Uzmanlık Tezleri Serisi No: 158

REKABET KURUMU

YERİNDE İNCELEMELERDE ELEKTRONİK POSTA ANALİZİNE İLİŞKİN SÜREÇ MODELİ ÖNERİSİ

ÖMER FARUK ÇELİK

YERİNDE İNCELEMELERDE ELEKTRONİK POSTA ANALİZİNE İLİŞKİN SÜREÇ MODELİ ÖNERİSİ

ÖMER FARUK ÇELİK

Ankara 2017

Baskı, Mayıs 2017
Rekabet Kurumu-ANKARA

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

Bu tez, Rekabet Kurumu Başkan Yardımcısı Hasan Hüseyin ÜNLÜ, Rekabet Kurumu Başkan Yardımcısı Kürşat ÜNLÜSOY, Bilgi Yönetimi Dairesi Başkanı Ferhat TOPKAYA, Baş Hukuk Müşaviri Salim AYDEMİR ve Prof. Dr. Fuat OĞUZ'dan oluşan Tez Değerlendirme Heyeti tarafından 24-25-26 Ekim 2016 tarihlerinde yürütülen Tez Savunma Toplantısı sonucunda yeterli ve başarılı kabul edilmiştir.

Tez yazarı Ömer Faruk ÇELİK, 02.12.2016 tarihinde yapılan Yeterlik Sınavında başarılı olmuş ve Başkanlık Makamının 16.12.2016 tarih ve 13645 sayılı onayı ile Rekabet Uzmanı olarak atanmıştır.

YAYIN NO **336**

Canım kızlarım Ayşe Nazlı ve Elif Masal ile
sevgili eşim Demet'e ithafen…

İÇİNDEKİLER

BÖLÜM 4

YERİNDE İNCELEMELERDE ELEKTRONİK POSTA ANALİZİ KONUSUNDA TAKİP EDİLMESİ ÖNERİLEN SÜREÇ MODELİ

TABLO DİZİNİ

GRAFİK DİZİNİ

ŞEKİL DİZİNİ

KISALTMALAR

A.g.k.	**:** Adı Geçen Kaynak
ABD	**:** Amerika Birleşik Devletleri
Bkz.	**:** Bakınız
DNS	**:** Domain Name System
EAC	**:** Exchange Admin Center
EPD	**:** Elektronik Posta Dosyası
Komisyon	**:** Avrupa Birliği Komisyonu Rekabet Genel Direktörlüğü
Kurul	**:** Rekabet Kurulu
MFA	**:** Managed Folder Assistant
MTA	**:** Message Transfer Agent
MUA	**:** Message User Agent
OCR	**:** Optical Character Recognition
OWA	**:** Outlook Web App
PFF	**:** Personal Folder File
Proje	**:** Avrupa Antitröst Adli Bilişim Araçları Projesi
RKHK	**:** 4054 Sayılı Rekabetin Korunması Hakkında Kanun
s.	**:** Sayfa
SMTP	**:** Simple Mail Transfer Protocol
vb.	**:** ve benzeri
vd.	**:** ve diğerleri
vol.	**:** Volume
Yİ	**:** Yerinde İnceleme
YİY	**:** 4054 Sayılı Rekabetin Korunması Hakkında Kanun'un Uygulanması Çerçevesinde Rekabet Kurumunca Yapılacak Yerinde İncelemelere İlişkin Usul ve Esaslara Dair Yönerge

GİRİŞ

Tarih boyunca insanlar bilgi, duygu ve düşüncelerini başkalarına aktarmak amacıyla çeşitli yöntemler kullanmışlardır. Taş tabletlerin kullanımıyla temelleri atılan yazılı iletişim, mesajların iletiminde elektriksel sinyallerin ilk olarak telgrafta kullanımıyla birlikte, farklı bir boyut kazanmıştır. Uzun mesafeli ve hızlı iletişimin kapılarını aralayan bu yaklaşım, hayatımızın vazgeçilmez bir parçası haline gelen iletişim teknolojilerinin geliştirilmesine ilham kaynağı olmuştur. Günümüzde en yaygın kullanılan yazılı iletişim yöntemi elektronik posta haberleşmesidir (Chhabra ve Bajwa 2015, 201). Bu yöntem, 1971 yılında Ray TOMILSON tarafından gönderilen ilk elektronik postadan günümüze, kişisel bilgisayarlar ve internet kullanımının artmasıyla birlikte yaygınlaşarak küresel bir boyut kazanmıştır (Markagić 2013, 113). Radicati Group'un 2015 yılında yayımladığı "Email Statistics Report, 2015-2019" adlı raporunda (2015, 3), dünya genelinde günlük gönderilen/alınan elektronik posta sayısının 205 milyardan fazla olduğu belirtilmektedir. Başlangıçta sadece düz yazı şeklinde mesajların iletilmesi amacıyla geliştirilen bu teknoloji, zamanla başta fotoğraf, ses, video olmak üzere her çeşit verinin gönderilmesine imkân sağlayan bir platforma dönüşmüştür (Durmaz 2014, 282). Elektronik posta haberleşmesi, sağladığı tüm bu avantajlar sayesinde kişisel kullanım yanında iş yaşamının[1] da ayrılmaz bir parçası haline gelmiştir.

Rekabet ihlallerine ilişkin açılan dosyalar kapsamında gerçekleştirilen yerinde incelemelerde (Yİ), teşebbüs çalışanlarınca sıklıkla kullanılan bu iletişim yöntemine ait kayıtlar, meslek personelince öncelikli olarak incelenmektedir. Rekabet Kurulunun

[1] 2015 yılı genelinde günlük olarak gönderilen/alınan, iş dünyasındaki (*business email*) elektronik posta sayısı ortalama 112,5 milyardır (Radicati Group 2015, 4).

(Kurul) idari para cezasına hükmettiği *Otomotiv*[2], *Bankacılık*[3], *Turkcell*[4], *Doğu Anadolu Çimento*[5], *Banka Promosyon*[6] vb. dosyalarda, ihlalin tespitine dayanak gösterilen önemli delillerin elektronik posta kayıtları olduğu görülmektedir. Teşebbüs çalışanlarının posta kutuları üzerinde gerçekleştirdikleri bilinçli ya da bilinçsiz silme işlemleri ve rekabet uyum programları kapsamında danışman firmalarca düzenli aralıklarla gerçekleştirilen Yİ tatbikatları ile posta kutularının kontrol ediliyor oluşu gibi nedenler, meslek personelinin Yİ'lerde posta kutularından dijital delil elde etmesini gün geçtikçe zorlaştırmaktadır. Bu durum, incelemelerde doğru bir yaklaşım sergilenmemesi durumunda önemli delillerin gözden kaçırılması sonucunu doğurmaktadır. Bu nedenle bu tez çalışması kapsamında, Yİ'lerde elektronik postaların analizi konusunda takip edilmesi gerektiği düşünülen yöntemin ne olduğu sorusu yanıtlanmaya çalışılacaktır.

Çalışmanın birinci bölümünde, elektronik posta iletişimi altyapısına ve iletişim esnasında aktif rol alan unsurlara yer verilecektir. Temel kavramların ardından, adli bilişim uzmanlarının ve rekabet otoritelerinin, elektronik posta analizi konusunda takip ettikleri yöntem farklılıklarına değinilecektir.

İkinci bölümde, silinmiş elektronik postaların geri getirilmesi, posta kutusu incelenecek teşebbüs çalışanlarının doğru belirlenmesi ve inceleme esnasında elektronik postaların silinmesi durumunun tespiti ve kanıtlanması gibi Yİ'lerde kritik öneme sahip faktörler ortaya konacaktır. Bölümün devamında, Kurulun sahip olduğu Yİ yetkisine dayanarak belirlediği inceleme usulü çerçevesinde, elektronik posta sunucularında bulunan özelliklerin kullanımıyla, bu sorunlara ne gibi çözümler üretilebileceği tartışılacaktır. Bölüm sonunda ise, meslek personelinin Yİ'lerdeki elektronik posta analizi performansını arttıracağı düşünülen işlem adımlarına ilişkin iş-akış diyagramına yer verilecektir.

Tezin üçüncü bölümü, elektronik posta analizi konusunda bir diğer yaklaşım olan adli bilişim araçlarının kullanımına ayrılacaktır. Bölüm içerisinde üç farklı adli bilişim aracının elektronik posta analizi yetkinlikleri irdelenecektir. Bu üç aracın, Yİ'lerde

[2] 18.04.2011 tarihli ve 11-24/464-139 sayılı Kurul kararı (*Otomotiv*).
[3] 08.03.2013 tarihli ve 13-13/198-100 sayılı Kurul kararı (*Bankacılık*).
[4] 06.06.2011 tarihli ve 11-34/742-230 sayılı Kurul kararı (*Turkcell*).
[5] 06.04.2012 tarihli ve 12-17/499-140 sayılı Kurul kararı (*Doğu Anadolu Çimento*).
[6] 07.03.2011 tarihli ve 11-13/243-78 sayılı Kurul kararı (*Banka Promosyon*).

karşılaşılması muhtemel sorunlar gözetilerek oluşturulmuş örnek vaka üzerindeki analiz başarımlarını ölçmek amacıyla gerçekleştirilen teste ise bölüm sonunda değinilecektir.

Son bölümde, elektronik posta sunucularının varsayılan yapılandırma ayarlarından kaynaklanan nedenlerle tezin ikinci bölümünde kullanımı önerilen özelliklerin, her teşebbüste aynı etkinlikle kullanılamayacağına ilişkin öngörümüze ve bu öngörümüzün doğruluğunu teyit etmek amacıyla uyguladığımız anket çalışmasının sonuçlarına yer verilecektir. Avrupa Birliğine (AB) üye ülkelerin rekabet otoritelerinin Yİ'lerde adli bilişim aracı kullanım istatistiklerine değinilmesinin ardından Kurulun ve Avrupa Birliği Komisyonu Rekabet Genel Direktörlüğünün (Komisyon) Yİ yetkilerinin sınırları karşılaştırılacaktır. Çalışmanın sonunda ise, üçüncü bölümde bulunan örnek vaka üzerindeki incelemeden elde edilen geri besleme ışığında oluşturduğumuz, elektronik posta sunucularındaki özellikler ile adli bilişim aracının ortak kullanımını içeren hibrit süreç modeline ilişkin önerimiz ortaya konacaktır.

BÖLÜM 1

ELEKTRONİK POSTA HABERLEŞMESİ

Elektronik posta sistemleri istemci/sunucu ve web tabanlı olmak üzere iki şekilde çalışabilmektedir (Maras 2011, 249). İstemci/sunucu tabanlı sistemlerde elektronik posta iletişimi, organizasyon bünyesinde bulunan posta sunucuları aracılığıyla sağlanmaktadır. Elektronik posta sunucularında tutulan posta kutularında kayıtlı ögelere, kullanıcı bilgisayarlarında kurulu istemciler aracılığıyla erişilebilmektedir. Web tabanlı sistemlerde ise posta kutularına web tarayıcılar aracılığıyla erişilmekte ve ögeler elektronik posta servis sağlayıcıların internet üzerinde konumlandırdıkları sunucular üzerinde tutulmaktadır. Kurumsal ölçekteki şirketlerde istemci/sunucu tabanlı elektronik posta sistemleri kullanılması nedeniyle, tez kapsamında web tabanlı sistemlerde analiz konusuna değinilmeyecektir.

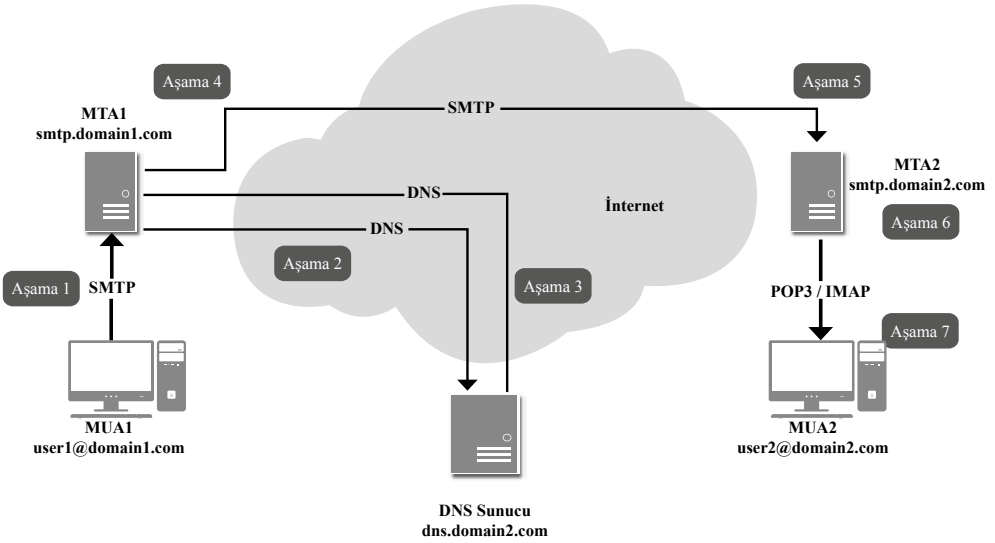
Microsoft Exchange, IBM Lotus Domino ve Novell Groupwise en sık kullanılan istemci/sunucu tabanlı elektronik posta sunucularından bazılarıdır. Radicati Group'un yayımladığı bir diğer raporda[7], Microsoft Exchange Server'ın, 2016 yılında %68'lik payla sunucu/istemci tabanlı elektronik posta sistemleri pazarındaki liderliğini koruyacağı öngörülmektedir. 2013 yılından bu yana, Rekabet Kurumu, Bilgi Yönetimi Dairesi olarak destek verilen Yİ'lerde, istemci/sunucu tabanlı elektronik posta altyapısına sahip teşebbüslerin %90'dan fazlasının Microsoft Exchange kullandıkları görülmüştür. Küresel ölçekte pazar lideri ve Yİ'lerde en sık karşılaşılan elektronik posta

[7] "Microsoft Exchange Server and Outlook Market Analysis, 2012-2016" http://www.radicati.com/wp/wp-content/uploads/2012/03/Microsoft-Exchange-Server-and-Outlook-Market-Analysis-2012-2016-Executive-Summary.pdf Erişim Tarihi: 05.04.2016

sunucusu olması nedeniyle, tez kapsamında "Microsoft Exchange Server" üzerinde yapılan incelemelere değinilecektir[8].

1.1. ELEKTRONİK POSTA İLETİM SÜRECİ

Elektronik postaların etkin bir biçimde analiz edilebilmesi için öncelikle mesajların ne şekilde iletildiğinin anlaşılması gerekmektedir (Guo vd. 2013, 341). İstemci/sunucu tabanlı sistemlerde elektronik posta iletim süreci en sade haliyle Şekil 1'de gösterilen yedi aşamayla özetlenebilir:



Şekil 1: Elektronik Posta İletişiminin Aşamaları (Banday 2011a, 228)

Aşama 1: Bu aşamada, *user1 (*MUA1[9]*)* kullanıcısı tarafından oluşturulan elektronik posta, *user2@domain2.com* adresine iletilmek üzere *domain1.com* "alan adına[10]" kayıtlı elektronik posta sunucusuna (MTA1[11]) gönderilmektedir.

[8] Kelime sınırlaması nedeniyle, diğer elektronik posta sunucuları çalışma kapsamı dışında bırakılmıştır.
[9] Mesaj Kullanıcı Aracı (*Message User Agent - MUA*)
[10] Alan adı, bir istemcinin internet üzerindeki başka bir bilgisayarı bulabilmesine imkân tanıyan sayısal adresler (IP) yerine kullanılan alfasayısal karakter dizileridir. Örneğin *amazon.com* bir alan adıdır (Rooksby 2015, 857).
[11] Mesaj Aktarım Aracı (*Message Transfer Agent - MTA*)

Aşama 2: MTA1 sunucusu, elektronik postanın gönderileceği adresin *alan adına* kayıtlı DNS[12] sunucusuna MX[13] sorgusu yaparak, hedef sistemin IP adresini öğrenmeye çalışır[14].

Aşama 3: DNS sunucusu, *domain2.com alan adına* ait elektronik posta sunucusunun (MTA2) IP adresini MTA1'e gönderir.

Aşama 4: Elektronik posta, MTA2 sunucusuna gönderilir.

Aşama 5: MTA1'in gönderdiği elektronik posta, MTA2'ye ulaşır.

Aşama 6: MTA2 sunucusu, gelen elektronik postayı *user2@domain2.com* posta kutusuna kaydeder.

Aşama 7: *user2* kullanıcısı *user1'*den gelen elektronik postayı, MUA2 aracılığıyla posta kutusunun (*user2@domain2.com*), kişisel bilgisayarında bulunan yerel kopyasına kaydeder.

1.1.1. Elektronik Posta İletiminde Görev Alan Bileşenler

1.1.1.1. Mesaj Kullanıcı Aracı (Message User Agent - MUA)

MUA, son kullanıcıların elektronik posta oluşturup göndermelerini ve gelen elektronik postaları okuyabilmelerini sağlayan, istemci bilgisayarların üzerinde kurulu uygulamalardır (Banday 2011a, 231). MUA, periyodik olarak posta kutusu içeriğini sunucu üzerinden kontrol etmek suretiyle (Otman 2014, 35) içeriğin güncel tutulmasını sağlar.

Çoğu kullanıcı tarafından elektronik posta programı olarak adlandırılan MUA'lara (Guo vd. 2013, 341), "Microsoft Outlook", "Lotus Notes", "Apple Mail" ve "Mozilla Thunderbird" örnek olarak verilebilir (Banday 2011a, 231). Tez kapsamında Microsoft Exchange sunucular üzerinde yapılan incelemelere değinileceğinden, uygulama örneklerinde MUA olarak "Microsoft Outlook" istemcisi seçilmiştir.

[12] Alan Adı Sistemi (*Domain Name System – DNS)*
[13] Posta Değiştirici (*Mail Exchanger – MX)*
[14] Bu aşamaya ilişkin detaylara, çalışmanın "1.1.2.2. Alan Adı Sistemi (Domain Name System – DNS)" başlığı altında yer verilmiştir.

1.1.1.2. Mesaj Aktarım Aracı (Message Transfer Agent - MTA)

Elektronik posta gönderimi yapan MUA'dan gelen verinin alıcı tarafa iletiminden sorumlu sistemler MTA olarak adlandırılmaktadır. MTA'lar, gelen elektronik postanın başlık bilgisini analiz ederek, hangi hedef sunucuya iletileceğini bilgisini öğrenir ve postayı alıcı MTA'sına gönderir (Guo vd. 2013, 341). MTA'lar arası elektronik posta iletimi esnasında SMTP[15] ve DNS protokolleri kullanılır (Crocker 2009, 22).

MTA'lar, elektronik posta iletiminin sağlanmasının yanında, kullanıcı posta kutularının saklanması ve organizasyonu gibi ek görevler de üstlenirler. Sendmail, Postfix, Exim, Exchange Server ve IBM Lotus MTA'lara örnek olarak verilebilir. Çalışmanın geri kalan kısmında MTA, elektronik posta sunucusu olarak adlandırılacaktır.

1.1.2. Elektronik Posta İletiminde Kullanılan Protokoller

1.1.2.1. Basit Posta İletim Protokolü (Simple Mail Transfer Protocol – SMTP)

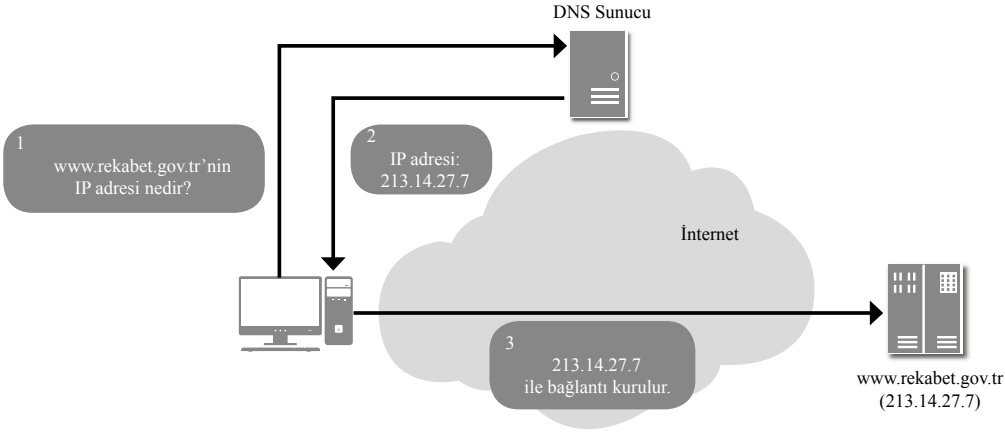
SMTP, ağlar arasında elektronik haberleşmenin standardize edilmesi amacıyla geliştirilmiş (Staden ve Venter 2010, 1) ve günümüzde elektronik postaların internet üzerinden iletiminde en sık kullanılan protokoldür. İlk olarak RFC 821[16] standardında tanımlanan SMTP, istemci/sunucu tabanlı bir protokol olup, gönderilen elektronik postaların iletiminin ne şekilde yapılacağına dair kuralları içermektedir (LaRoche vd. 2011, 154).

1.1.2.2. Alan Adı Sistemi (Domain Name System – DNS)

İnternete bağlı cihazlar[17] birbirleriyle, her cihaza atanmış tekil adresler aracılığıyla haberleşirler. IP olarak adlandırılan bu adresler, iletişim kurulacak hedef sistemin tanımlanmasında kullanılır. IP adresi, akılda tutulması zor[18] bir formata sahiptir. Bu nedenle, internete bağlı cihazlara IP adresi yerine *alan adı* kullanarak erişebilmeye olanak sağlayan DNS altyapısı geliştirilmiştir (Dostálek ve Kabelová 2006, 5). *Alan adı*

[15] Basit Posta İletim Protokolü (*Simple Mail Transfer Protocol – SMTP*)
[16] Standardın ilk hali RFC 821'dir (Postel 1982). Zaman içerisinde üç farklı sürümü yayımlanan standardın güncel versiyonu (draft) RFC 5321'dir (Klensin 2008).
[17] Kişisel bilgisayar, sunucu, akıllı telefon, yönlendirici, IP kameralar vb.
[18] Örneğin Kurum'un web sayfasının IP adresi, 213.14.27.7'dir.

bilgisi ve IP adresi eşleştirmesinin yapıldığı kayıtlar DNS sunucular üzerinde tutulur. Bir kullanıcı, web tarayıcının adres satırına *www.rekabet.gov.tr* yazdığında, ulaşılmak istenen *alan adının* IP adresi DNS sunucu üzerinden sorgulanarak öğrenilir. Hedef sunucu ile bağlantı, öğrenilen IP adresi aracılığıyla sağlanır (Bkz. Şekil 2).



Şekil 2: DNS ile Hedef Sistemin IP Adresinin Öğrenilmesi (A.g.k. 5)

Elektronik posta haberleşmesinde DNS sunucular, hedef elektronik posta sunucusunun IP adresinin öğrenilmesi esnasında aktif rol alırlar. Posta sunucularına ait *alan adı* ve IP adresi eşleştirme bilgisi DNS sunucuların MX tipi kayıtları üzerinde tutulur. MX kaydı, elektronik postanın *alan adı* üzerinde kayıtlı hangi sunucuya gönderileceğini belirtir (A.g.k. 85).

1.1.2.3. POP3/IMAP

POP3 (*Post Office Protocol version 3*) ve IMAP (*Internet Message Access Protocol*) protokolleri kullanıcıların, MTA'ya kaydedilen elektronik postalara MUA aracılığıyla erişebilmelerine imkân sağlamaktadır.

POP3 protokolü, elektronik posta sunucusunda bulunan elektronik postaların, posta kutusunun istemci bilgisayardaki yerel kopyasına indirilmesi işlemini gerçekleştirir (Myers ve Rose 1996, 2). Bu sayede kullanıcı, istemci-sunucu arasında çevrimiçi bağlantı kurulamasa dahi kullanıcının elektronik postalarına erişim imkânı elde edebilmektedir. IMAP protokolünden farklı olarak POP3'te, elektronik postalar

yerel istemciye indirildikten sonra sunucu üzerindeki kopyaları silinir (Maras 2011, 249).

IMAP protokolü, istemcilerin sunucu üzerindeki elektronik postalara erişim ve yönetimine olanak sağlar (Crispin 1994, 1). Maras (2011, 249)'a göre, POP3 kadar yaygın kullanılmasa da POP3'e göre daha esnek özelliklere sahiptir. IMAP'te elektronik postalar, indirildikten sonra bile sunucu üzerinde saklanmaya devam eder. Kullanıcılar IMAP protokolü sayesinde sunucular üzerindeki posta kutularını yönetebilme[19] imkânına sahiptir.

1.2. ELEKTRONİK POSTANIN UNSURLARI

1.2.1. Başlık bilgisi

Elektronik postalar başlık ve gövde olmak üzere temel iki bileşenden oluşmaktadır. Başlık bilgisi, son kullanıcı tarafından okunduğunda çok bir anlam ifade etmese de, adli analiz ve bilgi toplama açısından oldukça önemli veriler içermektedir (Önal 2009, 4).

Başlık bilgisinde, gönderen/alıcı ve elektronik postanın hedefine ulaşıncaya kadar takip ettiği yol hakkında veriler bulunmaktadır (Chhabra ve Bajwa 2015, 208). Elektronik posta analizi konusunda öne çıkan bazı başlık bilgisi alanları şu şekilde sıralanabilir:

2.2.1.1. Temel Alanlar

```
Received: from 81.214.185.147 .dynamic . ttnet. cam. tr (HELO LEAMEE)
(81.214.185.147)
   by  srv47. turhost . com with ESMTPA; 15 mAR 2016 12:08:15 +0200

Message-ID: <D450D047DA1147B2ACE9DC7FF06FCD0A@LEAMEE>
From: =?iso-8859-9?Q?DEN=DDZ_KAMACI?= <deniz.gok@canhastanesi.com.tr>
To :  =?iso-8859-9?B?1m1lciBGYXJ1ayDHRUzdSw==?= <ofcelik@rekabet.gov.tr>|
Subject: =?iso-8859-9?B?SEFLRUTd3kxFUg==?=
Date: Tue, 15 Mar 2016 12:06:41 +0200
MIME - Version: 1.0
Content - Type :  multipart / alternative ;
          boundary="----=_NextPart_000_000A_01D17EB3. 22FF7DB0"
X -Priority:  3
```

Şekil 3: Elektronik Posta Başlık Bilgisindeki Temel Alanlar.

[19] Oluşturma, silme, yeniden adlandırma, arama vb.

Kimden (From): Bu alan, mesajı gönderen kişinin elektronik posta adresini içerir. SMTP'de başlık bilgisinde yer alan veriler doğrulanmadığı için gönderilen elektronik postalar farklı bir adresten geliyormuş gibi gösterilebilmektedir (Maras 2011, 250).

Kime (To): Bu alanda, alıcının elektronik posta adresi bulunur.

