## İÇİNDEKİLER

|                  |    |
|------------------|----|
| KISALTMALAR..... | vi |
|------------------|----|

|             |   |
|-------------|---|
| GİRİŞ ..... | 1 |
|-------------|---|

### BÖLÜM I ADLI BİLİŞİM VE YERİNDE İNCELEME

|                                             |    |
|---------------------------------------------|----|
| 1.1. ADLİ BİLİŞİM.....                      | 3  |
| 1.2. CANLI SİSTEMLERDE İNCELEME .....       | 4  |
| 1.3. YERİNDE İNCELEMELERE GENEL BAKIŞ ..... | 5  |
| 1.4. İNCELEME SÜREÇ MODELLERİ.....          | 6  |
| 1.4.1. Hazırlık.....                        | 7  |
| 1.4.2. Kontrol ve Koruma.....               | 9  |
| 1.4.3. İnceleme ve Analiz .....             | 10 |
| 1.4.4. Elde Etme .....                      | 11 |
| 1.4.5. Sunum.....                           | 11 |
| 1.5. TEŞEBBÜS BİLİŞİM SİSTEMLERİ.....       | 11 |

### BÖLÜM II SUNUCU SİSTEMLERİ

|                                             |    |
|---------------------------------------------|----|
| 2.1. SUNUCU SANALLAŞTIRMA YAZILIMLARI ..... | 14 |
| 2.2. ACTIVE DIRECTORY .....                 | 15 |
| 2.3. DNS VE DHCP .....                      | 17 |
| 2.4. EXCHANGE E-POSTA SUNUCUSU.....         | 19 |
| 2.5. DOSYA SUNUCUSU .....                   | 26 |
| 2.6. UZAK MASAÜSTÜ YAZILIMLARI .....        | 29 |
| 2.7. GÜNLÜKLER.....                         | 31 |
| 2.8. YEDEKLEME VE KURTARMA ÇÖZÜMLERİ.....   | 36 |
| 2.9. VERİ KAYBI ÖNLEME ÇÖZÜMLERİ .....      | 38 |



---

|                                                          |    |
|----------------------------------------------------------|----|
| 2.10. SEKTÖREL VE YEREL YAZILIMLAR VE VERİTABANLARI..... | 40 |
|----------------------------------------------------------|----|

### **BÖLÜM III**

#### **KULLANICI BİLGİSAYARLARI**

|                                               |    |
|-----------------------------------------------|----|
| 3.1. WINDOWS ARAMA.....                       | 43 |
| 3.2. E-POSTA VERİLERİ .....                   | 48 |
| 3.3. TARAYICI VERİLERİ .....                  | 51 |
| 3.4. SOSYAL MEDYA VE SOHBET UYGULAMALARI..... | 57 |
| 3.5. BULUT DEPOLAMA UYGULAMALARI .....        | 59 |
| 3.6. WINDOWS KAYIT DEFTERİ.....               | 62 |
| 3.7. ATLAMA LİSTELERİ.....                    | 64 |
| 3.8. UÇUCU VERİLER .....                      | 65 |
| 3.9. SİLİNER VERİLER.....                     | 65 |
| 3.10. DOSYA ÜST VERİ BİLGİLERİ .....          | 66 |

### **BÖLÜM IV**

#### **Yİ'NİN SON AŞAMALARI, DİĞER HUSUSLAR VE Yİ AKIŞ ŞEMASI ÖNERİSİ**

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| 4.1. ELDE ETME.....                                                         | 68 |
| 4.1.1. Delillere El Koyma Yöntemleri.....                                   | 68 |
| 4.1.2. Hash Alma .....                                                      | 70 |
| 4.1.3. Şifreleme Ve Taşıma.....                                             | 73 |
| 4.2. SUNUM.....                                                             | 74 |
| 4.3. ADLİ BİLİŞİM YAZILIMLARI İLE İNCELEME .....                            | 74 |
| 4.4. DİĞER ÜLKE UYGULAMALARI .....                                          | 81 |
| 4.5. Yİ AKIŞ ŞEMASI ÖNERİLERİ.....                                          | 82 |
| 4.5.1. Hazırlık Aşaması Akış Şeması .....                                   | 83 |
| 4.5.2. Sunucu Sistemlerinde Kontrol ve Koruma Aşaması Akış Şeması .....     | 84 |
| 4.5.3. Kullanıcı Bilgisayarlarında Kontrol ve Koruma Aşaması Akış Şeması .. | 86 |
| 4.5.4. Sunucu Sistemlerinde İnceleme ve Analiz Aşaması Akış Şeması.....     | 88 |

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| 4.5.5. Kullanıcı Bilgisayarlarında İnceleme ve Analiz Aşaması Akış Şeması ....               | 90 |
| 4.5.6. Elde Etme Aşaması Akış Şeması.....                                                    | 91 |
| 4.5.7. Sunum Aşaması Akış Şeması .....                                                       | 93 |
| <b>SONUÇ</b> .....                                                                           | 94 |
| <b>ABSTRACT</b> .....                                                                        | 95 |
| <b>KAYNAKÇA</b> .....                                                                        | 96 |
| <b>ŞEKİL DİZİNİ</b>                                                                          |    |
| Şekil 1 : OSINT araçları ile kişi adı üzerinden OSINT yapılması.....                         | 9  |
| Şekil 2 : 2016 yılı teşebbüslerin sunucu sanallaştırma yazılımı kullanma oranı ..            | 14 |
| Şekil 3 : Microsoft Hyper-V yazılımı ara yüzü .....                                          | 15 |
| Şekil 4 : AD'deki kullanıcıları ve grupları görüntüleme ekranı .....                         | 17 |
| Şekil 5 : DNS Yönetim Panelinden bilgisayarlara atanmış IP'lerin<br>görüntülenmesi .....     | 18 |
| Şekil 6 : DHCP ara yüzünden IP alan bilgisayarlar .....                                      | 19 |
| Şekil 7 : Exchange Yönetim Merkezi .....                                                     | 20 |
| Şekil 8 : E-posta kutusu özellikleri ekranı .....                                            | 23 |
| Şekil 9 : Yerinde e-Keşif ile e-posta kutularında arama (Elfassy 2013, 479) .....            | 24 |
| Şekil 10 : EAC “delivery reports” ekranı .....                                               | 24 |
| Şekil 11 : Exchange e-posta kutusu seçenekleri .....                                         | 25 |
| Şekil 12 : Dosya sunucusundaki dosyaların ağ üzerinden görüntülenmesi .....                  | 26 |
| Şekil 13 : Dosya sunucusunda paylaşılan dosyaların görüntülenmesi .....                      | 27 |
| Şekil 14 : Dosya sunucusundaki bir belgeye erişim izinleri .....                             | 27 |
| Şekil 15 : Dizin oluşturma seçenekleri ve izin oluşturma konumları<br>pencereleri .....      | 28 |
| Şekil 16 : Windows Arama Servisi'nin açılması .....                                          | 28 |
| Şekil 17 : Bağlantı öncesi TightVNC yazılım logosunun bildirim alanındaki<br>görünümü.....   | 30 |
| Şekil 18 : Bağlantı sonrası TightVNC yazılımı logosunun bildirim alanındaki<br>görünümü..... | 30 |
| Şekil 19 : Bağlantı sonrası ilgili yazılımın günlük kayıtları .....                          | 30 |
| Şekil 20 : Bağlantı sonrası Windows günlüklerine düşen kayıt.....                            | 31 |
| Şekil 21 : Olay Görüntüleyicisi yazılımı ara yüzü.....                                       | 32 |

|          |                                                                                                                                  |    |
|----------|----------------------------------------------------------------------------------------------------------------------------------|----|
| Şekil 22 | : Log Parser Studio Uygulaması.....                                                                                              | 33 |
| Şekil 23 | : Grup Politikası Yönetim aracından yeni bir nesne oluşturma .....                                                               | 35 |
| Şekil 24 | : Grup politikası nesnesinden erişim denetim kayıtlarının açılması..                                                             | 36 |
| Şekil 25 | : Herkes (Everyone) grubunun denetim girişlerine eklenmesi .....                                                                 | 36 |
| Şekil 26 | : Commvault'un Exchange E-Posta Kutusu yedekleme ve<br>kurtarma seçenekleri .....                                                | 37 |
| Şekil 27 | : Commvault ile e-posta kutusu kurtarma işlemi .....                                                                             | 38 |
| Şekil 28 | : Exchange Yönetim Paneli ara yüzünde tanımlanmış DLP politikaları ..                                                            | 39 |
| Şekil 29 | : IIS sunucu ara yüzünden site yazılım klasörüne erişim .....                                                                    | 42 |
| Şekil 30 | : Dizin oluşturma seçenekleri ekranı .....                                                                                       | 45 |
| Şekil 31 | : Dizin oluşturma seçeneklerinden erişilen “Dizine Eklenen<br>Konumlar” ve “Dosya Türleri” ekranları .....                       | 46 |
| Şekil 32 | : Outlook'ta silinmiş öğeleri kurtarma.....                                                                                      | 49 |
| Şekil 33 | : Outlook'un çevrimdışı çalışma moduna alınması .....                                                                            | 49 |
| Şekil 34 | : Outlook'ta “Dizin Oluşturma Seçenekleri” ve “Dizine Eklenen<br>Konumlar” Ekranları .....                                       | 50 |
| Şekil 35 | : Chrome'da otomatik doldurma verileri .....                                                                                     | 53 |
| Şekil 36 | : Chrome'da otomatik doldurma için kayıtlı şifrelerin görüntülenmesi ...                                                         | 53 |
| Şekil 37 | : Chrome'da çerezler ekranı .....                                                                                                | 54 |
| Şekil 38 | : Chrome'da tüm çerezler ve site verileri ekranı .....                                                                           | 54 |
| Şekil 39 | : Chrome'da çerez verilerinin okunması .....                                                                                     | 55 |
| Şekil 40 | : Chrome'da menü seçenekleri .....                                                                                               | 55 |
| Şekil 41 | : Chrome'da tahmin hizmeti verilerinin görüntülenmesi .....                                                                      | 56 |
| Şekil 42 | : Google Drive yazılımı ara yüzü .....                                                                                           | 60 |
| Şekil 43 | : Dropbox yazılımı ara yüzü .....                                                                                                | 60 |
| Şekil 44 | : Windows Kayıt Defterinin bilgisayarda yüklü bulunan bir yazılım<br>(TightVNC) hakkında içerdiği veriler .....                  | 63 |
| Şekil 45 | : Windows Kayıt Defterinde aktif kullanıcıya ait bazı kayıtlar .....                                                             | 63 |
| Şekil 46 | : Farklı Windows uygulamalarına ilişkin Atlama Listesi örnekleri<br>(kısa yollar üzerine fare (mouse) ile sağ tıklanmıştır)..... | 64 |
| Şekil 47 | : Bir belgenin üst veri bilgileri.....                                                                                           | 66 |
| Şekil 48 | : CertUtil aracı ile hash alma .....                                                                                             | 71 |
| Şekil 49 | : Powershell ile hash alma .....                                                                                                 | 72 |
| Şekil 50 | : HashMyFiles yazılımı ile hash alma .....                                                                                       | 72 |

|          |                                                                                                                                                              |    |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Şekil 51 | : BitLocker ile sürücü şifreleme sırasında parola belirlenmesi .....                                                                                         | 73 |
| Şekil 52 | : USB bellek üzerinden çalıştırılan EaseUS Data Recovery yazılımı ile silinmiş öğelerin kurtarılması.....                                                    | 76 |
| Şekil 53 | : USB bellek üzerinden çalıştırılan Nirsoft LastActivityView yazılımı ile bilgisayarda gerçekleştirilen son işlemlerin görüntülenmesi.....                   | 76 |
| Şekil 54 | : USB bellek üzerinden çalıştırılan MiTec İnternet History Browser yazılımı ile bilgisayarda kullanılan tüm tarayıcıların geçmişlerinin görüntülenmesi ..... | 77 |
| Şekil 55 | : USB bellek üzerinden çalıştırılan NirSoft MyLastSearch yazılımı ile tarayıcılarda arama motorlarından yapılan son aramaların görüntülenmesi .....          | 77 |
| Şekil 56 | : Belkasoft Live RAM Capturer Yazılımı ile Bellek İmajı Alma .....                                                                                           | 78 |
| Şekil 57 | : Volatility ile bellek imajı inceleme.....                                                                                                                  | 78 |
| Şekil 58 | : Encase Portable Collector yazılımı .....                                                                                                                   | 79 |
| Şekil 59 | : Harvester Portable Edition yazılımı .....                                                                                                                  | 80 |
| Şekil 60 | : Nuix Portable Collector yazılımı.....                                                                                                                      | 80 |

## **TABLO DİZİNİ**

|         |                                                                                |    |
|---------|--------------------------------------------------------------------------------|----|
| Tablo 1 | : Windows Aramada kullanılacak parametreler.....                               | 47 |
| Tablo 2 | : Outlook'ta arama ifadelerinin kullanımı .....                                | 50 |
| Tablo 3 | : Tarayıcıların kayıt konumları (Akbal vd. 2016, 633).....                     | 52 |
| Tablo 4 | : Sosyal medya delillerinin potansiyel konumları (Cusack ve Son 2012, 34)..... | 57 |
| Tablo 5 | : Facebook “messages.db” veri tabanı (Majeed vd. 2016, 76) .....               | 58 |
| Tablo 6 | : Skype “main.db” veri tabanı (Majeed vd. 2016, 77).....                       | 59 |

## KISALTMALAR

|              |                                                       |
|--------------|-------------------------------------------------------|
| <b>Bkz.</b>  | : Bakınız                                             |
| <b>vb.</b>   | : ve benzeri                                          |
| <b>vd.</b>   | : ve diğer                                            |
| <b>Kurum</b> | : Rekabet Kurumu                                      |
| <b>Kurul</b> | : Rekabet Kurulu                                      |
| <b>RAM</b>   | : Rastgele Erişilebilir Bellek (Random Access Memory) |
| <b>USB</b>   | : Universal Serial Bus                                |
| <b>Yİ</b>    | : Yerinde inceleme                                    |
| <b>DVD</b>   | : Digital Versatile Disc                              |
| <b>OSINT</b> | : Open Source Intelligence                            |
| <b>DS</b>    | : Directory Services                                  |
| <b>AD</b>    | : Active Directory                                    |
| <b>DNS</b>   | : Domain Name System                                  |
| <b>DHCP</b>  | : Dynamic Host Configuration Protocol                 |
| <b>EAC</b>   | : Exchange Admin Center                               |
| <b>RBAC</b>  | : Role Based Access Control                           |
| <b>DLP</b>   | : Data Loss Prevention                                |
| <b>RDS</b>   | : Remote Desktop Services                             |
| <b>RDP</b>   | : Remote Desktop Protocol                             |
| <b>VNC</b>   | : Virtual Network Computing                           |
| <b>IIS</b>   | : Internet Information Services                       |
| <b>IP</b>    | : Internet Protocol                                   |
| <b>SD</b>    | : Secure Memory                                       |
| <b>API</b>   | : Application Programming Interface                   |
| <b>SQL</b>   | : Structured Query Language                           |
| <b>VM</b>    | : Virtual Machines                                    |
| <b>NTFS</b>  | : New Technology File System                          |
| <b>MD5</b>   | : Message-Digest 5                                    |
| <b>SHA1</b>  | : Secure Hash Algorithm 1                             |

## GİRİŞ

Teknoloji günden güne gelişmekte, buna bağlı olarak elektronik cihazlar çalışma hayatının vazgeçilmez bir parçası haline gelmektedir. Bu durum bilgiyi toplamak, düzenlemek ve saklamak gibi amaçlar için kullanılan bilişim sistemlerini büyük veri yığınlarına dönüştürmektedir. Bu yığınlar içerisinde bir konuya ilişkin bilgi aramak ve bilgiyi ortaya çıkarmak, zaman zaman ihtiyaç duyulan bir iş olarak karşımıza çıkmaktadır.

Rekabet Kurumu (Kurum), yerinde inceleme (Yİ) yetkisini, rekabet ihlallerinin ortaya çıkarılmasında en büyük araç olarak kullanmaktadır. 4054 sayılı Kanun'un<sup>1</sup> 15. maddesinde tanımlanan söz konusu yetki ile teşebbüs ve teşebbüs birliklerinde (bundan sonra teşebbüs olarak anılacaktır) incelemeler yapılmakta, bu esnada her türlü belge incelenerek bir rekabet ihlaliyle ilişkili olduğu düşünülen belgelerin kopyası alınmaktadır. Alınan bu belgeler ise Rekabet Kurulu (Kurul) kararlarında birincil delil kaynağı olarak kullanılmaktadır.

Bilişim sistemlerinde gerçekleştirilen adli bilişim incelemeleri genellikle bir süreç modeli içerisinde ele alınmakta ve bir plana bağlı kalınarak yapılmaktadır. Yİ'lerin de bir modele bağlı kalınarak ve tüm aşamalarının bir plana uyularak dikkatle yapılması, ele geçirilecek delilin miktarına ve niteliğine doğrudan yansımaktadır. Yİ'lerin etkinliğinin artırılması ise Kurul kararlarının da etkinliğinin artırılması anlamına gelmektedir.

Bu bağlamda dört bölümden oluşan çalışmanın birinci bölümünde adli bilişim kavramı anlatılmakta, ardından Yİ'lerin etkinliği sorgulanmakta ve eksik yönlerine değinilmektedir. Daha sonra inceleme süreç modelleri ele alınmakta ve

---

<sup>1</sup> 4054 sayılı kanuna erişmek için bkz. <https://www.rekabet.gov.tr/tr/Sayfa/Mevzuat/4054-sayili-kanun> Erişim Tarihi: 10.10.2018

Yİ’lerde karşımıza çıkan teşebbüs bilişim sistemlerinden bahsedilmektedir.

İkinci bölümde Yİ sırasında teşebbüslerde karşılaşılması muhtemel sunucu sistemleri anlatılmakta ve bu sistemlerin incelenmesi ile ilgili detaylara yer verilmektedir.

Üçüncü bölümde Yİ’lerin kullanıcı bilgisayarları üzerinde gerçekleştirilen kısmı irdelenmektedir. Bu bölümde, kullanıcı bilgisayarlarındaki delil kaynakları ortaya koyulmakta ve bu kaynakları inceleme yöntemlerine yer verilmektedir.

Son bölümde ise delillere el koyma yöntemlerine ve el koyulan delillerin uygun şekilde alınıp taşınması ile ilgili hususlara yer verilmektedir. Bölümde, Yİ’lerde adli bilişim yazılımlarının kullanılmasına dair bir takım öneriler ve örnekler de yer almaktadır. Diğer ülke uygulamalarının anlatılmasının ardından, son olarak Yİ süreçlerine dair akış şemaları ortaya koyulmaktadır.

## BÖLÜM 1

### ADLİ BİLİŞİM VE YERİNDE İNCELEME

Teknolojinin hızla ilerlemesi ve buna bağlı olarak gelişen bilişim sistemleri ile işlenen suçlar ve ihlaller artmıştır. Bu durum bilişim sistemlerindeki incelemeleri daha önemli hale getirmektedir. Bu incelemeler çeşitli şekillerde gerçekleştirilebilmektedir.

Çalışmanın bu bölümünde adli bilişim kavramı anlatılmakta, canlı adli bilişim veya canlı sistemlerde inceleme olarak adlandırılan inceleme yönteminden bahsedilmektedir. Ardından Yİ'ler irdelenmekte, elektronik kaynaklarda inceleme süreç modelleri hakkında bilgi verilmekte ve Yİ'lerde karşılaşılan teşebbüs bilişim sistemlerine değinilmektedir.

#### 1.1. ADLİ BİLİŞİM

Adli bilişim kavramı, elektronik kaynaklardaki delilleri toplama, koruma, analiz etme ve sunma olarak tanımlanmaktadır (Dezfouli vd. 2014, 48). Dolayısıyla adli bilişim genel olarak, bilişim sistemlerinde inceleme yapılarak elde edilen ve delil niteliği taşıyan verilerin sunulmasıdır.

Bilişim sistemlerinde gerçekleştirilen her inceleme aynı yetkilerden güç alarak veya aynı amaçları güderek yapılmamakta ve incelemelerde her zaman aynı imkânlar sahip olunmamaktadır. Bu durum bilişim sistemlerinde gerçekleştirilen söz konusu incelemelerin farklı şekillerde yapılmasına yol açmaktadır. İncelemelerde kullanılan araçlardan, inceleme süreç modellerine ve izlenen yöntemlere kadar birçok adımda çeşitlilikler meydana gelmektedir.

Elektronik kaynaklardaki incelemeler statik (ölü) veya canlı inceleme



tekniklerini içerebilmektedir (Carrier 2006, 58). Statik incelemede bilgisayardaki disklerin kopyası alındıktan sonra sistem kapatılırken, canlı sistemlerde yapılan incelemede, sistem çalışırken çeşitli yöntemlerle ve yazılımlarla veriler alınmakta, analiz edilmekte ve sunulmaktadır (Rafique ve Khan 2013, 1048). Gelenekçi adli bilişim uzmanları, bilgisayar sistemlerindeki delillerde oluşabilecek bozulmaları veya değişiklikleri engellemek için sistemin kapatılıp incelenmesi hususunda görüş birliği içerisinde (Reyes vd. 2007, 90). Ağırlıklı olarak statik inceleme metodlarını içeren incelemeler, geleneksel adli bilişim incelemeleri olarak ifade edilmektedir.

Günümüz teknolojisinde, bilişim sistemleri karmaşık ve/veya çok büyük yapılardan oluşabilmektedir. Dolayısıyla tüm sistemin kapatılarak incelenmesi bazen uygun bazen de mümkün olmamaktadır. Ayrıca sistemde, sistem kapalıyken elde edilemeyen ancak incelemenin gidişatını değiştirebilecek nitelikte değerli veriler de bulunabilmektedir.

## 1.2. CANLI SİSTEMLERDE İNCELEME

Canlı adli bilişim, canlı analiz, canlı inceleme ya da canlı sistemlerde inceleme olarak anılan terim, çalışan bir sistemde inceleme yapılmasını ifade etmektedir. Canlı sistemlerde inceleme, geleneksel adli bilişime nazaran önemli bir takım avantajlara sahipken, bazı dezavantajları da içerisinde barındırmaktadır.

Geleneksel adli bilişimde sistemin kapatılmasıyla ağ bağlantıları kopmakta, şifrelenmiş disklerdeki önemli delillere erişim imkânsızlaşmakta, kritik sistemlerin devre dışı kalma<sup>2</sup> ihtimali ortaya çıkmaktadır (Yingxin vd. 2017). Canlı sistemlerde inceleme ile hafızadaki veriler, devam eden işlemlerin verileri ve hali hazırda şifrelenmemiş durumda olan veriler elde edilebilirken bu verilerin geleneksel adli bilişimde elde edilememesi, canlı sistem incelemelerini, veri tutarlılığını ve bütünlüğünü sağlaması açısından öne çıkarmaktadır (Rafique ve Khan 2013, 1048). Canlı sistemlerde inceleme, uçucu veriler ve sistem durumu gibi kapalı sistemlerden elde edilemeyecek birçok verinin de elde edilmesini

---

<sup>2</sup> Teşebbüs bilişim sisteminde sürekli açık kalması gereken uygulamaların kapatılması sisteme zarar verip sistemi sekteye uğratabilir.

sağlayarak incelemenin verimliliğini artırabilmektedir (Zhang vd. 2010). Ayrıca canlı sistemlerde inceleme sırasında bulut verileri gibi sonradan erişilemeyecek bilgilerin de elde edilmesi mümkün iken, geleneksel adli bilişimde bu imkân her zaman sahip olunamamaktadır.

Her ne kadar canlı sistemlerde inceleme birçok avantaja sahip olsa da geleneksel adli bilişimin sunduğu bazı kolaylıkları da sunamamaktadır. Canlı sistemlerde inceleme sırasında, delillerde meydana gelebilecek bozulmaların ve değişikliklerin telafisi mümkün olmayabilmektedir. Bir verinin geri getirilemeyecek şekilde silinmesi veya veriler üzerine geri dönülemez yazma işlemi yapılması gibi durumlar canlı sistemlerde yapılan inceleme sürecinde karşılaşılabilecek problemler arasındadır. İlgili veriye erişim, veriye el koymadaki süre kısıtı ve inceleme sırasında yapılan işlemlerin bellekte meydana getirdiği değişiklikler de canlı sistem incelemelerinin zorlukları arasında yer almaktadır (Bashir ve Khan 2013, 43).

### **1.3. YERİNDE İNCELEMELERE GENEL BAKIŞ**

Yİ'ler yetki çerçevesinde, teşebbüs mal varlıklarında gerçekleştirilen, yazılı veya elektronik delil bulmak amacıyla yapılan incelemelerdir. Yİ sırasında ele geçirilen deliller, dosya sonucuna (karara) doğrudan etki edebilecek nitelikte olabilmektedir. Yİ'ler birden çok teşebbüste veya aynı teşebbüsün farklı mal varlıklarında gerçekleştirilebilmektedir. Yİ'lerde, inceleme konusuyla ilgili bulunan yazılı veya elektronik belgeler, bir kopyası teşebbüse bırakılarak alınmaktadır.

Yİ'lerde geleneksel adli bilişim yöntemleri kullanılmamaktadır. Yİ'ler, teşebbüs bilişim sistemlerinde, canlı sistem incelemeleri kapsamına girebilecek bir şekilde gerçekleştirilmektedir. Dolayısıyla Yİ'lerde, geleneksel adli bilişim uygulaması olan disklerin veya belleklerin imajını alma<sup>3</sup> yöntemlerine başvurulmamaktadır. İncelenen elektronik verilerden ilgili görülen belgeler ya yazıcıdan çıktı olarak ya da elektronik ortamda alınmaktadır. Bu incelemelerde adli bilişim yazılımları da kullanılmamaktadır.

<sup>3</sup> Bilgisayar sabit diskinin veya belleğinin kopyasının alınması işlemidir.

Canlı sistem incelemesi olarak değerlendirildiğinde, Yİ'lerde ele geçirilen delillerin çoğunlukla e-posta<sup>4</sup> verilerinden oluşması dikkat çekmektedir. Bir canlı sistem incelemesinde, tarayıcı verilerinden, sosyal medya hesaplarından, açık yazılım verilerinden, sunuculardan vb. birçok kaynaktan da önemli deliller elde edilebilir.

Elektronik verilerin çok çeşitli yerlerde ve hassas kaynaklarda yer alması, delil elde etme sürecinde planlamayı gerekli kılmaktadır. Etkin bir planlamanın, bir süreç modeli içerisinde yapılabileceği değerlendirilmektedir.

#### **1.4. İNCELEME SÜREÇ MODELLERİ**

Arnes (2017, 16), adli bilişim inceleme süreçlerini, tanımlama, toplama, inceleme, analiz ve sunum olarak 5 aşamada ele almaktadır. Daniel ve Daniel (2011, 11) bu süreçleri, edinme, koruma, analiz ve sunum olarak 4 aşamada incelemektedir. Sachowski (2018, 19-24) ise birçok süreç modelini bir araya toplayarak ortak bir model önerisi getirmekte ve temel olarak 4 aşamadan (hazırlık, toplama, işleme, sunum) oluşan şu 7 aşamayı önermektedir:

1. Hazırlık: Ekipman ve personel temin etme faaliyetlerini içeren aşamadır.
2. Tanımlama: Olayın tespit edilmesini içeren aşamadır.
3. Toplama: Kabul görmüş teknikleri kullanarak ilgili verilerin toplanması aşamasıdır.
4. Koruma: Delillerin uygun şekilde alınıp delil zincirinin korunması için ortamın oluşturulması aşamasıdır.
5. İnceleme: İstenen veriyi ortaya çıkarmak ve veri hacmini azaltmak için dijital delilleri değerlendirme aşamasıdır.
6. Analiz: Alaka düzeyini belirlemek için elektronik delilin içeriğini inceleme aşamasıdır.
7. Sunum: Rapor dokümanlarının hazırlanması aşamasıdır.

---

<sup>4</sup> Kurul kararları incelendiğinde, Yİ'lerde elde edilen delillerin çoğunlukla e-posta verilerinden oluştuğu görülmektedir. Bkz. 29.08.2013 tarihli ve 13-49/711-300 sayılı; 22.10.2014 tarihli ve 14-42/783-346 sayılı; 23.02.2017 tarihli ve 17-08/99-42 sayılı; 22.11.2018 tarihli ve 18-44/703-345 sayılı; 19.09.2018 tarihli ve 18-33/556-274 sayılı Kurul kararları

Adli bilişim incelemelerinde önerilen süreç modelleri incelendiğinde ve Yİ'lerin gerçekleştirilme biçimi göz önüne alındığında, birçok açıdan Yİ'lerin adli bilişim süreçleriyle farklılıklar gösterdiği görülmektedir. Örneğin, Yİ'ler için ekipman temini önemli bir adım değildir. Çünkü Yİ'lerde adli bilişim araçları kullanılmamaktadır. Yİ'ler şikayet üzere ya da resen gerçekleştirilebilmektedir. Tanımlama aşaması, Yİ süreçleri içerisinde yer almamaktadır. Çünkü Yİ'ler yetki çerçevesinde ve önceden tanımlanmış bir konu kapsamında gerçekleştirilmektedir. Yİ sürecinde, kontrol ve koruma, inceleme ve analiz ile toplama adımları içiçe geçebilmektedir. Çünkü Yİ sırasında bulunan belgeler, incelemeyi gerçekleştiren uzman tarafından yerinde incelenerek analiz edilmekte ve toplanmaktadır. Bu gibi gerekçelerle, Yİ'lerin adli bilişim süreçlerinden oldukça farklılık gösterdiği anlaşılmaktadır. Yİ'ler temel olarak beş aşamalı bir süreç içerisinde ele alınabilir. Bunlar;

- hazırlık,
- kontrol ve koruma,
- inceleme ve analiz,
- elde etme,
- sunum

aşamalarıdır.

#### **1.4.1. Hazırlık**

Doğru planlama yapmak, bir incelemenin düşük performans ile yapılmasını veya standart altı sonuçları olmasını engeller, verimli ve etkili bir sonuç için ise ön koşuldur (Arnes 2017, 18). İnceleme öncesi hazırlık, Yİ'nin etkin bir şekilde gerçekleştirilmesine katkı yapabilecek önemli bazı adımları içerebilmektedir. Yİ'de görevli uzmanlar arası toplantılar, Yİ gerçekleştirilecek teşebbüsler hakkındaki araştırmalar, Yİ sırasında ihtiyaç duyulabilecek teknik bilginin edinilmesi ve Yİ sırasında uzmanların teşebbüste dağılımlarının planlanması gibi adımlar bu kapsamda değerlendirilebilir.

Yİ sırasında çok geniş bir veri yığını ile karşılaşılabilir. Yapılacak filtrelemeler bu yığında ciddi oranda bir azalma sağlayıp incelemeyi kolaylaştırabilir. Sunucularda ve kullanıcı bilgisayarlarında yapılacak incelemede filtreleme yapabilmek için ise konuya ve sektöre hâkimiyet gerekmektedir. Hazırlık aşamasında yapılacak toplantılarla inceleme görevindeki tüm uzmanların sektör hakkındaki (sektörel kavramlar, finansal büyüklükler, kişiler, şirketler, kuruluşlar vb.) bilgi eksikliği giderilebilir.

Yİ öncesinde yapılacak araştırmalar ile Yİ sırasında yarar sağlayabilecek bazı bilgilere de ulaşılabilir. Bunun için Açık Kaynak İstihbarat (Open Source Intelligence - OSINT) yapılabilir. Chauhan ve Panda (2015, 16), OSINT'i halka açık bir şekilde var olan kaynaklardan toplanan istihbarat olarak tanımlamakta ve OSINT'in, diğer istihbarat toplama yöntemlerinin çoğunun aksine, gizli olan bilgileri kullanmadığını vurgulamaktadır.

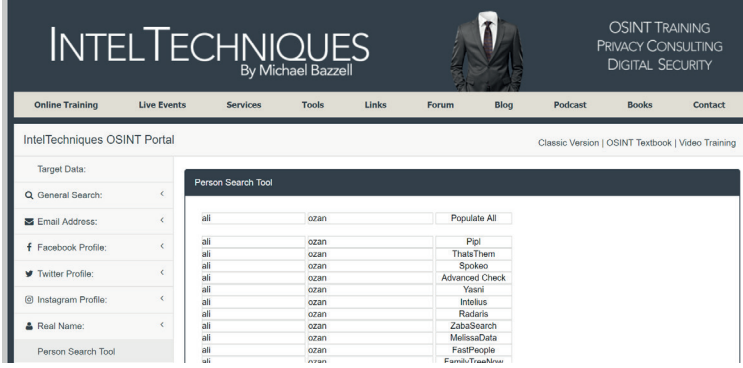
Waddell (2017, 2), OSINT ile şu verilerin elde edilebileceğini belirtmektedir:

- Gerçek isimler, adresler, doğum tarihleri, telefon numaraları, istihdam verileri;
- Müşteri ve tedarikçi adları;
- Takma adlar, kullanıcı adları, şifreler, hesap numaraları;
- Dâhili notlar, toplantı tutanakları, hassas belgeler, elektronik tablolar, bültenler, kimlik belgeleri;
- Coğrafi faaliyet yerleri ve mevcudiyetler;
- Rakip stratejileri ve envanterleri;
- İlgili ek adlar, adresler ve ortaklar;
- Önceki satışlar ve önbellemenmiş web etkinliği;
- Etki alanları, e-postalar ve web siteleri;
- Sosyal medya içerikleridir.

OSINT yapmak için çeşitli uygulamalar bulunmaktadır. Hem masaüstü uygulamalar hem de web uygulamaları (Bkz. Şekil 1) bu kapsamda kullanılmaktadır<sup>5</sup>.

---

<sup>5</sup> Diğer OSINT araçları için bkz. <https://inteltechniques.com/menu.html> Erişim Tarihi: 13.01.2019



**Şekil 1:** OSINT araçları ile kişi adı üzerinden OSINT yapılması

Yİ öncesinde teşebbüs çalışanlarına ait sosyal medya hesapları, web siteleri, şahsi e-posta adresleri<sup>6</sup>, telefon numaraları vb. bilgiler halka açık verilerden tespit edilebilir. Bu veriler, Yİ sırasında aramalarda kullanılacak anahtar kelimelerin ve hangi veri kaynaklarına (web tarayıcıları, e-postalar, dokümanlar vb.) yoğunlaşılacağıının belirlenmesinde yardımcı olabilir.

#### 1.4.2. Kontrol ve Koruma

Yİ'lerin genelde bir veya bir kaç günlük incelemeler olması ve çok kullanıcıli bilişim sistemlerinde gerçekleştirilebilmesi, kısa zamanda büyük miktarda elektronik veri üzerinde kontrol ve koruma ortamının sağlanması ihtiyacını ortaya çıkarmaktadır. Çoğu kez tüm kullanıcıların bilgisayarları üzerinde kontrolün sağlanması mümkün olmamaktadır. Dolayısıyla merkezi bir yaklaşıma ihtiyaç duyulmaktadır.

Yİ uzmanı, sistemi tamamen anlamak, olası delilleri doğru bir şekilde ele almak, böylece değerli bilgileri kaybetmemek ve ilgili delilleri gözden kaçırmamak için sorumlu kişilerle görüşerek olayın koşullarını ve sistemin yapısını anlayabilir. (Shaaban ve Sapronov 2016, 8). Dolayısıyla kontrol ve koruma aşamasında teşebbüs bilişim personelinin verdiği bilgiler işleri hızlandırabilir.

Teşebbüs bilişim sistemi merkezi bir yerden yönetiliyorsa, teşebbüs bilişim personelinin yardımı ile ilk olarak bu kısımlar kontrol altına alınabilir. Sunucu

<sup>6</sup> Teşebbüs çalışanları, işle alakalı yazışmaları teşebbüs bilgisayarlarından şahsi e-posta adresleriyle yapabilmektedir. Dolayısıyla Yİ'lerde şahsi e-posta adreslerinin de incelenmesi gerekebilmektedir.

sistemlerinin kontrol ve koruma altına alınması işlemi, kullanıcıların veri silmelerinin engellenmesi, kaynaklara erişimin ve kullanıcı giriş çıkışlarının kontrol edilmesi, yönetimi sağlayan bilgisayarlar üzerinde izleme mekanizmalarının aktif edilmesi gibi adımları içermektedir.

Kullanıcı bilgisayarlarındaki verilerde meydana gelebilecek silme ve değişikliklere karşı alınacak önlemler ise kullanıcı bilgisayarlarında kontrol ve koruma sağlanması aşamasının adımları olarak değerlendirilebilir. Bilgisayardaki elektronik delillerin korunması aşamasında verilerin güvenliğinin sağlanması için sistem tüm bağlı kablolardan ve aktif wi-fi bağlantılarından izole edilebilmektedir (Boddington 2016, 104).