Tarih (Date): Bu alanda tarih, gün, saat ve saat dilimi bilgisi kayıtlıdır. Elektronik postanın yollandığı bilgisayardaki zaman bilgisi kullanılarak doldurulur. Bilgisayardaki saat ayarı değiştirilerek (art niyetle ya da yanlışlıkla) elektronik postanın gönderim zamanını farklılaştırmak mümkündür[20].

2.2.1.2. X-Originating-IP

Bu alanda, elektronik postanın gönderildiği bilgisayarın IP adresi bulunmaktadır (A.g.k. 250). İstemci/sunucu tabanlı sistemlerde, mesajın gönderildiği elektronik posta sunucusunun IP adresi de bu alana yazılmaktadır (Banday 2011b, 57).

2.2.1.3. Received

Received alanında, elektronik postayı gönderen istemcinin IP adresi, elektronik postayı karşılayan sunucuya ait alan adı bilgisi (ya da IP adresi) ile iletim esnasında kullanılan internet protokol tipi ve mesajın sunucudan geçtiği ana ait tarih[21] bilgisi saklanmaktadır (Bkz. Şekil 4).

```
Received: (qmail 15202 invoked from network) ; 15 Mar 2016 12:08:15  +0200

Received: from 81 .214.185.147 .dynamic .ttnet.com.tr (HELO LEAMEE) (81.241.185.147)
   by  srv47 . turhost.com with ESMTPA;    15 Mar 2016  12:08:15  +0200
Message - ID:  <D450D047DA1147B2ACE9DC7FF06FCDOA@LEAMEE>
From:  =?iso-8859 - 9?Q?DEN=DDZ_KAMACI?=  <deniz.gok@canhastanesi.com.tr>
To:    - ?iso-8859 - 9?B?1m1lciBGYXJ1ayDHRUzdSw--?-    <ofcelik@rekabet.gov.tr>|
Subject:  =?iso-8859 - 9?B?SEFLRUTd3kxFUg==?=
Date:  Tue, 15 Mar 2016  12:06:41  +02000
MIME - Version: 1.0
Content - Type:  multipart / alternative ;
          boundry=''----=_NextPart_000_000A_01D17EB3 . 22FF7DB0''
```

Şekil 4: Received Alanı

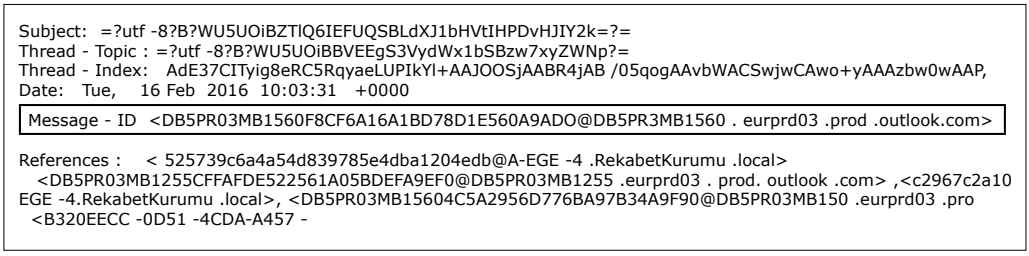
[20] A.g.k 250

[21] Gün, ay, yıl, saat ve saat dilimi.

Bazı elektronik postaların başlık bilgilerinde birden fazla *received alanı* bulunabilir. Bunun nedeni, elektronik postanın internet üzerinde iletilmesi esnasında çok sayıda *yönlendirici*[22] üzerinden geçiyor oluşudur. Her bir *yönlendirici* kendi IP adresi, protokol ve zaman bilgisini elektronik posta başlığına ekler. Böylelikle adli bilişim uzmanları, başlık bilgisinde bulunan *received alanları* üzerinden, elektronik postanın alındığı adresten geriye doğru kaynağının izini sürebilirler[23] (Maras 2011, 252).

2.2.1.4. Message ID

Message ID alanında, elektronik postanın gönderildiği sunucu tarafından her bir mesaj için ayrı olarak üretilen kimlik numarası bilgisi saklanmaktadır. Genellikle, rastlantısal olarak üretilen tekil bir karakter dizisini takip eden *alan adı* bilgisinden oluşmaktadır (Bkz. Şekil 5) (Banday 2011b, 59).



Şekil 5: Message ID Alanı

Bu alanda kayıtlı kimlik bilgisinin tekil yapıda oluşu, elektronik posta sunucularının iletim kayıtları üzerinde yapılacak adli incelemeler neticesinde mesajların hangi kaynaktan gönderildiğinin ve iletim esnasında hangi yolu takip ettiğinin tespit edilebilmesine imkân sağlamaktadır (Pasupatheeswaran 2008).

[22] Bilgisayar ağları arasında veri paketlerinin iletimini ve yönlendirilmesini sağlayan ağ cihazı.
[23] Elektronik posta başlık bilgisindeki *received* alanları, kaynak en altta olacak şekilde yukarı doğru sıralanır (Hedef sunucu en üstteki alanda saklanır).

2.2.1.5. X-Mailer

X-Mailer alanı, elektronik postanın gönderildiği istemcideki MUA bilgisini içermektedir. Aşağıda Outlook Express kullanılarak gönderilmiş elektronik postaya ait X-Mailer alanı bilgisi gösterilmektedir:

```
Content -Type:  multipart/ alternative ;
          boundary=”----=_NextPart_000_000A_01D17EB3 .22FF7DB0”
X -Priority:  3
X -MSMail -Priority: Normal
X -Mailer: Microsoft Outlook Express  6 .00.2900 .5931

X -MimeOLE :  Produced By Microsoft MimeOLE  V6. 00. 2900 .6157
X -EsetScannerBuild :    28582
X -Brightmail -Tracker:  H4sIAAAAAAAAA11TXUwcVRjl251uZ+1eGIa/yxSMHa2JrUApbUSjjTGtktg
```

Şekil 6: X-Mailer Alanı

1.2.2. Gövde ve Ekler

Elektronik postanın gövdesi, iletilmek istenen esas mesajın bulunduğu alandır (Guo vd. 2013, 341). Elektronik postayla birlikte, “ek” olarak adlandırılan dosyaların da gönderilmesi mümkündür. Gövdeye ilave edilen ekler, düz yazı olabileceği gibi resim, ses, program vb. tipte dosyalar da olabilmektedir (Durmaz 2014, 283).

Eklenmiş dosya, elektronik postanın iletimi esnasında Çok Amaçlı Internet Posta Uzantıları (Multipurpose Internet Mail Extensions - MIME) olarak adlandırılan bir formata dönüştürülür (Guo vd. 2013, 341). MIME ile, eklenmiş dosyanın gönderen bilgisayarda şifrelenmesi ve alıcı bilgisayarda çözümlenmesi sağlanmaktadır. Böylelikle elektronik postayı alan kişi eklenmiş dosyayı yerel diskine kopyalayabilmektedir (Durmaz 2014, 283).

1.3. ELEKTRONİK POSTALAR ÜZERİNDE ADLİ İNCELEME

1.3.1. Adli Bilişim Uzmanları Açısından İnceleme

Milyonlarca kullanıcı her gün kişisel ya da ticari faaliyetleriyle alakalı elektronik posta yoluyla iletişim kurmaktadır. Elektronik posta haberleşmesinin hayatın vazgeçilmez bir parçası olduğu günümüz dünyasında, siber suçlular da art niyetli amaçlarına ulaşmak için elektronik postaları bir araç olarak kullanmaktadır (Chhabra ve

Bajwa 2015, 201). Dolayısıyla bilişim yoluyla işlenen suçların soruşturulması esnasında elektronik postaların analiz edilmesi, adli bilişim uzmanlarınca gerçekleştirilecek incelemelerin kaçınılmaz bir parçası konumundadır.

Elektronik postaların adli analizi, gönderen/alıcı kimliğinin tespiti, gönderim/erişim zamanının belirlenmesi gibi kaynak ve içerik üzerinde yapılacak çalışmaları kapsamaktadır (Banday 2011b, 50). Bu bilgilerin neredeyse tamamı elektronik posta başlık bilgisinde bulunmaktadır. Başlık içinde bulunan en yararlı bilgilerden birisi olan "gönderici IP adresi" sayesinde elektronik postanın izinin sürülmesi mümkün olmaktadır. Gönderim yapan elektronik posta sunucusu tarafından, iletilen mesaja verilen tekil kimlik numarası sayesinde; elektronik postanın hedef posta kutusuna kadar takip ettiği sanal yol belirlenebilmektedir (Markagić 2013, 115). Elektronik postaların ne zaman gönderildiğine ya da alındığına ilişkin verilere, yine başlık bilgisi analiz edilerek ulaşılabilmektedir.

SMTP'de başlık bilgisinin şifrelenmeden iletiliyor oluşu (*clear text*), başlık bilgisi üzerindeki verinin kolaylıkla manipüle edilebilmesine imkân sağlamaktadır (Staden ve Venter 2010, 1). Bu nedenle yalnızca mesaj üzerinde inceleme yapmakla yetinilmeyip, elektronik postanın gönderildiği/alındığı bilgisayarlarda ve iletildiği sunuculardaki kayıtlarda da adli analiz yapılmaktadır (Banday 2011b, 50).

Elektronik posta analiz sürecinde adli bilişim uzmanlarının işini kolaylaştırıcı birçok yazılım tasarlanmıştır. Bu araçlardan bir kısmı sadece elektronik posta analizi amacıyla üretilmişken, bazıları ise diğer adli analiz alanlarında da işlem yapabilecek yetkinliktedir (Chhabra ve Bajwa 2015, 209).

1.3.2. Rekabet Uzmanları Perspektifinden İnceleme

Meslek personelince gerçekleştirilen Yİ'lerde, teşebbüs çalışanlarına ait posta kutularında yapılan incelemeler Yİ'nin en kritik noktasını oluşturmaktadır. Rekabet uzmanları, adli bilişim uzmanlarına ait elektronik posta analizi yaklaşımından farklı olarak, posta kutuları üzerinde anahtar kelime aramalarına yoğunlaşmaktadır. Teşebbüs çalışanlarına ait posta kutularında, rekabet ihlallerine ilişkin iletişim kayıtlarının aranması her Yİ'de rutin olarak yapılan öncelikli bir prosedür halini almıştır.

Meslek personelince belirlenen anahtar kelimeler, elektronik postaların başlık, gövde ve eklerinde aranmaktadır. İncelenen posta kutularındaki ögelerin sayısının çokluğu göz önünde bulundurulduğunda, arama işleminin hızı ve sonuçların doğruluğu önem kazanmaktadır. Rekabet uzmanlarının çok sayıda anahtar kelimeyi hızlı bir şekilde tüm posta kutusunda arayabilmeleri, *indeksleme* servisi sayesinde mümkün olmaktadır. İndeksleme işleminde, arama yapılacak veri üzerinde bulunan tüm kelimeler tespit edilerek, veri üzerinde bulundukları yer bilgisi ile birlikte veri tabanına kaydedilmektedir (Durmaz 2014, 286). Anahtar kelime araması esnasında veri tabanından kelimenin geçtiği alanlar sorgulanarak hızlıca sonuca ulaşılabilmektedir[24].

Anahtar kelime araması, inceleme esnasında posta kutusunda bulunan ögeleri kapsamaktadır. Oysa mevcut ögelerin incelenmesi kadar, silinmiş elektronik postaların tekrar elde edilerek aramalara dâhil edilmeleri de önemlidir (Çakır ve Kılıç 2013, 38). Böylelikle, bilgisayarlarında inceleme yapılan teşebbüs çalışanlarınca bilinçli ya da bilinçsiz olarak silinen elektronik postalarda bulunabilecek olan, rekabet ihlaline ilişkin delillere ulaşılabileceği düşünülmektedir.

Meslek personelince gerçekleştirilen Yİ'ler, RKHK'nin 15. maddesinden alınan yetkiyle, "4054 Sayılı Rekabetin Korunması Hakkında Kanun'un Uygulanması Çerçevesinde Rekabet Kurumunca Yapılacak Yerinde İncelemelere İlişkin Usul Ve Esaslara Dair Yönerge'ye (YİY)" göre yürütülmektedir. Mevcut uygulamada, teşebbüs çalışanlarına ait elektronik ortamda saklanan verilerin incelenmesi esnasında herhangi bir adli bilişim aracı kullanılmamaktadır. Elektronik posta incelemeleri, Microsoft Outlook üzerinde anahtar kelime araması yapmak suretiyle gerçekleştirilmektedir. Tezin ikinci bölümünde, adli bilişim aracı kullanmaksızın gerçekleştirilebilecek elektronik posta analizi için takip edilmesi önerilen işlem adımlarına değinilecektir. Üçüncü bölümde ise, adli bilişim araçlarının elektronik posta analiz kabiliyetleri karşılaştırılacaktır.

[24] Microsoft Outlook üzerinde gerçekleştirilen anahtar kelime aramalarında, arka planda çalışan "Windows İndeksleme Motoru" kullanılmaktadır. Windows'un indeksleme hızıyla diğer adli bilişim araçlarının indeksleme performanslarının karşılaştırıldığı çalışmaya üçüncü bölümde yer verilecektir.

BÖLÜM 2

ELEKTRONİK POSTA SUNUCULARI ÜZERİNDE İNCELEME

İş süreçlerinde yoğun şekilde bilişim sistemlerini kullanan teşebbüslerde gerçekleştirilen Yİ'lerde, bilgisayarlar üzerinde yapılan anahtar kelime aramaları incelemelerin bel kemiğini oluşturmaktadır. Teşebbüs çalışanlarına ait elektronik postaların incelenmesi esnasında kullanılan anahtar kelimeler, o an posta kutusunda kayıtlı ögeleri kapsamakta; kullanıcı tarafından silinmiş postalar aramalara dâhil edilmemektedir. Çalışanların delil karartma amacıyla elektronik postaları silme riski de göz önünde bulundurulduğunda, posta kutularından silinmiş ögelerin kurtarılarak incelemeye dâhil edilmesi büyük önem taşımaktadır. Bu amaçla geliştirilmiş ve etkinliğini kanıtlamış çok sayıda adli bilişim aracı bulunmasına rağmen, Kurum tarafından benimsenen Yİ usulü uyarınca bu tip yazılımlar inceleme esnasında kullanılmamaktadır.

Çalışmanın bu bölümünde Microsoft Exchange[25] sunucular üzerinde adli bilişim aracı kullanmaksızın uygulanabilecek, veri kaybını önleyici koruma ve kurtarma özellikleri detaylıca işlenecektir. Posta kutuları üzerinde yapılan anahtar kelime aramalarının etkinliğini artırıcı Exchange sunucu özellikleri ile birlikte Yİ'nin zorlaştırılması durumunun tespiti ve ispatlanması konusunda uygulanabilecek adımlara ilişkin öneriler de bölüm içerisinde değinilecek diğer konu başlıklarıdır.

[25] Tez boyunca kullanılan yazılımların sürüm bilgilerine EK-1'de yer verilmiştir.

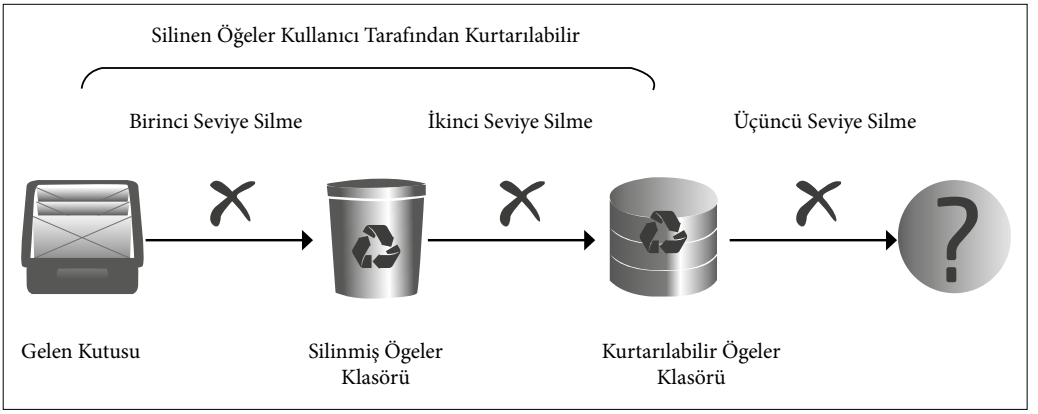
2.1. SİLİNMİŞ POSTALARIN GERİ GETİRİLMESİ

Exchange sunucular, silinen elektronik postaların kurtarılması konusunda kullanıcılara ve yöneticilere önemli kolaylıklar sunmaktadır. Standart kullanıcılar belirli bir aşamaya kadar silinen elektronik postaları kurtarabilirler. Daha ileri seviyelerde kurtarma yapabilmek için özel yetkilere sahip yönetici grubuna üye olmak gereklidir. Microsoft Exchange sunucu üzerinde elektronik posta silme-kurtarma döngüsü şu aşamalardan oluşur:

- **Birinci Seviye Silme (*delete*):** Kullanıcı, posta kutusunda bulunan herhangi bir ögeyi silerse, bu öge **silinmiş** öge**ler klasörüne** (*deleted items*) taşınır. Kullanıcı bu klasöre giderek sildiği elektronik postayı geri getirebilir (Şahin 2014, 454).
- **İkinci Seviye Silme** (***soft delete*):** Kullanıcı, *silinmiş* öge*ler klasöründe* bulunan bir ögeyi siler ya da posta kutusundaki bir ögeyi *Shift+Del* tuş kombinasyonuyla kaldırırsa; bu öge **kurtarılabilir** öge**ler klasörüne** (*recoverable items*) taşınır. Silinen öge, bu aşamada da kullanıcı tarafından kurtarılabilir.
- **Üçüncü Seviye Silme** (***hard delete*):** Bir posta kutusu üzerinde *hard delete* işlemi üç farklı şekilde gerçekleşebilir.
  - *Kurtarılabilir* öge*ler klasöründen* bir posta silindiğinde
  - *Kurtarılabilir* öge*ler klasöründeki* elektronik postanın *yaşlanma süresi*[26] dolduğunda
  - *Kurtarılabilir* öge*ler klasörünün* kotası[27] dolduğunda

[26] Elektronik postalar, kurtarılabilir ögeler klasöründe; Exchange sunucu üzerinde ayarlanan **silinen** öge **saklama süresi** (*deleted item retention period*) boyunca tutulur. Bu sürenin varsayılan değeri 14 gündür (Morimoto vd. 2012, 322). Sürenin dolmasının ardından elektronik posta bu klasörden otomatik olarak kaldırılır.

[27] Bu değer her bir posta kutusu için varsayılan olarak 30 GB'dir. Kota dolduğunda dizine ilk gelen elektronik postadan başlanmak üzere silme işlemi otomatik olarak gerçekleştirilir.



Şekil 7: Elektronik Posta Silme-Kurtarma Seviyeleri

Standart kullanıcı yetkisiyle *ikinci seviyeye* kadar silinmiş postalar *kurtarılabilir* öge*ler klasöründen* rahatlıkla çağrılabilir. Ancak Yİ'nin sağlıklı olarak yerine getirilebilmesi için üçüncü seviye silinmiş ögelerin de kurtarılarak anahtar kelime aramalarına dâhil edilmesi gerektiği düşünülmektedir.

Exchange sunucularda, herhangi bir adli bilişim aracı kullanmaksızın üçüncü seviye silinmiş ögeler belirli koşullar altında kurtarılabilmektedir. Tezin bu kısmında sırasıyla, üçüncü *seviye silinmiş* ögelerin kurtarılmasına imkân veren *tek* öge *kurtarma* ve *koruma* özelliklerine ve bu özelliklerin kullanımı sırasında aktif rol alan *kurtarılabilir* öge*ler klasörünün* yapısına değinilecektir. Sonrasında, silinmiş postalara erişim konusunda bir diğer seçenek olan *kurumsal yedek* kavramı açıklanmaya çalışılacaktır.

2.1.1. Tek Öge Kurtarma (Single Item Recovery) Özelliği

Kurtarılabilir öge*ler klasöründe* bulunan elektronik postaların üçüncü seviye *silme* işlemine maruz kalması durumunda, silinen ögeler kullanıcı tarafından kurtarılamaz duruma gelir. Bu durumdaki postaların kurtarılma işlemi Microsoft Exchange sunucularda *tek* öge *kurtarma* olarak adlandırılır ve bu kurtarma işlemi ancak sistem yöneticileri tarafından yapılabilir.

Kullanıcı üçüncü seviye silme işlemini farkında olmaksızın yapabileceği gibi, Yİ öncesinde ya da esnasında delil karartma amacıyla da gerçekleştirebilir. Bu nedenle

posta kutusu üzerinde incelemeye başlamadan önce *tek* öge *kurtarma* işleminin mutlak suretle yapılması gerektiği düşünülmektedir.

Tek öge *kurtarma* işlemi, Exchange sunucular üzerinde tanımlı *discovery management* grubuna üye yetkili kullanıcı tarafından **keşif araması** (*in-place eDiscovery*) özelliği kullanılarak yapılabilmektedir. *Keşif araması* konusuna ve kurtarma işlemi yapılırken takip edilmesi gereken adımlara ilişkin detaylara çalışmanın "2.2. Keşif Araması (In-Place Edıscovery) ile Tüm Posta Kutuları Üzerinde Arama" başlıklı bölümünde yer verilecektir.

2.1.2. Koruma (In-Place Hold)

Kurumsal ölçekteki şirketler, organizasyonel ya da hukuki gerekçelerle çalışanları tarafından gerçekleştirilen elektronik posta iletişimini denetlemek amacıyla katı kullanım ilkeleri oluşturma gereği duymaktadır. Fikri haklar, ticari sırlar, iş planları ya da kişisel mahremiyete ilişkin bilgiler gibi şirketler açısından hassas kabul edilen verilerin elektronik posta yoluyla dışarı sızdırılma ihtimali de bu gerekliliği doğuran bir diğer gerekçe olarak kabul edilebilir (Mota 2014a). Microsoft Exchange Sunucu ailesi sahip olduğu **koruma** (*in-place hold*) özelliği sayesinde, istenilen posta kutusu üzerindeki ögelerin silinmeye veya değiştirilmeye karşı, sınırsız ya da belirli süre boyunca muhafaza altına alınabilmelerine imkân sağlar. Yİ esnasında incelenen posta kutularında bulunan *koruma* altındaki ögeler, kullanıcılar tarafından üçüncü seviye silme işlemine tabi tutulsalar dahi, kurtarılarak anahtar kelime aramalarına dâhil edilebilmektedir.

Exchange sunucularda, posta kutusu ögelerinin *koruma* altına alınabilmesi için ögenin, sistem yöneticisi tarafından tanımlanmış *koruma ilkeleriyle* eşleşmesi gerekmektedir. Herhangi bir ögenin ilkelerden en az birisiyle eşleşmesi durumunda, sunucu üzerinde otomatik olarak gerçekleşen kopyalama ve yazma işlemleriyle birlikte ögenin hem orijinal hem de değişikliğe uğramış sürümü *koruma* altına alınır.

Microsoft Exchange Server 2013'te ögelere uygulanabilecek *koruma ilkeleri* dört temel başlık altında toplanabilir:

- **Süresiz Koruma (*Indefinite hold*):** Elektronik posta kutusundaki tüm ögeler, süresiz olarak silinmeye karşı koruma altına alınır (Şahin 2014, 328). Bu koruma, özellik devre dışı bırakılmadığı sürece devam eder.
- **Zaman Tabanlı Koruma (*Time-based hold*):** Bu özellik sayesinde yöneticiler, posta kutusu ögelerinin tam olarak ne kadar süre boyunca saklanacağını belirleyebilmektedirler. Bu süre ögenin alındığı ya da oluşturulduğu andan itibaren hesaplanmaya başlanır. Örneğin 365 günlük koruma tanımlanmış bir posta kutusunda, 300 gün önce alınmış bir elektronik postanın silinmesi halinde, bu öge tamamen silinmeden önce ilave olarak 65 gün daha muhafaza edilir (Mota 2014a).
- **Sorgu Tabanlı Koruma (*Query-based hold*):** Bu özellikteki korumada posta kutusundaki tüm ögeler yerine; anahtar kelime, gönderen/alıcı bilgisi, başlangıç/bitiş tarihi, öge tipi (posta, takvim, toplantı) gibi belirli sorgu parametrelerine uyan ögeler *koruma* altına alınır (Şahin 2014, 328). *Sorgu tabanlı koruma* oluşturulduktan sonra, üzerindeki sorgu parametrelerine uyan (posta kutusunda bulunan ve gelecekte oluşturulacak) tüm ögeler *koruma* altına alır (Mota 2014a).
- **Çoklu Koruma:** Birden fazla *koruma* tipi aynı anda uygulanabilmektedir. Bu tür durumlarda tüm *korumalar VEYA* (OR) operatörüyle birleştirilir. Bir posta kutusu üzerinde uygulanan koruma sayısı beşten fazla olursa, hesap üzerinde otomatik olarak *süresiz koruma* başlatılır.

Koruma altındaki ögeler, posta kutusunun *kurtarılabilir* öge*ler klasörünün* alt dizinlerinde muhafaza edilir. Bu ögeler *tek* öge *kurtarma* özelliğinde olduğu gibi, *keşif aramaları* aracılığıyla kurtarılarak inceleme yapılacak posta kutusuna taşınabilmektedir. Böylelikle teşebbüs çalışanlarınca tamamen silindiği düşünülen *koruma* altındaki ögeler, anahtar kelime aramalarına dâhil edilebilmektedir.

2.1.3. Litigation Hold

İlk olarak Microsoft Exchange'in 2010 sürümüyle getirilen bu özellik sayesinde kullanıcı posta kutusundaki ögeler herhangi bir koşula bağlanmaksızın silinmeye karşı koruma altına alınmaktadır. *Litigation Hold* özelliği aktifleştirilmiş posta kutularında,

kullanıcıların içgüdüsel olarak ögeleri gizlemesi ya da yok etmesi engellenmektedir. Bu özellik kullanımı bakımından, Exchange 2013'ün *süresiz koruma* özelliğine çok benzemekle birlikte, arka planda gerçekleşen işlemler açısından bazı teknik farklılıklar taşımaktadır. Bu farklılıklara ilişkin teknik detaylara çalışmanın bir sonraki başlığında değinilecektir.

2.1.4. Kurtarılabilir Ögeler Klasörü

Kurtarılabilir Öge*ler Klasörü,* silinmiş elektronik postaların kurtarılması amacıyla Yİ'lerde kullanımı önerilen *koruma*, *tek* öge *kurtarma ve litigation hold* özelliklerinin uygulanması esnasında aktif rol üstlenmektedir. İkinci ve üçüncü seviye silme işlemine tabi tutulan elektronik postalar bu klasör içerisine taşınır. Bu dizin kullanıcı posta kutusu bünyesinde bulunan ayrı bir depolama alanı olup, Outlook istemci üzerinden doğrudan görüntülenemez[28].