#### **1.4.3. İnceleme ve Analiz**

Bu aşamada Yİ uzmanı, incelenen bilgisayarlarda inceleme konusu ile ilgili belgeler aramakta ve bulduğu belgeleri analiz ederek delil niteliği taşıyıp taşımadığına karar vermektedir.

Yİ sırasında birçok bilgisayarda inceleme yapılması gerekebilmektedir. Yİ açısından veri tabanları, e-postalar, sunucular ve tarayıcılar gibi birçok değerli veri kaynağı bulunmaktadır. Karşılaşılan büyük miktardaki veri, etkin bir inceleme yapılmasının önünde zorluk teşkil etmektedir. Dolayısıyla veri hacminin güvenli bir şekilde azaltılması için tüm yöntemler göz önünde bulundurulmalıdır (Arnes 2017, 36). İnceleme sırasında verilerin bulunup çıkarılabilmesi için uzmanın yeterli teknik bilgiye ve araştırma yeteneklerine sahip olması önemlidir (Shaaban ve Sapronov 2016, 9).

İnceleme sırasında dikkatle uyulması gereken bir diğer husus ise adli bilişim incelemelerinde de üzerinde önemle durulan delil zincirinin korunmasıdır. Çünkü delil zincirindeki herhangi bir kırılma, delillerin geçerliliği hakkında şüphelere yol açabilmektedir (Daniel ve Daniel 2011, 12). Canlı sistemler üzerindeki inceleme yöntemleri, sisteme müdahale etmemeli ve değiştirmemelidir (Yingxin vd. 2017, 24).

#### 1.4.4. Elde Etme

Elde etme aşaması, veriyi elde etmek için bir plan geliştirmek, veriyi elde etmek ve elde edilen verilerin bütünlüğünü doğrulamak şeklinde üç aşamalı bir süreçtir (Kent vd. 2006, 3-3).

Elde etme adımı, delillerin bütünlüğünü sağlamak için kritik bir öneme sahiptir (Daniel ve Daniel 2011, 12). Elektronik delil elde etme yöntemleri, delillerin bütünlüğünün korunmasını sağlamalı ve gerektiğinde inceleme uzmanının veriler üzerinde değişiklik yapmadığını kanıtlayacak mekanizmaları içermelidir (Shaaban ve Sapronov 2016, 8).

Yİ sonunda alınmasına karar verilen veriler ya yazıcıdan çıktı olarak alınmakta, ya da kriptografik özeti (hash<sup>7</sup>) ile birlikte bir DVD'ye veya USB belleğe yazılarak alınmaktadır. Hash alma işlemi ile verilerin daha sonra bir değişikliğe maruz kalmadığı kanıtlanmaktadır.

#### 1.4.5. Sunum

Yİ sırasında toplanan veriler kuruma getirilmekte ve dosya raportörü uzmanların inisiyatifi ile dosyaya dâhil edilmektedir. Yİ sonunda, veri tabanlarından alınan veriler ile yazılımlara ait günlük verileri gibi okunması ve anlamlandırılması için bazı işlemlere ihtiyaç duyulan veriler bulunabilmektedir. Bu gibi durumlarda verilerin çeşitli yazılımlar aracılığı ile okunması, veri tabanına yüklenerek işlenmesi vb. işlemlerin yapılması gerekebilmektedir.

### 1.5. TEŞEBBÜS BİLİŞİM SİSTEMLERİ

Büyük çaplı teşebbüslerde karşılaşılan bilişim sistemlerinin, genellikle birden çok bilgisayarın bir araya geldiği, bilgisayarlar arası iletişimin ve veri paylaşımının olduğu, çeşitli kontrol mekanizmaları ile ortamdaki bilgisayarların kontrol edilebildiği ağlardan meydana geldiği görülmektedir.

Bir ağdaki kaynakların etkin şekilde kullanılıp, kullanıcıların haberleştirilmesi ve yönetilebilmesi için dizin servisleri (directory services - DS) kullanılmaktadır<sup>8</sup>.

---

<sup>7</sup> Hash alma işlemi, verilerin sonradan bir değişikliğine uğramadığını kanıtlamak için yapılan bir işlemdir. Ayrıntılı bilgiye “4.1.2. Hash Alma” başlığında yer verilmiştir.

<sup>8</sup> <https://docs.oracle.com/cd/E19396-01/817-7619/intro.html> Erişim Tarihi 6.12.2018



Bir dizin (directory) ağdaki nesneler hakkında bilgi depolayan hiyerarşik bir yapıdır<sup>9</sup>. Örneğin Windows<sup>10</sup> <sup>11</sup> işletim sistemi ile kullanılan dizin servisi, Microsoft firmasına ait Active Directory<sup>12</sup> (AD)'dir (Dauti 2017, 14).

AD gibi yapılar sistem yöneticilerine büyük kolaylıklar sağlasa da bazı teşebbüsler bilişim sistemlerinde bu tür yapılar kullanmayabilmektedir. Küçük ölçekli ya da bilişim teknolojileri kullanım ihtiyacı düşük düzeyde olan teşebbüsler AD gibi yapıları kullanma gereksinimi duymayabilmektedir. Bu durumda teşebbüste bilgisayarları kontrol eden merkezi bir sistem bulunmamakta ve ortamdaki bilgisayarlar birbirinden bağımsız olmaktadır.

Teşebbüsün büyüklüğü, çalışan sayısı, faaliyet sektörü vb. birçok etken sunucu sistemlerinde farklılaşmaya yol açabilmektedir. Yİ'lerde birkaç bilgisayarın bulunduğu ve hiçbir sunucuya sahip olmayan teşebbüslerle karşılaşılabilir. Zaman zaman sisteme ait kritik hizmetlerin dışardan hizmet alımı yoluyla yürütüldüğü de görülebilmektedir. Yİ gerçekleştirilen teşebbüsün bilişim sistemi, farklı bir ülkede merkezi bulunan bilişim sisteminin bir parçası da olabilmektedir<sup>13</sup>.

Karşılaşılan bilişim sistemlerinin çeşitliliği sebebiyle çoğu kez sadece belirli bir bilişim alt yapısı üzerine Yİ planlaması yapılması mümkün olamamaktadır. Ancak bilişim sistemlerinde yapılan incelemeleri, temelde sunucu sistemleri ve kullanıcı bilgisayarları olarak ikiye ayırmak mümkündür. Bu doğrultuda, sunucu sistemleri hakkındaki bilgilere ikinci bölümde ve kullanıcı bilgisayarları hakkındaki bilgilere ise üçüncü bölümde yer verilmektedir.

---

<sup>9</sup> <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> Erişim Tarihi: 6.12.2018

<sup>10</sup> Masaüstü platformlarda en çok kullanılan işletim sistemi Windows'tur. Kullanım oranları için bkz. <http://gs.statcounter.com/os-market-share/desktop/worldwide> Erişim Tarihi:23.12.2018.

<sup>11</sup> Bu çalışmada Yİ'lerde en çok karşılaşılan işletim sistemi olan Windows işletim sistemi ve sunucu sistemleri temel alınmıştır.

<sup>12</sup> AD ile ilgili daha geniş bilgiye çalışmanın "2.2. Active Directory" başlığında yer verilmektedir.

<sup>13</sup> Örneğin çok uluslu teşebbüslerde bilişim sisteminin merkezi yurtdışında olabilmektedir.

## BÖLÜM II

### SUNUCU SİSTEMLERİ

Sunucu, diğer yazılımlara (istemciler) belirli bir hizmet türü sağlayan, çeşitli donanımsal gereklilikleri olan bir bilgisayar yazılımıdır (Chauhan ve Panda 2015, 7). İnternet sitelerini sunmak için kullanılan web sunucusu, e-postaları yönetmek için kullanılan e-posta sunucusu, dizin servisi hizmeti için kullanılan sunucular, dosyaları yönetmek için kullanılan dosya sunucusu, yoğun olarak kullanılan sunucu tipleri arasında yer almaktadır.

Sunucuların her yazılım gibi bir bilgisayara kurulmaları ve/veya bir bilgisayar üzerinden çalıştırılmaları gerekmektedir. Birden çok sunucunun tek bir bilgisayara kurulması teknik olarak mümkün ise de, kriz yönetimi, yedekleme, günlüklenme gibi hizmetlerde ortaya çıkacak aksaklıkların tespitinde yaşanabilecek zorluklardan dolayı bu yöntem genellikle tercih edilmemektedir. Bu sebeplerle genellikle her sunucu için ayrı bir bilgisayar kullanılmaktadır.

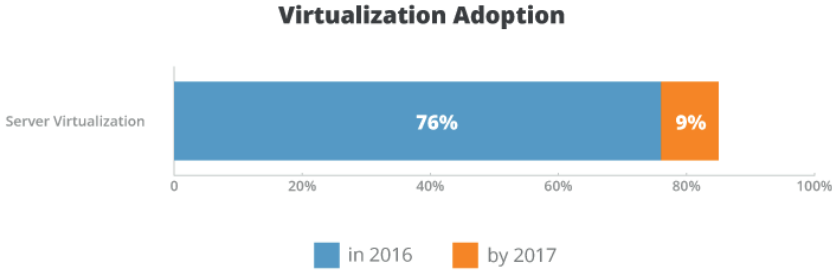
Her bilgisayar ortamı için fiziksel donanım ve yazılım hazırlanıp sistemin yapılandırılması, zaman alıcı, hataya müsait ve yönetilebilir olmaktan uzak olduğu için genellikle teşebbüsler daha efektif bir yöntem olan sunucu sanallaştırma yazılımlarını kullanmaktadır. Bilişim sistemlerinin günümüz dünyasındaki büyük, karmaşık ve sürekli değişen yapısının doğurduğu problemlere, sunucu sanallaştırma yazılımları sahip olduğu esnek yapılandırma ayarlarıyla, neredeyse sınırsız donanımsal limitlerle ve sunduğu diğer kolaylıklarla etkin bir çözüm sunmaktadır (Oguchi ve Yamamoto 2008, 46).

Çalışmanın bu bölümünde ilk olarak sunucu sanallaştırma yazılımları ele alınmaktadır. Ardından yönetim pozisyonundaki sunucuların incelemelerdeki rolüne değinildikten sonra inceleme için önemli delil kaynakları olarak görülen

e-posta ve dosya sunucularından bahsedilmektedir. Uzak masaüstü yazılımları anlatıldıktan sonra çoğunlukla bir izleme mekanizması olarak kullanılan günlüklere yer verilmektedir. Daha sonra sunucularda karşılaşılabilecek yedekleme sistemlerinin incelemelerde kullanımı ile ilgili bilgilere yer verilmektedir. Özellikle son zamanlarda daha sık karşılaşılan veri kaybı önleme çözümlerinin incelemelerdeki rolü de değerlendirildikten sonra son kısımda, yazılımların genel olarak çalışma şekillerinden bahsedilmektedir.

## 2.1. SUNUCU SANALLAŞTIRMA YAZILIMLARI

Bir sanal makine fiziksel bir sistemle aynı görevi gören sanal donanım kaynaklarından, işletim sisteminden ve uygulamalardan oluşan yapıdır (Lim vd. 2012, 151). Sanal makinelere istenilen sunucular kurulabilmekte ve bu sayede görece (fiziki sistemlerden daha geniş) büyük sistemler daha kolay tasarlanabilmektedir. Sunucu sanallaştırma yazılımları ise sanal makinelerin oluşturulabildiği, yönetilebildiği ve silinebildiği bilgisayar yazılımlarıdır. Teşebbüsler gitgide büyük oranda sunucu sanallaştırma yazılımlarından faydalanmaktadır (Bkz. Şekil 2).

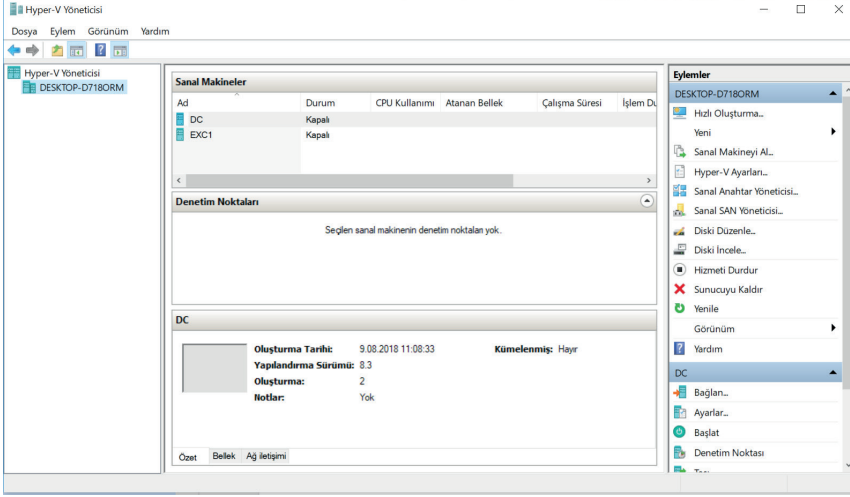


**Şekil 2:** 2016 yılı teşebbüslerin sunucu sanallaştırma yazılımı kullanma oranı<sup>14</sup>

Vmware vSphere, Citrix XenServer, Red Hat Enterprise Virtualization vb. yazılımlar sunucu sanallaştırma yazılımları arasında yer almaktadır. Microsoft

<sup>14</sup> <https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends>  
Erişim Tarihi: 18.01.2019

firmasının geliřtirdiđi Hyper-V Server (Bkz. řekil 3) ise en ok kullanılan sunucu sanallařtırma yazılımları arasındadır.



**řekil 3:** Microsoft Hyper-V yazılımı ara yüzü

Yİ esnasında henüz başlangıta, teřebbüs sistemini tanımak, eđer mevcutsa sunucu sanallařtırma yazılımının yönetim panelini incelemek sistemin yapısı hakkında genel bir fikir verebilmektedir. Yönetim panelinden teřebbüsün oluřturduđu tüm sanal sunucular kontrol edilerek, teřebbüs biliřim personelinin de beyanlarıyla teřebbüsün kullandığı yazılımlar tespit edilebilmektedir. Bu sayede Yİ'ye hangi sistemlerin dâhil edilmesi gerektiđine daha dođru bir řekilde karar verilebilmektedir.

Sunucu sanallařtırma yazılımlarından, AD sunucusu gibi yönetim sunucuları tespit edilerek teřebbüs biliřim sistemini tanımak, kontrol ve koruma ortamı oluřturmak için gerekli olan bilgiler edinilebilmektedir.

## 2.2. ACTIVE DIRECTORY

AD ile organizasyondaki, bilgisayarlar, kullanıcılar, gruplar, yazıcılar, uygulamalar, vb. hizmetler verimli bir řekilde yönetilebilmektedir (Desmond vd. 2013, 1). AD dizin bilgilerini tutmakta, ađdaki kullanıcılar ve yöneticiler

ile paylaşmaktadır<sup>15</sup>. Bu sayede birden çok bilgisayardan oluşan sistemlerde kaynaklara erişim, güvenlik ve yetkilendirme noktasında merkezi bir kontrol sağlanabilmektedir.

Siddaway (2014, 3), AD'nin temel yapı taşlarını şu şekilde belirtmektedir:

- Orman (Forest): AD'nin tamamıdır. Bir veya daha fazla etki alanı içerebilir. Ormandaki tüm etki alanları ortak bir yapılandırmayı paylaşır. Orman, AD için güvenlik sınırır. Çoğu kuruluş sadece tek bir ormana ihtiyaç duyar.
- Etki Alanı (Domain): Etki alanı, kullanıcılar, bilgisayarlar, gruplar vb. nesneler için bir kaptır. Etki alanı, kuruluş içinde bir takım sınırlar sağlar. Örneğin etki alanı yöneticileri, diğer alanlarda izinlere sahip değildir ve oradaki nesneleri etkileyemez. Çoğu kuruluş için yalnızca tek bir etki alanı yeterlidir.
- Organizasyon Birimi (Organizational Unit): Kullanıcı, bilgisayar, grup ve diğer nesneleri tutmak için kullanılabilen ve bir etki alanı içinde yer alan kapsayıcıdır. İdari ayrıcalıklar sağlamak ve grup ilkesi uygulamalarını kontrol etmek gibi etki alanından daha esnek kolaylıklar sağlamaktadır.

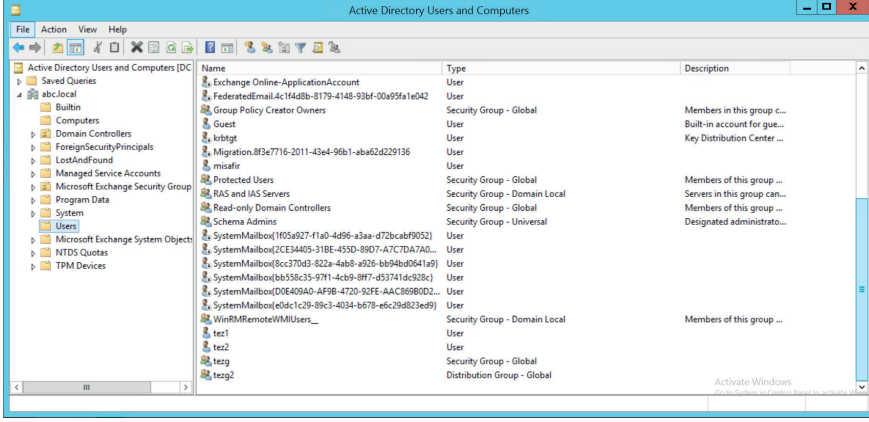
Bir etki alanı çok sayıda organizasyon birimi içerebilmektedir. AD içerisinde kullanıcılar, bilgisayarlar ve gruplar oluşturulabilmekte, bu yapılar ile organizasyon birimleri meydana getirilebilmektedir<sup>16</sup>.

AD içerisinde oluşturulan gruplar, dosyalara erişim yetkisi verilirken, e-posta dağıtım grupları belirlenirken ve AD ile ilişkisi olan diğer yerlerde kullanılabilir. Gruplar, kaynaklara erişim izni için kullanılan güvenlik grupları ve e-posta dağıtımı için kullanılan dağıtım grupları olmak üzere iki çeşittir (Francis 2017, 235). Dosyalara erişim yetkisine sahip kullanıcıları tespit etme ve grup e-postalarını görebilen kullanıcıları belirleme gibi işler için AD ara yüzünden gruplar ve kullanıcılar görüntülenebilir (Bkz. Şekil 4).

---

<sup>15</sup> <https://docs.microsoft.com/tr-tr/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> Erişim Tarihi: 6.12.2018

<sup>16</sup> AD içerisinde, organizasyon birimleri genellikle kullanıcıların teşebbüsteki idari birimleri dikkate alınarak oluşturulmaktadır.



**Şekil 4:** AD'deki kullanıcıları ve grupları görüntüleme ekranı

Krause (2016, 62) AD'nin, kullanıcı adlarını, şifreleri, bilgisayar hesaplarını, bilgisayar gruplarını, sunucuları, sunucu gruplarını ve koleksiyonları, güvenlik politikalarını, dosya çoğaltma hizmetlerini ve daha birçok nesneyi depoladığını ve yönettiğini belirtmektedir. Dolayısıyla AD genel olarak kullanıcıların kaynaklara erişiminde kimlik doğrulama ve yetkilendirme işlemlerinin yönetim servisi olarak kullanılmaktadır. Örneğin, sistemde bir çalışan adına açılan kullanıcı hesapları silinmemiş<sup>17</sup> ise ilgili çalışanın hak ve izinleri de sistemde mevcuttur. Bu bilgiler, belge erişim kayıtlarının, e-posta gruplarının vb. hak ve izinlerin anlamlandırılmasında kullanılabilir.

Bilişim sistemlerinde, kaynaklara erişim ve yetkilendirme görevlerinin yerine getirilmesi için servislere ve istemcilere adres gösteren yapılara da ihtiyaç duyulmaktadır. Bu noktada karşımıza DNS ve DHCP hizmetleri çıkmaktadır.

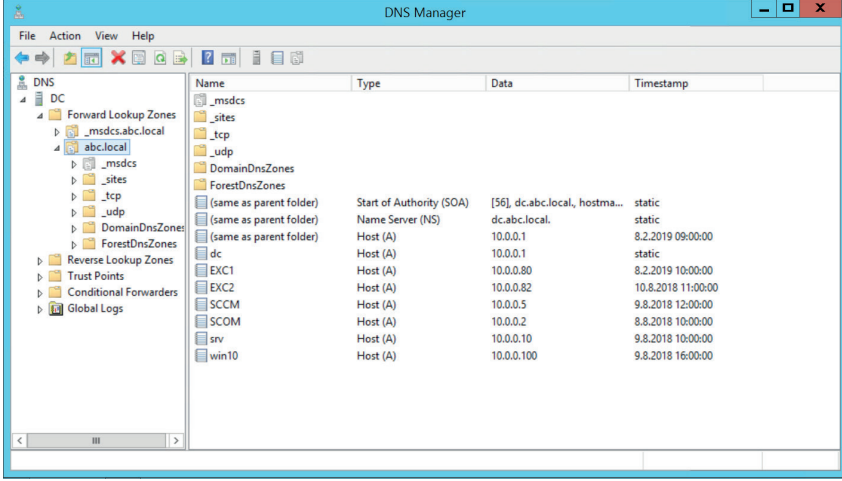
### 2.3. DNS VE DHCP

DNS (Etki Alanı Sistemi - Domain Name System), sunucu ve bilgisayar adlarını IP<sup>18</sup> (Internet Protocol) adreslerine ve IP adreslerini de bilgisayar adlarına çevirir. DNS sunucularındaki özel kayıtları sorgulayarak e-posta sunucularını bulmak, sunucuları adlandırmak, etki alanı sahipliğini doğrulamak vb. işlemleri yerine getirmek mümkün olmaktadır (Thomas 2017, 157).

<sup>17</sup> Hesaplar aktif veya pasif durumda olabilir. Silinmediği sürece hak ve izinler mevcuttur.

<sup>18</sup> IP, ağda bulunan cihazların birbirleri ile iletişim kurması için kullanılan bir adres bilgisidir. Örneğin Rekabet Kurumu web sitesinin (<https://www.rekabet.gov.tr/>) IP adresi 213.14.27.7'dir.

AD de, hizmetleri için DNS'ye güvenir (Siddaway 2014, 205).



**Şekil 5:** DNS Yönetim Panelinden bilgisayarlara atanmış IP'lerin görüntülenmesi

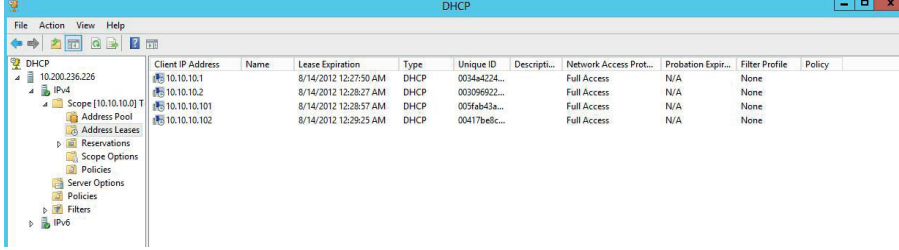
Ortamda hangi sunucuların bulunduğu DNS Yönetim Panelinden (DNS Manager) görüntülenebilmektedir (Bkz. Şekil 5).

Yİ sırasında DNS kayıtları önemli bilgiler sunabilir. Örneğin iki farklı teşebbüsün kurdukları bir web sitesi aracılığı ile rekabet ihlali içeren faaliyetlerde bulunduğu bir durumda (bilgi alışverişi gibi), ilgili web sitesine tahsis edilmiş sunucu, inceleme yapılan teşebbüse ait sunucuların arasında ise bu durum DNS kayıtları yardımı ile tespit edilebilir<sup>19</sup>.

IP adresleri ile ilgili bir başka servis ise DHCP (Dynamic Host Configuration Protocol) servsidir. Kimlikleri doğrulamak ve ağ kaynaklarını kullanmak gibi işlemler için ağa yeni bağlanan her cihaz, ağ adresi ayarlarıyla yapılandırılmaya ihtiyaç duyar (Morimoto vd. 2017, 321). Dolayısıyla bir ağ ortamına sahip bilişim sistemlerinde, bağlı tüm cihazlar için düzgün IP adreslemesi ve ad çözümlemesi gerekmektedir. Bu işlemin tüm cihazlar için yapılması ve yönetilmesi çok zor olacağından, ağda IP adresleme işini otomatik yapan DHCP hizmetleri

<sup>19</sup> Sunucu sanallaştırma yazılımı ara yüzünü incelemek, DHCP kayıtlarına bakmak vb. yöntemler de sunucuları bulmak için kullanılabilecek seçenekler arasındadır.

kullanılmaktadır. Ağa bağlanan cihazlar DHCP servisinin sağladığı IP adresini alırlar.



| Client IP Address | Name | Lease Expiration      | Type | Unique ID    | Descripti... | Network Access Prof... | Probation Expir... | Filter Profile | Policy |
|-------------------|------|-----------------------|------|--------------|--------------|------------------------|--------------------|----------------|--------|
| 10.10.10.1        |      | 8/14/2012 12:27:50 AM | DHCP | 0034a4224... |              | Full Access            | N/A                | None           |        |
| 10.10.10.2        |      | 8/14/2012 12:28:27 AM | DHCP | 003096922... |              | Full Access            | N/A                | None           |        |
| 10.10.10.101      |      | 8/14/2012 12:28:37 AM | DHCP | 005fab43a... |              | Full Access            | N/A                | None           |        |
| 10.10.10.102      |      | 8/14/2012 12:29:25 AM | DHCP | 00417be8c... |              | Full Access            | N/A                | None           |        |

**Şekil 6:** DHCP ara yüzünden IP alan bilgisayarlar<sup>20</sup>

DHCP servisi birçok teknik detaya sahip olsa da önemli olan bilgi, ağa bağlanan tüm cihazların iletişim kurmak için DHCP'den IP adresi alması gerektiği bilgisidir. Herhangi bir kullanıcının gün içinde oturum açıp açmadığı, sunucuların aktif olup olmadığı gibi durumlar, DHCP yönetim panelinden IP adresi alan cihazlara bakılarak tespit edilebilmektedir. DHCP, DNS'den farklı olarak kira süresi (leasing expiration) bilgisini sunmaktadır. Bu kayıtlar bir bilgisayardan gün içinde oturum açılıp açılmadığı bilgisini verebilmektedir.

Bilişim sisteminde yönetim görevini üstlenen ve adresleme işini yerine getiren sunucular belirlendikten sonra, Yİ açısından en önemli veri kaynakları olan e-posta ve dosya sunucuları incelemeye alınabilir.

## 2.4. EXCHANGE E-POSTA SUNUCUSU

E-posta sunucusu, e-postaların toplandığı ve dağıtıldığı bir sunucudur. Kullanıcılar e-posta hesaplarını bir web tarayıcısı üzerinden kullanabildikleri gibi Outlook, Thunderbird gibi e-posta istemcisi olarak adlandırılan bilgisayar yazılımları aracılığı ile de kullanabilmektedirler. Her durumda e-postalar, kullanıcılar tarafından gönderildikten sonra, e-posta sunucularına düşmekte ve buradan gönderilen adrese iletilmektedir. Dolayısıyla e-posta sunucusu, e-postaların yönetimini sağlayan sistem olarak karşımıza çıkmaktadır.

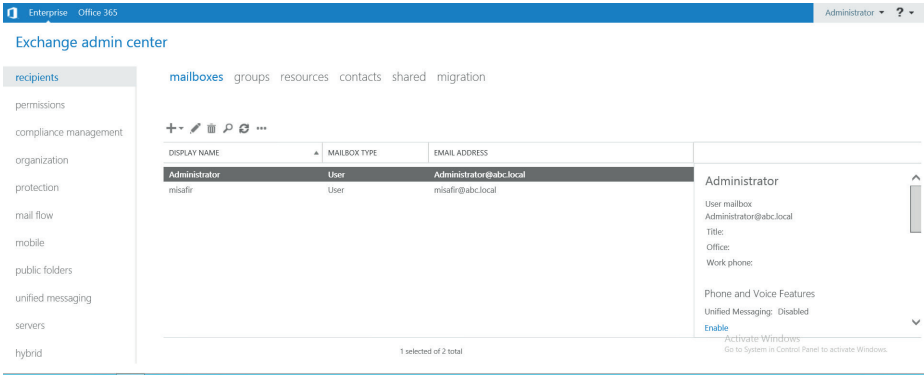
Microsoft Exchange E-Posta Sunucusu, e-posta verilerini depolamak için

<sup>20</sup> <https://blogs.technet.microsoft.com/teamdhcp/2012/08/06/dhcp-failover-load-balance-mode/>  
Erişim Tarihi: 08.02.2019



veri tabanı, e-posta verilerini bir yerden başka bir yere taşımak için taşıma altyapısı ve birkaç farklı yöntemle e-posta verilerine erişmek için erişim noktaları sağlar (Elfassy 2013, 5). Dolayısıyla Exchange, e-postaları depolamak, taşımak ve sunmak için tasarlanmış bir yazılım olarak tanımlanabilir.

Exchange'in yönetimi için Exchange Yönetim Merkezi (Exchange Admin Center - EAC) (Bkz. Şekil 7) kullanılmaktadır. EAC, Exchange Server 2013 ile gelen<sup>21</sup> yeni web tabanlı yönetim ara yüzüdür ve e-postalar için web tarayıcıları üzerinden bir yönetim ara yüzü sunar (Wesselius 2014, 4).



**Şekil 7: Exchange Yönetim Merkezi**

EAC ara yüzünden erişilip kontrol edilebilen birçok özellik Yİ sırasında ihtiyaç duyulabilecek öğeler barındırmaktadır. Herhangi bir tarayıcıdan <https://<ServerFQDN>/ecp><sup>22</sup> adresi ile erişilebilen EAC kullanıcı ara yüzünün elemanlarından bazıları şunlardır<sup>23</sup>:

**Alıcılar (Recipients):** E-posta kutularının, grupların, kişilerin, paylaşılan e-posta kutularının ve e-posta kutusu taşımalarının yönetim menüsüdür.

**İzinler (Permissions):** Role dayalı erişim denetimi (RBAC) yönetici rollerinin, kullanıcı rollerinin ve Outlook'u web ilkelerinde yönetme ile ilgili işlemlerin olduğu menüdür.

<sup>21</sup> Exchange Server 2010'da Exchange Management Console ve Exchange Control Panel kullanılmaktaydı.

<sup>22</sup> ServerFQDN, sunucu etki alanının tam adıdır (fully-qualified domain name).

<sup>23</sup> <https://docs.microsoft.com/en-us/exchange/architecture/client-access/exchange-admin-center?view=exchserver-2019> Erişim Tarihi 20.01.2019

Uygunluk yönetimi (Compliance management): Bu menüden, *yerinde keşif (in-place ediscovery)*, *yerinde bekletme (in-place hold)*, denetleme (posta kutusu denetim günlüğü ve yönetici denetim günlüğü), *veri kaybı önleme*<sup>24</sup> (DLP), saklama politikaları, saklama etiketleri ve günlük kuralları<sup>25</sup> ile ilgili yönetsel seçeneklere erişilebilmektedir.

Posta akışı (Mail flow): Posta akışı kurallarının (taşıma kuralları), teslimat raporlarının, kabul edilen etki alanlarının, uzak etki alanlarının ve e-posta adresi politikalarının yönetilebileceği menüdür.

EAC’de tüm fonksiyonlar bulunmamakta, sadece temel yönetim fonksiyonları yer almaktadır. Diğer tüm yönetim fonksiyonları için, Exchange Management Shell (EMS) kullanılabilir (Wesselius 2014, 4).

Exchange sunucusunun bulunduğu bir teşebbüste inceleme yapılması durumunda, kullanıcı e-postalarının silinmelerinin engellenmesine, silinen e-postaların yakalanmasına ve yapılabilecek herhangi bir hareketin izlenmesine ihtiyaç duyulabilir. Bu kapsamda Exchange’in resmi dokümanlarının sunduğu<sup>26</sup> şu bilgilerin kullanılabilirliği düşünülmektedir:

- Bir e-postanın; normal silinmesi *silme (delete)*; silinmiş öğelerden silinmesi<sup>27</sup> *yumuşak silme (soft delete)* ve e-posta kutusu veri tabanında temizlenecek olarak işaretlenmesi ise *sert silme (hard delete)* olarak adlandırılmaktadır.
- Exchange’de, belirlenen sorgu filtre parametreleriyle eşleşen e-posta kutusu öğelerini korumak için *yerinde tutma (in-place hold)* kullanılabilir. Kullanıcı e-posta kutularındaki tüm öğeleri korumak için ise *dava tutma (litigation hold)* kullanılmaktadır<sup>28</sup>. Ayrıca *tek öğe kurtarma (single item recovery)* özelliğinin aktif edilmesi ile de

---

<sup>24</sup> Bu menü ile ilgili bilgilere “2.9. Veri Kaybı Önleme Çözümleri” başlığında yer verilmiştir.

<sup>25</sup> Günlük kuralları konusuna “2.7. Günlükler” başlığında değinilmiştir.

<sup>26</sup> <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder?view=exchserver-2019> Erişim Tarihi: 20.01.2019

<sup>27</sup> Doğrudan klavyeden, Shift + Delete tuş kombinasyonu ile bir e-posta yumuşak silinebilir. Bu e-postalar, “3.2. E-Posta Verileri” başlığında da bahsedileceği üzere, belli bir süre boyunca kullanıcılar tarafından geri getirilebilmektedir.

<sup>28</sup> *Yerinde tutma* ve *dava tutma* özellikleri, e-postaları sistemin (otomatik olarak) silmesinden de koruyabilmektedir.

*sert silmeye* maruz kalan e-postalar aramalarda bulunabilmektedir<sup>29</sup>.

- “Uyum yönetimi” menüsündeki “Yerinde e-Keşif & Tutma” sekmesinden “Yeni (New)” seçeneğinin seçilmesiyle ile belirlenen filtreye takılan e-posta kutuları, *yerinde tutma* ile koruma altına alınabilir<sup>30</sup>.
- Bir e-posta kutusu *dava tutmaya* şu yolla dâhil edilebilir: “Alıcılar > E-posta Kutuları” sekmesinden “Değiştir (Edit)” linki seçilir. Çıkan ekranda “E-posta Kutusu Özellikleri (Mailbox Features)” sekmesindeki “Dava Tutma > Aktif” linki seçilir<sup>31</sup>.
- *Tek öge kurtarmanın* tüm e-posta kutularında aktif edilmesi için ise EMS içerisinde şu komut girilmelidir:

*Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Set-Mailbox -SingleItemRecoveryEnabled \$true*<sup>32</sup>

- Tüm e-posta kutularının içerisinde *kurtarılabilir öğeler klasörü* (*recoverable items folder*) bulunmaktadır. Bu klasörün tüm içeriği kullanıcıya görünmemektedir<sup>33</sup>. İçerisinde *sert silmeye* maruz kalmış e-postaları, *yerinde tutmaya* takılan e-postaları, *dava tutmaya* takılan e-postaları ve *denetim günlüklerini*<sup>34</sup> barındırmaktadır. İçerisindeki öğeler, *yerinde keşif* aramalarında, aramaya dâhil edilmektedir ve arama sonuçları içerisinde gösterilmektedir.

<sup>29</sup> E-postalar tek öge kurtarma özelliği aktif edildiğinde tutma/alıkoyma politikasında (retention policy) belirtilen gün süresince tutulmaktadır.

<sup>30</sup> <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/in-place-holds?view=exchserver-2019> Erişim Tarihi: 10.02.2019

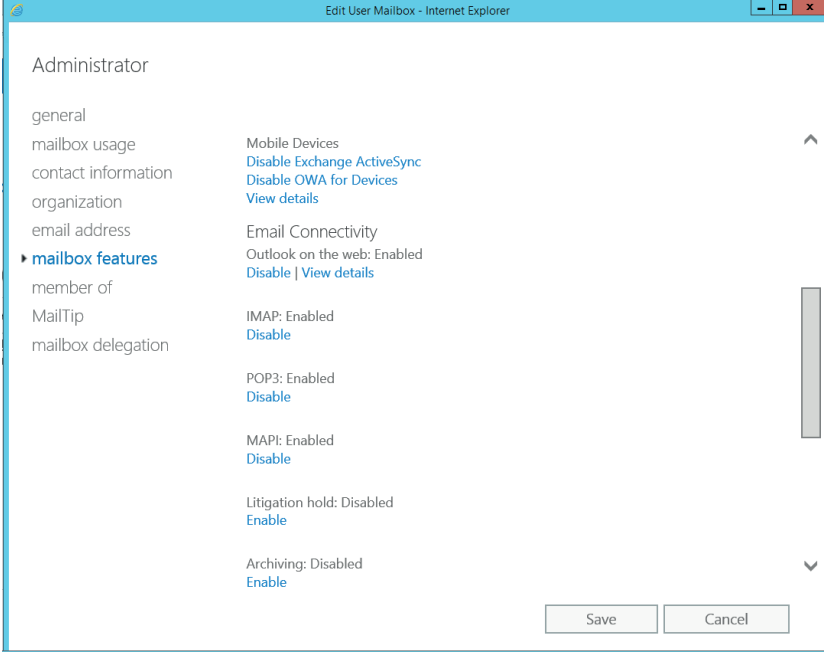
<sup>31</sup> <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/litigation-holds?view=exchserver-2019> Erişim Tarihi: 10.02.2019

<sup>32</sup> <https://docs.microsoft.com/en-us/exchange/recipients/user-mailboxes/single-item-recovery?view=exchserver-2019> Erişim Tarihi: 10.02.2019

<sup>33</sup> Tutma özelliklerinin aktif olması durumunda *sert silmeye* maruz kalmış dosyalar ile versiyonlar ve ayrıca takvim değişikliklikleri ile ilgili kayıtlar kullanıcıya görünmemektedir. Ancak silinenler klasörünün içeriği “Silinen Öğeleri Kurtar” özelliği ile kullanıcılar tarafından görüntülenebilmektedir. Bkz: <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder?view=exchserver-2019>

<sup>34</sup> Denetim günlükleri, e-postalar üzerinde yapılan eylemlerin (silme, değiştirme vb.) kayıtlarıdır. Bu konu ile geniş bilgiye “2.7. Günlükler” başlığında değinilecektir.