Kurtarılabilir öge*ler klasörü* şu alt dizinlerden oluşur:

- **Deletions:** *Silinmiş* öge*ler* klasöründe bulunan bir elektronik posta silindiğinde, *kurtarılabilir* öge*ler klasörü* altında bulunan bu alana taşınır. Bu alt klasördeki ögeler kullanıcı tarafından Outlook ve Outlook Web App (OWA)[29] üzerinden kurtarılabilir (Elfassy 2013, 713).
- **Purges:** *Kurtarılabilir* öge*ler klasörü* içinde bulunan bir elektronik posta kullanıcı tarafından silindiğinde ya da posta kutusu için tanımlı *silinen* öge *saklama süresi* dolduğunda ilgili öge bu klasöre taşınır (Mota 2014b). Taşınan öge, Microsoft Exchange sunucularda tanımlı *Managed Folder Assistant* (MFA) hizmetinin otomatik[30] olarak devreye girmesiyle kalıcı olarak silinir. Bu durumun istisnası posta kutusu üzerinde *tek* öge *kurtarma* ya da *litigation hold* özelliklerinden en az birinin aktif edilmiş olmasıdır. *Tek*

[28] Kullanıcı posta kutusunda bulunan kurtarılabilir ögeler klasörünü görüntülemek için MFCMAPI aracı kullanılabilir. MFCMAPI ile kurtarılabilir ögeler klasörü ve alt dizinlerinin nasıl görüntüleneceğine ilişkin detaylara EK-2'de yer verilmiştir.

[29] Outlook Web App (OWA), Microsoft Exchange kullanıcılarının posta kutularına web tarayıcısı üzerinden ulaşmalarına imkân sağlayan platformdur.

[30] MFA, zamanlanmasına gerek olmaksızın sürekli olarak çalışan bir servistir. Sistem kaynaklarının kullanımının artması durumunda otomatik olarak devreye girer. Detaylı bilgi için bkz. https://technet.microsoft.com/en-us/library/bb123958(v=exchg.150).aspx Erişim Tarihi: 05.04.2016

öge *kurtarma* özelliğinin kullanılması durumunda bu klasöre taşınan ögeler varsayılan olarak 14 gün daha burada tutulur. Bu sürenin dolmasıyla birlikte MFA yine devreye girerek ögeleri kurtarılamayacak şekilde siler. *Litigation hold* durumunda ise *koruma* altındaki ögeler *koruma* kalkıncaya kadar bu klasörde saklanmaya devam eder.

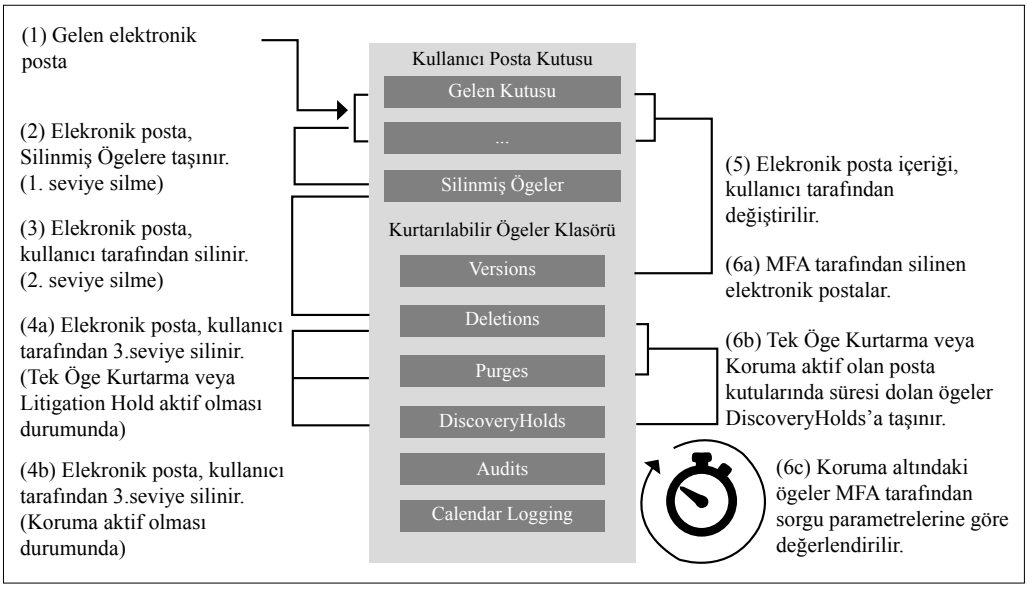
- **DiscoveryHolds:** Kullanıcı posta kutusu üzerinde *koruma* özelliği aktifleştirilse, *koruma ilkelerinden* herhangi biriyle eşleşen ve üçüncü seviye silme işlemine uğrayan ögeler, bu alana taşınır. Taşınan ögeler üzerlerindeki *koruma* kaldırılıncaya kadar burada muhafaza edilmeye devam eder (Şahin 2014, 458).
- **Versions:** *Koruma* altındaki ögelerin orijinal halleriyle birlikte, belirli alanları[31] değişikliğe uğramış sürümleri de saklanmaktadır. Bu ögelere ilişkin tüm sürümler *versions* klasörü altında tutulur.
- **Audits:** *Posta kutusu denetim kayıtları*[32] özelliği etkinleştirilmişse, erişim kayıtları bu klasörde saklanır.
- **Calendar Logging:** Bu klasör, posta kutusu üzerinde takvim kayıt özelliğinin etkinleştirilmesi durumunda, takvim üzerinde yapılan değişiklikleri saklamak için kullanılır (Mota 2014b).

Şekil 8'de, *kurtarılabilir* öge*ler klasörü* ve *alt dizinlerine*, silinen elektronik postaların uğradığı aşamalara ve *tek* öge *kurtarma*, *koruma/litigation hold* özelliklerinin kullanımı durumunda takip edilen iş akış süreçlerine ilişkin detaylar özetlenmiştir[33].

[31] Konu, gövde, ek, gönderen/alıcı bilgisi vb.

[32] Posta kutusu denetim kayıtları, kullanıcının posta kutusu üzerinde gerçekleştirdiği eylemlerin kayıt altına alınmasına yarar. Bu kayıtlara çalışmanın "3.3.2.1 Posta Kutusu Denetim Kayıtları" başlığı altında detaylıca değinilecektir.

[33] https://technet.microsoft.com/en-us/library/ee364755(v=exchg.150).aspx Erişim Tarihi: 05.04.2016



Şekil 8: Kurtarılabilir Ögeler Klasörü ve Elektronik Posta Silme Döngüsü[34]

2.1.5. Kurumsal Yedekler Üzerinden Silinmiş Elektronik Postalara Erişim

Kurum ve kuruluşlar, günlük iş süreçlerinin birçoğunu bilgi teknolojileri altyapısı üzerinden yürütmektedir. İşletmelerin bilgi teknolojilerini kullanmaları yönetim, hizmet ve üretim faktörleri performanslarına katkı sağlamış ve verimliliği artırmada belirleyici bir unsur olmuştur (Dulkadir ve Akkoyun 2013, 73).

Bilişim altyapısı üzerinden yürütülen süreçlerin iş sürekliliğini[35] sağlamak amacıyla, kritik sistemlerin yedeklerinin alınarak saklanması ihtiyacı doğmuştur. Kritik sistemlerin yedeklenmesi konusuna, bilgi güvenliği alanında kabul gören birçok standartta değinilmektedir. Örneğin, *TS ISO/IEC 27001:2013* standardının[36], "A.12.3 Yedekleme" maddesinde, üzerinde anlaşılmış bir yedekleme politikası doğrultusunda kritik sistemlerin veri kaybını önlemek amacıyla yedeklenmesi gerektiği belirtilmektedir.

[34] https://technet.microsoft.com/en-us/library/ee364755(v=exchg.150).aspx Erişim Tarihi: 05.04.2016
[35] İş sürekliliği, kurumun kritik iş süreçlerinin devamlılığını sağlamak, sağlanamadığı durumlarda öngörülen kesinti süreleri içerisinde yeniden çalışır hale getirmek için gerçekleştirilen çalışmalara verilen isimdir (Akyol 2013, 17).
[36] (TSE 2013).

İşletmeler açısından kritik bilişim altyapılarından biri de elektronik posta sunucularıdır. Posta kutularını içeren veri tabanlarının yedekleri, düzenli aralıklarla alınarak saklama kapasitesinin el verdiği sürece muhafaza edilmektedir. Yİ esnasında, teşebbüslerce alınmış posta kutusu yedeklerinin, silinmiş elektronik postaların geri getirilmesi için kullanılabileceği düşünülmektedir. Benzer şekilde, Yİ'nin yapıldığı tarih öncesinde işten ayrılmış eski teşebbüs çalışanlarının geçmiş dönemki elektronik postalarına da bu yedekler aracılığıyla ulaşılabilir.

Microsoft Exchange sunucularda, veritabanı yedekleme süreci, üçüncü parti yazılımlar[37] aracılığıyla etkin bir şekilde yönetilebilmektedir. Nesne tabanlı yedekleme imkânı sunan bu yazılımlar aracılığıyla, belirlenen tarih aralığındaki yedekler posta kutusu, klasör ve hatta öge bazında kurtarılabilmektedir. Yİ'lerde rekabet uzmanlarınca incelenecek posta kutusu, bir gün önceki yedeklenmiş haliyle karşılaştırılarak; teşebbüs çalışanı tarafından çok sayıda elektronik postanın silinip silinmediği tespit edilip, yedekleme yazılımı üzerinden silinen ögelerin kurtarılması sağlanabilir.

Çalışmanın EK-3 bölümünde, kurumsal yedekler konusunda yetkinliğini kanıtlamış ve sıkça kullanılan bir üçüncü parti yedekleme çözümü aracılığıyla posta kutusundan kalıcı olarak silinen ögelerin nasıl kurtarılabileceğine ilişkin işlem adımlarına ve detaylara yer verilmektedir.

2.2. KEŞİF ARAMASI (IN-PLACE EDISCOVERY) İLE TÜM POSTA KUTULARI ÜZERİNDE ARAMA

Yİ'ler esnasında, inceleme süresinin kısalığı ve Yİ'ye katılan meslek personeli sayısının sınırlı olması gibi nedenlerden ötürü ancak belirli sayıda teşebbüs çalışanının posta kutusu incelenebilmektedir. İncelenecek kişiler belirlenirken, teşebbüsün Yİ'ye konu olan biriminde görevli çalışanlar ve üst yönetim kadrosu üzerine yoğunlaşılarak mümkün olduğunca çok personelin bilgisayarı ve posta kutusu incelenmeye çalışılmaktadır. Bu yöntem, rekabet ihlaline ilişkin önemli delilleri içeren posta kutularının göz ardı edilmesi riskini de beraberinde getirmektedir. Bu riski en aza indirmek amacıyla, incelenecek teşebbüs çalışanları belirlenirken Exchange sunucuların

[37] Yazılımın kullanılacağı platform üreticisinden bağımsız kişi ya da kuruluşlarca geliştirilen uygulamalar.

keşif araması özelliğinin kullanılmasının incelemeleri daha etkin hale getireceği düşünülmektedir.

Keşif araması özelliği sayesinde sunucuda tanımlı tüm posta kutuları ya da seçilen belirli sayıdaki posta kutusu üzerinde aynı anda anahtar kelime araması yapmak mümkündür. Çoklu posta kutusu araması olarak da adlandırılan bu özellik sayesinde Yİ öncesi hazırlanan anahtar kelime listesi, tüm posta kutuları üzerinde kolaylıkla taranabilmektedir.

Çoklu posta kutusu aramaları; gelen kutusu, gönderilmiş ögeler, silinmiş ögeler gibi standart posta kutusu bileşenlerinin yanında *kurtarılabilir* öge*ler klasörüne* ve onun *alt dizinlerini* de (deletions, purges, discoveryholds vb.) kapsamaktadır. Bu sayede, *tek* öge *kurtarma* ve *koruma* özellikleri aktifleştirilmiş posta kutularında, üçüncü seviye silme işlemine uğrayan ögeler de aramalara dâhil edilmektedir.

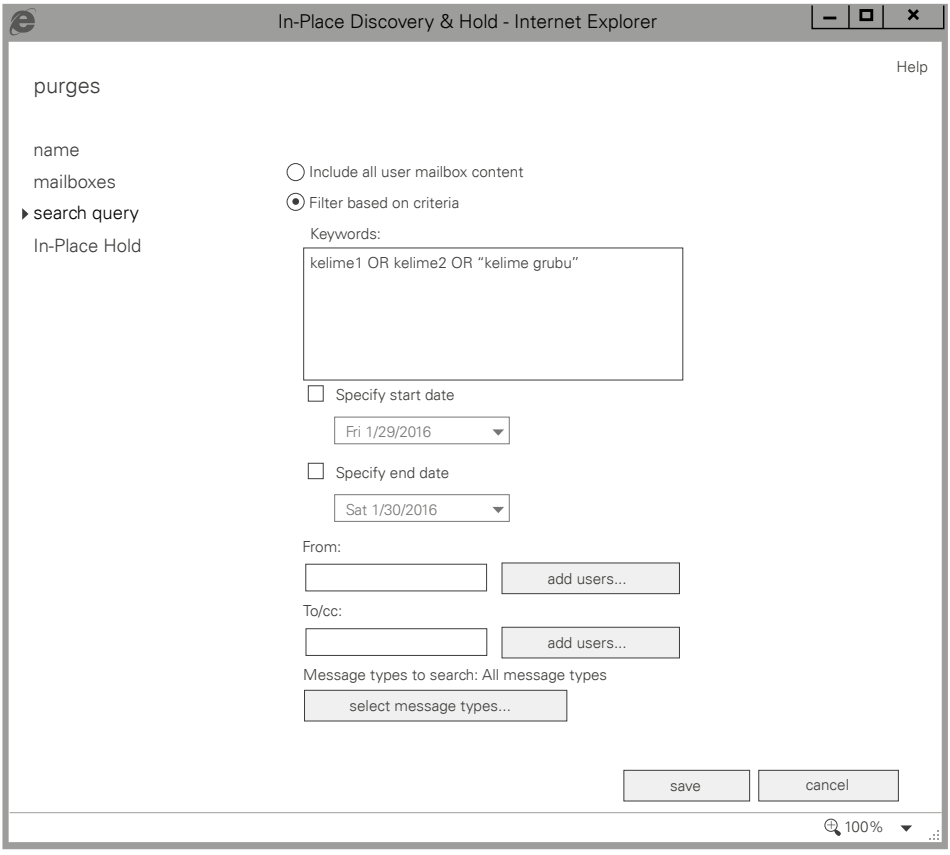
Keşif özelliği, inceleme yapılacak teşebbüs çalışanlarının tespiti ve önceliklendirilmesi konularında da önemli avantajlar sağlamaktadır. Örneğin, RKHK'nin 4. maddesinin ihlaline ilişkin bir dosyada, ihlale karıştıkları düşünülen teşebbüslerin *alan adları* anahtar kelime listesi olarak hazırlanıp çoklu posta kutusu aramasına tabi tutulursa, rakip teşebbüs çalışanlarıyla iletişime geçmiş personel tespit edilerek yerinde incelemenin bu şahıslar üzerinde yoğunlaştırılması sağlanabilir.

Çoklu posta kutusu arama özelliği ile tüm mesajlaşma trafiği üzerinde arama yapılabildiği için bu hakka erişim Exchange sunucu ortamında sınırlı tutulmuştur (Şahin 2014, 337). Keşif araması yapacak kullanıcının Microsoft Exchange üzerinde "Discovery Management" isimli yetki grubuna üye olması gerekmektedir. Arama sonuçları *keşif arama posta kutusuna* denilen özel bir posta kutusu üzerinde tutulur. *Discovery management* grubuna üye, *keşif araması* yapmaya yetkili kullanıcılar bu posta kutusu üzerinde **tam denetim yetkisine**[38] (*full-access permission*) sahiptir (Wesselius 2013, 211).

[38] Hedef posta kutusunda bulunan ögeleri görüntüleyebilme olanağı tanıyan erişim yetkisi.

Keşif aramaları, Exchange Server 2013'ün web tabanlı yönetim arayüzü olan *Exchange Admin Center* (EAC)[39] üzerinden ya da *exchange-powershell* komutları kullanılarak yapılabilir.

EAC üzerinden gerçekleştirilen çoklu posta kutusu aramalarında çeşitli filtreler kullanılabilmektedir. Bu filtreler; gönderen/alıcı bilgisi, tarih aralığı, öge tipi seçimi (posta, takvim, görevler vb.), anahtar kelime belirleyebilme gibi oldukça detaylı seçenekler sunmaktadır (Bkz. Şekil 9).



Şekil 9: Keşif Arama Sorgusu Ekranı

[39] Exchange Admin Center, Microsoft Exchange 2013'ün yeni web tabanlı yönetim aracına verilen isimdir (Hallberg 2014, 268). Elektronik posta altyapısına ilişkin tüm tanımlamalar ve yapılandırma değişiklikleri bu ara yüz aracılığıyla yapılır.

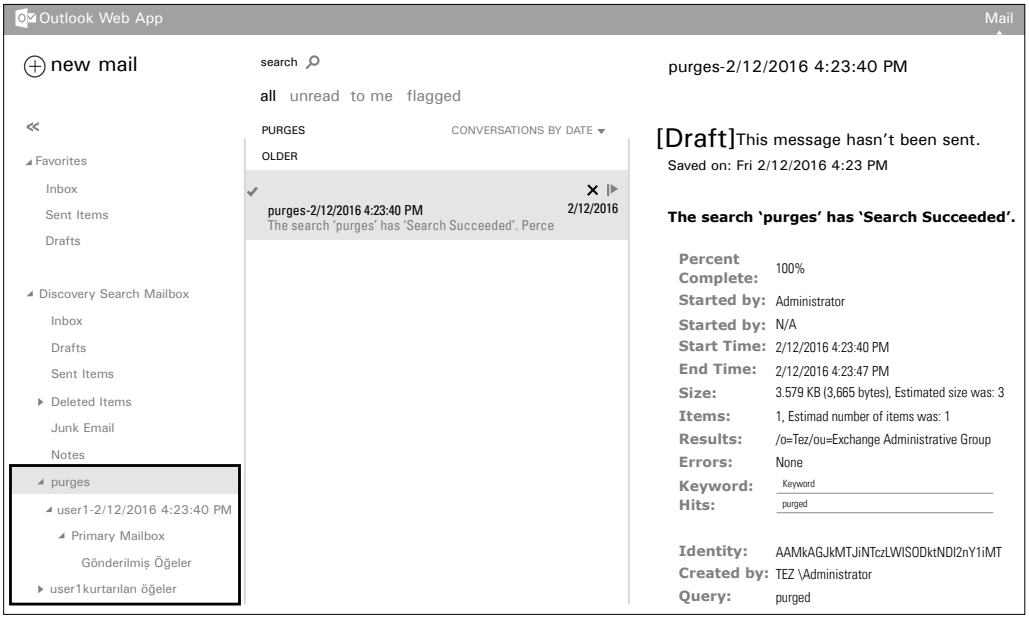
Keşif aramalarında Microsoft tarafından geliştirilen "Keyword Query Language (KQL)[40]" kullanılmaktadır (Şahin, 338). Bu sayede arama sorgusu ekranındaki anahtar kelime alanında, arama operatörleri[41] (AND, OR, NOT, NEAR vb.) kullanılarak birden fazla anahtar kelime içeren sorgular hazırlanabilir.

EAC üzerinden yapılan *keşif araması* tamamlandığında, aramayı gerçekleştiren kişi sonuçları şu iki şekilde görüntüleyebilir:

- **Preview Search Results:** Bu seçenek vasıtasıyla "eDiscovery Search Preview" ekranına ulaşılır. Bu pencerede arama sonuçları, posta kutusu bazında, arama kriterlerini içeren öge sayısını ve boyutunu içerecek şekilde listelenir (Elfassy 2013, 478).
- **Copy Search Results:** Sonuçlar *keşif arama posta kutusuna* kopyalanır. Her bir arama, posta kutusu üzerinde farklı klasörlerde tutulur. Bu sayede arama sonuçlarının birbirine karışması önlenmiş olur (Bkz. Şekil 10).

[40] Detaylı bilgi için bkz. https://msdn.microsoft.com/library/ee558911(v=office.15).aspx Erişim Tarihi: 05.04.2016

[41] Anahtar kelime alanında AND, OR, NOT ve NEAR operatörleri kullanılabilir. Örneğin içinde "exchange" ve "kitap" kelimeleri geçen ögeleri bulmak için "kitap AND exchange" yazılır. Operatörler büyük harfle yazılmalıdır. Operatörler anahtar kelimelerden bu şekilde ayrılır (Şahin 2014, 339).



Şekil 10: Keşif Arama Posta Kutusunda Arama Sonuçları

Posta kutusunda bulunan ögelerin, üçüncü seviye silme işlemine uğraması durumunda *kurtarılabilir* öge*ler klasörü* altındaki *purges* dizininde, *koruma* özelliğinin aktifleştirilmesi durumunda ise kriterlere uyan ögelerin yine aynı klasörün altındaki *discoveryholds* dizininde tutulduğuna önceki bölümlerde değinilmişti. Exchange sunucularda *purges* ve *discoveryholds* dizinleri altındaki ögelere ancak *keşif aramaları* vasıtasıyla erişilebilmektedir. Kurtarma işlemi yapılacak posta hesabı belirlendikten sonra, *exchange-powershell* üzerinde ilgili parametreleri güncellenmiş aşağıdaki komut çalıştırılarak, kullanıcıya ait *ikinci* ve üçüncü seviye silinmiş tüm ögelerle birlikte *koruma* altındaki ögeler de *keşif arama posta kutusu* altına kopyalanır.

Search-Mailbox user1 -SearchDumpsterOnly -TargetMailbox "Discovery Search Mailbox" –TargetFolder "user1 kurtarılan öge*ler"*

Keşif arama posta kutusu içindeki "*user1 kurtarılan* öge*ler*[42]*"* isimli dizin altına kopyalanan ögeler ikinci bir komut vasıtasıyla tekrar *user1* posta kutusuna taşınır:

[42] Klasör ismi ilgili komutta istenilen şekilde değiştirilebilir.

Search-Mailbox "Discovery Search Mailbox" -TargetMailbox user1 -TargetFolder "user1 kurtarılan öge*ler" –DeleteContent*

Böylelikle *user1* posta kutusunda *koruma* altındaki ögeler ile *ikinci* ve üçüncü seviye silinmiş elektronik postalar "*user1 kurtarılan* öge*ler"* dizini altına kopyalanarak, meslek personelince gerçekleştirilecek anahtar kelime aramalarına dâhil edilmiş olur.

Taşıma işleminin iki aşamalı oluşu, *SearchMailbox* komut setinde bulunan kısıtlamadan kaynaklanmaktadır. Bu komut setinde kaynak posta kutusu ile hedef posta kutusu aynı olamamaktadır. Dolayısıyla taşıma işlemi *keşif arama posta kutusu* üzerinden ancak iki aşamalı olarak gerçekleştirilebilmektedir.

2.3. EXCHANGE SUNUCU LOGLARI ÜZERİNDE İNCELEMELER

Elektronik posta iletişiminde hizmet sürekliliğinin sağlanabilmesi için sistemin performansının ve sağlık durumunun sürekli olarak izlenmesi gereklidir. Exchange sunucularda, izleme, raporlama ve bakım faaliyetlerinde kullanılabilecek ve aynı zamanda sistem yönetimini kolaylaştırıcı detaylı bir **günlük tutma** (*logging*) altyapısı bulunmaktadır. Tutulan bu kayıtlar, sunucu ya da istemci tarafında oluşan hataların giderilmesi, sistem üzerinde meydana gelen performans kayıplarının tespiti ve çözülmesi, geçmiş dönemde meydana gelen olayların analizi gibi durumlarda aktif rol almaktadır.

Microsoft Exchange sunucular üzerinde tutulan *kayıtlardan* bir kısmının, Yİ sürecinde rekabet uzmanlarının işlerini kolaylaştırmak amaçlı kullanılabileceği düşünülmektedir. Örneğin, mesajlaşma trafiğinin izlenmesine ilişkin Exchange sunucular üzerinde tutulan **mesaj izleme kayıtlarında** (*message tracking logs*) giden/gelen elektronik postalara ait kayıtlar saklanmaktadır. İletilen elektronik posta, sunuculardan tamamen silinse dahi saklanmaya devam edilen bu kayıtlar, Yİ'lerde rakip teşebbüsler arasında gerçekleşmiş olası iletişimin tespitinde kullanılabilir. Teşebbüs çalışanlarının Yİ öncesi, delil karartma amacıyla posta kutuları üzerinde tahrifat yapmaları durumunda; **denetim kayıtları** (*audit logs*) incelenerek yapılan değişiklik işleminin kimin tarafından, ne zaman ve ne şekilde gerçekleştirildiğine ilişkin kayıtlar elde edilebilir.

Çalışmanın bu kısmında Microsoft Exchange sunucular üzerinde tutulan bazı *günlük kayıtlarının* yerinde inceleme süreçlerinde rekabet uzmanlarınca ne şekilde kullanılabileceğine ilişkin görüşlere yer verilecektir.

2.3.1. Mesaj İzleme Kayıtları ile Mesajlaşma Trafiğinin Takibi

Mesaj izleme kayıtları, Exchange sunucular üzerindeki mesajlaşma trafiğine ilişkin detaylı bilgilerin tutulduğu günlüklerdir. Bu kayıtlar incelenerek elektronik posta akış analizi, raporlama, servislerde oluşan aksaklıkların tespiti/giderilmesi ve adli inceleme gibi işlemler gerçekleştirilebilir (Morimoto vd. 2012, 368).

Kayıtlar sunucularda CSV[43] formatındaki metin dosyaları içinde tutulur. Mesaj trafiğine ilişkin her olayın ayrı bir satırda saklandığı bu *kayıtlarda*; gönderen/alıcı adresi, elektronik postanın konusu, gönderim/alım zamanı gibi yerinde inceleme süreçlerinde kullanılabilecek önemli bilgiler bulunmaktadır (Şahin 2014, 566).

Mesaj izleme kayıtlarında arama işlemleri EAC ya da *exchange-powershell* üzerinde yapılabilir. EAC üzerindeki aramalarda, *iletim raporları* (Delivery Reports) ekranı vasıtasıyla arama yapılacak posta kutusu seçilir ve sonuçlar listelenir. Arama sonuçları, gönderen/alıcı posta kutusu ve mesaj konusu filtre alanlarına girilen değerler yardımıyla daraltılabilir. Benzer aramaları e*xchange-powershell* aracılığıyla yapmak içinse *Get-MessageTrackingLog* komut seti kullanılır (Andersson ve Pfeiffer 2015, 253). Bu yöntemde, EAC üzerinden yapılan aramalara göre daha ayrıntılı seçenekler sunulsa da; gönderen/alıcı (-Sender, -Recipients) parametrelerinde tam SMTP adresi kullanım zorunluluğu olması, detaylı sorguların hazırlanmasını engellemektedir[44].