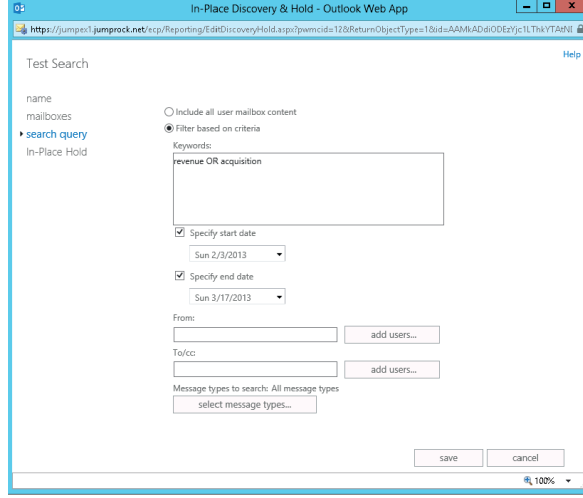
E-posta silinmelerinin engellenmesi için kullanılabilecek bir başka yöntem ise EAC ara yüzündeki “Değiştir” menüsünün “E-posta Kutusu Özellikleri” sekmesinde bulunan seçeneklerden e-posta kutusunun mobil ve web üzerinden erişime kapatılmasıdır (Bkz. Şekil 8).



**Şekil 8:** E-posta kutusu özellikleri ekranı

EAC’de inceleme süresini kısaltabilecek araçlar da bulunmaktadır. EAC’de, “Uyum Yönetimi” menüsündeki “Yerinde e-Keşif & Tutma” sekmesinden erişilebilen arama özelliği sayesinde tüm kullanıcı e-postalarında ya da belirtilen e-posta kutularında anahtar kelime araması yapılabilmektedir. Ayrıca burada AND, OR, NOT gibi arama operatörleri<sup>35</sup> de kullanılabilmektedir (Bkz. Şekil 9).

<sup>35</sup> Arama operatörleri, arama etkinliğini artırmak için kullanılan anahtar kelimelerdir. Bu konuya “Kullanıcı Bilgisayarları” bölümündeki “3.2. E-Posta Verileri” başlığında daha geniş yer verilecektir.



**Şekil 9:** Yerinde e-Keşif ile e-posta kutularında arama (Elfassy 2013, 479)

Bir başka hız kazandıracak yöntem ise, inceleme sırasında birden çok yönetici hesabı ile farklı bilgisayarlardan aynı anda e-posta kutularında arama yapmaktır. Bu sayede e-posta kutularında eş zamanlı inceleme yapılabilmektedir.

EAC üzerinden bir e-postanın *teslimat raporları (delivery reports)* ile teşebbüsteki belirli bir e-posta kutusundan gönderilen veya alınan mesajlar hakkındaki teslimat bilgileri de izlenebilmektedir. Bunun için, “E-posta Akışı” menüsündeki “Teslimat Raporları” sekmesinin kullanılması gerekmektedir (Bkz. Şekil 10).

### Exchange admin center

recipients  
permissions  
compliance management  
organization  
protection  
**mail flow**  
mobile  
public folders  
unified messaging

rules **delivery reports** accepted domains email address policies receive connectors send connectors

Search for delivery information about messages sent to or from a specific person. You can narrow the search to messages with certain keywords in the subject.

\*Mailbox to search:

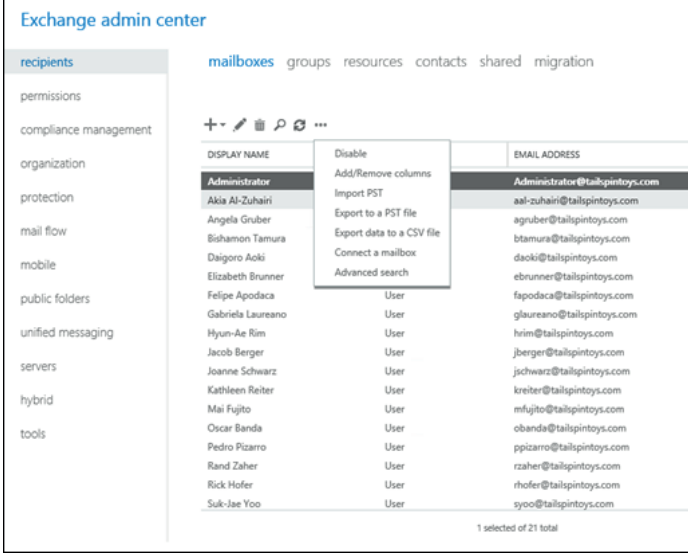
Search for messages sent to:

Search for messages received from:

Search for these words in the subject line:

**Şekil 10:** EAC “delivery reports” ekranı

EAC içerisinde bir kullanıcıya ait posta kutusunun tamamı (Bkz. Şekil 11) ya da *yerinde keşif* ile yapılan arama sonuçları PST<sup>36</sup> dosyası olarak dışarıya aktarılabilmektedir.



**Şekil 11:** Exchange e-posta kutusu seçenekleri<sup>37</sup>

Dışarı aktarılan bir e-posta kutusu, ayrı bir bilgisayara alınarak incelemeye tâbi tutulabilir. Bu işlem EAC'deki “Alıcılar” menüsü altında bulunan “E-posta Kutuları” sekmesinden yapılmaktadır. İlgili e-posta kutusu, kullanıcı adı ile bulunarak “e-posta Kutusu” seçeneklerinden “PST Dosyası Olarak Çıkar (Export to a PST file)” seçeneği ile dışarı aktarılabilmektedir.

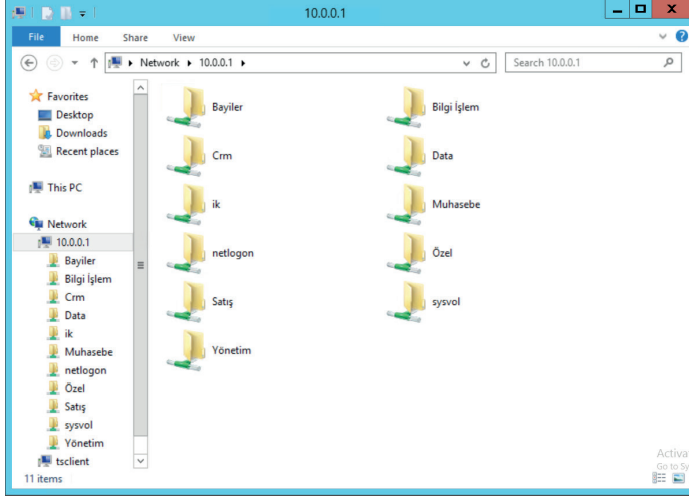
Exchange, kendi yapılandırması, kullanıcı doğrulaması ve kullanıcılar, kişiler, gruplar, ortak klasörler gibi e-postaya özgü özelliklerle ilgili olarak AD'den beslenir (Leonard vd. 2016, 11). Bu yüzden, Exchange ile ilgili bazı durumlarda (gruplar, Exchange yapılandırması, kişiler, ortak klasörler vb. bilgileri kontrol etmek) AD yönetim ara yüzlerinden de bilgi almak gerekebilmektedir.

<sup>36</sup> PST dosyaları birden çok e-postayı içerisinde barındıran “.pst” uzantılı dosyalardır.

<sup>37</sup> <https://docs.microsoft.com/en-us/exchange/recipients/mailbox-import-and-export/export-procedures?view=exchserver-2019> Erişim Tarihi: 10.02.2019

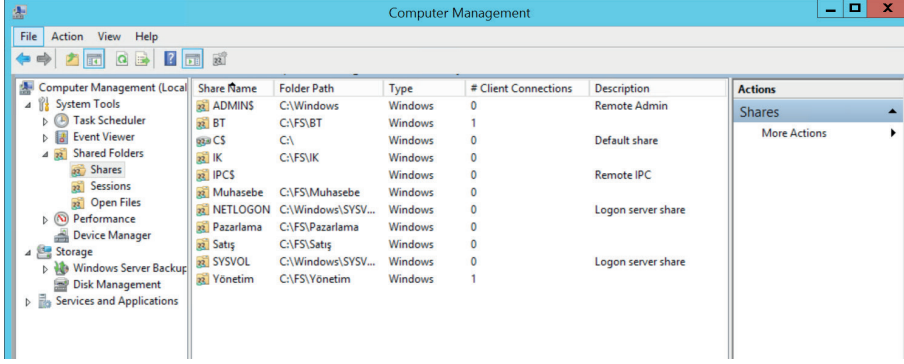
## 2.5. DOSYA SUNUCUSU

Her büyüklükteki kuruluş için dosya depolama ihtiyacı vardır ve kullanıcıların küçük ihtiyaçları için basit depolama alanları mevcut olsa da, bu iş için genelde ağda verileri depolamaktan sorumlu olan sunucular mevcuttur (Krause 2016, 347). Yİ’lerde verileri depolamaktan sorumlu olan dosya sunucularıyla karşılaşılabilir. Bu sunucular önemli delillerin bulunabileceği veri yığınları barındırmaktadır. Grup ve/veya kullanıcı tabanlı erişim izinlerinin verilebildiği birçok dosya içerebilen bu sunuculara ağ üzerinden erişilmektedir (Bkz. Şekil 12).



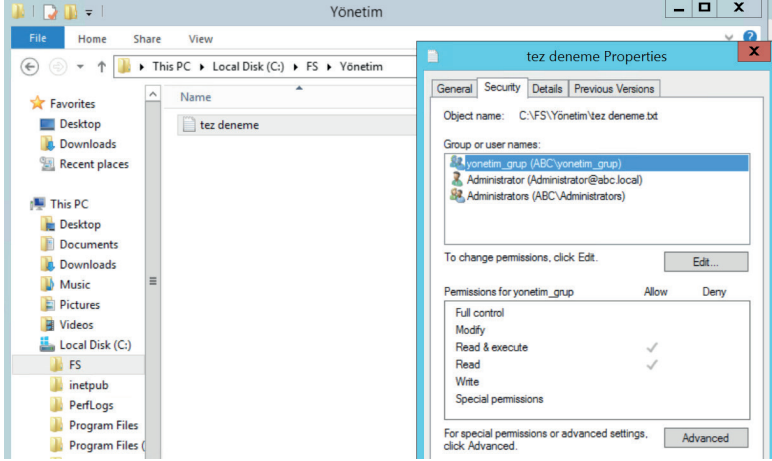
**Şekil 12:** Dosya sunucusundaki dosyaların ağ üzerinden görüntülenmesi

Dosya sunucusunda hangi dosyaların paylaşıldığına, dosya sunucusu bilgisayarın “Bilgisayar Yönetimi (Computer Management)” ekranından “Sistem Araçları (System Tools) > Paylaşılan Klasörler (Shared Folders) > Paylaşımlar (Shares)” yoluyla erişilebilmektedir (Bkz. Şekil 13). Ayrıca buradaki “Açık Dosyalar (Open Files)” menüsünden de, o anda açık olan dosyalar ve hangi kullanıcıların dosyayı görüntülediği görülebilmektedir.



**Şekil 13:** Dosya sunucusunda paylaşılan dosyaların görüntülenmesi

Dosya sunucusundaki bir belgenin kim tarafından oluşturulduğu, ne zaman oluşturulduğu ve belgede ne zaman değişiklik yapıldığı bilgileri, belgenin “Özellikler” menüsünden görülebilmektedir. Ayrıca dosya sunucusundaki bir belgenin paylaşım izinlerine, belgeye ait “Özellikler (Properties)” ekranındaki “Güvenlik (Security)” sekmesinden bakılabilmektedir (Bkz. Şekil 14).



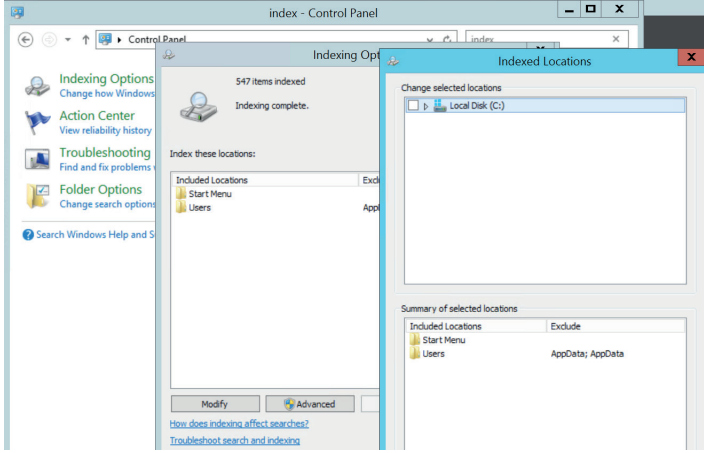
**Şekil 14:** Dosya sunucusundaki bir belgeye erişim izinleri

Dosya sunusundaki bir klasörde hızlı arama yapmak için klasörler dizine<sup>38</sup>

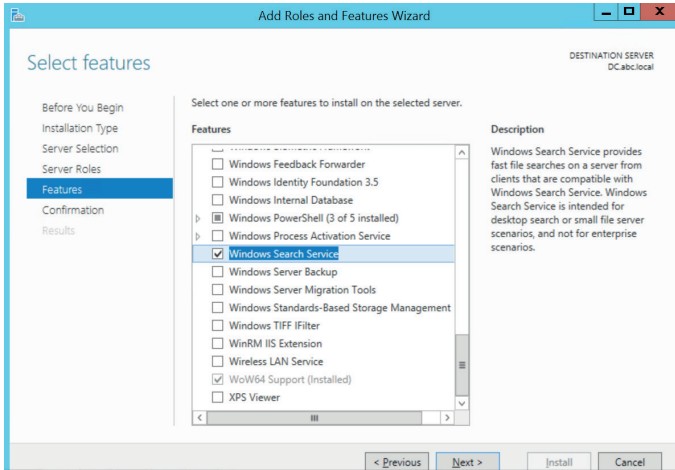
<sup>38</sup> Dizinleme hizmeti, Windows'ta kullanıcıların hızlı arama yapmasını sağlayan bir sistemdir. Bu sistemin çalışmasıyla ilgili ayrıntılara üçüncü bölümde “3.1. Windows Arama” başlığında yer verilecektir.



eklenmelidir (Bkz. Şekil 15). Klasörün dizine dâhil edilmesiyle Windows, klasördeki belgeleri de dizinine alacaktır. Bu sayede ilgili klasörde yapılan aramalar sadece belge isimlerinde değil aynı zamanda belge içeriğinde de yapılacaktır. Ancak bu işlem için *Windows Arama Servisi*'nin (*Windows Search Service*) de aktif edilmesi gerekmektedir (Bkz. Şekil 16).



**Şekil 15:** Dizin oluşturma seçenekleri ve dizin oluşturma konumları pencereleri



**Şekil 16:** Windows Arama Servisi'nin açılması

Dosya sunucusundaki tüm belgelere erişim izni olan bir kullanıcı hesabı ile dosya sunucusundaki tüm belgeler görüntülenebilmektedir.

Dosya sunucusunda inceleme yaparken, yapılan incelemenin gidişatının uzaktan izlenerek müdahale edilmesi ihtimali bulunmaktadır. Uzak bağlantı yapan yazılımlar ile inceleme yapılan bir bilgisayar izlenebilmekte ve dosya silme, dosya taşıma, dosya içeriğini değiştirme gibi tüm müdahaleler de uzaktan gerçekleştirilebilmektedir.

## 2.6. UZAK MASAÜSTÜ YAZILIMLARI

Özellikle çok kullanıcılı bilgisayar ağlarında kullanıcılara bilişim birimlerinin uzaktan teknik destek verebilmesi için uzak masaüstü yazılımları (remote desktop softwares - RDS) kullanılabilir. Bu yazılımlar, kullanıcılar arası masaüstü paylaşımı için de kullanılabilir. RealVNC, TeamViewer, TightVNC, AnyDesk, Windows RDP bunlara örnek olarak gösterilebilir.

Bu yazılımlar, çeşitli protokoller ve yöntemlerle çalışabilmektedir. Bu protokollerden biri olan *sanal ağ bilişimi* (*virtual network computing - VNC*) ‘bir bilgisayarın masaüstü ekranının bir ağ bağlantısı üzerinden uzaktan izlenmesini ve kontrol edilmesini sağlayan uzak masaüstü paylaşım teknolojilerinden birisidir (Yazdanipour vd. 2012). Bu teknolojiye, kullanıcı bilgisayarlarına yüklenmiş bir yazılım (VNC Viewer) sunucu (VNC Server) ile bağlantıya geçmekte ve diğer bir bilgisayarı uzaktan izlemek ve kontrol etmek mümkün olmaktadır. TightVNC, RealVNC, TigerVNC, UltraVNC bu yazılımlara örnek olarak gösterilebilir.

RDS yazılımlarından sıklıkla karşılaşılan TightVNC yazılımı ile bir bilgisayara bağlantı yapıldığı anda, bağlantı sağlanan bilgisayardaki tek değişiklik, bildirim alanında<sup>39</sup> gözüken yazılım logosundaki görsel değişiklik olmaktadır (Bkz. Şekil 17, Şekil 18). Bu durum, inceleme sırasında bilgisayara dışardan yapılacak bir müdahalenin dikkatlerden kaçabileceğini göstermektedir.

---

<sup>39</sup> Bildirim alanı, görev çubuğunun bildirimler ve durumlar için geçici bir alan sağlayan bölümüdür. Bkz. <https://docs.microsoft.com/en-us/windows/desktop/shell/notification-area> Erişim Tarihi: 08.02.2019

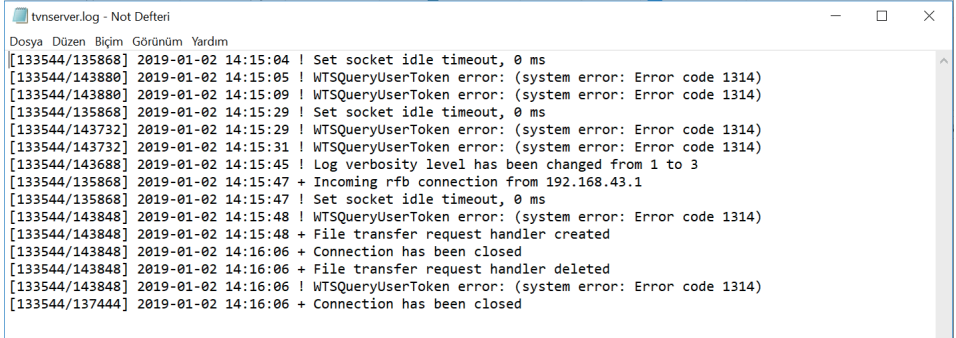


**Şekil 17:** Bağlantı öncesi TightVNC yazılım logosunun bildirim alanındaki görünümü



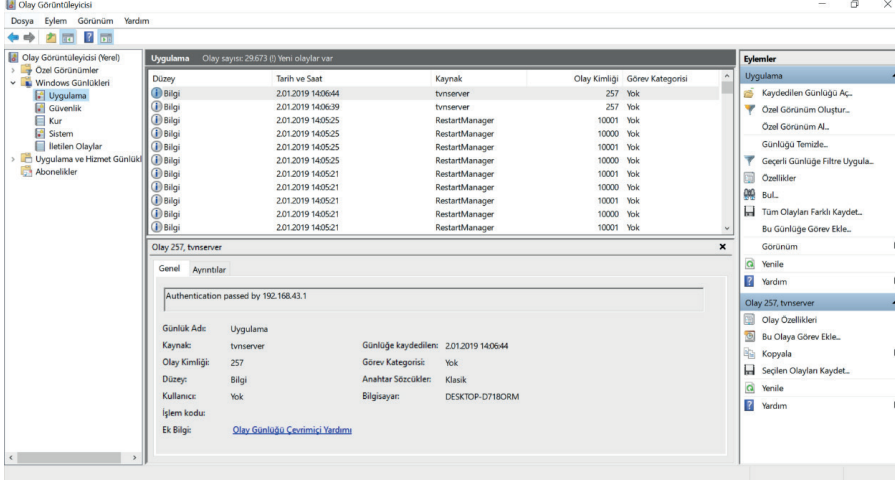
**Şekil 18:** Bağlantı sonrası TightVNC yazılımı logosunun bildirim alanındaki görünümü

İncelenmek istenen bilgisayarın ağ/internet bağlantısının kesilmesi, uzak bağlantı yapılması ihtimalini ortadan kaldıracak hızlı ve kolay bir yöntem olarak kullanılabilmektedir. Ayrıca uzak bağlantı sağlanıp sağlanmadığının anlaşılması için, varsa bu yazılımların günlük kayıtları da incelenebilir (Bkz. Şekil 19).



**Şekil 19:** Bağlantı sonrası ilgili yazılımın günlük kayıtları

Herhangi bir RDS yazılımı ile bilgisayara bağlantı yapıldığında, bu kayıt Windows günlüklerinde de görüntülenmektedir (Bkz Şekil 20).



**Şekil 20:** Bağlantı sonrası Windows günlüklerine düşen kayıt

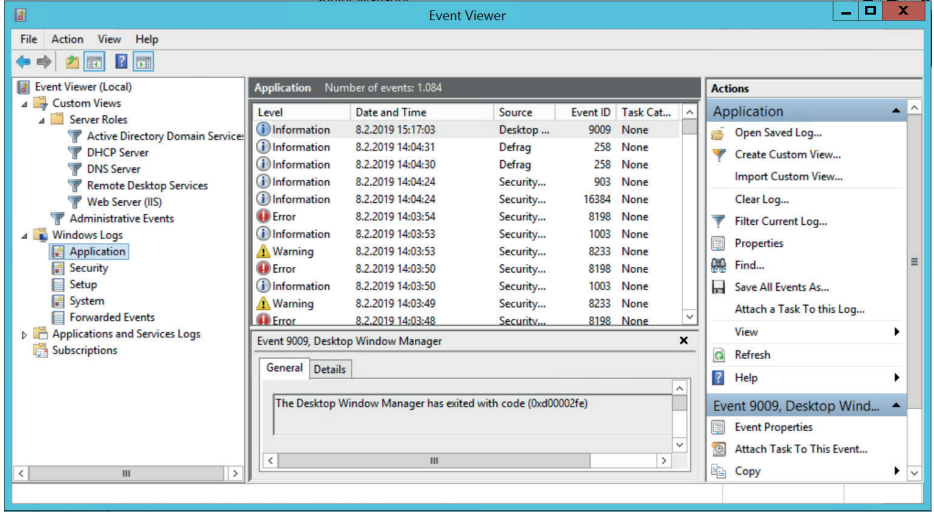
Dolayısıyla günlükler vasıtasıyla herhangi bir uzak bağlantı girişimi tespit edilebilmektedir.

## 2.7. GÜNLÜKLER

Günlükler (log), kullanıcı etkinliklerini kaydetmek, kimlik doğrulama girişimlerini ve diğer güvenlik etkinliklerini izlemek gibi amaçlar için kullanılabilir (Söderström ve Moradian 2013, 1249). Bunun yanı sıra günlüklerden, kullanıcıların giriş çıkış kayıtları, sunucudaki kaynaklara erişim kayıtları (kaynakların görüntülenip görüntülenmediği, görüntülenme zamanı vb.), gönderdikleri ve aldıkları e-posta içeriklerine kadar çeşitli bilgiler de edinilebilmektedir.

Hemen hemen Windows'un (arka planda, ön planda veya isteklere yanıt olarak) gerçekleştirdiği sistemle ilgili her görev kaydedilir ve bu olay günlükleri, Olay Görüntüleyicisi<sup>40</sup> (Bkz. Şekil 21) yardımcı yazılımı kullanarak incelenebilir (Bott 2016, 122).

<sup>40</sup> Olay Görüntüleyicisi yazılımı Windows'ta varsayılan olarak kurulu gelmektedir.



**Şekil 21:** Olay Görüntüleyicisi yazılımı ara yüzü

Olay Görüntüleyicisi yazılımındaki “Özel Görünümler (Custom Views)” ve “Windows Günlükleri (Windows Logs)” menüleri de bir takım önemli bilgiler verebilmektedir. “Özel Görünümler” menüsünden AD, DNS, DHCP ve IIS gibi sunucu rolleri günlüklerine erişilebilmektedir. Morimoto vd. (2017, 1242) Windows Günlükleri ile ilgili şu bilgileri vermektedir:

- Uygulama günlüğü: Bu günlük, sistemde bulunan uygulamalara veya yazılımlara dayalı olayları içerir.
- Güvenlik günlüğü: Yapılandırılan denetim ayarlarına bağlı olarak, kimlik doğrulama ve nesne erişimine özgü olayları yakalar.

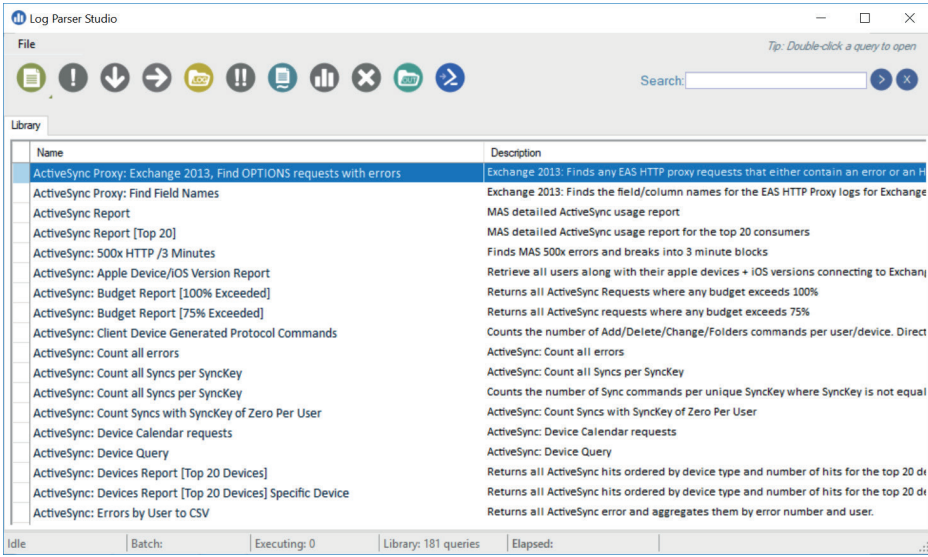
Olay Görüntüleyicisi kullanılırken karşımıza çıkan *olay kimliği (event ID)* kodunun da ne ifade ettiğinin bilinmesi gerekmektedir. Bu kodlar, olayın ne olduğunu açıklayan kodlardır. Örneğin, bazı *olay kimlikleri* ve açıklamaları şu şekildedir:

- 4658: Bir nesneye erişme girişiminde bulunuldu.
- 4672: Yönetici giriş yaptı.
- 5140: Ağ paylaşımına erişildi.

Uzaktan erişilip silinen bir dosyayı hangi kullanıcının sildiği, *olay kimlikleri*

analiz edilerek bulunabilmektedir<sup>41</sup>. Dolayısıyla, yaşanabilecek karartma girişimlerine karşı Olay Görüntüleyicisi önemli bir araç olarak kullanılabilir.

Birçok Windows servisinin standart Windows günlük kategorilerine günlük girişi yapabileceğini veya kendi günlük dosyalarını da oluşturabileceğini belirten Messier (2015, 202), bu günlüklerin tümünün, son Windows sistemlerinde standart günlük dizini olan “C:\Windows\System32\Winevt” konumunda bulunduğunu söylemektedir. Windows’un kendine özgü yapısında tutulan bu günlükler, Microsoft ürünü olan Log Parser<sup>42</sup> aracı ile de incelenebilmektedir (Chuvakin ve Schmidt 2012, 251). LogParser bir komut satırı aracıdır. Bu aracı grafik ara yüzü uygulaması olarak kullanmak için Log Parser Studio<sup>43</sup> (Bkz. Şekil 22) kullanılabilir. Log Parser Studio 170’den fazla sorgu içermektedir<sup>44</sup>.



Şekil 22: Log Parser Studio Uygulaması

<sup>41</sup> Detaylı bilgi için bkz. <https://blogs.technet.microsoft.com/askds/2009/08/04/tracking-a-remote-file-deletion-back-to-the-source/> Erişim Tarihi: 08.02.2019

<sup>42</sup> <https://www.microsoft.com/en-us/download/details.aspx?id=24659> Erişim Tarihi: 03.01.2019

<sup>43</sup> <https://gallery.technet.microsoft.com/office/Log-Parser-Studio-cd458765> Erişim Tarihi: 03.01.2019

<sup>44</sup> Detaylı bilgi için bkz. <https://blogs.technet.microsoft.com/exchange/2013/06/17/log-parser-studio-2-0-is-now-available/> Erişim Tarihi: 03.01.2019

En önemli delil kaynaklarından olan Exchange sunucusu ve dosya sunucusu için ise, bu servislere özgü günlükler aktif edilerek izleme mekanizmaları kullanılabilmektedir.

Exchange sunucusunun içerisinden aktif edilebilen denetim günlükleri, ihtiyaç duyulabilecek önemli bilgileri barındırmaktadır. E-posta kutusu denetim günlükleri etkinleştirilerek e-posta işlemlerinde kullanılan kullanıcı adları, IP adresleri, bilgisayar adları ve e-postalara erişme, e-postaları taşıma, e-postaları silme gibi bir e-posta kutusunda yapılabilecek eylemlerin<sup>45</sup> kayıtları tutulabilmektedir (Andersson ve Pfeiffer 2013, 266). Aynı zamanda Exchange sunucusunda yönetici hesabıyla yapılan değişiklikler de günlüklerden görülebilmektedir. Tüm bu günlüklere EAC ara yüzünde bulunan “Uyum Yönetimi” menüsündeki “Denetim” sekmesinden kısmi<sup>46</sup> olarak erişilebilmektedir. Daha detaylı denetim ve sorgulama yapmak için şu komutlar kullanılabilir:

- Bir kullanıcının denetim kayıtlarının etkinleştirilmesi için  
*Set-Mailbox -Identity “Ad Soyad” -AuditEnabled \$true*<sup>47</sup> komutu,
- Tüm kullanıcıların denetim kayıtlarının etkinleştirilmesi için  
*Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq “UserMailbox”} | Select PrimarySmtpAddress | ForEach {Set-Mailbox - Identity \$\_.PrimarySmtpAddress -AuditEnabled \$true}*<sup>48</sup> komutu,
- Bir kullanıcının denetim kayıtlarının aranması için (“user” adlı kullanıcı için)  
*Search-MailboxAuditLog -Identity user -ShowDetails* (Andersson ve Pfeiffer 2013, 368) komutu,
- Yönetici denetim kayıtlarının etkinleştirilmesi için

<sup>45</sup> Takip edilen eylemlerin tam listesi Microsoft dokümanlarından görülebilir. Bkz. <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging?view=exchserver-2019> Erişim Tarihi: 09.02.2019

<sup>46</sup> E-posta kutusu kullanıcısının, kendi e-posta kutusunda yaptığı eylemlerin günlükleri görülememektedir.

<sup>47</sup> <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019> Erişim Tarihi: 09.02.2019

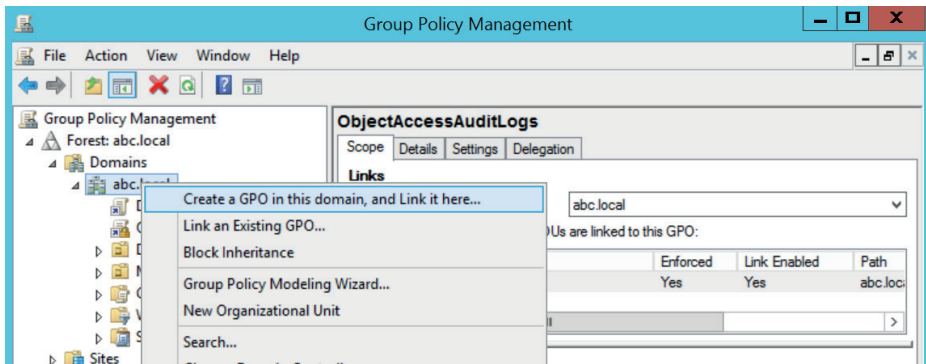
<sup>48</sup> <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019> Erişim Tarihi: 09.02.2019

*Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true*<sup>49</sup> komutu,

- Yönetici denetim kayıtlarının aranması için (örn: 01/04/2013 – 02/14/2013 tarihleri arası)

*Search-AdminAuditLog -Cmdlets Set-Mailbox -Parameters RoleAssignmentPolicy -StartDate 01/24/2013 -EndDate 02/14/2013* (Elfassy 2013, 321) komutu EMS penceresinden girilmelidir.

Dosya sunucusunda karşılaşılabilecek, belge silme, değiştirme ve taşıma işlemlerinin tespiti için *Nesne Erişim Denetimi (Object Access Audit)* günlükleri kullanılmaktadır. Bu sayede, Olay Görüntüleyicisinden söz konusu eylemler görüntülenebilmektedir. *Nesne Erişim Denetimi* günlüklerinin açılması, Sunucu Yönetimi<sup>50</sup> (Server Manager) yazılımındaki Grup Politikası Yönetimi (Group Policy Management) aracından yapılmaktadır. Oluşturulan yeni bir grup politikası nesnesi (Bkz. Şekil 23) düzenlenerek ilgili özellik politikanın alındığı tüm bilgisayarlarda aktif edilebilmektedir (Bkz. Şekil 24). Bu işlem ayrıca lokal olarak, denetim altına alınmak istenen dosya sunucusu klasörüne ait “Özellikler” penceresindeki “Güvenlik (Security) > Gelişmiş (Advanced) > Denetleme (Auditing)” yoluyla ulaşılan ekrandan, tüm kullanıcıları içeren “Herkes (Everyone)” grubunun da denetim girişlerine (auditing entry) eklenmesi ile de yapılabilmektedir. (Bkz. Şekil 25).

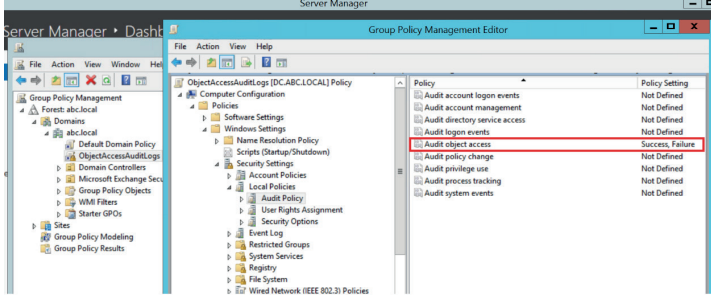


**Şekil 23:** Grup Politikası Yönetim aracından yeni bir nesne oluşturma

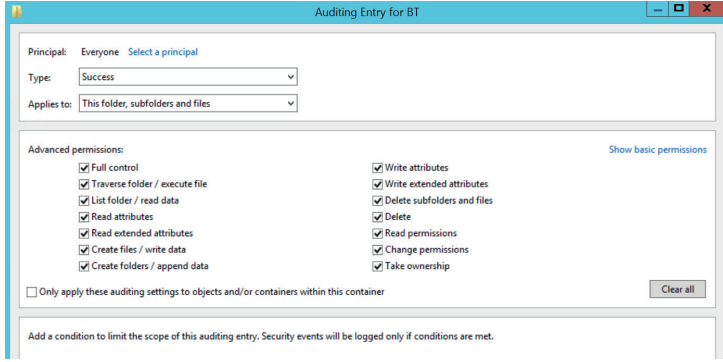
<sup>49</sup> <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/admin-audit-logging/manage-admin-audit-logging?view=exchserver-2019> Erişim Tarihi: 09.02.2019

<sup>50</sup> Bu yazılım, Windows Server’da varsayılan olarak gelmektedir.





Şekil 24: Grup politikası nesnesinden erişim denetim kayıtlarının açılması



Şekil 25: Herkes (Everyone) grubunun denetim girişlerine eklenmesi

Günlükler, sistemde yapılan değişiklikleri izlemede kullanışlı araçlar olarak karşımıza çıkmaktadır. Ancak birçok durumda varsayılan olarak günlüklerden faydalanmak mümkün olmamakta ek işlemlerin yapılmasına ihtiyaç duyulmaktadır. Ayrıca, yapılan bir işlemin günlüklerde görülmesi, o işlemin her zaman geri alınabileceği anlamına gelmemektedir. Örneğin, dosya sunucusundan bir belge silindiğinde, bu belgeyi geri getirmek için günlüklerin bir yardımı olmamaktadır. Canlı sistemde bir belgeye erişilememesi durumunda, yedekleme ve kurtarma çözümlerinden faydalanılabilmektedir.

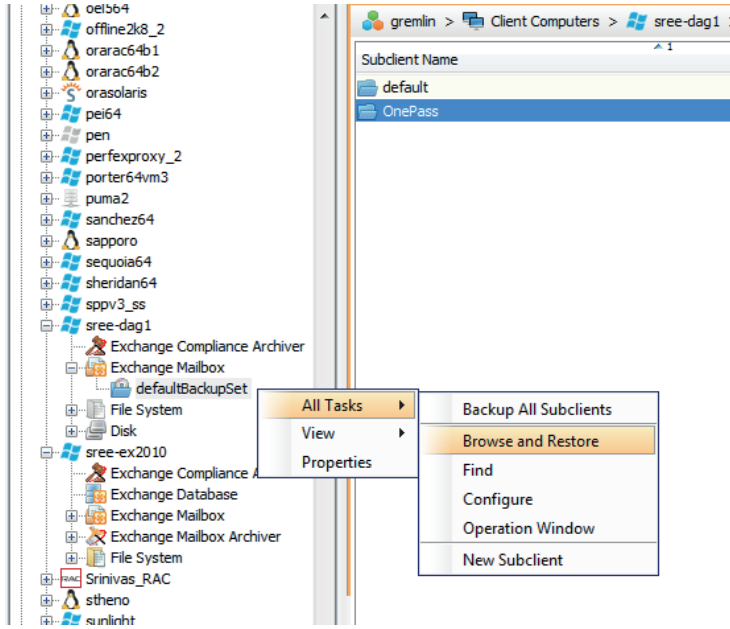
## 2.8. YEDEKLEME VE KURTARMA ÇÖZÜMLERİ

Bir sistemde uygun bir yedekleme stratejisi yoksa eldeki tüm veriler kaybedilebilmektedir (Watters 2013, 207). Genellikle kuruluşların bilgi teknolojileri departmanları bazı felaket kurtarma prosedürlerine sahiptir ve

sunucularındaki kritik verilerin yedeğini uygun şekilde alarak kurtarma politikaları geliştirmektedir (Snedaker 2013, 12).

Sunucularda kullanılan bazı yazımlarda daha az işlevsellikte dâhili yedekleme çözümleri bulunmaktadır. Büyük ölçekli teşebbüslerde ise yedekleme ve kurtarma işi için özelleşmiş yazılımlarla karşılaşılabilir. Veeam, Rubrik, Commvault, Adonis, Veritas Backup Exec gibi yazılımlar bunlara örnek olarak gösterilebilir.

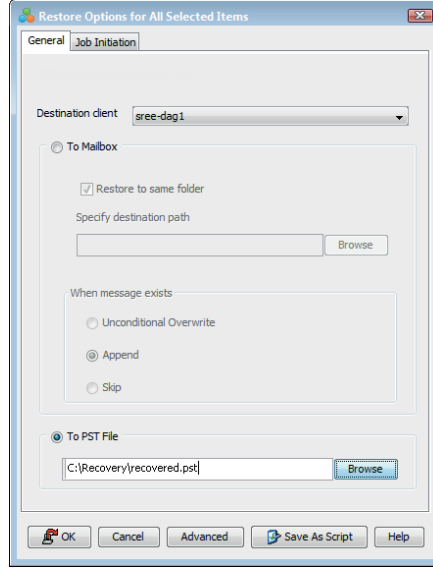
En çok kullanılan yedekleme çözümlerinden Commvault yazılımı, tüm dosya sistemleri, kurumsal uygulamalar ve sanal platformlar için destek sunduğunu belirtmektedir<sup>51</sup>. Commvault yazılımında, Exchange sunucu (Bkz. Şekil 26), dosya sunucusu, sanal sunucular ve kullanıcılara ait veriler için yedekleme ve kurtarma (Bkz. Şekil 27) çözümleri olduğu görülmektedir.



**Şekil 26:** Commvault'un Exchange E-Posta Kutusu yedekleme ve kurtarma seçenekleri<sup>52</sup>

<sup>51</sup> Bkz. <https://www.commvault.com/resources/commvault-complete-backup-and-recovery-data-sheet> Erişim Tarihi 01.01.2019

<sup>52</sup> [http://documentation.commvault.com/hds/v10/article?p=products/exchange\\_mailbox/restore\\_basics.htm](http://documentation.commvault.com/hds/v10/article?p=products/exchange_mailbox/restore_basics.htm) Erişim Tarihi 01.01.2019



**Şekil 27:** Commvault ile e-posta kutusu kurtarma işlemi<sup>53</sup>

Aranan verilerin canlı ortamda bulunamaması durumunda, geçmiş e-posta kutularına, dosya sunucusu verilerine ve hatta teşebbüs yedekleme politikasında yer alıyorsa kullanıcıların tüm verilerine yedeklerden erişilebilmektedir.

Verileri üzerinde kontrol sağlamayı isteyen kuruluşlar için bilişim sistemlerindeki büyük veri yığınları ve bu yığınların canlı sistemden yedeklere kadar birçok yerde olabilmesi bir risk barındırmaktadır. Bu noktada verilerin depolanmadan veya yedeklenmeden önce kontrolden geçirilebilmesi için, veri kaybı önleme çözümleri kullanılabilmektedir.

## 2.9. VERİ KAYBI ÖNLEME ÇÖZÜMLERİ

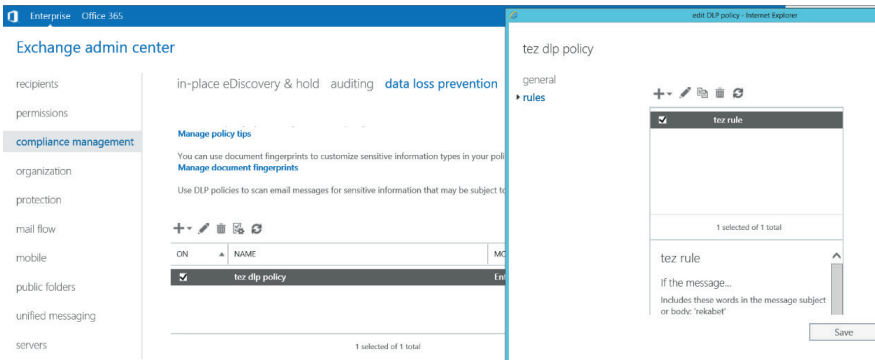
Kuruluşlar müşterilerin, iş ortaklarının, düzenleyicilerin ve hissedarların korunmasını beklediği hassas verilere sahiptir (Liu ve Kuhn, 2010, 10). Verilerin uygun şekilde korunmaması, sadece bir teşebbüse duyulan güveni sarsmakla kalmayıp aynı zamanda karışıklığa, marka imajının zedelenmesine, finansal kayıplara, hatta kuruluşlar veya düzenleyiciler tarafından önemli para cezaları

<sup>53</sup> [http://documentation.commvault.com/hds/v10/article?p=products/exchange\\_mailbox/restore\\_basic.htm](http://documentation.commvault.com/hds/v10/article?p=products/exchange_mailbox/restore_basic.htm) Erişim Tarihi 01.01.2019

verilmesine sebep olabilmektedir<sup>54</sup>. Dolayısıyla, bir teşebbüsün sahip olduğu veriler en önemli varlıklarındandır ve bu nedenle de söz konusu verilerin korunması gerekmektedir (Tahboub ve Saleh, 2014). Bu kapsamda Veri Kaybı Önleme (Data Loss Prevention - DLP) yazılımları, gelişmiş çözümler olarak karşımıza çıkmaktadır.

DLP ürünleri, içerdikleri politikalarla, atılan her e-postayı, kopyalanan veya taşınan tüm verileri, USB belleklere alınan her içeriği ve daha birçok işlemde veri akışını kontrol edebilmekte ve belirlenen politikayı ihlal eden bir eylem gerçekleştirildiğinde işlemi engelleyerek ya da kontrollü izin vererek, çeşitli şekillerde uyarılar verebilmektedir. Symantec DLP, Trustware DLP, McAfee Total Protection DLP gibi yazılımlar DLP ürünlerine örnek olarak gösterilebilmektedir.

Sunucularda kullanılan bazı servis veya yazılımlar da kısmen DLP görevi gören işlevlere sahip olabilmektedir. Exchange de, veri kaybı önleme görevini yerine getirebilen bir işleve sahiptir (Bkz. Şekil 28). Gönderici ve alıcı ismine, başlık ve içerikte belirlenen geçen bir ifadeye, kullanıcının belirlenen bir AD grubuna üyeliği olmasına, e-posta adresi uzantısı eşleşmesine vb. birçok duruma göre kural koyularak e-postalar kontrol edilebilmektedir. Bu kurallara takılan e-postalar sunucudan silinebilmekte, başka bir kişiye yönlendirilebilmekte, e-posta gönderilmesi reddedilebilmekte, e-posta göndermek isteyen kullanıcıya uyarı mesajı gösterilebilmektedir.



**Şekil 28:** Exchange Yönetim Paneli ara yüzünde tanımlanmış DLP politikaları

<sup>54</sup> <https://www.symantec.com/content/dam/symantec/docs/solution-briefs/why-you-need-an-information-centric-security-model-for-the-gdpr-en.pdf> Erişim Tarihi: 05.01.2019

DLP ürünleri, bilişim sistemindeki tüm veriler üzerinde kontrol yetkisine sahip olmayabilmektedir. Bu durumda, DLP'nin kontrolünün olmadığı yerlerde, DLP'nin engellemediği veya silmediği verilerle karşılaşmak olasıdır. Dolayısıyla DLP'de saptanacak filtreleme ifadeleri, kullanıcı bilgisayarlarındaki veriler içerisinde yapılan aramalarda kullanılabilir. İnceleme öncesi kullanılması planlanan arama ifadeleri de DLP'deki filtreleme ifadeleri doğrultusunda genişletilip daraltılabilir.

Yİ sırasında DLP ürünleri gibi spesifik işler için kullanılan başka sektörel ve/veya yerel yazılımlar ile de karşılaşmaktadır. Bu tarz yazılımlarla karşılaşıldığında, yazılımların çalışma prensipleri hakkında genel olarak bilgi sahibi olmak gerekebilmektedir.

## **2.10.SEKTÖREL VE YEREL YAZILIMLAR VE VERİTABANLARI**

Her kurumsal ağ, işletmek ve iş yapmak için gerekli anahtar hizmetleri sağlayan bir destek altyapısına sahiptir ve bu hizmetlerden bazıları yalnızca büyük kuruluş ortamlarında bulunurken, diğerleri neredeyse her ağda bulunur (Luttgens vd. 2014, 215).

Yİ sırasında teşebbüslerde sektörel veya yerel yazılımlarla karşılaşılabilir. Dolayısıyla, masaüstü ve web uygulamalarının<sup>55</sup> genel olarak çalışma şekillerini, verilerini nasıl sakladıklarını vb. temel özelliklerini bilmek gerekebilmektedir.

Uygulamalar temel olarak<sup>56</sup>, bulunduğu bilgisayara yüklenerek<sup>57</sup> (masaüstü uygulamaları) ya da bir tarayıcı üzerinden (web uygulamaları) erişilerek çalıştırılıp kullanılmaktadır. Bir masaüstü uygulamasının çalışması için önceden bilgisayara yüklenmiş yazılım kütüphanelerine (.net framework, java vb.) de ihtiyaç olabilmektedir. Çalışma yapısı farklı bir mantığa dayanan web uygulamaları ise genellikle bir sunucu üzerine yüklenmekte ve sunucu üzerinde yüklü bulunan Apache, IIS, Tomcat gibi bir Web/Http Server (Web Sunucu) yazılımı, bu web

<sup>55</sup> Tarayıcı tabanlı uygulamalar, güncelleme, geliştirme, paylaşım gibi açılardan getirdikleri kolaylıklar sebebiyle ile daha çok tercih edilmektedir (Jazayeri, 2007).

<sup>56</sup> Uygulamaları, taşınabilir cihazlar üzerinden, uzak bağlantı yoluyla vb. çalıştırma şekilleri de bulunmaktadır.

<sup>57</sup> Bazı uygulamaların kullanılması için kurulum yapılması gerekirken, bazıları için ise sadece çalıştırılabilir dosyanın çalıştırılması yeterlidir.

uygulamasını sunmaktadır. Herhangi bir bilgisayardaki tarayıcı üzerinden web sunucusuna bir istek geldiğinde<sup>58</sup>, sunucu ilgili web uygulamasını çalıştırıp ürettiği çıktıyı istek yapan adrese göndermektedir.

Hem masaüstü hem de web türlerinde, uygulama, çalışma sırasında tuttuğu verileri yerel olarak depolayabilmekte ve/veya uzak bir noktadaki veri tabanına kaydedebilmektedir. Masaüstü uygulamalar yerel depolama işlemi için genellikle *txt*, *xml*, *sqlite*, *db* vb. uzantılı dosyalar kullanmakta ya da Windows Kayıt Defteri'ne<sup>59</sup> (Windows Registry) kayıt yapmaktadır. Bu uygulamalar, çalışma zamanında oluşan bilgileri, veri tutma anlamında uçucu niteliğe sahip olan bellekte (memory) saklayabildikleri gibi kalıcı olan disklere de yazabilmektedir. Web uygulamaları ise verilerini çoğunlukla sunuculardaki veri tabanlarına kaydetmektedir.

Bir kullanıcı, bilgisayarında yüklü bulunan tarayıcı üzerinden bir web adresine giriş yaptığında, bu adresteki uygulama tarayıcıya yüklenip çalışmakta ve tarayıcının imkân verdiği ölçüde kullanıcının bilgisayarına da bir takım kayıtlar yapmaktadır. Çerezler (cookies), Web Storage and IndexedDB ve Cache API istemci tarafı depolama (client side storage) olarak adlandırılan bu kayıtlar arasında yer almaktadır<sup>60</sup>. Ayrıca tarayıcılar da kullanıcı bilgisayarlarında ziyaret edilen sitelerle alakalı çeşitli kayıtlar tutabilmektedir. Tarayıcı geçmiş verileri, yer imleri ve önbellek verileri bu tip kayıtlar arasındadır<sup>61</sup>.

Bir web uygulaması, Windows Server işletim sisteminde IIS servisi etkinleştirilip gerekli işlemler<sup>62</sup> yapıldıktan sonra yayına alınabilmektedir. Windows Server işletim sisteminde sadece IIS değil, aynı zamanda Apache ve Tomcat adlı web sunucularına da rastlanabilmektedir. Web sunucusu ne olursa olsun, web

<sup>58</sup> Örneğin bir siteye/adrese giriş yapıldığında, o sitenin yayına alındığı web sunucusuna istek gitmektedir.

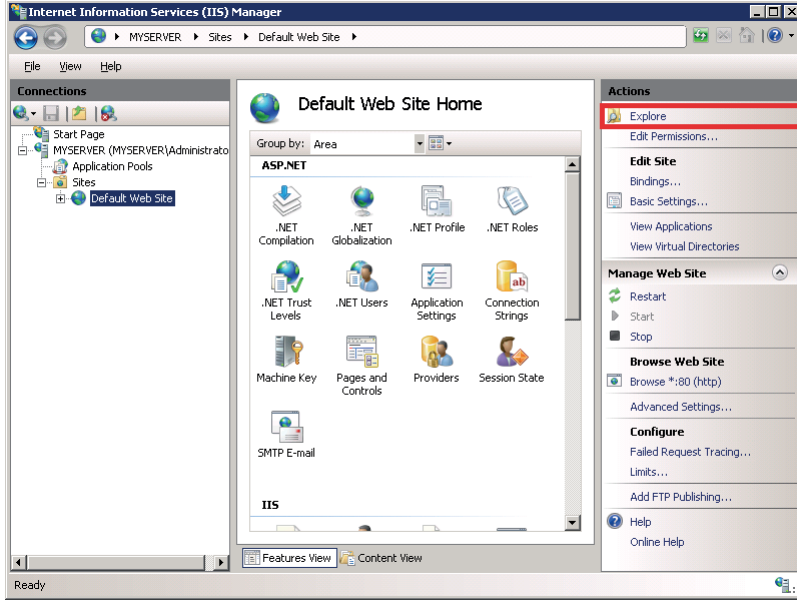
<sup>59</sup> Windows Kayıt Defteri, çekirdek sistem yapılandırması, kullanıcıya özel yapılandırma, yüklü uygulamalarla ilgili bilgiler ve kullanıcı kimlik bilgileri gibi çok çeşitli bilgileri depolamaktadır (Morgan 2008, 33).

<sup>60</sup> Detaylı bilgi için bkz. [https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Client-side\\_web\\_APIs/Client-side\\_storage](https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Client-side_web_APIs/Client-side_storage) Erişim Tarihi: 07.01.2019

<sup>61</sup> Tarayıcıların tuttukları kayıtlarla ilgili daha geniş bilgiye “3.3. Tarayıcı Verileri” başlığında yer verilmektedir.

<sup>62</sup> Bir web uygulamasının yayına alınabilmesi için, uygulamanın erişim izinlerinin ayarlanması, dosya izinlerinin ayarlanması, yönlendirmelerin yapılması gibi bir takım işlemlerin yapılması gerekmektedir.

uygulamasının bu sunucudan yayına geçirilmesi için, web uygulama klasörünün, sunucudaki ayara göre belirlenen bir yerde bulundurulması gerekmektedir. Bu klasöre web sunucusunun yönetim ara yüzünden erişilebilmektedir (Bkz. Şekil 29). Söz konusu klasörden, kodlama diline göre değişkenlik göstermekle birlikte, uygulamanın kullandığı veri tabanı adreslerine erişmek mümkün olmaktadır.



**Şekil 29:** IIS sunucu ara yüzünden site yazılım klasörüne erişim

Veri tabanlarından SQL<sup>63</sup> kullanılarak filtrelenen veriler, istenilen formatta alınabilmektedir. Ayrıca web uygulamaları kullanılarak yüklenmiş belgeler de, uygulamadaki yüklenen belgeler için belirlenmiş adresten elde edilebilmektedir.

Sunucularda onlarca farklı sistemle ve veri kaynağı ile karşılaşılabilir. Bu sistemlerin tamamının incelenip kullanıcı bilgisayarlarının daha sonra incelemeye alınması, birçok delilin yok edilmesine sebebiyet verebilir. Dolayısıyla Yİ'lerde, teşebbüsteki sunucularda ve kullanıcı bilgisayarlarında eş zamanlı incelemeler yapılmaktadır. Bir sonraki bölümde kullanıcı bilgisayarlarında gerçekleştirilen incelemeye dair bilgilere yer verilmektedir.

<sup>63</sup> SQL, veri tabanlarındaki verileri sorgulamak, düzenlemek, silmek gibi amaçlar için kullanılabilen bir dildir.

## BÖLÜM III

### KULLANICI BİLGİSAYARLARI

İş hayatında bilgisayar teknolojilerinin hâkimiyeti her geçen gün artmaktadır. Teşebbüsler hemen hemen tüm çalışanlarına bir bilgisayar tahsis etmektedir. Çalışanlar ise sektöre göre değişkenlik göstermekle birlikte genellikle işlerinin büyük kısmını tahsis edilen bilgisayarlar üzerinden gerçekleştirmektedirler. Dolayısıyla, rekabet ihlallerinin soruşturulmasında kullanıcı bilgisayarlarının uygun şekilde incelenerek delillerin açığa çıkarılması aşaması önemli bir yer kaplamaktadır.

Çalışmanın bu bölümünde ilk olarak, Yİ’lerde, teşebbüsteki kullanıcı bilgisayarlarında delil arama işlemi için kullanılan Windows Arama’nın ayrıntılarına değinilmektedir. Ardından, öncelikli delil kaynakları olarak görülen e-postaların ve tarayıcı verilerinin incelenmesine yer verilmektedir. Önemli görülen diğer uygulamaların da incelenmesinin ardından yazılım kullanılmaksızın elde edilemeyecek olan uçucu ve silinen verilerden bahsedilecektir. Son olarak ise, “veri hakkındaki veri” olarak bilinen dosya üst veri bilgilerine yer verilmektedir.

#### 3.1. WINDOWS ARAMA

Windows Arama (Windows Search), yaygın dosya türleri ve veri türleri için arama yeteneklerine sahip bir masaüstü arama platformudur ve kullanıcıların, büyük miktardaki verilerinden istediklerini bulmasını ve yönetmesini sağlar<sup>64</sup>. Windows 2003 ve XP sürümlerinde Windows Masaüstü Arama (Windows Desktop Search - WDS) olarak adlandırılan ve eklenti olarak kullanılabilen bu

---

<sup>64</sup> <https://docs.microsoft.com/en-us/windows/desktop/search/windows-search> Erişim Tarihi: 16.12.2018



işlev, Windows Vista versiyonuyla beraber Windows Arama (Windows Search) ismiyle standart hale gelmiştir<sup>65</sup>.

Windows Arama işlevi, Windows'ta farklı yerlerde karşımıza çıkmaktadır. Dosya Gezinisinden (File Explorer) kullanılan Windows Arama ile sadece ilgili dosyada ve alt dosyalarda arama yapılabilir. Ancak çoğu zaman, arama işlevinin daha fazla alanda arama yapması istenmektedir. Bu durumda Windows Arama tüm dosyaları, klasörleri, yazılımları, Windows Mail'deki e-posta mesajlarını, adres defteri girişlerini, takvim randevularını, PDF belgelerini, Internet Explorer'daki yer imlerini ve ofis belgelerini listelemek, adından veya klasör konumundan bağımsız olarak tüm sistemde arama yapmak için Başlat Menüsü içerisinde (Start Menu) kullanılabilir (Pogue 2010, 122). Windows Arama, ayrıca Windows 8'de Gezinti Çubuğundan (Charm Bar) (Pogue 2013, 252) ve Windows 10'da ek olarak birçok alanda da arama<sup>66</sup> yapan Cortana<sup>67</sup> Servisi (Pogue 2015, 119) üzerinden de kullanılmaktadır.

Windows Arama, bir bilgisayardaki tüm kullanıcılara ait dosyalar, e-postalar, yazılımlar, tarayıcı geçmiş gibi içeriklerin tek bir veri tabanını içermektedir (Chivers ve Hargreaves 2011, 114). Bu veri tabanı, Yİ'ler için değerli bir veri kaynağı olarak karşımıza çıkmaktadır.

Windows Arama, arka planda bilgisayardaki içerikleri kataloglamakta<sup>68</sup> ve bu sayede aramalar daha hızlı yapılabilir<sup>69</sup>. Buna dizin oluşturma (indexing) adı verilmektedir. Arama dizinleri “%ProgramData%\Microsoft\Search\Data” klasörünün içerisinde ve buraya sadece sistem ve yönetici (administrator) grubu kullanıcıların erişim izni bulunmaktadır (Bott 2016, 442). Dizini oluşturma, sistem dosyaları hariç, bilgisayarda depolanan dosyaları, uygulama isimlerini, ortak görevleri, dosya adlarını ve içeriklerini (mümkün olduğunda), ses ve

<sup>65</sup> <https://docs.microsoft.com/en-us/windows/desktop/search/-search-3x-wds-overview> Erişim Tarihi: 16.12.2018

<sup>66</sup> Cortana servisinin işlevleri için bkz. <https://support.microsoft.com/tr-tr/help/17214/windows-10-what-is> (Erişim Tarihi 16.10.2018)

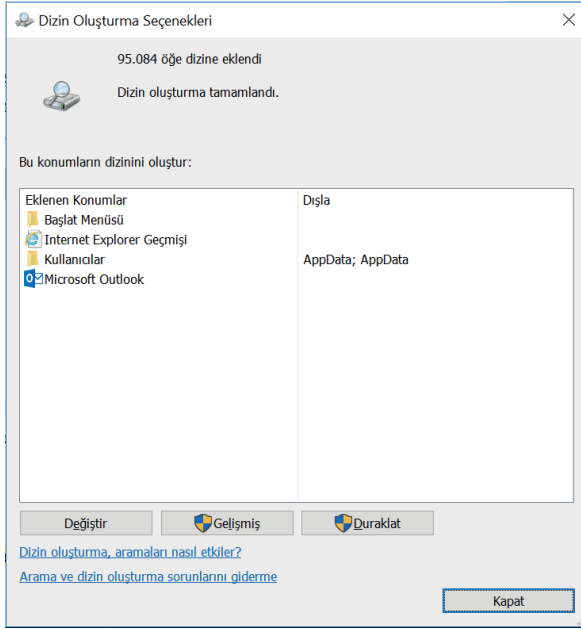
<sup>67</sup> Cortana servisi hali hazırda Türkçe dil desteği sunmamakta ve desteklemediği dillerle de işlevselliği sınırlı olmaktadır. Bkz. <https://support.microsoft.com/tr-tr/help/4026948/cortanas-regions-and-languages> (Erişim Tarihi 16.10.2018)

<sup>68</sup> Bu katalog, sistemin oluşturduğu Windows'a özgü bir veri tabanında saklanmaktadır.

<sup>69</sup> <https://support.microsoft.com/en-us/help/4098843/windows-10-search-indexing-faq> Erişim Tarihi: 16.10.2018

video kayıtlarını, resimleri, e-posta mesajlarını vb. bilinen birçok dosya türünü kapsamaktadır. Bu sayede, bir arama yapıldığında Windows, gerçek dosyalara değil dizinlere bakmaktadır (Lambert 2018,186).

Dizine dâhil edilmemiş alanlarda da arama yapılabilir. Ancak bu arama daha yavaş olmakta ve belge içeriklerini dikkate almamaktadır<sup>70</sup>. Dolayısıyla, canlı sistemlerde yapılan incelemelerde, Windows Arama'nın etkin şekilde kullanılması delilleri ortaya çıkarmada önemlidir ve ciddi miktarda zaman kazandırabilmektedir. Bu yüzden, hızlı arama yapılmak isteniyorsa ilk olarak aranmak istenen klasörlerin dizine dâhil edilmesi gerekmektedir. Bu işlem Windows'ta Dizin Oluşturma Seçenekleri ekranından<sup>71</sup> yapılmaktadır (Bkz. Şekil 30).



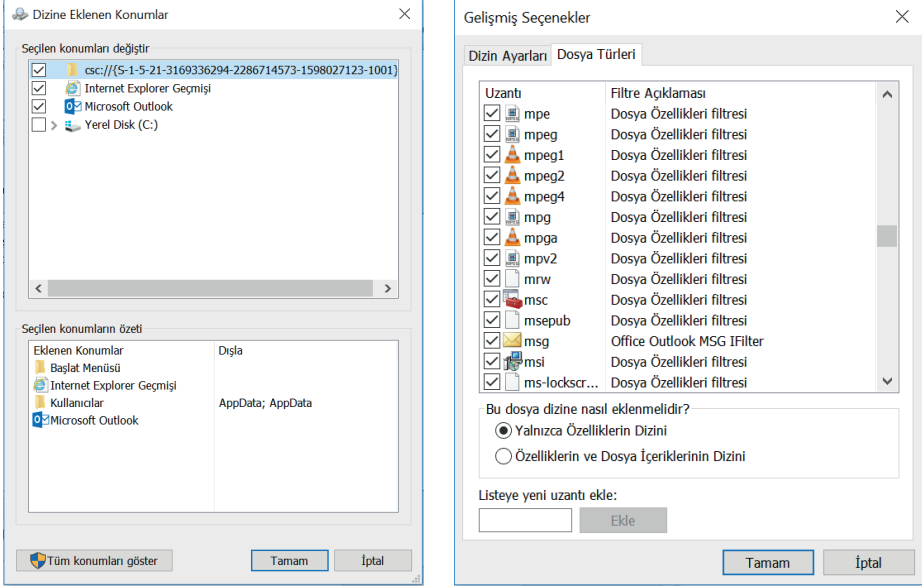
**Şekil 30:** Dizin oluşturma seçenekleri ekranı

Bu ekrandan ulaşılabilen “Dizine Eklenen Konumlar” ekranından dizine eklenecek dosyalar, klasörler veya sürücüler değiştirilebilmekte ve “Gelişmiş

<sup>70</sup> Dizine dâhil edilmemiş dosyalarda belge içeriği de aranmak isteniyorsa Dosya Gezgini Seçeneklerinden bu ayar yapılabilir.

<sup>71</sup> İlgili ekrana, “Başlat” Menüsünden veya Denetim Masasından arama yaparak erişmek mümkündür.

Seenekler” ekranından da aranacak dosya t rleri seilebilmektedir (Bkz.  ekil 31). Bu seenekler ile ihtiyaa g re arama geni letilebilmekte veya daraltılabilmektedir.



** ekil 31:** Dizin olu turma seeneklerinden eri ilen “Dizine Eklenen Konumlar” ve “Dosya T rleri” ekranları

Dizine d hil etme i leminin alacaėı zaman, bilgisayarın o anki i  y k ne, sabit diskinin hızına, i lemci g c ne, dizin b y kl klerine vd. fakt rlere g re deėi iklik g sterebilmektedir. B y k ve yava  disklerde bu i lem kabul edilebilir d zeyden daha uzun zamanlar s rebilmektedir. Dolayısıyla, dizinlere eklemekten yapılan aramanın daha kısa s rmesi durumu deėerlendirilerek dizinlerin kullanılması ile ilgili karar verilmesi gerekebilmektedir.

Bir diėer  nemli nokta ise, Windows Aramada geli mi  sorgu s z dizimini (advanced query syntax) kullanımınıdır. Geli mi  sorgu s z dizimini ile arama sorguları daha yakın sonular iin kullanılabilir. Windows’ta aramalar a aėıdaki parametrelerle daraltılabilmektedir<sup>72</sup>:

<sup>72</sup> Geni  bilgi iin bkz. <https://docs.microsoft.com/en-us/windows/desktop/lwef/-search-2x-wds-aqsreference> Eri im Tarihi: 19.12.2018

- Dosya çeşitleri: klasörler, belgeler, sunumlar, resimler vb.
- Dosya depoları: belirli veri tabanları ve konumlar.
- Dosya özellikleri: boyut, tarih, başlık vb.
- Dosya içeriği: “proje teslimatları”, “RK”, “anlaşma yapıldı” vb. anahtar kelimeler.

Ayrıca arama parametreleri, çeşitli operatörlerle (AND, OR, <, >, tür, dün, bugün durum vb.) ile aynı anda kullanılabilir. Tablo 1’de Windows aramalarında kullanılabilecek çeşitli parametreler<sup>73</sup> gösterilmektedir.

| Özellik           | Açıklama                                                  | Örnek              |
|-------------------|-----------------------------------------------------------|--------------------|
| Tür               | Belgeleri türüne (belgeler, resim, müzik) göre filtreler. | tür:belgeler       |
| Ext               | Belgeleri uzantısına göre filtreler.                      | ext:.docx          |
| Değiştirme tarihi | Belgeleri değiştirme tarihine göre filtreler.             | değiştirtarihi:dün |
| Boyut             | Belgeleri boyutuna göre filtreler.                        | boyut:>1 MB        |

**Tablo 1:** Windows Aramada kullanılacak parametreler

Her ne kadar Windows Arama ile birçok veriye ulaşmak mümkün olsa da USB bellekler ve şifrelenmiş diskler gibi bazı verilerin içeriği Windows Arama veri tabanında bulunmamaktadır. Ayrıca, dosyalar sistemden silindiğinde bu dosyalara ilişkin kayıtlar da veri tabanından silinmektedir.

Aramalar sırasında bulunan bazı dosyaların okunması için, bu dosya formatlarını açabilen yazılımlara ihtiyaç olabilmektedir. Bu gibi durumlarda ilgili dosyalar, farklı bir bilgisayara aktarılarak incelenebilmektedir. Windows Arama birçok işlevselliğe sahip olsa da, e-posta verileri ve tarayıcı verileri gibi bazı verilerin incelenmesi ek işlemlerin yapılmasını gerektirebilmektedir.

<sup>73</sup> Diğer parametreler için bkz. <https://docs.microsoft.com/en-us/windows/desktop/lwef/-search-2x-wds-aqsreference> Erişim Tarihi: 19.12.2018

### 3.2. E-POSTA VERİLERİ

Bütün potansiyel elektronik delil kaynakları arasında, e-posta verileri en iyilerden biridir (Sammons 2012, 126). E-postalar, günümüzde özellikle şirket ortamlarında en çok kullanılan iletişim yöntemleri arasındadır (Shaaban ve Sapronov 2016, 221). E-postaları araştırırken deliller, şüphelinin makinesi, herhangi bir alıcının makinesi, şirket sunucusu veya yedekleme medyası, akıllı telefon, servis sağlayıcı ve mesajın son hedefine ulaşmış olabileceği herhangi bir sunucu gibi birkaç yerde bulunabilmektedir (Sammons 2012, 127). Dolayısıyla, e-postaları incelemeye başlamadan önce, kontrol ve koruma ortamının sağlanması önem arz etmektedir.

Kontrol ve koruma ortamının sağlanması için, sunucu tarafında daha merkezi (tüm e-postaları kapsayacak) işlemler yapılabilecekken, sunucuya erişimin olmaması veya gecikmesi durumunda ise kullanıcı bilgisayarlarında alınabilecek birtakım önlemler bulunmaktadır. Bu noktada, e-posta işlemlerinin istemci üzerinden mi tarayıcı üzerinden mi yapıldığı ayrımı önem arz etmektedir.

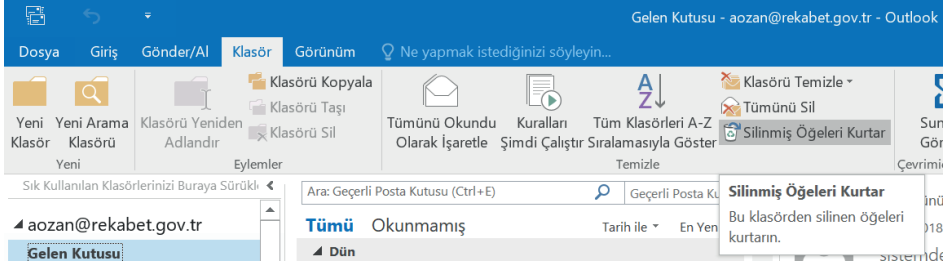
Microsoft firmasının ürünü olan Outlook istemci uygulaması, Windows'ta en çok kullanılan ve teşebbüslerde de en çok karşılaşılan e-posta istemci uygulamasıdır. Outlook yerel olarak verileri PST veya OST formatında depolamaktadır (Messier 2015, 178). Bu sayede çevrimdışı çalışmak da mümkün olmaktadır.

Outlook'ta bir e-posta silindiğinde önce silinmiş öğeler klasörüne düşmektedir. Silinmiş öğeler klasöründen de silinen veriler artık sadece e-posta sunucusunda izlenen politika çerçevesinde belirlenen gün sayısınca<sup>74</sup> tutulmaktadır. Bu e-postalar, Outlook içerisinden kurtarılabilmektedir. Silinmiş e-postaların kurtarılması için Outlook'ta "Klasör" menüsünden "Silinmiş Öğeleri Kurtar" seçeneği kullanılmaktadır<sup>75</sup> (Bkz. Şekil 32).

---

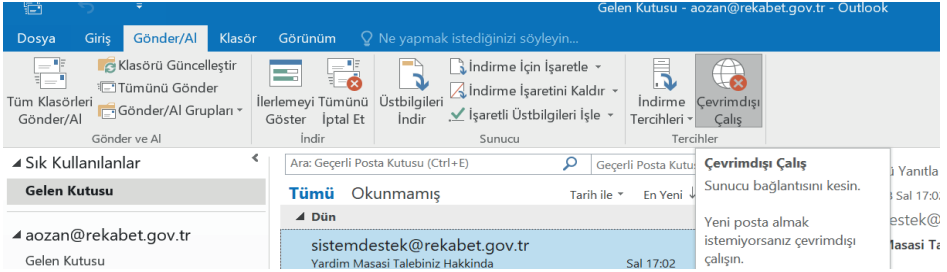
<sup>74</sup> Varsayılan olarak 14 gündür. Bkz. <https://docs.microsoft.com/en-us/exchange/configure-deleted-item-retention-and-recoverable-items-quotas-exchange-2013-help> Erişim Tarihi: 10.02.2019

<sup>75</sup> Bu işlem için e-posta sunucusuna bağlantı sağlanabiliyor olması gerekmektedir.