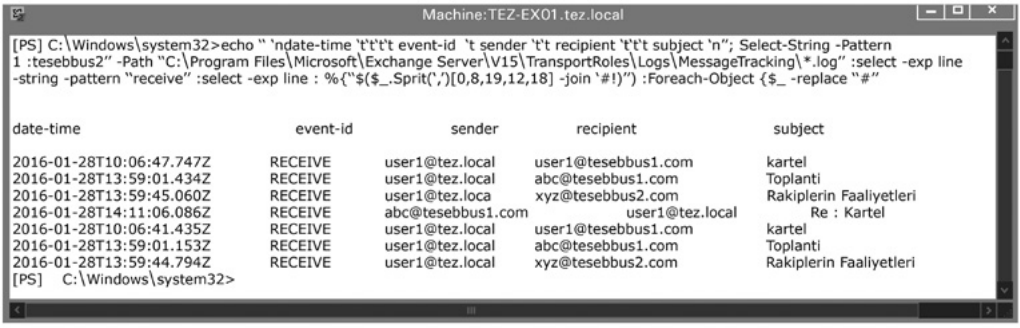
Mesajlaşma trafiğine ilişkin *kayıtlar* üzerinde arama yaparken özel olarak hazırlanmış *powershell* özel kodları (custom scripts) kullanılarak, Microsoft Exchange'in sunduğu arama araçlarına göre daha detaylı sonuçlar elde edilebileceği düşünülmektedir.

[43] Her kaydın farklı bir satırda, virgülle ayırılmış değerler halinde tutulduğu formattır. Detaylı bilgi için bkz. https://tools.ietf.org/html/rfc4180#section-2 Erişim Tarihi: 05.04.2016

[44] https://technet.microsoft.com/en-us/library/bb124926(v=exchg.150).aspx Erişim Tarihi: 05.04.2016

echo "`ndate-time `t`t`t`t event-id `t sender `t`t recipient `t`t`t subject`n"; Select-String -Pattern "tesebbus1|tesebbus2" -Path "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking.log" | select -exp line | select-string -pattern "receive" | select -exp line | %{"$($_.Split(',')[0,8,19,12,18] -join '#')"} | Foreach-Object {$_ -replace "#", "`t`t"}*

Yukarıdaki örnek kod aracılığı ile *mesaj izleme kayıtları* varsayılan konumundan[45] okunarak, *tesebbus1* veya *tesebbus2* anahtar kelimelerini içeren satırlar süzülmektedir. Elde edilen satırlardaki virgülle ayrılmış değerlerden tarih, durum, gönderen, alıcı ve konu bilgilerini içeren kısımlar seçilerek sırasıyla ekrana basılmaktadır. Örnek kodun çıktısı şu şekildedir:



Şekil 11: Mesaj İzleme Kayıtları Üzerinde Çalıştırılan Özel Kod Çıktısı

Çıktı incelendiğinde, üzerinde inceleme yapılan *tez.local* alan adına sahip teşebbüs ile *tesebbus1.com* ve *tesebbus2.com* alan adlarına sahip teşebbüsler arasında elektronik posta alış-verişi yapan kullanıcıların listelendiği görülmektedir. Sorgulama işlemi EAC üzerinden ya da *Get-MessageTrackingLog* komut seti aracılığıyla yapılmaya çalışıldığında, iletişim halindeki kullanıcı posta adresleri sorgulama öncesinde tam olarak bilinmediği için (xyz@tesebbus2.com, abc@tesebbus1.com) arama işlemini gerçekleştirmek mümkün olamamaktadır.

Yukarıdaki örnek senaryo, RKHK'nin 4. maddesinin ihlaline ilişkin açılan dosya kapsamında gerçekleştirilen yerinde incelemelerde, teşebbüsler arası iletişimde

[45] İlgili kayıtlar sunucu üzerinde "*C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\ Logs\ MessageTracking*" dizini altında tutulur.

bulunan çalışanların tespiti için, *keşif aramalarını* desteklemek amacıyla kullanılabilir. Bu kod aracılığıyla yapılan aramalarda, kullanıcı posta kutusuna iletilen elektronik posta tamamen silinse bile, iletim kaydı *mesaj izleme kayıtları* üzerinde saklanmaya devam etmesi nedeniyle *keşif aramalarına* göre daha doğru ve detaylı sonuçlar elde edilmektedir.

2.3.2. Denetim Kayıtları (Audit Logs) ile Silinen Elektronik Postaların Takibi

YİY uyarınca rekabet uzmanları, incelemeye başlamadan önce en yetkili teşebbüs çalışanıyla görüşüp, inceleme konusu ve RKHK hakkında kısa bir bilgilendirme yapmaktadırlar. Bilgilendirme sonrası inceleme yapılacak teşebbüs çalışanları belirlenmekte ve öncelik sırasına göre inceleme işlemi uzmanlarca gerçekleştirilmektedir. Bu durum, fiili incelemenin teşebbüse intikalden ancak belli bir süre sonra başlanabilmesi sonucunu doğurmaktadır. Yaşanan bu zorunlu gecikme, inceleme açısından hayati öneme sahip elektronik delillerin karartılması riskini de beraberinde getirmektedir.

Teşebbüsler tarafından, elektronik delillerin Yİ öncesinde ve Yİ esnasında karartılması durumunda, ilgili teşebbüse 4054 sayılı RKHK'nin 16. maddesinin (d) bendinde belirtilen idari para cezası uygulanabilmektedir. Ancak bu tür bir yaptırımın uygulanabilmesi için delil karartma işleminin tespit edilmesi ve ispatlanması zorunludur. Exchange sunucularda bulunan **posta kutusu denetim kayıtlarının** (*mailbox audit logs*) ve **yönetici denetim kayıtlarının** (*administrator audit logs*) yerinde incelemenin zorlaştırılması halinin tespiti ve ispatlanması amacıyla kullanılabileceği düşünülmektedir[46].

3.3.2.1. Posta Kutusu Denetim Kayıtları

Bir posta kutusu üzerinde *denetim kayıt* özelliği etkinleştirilmesi durumunda, posta kutusundaki ögelerin oluşturulması, değiştirilmesi, taşınması veya silinmesi gibi

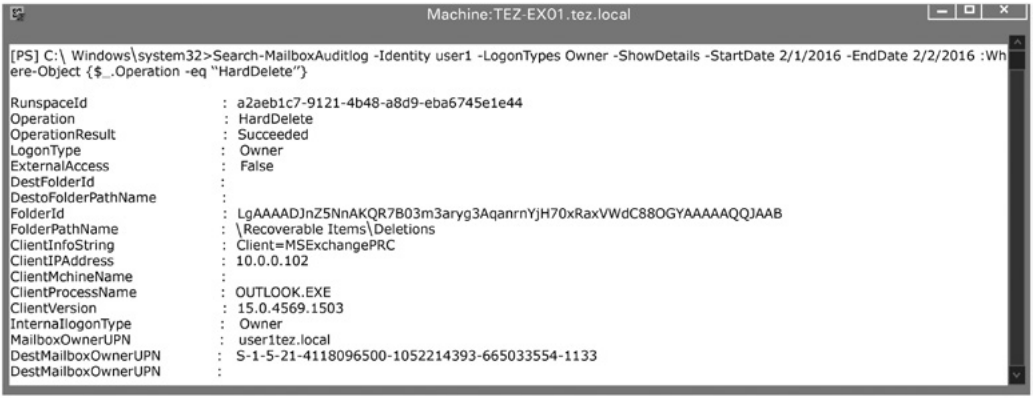
[46] Kurul, 18.07.2013 tarihli ve 13-46/601-M sayılı kararında TTNET A.Ş.'ye, yerinde inceleme esnasında bazı belgelerin saklanması/ortadan kaldırılması gerekçesiyle 4054 sayılı Kanun'un 16. maddesinin birinci fıkrası (d) bendi uyarınca idari para cezası verilmesine karar vermiştir. Söz konusu Yİ esnasında, incelenen dosyaların teşebbüs çalışanlarınca silindiği *nesne denetim kayıtları* (audit object access logs) aracılığıyla tespit edilerek tutanak altına alınmıştır.

işlemler ve bu işlemlerin kim tarafından yapıldığı bilgisi kayıt altına alınmaktadır. Bu kayıtlar, ilgili posta kutusunun *kurtarılabilir* öge*ler klasörü* altında bulunan *audits* dizini içinde saklanır.

Posta kutusu denetim kayıtlarına EAC ya da *exchange-powershell* üzerindeki *Search-MailboxAuditLog* komut seti aracılığıyla ulaşılabilir. Ancak *EAC* üzerinden yapılan aramalarda, kullanıcının kendi posta kutusunda gerçekleştirdiği işlemlerin kayıtları filtrelenememektedir. Bu nedenle denetim *kayıtlarının,* e*xchange-powershell* aracılığıyla sorgulanması gerektiği ve bu sayede daha detaylı sonuçların elde edilebileceği düşünülmektedir.

Search-MailboxAuditLog -Identity user1 -LogonTypes Owner -ShowDetails -StartDate 2/1/2016 -EndDate 2/2/2016 | Where-Object {$_.Operation -eq "HardDelete"}

Yukarıdaki örnek sorgunun çıktısında, 1 Şubat 2016 tarihinde *user1* posta kutusu üzerinde üçüncü seviye silme işlemine uğramış ögelere ilişkin *denetim kayıtları* listelenmektedir.



Şekil 12: Üçüncü Seviye Silinen Elektronik Postaya İlişkin Posta Kutusu Denetim Kaydı

Yİ'lerde, posta kutuları üzerinde incelemeye başlamadan önce, *denetim kayıtları* özelliği aktifleştirilerek, inceleme sonunda ilgili kayıtların kontrol edilmesinin;

elektronik postalar üzerinde yapılması muhtemel tahrifatların tespiti açısından son derece önemli olduğu düşünülmektedir.

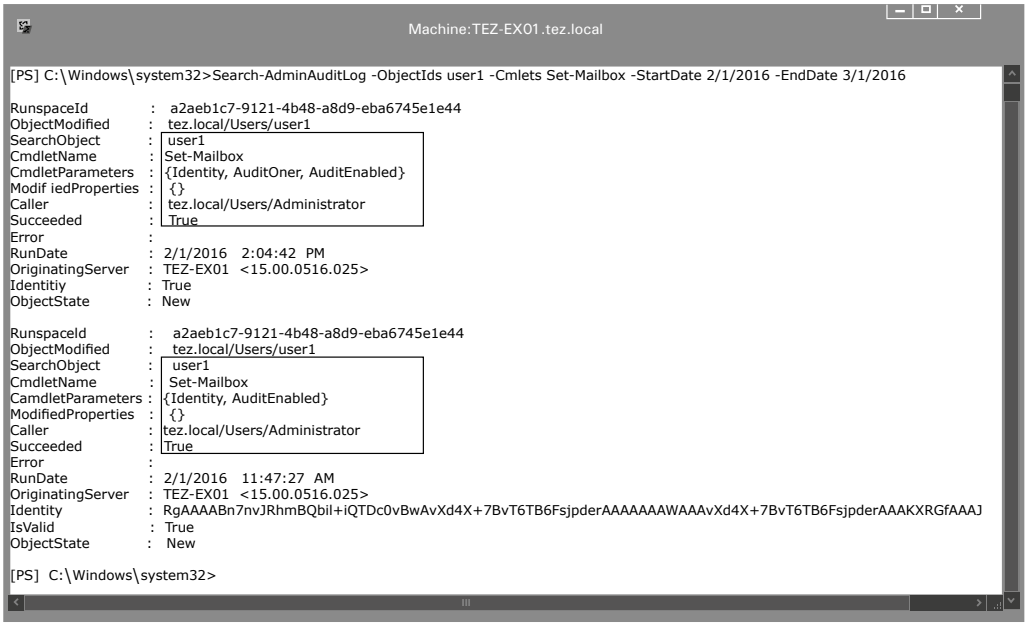
3.3.2.2. Yönetici Denetim Kayıtları

Exchange sunucularda yönetici haklarına sahip kullanıcılar (*exchange admins*), herhangi bir posta kutusu üzerinde *tam erişim yetkisi* tanımlamak suretiyle bu posta kutusundaki ögeleri taşıyabilir, değiştirebilir ya da silebilir. Sistem yöneticileri Yİ esnasında, meslek personelince incelenen posta kutularının yapılandırma ayarlarında değişiklik yaparak; silinmiş ögelerin *kurtarılabilir* öge*ler klasöründe* tutulmamasını sağlayabilir, *denetim kayıtlarının* saklanmasını engelleyebilir ya da *koruma, tek* öge *kurtarma* ayarlarında değişiklik yapabilir. Bu nedenle yerinde inceleme esnasında Exchange yöneticilerinin, incelenen posta kutuları üzerinde gerçekleştirdikleri yapılandırma değişikliklerinin de izlenmesi gerektiği düşünülmektedir.

Sistem yöneticilerinin, Exchange sunucu yapılandırmasında yaptıkları değişiklikler *yönetici denetim kayıtları* üzerinde tutulmaktadır. Bu özellik sunucu kurulumu ile birlikte varsayılan olarak etkin şekilde ayarlanmaktadır. Yönetici denetim kayıtlarında arama yapmak amacıyla parametrik olarak belirli bir posta kutusu üzerinde ve belirli bir tarih aralığı verilerek şu şekilde bir sorgu hazırlanabilir:

Search-AdminAuditLog -ObjectIds user1 -Cmdlets Set-Mailbox -StartDate 2/1/2016 -EndDate 3/1/2016

Bu örnekte; Yİ'nin yapıldığı varsayılan 1 Şubat 2016 tarihinde, *user1* posta kutusu üzerinde yönetici tarafından yapılmış ayar değişiklikleri sorgulanmaktadır. Sorgu çıktısı şu şekildedir:



Şekil 13: User1 Posta Kutusuna İlişkin Yönetici Denetim Kayıtları Çıktısı

Yönetici denetim kayıtları özelliği; *posta kutusu denetim kayıtlarında* olduğu gibi yerinde inceleme öncesinde kontrol edilerek özellik kapalıysa aktifleştirilmeli, yerinde inceleme sonunda ise kayıtlar sorgulanarak yönetici düzeyinde değişiklik yapılıp yapılmadığı denetlenmelidir. Yapılması önerilen bu denetimin önemi, Komisyonun EPH[47] kararı incelendiğinde daha açık biçimde ortaya çıkmaktadır. EPH grubunda gerçekleştirilen Yİ'de, bloklanması gereken elektronik posta hesaplarının inceleme esnasında farklı adreslere yönlendirildiği gerekçesiyle Komisyon tarafından 2.5 milyon Euro tutarında idari para cezası uygulanmıştır (Piazza 2013, 422). Yİ'lerde, teşebbüs çalışanlarınca gerçekleştirilebilecek benzer eylemlerin, *yönetici denetim kayıtları* incelenerek kolaylıkla tespit edilebileceği düşünülmektedir.

[47] Case COMP/39793 - EPH and others, 28.03.2012

2.4. ELEKTRONİK POSTA SUNUCULARI ÜZERİNDE, ADLİ BİLİŞİM ARACI KULLANILMAKSIZIN GERÇEKLEŞTİRİLEBİLECEK YERİNDE İNCELEME YÖNTEMİNE İLİŞKİN ÖNERİ

Kurumca benimsenmiş mevcut YİY uyarınca, teşebbüslere ait sayısal verilerin bütünlüğünü bozucu eylemlerden kaçınılmaktadır. Bölüm boyunca değinilen Exchange sunucu özellikleri, teşebbüs çalışanlarına ait verilere müdahale etmeksizin elektronik posta sistemi üzerinde uygulanabilmektedir. Bu özelliklerin mevcut Yİ sürecine bütünleştirilerek kullanılmaları durumunda, elektronik posta analizi konusunda daha etkin sonuçlar elde edileceği düşünülmektedir. Bu amaçla çalışmanın bu kısmında, belirtilen özelliklerin kullanımını içeren Yİ iş akış diyagramı önerilerek işlem adımları detaylandırılacaktır. Özelliklere ait komutlar ve komut çıktıları gibi teknik detaylara ise çalışmanın EK-4 kısmında yer verilecektir.

Rekabet uzmanlarının, Yİ'lerde teşebbüs çalışanlarına ait posta kutularını incelerken takip etmeleri önerilen işlem adımlarına ilişkin akış diyagramı şu şekildedir:

Şekil 14: Yerinde İnceleme Süreci Akış Diyagramı

Aşama 1: İlk olarak, inceleme öncesinde belirlenen anahtar kelimeler kullanılarak, teşebbüse ait tüm posta kutuları üzerinde *keşif araması* (çoklu posta kutusu araması) yapılır. Aynı anahtar kelimeler ile *mesajlaşma trafiği kayıtları* da sorgulanarak ulaşılan sonuçlar doğrulanır. Böylelikle, inceleme yapılacak posta kutuları belirlenirken önemli delillerin gözden kaçırılması riskinin azaltılacağı düşünülmektedir.

Aşama 2: İncelenecek posta kutuları, teşebbüs tarafından kullanılan *kurumsal yedekleme* yazılımı aracılığıyla, eski tarihli yedekleriyle karşılaştırılır[48]. Silinen çok sayıda ögenin olduğunun tespit edilmesi durumunda, ilgili ögeler yedekten kurtarılarak incelemeye posta kutusunun yeni hali üzerinden devam edilir. Bu sayede, elektronik posta kutularında bulanan olası delillerin teşebbüs çalışanlarınca karartılmasının önüne geçilebilir.

Aşama 3: Belirlenen posta kutuları üzerinde, *tek* öge *kurtarma* ve *posta kutusu denetim kayıtları* özelliklerinin etkin olup olmadığı kontrol edilir. Özellikler, denetlenecek tüm hesaplarda etkinleştirilerek; inceleme esnasında kullanıcı ve sistem yöneticilerinin posta kutularındaki ögelere olası müdahalelerinin kayıt altına alınması sağlanır.

Aşama 4: Bu aşamada, *keşif araması* özelliği kullanılarak, inceleme yapılacak her bir posta kutusunun *kurtarılabilir* öge*ler klasörü* ve *alt dizinlerinde* bulunan ögeler, gelen kutusu altında yeni oluşturulacak bir klasöre kopyalanır. Böylelikle, koruma altındaki ve *ikinci* ve üçüncü seviye silme işlemine uğramış elektronik postalar kurtarılarak anahtar kelime aramalarına dâhil edilmiş olur.

Aşama 5: Rekabet uzmanları tarafından, belirlenen posta kutuları üzerinde anahtar kelime arama işlemi gerçekleştirilir. Anahtar kelimeler arasında *arama operatörleri* kullanılarak daha hızlı ve daha verimli inceleme yapılabileceği düşünülmektedir.

Aşama 6: Belirlenen posta kutuları üzerindeki incelemeler tamamlandıktan sonra, *posta kutusu* ve *yönetici denetim kayıtları* kontrol edilerek; Yİ esnasında sayısal verilere müdahale edilip edilmediği tespit edilir. Olası müdahale durumunda ilgili kayıtlar "Yerinde İncelemenin Zorlaştırılması" tutanağına dayanak oluşturacak şekilde kullanılabilir.

Aşama 7: İnceleme tamamlandıktan sonra, yapılandırma ayarlarında değişiklik yapılan tüm posta kutuları eski haline getirilir.

[48] Karşılaştırma, posta kutusu boyutu ve/veya posta kutusunda bulunan öge sayısı üzerinden yapılabilir.

BÖLÜM 3

ELEKTRONİK POSTA ANALİZİNDE ADLİ BİLİŞİM ARAÇLARININ KULLANIMI

Teknolojinin ilerlemesi ve özellikle internet kullanımının yaygınlaşmasıyla birlikte, bilişim sistemleri suçlular için cazibe merkezi haline gelmiştir. Sürekli artış gösteren siber suçlar ve casusluk faaliyetlerinin, küresel ölçekte yıllık 300 Milyar ABD Doları'nın üzerinde ekonomik zarara yol açtığı tahmin edilmektedir[49]. Bilişim sistemleri aracılığıyla işlenen suçlarda gözlemlenen artış, ülkeleri bu alanda yasal düzenlemeler yapmaya, kolluk ve istihbarat teşkilatları bünyesinde siber suçlarla mücadele birimleri kurmaya yöneltmiştir. Zaman içerisinde uygulanan tekniklerin seviyesinin yükselmesi ve kullanılan araçların karmaşıklığının artması, adli bilişim enstrümanlarının da geliştirilmesi ihtiyacını doğurmuştur. Bu gereklilik neticesinde, son 20 yıllık süreçte bilişim incelemelerinde kullanılmak üzere çok sayıda yazılım üretilmiştir (Devendran vd. 2015, 112). Yaygınlaşan bu yazılımlar, günümüzde sadece bilişim suçlarıyla mücadele eden uzmanlarca değil, aynı zamanda finans, hukuk, danışmanlık, kamu gibi sektörlerde faaliyet gösteren kurumlarca da kullanılmaktadır.

Elektronik postalar, internet üzerinden işlenen birçok suç faaliyetinin birincil kaynağı durumundadır (A.g.k., 111). Bu durumun kaçınılmaz sonucu olarak, hemen hemen bütün adli bilişim yazılımlarında elektronik posta analiz bileşeni bulunmaktadır. Adli bilişim araçları, incelenecek yerel sabit sürücü üzerinde kayıtlı elektronik posta

[49] McAfee, "*The Economic Impact of Cybercrime and Cyber Espionage*" raporu (2013).

dosyalarını[50] (EPD) tespit ederek, elektronik delilleri bu dosyalar üzerinden elde etmeye çalışır.

Elektronik posta analizinde kullanılan adli bilişim yazılımlarının dijital verilerin analizi ile birlikte gerçekleştirmeyi amaçladıkları hedefler şu şekilde özetlenebilir:

- Elektronik posta başlık bilgisini analiz ederek gönderim/alım zamanı, gönderen/alıcı bilgisi gibi verileri tespit etmek,
- Sürücü üzerinde silinmiş EPD'leri kurtarmak,
- Bozulmuş ya da şifrelenmiş EPD'ler içinden elektronik postaları çıkarmak,
- EPD'lerdeki silinmiş elektronik postaları kurtarmak,
- Elektronik postalara ait verileri (başlık, gövde ve ekler) *indeksleyerek* anahtar kelime araması yapılabilmesini sağlamak.

Tez kapsamında Microsoft Exchange altyapısı özelinde yoğunlaşılması sebebiyle, çalışmanın bu bölümünde OST/PST uzantılı EPD'ler üzerinde adli bilişim araçlarının başarımı analiz edilmeye çalışılacaktır. Öncelikle OST/PST dosya yapısı incelenecek, ardından elektronik posta analizinde kullanılan üç farklı adli bilişim yazılımı, ön plana çıkan özellikleriyle birlikte mercek altına alınacaktır. Bölüm sonunda ise, bu yazılımların örnek bir vaka üzerinde elektronik posta analiz kabiliyetleri test edilecektir.

3.1. OST/PST DOSYA YAPISI

Elektronik posta sunucu olarak Microsoft Exchange'in tercih edildiği sistemlerde, istemci bilgisayarlarda posta kutusu ögelerinin kayıt ya da düzenlenme işlemleri Microsoft Outlook yazılımı aracılığıyla gerçekleştirilir. Bu yazılım, elektronik posta sunucusu ile çevrimiçi bir bağlantı üzerinden haberleşerek posta kutusunun işleyişini ve güncel tutulmasını sağlar.

[50] EPD, elektronik posta istemcilerinin posta kutusu ögelerini üzerinde sakladıkları, sabit sürücüde kayıtlı bulunan dosyalardır. Elektronik posta altyapısına göre dosyanın uzantısı değişiklik gösterir. Örneğin; Microsoft Outlook (PST), Microsoft Outlook Offline Storage (OST), Lotus Notes (NSF), America On-line (AOL) vb.

Microsoft Outlook yazılımı posta kutusu ögelerinin birer kopyasını kullanıcı bilgisayarının sabit sürücüsünde kayıtlı, OST uzantılı bir dosya[51] üzerinde saklar (Henkoğlu 2014, 125). Elektronik postaların yerel kopyasının saklandığı bu dosya biçimi *Personal Folder File* (PFF) olarak adlandırılır. Microsoft, PFF formatını açık kaynak kodlu[52] olarak paylaşmadığı için posta kutusu ögelerinin bu dosya tipi içinde ne şekilde saklandığı bilgisi ancak tersine mühendislik[53] teknikleri kullanılarak elde edilebilmiştir (Metz 2009, 1). PFF dosya formatına ilişkin teknik detayların aydınlatılmasıyla birlikte, adli bilişim araçlarının silinmiş/kayıtlı elektronik postaların çıkarılması, şifrelenmiş ya da bozulmuş dosyaların onarılması gibi işlemleri bu dosyalar üzerinde gerçekleştirmeleri mümkün olabilmiştir.

Çalışmanın devamında sırasıyla PFF başlık bilgisi, şifrelenmiş PFF dosyalarına erişim ve PFF dosyalarından silinmiş elektronik postaların kurtarılmasına ilişkin teknik detaylara değinilecektir.

3.1.1. PFF Başlık Bilgisi

PFF dosyasının sabit sürücü üzerindeki ilk 16 baytlık hexadecimal (onaltılık taban) görünümü aşağıdaki şekildedir:

```
0000000: 21 42 44 4e d3 4b 10 c0 53 4d 17 00 01 01   !BDN.K..SM.....
```

Şekil 15: 16 Byte Uzunluğundaki PFF Dosya Başlık İmzası (A.g.k, 1)

İlk dört byte (21 42 44 4e - !BDN), dosyanın PFF formatında olduğunu belirten tekil başlık imzasını[54] gösterir. Bu imza, sabit sürücüden silinmiş OST/PST dosyalarının bulunup kurtarılması işleminde önemli rol oynar. Üzerinde inceleme yapılacak sabit sürücünün birebir kopya görüntüsü[55] (*imaj*) alınarak **veri kazıma** (*data carving*) işlemi

[51] Bu dosyanın işletim sisteminin dosya dizinindeki konumu şu şekildedir:
"C:\Users\%username% \AppData\Local\Microsoft\Outlook\"

[52] Açık kaynak kodlu yazılımlar kaynak kodu kullanıcı tarafından değiştirilebilen ve kullanımı herkese açık olan yazılımlardır (Şirikçi 2013, 5).

[53] Tersine mühendislik (Reverse Engineering) bir aygıtın, objenin veya sistemin; yapısının, işlevinin veya çalışmasının, çıkarımcı bir akıl yürütme analiziyle keşfedilmesi işlemidir (Aras 2008, 1).

[54] Sürücü üzerinde kayıtlı, aynı tipteki dosyaların başında, belirli uzunluktaki ortak bayt dizileri bulunur. Dosyanın tipinin belirlenmesine yardımcı olan bu tekil diziler "dosya (başlık) imzası olarak adlandırılır.

[55] İmaj alma, sabit sürücü üzerinde yer alan her bit birebir yedeklenmesi işlemine verilen addır. Böylelikle kopyalanan sürücünün içeriği aynen elde edilmiş olur (Orta 2015, 153).

yapacak adli bilişim aracı ile açılır. Adli bilişim yazılımı, kopya görüntü üzerindeki baştan sona tüm sektörler[56] üzerinde "!BDN" imzasını tarar. İlgili ifadeye ulaştıktan sonra OST/PST dosyası kurtarılarak[57] veriler sürücü üzerinden *kazınır*. Başlık bilgisi aracılığıyla gerçekleştirilen bu *kazıma* işleminin Yİ esnasında, teşebbüs çalışanlarınca silinmiş OST/PST dosyalarının kurtarılarak anahtar kelime aramalarına dâhil edilebilmesi açısından oldukça önemli olduğu düşünülmektedir.