**Şekil 32:** Outlook'ta silinmiş öğeleri kurtarma

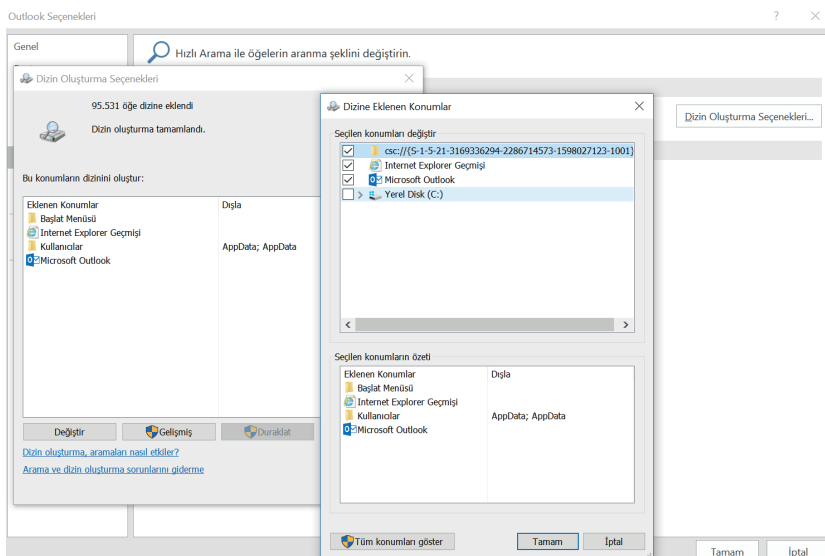
Silinmiş e-postaların kurtarılmasının ardından Outlook çevrimdışı moda alınırsa (Bkz. Şekil 33), yerel olarak tutulmakta olan kayıtlar üzerinden dış müdahale olmadan (başka cihazlardan e-posta hesabına erişim yapılarak bir işlem gerçekleştirilmeden) inceleme yapılabilmektedir.



**Şekil 33:** Outlook'un çevrimdışı çalışma moduna alınması

Outlook üzerinden, istenen e-posta veya e-posta grupları PST veya OST formatında dışarıya ve içeriye aktarılabilir. Bilgisayarda yapılan incelemede bu dosya formatlarına rastlanması durumunda, dosyaların bulunduğu klasör ve/veya diskler, Outlook'ta Seçenekler menüsündeki Arama sekmesinden ulaşılan "Dizin Oluşturma Seçenekleri" ekranı ve "Dizine Eklenen Konumlar" ekranından (Bkz. Şekil 34) dizine alınarak inceleme gerçekleştirilebilir. Outlook istemci uygulamasının sunduğu "İçeri Aktar" veya "Outlook Veri Dosyası Aç" işlevleri<sup>76</sup> de bu dosya türlerinde inceleme yapmak için kullanılabilir.

<sup>76</sup> Bu işlevler, Outlook'ta "Dosya" menüsündeki "Aç ve Dışarı Aktar" sekmesinde bulunmaktadır.



Outlook arama özelliğinin etkin kullanılması, inceleme sırasında oldukça zaman kazandırabilmektedir. Tablo 2’de bazı<sup>77</sup> özellik ve operatörler örnek arama ifadeleri ile birlikte gösterilmektedir.

**Tablo 2:** Outlook'ta arama ifadelerinin kullanımı<sup>78</sup>

<sup>78</sup> Aramalara tüm Outlook öğelerinin dâhil edildiği var sayılmaktadır.

E-postalarda, resim içeriğindeki metinler gibi, kelime araması sonucu bulunamayacak birçok delilin gözden kaçırılması ihtimali bulunmaktadır. Bu durumun engellenmesi için tüm e-postaların tek tek okunması gerekmektedir. Ancak çalışmanın son bölümünde değinileceği üzere adli bilişim yazılımlarının kullanımı ile birçok zaman alıcı işlem daha kolay bir şekilde yerine getirilebilmektedir.

E-postalar sadece Outlook gibi bir istemci yazılımı üzerinden kullanılmakla kalmayıp, tarayıcılar üzerinden de kullanılabilir. Tarayıcıların incelenmesi ile ilgili hususlara bir sonraki başlıkta yer verilmektedir.

### 3.3. TARAYICI VERİLERİ

Tarayıcılar, web sitelerine ve uygulamalarına erişim için kullanılan yazılımlardır. Kullanıcılar tarayıcıları bilgiye erişim, e-posta hesaplarına erişim, e-ticaret, bankacılık, mesajlaşma, blog uygulamaları ve sosyal ağlara erişim gibi amaçlar için kullanmaktadır (Akbal vd. 2016, 631). Tarayıcılar da, yapılan işle ilgili birçok veriyi kaydetmektedir. Dolayısıyla tarayıcılar, Yİ'ler için önemli veri kaynakları arasında yer almaktadır.

Günümüzde masaüstü platformlarda Chrome, Firefox ve Internet Explorer en popüler tarayıcılardır<sup>79</sup>. Bu yazılımlar bilgisayarlara doğrudan kurularak kullanılabilirdiği gibi, taşınabilir cihazlara yüklenerek de kullanılabilir.

Tarayıcılar, genellikle bir sabit disk sürücüsüne, veri kalıntılarını, çerezler<sup>80</sup>, geçmişte ziyaret edilen siteler, kayıtlı parolalar, önbelleğe alınmış web sayfaları ve indirilen nesneler olarak kaydetmektedir (Marrington vd. 2012). Standart ayarlarda, tüm büyük tarayıcılar, verimliliği artırmak ve kullanıcı deneyimini geliştirmek için sitelere ilk girişte önyükleme (cache) dosyaları da oluşturmaktadır (Horsman 2018, 105). Ayrıca tarayıcılar, ziyaret edilen sitelere tekrar giriş yapıldığında hızlı işlem yapılabilmesi için şifreleri, ödeme yöntemlerini, adresleri vb. verileri “otomatik doldurma verileri” adı altında kaydedebilmektedir.

---

<sup>79</sup> Bkz. <http://gs.statcounter.com/browser-market-share/desktop/worldwide> Erişim tarihi 6.12.2018

<sup>80</sup> Çerezler, ziyaret edilen web siteleri tarafından oluşturulan dosyalardır. Tarama bilgilerini kaydederek kullanıcı deneyimini arttırmayı amaçlamaktadır. Çerezler ile siteler kullanıcı oturumunu açık tutabilmekte, kullanıcının site tercihlerini hatırlayabilmekte ve alakalı içerik gösterebilmektedir.

Örneğin Chrome tarayıcısında kullanılan çerezlerin işlevi için bkz. <https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=en-GB> Erişim Tarihi: 01.02.2019



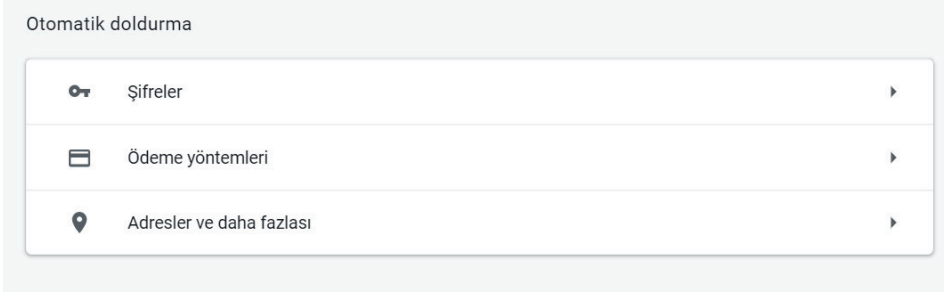
Tek bir tarayıcının bıraktığı kalıntıları incelemek, aranan verinin birkaç tarayıcının kayıt dosyasına yayılması ihtimalinden dolayı uygun ve yeterli bir yol değildir (Oh vd. 2011, 62). Bu durumda, bilgisayardaki tüm tarayıcı kayıtlarında arama yapılması gerekebilmektedir. Tarayıcıların dosya kayıt konumları Tablo 3’de verilmektedir.

| Web Browser       | Operating System                    | File Path                                                                                                                                                                                                           |
|-------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internet Explorer | Windows 95/98                       | C:\Temporary Internet Files\Content.IE5<br>C:\Cookies<br>C:\History\History.IE5                                                                                                                                     |
|                   | Windows 2000/XP                     | C:\Documents and Settings\%username%\Local Settings\Temporary Internet Files\Content.IE5<br>C:\Documents and Settings\%username%\Cookies<br>C:\Documents and Settings\%username%\Local Settings\History\history.IE5 |
|                   | Windows Vista, 7 and latest version | C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\<br>C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\                                                  |
|                   | Linux                               | /home/\$USER/.mozilla/firefox/\$PROFILE.default/places.sqlite                                                                                                                                                       |
|                   | MacOS-X                             | /Users/\$USER/Library/Application Support/Firefox/Profiles/\$PROFILE.default/places.sqlite                                                                                                                          |
|                   | Windows XP                          | C:\Documents and Settings\%username%\Application Data\Mozilla\Firefox\Profiles\%PROFILE.default\places.sqlite                                                                                                       |
| Firefox           | Windows Vista, 7 and latest version | C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE.default\places.sqlite                                                                                                                         |
|                   | MacOS-X                             | /Users/\$USER/Library/Safari/<br>/Users/\$USER/Library/Caches/com.apple.Safari/                                                                                                                                     |
|                   | Windows XP                          | C:\Documents and Settings\%username%\Application Data\Apple Computer\Safari\<br>C:\Documents and Settings\%username%\Local Settings\Application Data\Apple Computer\Safari\                                         |
| Safari            | Windows 7                           | C:\Users\%username%\AppData\Roaming\Apple Computer\Safari\<br>C:\Users\%username%\AppData\Local\Apple Computer\Safari\                                                                                              |
|                   | Linux                               | /home/\$USER/.opera/                                                                                                                                                                                                |
|                   | MacOS-X                             | /Users/\$USER/Library/Opera/                                                                                                                                                                                        |
| Opera             | Windows XP                          | C:\Documents and Settings\%username%\Application Data\Opera\Opera\<br>C:\Users\%username%\AppData\Roaming\Opera\Opera\                                                                                              |
|                   | Windows Vista, 7 and latest version |                                                                                                                                                                                                                     |
|                   | Linux                               | /home/\$USER/.config/google-chrome/Default/Preferences                                                                                                                                                              |
| Google Chrome     | MacOS-X                             | /Users/\$USER/Library/Application Support/Google/Chrome/Default/Preferences                                                                                                                                         |
|                   | Windows XP                          | C:\Documents and Settings\%username%\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences                                                                                                    |
|                   | Windows Vista, 7 and latest version | C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\Preferences                                                                                                                                       |

**Tablo 3:** Tarayıcıların kayıt konumları (Akbal vd. 2016, 633)

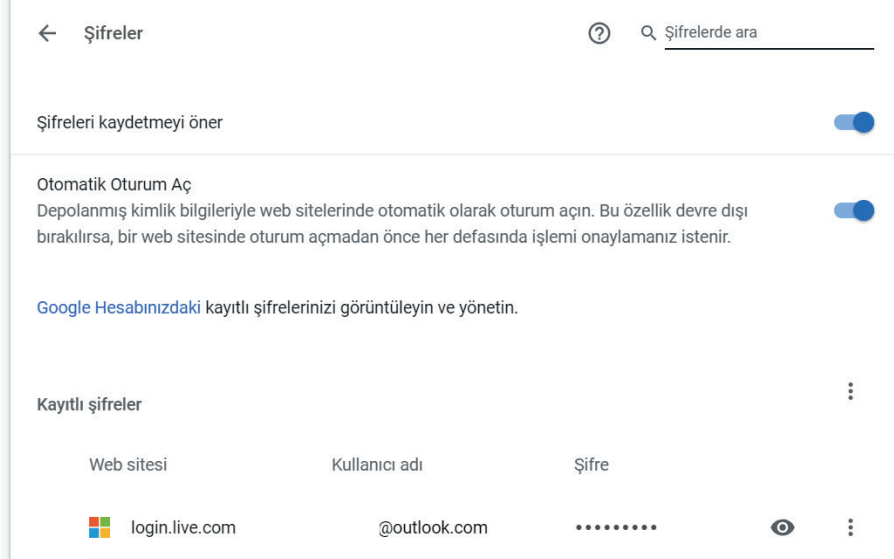
Bu konumdaki bazı dosyalar (txt, xml vb. uzantılı dosyalar), ek bir yazılım kullanılmadan okunabilmektedir. Ancak bazıları (sqlite, db vb. uzantılı dosyalar) için ise, ilgili dosyanın formatını okuyabilecek bir yazılımın kullanılmasına ihtiyaç bulunmaktadır.

Tarayıcıların sunduğu imkânlar çerçevesinde tarayıcı verilerinin bazıları görüntülenebilmektedir. Örneğin en çok kullanılan tarayıcılardan biri olan Chrome’un “Ayarlar” menüsünden *otomatik doldurma* verilerine (Bkz. Şekil 35) erişilebilmektedir.



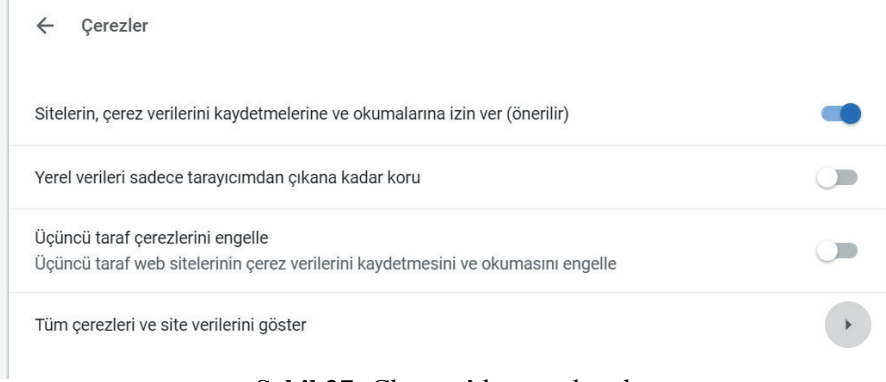
**Şekil 35:** Chrome’da otomatik doldurma verileri

”Otomatik doldurma” ekranındaki kayıtlı veriler görüntülenerek (Bkz. Şekil 36) ilgili sitelere, şifreleri bilmeye gerek kalmadan giriş yapılabilir.

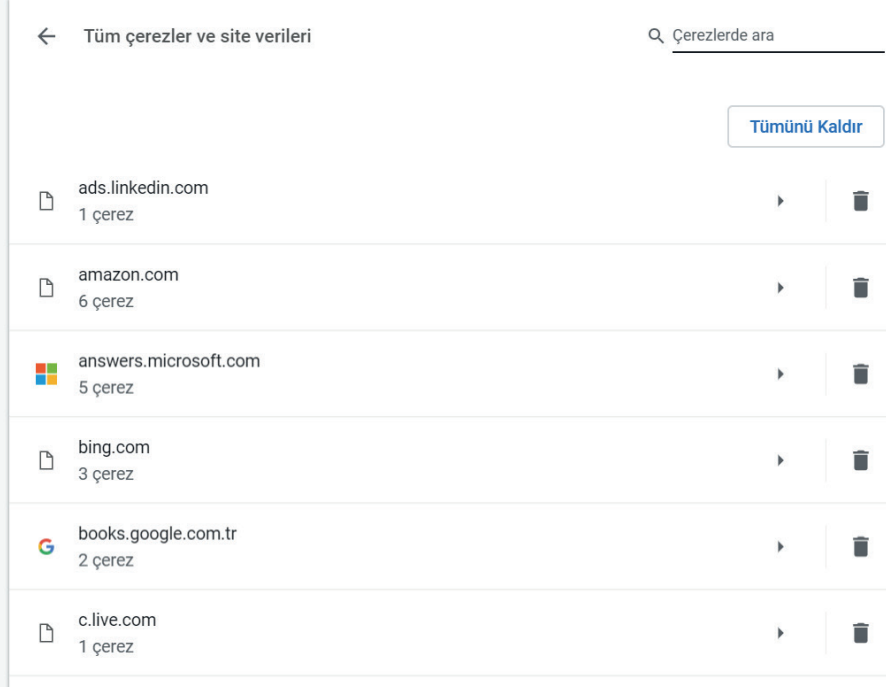


**Şekil 36:** Chrome’da otomatik doldurma için kayıtlı şifrelerin görüntülenmesi

Chrome’da “Ayarlar” menüsünün “Gelişmiş” bölümünde yer alan “Gizlilik ve Güvenlik” sekmesindeki “İçerik Ayarları” linkinin ardından “Çerezler” linki ile ulaşılan ekrandan (Bkz. Şekil 37) kayıtlı tüm çerezler (Bkz. Şekil 38) görüntülenebilmektedir.

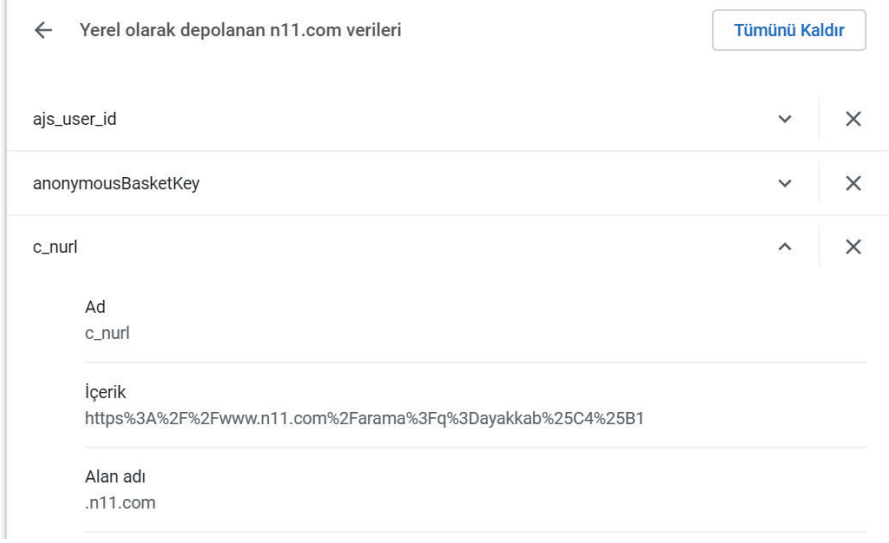


Şekil 37: Chrome’da çerezler ekranı



Şekil 38: Chrome’da tüm çerezler ve site verileri ekranı

Çerezler içerisinde, ziyaret edilen bir sitede yapılan eylemler hakkında verilere ulaşılabilmektedir (Bkz Şekil 39).



**Şekil 39:** Chrome’da çerez verilerinin okunması

Chrome içerisinde “Geçmiş” menüsünden daha önce ziyaret edilen siteler, “İndirilenler” menüsünden daha önce yapılan indirmeler ve “Yer İşaretleri” menüsünden kullanıcıların yer işaretlerine erişilebilmektedir (Bkz. Şekil 40).

|                    |                      |
|--------------------|----------------------|
| Yeni sekme         | Ctrl+T               |
| Yeni pencere       | Ctrl+N               |
| Yeni gizli pencere | Ctrl+ÜstKrkr+N       |
| Geçmiş             | ►                    |
| İndirilenler       | Ctrl+J               |
| Yer İşaretleri     | ►                    |
| Yakınlaştır        | - %100 + [Zoom Icon] |
| Yazdır...          | Ctrl+P               |
| Yayınla...         |                      |
| Bul...             | Ctrl+F               |
| Diğer araçlar      | ►                    |
| Düzenle            | Kes Kopyala Yapıştır |
| Ayarlar            |                      |
| Yardım             | ►                    |
| Çıkış              |                      |

**Şekil 40:** Chrome’da menü seçenekleri

Chrome’da adres çubuğuna yazılan arama ifadeleri anlık sonuçlar döndürmektedir. Bu arama ifadelerine ve döndürülen sonuçlara Chrome adres çubuğundan “chrome://predictors/” linki ile erişilebilmektedir (Bkz. Şekil 41).

Autocomplete Action Predictor

Resource Prefetch Predictor

☐ Filter zero confidences

Entries: 26

| User Text | URL                                                                                                  | Hit Count | Miss Count | Confidence |
|-----------|------------------------------------------------------------------------------------------------------|-----------|------------|------------|
| m         | https://www.google.com/search?q=m&oq=m&aqs=chrome.69i57&sourceid=chrome&ie=UTF-8                     | 0         | 1          | 0          |
| ms        | https://www.google.com/search?q=ms&oq=ms&aqs=chrome.69i57&sourceid=chrome&ie=UTF-8                   | 0         | 1          | 0          |
| msn       | https://www.google.com/search?q=msn&oq=msn&aqs=chrome.69i57&sourceid=chrome&ie=UTF-8                 | 0         | 1          | 0          |
| msn.      | https://www.google.com/search?q=msn.&oq=msn.&aqs=chrome.1.69i57j0i5&sourceid=chrome&ie=UTF-8         | 0         | 1          | 0          |
| msn.      | https://www.google.com/search?q=msn+a%C3%A7&oq=msn.&aqs=chrome.2.69i57j0i5&sourceid=chrome&ie=UTF-8  | 0         | 1          | 0          |
| msn.      | https://www.google.com/search?q=msn+haber&oq=msn.&aqs=chrome.4.69i57j0i5&sourceid=chrome&ie=UTF-8    | 0         | 1          | 0          |
| msn.      | https://www.google.com/search?q=msn+kaydol&oq=msn.&aqs=chrome.3.69i57j0i5&sourceid=chrome&ie=UTF-8   | 0         | 1          | 0          |
| msn.      | https://www.google.com/search?q=msn+sign&oq=msn.&aqs=chrome.5.69i57j0i5&sourceid=chrome&ie=UTF-8     | 0         | 1          | 0          |
| msn.      | https://www.google.com/search?q=msn.&oq=msn.&aqs=chrome.69i57j0i5&sourceid=chrome&ie=UTF-8           | 0         | 1          | 0          |
| msn.c     | https://www.google.com/search?q=msn.&oq=msn.c&aqs=chrome.1.69i57j0i5&sourceid=chrome&ie=UTF-8        | 0         | 1          | 0          |
| msn.c     | https://www.google.com/search?q=msn+a%C3%A7&oq=msn.c&aqs=chrome.2.69i57j0i5&sourceid=chrome&ie=UTF-8 | 0         | 1          | 0          |
| msn.c     | https://www.google.com/search?q=msn+haber&oq=msn.c&aqs=chrome.4.69i57j0i5&sourceid=chrome&ie=UTF-8   | 0         | 1          | 0          |
| msn.c     | https://www.google.com/search?q=msn+kaydol&oq=msn.c&aqs=chrome.3.69i57j0i5&sourceid=chrome&ie=UTF-8  | 0         | 1          | 0          |
| msn.c     | https://www.google.com/search?q=msn+sign&oq=msn.c&aqs=chrome.5.69i57j0i5&sourceid=chrome&ie=UTF-8    | 0         | 1          | 0          |
| msn.c     | https://www.google.com/search?q=msn.c&oq=msn.c&aqs=chrome.69i57j0i5&sourceid=chrome&ie=UTF-8         | 0         | 1          | 0          |
| msn.co    | http://msn.co/                                                                                       | 0         | 1          | 0          |
| msn.co    | https://www.google.com/search?q=msn&oq=msn.co&aqs=chrome.3.69i58j69i57j0i4&sourceid=chrome&ie=UTF-8  | 0         | 1          | 0          |

**Şekil 41:** Chrome’da tahmin hizmeti verilerinin görüntülenmesi

Chrome ara yüzlerinden tüm tarayıcı verilerinin incelenmesi mümkün olmamaktadır. Örneğin Chrome<sup>81</sup>, önbellek verilerinin okunması için dâhili bir imkân sunmamaktadır.

Tarayıcı incelemelerinde bir takım zorluklarla karşılaşılabilir. Tarayıcı verilerinden delil aramada karşılaşılan zorluklar arasında özel tarama modları ve taşınabilir tarayıcılar da yer almaktadır. Özel tarama modlarının amacı, kullanıcıların tarayıcıyı kullandıkları makinede iz bırakmalarını engellemek ve/veya giriş yaptıkları web sitesi sunucularından kimliklerini saklamaktır (Aggarwal vd. 2010). Özel tarama modunun bıraktığı kalıntılar ise sadece bellek imajı alınarak incelenebilmektedir<sup>82</sup>. Bir taşınabilir depolama cihazında saklanan taşınabilir tarayıcıyı kullanarak internette gezilmesi durumunda, tarama oturumlarının bilgisayar yerine taşınabilir depolama cihazında saklanması daha olasıdır (Ohana ve Shashidhar 2013, 135). Taşınabilir depolama cihazları incelenirken taşınabilir

<sup>81</sup> Kullanılan Chrome tarayıcı versiyonu: 72.0.3626.121

<sup>82</sup> Bkz. “3.8. Uçucu Veriler” başlığı

tarayıcı uygulamasına rastlanması halinde, tarayıcı kayıtları çalıştırma klasöründe bulunabilmektedir.

Tarayıcılar üzerinden kullanılan yazılımlar çok çeşitlidir. Örneğin, e-posta hesapları Outlook, Thunderbird gibi istemci uygulamaları aracılığı ile kullanılabildiği gibi, Gmail Web, Owa gibi web uygulamaları üzerinden de kullanılmaktadır. Bir sonraki başlıkta değinileceği üzere Facebook, Whatsapp, Twitter gibi sosyal platformlar da, hem tarayıcılar, hem de masaüstü yazılımlar vasıtasıyla kullanılabilmektedir.

### 3.4. SOSYAL MEDYA VE SOHBET UYGULAMALARI

Taylor vd. (2014)’ne göre, sosyal medya uygulamalarının bilgisayar adli bilişim (computer forensics) çerçevesinde incelenmesinde yaygın olarak kullanılan kurallar bulunmamakla birlikte, bir sosyal medya uygulamasının bilgisayarın sabit diskinde bıraktığı delillere (tarayıcı önbelleğinde, tarayıcı geçmişinde vb.) geleneksel adli bilişim yöntemleri kullanılarak erişilebilmektedir.

Cusack ve Son (2012, 34)’ın, tarayıcı üzerinden sosyal medya kullanımından sonra oluşabilecek potansiyel kalıntıları belirttiği liste Tablo 4’te yer almaktadır.

| Yapı             | Tanımlama                                                      | Birincil Verinin Konumu                                             |
|------------------|----------------------------------------------------------------|---------------------------------------------------------------------|
| İnternet Geçmişi | Ziyaret edilen web sitelerinin URL’lerinin listesi             | Tarayıcı Veritabanı(ör:index.dat)                                   |
| Oturum           | Çerezler ve SNS etkileşimi ile yaratılan diğer oturum verileri | Tarayıcı profil dosyaları<br>Tarayıcı ön belleği                    |
| Web Sayfası      | Web sitesi verileri ve dosyaları, html gibi                    | Tarayıcı ön belleği<br>Pagefile.sys,hiberfil.sys ve ayrılmamış alan |
| Resimler         | resimler ve diğer görüntüler, jpeg gibi                        | Tarayıcı ön belleği<br>Pagefile.sys,hiberfil.sys ve ayrılmamış alan |
| Video            | Video dosyaları, flash video gibi                              | Tarayıcı ön belleği<br>Pagefile.sys,hiberfil.sys ve ayrılmamış alan |
| Mailler          | SNSs tarafından sağlanan elektronik mail                       | Çeşitli e-posta istemcisi verileri                                  |
| İndirmeler       | SNS’den indirilen materyaller                                  | Tarayıcı ön belleği<br>Geçici dosyalar<br>Ayrılmamış alan           |

**Tablo 4:** Sosyal medya delillerinin potansiyel konumları (Cusack ve Son 2012, 34)

Tarayıcı üzerinden kullanılan sosyal medya uygulamalarının bıraktığı kalıntılar, “3.3. Tarayıcı Verileri” başlığında bahsedilen yöntemlerle elde edilebilmektedir.

Sosyal medya uygulamalarının birçoğu, masaüstü yazılımları üzerinden kullanım imkânı da sunmaktadır. Masaüstü yazılımları ise kendilerine özgü kayıt dosyaları oluşturmaktadır. Örneğin Facebook ve Skype için Majeed vd. (2016) şu bilgileri vermektedir:

- Facebook Kalıntıları: Arkadaşlar, hikayeler, arkadaşlık istekleri, mesajlar ve çıkartmalar gibi bilgileri içeren SQLite veri tabanı dosyaları (Bkz Tablo 5), “C:\Kullanıcılar\[kullanıcı\_adı]\AppData\Local\Packages\Facebook.Facebook\_\LocalState\FacebookID\DB” konumunda bulunmaktadır.

|   | id               | thread_id         | body              | sender              | timestamp     |
|---|------------------|-------------------|-------------------|---------------------|---------------|
|   | Filter           | Filter            | Filter            | Filter              | Filter        |
| 1 | m_mid.1434780... | t_mid.14347806... | hello             | {"user_id":"1000... | 1434780608827 |
| 2 | m_mid.1434780... | t_mid.14347806... | Hi                | {"user_id":"1000... | 1434780651491 |
| 3 | m_mid.1434780... | t_mid.14347806... | check logss in db | {"user_id":"1000... | 1434780662715 |
| 4 | m_mid.1434780... | t_mid.14347806... | ok sure           | {"user_id":"1000... | 1434780668574 |

**Tablo 5:** Facebook “messages.db” veri tabanı (Majeed vd. 2016, 76)

- Skype Kalıntıları: “C:\Kullanıcılar\[kullanıcı\_adı]\AppData\Local\Packages\Microsoft.SkypeApp\_kzf8qxf38zg5c\LocalState” konumunda “main.db” adında bir veri tabanı bulunmaktadır. Konuşmanın yapıldığı katılımcıların arama süresi, isim ve *Skype ID*<sup>83</sup> bilgileri ile belirli zaman damgaları bu dosyaya kaydedilmektedir (Bkz. Tablo 6).

<sup>83</sup> Skype ID, Skype kullanıcısına ait tekil Skype Name bilgisidir.

| from_dispname | body_xml                                                        | timestamp  |
|---------------|-----------------------------------------------------------------|------------|
| anonymous xyz | Hello Haleemah Zia, I&apos;d like to add you as a contact.      | 1434788107 |
| Haleemah Zia  | NULL                                                            | 1434788133 |
| anonymous xyz | <partlist alt=""> <part identity="haleemah42">                  | 1434788228 |
| anonymous xyz | <partlist alt=""> <part identity="live:anonymous_investigator"> | 1434788244 |

**Tablo 6:** Skype “main.db” veri tabanı (Majeed vd. 2016, 77)

*SQLite* formatındaki verileri görüntülemeye, *SQLite Database Browser*, *SQLite Viewer* ve *SQLite Analyzer* yazılımları kullanılabilir (Hayes 2014, 344). Facebook ve Skype’a ait veri tabanlarının görüntülenmesi için bu yazılımlardan herhangi biri yeterli olmaktadır.

Sosyal medya web uygulamalarındaki sürekli değişen kayıtların masaüstü bilgisayarların kalıcı disklerinde saklanmaması, delillerin elde edilmesinde zorluklar çıkarmaktadır (Barradas vd. 2018, 3). Sosyal medya uygulamalarının birçok platformdan (masaüstü tarayıcı, mobil uygulama, masaüstü uygulama) ve istenilen cihazdan kullanılması delillerin kısa zamanda yok edilebileceği anlamına gelmektedir. Dolayısıyla, delillere el koymada hızlı davranmak gerekebilmektedir.

Kullanıcıların hem tarayıcılar hem de masaüstü uygulamalar üzerinden kullanabildiği başka hizmetler de bulunmaktadır. Bu bağlamda, bir sonraki başlıkta bulut depolama uygulamalarına değinilmektedir.

### 3.5. BULUT DEPOLAMA UYGULAMALARI

Bulut bilişim, bilgi işlem hizmetlerinin (sunucu, depolama, veritabanı, ağ, yazılım, analiz vb.) internet üzerinden hızlı, esnek ve ekonomik bir şekilde sunulmasıdır<sup>84</sup>.

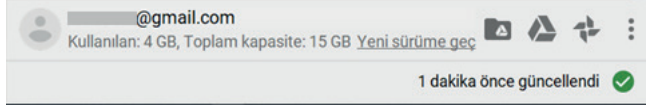
Bulut bilişim, paylaşımlı ve yapılandırılabilir bilgi işlem kaynaklarına (ağlar, sunucular, depolama birimleri, uygulamalar, hizmetler vb.) asgari yönetim çabası veya servis sağlayıcı etkileşimi ile her yerde ağ üzerinden erişimi mümkün kılan bir modeldir.

<sup>84</sup> Bkz. <https://azure.microsoft.com/tr-tr/overview/what-is-cloud-computing/> Erişim Tarihi: 22.12.2018

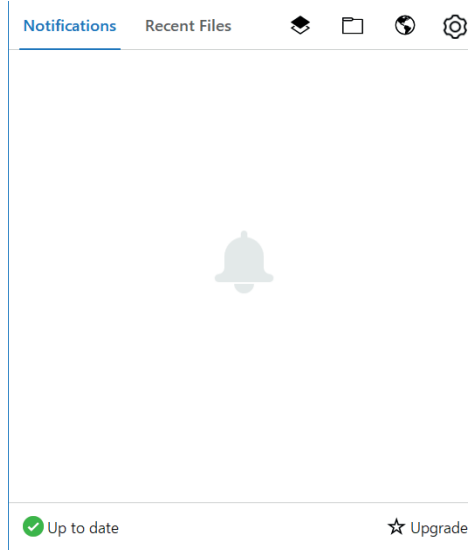


Bulut bilişimin son zamanlarda birçok teşebbüs ve kullanıcı tarafından tercih edilen bir model olması, büyük yatırımlar yapmak yerine yalnızca kullanılan kaynak kadar maliyet oluşturmaması, servis sağlayıcıların düşük ücretlerle hizmet vermesi, yüksek mobilite sağlaması, kolayca genişleyebilir olması ve güvenli olması gibi nedenler<sup>85</sup> sebebiyledir. Bulut bilişim yaygınlaştıkça, adli bilişim faaliyetlerinin bu yönde büyümesi ve incelemelerde yeni zorluklarla karşılaşılması, bulut bilişim ortamlarında da uzmanlaşmayı gerekli kılmaktadır (Ruan vd. 2011, 35).

Bulut bilişim özellikle sağladığı depolama hizmetleri ile son kullanıcıların bilgisayarlarında yer almaktadır. Google Drive (Bkz Şekil 42) ve Dropbox (Bkz Şekil 43), en çok kullanılan bulut depolama hizmetleri uygulamalarındandır.



**Şekil 42:** Google Drive yazılımı ara yüzü



**Şekil 43:** Dropbox yazılımı ara yüzü

<sup>85</sup> Bkz. <https://aws.amazon.com/tr/what-is-cloud-computing/>, <https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/> Erişim Tarihi: 23.12.2018

Uygulamalar bilgisayara kurulduğunda, varsayılan olarak sırasıyla “C:\Users\[KullanıcıAdı]\Google Drive” ve “C:\Users\[KullanıcıAdı]\Dropbox” klasörlerini oluşturarak bu klasörleri sunucuları ile senkronize etmektedir. Bu klasörler içerisine kopyalanan her dosya aynı zamanda bulut ortamında da tutulmaktadır. Bu sayede kullanıcılar, internet bağlantısı olan her yerden dosyalarına erişebilmektedir.

Senkronize edilen klasörlerden ve tarayıcı ara yüzünden silinen dosyalara, Dropbox’da üyelik planına göre 30-365 gün<sup>86</sup>, Google Drive’da ise 30 gün<sup>87</sup> içerisinde, tarayıcı ara yüzündeki “silinen dosyalar” menüsünden erişmek mümkündür.

Google Drive yazılımı bilgisayara kurulduğunda, “C:\Users\[kullanıcıadı]\AppData\Local\Google\Drive\” dizini içerisinde<sup>88</sup> “sync\_config.db” ve “snapshot.db” adında iki dosya oluşturmaktadır (Quick ve Choo 2014, 99). Bu iki dosya da *SQLite* formatındadır. “sync\_config.db” dosyası içerisinde Google Drive hesabına erişim sağlayan e-posta adresi ve bilgisayardaki senkronizasyon klasörü bilgileri bulunmakta, “snapshot.db” dosyasında da Google Drive’a yüklenen dosyaların adı, boyutu, oluşturulma ve değiştirilme tarihleri gibi bilgiler yer almaktadır (Quick ve Choo 2014, 99).

Dropbox kurulduğunda, “C:\Users\[kullanıcıadı]\AppData\Local\Dropbox” dizini altında<sup>89</sup> “filecache.dbx” dosyası oluşturulmaktadır. Şifreli “filecache.dbx” dosyasının verileri ise okunamamaktadır<sup>90</sup>.

İnceleme yapılan bilgisayarda, daha önce bulut depolama uygulamalarının ve diğer uygulamaların kullanılıp kullanılmadığı bilgisine, Windows Kayıt Defterinden erişilebilmektedir. İçerisinde çok çeşitli bilgiler barındırabilen Windows Kayıt Defterine bir sonraki başlıkta değinilmektedir.

---

<sup>86</sup> Bkz. <https://www.dropbox.com/help/security/deleted-files> Erişim Tarihi 24.12.2018

<sup>87</sup> Bkz. <https://support.google.com/a/answer/7376096?hl=en> Erişim Tarihi 24.12.2018

<sup>88</sup> Google Drive Versiyon 3.43.1584.4446 için “C:\Users\[kullanıcıadı]\AppData\Local\Google\Drive\user\_default” dizini altındadır.

<sup>89</sup> Dropbox Versiyon 63.4.107 için “C:\Users\[kullanıcı\_adı]\AppData\Local\Dropbox\instance1” dizini altındadır.

<sup>90</sup> Şifreli “filecache.dbx” dosyasını, Magnet Software web sitesine (2013) göre “IEF Triage” yazılımı yalnızca (imaj dosyalarında değil) canlı sistemlerde inceleme sırasında çözebilmektedir (Quick ve Choo 2013, 8).

### 3.6. WINDOWS KAYIT DEFTERİ

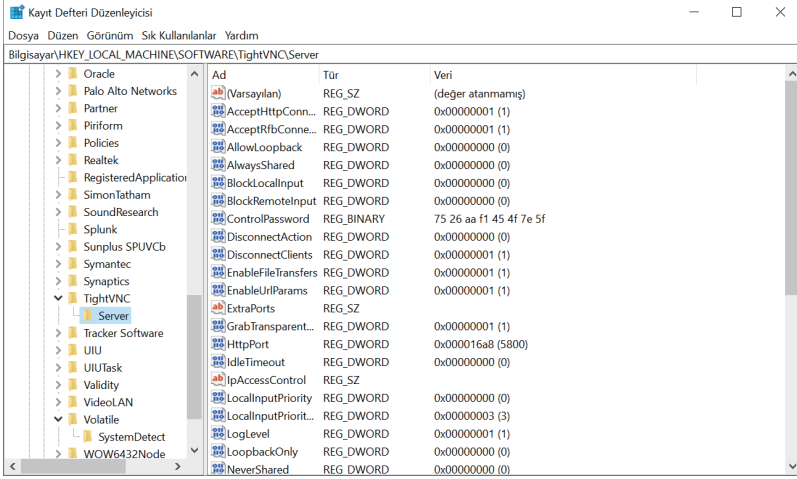
Windows Kayıt Defteri (Windows Registry), bir veya daha fazla kullanıcı için, uygulama ve donanım aygıtlarıyla ilgili sistem yapılandırılmasında ihtiyaç duyulan bilgileri depolamayı amaçlayan merkezi ve hiyerarşik bir veri tabanıdır (Carvey 2016, 15). Yapılandırma bilgilerinin yanı sıra, Windows Kayıt Defteri yakın zamanda erişilen dosyalarla ve kullanıcı etkinlikleriyle ilgili önemli bilgileri de tutar. Bu bilgiler, olayın niteliğine bağlı olarak son derece değerli olabilmektedir (Carvey 2009, 158).

Windows Kayıt Defteri şu bilgileri içermektedir<sup>91</sup>:

- HKEY\_CLASSES\_ROOT: Bu anahtara bağlı kayıt defteri girdileri, belge türlerini (veya sınıflarını) ve bu türlerle ilişkili özellikleri tanımlamaktadır.
- HKEY\_CURRENT\_USER: Bu anahtara bağlı kayıt defteri girdileri, mevcut kullanıcının tercihlerini tanımlamaktadır. Bu tercihler arasında ortam değişkenlerinin ayarları, yazılım grupları hakkında veriler, renkler, yazıcılar, ağ bağlantıları ve uygulama tercihleri bulunmaktadır.
- HKEY\_LOCAL\_MACHINE: Bu anahtara bağlı kayıt defteri girdileri, veri yolu türü, sistem belleği, kurulu donanım ve yazılım hakkındaki veriler gibi bilgisayarın fiziksel durumunu tanımlamaktadır. Tak ve Çalıştır bilgileri (sistemde bulunan tüm donanımların tam bir listesini içeren liste), ağda oturum açma tercihleri, ağ güvenliği bilgileri, yazılımla ilgili bilgiler (örneğin sunucu adları ve sunucu konumları) ve diğer sistem bilgileri de bu anahtar içerisinde yer almaktadır.
- HKEY\_USERS: Bu anahtara bağlı kayıt defteri girdileri, yerel bilgisayardaki yeni kullanıcılar için varsayılan kullanıcı yapılandırmasını ve geçerli kullanıcı için kullanıcı yapılandırmasını tanımlamaktadır.
- Windows Kayıt Defterinden bilgisayardaki yazılımların kullanım durumları ve özellikleri ile ilgili bilgiler edinilebilmektedir. Örneğin TightVNC yazılımının Windows Kayıt Defterindeki verilerine bakıldığında, günlük tutma seviyesi (LogLevel), dosya transferinin aktif olup olmadığı (EnableFileTransfers) gibi ayarları hakkında bilgi edinilmektedir (Bkz Şekil 44).

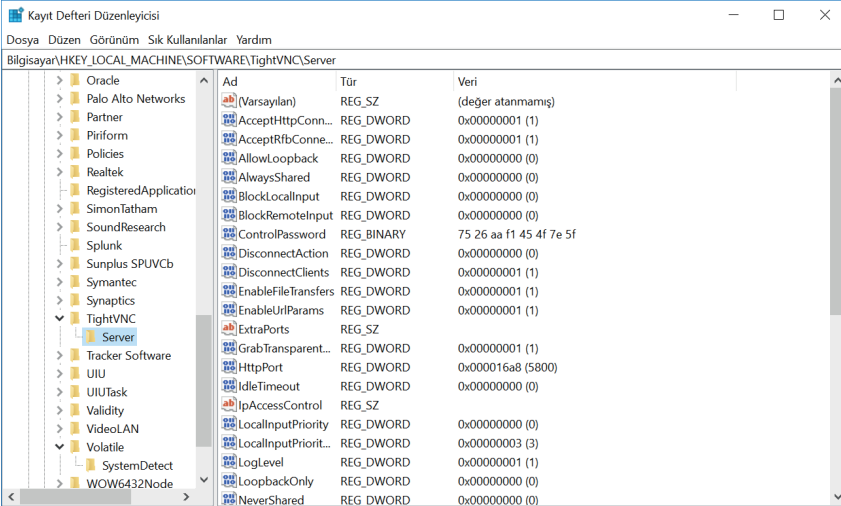
---

<sup>91</sup> <https://docs.microsoft.com/en-us/windows/desktop/sysinfo/predefined-keys> Erişim Tarihi: 12.01.2019



**Şekil 44:** Windows Kayıt Defterinin bilgisayarda yüklü bulunan bir yazılım (TightVNC) hakkında içerdiği veriler

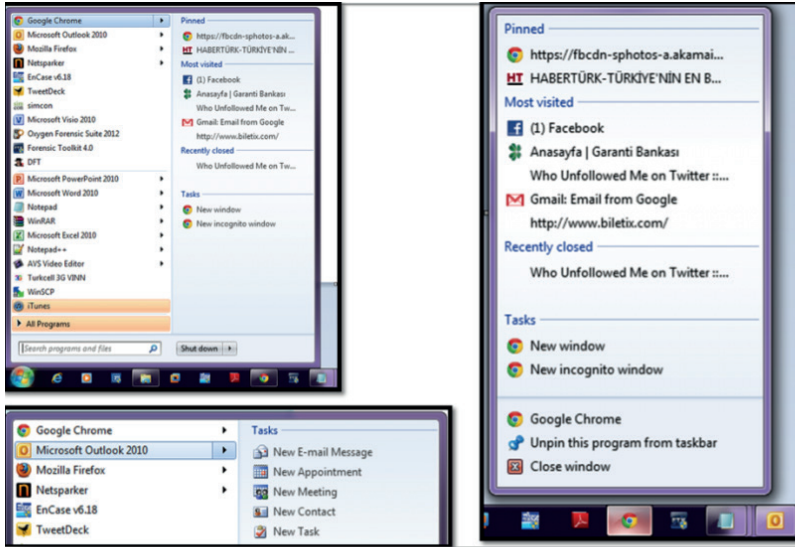
Windows Kayıt Defterindeki aktif kullanıcı hakkında tutulan kayıtlardan, bir yazılımı kullanıp kullanmadığı bilgisi de edinilebilmektedir. Şekil 45’de verilen bilgi, kullanıcının OneDrive isimli bulut depolama yazılımını kullandığını göstermektedir.



**Şekil 45:** Windows Kayıt Defterinde aktif kullanıcıya ait bazı kayıtlar

### 3.7. ATLAMA LİSTELERİ

*Atlama Listeleri (Jump Lists)* olarak adlandırılan ve Windows 7 ile gelen bir özellik sayesinde, yakın zamanda erişilen dosya ve klasörlerin kayıtları tutulmakta ve uygulama bazında gruplandırılmaktadır (Singh ve Singh 2016, 1) (Bkz. Şekil 46). *Atlama Listeleri*, *Başlat Çubuğu* veya *Görev Çubuğunda* sınırlı sayıda öge tutmakta, kaydedilen verilerin birçoğu görüntülenmemektedir. Ancak bazen yakın zamanda kullanıcının ne ile meşgul olduğu ve kullanılan son dosyaların bilgisine bu kayıtlardan erişmek mümkün olmaktadır.



**Şekil 46:** Farklı Windows uygulamalarına ilişkin *Atlama Listesi* örnekleri (kısa yollar üzerine fare (mouse) ile sağ tıklanmıştır)<sup>92</sup>

Değinildiği üzere Yİ'ler sırasında hiçbir yazılım kullanılmadan elde edilebilecek birçok veri bulunmaktadır. Ancak verilerin ortaya çıkarılması için, bir yazılım kullanmanın zorunlu olduğu bazı durumlar da olabilmektedir. Örneğin uçucu veriler ve silinen verilerin ortaya çıkarılması için yazılım kullanımına ihtiyaç vardır.

<sup>92</sup> <http://halilozturkci.com/windows-jump-list-forensics/> Erişim Tarihi: 12.01.2019

### 3.8.UÇUCU VERİLER

Sadece bilgisayar çalışırken mevcut olan, kapatıldığında kaybolan veriler uçucu verilerdir ve bu verilerin canlı sistem inceleme yöntemleri kullanılarak toplanması gerekmektedir (Daniel ve Daniel 2011, 26).

Yİ’lerde teşebbüs mülküne girilmesinden bilgisayarlarda incelemenin başlamasına kadar geçen sürede zaman kaybı yaşanmaktadır. Ayrıca bazı durumlarda (fazla sayıda çalışan olması, bulunan belgelerin içeriği vb.) ilk anda incelenmesi planlanmayan teşebbüs çalışanlarının bilgisayarları da daha sonra inceleme kapsamına alınabilmektedir. Geçen süre içerisinde bilgisayar kullanıcısı bilgisayardaki açık yazılımları kapatıp verileri silebilmektedir. Böyle durumlarda bellek incelemesi ile sistemin geçici olarak tuttuğu bu verilere kısmen ya da tamamen erişmek mümkün olabilmektedir. Dolayısıyla “bellek adli bilişimi” profesyonel incelemeler açısından artık bir seçenek değil zorunluluk haline gelmiştir (Shaaban 2016, 37).

Bellek incelemelerinden, e-posta ve anlık mesajlaşma uygulamalarının verileri gibi bazı hassas verilere ulaşmak mümkündür (Cai vd. 2013, 221). Ancak bu bilgilere erişmek için, belleğin tam kopyasının alınması ve alınan bu kopya üzerinde inceleme yapılması gerekmektedir.

### 3.9. SİLİNER VERİLER

Adli bilişim alanında silinen verileri kurtarma, herhangi bir vakanın en değerli işlemidir (Prajapati vd. 2015, 14).

Windows bilgisayarların varsayılan ayarlarında, bir veri silindiğinde ilk olarak geri dönüşüm kutusuna (recycle bin) düşmektedir<sup>93</sup>. Çıkarılabilir disklerdeki dosyalar, ağ sürücülerinden silinen dosyalar (kendi dosya sisteminde olsa bile), komut satırından silinen dosyalar ve sıkıştırılmış klasörlerden silinen dosyalar geri dönüşüm kutusuna gitmeden doğrudan silinmektedir (Bott 2016, 457).

---

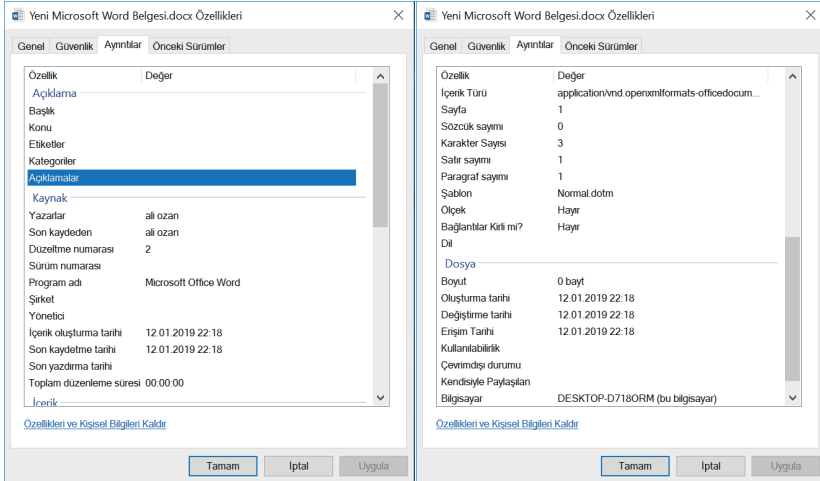
<sup>93</sup> Geri dönüşüm kutusuna sağ tıklanarak erişilebilen “özellikler” menüsünden, ilgili ayar değiştirilerek, bir veri silindiğinde geri dönüşüm kutusuna düşmeden doğrudan silinmesi sağlanabilmektedir.

Windows'ta ana dosya sistemi NTFS<sup>94</sup>'dir. NTFS'den bir dosya silmek, dosyanın kalıcı olarak silindiği anlamına gelmez (Oommen ve Sugathan 2016, 207). Bunun yerine dosya bilgileri<sup>95</sup> (küme üzerindeki yol, sektör bilgileri, oluşturma tarihi, değişiklik tarihi) silinmekte ve ücretsiz veya ticari bir üçüncü taraf yazılımının yardımı olmadan da bu dosyayı geri getirmek mümkün olmamaktadır (Nabity ve Landry 2015, 5). Dolayısıyla yedeklenmemiş veya başka bir yere de kaydedilmemiş durumdaki silinmiş verilere erişim sağlanmak isteniyorsa, yazılım kullanılması gerekmektedir.

### 3.10. DOSYA ÜST VERİ BİLGİLERİ

Bilgisayarlarda yapılan incelemeler sırasında bulunan belgelerin kim tarafından, ne zaman ve nerede oluşturulduğu bilgilerine ihtiyaç olabilmektedir. Böyle durumlarda, “veri hakkında veri” olarak tanımlanan üst veri bilgileri kullanılmaktadır.

Bir belgenin üst veri bilgisinden belgenin yazarı, oluşturulma tarihi, değiştirilme tarihi ve erişim tarihi, içerik türü, son kaydeden, yönetici ve bilgisayar adı gibi bilgilere erişilebilmektedir (Bkz. Şekil 47).



Şekil 47: Bir belgenin üst veri bilgileri

<sup>94</sup> Bkz. <https://docs.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview> Erişim Tarihi: 12.10.2019

<sup>95</sup> İşletim sistemi bu bilgileri tutmaktadır.

Üst veri bilgileri bazı durumlarda yararlı olmayabilir. Örneğin bir belge kopyalanıp başka bir yere yapıştırıldığında oluşturulma ve erişim tarihi değişmekte değiştirme tarihi, sahibi ve bilgisayar alanları aynı kalmaktadır. Bir belge içerisinden “farklı kaydet” yapılarak başka bir konuma kaydetme işlemi yapılırsa bu durumda üst verideki oluşturma, değiştirme ve erişim tarihi belgenin yapıştırıldığı zamanı göstermektedir.

Sunucu sistemlerinde ve kullanıcı bilgisayarlarında yapılan incelemenin sonunda “elde etme” aşamasına geçilmektedir. Bir sonraki bölümde, Yİ süreçlerinin “elde etme” aşamasından bahsedilmekte ve diğer hususlara yer verilmektedir.



## **BÖLÜM IV**

# **Yİ'NİN SON AŞAMALARI, DİĞER HUSUSLAR VE Yİ AKIŞ ŞEMASI ÖNERİSİ**

Yİ'lerde, sunucu sistemleri ve kullanıcı bilgisayarlarında bulunan delillere çeşitli şekillerde el koyulmakta, ardından deliller bir kopyası teşebbüse bırakılarak Kurum'a getirilmektedir.

Bu bölümde, delillere el koyma yöntemlerine ve el koyulan verilerin alınmasına yer verilmektedir. Bölümde, adli bilişim yazılımlarının gerekliliği ve Yİ sırasında kullanımları ile ilgili önerilere de yer verilmektedir. Ardından diğer ülke uygulamalarına göz atıldıktan sonra bölümün son kısmında bir Yİ süreci akış şeması ortaya koyulmaktadır.

### **4.1. ELDE ETME**

Yİ açısından elde etme aşaması, delillere el koyulması, bu delillerin uygun şekilde alınması ve güvenli bir yöntemle taşınması adımlarını içermektedir.

#### **4.1.1. Delillere El Koyma Yöntemleri**

Yİ sırasında, birçok farklı veri kaynağından, çeşitli formatlardaki delillere el koymak gerekebilmektedir. Bunlar arasında e-postalar, veri tabanları, ofis belgeleri, tarayıcı verileri, uygulama verileri, resimler gibi belge türleri bulunmaktadır. Bazı kaynaklardaki delillere el koyarken birden çok yöntem kullanmak mümkün olabilmektedir.

Yİ sırasında e-posta hesabı incelemeleri Outlook, ThunderBird gibi istemci yazılımlar üzerinden veya herhangi bir tarayıcı üzerinden gerçekleştirilebilmektedir. İstemci yazılımları, e-postaları kendine özgü formatlarda tutmaktadır. Örneğin

Outlook, e-postaları kendi oluşturduğu “.pst” ve “.msg” uzantılı dosyalarda tutmaktadır.

Outlook'ta herhangi bir e-postaya el koyarken, yazıcıdan yazdırma, e-postayı tamamen kopyalama, PDF formatına çevirip alma ya da e-postanın ekran görüntüsünü alma yöntemleri izlenebilmektedir. E-postanın kopyalanıp<sup>96</sup> alınması durumunda, e-postalar MSG formatında alınmaktadır. Böylece e-posta, ekleriyle<sup>97</sup> beraber kaydedilmektedir. Diğer yöntemlerde e-posta, tek bir dosyada ekleriyle beraber alınamamaktadır.

E-posta hesabı tarayıcı üzerinden inceleniyorsa, buradan Outlook'taki gibi kopyalama işlemi ile MSG formatında alınması mümkün olmamaktadır. Bu durumda ilgili e-posta, “yazdır” seçeneğinden PDF olarak kaydedilebilmekte ya da ekran görüntüsü alınabilmektedir. Ancak bu iki yöntemde de, eklerin de ayrı olarak indirilip alınması gerekmektedir.

Yırasında zaman zaman veri tabanı verilerine el koymak da gerekebilmektedir. Veri tabanları genellikle barındırdığı verileri çeşitli formatlarda (CSV, XLS, TXT, XML vb.) dışarı aktarma imkânı sunmaktadır. Örneğin çok kullanılan MySQL, SQL Server, PostgreSQL ve Oracle veri tabanları, ya ekstra araçlarla ya da dâhili araçlarla verileri birçok formatta dışarı aktarma imkânı vermektedir.

Veri tabanlarından alınan verilerin büyük miktarda<sup>98</sup> olması ve SQL harici formatlarda (Excel uyumlu formatlar vb.) alınması, daha sonra verilerin işlenmesi ve analiz edilmesi sırasında zorluklara<sup>99</sup> sebebiyet verebilmektedir. Bu yüzden veri tabanı verilerine el koyarken, SQL komutlarının yardımı ile veri tabanı tablolarındaki veriler filtrelenerek istenilen veri setine el koyma işlemi gerçekleştirilebilir.

Bir başka veri kaynağı olan tarayıcılarda ise karşılaşılan veri formatları çok çeşitli olabilmektedir. Tarayıcılar üzerinde inceleme yaparken, başka bir cihaz

<sup>96</sup> Kopyalama işlemi, Outlook istemci yazılımından fare'nin sağ tık hareketiyle açılan menüden veya klavyeden “CTRL + C” tuş kombinasyonu ile yapılabilmektedir.

<sup>97</sup> El koyma işlemi sırasında, eklerin başka sunucularda olup olmadığına dikkat etmek gerekmektedir. E-postaların alınıp Kurum'a getirildikten sonra incelenmesi sırasında, başka sunucuda barındırılan eklerin açılmaması ihtimali bulunmaktadır.

<sup>98</sup> Örneğin üç yüz bin satırlık veri.

<sup>99</sup> Örneğin Excel uyumlu formatlarda, birkaç yüz bin satır veriden sonra, verinin işlenmesi ciddi şekilde yavaş olabilmektedir.

üzerinden yapılan bir müdahale<sup>100</sup> ile incelenen verilerde değişiklik meydana gelebileceğinden ve verilere erişimin kesilmesinden sonra tekrar erişilememesi ihtimali de bulunduğundan dolayı verilere hızlı bir şekilde el koyma işleminin gerçekleştirilmesi gerekebilmektedir. Tarayıcı verilerine el koyulurken, incelenen web sayfasını kaydetmek, ekran görüntüsü almak, video çekmek veya yazıcıdan çıktı olarak almak gibi alternatiflerden birisi kullanılabilir. Windows'ta dâhili araçlarla<sup>101</sup> ekran görüntüsü alınabilmektedir. Ancak bir web sayfası büyük boyutta ve sayfalarca veri içeriyorsa, ekran görüntüsü alma işlemi zor olabileceğinden, söz konusu web sayfasının tamamen kaydedilmesi<sup>102</sup> yöntemine de başvurulabilmektedir.

Delillere el koyma işlemi tamamlandıktan sonra, delil zinciri içerisinde yer alan “hash alma” aşamasına geçilmektedir.

#### 4.1.2. Hash Alma

Teşebbüs bilgisayarlarından alınıp Kurum'a getirilen verilerin sonradan bir değişikliğe uğramadığının kanıtlanabiliyor olması, delil zincirinin sağlanması için gereklidir. Bu amaçla kullanılabilen hash alma işlemi, girdi olarak isteğe bağlı miktarda verilen verinin, sabit boyutlu bir dize olarak çıktı alınmasıdır (Altheide ve Carvey 2011, 56). Çıktı verisi, girdi olarak verilen verinin karıştırılması ile elde edilmiş bir karakter dizisidir.

Yİ sonunda, incelenen bilgisayarlardaki verilerin ayrı ayrı hash değerini almak yerine, veriler bir araya getirilerek toplu bir hash alma işlemi yapılabilir. Bu sayede kısa sürede hash değeri alınabilmektedir.

Hash almak için MD5 ve SHA1 algoritmaları<sup>103</sup> kullanılabilir<sup>104</sup>. Bu

<sup>100</sup> Tarayıcılardaki bazı uygulamaların birçok cihazdan erişim imkânı sunduğuna üçüncü bölümde değinilmişti. Örneğin bir bulut depolama uygulaması, hem tarayıcıdan hem masaüstü uygulamadan hem de mobil uygulamadan kullanılabilir. İstemcideki verilerde yapılan bir değişiklik, tarayıcıdaki verilere erişim olanağını ortadan kaldıracaktır.

<sup>101</sup> Windows'ta dâhili ekran görüntüsü alma aracı (snipping tool) kullanılabilir.

<sup>102</sup> Tarayıcının sunduğu “sayfayı kaydet” işlevi veya klavyeden yapılan “CTRL +S” tuş kombinasyonu, kaydetme işlemi için kullanılabilir.

<sup>103</sup> Algoritma, iyi tanımlanmış kuralların ve işlemlerin adım adım uygulanmasıyla bir sorunun giderilmesi veya sonuca en hızlı biçimde ulaşılması işlemidir. Bkz. <http://sozluk.gov.tr/> Erişim Tarihi: 02.02.2019

<sup>104</sup> MD5 ve SHA1, adli bilişim incelemelerinde yaygın olarak kullanılan hash alma algoritmalarıdır.

işlem için Windows 7 ve Windows 10’da dâhili bulunan CertUtil<sup>105</sup> <sup>106</sup> aracından faydalanılabilmektedir (Bkz. Şekil 48). Hash almak için “CertUtil [Seçenekler] -hashfile InFile [HashAlgoritması]” komutu kullanılabilmektedir. Örneğin “CertUtil -hashfile tez-rekabet-incelemesi.zip sha1” komutu, “tez-rekabet-incelemesi” adlı *zip* dosyasının SHA1 hash algoritmasına göre hash değerini vermektedir.

```

Komut İstemi

C:\Users\ALIOZAN\Desktop>certutil -hashfile -?
Usage:
  CertUtil [Options] -hashfile InFile [HashAlgorithm]
  Generate and display cryptographic hash over a file

Options:
  -Unicode           -- Write redirected output in Unicode
  -gmt               -- Display times as GMT
  -seconds           -- Display times with seconds and milliseconds
  -v                -- Verbose operation
  -privatekey        -- Display password and private key data
  -pin PIN           -- Smart Card PIN
  -sid WELL_KNOWN_SID_TYPE -- Numeric SID
                        22 -- Local System
                        23 -- Local Service
                        24 -- Network Service

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

CertUtil -?           -- Display a verb list (command list)
CertUtil -hashfile -? -- Display help text for the "hashfile" verb
CertUtil -v -?        -- Display all help text for all verbs

C:\Users\ALIOZAN\Desktop>certutil -hashfile tez-rekabet-incelemesi.zip md5
MD5 hash of tez-rekabet-incelemesi.zip:
bfb4b2b6944c71893622564892d43e26
CertUtil: -hashfile command completed successfully.

C:\Users\ALIOZAN\Desktop>certutil -hashfile tez-rekabet-incelemesi.zip sha1
SHA1 hash of tez-rekabet-incelemesi.zip:
1a1a1c2baa577d31f84ee06e58713b2d546e1341
CertUtil: -hashfile command completed successfully.

C:\Users\ALIOZAN\Desktop>

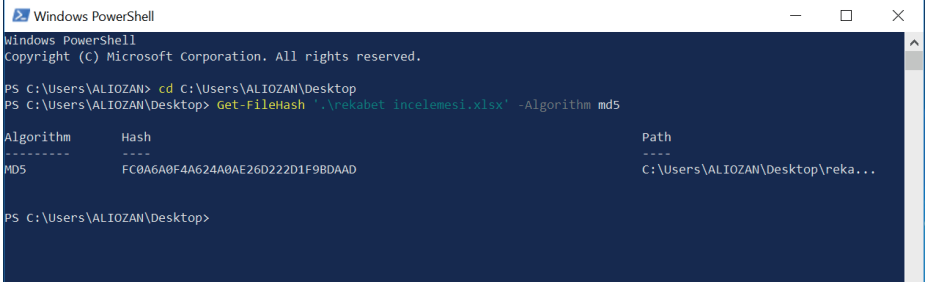
```

Şekil 48: CertUtil aracı ile hash alma

Windows üzerinde bir başka komut satırı aracı olan Powershell ile de hash alınabilmektedir (Bkz. Şekil 49). “Get-FileHash ‘.\rekabet\_incelemesi.xlsx’ -Algorithm md5” komutu ile “.\rekabet\_incelemesi.xlsx” adlı belgenin MD5 hash’i alınabilmektedir.

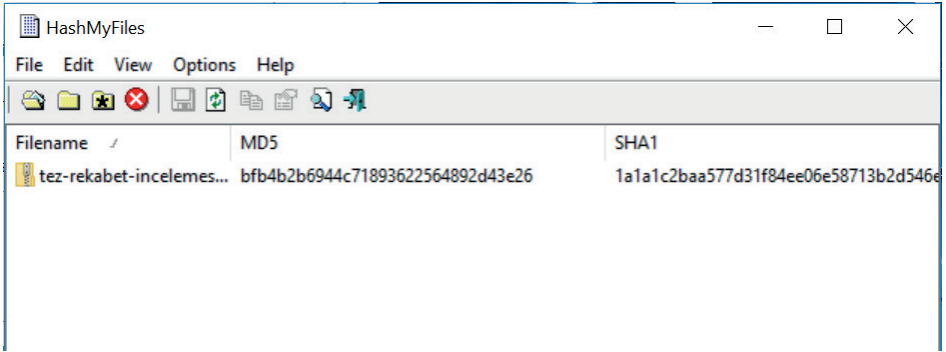
<sup>105</sup> Bkz. <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil> Erişim Tarihi: 02.02.2019

<sup>106</sup> Bu araç ile bir klasörün hash değeri alınmak istendiğinde hata alınmaktadır. Klasör sıkıştırılarak (zip) hash alma işlemi ise başarı ile gerçekleştirilebilmektedir.



**Şekil 49:** Powershell ile hash alma

Ayrıca komut satırı kullanımı gerektirmeyen, görsel kullanıcı ara yüzüne sahip HashMyFiles<sup>107</sup> gibi bir yazılım da hash almak için kullanılabilir (Bkz. Şekil 50).



**Şekil 50:** HashMyFiles yazılımı ile hash alma

El koyulan veriler için MD5 ve SHA1 değerlerinin her ikisinin de hesaplanması hash değerlerinin tutarlılığını arttırmaktadır. Çünkü çok nadiren de olsa farklı girdilerin aynı MD5 değerlerini üretebilme ihtimali olduğu kanıtlanmıştır<sup>108</sup>.

Yİ sonrası hash değeri alınan veriler DVD'ye veya USB belleğe kopyalanmaktadır. Ayrıca hash değerleri de bir metin belgesine kaydedilerek aynı DVD veya USB'ye alınmaktadır.

<sup>107</sup> [https://www.nirsoft.net/utils/hash\\_my\\_files.html](https://www.nirsoft.net/utils/hash_my_files.html) Erişim Tarihi: 02.02.2019

<sup>108</sup> Detaylı bilgi için bkz. <https://www.mscs.dal.ca/~selinger/md5collision/> Erişim Tarihi: 02.02.2019

### 4.1.3. Şifreleme Ve Taşıma

Yİ sonrası teşebbüsten alınan veriler Kuruma getirilmektedir. Taşınabilir verilerin şifrelenmemesi, verilerin ifşa edilmesi riskini barındırmaktadır (Knott ve Steube 2011, 21). Bu yüzden verilerin kabul görmüş bir şifreleme yöntemi ile şifrelenerek taşınmasına ihtiyaç bulunmaktadır.

Yİ sonunda hash değeri alınan verilerin taşınması için DVD veya USB bellek kullanılabilir. İki yöntemin birbirlerine göre avantaj ve dezavantajları vardır.

Windows 7 ile tanıtılan bir özellik olan BitLocker To Go ile bir USB belleğin (sürücünün) tüm içeriği şifrelenebilmekte, cihazın kayıp olması veya çalınması durumunda ise verilere şifre olmadan erişilememektedir (Bott vd. 2016, 455).

Windows 10'da bilgisayara takılan USB belleğe sağ tıklanmasıyla gelen menüden BitLocker'ı Aç seçeneği ile taşınabilir bir USB bellek şifrelenebilmektedir. Bu işlemde, USB belleğin açılması sırasında kullanılacak bir parola belirlenmekte (Bkz. Şekil 51) ve ardından parolanın unutulması halinde şifrelenmiş veriye erişmekte kullanılabilen kurtarma anahtarı oluşturulmaktadır.

**Şekil 51:** BitLocker ile sürücü şifreleme sırasında parola belirlenmesi

DVD’ler Bitlocker ile şifrlenmeye imkân vermemektedir. Ancak el koyulan belgeler yazılımlar aracılığı ile şifrlenerek<sup>109</sup> DVD’ler de güvenli bir taşıma aracı olarak kullanılabilir.

DVD’lerin içeriği silinmeye karşı korumalı olarak ayarlanabiliyorken<sup>110</sup>, bir USB bellek bilgisayara takıldığında bilgisayardaki çeşitli yazılımlar, herhangi bir onay beklemeden USB belleğin içeriğini silebilmektedir.

## 4.2. SUNUM

Elde etme aşamasının ardından Kurum’a getirilen verilerin okunması ve anlamlandırılması için çeşitli işlemlerin yapılmasına ihtiyaç duyulabilmektedir.

Alınan veriler arasında sadece belirli yazılımların açabileceği dosyalar bulunabilmektedir. Örneğin PST ve MSG formatlı dosyaların okunması için Outlook kullanılmaktadır. HTML formatlı dosyalar herhangi bir tarayıcı ile açılabilir. XML gibi metin tabanlı olan ve kendine özgü bir yapısı bulunan dosyalar ise genelde metin belgelerini açabilen herhangi bir yazılım ile okunabilmektedir.

El koyulan veriler arasında binlerce satırlık veriler içeren Excel formatında belgeler bulunabilmektedir. Ya da binlerce satırdan oluşan veri tabanı verileri de olabilmektedir. Bu durumda, verilerin anlamlı hale getirilmesi için bazı işlemlere ihtiyaç olmaktadır. Excel verileri, Excel yazılımının sunduğu araçlar ile düzenlenebilmektedir. Veri tabanından alınan veriler için ise SQL dili yardımı ile istenilen düzenlemeler gerçekleştirilebilmektedir.

## 4.3. ADLİ BİLİŞİM YAZILIMLARI İLE İNCELEME

Adli bilişim incelemelerinde bilgisayarlar üzerindeki aramaları kolaylaştıran, insan gücüyle yakalanması çok zor olan delilleri ortaya çıkarabilecek ve oldukça

---

<sup>109</sup> Örneğin ZIP formatlı belgeler 7zip veya Winrar gibi bir programla şifrelenebilir. Ancak burada dikkat edilmesi gereken husus şifreleme işleminin hash alma işleminden sonra yapılmasıdır. Çünkü şifreleme işlemi, aynı belgeye aynı şifre verilmesi halinde dâhi farklı hash değerleri alınmasına sebep olmaktadır.

<sup>110</sup> Bir DVD ilk yazma işlemi sırasında tekrar yazılabilir olarak ya da tekrar yazmaya kapalı olarak ayarlanabilmektedir.

zaman kazandırabilecek yazılımlar kullanılmaktadır. Bazıları canlı sistemler üzerinde kullanılmakta iken, bazıları ise alınan imajlar üzerinde inceleme yapmakta kullanılmaktadır. İmajlar üzerinden inceleme yapmak için özelleşmiş birçok yazılım (Nuix, Encase, X-Ways Forensics vb.) bulunmaktadır. Bu yazılımlar gelişmiş işlevler sunmaktadır. Ancak daha önce de değinildiği üzere, Yİ'lerde imaj alma işlemine yer verilmemektedir. Dolayısıyla ihtiyaç halinde Yİ'lerde adli bilişim yazılımlarının kullanılması noktasında geleneksel adli incelemelerden farklı bir tutum sergilenebilir.

Yİ'lerde incelenen bilgisayarlarda bulunan dosyaların açılmaması durumunda, dosyalar bir başka bilgisayara aktarılarak inceleme yapılabilmektedir. Bu noktada adli bilişim araçlarından yararlanılması mümkün olabilir.

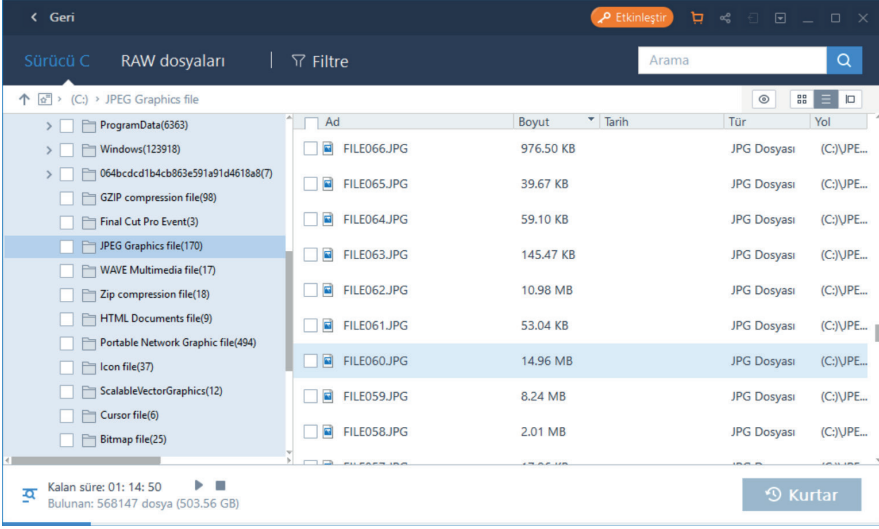
Yİ'lerde adli bilişim yazılımlarının kullanılması için bir başka seçenek, bilgisayara takılan bir USB bellek içerisinden çalıştırılan adli bilişim yazılımlarının (taşınabilir uygulamalar) kullanılması olabilir. Ancak teşebbüslerde politika gereği bilgisayarlardaki USB girişleri pasif olan veya kurulu güvenlik yazılımının USB bellek üzerinden yazılım çalıştırılmasının engellendiği durumlarda, bu yöntemin kullanılması bazı izinler veya işlemler gerektirebilir<sup>111</sup>.