Çalışmanın EK-5 bölümünde, *foremost*[58] isimli açık kaynak kodlu *veri kazıma* yazılımı kullanılarak, sürücü üzerinden tamamen silinmiş bir PST dosyasının nasıl kurtarıldığına ilişkin işlem adımlarına yer verilmiştir.

3.1.2. Şifrelenmiş OST/PST Dosyaların İçeriğine Erişim

Microsoft Outlook, kullanıcıların OST/PST dosyaları için koruma şifresi belirlemelerine imkân vermektedir. Bu şifre PFF dosyasının "Message Store" alanında saklanmaktadır. PFF dosyasında bulunan veriler bu şifre ile korunmamakta, mevcut şifre sadece dosyaya erişim kontrolü yapmaktadır. Dolayısıyla şifrenin kolaylıkla kırılarak dosya içerisindeki posta kutusu ögelerine erişmek mümkün olabilmektedir (Metz 2009, 18).

[56] Sabit sürücülerin veri saklanabilen en küçük birimine sektör denir.

[57] Kurtarma işleminin tam olarak yapılabilmesi için, silinen dosya üzerine herhangi bir yazma işleminin yapılmaması gereklidir.

[58] Foremost, Amerika Birleşik Devletleri Hava Kuvvetleri Özel Araştırma Bürosu (United States Air Force Office of Special Investigations) tarafından geliştirilen ve sürücü üzerinden silinmiş dosyaların başlık ve alt bilgi imzasına göre kazınmasını sağlayan açık kaynak kodlu adli bilişim yazılımıdır. http://foremost.sourceforge.net Erişim Tarihi: 05.04.2016

```
sansforensics@siftworkstation: ~/Desktop
sansforensics@siftworkstation:~/Desktop$ pffinfo test-archive.pst
pffinfo 20131028

Personal Folder File information :
        File size:              271360 bytes
        File content type:      Personal Storage Tables (PST)
        File type:              64 - bit
        Encryption type:        compressible

Message store:
        Folders:                Subtree, Wastbox, Common views, Finder
        Password checksum:      N/A

sansforensics@siftworkstation:~/Desktop$
```

Şekil 16: Şifre Koruması Olmayan PST Dosyasının Pffinfo Çıktısı

```
sansforensics@siftworkstation: ~/Desktop
sansforensics@siftworkstation:~/Desktop$ pffinfo test-archive-2.pst
pffinfo 20131028

Personal Folder File information :
        File size:              271360 bytes
        File content type:      Personal Storage Tables (PST)
        File type:              64 - bit
        Encryption type:        compressible

Message store:
        Folders:                Subtree, Wastbox, Common views, Finder
        Password checksum:      0xbaa73fbf

sansforensics@siftworkstation:~/Desktop$
```

Şekil 17: Şifre Koruması Olan PST Dosyasının Pffinfo Çıktısı

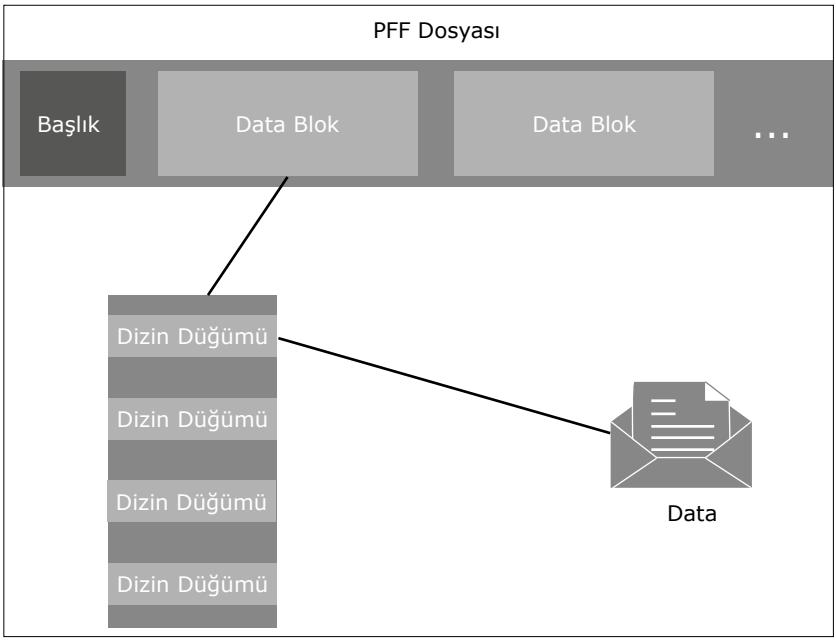
Yukarıda, aynı PST dosyasının şifrelenmiş ve şifrelenmemiş halinin *pffinfo*[59] aracı ile analizine ilişkin ekran görüntüleri yer almaktadır. Şifre koruması getirilmiş PST

[59] *Pffinfo,* Joachim METZ tarafından geliştirilen ve PFF formatındaki dosyaların boyut, içerik, şifre koruma gibi özelliklerinin görüntülenmesine yarayan açık kaynak kodlu bir adli bilişim aracıdır.

dosyasının CRC32 değeri "0" yapılarak, dosya üzerindeki koruma kaldırılabilmektedir. Bu yöntemin, Yİ esnasında incelenecek bilgisayarlar üzerinde bulunan şifre korumalı OST/PST dosyalarının analiz edilebilmesi için kullanılabileceği düşünülmektedir.

3.1.3. OST/PST Dosyalarından Kalıcı Olarak Silinmiş Elektronik Postaların Kurtarılması

PFF dosya yapısı, dosya başlık bilgisi ve veri bloklarından oluşur. Her bir veri bloğu, tahsis tablolarına bağlı dizin düğümlerinden ve bu dizin düğümlerine bağlı verilerden meydana gelir (Bkz. Şekil 18).



Şekil 18: PFF Dosya Yapısı

Bir elektronik posta, son kullanıcı tarafında kalıcı olarak silindiğinde; PST/OST dosyası içindeki o verinin bağlı olduğu dizin düğümü tahsis tablosundan kaldırılır, ancak silinen postaya ait veri ve bağlı olduğu dizin düğümü PFF dosyası içerisinde tahsis edilmemiş alanda tutulmaya devam edilir. Muhafaza işlemi, posta kutusu üzerinde yeni oluşturulan bir öge, silinmiş postaya ait verilerin bulunduğu tahsis edilmemiş alana yazılıncaya kadar devam eder. PFF dosya formatının bu özelliği, kullanıcı

tarafından kalıcı olarak silinmiş elektronik postaların OST/PST dosyası üzerinden kurtarılabilmesine imkân sağlar. Adli bilişim araçları aracılığıyla PFF dosyası üzerinde tahsis edilmemiş dizin düğünleri bulunan data blokları belirlenerek, silinmiş postalara ait veriler kurtarılabilmektedir (Metz 2009, 17). Yİ sırasında bu yetenekte bir yazılımın kullanılmasının, teşebbüs çalışanlarının delil karartma riskini minimize etmek açısından önemli olduğu değerlendirilmektedir.

3.2. ELEKTRONİK POSTA ANALİZİNDE KULLANILAN ADLİ BİLİŞİM ARAÇLARI

Elektronik posta analizi yapabilen adli bilişim yazılımları, verilerin PFF formatındaki dosya üzerinde hangi alanlarda ve ne şekilde saklandığını çözümleyebilirler. Böylelikle, PST uzantılı dosya içerisinde kayıtlı elektronik postalara ve eklerine ilişkin karakter dizilerini çıkararak, bu karakter dizileri üzerinde daha hızlı arama yapabilmek için *indeksleme* işlemini gerçekleştirirler.

Her ne kadar ortak bir amaç için tasarlanmış olsalar da, elektronik posta analizinde kullanılan adli bilişim araçlarının dijital deliller üzerindeki temel başarımları birbirlerinden farklıdır (Devendran vd. 2015, 111). Bazı yazılımlar hızlı *indeksleme* özelliğiyle öne çıkarken, bazıları da silinmiş postaları kurtarmadaki başarısıyla diğerlerinden ayrılmaktadır. Çalışmanın bu kısmında, elektronik posta analizi yapabilen üç farklı adli bilişim aracı hakkında bilgiler verilecektir. Bunlardan ilki, Komisyon dâhil olmak üzere Avrupa Birliğine (AB) üye ülkelerin rekabet otoritelerinin birçoğu[60] tarafından da kullanılan NUIX'dir. Değinilecek bir diğer adli bilişim aracı olan Paraben Email Examiner, rakiplerinden farklı olarak sadece elektronik posta analizi üzerinde uzmanlaşmış bir üründür. Son olarak ise, Kurum'un da paydaşı olduğu "Avrupa Antitröst Adli Bilişim Araçları Projesi" kapsamında hazırlanan EAFIT aracına değinilecektir. Bölüm sonunda yer verilen örnek vaka üzerinde bu üç araç test edilerek, rekabet otoritelerinin Yİ esnasında elektronik posta analizi konusunda ihtiyaçlarını karşılamaya en uygun yazılım belirlenmeye çalışılacaktır.

[60] NUIX, AB'ye üye ülkelerin rekabet otoritelerinin %60'ı tarafından kullanılmaktadır. Konu hakkında detaylı bilgilere "4.2 Avrupa Birliğine Üye Ülkelerin Rekabet Otoritelerinde Adli Bilişim Araçlarının Kullanımı" başlığı altında yer verilecektir.

3.2.1. NUIX

NUIX; 60'tan fazla ülkede, finans kuruluşları, küresel ölçekte şirketler, kamu kurumları, düzenleyici ve denetleyici kuruluşlar, kolluk kuvvetleri ve hukuk danışmalık büroları gibi çeşitli sektörlerde faaliyet gösteren 1500'ün üzerinde müşteri tarafından kullanılan bir adli bilişim yazılımıdır (Nuix 2015a). Lotus Notes, Microsoft Exchange, webmail ve adli imaj dosyaları gibi karmaşık veri tipleri üzerinde işlem yapabilme kapasitesine sahiptir (Bakan ve Saluk 2014, 225).

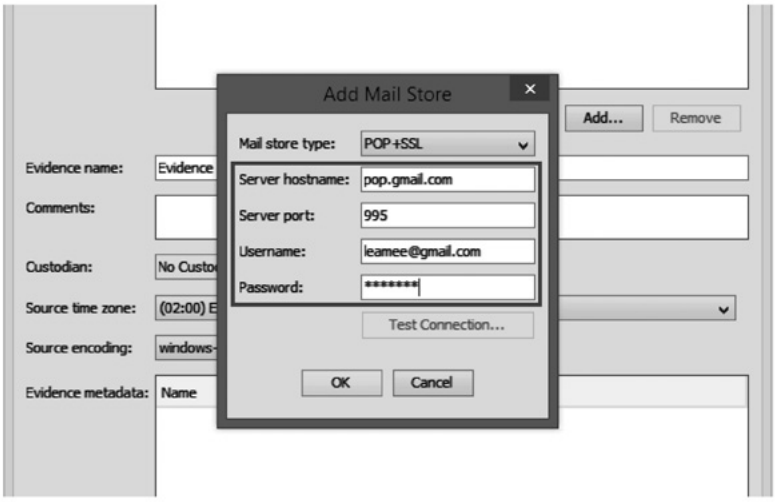
Yazılım, hızlı *indeksleyebilme* özelliğiyle ön plana çıkmaktadır. Sahip olduğu **paralel işleme motoru** (*parallel processing engine*) teknolojisi sayesinde petabayt[61]'lar mertebesindeki veriyi analiz edebilmektedir. Günümüzde kurumsal kullanıcıların posta kutularında on binlerce ögenin bulunması sıklıkla karşılaşılan bir durumdur (Sommer 2013, 84). Yİ'lerde, anahtar kelime sayısının ve incelenecek teşebbüs personeli adedinin çokluğu ile inceleme süresinin kısalığı göz önünde bulundurulduğunda, kullanılacak adli bilişim yazılımının işlem hızı büyük önem kazanmaktadır. NUIX'in, hızlı *indeksleme* özelliğiyle birlikte meslek personelinin sahadaki ihtiyaçlarını karşılayabilecek yetkinlikte olduğu düşünülmektedir.

NUIX, posta kutusu dosya tipindeki verilerin analizi sırasında etkinleştirilebilen *extractFromSlackSpace* özelliği sayesinde *ikinci* ve üçüncü seviye silinmiş elektronik postaları çıkarabilmektedir. Benzer şekilde, *recoverDeletedFiles* özelliğiyle de inceleme yapılan sabit sürücüden silinmiş EPD'leri kurtararak *indeksleyebilmektedir*.

Web tabanlı elektronik posta sistemleri, günümüzde çok yaygın şekilde kullanılıyor olmasına rağmen, bu sistemlerden veri elde ederek analiz yapabilecek az sayıda adli bilişim aracı bulunmaktadır (Paglierani vd. 2013, 11). NUIX, "Add Mail Store" seçeneği sayesinde web tabanlı elektronik posta hesaplarına bağlanarak, bu posta kutularında bulunan verileri *indeksleyebilmektedir*[62] (Bkz. Şekil 19).

[61] 1 PB (petabayt) = 10^{15} bayt

[62] Rekabet otoritelerinin, Yİ'ler esnasında teşebbüs çalışanlarının kişisel web tabanlı posta hesaplarını inceleyip inceleyemeyeceğine ilişkin tartışmaya, bu çalışma kapsamında değinilmeyecektir.



Şekil 19: Add Mail Store Özelliği

Yazılımı diğer adli bilişim araçlarından ayıran temel farklılıklardan bir diğeri de "Web Review & Analytics[63]" olarak adlandırılan teknolojidir. Bu özellik sayesinde analiz edilen veri üzerinde aynı anda birden fazla uzmanın inceleme yapması mümkün olabilmektedir. *Web Review & Analytics* platformu merkezi iş istasyonu üzerinde *indekslenen* elektronik postalara, web tarayıcılar üzerinden güvenli bağlantılar kurulmak suretiyle eş zamanlı inceleme imkânı sağlamaktadır. Yİ ekibinin, incelenecek tüm posta kutuları üzerinde eş zamanlı olarak anahtar kelime araması yapabildiği bir senaryonun mevcut Kurum uygulamasına göre çok daha verimli bir inceleme ortamı sunacağı değerlendirilmektedir.

NUIX, Exchange sunucularda otomatik olarak arşivlenmiş elektronik postalar üzerinde işlem yapabilmektedir. Otomatik arşivleme, posta sunucularındaki sınırlı saklama alanını daha verimli kullanabilmek amacıyla birçok organizasyonun sıklıkla başvurduğu bir özelliktir. NUIX, elektronik postaların arşivden çıkarılmasına gerek kalmaksızın doğrudan anahtar kelime araması yapabilmektedir (Nuix 2015b). Özellikle personel sayısı fazla olan teşebbüslerde gerçekleştirilen Yİ'lerde sıklıkla karşılaşılan

[63] http://www.nuix.com/fact-sheet/nuix-web-review-analytics-fact-sheet Erişim Tarihi: 05.04.2016

otomatik posta arşivlerini analiz edebilme yeteneğinin, NUIX'i rakip yazılımlara göre bir adım öne taşıdığı düşünülmektedir.

3.2.2. PARABEN E-Mail Examiner

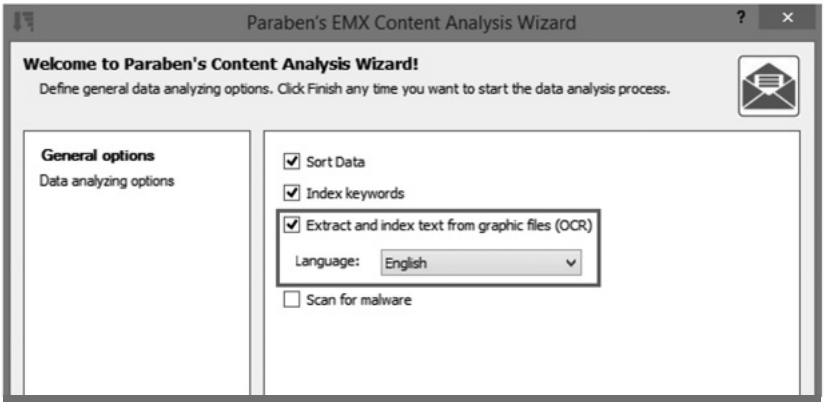
Paraben E-mail Examiner, kapsamlı analiz özelliklerine sahip, kolay raporlama ve gelişmiş mantıksal arama seçenekleri sunan ve elektronik posta incelemesi üzerine uzmanlaşmış bir adli bilişim yazılımıdır (Banday 2011a, 239). Microsoft Outlook (OST, PST), Lotus Notes (EML, NSF), America On-line (AOL), 750'nin üzerinde MIME tipi ve ilgili dosya uzantısı ile oldukça geniş bir elektronik posta format desteği vardır. Posta kutusunda bulunan ögelerin yanı sıra, silinmiş elektronik postaları da kurtararak analiz edebilmektedir.

Paraben E-mail Examiner birçok adli ya da sanal imaj formatı[64] desteğine sahiptir. Araç, imaj dosyaları ile çalışabilmenin yanı sıra incelenecek dosya ya da klasörleri içeren fiziksel veya mantıksal sürücüler üzerinde de analiz yapabilmektedir. Yazılım, *Deployable P2 Commander*[65] (DP2C) bileşeni sayesinde inceleme yapılacak bilgisayarlarda sadece belirli dosya tiplerini hedef alarak gereksiz dosyaların analiziyle zaman kaybedilmesinin önüne geçebilmektedir. **Veri önceliklendirme** (*data triage*) olarak adlandırılan bu adım sayesinde sadece EPD'ler üzerine yoğunlaşılarak inceleme süresinin kısaltılması sağlanmaktadır. Yİ'ler esnasında en kıt kaynaklardan biri olan zamanın verimli kullanılabilmesi adına tüm sürücü imajı üzerinde çalışmaktansa sadece hedef alınmış dosya tipleri üzerinde inceleme yapmanın önemli olduğu düşünülmektedir.

Yazılımın fark yaratan özelliklerden bir diğeri *Optical Character Recognition* (OCR) bileşenidir. Bu bileşen, resim formatında kaydedilmiş dosyalardaki karakter dizilerini çıkararak anahtar kelime aramalarına dâhil etmektedir. Örneğin, taranarak PDF formatında kaydedilmiş (*unsearchable PDF*) bir belgenin içeriğinde normal şartlarda anahtar kelime araması yapılamamaktadır. *Paraben E-mail Examiner*, OCR bileşeni sayesinde fotoğraf üzerindeki karakterleri görüntü işleme teknikleri aracılığıyla tanıyarak çıkartabilmektedir. Yİ esnasında incelenen teşebbüs çalışanlarına ait posta

[64] Raw DD, E01, PFR, VMWare, Virtual PC vb.
[65] https://www.paraben.com/dp2c.html Erişim Tarihi: 05.04.2016

kutularında bulunan taranmış dokümanların da incelenebilmesi açısından adli bilişim araçlarının OCR desteğine sahip olmaları gerektiği düşünülmektedir.



Şekil 20: Paraben OCR Eklentisi[66]

Paraben firması tarafından geliştirilen yazılım, yerel sürücülerde kayıtlı dosyalar üzerinde çalışmanın yanı sıra *Network E-Mail Examiner* bileşeni ile birlikte doğrudan elektronik posta sunucularının veri tabanlarına bağlanarak canlı inceleme de yapabilmektedir. Bu özellik sayesinde, posta kutusu ögelerinin ve arşivlenmiş postaların sunucu üzerinde tutulduğu altyapılarda hızlı ve kapsamlı analiz imkânı sunmaktadır. Bu kapsamdaki bir adli bilişim yazılımının, çalışan sayısının fazla olduğu teşebbüslerdeki Yİ'lerde meslek personelinin işini kolaylaştırıcı bir enstrüman olarak kullanılabileceği değerlendirilmektedir.

3.2.3. EAFIT Tools

2013 yılında, European Competition Network Forensic IT Working Group bünyesinde, koordinatörlüğünü İtalyan Rekabet Otoritesinin yaptığı "Avrupa Antitröst Adli Bilişim Araçları Projesi (proje)" hayata geçirilmiştir. Projenin temel amacı, Yİ ve dijital delil elde etme süreçlerinde rekabet otoritelerinin ihtiyaçlarını karşılayacak kapasite ve yetenekte bir yazılımın hazırlanmasını sağlamaktır. Aralarında Kurum'un da bulunduğu 27 ulusal rekabet otoritesi ve Komisyon'un paydaş olarak iştirak ettiği

[66] Unsearchable PDF'de bulunan sayfalar, grafik nesnesi olarak çıkartılarak OCR işleminden geçirilir.

proje neticesinde tasarımı ve altyapısı oluşturulan yazılım otoritelerin kullanımına sunulmuştur[67].

Hazırlanan yazılım, iki bileşenden oluşmaktadır. Deft0 olarak adlandırılan ilk bileşen, teşebbüs bilgisayarlarında bulunan verilerin çıkartılmasını sağlamakla görevlidir. Elde edilen veriler EDIT olarak adlandırılan ikinci bileşene yüklenerek, rekabet uzmanlarının anahtar kelime araması yapabilecekleri formata dönüştürülmektedir.

Deft0 bileşeni önyüklenebilir formatta bir USB sürücüye yazılarak kullanılmaktadır. İncelenecek teşebbüs çalışanına ait bilgisayar bu USB sürücü ile başlatılarak, yerel sürücülerin Deft0'ya **salt okunur** (*read-only*) biçimde bağlanması sağlanmaktadır. Bu sayede; hem sürücünün tamamının imajını almaya gerek olmaksızın canlı inceleme yapılabilmekte, hem de kullanıcıya ait verilerin bütünlüğünün korunmaktadır. Deft0 hedef sürücüde kayıtlı, karakter dizisi içerebilecek tipte dosyaları (Örneğin, ofis dokümanları, PDF, PST, metin dosyası vb.) – dosyalar silinmiş olsa dahi – seçerek çıkartabilmektedir. Bu sayede, üzerinde anahtar kelime araması yapılamayacak dosya türlerinin gereksiz yere analiz edilmesinin önüne geçilmektedir. Ayrıca, çıkartılacak dosyalar belirlenirken *dosya imzaları* analiz edilerek karar verildiğinden delil karartma amacıyla uzantısı değiştirilen dosyaların gözden kaçırılması engellenmektedir. Çıkartılan dosyaların, *hash*[68] değerlerinin her bir dosya için ayrı ayrı hesaplanarak harici bir sürücüye kopyalanmasının, dosya içeriklerinin değiştirilmediğinin kanıtlanabilmesi açısından önemli olduğu düşünülmektedir.

EDIT bileşeni, teşebbüs çalışanlarına ait bilgisayarlardan elde edilen dijital verilerin içinden karakter dizilerinin çıkartılması ve bu karakter dizilerinin *indekslenmesi* işlemini gerçekleştirmektedir. Bileşen tek bir bilgisayar üzerinde çalıştırılabileceği gibi, basit bir ağ kurularak sunucu-istemci mimarisiyle de kullanılabilmektedir. Bileşenin, sunucu-istemci mimarisi üzerine kurulu *dağıtık*[69] yapıda kullanımı, Deft0 ile farklı bilgisayardan elde edilen sayısal delillerin, birden fazla istemci üzerinden eş zamanlı olarak sisteme yüklenebilmesine imkân vermektedir. Aynı *dağıtık* yapı,

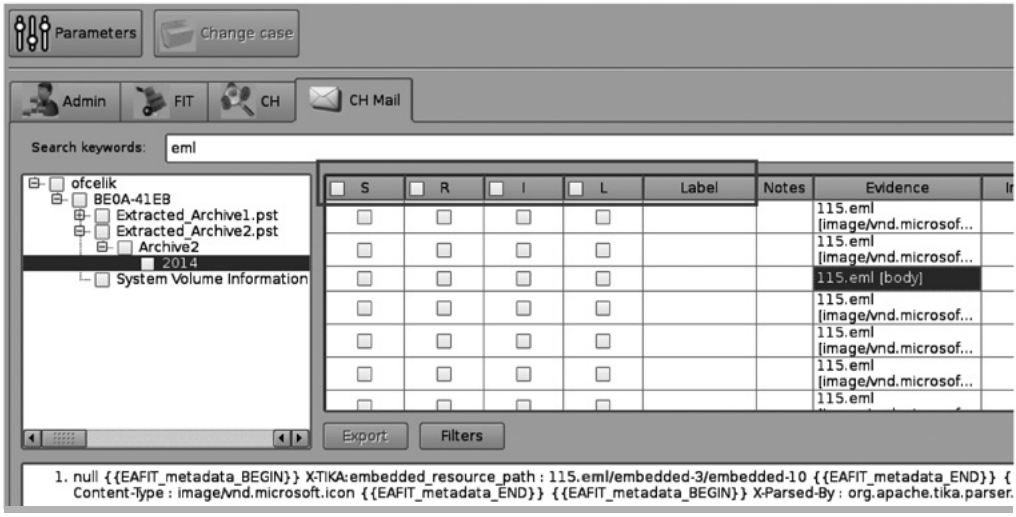
[67] http://www.eafit-tools.eu/stakeholders Erişim Tarihi: 05.04.2016

[68] Hash, hukuk uygulamamızda elde edilen dijital delillerinin değiştirilmediğini, orijinal şekillerinin muhafaza edildiğini, bu delillerin bütünlüğünün korunduğunu gösteren bir fonksiyondur (Payel 2014, 12).

[69] Ağ üzerinden bağlı bilgisayarların, ortak bir hedefe ulaşmak için sistem kaynaklarını paylaşmak suretiyle eylemlerinin koordinasyonunu sağladıkları yapıya *dağıtık sistem* denir.

veriler üzerinden karakter dizilerinin çıkartılması sırasında da kullanılarak, iş yükünün sunucu ve istemciler arasında paylaşımını ve böylelikle analiz süresinin kısaltılmasını[70] sağlamaktadır. Elde edilen karakter dizileri sunucu üzerinde *indekslenerek* rekabet uzmanlarının anahtar kelime araması yapmalarına hazır hale getirilmektedir.

EDIT bileşeninin arama modülü, birden fazla rekabet uzmanının eş zamanlı olarak anahtar kelime araması yapabilmesine olanak sağlayacak yapıda tasarlanmıştır. İncelenen deliller beş farklı şekilde (Selected, Reviewed, Important, LPP ve Kullanıcı tanımlı etiket) etiketlenebilmektedir (Bkz. Şekil 21).



Şekil 21: EDIT Bileşeni İle Etiketleme Ekranı

Bu sayede; aynı delilin tekrar tekrar incelenmesinin önüne geçileceği, etiketler aracılığıyla delillerin kolaylıkla gruplanarak süzülebileceği ve diğer uzmanların aynı delil üzerindeki yorumlarının görüntülenerek incelemenin etkinliğinin artırılacağı düşünülmektedir.