Yİ sırasında silinen dosyaların kurtarılması (Bkz. Şekil 52), bilgisayarda gerçekleştirilen son işlemlerin görüntülenmesi (Bkz. Şekil 53), tarayıcı geçmişlerinin görüntülenmesi (Bkz. Şekil 54), arama motorlarından yapılan son aramaların görüntülenmesi (Bkz. Şekil 55) vd. işler için taşınabilir uygulamalar kullanılabilir.

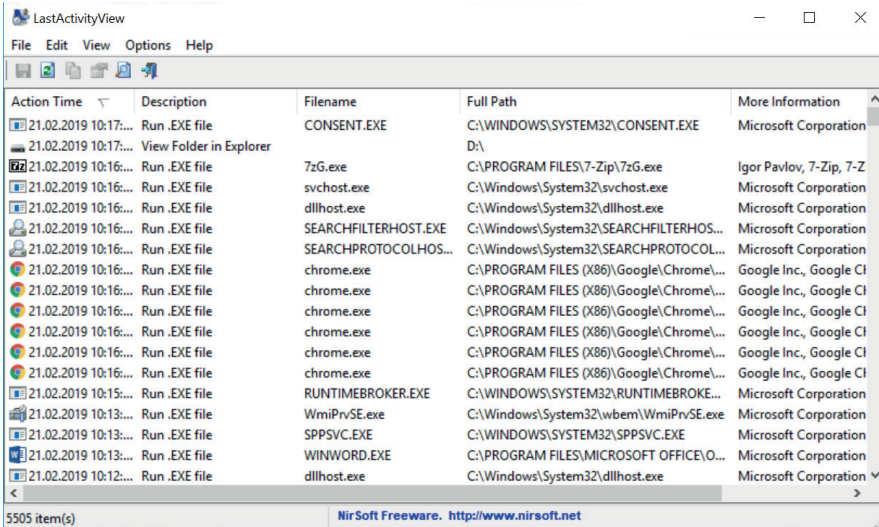
---

<sup>111</sup> Bazı durumlarda (USB portlarının aktif edilemeyecek durumda olması veya USB portlarının mevcut olmaması vb.) USB bellek üzerinden yazılım çalıştırmanın mümkün olamayacağı da düşünülmektedir.

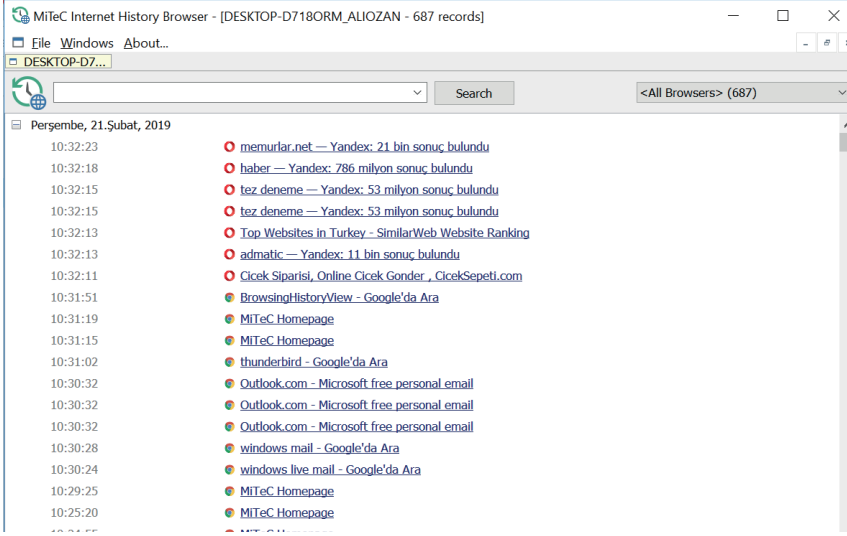




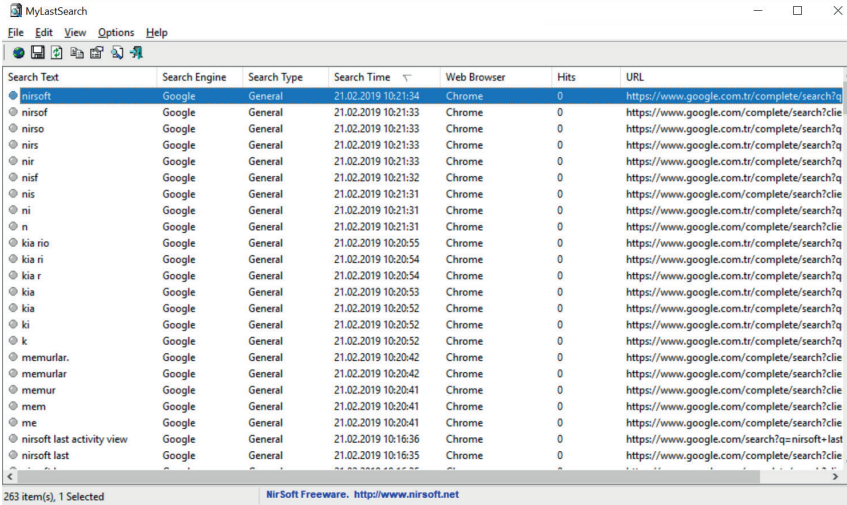
**Şekil 52:** USB bellek üzerinden çalıştırılan EaseUS Data Recovery yazılımı ile silinmiş öğelerin kurtarılması



**Şekil 53:** USB bellek üzerinden çalıştırılan Nirsoft LastActivityView yazılımı ile bilgisayarda gerçekleştirilen son işlemlerin görüntülenmesi

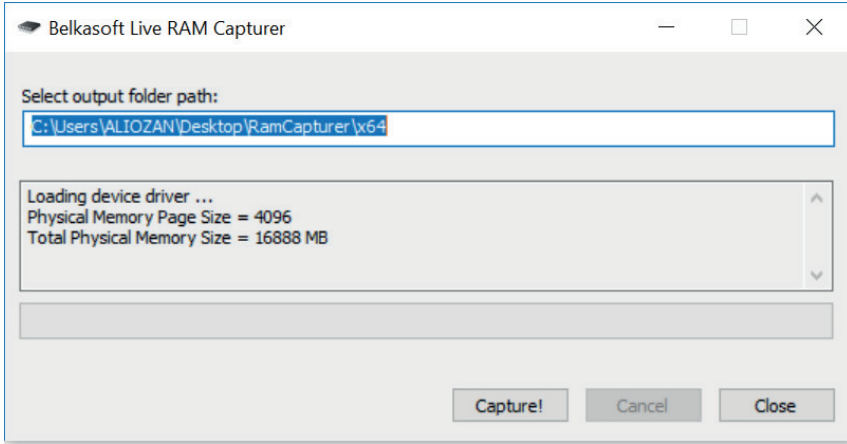


**Şekil 54:** USB bellek üzerinden çalıştırılan MiTec İnternet History Browser yazılımı ile bilgisayarda kullanılan tüm tarayıcıların geçmişlerinin görüntülenmesi

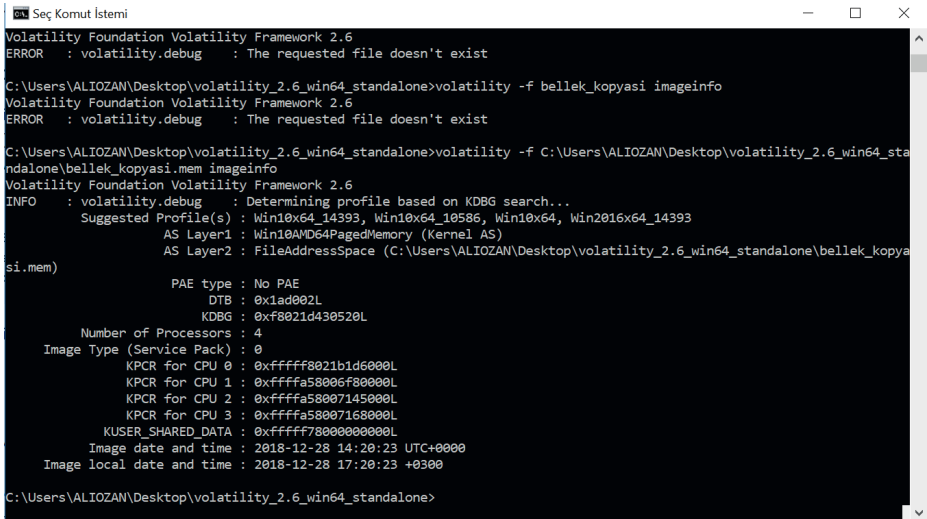


**Şekil 55:** USB bellek üzerinden çalıştırılan NirSoft MyLastSearch yazılımı ile tarayıcılarda arama motorlarından yapılan son aramaların görüntülenmesi

Bellek verilerini elde etmek gibi daha gelişmiş işlemler için de taşınabilir uygulamalar kullanılabilmektedir. Belkasoft Live RAM Capturer<sup>112</sup> yazılımı bir USB cihaz üzerinden kullanılabilmekte (Bkz. Şekil 56) ve elde edilen veriler de Volatility<sup>113</sup> yazılımı ile incelenebilmektedir (Bkz. Şekil 57).



Şekil 56: Belkasoft Live RAM Capturer Yazılımı ile Bellek İmajı Alma



Şekil 57: Volatility ile bellek imajı inceleme

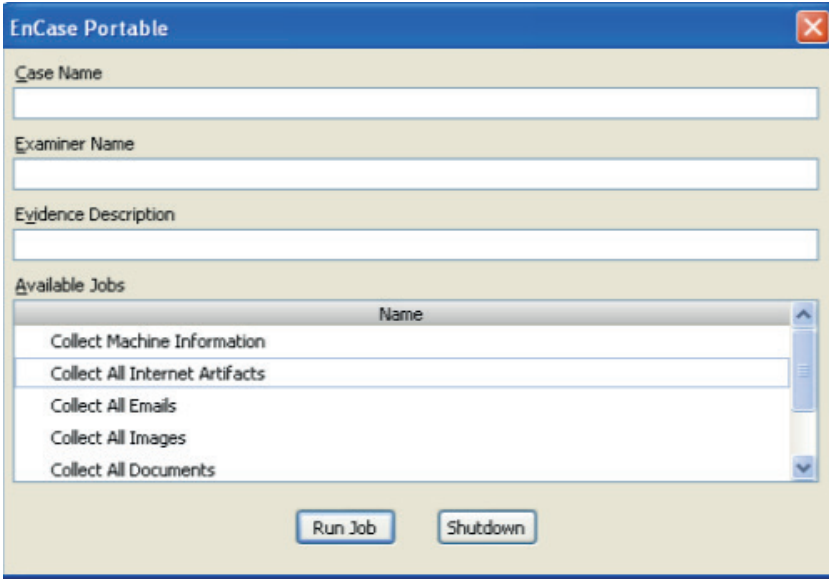
<sup>112</sup> <https://belkasoft.com/ram-capturer> Erişim Tarihi: 28.12.2018

<sup>113</sup> <https://www.volatilityfoundation.org/> Erişim Tarihi:28.12.2018

Volatility ve eklentileri<sup>114</sup> kullanılarak, imaj dosyasından çıkarılabilecek bilgilerde bazıları şunlardır:

- Çeşitli Windows Kayıt Defteri verileri,
- İnternet Explorer geçmiş ve ön bellek verileri,
- Chrome, Firefox tarayıcılarına ait geçmiş, çerez ve indirme bilgileri gibi veriler,
- Çalışan yazılımların ve sistemin tuttuğu çeşitli veriler.

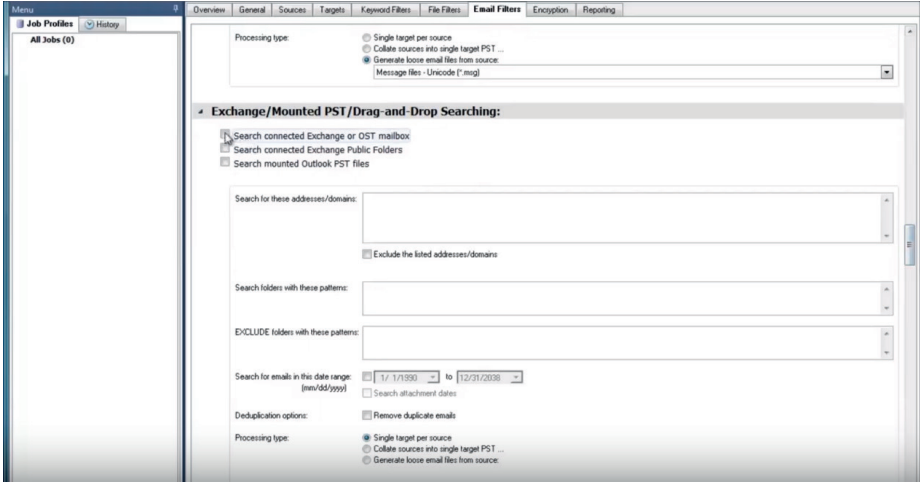
Encase Portable (Bkz. Şekil 58), Harvester Portable Edition (Bkz. Şekil 59), Nuix Portable Collector (Bkz. Şekil 60) gibi uygulamalar ise USB bellek üzerinden çalıştırılarak inceleme yapılan bilgisayarda hızlı veri (e-postalar, belgeler vb.) toplamak, imaj almak veya arama yapmak gibi görevler için kullanılabilmektedir<sup>115</sup>.



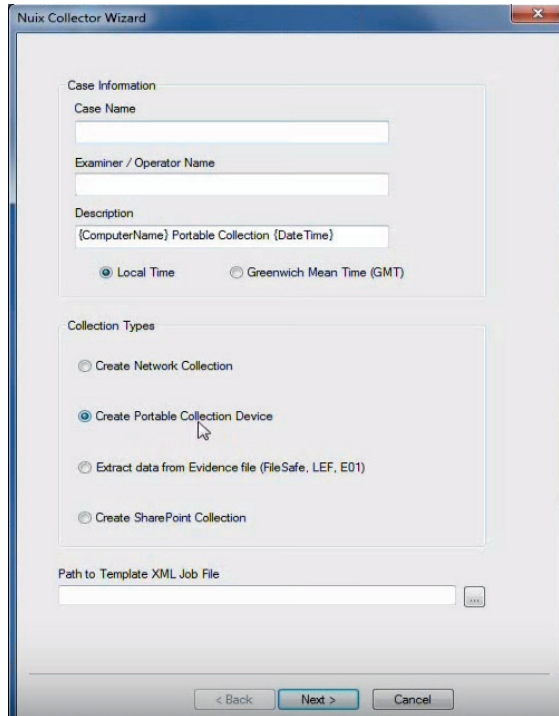
**Şekil 58:** Encase Portable Collector yazılımı

<sup>114</sup> Topluluk tarafından geliştirilen eklentilere şu adresten erişilebilmektedir: <https://github.com/volatilityfoundation/community>

<sup>115</sup> Yazılımların karşılaştırmaları için bkz. <https://www.forensicsmag.com/product-release/2010/09/collection-tool-comparison> Erişim Tarihi: 20.02.2019



Şekil 59: Harvester Portable Edition yazılımı



Şekil 60: Nuix Portable Collector yazılımı

Yİ'lerde kullanılabilecek birçok yazılım ürünü bulunmaktadır. Kurum'un belirleyeceği sınırlar çerçevesinde bu yazılım ürünlerinden faydalanılabileceği değerlendirilmektedir.

#### 4.4. DİĞER ÜLKE UYGULAMALARI

Yİ'lerin gerçekleştirilmesinde, Komisyon ve Avrupa Birliği üyesi ülkelerdeki tutum ile Kurum'un tutumu arasında farklılıklar bulunmaktadır.

Rekabet kurallarının uygulanmasına ilişkin 1/2003<sup>116</sup> sayılı Komisyon Tüzüğü'nün, Komisyon'un denetim yetkilerini ele alan 20. maddesine bakıldığında; Komisyon'un teşebbüs ve teşebbüs birliklerinin tüm mülklerindeki her türlü belgeyi inceleyebileceği, kopyasını alabileceği, denetim için gerekli ölçüde mühürlenebileceği ve belgeler hakkında açıklama isteyebileceği belirtilmektedir. Tüzüğün 20. Maddesinin 4. Fıkrasına (teşebbüslerin Komisyon tarafından verilen kararlara uymasının gerekli olduğunu belirtmektedir) istinaden çıkarılan Açıklayıcı Nota (Explanatory Note)<sup>117</sup> göre ise;

- Yİ'yi gerçekleştiren uzmanların, işle ilgili her türlü belgeyi, depolandıkları ortama bakılmaksızın inceleme ve kopyalarını alma hakkı vardır (Madde 9).
- Yİ'yi gerçekleştirilen uzmanlar, teşebbüs sistemlerinin ve verilerinin bütünlüğüne dikkat ederken verilerin kopyalanmasını, aranmasını ve kurtarılmasını sağlayan kendilerine ait yazılım ve/veya donanımları da kullanabilir (adli bilişim araçları) (Madde 10).
- Teşebbüsün, sahip olduğu bilişim sistemi hakkında açıklama yapma, Yİ uzmanlarına yardımcı personel temin etme, çalışan bilgisayarların geçici olarak ağ bağlantısını kesme, sabit sürücülerini bilgisayarlardan çıkarma/takma ve yönetici erişim hakları desteği sağlama gibi yükümlülükleri bulunmaktadır. Ayrıca Yİ uzmanları, teşebbüs tarafından sağlanan

---

<sup>116</sup> Bkz. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0001:EN:HTML>, Erişim Tarihi: 09.12.2018.

<sup>117</sup> Bkz. [http://ec.europa.eu/competition/antitrust/legislation/explanatory\\_note.pdf](http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf), Erişim Tarihi: 09.12.2018.

donanımı (örneğin, sabit disk DVD, USB bellek, bağlantı kabloları, tarayıcılar, yazıcılar) kullanmayı isteyebilir, ancak teşebbüsün donanımını kullanmak zorunda değildir (Madde 11).

Yıldız'ın (2014) çalışmasının üçüncü bölümünde yer verdiği, Avrupa Birliği üyesi ülkelerin Rekabet Otoriteleri ile yaptığı anket çalışmasına bakıldığında, ilgili ülkelerde (11 ülke) Yİ'lerle ilgili belirtilenlerden bazıları şunlardır:

- Yİ öncesi hazırlık kapsamında toplantılar yapılmakta, bazı ülkelerde Yİ yapılacak teşebbüsün bilişim altyapısı araştırılmakta, bazılarında ise kurum içi veya dışı adli bilişim uzmanlarına danışılmaktadır.
- Elektronik delillerin toplanması ve incelenmesine yönelik politika ve prosedürler bulunmaktadır.
- Yİ sırasında teşebbüs bilişim personeli ile işbirliği yapılmaktadır.
- Yİ sırasında çeşitli adli bilişim yazılım ve donanımları kullanılmaktadır. Ülkelerin çoğunluğu imaj alırken bazıları imaj almamakta ve yalnızca canlı sistemlerde inceleme (canlı adli bilişim) tekniklerini kullanmaktadır.
- Yİ sırasında elektronik delillerin silinmesini engellemek için her ülke farklı bir takım tedbirler almaktadır (teşebbüs çalışanlarını sözlü uyarma, kilit şahısları ve konumları gözetleme, sistem yöneticisi hesabıyla verilerin silinip silinmediğine bakılması, ağ kablolarının çıkarılması vb.).

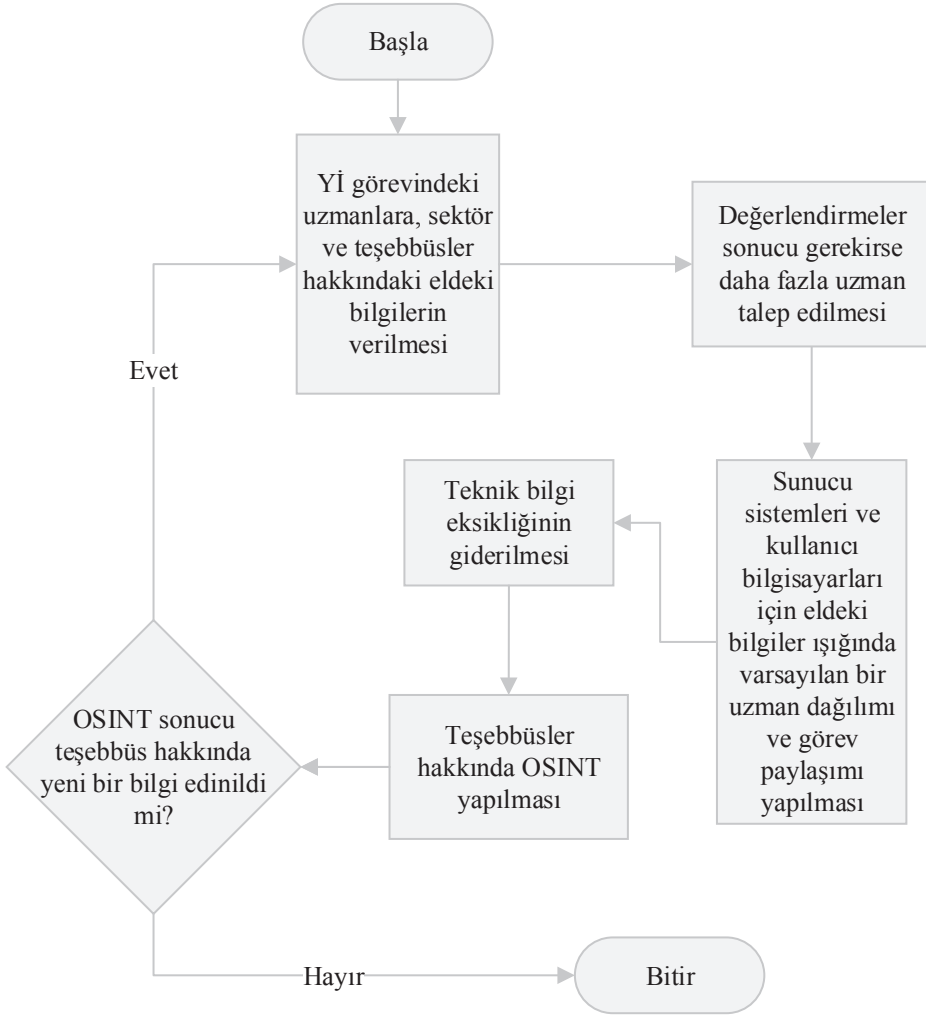
Avrupa Birliği üyesi ülkelere birçoğu, Yİ'lerde, politika ve prosedürlere sahip olmalarıyla ve adli bilişim yazılımları kullanımındaki tutumlarıyla ülkemizden farklılıklar göstermektedir.

#### **4.5. Yİ AKIŞ ŞEMASI ÖNERİLERİ**

Birinci bölümde belirlenen süreç modeli ve çalışmanın bu kısmına kadar anlatılanlar doğrultusunda Yİ akış seması önerileri alt başlıklarda verilmektedir. Akış şemaları sayesinde Yİ'lerin, belli standartlara ve prosedürlere bağlı kalınarak daha etkin bir şekilde yapılabileceği değerlendirilmektedir.

#### 4.5.1. Hazırlık Aşaması Akış Şeması

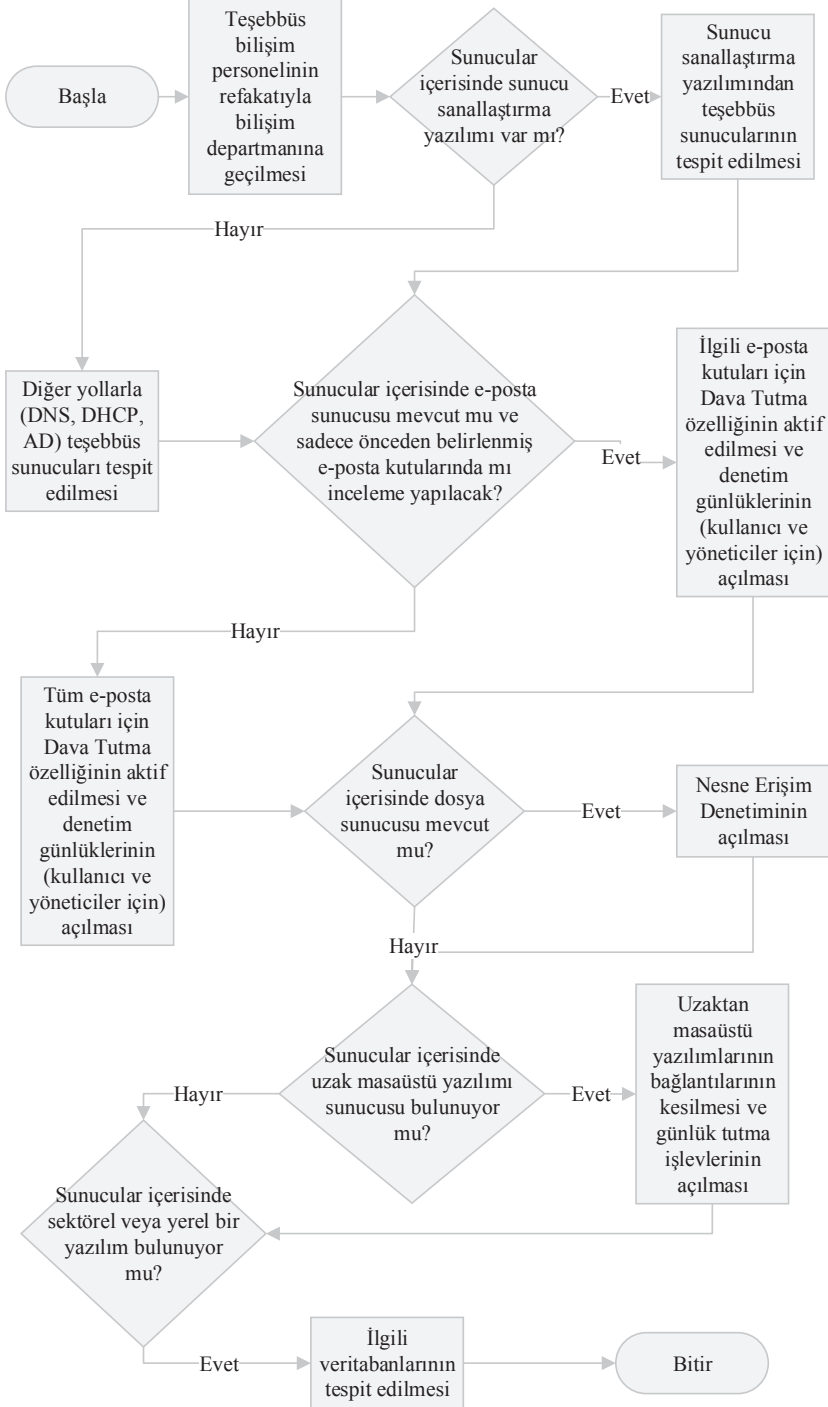
Hazırlık aşaması Yİ'ye katılacak tüm uzmanların yapılacak inceleme hakkında detaylı bilgilendirilmesi ile başlamaktadır. Bu aşamada yapılan değerlendirmeler ve araştırmalar sonucu elde edilen bilgiler doğrultusunda Yİ planlaması son halini almaktadır.





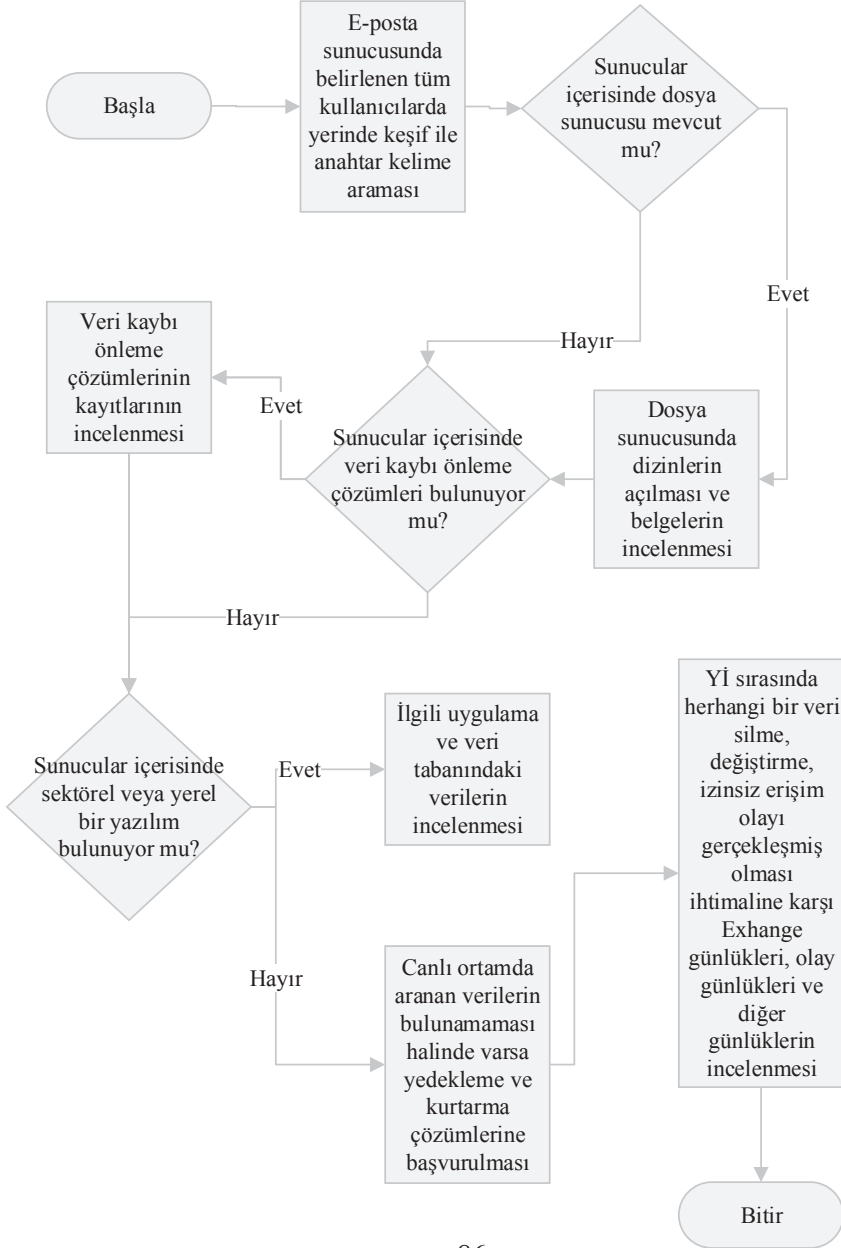
#### **4.5.2. Sunucu Sistemlerinde Kontrol ve Koruma Aşaması Akış Şeması**

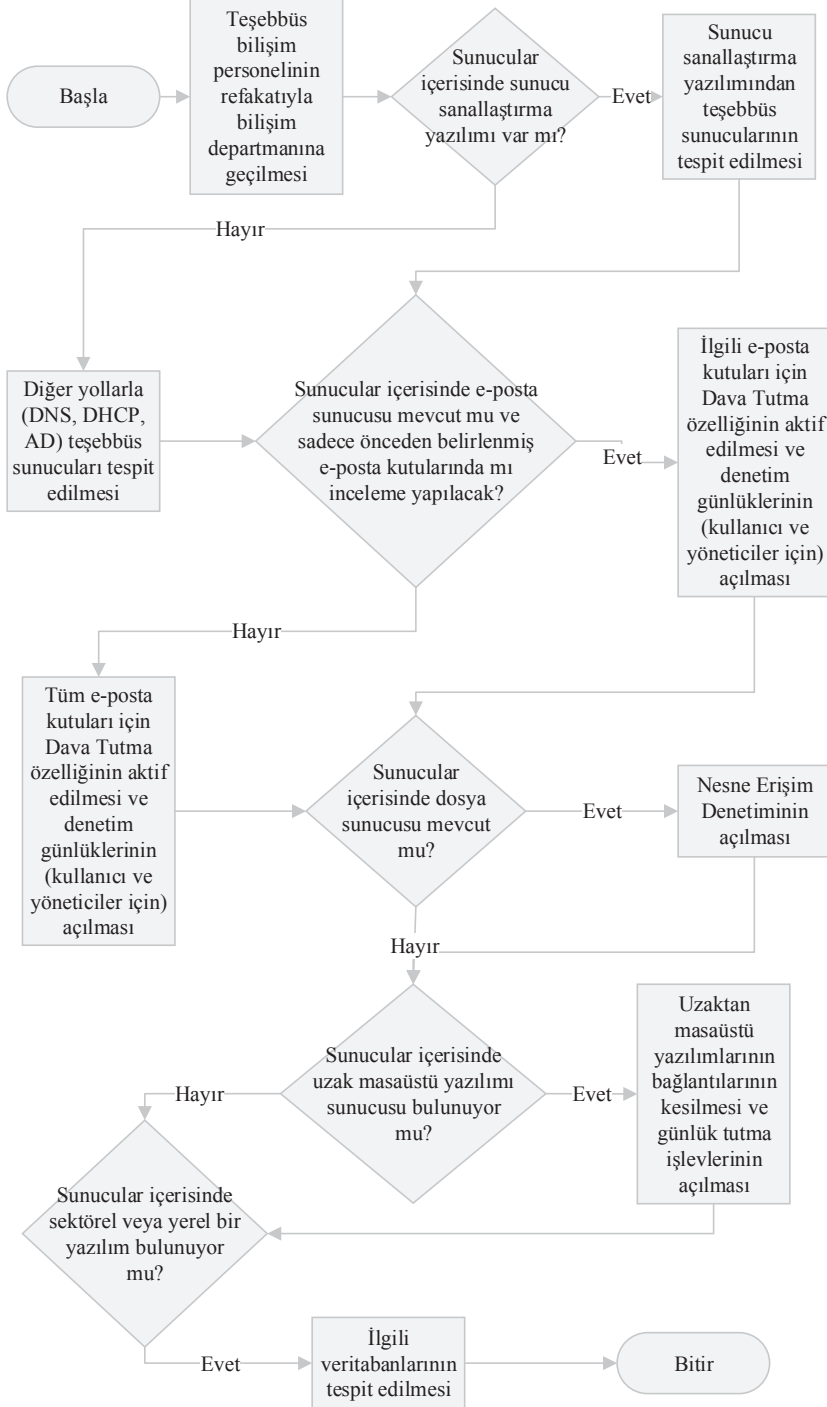
Bu aşama, sunucu sistemlerinde kontrol ve koruma ortamının sağlanması için gerekli adımları içermektedir. En önemli delil kaynakları olması sebebiyle e-posta ve dosya sunucularına öncelik verilmiştir. Tüm işlemlerin teşebbüs bilişim personelinin refakati ile yerine getirilmesi önerilmektedir.