EDIT bileşeni ara yüzünde elektronik postalar üzerinde arama yapılabilecek ayrı bir sekme bulunmaktadır. Analiz esnasında elektronik postalar diğer delillerden ayrılarak bu sekme altında toplanmaktadır. Her bir elektronik postaya ait *başlık bilgisi*,

[70] Yazılımın mevcut sürümünde *indeksleme* işlemi esnasında sadece sunucu bilgisayar görev almaktadır. EDIT aracının ilerleyen sürümlerinde *dağıtık* yapı üzerinde *indeksleme* yapılmasının, analiz sürecini daha da kısaltacağı düşünülmektedir.

gövde ve *ekler* ayrıştırılarak ayrı ayrı ögeler halinde *indekslenmektedir*. İndeks*lenen* elektronik postalar üzerinde arama operatörleri kullanılarak anahtar kelime araması yapılabilmekte, listelenen sonuçlar filtreler[71] aracılığıyla daraltılabilmektedir.

EAFIT Tools projesi kapsamında üretilen adli bilişim yazılımının; *dağıtık* şekilde çalışabilme sonucunda sağladığı etkinlik artışı, güçlü etiketleme yapısı, eş zamanlı inceleme yapabilmeye imkân vermesi, kullanıcı dostu arayüzü ve kolay kullanım özellikleriyle birlikte, rekabet otoritelerinin Yİ'lerde ihtiyaçlarını karşılamaya aday önemli bir alternatif olarak öne çıktığı değerlendirilmektedir.

3.3. ÖRNEK VAKA ÜZERİNDE İNCELEMELER

Çalışmanın bu kısmında, bölüm içerisinde değinilen adli bilişim yazılımlarının elektronik posta analiz performansları ölçülerek elde edilen sonuçlar mevcut Kurum uygulaması ile karşılaştırılacaktır. Örnek vaka üzerinden gerçekleştirilecek bu test ile NUIX, PEE ve EAFIT araçlarının, rekabet otoritelerinin sahadaki ihtiyaçlarını ne ölçüde karşıladıkları ortaya konmaya çalışılacaktır. Ölçülmesi planlanan performans kriterleri üç ana başlık altında şu şekilde belirlenmiştir:

- Analiz süresinin kısaltılması
    - Veri Önceliklendirme
    - İndeksleme süresi
    - Doğrudan Elektronik Posta Sunucusu Üzerinde İnceleme
- Önemli delillerin gözden kaçırılmasının engellenmesi
    - Silinmiş EPD'nin kurtarılabilmesi
    - Şifreli PST dosyalarının incelenebilmesi
    - Silinmiş Elektronik postaların kurtarılabilmesi
    - OCR Desteği
- İnceleme deneyiminin iyileştirilmesi
    - Anahtar kelime aramalarında arama operatörü kullanımı
    - Program arayüzünün kullanım kolaylığı

[71] Elektronik postalar, gönderen/alıcı, gönderim/alım zamanı ya da etiketlere göre filtrelenebilmektedir.

Yazılımların yukarıda sayılan kriterlerdeki başarımlarını ölçmek amacıyla belirli anahtar kelimeleri içeren postaların bulunduğu örnek PST dosyaları[72] hazırlanarak, bu dosyalar her bir adli bilişim aracıyla ayrı ayrı analiz edilmiştir. Araçların örnek vaka üzerindeki başarımına ait sonuçlar Tablo1'de derlenmiştir.

KRİTER		ADLİ BİLİŞİM ARACI			
		NUIX	PEE[73]	EAFIT	OUTLOOK
Veri Önceliklendirme		✓	✓	✓	x
Doğrudan Elektronik Posta Sunucusu Üzerinde İnceleme		✓	✓	x	x
İndeksleme süresi		00:05:12	00:12:09	00:11:00	00:39:00
Silinmiş EPD kurtarılabilmesi		✓	✓	✓	x
Şifreli PST dosyalarının incelenebilmesi		✓	✓	✓	x
Silinmiş Elektronik postaların kurtarılması	**Birinci seviye silinmiş**	✓	✓	✓	✓
	İkinci seviye silinmiş	✓	✓	✓	✓
	Üçüncü seviye silinmiş	✓	✓	✓	✓
Anahtar kelime araması	**Basit arama operatörleri**	✓	✓	✓	✓
	Regular Expression	✓	✓	✓	x
	Gelişmiş arama operatörleri	✓	x	✓	x
OCR Desteği		✓	✓	x	x
Program arayüzü kullanım deneyimi	**Etiketleme**	✓	✓	✓	x
	Çoklu inceleme	✓	x	✓	x
	Kolay kullanım	✓	✓	✓	✓

Tablo 1: Adli Bilişim Aracı Performans Testi Sonuçları

[72] PST dosyalarına ilişkin detaylar ve test sonuçları için bkz. EK-6.

[73] Paraben Email Examiner yazılımı, testin yapıldığı tarihte OST dosyalarının 2013 versiyonunu desteklemediği için, testte kullanılan posta kutusu elektronik posta sunucusu üzerinden PST formatında çıkartılarak, analiz edilmiştir.

Yİ'lerde zamanın verimli şekilde kullanılması büyük önem taşımaktadır. Kullanılacak adli bilişim yazılımının ön analiz sürecini bir an önce tamamlayarak, elektronik verileri anahtar kelime araması yapılabilecek hale getirmesi gerekmektedir. Bu amaçla, incelenecek veriler önceliklendirilerek ihtiyaç duyulan tipteki dosyalar hızlıca *indekslenmelidir*. Her üç yazılımın da verileri önceliklendirerek analiz edebilme yeteneğine sahip olduğu görülmüştür. İndeksleme hızında ise NUIX'in yaklaşık olarak 8000 elektronik posta ögesini 5 dakika gibi kısa bir sürede (8,55 GB/sa) anahtar kelime araması yapılabilir hale getirdiği görülmüştür. Outlook'un kullandığı *Microsoft Indexing Engine* ise, 39 dakikalık *indeksleme* süresiyle, en kötü performansına sahip ürün konumundadır.

Yİ'nin başarıyla yerine getirilmesinin önündeki engellerden bir diğeri de teşebbüs çalışanlarının delil karartma riskidir. Silinmiş PST/OST dosyaları ya da içi boşaltılmış posta kutuları üzerinde yapılacak anahtar kelime aramalarıyla sağlıklı bir inceleme yapılamayacağı açıktır. Dolayısıyla Yİ'de kullanılacak bir adli bilişim aracı *indeksleme* işlemine başlamadan önce sürücü üzerinde şifreyle korunan ya da silinmiş PST/OST dosyalarını analiz edebilmeli, posta kutusundan silinmiş ögeleri kurtarabilmelidir. Yapılan testlerde her üç adli bilişim aracının da silinmiş PST/OST dosyalarını sürücüden *kazıyabildiği* görülmüştür. Mevcut Yİ prosedüründe incelenen bilgisayarlardan silinmiş dosya kurtarma işlemi yapılmamaktadır. Bu durumun Yİ performansını olumsuz yönde etkilediği düşünülmektedir. Test edilen yazılımların şifreyle korunan PST/OST dosyalarındaki başarımı da benzer şekildedir. Şifreli dosyalardaki elektronik postalara, anahtar kelime aramalarında ulaşılabilmiştir. Test kapsamındaki en önemli ölçütlerden biri olan silinmiş postaların geri getirilmesi konusunda ise NUIX ve Paraben'de diğer uygulamalara göre daha başarılı sonuçlar elde edilmiştir. Her iki uygulamada da, üçüncü seviye silinmiş postalara ulaşılabilmiştir. OCR özelliği ise NUIX ve Paraben Email Examiner yazılımlarında bulunmaktadır. Özellikle NUIX'in Abbyy OCR bileşeni, resim formatında eki olan postalardaki karakter dizilerini başarıyla çıkarabilmiştir.

Adli bilişim araçlarınca posta kutusu ögelerinin *indekslenmesinin* ardından sıra rekabet uzmanları tarafından yapılacak anahtar kelime aramalarına gelmektedir. Arama operatörleri, aynı anda birden fazla anahtar kelimeyi birleştirerek arama yapmaya imkân sağlaması nedeniyle inceleme hızını artırmaktadır. Basit arama operatörleri

olarak adlandırılan AND, OR ve NOT, Outlook dâhil test edilen tüm araçlarda kullanılabilmektedir. Ancak arama kutucuğunda düzenli ifadeler[74], bulanık mantık[75] ve yakınsama[76] arama operatörleri kullanılmak istendiğinde, bu özelliklerin sadece adli bilişim araçlarında yer aldığı gözlenmiştir. NUIX ve EAFIT araçları, sahip oldukları sunucu-istemci mimarisi sayesinde birden fazla rekabet uzmanına aynı anda anahtar kelime araması yapabilme olanağı sunmaktadır. Böylelikle Yİ'ye katılan meslek personeli, tek bir platform üzerinden, denetlenen çalışanlara ait posta kutularını eş zamanlı olarak inceleyebilmektedir.

Örnek vaka üzerinde adli bilişim araçlarının başarımlarının karşılaştırıldığı bu çalışmayla, test edilen yazılımların rekabet otoritelerinin Yİ'lerdeki ihtiyaçlarını karşılayabilecek yetkinlikte olup olmadıklarının belirlenmesi amaçlanmıştır. Değerlendirme sonuçlarına göre NUIX; sunucu-istemci mimarisiyle çalışabilme, hızlı *indeksleme*, gelişmiş arama operatörlerinin kullanımına olanak sağlaması ve silinmiş ögelerin kurtarılmasındaki başarımı gibi ölçütler göz önünde bulundurulduğunda diğer araçlara göre bir adım öne çıkmaktadır. Avrupa Birliği'ne üye ülkelerin rekabet otoritelerinin birçoğu tarafından tercih ediliyor oluşu da bu durumu destekler niteliktedir. Elde edilen sonuçlar ışığında, Yİ esnasında adli bilişim yazılımı kullanılması durumunda, mevcut Kurum uygulamasında kullanılan tekniklere göre çok daha etkili inceleme imkânı sağlanabildiği gerçeğinin, dikkat çekilmesi gereken bir diğer nokta olduğu değerlendirilmektedir.

[74] **Düzenli ifadeler** (*regular expressions*), değişken sayıda karakter dizisinden oluşan ve belirli koşulları sağlayabilen ifadelerdir (Demirsöz 2009, 30). Örneğin, ^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$ ifadesi NUIX'de IP adresi formatındaki tüm sonuçları listelemeyi sağlar (192.168.1.4, 22.32.133.14 vb.).

[75] Bulanık mantık (fuzzy search) arama operatörüyle, aranacak anahtar kelimeye benzer ifadeleri içeren sonuçlara da ulaşılması sağlanır. Örneğin, EDIT aracında "cartel~" olarak arama yapıldığında, hem "cartel" hem de "kartel" yazılı sonuçlara ulaşılabilir.

[76] Aranan iki anahtar kelimenin belge içerisindeki birbirlerine uzaklıklarının (kelime sayısı cinsinden) sorgulanabildiği operatördür. Örneğin, "kelime1 kelime2"~5 ifadesi EDIT aracında anahtar kelimelerin birbirine en fazla 5 kelime uzaklıkta bulunduğu sonuçları listeler.

BÖLÜM 4

YERİNDE İNCELEMELERDE ELEKTRONİK POSTA ANALİZİ KONUSUNDA TAKİP EDİLMESİ ÖNERİLEN SÜREÇ MODELİ

4.1. ELEKTRONİK POSTA SUNUCULARI ÜZERİNDE YAPILAN ARAMALARIN SINIRLARI VE EXCHANGE SUNUCU YAPILANDIRMASINA İLİŞKİN ANKET ÇALIŞMASININ SONUÇLARI

4.1.1. Elektronik Posta Sunucuları Üzerinde Yapılan Aramaların Sınırları

Microsoft Exchange sunucularda bulunan birçok özellik, sunucunun ilk kurulumuyla beraber, ön tanımlı olarak sınırlandırılmış ya da devre dışı bırakılmış şekilde ayarlanmaktadır. İlgili özelliklerin, elektronik posta sunucusunun kullanılacağı organizasyondaki ihtiyaçlar doğrultusunda sistem yöneticileri tarafından yeniden yapılandırılacağı varsayılmaktadır. Böylelikle bilişim altyapısındaki sınırlı kaynakların[77] asgari düzeyde tüketilmesi amaçlanmaktadır.

Meslek personelince gerçekleştirilen Yİ'lerde, inceleme etkinliğini artırmaya yönelik katkıda bulunacağı düşüncesiyle tezin ikinci bölümü boyunca değinilen Exchange sunucu özelliklerinden bazılarında da varsayılan yapılandırma ayarlarından kaynaklı sınırlamalar mevcuttur. Çalışmanın bu kısmında, *tek* öge *kurtarma*, *keşif aramaları*, *mesajlaşma trafiği kayıtları* ve *posta kutusu denetim kayıtları* özelliklerinin ön tanımlı yapılandırma ayarlarına değinilecektir.

[77] Depolama ünitesindeki veri saklama kapasitesi, sunucuların işlemci ve RAM kullanım kapasiteleri vb.

Tek öge kurtarma özelliği varsayılan olarak hiçbir posta kutusuna uygulanmamaktadır. Özellik etkinleştirildiğinde ise, *kurtarılabilir* öge*ler klasöründen* silinen elektronik postalar (üçüncü seviye silme) ön tanımlı olarak silinme tarihinden itibaren 14 gün süresince kurtarılabilmektedir.

Exchange sunucular üzerinde, eş zamanlı olarak yapılabilecek maksimum *keşif araması* sayısı varsayılan olarak iki ile sınırlandırılmıştır. Aramalarda kullanılabilecek maksimum anahtar kelime sayısı da 500 olarak belirlenmiştir.

Mesajlaşma trafiğine ilişkin kayıtlar, sunucu üzerinde varsayılan olarak 30 gün boyunca tutulmaktadır. Kayıtların saklandığı klasörün boyutu 1 GB'ı geçmesi durumunda, 30 günlük süre beklenmeksizin en eski kayıttan başlanarak yeni kayıtlar, eski kayıtların üzerine yazılmaktadır.

Posta kutusunda bulunan ögeler üzerinde kullanıcıların gerçekleştirdikleri eylemlerin kayıt altına alınmasına yarayan *posta kutusu denetim kayıtları* özelliği, yeni oluşturulan hesaplarda varsayılan olarak pasif konumdadır.

Yukarıda bahsedilen ön tanımlı yapılandırma ayarlarından kaynaklanan sınırlamalar, Yİ'lerde kullanımı önerilen Exchange sunucu özelliklerinin başarımını, elektronik posta altyapısını yöneten kişilerin sunucular üzerinde yaptıkları yapılandırma ayarlarına doğrudan bağlı hale getirmektedir. Bu durumun, meslek personelinin Yİ performansını arttıracağı ileri sürülen bu özelliklerin her teşebbüste eşit etkinlikle kullanılmasını engellediği düşünülmektedir.

4.1.2. Exchange Sunucu Yapılandırmasına İlişkin Anket Çalışması Sonuçları

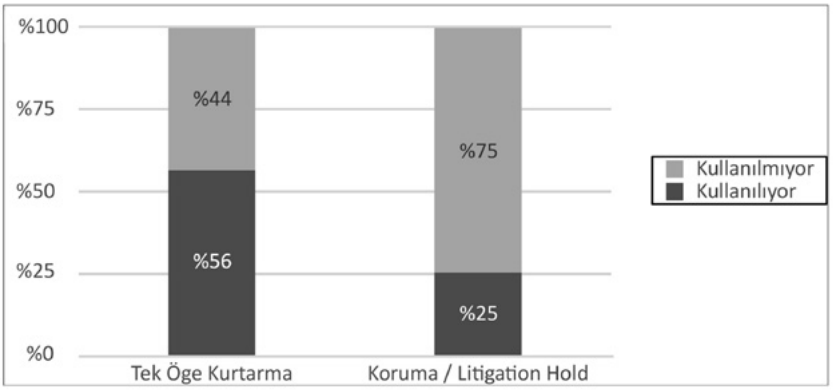
Çalışmanın bu kısmında, Microsoft Exchange sunucularda bulunan *tek* öge *kurtarma*, *koruma*, *litigation hold*, *mesajlaşma trafiği kayıtları*, *posta kutusu denetim kayıtları* özelliklerinin ve kurumsal yedekleme politikalarının ne şekilde yapılandırıldığının sorgulandığı anket çalışmasına ilişkin değerlendirmelere yer verilecektir. Bu anket çalışması neticesinde, mevcut yetkiler çerçevesinde Yİ'lerde takip edilmesi önerilen işlem adımlarının uygulanmasıyla birlikte ortaya çıkacağı düşünülen etkinlik artışının ön görülebilmesi amaçlanmıştır.

Çalışma kapsamında hazırlanan soru seti[78] finans, bilişim, danışmanlık, perakende, sağlık, kamu, güvenlik gibi birçok sektörde faaliyet gösteren 16 teşebbüsün sistem yöneticilerine yöneltilmiştir. Elde edilen sonuçlar üç başlık altında değerlendirilerek aşağıda sıralanmıştır.

Üçüncü seviye silinmiş elektronik postaların kurtarılabilmesine imkân sağlayan *tek* öge *kurtarma*, *koruma* ve *litigation hold* özelliklerinin kullanım istatistikleri Tablo 2'de yer almaktadır.

Özellik	Kullanılıyor		Kullanılmıyor	
	Frekans (f)	Yüzde (%)	Frekans (f)	Yüzde (%)
Tek Öge Kurtarma	9	56%	7	44%
Koruma / Litigation Hold	4	25%	12	75%

Tablo 2: Tek Öge Kurtarma, Koruma ve Litigation Hold Özelliklerinin Kullanım İstatistikleri



Grafik 1: Tek Öge Kurtarma, Koruma ve Litigation Hold Özelliklerinin Kullanım İstatistikleri

[78] Anket çalışması kapsamında, teşebbüslerin sistem yöneticilerine yöneltilen soru setine EK-7'de yer verilmiştir.

Teşebbüs çalışanları tarafından bilinçli ya da bilinçsiz olarak silinmiş elektronik postaların, anahtar kelime aramalarına dâhil edilebilmesine imkân sağlayan *tek* öge *kurtarma*, *koruma* ve *litigation hold* özelliklerinin kullanım oranlarının %40'ın altında kaldığı görülmüştür. Bu durum, Yİ'lerin en kritik aşaması olduğu düşünülen elektronik posta analizi sürecinde, üçüncü seviye silinmiş postaların birçok teşebbüste kurtarılamayacağı anlamına gelmektedir.

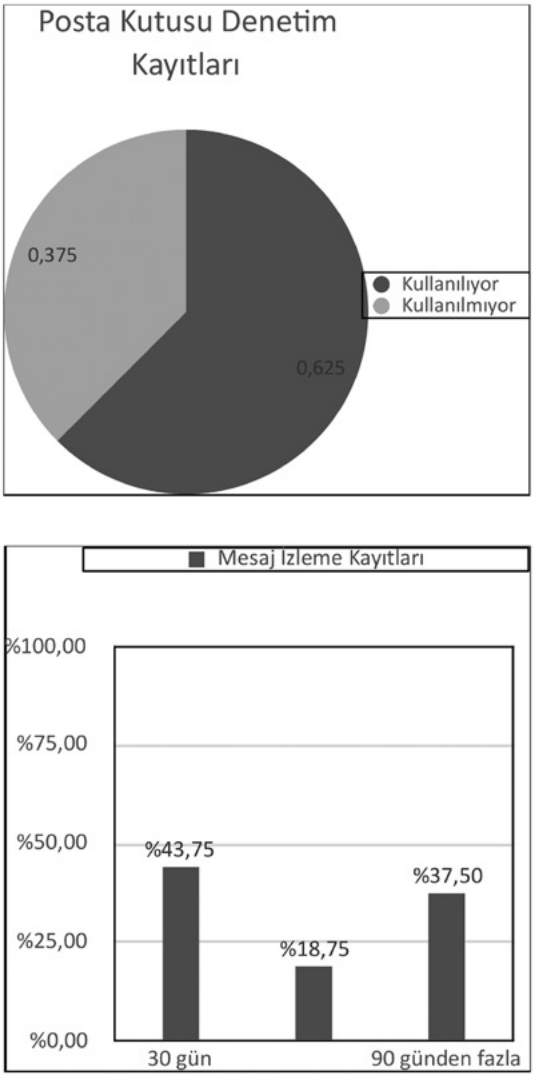
Ankete katılan teşebbüslerin sistem yöneticilerinin, elektronik posta sunucularındaki *mesajlaşma trafiği kayıtları* ve *posta kutusu denetim kayıtları* parametrelerini ne şekilde yapılandırdıklarına ilişkin detaylar şu şekildedir:

Posta Kutusu Denetim Kayıtları	Frekans (f)	Yüzde (%)
Kullanılıyor	10	62,5%
Kullanılmıyor	6	37,5%

Tablo 3: Posta Kutusu Denetim Kayıtlarının Kullanım İstatistiği

Mesaj İzleme Kayıtları	Frekans (f)	Yüzde (%)
30 gün	7	43,75%
30-90 gün arası	3	18,75%
90 günden fazla	6	37,50%

Tablo 4: Mesaj İzleme Kayıtlarının Saklanma Süresi İstatistiği



Grafik 2: Posta Kutusu Denetim Kayıtları Kullanımı ve Mesaj İzleme Kayıtlarının Saklanma Süresi İstatistikleri

Yİ'ler esnasında incelenecek posta kutularının tespiti konusunda aktif rol alabileceği düşünülen *mesajlaşma trafiğine ilişkin kayıtların*, ankete katılan teşebbüslerin %43'ünde, en fazla 30 günlük süreyle saklandığı görülmektedir. Benzer şekilde, Yİ'lerde analiz edilen posta kutuları üzerinde, inceleme süresince gerçekleştirilen yapılandırma ayarlarındaki değişikliklerin tespit edilebilmesini sağlayan *posta kutusu*

denetim kayıtları özelliğinin de %37,5'luk oranla kullanılmıyor oluşu, dikkat çekici bir diğer durum olarak değerlendirilmektedir.

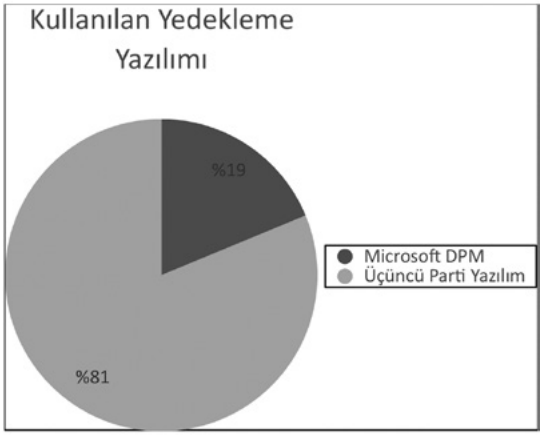
Anket sonuçlarına göre, elektronik posta kutularının yedeklenmesi konusunda teşebbüslerin belirledikleri politikaların Tablo 5'deki gibi olduğu tespit edilmiştir:

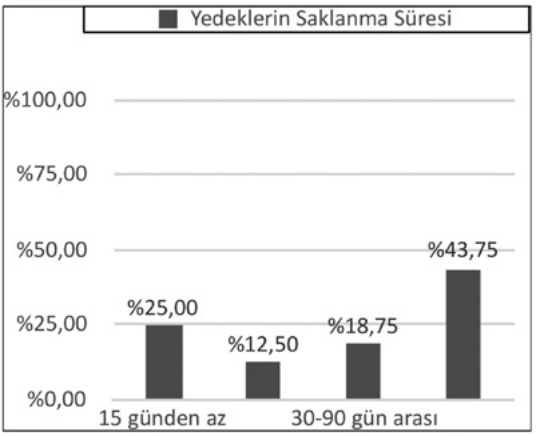
Kullanılan Yedekleme Yazılımı	Frekans (f)	Yüzde (%)
Microsoft DPM	3	19%
Üçüncü Parti Yazılım	13	81%

Tablo 5: Elektronik Posta Kutularının Yedeklenmesinde Kullanılan Yazılımlar

Yedeklerin Saklanma Süresi	Frekans (f)	Yüzde (%)
15 günden az	4	25%
15-30 gün arası	2	12,50%
30-90 gün arası	3	18,75%
90 günden fazla	7	43,75%

Tablo 6: Elektronik Posta Kutularının Yedeklerinin Saklanma Süresi





Grafik 3: Elektronik Posta Kutularının Yedeklenmesinde Kullanılan Yazılım ve Yedeklerin Saklanma Süresine İlişkin İstatistik

Ankete katılan tüm teşebbüslerde, posta kutularının yedeklendiği görülse de, teşebbüslerin %37'sinde alınan yedeklerin 30 günden daha kısa süreyle saklanıyor oluşu, kurumsal yedeklerden silinmiş elektronik postaların ancak sınırlı periyotlar dâhilinde kurtarılabileceği sonucunu doğurmaktadır.

Anket çalışması sonucunda elde edilen verilerin, sistem yöneticilerinin elektronik posta sunucuları üzerinde uyguladıkları yapılandırma ayarlarındaki farklılıklar nedeniyle, ikinci bölümün sonunda vurgulanan Exchange sunucu özelliklerinin, her Yİ'de tam performansla kullanılamayacağı yönündeki düşüncemizi destekler nitelikte olduğu görülmüştür. Bu noktadan hareketle, Yİ'lerde hedeflenen başarımın elde edilebilmesi için bahsi geçen özelliklerin tek başına kullanımının yeterli olmadığı, incelemelerin elektronik posta analizi yapabilen adli bilişim araçlarıyla desteklenmesi gerektiği düşünülmektedir.

4.2. AVRUPA BİRLİĞİNE ÜYE ÜLKELERİN REKABET OTORİTELERİNDE ADLİ BİLİŞİM ARAÇLARININ KULLANIMI

Avrupa Birliğine üye ülkelerin rekabet otoritelerinin Yİ'lerde adli bilişim aracı kullanım durumları incelendiğinde; Kurum'un benimsediği mevcut usulden farklı

olarak, rekabet otoritelerinin %91'inin[79] Yİ'ler esnasında ya da sonrasında en az bir adli bilişim aracı kullandığı görülmektedir. Otoritelerce kullanılan adli bilişim araçlarının tamamının elektronik posta analiz kabiliyeti olmasına karşın, her beş otoriteden birisi elektronik posta analizi konusunda uzmanlaşmış ilave bir yazılım[80] daha kullanmaktadır.

Komisyon'da da, üye ülkelerin rekabet otoritelerinin birçoğunda olduğu gibi, elektronik ortamda saklanan teşebbüslere ait verilerin analizi için adli bilişim araçlarından yardım alınmaktadır. 2006 yılından bu yana, Komisyon'un yürüttüğü soruşturmalardaki Yİ faaliyetlerinde görev alan adli bilişim grubu, elektronik verilerin analizi amacıyla NUIX yazılımını kullanmaktadır (Erps ve Doury 2013, 213). Komisyonla birlikte, AB'ye üye ülkelerin rekabet otoritelerinin dokuzunun daha envanterinde bulunan bu aracın bu denli popüler oluşu; tezin üçüncü bölümünde yer verilen adli bilişim araçlarının karşılaştırıldığı testteki başarımının tesadüf olmadığına kanıt olarak gösterilebilir.