#### 4.5.3. Kullanıcı Bilgisayarlarında Kontrol ve Koruma Aşaması Akış Şeması

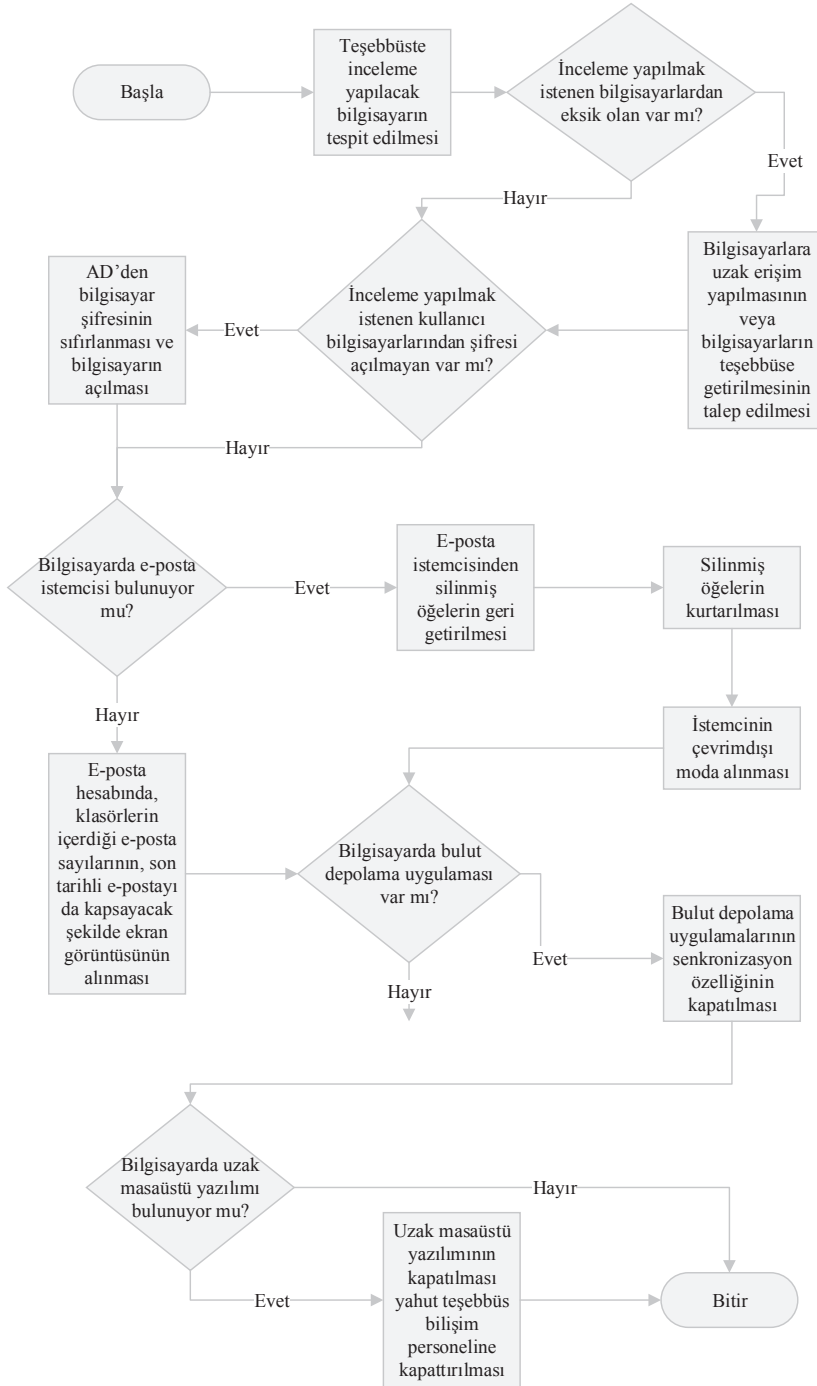
İnceleme yapılacak bilgisayara doğrudan veya uzaktan erişim yapılarak gerçekleştirilecek bu aşamada ilk olarak verilere dış müdahalelerin önlenmesi amaçlanmaktadır.





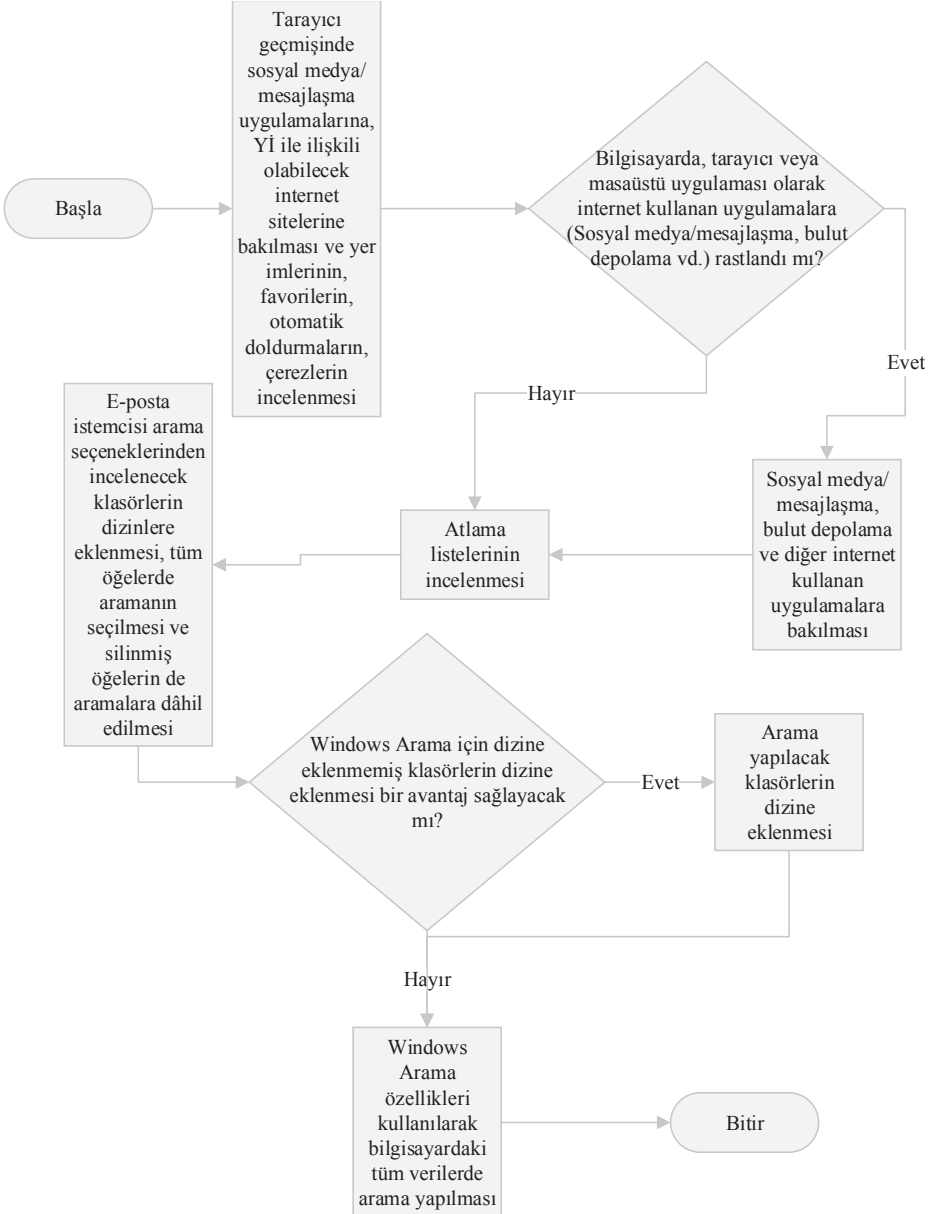
#### **4.5.4. Sunucu Sistemlerinde İnceleme ve Analiz Aşaması Akış Şeması**

Bu aşamada, sunucu sistemlerinde delillere erişim için izlenen adımlara yer verilmektedir. Sunucularda rastlanan her uygulama için bir prosedür belirlenmesi mümkün olmasa da, özellikle uygulamalara ait veri tabanlarının incelenmesi önem arz etmektedir.



#### 4.5.5. Kullanıcı Bilgisayarlarında İnceleme ve Analiz Aşaması Akış Şeması

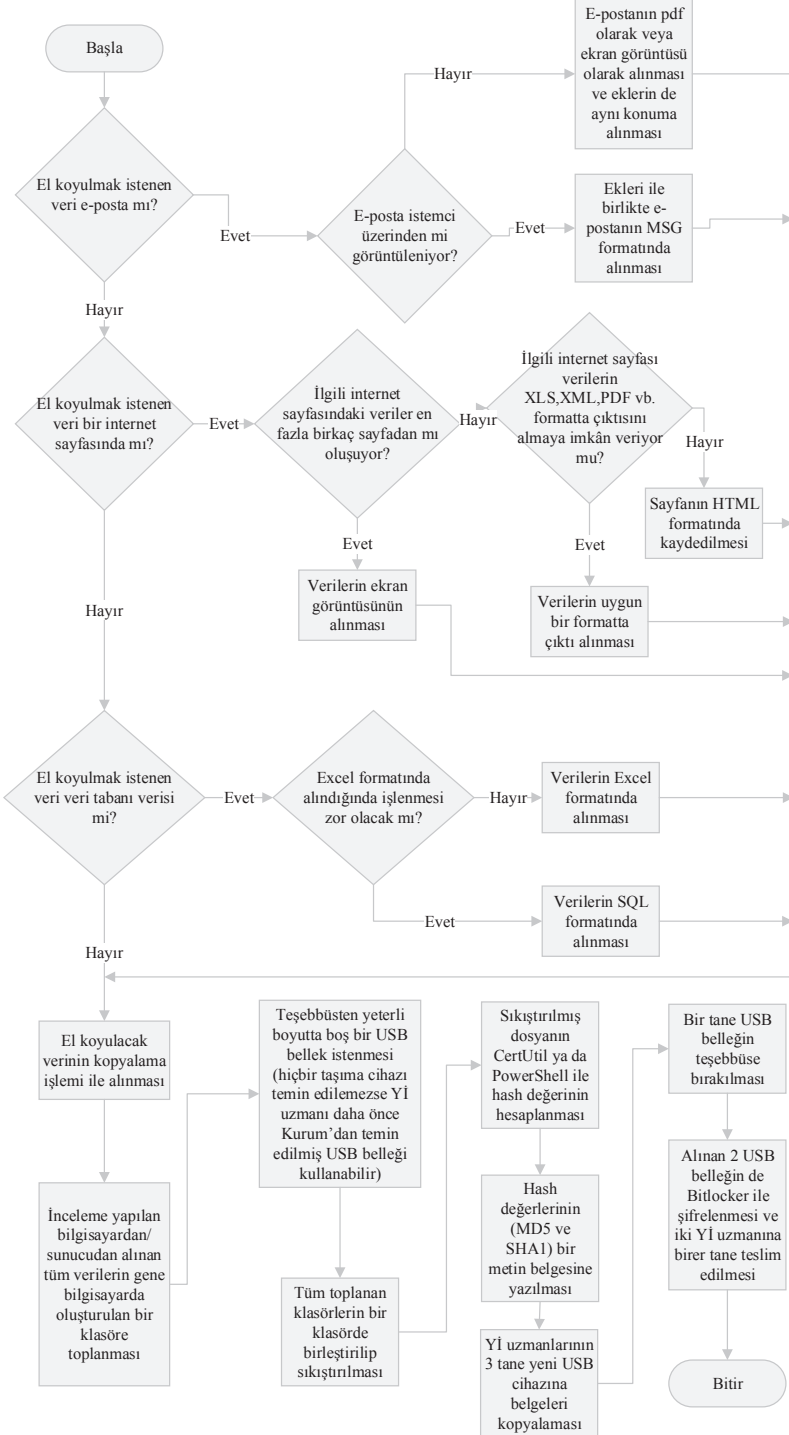
Tarayıcı ve e-posta verilerinin incelenmesine öncelik verilen bu aşamada, diğer önemli delil kaynakları için de adımlara yer verilmektedir. Bu aşamada Windows Arama'nın da etkin şekilde kullanımı önemlidir.



#### **4.5.6. Elde Etme Aşaması Akış Şeması**

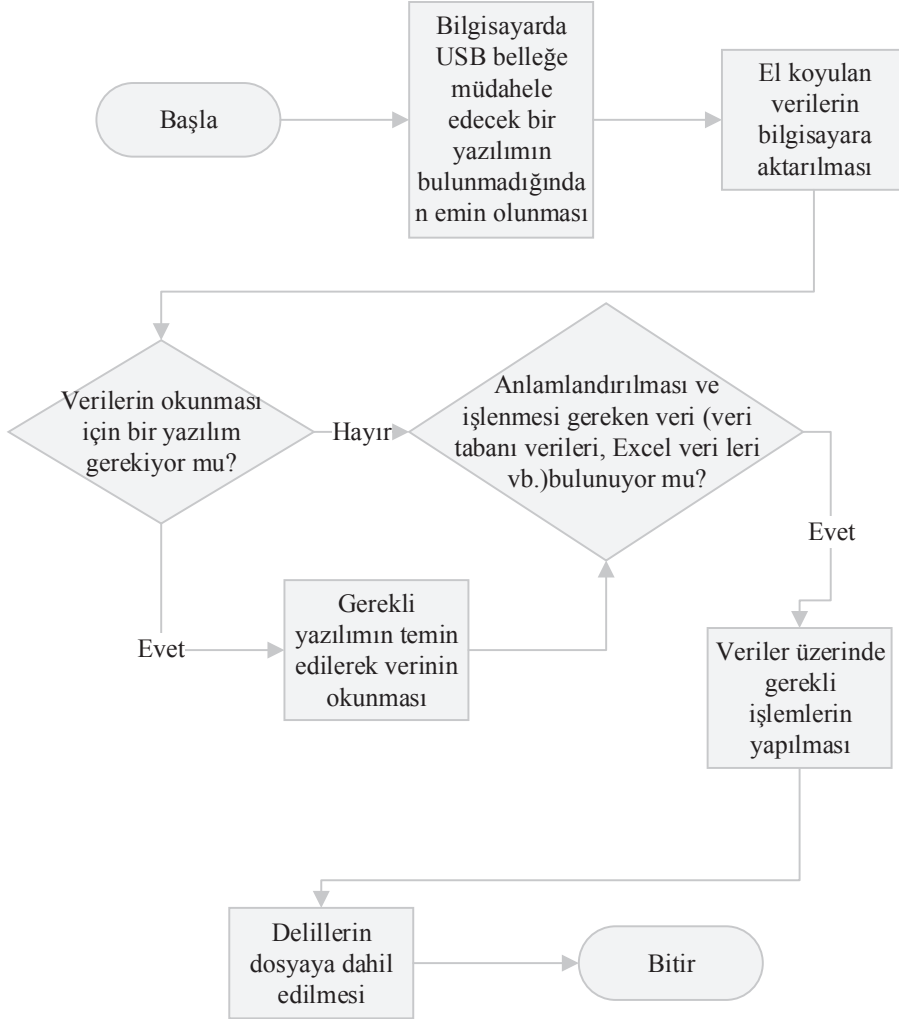
Verilere el koyulması aşamasında birçok yöntem bulunmaktadır. Uygun yöntem mevcut şartlar göz önünde bulundurularak belirlenebilir. Veriler hash değerleri hesaplanıp bir USB'ye yazılarak alınmaktadır.





#### 4.5.7. Sunum Aşaması Akış Şeması

Sunum aşaması el koyulan verilerin dosyaya dâhil edildiği aşamadır. El koyulan verilerin anlamlandırılması için bir takım işlemlerin yapılması gerekebilmektedir.



## SONUÇ

Gün geçtikçe kapsamı genişleyerek artan yazılım ve donanım ürünleri, bulut bilişim gibi artan kullanım alanları, Yİ'lerin etkinliğini tehdit etmektedir. Teşebbüslerin Yİ'lere karşı aldığı önlemler ise, rekabet otoritelerinin karşısına çıkan bir diğer zorluktur. Yİ'lerde izlenen yöntemlerin gelişimlere ayak uyduramaması ve Yİ'lerin tamamen kısır kalması riski ise zamanla daha da hissedilecek bir tehdit olacaktır.

Yİ süreçleri hazırlık, tanıma, kontrol/koruma, teşhis/inceleme, toplama ve analiz/sunum aşamaları olarak ele alınmalı ve her bir aşaması dikkatle yerine getirilmelidir. Bilişim sistemlerinde gerçekleştirilen bu incelemelerin, teknik bilgisi yeterli uzmanlarca, incelenen sistemin farklılıklarına ve delil zincirine özen gösterilerek Yİ'nin doğasına uygun şekilde yapılması gerekmektedir. Büyük miktardaki veri yığınlarında arama şeklinde gerçekleşen Yİ'ler, sunuculardan kullanıcı bilgisayarlarına sistematik bir şekilde gerçekleştirilmelidir. Adli bilişim yazılımlarının bu denli müdâhil olduğu inceleme dünyasının mevcut Yİ süreçlerinde göz ardı edilmesi ise hiç şüphesiz bir etkinsizlik doğurmaktadır.

Çalışmada, mevcut Yİ süreçleri ve eksik yönleri ele alınmıştır. Ardından Yİ'lerin gerçekleştirilme şekilleri göz önünde bulundurularak bir inceleme süreç modeli ortaya koyulmuştur. Bu süreç modelinden hareketle, teşebbüslerde karşılaşılabilecek sunucu sistemleri ve kullanıcı bilgisayarlarının incelenmesine yer verilmiş, potansiyel delil kaynakları ele alınmıştır. Çalışmada bilişim sistemlerinde gerçekleştirilecek bir Yİ sürecinin başından sonuna kadar dikkat edilmesi gereken hususlar ortaya koyulmuştur. Yİ sürecinin etkinliğinin artırılmasını amaçlayan yazılım kullanım önerilerine ve son kısımda ise akış şemasalarına yer verilmiştir.

Son olarak ifade etmek gerekir ki; Yİ'ler ile ilgili daha ayrıntılı bir mevzuata ihtiyaç olduğu düşünülmektedir. Ayrıca ortaya çıkacak mevzuat doğrultusunda Yİ süreçlerinin en ince noktasına kadar şekillendirilmesinin gerektiği değerlendirilmektedir.

## **ABSTRACT**

Dawnraids are the most important evidence gathering methods for competition authorities. These operations, which can be carried out in a wide variety of information systems, require a cleverly designed, accurate approach. Dawnraids specialists should have adequate technical knowledge and follow up the adopted methods during the operations.

The contribution of the use of forensic tools on the information systems can not be ignored. EU Commission and EU member states have differences, but most of them use advanced forensic tools. The use of advanced forensic tools is not included in the dawnraids carried out by the Turkish Competition Authority.

This study evaluates dawnraids as a process and then divides it into two parts: Server systems and user computers. In the study, the systems and applications that are likely to be encountered in the servers and user computers introduced. Then the measures to be taken during the operations and the parts recommended to be examined are included. Finally, a flowchart for dawnraids is presented after evaluations of the use of forensic IT tools in the dawnraids.

## KAYNAKÇA

- AGGARWAL, G. , E. BURSZEIN,C. JACKSON ve D. BONEH (2010). “Analysis of Private Browsing Modes in Modern Browsers”, <https://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf> Erişim Tarihi: 20.12.2018
- AKBAL, E., F. GÜNEŞ ve A. AKBAL (2016), “Digital Forensic Analyses of Web Browser Records”, *Journal of Software*, Vol:11, No:7, s.631-637.
- ALTHEIDE, C. ve H. CARVEY (2011), *Digital Forensics with Open Source Tools*, First Edition, Syngress, Waltham, USA.
- ANDERSSON, J. ve M. PFEIFFER (2013), *Microsoft Exchange Server 2013 Powershell Cookbook*, Second Edition, Packt Publishing, Birmingham, UK.
- ARNES, A. (2017), *Digital Forensics*, First Edition, Wiley, Hoboken, USA.
- BARRADAS, D. , T. BRITO, D. DUARTE, N. SANTOS ve L. RODRIGUES (2018), “Forensic analysis of communication records of messaging applications from physical memory”, *Computers&Security* <https://www.sciencedirect.com/science/article/pii/S0167404818311313?via%3Dihub> Erişim Tarihi: 03.01.2019
- BASHIR , M. S. ve M. N. A. KHAN (2013), “Triage in Live Digital Forensic Analysis”, *The International Journal of Forensic Computer Science*, Vol:8, Sayı:1, s.35-44.
- BODDINGTON, R. (2016), *Practical Digital Forensics*, First Edition, Packt Publishing, Birmingham, UK.
- BOTT, E. (2016), *Introducing Windows 10 for IT Professionals*, First Edition, Microsoft Press, Washington, USA.
- BOTT, E. , C. SIECHERT ve C. STINSON (2016), *Windows 10 Inside Out*, Second Edition, Microsoft Press, Washington, USA.
- CAI , L. , J. SHA ve W. QIAN (2013), “Study on forensic analysis of physical memory”, *Proceedings of 2nd International Symposium on Computer, Communication, Control and Automation*, s.221–224, Atlantis Press, <https://www.atlantispress.com/proceedings/3ca-13/10172>, Erişim Tarihi: 13.01.2019.

- CARRIER, B. D. (2006), "Risks of live digital forensic analysis", *Communications of the ACM*, Vol:49, No:2, s.56-61.
- CARVEY, H. (2016), *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry*, Second Edition, Syngress, Cambridge, USA.
- CARVEY, H. (2009), *Windows Forensic Analysis DVD Toolkit*, Second Edition, Syngress, Barlington, USA.
- CHAN, E., S. VENKATARAMAN, F. DAVID, A. CHAUGULE ve R. CAMPBELL (2010), "Forenscope: A Framework for Live Forensics", Twenty-Sixth Annual Computer Security Applications Conference, [https://www.researchgate.net/publication/221046319\\_Forenscope\\_A\\_framework\\_for\\_live\\_forensics](https://www.researchgate.net/publication/221046319_Forenscope_A_framework_for_live_forensics), Erişim Tarihi: 19.11.2018.
- CHAUHAN S. , N. K. PANDA (2015), *Hacking Web Intelligence Open Source Intelligence and Web Reconnaissance Concepts and Techniques*, First Edition, Syngress, Waltham, USA.
- CHIVERS, H. ve C. HARGREAVES (2011), "Forensic data recovery from the Windows Search Database", *Digital Investigation*, Vol:7, Sayı:3-4, s.114-126.
- CHUVAKIN, A. A. , K.J. SCHMIDT ve C. PHILLIPS (2012), *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*, First Edition, Syngress, Waltham, USA.
- CUSACK, B. ve J. SON (2012), "Evidence Examination Tools for Social Networks", 10th Australian Digital Forensics Conference, s.33-40, <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1108&context=adf>, Erişim Tarihi: 23.02.2019.
- DANIEL, L. ve L. DANIEL (2011), *Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom*, First Edition, Syngress, Waltham, USA.
- DAUTI, B. (2017), *Windows Server 2016 Administration Fundamentals*, First Edition, Packt Publishing, Birmingham, UK.
- DESMOND, B. , J. RICHARDS, R. ALLEN ve A. G. LOWE-NORRIS (2013), *Designing, Deploying and Running Active Directory*, Fifth Edition, O'Reilly Media, USA
- DEZFOULI, F. ve A. DEHGHANTANHA (2014), "Digital forensics trends and future", *International Journal of Cyber-Security and Digital Forensics*, s.48-76.
- ELFASSY, D. (2013), *Mastering Microsoft Exchange Server 2013*, First Edition,

Sybex, Indiana, USA.

FRANCIS, D. (2017), *Mastering Active Directory: Understand the Core Functionalities of Active Directory Services Using Microsoft Server 2016 and PowerShell*, First Edition, Packt Publishing, Birmingham, UK.

HAYES, D. R. (2014), *Practical Guide to Computer Forensics Investigations*, First Edition, Pearson IT Certification, USA.

HORSMAN, G. (2018), “I didn’t see that! An examination of internet browser cache behaviour following website visits”, *Digital Investigation*, Vol:25, s.105-113.

JAZAYERI, M. (2007), “Some Trends in Web Application Development”, *Future of Software Engineering (FOSE ‘07)*, s.199-213.

KENT, K., S. CHEVALIER, T. GRANCE ve H. DANG (2006). “Guide to integrating forensic techniques into incident response”, NIST Special Publication, s.800–886, <https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response>, Erişim Tarihi: 07.08.2018.

KNOTT, C.L. ve G. STEUBE (2011), “Encryption And Portable Data Storage”, *Journal of Service Science*, Vol: 4, Sayı:1, s.21-30.

KRAUSE, J. (2016), *Mastering Windows Server 2016*, First Edition, Packt Publishing, Birmingham, UK.

LAMBERT, J. (2018), *Windows 10 Step by Step*, Second Edition, Microsoft Press, USA.

LEONARD, C. , B. SVIDERGOL, B. WRIGHT ve V. MELOSKI (2016), *Mastering Microsoft Exchange Server 2016*, Second Edition, Sybex, Indiana, USA.

LIM, S. , B. YOO, J. PARK, K. BYUN ve S. LEE (2012), “A research on the investigation method of digital forensics for a VMware Workstation’s virtual machine”, *Mathematical and Computer Modelling*, Vol: 55, Sayı:1–2, s.151-160.

LIU, S. ve R. KUHN (2010), “Data Loss Prevention”, *IT Professional*, Vol:12, Sayı:2, s.10–13.

LUTTGENS, J.T. , M. PEPE ve K. MANDIA (2014), *Incident Response & Computer Forensics*, Third Edition, McGraw-Hill Education, New York, USA.

MAJEED, A. , H. ZIA, R. IMRAN ve S. SALEEM (2016), “Forensic analysis of three social media apps in windows 10”, 2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET), s.1-5, <https://ieeexplore.ieee.org/document/7395419>, Erişim Tarihi:13.02.2019.

MARRINGTON, A. , I. BAGGILI, T. ISMAIL ve A. KAF (2012), “Portable Web

Browser Forensics: A Forensic examination of the privacy benefits of portable web browsers”, 2012 International Conference on Computer Systems and Industrial Informatics, s.1-6, <https://ieeexplore.ieee.org/document/6454516>, Erişim Tarihi: 29.01.2019.

MESSIER, R. (2015), *Operating System Forensics*, First Edition, Syngress, Waltham, USA.

MORGAN, T.D. (2008), “Recovering deleted data from the Windows registry”, *Digital Investigation*, Vol:5, s.33-41.

MORIMOTO, R. , J. SHAPIRO, G. YARDENI, O. DROUBI, M. NOEL, A. AB-BATE ve C. AMARIS (2017), *Windows Server 2016 Unleashed*, First Edition, Sams Publishing, Indianapolis, USA.

NABITY, P. ve B. J. L. LANDRY (2015). “Recovering Deleted and Wiped Files: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator”, [https://www.researchgate.net/publication/267959752\\_Recovering\\_Deleted\\_and\\_Wiped\\_Files\\_A\\_Digital\\_Forensic\\_Comparison\\_of\\_FAT32\\_and\\_NTFS\\_File\\_Systems\\_using\\_Evidence\\_Eliminator](https://www.researchgate.net/publication/267959752_Recovering_Deleted_and_Wiped_Files_A_Digital_Forensic_Comparison_of_FAT32_and_NTFS_File_Systems_using_Evidence_Eliminator) Erişim Tarihi: 17.09.2018.

OGUCHI, Y. ve T. YAMAMATO (2008), “Server virtualization technology and its latest trends”, *Fujitsu Scientific and Technical Journal*, Vol:44, Sayı:1, s.46-52.

OH, J. , S. LEE ve S. LEE (2011), “Advanced evidence collection and analysis of web browser activity”, *Digital Investigation*, Vol:8, s.62-70.

OHANA, D.J. ve N. SHASHIDHAR (2013), “Do Private and Portable Web Browsers Leave Incriminating Evidence?”, 2013 IEEE Security and Privacy Workshops, <https://ieeexplore.ieee.org/abstract/document/6565242>, Erişim Tarihi: 03.01.2019.

OOMMEN, R.R. ve P. SUGATHAN (2016), “Recovering Deleted Files from NTFS”, *International Journal of Science and Research (IJSR)*, Vol:5, Sayı:5, s.205-208.

ÖZTÜRKÇİ. H. (2014), “Windows Jump List Forensics”, <http://halilozturkci.com/windows-jump-list-forensics/> Erişim Tarihi: 12.01.2019

POGUE, D. (2015), *Windows 10: The Missing Manual*, Second Edition, O'Reilly Media, Sebastopol, USA.

POGUE, D. (2013), *Windows 8: The Missing Manual*, First Edition, Sebastopol, USA.

POGUE, D. (2010), *Windows 7: The Missing Manual*, First Edition, Sebastopol,



USA.

PRAJAPATI, P. , A. ANJANEYULU ve N. PATEL (2015), “Analysis Of Deleted Data In NTFS Filesystem”, *International Journal for Science And Research In Technology (IJSART)*, Vol:1, Sayı:2.

QUICK, D. ve K.R. CHOO (2014), “Google Drive: Forensic analysis of data remnants”, *Journal of Network and Computer Applications*, Vol:40, s.179-193.

QUICK, D. ve K.R. CHOO (2013), “Dropbox analysis: Data remnants on user machines”, *Digital Investigation*, Vol:10, No:1, s.3-18.

RAFIQUE, M. ve M. N. A. KHAN (2013), “Exploring Static and Live Digital Forensics: Methods, Practices and Tools”, *International Journal of Scientific & Engineering Research*, Vol:4, Sayı:10, s.1048.

REYES, A. , R. BRITTON, K. O’SHEA ve J. STEELE (2007), *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*, First Edition, Syngress, Rockland.

RUAN, K. , J. CARTHY, T. KECHADI ve M. CROSBIE (2011), “Cloud forensics: An overview”, *Advances in Digital Forensics VII*, 7th IFIP WG 11.9 International Conference on Digital Forensics, s.35-46.

SACHOWSKI, J. (2018), *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise*, First Edition, CRC Press, Florida, USA

SAMMONS, J. (2012), *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, First Edition, Syngress, Waltham, USA.

SHAABAN, A. ve K. SAPRONOV (2016), *Practical Windows Forensics*, First Edition, Packt Publishing, Birmingham, UK.

SIDDAWAY, R. (2014), *Learn Active Directory Management in a Month of Lunches*, First Edition, Manning Publications, Shelter Island, USA.

SINGH, B. ve U. SINGH (2016), “A forensic insight into Windows 10 Jump Lists”, *Digital Investigation*, Vol:17, s.1-13.

SNEDAKER, S. (2013), *Business Continuity and Disaster Recovery Planning for IT Professionals*, Second Edition, Syngress, Waltham, USA.

SÖDERSTRÖM, O. ve E. MORADIAN (2013), “Secure Audit Log Management”, *Procedia Computer Science*, Vol: 22, s.1249-1258.

TAHBOUB, R. ve Y. SALEH (2014), “Data Leakage/Loss Prevention Systems (DLP)”, 2014 World Congress on Computer Applications and Information Sys-

tems (WCCAIS), <https://ieeexplore.ieee.org/document/6916624> Erişim Tarihi: 01.02.2019.

TAYLOR, M. , J. HAGGERTY, D. GRESEY, P. ALMOND ve T. BERRY (2014), “Forensic investigation of social networking applications”, *Network Security*, Vol:2014, Sayı:11, s.9-16.

THOMAS, O. (2017), *Windows Server 2016 Inside Out*, First Edition, Microsoft Press, USA.

WADDELL, A. (2017), “Guide to Open Source Intel Search Methods”, Open Source Information Research, [https://www.researchgate.net/publication/320871796\\_Guide\\_to\\_Open\\_Source\\_Intel\\_Search\\_Methods](https://www.researchgate.net/publication/320871796_Guide_to_Open_Source_Intel_Search_Methods) Erişim Tarihi: 09.09.2018.

WATTERS, J. (2013), *Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference*, First Edition, Apress, New York, USA.

WESSELIUS, J. (2014), *Pro Exchange Server 2013 Administration*, First Edition, Apress, New York, USA.

YAZDANIPOUR, M. , D. MAHMOUDI, A. YAZDANIPOUR, M. YAZDANIPOUR ve A. MEHDIPOUR (2012), “Comprehensive review and selection criteria for virtual network computing technology”, IEEE, <https://ieeexplore.ieee.org/document/6335529> Erişim Tarihi: 23.11.2018.

YILDIZ, G. (2014), “AB Rekabet Otoritelerinde Adli Bilişim Uygulamaları, Bilişim Teknolojisi Politikaları Ve Türk Rekabet Kurumu İçin Öneriler”, Yayınlanmamış Çalışma, Selçuk Üniversitesi, Konya.

YINGXIN, C. , F. XIAO, D. XIAOJIANG, L. BIN ve M. GUIZANI (2017), “A lightweight live memory forensic approach based on hardware virtualization”, *Information Sciences*, Vol:379, s.23-41.

ZHANG, L. , D. ZHANG ve L. WANG (2010), “Live digital forensics in a virtual machine”, 2010 International Conference on Computer Application and System Modeling (ICCSM), Vol: 4, s.328-332, <https://ieeexplore.ieee.org/document/5620364>, Erişim Tarihi: 10.10.2018.

### **Rekabet Kurulu Kararları**

29.08.2013 tarihli ve 13-49/711-300 sayılı Kurul kararı

22.10.2014 tarihli ve 14-42/783-346 sayılı Kurul kararı

23.02.2017 tarihli ve 17-08/99-42 sayılı Kurul kararı

22.11.2018 tarihli ve 18-44/703-345 sayılı Kurul kararı

19.09.2018 tarihli ve 18-33/556-274 sayılı Kurul kararı

### **Diğer Kaynaklar**

Commvault Documentation, “Restore - Exchange Mailbox Agent, ”[http://documentation.commvault.com/hds/v10/article?p=products/exchange\\_mailbox/restore\\_basic.htm](http://documentation.commvault.com/hds/v10/article?p=products/exchange_mailbox/restore_basic.htm) Erişim Tarihi: 01.01.2019

European Commission (2015), “Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003”, [http://ec.europa.eu/competition/antitrust/legislation/explanatory\\_note.pdf](http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf), Erişim Tarihi: 09.12.2018.

European Council (2002), “Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance)”, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0001:EN:HTML>, Erişim Tarihi: 09.12.2018.

IntelTechniques, “OSINT Tools”, <https://inteltechniques.com/menu.html> Erişim Tarihi: 13.01.2019

Microsoft Azure, “Bulut bilişim nedir?”, <https://azure.microsoft.com/tr-tr/overview/what-is-cloud-computing/> Erişim Tarihi: 22.12.2018

Microsoft Docs (2017), “Active Directory Domain Services Overview”, <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> Erişim Tarihi: 6.12.2018

Microsoft Docs (2018a), “Advanced Query Syntax”, <https://docs.microsoft.com/en-us/windows/desktop/lwef/-search-2x-wds-aqsreference> Erişim Tarihi: 19.12.2018

Microsoft Docs (2018b), “Create or remove an In-Place Hold”, <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/in-place-holds?view=exchserver-2019> Erişim Tarihi: 10.02.2019

Microsoft Docs (2018c), “Enable or disable mailbox audit logging for a mailbox”, <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019> Erişim Tarihi: 09.02.2019

Microsoft Docs (2018d), “Enable or disable single item recovery for a mailbox”, <https://docs.microsoft.com/en-us/exchange/recipients/user-mailboxes/single-item-recovery?view=exchserver-2019> Erişim Tarihi: 10.02.2019

Microsoft Docs (2018e), “Manage administrator audit logging”, <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/admin-audit-logging/manage-admin-audit-logging?view=exchserver-2019> Erişim Tarihi: 09.02.2019

Microsoft Docs (2018f), “Place a mailbox on Litigation Hold”, <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/litigation-holds?view=exchserver-2019> Erişim Tarihi: 10.02.2019

Microsoft Docs (2018g), “Predefined Keys”, <https://docs.microsoft.com/en-us/windows/desktop/sysinfo/predefined-keys> Erişim Tarihi: 12.01.2019

Microsoft Docs (2018h), “Procedures for mailbox exports to .pst files in Exchange Server”, <https://docs.microsoft.com/en-us/exchange/recipients/mailbox-import-and-export/export-procedures?view=exchserver-2019> Erişim Tarihi: 10.02.2019

Microsoft Docs (2018i), “Windows Search Overview”, <https://docs.microsoft.com/en-us/windows/desktop/search/-search-3x-wds-overview> Erişim Tarihi: 16.12.2018

Microsoft Docs (2018j), “Windows Search”, <https://docs.microsoft.com/en-us/windows/desktop/search/windows-search> Erişim Tarihi: 16.12.2018

Microsoft Docs (2018k), “Exchange admin center in Exchange Server”, <https://docs.microsoft.com/en-us/exchange/architecture/client-access/exchange-admin-center?view=exchserver-2019> Erişim Tarihi: 20.01.2019

Microsoft Docs (2018l), “Recoverable Items folder in Exchange Server”, <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder?view=exchserver-2019> Erişim Tarihi: 20.01.2019

Microsoft Support (2018), “Search indexing in Windows 10: FAQ”, <https://support.microsoft.com/en-us/help/4098843/windows-10-search-indexing-faq> Erişim Tarihi: 16.10.2018

Microsoft Technet (2012), “DHCP Failover Load Balance Mode”, <https://blogs.technet.microsoft.com/teamdhcp/2012/08/06/dhcp-failover-load-balance-mode/> Erişim Tarihi: 08.02.2019

Oracle Docs (2005), “Introduction to Directory Services and Directory Server”, <https://docs.oracle.com/cd/E19396-01/817-7619/intro.html> Erişim Tarihi: 6.12.2018

Spiceworks Community (2016), “Server Virtualization and OS Trends”, <https://community.spiceworks.com/networking/articles/2462-server-virtualization>

on-and-os-trends Erişim Tarihi: 18.01.2019

Symantec, “Why you need an Information Centric Security model for the GDPR”, <https://www.symantec.com/content/dam/symantec/docs/solution-briefs/why-you-need-an-information-centric-security-model-for-the-gdpr-en.pdf> Erişim Tarihi: 05.01.2019

TDK, “Güncel Türkçe Sözlük” <http://sozluk.gov.tr/> Erişim Tarihi: 02.02.2019



Üniversiteler Mahallesi  
1597. Cadde No: 9  
06800 Bilkent - Çankaya /ANKARA  
[http:// www.rekabet.gov.tr](http://www.rekabet.gov.tr)