Komisyon bünyesinde çalışan adli bilişim grubunu Yİ'lerde takip ettiği usul incelendiğinde, teşebbüs çalışanlarının bilgisayarlarından belirli tipteki dokümanların[81] *ayrıştırılarak*, analiz ve *indeksleme* amacıyla, donanımsal olarak oldukça güçlü bir dizüstü bilgisayara kurulmuş NUIX yazılımına (*NUIX sunucusu*) kopyalandığı görülmektedir. İndekslemenin tamamlanmasıyla birlikte, incelemeye katılan uzmanlar, kendi dizüstü bilgisayarlarındaki "NUIX Web Review & Analytics" bileşeni üzerinden NUIX sunucuya bağlanmak suretiyle anahtar kelime arama işlemini gerçekleştirmektedir. Uzmanlarca tespit edilen, rekabet ihlaliyle ilişkili dosyalar kriptolanmış veri taşıyıcılara (DVD, USB sürücü, sabit sürücü) kopyalanmakta, kopyalanan dosyaların *hash* değerlerini de içeren liste teşebbüs yetkilisi ve incelemeye katılan uzman tarafından imzalanarak kayıt altına alınmaktadır (A.g.k., 214). Komisyonca benimsenen bu prosedür sayesinde, teşebbüse

[79] Çalışmanın bu kısmında verilen, adli bilişim araçlarının kullanımına ilişkin istatistikler; 29.04.2014 tarihinde Roma'da düzenlenen "Avrupa Antitröst Adli Bilişim Araçları Projesi 1. Çalıştayı"'na katılan ülkelerin yapmış olduğu sunumlardan derlenmiştir. Detaylı bilgi için bkz. http://eafit-tools.matfis.uniroma3.it/~eafit_tools_repo/requestRM3.php?reqhash=21de0683e456fefccd382a823e7deb72aa5bf8d7 Erişim Tarihi: 05.04.2016

[80] Intella, Paraben.

[81] Bazı istisnai durumlarda, incelenen bilgisayarlardan belirli tipteki dosyalar yerine sabit sürücünün tamamının adli kopyası alınabilmektedir. Böyle durumlarda, imaj dosyasının kaydedildiği kriptolu veri taşıyıcısı zarfa konup mühürlenerek, Brüksel'deki merkeze götürülmektedir. İmaj dosyası burada, teşebbüs temsilcilerinin eşliğinde analiz edilmektedir. Bu süreç "Mühürlü Zarf Prosedürü olarak adlandırılmaktadır (A.g.k. 214).

ait verilerin dışarı çıkmasına gerek kalmaksızın (istisnai durumlar hariç), hızlı ve kapsamlı bir Yİ gerçekleştirmek mümkün olmaktadır.

4.3. REKABET KURUMU AÇISINDAN DEĞERLENDİRMELER

Meslek personelince gerçekleştirilen Yİ'lerde etkin bir elektronik posta analizi yapabilmek için adli bilişim aracı kullanılması gerektiğine dair düşüncemize, gerekçeleriyle birlikte çalışmanın önceki bölümünde değinmiştik. Böyle bir gereklilik olduğu düşünülmesine karşın, mevcut Kurul uygulamasında, Yİ'lerde herhangi bir adli bilişim aracı kullanılamamaktadır. Bu tercihin dayanağının, yetkisizlikten ziyade Yİ yetkisinin sınırlarındaki belirsizlikten kaynaklandığı düşünülmektedir.

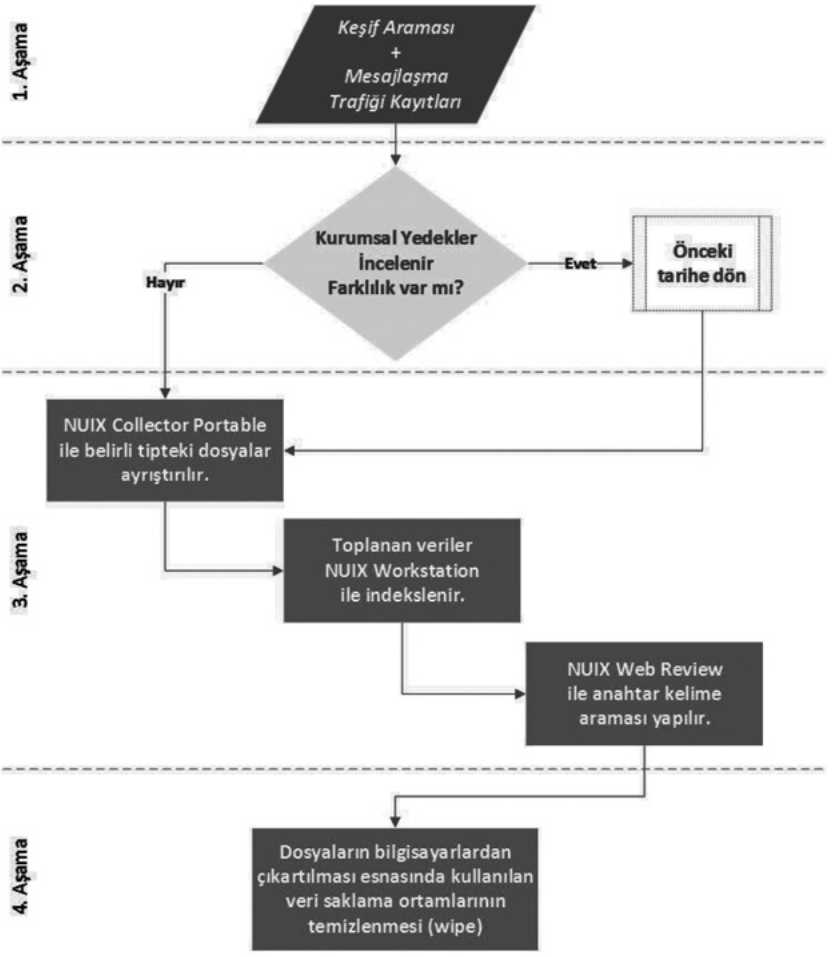
Yİ süreçlerinde aktif ve başarılı bir biçimde adli bilişim araçlarını kullanan Komisyon'un, Yİ yetkisinin dayanağı incelendiğinde, Kanun'un ilgili maddesinin lafzıyla paralellik içerdiği değerlendirilmektedir. Komisyon'un Yİ yetkisinin hukuki dayanağına "1/2003 Sayılı Tüzüğün[82] 20. Maddesinin 2. Fıkrasında" yer verilmektedir. İlgili maddenin (b) bendinde, her türlü ortamda saklanan işle ilgili belge ve kayıtların incelenebileceği belirtilmektedir. Yine aynı maddenin (c) bendinde ise, (b) bendinde belirtilen belge ve kayıtlardan ayrıştırılan her çeşit kopyanın alınabileceği bildirilmektedir. Son olarak 11 Ekim 2015 tarihinde güncellenen ve Komisyon'un Yİ'lerde takip edeceği işlem adımlarına ilişkin detayları içeren bilgi notunda[83], teşebbüslere ait bilişim altyapısı üzerinde adli bilişim araçları kullanmak suretiyle inceleme yapılabileceği belirtilmektedir.

Kurulun Yİ yetkisinin hukuki dayanağı irdelendiğinde, bu yetkinin RKHK'nin 15. maddesinden alındığı görülmektedir. İlgili maddenin (a) bendinde: *"(Kurul, teşebbüslerin ve teşebbüs birliklerinin) Defterlerini, her türlü evrak ve belgelerini inceleyebilir ve gerekirse suretlerini alabilir*" denilmektedir. Bu ifadenin, Komisyon'a ait düzenlemedeki kadar açık bir şekilde kaleme alınmamış olmasının; Yİ'lerde adli bilişim araçlarının kullanılamayışının nedeni olduğu düşünülmektedir. Hukuki belirlilik ve şeffaflığın sağlanabilmesi amacıyla, gerekli birincil ve ikinci düzenlemelerin

[82] COUNCIL REGULATION (EC) No 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.
[83] 1/2003 Sayılı Tüzüğün 20. Maddesinin 4. Fıkrası Kapsamında Gerçekleştirilen İncelemelere İlişkin Bilgi Notu http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf, Erişim Tarihi: 05.04.2016.

ivedilikle hayata geçirilerek, Yİ'lerde adli bilişim aracı kullanımının önünün açılması gerektiği savunulmaktadır. Meslek personelince, etkili bir elektronik posta analizinin ancak bu şekilde yapılabileceği düşünülmektedir.

Yİ'lerde takip edilmesi önerilen süreç modeli, Kurumun incelemeler esnasında adli bilişim aracı kullanabileceği varsayımı altında oluşturulmuştur. Bu modelde, tezin ikinci bölümünün sonunda vurgulanan işlem adımlarıyla, adli bilişim aracının (NUIX) ortak kullanımından doğan hibrit bir süreç önerilmektedir. Böylelikle her iki yaklaşımın olumlu yönleri birleştirilerek etkin bir elektronik posta analiz yöntemi oluşturulacağı düşünülmektedir. Kullanımı önerilen süreç modeline ilişkin iş-akış diyagramı şu şekildedir:



Şekil 22: Elektronik Posta Analizinde Kullanılması Önerilen Hibrit Süreç Modeline İlişkin İş-Akış Diyagramı

Süreç modelinin ilk aşaması, bir önceki modelde olduğu gibi, posta kutuları incelenecek teşebbüs çalışanlarının doğru şekilde tespiti amacıyla *keşif araması* ve *mesajlaşma trafiği kayıtlarının* kullanımından oluşmaktadır. İkinci aşama, incelenecek posta kutularından çok sayıda elektronik postanın inceleme öncesinde silinip silinmediğinin, kurumsal yedekler aracılığıyla kontrol edilmesinden ibarettir[84].

[84] Tekrardan kaçınmak amacıyla, ikinci bölümün sonunda detaylıca işlenen ilk iki adıma ilişkin ayrıntılara bir kez daha değinilmeyecektir.

Üçüncü aşama, NUIX'e ait bileşenlerin aktif olarak kullanıldığı işlem adımlarından oluşmaktadır. Öncelikle, "NUIX Collector Portable" bileşeni aracılığıyla, inceleme yapılacak teşebbüs çalışanlarının bilgisayarlarından PST ve OST uzantılı dosyaların ayrıştırılması işlemi gerçekleştirilir[85]. Veriler bu yöntemle elde edildikten sonra, kullanıcılar posta kutuları üzerinde değişiklik yapsalar dahi, ayrıştırılan dosyalar bu değişikliklerden etkilenmeyecektir. Bir önceki modelde bulunan, incelemenin yapıldığı esnada elektronik postaların silinmesi durumunda, silinen ögelerin kurtarılmasını ve silme eyleminin ispat edilmesini sağlayan üçüncü aşamaya gerek kalmamaktadır. Bu nedenle, *tek* öge *kurtarma* ve *denetim kayıtları* özelliklerinin aktifleştirilmesi işlemlerine mevcut süreç modelinde yer verilmemiştir. Bir sonraki adımda, ayrıştırılan veriler "NUIX Sunucu (Workstation bileşeni)" üzerinde indekslenerek anahtar kelime araması yapılabilecek hale getirilir. Posta kutularından, *ikinci* veya üçüncü seviye silinmiş ögeler NUIX tarafından kurtarılabildiği[86] için, incelemeye başlamadan önce *keşif araması* yardımıyla *kurtarılabilir* öge*ler klasörünün* kullanıcı posta kutusuna kopyalanması işlemine ihtiyaç duyulmamaktadır. Üçüncü aşamanın son adımında ise, "NUIX Web Review" bileşeni ile NUIX sunucuya eş zamanlı olarak bağlanan meslek personeli, anahtar kelime araması işlemini gerçekleştirirler. Bulunan deliller, hash değerleri alındıktan sonra kriptolu sürücülere kaydedilerek, basılı kopya alınmasına gerek kalmaksızın Kurum merkezine götürülebilir.

Dördüncü ve son aşamada ise, inceleme süresince kullanılan veri depolama aygıtlarının temizlenmesi (wipe) işlemi uygulanır. Böylelikle, teşebbüse ait ve ihlalle alakası olmayan verilerin, sürücüler üzerinden bilinen hiçbir teknikle geri kurtarılamayacak şekilde tamamen silinmesi sağlanır (Erps ve Doury 2013, 214).

[85] Önerilen süreç modeli, NUIX Collector Portable'da bulunan, ayrıştırılacak dosya tiplerinin belirlendiği alanda, PST ve OST ile birlikte ofis dosya uzantıları, PDF ve TXT gibi karakter dizileri içeren diğer dosya türlerinin de seçilmesiyle, elektronik posta analizi yapılan bir süreç olmaktan çıkarılarak, elektronik ortamda saklanan tüm verileri kapsar hale getirilebilir.

[86] Tezin üçüncü bölümünün sonunda yapılan testte, NUIX'in *ikinci* ve üçüncü seviye silinmiş elektronik postaları kurtarabildiği görülmüştür.

SONUÇ

Yİ'lerde rekabet ihlallerine ilişkin delillerin elde edilmesinin gün geçtikçe zorlaştığı gerçeğinden hareketle; meslek personelinin takip ettiği inceleme yönteminin gözden geçirilerek iyileştirilmesi gerektiği düşünülmektedir. Bu nedenle, Yİ'nin en önemli adımı olduğu savunulan elektronik posta analizi aşamasının geliştirilmesi amacıyla, tez kapsamında iki farklı süreç modeli önerisinde bulunulmuştur.

İlk model, Kurulun mevcut Yİ yetkisi ve meslek personelinin uyması gereken YİY gözetilerek oluşturulmuştur. Elektronik postaların analizi esnasında herhangi bir araç kullanılmaksızın uygulanabilecek bu modelde; inceleme öncesinde veya inceleme esnasında delil karartmak amacıyla elektronik postaların silinme ihtimali, posta kutuları incelenen teşebbüs çalışanlarının doğru tespit edilip edilmediği gibi endişeleri giderecek işlem adımlarına yer verilmiştir. Exchange sunucularda bulunan, *tek* öge *kurtarma*, *koruma*, *keşif araması*, *mesaj izleme kayıtları*, *posta kutusu* ve *yönetici denetim kayıtları* özelliklerinin belirli bir sıra ve bütünlük içinde kullanıldığı süreç modeli ile meslek personelinin Yİ etkinliğinin arttırılması hedeflenmiştir.

Tez içerisinde yer verilen, ilk modelde kullanılan Exchange sunucu özelliklerinin, ön tanımlı yapılandırma ayarlarından kaynaklanan sebeplerle, her teşebbüste eşit etkinlikte kullanılamayacağı ön görüsü; yapılan anket çalışmasıyla da doğrulanmıştır. Bu veriler ışığında, Yİ'lerde elektronik posta analizi başarımını, Exchange sunucu konfigürasyonu bağımlılığından kurtaracak, alternatif bir yaklaşım sergilenmesi gerektiği sonucuna ulaşılmıştır. Doğru modelin, birçok rekabet otoritesinde başarıyla uygulanan, Yİ'lerde adli bilişim aracı kullanımıyla kurulabileceği düşünülmektedir. Tezin üçüncü bölümünde yer verilenen örnek vaka çalışması ile elektronik posta analizi konusunda adli bilişim araçlarının, klasik yöntemlere göre üstünlüğün açık biçimde

ortaya konmuştur. Örnek vaka çalışmasındaki başarımı ve rekabet otoriteleri tarafından yaygın kullanımı göz önünde bulundurulduğunda, merkezinde NUIX yazılımının olduğu ikinci bir süreç modeli tasarlanmıştır. Bu yeni modele, tamamlayıcı unsur olarak, ilk modeldeki *keşif araması*, *mesaj izleme kayıtları* ve kurumsal posta kutusu yedekleri kavramları bütünleştirilerek, elektronik posta analizi konusunda kullanılması önerilen nihai, hibrit süreç modeline son hali verilmiştir.

Bu çalışma neticesinde, meslek personelinin Yİ'lerde elektronik postaların analizi konusunda takip etmesi önerilen süreç modeli, gerekçeleriyle birlikte ortaya konmaya çalışılmıştır. Önerilen bu modelin, eksiksiz bir biçimde uygulanabilmesi amacıyla, Yİ'lerde adli bilişim aracı kullanılabilmesinin önünü açacak yasal düzenlemelerin ivedilikle hayata geçirilmesi gerektiği düşünülmektedir.

ABSTRACT

Email is a ubiquitous and essential way of communication in the modern-day business environment. Due to this widespread usage, analyzing emails plays a significant role during dawnraids. In order to avoid missing substantial digital evidences which can be located in the mailboxes, an accurate approach for examining emails must be implemented by competition experts. This paper aims to determine the steps of the email analyzing procedure to be followed by the Turkish Competition Authority during dawnraids.

The current procedure of the Turkish Competition Authority which is applied at dawnraids does not include usage of the forensics tools. Towards this direction, the properties of Microsoft Exchange Server such as single item recovery, in-place hold, litigation hold, in-place eDiscovery, message tracking logs and audit logs can be theoretically used to improve the digital evidence gathering process from mailboxes. However, since most of these properties are not enabled by default, the proposed methods cannot be used with the same efficiency in every undertaking.

In order to overcome this limitation in analyzing emails during dawnraids, a hybrid procedure which combines Microsoft Exchange properties and forensics tools is recommended to be followed.

KAYNAKÇA

AKYOL, F. (2013), "Cobit (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri) Uygulayan Şirketlerdeki Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçlere Etkileri", Yayımlanmamış Yüksek Lisans Tezi, Beykent Üniversitesi, İstanbul.

ANDERSSON, J. ve M. PFEIFFER (2015), Microsoft Exchange Server PowerShell Cookbook, Third Edition, Packt Publishing, Birmingham.

ARAS, S. (2008), "Tersine Mühendislik Yöntemlerini Kullanarak. Net Çevrelerinde Kaynak Koda Dönüşüm ve Dosya Sistemi İşlemlerinin Kontrolü", Yayımlanmamış Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Trabzon.

BAKAN, M. ve A. SALUK (2014), "Adli Bilişimde Kullanılan Ekipmanlar", ÇAKIR H. ve S. KILIÇ (der.), *Adli Bilişim ve Elektronik Deliller* içinde, Seçkin Yayıncılık, Ankara, s.199-257.

BANDAY, M. T. (2011a), "Techniques And Tools For Forensic Investigation Of E-Mail", *International Journal of Network Security & Its Applications (IJNSA)*, Vol:3, No:6, s.227-241.

BANDAY, M. T. (2011b), "Analysing E-Mail Headers for Forensic Investigation", *Journal of Digital Forensics, Security and Law*, Vol:6, No:2, s.49-64.

CHHABRA, G. S. ve D. S. BAJWA (2015), "Review of E-mail System, Security Protocols and Email Forensics", *International Journal of Computer Science and Communication Networks*, Vol:5, No:3, s.201.211.

CRISPIN, M. (1994), "Internet Message Access Protocol - Version 4, , RFC 1730", University of Washington, https://tools.ietf.org/html/rfc1730, Erişim Tarihi: 05.04.2016

CROCKER, D. (2009), "Internet Mail Architecture, RFC 5598", Brandenburg InternetWorking, https://tools.ietf.org/html/rfc5598, Erişim Tarihi: 05.04.2016

ÇAKIR, H. ve M. S. KILIÇ (2013), "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", *Polis Bilimleri Dergisi*, Vol:15, No:3, s.23-44.

DEMİRSÖZ, O. (2009), "Metin Dosyaları İçin Arayıcı", Yayımlanmamış Yüksek

Lisans Tezi, Gazi Üniversitesi, Ankara.

DEVENDRAN, V. K., H. SHAHRIAR, V. CLINCY (2015), "A Comparative Study of Email Forensic Tools", *Journal of Information Security*, No:6, s.111-117.

DOSTÁLEK, L. ve A. KABELOVÁ (2006), DNS in Action: A Detailed And Practical Guide To Dns Implementation, Configuration, And Administration, Packt Publishing, Birmingham.

DULKADİR B. ve B. AKKOYUN (2013), "Bilişim Teknolojilerinin İşletme Performansı Üzerine Etkileri ve Gaziantep İlinde Tekstil Sektöründe Bir Araştırma", *Sosyal Bilimler Elektronik Dergisi*, No:7, s.72-90.

DURMAZ, Ş. (2014), "Elektronik Verilerin Delillendirilmesi", ÇAKIR H. ve S. KILIÇ (der.), *Adli Bilişim ve Elektronik Deliller* içinde, Seçkin Yayıncılık, Ankara, s.271-305.

ELFASSY, D. (2013), Mastering Microsoft Exchange Server 2013, Sybex, Indiana.

ERPS, D. V. ve N. J. DOURY (2013), "Digital Evidence Gathering: An Up-Date", *Concurrences*, No:2-2013, 213-219.

GUO, H., B. JIN ve W. QIAN (2013), "Analysis of Email Header for Forensics Purpose", International Conference on Communication Systems and Network Technologies 2013, India, s.341-344.

HALLBERG, B. (2014), Networking A Beginner's Guide, Sixth Edition, McGraw-Hill Education, New York.

HENKOĞLU, T. (2014), "Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi", İkinci Baskı, Pusula, İstanbul.

KLENSIN, J. (2008), "Simple Mail Transfer Protocol, RFC 5321 (Draft Standard)", Internet Engineering Task Force, http://www.ietf.org/rfc/rfc5321.txt, Erişim Tarihi: 05.04.2016

LAROCHE, P., A. N. ZİNCİR ve M. I. HEYWOOD (2011), "Exploring the State Space of an Application Protocol: A Case study of SMTP", Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium, Paris, s.152-159.

MARAS, M. H. (2011), Computer Forensics: Cybercriminals, Laws, and Evidence, Jones & Bartlett Learning, Sudbury.

MARKAGIĆ, M. (2013), "Electronic Mail Forensics", *Military Technical Courier*, Vol:61, No:3, s.113-121.

METZ, J. (2009), "Personal Folder File (PFF) Forensics: Analyzing the Horrible Reference File Format", https://da1ba3cfdffc2404250f16d3711dfb32dcd40e96.googledrive.com/host/0B3fBvzttpii ScU9qcG5ScEZKZE0/PFF%20

Forensics%20-%20analyzing%20the%20horrible%20reference%20file%20format.pdf, Erişim Tarihi: 05.04.2016

MORIMOTO, R., M. NOEL, G. YARDENI, C. AMARIS ve A. ABBATE (2012), Microsoft Exchange Server 2013 Unleashed, Sams, Indiana.

MOTA, N. (2014a), "Exchange 2013 In-Place Hold and In-Place eDiscovery", http://www.msexchange.org/articles-tutorials/exchange-server-2013/compliance-policies-archiving/exchange-2013-place-hold-and-place-ediscovery-part1.html, Erişim Tarihi: 05.04.2016

MOTA, N. (2014b), "Exchange 2013 In-Place Hold and In-Place eDiscovery", http://www.msexchange.org/articles-tutorials/exchange-server-2013/compliance-policies-archiving/exchange-2013-place-hold-and-place-ediscovery-part2.html, Erişim Tarihi: 05.04.2016

MYERS, J. ve M. ROSE (1996), " Post Office Protocol - Version 3, , RFC 1939 (Standard)", Dover Beach Consulting, https://www.ietf.org/rfc/rfc1939.txt, Erişim Tarihi: 05.04.2016

ORTA, M. (2015), "Bilişim Suçlarında Adli Analiz", Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi, Konya.

OTMAN, M. F. (2014), "CPN Tools Programı Kullanılarak SMTP (Basit Posta Aktarım Protokolü)'nin Modellenmesi", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul.

ÖNAL, H. (2009), "E-posta (Mail) Başlık Bilgileri: E-posta Başlıklarından Bilgi Toplama", www.bga.com.tr/calismalar/mail_headers.pdf, Erişim Tarihi: 05.04.2016

PAGLIERANI, J., M. MABEY ve G. J. AHN (2013), "Towards Comprehensive and Collaborative Forensics on Email Evidence", 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing, Texas.

PASUPATHEESWARAN, S. (2008), "Email Message-IDs Helpful for Forensic Analysis?", 6th Australian Digital Forensics Conference, Perth.

PAYEL, H. (2014), "MD5 Hash değerinin Hukuken geçerliliği Sorunu", *Adli Bilişim Dergisi*, No:1, s.12.

PIAZZA, L. (2013), "The Revision of the Commission Explanatory Note on European Commission Surprise Inspections", *Journal of European Competition Law & Practice*, Vol:4, No:5, s.421-423.

POSTEL, J. (1982), "Simple Mail Transfer Protocol, RFC 821 (Standard)", Internet Engineering Task Force, http://www.ietf.org/rfc/rfc821.txt, Erişim Tarihi: 05.04.2016

ROOKSBY, J. H. (2015), "Defining Domain", *Brooklyn Law Review*, Vol:80, No:3, s.857-942.

SHAFRANOVICH, Y. (2005), "Common Format and MIME Type for Comma-Separated Values (CSV) Files, RFC 4180", SolidMatrix Technologies, https://tools.ietf.org/html/rfc4180#section-2, Erişim Tarihi: 05.04.2016

SOMMER, P. (2013), "Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers", Fourth Edition, IAAC, Swindon.

STADEN, F. R. V. ve H. S. VENTER (2010), "Adding Digital Forensic Readiness To The Email Trace Header", Information Security for South Africa (ISSA), 2010 IEEE Conference, Johannesburg.

ŞAHİN, N. (2014), Exchange Server 2013, Kodlab Yayın Dağıtım, İstanbul.

ŞİRİKÇİ, A. S. (2013), "Veri Kurtarma Açısından Açık Kaynak Kodlu ve Kapalı Kaynak Kodlu Yazılımların Karşılaştırılması", Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi, Ankara.

WESSELIUS, J. (2013), Pro Exchange Server 2013 Administration, Apress, New York.

Rekabet Kurulu Kararları

18.07.2013 tarihli ve 13-46/601-M sayılı Kurul kararı (*TTNET*).

08.03.2013 tarihli ve 13-13/198-100 sayılı Kurul kararı (*Bankacılık*).

06.04.2012 tarihli ve 12-17/499-140 sayılı Kurul kararı (*Doğu Anadolu Çimento*).

06.06.2011 tarihli ve 11-34/742-230 sayılı Kurul kararı (*Turkcell*).

18.04.2011 tarihli ve 11-24/464-139 sayılı Kurul kararı (*Otomotiv*).

07.03.2011 tarihli ve 11-13/243-78 sayılı Kurul kararı (*Banka Promosyon*).

Komisyon Kararı

Case COMP/39793 - EPH and others, 28.03.2012

Diğer Kaynaklar

Eafit Tools (2014), "European Antitrust Forensic IT Tools Project Stakeholders", http://www.eafit-tools.eu/stakeholders, Erişim Tarihi: 05.04.2016

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, Erişim Tarihi: 05.04.2016

McAfee (2013), "The Economic Impact of Cybercrime and Cyber Espionage Report", http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf, Erişim Tarihi: 05.04.2016

Microsoft Technet (2015a), "Recoverable Items Folder", https://technet.microsoft.com/en-us/library/ee364755(v=exchg.150).aspx, Erişim Tarihi: 05.04.2016

Microsoft Technet (2015b), "Keyword Query Language (KQL) Syntax Reference", https://msdn.microsoft.com/en-us/library/office/ee558911.aspx, Erişim Tarihi: 05.04.2016

Microsoft Technet (2014), "Configure the Managed Folder Assistant", https://technet.microsoft.com/en-us/library/bb123958(v=exchg.150).aspx, Erişim Tarihi: 05.04.2016

Microsoft Technet (2013), "Search Message Tracking Logs", https://technet.microsoft.com/en-us/library/bb124926(v=exchg.150).aspx, Erişim Tarihi: 05.04.2016

NUIX (2015a), "Nuix History", http://www.nuix.com/nuix-history, Erişim Tarihi: 05.04.2016

NUIX (2015b), "eDiscovery Best Practices When Dealing with Email Archives", http://www.nuix.com/blog/ediscovery-best-practices-when-dealing-email-archives, Erişim Tarihi: 05.04.2016

NUIX (2015c), "Nuix Web Review & Analytics Fact Sheet", http://www.nuix.com/fact-sheet/nuix-web-review-analytics-fact-sheet, Erişim Tarihi: 05.04.2016

PARABEN (2015), "Paraben's DP2C", https://www.paraben.com/dp2c.html, Erişim Tarihi: 05.04.2016

The Radicati Group (2015), "Email Statistics Report, 2015-2019", http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf, Erişim Tarihi: 05.04.2016

The Radicati Group (2012), "Microsoft Exchange Server and Outlook Market Analysis, 2012-2016", http://www.radicati.com/wp/wp-content/uploads/2012/03/Microsoft-Exchange-Server-and-Outlook-Market-Analysis-2012-2016-Executive-Summary.pdf, Erişim Tarihi: 05.04.2016

Türk Standardları Enstitüsü (2013), "TS ISO/IEC 27001:2013 Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler", TSE, Ankara.

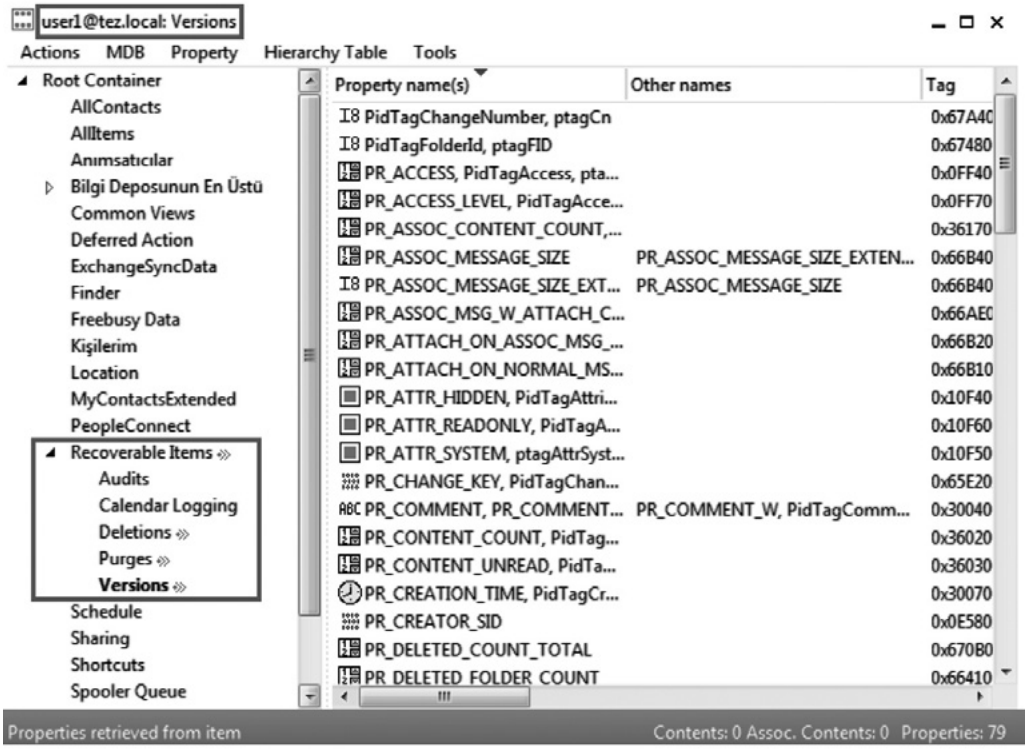
EKLER

EK-1: Kullanılan Yazılımların Versiyon Bilgileri

Yazılım	Versiyon
Microsoft Exchange Server 2013	Version 15.0 (Build 516.32)
Microsoft Outlook 2013	Version 15.0.4569.1503
MFCMAPI	15.0.0.1043
Commvault	?
Foremost	1.5.7
Pffinfo	20131028
Pffexport	20131028
NUIX Workstation Plus	6.2.7
Paraben E-mail Examiner	9.0.8719.6394
EAFIT Evidence Discovery Tool	1.2.9

Tablo 7: Tez İçerisinde Kullanılan Yazılımların Versiyon Bilgileri

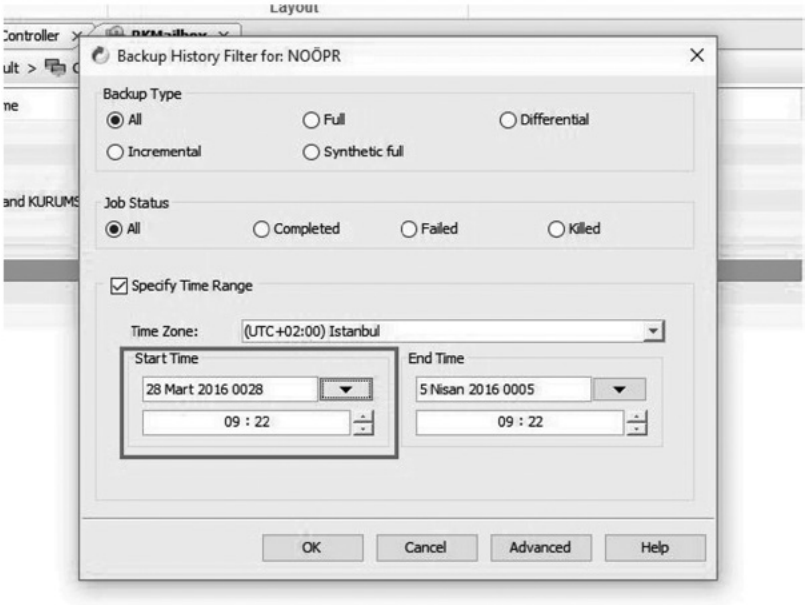
EK-2: MFCMAPI ile Kurtarılabilir Ögeler Klasörünün Görüntülenmesi



Şekil 23: MFCMAPI ile Kurtarılabilir Ögeler Klasörü ve Alt Dizinlerinin Görüntülenmesi

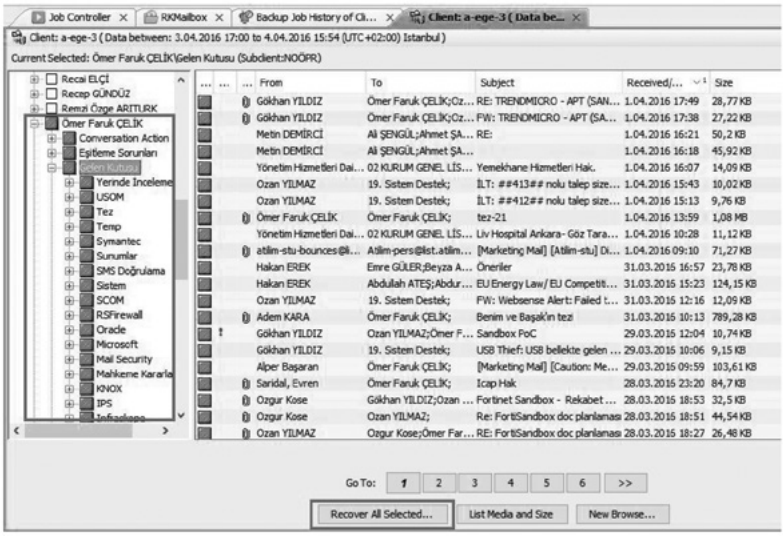
EK-3: Commvault ile Elektronik Posta Kutularının Yedeklenmesi

İlk olarak program ara yüzünden, geri dönülmek istenen yedeklenme tarihi seçilir:



Şekil 24: Commvault, Tarih Seçimi

Bir sonraki adımda, yedeklerine ulaşılmak istenen posta kutusu seçilerek klasörlere ilişkin detaylar incelenir:



Şekil 25: Posta Kutusu Seçimi

Son olarak, seçilen posta kutusu PST formatında istenilen konuma kaydedilir:

Şekil 26: Commvault, PST Olarak Kaydetme

EK-4: Yİ İş Akış Diyagramında Kullanılan Powershell Komutları

Birinci aşamada, *mesajlaşma trafiği kayıtları* üzerinde rakip teşebbüslerin *alan adları* şu powershell komutuyla aratılır:

*echo "`ndate-time `t`t`t event-id `t sender `t`t recipient `t`t`t subject`n"; Select-String -Pattern "**tesebbus1**|**tesebbus2**" -Path "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking*.log" | select -exp line | select-string -pattern "receive" | select -exp line | %{"$($_.Split(',')[0,8,19,12,18] -join '#')"} | Foreach-Object {$_ -replace "#", "`t`t"}*

Üçüncü aşamada, *user1* kullanıcısı için *tek* öge *kurtarma* ve *posta kutusu denetim kayıtları* özellikleri şu şekilde aktifleştirilir:

*Set-Mailbox -Identity **user1** -SingleItemRecoveryEnabled $true*

*Set-Mailbox -Identity **user1** -AuditEnabled $true*

Dördüncü aşamada, iki aşamalı olarak aşağıdaki komutlar yardımıyla *user1* kullanıcısına ait *ikinci* ve üçüncü seviye silinmiş tüm ögeler ve *koruma* altındaki ögeler user1 posta kutusu altındaki *"user1 kurtarılan* öge*ler"* klasörüne kopyalanır:

*Search-Mailbox **user1** -SearchDumpsterOnly -TargetMailbox "Discovery Search Mailbox" –TargetFolder "user1 kurtarılan* öge*ler"*

*Search-Mailbox "Discovery Search Mailbox" -TargetMailbox **user1** -TargetFolder "**user1 kurtarılan** öge**ler**" –DeleteContent*

Altıncı aşamada, posta kutusu ve yönetici denetim kayıtları powershell komutlarıyla şu şekilde sorgulanır:

*Search-MailboxAuditLog -Identity **user1** -LogonTypes Owner -ShowDetails -StartDate 4/1/2016 -EndDate 4/2/2016 | Where-Object {$_.Operation -eq "HardDelete"}*

*Search-AdminAuditLog -ObjectIds **user1** -Cmdlets Set-Mailbox -StartDate 4/1/2016 -EndDate 4/2/2016*

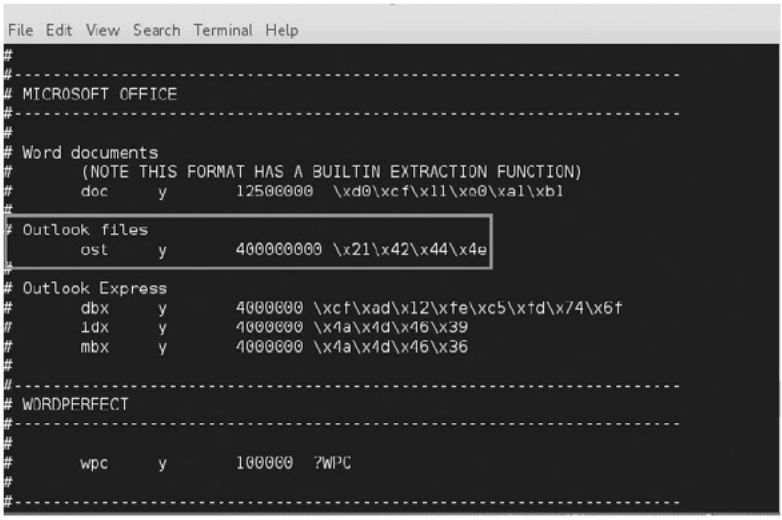
Son aşamada, *user1* kullanıcısı için üçüncü adımda aktifleştirilen *tek* öge *kurtarma* ve *posta kutusu denetim kayıtları* özellikleri şu şekilde kapatılır:

*Set-Mailbox -Identity **user1** -SingleItemRecoveryEnabled $false*

*Set-Mailbox -Identity **user1** -AuditEnabled $false*

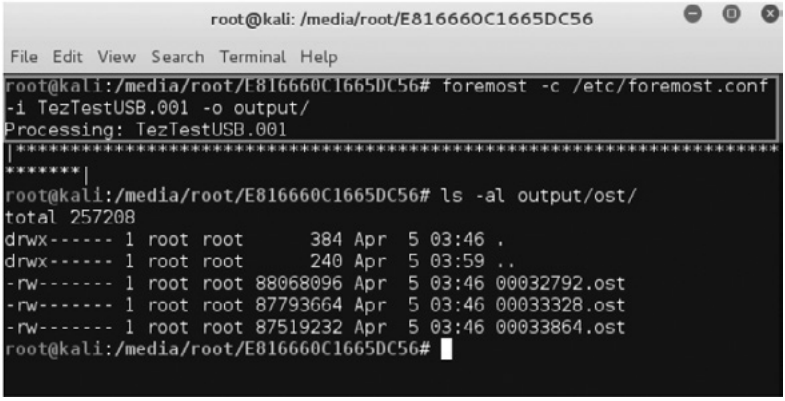
EK-5: Foremost ile Silinmiş PST'lerin Kurtarılması

Foremost ile kazıma işlemini gerçekleştirmeden önce, yapılandırma dosyasındaki PFF dosya tipine ait başlık bilgisi (21 42 44 4e - !BDN) ayarının aktifleştirilmesi gereklidir:



Şekil 27: Foremost Yapılandırma Dosyasındaki PFF İmzası

Yapılandırma dosyası ayarlandıktan sonra Şekil 24'teki komut yardımıyla silinmiş PST dosyası kurtarılır:



Şekil 28: Foremost ile Silinmiş PFF Dosyasının Kurtarılması

EK-6: Adli Bilişim Aracı Performans Testi Sonuçları

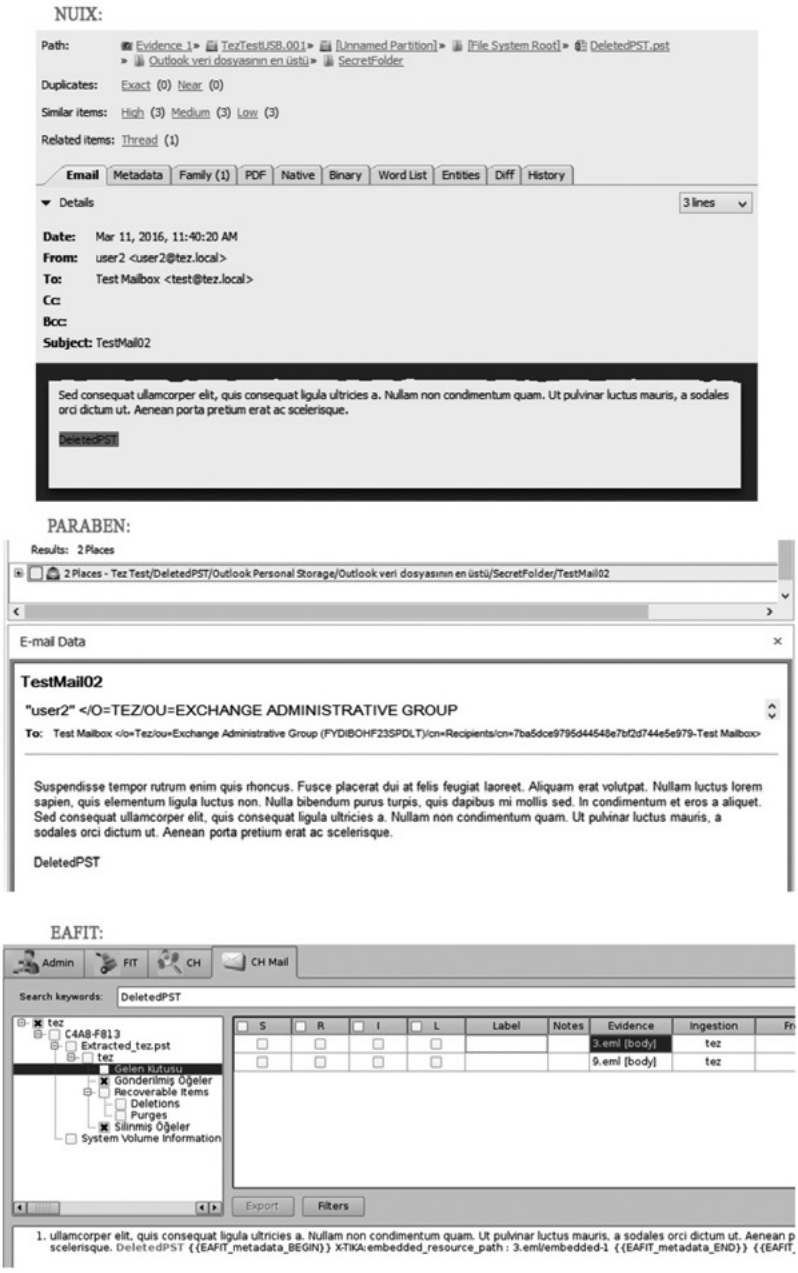
Adli bilişim araçları karşılaştırma testi için hazırlanan elektronik postalar ve anahtar kelimeler şu şekildedir:

Test Edilen Özellik	Konu	Anahtar Kelime
Silinmiş EPD kurtarılabilmesi	TestMail02	DeletedPST
Şifreli PST dosyalarının incelenebilmesi	TestMail01	PasswordProtectedPST
Birinci seviye silinmiş	TestMail03	FirstLevelDeleted
İkinci seviye silinmiş	TestMail04	SecondLevelDeleted
Üçüncü seviye silinmiş	TestMail05	ThirdLevelDeleted
Basit arama operatörleri	TestMail07	Keyword1, Keyword2, Keyword3
Regular Expression	TestMail08	213.14.27.7
Gelişmiş arama operatörleri	TestMail10, TestMail11	Cartel, Kartel

Tablo 8: Karşılaştırma Testinde Kullanılan Elektronik Postalardaki Anahtar Kelimeler

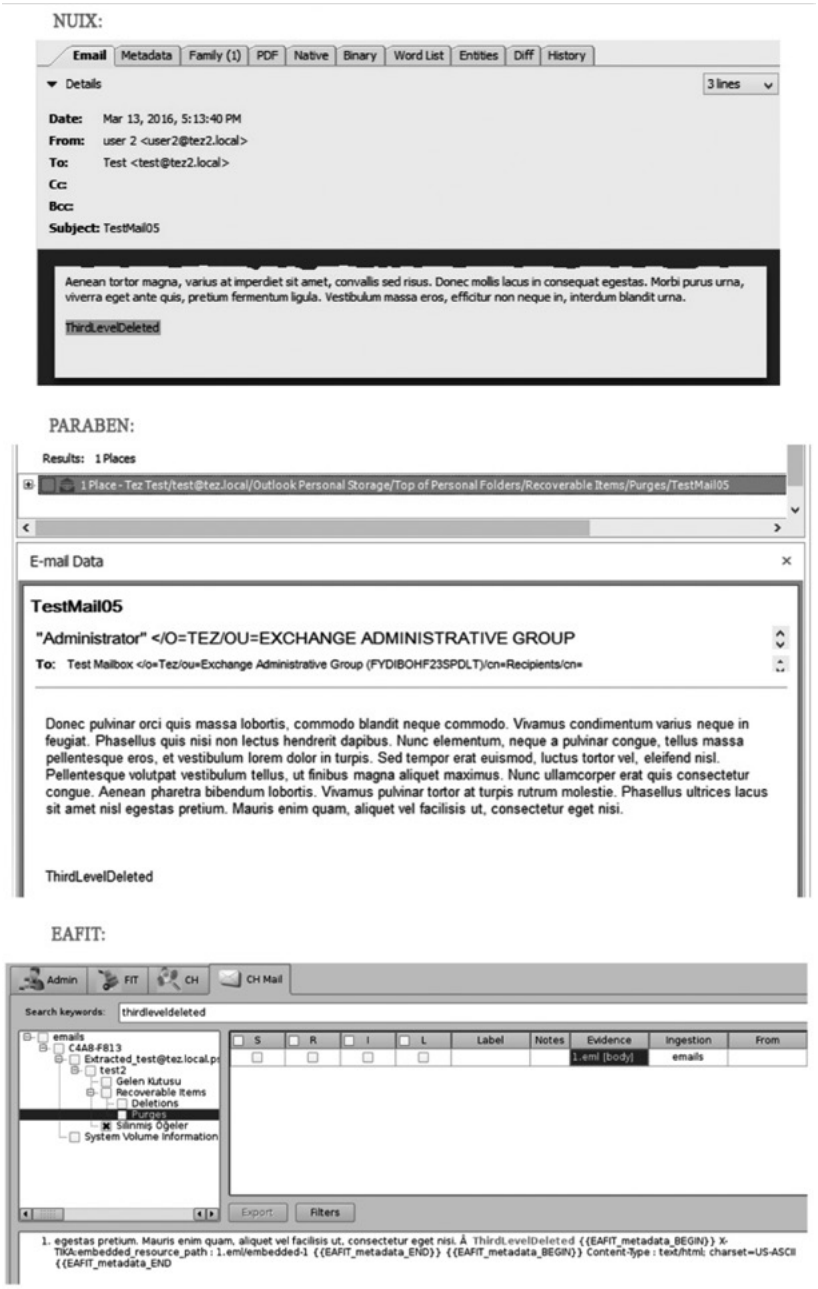
Şekil 29: İndeksleme Hızı

Şekil 30: Doğrudan Elektronik Posta Sunucusu Üzerinde İnceleme



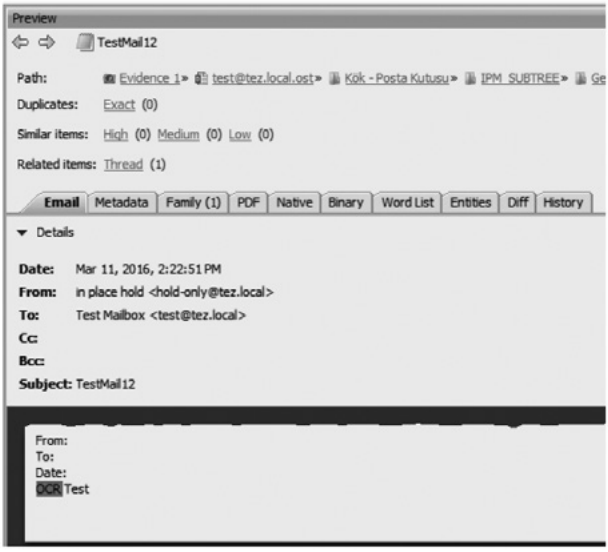
Şekil 31: Silinmiş EPD'nin Kurtarılması

Şekil 32: Şifreli PST Dosyalarının İncelenmesi

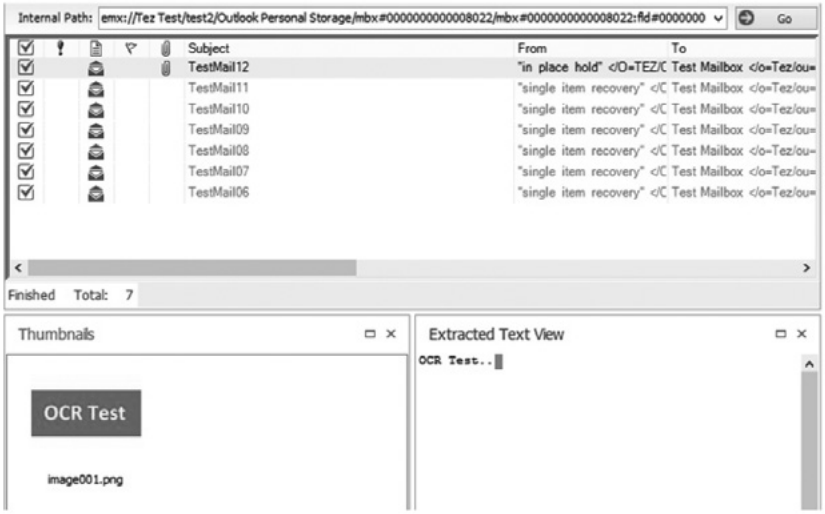


Şekil 33: Silinmiş Elektronik Postaların Kurtarılması

NUIX:



PARABEN:



Şekil 34: OCR Desteği

NUIX:

EAFIT:

Şekil 35: Bulanık Mantık Arama Operatörünün Kullanımı

EK-7: Exchange Sunucu Yapılandırmasına İlişkin Anket Çalışması

Genel Bilgiler

Sektör**(*)**

○ Kamu ○ Özel

Kullandığınız Exchange versiyonu?

○ 2010 ○ 2013 ○ 2016 ○ Diğer

Single Item Recovery Özelliği

Herhangi bir posta kutusu için "Single Item Recovery" özelliğini kullanıyor musunuz?

○ Evet ○ Hayır

"Single Item Recovery" özelliği için "Deleted Item Retention Period" ayarı kaç gün olarak tanımlanmıştır?

○ Varsayılan Değer (14 gün) ○14-30 gün arası ○30-90 gün arası ○90 günden fazla

In-Place Hold / Litigation Hold Özelliği

Herhangi bir posta kutusu için "In-Place Hold" ya da "Litigation Hold" özelliğini kullanıyor musunuz?**(*)**

○ Evet ○Hayır

Hangi tip "Hold" policy uyguluyorsunuz?

☐ Indefinite (Litigation Hold) ☐ Time-based ☐ Query-based

Mailbox Audit Logs Kayıtları

Herhangi bir posta kutusu için "Mailbox Audit Logs" özelliğini aktifleştirdiniz mi?

○ Evet ○ Hayır

Mailbox Audit Logs'da hangi eylemler için loglama yapıyorsunuz?

☐ Create ☐ Update ☐ Move ☐ SoftDelete ☐ HardDelete

Message Tracking Logs Kayıtları

"Message Tracking Logs" sisteminizde kaç gün süreyle tutulmaktadır?

○ Varsayılan Değer ○ (30 gün) ○ 30-90 gün arası ○ 90 günden fazla

Kurumsal Yedekleme

Exchange posta kutularının kurumsal yedeklerini alıyor musunuz?

○ Evet ○ Hayır

Yedekleme için ne tür bir çözüm kullanıyorsunuz?

○ Microsoft DPM ○ 3. Parti Yazılım

Exchange posta kutusu yedekleri kaç gün boyunca saklıyorsunuz?

○ 15 günden az ○ 15-30 gün arası ○ 30-90 gün arası ○ 90 günden fazla

REKABET KURUMU

Üniversiteler Mahallesi
1597. Cadde No: 9
06800 Bilkent/ANKARA
http:// www.rekabet.gov.tr